idb

Crypto…:

самая точная из оккультных наук

kiwibyrd.org

октябрь 2019

kiwi byrd (1998-2018), **idb** (2019)
Crypto…: самая точная из оккультных наук
2019

Криптография и криптоанализ. Криптология, криптоакустика и криптохакинг. Криптовалюта, наконец, в последние годы чуть ли не перетянувшая на себя исходный смысл термина, накрывающего весь необъятный мир защиты информации. Что в корне неверно, конечно же, принимая во внимание младенческий возраст цифровых денег и уходящую вглубь тысячелетий историю крипто как тайнописи. Или как одной из разновидностей оккультных наук и искусства магии.

Собранные здесь тексты рассматривают общеизвестный вроде бы предмет именно под этим нестандартным углом. Поскольку публиковались данные материалы в разное время на протяжении двадцати лет и в существенно разных изданиях, в текстах, конечно же, с неизбежностью встречается немало повторений. Но ничего страшного в этом нет. Скорее даже наоборот, для укрепления душевного здоровья только полезно.

Под душевным здоровьем здесь понимается твердое и отчетливое представление людей о таких абсолютных ценностях, как свобода и достоинство, порядочность и честность. Ну, а если именно такого представления о жизненных ценностях у кого-то из читателей пока еще не сформировалось, что ж…

Быть может, эта книга поможет.

Содержание

Традиционные и открытые формы Магии

Неизвестные страницы известных событий

– Роковая ошибка противника – Автоматизация рыбного хозяйства – Победа, смерть и возрождение]

Параллельные миры. О мистических совпадениях в истории синхронного изобретения криптографии с открытым ключом в секретной спецслужбе и в академическом сообществе.

Правда и вымысел. Необычный монумент Kryptos, украшающий двор штаб-квартиры ЦРУ в Лэнгли, за четверть века успел стать своеобразным олицетворением сути шпионской профессии. [*Тайны Kryptos – Правду говорить трудно – Намек или прямая угроза? – Смерть со многими неизвестными – Убийства без закона – Вместо эпилога: снова о Kryptos*]

Шпион, который пришел из пустыни. В Австралии опубликована мемуарная книга бывшего сотрудника разведслужбы. Как это часто бывает с подобной литературой, книга не столько дает ответы, сколько порождает новые вопросы.

Контакт до и после «Прибытия» . Новый фильм Arrival о первом контакте человечества с инопланетянами практически сразу занесен в разряд шедевров кинофантастики. Разбирательство с секретами успеха картины выводит на чрезвычайно странные факты и документы из истории создания АНБ США… [*Пролог про эпилог — Что обсуждают сейчас — Что было до — Что будет после — Эпилог как пролог*]

Секреты волшебства и их сокрытие

Выпиливание реальности. О мощных и странных взаимосвязях между изощренными шпионскими закладками для компьютеров и природой нашего сознания. [*Плюс Покемоны, минус что? – Минус GSMem, или выпиливание методов доступа – Минус Картье, или выпиливание генерала – Минус криптография и левитация, или выпиливание сути – Как сие понимать, или Знание это сила*]

Секреты дальночувствия. История зарождения и эволюции шпионских технологий TEMPEST [*Вещь в себе – Тайны для двоих – Вещь для всех – О сколько нам открытий чу́дных…*]

Крипто-акустика. Об одном из наиболее экзотичных разделов криптографического анализа [*Мистическое начало – Трудные годы войны – Странное послевоенное время – Крипто на свободе – Невероятно, но факт – Вместо эпилога*]

Хитрости крипторемесла. В теории хорошо известно, как делать сильные шифры. Однако в жизни крипто обычно оказывается слабое. Как это происходит технически. [*Что такое «уязвимость» – Чему учит история – Слабость*

спереди и сзади – WEP или слабый эквивалент приватности – Криптогенератор — это непросто]

Объяснимые слабости. Почему теоретически сильная криптография на практике обычно оказывается значительно хуже, чем могла бы быть. История и философия проблемы. [*Не просто дыра – Была война – Процесс пошел – В движении словно в покое – Как это все называть?*]

Хакинг чипов Mifare : **Ясно, что небезопасно.** Подробности о взломе секретной криптосхемы RFID-чипов Mifare [*Маленькие секреты больших технологий – И грянул гром – Технические нюансы – Слабости в защите Mifare Classic – Эксплуатация слабостей и контрмеры – Проблемы и вопросы*]

Суета заранее, или Пост-квантовые тайны криптографии. В высших сферах крипто-мира отмечена весьма оживленная активность вокруг «квантово-безопасной криптографии». Почему так интенсивно все вдруг тут завертелось, никто толком не понимает. За кулисами явно знают больше – но помалкивают, как обычно. Да еще прячут концы…

Шизо-крипто, Ответственное крипто и другие формы патологического оккультизма

Шизо-криптография. Отчего на стыке большой политики и защиты информации из уст высокого государственного руководства по всему миру звучит просто-таки зашкаливающее количество неправды.

«Ответственное крипто» и другие формы обмана. Мировому сообществу активно навязываются в качестве стандарта новые шифры Simon и Speck от АНБ США. Имеет смысл разобраться, что в них действительно нового. И что, соответственно, старого…

Плохой носорог, хороший носорог. Практически все, наверное, в курсе, что у людей, волею судьбы или случая оказавшихся на высоких государственных постах, очень часто натурально «сносит крышу». Отчего еще недавно вполне разумные и гибкие люди буквально на глазах превращаются в тупых и агрессивных носорогов…

Сигнал без шума, или Криптография как метафора. Новый российский закон, вводящий для интернета черные списки, вызывает естественные вопросы. Слишком уж много признаков, что декларируется тут одно, а подразумевается нечто существенно иное [*О чем шумим? – Теория информации и криптография – Статистические аномалии – Частые повторения – Многократное использование одного ключа – Открытый текст – Информация без смысла*]

Темная сторона Силы

Серийные самоубийцы. О крайне мрачных делах международной сети спецслужб и Глубокого Государства при организации тайного прослушивания мобильной связи.

Вопросы на греческом. Компрометация Vodafone Greece как одна из наиболее подробно расследованных историй вокруг загадок с «серийными самоубийцами» [*Что случилось? – Кому это выгодно? – Как это было? – Почему Костас? – Кто виноват? – Что теперь будет?*]

Секс, ложь и шпионы. Подробности чрезвычайно странной истории вокруг необъяснимой смерти Гарета Уильямса, одного из ведущих криптоаналитиков британской разведки.

Стойкость к имитации. О загадках и странностях, окружающих феноменально успешную картину «Игра в имитацию» – как первую в истории кино биографию Алана Тьюринга, великого математика, криптографа и «отца» современных компьютеров.

Универсальная модель для усвоения уроков

Всего три слайда. Сливы от Эда Сноудена как фон для рассказа о тех «волшебных» механизмах, с помощью которых и руководством ООН, и властями далеко не последних государств планеты можно манипулировать, словно безмозглыми марионетками. [*Слайд # 1: «Грязь по каплям» – Слайд # 2: «Облачность и туман» – Слайд # 3: «Масштабы заражения» – В заключение*]

Сноуден как повод. Годовщина событий 9/11 и биография человека по имени Эдвард Сноуден предоставляют весьма особый угол зрения на то, что происходит ныне с миром и какова здесь роль инфотехнологий. [*От Гавайев до Москвы – «Это делается просто» – Примечательная череда случайностей – Банальность зла, или ложь как работа – Что нам со всем этим делать?*]

Бизнес в помощь. Шум прессы вокруг гранд-слива компромата от Эдварда Сноудена все время норовят опустить до мелочей и пустяков. То есть «понизить уровень дискуссии», выражаясь профессиональными терминами. Именно поэтому здесь хотелось бы уровень повысить. И поговорить о вещах действительно серьезных.

Биткойн как знак перемен. О своеобразном проявлении Глубокого Государства в США при синхронном запуске обсуждения криптовалюты BitCoin во всех трех ветвях государственной власти.

Невыученные уроки истории. Невозможно хоть чему-то у истории научиться, если не замечать важные исторические параллелизмы. [*Пролог: Страхи и тайны Глубокого Государства – Тема «У»: U-2 и Украина – Тема «Р»: Раскрытие – Тема «О»: Остров – Тема «К»: Криптография – Эпилог: так в чем же УРОК?*]

Криптография как универсальная модель для науки. О том, почему для лучшего понимания настоящего и будущего полезно внимательно смотреть в прошлое. И о том, каковы взаимосвязи между проблемами фундаментальной науки, взломом черных ящиков и гражданским неповиновением ученых.

Традиционные и открытые формы Магии

Тайны криптографической могилы

(Апрель 2018)

В январе нынешнего года, на проходившей в столице США конференции по инфобезопасности, был сделан занятный доклад «о тайне Арлингтонского кладбища». Точнее, о вскрытии шифра, полвека прятавшегося в буквах надгробия самой знаменитой супружеской пары правительственных криптологов. И хотя ныне их тайное послание вроде как прочитано, суть его, однако, не прозвучала абсолютно никак…

Собственно доклад сделала Илонка Данин [ED], чрезвычайно активная дама и общественница, знаменитая своим безграничным энтузиазмом во всем, что связано со вскрытием шифров. Наибольшую известность Данин обрела в свое время как автор сборника «самых знаменитых криптограмм в истории» и как наиболее заметная организующая сила в коллективных усилиях по дешифрованию скульптуры Kryptos в штаб-квартире ЦРУ в Лэнгли. Кроме того, она же является директором Фонда под-

держки Национального музея криптологии при АНБ США. А также затрачивает массу усилий на создание еще одного музея криптологии, от АНБ независимого…

Здесь, впрочем, рассказ будет не об этой энергичной даме, а о тайнах того зашифрованного крипто-послания, что Илонка нашла среди могил Арлингтонского национального кладбища. В находке её интересно все: и то, чья именно это могила; и то, каким образом тайная надпись оставалась незамеченной у всех на виду около полувека; и то, наконец, почему Данин решила разыскать именно это надгробие среди более чем 400 тысяч могил самого знаменитого кладбища США.

Последний в списке момент пояснить проще всего. Надгробие находится на могиле Уильяма Ф. Фридмана, почитаемого в США как «отец национальной криптологии», и его также знаменитой в области криптографии супруги Элизебет С. Фридман. На официальном сайте АНБ США, в разделе «Зал почета», супругам Фридманам отведено по отдельной веб-странице. Вот только рассказ об «отце криптологии» Уильяме Фридмане, правда, выглядит здесь на редкость куцым и малосодержательным – всего три небольших абзаца (200 слов или примерно 1400 знаков включая пробелы).

В дословном переводе на русский этот краткий текст выглядит так:

> *Вольф Фредерик Фридман родился 24 сентября 1891 в Кишиневе, тогда входившем в состав Российской империи, а ныне столице Молдовы. Его отец, служивший переводчиком в царской почтовой службе, на следующий год эмигрировал в США из-за нараставших антисемитских порядков. Семья Фридмана присоединилась к отцу в Питтсбурге в 1893. Еще три года спустя, когда глава семейства получил гражданство США, имя его сына Вольфа поменяли на Уильям.*
>
> *После получения степени бакалавра в области генетики и занимаясь аспирантской работой в Корнеллском университете, Уильям Фридман был нанят расположенными в пригороде Чикаго Ривербэнкскими Лабораториями, которые сегодня назвали бы научно-исследовательским институтом. Там Фридман заинтересовался изучением кодов и шифров – благодаря интересу к девушке Элизебет Смит, занимавшейся в том же Ривербэнке криптоаналитическими исследованиями. Во время Первой мировой войны Фридман покинул Ривербэнк ради военной службы офицером-криптологом. Так было положено начало его выдающейся карьеры на службе правительству.*
>
> *Последующий вклад Фридмана широко известен – как плодотворного автора, преподавателя и практика в области криптологии. Его величайшими достижениями, наверное, стали те математические и научные методы анализа, что он ввел в криптологию, и подготовленные им учебные пособия и материалы, которые затем использовали несколько поколений учеников. Его работа существенно улучшила как разведку средств связи, так и защиту информационных систем. Большинство из*

того, чем занимается АНБ ныне, в основах своих ведет начало от новаторских трудов Уильяма Фридмана.

Дабы никто вдруг не подумал, что три коротеньких абзаца для отца американской криптологии – это совершенно нормально, надо сразу отметить такой факт. Соседняя веб-страничка, посвященная жене криптографа Элизебет Смит Фридман, тоже весьма продвинутой криптографине с большим стажем госслужбы, содержит рассказ, по своему объему (около 12 тыс знаков) превышающий лаконичный текст об У.Ф.Ф. более чем в 7 раз. И это притом, надо подчеркнуть, что Элизебет никогда не состояла в кадрах АНБ (специализируясь, главным образом, на борьбе с внутренним криминалом и контрабандистами)…

Главная причина столь выдающейся краткости Агентства в рассказе о своем самом знаменитом криптографе – это, конечно же, чрезвычайная деликатность его сверхсекретной работы. Сводившейся, по сути дела, к постоянному и изобретательному чтению чужих зашифрованных писем. Причем авторами этих писем, как правило, были весьма важные люди и организации, непосредственно влиявшие на ход мировых событий. И многие, очень многие из материалов подобной тайной переписки до сих пор спрятаны в секретных архивах АНБ, абсолютно недоступные для исследований историков. А может быть и так, что наиболее интересные вещи вообще уничтожены давно…

Несмотря на скрытность его конторы, однако, биография самого Уильяма Фридмана восстановлена и изучена независимыми историками спецслужб весьма обстоятельно. И поскольку подлинная криптология в её полном виде – это не только математическая наука, но также и отчасти оккультно-магическое искусство, то пристальный интерес к жизни и деятельности настоящего криптографа Фридмана уже не раз приносил исследователям большие сюрпризы.

Благодаря фактам-сюрпризам такого рода не только известные события XX века, но и дела куда более давних времен начинают выглядеть существенно иначе и в высшей степени удивительно. Даже неправдоподобно, можно сказать. Но если тех, кто ищет ответы, интересует реальная картина, а не выдумки и умолчания правдоподобной официальной истории, то факты имеет смысл принимать именно так, как они есть. Сколь бы странно эта реальность ни выглядела.

Самый простой и наглядный способ убедительно проиллюстрировать данные тезисы – это прямо и без затей выбрать несколько скупых фраз из коротенького официального текста АНБ о своем неординарном сотруднике Уильяме Фридмане. А затем привлечь достоверно известные и неопровержимые факты для несколько более развернутого рассказа о том, что же на самом деле эти лаконичные слова означают.

Оккультизм и шифры Фрэнсиса Бэкона

Цитата #1: «**Уильям Фридман был нанят расположенными в пригороде Чикаго Ривербэнкскими Лабораториями, которые сегодня назвали бы научно-исследовательским институтом**».

Факты истории таковы, что в сентябре 1915, когда молодой генетик Фридман переехал жить и работать в городок Женева неподалеку от Чикаго, никаких Ривербэнкских Лабораторий там еще не было. А было лишь недавно купленное, обширное поместье текстильного магната Джорджа Фабиана, которое он назвал Ривербэнк и решил превратить в место передовых научных исследований. Со временем Ривербэнк действительно войдет в историю как первое частное научно-исследовательское заведение в США. Но произойдет это несколько позже.

А пока богач Фабиан, не отличавшийся особой ученостью, но зато переполненный энергией и энтузиазмом, решил заняться здесь воплощением своих разнообразных идей о новых путях к революционным свершениям в науке. Эти намерения, что немаловажно, подкрепляла куча денег, которые миллионер стал решительно тратить на благо научного прогресса.

Что касается конкретно Фридмана, то его Фабиан пригласил в качестве главы задуманного им «департамента» генетических исследований, силами которого планировалось по-новому выводить особо сильные породы животных и сорта растений. Одним из новшеств, привлекавших Фабиана, была, скажем, идея получения «лунных сортов» растений – не только благодаря их засеву под лунным светом, но и в определенные фазы цикла Луны.

Причем это был далеко не самый странный из научных проектов полковника Фабиана (свой солидный военный чин получившего не в армии, а лично от губернатора штата Иллинойс). Когда Уильям Фридман переехал в Ривербэнк, там по приглашению хозяина уже жила и работала некая миссис Элизабет Уэллс Гэллап. А также её младшая сестра Кэти Уэллс, помогавшая Гэллап в её необычных крипто-исторических изысканиях.

Областью обширных исследований этой дамы были старинные печатные книги XVII века, а главным рабочим инструментом – так называемый двухлитерный шифр Фрэнсиса Бэкона, знаменитого философа, ученого и государственного деятеля шекспировской эпохи. Освоив выявление и вскрытие-чтение этого шифра, с помощью шрифтов разных типов прячущего тайные послания в основном тексте, миссис Гэллап сумела извлечь из старинных книг массу новой и весьма неординарной информации. [BS]

Из этой информации, в частности, следовало, что Фрэнсис Бэкон считал себя внебрачным сыном королевы Елизаветы, а значит, и законным наследником английского трона (из-за чего, ради сохранения собственной жизни, был вынужден всячески данный

факт скрывать). В других шифрованных текстах Бэкона сообщалось, что это он был автором всех пьес и сонетов, ставших известными под именем Шекспира (более того, на страницах одной из древних книг Гэллап даже удалось выявить и извлечь текст прежде неизвестной «шекспировской» пьесы).

Наконец, в тех же зашифрованных посланиях сообщалось, что Бэкон был одним из руководителей тайного ордена розенкрейцеров, ставившего себе целью в корне изменить общество и его порядки с опорой на свою оккультную науку. Выстроенную на основе трех базовых компонентов – магии, астрологии и алхимии. Среди научно-магических опытов, проводимых розенкрейцерами, Бэкон описал, в частности, и устройство машины акустической левитации, с помощью которой они поднимали предметы в воздух одной лишь силой звука…

Вся эта в высшей степени необычная информация, добываемая миссис Гэллап из старинных книг, до такой степени распалила интерес Фабиана, что он убедил даму переехать вместе с сестрой в своё поместье, создав им в Ривербэнке идеальные условия для продолжения криптографических изысканий. А кроме того, миллионер загорелся идеей построить и реальный акустический левитатор – на основе дешифрованного описания от Фрэнсиса Бэкона.

Именно так, собственно, в дополнение к криптографическому и генетическому направлениям исследований в Ривербэнке вскоре возникнет еще один департамент – акустический. Который не только приведет к появлению в США самой продвинутой по тем временам лаборатории для исследований физики звука, но и даст этому месту его нынешние название – «Акустические лаборатории Ривербэнк».

Но все это, повторим, будет позднее. А пока, в начале 1916 года, Джордж Фабиан занялся активными поисками помощницы для расширения крипто-изысканий Гэллап и её сестры. Уже весной удается найти именно ту, кто был нужен. Молодая и хорошо образованная филологиня по имени Элизебет Смит, найденная для Фабиана знакомой библиотекаршей, активно интересовалась творчеством Шекспира и как раз находилась в поисках работы.

Фабиану не составило большого труда уговорить и её перебраться в усадьбу Ривербэнк. Девушка оказалась не просто умная и сообразительная, но и – что особо важно – явно способная к криптографическому анализу. Ну а самое главное, новой молоденькой ассистенткой возле пожилой миссис Гэллап не на шутку увлекся главный местный агроном-генетик Уильям Фридман. С чего, собственно, и начинается одна из самых занятных (и ныне либо умалчиваемых, либо искажаемых) страниц в истории рождения Агентства национальной безопасности США.

Когда романтический интерес Фридмана к Элизебет Смит естественным образом расширился до интереса и к профессиональным занятиям девушки, то неожиданно для всех вдруг обнаружился мощнейший криптографический талант ученого-генети-

ка. Фридман, как выяснилось, с легкостью мог вскрывать такие шифры, которые для остальных казались весьма сложными. И что еще более важно, попутно он очень умело стал привлекать для взлома шифров теорию вероятностей, статистические и прочие математические методы анализа, которые использовались в генетике. Причем в дело скоро пошли не только методы известные, но и изобретенные самим Фридманом – еще более мощные и особо эффективные для специфической работы криптоаналитиков…

Короче говоря, следующий 1917 год ознаменовался в Ривербэнке большими переменами. По весне взаимная симпатия молодых людей вылилась в свадьбу-женитьбу и очень прочный последующий брак на всю жизнь. Параллельно с генетическим департаментом Уильям Фридман возглавил теперь еще и департамент шифров, где под его руководством над выявлением и вскрытием бэконовских криптограмм в старинных книгах трудился уже целый коллектив дам-криптографинь. Ну а поскольку в тот же год власти США решили вступить в Первую мировую войну, то с осени 1917 для ривербэнкского департамента шифров и кодов быстро нашлись и более серьезные занятия.

Департамент шифров Ривербэнкских лабораторий. Крайняя слева в нижнем ряду – Элизабет Уэллс Гэллап. В центре следующего ряда – Элизебет Смит Фридман.

Формулируя более аккуратно, занятия эти нашел для себя сам Джордж Фабиан. Ибо вместе с вступлением страны в войну быстро выяснилось, что у американской армии фактически отсутствуют собственные специалисты-криптографы, способные ко взлому вражеских шифров. Зато именно такие специалисты в достатке имелись в Ривербэнке у полковника Фабиана. Причем благодаря передовым научным методам Уильяма Фридмана это были уже опытные квалифицированные профессионалы, способные не только помогать государству во вскрытии шифров, но и обучать военные кадры эффективным приемам криптоанализа.

Фабиан инициативно предложил властям помощь и в том, и в другом деле разом. Предложение его было воспринято с интересом и по-деловому, так что уже осенью 1917 в Ривербэнке не только начали заниматься вскрытием «боевых» криптограмм, но и готовить пробную небольшую группу криптоаналитиков для армии. Первый же опыт оказался вполне успешным, поэтому в начале 1918 специалисты Ривербэнка в ускоренном порядке подготовили и выпустили уже вполне солидный курс офицеров-криптографов численностью около 70 человек.

Большая фотография, на общем снимке запечатлевшая тот достопамятный выпуск вместе с инструкторами Ривербэнка, сидящими среди офицеров в гражданской одежде, по некоторым «зашифрованным» причинам стала очень дорогой для Фридманов семейной реликвией. Причем секрет послания на данном фото непосредственно связан и с тайной прощальной шифровки супругов-криптографов на их надгробном камне. Но об этих загадках удобнее будет рассказать ближе к финалу.

Здесь же надо отметить, что приводимая пара фотографий позаимствована из материалов доклада Илонки Данин. Которая на втором, увеличенном фрагменте решила почему-то несколько подрезать коллектив представителей Ривербэнка – аккуратно изъяв из данной картины личность Джорджа Фабиана. То есть собственно организатора всей этой военно-криптографической затеи. Исторически более справедливая версия

того же самого фрагмента должна выглядеть так (крайний слева гражданский – Фабиан, крайний справа – Фридман, дама в центре – Элизебет Смит Фридман).

Каковы были мотивы Илонки Данин, когда она удаляла с фото Джорджа Фабиана, сие, как говорится, осталось неизвестным. Но зато известно и неоспоримо, что эта операция «выпиливания» находится в полном согласии с официальным текстом об Уильяме Фридмане на странице АНБ США. Где про Фабиана и его ключевую роль в этой истории о зарождении национальной криптографической спецслужбы тоже нет ни единого слова.

Продолжим, однако, цитирование.

Друзья на высоких постах

Цитата #2: «**Во время Первой мировой войны Фридман покинул Ривербэнк ради военной службы офицером-криптологом. Так было положено начало его выдающейся карьеры на службе правительству**».

Супруги Фридманы летом 1918

Военная служба лейтенанта Фридмана началась летом 1918, а уже в ноябре того же года Первая мировая война закончилась. Отсюда понятно, наверное, что опыт личного участия в военных действиях конкретно для этого офицера-криптографа оказался минимальным. (По интересному совпадению военная служба подполковника Уильяма Фридмана закончится аккурат накануне того, как США вступят во Вторую мировую войну. Так что дальше он еще много лет будет преданно и на солидных должностях служить правительству уже в качестве сугубо гражданского лица.)

Первая мировая война, однако, несмотря на свою кратковременность лично для Фридмана, сыграла в его судьбе важнейшую определяющую роль. И на всю остальную жизнь прочно связала талантливого аналитика с секретами государственной разведки

и криптографии США. Кроме того, именно Первая мировая свела молодого офицера с тремя выдающимися генералами. Которые хотя и не имеют прямого отношения к истории Агентства национальной безопасности, однако в нашей «истории о тайнах криптографа Фридмана» занимают место весьма заметное.


Генералы Джон Першинг и Франсуа Картье

Генерала первого звали Джон Першинг, и на полях сражений Первой мировой войны он командовал Американскими экспедиционными силами, штаб-квартира которых находилась в городе Шомон, Франция. Именно туда в июле 1918 и прибыл новоиспеченный лейтенант Фридман, чтобы возглавить в штабе Першинга им же и обученное подразделение криптоаналитиков, занимавшихся вскрытием немецких шифров в непосредственной близости от фронта.
Генерала второго звали Франсуа Картье, а в интересующий нас военный период он возглавлял криптографическую службу Франции, отвечая как за шифрованную защиту коммуникаций французской армии, так и за перехват-дешифрование секретной переписки неприятеля. Поскольку криптослужбы союзников работали в контакте друг с другом, между Картье и Фридманом завязалось личное знакомство. При этом, несмотря на очень серьезную разницу в чинах и возрасте, французский генерал относился к молодому американскому коллеге с огромным уважением. Ибо как профессионал он сразу оценил криптографические таланты Фридмана и был весьма впечатлен его новаторскими методами криптоанализа. Среди же всего прочего, что рассказал Фридман генералу Картье, была и история о том нетривиальном пути, которым генетик-агроном пришел в военную криптографию – через выявление и анализ бэконовских шифров в книгах шекспировской эпохи. История эта не только сильно заинтересовала Картье, но и на долгие годы обеспечила ему обширное поле для собственных исследований по выходу на пенсию после войны.

Третьего генерала из этой примечательной группы военных звезд звали Джордж Маршалл. Четверть века спустя, во время Второй мировой войны и в последующие годы Маршалл прославится как начальник генерального штаба, затем госсекретарь и ми-

нистр обороны США, как инициатор известного всем Плана Маршалла по послевоенному восстановлению Европы и единственный лауреат Нобелевской премии мира среди американских кадровых военных.

На исходе же Первой мировой войны он был совсем еще не генерал, а лишь молодой и перспективный офицер, быстро продвинувшийся из капитанов в полковники и в штабе Першинга занимавшийся планированием-организацией боевых операций. Джордж Маршалл появился в окружении командующего тем же летом 1918, что и Уильям Фридман, и благодаря несомненным военно-организаторским талантам на несколько последующих лет станет ближайшим помощником генерала Першинга не только во Франции, но и по возвращении в Вашингтон.

Полковник Маршалл и генерал Першинг

По причинам, которые станут вполне ясны далее – при чуть более подробном разборе «кратких цитат» – официальные историки АНБ и американских спецслужб в целом стараются всячески умалчивать факты личного знакомства молодого Фридмана не только с французским генералом Картье, но и с будущим лидером нации Джорджем Маршаллом. Хотя – в случае с последним – крайне сложно представить работу фронтового штаба, в котором человек, занимавшийся планированием боевых операций генерала Першинга, был бы не знаком с начальником дешифровальной службы, вскрывавшей для Першинга секретную переписку противника.

Весьма выразителен и другой факт. В конце 1960-х, уже на исходе жизни, весь свой личный архив и ценную криптографическую коллекцию, собранную им за долгие годы службы, Уильям Фридман завещал передать на хранение в библиотеку Фонда Джорджа Маршалла. Где материалы и хранятся по сию пору, время от времени обретая то новые, прежде «закрытые» документы, рассекреченные из архивов АНБ, то теряя старые «открытые» – когда их вдруг решают спрятать и неясно почему засекретить… [VR]

[*Продолжение следует*]

Ссылки на источники и дополнительное чтение

[ED] Elonka Dunin, «Cipher on the William and Elizebeth Friedman tombstone at Arlington National Cemetery is solved», http://elonka.com/friedman/index.html

[BS] О фактах и аргументах в спорах о подлинном авторе шекспировских произведений: «Если дело дойдет до суда…», https://kiwibyrd.org/2014/01/05/107/

[VR] О фактах «прореживания» архивов Фридмана см. текст «Выпиливание реальности», раздел «Минус Картье, или выпиливание генерала», https://kiwibyrd.org/2016/08/09/168/

Тайны крипто-могилы. Часть 2

(Апрель 2018)

Магия и SIGABA

> Цитата #3: «**Работа Фридмана существенно улучшила как разведку средств связи, так и защиту информационных систем**».

По окончании войны и возвращении из Франции весной 1919, Уильям Фридман попытался вновь начать прежнюю гражданскую жизнь – там же в Ривербэнке, где на Фабиана продолжала работать его жена Элизебет. Однако ничего путного из этого не получилось.

По-феодальному властный Фабиан как и прежде относился к Фридману словно к своей собственности, на время предоставлявшейся в аренду вооруженным силам США. А на учебных пособиях Фридмана по криптоанализу, печатавшихся в типографии Ривербэнкских лабораторий, то и дело норовил убрать имя автора, не забывая при этом оставлять своё.

Естественно, все подобные трения и конфликты привели к попыткам Фридмана найти приличную работу где-то в другом месте. Вернуться на линию генетических исследований, однако, ему не удалось. Но вот в Вашингтоне, в генштабе сухопутных войск, который после войны возглавил его хороший знакомый генерал Першинг, талантливого криптографа брали на достойную должность абсолютно без проблем.

Так что в последние дни декабря 1920 года супруги Фридманы без ведома Фабиана и фактически тайно сбежали из Ривербэнка в Вашингтон. А уже с первых чисел января 1921 Уильям Фридман приступил к новой государственной службе – теперь в качестве начальника отдела кодов и шифров в Корпусе войск связи США.

Новая работа криптографа была вроде бы и солидной, и в трудные годы экономического спада позволяла прокормить растущую молодую семью (с интервалом в несколько лет у них родились двое детей, дочь и сын). Однако то, чем Фридман на своей службе занимался – обеспечением надежных шифр-средств для защиты коммуникаций армии – оказалось весьма скучной рутиной, никак не сравнимой с волнующей работой криптоаналитика, вскрывавшего вражеские шифры в годы войны.

В корне все переменилось лишь в самом конце 1920-х, когда Белый дом занял президент Герберт Гувер, а иностранными делами США стал ведать новый госсекретарь Генри Стимсон, имевший весьма возвышенные представления о честности в политике. По этой причине, как только Стимсону стало известно, что при Госдепартаменте работает «Черная комната» Герберта Ярдли, на регулярной основе вскрывающая шифрованную дипломатическую переписку иностранных государств, то он тут же это суперсекретное и «не подобающее джентльменам» дело решительно прикрыл. А

точнее, лишил эту разведструктуру львиной доли финансирования, поступавшей от Госдепартамента. Что и было равнозначно ликвидации.

Поскольку же остальная часть финансирования «Черной комнаты» поступала от военных, то Армия получила в свое полное распоряжение ценнейший архив с дешифрованными материалами и аналитическими разработками тайной спецслужбы. И поскольку прагматичные представления военного командования о международных делах в корне отличались от возвышенных идей главы дипломатов, то вскрытие иностранных шифров было решено непременно продолжать – но теперь уже целиком в вооруженных силах. Именно тогда-то и начался подлинный восход звезды Уильяма Ф. Фридмана…

Как опытный криптограф и аналитик – да еще с личными знакомствами в высших военных эшелонах – Фридман стал естественным выбором на пост начальника нового подразделения SIS или Signal Intelligence Service, то есть «Служба разведки средств связи». В трудные годы экономической депрессии для новой спецслужбы выделили весьма скромный бюджет, однако его вполне хватало на формирование коллектива их свежих-молодых криптоаналитических кадров.

И задачу эту Фридман решил блестяще. Четверо первых же лично отобранных их молодых людей быстро стали даровитым костяком новой криптоаналитической разведки. Трое из них – Фрэнк Роулетт, Абрахам Синков и Соломон Кульбак – были продвинутыми математиками, причем каждый с хорошим знанием одного из ключевых иностранных языков (немецкого, испанского, французского).

Что же касалось еще одного очень важного для военных шпионов языка, японского, то здесь найти математика-но-не-японца никак не удавалось. Однако вскоре отыскался молодой и даровитый лингвист Джон Херт. Который терпеть не мог математику, но зато не только прекрасно владел японским плюс несколькими другими языками, но и надолго стал лучшим и главным переводчиком-японистом военной американской разведки.

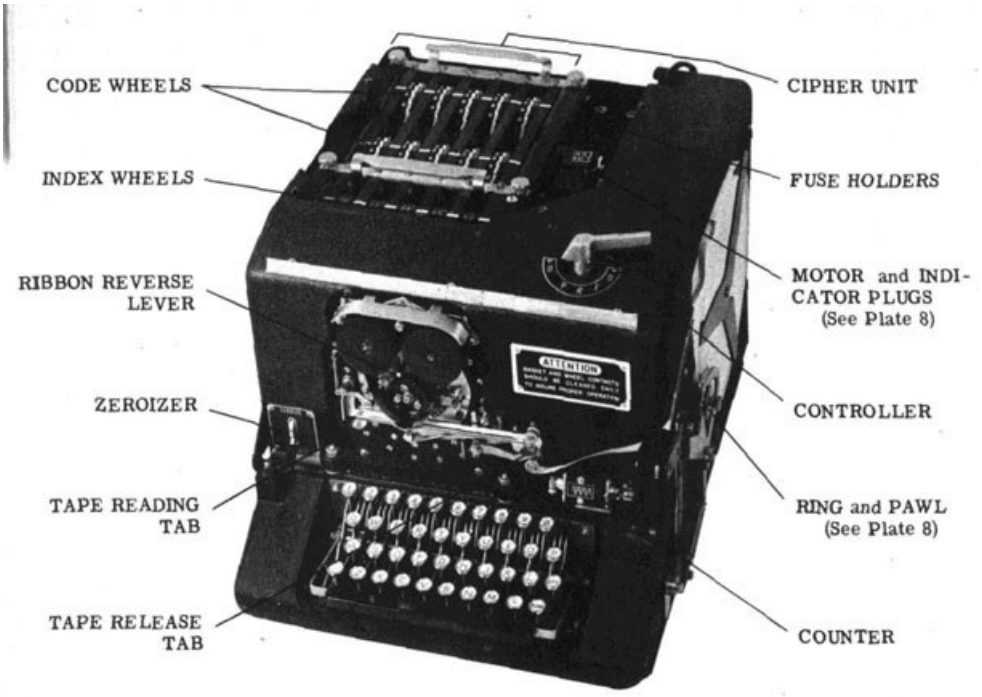
На основе этой команды, которую Фридман лично обучил основам и тонкостям криптоанализа, вскоре сформировалась чрезвычайно компетентная спецслужба, творившая в делах вскрытия шифров совершенно удивительные вещи, зачастую похожие на волшебство. И совсем не случайность, что когда все это дело было поставлено на поток, то секретные сводки по материалам дешифрованной переписки стали именоваться кодовым словом MAGIC или «Магия»…

Волшебники-криптоаналитики SIS, в центре Уильям Фридман.

Помимо сугубо разведывательной магии здесь же занимались порой и волшебством иного рода, изобретая для защиты американской военной связи чрезвычайно сильные шифры и шифраторы. Наиболее продвинутая из шифрмашин, придуманная лично Фридманом и существенно улучшенная Роулеттом, получила кодовое наименование SIGABA. И вошла в историю как самый стойкий американский шифратор периода Второй мировой войны. Причем и в послевоенное время криптосхема аппарата считалась настолько важной и ценной, что рассекретить её власти США решились лишь в начале 2000-х годов, то есть почти через 70 лет после рождения.

Ныне, впрочем, это дела уже хорошо известные. Однако с тем же аспектом – очень жесткой сверхсекретностью вокруг SIGABA – связана и другая, куда менее известная история. Не раз повергавшая криптографа в глубокую депрессию, особо обострившуюся к середине 1950-х, когда Фридман по делам шпионской службы навестил в Швейцарии своего давнего знакомого и приятеля по имени Борис Хагелин. Который в ту пору был уже не только весьма успешным бизнесменом, но и очень богатым человеком, сделавшим миллионы на собственных шифраторах, «надежных как швейцарские часы и банки». Хагелин принял старого приятеля очень хорошо и щедро, однако на Фридмана этот визит произвел крайне подавляющее воздействие, вызвав в итоге приступ сильнейшей депрессии. Причина недуга вслух обычно не произносится, однако чисто по-человечески вполне понятна.

Как высококлассный криптограф-профессионал, Фридман отлично знал, что их собственный аппарат SIGABA был намного сильнее и круче, чем шифраторы Hagelin. Однако Борис Хагелин на своих изобретениях стал процветающим мульти-миллионером, а Фридман с Роулеттом не получили от своего государства вообще ни цента. Более того, власти США даже не дали им оформить патенты на SIGABA, «в интересах национальной безопасности» подвесив изобретение в засекреченном состоянии на неопределенно долгое время (вплоть до начала 2000-х годов, когда ни Роулетта, ни Фридмана, тем более, на этом свете уже не было).



Шифратор SIGABA

Нельзя сказать, что криптографы-изобретатели с кроткой покорностью принимали эту вопиющую несправедливость. Они много лет пытались бороться за свои права через суд, и в общем-то не без успеха. Фридман сумел добиться хоть какой-то финансовой компенсации в середине 1950-х (что примечательно совпало с его визитами в Швейцарию), а Фрэнк Роулетт отсудил свои 100 тысяч долларов в середине 1960-х. Сколько сил и нервов, однако, было ими на это затрачено, не ведает, наверное, никто.

Уильям Фридман, по своей душевной организации отличавшийся тонкой и ранимой психикой, был практически уверен, что неоднократные депрессии и нервные срывы, требовавшие серьезной медицинской помощи, были вызваны экстраординарной секретностью и двусмысленностью его шпионско-криптографической работы. И в этой связи особого рассмотрения заслуживает самый первый нервный срыв Фридмана в 1941 году, по времени практически совпавший с разгромом американского флота в Перл-Харборе.

По очень давней традиции, заведенной в официальной истории – «отражать события не так, как было на самом деле, а так, как это целесообразно» – вокруг той военной

катастрофы до сих пор остается много темных и не выясненных до конца вопросов. Достоверные факты истории, тем не менее, здесь таковы.

Под руководством Фридмана криптоаналитики SIS, и в первую очередь люди из команда Роулетта, к 1940-му году достигли с помощью своей математической «магии» воистину грандиозных успехов в дешифровании секретной переписки Японии. Главным же успехом на данном направлении было массовое вскрытие системы под кодовым названием Purple – нового японского шифратора, закрывавшего дипломатическую переписку. И хотя переписка вооруженных сил Японии вскрывалась значительно хуже и медленнее, объемы и оперативность дешифрования материалов японского МИДа давали аналитикам разведки все основания считать, что руководство США вполне осведомлено о планах и замыслах потенциального противника.

В частности, незадолго до катастрофы в Перл-Харборе имел место такой эпизод – воспроизводимый здесь по личному свидетельству его участника, военного лингвиста Джона Херта [JH], переводившего те шифрованные телеграммы японского МИДа, которые вскрывали аналитики Фридмана.

За десять дней до атаки, в ноябре 1941, когда Херт и Фридман посещали в санатории общего друга, криптограф спросил у переводчика, как он оценивает из вскрытых депеш текущее состояние отношений между США и Японией. Херт ответил, что переговорам между Токио и Вашингтоном, похоже, настал конец. И в свою очередь спросил у Фридмана, что же, по его мнению, означает такое обострение отношений? На что Фридман ответил очень коротко: «Это означает войну». Пораженный этими словами, Херт тут же в волнении спросил криптографа, куда более близкого к высокому начальству, а готовы ли США к такому обострению вражды? – «Надеюсь, что это так», ответил Фридман…

О том, что произошло с Фридманом в день катастрофы, утром в воскресенье 7 декабря 1941, жена криптографа Элизебет рассказывала такими словами [RC]:

> *Услышав по радио новость об атаке в Перл-Харборе, Фридман поначалу просто не мог в это поверить. В течение какого-то времени … он вообще не мог делать ничего, кроме как ходить взад и вперед по комнате, бормоча тихо одно и то же снова и снова: «Но ведь они же знали, они же знали»…*

Самым поразительным в этой драматичной истории является, однако, то, что полтора десятка лет спустя Уильям Фридман сумеет перестроить свои взгляды на произошедшее буквально с точностью до наоборот. И напишет аналитическую работу, где очень компетентно, авторитетно и аргументированно станет всем доказывать, что на самом деле «ОНИ не знали». Ибо дело это, понимаете ли, крайне непростое…

Обман как государственная необходимость

> Цитата #4: «**Последующий вклад Фридмана широко известен – как плодовитого автора, преподавателя и практика в области криптологии**».

Рассказы о выдающихся и широко известных делах Уильяма Фридмана в качестве «преподавателя и практика» здесь по некоторым причинам удобнее отделить от рассказа о Фридмане как о «плодовитом авторе». Ибо те два конкретных произведения, автором которых является, к сожалению, Уильям Фридман, и о которых пойдет речь сейчас, не сыграли абсолютно никакой роли в делах развития теории криптологической науки или практического освоения её тонкостей. Но определенно послужили очень прочному закреплению умышленно сконструированной лжи в умах широкой публики.

Такого рода вещами – систематическим «обманом и отрицанием» – с давних пор занимаются практически все шпионские спецслужбы. По давней традиции там принято считать, что интересы национальной безопасности обязывают государство постоянно вводить в заблуждение всех своих оппонентов относительно реального положения дел. Как это ни печально, но «оппонентами» здесь часто оказываются и собственные сограждане государства. Особо же грустно, когда авторами тонкой-креативной лжи оказываются умные, талантливые и в остальном весьма приличные люди. Как в данном случае. А точнее, в двух конкретных случаях из биографии Уильяма Ф. Фридмана.

Оба этих сюжета имели место примерно в одно и то же время – в 1957 году. То есть вскоре после того, как Фридман официально ушел на пенсию, но продолжал сохранять очень тесные – рабочие и коммерческие – отношения с Агентством национальной безопасности. В частности, одна из его «коммерческих» работ того периода была подготовлена по заказу руководства АНБ (в архиве к статье приложен счет на оговоренную стоимость заказа – 4000 долларов, что для примерного сопоставления с нынешним курсом валют надо умножить на десять) и имела непосредственное отношение к предыдущей теме – катастрофе в Перл-Харборе. С этой статьи и имеет смысл начать.

Работа Фридмана носит довольно необычное для подобных статей название: «*Определенные аспекты “Магии” в подоплеке нескольких официальных расследований атаки на Перл-Харбор*» [PH]. В те времена даже в государственных структурах, не говоря уже о широкой публике, мало кто знал, что обозначает кодовое слово Магия. Но поскольку работа изначально мыслилась как секретная и предназначенная для распространения в кругах правительственных людей, имеющих доступ к гостайне, Фридман решил позволить себе здесь некоторую вольность.

Хотя заголовок статьи отчетливо заявляет об официальных расследованиях катастрофы, на самом деле для историков очевидно, что все аргументы этой работы заточены для опровержения выводов расследований неофициальных – от так называемых «ревизионистов истории». А самой главной из этих ревизионистских атак на официальную позицию государства (полностью снявшего какую-либо ответственность с высшего военно-политического руководства США) в ту пору была, несомненно, вышедшая в 1954 году книга адмирала Роберта Теобальда «*Последняя тайна Перл-Харбора: Вклад Вашингтона в японскую атаку*» [RT].

В этой работе от вице-адмирала Теобальда, который во время атаки на Перл-Харбор командовал одной из эскадр, подвергнувшихся неожиданному нападению японцев, по-военному прямо и без всяких скользких двусмысленностей было заявлено, что президент Ф.Д. Рузвельт, начальник генштаба сухопутных войск Джордж Маршалл (отметим знакомое имя из фронтовой молодости Фридмана) и командующий военно-морским флотом Гарольд Старк несут прямую ответственность за разгром тихоокеанского флота США в Перл-Харборе.

Цитируя адмирала дословно, «никакого Перл-Харбора не было бы, если бы гавайское командование не лишили Магии», причем это именно Рузвельт приказал Маршаллу и Старку придерживать дешифрованную информацию из секретной японской переписки. Делалось же это ради того, чтобы неожиданный и чувствительный удар союзника Германии вынудил нейтральные США к вступлению в мировую войну на стороне Британии и антигитлеровской коалиции в целом – к чему всячески стремился Рузвельт, но активно сопротивлялся Конгресс, где доминировали прогерманские и антисоветские настроения…

Серьезнейшие обвинения Теобальда, что очень важно, были основаны не на его личных домыслах или мутных слухах, а на документальных фактах из рассекреченных материалов нескольких официальных расследований. Именно поэтому, собственно, никаких судебных исков против строптивого адмирала, порочащего честь и достоинство высших людей страны, здесь не последовало (ибо на подобных судах обычно всплывает еще больше неудобной и компрометирующей информации).

Вместо судов, однако, как только Роберт Теобальд умер в мае 1957, руководство АНБ поручило своему главному специалисту по Магии подготовить – причем далеко не бесплатно – солидное и убедительное «опровержение» в ответ на все обвинения адмирала. Благо сам мертвый адмирал со своими рассекреченными документами парировать контр-доводы уже не мог.

Ну а все прочие независимые и еще живые исследователи были лишены возможности анализировать и критиковать «опровержение» весьма простым способом – засекречиванием работы Фридмана и её рассылкой лишь по компетентным правительственным инстанциям. В точности по той же схеме несколькими годами ранее был распространен секретный «Отчет о НЛО», подготовленный научной комиссией Робертсона и ав-

торитетно «разоблачивший» все свидетельства и факты об участившихся наблюдениях инопланетян в небе США.

Ученые этой комиссии нашли довольно странные и местами нелепые, но главное «естественные» объяснения для всех аномальных событий. Чем всячески успокоили сильно нервничающие структуры власти в Вашингтоне, заверив их, что ни инопланетян, ни угроз для государства, тем более, здесь вовсе нет. О том же, что глава комиссии и её секретарь, готовивший итоговый отчет, являются тайными сотрудниками ЦРУ с задачами предотвращения паники и внедрения дезинформации, никому говорить, конечно, не стали… [RP]

Секретная аналитическая работа от главного криптографа разведки У.Ф. Фридмана сыграла, по сути, ту же самую роль – предоставив компетентное опровержение-успокоение для всех тех, кто начал беспокоиться и задаваться ненужными вопросами из-за всплытия «иной правды» о Перл-Харборе. Попутно же отчет Фридмана решал и еще одну задачу. Дабы в будущем – при рассекречивании гостайн за давностью лет – именно этот документ всплыл бы и занял место в истории как «правда окончательная».

Что, собственно, и произошло ныне, когда в 2014 году был рассекречен комплекс тех работ Фридмана, которые хранились в закрытых архивах АНБ. Ну а официальные историки Агентства, соответственно, уже цитируют статью Фридмана о роли Магии в катастрофе Перл-Харбора как финальное и неоспоримое подтверждение официальной позиции государства в этом спорном и по сию пору активно дебатируемом вопросе истории. [DS]

Как же был достигнут столь замечательный результат? Суть развернутой, местами ловкой и местами действительно убедительной аргументации от Фридмана сводится к тому, что среди всех дешифрованных ими материалов Японии нет ни одного послания, в котором было бы в явном виде сказано, где именно и когда именно будет нанесен военный удар по США. А значит, читавшее эти дешифровки высшее руководство страны никак не могло ни знать, ни предупредить флот на Гавайях о грядущем нападении…

Вполне возможно, что Уильям Фридман даже здесь пытался быть честным. Сумев каким-то образом в корне переосмыслить свою прежнюю абсолютную уверенность в противоположном и своё тяжкое отчаяние оттого, что «они же знали, они же знали» – и не сделали, однако, ничего для предотвращения катастрофы. Но эта смена позиции была бы действительно честной лишь в том случае, если бы Фридман вступил с адмиралом Теобальдом в открытую дискуссию – подразумевающую компетентное обсуждение сторонами тех рассекреченных документов, что уже стали известны. Опровергать же серьезные доводы от человека, сведущего в теме, сразу же после того, как он умер… Такие вещи можно называть разными словами, но слов «честно и благородно» там совершенно точно нет.

А самое неприятное, что буквально за несколько месяцев до подготовки данной работы с «плодовитым автором» Уильямом Фридманом происходила на удивление похожая история, словно скроенная по тому же самому лекалу. Когда этот же очень авторитетный специалист, но уже в сотрудничестве с другим ветераном-криптографом, собственной супругой Элизебет Смит Фридман, выпустил еще одно серьезно обоснованное «опровержение». Но только не засекреченное, а открыто опубликованное для всех. И не о темных тайнах военно-шпионской криптографии, а о странных и неумелых потугах всяких дилетантов, пытавшихся с помощью псевдо-криптоаналитических фокусов доказать, что автором шекспировских текстов был якобы Фрэнсис Бэкон…

Книга получила название «Проверка шекспировских шифров» [FF], принеся авторам ощутимые финансовые бонусы в виде гонораров и литературной премии от шекспироведов. А также, ясное дело, вошла в историю шекспироведения и по сию пору регулярно цитируется как «окончательное слово» криптографов-специалистов, компетентно засвидетельствовавших, что никаких зашифрованных посланий в первых изданиях Шекспира и Бэкона на самом деле нет и никогда не было…

Вполне возможно (точнее говоря, отчасти известно и документально), что у супругов Фридманов имелись некоторые глубоко личные причины на старости лет полностью пересмотреть яркие дела собственной молодости, попутно опорочив и всех тех, кто привел их в криптографию. Обозвав Элизабет Уэллс Гэллап «женщиной, полностью погрязшей в своих собственных фантазиях», а полковника Фабиана «сумасбродным,

ничего не смыслившим в криптографии богачом, озабоченным лишь собственным самопрославлением».

Здесь нет никакой нужды вникать в доводы и аргументы книги Фридманов. Но обязательно надо подчеркнуть, что те, кого они разоблачают особенно энергично – Гэллап и Фабиан – к тому времени давным-давно уже умерли, еще в довоенные 1930-е годы. Особо же нехорошо все это как бы «разоблачение» от крипто-супругов выглядит по той причине, что первоначальная – еще более подробная – версия данной работы была подготовлена в 1955. То есть вскоре после смерти в 1953 уже знакомого нам по Первой мировой французского генерала-криптографа Франсуа Картье (в 1954 по запросу Фридмана ему через каналы НАТО был предоставлен обзор биографии генерала, подготовленный коллегами из Парижа).

В 1920-30-е годы, завершив службу в армии, Картье с подачи Фридмана и по конкретным наводкам Джорджа Фабиана кучу времени потратил на исследования и криптоанализ двухлитерного шифра Бэкона в старинных книгах XVII века. И опубликовал сначала серию статей, а затем и обобщающую монографию «Проблема криптографии и истории» [FC], где в целом подтвердил и находки Гэллап, и целесообразность дальнейших исследований материалов подобного рода.

Иначе говоря, супруги Фридманы имели более чем достаточно времени, чтобы на уровне высококлассных профессионалов всесторонне обсудить с генералом Картье их столь существенные расхождения в оценках одного и того же, равно интересного для сторон материала. Однако Фридманы предпочли дождаться, когда Картье умрет, наконец, – в возрасте 90 с лишним лет. А уж потом выдали свое компетентное и куда более удобное для официальной науки «опровержение», прочно закрепившееся в истории и литературоведении…

Коль скоро и Уильям Ф. Фридман, и его не менее крипто-государственная жена уже давным-давно также покинули этот мир, мы вряд ли узнаем подлинные мотивы, руководившие почтенными людьми в их столь сомнительном творчестве, отчетливо похожем на умышленное внедрение дезинформации.

С другой стороны, имеется вполне достаточно фактов для понимания того, зачем подобного рода обман мог понадобиться государству и его шпионской спецслужбе. В ситуации с Перл-Харбором картина, конечно же, куда более понятная. Всегда и всюду первых лиц государства – и в особенности лидеров государства-победителя в большой войне – принято изображать в сильно приукрашенном и искусственно облагороженном виде. То есть без всей той кровавой грязи, что сопутствует любым войнам…

Но вот с какой стати у супер-секретной спецслужбы АНБ мог появиться интерес к активному вмешательству в сугубо литературоведческие споры о реальном авторе шекспировских произведений? Для того, чтобы хотя бы отчасти понять этот темный момент, понадобится еще одна – заключительная – цитата. И сопутствующий ей развер-

нутый комментарий – помогающий в корне иначе смотреть на давно вроде бы известные вещи…

[*Окончание следует*]

Ссылки на источники и дополнительное чтение

[JH] *John Hurt. «The Japanese Problem in the Signal Intelligence Service»*. NSA William F. Friedman Collection, Document A58132. https://www.nsa.gov/news-features/declassified-documents/friedman-documents/

[RC] *Ronald Clark. «The Man Who Broke Purple: The Life of Colonel William F. Friedman, Who Deciphered the Japanese Code in World War II»*. Boston, MA: Little Brown, 1977.

[PH] *Friedman, William F. «Certain Aspects of "Magic" in the Cryptological Background of the Various Official Investigations into the Attack on Pearl Harbor»*. NSA William F. Friedman Collection, Document A485355. https://www.nsa.gov/news-features/declassified-documents/friedman-documents/

[RT] *Robert A. Theobald. «The Final Secret of Pearl Harbor. The Washington contribution to the Japanese Attack»*. New York: The Devin-Adair Company, 1954.

[RP] Подробности о весьма специфической роли ЦРУ и Комиссии Робертсона в теме НЛО см., к примеру, в текстах «**Sci-Myst#3: Обман трудящихся, или Следим за руками**», раздел «*Тайные истории*»; «**НЛО: история болезни**», раздел «*1993-1997: Официальный отчет ЦРУ*».

[DS] *David Sherman. «William Friedman and Pearl Harbor»*, Intelligence and National Security, 2017 November, http://dx.doi.org/10.1080/02684527.2017.1400226

[FF] *W. F. Friedman, and E. S. Friedman. «The Shakespearean Ciphers Examined»*. London: Cambridge University Press, 1957.

[FC] *François Cartier, «Un problème de Cryptographie et d'histoire»*. Paris: Editions du Mercure de France, 1938

Тайны крипто-могилы. Часть 3

(*Апрель 2018*)

Бэкдоры, TEMPEST и еще кое-что…

> Цитата #5: «**Большинство из того, чем занимается АНБ ныне, в основах своих ведет начало от новаторских трудов Уильяма Фридмана**».

Основная часть того, чем реально занимается АНБ ныне, вплоть до недавнего времени оставалось одной из главных государственных тайн США. Раскрылась же эта «ужасная тайна» в 2013 году, благодаря человеку по имени Эдвард Сноуден и великому множеству предоставленных им секретных документов из повседневной шпионской работы Агентства.

Суть же этой работы, если совсем кратко, сводится не столько к созданию сильных шифров своих и аналитическому вскрытию шифров чужих (как принято считать по традиции), сколько к очень настойчивому и агрессивному внедрению искусственных слабостей – или иначе «бэкдоров» – в любую криптографию, до которой АНБ способно дотянуться. Ибо с такими бэкдорами любые, даже формально вроде бы сильные шифры взламываются Агентством не только легко и просто, но и в индустриальных масштабах.

Другая важнейшая часть из того, чем занимается АНБ, носит кодовое наименование TEMPEST и в прежние времена тоже считалась чрезвычайно серьезной гостайной. С начала 2000-х годов, однако, с темы TEMPEST понемногу и вполне официально стали снимать плотную завесу секретности – но делая это весьма специфическим образом. Поскольку суть TEMPEST – это побочные сигналы и каналы утечки защищаемой информации, то для спецслужб равно важны как технологии шпионажа через эти каналы, так и умение защищать собственные компрометирующие излучения.

При официальном раскрытии подробностей о таких технологиях, однако, АНБ старательно делает вид, что TEMPEST – это сугубо оборонительные дела для защиты собственных секретов. А потому до сих пор среди всех рассекреченных Агентством документов нет описания ни одной разведывательной TEMPEST-операции АНБ. Хотя при этом отлично и документально известно, что вся данная тема возникла и получила развитие именно как шпионская – в начале 1950-х годов, в результате взаимно-согласованных исследований АНБ и ЦРУ.

И наконец, равно важная, можно сказать, третья главная часть из фундаментальной шпионской триады «того, чем занимается АНБ ныне» – это то, что органично сочетает в себе и «классический» криптоаналитический шпионаж, и обе «особо тайные» развед-технологии – бэкдоры и TEMPEST. То, что в явном виде не звучит практически нигде и никогда, оставаясь великим секретом у всех на виду. И это то, наконец, что ведет своё начало даже не столько от трудов Уильяма Ф. Фридмана, сколько от ку-

да более древних разработок его главного вдохновителя – английского розенкрейцера Фрэнсиса Бэкона.

Для понимания сути этой «магической тайны на виду у всех» необходимо осмыслить и переварить в их общей совокупности несколько фактов истории. Фактов достоверных и неоспоримых, однако всегда рассматриваемых историками по отдельности и в изоляции друг от друга. Отчего и не видящих очевидное.

Литературная слава Уильяма Шекспира (не оставившего после себя ни одной рукописной странички из своих гениальных текстов) началась через семь лет после его смерти, в 1623 году – вместе с печатным изданием так называемого Первого фолио. Большого формата толстой книги, подготовленной и изданной не очень ясно кем именно, но впервые собравшей в одном томе все пьесы и сонеты великого мастера слова (как поймут впоследствии благодарные читатели и ученые-литературоведы).

В том же 1623 году – что примечательно – была опубликована и очередная книга Фрэнсиса Бэкона, в ту пору еще вполне живого и здорового. Книга была написана на латыни и носила название De Augmentis Scientarum. По своему содержанию это была расширенная латинская версия более ранней бэконовской работы 1605 года «О достоинстве и приумножении наук», а особо интересным для нашей истории расширением стал здесь раздел о шифрах. Ибо в новой версии работы Бэкон с подробностями описал придуманный им в молодости совершенно чудесный метод шифрования. Так называемый «двухлитерный шифр» Бэкона (или стеганографический шифр бинарной замены, как назвали бы это сейчас), позволяющий у всех на виду и не вызывая подозрений шифровать «что угодно чем угодно». Или Omnia Per Omnia на латыни.

Возвращаясь к Первому фолио Шекспира, следует подчеркнуть, что открывала книгу пьеса «Буря» – или TEMPEST по-английски. Ну а далее богатейшая криптографическая судьба этой книги сложится так, что и в самых первых страницах трагикомедии «Буря», и во всех прочих местах данного тома исследователи XIX и XX веков обнаружат великое множество скрытых посланий, зашифрованных бэконовским методом Omnia Per Omnia. [BS]

Полковник Джордж Фабиан, в своих Ривербэнкских лабораториях оборудовавший специальную типографию для популяризации этих открытий, в начале XX века опубликовал несколько книг с подробными инструкциями и инструментами, помогающими всем ищущим самостоятельно выявлять и вскрывать бэконовские шифры в книгах шекспировской эпохи. Ныне, однако, ВО ВСЕХ современных книгах по истории криптографии о Фабиане можно прочесть только одно: что это был «эксцентричный текстильный миллионер, пытавшийся отыскать в произведениях Шекспира подтверждения тому, будто их автором является Бэкон». И конечно же, ничего он на самом деле там не нашел – ибо так сказал великий криптограф Уильям Фридман.

Авторы всех подобных книг, естественно, анализировать самостоятельно Первое фолио с помощью книг Фабиана даже не пытались. Что же касается настоящего профессионального криптографа, генерала Франсуа Картье, которого Фабиану удалось всерьез заинтересовать темой и сподвигнуть на собственный анализ, то выводы этого профессионала из современной истории криптографии просто вычеркнули. А заодно и имя самого генерала. Так что сегодня ни в энциклопедии Википедия на любом из ее языков, ни во всем Интернете вообще вы не найдете практически никакой содержательной информации об этом человеке.

Даже в знаменитой работе Дэвида Кана «*Взломщики кодов*» [DK], как наиболее подробной истории криптографии, в дополненном виде переизданной в 1996 году, где в разделах о Первой мировой войне имя главного французского криптоаналитика упоминается неоднократно, вы все равно не отыщите ни единого упоминания о книге генерала Картье «*Проблема криптографии и истории*». Но зато там есть целый раздел «Патологический криптоанализ», с благоговением пересказывающий фрагменты книги Фридманов с разгромной критикой «бэконианцев» и всячески высмеивающий тех дилетантов, что ковыряются в книгах шекспировских времен в поисках шифров, которых там нет.

То, что одного из таких дилетантов благодарное правительство США в лице АНБ отметило лично – специальной мемориальной доской на здании Ривербэнкских лабораторий и в память именно о криптографических заслугах Джорджа Фабиана – этот факт в исторической работе Дэвида Кана просто проигнорирован. О темах TEMPEST и о криптографических бэкдорах АНБ, что характерно, в толстенной – свыше 1000 страниц – книге Кана тоже нет ни слова.

Факты истории АНБ, однако, выглядят так. С момента рождения этой суперсекретной разведслужбы в 1952 году, когда на основе нескольких разрозненных подразделений в войсках было создано единое мощное Агентство, должность главного криптографа там занял Уильям Ф. Фридман. А одной из самых ранних «крипто-активных» затей АНБ на международной арене стали усилия по внедрению искусственных слабостей или бэкдоров в популярные на мировом рынке шифраторы. Подробности этих операций по сию пору остаются засекреченными, однако давно уже не тайна, что начиналось тут все с визитов Уильяма Фридмана в Европу, и в первую очередь в Швейцарию – к давнему приятелю Борису Хагелину. [BL]

Другие документально известные факты из истории АНБ таковы, что примерно в те же годы началась и разработка темы побочных каналов утечки, получившая кодовое название TEMPEST. Откуда взялся этот термин, в рассекреченной официальной истории спецслужбы по сию пору умалчивается. Однако совершенно невозможно утаить тот факт, что первый главный криптолог АНБ Уильям Фридман пришел в большую криптографию через анализ Первого фолио Шекспира, а эту книгу открывает пьеса TEMPEST. Где буквально с первых же букв и страниц через «побочные каналы пере-

дачи информации» сообщаются важные секретные сведения. Если верить всяким дилетантам-бэконианцам, конечно.

Ну а самое интересное, что если странные идеи бэконианцев принимать действительно всерьез, то можно увидеть, что еще в XVII веке Фрэнсис Бэкон с его гениальным методом шифрования Omnia per Omnia предсказал, по сути дела, самые продвинутые из современных TEMPEST-бэкдоров. Имеются в виду такого рода активные бэкдоры, которые выдают секретную информацию (в первую очередь криптоключи), двоичным «бэконовским» методом модулируя естественные эффекты в работе компьютерных устройств. Такие в частности эффекты, как звуки в работе компонентов, тепловыделение или естественные электромагнитные излучения. [VR]

Подобного рода шпионские технологии независимые исследователи компьютерной безопасности начали открывать лишь в самые последние годы. Однако есть сильные доводы за то, что в АНБ США об этом знали всегда – еще со времен «магии» Уильяма Фридмана…

Еще раз о Магии

Вся современная наука, прочно опирающаяся на фундамент математики, ведет своё начало из XVII века – от основополагающих работ титанов вроде Галилея, Декарта и Ньютона. Но выросли их великие достижения, конечно же, не на пустом месте, а на трудах исследователей-предшественников, занимавшихся такими (сомнительными для современных ученых) вещами, как алхимия, астрология и магия. Из алхимии, как известно, со временем родилась нынешняя химия, из астрологии, соответственно, появилась респектабельная астрономия, а вот прямыми наследницами средневековой магии вполне можно считать современную физику и криптологию.

О том, как эта магия древних работает в передовой физической науке, известно достаточно хорошо. В основах квантовой физики, к примеру, есть поразительно мощный математический инструментарий – вроде релятивистского уравнения Дирака или Фейнмановского интегрирования по траекториям, – который подошел для научных предсказаний не просто хорошо, а воистину превосходно. То есть у ученых имеются формулы, бесспорно верные и очень широко применяемые. Но при этом абсолютно никто не знает и не может объяснить, почему эти формулы работают. Ибо они ниоткуда не следуют и по сути дела появились у их авторов в голове совершенно неведомым «магическим» образом. Подозрительное слово Магия, впрочем, в данном случае среди серьезных ученых употреблять не принято. [WP]

В науке криптографии с её куда более глубокими оккультными корнями, термин Магия, как мы уже видели, даже очень серьезные люди применять не стеснялись. Но на всякий случай – или для маскировки – превратили её в еще одно специфическое кодовое слово, каких в работе секретных разведслужб всегда пруд пруди. Однако из этого

вовсе не следует, что подлинные магия и волшебство из работы настоящих криптографов ныне исчезли. Вовсе нет. И тому есть сколько угодно наглядных примеров.

Вот как, скажем, выглядел достаточно типичный случай криптографического волшебства в работе супругов Фридманов (эта история приводится в уже упомянутой книге Кана «*Взломщики кодов*»). В 1917 году, когда Ривербэнкские лаборатории начали помогать правительству США в криптоаналитическом взломе шифров, английские коллеги из военной разведки прислали им пять коротких сообщений для контрольного теста на вскрытие. Тексты были зашифрованы не вручную, а особым устройством – новым шифратором, который изобрел Винсент Плеттс, один из сотрудников криптобюро английской разведки.

Англичане были абсолютно уверены в стойкости своего нового шифра и прислали его американским коллегам лишь для того, чтобы дополнительно в этом убедиться с помощью независимой экспертизы. Даровитый Уильям Фридман, однако, практически сразу сумел дешифровать часть материала, определив систему и отыскав один из криптоключей (ключом оказалось слово CIPHER, то есть «шифр»). Второй ключ, однако, вычислить аналитически не удавалось никак. И вот тогда Фридман решил прибегнуть к несколько иному методу – к «магии» или «психологическому криптоанализу», если угодно.

В той же комнате за соседним столом над вскрытием других криптограмм работала жена Фридмана Элизебет. На минутку прервав её занятия, криптограф попросил жену отвлечься, расслабиться и «сделать свой разум чистым»… А теперь, продолжил Фридман после некоторой паузы, я хочу, чтобы ты сказала мне то слово, которое придет тебе на ум первым, когда я скажу тебе своё… Сделав еще одну небольшую паузу, он произнес: «Шифр»… – «Машина», тут же сказала ему в ответ Элизебет. Подставив это слово – MACHINE – в качестве криптоключа, Фридман сразу увидел, что ключ действительно подходит и вскрыл весь тестовый материал полностью (самая первая из дешифрованных фраз выглядела так: «Этот шифр абсолютно невскрываем»)…

Подобного рода эпизоды – с интуитивным угадыванием промежуточного ответа – в работе талантливых криптоаналитиков происходят регулярно и какой-то особой магией даже не считаются. Но вот когда коллективу криптографов по одним лишь текстам шифрованных телеграмм, перехваченных в радиоэфире, удается не только полностью вскрыть хитрую схему неизвестной шифр-машины, применяемой для засекречивания связи, но и организовать массовое дешифрование этой криптопереписки – вот такие вещи действительно выглядят как фантастическое волшебство. Даже для профессиональных опытных криптографов. И что особенно важно, поразительные чудеса подобного рода не только возможны, но и действительно происходили в истории криптоанализа неоднократно.

Именно так, в частности, люди Фридмана в спецслужбе SIS на рубеже 1930-40-х годов вскрыли криптосхему шифратора, закрывавшего дипломатическую переписку

Японии и получившего у американцев кодовое наименование PURPLE. И точно так же – исключительно по шифртекстам радиоперехвата – их коллеги из английской крипторазведки в 1940-е годы полностью вскрыли и массово дешифровали самый стойкий германский шифратор «Лоренц Шлюссельцузатц», закрывавший переписку Гитлера и верховного командования Вермахта. [СВ]

Конечно же, все подобные фантастические успехи при желании можно объяснить и без магии, чисто математическими талантами и потрясающей интуицией криптоаналитиков. Однако в истории криптографии XX века есть немало и таких страниц, которые обычными «посюсторонними» причинами объяснить совершенно невозможно. И оттого объяснением может быть или нечто совсем нелепое-беспомощное – типа «случайное совпадение», или же фактор реальный, но для современных людей звучащий крайне неправдоподобно: «просто магия с участием потусторонних сил»…

И вот тому несколько примеров навскидку – из параллельных и местами даже поныне засекреченных историй криптоспецслужб в США и СССР.

Всемирно знаменитый советский инженер, изобретатель и музыкант Лев Термен в 1940-е годы изобрел для чекистов совершенно гениальное подслушивающее «изделие», получившего условное название «БУРАН». По принципам своего устройства и функционирования это было типичное TEMPEST-устройство, как назвали бы это ныне. Или «БУРЯ-устройство», в дословном переводе на русский. Поразительный факт заключается в том, что изобретение Термена советская разведка начала активно применять для прослушивания американского посла в ту пору, когда в США еще не было ни АНБ, ни темы «Буря» (TEMPEST).

Подобно тому, как покров государственной тайны продолжает окутывать в АНБ не только шпионские аспекты темы «Буря», но и историю происхождения собственно термина Tempest, так и подробности об «изделии Буран», аналогично, тоже долго были большой тайной советских спецслужб. Но зато никогда не было секретом устройство другого, самого знаменитого изобретения Льва Термена – электромузыкального инструмента под названием «Терменвокс».

И если профессионалы акустической электроники посмотрят на этот инструмент с точки зрения шпионов, то они без труда увидят, что физические принципы работы у Терменвокса и у «изделия Буран» по сути дела одни и те же. Ибо построены они на основе глубокого понимания изобретателем тех взаимодействий и взаимных влияний, что характерны для вибраций и движений предметов, акустических волн и волн электромагнитных.

Формулируя чуть иначе, Лев Термен очень тонко чувствовал, как звуки и движения могут модулировать – или иначе кодировать – электромагнитные волны. А это, в свою очередь, одно из воплощений глубоко бэконовской по своей сути идеи Omnia Per Omnia – кодировать «что угодно с помощью чего угодно»…

Дабы влияние бэкон-розенкрейцеровской магии на криптографию XX века стало очевидным и несомненным, необходимо принимать во внимание и такой абсолютно достоверный факт истории. В 1930-е годы основатель и глава первой советской криптослужбы или Особого отдела ВЧК-ОГПУ, старый большевик и чекист Глеб Бокий, довольно близко сошелся с подпольными кругами мистиков-оккультистов. В частности, тесные отношения завязались у него с биологом Александром В. Барченко, членом российского отделения ордена розенкрейцеров-орионийцев. Под сильным влиянием Барченко, для которого Бокий стал защитником и покровителем, в ОГПУ одно время даже действовало тайное общество «Древняя Наука» для изучения секретных мистических знаний. [АВ]

О тайном влиянии ордена розенкрейцеров на государственную криптографию 1930-х и прочих годов в США или Великобритании не известно практически ничего. Ибо что в открытых-общедоступных, что в раскрываемых понемногу секретных книгах по истории криптографии об этих вещах авторы либо не знают, либо умалчивают.

Но зато прекрасно и документально известно, что тема бэконовских шифров и розенкрейровской магии была главной областью исследований в Ривербэнкских лабораториях полковника Фабиана. Причем даже своё нынешние название «Акустические лаборатории» это заведение получило исключительно благодаря Бэкону, розенкрейцерам и их магическим опытам с необычными возможностями звука. Но об этом, правда, практически никто ныне вслух не говорит. Ибо в официальных текстах Бэкона ничего про это нет, а все якобы дешифрованные «у Шекспира» и в прочих старых книгах сведения на данный счет трактуются как смешные выдумки всяких чудаков.

О том, насколько поверхностной и немудрой является подобная позиция, говорит уже тот факт, что к подобным «чудакам» следует относить и отца американской криптологии Уильяма Ф. Фридмана.

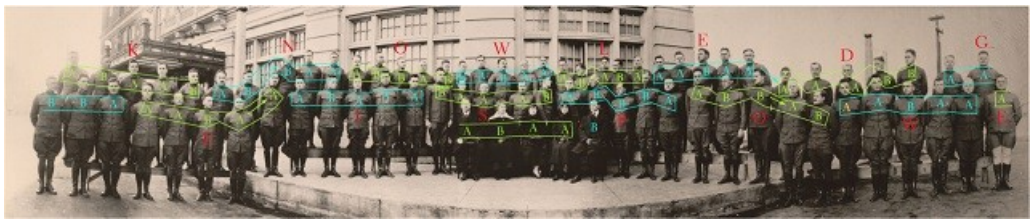
Имеются достоверные и абсолютно неопровержимые факты, свидетельствующие о том что, Уильям Фридман не только чрезвычайно высоко оценивал двухлитерный шифр Бэкона и его гениальный метод засекречивания Omnia Per Omnia, но и вдохновлялся бэконовскими идеями вплоть до последних дней своей жизни.

Но особо существенно здесь вовсе не то, что данные факты являются несомненными, а то, что во все официальные версии биографии эта информация не попадает. Имеет смысл обращать на это внимание и задумываться о причинах и подоплеке происходящего…

«Знание – это сила»…

Факт # 1:

Особо дорогая для Фридмана фотография из 1918 года – с групповым снимком его первого большого курса офицеров-криптографов – это далеко не просто памятный снимок, который он всю жизнь держал на рабочем месте. Это тщательно выстроенное засекреченное послание, демонстрирующее всю мощь бэконовского метода шифрования «у всех на виду». В поворотах головы людей, которые смотрят либо прямо перед собой, либо в сторону, закодированы биты сообщения. Которое, при аккуратном разбиении битов на пятерки, складывается в буквы знаменитого девиза Фрэнсиса Бэкона, ордена розенкрейцеров и множества прочих мистиков-оккультистов древности: «KNOWLEDGE IS POWER», то есть «Знание это сила»…



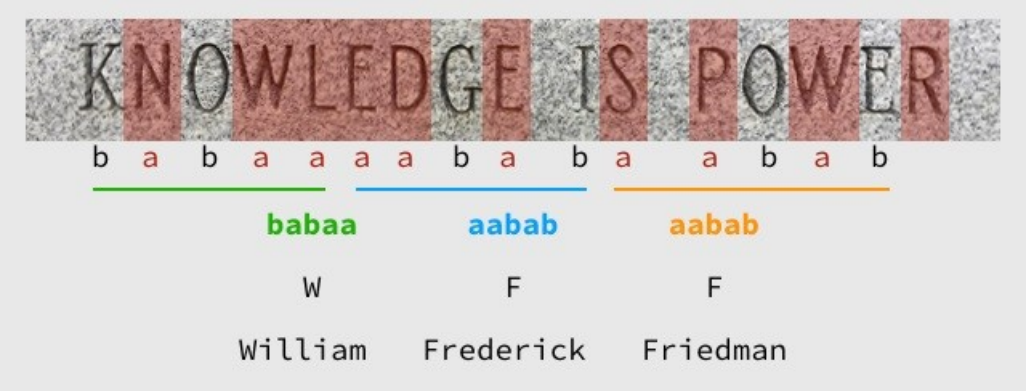
*Увеличенный вариант снимка **см. тут**.*

Но самое интересное, однако, даже не это. А то, что на официальных веб-страницах Фонда Маршалла, рассказывающих о хранимом здесь архиве «отца криптологии», именно вот этой – особо дорогой и важной для Фридмана – фотографии почему-то

нет… Но зато с некоторых пор там можно найти отдельный видеоролик, где голос ведущего расскажет вам об истории данного снимка и объяснит, как его следует правильно понимать. Дабы стало ясно, что отсутствие собственно фотографии – это вовсе не случайность или недосмотр, там же полезно найти раздел «Фотографии, лежавшие под стеклом на рабочем столе Уильяма Фридмана». Где по всем свидетельствам этот снимок находился у криптографа всегда. В «музейной версии стола» для истории, однако, важное фото изъято без объяснений и вообще без упоминания…

Факт # 2:

Ту же самую фразу «Знание – сила», столь дорогую для криптографа и для трудов всей его жизни, он завещал выбить на своем могильном камне. Что, конечно же, настоящим историкам криптографии было известно всегда. Но лишь в 2017 году, почти через полвека после смерти Фридмана, в этой надписи на надгробии было вдруг обнаружено, что и она содержит в себе тайное послание, зашифрованное двухлитерным методом Бэкона. Причем Илонка Данин не только вскрыла эту коротенькую криптограмму – зашифрованную подпись из инициалов криптографа W-F-F, – но и сумела отыскать в архивах его жены, Элизебет Фридман, личную записку, полностью подтверждающую верность этой расшифровки. [ED]



Но самое интересное в данном сюжете, опять же, не собственно факт выявления шифрованного послания от великого криптографа. А то, как с ним обошлись обычно весьма патриотичные американские средства массовой информации США. Ведь Уильям Ф. Фридман – человек в американской истории очень известный, отец национальной криптологии США, как ни крути. Однако, как это ни поразительно, но – если доверять глобальному новостному агрегатору Google News – в американских СМИ не появилось вообще НИ ОДНОЙ публикации на эту тему. Ни о докладе Илонки Данин на конференции в Вашингтоне в январе 2018, ни о зашифрованных буквах на могильном камне Фридмана. (Тема оказалась интересна лишь британцам – одному ИТ-изданию, и одному блоггеру на страницах английского антивирусного бюллетеня).

Однако ни въедливая Данин, как автор открытия, ни британские комментаторы – при всем их интересе к истории криптографии – совершенно не уловили тонкую суть прощального послания от Фридмана.

#

Что же тут такого тонкого-особенного в данной истории?

Для начала следует обратить внимание на любопытный замкнутый цикл. В самом начале своей военно-шпионской крипто-карьеры Фридман был явно и отчетливо впечатлен мощью гения Бэкона и его двухлитерного шифра. В самом конце жизни, уже сходя в могилу, Фридман счел необходимым еще раз указать на прямую связь своей службы с Бэконом и его шифром. Ну а в промежутке между этими эпизодами мы видим нечто в корне иное: как авторитетный государственный криптограф Фридман говорит вслух исключительно о гении Шекспира, всячески отрицая факты бэконовских шифров в книгах шекспировской эпохи…

При этом, однако, имеются очень четкие свидетельства, что сам криптоаналитик к концу жизни испытывал сильнейший душевный дискомфорт от итогов своей тайной шпионской службы государству, которое все дальше и дальше уходило от широко декларируемых им же принципов свободы и демократии. Особенно отчетливо эти переживания отразились в публичной лекции Фридмана «*Шекспир, тайная разведка и государство*» [FS], которую он прочел в 1962 году на заседании Американского философского общества. И которую завершали такие – весьма неожиданные для «государственного взломщика» – слова:

> *Имел ли Шекспир какое-то личное мнение относительно этичности перехвата корреспонденции, относительно тайного сбора такого рода разведданных, и относительно использования этих сведений для ведения общественных дел? Интересно было бы это знать.*
>
> *Понимал ли он, насколько сложно соединять подобного рода действия с демократическими идеалами свободного и открытого общества? Которое предпочло бы, чтобы его правительство вело все свои внутренние дела настолько открыто, насколько это вообще возможно. А также, чтобы и все внешние или иностранные дела велись в подобной открытой манере…*

Для лучшего понимания всей степени мучительности тех вопросов, которыми задавался Фридман по завершении своей шпионской карьеры и на закате всей жизни, очень полезно сопоставить их с высказываниями госсекретаря США Генри Стимсона. Того самого Стимсона, который в 1929 лично разогнал «Черный кабинет» при госдепартаменте (и тем невольно дал начало для восхождения шпионско-криптоаналитической карьеры Уильяма Фридмана).

Как джентльмен и просто человек в высшей степени порядочный, Стимсон был категорически против сочетания дипломатии со шпионажем. Поэтому он считал совершенно неприемлемым, чтобы криптоаналитики госдепартамента читали почту иностранных дипломатов, а добытую подобным образом информацию сообщали амери-

канским послам. Объясняя свою позицию так (цитируется по документам из историко-биографической работы Дэвида Кана [HY]):

> *Посол – это гость той страны, в которой он находится. Он удостоен дипломатических привилегий – таких, как неприкосновенность и иммунитет от арестов. И это же, по убеждению Стимсона, включает в себя и абсолютную свободу общаться со своей страной без всякого шпионажа. Дипломаты, продолжал он, это единственная категория государственных служащих, для которой предполагается джентльменское поведение в международных делах. Госсекретарю не пристало поступать как шпиону в отношении людей, которых он воспринимает как своих братьев. Суть же своих воззрений Стимсон заключил лапидарной фразой, прочно вошедшей в историю: «Джентльмены не читают почту друг друга»…*

Уильям Фридман никогда не служил дипломатом и наверняка был в курсе, что для людей военных даже крайне щепетильный госсекретарь Стимсон всегда допускал и неджентльменское поведение вообще, и чтение переписки своих оппонентов в частности.

Но как человек умный и проницательный, Фридман отлично понимал, что все дело его жизни – чтение чужих писем – практически никак не сочетается с демократическими идеалами свободного и открытого общества. Он же, подобно всем, кто считает себя честными и порядочными людьми, очевидно предпочел бы жить в таком государстве, которое ведет все свои дела – как внутренние, так и внешние – настолько открыто, насколько это вообще возможно.

Приближаясь к финалу жизненного пути, однако, криптограф прекрасно видел, что вместе с созданием мощных централизованных спецслужб вроде ЦРУ и АНБ, требовавших все большей и большей секретности, его государство стремительно движется совсем в другом направлении. Уводящем все дальше и дальше от демократических идеалов и свободного открытого общества. Причем к формированию именно такого вот государства выдающийся шпион-криптоаналитик Уильям Фридман приложил массу своих собственных сил и талантов – в изобилии наделяя власти тайными знаниями, а значит, и новыми силами…

Конечно же, Фридман прекрасно всё это понимал. Но вот что он при этом чувствовал?

Интересно было бы знать….

# # #

Ссылки на источники и дополнительное чтение

[BS] Подробности о методе шифрования Omnia Per Omnia и о его разновидностях см. в материале «**Если дело дойдет до суда…**»

[DK] *David Kahn, «The Codebreakers. The Comprehensive History of Secret Communication from Ancient Times to the Internet»,* Scribner, 1996

[BL] О том месте, что официальная история АНБ США отводит служебным визитам Фридмана в послевоенную Европу, см. материал «**Чтение между строк**», раздел «*Проект BORIS*»

[VR] О недавнем переоткрытии TEMPEST-бэкдоров академическим сообществом инфобезопасности см. текст «**Выпиливание реальности**», раздел «*Минус GSMem, или выпиливание методов доступа*»

[WP] О том, как в 1952 (в год создания АНБ, по случайному совпадению) знаменитый физик-теоретик Вольфганг Паули опубликовал аналитическую работу с попыткой синтеза магических методов древних алхимиков и современных математических методов науки, см. текст «**Язык синтеза**» в материале «Сны Вольфганга П.»

[CB] Подробности о первом в истории суперкомпьютере и фантастических успехах криптоаналитиков в годы Второй мировой войны: «**Колосс британский**»

[AB] *Андреев А., Бережков В. «Оккультисты Лубянки»*. — Москва: Издатель Быстров, 2006.

[ED] *Elonka Dunin, «Cipher on the William and Elizebeth Friedman tombstone at Arlington National Cemetery is solved»,* 2017 http://elonka.com/friedman/index.html

[FS] *William F. Friedman, «Shakespeare, Secret Intelligence, and Statecraft». Proceedings of the American Philosophical Society 106, no. 5 (Oct. 1962): 401–41.* Подробности о том историческом контексте, в котором рождалась данная работа Фридмана, см. в материале «**Невыученные уроки истории**», раздел *Тема «К»: Криптография* .

[HY] *David Kahn, «The Reader of Gentlemen's Mail: Herbert O. Yardley and the Birth of American Codebreaking»*. Yale University Press, 2004

Экстрасенсы от криптографии

(Октябрь 2014)

О чрезвычайно тонкой, практически неразличимой грани между искусством крипто-хакинга и паранормальными феноменами экстрасенсов (в народе именуемыми волшебством).

Обыкновенное чудо

Идеи о том, что современные достижения науки и техники для людей прошлого выглядели бы словно поразительные чудеса и волшебная магия, уже давно воспринимаются как затертый штамп. Но при этом, что любопытно, и на сегодняшний день хватает таких технологий, которые не только широкая публика, но даже и специалисты в большинстве своем воспринимают с сильнейшим недоверием – то ли это изощренный обман, то ли и впрямь нечто сверхъестественное…

Особенно отчетливо данный парадокс можно наблюдать в области компьютерного хакинга. И для наглядного примера тому достаточно упомянуть пару примечательных работ, вызвавших повышенное внимание хакерско-криптографического сообщества в последние месяцы – на конференциях в США и Южной Корее.

В рамках знаменитого форума Black Hat USA, проходившего в августе в Лас-Вегасе, давно заведена традиция ежегодно отмечать премиями Pwnie Awards особо выдающиеся события – причем как достижения, так и провалы – в разных областях хакерского искусства.

В наиболее же почетном, пожалуй, разделе – «Самое новаторское исследование года» – на этот раз золотым призом-лошадкой Pwnie была отмечена работа под названием «**Акустический криптоанализ**» («*RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis», by Daniel Genkin, Adi Shamir, Eran Tromer*). Если в двух словах, то суть достижения израильских ученых – это способность добывать секретные криптоключи, которыми компьютер шифрует информацию, по звукам работы электронных схем.

Даже многоопытные члены жюри, всякого повидавшие на своем хакерском веку, охарактеризовали эту поразительную работу как «чарующе пленительную».

Пример второй – с очередного форума CHES 2014 (www.chesworkshop.org/ches2014/) или, более официально, международного научно-технического семинара «Криптография в аппаратуре и встроенных системах», проходившего в 20-числах сентября в городе Пусане, Корея.

На этой конференции особое внимание прессы и профессионального сообщества привлек анонс доклада под названием «**Руки прочь от моего ноутбука**» («*Get Your Hands*

Off My Laptop: Physical Side-Channel Key-Extraction Attacks on PCs» by Daniel Genkin, Itamar Pipman, and Eran Tromer).

Несмотря на несколько игривое название, речь в данной работе идет о вещах весьма серьезных и воистину удивительных. Фактически, те же самые израильские исследователи демонстрируют, что теперь они могут извлекать секретные криптоключи из компьютера одним лишь «наложением рук» – то есть просто прикасаясь к машине в нужном месте…

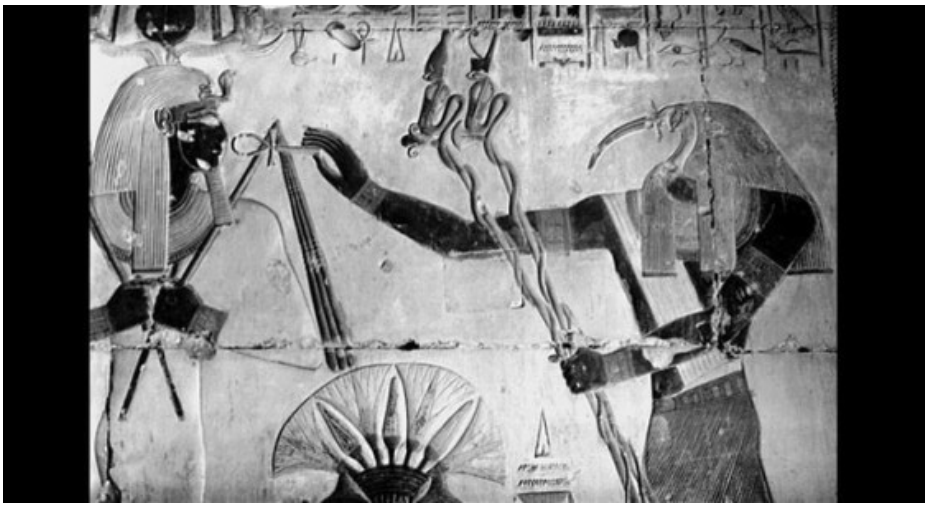
Для всякого человека, хоть что-то понимающего в компьютерах и в шифрах, но далекого от эзотерической области «побочных каналов компрометации», подобного рода новости должны звучать как шутка или издевательская насмешка. Ибо в традиционной теории, подкрепляющей криптографическую науку, такого рода фокусов быть не может и не должно быть в принципе.

Однако в реальности это есть. И демонстрируют подобные вещи не какие-то подозрительные шарлатаны, а серьезные ученые, хорошо известные в исследовательском сообществе.

Короче говоря, явно пора разъяснить, в чем заключается секрет подобных чудес. Но сделать это целесообразно в подобающем историко-культурологическом контексте.

Оккультные корни

У современной науки, насколько известно, нет абсолютно никаких оснований предполагать, что общеупотребимые ныне термины HACK (в английском звучит как «хэк») и HACKER (хэка) исторически ведут свою родословную из глубины тысячелетий – от цивилизации Древнего Египта.



Но при этом, однако, всякий внимательный читатель книги «Египетская магия», выпущенной известным британским ученым Уоллисом Баджем еще в конце XIX века, скорее всего обратит внимание на следующий упоминаемый там факт:

[В Древнем Египте] термином «ХЭКА» обозначалась магия, то есть «слова власти» — магические слова, заклинания. (EA Wallis Budge, Egyptian Magic, 1899 London, Kegan Paul)

Конечно же, столь очевидное созвучие терминов можно считать просто лишь забавным совпадением. И не более того.

Но также можно принять этот пустячок во внимание и аккуратно сопоставить его с другими бесспорными фактами. С тем, к примеру, что на всем протяжении нашей истории – с момента изобретения письменности – любые тайные знания и особенно знания магов всегда были неразрывно связаны с шифрованием ценной информации. Дабы она не стала ненароком известна тем, для кого не предназначена.

Известным фактом является и то, что со времен Древнего Египта основы криптографии (как искусства тайнописи и вскрытия зашифрованных смыслов) наряду с заклинаниями входили в базовый комплекс оккультных знаний, которым обучали жрецов и детей фараонов. При этом отношение публики к криптографии как к одной из разновидностей оккультизма сохранялось в истории на редкость долго. По сути дела, вплоть до середины XX века, пока Клод Шеннон не создал строго математические единые основы для криптографии и теории информации.

Но если для широкой публики неразрывные связи криптографической магии с математикой стали очевидны лишь сравнительно недавно, то для самих оккультистов и мистиков это было известно всегда.

В традициях европейской культуры, скажем, вовсе не секрет, что основы информационного взгляда на мир идут еще от Пифагора и мистической школы его последователей-пифагорейцев, видевших «числа в основе всего». Соответственно, развитие математических знаний этой школой было тесно увязано с постижением тайн в основах мироздания. К сожалению, практически все обретенные пифагорейцами знания очень строго и глубоко шифровались, но это, увы, одна из древнейших традиций оккультистов.

О тесных взаимосвязях между мистицизмом и математикой куда лучше известно благодаря суфиям – также весьма древнему и широко разветвленному мистическому течению в рамках исламской традиции. Практически все, наверное, наслышаны, что слово «алгебра» имеет арабское происхождение. Значительно меньше известно о том, что главный трюк алгебраического подхода – замена чисел на буквы – берет свое начало от криптографической системы Абджад мистиков-суфиев.

Table of Sequential & Gematrical Values of the Arabic Alphabet

Sequential Value	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Arabic Letters	ا	ب	ج	د	ه	و	ز	ح	ط	ي	ك	ل	م	ن
English	elif	be	cim	dal	he	vav	ze	ha	tı	ye	kef	lam	mim	nun
Gematrical Value	1	2	3	4	5	6	7	8	9	10	20	30	40	50
Sequential Value	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Arabic Letters	س	ع	ف	ص	ق	ر	ش	ت	ث	خ	ذ	ض	ظ	غ
English	sin	ayn	fe	sad	kaf	re	şin	te	se	hı	zel	dad	zı	ğayn
Gematrical Value	60	70	80	90	100	200	300	400	500	600	700	800	900	1000

Главное различие заключается тут вот в чем. Алгебраический подход подразумевает применение букв для кодирования числовых соотношений и для решения чисто математических задач. Система же Абджад позволяет суфиям извлекать скрытые смыслы и глубокие истины из совершенно обычных, на первый взгляд, слов и словосочетаний – сначала преобразуя буквы к известным числовым эквивалентам и вычисляя их сумму, а затем отыскивая для этого результата подлинный, но зашифрованный смысл…

Поскольку рассказ об этих вещах уведет историю очень далеко от нашей главной темы, всех интересующихся можно отослать к книгам-первоисточникам (например, для содержательного введения в тему вполне сгодится такая работа: *Идрис Шах. Суфизм. Раздел «Тайный язык»*).

Здесь же пора вернуться к делам более актуальным. К компьютерному хакингу и криптографии – в контексте их взаимосвязей с мистическими чудесами магии. Или, выражаясь языком более современным, с феноменами экстрасенсорного восприятия.

Ясновидение Блэйза

Вся тема экстрасенсов в своей совокупности, как известно, слывет областью весьма одиозной – коль скоро с одной стороны она тесно соприкасается с махровым шарлатанством, а с другой стороны не поддается внятному научному объяснению и стабильному воспроизведению феноменов в лабораторных условиях.

По этим причинам о бесспорно феноменальных экстрасенсорных способностях некоторых хакеров-криптографов нагляднее всего будет рассказать с точки зрения закоренелого скептицизма. То есть с позиций таких людей, которые просто «не верят» ни в какие такие сверхъестественные способности на все 100%. И заранее абсолютно уверены, что все это только обман доверчивых обывателей.

Один из ярчайших представителей этой скептической категории человечества – известный маг-иллюзионист Джеймс Рэнди, которому к старости несколько поднадоело обманывать зрителей фальшивыми чудесами и фокусами, а потому заключительную часть своей жизни он посвятил энергичному разоблачению всевозможной «паранормальщины».

Ради этого дела экс-иллюзионист учредил специальный Образовательный фонд Джеймса Рэнди или кратко JREF (http://web.randi.org/), где методично занимаются расследованиями и демистификацией всевозможных «чудес», прививая людям основы критического мышления, скептицизма и научных методов анализа. Самая же знаменитая, наверное, акция JREF – это давно объявленный приз в размере 1 миллион долларов любому, кто убедительно продемонстрирует свои сверхъестественные способности в условиях надежно контролируемого эксперимента.

И хотя в мире полным-полно людей, зарабатывающих на жизнь в качестве экстрасенсов, получить миллион долларов от Джеймса Рэнди никто из них не сумел. На протяжении нескольких десятилетий многие чудотворцы пытались это сделать, однако доказать свои сверхъестественные способности в строгих условиях научного тестирования JREF никто не сумел.

И продолжалось так вплоть до 2007 года, пока «вызов Рэнди» не принял человек по имени Мэтт Блэйз – известный в мире отнюдь не как великий экстрасенс, а как хакер-аналитик и профессор-криптограф одного из американских университетов. Заинтересовала же вся эта история Блэйза лишь по той причине, что в JREF – для подогрева интереса к их конкурсу – решили привлечь довольно модную среди публики тему шифров.

К тому времени, следует отметить, все мало-мальски известные экстрасенсы о «страшном Джеймсе Рэнди» уже и слышать не хотели, поэтому он упростил условия

своего теста до следующей задачи. В надежный сейф в штаб-квартире JREF Рэнди в запечатанном виде спрятал некий особый предмет и объявил, что отдаст миллионный приз всякому, кто с помощью своего чудесного дара правильно угадает и опишет, что за вещь положена в тайник.

Ну а дабы никто не заподозрил экс-мага в жульничестве и быстрой подмене угаданного кем-нибудь предмета, Рэнди опубликовал своего рода «цифровое обязательство» – то есть описание этой вещи в зашифрованном виде. И выглядела эта закодированная проверочная информация следующим образом:

0679
4388
66/27
5 -14

Никто не знает, что сказал бы о скрытом смысле этих цифр восточный мистик-суфий, в совершенстве владеющий системой Абджад. Но зато отлично известно, что для хакера-криптографа Мэтта Блэйза данных чисел оказалось вполне достаточно, чтобы совершенно точно угадать и описать предмет, спрятанный в сейфе JREF. А значит, и абсолютно чисто – одним лишь напряжением своих ментальных способностей – выиграть приз конкурса, «миллион для экстрасенса» (от которого, впрочем, Блэйз великодушно отказался).

Подробности о том, как именно талантливому криптоаналитику удалось всего по нескольким цифрам постичь, что в запечатанном боксе своего сейфа Джеймс Рэнди спрятал компакт-диск, можно прочесть в материале «Хакер, слесарь, экстрасенс». Здесь же лишь еще раз подчеркнем важную суть этой истории: искусство хакинга и криптографии действительно находятся на очень тонкой грани между обычным и сверхъестественным. Поэтому даже когда каждый отдельный шаг анализа вполне можно объяснить рационально, итоговая картина все равно выглядит поразительно – словно чудо.

Биошаманство Кочера

Предыдущий сюжет о ясновидении Блэйза интересен и поучителен также по той причине, что очень наглядно демонстрирует значимость побочных компрометирующих сигналов, непременно сопровождающих функционирование всякой работающей системы. И соответственно, принципиальную важность подобных утечек для общего успеха хакинга.

Ведь если бы Дж. Рэнди просто запечатал свой секрет в сейф и абсолютно ничего никому при этом не сообщил, то и Мэтт Блэйз не смог бы тут ничего угадать. Однако, чтобы вся эта система «жила и работала», оказалось необходимым выдать хотя бы часть информации, пусть и в тщательно зашифрованном виде. Ну а для одаренного

хакера, как видим, даже этой минимальной утечки оказалось вполне достаточно, чтобы скомпрометировать всю систему.

С другой стороны, впрочем, яркий пример с Блэйзом не совсем хорош по той причине, что успех вскрытия тут полностью сведен к личным аналитическим талантам одного конкретного хакера. А значит, не позволяет увидеть общих черт и закономерностей, свойственных анализу побочных утечек в целом. Для взгляда на предмет именно в таком – обобщающем – аспекте куда лучше подходит история о методах криптохакинга, изобретенных и отточенных Полом Кочером во второй половине 1990-х годов.

Наиболее знаменитыми разработками этого исследователя (уже примерно лет двадцать возглавляющего небольшую, но весьма известную среди специалистов фирму Cryptography Research) являются в высшей степени эффективные способы криптоанализа, известные под названиями «таймерная атака» и «дифференциальный анализ питания».

Представляется далеко не случайной мелочью, что в область компьютеров и защиты информации Пол Кочер пришел как исследователь, в качестве основного имеющий за плечами профессиональное образование биолога. А хакерством электронных схем он занимался с детства забавы ради – в качестве занимательного хобби. И похоже на то, что именно биологические подходы к анализу живых организмов помогли Кочеру выработать свой собственный, весьма индивидуальный стиль анализа «черных ящиков» (как по традиции принято именовать стандартные объекты исследований криптохакинга).

Трактуя криптосистемы, зашитые в «черные ящики» микросхем, словно живые организмы и внимательно исследуя все доступные для наблюдений признаки их «жизнедеятельности», Кочер в буквальном смысле произвел революцию в академическом криптоанализе. Ибо в традиционном анализе криптоустройств и защищенных протоколов

всегда было принято предполагать, что злоумышленнику доступны сообщения на входе и выходе системы, а какая-либо информация о хранимых внутри данных (о криптоключах, к примеру) ему неизвестна.

Однако в реальной жизни любое электронное устройство состоит из конкретных элементов, которые выдают в окружающую среду информацию о своей работе. А значит, на самом деле атакующей стороне может быть доступна и всевозможная побочная информация, выдаваемая криптоустройством: электромагнитное излучение элементов схем, сигналы об ошибках или об интервалах времени между выполняемыми инструкциями, колебания в потреблении электроэнергии и другие подобные данные. Аккуратно фиксируя и анализируя эту информацию математическими методами, Кочер на множестве примеров показал, что побочных утечек схемы вполне достаточно для извлечения секретных криптоключей.

Вообще говоря, принципиальная возможность подобных вещей давно и прекрасно известна военным и спецслужбам, где разработаны специальные методы работы с побочными каналами компрометации. Но тема эта – под кодовым наименованием Tempest – строго засекречена и открытых публикаций о ней крайне мало (подробнее об этом см. в текстах «Секреты дальночувствия» и «Мужчины с ошеломительным оснащением»).

Ну а Пол Кочер и его коллеги по команде, можно сказать, творчески переизобрели секретные методы спецслужб и научились собственными методами деликатно преодолевать защиту таких криптоустройств, которые прежде считались весьма безопасными – вроде смарткарт или серверов, обеспечивающих онлайновую торговлю в интернете.

Точно замеряя флуктуации в потреблении чипом электропитания или интервалы времени, нужные программе на отдельные этапы онлайновых транзакций (а также привлекая для анализа продвинутый аппарат матстатистики и алгебраических методов исправления ошибок), хакеры Cryptography Research продемонстрировали, что реально возможно извлекать криптоключи практически из любых устройств защиты информации, широко распространенных на коммерческом рынке…

Звуки и прикосновения

Воистину поразительные, революционные для своего времени достижения Кочера и его коллег произвели на сообщество инфобезопасности чрезвычайно сильное впечатление. С конца 1990-х готов степень защиты системы от таймерных атак и атак по питанию стала регулярно входить в набор стандартных критериев, по которым оценивается уровень безопасности криптоустройства.

Иначе говоря, смарткарты с тех пор укрепили, старое криптографическое ПО переписали и сменили, а новое программное обеспечение стараются делать посильнее. Однако и биологические идеи «экстрасенсорного» хакинга не только продолжают жить, но

и более чем успешно развиваются. В частности, за последнее десятилетие весьма впечатляющий прогресс достигнут на акустическом и тактильном, так сказать, направлениях в анализе побочных утечек.

Начало этой истории логично отсчитывать с весны 2004, когда два известных израильских ученых-криптографа, Ади Шамир и Эран Тромер (Adi Shamir, Eran Tromer), опубликовали в Сети любопытную работу о возможностях дистанционного съема секретной информации с компьютера – исключительно по звукам работы его электронных схем.

В статье Шамира и Тромера было особо оговорено, что исследование их носило сугубо предварительный оценочный характер, однако даже этих данных ученым хватило для следующего вывода: анализ акустических сигналов, порождаемых при работе ПК, убедительно демонстрирует, что звук является на удивление богатым источником информации о работе процессора.

В частности, анализируя характерные особенности спектра звукового сигнала от компьютера, исследователи показали, что конкретные криптооперации процессора не только имеют вполне характерную акустическую сигнатуру, но даже есть возможность без труда выделять раздельные этапы возведения в степень больших чисел (модулей P и Q), лежащих в основе стойкости популярного криптоалгоритма RSA (Ади Шамир, кстати, это буква S в названии шифра, составленного из имен его авторов).

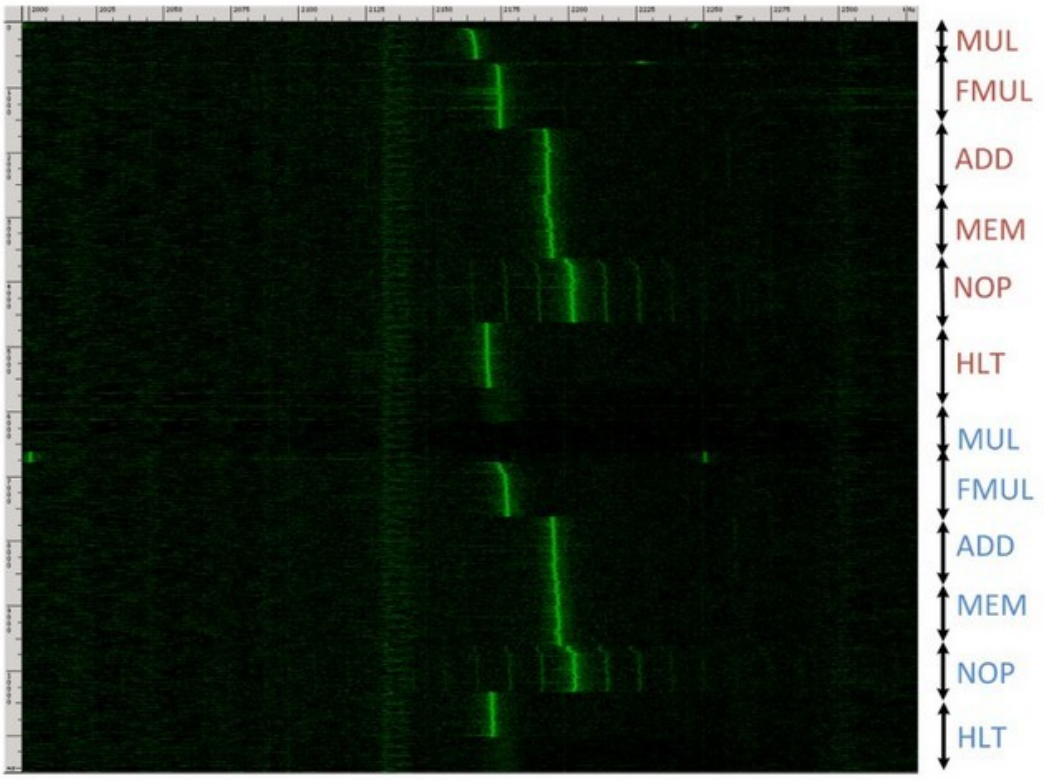
Отсылая к общеизвестным к тому времени работам Пола Кочера, израильские ученые напомнили, что по опыту дифференциального анализа питания и таймерных атак, такого рода данных бывает уже вполне достаточно для восстановления самих значений P и Q, а значит, и для вскрытия ключа RSA…

Дальнейшие события вокруг этого интересного открытия израильтян сложились таким образом, что от фазы первичного анализа до демонстрации реальной полноценной атаки через акустический канал утечек прошло полных десять лет. Почему так долго, теперь уже и не суть важно, наверное. А важно то, что молодой коллега Шамира и Тромера, Даниэль Генкин, не только помог успешно завершить давнее перспективное исследование, но и существенно продвинуть наработанные методы анализа в другие области «экстрасенсорного хакинга».

Массу подробностей о добыче секретной информации по звукам работы аппаратуры можно найти в материалае «Крипто-акустика» и непосредственно на веб-странице исследователей Acoustic Cryptanalysis . Ну а здесь – для финала – самое время в нескольких словах рассказать, как те же самые, по сути, методы были развиты за последний год.

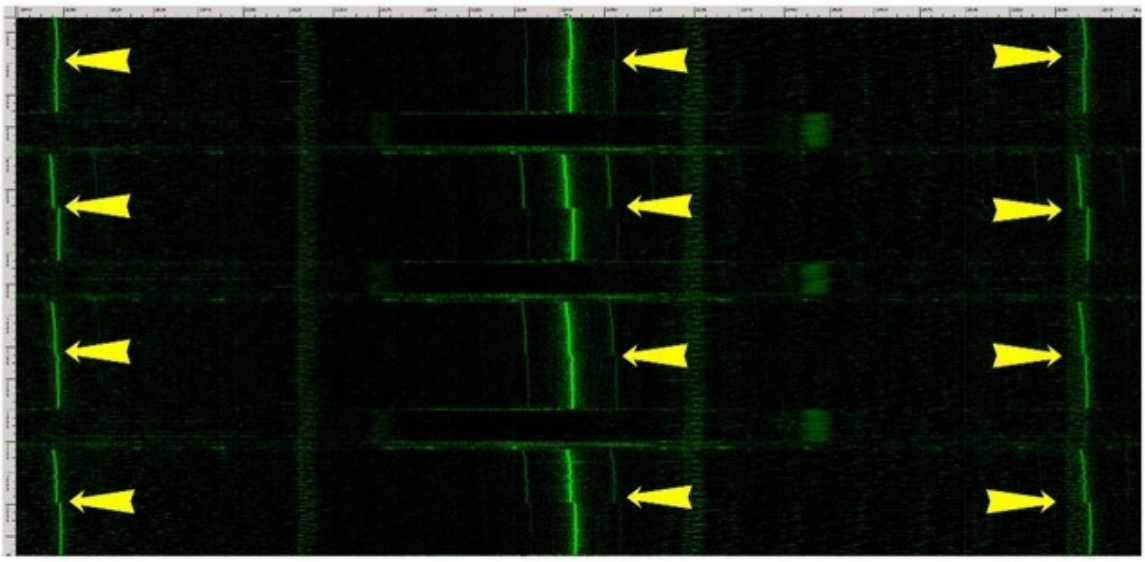
Сентябрьский доклад израильтян на эту тему в рамках конференции CHES 2014 сосредоточен на теме компрометирующих утечек аппаратуры через каналы заземления.

Иначе говоря, теперь команда исследователей (Genkin, Pipman, Tromer) разрабатывала тот факт, что «земля» или электрический потенциал заземления компьютера в большинстве случаев отнюдь не постоянен, а претерпевает постоянные флуктуации. При этом – по уже известной схеме – колебания потенциала «земли» происходят вычислительно зависимым образом от того, что за задачу решает в данный момент компьютер.



Частотная спектрограмма для потенциала шасси ноутбука Lenovo 3000 N200, когда ЦПУ компьютера выполняет различные вычислительные операции.

С позиций криптохакинга это означает, что человек атакующей стороны может незаметно измерять этот сигнал – либо подсоединив провод к выступающей наружу металлической части компьютерного шасси, либо даже просто касаясь машины голой рукой. Ну а кроме того, этот же сигнал может быть измерен и на удаленном конце от компьютера – через «землю» выходящих из него кабелей Ethernet, VGA или USB.



Измерения сигнала от шасси в диапазоне 1.9-2.6 MHz, когда в программе GnuPG происходит вычисление четырех сигнатур RSA. Переходы между модулями P и Q отмечены желтыми стрелками.

Итогом проделанной работы стала абсолютно реалистичная атака, в ходе которой – как показали исследователи – можно извлекать из ноутбуков, шифрующих информацию популярной криптопрограммой GnuPG, секретные ключи RSA длиной 4096 битов и ключи ElGamal длиной 3072 битов. В зависимости от условий доступа к аппаратуре, эти атаки требуют либо всего лишь нескольких секунд измерения при работе с сигналами в среднечастотном диапазоне (около 2 МГц), либо же порядка одного часа – при опоре на низкочастотные сигналы (до 40 килогерц).

Как обычно, массу подробностей о данной работе можно найти на сайте исследова-

Адаптивная атака «человеческое прикосновение» с помощью голой руки. Браслет на другой руке подсоединен к измерительному проводу.

телей (www.cs.tau.ac.il/~tromer/handsoff/) и в их PDF-статье, подготовленной для доклада на конференции (http://eprint.iacr.org/2014/626).

# # #

Дополнительное чтение

О роли и месте хакеров в общей истории человеческой культуры: «**Новая мифология**».

О разносторонних талантах профессора-криптографа Мэтта Блэйза: «**Хакер, слесарь, экстрасенс**».

Об особенностях побочных компрометирующих излучений и важнейших этапах в истории их исследований: «**Секреты дальночувствия**», «**Мужчины с ошеломительным оснащением**».

Об одном из наиболее экзотичных разделов криптографического анализа: «**Криптоакустика**».

Неизвестные страницы известных событий

Если дело дойдет до суда…

(*Июль 2001*)

«Тело похоронить в неизвестном месте, имя мое и память отдать на милость людской молвы другим векам и народам, **а также моим собственным соотечественникам по прошествии некоторого времени**»…

(Из черновика завещания Фрэнсиса Бэкона, где выделенные жирным шрифтом слова были автором вычеркнуты и не вошли в окончательный вариант документа.)

Вынесенные в эпиграф загадочные строки весьма плохо прикладываются к биографии и творчеству Фрэнсиса Бэкона (1561-1626), одного из умнейших людей своего времени и автора более чем двух десятков работ, опубликованных и получивших признание современников еще при жизни этого философа и видного государственного деятеля.

Но туманные намеки завещания становятся куда яснее, если вспомнить веками длящиеся споры об истинном авторе произведений, приписываемых историей современнику Бэкона по имени Уильям Шекспир (1564-1616).

На сегодняшний день собрано более чем достаточно фактов и аргументов для объективного восстановления исторической справедливости, однако традиционно общепринятую точку зрения подпирает уже столь гигантская гора всякого рода литературоведческих трудов, что радикальная смена автора будет означать по сути дела катастрофу для многих научных авторитетов.

А потому на решение проблемы в рамках честного научного спора рассчитывать не приходится. Разве что через суд, с привлечением принятых в системе правосудия жестких методов экспертизы.

В этой связи уместно вспомнить довольно комичный сюжет из начала XX века – о судебном процессе в городе Чикаго, где местный судья Ричард Татхилл вник в доводы препирающихся сторон и властью своего вердикта объявил Фрэнсиса Бэкона автором всех шекспировских произведений.

Несколько позже, правда, Татхилл получил за это по шапке от вышестоящих инстанций, расценивших подобное литературно-историческое самоуправство как «превышение полномочий» обычного судьи.

Поскольку доводы, накопленные исследователями в течение XIX-XX веков, представляют безусловный научный интерес, имеет смысл рассмотреть хотя бы некоторую их часть для общего представления о сути проблемы. Попутно будут приведены и некоторые из аргументов, выдвигавшихся в достопамятном судебном разбирательстве в Чикаго.

Факты биографии

Свидетельств о жизни Шекспира крайне мало, но и те, что имеются, достаточно выразительны. Известно, что читать не умели ни родители величайшего писателя (что было естественно при незнатном происхождении), ни его собственные дети (что вызывает некоторое недоумение).

Нет ни одного документального подтверждения, что и сам Шекспир умел хоть сколько-нибудь бойко писать, поскольку не обнаружено ни рукописей его пьес или стихов, ни даже деловых бумаг, хотя в родном городе Стратфорде этот человек был известен не как писатель, а как бизнесмен.

Напомним, что молодой Шекспир появился в Лондоне практически нищим, а после весьма удачной карьеры в столичных театрах через много лет вернулся в Стратфорд достаточно зажиточным торговцем.

Известный как человек крайне прижимистый и изнурявший партнеров по бизнесу даже за копеечные долги, в своем завещании Шекспир скрупулезно, вплоть до чашек и ваз расписывает, кому какие предметы хозяйства оставляет, но ни словом не упоминает свои литературные произведения, большинство из которых еще даже не опубликовано. В завещании вообще ничего нет о книгах, даже других авторов, из чего очевидным образом следует, что в доме Шекспира такого добра просто не было.

На смерть известных людей было принято писать эпитафии. К примеру, на смерть драматурга Бена Джонсона, коллеги и приятеля Шекспира по Лондону, ученые имеют не менее 37 стихотворений-посвящений. На смерть Шекспира — ни одного. Не прореагировал никто, кроме шекспировского зятя, оставившего в личных записях строчку «тесть мой преставился».

Вообще, все факты свидетельствуют о том, что Шекспир умер как самый обычный, ничем неприметный торговец в тихом провинциальном городке. По сути дела, лишь спустя еще семь лет, когда в 1623 году в Лондоне был подготовлен канонический свод «произведений Уильяма Шекспира», так называемое «Первое фолио», начинается слава великого писателя.

Шекспировские пьесы и стихи публиковались и ранее, поначалу анонимно (скупой автор не предпринимал ни малейших усилий восстановить свои права на эти книги), затем в сравнительно небольших форматах «кварто». Но именно «Первое фолио» стало фундаментом мировой славы гения и именно это издание, вышедшее при жизни Фрэнсиса Бэкона, дает львиную долю свидетельств, указывающих на истинного автора.

Стилистическая и текстологическая экспертиза

В пьесах «Виндзорские проказницы», «Генрих IV», «Король Джон», «Ричард III» и «Отелло» в Первом Фолио добавлено около 4479 новых строк после того, как эти пьесы уже были опубликованы в изданиях «кварто», выходивших спустя 3-6 лет после смерти Шекспира.

Иными словами, какой-то неизвестный человек добавил от себя еще четыре с половиной тысячи строк через 7 лет после смерти гения, но с таким мастерством скопировал стиль автора, что нет никакой возможности отличить эти добавления от исходного текста.

Принято считать, что среднестатистический ремесленник или фермер использует в своем лексиконе около 500 слов, образованный деловой человек — примерно 3000, писатель средней руки порядка 5000 слов, а большой ученый — 7 тысяч слов.

В стихотворениях и пьесах Шекспира насчитана 21000 слов, причем столь гигантский лексикон не свойственен более никому из известных авторов за единственным исклю-

чением. Лишь для произведений Фрэнсиса Бэкона характерен столь же богатый вокабуляр, пересекающийся с шекспировским на 95%.

Случилось так, что авторам двух самых выдающихся по лексическому богатству наследий в мировой литературе довелось жить не только в одно и то же время, но и в одном и том же месте. Более того, в бэконовских и шекспировских произведениях допускаются одни и те же ошибки при цитировании античных авторов.

Наконец, в личных записных книжках Бэкона 1594-1596 годов, опубликованных позже как том «Promus», в изобилии зафиксированы идеи, мысли и разного рода удачные предложения, которые практически дословно затем обнаруживаются в более поздних шекспировских пьесах.

Подписи Бэкона и нумерологическая экспертиза

Первое Фолио, подготовленное к печати при жизни Бэкона, буквально побуквенно проштудировано целой армией дотошных исследователей. А если что-то очень хочется найти, то в том или ином виде оно непременно обнаруживается.

Например, собрание произведений открывает трагедия «Буря» (The Tempest), а самое первое слово пьесы – «Боцман» (Boteswaine) – начинается, как обычно, с буквицы, окруженной замысловатыми виньетками. В 1930-е годы среди этих виньеток исследователи разглядели многократно повторенное имя «Francis Bacon».

Другие подписи — нумерологические. Числовая подпись Бэкона равна 33. Люди, знакомые с нумерологией, знают, что вычисляется это очень просто — суммированием номеров букв в алфавите: B=2; A=1; C=3; O=14; N=13; итого 33. Для особо въедливых, но не слишком осведомленных следует отметить, что в эпоху королевы Елизаветы в английском алфавите было лишь 24 буквы, поскольку I и J писались как I, а также одной буквой обозначались U и V.

В Первой части пьесы «Генрих IV» есть фрагмент, где слово «Фрэнсис» встречается 33 раза на одной странице. В Первом Фолио все 33 раза имя уложено даже в одну колонку.

Для того, чтобы добиться такого результата, автору пришлось пойти на тяжеловесные до нелепости конструкции типа «Сейчас, Фрэнсис? Нет, Фрэнсис, но завтра, Фрэнсис; или, Фрэнсис, в четверг; или в самом деле, Фрэнсис, когда захочешь. Но Фрэнсис…». (В переводе Бориса Пастернака этой чудовищной тираде придан более пристойный вид: «Сейчас, Френсис? Нет, ты слишком нетерпелив. Сейчас нельзя. Но завтра или в будущий четверг, пожалуйста. Однако, Френсис…»)

Поскольку полное имя Francis Bacon имеет числовую подпись 100: F=6 R=17 A=1 N=13 C=3 I=9 S=18 итого=67; B=2 A=1 C=3 O =14 N=13 итого=33; то, теоретически, можно было бы ожидать, что и на 100-й странице Первого Фолио найдется какой-нибудь характерный «знак».

И действительно, в книге эта страница приходится на финал пьесы «Комедия ошибок», где Аббатиса говорит «тридцать три года провела я в непосильных трудах», хотя зафиксированные в пьесе события свидетельствуют, что данный период никак не мог быть более 25 лет.

Естественно, что подобные «виньеточные» и «нумерологические» доводы способны убедить лишь тех людей, кто априори верит в важность такого рода «знаков». Но имеются и более существенные аргументы.

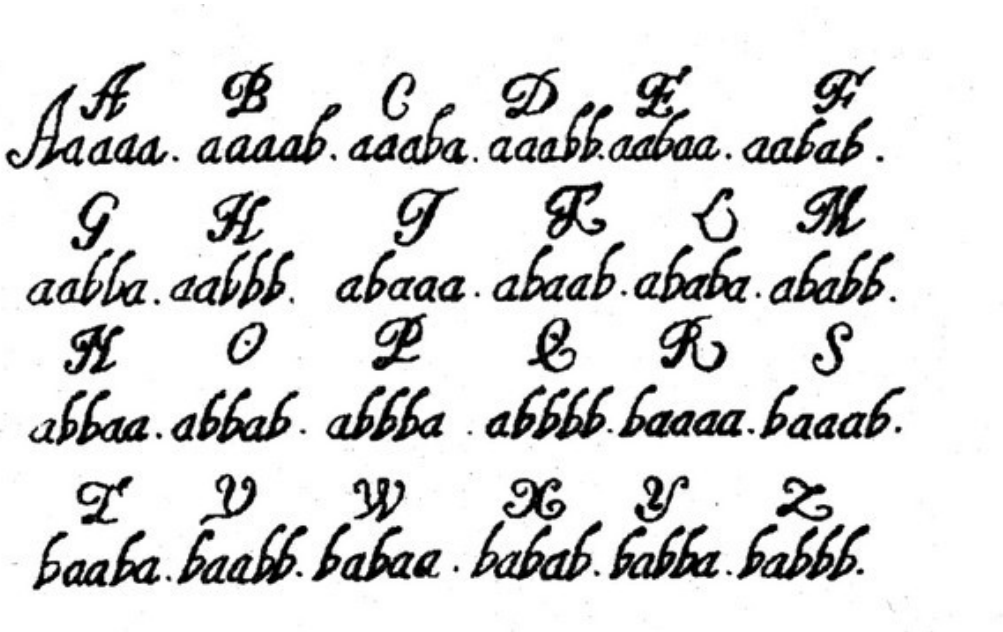
Криптографическая экспертиза

Наиболее серьезные криптографические доводы в пользу авторства Бэкона собраны в книге французского генерала Картье, опубликованной в 1938 году. Генерал Картье долгое время возглавлял шифрслужбу разведки Франции, наиболее отличившись на этом поприще в годы Первой мировой войны.

Следует также отметить, что в 1918 году в составе американского экспедиционного корпуса во Франции занимался вскрытием германских шифров и лейтенант Уильям Фридмен, будущий «отец-основатель» АНБ США. Оба криптографа, безусловно, были хорошо знакомы, благодаря чему у Картье завязалась переписка и с полковником Фабианом, покровителем не только Фридмена, но и Элизабет Уэллс Гэллап, главной

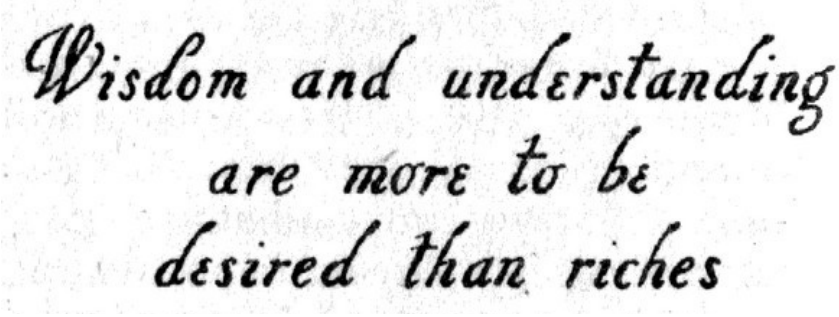
американской «криптографини-бэконистки» (подробности этой истории можно найти в материале «Наука a la Ривербэнк»).

Из писем Джорджа Фабиана генерал Картье и узнал впервые о своеобразном шифре, когда-то изобретенном Фрэнсисом Бэконом и описанном в двух его работах – «Успех познания» и «О достоинстве и приумножении наук».



Бэкон придумал эту систему тайнописи еще молодым человеком, назвав ее «двухбуквенным (или иначе, двухлитерным) шифром». По сути дела, это была стеганографическая бинарная система, поскольку с помощью шрифтов двух видов (названных A и B) в буквы произвольного текста скрытно вносилась дополнительная информация. Как видно из рисунка, каждой букве стеганограммы ставится в соответствие пять последовательных букв основного, маскирующего шифр текста.

Из следующего примера, приведенного в книге «О достоинстве и приумножении наук», можно видеть, насколько тонкими и неуловимыми могут быть признаки тайнописи, где весь смысл скрыт в нюансах различного начертания букв «i», «e», «d» и так далее.



Когда Картье ознакомился с этим шифром, Фабиан порекомендовал французу тщательно изучить одну страницу в первом издании книги Бэкона «Новый Органон». Раздобыв в парижской Национальной библиотеке эту редкую книгу и вооружившись для верности лупой, Картье обнаружил, что текст явно набран шрифтами двух видов.

Когда сам факт тайнописи был обнаружен, для профессионала-криптографа уже не составило особого труда разбить двоичную последовательность на буквы и вскрыть смысл зашифрованных слов…

Ну, а дальше пошла работа с другими текстами, в результате чего и появилась криптографическая книга Картье, в целом подтвердившая результаты удивительных изысканий миссис Гэллап, хотя и не обладавшей солидными титулами или чинами, но посвятившей своему делу более 30 лет жизни.

Проанализировав 34 книги XVII века, подписанных как Бэконом и Шекспиром, так и другими авторами данного круга, Гэллап восстановила «тайную и неизвестную» биографию Бэкона, доверенную лишь шифру. Конкретно о Шекспире в этой биографии, в частности, пишется следующее:

> *«Я писал разные пьесы — исторические хроники, комедии, трагедии. Большинство из них были поставлены в театре, где их автором объявляли Шекспира, и они, бесспорно, имели большой успех…*
>
> *Те из моих произведений, что были опубликованы, также подписаны его именем, поскольку я предпочел Шекспира другим, хотя они были ничуть его не хуже. Отдав однажды несколько моих пьес в его театр, я продолжу отдавать их ему и дальше, поскольку так он становится рабом моей воли…»*

Полностью оставим за пределами данного повествования соображения о причинах, побудивших гениального автора сначала к анонимности, а затем привязавших его к одному из выбранных псевдонимов.

Однако, для дополнительного подтверждения правильности изысканий Гэллап, выстроенных на довольно зыбкой — для неспециалистов — почве тонких различий в шрифтах, целесообразно привести еще один важный факт.

Следственный эксперимент

Изучая текст одного из авторов бэконовского круга, книгу Уильяма Роули «Воскрешение», вышедшую в 1657 году, миссис Гэллап наметанным взглядом наткнулась на место, зашифрованное по системе Бэкона.

В восстановленном ею фрагменте говорилось, в частности, следующее:

«В комнате (Фрэнсиса), в башне, есть тайник, в котором спрятаны редкие бумаги — рукописи Бэкона; чтобы найти тайник, нужно задвинуть пятую панель за пятидесятую».

Из контекста было вполне очевидно, что речь идет о Кэнонберийской башне, где Фрэнсис Бэкон жил в течение нескольких лет до 1619 года.

Накануне Первой мировой войны Гэллап приехала из Америки в Лондон и, сопровождаемая местным интендантом, отправилась исследовать Кэнонберийскую башню, хотя надежд на обнаружение тайника было, ясное дело, довольно мало.

Как это ни удивительно, но в большом зале башни настойчивая мадам действительно обнаружила пятьдесят панелей, расположенных по окружности в два ряда — 34 панели в нижнем ряду и 16 в верхнем. Чтобы определить нужную, Гэллап стала простукивать и надавливать на панели, как вдруг одна из них (пятая в верхнем ряду) сместилась и ушла вниз, за крайнюю в нижнем ряду («пятидесятую»)…

Увы, за панелью оказалась глухая стена. Но тут сам интендант припомнил, что однажды по какой-то причине эта панель уже проваливалась за соседнюю, в результате чего в стене обозначилась дыра, поэтому вызвали каменщиков и они данную нишу заделали.

Короче говоря, тайник в башне действительно был, хотя и давно опустевший.

Но если вспомнить, сколь необычным способом вышла на него миссис Гэллап, то нельзя не признать, что все результаты ее изысканий заслуживают значительно более пристального внимания профессиональных историков и литературоведов.

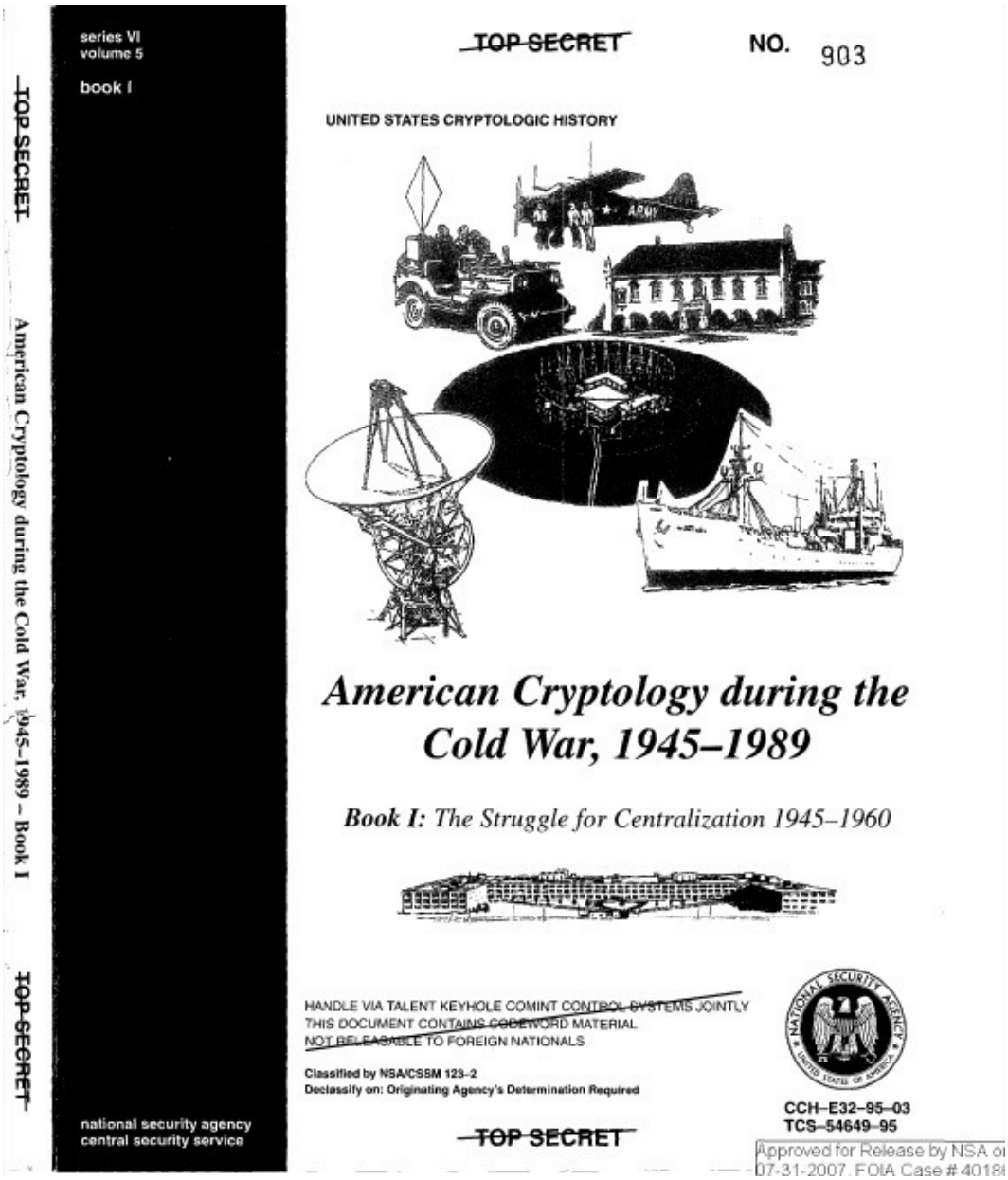
Сколь бы экзотическими эти результаты ни выглядели.

# # #

Чтение между строк

(*Март 2009*)

Спецслужба АНБ США искусно рассекретила свою историю, не раскрыв никаких секретов.



На официальном сайте Агентства национальной безопасности США, www.nsa.gov, уже многие годы регулярно выкладываются для всеобщего доступа рассекречиваемые документы из закрытых архивов этой спецслужбы. Наиболее примечательные из подобных материалов, также как и аналогичные документы с сайтов других американских спецслужб, вроде ЦРУ или ФБР, позволяющие узнать массу нового и интересного о тайных страницах новейшей истории, освещаются в СМИ регулярно.

Попутно с этими рассказами приходится то и дело сетовать, что в России, к сожалению, все никак не появится так называемый «Закон о праве граждан на доступ к информации». То есть закон, позволяющий, как в других демократических странах, любым честным налогоплательщикам послать официальный запрос на получение интересующих их документов о деятельности финансируемых ими государственных органов, будь они хоть секретные или какие угодно еще.

У нас такой закон был бы особо актуален, принимая во внимание, что огромная часть секретных архивов СССР, приоткрывшихся было в начале 1990-х, довольно быстро российскими властями была пересекречена и вновь стала недоступной для исследователей.

Рано или поздно, надо полагать, и в нашей стране граждане научатся требовать и получать от государства документальные отчеты о своей работе. Ну а пока этого нет, полезно почаще знакомиться с тем, как подобные вещи происходят в других государствах.

В тех же США, к примеру, где в январе этого (2009) года на сайте АНБ в публичный доступ был выложен очередной очень интересный и объемистый документ под снятым грифом TOP SECRET и названием «Американская криптология в годы Холодной войны, 1945-1989» [*Thomas R. Johnson, "American Cryptology during the Cold War, 1945-1989". National Security Agency: Center for Cryptological History, 1998, Top Secret Umbra, Excised copy*].

Контекст вместо секретов

Как и в ситуациях с раскрытием практически всех прочих материалов подобного рода, этот многотомный исторический обзор АНБ рассекретило отнюдь не по собственной инициативе, а благодаря настойчивым запросам извне – в данном случае, стараниями известного историка разведки Мэтью Эйда. О существовании данного монументального труда объемом свыше 1000 страниц Эйд прознал по сути дела случайно, но зато непосредственно от автора книги, ветерана АНБ Томаса Джонсона, с которым пересекся в кулуарах одной из научных конференций, посвященных истории разведслужб.

Эйд увлекся идеей вытащить книгу из секретных архивов и в 2006 объединил усилия с «Архивом национальной безопасности» при университете Джорджа Вашингтона, вместе с которым они составили официальный запрос на получение 4-томного отчета. К концу 2007 года АНБ обработало запрос и передало им первые три тома, полностью исключив из них порядка сотни страниц, которые были сочтены чересчур чувствительными к разглашению. Почти все остальные страницы в изобилии прорежены удалениями отдельных абзацев, строк и слов.

Тем не менее, признает Эйд, он был буквально ошеломлен столь редким подарком. В первую очередь, потому что по всей книге видно – она явно предназначалась исклю-

чительно для внутреннего употребления в стенах спецслужбы. Примерно около года после этого Эйд кропотливо работал над текстами сам, в других доступных источниках добывая недостающую информацию и восстанавливая целостную картину, ныне представленную им в собственной книге «Тайный караул. Совершенно секретная история Агентства национальной безопасности» [*Matthew Aid, "The Secret Sentry: The Top Secret History of the National Security Agency". Bloomsbury, 2009*].

Когда монография Эйда была закончена, то имевшиеся три первых тома истории АНБ университет Джорджа Вашингтона в конце прошлого года выложил для всеобщего доступа на своем сайте «Архив национальной безопасности» (www.gwu.edu/~nsarchiv/), добавив их к целой онлайн-библиотеке подобных материалов, получаемых по индивидуальным запросам из секретных государственных хранилищ. Лишь после того, как PDF-файлы с частями книги появились на сайте Университета, в АНБ решили опубликовать их также и у себя, в комплекте с целым рядом других рассекреченных документов похожей исторической тематики.

По свидетельству всех, кто уже успел ознакомиться с книгой «Американская криптология в годы Холодной войны», эта работа предоставляет историкам редкую возможность заглянуть непосредственно внутрь агентства, которое в обстановке строжайшей секретности добывает разведывательную информацию через перехват и дешифрование коммуникаций. Однако при первом же взгляде на эти крайне интересные материалы становится очевидно, что там отсутствует одна очень важная вещь – описания и даже упоминания о крупнейших успехах этой мощной спецслужбы.

Явно не желая раскрывать слишком много, в АНБ самым тщательным образом вычистили из текста книги все мало-мальски содержательные факты и фрагменты, которые – по свидетельству сведущих экспертов – излагают хронику подлинных прорывов в криптоаналитической разведке. Вся же прочая информация, оставшаяся в текстах после изъятий цензуры, создает у читателя такое впечатление, будто самое большое в мире шпионское ухо то и дело страдало приступами глухоты.

Комментируя столь своеобразную подачу материала, Мэтью Эйд говорит так: «Для АНБ это была прекраснейшая возможность представить себя в самом наилучшем свете. А вместо этого перед вами предстает картина разведывательного агентства, работавшего где-то на уровне между неплохо и посредственно».

С другой стороны, тут же подчеркивает Эйд, одна из вещей, делающих книгу Томаса Джонсона поистине уникальной среди всего ряда официальных историй, «это ее освежающая открытость и честность, в равной доле признающая как впечатляющие успехи АНБ, так и тяжелейшие провалы в годы Холодной войны».

Для примера, напоминает Эйд, большинство несекретных исторических работ, выпущенных Центром исследований разведки при ЦРУ, сфокусировано на тех исторических эпизодах или системах добычи информации, которые были бесспорно успешны-

ми – вроде историй о легендарном самолете разведки U-2 или недавно рассекреченная история проекта «Берлинский туннель» (1954-1956).

Однако ЦРУ упорно и последовательно отказывается рассекречивать те из своих историй, которые были куда менее успешными. Такие, в частности, как примечательные провалы в попытках организации тайных операций и сбора разведывательной информации через агентуру на территории СССР и Восточной Европы в 1940-е и 1950-е годы. Или те же самые неудачи с Китайской народной республикой в период 1950-х и 1960-х годов.

Что касается собственно автора рассекреченной ныне книги об АНБ, Томаса Джонсона, то он всячески уклоняется от прямого ответа на вопрос, насколько отредактированная цензорами история отличается от его оригинальной версии. Другие же эксперты по разведке свидетельствуют, что для АНБ это совершенно обычная практика – побольше делать достоянием гласности провалы, нежели успехи, потому что достижения в этой сфере разведки нередко могут быть слишком уж хороши, чтобы их раскрывать (см. врезку «Проект BORIS»).

Публикация даже старых успехов, говорят они, может невольно раскрыть и поныне утаиваемые источники, дать нежелательные подсказки о продолжающихся разведывательных усилиях или же повредить дипломатическим отношениям.

Например, когда АНБ несколькими годами ранее рассекретило материалы о дешифровальной активности американского правительства в годы второй мировой войны, то тут же последовала критика со стороны коллег из Госдепартамента, крайне недовольных тем, что всплыли факты систематического шпионажа Америки за собственными союзниками.

[ВРЕЗКА]

Проект BORIS

Одна из наиболее важных тайных операций АНБ, запущенная еще в 1950-е годы, среди историков разведки носит условное наименование «проект Boris». Это название пошло от имени весьма известного предпринимателя, Бориса Цезаря Вильгельма Хагелина (Boris Caesar Wilhelm Hagelin), в годы второй мировой войны сделавшего состояние на шифраторах для армии США, а в послевоенный период основавшего в Европе знаменитую и поныне корпорацию Crypto AG.

После окончания войны в мире отчетливо обозначился растущий спрос на современные шифраторы – для закрытия важных коммуникаций не только в военных, но также в дипломатических, банковских и промышленных системах связи. Однако собственную криптоиндустрию имели по преимуществу лишь наиболее мощные державы, вроде США, Англии или Германии.

Однако все они входили в однозначно проамериканский блок НАТО, а многие государства, особенно неприсоединившиеся к НАТО или Варшавскому пакту, имели вполне разумные основания не доверять криптографии, сработанной в одном из враждующих блоков.

По этой причине в нейтральных странах с внушительным научно-промышленным потенциалом, вроде Швейцарии или Австрии, сложились очень благоприятные условия для расцвета бизнеса независимых криптофирм, шифраторам которых все могли бы доверять свои секреты примерно так же, как доверяют деньги швейцарским банкам.

Уже к середине 1950-х годов швейцарская фирма Crypto AG была на рынке коммерческих шифраторов примерно тем же, чем корпорация General Motors на рынке автомобильном. В такой обстановке руководство АНБ в 1957 г. направило в Европу с чрезвычайно деликатной тайной миссией Уильяма Фридмена (William F. Friedman), одного из ветеранов-основателей американской криптослужбы и просто авторитетнейшего криптографа.

Фридмен имел не только хорошие связи в западноевропейских разведках еще с первой мировой войны, но и лично был прекрасно знаком с Хагелином со времен его бизнеса в Америке. (Примечательно, что Фридмен и Хагелин родились почти в один год на территории Российской империи – первый в семье местечковых евреев в Бессарабии, а второй в семье шведского инженера-нефтяника в Баку.)

Итоги и сам факт секретных переговоров Фридмена с изготовителями шифраторов в Швейцарии по сию пору остаются большой государственной тайной. Однако в 1990-е годы целый ряд журналистских расследований и собранные ими документальные свидетельства убедительно продемонстрировали, что в результате закулисного сговора коммерческие шифраторы от фирм западных нейтральных стран, в частности Crypto AG, на протяжении десятилетий имели искусственно ослабленные криптосхемы, облегчавшие их вскрытие для АНБ США.

[КОНЕЦ ВРЕЗКИ]

Факты истории

Историю АНБ, англоязычную аббревиатуру которого – NSA – до недавних пор в шутку расшифровывали как No Such Agency, т.е. «Нет такого агентства», принято отсчитывать от секретного президентского указа Гарри Трумена 1952 года, когда на основе нескольких радиоразведывательных структур в вооруженных силах США было создана единая спецслужба для перехвата и дешифрования электронных коммуникаций. Лишь спустя 16 лет полномочия этого особо секретного агентства были официально зафиксированы в американском законе.

Еще через несколько десятилетий по трем самостоятельным поводам в АНБ вставал вопрос о написании собственной истории, однако каждое из этих начинаний было в свое время прекращено из-за гигантских масштабов работы в условиях чрезвычайной секретности. Наконец, к 40-й годовщине АНБ руководство агентства поручило одному из ветеранов спецслужбы, Томасу Джонсону, предпринять еще одну попытку.

На написание этого исторического отчета у Джонсона ушло свыше шести лет. Вся работа была поделена им на 4 тома или 4 эры в работе радиоразведки (1945-1960: Борьба за централизацию; 1960-1972: Централизация побеждает; 1972-1980: Сокращения и реформы; 1980-1989: [пока не раскрыто]). Когда в годы работы над книгой друзья Джонсона, не имевшие высоких допусков к гостайне, спрашивали о том, как скоро им удастся прочесть сей монументальный труд, автор обычно им отвечал: «Все мы давно уже будем на том свете, когда это разрешат рассекретить».

В 1998 году Джонсон завершил, наконец, свой отчет, а на следующий год уволился из АНБ после 35 лет службы. Все страницы его работы были проштампованы суровым грифом TOP SECRET UMBRA, что на жаргоне агентства означает материал не просто совершенно секретный, а чрезвычайно чувствительный к внешним разглашениям.

Сегодня, когда все грифы гостайны с отчета неожиданно оказались сняты, то с точки зрения простых американских (а также российских и всех прочих) читателей, неосведомленных в тонкостях криптографии, как одно из наибольших откровений этой книги воспринимается полная неспособность США на протяжении десятилетий взломать секретные советские коммуникации – после памятного дня в октябре 1948 года, который в АНБ получил название «Черной пятницы». В этот день власти СССР резко сменили шифры на всех своих важных линиях связи.

Хотя формально АНБ в тот период еще не существовало, военные криптологические спецслужбы-предшественницы, конечно же, работали в США очень активно. История Джонсона предоставляет несколько важных эпизодов из тех лет, включая и энергичную борьбу с шифрами Советского Союза. В частности, подробно описана предыстория атак АНБ на советские шифры в годы второй мировой войны, включая детали об успешной англо-американской операции Venona по вскрытию одноразовых шифр-блокнотов советской разведки (оказавшихся «не совсем одноразовыми»).

[ВРЕЗКА]

Проект TICOM

Американский исследователь и публицист Джеймс Бэмфорд (James Bamford) известен как автор целого ряда весьма информативных книг об АНБ США и с начала 1980-х годов имеет репутацию одного из ведущих независимых экспертов по истории этой спецслужбы. В конце 1990-х годов, работая над одной из своих книг, «Body Of Secrets», Бэмфорд раздобыл материалы о деятельности в последние месяцы второй

мировой войны некоего суперсекретного англо-американского «Комитета по целевой разведке» или кратко TICOM (Target Intelligence Committee).

Под эгидой TICOM зимой и весной 1945 года две сотни ведущих немецких криптографов были тайно переброшены из Германии в Великобританию для работы против СССР. Впоследствии, на протяжении нескольких послевоенных лет благодаря этому подразделению для США и Англии было обеспечено массовое дешифрование секретных советских коммуникаций – на основе средств и методов, разработанных криптоаналитиками нацистской Германии.

Начиналась же эта операция с того, что в марте 1945 года шесть специально подготовленных групп англо-американского спецназа были переброшены в Германию с конкретной целью захвата немецких криптографических центров. Задача групп TICOM состояла в том, чтобы заполучить столько германского криптооборудования, документации и специалистов, сколько окажется возможным. В результате одного из таких рейдов, к примеру, был захвачен замок в Саксонии, где находился архив радиоразведки германского МИДа, так что весь этот объект, включая и штатных сотрудников, был целиком переправлен в Британию.

В ходе другого рейда была вывезена специализированная 7-тонная вычислительная машина, с помощью которой немцы вскрывали шифры высшего эшелона советского военного командования. Когда это оборудование вывезли и смонтировали под руководством германских специалистов, машина заработала и действительно начала дешифровать важную секретную переписку СССР.

В целом же, как свидетельствуют добытые Бэмфордом документы, собранные TICOM данные позволили англо-американской разведке впоследствии читать не только советские шифры, но и секретную переписку по крайней мере 35 стран, включая Францию, Италию, Японию, Испанию, Швейцарию и Ирландию.

В рассекреченной ныне книге Т. Джонсона деятельность TICOM несколько раз упоминается, однако без каких-либо подробностей и фактов по существу.

[КОНЕЦ ВРЕЗКИ]

Но к сожалению, как отмечает в своих комментариях к книге Мэтью Эйд, пока что АНБ категорически отказывается рассекречивать тот раздел в своей истории, что относится к «Черной пятнице». Известно лишь то, что всеобщая смена советских кодов и шифров в 1948 году абсолютно эффективно уничтожила весь англо-американский криптоаналитический доступ к секретным коммуникациям Москвы высокого уровня.

В значительной степени именно по этой причине разведслужбы США были крайне удивлены, обнаружив, что СССР в сентябре 1949 года провел испытание собственной ядерной бомбы. Четыре года спустя с таким же удивлением они обнаружили, что на

одном из советских полигонов взорвали бомбу водородную. Под большим впечатлением от этих провалов разведки в правительственных кругах США стали звучать голоса, что весьма недешевые усилия по взлому советских шифров «являются безнадежными, а потому пора прекращать их финансирование».

Еще один весьма важный элемент в истории АНБ, вряд ли, впрочем, являющийся для кого-то большим секретом, – это тяжелейшие междоусобные битвы, которые АНБ приходилось вести с родственными спецслужбами, особенно с Центральным разведывательным управлением. Наиболее впечатляющий пример этой войны из начального периода истории дает эпизод с «Берлинским туннелем».

ЦРУ совершенно умышленно полностью отрезало АНБ от какого-либо участия в операции с подкопом и доступом к важным коммуникационным кабелям советских сил и ГДР на территории Восточного Берлина в 1954-1956 годах. Тогдашний (он же первый) директор АНБ, генерал Ральф Кэнайн (Ralph Canine), как и миллионы рядовых американских граждан узнал об этой операции из газеты «Нью-Йорк Таймс» после того, как советская сторона обнаружила этот туннель в апреле 1956 года.

Еще один весьма драматичный эпизод в истории американских спецслужб – это знаменитый Карибский ракетный кризис начала 1960-х годов. Книга Джонсона признает, что радиоразведка не смогла выявить никаких признаков, указывававших на то, что СССР разместил на Кубе наступательные баллистические ракеты. Обнаружили их лишь в ходе полетов U-2, разведывательного самолета ЦРУ в октябре 1962 года.

Этот провал имел весьма значительные последствия для падения авторитета АНБ, поскольку еще с первых дней администрации Эйзенхауэра разведывательное сообщество США зависело от АНБ примерно на 90% в той части своих разведданных, что предупреждали о советской стратегической угрозе для Америки.

Если говорить о 3-й книге отчета Джонсона, посвященной очень непростому для АНБ периоду 1970-х годов, то этот том администрация агентства, ведающая процессом рассекречивания, вымарала чрезвычайно обильно. Тем не менее, историки все равно отыскивают там некоторое число весьма интересных фрагментов, прослаивающих массивные изъятия цензуры.

Например, хотя 1970-е были периодом уменьшения бюджета и существенных штатных сокращений в Форт-Миде, штаб-квартире АНБ, агентство сумело-таки до некоторой степени восстановить доступ к советским шифрованным коммуникациям в годы администрации президента Картера. На этот успех, а также на ряд других криптоаналитических достижений указывает лишь единственная коротенькая фраза, которую цензура не удалила из текста Джонсона: «Даже в условиях урезанного финансирования криптология выдавала самую лучшую информацию из всего, что ей удавалось добывать со второй мировой войны».

Косвенно этот успех подтверждает и оставленный цензорами фрагмент с обсуждением темы советского вторжения в Афганистан. Согласно книге Джонсона, «обобщенные предупреждения о возможном вторжении начали поступать в сентябре, а специфические предупреждения предшествовали операции по крайней мере дней на десять». Впоследствии Белый дом квалифицировал эту добывавшуюся криптоаналитиками АНБ информацию как несомненный разведывательный успех…

В ожидании тома 4

Интересно отметить, что сам автор книги, Томас Джонсон, когда узнал, что один из экземпляров его труда рассекречен и передан университету, тоже захотел получить копию и для себя, для чего позвонил своей давней знакомой, занимающей заметный пост в АНБ. Однако бывшая коллега никакой книги автору не дала.

По словам автора, «она сказала, что не уверена, хочет ли АНБ это сделать, потому что тогда я начну всем рассказывать об этом, а им надо сначала самим разобраться со сложившейся ситуацией»… В итоге из АНБ Джонсону так больше и не перезвонили, поэтому ему пришлось получить копию своей же работы из рук Мэтью Эйда.

Сейчас историки энергично работают над тем, чтобы заполучить в свое распоряжение и последний, четвертый том «Американской криптологии». Как рассказывает Джонсон, последняя часть, охватывающая 1980-е годы, содержит среди прочего «несколько эпизодов, когда кое-кто наделал здесь очень большие ошибки, за которые по справедливости следовало бы увольнять».

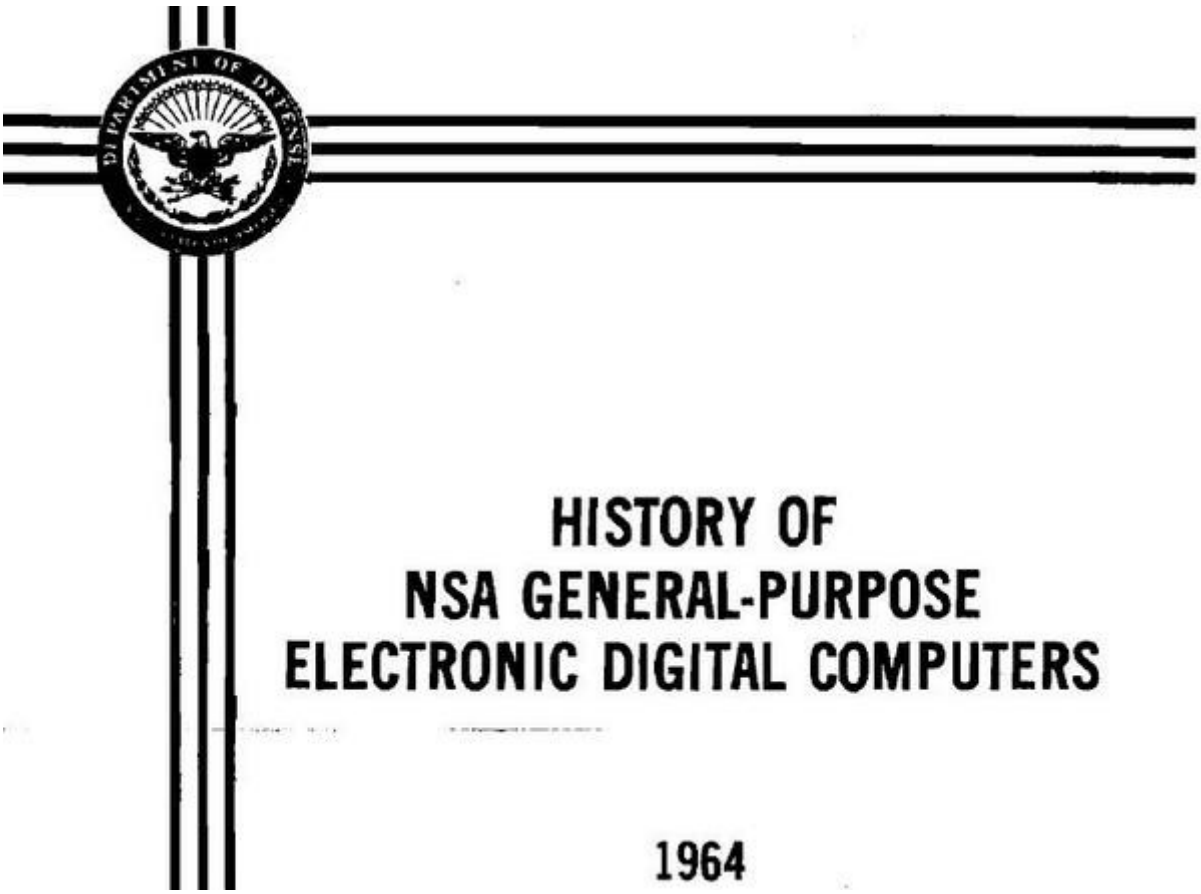
Автор надеется, что эти весьма поучительные для истории эпизоды из четвертого тома со временем всплывут, однако пока что весь данный период остается строго засекреченным.

# # #

Тайная история компьютеров

(*Май 2010*)

Раскрытие документов из секретных архивов всегда проливает дополнительный свет на известные исторические события. Ныне можно узнать кое-что новое о роли АНБ США в компьютерной революции.



Несколько дней назад, 17 мая (2010), в интернете опубликован любопытный документ, рассекреченный Агентством национальной безопасности США и содержащий неизвестные прежде сведения относительно подлинной истории рождения компьютерных технологий.

Документ этот, объемом около 100 страниц, носит название «История электронных цифровых компьютеров АНБ общего назначения», для внутреннего употребления в агентстве он был подготовлен аж в 1964 году, а автором работы являлся один из старейших сотрудников американской спецслужбы Сэмюэл Снайдер (Samuel S. Snyder, 1911-2007).

Работа Снайдера в американской криптоаналитической разведке началась еще в 1936 году, когда единой структуры под названием АНБ не было даже в проекте, а существовали лишь раздробленные службы радиоперехвата и дешифрования в каждом из родов войск.

В одной из таких служб, U.S. Army Signal Intelligence Service, где вскрытием шифров потенциальных неприятелей командовал «отец» американской криптологии Уильям Фридмен (William Friedman), и началась служба Снайдера. В годы второй мировой войны он уже возглавлял несколько групп, весьма успешно вскрывавших военно-дипломатические шифры Японии.

После окончания войны Снайдер сыграл ведущую роль в разработке и создании вычислительной машины ABNER, по тем временам весьма мощной компьютерной системы для вскрытия шифров.

В одном из интервью 1990-х годов ветеран-криптограф рассказал, что свое название эта машина получила по имени персонажа комиксов — «Крошкой Абнером» звали здоровенного и очень сильного парня, который при этом практически ничего не знал. Наш ABNER выглядел чудовищно, вспоминал Снайдер, но это был самый сложный для своего времени компьютер.

В последующие годы на Снайдера были возложены обязанности по сопровождению разработки и программирования новых компьютерных систем, включая и знаменитую машину HARVEST. То есть один из первых компьютеров общего назначения, созданный совместными усилиями спецслужбы и IBM в качестве ответа на доминировавшую тогда систему Univac.

Когда несколько лет назад Сэмюэла Снайдера торжественно вводили в число героев «зала славы и почета» АНБ, то в приветственном адресе прозвучали слова о том, что его «новаторские работы над ранними компьютерами непосредственно привели к развитию тех компьютеров, которые мы знаем сегодня, и заложили основы для многих аспектов современной компьютерной индустрии»…

Короче говоря, более компетентного и знающего человека для подготовки обзорной работы о роли АНБ США в становлении компьютерных технологий и отыскать, наверное, было бы невозможно. Пересказывать же, пусть даже вкратце, содержание рассекреченного обзора в столь небольшой статье — дело совершенно нереальное. Однако хотя бы для общего представления о материале имеет смысл привести несколько упоминаемых Снайдером фактов.

Помимо контрактов на закупку и аренду вычислительной техники или совместной разработки инженерных подходов, важнейшим влиянием АНБ на индустрию было то, что запросы спецслужбы диктовали и непосредственно направляли прогресс в компьютерных технологиях. Вот лишь некоторые тому примеры.

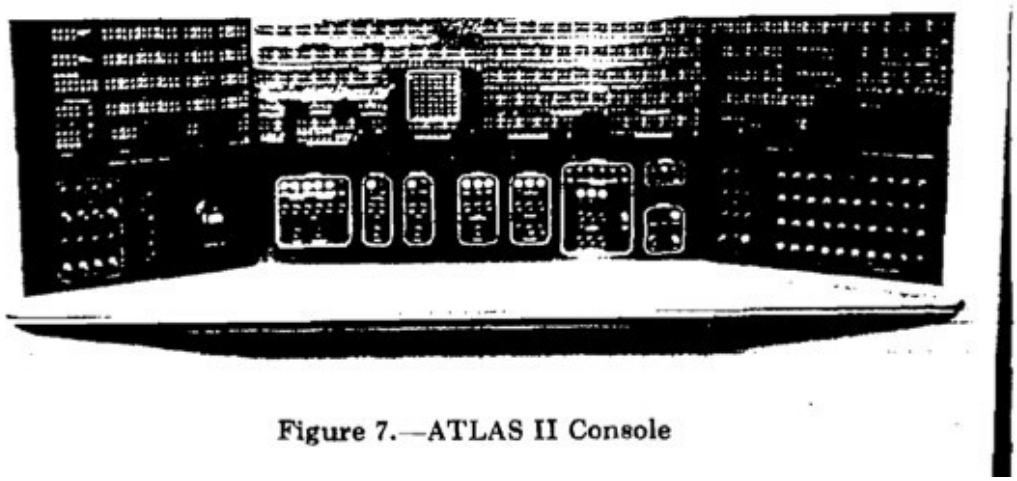


Figure 7.—ATLAS II Console

Финансирование спецслужбой работ по созданию машины ATLAS I вывело компанию Engineering Research Associates (ERA) на позиции одной из наиболее передовых компьютерных корпораций в стране. Последовавшие за этим коммерческие компьютеры ERA 1101 и 1103 были практически идентичны «секретным» машинам ATLAS I и ATLAS II. После слияния фирм ERA и Eckert-Mauchly Corporation в единую структуру под названием Remington-Rand-UNIVAC, машины 1101 и 1103 стали частью знаменитой линейки UNIVAC.

Еще один пример — контракт АНБ на создание системы NOMAD корпорацией Raytheon. Конструкция NOMAD явилась прямым предшественником компьютера Datamatic-1000, который затем трансформировался в первые машины линии Honeywell.

Раннее осознание в 1955 году того, сколь яркое будущее имеют транзисторы в качестве компонента электроники, подтолкнуло АНБ к финансированию SOLO, первого для спецслужбы практичного компьютера на транзисторах, разработанного корпорацией Philco. Позднее эта же машина стала известна на рынке как Transac 8-1000 — первый в мире коммерческий транзисторный компьютер.

Начиная с системы EDPM Type 701, чрезвычайно впечатляющим стало сотрудничество АНБ с корпорацией IBM. Очень мало кто осознает (писал Снайдер в 1964 году), что в основе ранней компьютерной философии IBM по преимуществу заложен опыт АНБ в решении проблем с обработкой больших массивов данных. Определенные особенности системы 704, составлявшие улучшения конструкции относительно модели 701, родились из предложений сотрудников АНБ. По аналогичной траектории модель 705 стала улучшенной версией машины 702.

Контракт АНБ на исследования и разработку передовой системы HARVEST, а также финансирование спецслужбой исследований по новым устройствам оперативной памяти и накопителям на магнитной ленте, не только сильно повлияли на конструкцию коммерческой машины IBM 7030 (STRETCH), но также — как формулирует это автор

работы — «привели к решению целого ряда фундаментальных проблем в машинной логике и обработке, никогда прежде не появлявшихся в компьютерной области».

Понятно, что для современного читателя, интересующегося историей компьютеров, было бы любопытно узнать, что же это были за «фундаментальные проблемы».

Однако обзор Снайдера был написан почти полвека назад, когда государственной тайной был даже сам факт существования в США спецслужбы под названием АНБ — разведывательного агентства, на регулярной основе вскрывающего шифры и читающего засекреченную переписку других государств.

А гриф секретности у данного документа даже изначально был явно небольшой, поскольку в нем — как это ни поразительно — нет ни одного появления терминов типа «шифр, криптография, дешифрование» и тому подобных слов. То есть из более чем 100-страничного обзора о компьютерных аспектах в работе АНБ вообще нельзя понять, чем же конкретно это агентство занимается.

Самих сотрудников АНБ, похоже, эти чрезмерные режимные строгости несколько раздражали. Спустя полтора десятка лет, когда со строгостями вокруг тайн криптографии стало несколько полегче, Снайдеру довелось написать для одного из внутренних журналов АНБ еще одну обзорно-историческую статью на примерно ту же самую тему.

В предисловии к этой статье он написал так:

> *«Неудачным аспектом исторических отчетов о создании вычислительной техники, публикуемых в открытой печати, является бросающееся в глаза (для некоторых из нас, по крайней мере) умолчание относительно роли криптологических организаций США. А также умолчание о тех вкладах данных организаций, которые помогали заложить основы всей компьютерной индустрии.*
>
> *АНБ и прочие предшествовавшие криптологические структуры были обязаны на протяжении многих лет соблюдать полную анонимность. И для этого были серьезные причины. Однако ныне, в эпоху применения компьютеров практически во всех областях цивилизованного общества, настало время признать их выдающиеся вклады в становление компьютерной промышленности».*

Найти в Сети электронные PDF-версии работ С. Снайдера можно по следующим адресам.

Большой исторический обзор начала 1960-х годов («History of NSA General-Purpose Electronic Digital Computers» by Samuel S. Snyder, 1964) выложен на архивном сайте www.governmentattic.org.

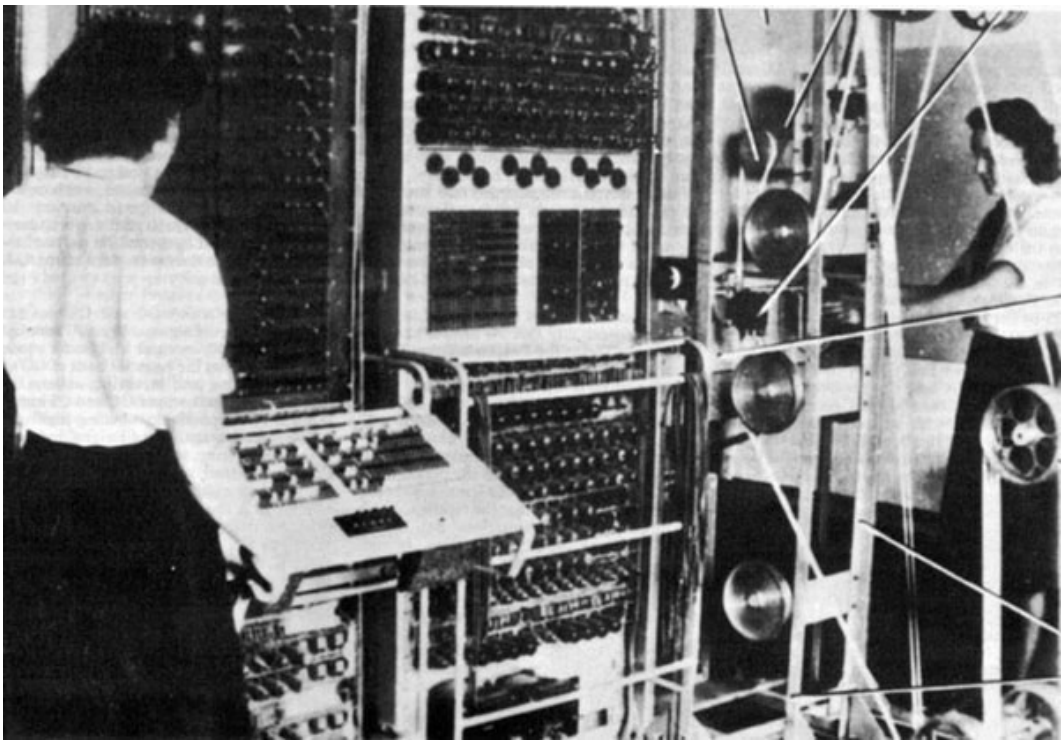
Более краткий обзор конца 1970-х годов («Influence of U.S. Cryptologic Organizations on the Digital Computer Industry» by S. SNYDER, Cryptologic Spectrum: Vol. 7, No.4, 1977 and Vol. 8, No.2, 1978), сконцентрированный на том влиянии, которое разработки АНБ оказали на компьютерную индустрию, выложен на официальном сайте спец-службы www.nsa.gov .

# # #

Колосс британский

(*Впервые опубликовано – июнь 2006*)

Факты и фактоиды из истории секретного предка компьютеров



Среди легендарных Семи чудес древнего мира видное место занимал Колосс родосский (ок. 292-280 гг. до н.э.) — гигантская, высотой более 30 метров бронзовая статуя бога Гелиоса, стоявшая у входа в главную гавань греческого острова Родос. Судьбе, увы, было угодно так, что срок жизни этого творения оказался самым малым среди всех «чудес света» — короче даже одной жизни человеческой.

В результате сильного землетрясения 225 года до н.э. статуя надломилась у коленей и обрушилась. На ее восстановление сил у родосских граждан уже не нашлось, однако останки рухнувшего колосса оставались на том же месте еще много веков, вплоть до 653 года н.э., пока не явились предприимчивые арабские разбойники и, измельчив статую, продали ее как металлолом сирийскому купцу. Для транспортировки груза в Сирию, согласно преданию, был снаряжен караван из 900 верблюдов.

Много-много лет спустя, в середине XX века на совсем другом острове – Британия – в тихой викторианской усадьбе Блечли-Парк был сооружен еще один выдающийся колосс, на этот раз компьютерный. По странной иронии судьбы это грандиозное творение рук человеческих разделило со своим родосским предшественником не только имя Colossus, но и основные черты биографии — очень яркую поначалу и в то же время совсем короткую жизнь, закончившуюся полным и бесславным демонтажом.

Специфика новой эпохи, правда, внесла в этот исторический повтор и некоторые коррективы. Поскольку компьютер Colossus создавался для суперсекретных задач вскрытия шифрованной иностранной переписки, то сам факт его существования более полувека продолжал официально оставаться большой государственной тайной.

А потому вычислительная машина хоть и была для своего времени бесспорным «чудом света», однако человечество об этом и ведать не ведало. Вернее сказать, кое-что знало, конечно, но только лишь по слухам и фрагментарным, не слишком достоверным мемуарам людей, так или иначе соприкасавшихся с важной тайной в годы Второй мировой войны.Вполне естественно, что в подобных условиях история британского «Колосса» обросла множеством всевозможных мифов. В обобщенной и самой поверхностной передаче эта мифология выглядит примерно так:

> *В годы войны английские криптоаналитики вскрывали и читали практически всю засекреченную переписку нацистской Германии, шифровавшуюся знаменитой машиной Enigma. Быстрое вскрытие ключей «Энигмы» и тотальное чтение шифрованных телеграмм вермахта обеспечивал мощный программируемый компьютер Colossus — первая в мире цифровая электронно-вычислительная машина, сконструированная великим математиком Аланом Тьюрингом.*

По сути дела, все из приведенных фактоидов не соответствуют истине — хотя при этом довольно близки к реальному положению вещей [*Примечание*. Фактоиды — термин, появившийся на рубеже 1960-70 гг. для обозначения вымышленных событий, похожих на реальные, либо опубликованных в печати под видом действительно происходившего].

Британской криптослужбой действительно были достигнуты потрясающие успехи в дешифровании немецкой переписки, и делалось это действительно на основе электронной вычислительной техники. Но читать удавалось далеко не все шифрсообщения, закрытые «Энигмой», а кроме того, Германия применяла и другие шифраторы существенно иной конструкции.

Для вскрытия одного из таких аппаратов, телеграфного шифратора Lorenz Schlüsselzusatz 40/42 (читается «Лоренц Шлюссельцузатц»), закрывавшего коммуникации лично Гитлера и высшего командования вермахта, и был, в частности, создан компьютер Colossus.

Алан Тьюринг никакого участия в разработке этой вычислительной машины не принимал, хотя и был, конечно, в курсе, поскольку работал в параллельном направлении — по преимуществу, над вскрытием «Энигмы».

Построенный же в конце 1943 года Colossus, действительно цифровой программируемый компьютер, вряд ли правомерно называть самой первой в мире электронной машиной подобного рода, однако это на самом деле была беспрецедентная по многим

параметрам разработка, созданная при любопытнейших обстоятельствах, достойных отдельного рассказа.

[ВРЕЗКА]

Клуб любителей стрельбы, шахмат и сыра

Живописная усадьба Блечли-Парк расположена в графстве Бакингемшир, примерно в 80 км к северо-западу от Лондона. В XIX веке принадлежавшая богатому лондонскому финансисту, к 1930-м годам усадьба пришла в запустение, ожидая сноса зданий и распродажи земли по частям.

Однако политическая обстановка в мире становилась все мрачнее — в 1938 году, когда Гитлер аннексировал Австрию и оккупировал часть Чехословакии, в Европе отчетливо запахло новой большой войной. В этих условиях британское правительство всерьез озаботилось переводом стратегически важных спецслужб из Лондона в более безопасную при авианалетах сельскую местность.

Десятым по счету объектом, среди приобретенных в тот период разведкой MI6 загородных владений, оказалась усадьба Блечли-Парк. Получив кодовое название Station X, эта «станция» была удобно расположена на пересечении автомагистрали и железной дороги, имея к тому же поблизости телефонный узел и телеграфную связь со всеми регионами страны.

По этим причинам именно сюда было решено перебазировать секретную спецслужбу GC&CS или в полном наименовании Government Code and Cypher School, т.е. «Правительственную школу кодов и шифров», занимавшуюся дешифрованием дипломатической и военной переписки иностранных государств. Острые на язык сотрудники спецслужбы предпочитали в шутку расшифровывать аббревиатуру GC&CS как Golf, Cheese and Chess Society, т.е. «Общество любителей гольфа, сыра и шахмат».

Когда в августе 1939 года все члены этого «общества» — математики, криптоаналитики, лингвисты и прочий персонал — переехали работать в Блечли-Парк, то для конспиративного прикрытия проснувшуюся от спячки усадьбу стали называть «Стрелковым клубом капитана Ридли». Командовать хозяйством «клуба» действительно назначили капитана — капитана второго ранга Элистера Деннистона.

[КОНЕЦ ВРЕЗКИ]

Рыбная ловля в волнах эфира

В начале 1940 года спецгруппа английской полиции, занимавшаяся прослушиванием радиоэфира для выявления возможных германских шпионов на территории острова, случайно отловила шифрованную немецкую радиопередачу необычного вида.

Новый материал радиоперехвата был передан для изучения криптоаналитикам службы GC&CS в Блечли-Парк, где чрезвычайно заинтересовались этими шифртелеграммами, переданными не более привычным в ту пору кодом Морзе, характерным и для криптограмм «Энигмы», а телеграфным кодом Бодо.

В точках и тире кода Морзе, напомним, знаки сообщения передаются двоичными комбинациями различной длины. А в коде Бодо, или более официально МТК-2 (международном телеграфном коде № 2), все знаки имеют равную длину кодовой комбинации — по 5 бит, что сделало очень удобным применение 5-дорожечных перфолент для стандартизованного ввода и вывода информации в телеграфных аппаратах.

В период между двумя мировыми войнами код Бодо уже начал заметно теснить более распространенную в то время «морзянку». Особо успеху МТК-2 способствовали «телетайпы», печатающие телеграфные аппараты, выпущенные на рынок американской фирмой AT&T в 1924 году.

А чуть раньше, в 1918 инженером той же компании Гильбертом Вернамом был изобретен чрезвычайно удачный и остроумный метод шифрования телеграфной переписки на основе кода Бодо. По сути дела, Вернам открыл эффективный метод «цифрового шифрования» информации — двоичное сложение битов текста послания и битов длинной шифрующей последовательности (или «гаммы» в терминах отечественной криптографии). Эта идея, заметим попутно, продолжает широко использоваться и сегодня в самых современных шифраторах, правда, на основе другой элементной базы.

Конструктивно Вернам реализовал свою идею в виде двух перфолент — одна с текстом телеграммы, другая с шифрпоследовательностью такой же длины, — которые синхронно движутся через считыватель-сумматор, сразу отправляющий результирующий шифртекст в линию.

Вся прелесть данного метода заключается в том, что на приемном конце получателю шифрованного текста достаточно заправить в аппарат-сумматор точно такую же как у отправителя перфоленту с гаммой, обеспечить синхронизацию начал гаммы и шифртекста, а дальше та же самая процедура побитного сложения знаков дает на выходе уже открытый текст. Иными словами, процедура зашифрования и расшифрования здесь в точности одна и та же.

Шифрсистема Вернама, как видим, чрезвычайно проста по своему принципу и в то же время может быть чрезвычайно надежна, поскольку однократное прибавление качественной гаммы (полностью случайной равновероятной двоичной последовательности) превращает открытый текст телеграммы в зашифрованное послание, в принципе не поддающееся аналитическому вскрытию. Правда, это лишь в теории.

На практике же пользователи шифра Вернама должны были заранее иметь на двух концах каждой линии связи идентичные рулоны с гаммой-перфолентой. Причем количество рулонов огромно, поскольку для стойкости шифра гамма может использоваться только однократно, а ее длина должна соответствовать длине отправляемых телеграмм.

Понятно, что в таком виде криптосистема Вернама не особо практична, поскольку в реальной жизни, не говоря уже об условиях войны, постоянная генерация и безопасная рассылка гаммы в больших количествах представляет собой гигантскую, часто просто неподъемную по сложности задачу.

Поэтому на интересную в принципе идею специалисты-криптографы обратили, конечно, внимание, но одновременно стали думать, как бы сделать ее попрактичней в использовании. Наиболее естественный путь — вырабатывать псевдослучайную гамму с помощью какого-нибудь механизма-генератора (детерминированного, но хитроумного), избавившись от обременительной рассылки рулонов перфолент.

Перед войной разного рода экспериментами с шифраторами, сочетающими идею Вернама с генератором гаммы, занимались криптослужбы нескольких стран. И вот теперь, т.е. весной 1940 года, результаты первичного криптоанализа англичан в Блечли-Парке показали, что в германских шифтрелеграммах нового вида использован, вероятнее всего, именно шифр этого рода.

Новой криптосистеме противника дали кодовое наименование FISH (такими же рыбными терминами — «лещь, макрель, селедка» — станут именовать и линии связи, от которых пойдет перехват по данному шифру), взяв «объект» в пристальную разработку. Ибо шифровальщикам, готовящим и отправляющим телеграммы, как и всем прочим людям, свойственно ошибаться, а для криптоаналитков, вскрывающих шифры, эти ошибки являются важнейшим подспорьем, облегчающим взлом.

Конкретно для случая с шифром Вернама наиболее типичный вид ошибок шифровальщиков — это повторное использование гаммы. А в математически строгом искусстве криптоанализа хорошо освоены методы, в принципе позволяющие прочесть комплект из двух или более телеграмм, зашифрованных одной и той же гаммой — сколь бы случайной и равновероятной она ни была.

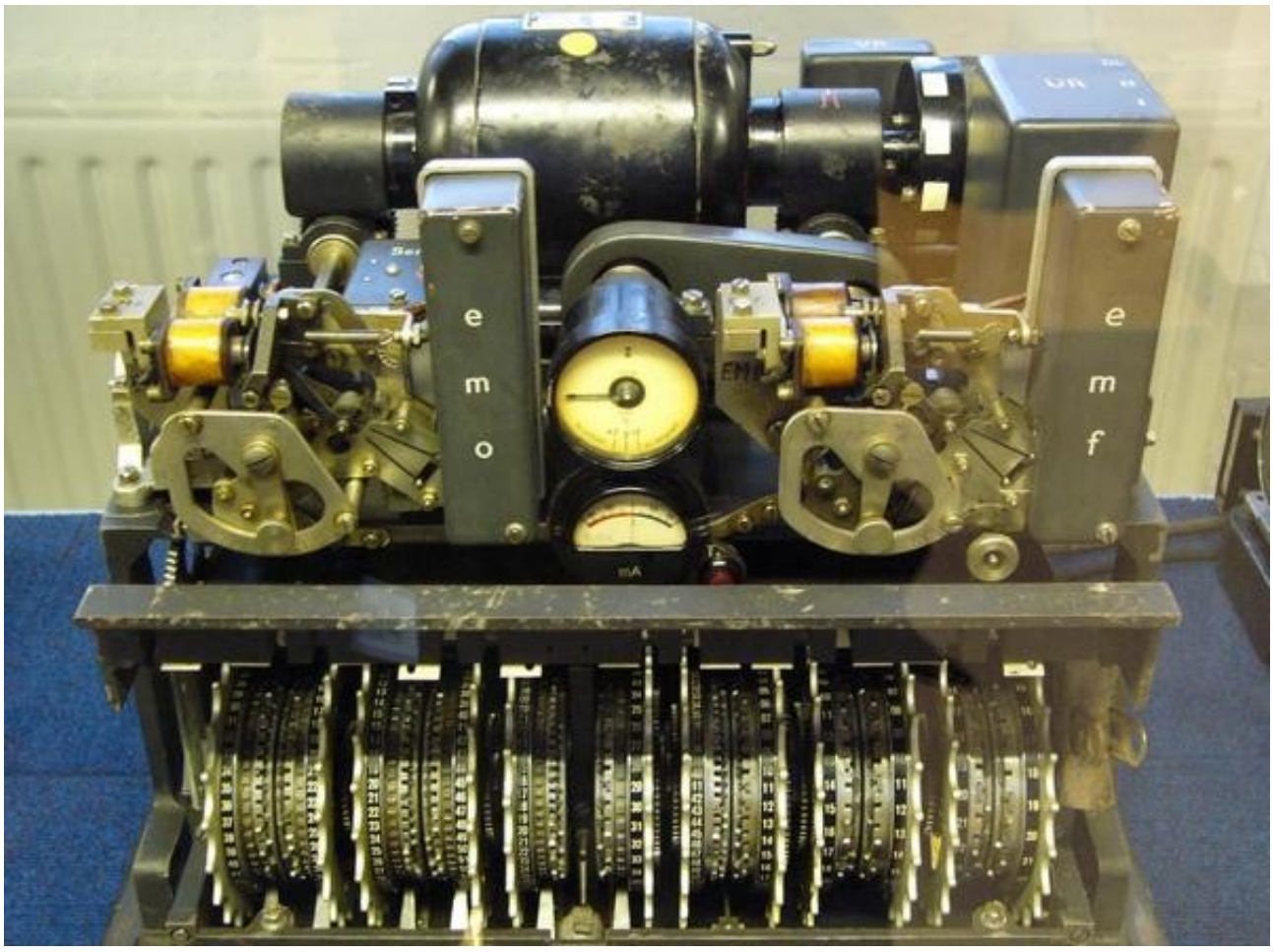
Ну, а если же при вскрытии телеграмм выяснится, что эта гамма не случайная, а выработана каким-то детерминированным способом генерации, то тогда появляются шансы вскрыть и внутренний механизм шифратора. Однако для успеха подобной работы требуется как можно более полный радиоперехват.

[ВРЕЗКА]

Рыба по имени Lorenz SZ

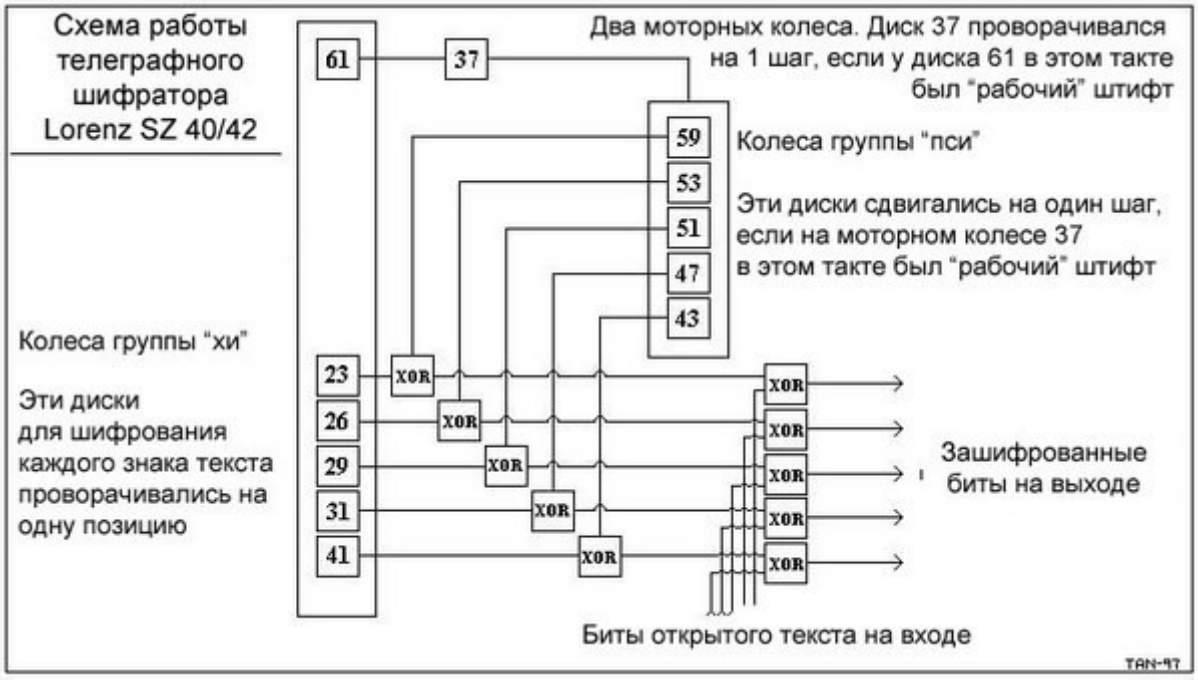
Общеизвестно, что подавляющая часть секретной переписки 3-го рейха велась с помощью компактного и удобного для транспортировки шифратора «Энигма». В годы войны в общей сложности около 200 тысяч таких аппаратов работало в войсковых подразделениях до тактического звена, на всех кораблях, авиабазах и железнодорожных станциях.

Менее известно, что для коммуникаций высшего военного эшелона — телеграфной радиосвязи Гитлера и генштаба с командованием армий — использовалась более серьезная и тяжелая машина, рассчитанная на совместную работу со стационарным оборудованием. Шифратор был выпущен фирмой «Лоренц» в 1940 году в виде приставки к ее же стандартным телепринтерам, имел размеры 51×46×46 см, и получил соответствующее название Lorenz SZ 40, где SZ означает Schlüsselzusatz, т.е. «шифрприставка».



Телепринтер давал на выходе знаки открытого текста в коде Бодо — пять бит по пяти параллельным линиям. На каждый такт выхода телепринтера шифрприставка выдавала свою группу из пяти псевдослучайных бит, которые в сумматоре побитно складывались со знаком открытого текста.

Псевдослучайные биты шифрпоследовательности генерировались с помощью 10 «штифтовых колес», т.е. особых дисков с разным количеством расположенных по ободу штифтов, которые могли находиться в двух разных положениях: «рабочем» и «нерабочем», что соответствовало снимаемому с колеса значению бита 1 или 0.



По принципу движения диски были разделены на две группы, так что пять в каждом такте проворачивались равномерно на 1 позицию (англичане на греческий манер назовут эту группу колесами χ, т.е «хи»), а другие пять проворачивались неравномерно (получив у англичан название колес ψ, т.е. «пси»). Общий закон движения для колес «пси» — когда всем стоять или всем проворачиваться на 1 позицию — определяли еще два добавочных диска, получивших название «моторные колеса».

С криптографической точки зрения, шифратор Лоренц представлял собой пять параллельных псевдослучайных генераторов, поскольку между пятью линиями порождения гаммы не было практически никакой зависимости, кроме общего закона движения для колес «пси».

Количество штифтов на всех дисков было разным и взаимно-простым, что согласно азам криптографической науки в принципе позволяло создать достаточно сильную криптосхему.
Однако в конкретной германской конструкции был допущен ряд фатальных просчетов и слабостей, из-за чего результирующая псевдослучайная последовательность получалась гораздо больше «псевдо-», нежели «случайная». Почему и была вскрыта английскими криптоаналитиками.

[КОНЕЦ ВРЕЗКИ]

Роковая ошибка противника

Специально под криптосистему FISH в Блечли-Парк было создано отдельное подразделение, занявшееся тщательным анализом перехвата и поисками возможностей для вскрытия шифра. Подразделение возглавил майор Ральф Тестер, отчего его команда получила среди обитателей усадьбы шутливое название «Тестиарий».

В течение первого года сотрудниками Тестиария было выявлено и частично прочитано несколько небольших одноключевых комплектов, однако поставить чтение на поток или почерпнуть сколь-нибудь существенную информацию о внутреннем устройстве шифрсистемы поначалу не удавалось.

Но вот летом 1941 года один из германских шифровальщиков совершил чудовищную ошибку — дважды на одном ключе передал длинную (около 4000 знаков) телеграмму, причем во второй раз слегка сокращая по лени текст, который приходилось набивать вручную. Делать подобные вещи — применять один и тот же ключ к неидентичным текстам — инструкции абсолютно запрещают всем шифровальщикам. Однако несовершенен человек — а противник всегда начеку.

Служба английского радиоперехвата зафиксировала обе передачи, а в Блечли-Парк со всей тщательностью вскрыли комплект. В результате была не только полностью прочитана телеграмма, но и — что самое главное — с высокой точностью восстановлена большущая, суммарной длиной 20 тысяч битов, последовательность гаммы. Британские аналитики не имели ни малейшего понятия, что это за шифратор, но они уже точно знали, какую гамму FISH вырабатывает.

Кроме того, было известно, что в начале каждой шифртелеграммы немцы дают специфической структуры последовательность из 12 знаков, которую аналитики называли «индикатор». Поскольку при одном и том же индикаторе из разных телеграмм с одной линии связи получался одноключевой комплект, то англичане предполагали, что такой индикатор может свидетельствовать о начальных установках 12 шифрующих колес FISH. Просто по той причине, что на основе шифрколес с шестернями движения разного периода были устроены практически все известные в ту пору шифраторы, включая и немецкие.

Около трех месяцев добытая гамма не поддавалась криптоаналитикам, пока не попала на стол к молодому выпускнику Кембриджа по имени Билл Тут, только-только пришедшему в GC&CS после подготовительных криптографических курсов в Лондоне. Молодому математику сопутствовала удача. В одной из 5 дорожек гаммы Тут выявил признаки суммирования битов от двух колес с периодами 41 и 43, но проворачивающихся в каждом такте не равномерно, а по более сложному закону.

Это было очень важное открытие, позволившее в течение следующих двух месяцев Туту совместно с коллегами полностью вскрыть логику работы шифратора — принцип расположения, все периоды и штифтовые комбинации пяти пар дисков для пяти дорожек и устройство двух дополнительных «моторных колес», управлявших законом проворачивания основных дисков.

Полное вскрытие совершенно неизвестной криптосхемы исключительно по шифртексту — это всегда фантастический успех криптоанализа, почти чудо. Конечно, немалый вклад сделали тут и сами немцы, невольно заложившие в конструкцию шифратора серьезные недочеты и допускавшие передачу одноключевых комплектов. Однако без гения британских криптографов все эти слабости так и могли бы до конца войны оставаться в разряде «потенциальных».

Первым важным итогом грандиозного мозгового штурма англичан стало то, что Исследовательская лаборатория британского Министерства почт (где ведали тогда всей

механизацией коммуникаций) в начале 1942 года получила заказ на изготовление электромеханической машины, реализующей логику FISH. Данная машина, быстро построенная на основе реле и шаговых переключателей, получила название «Тунец».

С этого момента всякий раз, когда криптоаналитикам из Тестиария удавалось вручную вскрыть ключевые установки (начальные положения дисков) одной из шифртелеграмм, они выставлялись в параметрах «Тунца», на вход подавался шифртекст, а на выходе — если все было вскрыто правильно — выходил открытый немецкий текст телеграммы.

Но на ручное вскрытие ключей к каждой телеграмме уходило от четырех до шести недель кропотливого труда. Иными словами, хотя принципиальная возможность дешифрования FISH была вполне убедительно продемонстрирована, большое время, затрачиваемое на вскрытие, с оперативной точки зрения делало столь тяжело добытую информацию практически бесполезной.

Автоматизация рыбного хозяйства

В 1942 году к работам в Блечли-Парк подключился известный английский математик Макс Ньюмен, один из наставников Алана Тьюринга в Кембридже. Наряду с помощью по вскрытию «Энигмы», Ньюмена попросили также посодействовать ускорению процесса дешифрования FISH.

У Билла Тута к тому времени уже был разработан и реализован в деле весьма интересный алгоритм, позволявший чисто статистически, с помощью большого объема вычислений отыскивать наиболее вероятные стартовые позиции шифрколес для каждого сообщения. Ознакомившись с этим алгоритмом Макс Ньюмен пришел к выводу, что некоторые наиболее трудоемкие части данной работы вполне можно попытаться автоматизировать с помощью специализированной машины-вычислителя — арифметическо-логического устройства на основе электронных ламп.

Под автоматизацию дешифрования создали специальное подразделение, получившее неофициальное название «Ньюменарий» в честь его начальника. За технической помощью математики обратились к Томми Флауэрсу, блестящему инженеру-электронщику Министерства почт.

До войны Флаурс занимался разработкой ламповых схем для радиорелейных ретрансляторов и по опыту знал, что эти схемы можно делать быстрыми и чрезвычайно стабильными в обработке сигналов, но при условии, если их все время держать в «горячем» состоянии (обеспечив надлежащее охлаждение), а не заниматься постоянным включением-выключением.

Именно Флауэрс стал главным конструктором электронно-вычислительной машины Colossus. Самой выдающейся, вероятно, заслугой этого инженера стало то, что он предложил сделать в машине внутреннее хранение данных — генерировать всевоз-

можные варианты установки шифрколес чисто электронными средствами, с помощью ламповых кольцевых схем.

Для реализации подобной электронной машины требовалось воистину гигантское количество электронных ламп — свыше 1500, откуда и пошло название «Колосс», поскольку максимум ламп в одном приборе составлял тогда около полутора сотен штук. Поскольку ничего подобного прежде не делалось, практически все, кто участвовал в создании этой машины в Лаборатории министерства почт, относились к успеху затеи с сильным скепсисом, мягко говоря.

Хотя проект был весьма масштабным и в нем принимало участие довольно много инженеров, лишь самое их минимальное число имело представление о том, что за части образуют машину в целом и для чего она вообще предназначена. Сам же Томми Флауэрс был твердо убежден, что всю эту схему можно будет заставить работать. Проектирование электронного вычислителя началось в марте 1943 года, а к концу декабря готовый компьютер, получивший название Mark 1 Colossus уже собрали в Блечли-Парк.

В первых числах января 1944 года «Колосс» опробовали на реальном шифрматериале перехвата — и при первом же настоящем испытании компьютер успешно вскрыл ключ, обрабатывая массив данных с фантастической скоростью 5000 знаков в секунду. Благодаря этой машине англичане получили возможность каждый месяц вскрывать около 300 телеграмм, зашифрованных криптосистемой FISH. Ввод в действие компьютера Mark 1 (или Colossus I) сократил время вскрытия шифртелеграмм высшего командования вермахта с нескольких недель до часов.

Этот гигантский прорыв криптоаналитиков произошел как нельзя более кстати, поскольку своевременное дешифрование столь информативной переписки предоставляло важнейшие сведения генералам Эйзенхауэру и Монтгомери накануне открытия второго фронта в Европе. Дешифрованные телеграммы объекта FISH свидетельствовали, что Гитлер действительно поверил в обманный трюк союзников — в фантомную армию, якобы концентрируемую в Южной Англии, и в ложную подготовку высадки через пролив Па-де-Кале.

Но в деле дешифрования FISH далеко не все было гладко и просто. Немцы постоянно работали над усилением своих криптосистем, и, в частности, в начале 1944 года было в очередной раз предпринято весьма существенное усложнение процедуры шифрования в аппарате Lorenz.

Эти шаги немецких криптографов серьезно затруднили работу в Блечли-Парк, так что к марту англичанам стало ясно — для дальнейшего успешного вскрытия FISH необходимо существенно усовершенствовать конструкцию Colossus. Был запущен новый проект разработки, к 1 июня 1944 завершившийся созданием машины, получившей название Colossus Mark 2 (или просто Colossus II).

Никто, ясное дело, не мог запланировать это заранее, но новейший компьютер был поставлен в строй аккурат за несколько дней до открытия второго фронта. Colossus II был примерно в 5 раз быстрее своего предшественника, предоставлял возможности программирования и содержал около 2500 электронных ламп. На этом основании Colossus II в целом ряде современных работ по истории вычтехники расценивается ныне как первый в мире электронный программируемый компьютер.

После «Дня Д», когда авиация союзников разбомбила и повредила большинство наземных телефонных и телеграфных коммуникций в Северной Франции, немцам пришлось в значительно более крупных масштабах прибегать к радиосвязи, что чрезвычайно повысило и объем перехватываемых шифртелеграмм, закрытых системой FISH.

Ударными темпами англичане построили еще восемь машин Colossus II для обработки мощно возросшего трафика. Компьютеру Mark 1 сделали апгрейд до Mark 2, так что вплоть до конца войны в Блечли Парк непрерывно работали в три смены 10 мощных электронных машин, вскрывавших важнейшую переписку противника.

Победа, смерть и возрождение

В общей сложности с помощью «Колоссов» было дешифровано свыше 63 миллионов знаков телеграмм немецкого верховного командования, что обеспечивали примерно 550 сотрудников (точнее, в большинстве своем сотрудниц) Блечли-Парк, плюс, конечно же, службы радиоперехвата.

Но с приходом мая 1945 года и наступлением столь долгожданного Дня победы, звезда компьютеров Colossus стремительно закатилась. Машины-гиганты были слишком специализированы под конкретную задачу, а высшее политическое руководство страны слишком озабочено, чтобы Сталин и быстро формировавшийся вокруг СССР блок просоветских государств ничего не узнали о мощных дешифровальных возможностях Великобритании.

Уинстон Черчилль лично дал указание, чтобы «Колоссов» разобрали на части, размерами «не больше руки человека», так что восемь из десяти машин в Блечли-Парк были полностью демонтированы уже в том же 1945 году.

Два последних компьютера сначала перевезли в Северный Лондон, а затем в город Челтнем, где разместилась (и базируется по сию пору) преемница GC&CS, криптографическая спецслужба Великобритании GCHQ или Штаб-квартира правительственной связи (Government Communications Headquarters).

Здесь, за плотной завесой секретности эти компьютеры использовались еще полтора десятка лет для тренировочных и вспомогательных криптографических задач, вроде статистической оценки качества гаммы. В 1959-1960 годах демонтировали и две последние машины, тогда же были сожжены и все рабочие схемы-чертежи компьютеров

Colossus. При этом сам факт существования столь выдающихся для своего времени вычислительных устройств продолжали держать в строжайшей тайне еще многие годы.

Хотя официальной информации о Colossus не публиковалось вплоть до конца XX века, обрывочные сведения об этом компьютере стали появляться с середины 1970-х годов, когда истек стандартный для Британии 30-летний срок хранения государственных секретов.

К 1996 году группе энтузиастов при национальном криптомузее Блечли-Парк даже удалось воссоздать работоспособную копию этой машины, правдами и неправдами накопив достаточное количество подробностей, приватных воспоминаний и эскизов от оставшихся в живых участников проекта.

В подобных условиях продолжать делать тайну из того, что так или иначе уже известно всем, стало совсем бессмысленно. В октябре 2000 года власти Великобритании решились-таки, наконец, рассекретить подробный технический отчет о вскрытии FISH и машинах Colossus, подготовленный в 1945 году сразу по окончании войны. Все это время объемный 500-страничный документ скрывали в архивах GCHQ, теперь же спецслужба передала его в общедоступный Государственный архив (Public Record Office) в городе Кью.

Наиболее полную информацию о компьютерах Colossus, включая и онлайновую версию рассекреченного отчета 1945 года, можно найти на веб-сайте английского инженера-энтузиаста Тони Сэйла (www.codesandciphers.org.uk), благодаря усилиям которого и удалось возродить из небытия полностью, казалось бы, утраченную для истории машину.

# # #

Параллельные миры

(*Ноябрь 2000*)

Мистические и просто любопытные страницы из истории создания криптографии с открытым ключом.

Поскольку материалистическое мировоззрение является строго детерминистским и не принимает возможности существования «многозначительных совпадений», то любые намеки на необычные синхронности автоматически толкуются как бред…

Однако не может быть никаких сомнений в том, что существуют подлинные синхронности, где любой человек, имеющий доступ к этим фактам, должен признать, что данные совпадения выходят за рамки статистической вероятности.

Станислав Гроф, «Космическая игра»
(тексты трансперсональной психологии)

В последние дни октября (2000 г) по Четвертому каналу британского телевидения прошла заключительная передача из серии «Наука тайны», включавшая в себя интервью с Клиффордом Коксом, сотрудником Штаб-квартиры правительственной связи (GCHQ) Великобритании и «тайным» изобретателем криптосхемы RSA.

Примерно с конца 1997 года миру стало известно, что группа криптографов из спецслужбы GCHQ, базирующейся в Челтнеме, открыла основные принципы криптографии с открытым ключом на несколько лет раньше, чем их коллеги из академического и индустриального сообщества.

За прошедшие 3 года в Интернете опубликованы несколько основополагающих работ английских правительственных криптографов в этой области, однако лишь ныне одному из них впервые было разрешено дать интервью средствам массовой информации.

Постепенно всплывающие при этом факты демонстрируют, что история параллельного изобретения нового направления в криптографии – учеными секретного и открытого сообществ – содержит целый ряд удивительно синхронных совпадений.

#

GCHQ является наследницей знаменитой криптослужбы, работавшей в Блечли-Парк и вскрывавшей вражеские шифры в годы Второй мировой войны (см. «Колосс британский»). В некотором смысле GCHQ является аналогом американской спецслужбы АНБ или российской ФАПСИ.

Однако, есть и существенные отличия: GCHQ – это сугубо гражданское ведомство, формально входящее в структуру Министерства иностранных дел (вероятно, по той причине, что основным объектом дешифровальных усилий спецслужбы является дипломатическая переписка зарубежных стран). Однако для другого основного направления деятельности криптослужбы, сводящегося к заботе о надежных средствах засекречивания коммуникаций, главным потребителем являются, естественно, военные.

В конце 1960-х годов британские военные уже вполне реально ощущали вступление в эру высоких технологий, сулившую обеспечить каждого бойца собственным входом в тактическую радиосеть. Перспективы разворачивания таких сетей обещали грандиозные перемены и упрощение задач по руководству военными операциями, однако ставили и очень серьезные проблемы перед службой, отвечающей за безопасность и засекречивание подобной связи.

Настоящей головной болью становилась необходимость распределения и управления гигантскими количествами криптоключей, причем передавать каждый из ключей надо было в строжайшем секрете от неприятеля. Поэтому в 1969 году одному из выдающихся творческих умов GCHQ по имени Джеймс Эллис (James Ellis) было поручено поразмышлять как следует над возможным выходом из столь безнадежной ситуации.

Поначалу для Эллиса, как и для всех, было очевидно, что не может быть никакой засекреченной связи без секретного ключа, какой-то другой секретной информации, или по крайней мере какого-то способа, с помощью которого законный получатель находился бы в позиции, отличающей его от того, кто перехватывает передачи. В конце концов, если бы они были в одинаковом положении, то как один имел бы возможность получать то, что другой не может?

Но тут, как это часто случается накануне открытия, внимание Эллиса привлекла давнишняя, времен войны техническая статья неизвестного автора из компании Bell-Telephone, в которой описывалась остроумная, но так и не реализованная идея засекречивания телефонной связи.

Там предлагалось, чтобы получатель маскировал речь отправителя путем добавления в линию шума. Сам получатель впоследствии мог вычитать шум, поскольку он же его и добавлял и, следовательно, знал, что тот собой представляет. Принципиально же важным моментом было то, что получателю уже не было нужды находиться в особом положении или иметь секретную информацию для того, чтобы получать засекреченную речь…

Первичный идейный толчок оказался достаточным: различие между описанным и общепринятым методом шифрования заключалось в том, что здесь получатель сам принимает участие в процессе шифрования.

Далее перед Эллисом встал достаточно очевидный вопрос: «А можно ли нечто подобное проделать не с каналом электрической связи, а с обычным шифрованием»?

Как известно, главное — правильно сформулировать вопрос, поэтому как только однажды (среди ночи в постели) вопрос уложился у Эллиса в нужную форму, то доказательство теоретической возможности этого заняло всего несколько минут. Так родилась «теорема существования».

То, что было немыслимо, на самом деле оказалось вполне возможным.

В итоге Эллис пришел к схеме, позже получившей название «криптография с открытым ключом», сам же он назвал свою концепцию «несекретное шифрование». Суть концепции, сформулированной и формально подтвержденной к началу 1970 года, сводилась к схеме из открытого и секретного ключа, управляющих однонаправленной математической операцией.

Правда, поскольку Эллис был прежде всего экспертом в системах коммуникаций, а не в математике, то его революционная концепция не была доведена до конкретных математических формул. На начальство доклад Эллиса произвел большое впечатление, однако никто не смог решить, что с этими экзотическими идеями делать… и на несколько лет дело полностью встало.

#

А вот что происходило точно в то же самое время по другую сторону океана, в Стэнфордском университете. Здесь на рубеже 1969-1970 гг. молодой профессор Мартин Хеллман начал заниматься вопросами проектирования электронных коммуникационных систем, активно привлекая математический аппарат криптографии и кодирования.

Этими вещами он увлекся с тех пор, как прочитал военного периода статьи Клода Шеннона по теории информации и криптографии, подготовленные в годы секретной работы ученого в Bell Labs и опубликованные в 1948-1949 годах. По рассказам Хеллмана, до этого он «и представить себе не мог, насколько тесно связаны шифрование и теория информации».

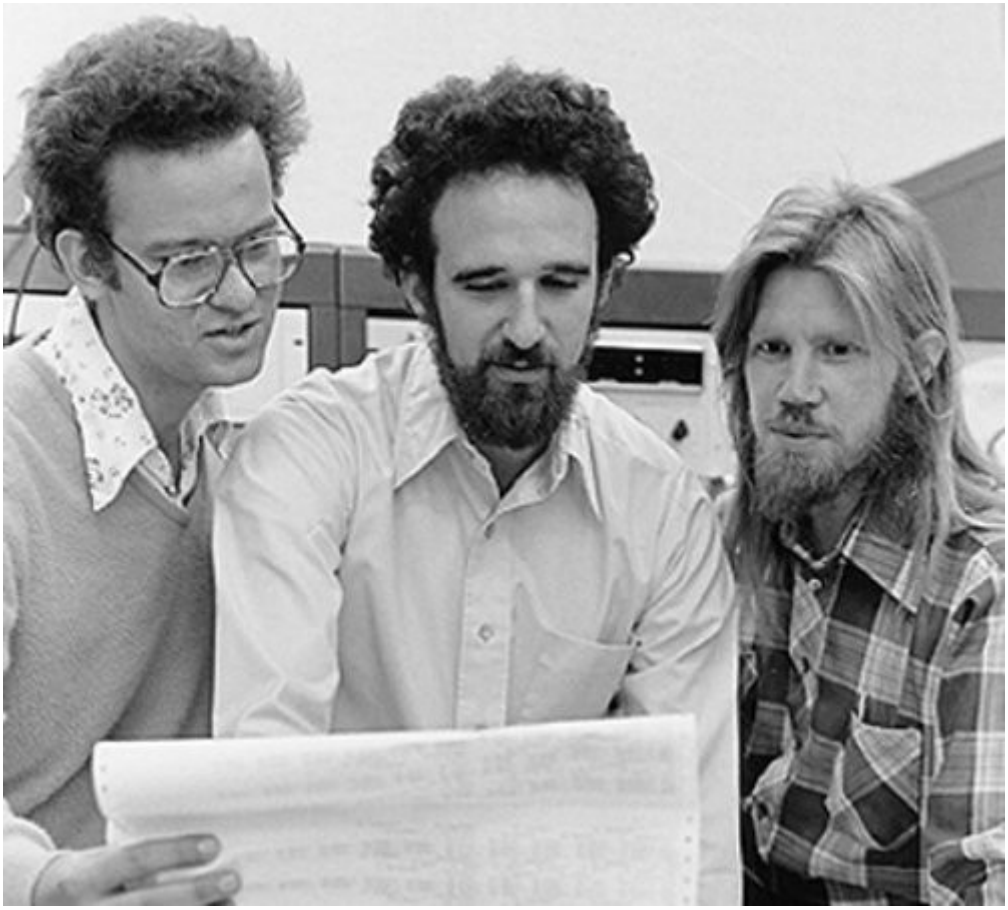
В статьях Шеннона вопросы кодирования рассматривались в связи с задачей снижения шумов электростатических помех, мешающих передаче радиосигналов. Хеллману стало ясно, что «шифрование решает диаметрально противоположную задачу. Вы вносите искажения при помощи ключа. Для того, кто слышит сигнал и не знает ключа, он будет выглядеть максимально искаженным. Но легитимный получатель, которому известен секретный ключ, может удалить эти помехи»…

Нетрудно заметить, что траектория выхода на изобретение у Хеллмана обозначилась по сути дела та же самая, что и у Эллиса.

В те времена, однако, ни информативных книг, ни справочников по криптографии у академических ученых по сути дела не было, поскольку эта наука считалась строго засекреченным делом военных и спецслужб.

Пытаясь собрать и объединить разрозненные идеи по шифрованию данных, Хеллман продолжал искать единомышленников. Но случилось так, что главный единомышленник вышел на него сам.

В сентябре 1973 года Хеллмана нашел Уитфилд Диффи, выпускник МТИ и молодой сотрудник Стэнфорда, страстно увлеченный криптографией. Их получасовая встреча плавно перешла в обед у Хеллмана, а разговоры затянулись далеко за полночь.



Слева направо: Ральф Меркль, Мартин Хеллман, Уитфилд Диффи

Вскоре началось и практическое сотрудничество. Хеллман и Диффи стали совместно работать над созданием криптосхемы для защиты транзакций покупок и продаж, выполняемых с домашних терминалов. Главная проблема, которую с подачи Диффи поставили перед собой ученые, сводилась к следующему «Как (не пересылая секретный ключ) получать сообщение и преобразовать его таким образом, чтобы его воспринимали только те, кому оно предназначено, а посторонним информация была бы недоступна»…

#

В том же самом сентябре того же 1973 года, но уже в Великобритании на работу в GCHQ пришел молодой талантливый математик Клиффорд Кокс (Clifford Cocks), только что закончивший Кембридж и весьма продвинутый в теории чисел (которую в

те времена обычно расценивали как один из наиболее красивых и самых бесполезных разделов математики).

Уже на начальном этапе вхождения новичка в курс работы, кто-то из наставников поведал Коксу о «воистину кучерявой» концепции несекретного шифрования. Идея крайне заинтересовала молодого человека, и он начал играть с ней в контексте простых чисел и проблем факторизации.

Слева направо: Рональд Райвест, Ади Шамир, Леонард Адлеман

Буквально через полчаса Кокс пришел по сути дела к той схеме, которой будет суждено через несколько лет стать знаменитой под именем RSA, или алгоритм Райвеста-Шамира-Адлемана. Сам же изобретатель в тот момент воспринимал свое открытие просто как решение достаточно тривиальной математической головоломки.

Кокс был весьма удивлен тем, в какое волнение и возбуждение пришли его коллеги. Но при этом руководство GCHQ вновь не стало предпринимать каких-либо шагов к практической реализации идеи, поскольку для широкого внедрения целочисленных операций над огромной длины числами требовались вычислительные мощности, чересчур по тем временам дороговатые.

Несколько месяцев спустя на работу в GCHQ поступил другой даровитый математик по имени Мэлколм Уильямсон (Malcolm Williamson), приятель Кокса еще со школьных лет. Когда Кокс рассказал другу о любопытной криптосхеме, то недоверчивый

Слева направо: Джеймс Эллис, Клиффорд Кокс, Мэлколм Уильямсон

Уильямсон решил, что она чересчур красива, чтобы быть правдой, и поэтому ринулся отыскивать в ней скрытые дефекты.

Слабостей ему найти так и не удалось, но зато в процессе поисков он пришел к еще одному элегантному алгоритму формирования общего ключа шифрования. Другими словами, в 1974 году Уильямсон открыл то, что уже, считай, почти родилось в Америке и совсем скоро станет известно как схема распределения ключей Диффи-Хеллмана-Меркля.

Ни одну из изобретенных схем в GCHQ патентовать не стали, поскольку патентная информация становилась известна широкой публике, а абсолютно все работы велись спецслужбой в условиях строжайшей секретности.

Когда в 1976 году Диффи и Хеллман объявили о своих открытиях, то Уильямсон попытался было, как мог, склонить руководство GCHQ к публикации результатов, полученных засекреченными английскими криптографами. Однако молодому человеку абсолютно не удалось пробить железобетонный консерватизм начальства, которое предпочло не нарушать традиций и не высовываться со своими приоритетами.

Через несколько лет, благодаря личным знакомствам в АНБ США, любопытный Уитфилд Диффи все же прослышал о работах в GCHQ и даже самолично ездил в Челтнем со своей женой, чтобы встретиться и пообщаться с Джеймсом Эллисом.

Встреча была крайне теплой и приветливой, однако Эллис, по рукам и ногам повязанный обязательством хранить служебные тайны, самым вежливым образом уклонялся от всех попыток Диффи перевести разговор в русло криптографии.

В конце концов, когда потерявший терпение и менее склонный к политесу Уит Диффи уже прямо в лоб спросил Эллиса о его роли в создании криптографии с открытым ключом, тот на некоторое время замолк, а потом тихо-тихо прошептал: «Ну не знаю я, сколько здесь можно рассказывать. Позвольте я лишь скажу, что вы, ребята, сделали со всем этим гораздо больше, чем мы»…

В последующие годы руководство GCHQ несколько раз намеревалось поведать правду. В 1987 году, в частности, Джеймсу Эллису, в связи с уходом ветерана на пенсию, даже заказали обзорную статью – для возможного широкого опубликования. Однако на главный шаг опять так и не решились, засунув ее в секретный архив.

До читателей статья дошла лишь в декабре 1997 года, уже в качестве мемориальной публикации в память об Эллисе, скончавшемся за месяц до этого в возрасте 71 года. Одновременно Клиффорду Коксу впервые разрешили опубликовать несколько работ по решению ряда проблем вокруг схемы RSA и выступить на открытых научных конференциях.

* *

Когда вдруг обнаружилось, что у схем с открытым ключом объявились новые «авторы невидимого фронта», то поначалу многие испытали нечто вроде шока. Ведь это направление всегда было предметом особой гордости открытого криптосообщества.

Понемногу, впрочем, страсти и недоверчивые споры улеглись, поскольку стало ясно, что никто не собирается посягать на приоритеты традиционных авторов, а просто отчасти восстановлена историческая справедливость.

Ныне же остается лишь непреходящее удивление тому, как две пары по сути дела идентичных схем (правда, в обратной последовательности) были изобретены практически одновременно людьми, абсолютно никак не связанными друг с другом.

Или, скажем так, не связанными с материалистической точки зрения… :)

# # #

Послесловие из 2007 г:

Секреты криптографии

(*Март 2007*)

Как-то необычно тихо и вообще без освещения мировой прессой в истории криптографии ныне полностью, можно сказать, удалось закрыть один любопытный и долгое время остававшийся без ответа вопрос.

Речь идет об известном сюжете из первой половины 1970-х годов, когда базовые принципы и конкретные алгоритмы криптографии с открытым ключом были открыты одновременно и независимо в «параллельных мирах»: коллективом засекреченных математиков из разведслужб и учеными открытого академического сообщества.

О работах криптографов из английской спецслужбы GCHQ (Штаб-квартира правительственной связи), чуть-чуть опередивших общепризнанных в мире первооткрывателей Диффи, Хелмана, Райвеста, Шамира и Адлемана, известно уже около 10 лет.

Но в этой истории до последнего времени оставался один неясный и довольно существенный нюанс — о роли Агентства национальной безопасности США.

Ибо еще четверть века назад, на рубеже 1970-1980-х годов тогдашний директор АНБ адмирал Бобби Инман в одном из своих публичных выступлений мимоходом отметил, что принципы криптографии с открытым ключом были изобретены в стенах его спец-

службы на несколько лет раньше, чем появилась в печати новаторская работа Уитфилда Диффи и Мартина Хелмана.

И поскольку в дальнейшем от выдачи каких-либо уточняющих комментариев АНБ упорно уклонялось, то после подтвержденного документами признания английской спецслужбы в 1997 получалось, что одна и та же важная криптотехнология была изобретена независимо и одновременно сразу в трех местах…

Очень для многих столь удивительное совпадение представлялось крайне маловероятным. И лишь теперь получены документальные свидетельства тому, что адмирал Инман своими словами ввел всех в заблуждение.

Неизвестно, сделал он это преднамеренно или будучи неверно информирован своими подчиненными, но наверняка можно говорить, что речь у него шла явно об изобретении математиков из GCHQ, с которыми криптографы АНБ давно и весьма тесно связаны по линиям сотрудничества дружественных спецслужб.

Достоверно известно это стало отнюдь не по добровольному признанию АНБ, а благодаря подвижнической деятельности нью-йоркского архитектора и правозащитника Джона Янга, более всего знаменитого в интернете благодаря своему «разоблачительному» сайту Cryptome.

Еще в 1999 году Янг направил в АНБ соответствующий FOIA-запрос (т.е. официальный запрос документов на основании закона о праве граждан на доступ к государственной информации) относительно материалов, касающихся разработки методов крипто с открытым ключом.

И вот теперь, по прошествии 7 с лишним лет, из АНБ прислали Янгу пакет из десятка, примерно, документов по этой теме (cryptome.org/nsa-nse/nsa-nse-01.htm). В основном, правда, это уже известные и опубликованные в других местах работы, включая статьи англичан из GCHQ, но есть и несколько американских, со снятыми серьезными грифами вплоть до Top Secret.

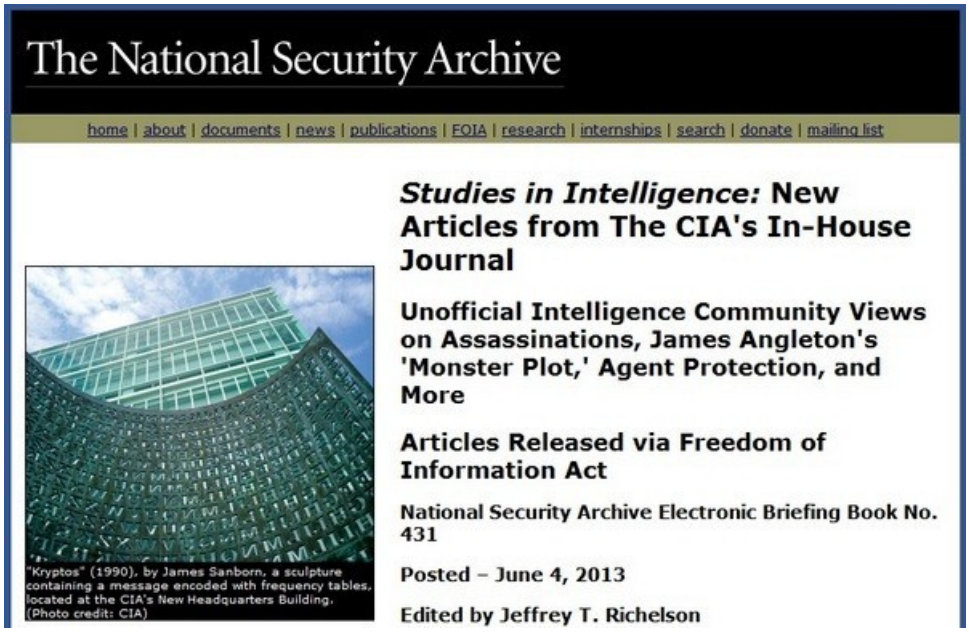
И из этих текстов вполне отчетливо видно, что все обсуждение проблем криптографии с открытым ключом идет исключительно в контексте секретных изобретений англичан и общеизвестных работ открытого криптосообщества. Иначе говоря, чудеса синхронных открытий, конечно, случаются, но все же лишь до определенной степени.

Год 2000-й. Слева направо: Шамир, Райвест, Адлеман, Меркль, Хеллман, Диффи.

Правда и вымысел

(*Июнь 2013*)

Необычный монумент Kryptos, украшающий двор штаб-квартиры ЦРУ в Лэнгли, за (без малого) четверть века успел стать своеобразным олицетворением сути шпионской профессии.



В первых числах июня 2013 на известном американском сайте «Архивы национальной безопасности» для всеобщего свободного доступа выложен очередной весьма любопытный комплекс исторических документов.

Данный сайт, National Security Archive, не имеет отношения к официальным структурам правительства США и является коллективным детищем ученых-исследователей Университета Джорджа Вашингтона, но прежде всего – Джефри Ричелсона (Jeffrey T. Richelson), одного из главных в стране экспертов по истории американских разведслужб.

Вот уже несколько десятилетий Ричелсон и его единомышленники на основе FOIA, закона о праве граждан на доступ к информации, методично добывают из секретных архивов США – а затем открыто публикуют – множество документов, проливающих дополнительный свет на известные исторические события, так или иначе связанные с проблемами национальной безопасности.

Опубликованный ныне комплекс документов – это два десятка статей, в разные годы – с середины 1990-х по 2011 – появлявшихся на страницах закрытого (грифом секретности) журнала ЦРУ «Исследования по разведке» или Studies in Intelligence.

Как показывает опыт изучения данных материалов, никаких великих откровений там, конечно же, не обнаруживается. Во-первых, гриф секретности у документов маловат,

а во-вторых, даже то, что хоть как-то могло бы потянуть на сенсацию, тщательно вымарано цензорами перед публикацией.

Тем не менее, перекрестное сопоставление всплывающих попутно малоизвестных фактов, плюс отталкивающиеся от них розыски дополнительной информации, позволяют выходить на весьма удивительные и хитро заплетенные истории, в деталях неведомые практически никому.

Вот как, скажем, выглядит одна из таких историй, раскопанная в связи с нынешней публикацией сайта «National Security Archive».

Тайны Kryptos

Две очень разных по тематике статьи из журнальной подборки Studies in Intelligence – Документ #1 «Тайные операции и запрет на физическое устранение людей, 1976-1996» и Документ #10 «Взлом криптографии во дворе» (1998) – на первый взгляд, не имеют друг с другом абсолютно ничего общего.

Первая статья посвящена юридическим и прочим аспектам тех проблем, что связаны с целенаправленными убийствами иностранных политических лидеров и прочих людей, деятельность которых рассматривается как угроза национальной безопасности США.

Фокус статьи сосредоточен на последствиях известной директивы президента Джеральда Форда, в 1976 году запретившей подобного рода физические устранения.

Главным образом, рассматривается то, каким образом ЦРУ приходилось обходить этот официальный запрет для дальнейшей поддержки тайных военных операций и заговоров по свержению лидеров иностранных государств (в частности, специфический случай с устранением от власти в Панаме генерала Мануэля Норьеги в 1989 году)…

Через год после военного вторжения США в Панаму и захвата в плен Норьеги, осенью 1990, началась цепь совершенно других, казалось бы, событий, которым посвящена вторая статья, или Документ # 10.

Этот материал рассказывает о весьма необычной скульптурной композиции, которая носит название Kryptos и в качестве декоративного украшения в ноябре 1990 была установлена во внутреннем дворе штаб-квартиры ЦРУ в Лэнгли.

В переводе с греческого Kryptos означает «Сокрытое». И есть основания считать, что название это как нельзя более подходит что для собственно монумента, что для работы разведки, олицетворением которой данная скульптура призвана выступать.

Бесспорная неординарность монумента Kryptos заключается в том, что фактически вся его поверхность – это множество букв зашифрованного послания плюс буквы-подсказки об устройстве ключа.

Автором произведения является американский скульптор Джим Сэнборн, и лично от него всегда было известно, что в многослойном тексте послания сокрыт некий весьма и весьма глубокий смысл… Вот только вскрыть этот шифр полностью никому так и не удается.

Значительная часть дешифровки, правда, давно уже осуществлена. Опубликованная ныне статья из журнала Studies in Intelligence за 1998 год, собственно, и рассказывает в подробностях о том, как были выявлены, вскрыты и прочитаны три части из четырех, зашифрованные разными ключами и криптосистемами.

Автором этого взлома (и автором статьи в журнале) является непрофессиональный криптограф, любитель кроссвордов и головоломок, а по роду основной деятельности – один из аналитиков-физиков Директората разведки в составе ЦРУ.

Шпионская профессия этого криптографа-дилетанта, вскрывавшего нетривиальные шифры «дедовскими методами» с помощью карандаша и бумаги, стала причиной, по которой результаты дешифрования руководство ЦРУ решило не предавать огласке.

Поэтому в открытом сообществе любителей и профессионалов криптографии все лавры принадлежат калифорнийскому компьютерщику Джиму Гиллоглы, в 1999 году решившему ту же задачу по-современному – с помощью Pentium II и специальных криптоаналитических программ.

Но ни любитель головоломок из ЦРУ, ни компьютерщик из Калифорнии, ни даже, говорят, профессионалы из Агентства национальной безопасности США, забавы ради вскрывшие этот шифртекст еще в 1992 году – никто так и не сумел взломать четвертую, самую важную часть послания.

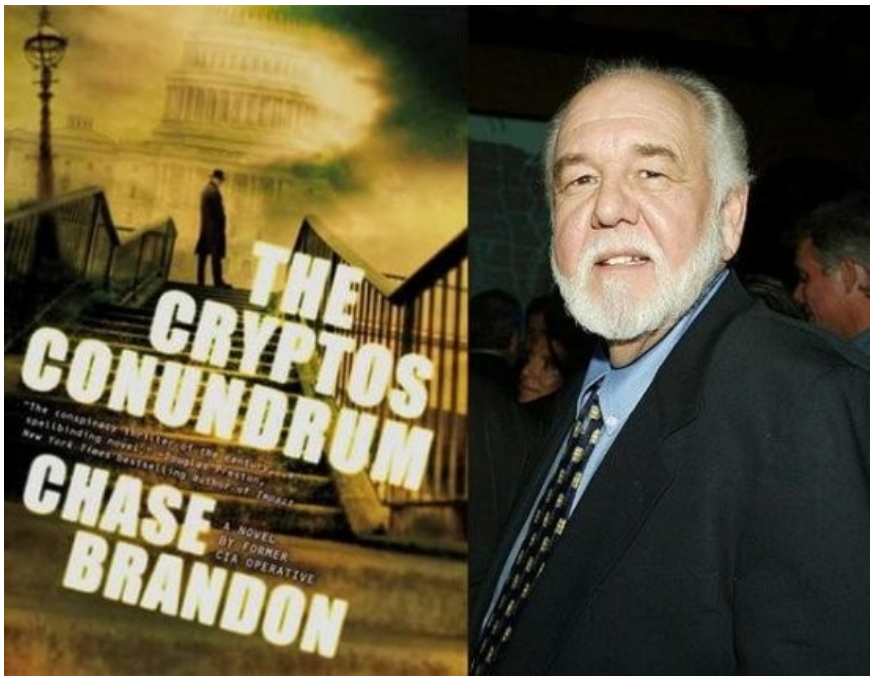
Причем нераскрытой тайной она остается вплоть до сегодняшнего дня, уже сделав скульптуру Kryptos одной из самых знаменитых криптограмм в истории.

За прошедшие годы эта волнующая многих загадка уже успела попасть не в одно литературное произведение, включая, например, и «Код Да Винчи» Дэна Брауна.

Однако самая, пожалуй, примечательная роль для данной криптограммы отведена в книге бывшего оперативника ЦРУ Чейза Брэндона, вышедшей в 2012 году под названием «Cryptos Conundrum». (Переводить название на русский вряд ли имеет смысл, ибо оно – как игра слов – составлено из двух заведомо вымышленных кодовых названий неких «суперсекретных» проектов ЦРУ)

Правду говорить трудно

Вкратце рассказывая об этой книге Брэндона (у него уже есть и другие), сразу следует подчеркнуть, что речь идет о событиях, вымышленных автором в жанре научной – а также не очень научной – фантастики.



Однако и в первых же строках своего романа, и в нескольких интервью для СМИ Чейз Брэндон подчеркнуто ссылается на известные слова английского мыслителя эпохи Возрождения Фрэнсиса Бэкона: «Правду так трудно поведать. Порою нужен вымысел, чтобы сделать ее правдоподобной».

Иначе говоря, ветеран шпионской службы настойчиво рекомендует читать его роман «между строк». Ибо там – помимо нескончаемых гимнов во славу фантастической мудрости, прозорливости и самоотверженности незримых героев из ЦРУ – содержится и «очень много правды». В частности, и великая неправдоподобная правда об истинной роли этой организации в истории спасения человечества…

В явном же виде страницы романа рассказывают об этом читателю примерно так:

> *Пятиметровой высоты скульптура из металла стоит во дворе Центрального разведывательного управления – украшенная посланием, которое никто не в силах расшифровать.*
>
> *В трехдюймовых буквах скульптуры закодировано сообщение, важнейшее для самого выживания человечества. Послание, скрытое у всех на виду, весь текст которого доступен любому, кто имеет подключение к интернету.*
>
> *Лишь один человек знает точно, что именно говорится в данном послании – потому что это он его создал.*
>
> *Доктор Джонатан С. Чалмерс возглавляет особое подразделение ЦРУ, задача которого – охранять величайшую тайну из всех секретов нашего правительства. А также планировать последствия этой тайны. Лишь он один знает полную историю всех тех угроз, что стоят перед Америкой.*
>
> *Угроз, которые привели бы нас в ужас, если бы только мы о них узнали.*
>
> *Угроз, которые формировали прошлое, настоящее и будущее этой державы.*
>
> *Угроз, которые стали работой его жизни, угроз, потребовавших всех его талантов, всей его энергии и даже жизней членов его семьи…*
>
> *Если Чалмерс не сможет нас спасти, то не сможет спасти уже никто.*

В рекламных анонсах, сопровождавших выход книги Чейза Брэндона, это произведение именуется «мощной космической сагой», главная суть которой в том, что практически все невероятные истории из арсенала «чокнутых конспирологов» – это на самом деле правда…

То есть и заговор с целью убийства президента Джона Кеннеди – это правда, и падение НЛО под Розуэллом – правда, и контакты правительства США с инопланетянами – тоже правда, и все-все остальное – вплоть до Лох-Несского чудовища и битвы небесных ангелов с темными силами сатаны – тоже чистая правда.

Просто люди в силу своей ограниченности и недоразвитости всю эту правду воспринимают неадекватно, а в адекватном виде получить и переварить ее пока не способны. За исключением лишь очень отдельных героических личностей вроде главного персонажа книги Джонатана Чалмерса (в характерных чертах которого знающие люди без труда усматривают скромный облик автора книги, Чейза Брэндона).

Чтобы стало яснее, насколько прозрачно Брэндон вплетает в канву сюжета и себя любимого, и то весьма специфическое подразделение, которое он много лет возглавлял в ЦРУ, достаточно упомянуть лишь одно из сюжетных ответвлений романа.

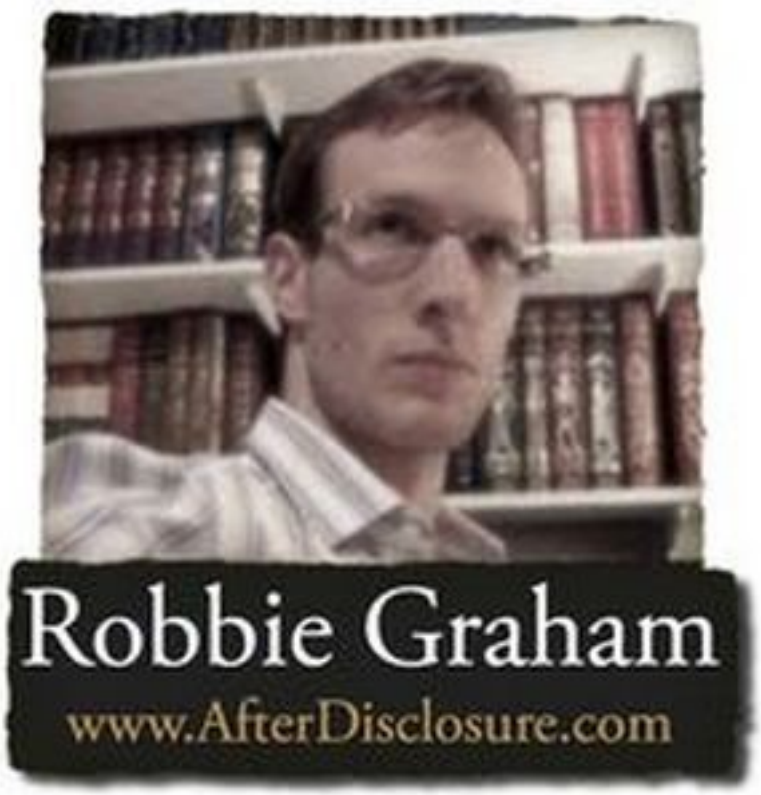
Намек или прямая угроза?

Среди гигантского количества всевозможных тем, затрагиваемых в книге Cryptos Conundrum, отчетливо проходит линия о некоем чересчур любопытном и непонятливом журналисте, который упорно не желает признавать важность секретности для успехов работы разведки.

Этот журналист решительно настроен срывать покровы тайны со всех тех заговоров и загадочных историй, что постоянно окружают деятельность ЦРУ и федерального правительства США. И поскольку практически в любой из этих историй раньше или позже непременно всплывает имя Джонатана Чалмерса, настырный журналист начинает собственное расследование с целью добраться до истинной роли и намерений этого человека.

Чалмерс, в свою очередь, не испытывает никаких добрых чувств к разнюхиваниям репортера, то и дело путающегося под ногами. Так что в конечном счете «всемогущий Ч.» устраивает дела таким образом, чтобы журналиста при подходящем случае грохнули. То есть естественным результатом этой коллизии становится известная у шпионов и бандитов формула «нет человека – нет проблемы».

Самое же примечательное в этой сюжетной ветви то, что незадачливого журналиста звали Роберт Грэм (Robert Graham). И по явно неслучайному совпадению именно так, Robert Graham, зовут вполне реального и до сих пор живого, к счастью, человека, входящего, по его собственным словам, «в ту очень небольшую группу авторов в мире», кто публикует время от времени статьи-расследования о закулисной деятельности реального цэрэушника по имени Чейз Брэндон.



Повышенный интерес к персоне Брэндона вызван тем, что если вы забьете в окне запросов Google или другой подобной ей поисковой интернет-системы всего пару содержательных слов типа «CIA and Hollywood» (ЦРУ и Голливуд), то в первых строках поиска непременно окажется информация с упоминаниями об этом человеке.

Происходит так по следующей простой причине. Когда в 1996 году ЦРУ США создало в своей структуре специальный Отдел по связям с индустрией развлечений (Entertainment Liaison Office), то главой данного подразделения был назначен Чейз Брэндон – многоопытный сотрудник разведки, четверть века отслуживший в элитном подразделении ЦРУ, занимающемся тайными операциями (а непосредственно до нового назначения знакомивший президента США Билла Клинтона с ежедневными информационными сводками разведслужб).

Иначе говоря, проводить линию влияния ЦРУ в Голливуде назначили не какого-нибудь ушлого пиарщика, а человека, чрезвычайно искушенного в тайных делах разведки. Но при этом и не сказать, что абсолютно далекого от мира кино – двоюродным братом Брэндона является известный всем актер и «человек в черном» Томми Ли Джонс.

Если же говорить об исследовательских изысканиях Роберта Грэма, то на протяжении последних нескольких лет он является соискателем-докторантом британского Университета Бристоля, где готовит к защите культурологическую диссертацию на тему «Голливуд и НЛО».

И вот, в научных изысканиях Грэма все складывается так, что чем больше он роет материалов и документов об истории неувядающего интереса Голливуда к теме НЛО и

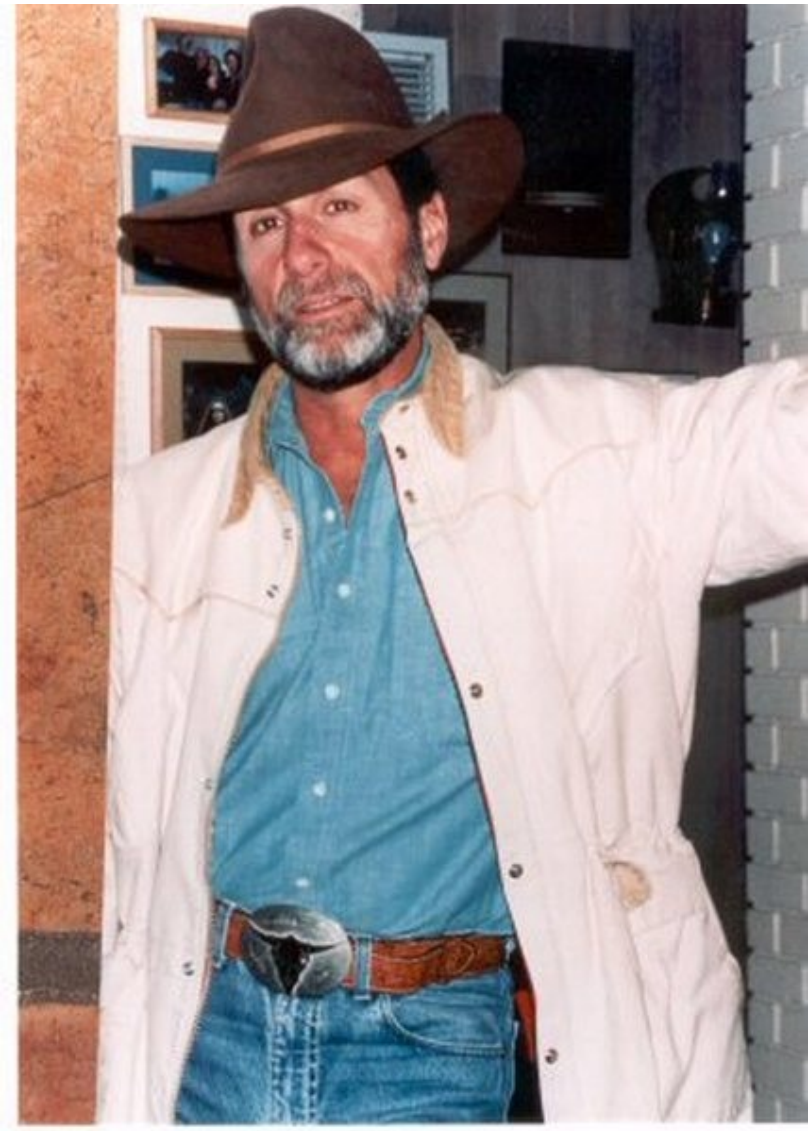
инопланетян, тем больше отовсюду начинают торчать уши ЦРУ. То есть, буквально с самого первого фильма 1951 года «Когда Земля остановилась», где впервые на кино-экране происходит появление и приземление инопланетной летающей тарелки, в представлении этой темы публике непременно обнаруживается непосредственное участие людей из разведки.

Ну а уж когда в ЦРУ начал работать специально созданный отдел «по связям с Голливудом», то понятно, что и в специфических изысканиях Роберта Грэма то и дело стало мелькать имя Чейза Брэндона. Однако по-настоящему исследователя встревожило, конечно, не это, а то, что Брэндон недвусмысленно фигурирует и в куда более жестких, без преувеличения трагических ситуациях из реальной жизни американского кинематографа.

Как, скажем, в такой истории с исчезновением довольно заметного в Голливуде человека – истории, в подробностях раскопанной и описанной Робби Грэмом и его частым соавтором, Мэтью Олфордом (Matthew Alford).

Смерть со многими неизвестными

В 1997 году Гэри ДеВор (Gary DeVore), прежде известный как сценарист целого ряда успешных голливудских боевиков со звездами типа Арнольда Шварценеггера и Курта Рассела, получил возможность снять собственный фильм уже в качестве режиссера. Понятно, что сценарий для своего режиссерского дебюта он готовил сам. В качестве же базовой темы для этой картины в кассовом жанре «экшн» было выбрано военное вторжение США в Панаму в 1989 году.



При подготовке сценария ДеВор много обсуждал тему Панамы со своим старым приятелем-цэрэушником Чейзом Брэндоном, с которым они познакомились и сошлись еще в 1986, на свадьбе Томми Ли Джонса. Наверняка у Брэндона имелось немало информации о панамском диктаторе Мануэле Норьеге – человеке, многие годы, еще с 1950-х годов работавшем на ЦРУ, в итоге сосредоточившем в своих руках почти безграничную государственную власть, а затем вдруг ставшем для США крайне нежелательной фигурой.

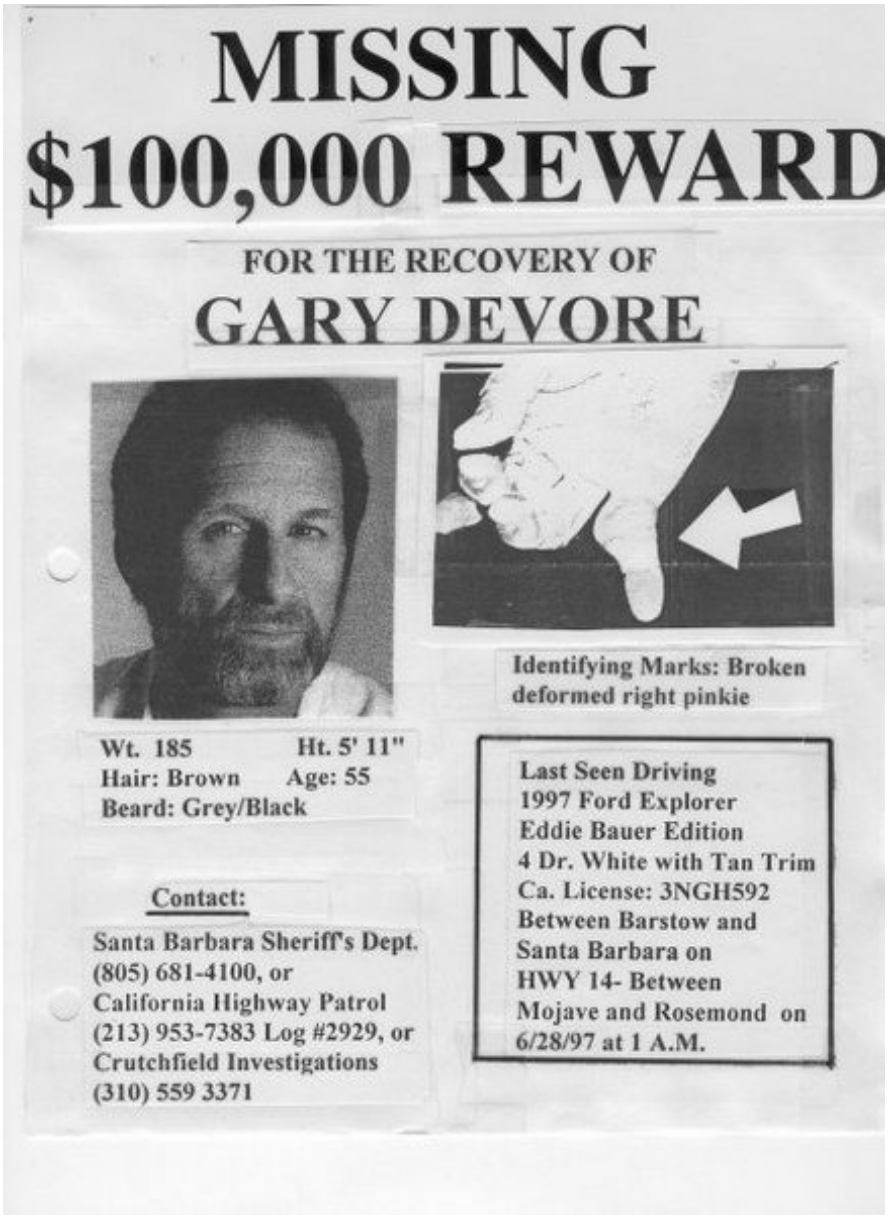
По свидетельству жены сценариста, Венди ДеВор, чем больше ее муж узнавал о закулисных подробностях панамской истории, тем мрачнее он становился. Или, выражаясь собственными словами автора, он осознал, что «чем глубже копаешь, тем грязнее и грязнее все это дело становится».

Собранные ДеВором факты указывали на то, что истинной причиной Панамской военной кампании были гигантские суммы нелегальных денег, под покровительством Норьеги отмывавшихся в банках этой небольшой страны и наркомафией, и тайными структурами в правительстве США.

Соответственно, генерала Норьегу свергли из-за того, по сути, что в какой-то момент его высокие «американские покровители» решили присвоить все эти деньги себе…

Твердо решив сохранить в своем фильме реальную основу событий, ДеВор стал вносить в сценарий соответствующие коррективы. И попутно, в конце июня 1997, на неделю отъехал из Калифорнии в город Санта-Фе, штат Нью-Мексико, по смежным делам кинопроизводства. На обратном пути, когда сценарист был уже в нескольких часах езды от дома, у них среди ночи произошел телефонный разговор с женой, который крайне встревожил Венди.

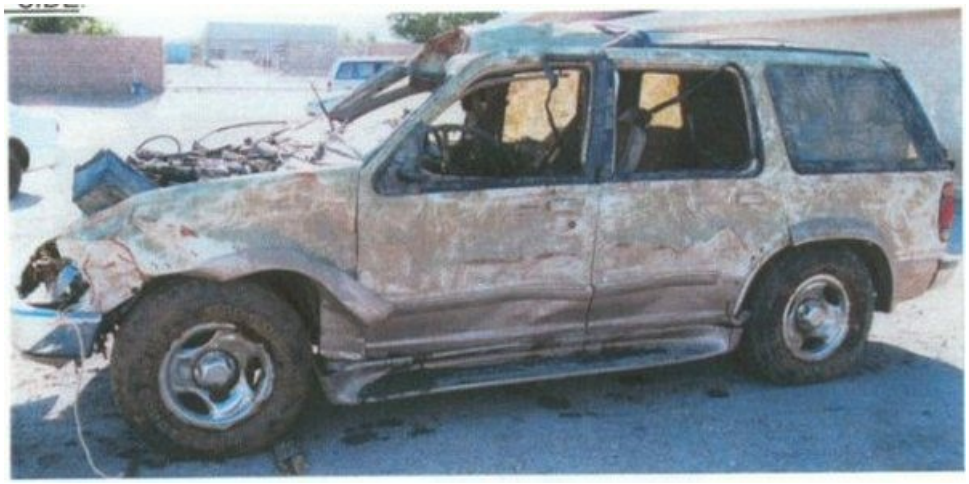
По некоторым необычным деталям в их разговоре жена поняла, что в машине рядом с мужем находился кто-то еще. Неясное беспокойство быстро переросла в ощущение трагической потери, когда ДеВор не только не вернулся домой к утру, но и вообще бесследно исчез вместе со своей машиной.



В течение года найти пропавшего человека не помогли ни полиция, ни нанятый женой частный детектив, ни объявленная денежная награда за информацию о Гэри ДеВоре и его машине. Но при этом сразу несколько параллельных расследований выявляли все больше и больше признаков явной замешанности ЦРУ в исчезновении человека.

То есть дело о пропаже не просто никак не удавалось спустить на тормозах, но более того, год спустя, летом 1998, об этом престранном происшествии написала «Лос-Анджелес Таймс» – одна из ведущих в США газет, да еще и с воспроизведением обоснованных подозрений относительно «следа ЦРУ».

И вот тогда, примерно через неделю после публикации LA Times, разбитая машина вместе с разложившимся до скелета телом вроде бы ДеВора вдруг чудесным образом нашлись – на дне водоема в нескольких метрах от весьма оживленной автотрассы. Получив в свое распоряжение машину и тело, судебно-полицейские власти довольно быстро закрыли дело как «несчастный случай» с водителем, заснувшим за рулем и упавшим в воду. При этом огромное количество вопиющих нестыковок данной версии так и осталось без объяснения.



Начать можно с того, что на дороге, с которой машина должна была вылететь в воду, не нашли никаких повреждений металлической ограды. У автомобиля, среди ночи исчезнувшего вместе с водителем из поля зрения антенн сотовой связи, оказались выключены фары. А чтобы улететь с дороги туда, где ее обнаружили в воде, машина должна была нестись со скоростью свыше 100 км/час.

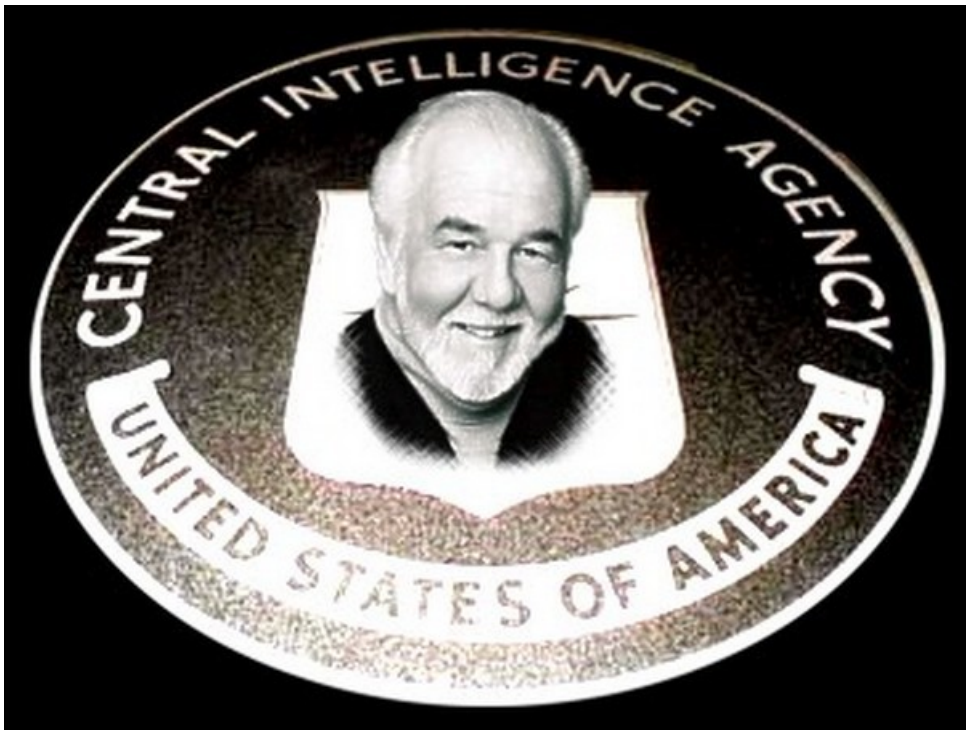
Но это только начало. Тело якобы ДеВора, пристегнутое к креслу водителя, почему-то оказалось без рук. Причем именно эта часть скелета могла бы стать важнейшим доказательством для опознания тела – у сценариста был сильно деформирован когда-то давно переломанный и неправильно сросшийся мизинец на правой руке. Когда Венди ДеВор начала поднимать по данному поводу шум и скандал, руки вдруг нашлись – где-то там в задней части машины. (Впоследствии выяснится, что по результатам экспертизы костям этих рук оказалось свыше 200 лет…)

Наконец, на то, что машина была явно кем-то подброшена на место ее обнаружения, указывало и отсутствие в салоне весьма важных вещей. Во-первых, в автомобиле не оказалось ни пистолета ДеВора, ни патронов к нему, хотя сценарист, отправляясь в дальние поездки, всегда брал с собой оружие «на всякий случай». А во-вторых, исчез ноутбук ДеВора со сценарием кинофильма, над которым он тогда работал.

В этой связи тут же вспомнили, что всего через несколько дней после исчезновения сценариста к нему домой под неким естественным предлогом заходил «один из друзей, работающий в ЦРУ».

Быстро выяснилось, что «друг» зачем-то уединялся в кабинете ДеВора и есть свидетели, видевшие, как он что-то делал с настольным компьютером сценариста. А вскоре после этого обнаружилось, что компьютер напрочь «умер», причем другие версии сценария и прочие рабочие материалы к фильму восстановить с жесткого диска было уже невозможно.

Этого «друга семьи», посещавшего дом ДеВоров в столь трагические дни, как несложно догадаться, зовут – ну конечно же – Чейз Брэндон…



По настояниям Венди ДеВор, сотрудники полиции Санта-Барбары, расследовавшие все это дело, несколько раз пытались связаться с Брэндоном для выяснения причин и обстоятельств, связанных с его подозрительными копошениями в компьютере погибшего. Однако руки местной полиции оказались явно коротки, чтобы дотянуться до столь важного человека.

Тогда голливудским друзьям ДеВоров, имеющим связи «наверху», удалось привлечь к расследованию этой истории ФБР. Но и сотрудники ФБР сумели добиться лишь того,

что Чейз Брэндон однажды согласился с ними побеседовать – в стенах штаб-квартиры ЦРУ в Лэнгли. По результатам этой беседы было сделано окончательное заключение, что для полиции «нет никакой необходимости разрабатывать эту ветвь расследования»…

Убийства без закона

Возвращаясь к самому началу всей этой замысловато сплетенной истории, можно напомнить, что исходной точкой была директива президента Форда от 1976 года, с одной стороны вроде бы запрещавшая ЦРУ физические устранения людей, но с другой не обозначившая четких границ этого запрета.

Как непосредственный результат этой нечеткости, возможно, бывшего агента ЦРУ генерала Норьегу убивать не стали – так что он по сию пору все сидит и сидит по тюрьмам разных стран (поначалу в США, потом во Франции, а теперь, говорят, уже дома в Панаме). В то же время, история с исчезновением Гэри ДеВора не оставляет практически никаких сомнений, что в этой истории с физическим устранением человека явно замешано ЦРУ.

И если как следует покопаться в соответствующих материалах, подобных (но менее изученных в деталях) историй даже в период до 2001 года можно отыскать немало. Что же касается совсем другой эпохи после 11 сентября 2001, то количество «врагов Америки», по сути уже без всяких прикрытий массово убиваемых ЦРУ с помощью летающих роботов-дронов, ныне вряд ли поддается какому-то учету.

И неудивительно, что саму идею о подобных убийствах людей разведкой – без всяких судов и следствий, на территории стран, с которыми США не ведет никакой войны – американским гражданам начали прививать подспудно и заранее, с экранов экшн-фильмов и телевизионных сериалов.

Причем есть непосредственные свидетельства кинорежиссеров о том, что идею вставлять в картину подобного рода ликвидации им подавал уже известный нам Чейз Брэндон, «человек ЦРУ в Голливуде».

Более того, поскольку под ракетную раздачу смерти с дронов уже понемногу стали попадать и граждане США (из разряда «опасных экстремистов», конечно же), сама идея подобных беззаконных ликвидаций в умах американских обывателей тоже понемногу становится приемлемой и в отношении сограждан. Ведь все это смертоубийство – ради спасения страны и мира, ясное дело…

Вместо эпилога: снова о Kryptos

Что же касается так и недорасшифрованного криптомонумента Джима Сэнборна во дворе ЦРУ в Лэнгли, то от самого скульптора достоверно известно, что текст послания составлял и шифровал он сам, наделав при этом кучу ошибок. (Подробности о технической стороне всей этой истории и переведенные на русский язык фрагменты дешифрованной криптограммы можно найти в материале: Монументальное искусство криптографии.)

Известно и то, что до победы в творческом конкурсе на декоративное украшение двора ЦРУ, никаких связей с разведслужбами у Сэнборна не было. Иначе говоря, зашифрованный текст в недовскрытом фрагменте его скульптуры, имеющий вид

OBKR
UOXOGHULBSOLIFBBWFLRVQQPRNGKSSO
TWTQSJQSSEKZZWATJKLUDIAWINFBNYP
VTTMZFPKWGDKZXTJCDIGKUHUAUEKCAR

и длину 97 знаков, по определению не может содержать в себе не то что государственные секреты, но и вообще сколь-нибудь существенную информацию о спецслужбе.

Так что все фантазии Чейза Брэндона относительно «ужасных тайн», скрытых в тексте Kryptos, это гарантированное вранье. И есть большое подозрение, что таким же враньем является и все остальное в его книге.

Кроме, разве что, тех вещей, которые все и так давно знают без Брэндона: что JFK был действительно убит в результате заговора, а в 1947 году под Розуэллом действительно разбились инопланетяне (см. НЛО: история болезни).

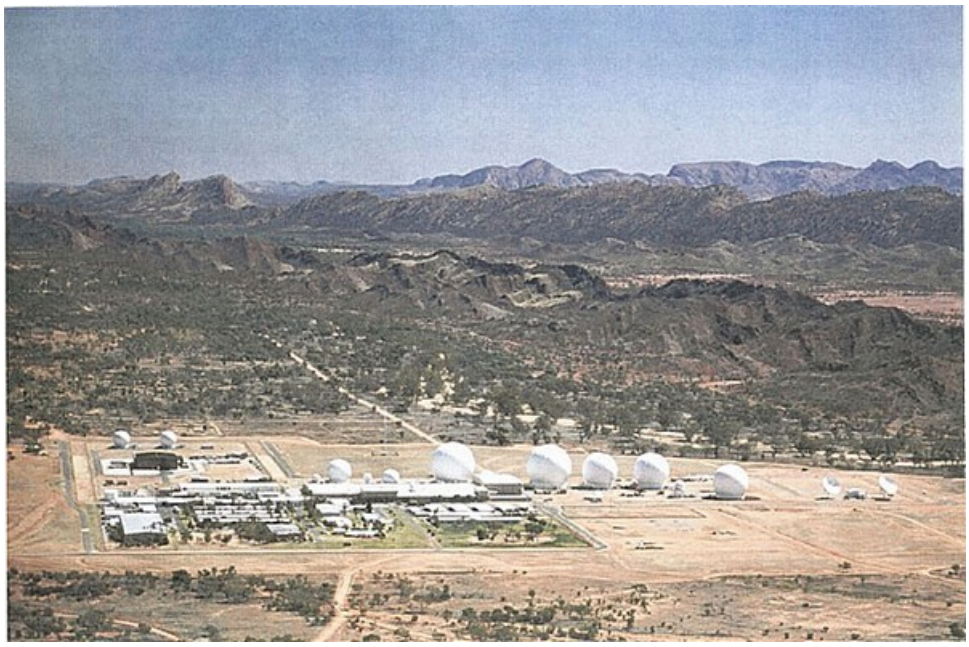
И что, конечно же, в сокрытии всех этих «тайн» реально замешано ЦРУ.

# # #

Шпион, который пришел из пустыни

(*Впервые опубликовано – июль 2011*)

В Австралии появилась мемуарная книга, имеющая самое непосредственное отношение к глобальной системе перехвата ECHELON. Как это часто бывает с подобной литературой, книга не столько дает ответы, сколько порождает новые вопросы.



Военная база Пайн-Гэп (Pine Gap), расположенная посреди гористой пустыни в самом центре австралийского материка, слывет в стране самой большой государственной тайной властей. Причем тайна эта засекречена настолько глубоко, что к ней не подпускаются даже люди из самого высшего руководства Австралии – от премьер-министра до законодателей из сенатского комитета по государственным договорам, включая секретные.

Кто же именно их «не подпускает» и как это вообще возможно в демократическом государстве – само по себе огромная тайна…

Понятно, что в подобном загадочном контексте новая автобиографическая книга, выходящая ныне из печати в Австралии, определенно должна вызывать у публики повышенный интерес. Книга носит название «Внутри Пайн-Гэп. Шпион, который пришел из пустыни» («Inside Pine Gap: the spy who came in from the desert», by David Rosenberg, 2011), а автор ее, Дэвид Розенберг, проработал на этой суперсекретной базе техническим специалистом без малого двадцать лет.

Вообще-то Розенберг по своей национальной госпринадлежности от рождения и вплоть до недавнего времени был гражданином США, а на протяжении 23 лет своей жизни являлся кадровым сотрудником американского Агентства национальной без-

опасности, то есть крупнейшей в мире спецслужбы по разведке средств связи. Однако из двадцати трех лет своей работы в АНБ девятнадцать последних, с 1990 по 2008, Розенберг провел в Австралии на базе Пайн-Гэп – как специалист по ELINT (от Electromagnetic Intelligence, разведка электромагнитных излучений). По увольнении из разведки он получил австралийское гражданство, решив остаться на новой родине с новой семьей.

Для людей, совсем далеких от тонкостей шпионской жизни, подобные факты биографии могут показаться несколько странными. Но для всех, кто мало-мальски интересуется деятельностью разведслужб вообще и радиоэлектронной разведки в частности, давно уже не секрет, что в действительности Пайн-Гэп является не австралийской базой, а секретной военно-разведывательной станцией США, изначально и полностью сооруженной американцами на арендуемой у Австралии территории. Используемое же для базы официальное название, «Совместный оборонный объект Pine Gap», придумано, похоже, ради того, чтобы не раздражать лишний раз беспокойную часть австралийской общественности.

Объект Пайн-Гэп известен как одна из самых крупных зарубежных станций разведывательного сообщества США. По сведениям австралийского профессора Деса Болла (Des Ball), главного в стране эксперта по этой базе, секретное соглашение о создании Пайн-Гэп было подписано правительствами Австралии и США 9 декабря 1966 года. Строительство объекта, расположенного в 18 километрах к юго-востоку от города Элис-Спрингс, заняло около 3 лет. К работе станция приступила в 1970-м, когда в Пайн-Гэп переехали вместе с семьями примерно 400 сотрудников американских разведслужб.

К настоящему времени на сильно разросшейся станции работают порядка 1000 человек, в основном это сотрудники АНБ, ЦРУ и NRO, Управления космической видовой разведки США. Количество антенн спутниковой связи увеличилось с первоначальных 2 до примерно 18 к 1999 году, однако точные цифры на сегодня неизвестны, поскольку большинство антенн закрыто кожухами, а все оценки делаются лишь на основе анализа фотографий.

Что там делает на базе вся эта туча людей и техники в общих чертах, конечно, понятно – ясное дело что, шпионят. Однако, как только дело доходит до уточнения подробностей, все тут же покрывается мраком тайны и непонятности.

Например, по свидетельству знающих людей, к базе Пайн-Гэп не подведено никаких линий электропередачи. Официально принято считать, что всю электроэнергию объект получает от собственной дизельной электростанции. Однако, опять-таки по свидетельству персонала из местной австралийской обслуги, эта станция практически всегда находится в неработающем состоянии… Одновременно есть устойчивый слух, что глубоко в подземных недрах (куда база уходит чуть ли не на 12 уровней, а австра-

лийцев туда и близко не подпускают) работает ядерный энергоблок, типа тех, что используют в подводных лодках.

Другой пример странностей – закрытая для полетов зона. Согласно официальным документам управления гражданской авиации, воздушное пространство над базой Пайн-Гэп является единственной на всю Австралию территорией, над которой запрещен пролет воздушным судам. Такого рода запреты хорошо известны для иных секретных объектов, вроде Зоны 51 в Неваде, но там находится полигон по испытанию оружия и новых летательных аппаратов. Разведстанция же Пайн-Гэп ничего похожего на подобные полигоны вроде как не имеет и иметь не должна.

Но самый, пожалуй, любопытный набор чудес вокруг Пайн-Гэп связан с тем, насколько мощно и решительно удается ограждать таинственную базу США от любых внешних посягательств на ее секреты.

Самый яркий пример на данный счет дают малоизвестные подробности в известной истории со смещением премьер-министра Австралии Гофа Уитлэма (Gough Whitlam) в 1975 году. Лейборист Уитлэм стал главой государства в 1972, когда руководимая им партия одержала победу на выборах, и за недолгое время правления успел сделать немало больших дел: в области бесплатного образования и здравоохранения, в ликвидации расовой дискриминации и укреплении прав коренного населения, в области более самостоятельной внешней политики страны, наконец.

Курс Австралии на отход от полной военно-политической поддержки США, естественно, не мог не обеспокоить американских союзников. Как показали рассекреченные в 1990-е годы документы, уже в 1974 между американским госсекретарем Генри Киссинджером и президентом Никсоном ходил меморандум, в котором австралийского премьера Уитлэма и его действия трактовали как угрозу национальной безопасности США. Критической же точкой в этой напряженности стал вопрос о базе Пайн-Гэп.

Поскольку в тот период австралийцев в принципе не подпускали к любым аспектам оперативной деятельности секретной станции (некоторые сдвиги начнутся лишь в 1980-е годы), Гоф Уитлэм – сам в прошлом военный летчик и ветеран второй мировой – был крайне недоволен, что не может получить никакой внятной информации о деятельности этого военного объекта.

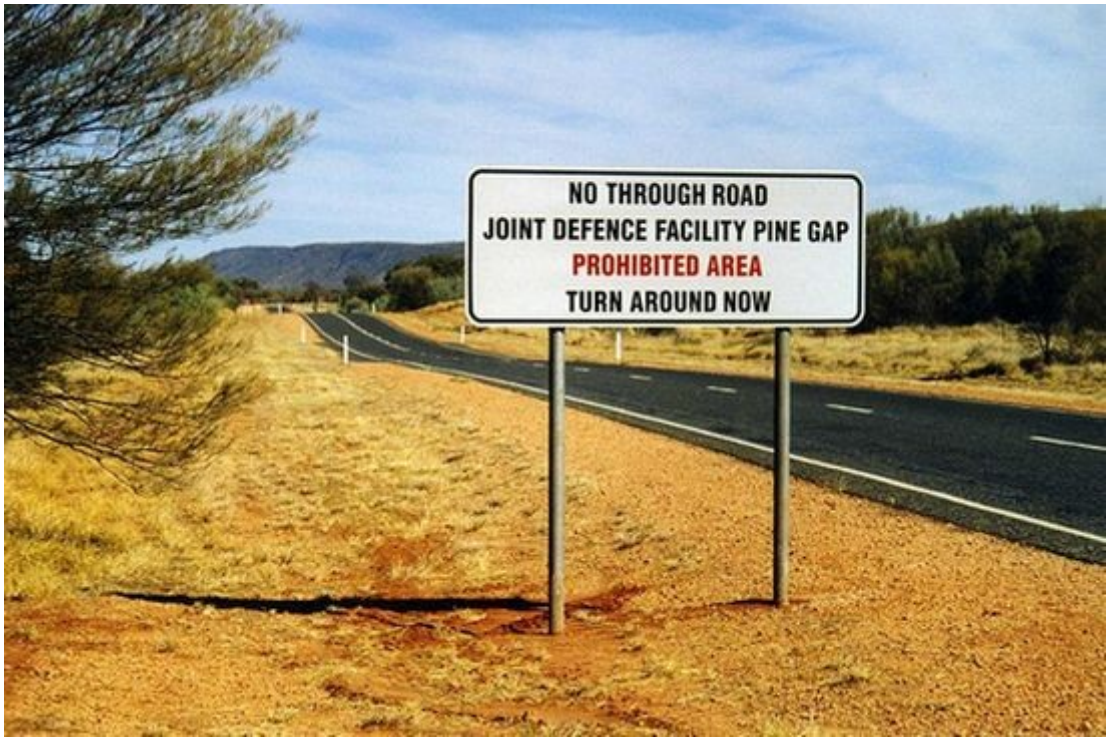
Только лишь после неоднократных и очень настойчивых запросов в министерство обороны Уитлэму удалось, наконец, узнать, что Пайн-Гэп является не центром туманных «военно-космических разработок» (как гласила официальная легенда), и тем более не «метеорологической базой» (как заявляли австралийцам в самом начале), а сугубо шпионским объектом, решающим некие темные задачи в интересах США.

Когда же Уитлэм выяснил, что Ричард Столлингс (Richard Lee Stallings), возглавлявший строительство базы Пайн-Гэп и самый первый начальник объекта, в действитель-

ности вовсе не американский военный, а кадровый сотрудник ЦРУ, работавший под прикрытием министерства обороны, то он потребовал предоставить ему списки всех подобных разведчиков США, тайно работающих на территории Австралии – своего ближайшего союзника в тихоокеанском регионе.

А попутно – дело было осенью 1975 – премьер-министр в одном из публичных выступлений объявил согражданам, что Пайн-Гэп является вовсе не военно-оборонительной базой, как всех прежде заверяли, а настоящим шпионским гнездом. В этой связи Уитлэм пообещал разобраться с базой, и всерьез рассмотреть вопрос о целесообразности ее дальнейшего пребывания на австралийской территории. Чем, по сути дела, и утвердил решение об отстранении себя от власти.

Очень скоро в действие были запущены весьма экзотические механизмы тайной политической кухни. Благодаря этим механизмам абсолютно номинальная фигура из колониального прошлого Австралии – генерал-губернатор, формально назначаемый английским монархом и давно не имеющий никакой реальной власти в стране – вдруг оказался всесильной инстанцией, которая в обход всех демократических процедур отстранила Уитлэма от руководства государством. Ни до, ни после этой истории ничего подобного в жизни Австралии больше не происходило…



База Пайн-Гэп, ясное дело, продолжила свою работу – причем уже без всяких подобных проблем в дальнейшем. А еще через четверть века австралийцам было наглядно продемонстрировано, что и законодательная власть их страны над этим удивительным объектом имеет примерно такую же степень контроля, что и власть исполнительная. То есть и тут, если разобраться, полномочия власти практически ничего не означают.

К 1999 году, можно напомнить, Холодная война уже давным-давно закончилась, однако разведывательные базы США по всему миру не только не исчезли, но и стали демонстрировать вполне отчетливые признаки роста. Поэтому в парламенте Австралии – по примеру коллег из Евросоюза – решили всерьез озаботиться вопросом о новых целях американского шпионажа, коли ни главного врага в лице СССР, ни его союзников из стран Варшавского договора на политической карте мира уже не осталось.

Особенно парламентариев беспокоила крупнейшая шпионская база Пайн-Гэп, поскольку на тот момент уже было обнародовано достаточно много секретных прежде сведений о глобальной системе радиоперехвата Echelon и о том немаловажном месте, которое занимает в этой системе Пайн-Гэп. Но как только сенатский комитет австралийского парламента, занимающийся государственными договорами страны, попытался выяснить текущее состояние дел на этой секретной базе, то тут же выяснилось, что по официальным каналам ничего конкретного узнать на данный счет никак невозможно.

То есть руководители австралийской разведки сослались на предоставленные ими американской стороне обязательства, требующие строго хранить тайну, а спецслужбы США просто парламентариев проигнорировали. По этой причине Сенату пришлось довольствоваться лишь заслушиванием отчета специально приглашенного независимого эксперта, уже упоминавшегося профессора Деса Болла. Однако Болл, ясное дело, никаких допусков к реальным секретам Пайн-Гэп не имел…

Для полноты этой унылой картины осталось лишь упомянуть о специфических отношениях с Пайн-Гэп третьей ветви австралийской демократии – власти судебной. Американские базы на территории Австралии давно, еще со времен вьетнамской войны, являются объектом мирных атак со стороны местного антивоенного движения. В знак протеста пацифисты проникают на базы с лозунгами и транспарантами, таких людей, естественно, отлавливают и затем штрафуют на ту или иную сумму за нарушение порядка.

Однако то, что произошло не так давно с аналогичной историей в Пайн-Гэп, как обычно, не имеет прецедентов в истории страны. В 2005 году австралийские пацифисты устроили особенно настырную антивоенную демонстрацию непосредственно у ворот базы, а несколько самых рьяных прорвались за ограду на велосипедах и стали там гонять по местной взлетно-посадочной полосе – пытаясь таким образом сорвать приземление здоровенного транспортного самолета ВВС США Galaxy с очередным секретным грузом для базы.

Нарушителей, как водится, арестовали и предали суду. Но не суду, точнее говоря, а позорному судилищу, поскольку специально для обвинения по этому делу из пыльных архивов самой дремучей эпохи Холодной войны извлекли никогда прежде не применявшееся особое приложение к закону о национальной обороне 1952 года. И на основании этой статьи попытались влепить велосипедистам-миротворцам не только по 3 с

половиной тысячи штрафа, но и еще по 7 лет тюрьмы. Из-за поднявшегося в обществе шума столь неадекватное «правосудие» вскоре пересмотрели и отменили, но крайне неприятный осадок, конечно же, у народа остался…

Короче говоря, уже понятно, наверное, что новая книга о секретах шпионской базы Пайн-Гэп, да еще рассказанная очевидцем-инсайдером, долго и непосредственно наблюдавшим все изнутри, не может не вызывать к себе интереса. Вот только интерес этот, увы, в книге Дэвида Розенберга удовлетворить практически нечем. Потому что никаких особых откровений или, тем более, раскрытия шпионских тайн там нет и в помине. А есть, главным образом, изложение общеизвестных банальностей о трудной работе бойцов невидимого фронта, да бытовые подробности из скучной жизни инженера-электронщика на изолированной от всего мира базе посреди пустыни.

Да и что можно ожидать от книги, которую целый год после ее написания выхолащивали в режимных инстанциях АНБ? А сам автор мемуаров, когда его напрямую спрашивают о том, чем же именно занимается Пайн-Гэп, в ответ способен лишь процитировать заявление бывшего премьер министра Австралии Боба Хоука (Bob Hawke) от 1988 года – как самый лучший, по его мнению, отчет о той роли, которую данная база играет в разведывательном сообществе Австралии и США.

Выступая в парламенте Австралии в ноябре 1988 года, Хоук дословно сказал следующее: «Пайн-Гэп – это спутниковая наземная станция, функция которой состоит в сборе разведывательных данных, обеспечивающих национальную безопасность Австралии и США. Разведывательная информация, собираемая в Пайн-Гэп, делает важный вклад в проверку обязательств государств по контролю за вооружениями и по выполнению соглашений о разоружении». То есть, иными словами – «мы сорок лет на страже мира».

Совершенно неясно только, к чему тогда вся эта дикая и нервная возня – вплоть до госпереворота – вокруг обеспечения секретности объекта, столь важного для дела мира во всем мире.

Как ни странно это прозвучит, но отчетливый намек на причины столь беспрецедентной таинственности дает общенародная энциклопедия Википедия в своей англоязычной статье (en.wikipedia.org/wiki/Pine_Gap), посвященной Пайн-Гэп. Многие, наверное, наслышаны (а кто не слышал, пора узнать, см., к примеру, материал «Шпионы в стране Wikipedia«), что все статьи Википедии, так или иначе касающиеся работы разведслужб, этими спецслужбами, как правило, плотно контролируются. Дабы не допускалось ни малейших отклонений информации от версии, официально принятой властями.

Ну а жесткое следование инструкциям, как известно, способно порождать эффект, прямо противоположный задуманному.

Если (через любой поисковик) сравнивать текст Wikipedia-статьи о базе с тем, что пишут чаще всего о Пайн-Гэп во всей остальной части интернета, то сразу же заметно бросающееся в глаза несоответствие. Потому что база Пайн-Гэп – это самое известное в Австралии место из тех, где чаще всего наблюдаются НЛО или, более нейтрально, «неустановленные воздушные феномены». И хотя на данный счет имеется сколько угодно свидетельств прессы, в статье обычно дотошных википедистов о Пайн-Гэп по поводу частых в этом районе НЛО нет ни малейшего упоминания.

Иначе говоря, сама собой приходит мысль, что если слова нет, то кем-то оно запрещено. А если слово запрещено, то приходится предположить, что кому-то здесь явно очень хочется что-то скрыть.

Ну а если подобная цепь рассуждений выглядит правдоподобной, то естественно задаться следующим вопросом: «Что же такого интересного-австралийского происходило за последнее время в одиозной области уфологии, если кому-то понадобилось не только широко рекламировать в прессе, но и срочно ускорять выпуск скучной и малосодержательной, в общем-то, книги Дэвида Розенберга о Пайн-Гэп»? Ибо, согласно анонсу книжного магазина Amazon, книга «Шпиона, который пришел из пустыни» прежде ожидалась к выходу только в сентябре. И вдруг все статьи-рецензии на книгу Розенберга, дружно появившиеся в конце июня, со знанием дела стали обещать ее выход «на этой неделе».

Недолгий, в общем-то, поиск информации в Сети показывает, что да, действительно появлялась недавно в прессе Австралии любопытная информация про загадки НЛО. А именно, австралийское министерство обороны в начале июня 2011 года официально известило своих сограждан, что запланированное ранее рассекречивание их файлов о наблюдениях и происшествиях с НЛО, к сожалению, не состоится. По той простой причине, что файлы эти, как выяснилось, «потерялись» (www.smh.com.au/technology/sci-tech/alien-abduction-defences-xfiles-are-lost-in-space-20110606-1fpea.html).

Для тех, кто более-менее знаком с фантасмагорической логикой событий в истории уфологии, эта новость ничуть не удивительна. По весьма похожей схеме ранее уже были «утрачены» подлежащие вечному хранению документы авиабазы США под Розуэллом (www.roswellfiles.com/Articles/destruct.htm), относящиеся именно к тому периоду, когда там в 1947 году были обнаружены обломки разбившихся НЛО. Затем аналогичная история с потерей секретных документов произошла и в Великобритании, когда пропали отчеты о таинственных событиях 1980 года в Рэндлшем Форест, в народе получивших название «английский Розуэлл».

Базу Пайн-Гэп, в свою очередь, нередко называют «австралийской Зоной 51». Как в местной прессе, так и – наверняка – в секретных отчетах военных собрано немало историй очевидцев о странных атмосферных явлениях и совершенно неземного вида летательных аппаратах, не только регулярно наблюдаемых в районе Пайн-Гэп, но и вы-

летающих, бывает, из приоткрывающегося на краткое время портала в склоне одной из гор на территории базы.

Какие именно наблюдения и отчеты были накоплены в секретных файлах у военных, теперь уже и не узнать. По крайней мере, в ближайшее время. Вместо этого всем любопытствующим предложено почитать мемуар шпиона о секретных сражениях базы Пайн-Гэп за дело мира и демократии. Пресновато, конечно, но зато никаких упоминаний о сомнительных НЛО. Гарантировано.

# # #

Контакт до и после «Прибытия»

(*Ноябрь 2016*)

Новый фильм Arrival или «Прибытие», по дружному мнению зрителей и критиков, практически сразу занесен в разряд шедевров кинофантастики. Естественно, хотелось бы разобраться с секретом успеха картины.

Поскольку мировая премьера Arrival состоялась совсем недавно, в очевидно с умыслом выбранный день 11-11, посмотреть кино наверняка довелось еще далеко не всем. А потому при рассказе о фильме и его ключевых идеях здесь будет сделано всё возможное, чтобы не допустить спойлеров и не испортить людям удовольствие от просмотра.

Пролог про эпилог

Несмотря на то, что количество новых кинокартин в жанре научной (а также околонаучной и совсем ненаучной) фантастики ежегодно исчисляется десятками, нечто действительно сильное и запоминающееся появляется, прямо скажем, нечасто. И совсем уж редко бывает так, чтобы очередной свежий фильм ставили в один ряд с такими общепризнанными шедеврами, как «2001: Космическая одиссея» Стэнли Кубрика и «Солярис» Андрея Тарковского.

С фильмом «Прибытие» канадского режиссера Дени Вильнёва, однако, произошла именно такая история. Причем вряд ли случайность, что как и в двух упомянутых эталонах, главная тема картины и здесь примерно та же самая – первый контакт человечества с инопланетным разумом.

И точно так же, как в фильмах Кубрика и Тарковского, особо важными для восприятия произведения оказываются финальные сцены. Или иначе, эпилог истории. Ибо зрители, внимательно следившие за происходящим на экране, по окончании первого просмотра каждой из этих киноисторий чаще всего оказываются в состоянии если и не шока, то озадаченного недоумения как минимум.

С одной стороны, финал предоставляет вроде бы вполне ясную картину. Но вот что именно эта картина означает для конкретных людей и человечества в целом – спорить можно очень долго.

Единственное, пожалуй, что бесспорно при такого рода эпилоге, так это следующая идея. «После Контакта» мир вселенной оказывается устроен не просто сильно, а в принципе иначе, нежели представлялось человеку прежде…

Что обсуждают сейчас

Если судить по множеству публикуемых ныне рассказов о подробностях создания фильма, то одним из важнейших факторов в успехе картины стала чрезвычайно тщательная подготовка, так сказать, твердой научной основы для всей фантастики на экране. Ибо ради придания максимальной реалистичности происходящему съемочная группа привлекла в кинопроизводство настоящих больших ученых, а режиссер, сценарист и художники-декораторы предельно достоверно воспроизвели их работу в соответствующих сценах.

Поскольку главными героями картины «по научной части» являются женщина лингвист (Луиза Бэнкс в исполнении Эми Адамс) и физик-теоретик мужчина (Иэн Доннели в исполнении Джереми Реннера), то и в качестве их реальной опоры были пригла-

шены подобающие консультанты. За дешифрование языка инопланетян «отвечала» профессор лингвистики Джессика Кун (Jessica Coon) из монреальского университета Макгилла. Ну а за всю прочую твердую науку – знаменитый ученый-компьютерщик Стивен Вольфрам, в прошлом физик-теоретик, а последние несколько десятков лет глава солидной научно-софтверной фирмы Wolfram Research, наиболее известной благодаря своему пакету программ Mathematica и особому языку программирования Wolfram Language в основе продуктов компании.

Задача ученых в фильме – быстро и эффективно научиться общаться с негуманоидными инопланетянами, об устройстве языка и мировосприятия которых люди не имеют ни малейшего представления. В частности, жизненно необходимо получить от пришельцев внятные ответы на совершенно конкретные вопросы. Типа самого главного:

«Зачем вы все здесь на Земле появились?»…

Первоначально данная статья задумывалась просто как обзор всевозможных идей, технологий и фантазий, которые создатели картины генерировали, обкатывали и встраивали в свое произведение. Но по мере углубления в материал стало совершенно ясно, что все это уже многократно было когда-то – там и тут, в разных формах, при создании прочих подобных картин.

Новая история, спору нет, сделана качественно и талантливо, но это опять-таки еще одна фантазия. А при всех её обсуждениях почему-то все время ускользает, что у всех подобных историй существует еще и абсолютно достоверная, реальная и многогранная основа. О которой очень мало кто знает, а потому и тема данная практически не затрагивается. А можно сказать и наоборот: особую тему отчего-то не обсуждают, поэтому и никто о ней по сути не наслышан…

Как бы там ни было, здесь определенно имеет смысл сосредоточиться именно на этой – реальной и малоизвестной – предыстории. (А всем, кто интересуется фантазиями ученых-соучастников в производстве Arrival, можно порекомендовать обширную запись в личном **блоге Стивена Вольфрама**, и интервью с профессором-лингвистом Джессикой Кун **в журнале Popular Science**.)

Что было до

Эту часть рассказа логично начать с 1952 года. Во-первых, потому что именно тогда известный британский ученый, профессиональный зоолог-генетик и статистик-математик (а также еще и лингвист-любитель) по имени Ланселот Хогбен сделал весьма необычный доклад перед Британским Межпланетным Обществом (**BIS**). Успешно существующее и поныне, общество BIS является, вероятно, старейшей на Земле организацией ученых, инженеров и прочих энтузиастов, которые еще с начала 1930-х годов всерьез поставили перед собой задачи по подготовке человечества к космическим и межпланетным экспедициям. Одним из председателей BIS, кстати, в свое время был писатель Артур Кларк.

Ну а доклад Хогбена от 1952 года, в переводе на русский озаглавленный как «Астра-Глосса, первые шаги в синтаксисе космического общения», впервые выдвинул продуманный комплекс идей относительно принципов нашего общения с инопланетным разумом. Прежде всего, Хогбен отметил, что Число – это наиболее универсальная концепция для установления коммуникаций между разумными существами. А потому именно математика должна быть базисом для первых шагов человечества в межзвездном общении.

После чего ученый проиллюстрировал, каким образом можно было бы передавать радиоимпульсы, представляющие целые и простые числа, а также прочие сигналы или «радиоглифы», представляющие концепции сложения, вычитания, равенства и так далее… Несмотря на новизну и оригинальность замысла с языком Astraglossa, сколь-нибудь заметной поддержки идеи Хогбена, правда, у коллег тогда не получили.

Но определенно интересно, что в том же 1952 году (это важнейшее «во-вторых») в США имело место другое, куда более существенное и чрезвычайно засекреченное событие, некоторым нетривиальным образом также связанное с темой коммуникаций между человечеством и внеземным разумом. Информация на данный счет по сию пору звучит очень глухо и как бы в ореоле «сомнительной недостоверности». Однако на

данный счет действительно имеются абсолютно серьезные свидетельства и достоверные документы, которые здесь хотя бы совсем вкратце полезно рассмотреть.

Речь, конечно же, идет о странных фактах вокруг рождения осенью 1952 года весьма особенной спецслужбы под названием NSA или Агентство Национальной Безопасности США. Впервые о подробностях этого всячески и очень долго скрывавшегося эпизода в своей знаменитой ныне книге-расследовании «Дворец загадок» в начале 1980-х годов написал Джеймс Бэмфорд. Книга начинается с того, как 4 ноября 1952 – в день выборов нового президента США – министр обороны Р. Ловетт подписал особую директиву о создании новой суперсекретной разведслужбы. И здесь же автор подчеркивает самое интересное – то, что послужило причиной директивы одиннадцатью днями ранее:

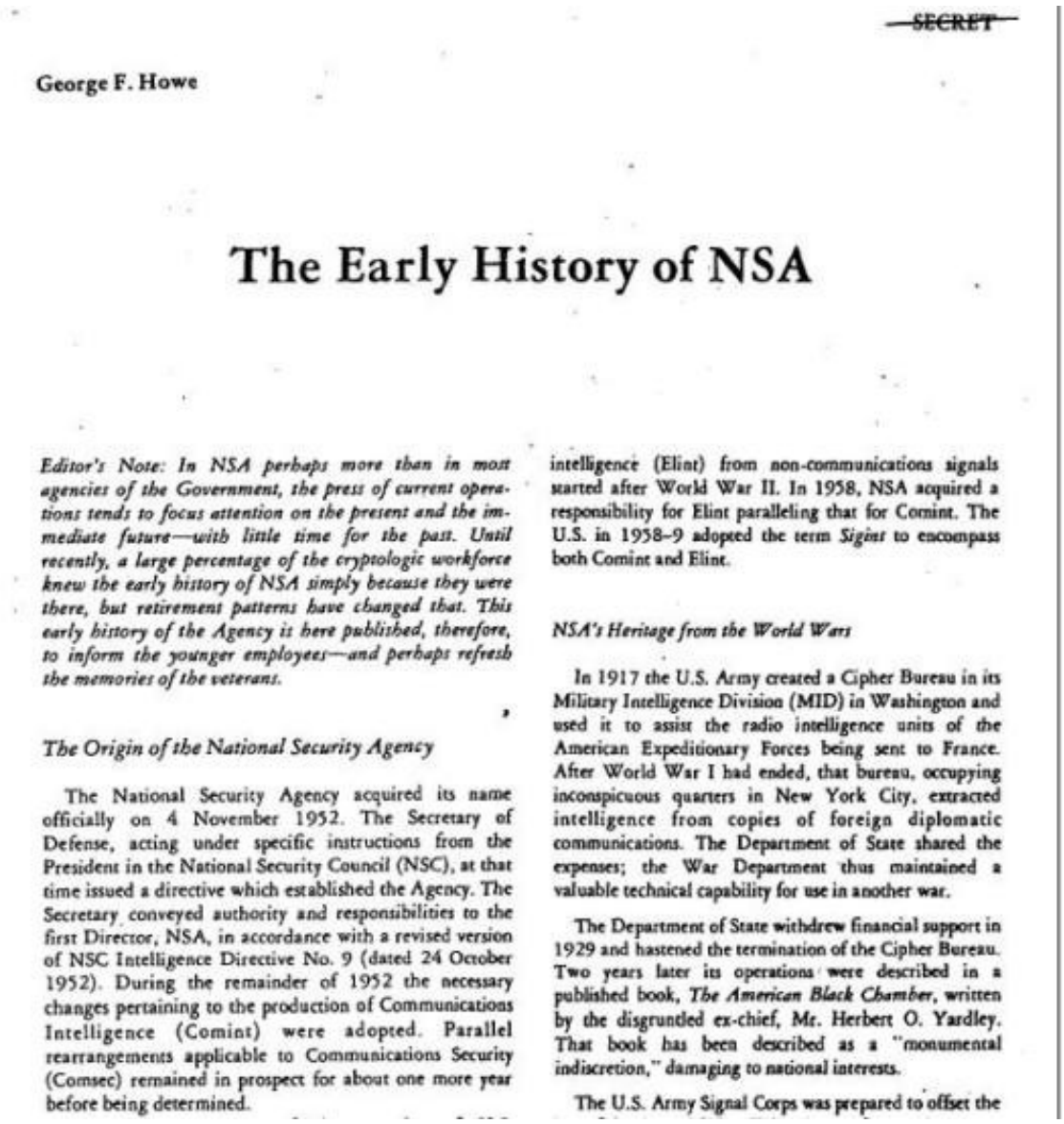
24 октября 1952 президент США Гарри Трумэн поставил свою подпись внизу семистраничного президентского меморандума, адресованного госсекретарю Дину Ачесону и министру обороны Роберту Ловетту. Получивший гриф Top Secret и проштампованный кодовым словом, которое само по себе было секретным, этот документ предписывал учредить агентство, которое станет известно как АНБ. Документ стал свидетельством о рождении новейшего и наиболее секретного агентства США, секретного настолько, что фактически всего нескольким людям в правительстве было разрешено знать о его существовании.

… 29 декабря 1952 – как одно из самых последних своих действий в качестве Президента – Трумэн тихо завизировал своей подписью одобрения документ NSCID No.9, новую версию Разведывательной директивы Совета нацбезопасности, переписанную в соответствии с рекомендациями о создании АНБ. Если меморандум Трумэна был свидетельством о рождении АНБ, то новая версия NSCID стала его официальным крещением.

Тридцать лет спустя меморандум господина Трумэна все еще остается одним из наиболее строго охраняемых секретов Вашингтона…

Далее из книги Бэмфорда можно узнать, что в 1970-е годы, когда факт существования АНБ уже не был тайной, доступ к этому важному документу очень долго не удавалось получить ни общественности через суд, ни по запросам комиссии Конгресса, курирующей деятельность разведки. Ну а еще четверть века спустя после выхода книги, уже в середине 2000-х годов, из собственных документов АНБ стало известно, что даже сам факт существования таинственного меморандума Трумэна долго скрывался и от самих сотрудников агентства.

Произошло это благодаря рассекречиванию статьи «Ранняя история АНБ», написанной в 1974 году официальным историком агентства Джорджем Хоу для одного из секретных внутренних сборников (*George F. Howe, “The Early History of NSA,”* Cryptologic Spectrum, Vol. 4, No. 2, Spring 1974).



~~SECRET~~

George F. Howe

The Early History of NSA

Editor's Note: In NSA perhaps more than in most agencies of the Government, the press of current operations tends to focus attention on the present and the immediate future—with little time for the past. Until recently, a large percentage of the cryptologic workforce knew the early history of NSA simply because they were there, but retirement patterns have changed that. This early history of the Agency is here published, therefore, to inform the younger employees—and perhaps refresh the memories of the veterans.

The Origin of the National Security Agency

The National Security Agency acquired its name officially on 4 November 1952. The Secretary of Defense, acting under specific instructions from the President in the National Security Council (NSC), at that time issued a directive which established the Agency. The Secretary conveyed authority and responsibilities to the first Director, NSA, in accordance with a revised version of NSC Intelligence Directive No. 9 (dated 24 October 1952). During the remainder of 1952 the necessary changes pertaining to the production of Communications Intelligence (Comint) were adopted. Parallel rearrangements applicable to Communications Security (Comsec) remained in prospect for about one more year before being determined.

intelligence (Elint) from non-communications signals started after World War II. In 1958, NSA acquired a responsibility for Elint paralleling that for Comint. The U.S. in 1958–9 adopted the term *Sigint* to encompass both Comint and Elint.

NSA's Heritage from the World Wars

In 1917 the U.S. Army created a Cipher Bureau in its Military Intelligence Division (MID) in Washington and used it to assist the radio intelligence units of the American Expeditionary Forces being sent to France. After World War I had ended, that bureau, occupying inconspicuous quarters in New York City, extracted intelligence from copies of foreign diplomatic communications. The Department of State shared the expenses; the War Department thus maintained a valuable technical capability for use in another war.

The Department of State withdrew financial support in 1929 and hastened the termination of the Cipher Bureau. Two years later its operations were described in a published book, *The American Black Chamber*, written by the disgruntled ex-chief, Mr. Herbert O. Yardley. That book has been described as a "monumental indiscretion," damaging to national interests.

The U.S. Army Signal Corps was prepared to offset the

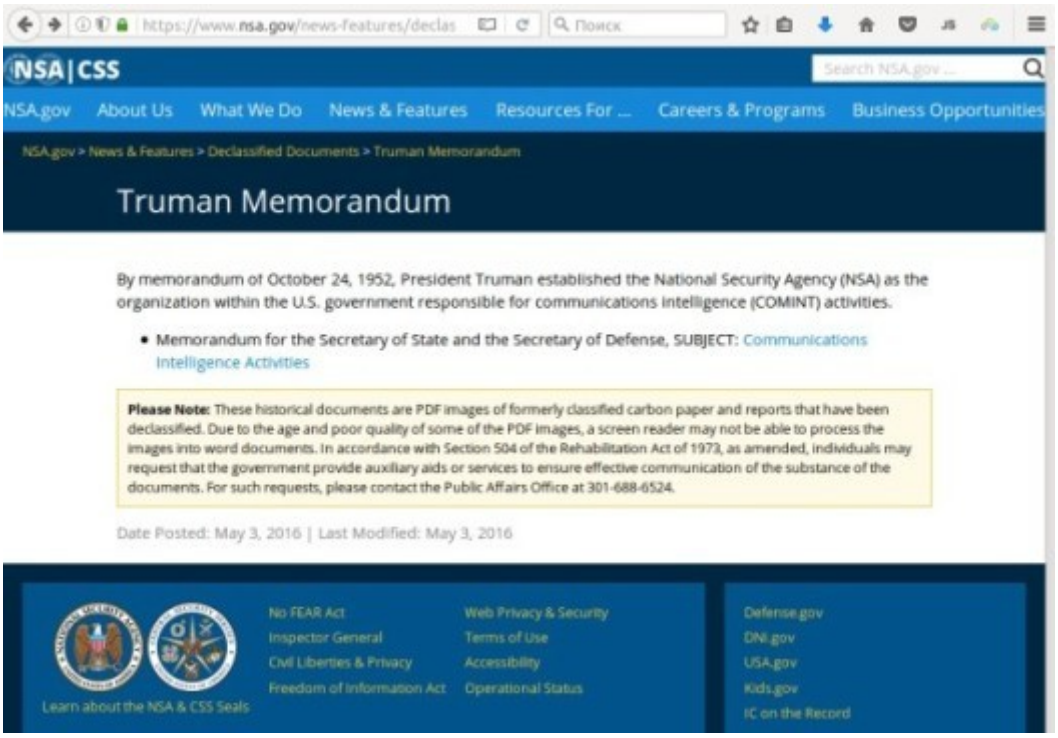
В этой статье о предпосылках и истории создания АНБ конкретно про момент учреждения рассказано так:

> *«Агентство национальной безопасности официально обрело своё название 4 ноября 1952 года. Министр обороны, действуя в соответствии с особыми инструкциями от Президента страны в рамках Совета национальной безопасности (NSC) в этот день издал директиву, согласно которой и было создано Агентство. Министр возложил соответствующие полномочия и ответственность на первого Директора АНБ в соответствии с дополненной версией Разведывательной директивы NSCID No. 9, датируемой 24 октября 1952 года…»*

Следует особо подчеркнуть, что автором статьи является официальный историк АНБ, а заведомая неправда – об ошибочной датировке NSCID No. 9, скрывающей факт существования меморандума – повторена для закрепления еще и в самом конце той же

публикации: «*Президент и Совет национальной безопасности 24 октября 1952 года издали пересмотренную версию NSCID No. 9*»…

И дабы стало ясно, наконец, с какого боку вся эта бюрократическая возня с разными директивами и их датами имеет хоть какое-то отношение к общению с инопланетным разумом, надо напомнить один исторический нюанс. Создание мощной, централизованной и суперсекретной спецслужбы, объединившей все прежде разрозненные военные подразделения, занимавшиеся вскрытием шифров, происходило через пять лет после известной истории с аварией НЛО под Розуэллом, штат Нью-Мексико. Согласно известным фактам, включая свидетельства военных, на месте падения среди останков НЛО были обнаружены и предметы, покрытые знаками письменности… Ну а согласно другим – еще более глухим – свидетельствам, в меморандуме Трумэна от 24.10.52 среди задач АНБ некоторым образом была упомянута и деятельность по дешифрованию материалов внеземного происхождения…



Подтвердить документально, впрочем, эти свидетельства пока что нет никакой возможности. Прежде всего по той причине, что когда в 1990-е годы – из-за развала СССР и резко изменившегося политического климата – АНБ все же пришлось отреагировать на требования о рассекречивании меморандума Трумэна, то взорам изумленной публики предстало нечто в высшей степени невыразительное (см. **сайт АНБ**). То есть предъявлен действительно и бесспорно документ «в тему», но практически слово в слово повторяющий уже рассекреченную ранее директиву NSCID No. 9 – причем на тех же восьми (а не семи) страницах.

Однако, что нельзя не заметить, рассекретили для открытой публикации почему-то сканы не с оригиналов этих документов, а с их копий, не имеющих подписей прези-

дента Трумэна (*пара копий одним файлом*). Ну а самое главное, наиболее «страшная гостайна», которую оба документа-близнеца в себе скрывали – это всего лишь функции АНБ по систематической разведке средств связи иностранных государств. Причем сформулированы эти вещи в самых общих выражениях и вообще без употребления слов типа дешифрование секретной переписки… Иначе говоря, причины не только активнейшей борьбы за засекречивание документа, но и попыток сокрытия даже самого факта его существования, так и остались для публики совершенно непонятными.

Но зато – вместе с процессом рассекречивания всяких старых сборников и журналов из тайной внутренней жизни АНБ – стало вполне очевидно, что в шпионской спецслужбе действительно интересовались проблемами коммуникаций с инопланетным разумом. Причем даже секрета большого из этого не делалось – особенно в первоначальный период истории.

Так, в частности, в 2008 году на сайте агентства появилась подборка рассекреченных статей из внутреннего сборника спецслужбы под названием **NSA Technical Journal**, то есть «Технический журнал АНБ». И среди множества разнообразных публикаций этого издания, посвященных проблемам криптографии, перехвата и анализа сигналов, для нашей истории особо интересны с полдюжины материалов такого рода:

– Выпуск 1958 года: «*Сигналы из внешнего космоса*» (Signals from Outer Space — April 1958 — Vol. III, No. 2);
– Выпуск 1962 года: «*Lincos: Конструкция языка для космического общения*» (Book Review: Lincos, Design of a Language for Cosmic Intercourse, Part 1 — Winter 1962 — Vol. VII, No. 1);
– Выпуск 1966 года: «*Коммуникации с внеземным разумом*» (Communications with Extraterrestrial Intelligence — Winter 1966 — Vol. XI, No. 1). Плюс еще несколько более

поздних статей подобного рода, переводящих обсуждение в подчеркнуто шутливый тон и по сути закрывающих тему к концу 1960-х годов.

В приведенном списке статья от 1966 года представляет наибольший интерес. Ибо автор ее, греческого происхождения математик и музыкант Ламброс Калимахос (Lambros D. Callimahos), в свое время был известен как один из ведущих криптологов АНБ. Ну а текст статьи – это на самом деле выступление Калимахоса на некоем весьма любопытном мероприятии. О котором в начале публикации рассказано в таких словах, цитируя дословно:

> *Содержимое данной статьи было доложено на групповом обсуждении в рамках секции под тем же названием «Коммуникации с инопланетным разумом» на Конференции IEEE по военной электронике, проходившей в Вашингтоне в сентябре 1965 года. Помимо автора, как профессионального криптолога, другими докладчиками и участниками обсуждения были лингвист д-р Пол Гарвин (Paul Garvin), дельфинолог Джон Лилли (John Lilly), физик Уильям Дэвис (William O. Davis), астроном Фрэнсис Хейден (Francis J. Heyden). Модератором дискуссии был д-р Хэролд Вустер (Harold Wooster), директор информационных служб в Управлении научных исследований Военно-воздушных сил США…*

Начинается же выступление большого криптолога из АНБ такими словами:

> *Мы не одиноки во вселенной. Некоторое время назад идея эта представлялась надуманной; сегодня же существование внеземного разума большинством ученых воспринимается как доказанная данность…*

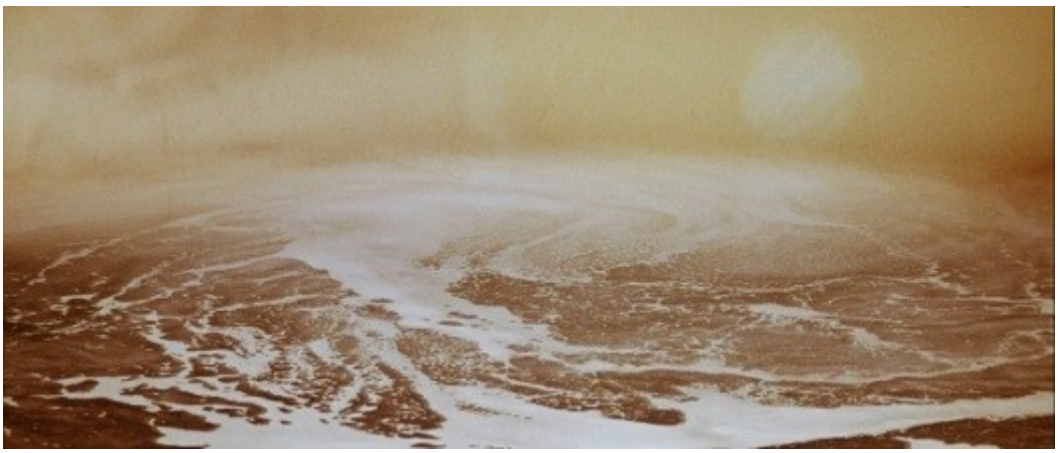
Никакого раскрытия больших государственных тайн на данный счет, конечно же, далее докладчик не делает. Однако сам факт абсолютно серьезного обсуждения данной темы при столь интересном составе участников вполне примечателен уже и сам по себе.

Что будет после

Сворачивание «просто секретных» интересов АНБ к общению с инопланетным разумом в конце 1960-х годов по времени совпало с закрытием аналогичного полусекретного проекта «Голубая книга» в ВВС США, занимавшегося сбором и изучением свидетельств о НЛО. Официально принято считать, что на этом интерес властей к «аномальщине» как бы закончился, однако есть масса свидетельств тому, что на самом деле все подобные работы просто перевели в значительно более глубокие недра гостайны.

История, однако, развернулась здесь так, что специфической «обратной реакцией» на это подавление информации стало появление все большего и большего интереса публики к контактам с инопланетянами. Что в первую очередь, конечно же, проявилось в фантастической литературе и кино. (Шедевр Кубрика «2001: Космическая одиссея», сделанный по сценарию Артура Кларка и «показавший всем, как надо делать кино про космос», вышел в 1968, можно напомнить.)

Вряд ли хоть кто-то будет возражать, что особо талантливые писатели-фантасты – вроде Жюля Верна или Герберта Уэллса, Артура Кларка или Станислава Лема – для современников выступают как своего рода маги-визионеры, своим внутренним взором умея заглядывать в будущие варианты развития человечества. Общеизвестно, что чуть ли не все из разнообразных технологических чудес, окружающих нас ныне, за много лет и десятилетий до их реального появления были предсказаны в произведениях фантастов.



Как правило, мы очень мало что знаем о работе «внутренней кухни» вот этой магии визионеров – как именно в голову к людям приходят интереснейшие идеи, сюжеты и концепции. Но иногда кое-что действительно любопытное раскопать все же можно. В частности, есть весьма неординарные факты об истории появления «Солярис», наиболее знаменитого романа Станислава Лема, рассказанные самим писателем в своих мемуарах.

Подробности этой истории можно найти в биографической книге Лема «Моя жизнь», а также в сборнике многочисленных интервью с писателем «Так говорил… Лем», выходившем в России в 2002 году (глава «В паутине»). Здесь же достаточно изложить лишь собственно суть.

Вспоминая молодость и вступление в мир литературы, Лем признался, что испытывает чувство стыда за свои первые две книги, неуклюже сконструированные из картонных героев, шаблонных сюжетов и идеологических штампов. Но зато потом у него вдруг начался период подлинного яркого творчества – как серия романов, начиная с «Солярис» и «Возвращение со звезд». Во всех книгах этого ряда, рассказывает Лем, он оказался в роли своего рода зрителя, наблюдающего картины, которые неведомым образом возникают у него в голове, и записывающего все происходящее, абсолютно не ведая, чем история закончится…

Подобного рода необычный опыт творчества, конечно же, характерен не только для писателей-фантастов. Если покопаться в мемуарах, то нечто весьма похожее по духу можно найти и у реалистов. А также и у литераторов-мистиков, конечно же. Которые – в отличие от твердого материалиста Лема – абсолютно уверены, что этим красивым способом они просто получают послания из других слоев реальности или от своего высшего уровня бессмертного сознания.

Именно к этой категории определенно относится творчество знаменитого писателя-мистика по имени Ричард Бах. Который в молодости – в начале 1960-х – служил летчиком-истребителем ВВС США, демобилизовался, к счастью (не успев никого поубивать), до начала войны во Вьетнаме, а в литературу затем вошел с удивительной и сразу прославившей его книгой «Чайка Джонатан Ливингстон». История же создания «Чайки», что невозможно не заметить, практически один-в-один, вплоть до существенных нюансов, совпадает с историей написания «Солярис». С тем лишь отличием, что Бах в отличие от Лема абсолютно уверен, что не сам придумал этот престранный сюжет, а получил его для записи и распространения от кого-то еще – в виде своего рода «кинопроекции» в сознание…

Мистику Баху такое признание делать намного проще и естественнее, поскольку он регулярно практикует медитацию. А для людей, занимающихся подобного рода изменениями состояния сознания, общение с иными формами разума, как известно, дело вполне обычное. В прежние эпохи такого рода нечеловеческие формы разума воспринимались в соответствии с традицией – как некие ангельские или демонические существа, как правило. Ну а с некоторых пор – с рубежа 1960-70-х годов примерно – очень

часто бывает так, что при телепатических контактах с «той стороной» незримые собеседники представляются как инопланетяне…

И вот именно на этом любопытном моменте, собственно, и настала пора зафиксировать фокус всей истории о контактах человечества с внеземным разумом. Ибо соль и перец данного сюжета заключаются в том, что ныне – и очень-очень постепенно – до человечества начинает доходить реальная ситуация с присутствием инопланетного разума на Земле. Представители которого всегда тут были, есть и будут. И более того, всегда готовы охотно с нами пообщаться, если мы того хотим. Ибо абсолютно никаких языковых препятствий для нашего общения на самом деле не существует. Ну а кроме того, наконец, очень многие из представителей человечества в своих прошлых жизнях и сами когда-то были инопланетянами.

Понятно, что для очень многих здраво- и рационально мыслящих людей подобные идеи звучат в высшей степени странно, почти как бред. Поэтому для начала и постепенного вхождения в тему многим будет очень полезно ознакомиться с **рассказом Ричарда Баха** (который и сам заинтересовался темой инопланетян совсем недавно) – о том, при каких обстоятельствах ему лично довелось встретиться с нашей галактической семьей.

Эта история «первого контакта», можно уточнить, произошла с писателем весной 2015 года – за несколько месяцев до начала съемок кинофильма «Прибытие». Поэтому особо интересно отметить, что первые же вопросы, которые Бах начал задавать инопланетянам, встретившись с ними непосредственно, звучали точно так же – как в кино:

«Зачем вы все здесь, на нашей планете? Чего вы от нас хотите?»

Братья и сестры по разуму довольно легко и быстро разъяснили писателю, в чем цель наших контактов. Бах, как смог, пересказал их ответ для всех своих читателей. Так что теперь остается лишь дождаться, когда эту совсем нехитрую, в общем-то, идею постигнут в большинстве своем и все остальные люди Земли.

Эпилог как пролог

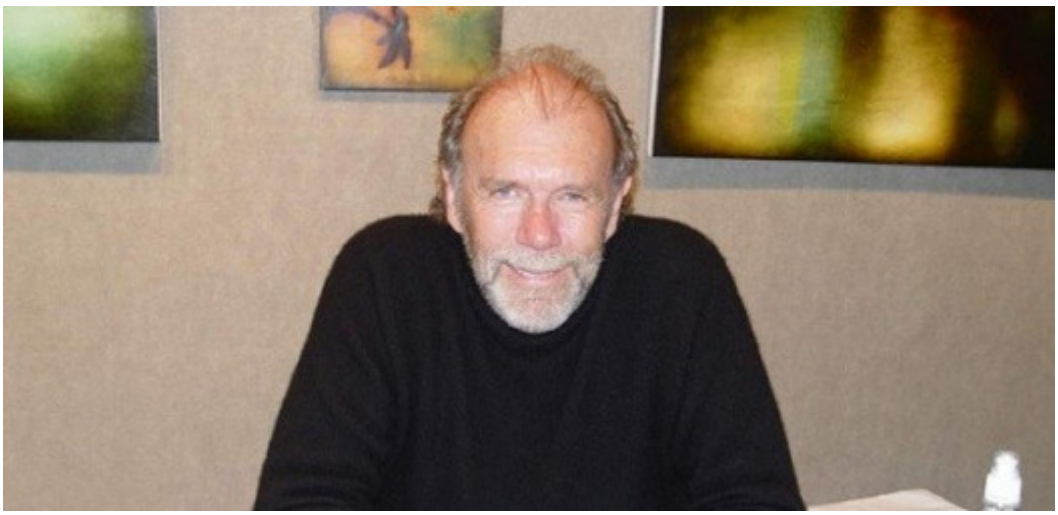
Когда при обсуждении только что вышедшего на экраны фильма «Прибытие» у автора сценария Эрика Хайссерера спросили о том, а хотел бы он сам иметь такого же рода знание, которое обрела его героиня Луиза в результате общения с пришельцами-гептаподами, сценарист ответил так:

> *«Я думаю, что более великая перспектива видения этого мира меня бы только обогатила. Лучшее понимание природы времени определенно нас обогатит. Но не думаю, что это с необходимостью означает, будто надо тут же менять свою собственную жизнь. Так что я отношусь к той же категории, что и Луиза. Конечно, я сожалею о каких-то прошлых своих поступках, но я знаю, что эти сожаления помогли формированию моей зрелости, помогли мне стать более лучшим человеком. Хотя в прошлом я может и вел себя порой как засранец, для меня важнее, что таким образом мы способны расти»…*

Для всех, кому подобный ответ покажется несколько замысловатым, для постижения его сути и глубины полезно напомнить другой ответ примерно в ту же тему.

Примерно лет за пять до того, как в Канаде начали снимать фильм Arrival, одна из центральных российских газет сумела взять интервью у Ричарда Баха. Который обычно избегает газетчиков, но в данном случае дал понять, что «ждал звонка от русских журналистов». Интервью довольно большое, полный текст его можно найти в онлайн-библиотеке Мошкова, на странице «**Р.Бах**», ну а для нашей истории особо интересен самый финал беседы.

> *– Назовите три самые красивые вещи на свете?*
> *– Самые красивые? Понимание того, что мы намного больше, чем нам кажется. Что мы обладаем силой, которая выходит за пределы нашего понимания. Что мир вокруг нас – всего лишь школа, в которую мы ходим, место, где мы можем опробовать свои навыки стать более хорошими людьми. Вот это мне нравится даже больше, чем летать!*



# # #

Дополнительное чтение в тему:

О том, как ситуация с инопланетным присутствием на Земле выглядит при взгляде с другой стороны: «**Знают все – кроме нас…**»

Рассказ известного писателя и летчика о личной встрече с инопланетянами: «**Птица по имени Ричард Бах**». Станислав Лем о мистике его первых настоящих романов: «**Новые горизонты**»

О недетских играх спецслужб и военных вокруг контактов с инопланетянами: «**НЛО: история болезни**», «**Правда и вымысел**»

Секреты волшебства и их сокрытие

Выпиливание реальности

(*Август 2016*)

Какая связь может быть между игрой Pokemon Go, изощренными шпионскими закладками для компьютеров, дебатами об авторе шекспировских произведений и природой нашего сознания? Связь тут прямая, хотя и странная…

Плюс Покемоны – минус что?

В течение одной недели лета 2016 – со среды 6 июля по среду 13-го – в разных странах мира имели место три абсолютно, казалось бы, независимых друг от друга события. Но вот если их сопоставить и рассмотреть во взаимном наложении, то проявляется весьма интересная картина той реальности, в которой всем нам доводится жить.

Такой реальности, в которую искусственно встраиваются всякие пустяки или «сенсации», почти целиком отвлекающие наше внимание. И одновременно методично изымаются или «выпиливаются», как принято с некоторых пор выражаться, действительно важные вещи, способные в корне изменять мировоззрение людей и их восприятие происходящего.

День 6 июля, о чем многие наверняка в курсе, ознаменовался выводом на рынок *Pokemon Go*, новой сенсационной игрушки для смартфонов, мгновенно ставшей гипер-успехом жанра и породившей массовое помешательство у народов мира. Главная фишка игры – «расширение реальности» путем встраивания в окружающую обстановку мультяшных персонажей-покемонов. Которых надо находить-отлавливать-тренировать, а затем в публичных местах выставлять их для сражений с покемонами всех прочих участников развлечения.

В итоге же все приобщившиеся безмерно счастливы – появилась новая крутая забава, мощно отвлекающая от проблем реальной жизни и вообще отключающая мозги от чего бы то ни было. Кроме покемонов.

Ближе к выходным той же недели вышел очередной, за период 9-15 июля, номер британского еженедельника New Scientist, в популярной форме рассказывающего о достижениях и новостях науки. Конкретно же в данном выпуске особый интерес представляет большая – на двухстраничный разворот – и довольно загадочная самореклама издания. Текст послания переводится примерно так: «В среднем внимание человека задерживается на 8 секунд. Фокусируйтесь дольше. Живите умнее». Сопровождает этот призыв загадочная картинка-шарада: емкость аквариума в форме прозрачной человеческой головы, внутри которой плавает и пускает пузыри золотая рыбка…

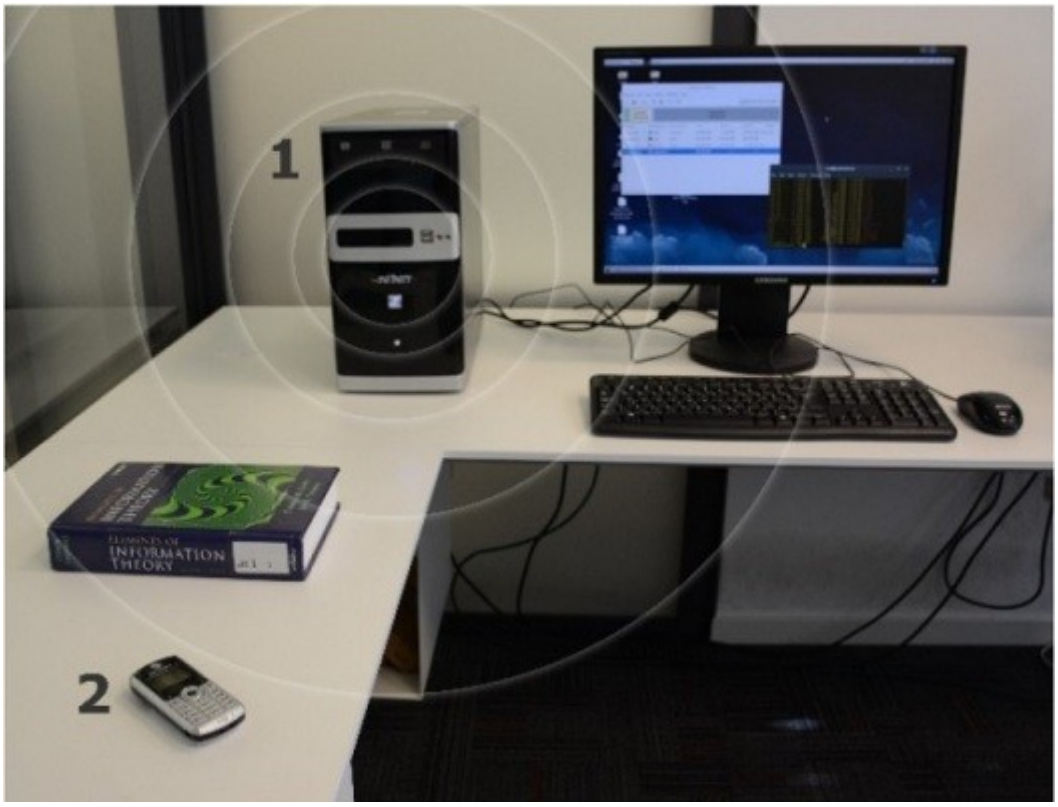
Разбор символов данной картинки увел бы рассказ сильно в сторону (интересующихся можно отослать к материалу «**Рекламная пауза**»), поэтому здесь имеет смысл сосредоточиться на собственно призыве – «более сфокусировано удерживать внимание». И перейти к третьему событию. Где повышенное внимание определенно необходимо.

В среду 13 июля на сайте научных препринтов Arxiv.org появилась новая статья от группы израильских ученых-хакеров, занимающихся исследованиями компьютерной безопасности в Университете Бен-Гуриона. Работа посвящена весьма модной ныне теме побочных компрометирующих излучений и носит название «***VisiSploit**: Оптический канал для скрытной передачи данных*» (*«VisiSploit: An Optical Covert-Channel» by Mordechai Guri, Ofer Hasson, Gabi Kedma, Yuval Elovici.* ArXiv:1607.03946).

Следует подчеркнуть, что это уже далеко не первое исследование от команды ученых, которую в чуть разных составах стабильно возглавляет Мордехай Гури. И которая за

последние три года выдала целый букет любопытных открытий – о том, сколь много разнообразных способов имеется для похищения информации из компьютеров, работающих отдельно от сети.

Первая статья этого ряда носила название *«**AirHopper**: Устройство радиочастотного моста через воздушный зазор между изолированными сетями и мобильными телефонами»*, arXiv:1411.0237, 2014. Затем, в 2015 последовала работа *«**BitWhisper**: Скрытный канал передачи на основе температурных модуляций для связи между компьютерами через воздушный зазор»*, arXiv:1503.07919, 2015. А совсем недавно, в июне 2016, опубликована созвучная работа о скрытной связи с помощью вентиляторов охлаждения: *«**Fansmitter**: Акустическая эксфильтрация данных через воздушный зазор из компьютеров, не имеющих громкоговорителей»*, arXiv:1606.05915, 2016.



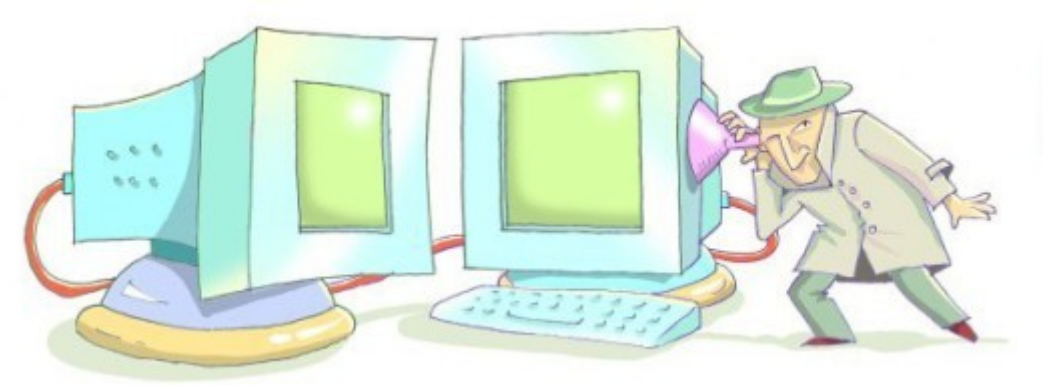
Короче говоря, в том комплексе исследовательских статей, что Мордехай Гури и его коллеги выложили на сайте Arxiv.org, можно найти очень много чего интересного о шпионском извлечении секретной информации из компьютеров, которые в целях безопасности работают без подключения к внешним сетям. Однако самое интересное здесь то, о чем во всех данных статьях не говорится. Хотя очевидно должно бы. Ну а чтобы важные умолчания выявить, надо читать материалы действительно с повышенным вниманием.

Минус GSMem, или выпиливание методов доступа

Область компрометирующих побочных излучений от аппаратуры, обрабатывающей информацию (или тема TEMPEST, как еще её называют с подачи американских спецслужб), активно исследуется и разрабатывается специалистами уже свыше 70 лет (см.

обзор «Секреты дальночувствия»). Но при этом все новые и новые неожиданные открытия делаются там регулярно и по сию пору.

Одной из самых впечатляющих работ подобного рода за последние годы, несомненно, стала публикация метода «Акустический криптоанализ», разработанного совсем другим коллективом также израильских ученых-криптографов. Которые в 2013 году продемонстрировали, что просто по звукам работы электронных схем компьютера, шифрующего информацию, они могут полностью восстановить секретный криптоключ, используемый для шифрования (*«RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis», by Daniel Genkin, Adi Shamir, Eran Tromer. PDF*).

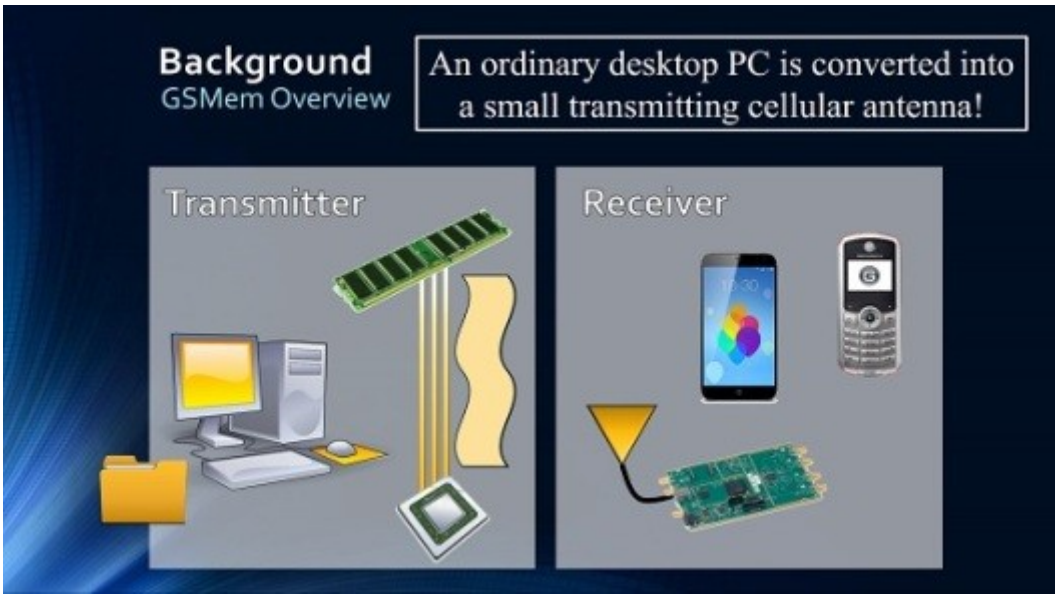


Особую пикантность тому открытию придавал факт присутствия среди авторов Ади Шамира, патриарха академической открытой криптографии и «буквы S» в названии знаменитого криптоалгоритма RSA, составленного из фамилий его изобретателей. Подробности о новой, в высшей степени неординарной работе Шамира и его коллег, а также о смежных с ней других открытиях исследователей, можно найти в материалах «Крипто-акустика» и «Экстрасенсы от криптографии». Здесь же она вспоминается вот по какой причине.

Поскольку созвучная серия исследований и публикаций Мордехая Гури и его команды началась в 2014, нет никаких сомнений, что эти ученые прекрасно знают о работе Генкина, Шамира и Тромера, сразу же получившей мощный резонанс в криптографическом сообществе. Но при этом, что не может не удивлять внимательного читателя, ни в одной из статей Гури и компании нет ни единого упоминания о достижениях их же израильских коллег. Хотя каждая из статей сопровождается краткой предысторией и длинной библиографией со ссылками на существенные результаты предшественников.

Но это, впрочем, далеко не самое странное. Куда интереснее тот факт, что в публикациях команды Гури имеется целый комплекс свидетельств, указывающих на то, что попутно заметаются следы и их собственной примечательной работы. Эти результаты были доложены летом прошлого года на USENIX Security ’15, респектабельной конференции по инфобезопасности в Вашингтоне, и сразу были оформлены авторами в виде статьи под названием «***GSMem**: Извлечение данных через канал GSM-частот из компьютеров, отделенных воздушным зазором*».

Вот только в общедоступный архив препринтов Arxiv.org работа о GSMem, в отличие от всех прочих, почему-то не попала. Найти и скачать статью в интернете не так сложно, в принципе, если искать конкретно ее или знать, на какой конференции работу докладывали. Но авторы по каким-то темным причинам детали скрывают, а в собственной библиографии ссылаются на статью в таком вот обрезанном виде: *A. K. O. H. G. K. Y. M. Y. E. Mordechai Guri, «GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies,» Washington, D.C., 2015* (имена и фамилии пяти соавторов Гури указаны только инициалами, название мероприятия опущено полностью, интернет-ссылки нет, естественно).



Дабы стало понятнее, почему все эти нюансы важны, надо хотя бы в нескольких словах пояснить, в чем заключается суть шпионского метода GSMem, описанного в работе. Специальная программа-закладка, внедренная в компьютер, похищает криптоключи и пароли доступа, а затем передает их электромагнитными сигналами на частотах GSM-связи, особым образом модулируя работу каналов в шине мультиканальной памяти. Делается этот трюк с помощью специфических внутренних команд ЦПУ, управляющих функциями памяти компьютера. Передаваемые таким образом сигналы могут быть приняты и демодулированы находящимся неподалеку сотовым телефоном даже самой примитивной конструкции, либо – уже на расстояниях в десятки метров – особым радиоприемником спецслужб.

Поскольку из всех методов «эксфильтрации данных», открытых и описанных командой Гури, лишь GSMem был удостоен столь специфического обращения, несложно понять, кто и по какой причине старательно прячет информацию о сути данной разработки. Вовсе не секрет, что спецслужбы США, Израиля и прочих технически продвинутых государств на много лет или даже десятилетий опережают открытые исследования во всех подобных делах. Ну а когда одни ненароком переоткрывают вещи, которые у других уже освоены и используются в реальной работе, то приходится принимать меры…

Минус Картье, или выпиливание генерала

Одной из важнейших особенностей технологий TEMPEST является то, что нужные для шпионов сигналы содержательной информации выдаются в естественных излучениях источника: радиочастотных, акустических, тепловых, оптических и так далее. А искусство шпиона заключается в том, чтобы такие утечки информации эффективно выделять из общего шума. Либо – при активном воздействии – умело и незаметно встраивать в обычные сигналы еще и особую информацию, модулируя «общий шум» битами скрытого сообщения.

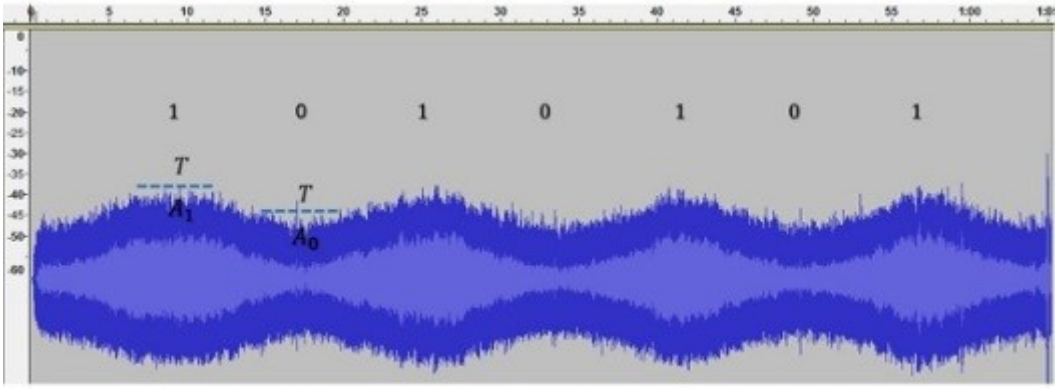


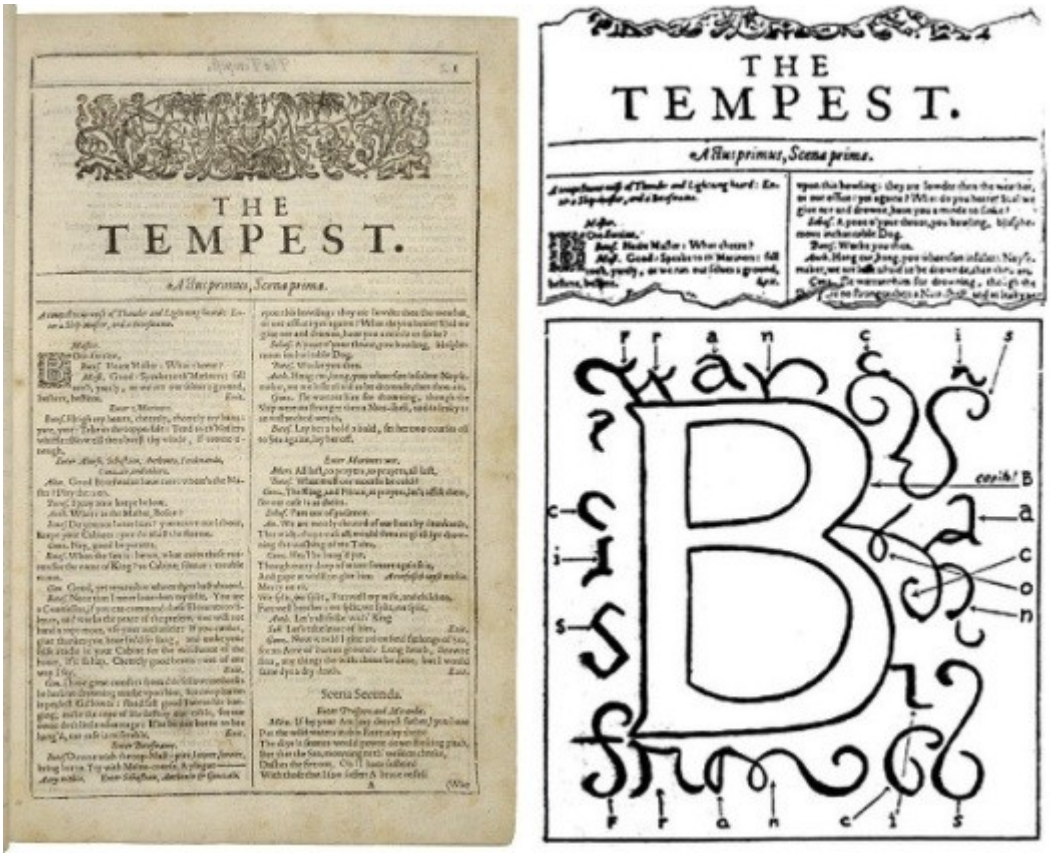
Figure 5. ASK modulation of "101010" over 60 seconds, when R_0=3000 RPM and R_1=3500 RPM

Именно так, в частности, работают и в большинстве своем Tempest-методы израильских криптографов из команды Гури. Где биты похищаемых криптоключей могут модулировать скорость работы вентилятора охлаждения (Fansmitter). Либо, наоборот, степень теплового излучения компонентов (Bitwhisper). Либо, как в методе GSMem, информация выводится через манипуляции количеством одновременно подключаемых каналов в шине памяти.

Кто и когда первым изобрел подобные шпионские хитрости, достоверно историкам неизвестно. Более того, нет и никаких документальных свидетельств относительно того, с какой стати в АНБ США для подобного рода технологий выбрали кодовое слово TEMPEST. Но при этом имеется комплекс абсолютно надежных фактов, которые за очевидностью никто по отдельности не отрицает, но и никогда не сопоставляет друг с другом в совокупности. Хотя явно следовало бы.

Факт первый – о принципе кодирования. Имеются бесспорные свидетельства тому, что именно такой принцип – двоичного модулирования сигнала – для скрытной передачи данных было подробно описан Фрэнсисом Бэконом четыре столетия тому назад. В начале XVII века, а точнее в 1623 году, этот знаменитый английский философ, ученый и политик эпохи Возрождения в одной из своих работ рассказал об изобретенном им методе тайнописи, получившем название «двухлитерный шифр». Суть метода заключается, как это назвали бы сейчас, в «двоичном модулировании» обычного – маскирующего – текста через применение в послании букв с шрифтами двух разных видов.

Факт второй – о появлении термина. Знаменитый современник Бэкона по имени Вильям Шекспир умер в 1616 году. Фрэнсис Бэкон умер десятью годами позже, в 1626. А в промежутке между этим датами, в 1623 (отметим год), был издан так называемый «первый фолио» – большой сборник пьес Шекспира, с которого началась литературная слава гения. Открывает же этот том пьеса «Буря» или TEMPEST на языке оригинала – хронологически одно из самых последних произведений автора, в печатном виде появившееся здесь впервые, что интересно.


THE
TEMPEST.

Actus primus, Scena prima.

THE
TEMPEST.

Actus primus, Scena prima.

Scena Secunda.

Ну а самое интересное, что пьеса эта начинается со слов капитана корабля, обращающегося к боцману (Botswain), причем первая буква его обращении (B) выделена в этом издании большущей буквицей, в виньетках которой внимательные люди усмотрели многократно повторяющееся имя Bacon Francis. Найдено это имя там не случайно, конечно же, а по причине очень давно ведущихся споров о Бэконе как подлинном авторе шекспировских произведений. Причем именно в первом фолио исследователи обнаруживают особенно много тому подтверждений, включая и тайные послания, зашифрованные двухлитерным шифром Бэкона. (Подробности на данный счет можно найти в материале «Если дело дойдет до суда».)

Нас же здесь куда больше интересует «Факт третий» – о прямых и бесспорных взаимосвязях между шифром Бэкона и АНБ США. Ибо в 1957 году (когда даже само существование этой суперсекретной спецслужбы считалось большой государственной тайной) один из старейших и наиболее авторитетных криптографов АНБ, Уильям Фридман, написал и открыто опубликовал весьма специфическую книгу под названием «Проверка шекспировских шифров» (*«The Shakespeare Ciphers Examined« by*

William F. Friedman). Суть и цель данной работы – с позиций профессионала-криптографа всячески разоблачить и отвергнуть идею о том, будто бы в книгах XVII века есть двухлитерные шифрованные послания, документально доказывающие, что Бэкон является автором шекспировских произведений.

Книга Фридмана, спору нет, написана очень компетентно и убедительно. И выводам ее легко поверить, особенно для людей, мало сведущих в делах истории, криптографической науки и секретных спецслужб. Но вот для тех, кто кое-что в подобных вещах смыслит, данное произведение Фридмана выглядит в высшей степени подозрительно. И больше всего похоже на умышленное внедрение дезинформации. Сработанное, правда, весьма аккуратно…

Здесь, конечно же, совсем не место для тщательного разбора и разоблачения столь давнего «вброса». Однако на важнейшие моменты, необходимые для понимания проблемы, указать следует обязательно. Прежде всего, надо обратить внимание на время выхода не только собственно книги, 1957 год, но и на дату публикации ее первичного варианта – 1955. Иначе говоря, обе версии этой работы появились вскоре после 1953 – года смерти человека по имени Франсуа Картье. То есть весьма авторитетного французского генерала, до этого игравшего роль главного эксперта-криптографа в нескончаемых спорах исследователей вокруг загадок бэкон-шекспировских текстов.

Для того, чтобы стало понятнее, сколь неслучайна эта последовательность дат, следует отметить, что Фридмана и Картье связывало весьма давнее личное знакомство, еще со времен Первой мировой войны. Генерал Картье, правда, на протяжении всего того периода, с 1909 по 1921, возглавлял криптографическую службу французской армии, отвечая как за национальные шифры, так и за перехват–дешифрование секретной переписки неприятеля. А Уильям Фридман в 1918 году был молодым новоиспеченным лейтенантом, отвечавшим за криптоанализ в штабе генерала Першинга, командующего экспедиционными войсками США во Франции.

Несмотря на огромную разницу в возрасте и в воинских званиях, Картье с большим уважением относился к юному американскому криптографу и к его новаторским методам криптоанализа собственной разработки. После войны генерал лично обеспечил перевод и выпуск на французском языке нескольких основополагающих работ коллеги о математических методах криптоанализа, а попутно заинтересовался и бэкон-шекспировской историей. Потому что именно она, собственно, и была той исходной причиной, которая в 1915 году мощно и навсегда переключила интересы ученого-генетика Фридмана с области биологии на шифры и криптоанализ.

Последовавшее вскоре вступление США в мировую войну в 1917, правда, радикально перевело работу самородка-криптографа с вопросов литературы на дела армейские. Ну а генерал Картье, выйдя в отставку в 1920-годы, напротив, всерьез заинтересовался давней проблемой историков и литературоведов, раздобыл в библиотеках старинные книги и занялся их собственным криптоанализом. Результатом чего поначалу стала серия из пяти исследовательских статей, последовательно опубликованных в начале 1920-х годов, а затем и обобщившая их отдельная книга «Проблема криптографии и истории» (*François Cartier, Un problème de Cryptographie et d'histoire; Paris: Editions du Mercure de France, 1938*).

Во всех этих работах генерал Картье вполне однозначно – как опытный эксперт-криптограф – подтвердил не только факт присутствия двухлитерного шифра Бэкона в целом ряде известных печатных книг XVII века, но и то, что шифр этот можно и сегодня вскрывать-читать. Так что вплоть до середины 1950-х – пока не вышла книга-опровержение от Уильяма Фридмана – криптоанализ Картье был единственным свидетельством на данный счет от специалиста-профессионала. Причем, к ужасу армии шекспироведов, это было свидетельство в пользу Бэкона…

Ну а как только французский генерал Картье умер в возрасте 90 с лишним лет, тут же подоспевшая работа от «отца американской криптологии», полковника Фридмана, оперативно предоставила ученым куда более удобную криптографическую эксперти-

зу, вновь расставившую знаменитых людей по привычным для историков местам. Бэкону, как говорится, бэконово, а Шекспиру, соответственно, шекспирово.

Вот только попутно имя прославленного генерала Франсуа Картье стали незаметно, но методично из истории выпиливать. И если после окончания Первой мировой войны премьер-министр Франции Жорж Клемансо говорил о вкладе Картье словами «он один был для нашей страны полезнее, чем целый армейский корпус», то ныне об этом человеке в интернете нет практически никакой информации. Ни в многочисленных версиях Википедии на разных языках, ни во всем французском сегменте интернета, ни в англоязычном, ни в каком-либо еще.

Единственное, фактически, содержательное упоминание – всего несколько строк – есть лишь на сайте APPAT.org, французской Ассоциации развития военной связи, откуда, собственно, и позаимствована цитата из Клемансо. По этой причине сегодняшним читателям крайне сложно познакомиться с фактами и аргументами, доказывающими «нетрадиционную» позицию генерала Картье.

С опровержениями от полковника Фридмана ознакомиться значительно проще, поскольку книгу его при желании можно найти и скачать в Сети. Но вот какая интересная штука попутно при розысках выясняется.

Уильям Фридман, как известно, был страстным собирателем предметов и документов, так или иначе относящихся к истории криптографии. За долгую жизнь он накопил весьма внушительную коллекцию, которую в начале 1970-х – вскоре после смерти Фридмана – семья передала на хранение в Библиотеку фонда Маршалла в Вашингтоне. Ныне, однако, исследователи этого ценнейшего архива с горечью отмечают, что в коллекции явно недостает не только отдельных единиц хранения, но даже порой и каталожных карточек с информацией о том, что пропало. Причем виноваты в этом вовсе не беспечные хранители библиотеки, а начальники всесильного АНБ США.

Пользуясь малоизвестным законом о пересекречивании документов, Агентство неоднократно прореживало коллекцию Фридмана «для сохранения тайн о защите национальной безопасности». И что особо любопытно, среди изъятых и засекреченных единиц архива обнаруживаются одна из статей пятичастевого цикла работ Картье о проблеме Бэкона-Шекспира плюс еще три, как минимум, документа из этого же комплекса материалов. С какой именно стороны изначально открытые публикации о делах XVII века, написанные за 30 лет до создания АНБ, могли бы угрожать нацбезопасности и компрометировать работу суперсекретной американской спецслужбы – внятно объяснить вряд ли кто сумеет…

Однако на этом странности и выпиливания вокруг сюжета далеко не заканчиваются.

Минус криптография и левитация, или выпиливание сути

Во всей той большой, разветвленной и замысловатой истории, что накручена вокруг совместной биографии криптографа Фридмана и суперсекретной спецслужбы АНБ США, тема Бэкона-Шекспира служит фактически стержнем, на который нанизано все остальное. Однако чтобы углядеть этот стержень, надо быть очень внимательным.

Потому что даже абсолютно достоверные факты воспринимаются крайне по-разному в зависимости от того, кто, когда и как их подает. Вот, для иллюстрации, три ключевых факта истории – в сопоставлении с тем, как подавал их полковник Фридман сорок лет спустя.

Факт #1. Как и откуда в американской шпионской криптографии появилась звезда по имени Уильям Фридман.

Произошло это в 1915-1918 годах, в городке Женева пригорода Чикаго, в так называемых «Ривербэнкских лабораториях», как именовал свой персональный НИИ текстильный фабрикант и миллионер Джордж Фабиан. Человек не особо образованный, но увлеченный и энергичный, Фабиан тратил кучу денег на развитие наук по своему собственному прихотливому выбору. По этой причине в Ривербэнке одновременно занимались вскрытием шифров в старинных книгах Бэкона и Шекспира, конструированием устройств акустической левитации, разведением зоопарка и генетическим улучшением сельскохозяйственных культур.

За криптографическое направление поначалу отвечала весьма пожилая миссис Элизабет Гэллап, книги которой о вскрытии бэконовских шифров весьма впечатлили Фабиана. А юного и даровитого аспиранта-генетика Фридмана поначалу пригласили в Ривербэнк развивать сельское хозяйство. Вскоре, однако, неожиданно обнаружилось, что таланты Фридмана простираются далеко за пределы биологии. И в делах вскрытия шифров, как выяснилось, ему просто не было равных.

Спустя 40 лет, в разоблачительной книге Фридмана от 1957 года, вполне однозначно сообщается, что мадам Гэллап, по компетентному мнению автора, хотя и была честной женщиной, но полностью погрузила себя в самообман собственных фантазий. И реально никаких шифров она на самом деле не вскрывала, выдавая за дешифровки ею же и придуманные домыслы.

Что же касается главы Лабораторий, полковника Фабиана (как его часто называли), то в весьма жестких и ядовитых оценках Фридмана его бывший и давно умерший благодетель был просто богатым сумасбродным коммерсантом, вообще ничего не смыслящим в криптографии. А научные исследования финансировавшим исключительно лишь ради собственного самопрославления.

Colonel George Fabyan, *c.* 1915.

Хорошо известно, что за этими нелицеприятными словами скрывается серьезный личный конфликт между Фридманом и Фабианом в конце их сотрудничества. Но самое главное, что подобные оценки очень плохо стыкуются со следующим фактом.

Факт #2. Как и почему на здании Ривербэнкских Лабораторий появилась мемориальная доска правительства – в память о полковнике Фабиане от благодарного АНБ США. Доска была установлена в 1992 году, в ознаменование 75-й годовщины криптографических курсов, которые Фабиан по личной инициативе устроил для обучения офицеров американской армии на базе своего собственного Криптографического департамента.

Суть же здесь такова, что в 1917, когда США вступили в мировую войну, неожиданно выяснилось, что у вооруженных сил страны катастрофически не хватает специалистов, понимающих в шифрах и в их вскрытии. А вот у Джорджа Фабиана такого рода специалисты (точнее специалистки-дамы) были в достатке, причем возглавлял их особо головастый Уильям Фридман. Который не только умел вскрывать шифры известными из книг способами, но и придумывал свои собственные математические методы. (Далеко не все криптографы ныне знают, что общепринятый термин «криптоанализ» был запущен в профессию с подачи Фридмана.)

Любой человек, даже ничего не смыслящий в криптоанализе, вполне способен постичь, что молодой ученый, впервые серьезно столкнувшийся с шифрами, в принципе не сможет проявить свой талант гениального криптографа, если ему подсовывать для вскрытия всякую ерунду из находок старой дамы, погрязшей в собственных фантазиях. Чтобы талант раскрылся, нужно непременно решать реальные задачи. Иначе никакого результата просто не будет. Мусор на входе – мусор на выходе.

Прекрасно известно, что криптографический гений ученого-биолога раскрылся в 1915-16 гг, когда он занимался исключительно шифрами в текстах Бэкона-Шекспира. Однако в своей книге от 1957 года полковник Фридман вполне определенно пытается убедить читателей, будто никаких шифров на самом деле в книгах бэконовского круга не обнаруживалось и не вскрывалось.

Это заявление противоречит не только логике и здравому смыслу, но и абсолютно не стыкуется со следующим достоверным фактом – о котором Фридман в своей книге не упоминает вообще ни слова.

Факт #3. Откуда у Джорджа Фабиана появился интерес к акустической левитации, и почему ныне его детище носит название «Акустические лаборатории Ривербэнк».

Здесь первопричина всему в том, что среди старинных текстов, дешифрованных миссис Гэллап, имелся такой, где Фрэнсис Бэкон дал описание одного из научных опытов, проводившихся участниками тайного общества розенкрейцеров. Эксперимент демонстрировал феномен акустической левитации, то есть подъем предмета силой зву-

ка, причем в бэконовском тексте имелось и общее описание для устройства такого «левитатора» – на основе двух соосных цилиндров с натянутыми на них струнами.

Хотя для серьезных ученых-физиков начала XX века это звучало как абсолютно ненаучная чепуха, Фабиан настолько сильно был впечатлен концепцией и несложной конструкцией устройства, что загорелся идеей воспроизвести феномен в собственной лаборатории. Первичные опыты закончились полной неудачей, однако Фабиан не сдавался и привлек к работе Уоллеса Сэбина – одного из наиболее авторитетных в США специалистов по акустике.

Ради исследований этого ученого и под его прямым руководством в Ривербэнке соорудили высококлассную акустическую лабораторию, едва ли не самую лучшую на тот период в стране. Которая, кстати, успешно работает и по сию пору. Вот только самому Сэбину поработать там практически не довелось. Сначала война полностью отвлекла ученого на решение технических задач в интересах армии и авиации, а как только война закончилась, в январе 1919 далеко не старый еще Сэбин вдруг скоропостижно скончался от послеоперационного инфекционного осложнения.

Джордж Фабиан, умерший в 1936, совсем немного не дожил до первых научных экспериментов с акустической левитацией, продемонстрировавших реальность феномена в 1940-е годы. Правда, происходило это уже не в Ривербэнкских лабораториях. Да и вообще, на протяжении нескольких последующих десятилетий к акустической левитации, поднимающей в воздух лишь очень легкие небольшие предметы, относились как к забавному физическому фокусу, не имеющему сколь-нибудь полезного применения.

Ситуация начала меняться к 1980-м годам, когда феномен начали осваивать для применения в специфических технологических процессах, требующих работы с предметами без прямых физических контактов. Причем особо удачную конструкцию такого

манипулятора – нерезонансный акустический левитатор – запатентовала и разрабатывала для НАСА американская компания Intersonics, штаб-квартира которой находится, что интересно, в городке Нортбрук. Интересно это по той причине, что городок Женева, где расположены Ривербэнкские акустические лаборатории, находится совсем рядом – в 30 милях к юго-западу от Нортбрука.

Но абсолютно никто, естественно, не видит никаких взаимосвязей между «выдуманной Гэллап» секретной машиной ордена розенкрейцеров и акустическим левитатором фирмы Intersonics Inc. По той, в частности, причине, что об акустической левитации от Фрэнсиса Бэкона в серьезной истории науки никогда не говорят и не пишут. Ибо в официальных бэконовских текстах ничего такого не обнаруживается.

Как сие понимать, или Знание это сила

Как рассказывали люди, близко знакомые с Уильямом Фридманом, на протяжении всей своей долгой секретной службы на правительство США – с начала 1920-х и до конца 1950-х – он всегда держал под стеклом на рабочем столе одну очень важную и дорогую для него фотографию. Причем к концу карьеры даже сделал ее увеличенную копию, которую поместил в рамку и повесил на стену кабинета.

Для людей непосвященных это была просто старинная памятная фотография, запечатлевшая большую группу офицеров американской армии, на рубеже 1917-1918 годов осваивавших учебный курс криптографии под руководством молодого инструктора Уильяма Фридмана (на фото он сидит по центру в группе гражданских, крайний справа).

Но вот для тех, кто знал Фридмана и его историю жизни поближе, картинка эта в высшей степени наглядно демонстрировала «оккультную» мощь криптографии, позволяющей у всех на виду размещать тайные послания таким образом, что их абсолютно никто не замечает. Ибо в действительности на фотографии этой Фридман закодировал все тем же «двухлитерным» шифром знаменитый девиз розенкрейцеров и Бэкона – KNOWLEDGE IS POWE(R), т. е. «знание это сила» (здесь битами информации являются различия в поворотах головы людей, а на кодирование последней буквы R просто не хватило курсантов).

Более того, для Фридмана этот бэконовский девиз был настолько важен, что он отправился под ним и в мир иной, завещав выбить те же слова и на надгробной плите своей могилы. Туда же, как свидетельствует понемногу расскречиваемая история АНБ, Фридман унес с собой и великое множество государственных тайн, к которым был приобщен по роду своей суперсекретной службы (подробности см. в текстах «Чтение между строк» и «Шизо-криптография»).

Ныне же, если кто-то вдруг захочет поинтересоваться дополнительной информацией о любопытнейшей истории Ривербэнкских лабораторий и для начала посмотрит соответствующую статью в Википедии, то быстро обнаружится вот какая неприятность. Ссылки на содержательные источники, привлекавшиеся для подготовки статьи, ныне ведут в никуда. Кто-то заботливо источники «выпилил», и трудно поверить, что это случайность.

По совершенно аналогичному сценарию из истории нашего государства кто-то неведомый выпиливает скудные крохи информации о факте прямых взаимосвязей между тайнами розенкрейцеров и секретами советской криптографической спецслужбы. Сколь бы странно сие ни звучало, но и это достоверный исторический факт.

Основатель и глава советской криптослужбы, или Особого отдела ВЧК-ОГПУ, старый большевик и чекист Глеб Бокий, в 1930-е годы близко сошелся с подпольными кругами мистиков-оккультистов. В частности, с биологом Александром В. Барченко, членом российского отделения ордена розенкрейцеров-орионийцев. Под сильным влиянием Барченко, для которого Бокий стал защитником и покровителем, в ОГПУ одно

время даже действовало тайное общество «Древняя Наука» для изучения секретных мистических знаний.

Вскоре, однако, последовал известный период большого террора, Глеб Бокий, как и многие другие старые большевики, был расстрелян, а все организации оккультистов в СССР были уничтожены, что называется, под корень… Однако вскоре, в середине 1940-х годов, вот какая интересная мистическая история произошла в одном из специфических «тюремных НИИ» чекистов, где ученые-заключенные занимались шпионскими и криптографическими задачами.

Один из заключенных этой «шараги», знаменитый изобретатель, музыкант – а также в прошлом советский шпион – Лев Термен придумал совершенно гениальное подслушивающее устройство (за которое впоследствии получит Сталинскую премию и квартиру на Ленинском проспекте столицы). Если говорить в общепринятых ныне словах, то Термен придумал Tempest-устройство, работающее на основе тонких взаимодействий между физикой акустических и электромагнитных волн.

В те времена, естественно, никто иностранной терминологией не пользовался, однако вещь получила примечательное название – «система Буран». Параллели в названиях между сверхсекретным советским «Бураном» и столь же глубоко засекреченным американским термином Tempest (Буря), родившимся примерно тогда же и для того же, просматриваются более чем очевидные. Однако без мистики вряд ли кто сможет вам объяснить, как происходят подобные случайные совпадения.

С помощью древнего «знания как силы» мистиков и шаманов подобные вещи объясняются довольно просто и естественно. Однако для науки, ясное дело, такие объяснения не годятся совершенно.

Некоторое время назад, правда, запущен большой междисциплинарный исследовательский проект под названием «Sci-Myst или научно-мистическое детективное расследование» . Для всех затронутых здесь тем в данном исследовании обнаруживается не только множество дополнительных взаимосвязей, но и значительно более широкий контекст – выводящий на тему единого устройства сознания и материи.

В подобном контексте – где все найденные выпиливаемые вещи возвращены обратно на свои места – картина нашей реальности начинает выглядеть совершенно иначе, чем казалось прежде. Если как следует фокусировать внимание, конечно. А не отвлекаться на пустяки вроде покемонов…

# # #

Дополнительное чтение

Об отчетливых взаимосвязях между оккультными науками и криптографией: **«Секреты дальночувствия», «Экстрасенсы от криптографии», «Крипто-акустика»**

О наименее известных страницах из истории АНБ США: **«Чтение между строк»**, **«Шизо-криптография»**

О своеобразной траектории гностических учений, сводящих в единое русло науку, инопланетян и религию: «**Шаманы матрицы**», **«Главная тайна Со-Знания», «Sci-Myst или Научно-мистический детектив».**

Секреты дальночувствия

(*Впервые опубликовано – апрель 2009*)

На официальном веб-сайте крупнейшей в мире спецслужбы, Агентства национальной безопасности США, имеется постоянный раздел (www.nsa.gov/public_info/), где из секретных архивов для всеобщего доступа регулярно выкладываются рассекречиваемые документы, представляющие исторический интерес.

Количество страниц в обнародованных таким образом материалах разведки, еще недавно носивших грифы SECRET и TOP SECRET, на сегодняшний день исчисляется многими и многими тысячами. Информативная ценность этих документов, естественно, варьируется очень широко, однако попадаются и подлинные жемчужины.

Один из таких материалов, в частности, – это статья из внутриведомственного секретного сборника АНБ *Cryptologic Spectrum* за 1972 год, где рассказывается об истории возникновения крайне любопытного комплекса разведывательных технологий под названием «анализ побочных каналов утечки информации».

Данное направление технической разведки, также известное под кодовым словом TEMPEST, на протяжении многих десятилетий остается одной из самых больших тайн спецслужб. Официальная информация на эту тему практически отсутствует, так что рассекреченная журнальная публикация – для США чуть ли не первое достоверное свидетельство, полученное, что называется, из первых рук.

В сочетании с уже известными сведениями, опубликованными ранее в виде рассказов-воспоминаний от непосредственных участников тех же событий в СССР и Великобритании, таинственная история TEMPEST обретает, наконец, хоть какую-то целостность. И вкратце может быть изложена примерно в таком виде.

Вещь в себе

Первое свидетельство о внимании специалистов к компрометирующим побочным сигналам от аппаратуры, обрабатывающей информацию, относится к 1943 году.

В годы второй мировой войны для шифрования наиболее серьезных телеграфных коммуникаций американской армии и военного флота использовались так называемые «смесители», изготовлявшиеся компанией Bell Telephone. Суть этого конструктивно простого и в то же время криптографически очень сильного шифратора – прибавление к каждому знаку открытого текста, выдаваемого телетайпом, очередного знака с одноразовой шифрующей перфоленты ключа.

Смешивая эти две «струи», такой шифратор-смеситель обеспечивает телеграмме абсолютную криптографическую защиту, если знаки с ключевой перфоленты случайны и равновероятны. Иначе говоря, у противника, сумевшего перехватить зашифрованное послание, нет никаких шансов аналитически восстановить открытый текст… Но это лишь в теории.

На практике же, когда один из таких смесителей тестировали в Bell Labs, инженер-исследователь случайно обратил внимание на интересный факт. Всякий раз, когда аппарат шифровал очередную букву, на осциллографе в другом конце лаборатории проскакивал характерный всплеск сигнала. Занявшись более тщательным изучением структуры этих всплесков, инженер с удивлением обнаружил, что может по их форме восстанавливать знаки открытого текста в том сообщении, которое зашифровывал смеситель.

Обеспокоенное руководство компании Bell рассказало военным о выявленной потенциальной угрозе в их оборудовании, однако в министерстве обороны к этой новости отнеслись крайне скептически. В мире бушевала война, и какие-то там слабенькие, регистрируемые лишь вблизи от шифратора электромагнитные сигналы в качестве реальной угрозы совершенно не воспринимались.

Однако инженеры Bell настаивали на своем и вызвались доказать на практике серьезность проблемы. Для эксперимента было выбрано одно из нью-йоркских зданий, где располагался криптоцентр американской армии. Укромно расположившись в другом доме через улицу, примерно на расстоянии 30 метров, инженеры записывали перехватываемые сигналы примерно в течение часа. После чего, затратив на анализ всего 3-4 часа (рекордное время даже для нынешней хайтек-электроники), сумели восстановить порядка 75% текстов из секретных посланий, передаваемых криптоцентром.

Столь внушительная демонстрация, ясное дело, произвела на военных начальников куда большее впечатление. Хоть и со скрипом, они все же согласились рассмотреть предлагаемые Bell меры по усилению шифраторов от компрометирующих излучений.

Но как только стало ясно, что в полевых условиях подобные модернизации никак невозможны, а каждый аппарат придется индивидуально возвращать изготовителю, от подобной идеи тут же отказались, решив ограничиться организационными мерами защиты. Типа бдительных осмотров местности вокруг криптоцентра в радиусе до 70 метров…

Ну а когда война закончилась и начались существенно иные сложности мирного времени, то о «мелкой» проблеме компрометирующих излучений в США на некоторое время просто забыли.

А вот в СССР, напротив, к 1945 году то же самое в идейном смысле направление добычи разведданных разрабатывалось спецслужбами уже очень активно. С существенно иной, правда, конкретной спецификой. Советское руководство тогда крайне интересовали не столько сигналы от шифраторов, сколько разговоры важных иностранцев за стенами дипломатических посольств в Москве.

Для решения этой задачи был привлечен гениальный изобретатель Лев Термен – в 1920-е годы создатель электронных музыкальных инструментов и телевидения, а в1940-е заключенный тюрьмы-шарашки НКВД «Марфино» (увековеченной в романе Солженицына «В круге первом»). Именно там Термен и изобрел свое совершенно фантастическое подслушивающее устройство.

Это изделие представляло собой миниатюрный, диаметром примерно с карандаш, полый цилиндрик, оканчивающийся гибкой мембраной с закрепленным на ней коротким штырьком антенны. В этом, собственно, и заключалось все устройство – никакой электроники, ничего более вообще.

Столь своеобразного «жучка» аккуратно встроили в роскошное, сработанное мастерами из ценных пород дерева панно, изображавшее герб США с белоголовым орлом. И при удобном торжественном случае через группу пионеров подарили этот шедевр американскому послу Авереллу Гарриману.

Впечатленный подарком, тот повесил его над своим столом, а чекисты таким образом на много лет заполучили микрофон-передатчик, стабильно работающий непосредственно из рабочего кабинета американского посла в его постоянной московской резиденции Спасо-хаус.

Секрет работы терменовского изобретения, представлявшего собой пассивный объемный резонатор, заключался в следующем. В здании напротив диппредставительства находился передатчик, излучавший в кабинет посла немодулированные радиоволны с частотой 330 МГц. При воздействии внешнего электромагнитного поля именно такой частоты «жучок» активизировался – полость цилиндра вступала с ним в резонанс и радиоволна переизлучалась обратно через антенну-штырек.

Если же в комнате, где находилось это устройство, шел разговор, то вибрирующая под действием звуковых колебаний мембрана модулировала переизлученную волну. Сигналы, промодулированные таким емкостным микрофоном-передатчиком, принимались соответствующим радиоприемником советской спецслужбы и записывались на магнитофон.

Закладка работала чрезвычайно успешно и была повторена еще в нескольких посольствах. Вскоре Лев Термен усовершенствовал технологию своей системы, именовавшейся «Буран», что позволило вообще отказаться от внедрения резонаторов и подслушивать разговоры в помещениях по колебаниям оконных стекол, также модулировавших речью отражения направленных радиоволн. Впоследствии, уже без Термена, для этих же целей стали еще более эффективно использовать лазеры.

«Жучок» в деревянном панно пережил четырех американских послов и мог бы исправно работать еще хоть сто лет, но в 1952 году его выявил, случайно настроившись на волну передачи прослушки, один из работавших в Москве британских специалистов. Хотя и с большим трудом, сотрудникам ЦРУ удалось-таки отыскать закладку, однако для них осталось совершенно непонятным, как подобное изделие вообще могло работать – без источника питания, без проводов и без радиодеталей.

За устройством, похожим на инопланетную технологию, как-то само собой закрепилось весьма характерное название The Thing, что в зависимости от конкретного контекста можно понимать как «вещь», «нечто», «штуковина» или даже «хреновина».

Разобраться в конструкции помогли все те же англичане. Питеру Райту (Peter Wright), ведущему научно-техническому сотруднику британской спецслужбы MI5, удалось восстановить принцип работы этой «штуковины». Чуть позже в MI5 стали делать реплику столь остроумного шпионского гаджета, который под названием SATYR использовался разведками Великобритании и США.

Тайны для двоих

Примерно в то же время, в 1951 году, инженеры-исследователи ЦРУ повторно переоткрыли уже подзабытый эффект компрометирующих ЭМ-излучений от шифраторов и поделились своим открытием с военной радиоразведкой (спецслужбой-предшественницей АНБ). Поскольку на этот раз без особых проблем удалось восстановить открытый текст сообщения на расстоянии около полукилометра, последовали многочисленные эксперименты с феноменом в его разных вариантах проявления.

В ходе этих опытов выяснилось, что компрометирующие побочные сигналы, причем весьма сильно, выдает практически любое оборудование, обрабатывающее информацию: телетайпы и телефоны, шифраторы и печатные машинки, множительная техника и факсимильные аппараты, не говоря уже о компьютерах.

При этом весьма разнообразны оказались и каналы возможных утечек – электромагнитные сигналы через эфир и по проводам связи, через кабели питания и водопроводные трубы, а также просто акустические звуки работы аппаратуры.

С этого момента, собственно говоря, и началось направление работ под кодовым названием TEMPEST – выявление побочных каналов утечки информации у противника для добычи через них разведданных и соответствующая защита от подобных утечек собственного оборудования.

О реальных успехах американских разведок на этом поприще по сию пору неизвестно практически ничего. А вот о нескольких очень удачных темпест-атаках англичан рассказал сам Питер Райт в своей мемуарной книге «Ловец шпионов», опубликованной в 1987 году в Австралии – несмотря на чрезвычайно энергичное сопротивление британских властей.

По свидетельству Райта, в 1956 году, в ходе одной из операций, носившей название Engulf, чувствительные микрофоны, тайно установленные в посольстве Египта в Лондоне, позволили англичанам по звукам механического шифратора Hagelin получить доступ к секретной дипломатической переписке арабов в период суэцкого кризиса.

Другая технически еще более изощренная операция Stockade была проведена против Франции. В 1960 году англичане вели переговоры о присоединении к Европейскому экономическому сообществу, и премьер-министр Макмиллан беспокоился, что французский президент де Голль, недовольный особыми отношениями Британии с США, заблокирует вхождение страны в Сообщество. Поэтому премьер попросил разведчиков выяснить позицию Франции на переговорах.

Разведка попыталась вскрыть французский дипломатический шифр, но безуспешно. Однако Райт и его команда обратили внимание, что шифрованный трафик нес слабый вторичный сигнал, и сконструировали оборудование для восстановления этого сигнала. Оказалось, что это был открытый текст, который каким-то образом просачивался через шифратор в линию…

Вскоре после этих событий, в 1964 тесно сотрудничавшим спецслужбам Британии и США стало понятно, что и советская техническая разведка все эти годы отнюдь не стояла на месте. Предпринятая в тот период большая зачистка в здании американского посольства в Москве выявила не только свыше 40 микрофонов прослушки, но и множество новых технических приспособлений с неясными принципами работы.

Например, непосредственно над зоной криптоцентра, где шифраторы обрабатывали секретную дипломатическую переписку Госдепартамента, была обнаружена здоровенная металлическая решетка, тщательно замурованная в бетон пола. В других помещениях обнаружились решетки поменьше – с проводами, которые уходили в стену и вели неведомо куда.

А еще были найдены просто куски проводов, имевшие, однако, на конце ювелирно сработанную сеточку из микроскопически тонких проволочек толщиной с волос. Столь же загадочные находки то и дело обнаруживались в посольствах США в Праге, Будапеште и Варшаве.

Вещь для всех

Хотя, как можно видеть, к середине 1960-х годов темпест-операции спецслужб уже носили вполне зрелый характер и весьма внушительный размах, уровень секретности был таков, что широкая общественность ничего не ведала о побочных каналах компрометации еще лет двадцать, до середины 1980-х. После чего произошло самостоятельное переоткрытие этих же принципов учеными и инженерами, никак не связанными с государственными тайнами.

Причем теперь уже открытия сопровождались соответствующими публикациями результатов в общедоступных статьях и эффектными публичными демонстрациями «шпионских технологий», порою очень похожих на фокус или розыгрыш.

Первый важный результат был получен в 1985 году, когда голландский инженер-компьютерщик Вим ван Экк, занимавшийся медицинской техникой, в ходе своих экспериментов обнаружил, что с помощью телевизора, антенны и вручную настраиваемого генератора синхроимпульсов можно дистанционно восстанавливать изображение другого видеодисплея – даже если тот работает в другом здании.

Статья ван Экка в журнале Computers & Security и эффектная 5-минутная демонстрация его «шпионской» техники по телевидению, в передаче Би-Би-Си «Мир завтрашнего дня», имели весьма большой резонанс в мире ученых и инженеров. За несколько лет открытым академическим сообществом были переобнаружены практически все основные каналы побочных утечек информации – как электромагнитные (особенно от соединительных кабелей), так и акустические (например, от звуков нажимаемых кнопок клавиатуры).

Пытливые исследователи в университетских лабораториях самостоятельно открыли и новые, весьма оригинальные каналы утечек. Так, работающий в Кембридже немецкий ученый Маркус Кун в 2002 году продемонстрировал, что в принципе имеется возможность восстанавливать картинку на экране телевизора или компьютерного монитора по одному лишь мерцанию света в комнате – с расстояния в несколько сотен метров. Куну для этого потребовались хорошая оптическая труба, качественный светочувствительный датчик и доскональное понимание тонкостей работы электронно-лучевых трубок.

Примерно тогда же американский исследователь Джо Локри показал, что с помощью аналогичной техники – приличной оптики и светового сенсора – можно при расстоянии до полутора километров снимать данные с постоянно мигающих лампочек-инди-

каторов компьютерного оборудования. Например, в модемах, подключающих ПК к сети, мигание светодиода, как выяснилось, в точности соответствует битам проходящей через компьютер информации.

Ныне тема побочных каналов утечки также нередко упоминается в связи с открытыми хакерами новыми методами компрометации смарткарт. В конце 1990-х годов было продемонстрировано, что через анализ флуктуаций в электропитании смарткартных процессоров можно извлекать из них криптоключи, защищающие наиболее важную информацию.

Эта знаменитая работа американца Пола Кочера вдохновила целый ряд глубоких темпест-исследований в криптографическом сообществе. В результате чего было показано, в частности, что подобной по сути атакой с помощью направленной радиоантенны можно дистанционно извлекать ключи из специализированных криптоакселераторов, которые в серверах компаний обеспечивают ускореннную обработку шифрованных финансовых транзакций с участием банковских кредитных карт…

Один из видных экспертов по безопасности в своих комментариях ко всем этим работам резонно отметил, что главным секретом «Темпеста», как и атомной бомбы, был сам факт возможности технологии. А когда этот факт становится общеизвестен, установить важнейшие каналы побочных утечек информации может любой грамотный инженер.

О сколько нам открытий чу́дных…

Упомянутая в самом начале историческая статья из секретного сборника АНБ США Cryptologic Spectrum отмечает также следующий факт. Небезынтересно, что практически с самого начала комплекса исследований, получивших название Tempest, задача разведывательной добычи сигналов-утечек решалась намного более эффективно и творчески, чем защита собственного оборудования от компрометирующих излучений. Почему так происходило, пишет автор статьи, наверняка никто не знает, но вполне возможно, что людям элементарно гораздо интереснее шпионить за другими, чем охранять собственные секреты.

Оценивая же в целом содержание этого примечательного документа спецслужбы, датированного, можно напомнить, 1972 годом и рассекреченного в 2008, необходимо отметить, что три последних раздела – т.е. около половины статьи – перед открытой публикацией были практически полностью вымараны цензурой.

Оставлены лишь наименования разделов, условно обозначающие еще три метода добычи компрометирующей побочной информации: Seismics, Flooding, Anomalies (Сейсмическая разведка, Затопление, Аномалии). В дискуссионных форумах интернета при желании можно отыскать множество гипотез относительно того, что реально

означают эти слова. Насколько же эти домыслы соответствуют истине, достоверно пока неизвестно.

А это, соответственно, означает, что и в будущем о TEMPEST предстоит узнать еще немало нового и интересного.

# # #

Крипто-акустика

(*Январь 2014*)

Акустические технологии – одно из самых экзотических, пожалуй, направлений в составе науки криптологии. Но и здесь имеется своя, довольно колоритная и богатая на события история.

Под самый конец уходящего 2013 года группа израильских ученых-криптографов опубликовала в интернете весьма неординарную исследовательскую работу.

Суть этого исследования, если совсем вкратце, сводится к тому, что в принципе по одним лишь звукам работы компьютера удается реально восстанавливать секретный криптографический ключ, с помощью которого данный компьютер шифрует информацию…

Люди, имеющие скептический склад ума, но при этом не обремененные познаниями относительно обширной предыстории вопроса, тут же отвергли результаты израильтян – как технически невозможные и просто невероятные.

О том, сколь глупо выглядят «скептики», решительно отметающие любые факты лишь потому, что те противоречат их личным взглядам и опыту, рассказывать надо отдельно и с подробностями.

Здесь же – для общего представления о предмете и понимания глубины конкретно решенной задачи – лучше рассказать об истории появления и развития акустического направления в криптологии.

Мистическое начало

Как многие, возможно, наслышаны, искусство тайнописи и вскрытия шифров на протяжении тысячелетий считалось одной из разновидностей оккультизма. То есть тайным знанием вроде алхимии, занятия которым происходят не без участия потусторонних сил.

На подлинно научный фундамент – в виде строгой математики – криптология встала лишь в XX веке, благодаря, в частности, трудам таких людей как Уильям Фридман и Клод Шеннон.

О том, кто такой Клод Шеннон – отец теории информации и научной криптографии – наслышаны сегодня практически все. Про Уильяма Фридмана публике известно куда меньше, и тому имеются вполне естественные причины.

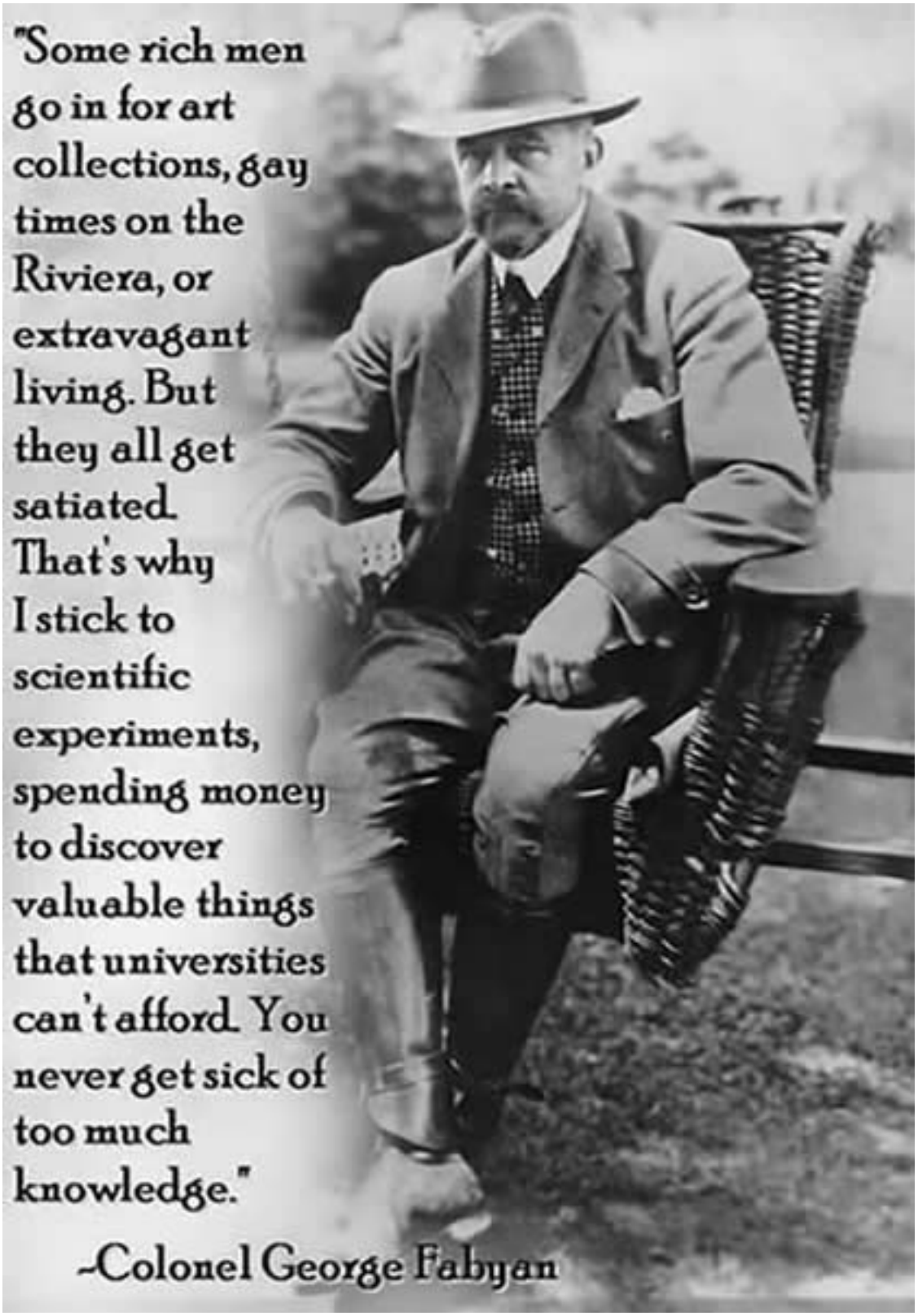
Самая главная среди них заключается в том, что есть все основания считать Уильяма Фридмана если и не главным, то одним из главных «отцов-основателей» американского АНБ, крупнейшей в мире секретной спецслужбы, сосредоточенной на криптографии и радиоэлектронной разведке.

Одна лишь история о том, как тихого и умного еврейского мальчика родом из местечковой Бессарабии угораздило оказаться среди основателей Агентства национальной безопасности США, бесспорно заслуживает не только большого романа, но и захватывающего биографического фильма.

Но подобного рода книга почему-то до сих пор так и не написана. Ключевые моменты этого никем еще не востребованного сюжета можно найти в материале «Наука a la Ривербэнк», ну а здесь следует упомянуть лишь существенные для данного рассказа эпизоды. В первую очередь – об акустическо-криптографических «родовых связях».

В начале XX века, когда Первая мировая война для Америки была еще делом далеким и чужим, молодой биолог-генетик Уильям Фридман впервые столкнулся с проблемами криптографии при крайне необычных обстоятельствах.

Американский миллионер и текстильный магнат, полковник Джордж Фабиан (в те времена в США солидное военное звание можно было обрести и без службы в армии), неподалеку от Чикаго создал нечто вроде собственного научно-исследовательского института, получившего имя «Ривербэнкские лаборатории».



В соответствии с личными интересами и предпочтениями эксцентричного хозяина, эти лаборатории одновременно занимались разработкой столь несовместимых, казалось бы, направлений, как криптографические исследования, улучшение пород домашнего скота и зерновых культур, эксперименты в области акустической левитации…

В условиях Ривербэнка, однако, связь между всеми этими направлениями имелась самая что ни на есть непосредственная. Так, ученого генетика Фридмана пригласили в лаборатории для продвижения сугубо сельскохозяйственного направления. Но уже на месте довольно быстро выяснилось, что молодой биолог оказался не только даровитым от рождения криптографом, способным лихо вскрывать мудреные для прочих шифры, но еще и головастым математиком, применяющим свои познания для научного анализа криптограмм.

Прямая же связь этих исследований с акустикой была еще более удивительной. Страсть Фабиана к криптографии объяснялась тем, как и куда это направление в его лабораториях вела некая миссис Элизабет Уэллс Гэллап. То есть весьма известная в свое время дама, прославившаяся расшифровкой стеганографических (как это именуют ныне) текстов в первом издании трудов Шекспира (Первое Фолио) и в других книгах его современников.

Подробности об этом методе тайнописи, носящем название «двухлитерный шифр» и изобретенном в шекспировскую эпоху Фрэнсисом Бэконом, можно найти в материале «Если дело дойдет до суда». Здесь же нас интересует одно конкретное, сугубо прикладное открытие миссис Гэллап.

Элизабет Гэллап

Среди разнообразной информации, дешифрованной этой дамой в книгах начала и середины XVII века, содержались не только признания и разъяснения относительно того, кто является подлинным автором шекспировских текстов, но и описание конструкции машины для акустической левитации – как еще одно изобретение Фрэнсиса Бэкона.

Столь необычная машина, способная поднимать предметы в воздух одной лишь силой звука, чрезвычайно заинтересовала полковника Фабиана. Ну а практическим результатом этого интереса магната стало создание в Ривербэнке превосходной акустической лаборатории, без преувеличения самой лучшей на тот момент в США по своему техническому оснащению.

Дальнейшая судьба всего этого предприятия сложится таким образом, что Фабиану в итоге так и не удастся дожить до экспериментального подтверждения феномена акустической левитации. Однако запущенное им начинание по сию пору живет и известно как «Акустические лаборатории Ривербэнк».

Акустические лаборатории Ривербэнк

Ныне на здании лаборатории, что интересно, висит мемориальная доска от правительства США – в знак благодарности за вклад полковника в большое и важное дело. Но только отнюдь не в области акустики, а за непосредственное участие в создании национальной криптографической спецслужбы…

(Подробности о том, как фабиановский протеже и отец научного криптоанализа Уильям Фридман на заре своей карьеры занимался вскрытием шифров Бэкона в шекспировских текстах, вспоминать обычно не принято. Ну а уж про то, что об акустической левитации впервые стало известно из того же экзотического источника, так и вообще давно забыли.)

Трудные годы войны

Крутой военный поворот в абсолютно мирной прежде карьере Уильяма Фридмана произошел в тот момент, когда США решили подключиться к боевым действиям союзников на фронтах Первой мировой. Ибо тут же выяснилось, что у американской армии имеется острейшая нехватка квалифицированных кадров для работы с шифрами. А самой компетентной национальной инстанцией в области криптоанализа, по сути дела, оказались Ривербэнкские лаборатории Джорджа Фабиана.

Как результат, по предложению Фабиана в Ривербэнке были устроены учебные курсы, где Уильям Фридман стал готовить для армии группы специалистов по вскрытию шифров. Ну а вскоре после этого ученого-инструктора зачислили на полную военную службу – и отправили в Европу в качестве главного криптоаналитика при генерале Першинге, командовавшем американским корпусом.

Так что дальше и уже на всю остальную жизнь Уильям Фридман оказался неразрывно связан с военной криптографией, через несколько десятилетий – уже после Второй мировой – став также и одним из отцов-основателей крупнейшей в мире спецслужбы, американского Агентства национальной безопасности.

Уильям Фридман на государственной службе

Что же касается вступления США во Вторую мировую войну (произошедшего, как всем известно, в результате Перл-Харбора), то в связи с этим драматичным моментом лично у Фридмана произошла тяжелейшая психологическая травма.

Именно в тот исторический период Уильям Фридман возглавлял важнейшее направление криптоаналитических усилий нации, нацеленных на вскрытие военных и дипломатических шифров Японии – как главного потенциального противника. И именно здесь американскими криптографами были достигнуты грандиозные успехи: секретная переписка японских милитаристов не просто дешифровалась, но систематически читалась руководством США в массовых количествах.

Когда же японцы «неожиданной» атакой тотально разгромили не готовый к нападению тихоокеанский флот США в Перл-Харборе, Уильям Фридман чуть не сошел с ума. По свидетельству коллег, он практически перестал реагировать на окружение, бесконечно повторяя лишь одну и ту же фразу: «Но ведь они же знали, они же знали!»…

Закончилось это все сильнейшим нервным срывом и помещением криптографа в лечебницу. (В официальной истории США, кстати говоря, по сию пору принято считать, что руководство страны и лично президент Рузвельт – искавший поводы для вступления в войну – «ничего не знали» о подготовке Японией нападения. Хотя прямо противоположные свидетельства имеются и от других руководителей криптослужбы.)

Дабы вернуть рассказ в русло криптографической акустики, следует упомянуть два таких исторических факта.

В годы войны американский исследовательский центр Bell Labs, где среди прочих ученых-разработчиков был и Клод Шеннон, стал той лабораторией, в которой работы над засекречиванием речи породили революционную идею о «криптографии с открытым ключом».

В столь давнюю пору термина такого, правда, не было и в помине (он появится лишь через три десятка лет), да и об участии Шеннона именно в этом проекте ничего достоверного не известно, однако факт появления собственно идеи является несомненным и задокументированным.

Суть изобретения заключалась в том, чтобы сторона, принимающая информацию, тоже участвовала в ее засекречивании – наряду с отправителем. Конкретно в приложе-

нии к акустике и обработке речи в телефонной линии это сводилось к тому, чтобы на приемном конце инвертировать волновой сигнал и в таком виде сразу же отправлять его обратно в канал.

Как результат такого наложения двух вариантов одной волны, находящихся в противофазе, в линии все информативные сигналы взаимно гасились, так что третья сторона, подслушивающая передачу, могла услышать в канале связи лишь только одну тишину…

Подробности о том, как эта нереализованная в военные годы идея в начале 1970-х вдохновит ученых на изобретение принципиально новой криптографии, можно прочитать в материале «Параллельные миры». Здесь же пора вспомнить еще один – шпионско-акустический – эпизод в тему, только уже из истории спецслужб СССР.

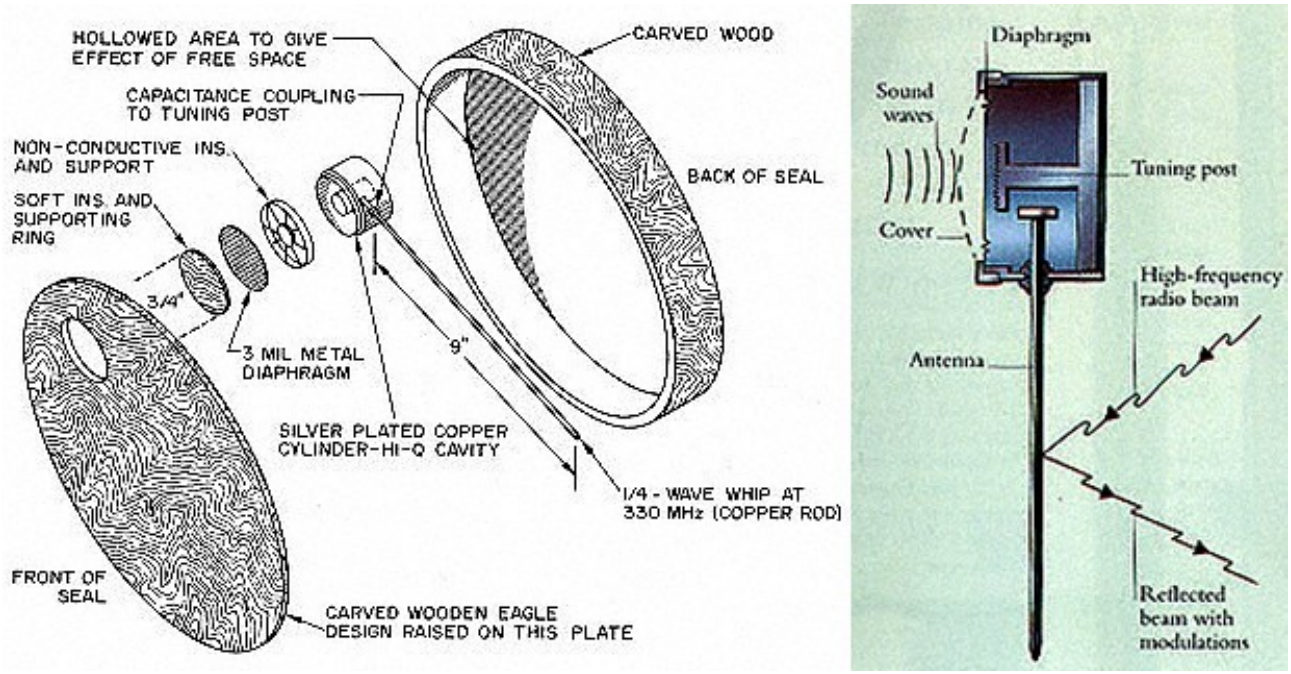
Случилось так, что широко известный в мире изобретатель и инженер Лев Термен, знаменитый прежде всего своим электромузыкальным инструментом «терменвокс», в период между двумя мировыми войнами был не только популярным, с успехом гастролирующим по миру музыкантом, но еще и натурально советским разведчиком.

Лев Термен и его терменвокс

В конце 1930-х, как и очень многих других приличных людей, Термена, известное дело, советские власти посадили (хорошо не убили). Так что в 1940-е годы, уже пережив магаданские лагеря, он работал в небезызвестном тюремном НИИ или, иначе, шарашке НКВД в Марфино. (Где также доводилось отсиживать свой срок над инженерно-крипто-математическими задачами и Александру Солженицыну, см. его роман «В круге первом»).

Именно там заключенный Лев Термен изобрел одну из самых гениальных своих вещей – шпионскую радио-акустическую технологию под названием «система Буран». Досконально понимая тонкости взаимодействий звука и радиоволн, изобретатель сумел придумать такое подслушивающее устройство, которое состояло всего лишь из кусочка трубки диаметром с карандаш, упругой мембраны в торце трубки и прикрепленного к ним штырька-антенны.

При этом данное устройство функционировало как совершенно полноценный жучок-радиопередатчик прослушки – вообще без всяких радиодеталей, проводов и элементов питания… Много позже, когда американские контрразведчики из-за удачного для них стечения обстоятельств все-таки сумели отыскать этого жучка, к тому времени уже давно работавшего в кабинете посла США в Москве, то довольно долго они вообще не могли понять, как такая штука (The Thing) в принципе может действовать.



Система Буран или The Thing

Технические детали вокруг этого сюжета можно найти в материале «Секреты дальночувствия». И там же представлена общая история темы TEMPEST – как комплекса особо секретных шпионских технологий, выстроенных спецслужбами вокруг побочных утечек компрометирующей информации.

(По любопытному совпадению, именно так – The Tempest или «Буря» – называется пьеса, открывающая «Первое Фолио» 1623 года, то есть исторически самое раннее полное издание трудов Шекспира… или Бэкона. Для добавления мистики, полезно обратить внимание и на очевидное созвучие названий для идейно близких, но появлявшихся независимо друг от друга технологий разведки – «Буря» в США и «Буран» в СССР…)

Странное послевоенное время

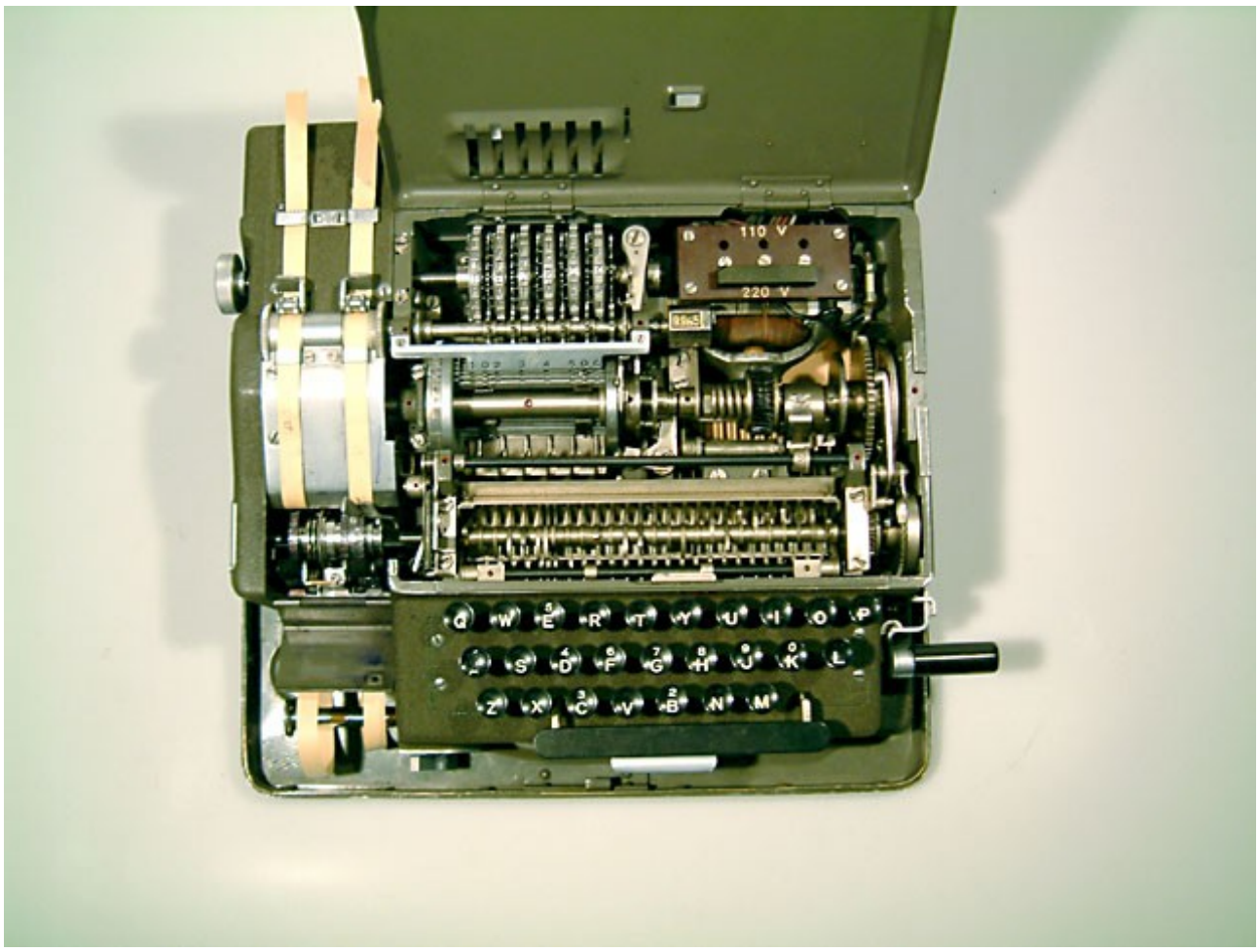
Рассекреченные за последние годы документы спецслужб свидетельствуют, что по-настоящему серьезные исследования и разработки шпионских технологий, объединяемых термином TEMPEST, начались после окончания Второй мировой войны.

В ходе этих исследований довольно быстро выяснилось, что компрометирующие побочные сигналы выдает – причем выдает весьма сильно – практически любое оборудование, обрабатывающее информацию: телеграфные аппараты и телефоны, шифраторы и пишущие машинки, множительная и факсимильная техника, не говоря уже о компьютерах.

При этом весьма разнообразными оказались и каналы возможных утечек. Доступ к обрабатываемой информации, как выяснилось, при грамотном инженерном подходе предоставляют шпионам не только электромагнитные сигналы утечек через эфир и по проводам связи, но также утечки через кабели питания, вентиляцию и водопроводные трубы. Ну и, наконец, просто акустические звуки работы аппаратуры.

Примером ранней и чрезвычайно успешной крипто-акустической атаки подобного рода можно считать операцию Engulf британской разведки MI5. В 1956 году, в политически крайне напряженный период суэцкого кризиса, эта операция обеспечила англичанам доступ к секретной дипломатической переписке Египта.

Технически это было осуществлено с помощью очень чувствительных микрофонов, которые были тайно установлены в шифровальном помещении египетского посольства в Лондоне. По звукам шестеренок и дисков механического шифратора Hagelin эти микрофоны позволяли восстанавливать секретные криптоключи, применяемые в переписке.



Один из шифраторов Hagelin, BC-543

С швейцарскими шифраторами Hagelin, знаменитыми в мире и по сию пору, связана, кстати, история еще одного нервного срыва у уже известного нам героя невидимого фронта, Уильяма Фридмана. Который, надо отметить, обладал обоюдоострым криптографическим талантом. То есть не только с блеском вскрывал чужие шифры, но и успешно изобретал качественные шифраторы для американской армии.

Мир же криптографической техники, надо сказать, всегда был довольно невелик, особенно в те времена. Так что изобретателя шифраторов Hagelin, шведского предпринимателя Бориса Хагелина, Уильям Фридман не только хорошо знал, но и был довольно близко знаком с ним лично (в годы войны бизнесмен сделал состояние на поставках своих шифраторов вооруженным силам США).

Штаб-квартира Crypto AG в г. Цуг, Швейцария

В послевоенное время Хагелин перевел свой бизнес в нейтральную Швейцарию, где в городе Цуг обосновалась штаб-квартира его фирмы. Получив название Crypto AG, эта компания весьма быстро добилась успеха – уже в 1950-е став своего рода аналогом «надежных швейцарских часов и банков» на мировом рынке криптографической техники.

В те же 50-е годы в США произошло тотальное объединение всех разрозненных криптоспецслужб страны – в единую, мощную и чрезвычайно секретную разведывательную структуру под названием Агентство национальной безопасности. (На протяжении нескольких первых десятилетий сам факт существования АНБ считался государственной тайной.)

Одной же из самых ранних суперсекретных инициатив нового агентства стала так называемая «операция BORIS» (как именуют ее ныне историки спецслужб). Официально суть операции не раскрыта по сию пору, но имеется масса документальных свидетельств, согласно которым уже известный нам Уильям Фридман по заданию властей США в середине 1950-х годов совершил поездку в Европу с крайне деликатной тайной миссией.

Борис Хагелин

Суть этой миссии сводилась к секретным встречам с руководством ведущих компаний криптографической индустрии – прежде всего Crypto AG, но также и других фирм. Много-много лет спустя, уже в 1990-е, независимые журналистские расследования позволили восстановить в общих чертах картину произошедшего. Из этой картины стало видно, как напирая на страхи Западной Европы перед коммунистами, АНБ США сумело склонить по крайней мере некоторые из этих фирм к тайному сотрудничеству.

Итогом этого сотрудничества становились определенные модификации криптосхем в шифраторах, своего рода «закладки», обеспечивавшие АНБ тайный ход для доступа к секретной переписке, закрываемой подобными шифраторами.

Более развернутый рассказ об этой специфической стороне криптографии можно найти в материале «Объяснимые слабости», ну а здесь пора вернуться к Уильяму Фридману. Который из своей секретной командировки в Европу вернулся в крайне подавленном состоянии, закончившемся еще одним нервным срывом.

У историков спецслужб нет, насколько известно, свидетельств и документов, объясняющих причины этого душевного кризиса. Одни полагают, что Фридмана могла сильно угнетать глубочайшая «нечистоплотность» той тайной миссии, которую возложило на него государство. Другие же – более приземленные аналитики – подозревают, что причиной глубокой депрессии и срыва стали встречи в Швейцарии с давним знакомым, Борисом Хагелином.

Получив возможность непосредственно наблюдать, сколь благополучно и богато складывается жизнь у успешного крипто-изобретателя, Фридман не мог не сопоставить эту картину с собственной реальностью скромного и безвестного госслужащего. Как человек, создавший для США ничуть не менее сильный – а может даже и еще лучший – шифратор, Фридман за свое изобретение не получил от государства фактически ни копейки…

На то, что причиной психологических проблем стали деньги, может косвенно указывать странноватая история, произошедшая с Фридманом вскоре после «операции Boris». На старости лет матерый криптограф решил вдруг вернуться к годам своей невинной юности и написал книгу, в которой в пух и прах «разоблачил» дилетантские упражнения миссис Гэллап в области расшифровки бэкон-шекспировских текстов.

Уильям Фридман на закате жизни

Без надлежащих документов и свидетельств довольно трудно объяснить, кому еще, кроме самого разоблачителя, в середине 1950-х годов в США могла понадобиться подобная работа, всячески доказывающая, что в первых изданиях книг «бэкон-шекспировского круга» вообще не было и нет никаких скрытых шифров. Но одно можно констатировать определенно. Помимо гонорара, за этот свой труд Уильям Фридман как автор вскоре получил вполне конкретный денежный приз – литературную премию от шекспироведов…

Примерно в тот же период, но только в СССР и с иным, сугубо советским перекосом в давлении государства на человека, с другим героем невидимого фронта – Львом Терменом – происходила собственная странноватая история. Когда после смерти Сталина гениального изобретателя, наконец, освободили и реабилитировали, Термен еще много лет так и продолжал ездить на работу в свою бывшую тюрьму. Без всякого принуждения, совершенно добровольно…

Крипто на свободе

Одним из замечательных явлений компьютерной науки в последнюю четверть XX века стало то, что в среде открытого академического сообщества зародилась и стала бурно развиваться собственная криптография, практически независимая от скрытного и необщительного мира спецслужб.

Академическим ученым-криптографам не было никакого дела до шпионских проблем государства, они развивали свою науку ради защиты онлайновой коммерции и вообще – для самых разнообразных приложений в области защиты информации в эпоху цифровых коммуникаций.

Вряд ли удивительно, что в процессе всех этих исследований были повторно переизобретены и теперь уже широко опубликованы очень многие из секретных алгоритмов, методов анализа и прочих хитростей спецслужб, прежде сокрытых под покровом гостайны.

Не обошла эта участь стороной и многочисленные секреты технологий TEMPEST. Начиная примерно с 1985 года в открытой прессе то и дело стали появляться результаты исследований, обнаруживавших все новые и новые каналы побочных утечек информации. Поначалу основной интерес вызывали электромагнитные каналы компрометации, однако со временем были открыты и оптические каналы, и акустические.

Можно сказать, что пик акустических Tempest-переоткрытий пришелся на первое десятилетие 2000-х годов. В этот период, в частности, коллективы ученых из разных стран и университетов продемонстрировали, что по одним лишь звукам работы компьютерной техники оказывается возможным получить массу данных об обрабатываемой в этот момент информации.

Например, были продемонстрированы весьма эффективные методы съема паролей и прочих текстов, вводимых через компьютерную клавиатуру – по характерным и сугубо индивидуальным кликам каждой из кнопок-клавиш. Другая впечатляющая демонстрация – акустический съем информации с распечатываемого документа по звукам работы матричного принтера.

Ну и апофеозом открытых исследований на крипто-акустическом поприще, можно сказать, стала масштабная работа от группы криптографов из израильских университетов, уже первые результаты которых, предъявленные публике в 2004 году, оказались воистину поразительными (см. материал «Особенности национальной забавы»).

По оценкам этих исследователей, явно обнаружилась потенциальная возможность для извлечения криптоключей из компьютера исключительно по звукам работы электронных схем…

Невероятно, но факт

Дальнейшие события вокруг столь интересного открытия израильтян сложились таким образом, что о супер-успешном продолжении этой работы мир узнал почти десятилетие спустя – в декабре 2013.

Какие именно причины растянули исследование на столь длинный срок, достоверно неизвестно, однако итог работы оказался настолько примечательным, что рассказать о нем необходимо чуть подробнее, нежели о прочих Tempest-атаках.

Метод акустического криптоанализа компьютерных процессоров разработан и реализован большим коллективом израильских ученых из нескольких университетов страны. Три основных деятеля группы (в порядке возраста и известности) – это Ади Шамир (Adi Shamir, буква S в знаменитом шифре RSA) из Вейцмановского научного института, Эран Тромер (Eran Tromer) из Тель-Авивского университета и Даниэль Генкин (Daniel Genkin) из университета Технион.

Имена остальных участников проекта, а также массу всевозможной информации о технических деталях этой разновидности «атак по побочному каналу» можно найти на вебсайте, посвященном данной работе: Acoustic Cryptanalysis, http://www.cs.tau.ac.il/~tromer/acoustic/ .

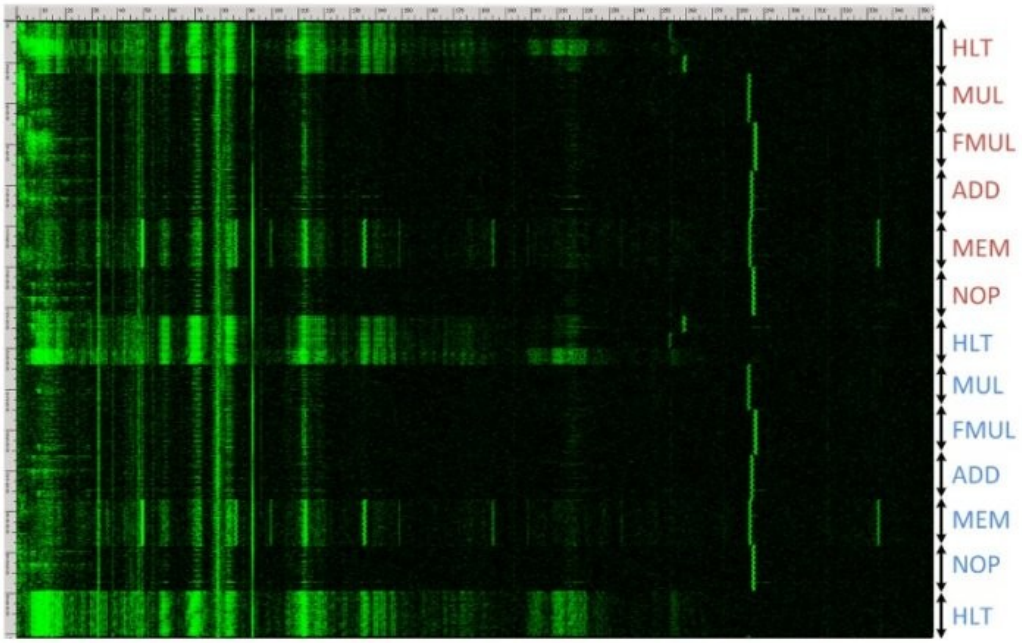
Главным же итогом исследования можно считать следующий факт. Разработанная авторами атака примерно за час времени позволяет успешно вскрывать один из самых безопасных, как принято считать, алгоритмов шифрования – RSA с длиной ключа 4096 битов.

Особо следует подчеркнуть, что с технической точки зрения эта атака весьма проста в реализации, так что может быть проведена с помощью недорогой и общедоступной аппаратуры. По сути дела, секретный криптографический ключ вскрывается в результате прослушивания – с помощью обычного микрофона – работы компьютерного процессора в тот период, когда он занят расшифровкой неких зашифрованных данных.

Дабы не нагнетать панику и не формировать у людей ложное представление, будто отныне оказываются безнадежно скомпрометированными все криптосистемы, применяющие общераспространенный алгоритм RSA, следует сразу подчеркнуть и весьма специфические нюансы данной атаки.

Во-первых, атака израильтян остро заточена под совершенно конкретную реализацию RSA – в программе шифрования GnuPG (свободно распространяемая вариация PGP) версий 1.x. Причем новая версия этой программы – при непосредственной помощи тех же израильских ученых – уже обновлена и сделана стойкой к методам акустического криптоанализа.

Во-вторых, секретный ключ по звукам процессора удается извлечь лишь в том случае, если этот процессор в течение около часа непрерывно занимается расшифрованием специально подсунутых ему особых шифртекстов. Такого рода материалы на входе носят название «подобранные шифртексты», и они умышленно сконструированы атакующими таким образом, чтобы порождать в компьютере определенные акустические эффекты.



Акустические спектрограммы разных операций ЦПУ

(Компрометирующие акустические сигналы в диапазоне частот от 10 до 150 КГц на самом деле генерируются не самим процессором, а регулятором напряжения ЦПУ, – по мере того, как он пытается поддерживать постоянное напряжение во время очень резко отличающихся по нагрузке вычислительных этапов обработки.)

Ну и в-третьих, наконец, под реальной угрозой компрометации оказываются лишь те компьютеры, к которым злоумышленники физически могут подобраться с микрофоном на расстояние непосредственной близости.

Атака через параболический микрофон

Но вот если настырному врагу все-таки удастся этого добиться, то – как продемонстрировали исследователи – становится возможным вполне успешно извлекать секретные ключи из ЦПУ с дистанции порядка четырех метров, если применяется высококачественный параболический микрофон.

Если же враг может подобраться на расстояние менее полуметра, то никакой особо чувствительной техники уже не требуется. Исследователям, в частности, удалось провести успешную атаку с помощью совершенно обычного смартфона, разместив его на удалении порядка 30 сантиметров от ноутбука жертвы.

Атака через смартфон

За время исследований учеными были организованы атаки против самых разных ноутбуков и настольных систем. В зависимости от конструктивных особенностей компьютеров, соответственно, весьма разной оказывалась и степень успеха атак.

Но в то же время, по мере накопления опыта и данных, была установлена еще одна важная вещь. Тот же самый тип электрических компрометирующих данных от ЦПУ можно выделять далеко не только акустически, но и от многих других источников побочных утечек: от электророзетки в стене; от удаленных концов сетевого кабеля Ethernet или видеокабеля VGA; наконец, даже просто положив руку на компьютер (одновременно измеряя электрический потенциал тела относительно потенциала заземления в комнате)…

Короче говоря, и в этом случае израильские ученые в очередной раз переоткрыли неисчерпаемый океан всевозможных Tempest-утечек через побочные каналы компрометации. О чем достаточно подробно написали в своей статье: «*RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis», by Daniel Genkin, Adi Shamir, Eran Tromer* [http://www.tau.ac.il/~tromer/papers/acoustic-20131218.pdf].

Вместо эпилога

Блог Брюса Шнайера, известного гуру в области защиты информации, часто становится площадкой для профессионального обсуждения подобного рода новостей. Поэтому в комментариях блога нередко можно найти весьма глубокие и компетентные суждения.

Но любой, даже высочайшего класса профессионал, в конечном счете все равно остается человеком с присущим людям несовершенством. А одним из признаков нашего несовершенства является заскорузлость мышления, не только блокирующая восприятие новой информации, но еще и обосновывающая негибкость ума «здоровым скептицизмом».

Конкретно в обсуждениях новости про акустический криптоанализ процессора появился, в частности, такой характерный комментарий (от некоего Джейкоба):

> *«Называйте меня скептиком, но я думаю, что эта исследовательская статья – первоапрельская шутка, появившаяся раньше срока. Независимо от больших имен ее авторов. Бьюсь об заклад, что никто не сможет независимо подтвердить их результаты.*
>
> *Я кое-что знаю про пассивные электронные компоненты и акустические вибрации … [далее следует довольно обширная подборка технических аргументов, по пунктам доказывающих, что вся проделанная израильтянами работа – это выдумки и ненаучная фантастика]… Короче, я на такое не куплюсь.»*

В ответ на тираду этого скептика и схожие комментарии его единомышленников, другой собседник (под кратким именем «q») совершенно резонно отмечает:

> *«Забавно, как множество людей торопятся огласить свою ‘скептическую’ реакцию, на самом деле даже не прочитав собственно публикацию… Но ведь это не ‘скепсис’ – это же ‘ВЕРУЮ!’, только с обратным знаком…*
>
> *Если бы вы взяли на себя труд все-таки прочесть статью, то обнаружили, что это хорошо известная и тщательно проработанная таймерная атака, где главное новшество – это очень умно подобранный (акустический) канал утечек для доступа к таймерным данным об обработке сигнала.*
>
> *Там нет никакого фантастического волшебства ‘с прослушиванием битов, летящих по шине’. Просто почитайте работу, это интересное и познавательное чтение»…*

Имеются сильные основания предполагать, что не только свежие результаты израильских криптографов, но и исторический материал данной статьи «про крипто и акусти-

ку» у людей со скептическим (но не любознательным) складом ума вызовет если и не полное отторжение, то по меньшей мере сильнейшие сомнения.

Но прежде, чем отвергать и сомневаться, имеет смысл все же покопаться самостоятельно в дополнительной, вполне достоверной информации. Можно узнать много нового и поучительного…

# # #

Дополнительное чтение

Весьма специфическая предыстория АНБ США – через факты биографии одного из ее основателей, Уильяма Фридмана: «Наука a la Ривербэнк», http://kniganews.org/map/e/01-11/hex70/

О малоизвестных страницах жизни Шекспира и творчества Фрэнсиса Бэкона: «Если дело дойдет до суда», https://kiwibyrd.org/2014/01/05/107/

О мистических совпадениях в истории синхронного изобретения криптографии с открытым ключом в секретной спецслужбе и академическом сообществе: «Параллельные миры», https://kiwibyrd.org/2013/12/03/0011/

История зарождения и эволюции шпионских технологий TEMPEST: «Секреты дальночувствия», https://kiwibyrd.org/2013/04/26/200904/

Почему теоретически сильная криптография на практике обычно оказывается значительно хуже, чем могла бы быть: «Объяснимые слабости», https://kiwibyrd.org/2013/08/31/0801/

О любопытных разработках хакеров и криптографов Израиля: «Особенности национальной забавы», https://kiwibyrd.org/2014/01/06/508/

Хитрости крипторемесла

(*Впервые опубликовано – декабрь 2007*)

В теории хорошо известно, как делать сильные шифры. Однако в жизни криптография обычно оказывается слабой. Как это происходит.

Что такое «уязвимость»

Группой израильских криптографов из университетов Иерусалима и Хайфы (Benny Pinkas, Zvi Gutterman, Leo Dorrendorf), недавно была вскрыта схема работы генератора псевдослучайных чисел, используемого Microsoft во всех криптоприложениях операционной системы Windows 2000 [eprint.iacr.org/2007/419].

Знание работы этого алгоритма позволило исследователям проанализировать общую стойкость подсистемы защиты и выявить в ней серьезнейшую уязвимость.

В частности, было показано, что из-за слабой схемы генератора злоумышленники могут без проблем, всего по одному внутреннему состоянию алгоритма, предсказывать большое количество криптоключей, вырабатываемых в ОС. Причем не только ключей для будущих потребностей, но и уже сгенерированных в прошлом.

Система Windows 2000 по сию пору используется многими компаниями и организациями, оставаясь, согласно общим оценкам, второй по популярности ОС Microsoft после XP. Но когда разнеслась весть о слабостях в PRNG (от pseudo-random number generator), то всех, естественно, взволновал вопрос об уязвимости крипто в более новых системах, XP и Vista. А именно, можно ли и их атаковать аналогичным образом?

Первая реакция Microsoft на подобные вопросы была довольно уклончивой и сводилась к заверениям публики в том, что последние версии Windows «содержат разнообразные изменения и доработки в схеме генератора случайных чисел».

Но коль скоро уже вскрытую схему выявить в системе гораздо легче, чем неизвестную, в Microsoft все же решились сказать правду и чуть позже признали, что Windows XP тоже уязвима для атаки, описанной в работе Пинкаса, Гуттермана и Доррендорфа.

Что же касается систем Windows Vista, Windows Server 2003 SP2 и планируемой к скорому выпуску Windows Server 2008, то там, по свидетельству Microsoft, схема генерации псевдослучайных чисел работает иначе и поэтому обладает иммунитетом к подобному методу взлома.

Попутно тут же была предпринята попытка интерпретировать работу израильтян не как выявление серьезной и реальной угрозы для безопасности XP (о старой Win2000 речи вообще не идет), а как сугубо «теоретическую атаку». Ибо, по официальному мнению Microsoft, выявленный «баг» не отвечает определению «уязвимость», поскольку для эксплуатации слабостей в PRNG злоумышленник должен обладать правами администратора.

Или, цитируя дословно, «поскольку администраторы по определению имеют доступ ко всем файлам и ресурсам системы, это [восстановление внутреннего состояния PRNG и вычисление ключей] не является недопустимым раскрытием информации».

То, что множество уже известных вредоносных программ, вроде всяких червей и троянцев, умеет повышать свои привилегии до уровня администратора, здесь, очевидно, считается не относящимся к делу.

Однако, дабы публика не слишком уж волновалась, Microsoft пообещала залатать-таки выявленную проблему в PRNG – где-нибудь в первой половине следующего года, вместе с выходом третьего сервис-пака, Windows XP SP3.

Иначе говоря, проблему хотят представить как нечто маловажное и не особо серьезное. Однако реальная проблема тут, строго говоря, заключается в ином.

Дело в том, что базовые принципы, на основе которых должен работать криптографически качественный PRNG, прекрасно известны. Грамотному разработчику, можно сказать, проще выбрать известный хороший криптоалгоритм, нежели разрабатывать собственный плохой.

Однако в программных продуктах Microsoft криптография всегда оказывается существенно слабее, чем могла бы быть. И вовсе не секрет, почему так происходит. Увидеть это совсем несложно, если взглянуть на историю вопроса в ретроспективе.

Чему учит история

Строго говоря, общедоступных официальных (или неофициальных) документов с хронологией развития и внятным рассказом о средствах защиты информации в программах MS не существует. По вполне очевидной причине общей закрытости кодов Windows-платформы.

Имеются, правда, заслуживающие доверия источники, вроде книги «Написание безопасных кодов» [*Michael Howard and David LeBlanc. «Writing Secure Code». Microsoft Press, 2002*], подготовленной специалистами корпорации и выпущенной издательством Microsoft Press. Но содержательные моменты в устройстве используемых криптоалгоритмов излагаются там лишь в самых общих чертах и без углубления в принципиально важные конструктивные подробности.

С другой стороны, учитывая грандиозные масштабы распространения программ Microsoft в мире, имеется также масса достоверной, хотя и обрывочной информации о взломе подсистем защиты в условиях Windows для всех периодов развития этой платформы. Сопоставляя эти сведения с информацией из упомянутой книжки, а также принимая во внимание общеполитические процессы, на фоне которых происходило развитие, можно вкратце восстановить картину примерно в таком виде.

Согласно авторам упомянутой книжки, Майку Ховарду и Дэвиду Лебланку, генератор псевдослучайных чисел, вызываемый функцией CryptGenRandom, впервые появился в ОС Windows 95, т.е. в середине 1990-х годов. С той поры его стали включать во все базовые версии операционных систем Microsoft и их вариации.

По свидетельству тех же авторов, конструкция алгоритма PRNG оставалась неизменной вплоть до Windows XP. При вскрытии схемы генератора в Win2000 израильтяне, правда, установили, что это не совсем так – некоторые модификации были, причем далеко не в лучшую сторону.

Но в любом случае трудно не поражаться, что алгоритм Windows PRNG – несомненно, самого распространенного в мире криптогенератора – оставался не вскрытым и никем не проанализированным на протяжении полутора без малого десятка лет.

Объяснить этот факт проще всего тем, что защиту в Windows удавалось вскрывать все эти годы и без знания работы генератора. Нагляднее всего, наверное, данное утверждение иллюстрируется на примере пакета MS Office. Историческая шкала эволюции которого плотно привязана к версиям ОС Windows, а потому и криптография примерно та же самая.

В процессе данной эволюции криптосредства для защиты информации претерпевали здесь, бесспорно, весьма серьезные усовершенствования. Однако на словах и безопасность, и этапы ее усиления всякий раз выглядели существенно иначе, нежели на деле.

В самом первом продукте, MS Office 95, скажем, уже имелись возможности шифрования документов. Но реально это шифрование сводилось к циклическому сложению (побитовой операцией XOR) пароля пользователя с текстом документа.

То есть с точки зрения криптоанализа и вскрытия никакой реальной защиты в действительности не обеспечивалось, а создавалась лишь ее видимость – превращение читаемого текста в нечитаемый.

Применение шифров из детского арсенала бойскаутов в тот период, когда миру уже была прекрасно известна программа PGP – символ общедоступного и очень сильного крипто – это, конечно, не злой умысел (или невежество) со стороны Microsoft.

Просто все предыдущие годы и десятилетия стойкие криптосредства подразумевались американскими законами столь же опасным военным товаром, как наступательные виды оружия, а значит – подлежащими строжайшим экспортным ограничениям на торговлю…

В течение 1990-х годов, впрочем, эти драконовские законы были существенно ослаблены. Вместе с их изменением заметно менялась и стойкость криптографии в версиях Windows / MS Office.

В частности, в последующих версиях программ начали применять вполне качественный поточный шифр RC4. В ранних экспортных версиях ПО, правда, длина ключа ограничивалась всего лишь 40 битами. При такой длине ключа, как известно, шифры без проблем вскрываются на ПК просто лобовым (тотальным) перебором всех возможных ключевых комбинаций.

Но затем, вместе с коррективами в экспортных законах, к концу 1990-х уже всем пользователям новых версий Microsoft Office в принципе стали доступны теоретически стойкие шифрсредства, в частности, RC4 с длиной ключа 128 бит. Вот только на практике предположительно сильный шифр оказался реализован так, что надежной защиты данных с его помощью все равно не получалось.

Среди фундаментальных основ криптографии имеется очень важное правило: если для засекречивания используется поточный шифр (наложение на открытый текст постоянно изменяющейся шифрпоследовательности), то никогда одну и ту же шифрпоследовательность не накладывают на два разных документа.

Причем в данном контексте к принципиально «разным» документам могут приводить любые модификации файла, включая вставку или изъятие единственного знака. Если же это сделано, то всего по двум (если больше, то вскрытие еще проще) одноключевым документам шифрование можно развалить и прочитать оба текста – причем собственно ключ и его длина тут никакой роли не играют.

В годы Второй мировой войны, скажем, английские криптоаналитики из-за такого рода ошибок германских шифровальщиков смогли не только читать важную переписку командования Вермахта, но и полностью вскрыть криптосхему применявшегося шифратора «Шлюссельцузатц». Что затем, с помощью «суперкомпьютера» Colossus, позволило им вскрывать ключи и читать всю переписку уже без одноключевых комплектов (подробности этой истории см. тут).

В программных же продуктах Microsoft шифр RC4 изначально был реализован таким образом, чтобы одноключевые комплекты порождались ВСЕГДА. Ключ без затей генерировался на основе пароля доступа к документу, поэтому разные версии документа оказывались зашифрованы одним и тем же ключом.

Как известно, разные версии одних и тех же файлов присутствуют в системе очень часто – в резервных кэшах, как архивные копии, как совместно подготавливаемые документы и так далее.

Для этих и любых других накладок в криптографии широко известен элементарнейший способ недопущения одноключевых комплектов – подмешивание в ключ наряду с паролем уникального, одноразового «вектора инициализации» (IV), который не является секретом, но всякий раз делает шифрпоследовательность иной.

То, что в Microsoft почему-то уклоняются от использования в поточном шифре IV, впервые стало известно в 1999 году еще для ОС Windows NT – когда хакеры обнаружили слабости в системе защиты криптоключей Syskey.

Серьезные недочеты в реализации криптографии допускаются регулярно и почти всеми разработчиками (см. врезку о WEP), однако в Microsoft не только проигнорировали тревожные сигналы, но и бережно перенесли ту же самую слабость в последующие версии системы.

В частности, в 2005 году, когда уже вышли Windows XP и MS Office 2003, стало известно [eprint.iacr.org/2005/007], что все та же по сути уязвимость – отсутствие IV и систематическое порождение одноключевых комплектов – выявлена в документах, подготовленных и зашифрованных программами Microsoft Word и Excel с помощью RC4.

В принципе, в качестве вектора инициализации можно использовать самую разную информацию – хоть системный штамп о текущих дате-времени. Но с точки зрения криптографии наиболее грамотное решение – вырабатывать IV с помощью генератора псевдослучайных чисел.

И если на протяжении многих лет имевшийся в системе PRNG явно игнорировался с очевидным ущербом для безопасности, то крайне сложно поверить, будто сделано это неумышленно.

Впрочем, и в тех ситуациях, когда PRNG используется для генерации секретных ключей или других криптопоследовательностей, делается это весьма небезопасным образом.

Слабость спереди и сзади

Качественный с точки зрения криптографии генератор псевдослучайных чисел должен отвечать трем главным требованиям: (1) выдавать последовательность, статистически неотличимую от случайной равновероятной; (2) противостоять восстановлению прошлых состояний по известному; (3) противостоять восстановлению будущих состояний по текущему состоянию алгоритма.

Нет никакого секрета в том, каким образом можно эффективно достигать все три нужных качества. Из этого, правда, не следует, что конструировать хорошие генераторы легко (см. врезку). Но если PRNG просто генерирует последовательность чисел, похожую на случайную, но явно не отвечает требованиям (2) и (3), то с точки зрения криптографии это слабый и небезопасный генератор.

Именно такой, увы, является схема алгоритма PRNG, использованного во всех версиях Windows вплоть до XP и ныне вскрытого коллективом израильских криптоаналитиков в работе, упомянутой в самом начале.

Этот генератор также построен на основе RC4. И коль скоро всякий приличный поточный шифр дает на выходе последовательность чисел, статистически неотличимую от равновероятной, то и генератор на его основе вполне отвечает требованию (1). Но вот дальше начинаются очень неприятные моменты конкретной реализации PRNG.

Чтобы обеспечить свойство (2) – не допустить восстановление прошлых состояний – в качестве тактов генерации принято использовать однонаправленные (хэш-)функции, легко вычисляемые только в одну сторону. В Windows же обратная функция вычисляется столь же просто, как и прямая генерация следующего состояния.

Такая же унылая картина установлена и для свойства (3). Дабы воспрепятствовать восстановлению будущих состояний криптогенератора, в его детерминированные алгоритмом состояния регулярно вводят так называемую рандомизацию – то есть обновляют случайно взятой последовательностью бит от какого-нибудь внешнего источника. Чем короче длина последовательности, генерируемой на выходе PRNG между такими «перезагрузками», тем выше криптостойкость генератора.

Хотя общая схема PRNG в Windows не менялась, в ранних версиях ОС длина между перезагрузками состояний составляла 512 байт, а в Win2000 – как установили израильтяне – она стала уже 16 килобайт. Если же учесть, что PRNG здесь реализован на основе 8 потоков от работающих в параллели шифров RC4, то получается, что реаль-

но длина генерируемой криптопоследовательности между перезагрузками состояний составляет 128 килобайт.

Иначе говоря, определив всего одно внутреннее состояние генератора (например, с помощью известного трюка с переполнением буфера памяти), злоумышленник далее может сам вычислить огромное количество ключей – как уже использованных в криптоприложениях прежде, так и на будущее.

Хуже того, перезагрузка состояний произойдет лишь в том случае, когда все эти 128 килобайт сгенерированы между включением и выключением компьютера. В терминах защищенных SSL-соединений веб-браузера это, огрубленно, означает от 600 до 1200 сеансов шифрованной связи.

Понятно, что для всякого обычного компьютера это нереально огромное число. Иными словами, в большинстве случаев криптогенератор вообще никогда не перезагружает свои состояния, так что всего одной «израильской атакой» можно восстановить по сути ВСЕ генерируемые им ключи – как вперед, так и назад.

В терминах корпорации Microsoft, напомним, этот мелкий недочет в конструкции не тянет даже на то, чтобы именоваться «уязвимостью». В терминах же криптографии это называется катастрофическое снижение стойкости, которое просто не могло появиться случайно.

Ситуация с ОС Vista

В новой системе Windows Vista, как многократно подчеркивалось разработчиком по самым разным поводам, защита информации реализована существенно иначе и на основе других алгоритмов.

Отчасти это сделано в угоду всемогущей индустрии контента – для надежной защиты файлов от бесконтрольного копирования пользователями. В другой же, не менее важной части – чтобы обеспечить интересы Агентства национальной безопасности США.

Тесное сотрудничество Microsoft с АНБ при разработке Vista является официально известным фактом [подробнее см. БОЛЬШАЯ ЖрАТВА], однако как именно интересы этой крупнейшей в мире разведслужбы были здесь учтены, в объявлении скромно умолчали. Хотя секрет этот относится к тому типу, что, как говорится, известен всем.

АНБ всегда – и в период холодной войны, и в 1990-е годы смягчения экспортных ограничений, и, тем более, в последующие годы войны с терроризмом – очень ревниво боролось с сильной криптографией на рынке. Понижая ее стойкость в продуктах разработчиков любыми способами. От кнутов-санкций для строптивых до технических хитростей-закладок и пряников-контрактов с правительственными ведомствами для лояльных.

Корпорация масштабов Microsoft нелояльной к правительству США быть просто не может по определению. Так что очевидно слабая криптография в ее продуктах – это своего рода дань уважения государству, которое считает себя просто обязанным все про всех знать.

В условиях же ОС Vista, где сильная криптография ныне с необходимостью должна присутствовать из-за требований партнеров по индустрии и пользователей из большого бизнеса, разведывательные интересы АНБ пришлось учесть, вероятно, более элегантным способом, нежели «неумелая» и слабая реализация известных криптосхем.

Иначе говоря, в условиях беспощадной войны с мировым терроризмом на массовый рынок общедоступных коммерческих программ просто в принципе не мог бы попасть американский продукт с непробиваемой криптографией.

«Черный ход» для себя, по крайней мере, АНБ наверняка там имеет. Ну а уж найдут ли его независимые исследователи – это другой вопрос.

Решаемый, как показывает опыт, иногда довольно долго.

# # #

[ВРЕЗКА]

WEP или слабый эквивалент приватности

Стандарт криптозащиты WEP, введенный для беспроводных сетей WiFi, иногда неверно расшифровывают как Wireless Encryption Protocol или «Протокол беспроводного шифрования».

На самом деле буквы названия означают Wired Equivalent Privacy, т.е. «Приватность, эквивалентная проводным сетям». Уже само имя дает основание предполагать, что защита, обеспечиваемая таким шифрованием, вряд ли обладает высокой стойкостью к атакам.

На первый взгляд, впрочем, все выглядело весьма пристойно. Хорошо исследованный и вполне качественный шифр RC4, своевременно увеличенная с 64 до 128 бит длина ключа – все эти базовые характеристики позволяли сделать добротную и достаточно надежную схему защиты.

Однако в конкретной реализации RC4 для WEP, особенно в алгоритме разворачивания ключа, аналитики вскоре нашли серьезные слабости, ощутимо понижающие стойкость системы. Начиная с 2001 года эффективность атак на WEP и скорость вскрытия ключей понемногу довели с нескольких часов до нескольких минут.

Апофеозом же этой работы можно считать наглядную демонстрацию в апреле 2007 года, когда трое исследователей из германского университета Дармштадта на одной из конференций по инфобезопасности вскрывали ключи «защищенной» с помощью WEP сети менее чем за 3 секунды. То есть по сути дела моментально.

И хотя с 2003 года для защиты беспроводных сетей разработаны и применяются существенно более стойкие протоколы WPA и WPA2, изготовителями сетевого оборудования стандарт WEP по-прежнему ставится первым в списках возможных опций для средств безопасности.

Вследствие этого, как показали исследования, проводившиеся в текущем году в Германии, около половины всех WiFi-сетей используют для защиты откровенно слабый WEP, и лишь чуть больше четверти – WPA. Остальные, правда, не применяют никакой защиты вообще.

[КОНЕЦ ВРЕЗКИ]

[ВРЕЗКА]

Криптогенератор – это непросто

Из того, что критерии, предъявляемые к качественному криптографическому генератору случайных чисел, хорошо известны, вовсе не следует, что сконструировать его проще простого. В истории криптографии имеется достаточно много случаев, когда слабости находили и в новых схемах известных авторов, и в уже известных алгоритмах, успевших получить распространение.

Например, в 1996 году одна из ранних версий протокола SSL была взломана именно из-за слабостей в генераторе случайных чисел. Совсем недавно были обнаружены криптографические слабости в PRNG операционных систем Linux и FreeBSD, всегда открытых для анализа.

По этой причине многие разработчики средств защиты весьма благосклонно восприняли инициативу НИСТ, американского Института стандартов и технологий, подготовившего и опубликовавшего недавно большой, на 130 страниц документ под названием NIST Special Publication 800-90, целиком посвященный генераторам псевдослучайных чисел. В этом документе, где они именуются DRBG или Deterministic Random Bit Generators, содержатся описания 4 изученных и рекомендуемых к применению генераторов разных конструкций.

Все четыре схемы построены на основе уже существующих криптографических примитивов, что принято считать плюсом. Один на основе хэш-функций, другой на основе HMAC или хешированного кода аутентификации сообщения, третий на основе блочных шифров, четвертый – на эллиптических кривых.

С последним, «эллиптическим», правда, вышел серьезный конфуз по целому ряду причин. В отличие от трех первых, где примитивы уже хорошо изучены и проверены криптографическим сообществом, этот был предложен совсем недавно, около года назад Агентством национальной безопасности США.

Алгоритм по независимым оценкам ничем хорошим не отличается, имеет мутную и не разъясненную разработчиком конструкцию, работает существенно медленнее остальных трех. Да еще в придачу несет в себе, как уже установлено, явные признаки математической закладки, с помощью секретных констант позволяющей взламывать генератор на лету.

Зачем в стандарты НИСТ включен столь сомнительный «подарок», в общем-то понятно. Но не факт, что хоть кто-то захочет по доброй воле им воспользоваться.

[КОНЕЦ ВРЕЗКИ]

# # #

Объяснимые слабости

(Январь 2008)

Среди отечественных филологов и лингвистов уже давно гуляет шутка о том, сколь существенный вклад внесла в русский язык уголовная братва.

В языках вроде английского или немецкого, как известно, есть такая вещь, как неопределенные и определенные артикли перед существительными. В русском языке артиклей, ясное дело, нет. Очевидную же их полезность все осознали лишь в 1990-е годы, когда криминальный мир не только мощно влился в слой новой русской буржуазии, но и заметно обогатил всеобщий бытовой лексикон. Так что с адекватным переводом иностранных артиклей теперь все стало очень просто.

Например, английское «the table» – это «конкретно стол», а вот «a table», соответственно, оказывается «типа стол». Разница в смысле слов, как видим, вполне очевидна.

В данной же статье речь пойдет о «**чисто конкретной криптографии**».

НЕ ПРОСТО ДЫРА

В декабре прошедшего (2007) года небольшая швейцарская фирма Dreamlab Technologies AG, специализирующаяся на компьютерной безопасности, объявила миру о выявленной ею серьезнейшей слабости в беспроводных клавиатурах. Большую статью с описанием подробностей этой истории можно найти на сайте компании www.dreamlab.net, здесь же вполне достаточно изложить лишь суть.

А суть такова, что изготовители бесшнуровых клавиатур (львиная доля которых приходится на Microsoft и Logitech) по какой-то причине упорно пренебрегают криптографической защитой информации.

Иначе говоря, пользователи почти любой беспроводной клавиатуры, связывающейся с компьютером по радиоканалу на частоте 27 МГц, должны четко себе представлять, что когда они нажимают на кнопки, то вся вводимая информация свободно доступна окружающим в радиусе нескольких десятков метров. А если любопытствующая сторона вооружена приличной антенной, то можно говорить и о многих сотнях метров.

Исследователи Dreamlab, проанализировавшие протокол передачи клавиатур типа Wireless Optical Desktop фирмы Microsoft, установили, что конкретно в данном семействе вся защита канала заключается в прибавлении к каждому коду клавиши одного и того же числа-байта.

Это число случайно выбирается из 256 возможных вариантов при самом первом сеансе связи между клавиатурой и компьютером в процессе синхронизации устройств. Строго говоря, называть эту уловку «защитой» можно лишь с очень большой натяжкой. Ибо в терминах криптографии подобное преобразование именуется простой заменой, в сути своей известно школьникам младших классов и по сложности обратного восстановления (дешифрования) практически не отличается от чтения открытого кода передачи.

Формулируя то же самое чуть иначе, можно сказать, что в беспроводных клавиатурах, выпускаемых индустрией без усиления защиты уже многие годы, имеется не просто дыра, а чудовищная уязвимость с точки зрения безопасности.

Дыру эту никак нельзя назвать случайной и можно приводить в качестве своего рода символа определенных воззрений на криптографию. Согласно которым широкой публике разрешено пользоваться лишь откровенно слабыми шифрами, не составляющими абсолютно никаких проблем для компетентных органов.

БЫЛА ВОЙНА

Чтобы стало яснее, как появилась и утвердилась столь своеобразная, а на сегодняшний день еще и очень влиятельная точка зрения, понадобится совершить небольшой экскурс в историю.

Отправной точкой станут первые годы холодной войны, когда политические лидеры Запада были крайне озабочены гигантской военной мощью СССР, только что сумевшего победить нацистскую Германию. А также вполне объяснимой популярностью коммунистических идей среди населения и партий, стремившихся к власти в странах вне советского блока.

В такой обстановке руководство США направило в Европу с секретной миссией Уильяма Фридмена, одного из основателей спецслужбы АНБ и просто авторитетнейшего специалиста-криптографа, имевшего хорошие связи в западноевропейских разведках еще с Первой мировой войны (подробности необычной биографии Фридмена можно найти тут: «Наука a la Ривербэнк«).

Миссия Фридмена, впрочем, подразумевала тайные встречи не столько с коллегами из спецслужб, сколько с ведущими компаниями криптографической индустрии Европы. Ибо после войны в мире отчетливо обозначился высокий спрос на современные шифраторы – для закрытия важных коммуникаций не только в военных, но и в дипломатических, банковских и промышленных системах связи.

Собственную криптоиндустрию имели по преимуществу лишь наиболее мощные державы, вроде Англии, Франции или Германии. Однако все они входили в однозначно проамериканский блок НАТО, а многие неприсоединившиеся страны имели вполне разумные основания не доверять криптографии, сработанной в одном из враждующих блоков.

По этой причине в нейтральных странах вроде Швейцарии или Австрии сложились очень благоприятные условия для деятельности независимых криптофирм, шифраторам которых все могли бы доверять свои секреты примерно так же, как доверяют деньги швейцарским банкам.

Именно такого рода компании, в частности в Швейцарии, и посетил Уильям Фридмен в ходе своей важной миссии в 1950-е годы, сумев до какой-то степени убедить их руководство в целесообразности тайного сотрудничества с США в лице спецслужбы АНБ. Известно об этих сверхсекретных соглашениях, заключенных явно в страхе перед коммунистами и обговоривших слабости-закладки в шифраторах, стало лишь много-много времени спустя.

Главным образом, информация об этом всплыла в 1990-е годы, когда целый ряд независимых расследований журналистов в разных странах позволил сложить в общую картину множество разрозненных эпизодов.

Каждый из подобных эпизодов документально рассказывал то о тайных встречах Фридмена в Швейцарии (откуда он вернулся, кстати говоря, в крайне подавленном состоянии, увидев красивую жизнь миллионеров, сделавших состояния на шифраторах, абсолютно ничем не лучших того, что изобретал для армии США – по сути бесплатно – сам Фридмен).

То о странных трансформациях криптосхем, разрабатывавшихся вроде бы собственными сотрудниками европейских фирм, однако на каком-то этапе получавших необъяснимую модификацию от «непонятно кого».

То, наконец, о кадровых сотрудниках АНБ, в 1960-70-е годы прикомандированных к швейцарским фирмам с задачами, категорически не подлежащими обсуждению и комментариям…

ПРОЦЕСС ПОШЕЛ

К началу 1970-х годов уровень компьютерной индустрии США вырос настолько, что здесь родилась идея о разработке собственной приличной криптографии без помощи АНБ. Ибо все сильные технологии шифрования, разработанные или одобренные Агентством национальной безопасности, несли на себе печать гостайны, абсолютно не подлежащей разглашению. А в законах, регулирующих экспорт, шифрсредства были приравнены к наступательным вооружениям и поэтому их продажа жестко контролировалась тем же АНБ.

Для компьютерной же индустрии и начинавших бурное развитие сетевых коммуникаций остро требовался единый криптографический стандарт – быстрый, достаточно надежный и стойкий ко взлому, но в то же время общедоступный для всех, то есть открытый в своей конструкции.

Примерно в таких исторических обстоятельствах в стенах фирмы IBM родился знаменитый ныне алгоритм DES. Новый криптостандарт блочного шифрования был построен на основе так называемой «сети Фейстела» – замечательного криптопреобразования, придуманного инженером-криптографом корпорации Хорстом Фейстелом. И, надо подчеркнуть, совершенно не похожего на поточные шифры, реализованные в подавляющем большинстве военных и дипломатических шифраторов того времени.

Главная разница, в двух словах, заключалась в следующем. Традиционные поточные шифры исторически ориентировались на телеграфные аппараты и перфоленту, где в каждом такте работы обрабатывался-шифровался один знак текста. В DES же, изначально ориентированном на обработку компьютерных данных, алгоритм оперировал «словами», т.е. стандартной длины наборами бит для регистров процессора, а эти слова сцеплялись в блоки, подлежащие шифрованию.

Для DES размер блока был выбран длиной в 64 бита, т.е. 8 знаков текста в терминах 8-битного кода ASCII, которые под управлением криптоключа единым махом перетряхивались и перемалывались для получения блока шифртекста такой же длины.

О криптоключе DES надо сказать особо, поскольку его «кривая» длина в 56 бит по сию пору вызывает недоумение у любого человека, мало-мальски знакомого с миром компьютеров и знающего, что там по естественным причинам предпочитают длины, кратные степени двойки (16, 32, 64, 128, …).

Шифр Фейстела «Люцифер», положенный в основу DES, имел естественную длину ключа 128 бит. Когда к рождению всеобщего криптостандарта на определенном этапе

подключилось АНБ, ключ поначалу сократился до 64 бит, а затем и до противоестественных 56. Которые и закрепились в схеме DES навсегда.

Чтобы хоть как-то объяснить этот трюк с укорачиванием ключа причинами, похожими на рациональные, был изобретен аргумент о необходимости добавления 8 проверочных битов в стандартный 64-битный блок ключевой последовательности. Ни до, ни после DES, сколько помнится, к подобной экзотической аргументации больше не прибегали, однако публике пришлось это съесть безоговорочно.

Потому что DES реально оказался превосходным для своего времени шифром, на примере которого обучают мастерству уже которое поколение криптографов.

Если не говорить о медленной программной реализации (на которую, собственно, DES и не был изначально рассчитан, подразумевая аппаратное воплощение в микросхеме), то единственная слабость алгоритма с точки зрения криптографии свелась к его малой длине ключа. Которая, как можно видеть, была шифру искусственно навязана извне.

Хотя официально это никогда не признавалось, известны кулуарные свидетельства бывших сотрудников или подрядчиков АНБ, согласно которым агентство с самого начала имело возможность быстро вскрывать DES в лоб. Но стоило это чудовищных затрат памяти и компьютерных ресурсов для предварительных вычислений.

Гигантских объемов запоминающее устройство – сначала на магнитных лентах, а затем на оптодисках – содержало отсортированные по порядку блоки шифртекста, представлявшие собой некую служебную последовательность байтов, заранее зашифрованную суперкомпьютером на всех возможных DES-ключах. В силу специфики работы вычтехники, в формате файлов почти всегда имеются такого рода скрытые или явные служебные последовательности, причем на вполне определенных местах.

Поэтому для вскрытия и чтения нужного файла, зашифрованного с помощью DES, специалистам АНБ обычно было достаточно взять блок (8 байт) шифртекста на определенном месте, быстро найти его в отсортированном массиве памяти и тут же, словно по известному адресу, узнать соответствующий ему ключ, использованный для зашифрования всего файла.

Следует особо подчеркнуть, что лобовое вскрытие ключа длиной 56 бит для большинства сторон представляло собой непреодолимую, воистину гигантской сложности вычислительную задачу не только в конце 1970-х, но и на протяжении еще нескольких десятилетий. И то, что было под силу спецвычислителям самой мощной в мире криптослужбы АНБ, еще долго оставалось совершенно недоступно, скажем, ФБР, не говоря уже о других правоохранительных органах или полиции на местах.

Да и для АНБ, надо сказать, быстрое и широкое распространение DES в самых разных приложениях в течение 1980-х годов оказалось неприятной и весьма обременительной неожиданностью. Шифр был все же слишком хорош, так что большие объемы требующих вскрытия материалов стали ощутимо напрягать небезграничные ресурсы даже этой спецслужбы.

Как признавали впоследствии ответственные чины агентства, они дали принципиальное согласие на публикацию схемы DES, будучи уверенными, что шифр предназначен исключительно для зашивания в чипы. Предполагалось, что общее описание криптоалгоритма не будет настолько подробным и полным, чтобы обеспечить его корректную программную реализацию.

Так что в каком-то смысле можно говорить, что отличный шифр DES достался миру в результате бюрократической ошибки инстанций.

В ДВИЖЕНИИ СЛОВНО В ПОКОЕ

В АНБ, естественно, довольно быстро осознали свой промах, который стал быстро разрастаться в проблему катастрофических размеров вместе с началом эры персональных компьютеров. То есть аппаратов, потенциально предоставлявших каждому человеку средство для удобного шифрования информации с любыми уровнями стойкости, вплоть до абсолютно невскрываемого.

Ибо в массах стали появляться и «тройной-DES» с неподъемной даже для АНБ длиной ключа 112 бит, и другие весьма качественные блочные шифры вроде швейцарского IDEA.

По этой причине в конце 1980-х годов с подачи АНБ в США была предпринята тотальная законодательная атака, попытавшаяся в принципе сделать нелегальной и уголовно наказуемой любую сильную криптографию в распоряжении обычных граждан. Поборники этой инициативы, правда, абсолютно не учли тогдашнюю степень чувствительности нации к попыткам ограничения свободы, а потому драконовский законопроект с треском провалился.

Побочным же продуктом данного конфликта стало рождение знаменитой криптопрограммы PGP, которую гражданский активист и программист Фил Зиммерман написал, а затем тут же начал широко распространять в компьютерных сетях – в качестве личного протеста против угрозы запрета на сильное крипто.

Зиммермана, как известно, государство попыталось (к счастью, безуспешно) посадить в тюрьму «за нарушение экспортных законов». А в АНБ тем временем родили другую идею – так называемый клиппер-чип. То есть аппаратный шифратор, встраиваемый для начала во все телефоны, а в перспективе и во все компьютеры. Дабы граждане имели возможность конфиденциально общаться, а государство, соответственно, имело

встроенный в криптографию «черный ход», обеспечивающий прослушивание коммуникаций в случае нужды.

С этой сомнительной инициативой, ясное дело, тоже абсолютно ничего не выгорело, и под давлением мощных протестов общественности администрация Клинтона была вынуждена проект зарубить на самой начальной стадии, в середине 1990-х.

И вот тогда в действие была запущена та самая стратегия регулирования криптографии, которая успешно функционирует вплоть до сегодняшнего дня. Строго говоря, в сущности своей она ничем не отличается от того, что на другом уровне обеспечил патриарх АНБ Уильям Фридмен в 1950-е, в ходе своей тайной швейцарской миссии.

Или от того, что было сделано в конце 1980-х с криптографией, встроенной в европейскую систему мобильной связи GSM (см. «Что показало вскрытие»). Где имеется достаточно приличный, по общей идее, криптоалгоритм A5 с длиной ключа 64 бита. Однако, по настоянию разведслужб, реализованный так, чтобы имелись разные способы ослабления защиты конфиденциальных переговоров.

Иначе говоря, как показало вскрытие GSM-криптографии независимыми хакерами в конце 1990-х, несколько важных элементов неплохой изначально криптосхемы принудительно ослаблены, что понижает общую стойкость шифра на много порядков и знающим специалистам позволяет его вскрывать практически «влет», одновременно с эфирным перехватом разговоров.

В самой примитивной форме эту стратегию контроля реализуют элементарным укорачиванием ключа, оставляя рабочими бит 40 или чуть больше-меньше, а остальные принудительно забивая нулями или оставляя постоянными. В 1990-е годы лишь такую длину, легко вскрываемую лобовым перебором, разрешали для американских криптосредств экспортные законы США.

Когда же этот порог был формально повышен, в реальных системах рабочую длину ключа все равно оставляли укороченной, особенно когда это можно было сохранить в тайне. Как это сделано, к примеру, в крипточипах противоугонных автомобильных систем.

В применяемых и поныне системах на основе RFID-чипов DST фирмы Texas Instruments длина ключа составляет всего 40 бит, а в системах на основе KeeLoq фирмы Microchip, где общая длина ключа 64 бита, реально работают и изменяются при каждом сеансе лишь 28 бит (подробности см. «Ключи, замки, отмычки«).

В несколько более изощренной форме эта же стратегия может принимать форму криптоалгоритмов с любой, в принципе, рабочей длиной ключа, но функционирующих таким образом, что для грамотного вскрытия этот ключ и отыскивать-то не нужно. Об-

ходясь ключами эквивалентными, которые либо вычисляются гораздо легче, либо вообще известны заранее.

В самой яркой и наглядной версии этот подход можно проследить на примере защиты контента на видеодисках – как в системе CSS DVD, так и в «продвинутой системе» AACS для дисков высокой четкости HD DVD и Blu-ray.

Систему CSS разрабатывали, как известно, специалисты уважаемой фирмы Intel, где давно и прекрасно знают, что такое грамотная защита информации. В итоге же у них получилась криптосхема, защиту которой современные хакерские программы снимают столь легко, что многие нынешние пользователи, копируя видеодиски, порой даже не понимают, что взламывают систему, некогда предполагавшуюся очень сильной.

Почему так вышло, официально никто не объяснял. Однако в кулуарах Сети давно гуляют анонимные признания сотрудников фирмы, согласно которым Intel просто «вынудили» реализовать слабую криптозащиту, понадеявшись на сохранение схемы в тайне. Что же касается взлома AACS и обнаружения хакерами универсального «ключа обработки», подходящего для отпирания всех дисков, то об этом лучше рассказывать отдельно и с подробностями.

Список не просто слабой, а чудовищно слабой криптографии, похожей на вполне достойную и реализованной во множестве популярнейших программ, от криптопротокола WEP для защиты WiFi до криптогенератора случайных чисел во всех версиях Windows вплоть до XP, можно продолжать и продолжать (см. «Хитрости крипторемесла»). Однако общая суть происходящего, вероятно, уже ясна.

У специалистов АНБ имеются два особых термина, характеризующих степень доступности добываемой информации для разведки. Один, «**info at rest**» или «информация в покое», обозначает открытые данные, когда они вводятся с клавиатуры или считываются с экрана. Другой же, «**info in motion**» или «информация в движении», обозначает противоположное состояние, когда данные обработаны криптографией для передачи или хранения.

И в идеале, по мнению спецслужб, у всех обычных граждан и врагов государства (а также, желательно, и у союзников) применяемая криптография в реальности должна быть примерно такого уровня, чтобы в случае нужды не было принципиальных различий между информацией «в покое» и «в движении». То есть, по сути, сама криптосхема может играть роль шпионской закладки, но уже без возни и усилий, требуемых для установки, скажем, программы-кейлоггера (перехватчика нажатия клавиш) в каждый конкретный компьютер.

КАК ЭТО ВСЕ НАЗЫВАТЬ?

Подводя же общий итог, можно так сформулировать главное отличие между двумя базовыми разновидностями криптографической науки.

Если «a cryptography» по определению сосредоточена на создании все более стойких и надежных схем защиты информации, то «the cryptography», напротив, всецело посвящена тому, как из сильного шифра сделать слабый. Но сделать это требуется так, чтобы слабость была как можно менее заметной и, в случае обнаружения, походила на случайные баги, допущенные по недосмотру или невежеству.

Однако для посвященных «the crypto» обеспечивает легкий и быстрый доступ к любой зашифрованной информации без знания ключей, применявшихся владельцем. В русском языке для такой науки прекрасно подходит название «**чисто конкретная криптография**».

P.S. на всякий случай. Лингвистические новации – это, конечно же, шутка. Но зато все остальное – реальное положение дел. Что же касается действительно сильных криптосредств, то они, несомненно, тоже имеются. Но это уже совсем другая история.

# # #

Хакинг чипов Mifare

МАЛЕНЬКИЕ СЕКРЕТЫ БОЛЬШИХ ТЕХНОЛОГИЙ

(*Январь 2008*)

Новая система проездных чип-карт, вводимая ныне в Голландии для универсальной оплаты проезда в общественном транспорте от автобусов и трамваев до железной дороги, оказалась намного менее защищенной, чем ожидалось.

На создание технологически продвинутой системы была затрачена внушительная сумма в 2 миллиарда евро, ощутимая даже для совсем небедных Нидерландов, однако уже три, по крайней мере, независимых исследования продемонстрировали очевидную небезопасность конечного продукта.

В целом новая система транспортных билетов, получившая название OV-chipkaart, построена на основе бесконтактных смарт-карт с RFID-чипом. Пассажир может купить или разовую картонную карточку на 1-2 поездки, или постоянную пластиковую карту для регулярной езды.

Для оплаты проезда карточку прикладывают к окошку-ридеру турникета как при входе, так и при выходе из транспорта, поскольку ридер проводит не только аутентификацию карты, но и снимает из памяти чипа разные суммы за разные поездки.

Разовая картонная и постоянная пластиковая карты построены на основе существенно разных технологий. Чип дешевой разовой карты, именуемой Mifare Ultralight, совсем прост по устройству и не имеет никакой криптографии вообще.

В постоянной пластиковой карте, или Mifare Classic, реализована существенно более серьезная защита информации. Но на деле, увы, куда менее безопасная, чем можно было бы ожидать при нынешнем уровне индустрии.

Первая известная атака – на проездные карты Ultralight – была опубликована в июле 2007 г. двумя голландцами (Pieter Sieckerman, Maurits van der Schee) из Амстердамского университета. Суть атаки свелась к тому, что память чипа оказалось возможным «перематывать» в предыдущее состояние, так что по одноразовой карте в принципе можно было ездить сколько угодно в пределах срока ее действия.

Исследователи показали, что эту очевидную дыру совсем несложно залатать, слегка подправив программное обеспечение системы. Но одновременно было установлено, что с умом сконструированная хакерами контрафактная карта Ultralight сможет постоянно обманывать ридеры, а отследить и заблокировать ее чрезвычайно сложно.

Фундаментальная проблема слабости одноразовых карт Ultralight в том, что они не имеют криптографии. Поэтому чип карты не способен утаить никаких секретов от атакующей стороны.

С помощью совсем недорогого оборудования злоумышленник может свободно считать RFID-чип, получить всю хранимую в нем информацию и без проблем изготовить другое устройство, идентичное исходной карте. С тем лишь отличием, что контрафактная карта будет постоянно сама возвращаться в полностью оплаченное состояние.

Студент другого голландского университета, Роэл Вердулт (Roel Verdult), недавно практически реализовал идею клонирования Mifare Ultralight как часть своей дипломной работы, затратив на устройство порядка 40 евро.

В начале года об изысканиях Вердулта рассказало национальное телевидение, передача получила большой резонанс, а студента пригласили выступить аж в парламенте. Многим депутатам захотелось в подробностях узнать, насколько слабой в реальности оказалась система, стоившая 2 миллиарда.

(В сетевых комментариях по этому поводу завистливые американцы отметили, что будь дело в США, инициативного студента уже давно повязали бы и отправили бессрочно куда-нибудь типа тюрьмы Гуантанамо – как пособника террористов.)

В более серьезные проездные карты Mifare Classic встроен чип с криптографией. Здесь для защиты информации имеются секретные ключи, используемые при аутентификации карты ридером. Поэтому в лоб клонировать такую карту злоумышленник не может.

Однако в качестве алгоритма шифрования, на основе которого построена безопасность системы, выбран не общеизвестный сильный криптоалгоритм, а засекреченный

фирменный (изготовителем карт Mifare является компания NXP, подразделение гиганта Philips).

Давным-давно известно, что уповать на секретность шифра – дело зряшное и безнадежное. В декабре прошлого года группа германских хакеров (Karsten Nohl, Starbug, Henryk Ploetz) на конференции 24CCC объявила о том, что завершила обратную инженерную разработку криптоалгоритма карты Mifare Classic – открыв чип и сделав для анализа снимки электронных схем в высоком разрешении.

Полное описание восстановленной криптосхемы публиковать из осторожности не стали, но и раскрытой информации вполне достаточно, чтобы слабость использованного в карте шифра стала очевидна для всех.

Хотя в семействе Mifare имеются заведомо более безопасные карты (например, применяемая в других странах Европы DESfire на основе стойкого шифра тройной-DES), для голландской транспортной системы по неизвестным пока причинам выбрали Mifare Classic с проприетарным шифром и ключом 48 бит.

Даже если этот шифр конструктивно хорош и не вскрывается быстрой атакой (что не факт), очевидно короткая длина ключа не в силах противостоять тотальному перебору всех возможных комбинаций. Их число, около 280 триллионов, может показаться довольно большим, однако при современных возможностях вычтехники на простое лобовое вскрытие ключа уйдет несколько дней или даже часов.

Если же воспользоваться хорошо освоенной технологией предвычислений и заранее подготовить данные на емком жестком диске, то вскрытие произвольного 48-битного ключа становится минутным делом…

Бурные дискуссии в Сети по поводу очевидных слабостей в защите новой голландской системы попутно вскрыли несколько малоизвестных фактов.

Например, что проездные, а теперь и платежные RFID-карточки знаменитой лондонской системы Oyster построены на основе тех же чипов Mifare Classic. Что карты такие хоть и неважно защищены, но зато хранят в своей памяти информацию о последних 35 поездках.

И что – самое интересное – голландская система подразумевает централизованное хранение информации обо всех маршрутах поездок по каждой пластиковой карте, оформляемой на человека персонально, в течение 7 лет.

Иначе говоря, есть основания полагать, что удешевленная и упрощенная защита карточек – это своего рода плата за обеспечение обостренных интересов государства ко всем перемещениям своих граждан.

* * *

И ГРЯНУЛ ГРОМ

(*Март 2008*)

Министр внутренних дел Нидерландов Хюшье тер Хорст (Guusje ter Horst) официально проинформировала парламент страны о серьезной компрометации защиты в бесконтактных смарт-картах Mifare. Вообще говоря, столь узкую и похожую на сугубо техническую проблему парламенты и правительства серьезных стран обычно не обсуждают. Однако этот случай весьма особый.

Скомпрометированные ныне карты Mifare Classic не только заложены в основу общенациональной системы оплаты общественного транспорта OV-chipcaart стоимостью 2 миллиарда евро, но и используются в качестве пропусков примерно на 2 миллионах автоматизированных пунктов контроля доступа в правительственных учреждениях и компаниях Голландии.

Похожая ситуация, можно заметить, характерна и для великого множества других стран, коль скоро количество проданных в мире карт Mifare Classic измеряется уже миллиардами, а серьезных конкурентов для них на рынке считай что нет.

Однако в Нидерландах восприняли давно уже назревавшую проблему особо болезненно, поскольку изготовителем карт Mifare является корпорация NXP Semiconductors, в свое время ответвившаяся от голландского хайтек-гиганта Philips.

Суть произошедшей компрометации, в двух словах, примерно такова. Профессор Барт Якобс (Bart Jacobs), работающий в университете Radboud старейшего голландского города Неймеген, вместе с группой своих аспирантов и студентов занимается систематическими исследованиями безопасности RFID-технологий и карт Mifare в особенности.

Эта группа ранее уже демонстрировала неудовлетворительную защиту проездных OV-chipcaart, однако теперь исследователи нашли способ быстрого и сравнительно дешевого клонирования не только проездных, защищенных криптографией, но и пропусков на охраняемые объекты.

В частности, дабы не ходить далеко, было продемонстрировано, насколько просто можно с расстояния в несколько метров считать информацию с карточек-пропусков студентов и преподавателей университета, а затем изготовить на основе этих данных сколько угодно поддельных пропусков-клонов…

В связи с чем уместно вспомнить несколько историй из недалекого прошлого, дающих расширенное представление о происходящем.

Осенью 2006 года на страницах русскоязычного блога, посвященного технологиям RFID (rfidigest.blogspot.com), промелькнула любопытная информация по поводу взлома защиты бесконтактных смарт-карт. О том, в частности, что специалисты зеленоградского хайтек-предприятия «Ангстрем» провели обратную инженерную разработку карты Mifare Classic и обнаружили в схеме закладку, позволяющую считывать содержимое чипа без знания секретного ключа.

Патриотически настроенные хакеры тут же известили о своей находке компетентные российские спецслужбы, коль скоро стало очевидно, что «с точки зрения государственной безопасности карта MIFARE – удобная игрушка, которую можно использовать в своих целях» (цитата из оригинала публикации).

Никакой дальнейшей огласке это открытие предавать не стали, ибо «на кой раскрывать свои возможности?» (еще одна цитата из источника). Тут мы имеем, так сказать, типичный русско-советский вариант реакции.

Несколько месяцев спустя, весной 2007 в пригороде Вашингтона проходила хакерская конференция Black Hat Federal, ориентированная на проблемы инфобезопасности с точки зрения государственных структур и крупных корпораций США.

В рамках этого форума местный умелец Крис Пейджет (Chris Paget), возглавлявший подразделение исследований и разработок небольшой фирмы IOActive, собирался продемонстрировать аудитории весьма впечатляющие результаты своих изысканий. А именно, насколько просто клонируются RFID-карточки пропусков в системах HID, массово используемых для контроля доступа на объекты правительства и в здания компаний не только в США, но и по всему миру.

Корпорация-гигант HID Global выпускает системы контроля доступа самых разных типов, однако про их бесконтактные «проксимити-карты» известно, что они, главным образом, построены на основе RFID-чипов Mifare.

Бесконтактные карты-пропуска, которые так легко клонировал Пейджет с помощью самодельного устройства стоимостью примерно 20 долларов, очевидно не имели криптографической защиты, как самые простые карточки типа Mifare Ultralight.

Но что там реально взломал американский хакер, так и осталось тайной. Потому что адвокаты HID Global заблокировали выступление Пейджета, заставили организаторов вырвать его доклад из тома с трудами конференции и пригрозили засудить до полного разорения всякого, кто еще раз попытается посягнуть на их «интеллектуальную собственность»…

Это, можно сказать, весьма типичный для Америки подход к решению проблем безопасности.

А вот как выглядела нынешняя реакция в Голландии. В пятницу, 7 марта (2008), университет Radboud проинформировал о своих результатах голландское правительство, поскольку под угрозой могли оказаться аспекты национальной безопасности.

Уже на следующий день, в субботу 8 марта, в университет для оценки ситуации прибыли специалисты NBV, национального Бюро безопасности связи, входящего в состав Службы общей разведки и безопасности (AIVD). После ознакомления с наглядной демонстрацией эксперты спецслужбы пришли к заключению, что это эффективная реальная атака.

В воскресенье, 9 марта, была проинформирована корпорация NXP, производящая Mifare, а 10 марта – компания Trans Link Systems, занимающаяся едиными смарт-картами для общественного транспорта.

Специалисты университета в полном объеме предоставили обеим компаниям технические детали о выявленных слабостях системы и ныне сотрудничают с ними в разработке возможных контрмер.

В тот же день, 10 марта, компания NXP Semiconductors издала пресс-релиз о выпуске к ноябрю 2008 новой бесконтактной карты MIFARE Plus, существенно более безопас-

ной и призванной обеспечить беспроблемную модернизацию существующих систем на основе MIFARE Classic (о факте компрометации Classic, можно отметить, в пресс-релизе нет ни слова).

В среду, 12 марта, министр внутренних дел Тер Хорст проинформировала парламент о случившемся и предпринимаемых контрмерах.

Технические детали о взломе Mifare Classic см. в материале «Ясно, что небезопасно».

# # #

Ясно, что небезопасно

(*Впервые опубликовано – март 2008*)

Подробности о взломе секретной криптосхемы RFID-чипов Mifare.

В первых числах марта (2008) коллективом студентов и сотрудников исследовательской группы «Цифровая безопасность» в голландском университете Radboud, г. Неймеген, была выявлена серьезнейшая уязвимость в бесконтактных смарт-картах широко распространенного типа (см. И грянул гром).

Подобные устройства, иногда называемые проксимити-картами, построены на основе RFID-чипов, то есть микросхем радиочастотной идентификации.

На сегодняшний день пластиковые и картонные карточки с запрессованным в них RFID массово используются по всему миру в таких качествах, как пропуска для автоматизированного контроля доступа на охраняемые объекты, карты оплаты проезда в транспорте, цифровые кошельки для мелких покупок, дисконтные карты в сетях торговли и куча других самых разных приложений.

Голландцами же была взломана система защиты в чипах типа Mifare Classic, изготовляемых компанией NXP, в прошлом – полупроводниковым подразделением корпорации-гиганта Philips.

Разных типов чипы Mifare на нынешнем рынке бесконтактных карт занимают абсолютно доминирующее положение, причем на Mifare Classic, имеющие оптимальное соотношение цена / безопасность, приходится доля порядка 90%. В более же конкретных цифрах, общемировое число продаж этих карт в разных источниках оценивается количествами от 1 до 2 миллиардов штук.

В современной жизни Голландии карты Mifare Classic занимают вообще особое место, поскольку на их основе реализован гранд-проект OV-chipkaart – разворачиваемая ныне общенациональная система единой оплаты проезда в общественном транспорте от метро и автобусов до железных дорог.

Похожая ситуация характерна для многих мегаполисов планеты вроде Лондона, Гонконга или Милана. В Москве, в частности, карточки Mifare Classic – это не только проездные в метро, но еще и «социальная карта москвича», перезаряжаемые карточки студентов и школьников, проездные для электричек и так далее.

Еще более важно, возможно, то, что чипы Mifare Classic очень широко используются и в Голландии, и по всему миру в картах пропусков для прохода в здания корпораций и правительственных учреждений.

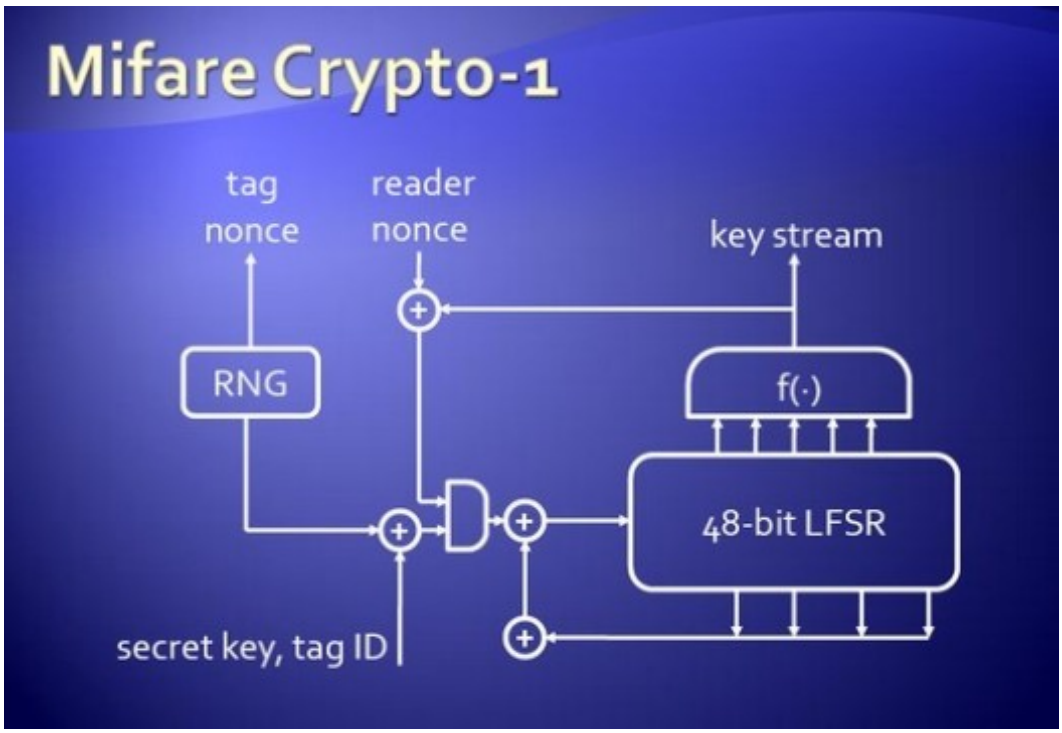
Все это означает, естественно, что слабости в защите подобной системы будут иметь весьма широкие и серьезные последствия. Если такую карту несложно клонировать, то в принципе становится, к примеру, возможен доступ на охраняемые объекты под видом чужой, украденной у кого-то личности.

Реалистичность этой атаки, собственно, и решили проверить «на себе» голландские исследователи из университета Radboud. Где допуск в здания контролируется, как и повсюду в Нидерландах, также с помощью Mifare Classic.

Говоря конкретнее, члены группы Digital Security поставили перед собой цель отыскать слабости в собственных пропусках, а найдя их, попытаться клонировать карты.

Результатом их исследований стало обнаружение серьезных дефектов в механизме аутентификации Mifare Classic. Это позволило: (1) полностью восстановить секретную схему алгоритма шифрования CRYPTO1, запечатанного в чип для защиты данных; (2) отыскать относительно простой и дешевый метод для извлечения из чипа криптогрфических ключей.

Два этих базовых открытия в совокупности позволили смоделировать реальную атаку, в процессе которой карточка-пропуск Mifare Classic, применяемая для входа в здания университета, была успешно клонирована.



[ВРЕЗКА]

Типы карт Mifare

Платформа Mifare до последнего времени включала в себя пять основных типов чипов для карт с бесконтактным, двойным (чип / магнитная полоса) и тройным (чип / полоса / USB) типами интерфейсов. В связи с компрометацией Mifare Classic фирмой NXP только что объявлено о вводе до конца 2008 г. нового, криптографически более сильного чипа на замену, получившего название Mifare Plus и оснащенного алгоритмом AES.

Самые простые, из-за этого самые дешевые и, следовательно, наиболее распространенные в реальных приложениях типы – это Ultralight (MF0 U10, U11) и Classic или Standard (MF1 S50, S70). У этих чипов нет процессора и, соответственно, операционной системы, а у Ultralight нет и никакой криптографии. Объем памяти EEPROM от 512 байт (Ultralight) до 1 и 4 килобайт (Classic).

Остальные три типа построены на основе процессора 80C51, имеют более развитую функциональность на основе JAVA, но и стоят существенно дороже – уже доллары, а не десятки центов как Mifare Classic или копеечный Ultralight.

Самый дешевый чип из дорогих, DESFire (MF3 D40), реализует крепкий шифр 3DES и имеет перезаписываемую память 4 Кбайт. Карта Mifare ProX (P8RF) имеет двойной интерфейс (плюс магнитная полоса), 3DES и криптографию с открытым ключом, от 32 до 64 Кбайт оперативной памяти.

Самый продвинутый чип для бесконтактных карт, SmartMX (P5xD, P5CT), оснащен тройным интерфейсом (плюс USB), более вместительной памятью ROM и EEPROM, а в наборе шифров дополнен стойким современным криптостандартом AES.

В приложениях, связанных с оснащением новых «электронных» паспортов технологией RFID, чипы SmartMX являются общепринятым, де факто стандартным решением по всему миру.

[КОНЕЦ ВРЕЗКИ]

Технические нюансы

Бесконтактная смарт-карта Mifare Classic была разработана в середине 1990-х годов. По сути своей, это чип памяти с дополнительными функциями защиты содержимого. Поскольку здесь нет процессора, функциональность карты не программируется.

Криптографические операции, которые способен выполнять чип, реализованы на аппаратном уровне в виде так называемого регистра сдвига с линейной обратной связью, или LFSR (linear feedback shift register) и «фильтр-функции» для усложнения генерируемой шифр-последовательности.

Этот криптоалгоритм, носящий название CRYPTO1, является коммерческой тайной NXP и никогда не публиковался для независимого анализа.

Таким образом, безопасность карт Mifare Classic в значительной степени опирается на то, что устройство криптоалгоритма хранится в тайне. Такой подход принято именовать «безопасность через неясность» (security by obscurity), причем среди большинства серьезных криптографов этот путь считается в корне ошибочным и бессчетное количество раз скомпрометированным. Не стал исключением и случай с CRYPTO1.

Типичный способ применения криптографии карт Mifare Classic – в процедурах аутентификации. Цель таких процедур, как известно, в том, что две связывающиеся стороны неким формальным способом доказывают друг другу, кем они являются.

Делается это предъявлением какой-либо известной обеим сторонам секретной информации, так называемого разделяемого секрета (или, иначе, общего криптоключа). Обе стороны, в данном случае карта Mifare и считывающий ее прибор картридер, выполняют определенные операции, а затем сверяют получившиеся результаты друг друга, дабы быть уверенными в легитимности оппонента.

Успешное завершение процедуры аутентификации является необходимым условием не только для открытия двери или турникета и входа на охраняемый объект, но и для выполнения операций считывания или записи информации в ячейках памяти Mifare

Classic. Память чипа поделена на независимые секторы, каждый из которых защищен двумя криптографическими ключами.

Правильное управление криптографическими ключами – это сама по себе большая и существенная область исследований, часто таящая в себе угрозы безопасности. Конкретно для случая Mifare Classic имеется два основных способа управления ключами.

1. Все карты и все картридеры, используемые в каком-то одном приложении, имеют одни и те же ключи для аутентификации. Это общепринятая ситуация для карт в системах контроля доступа.

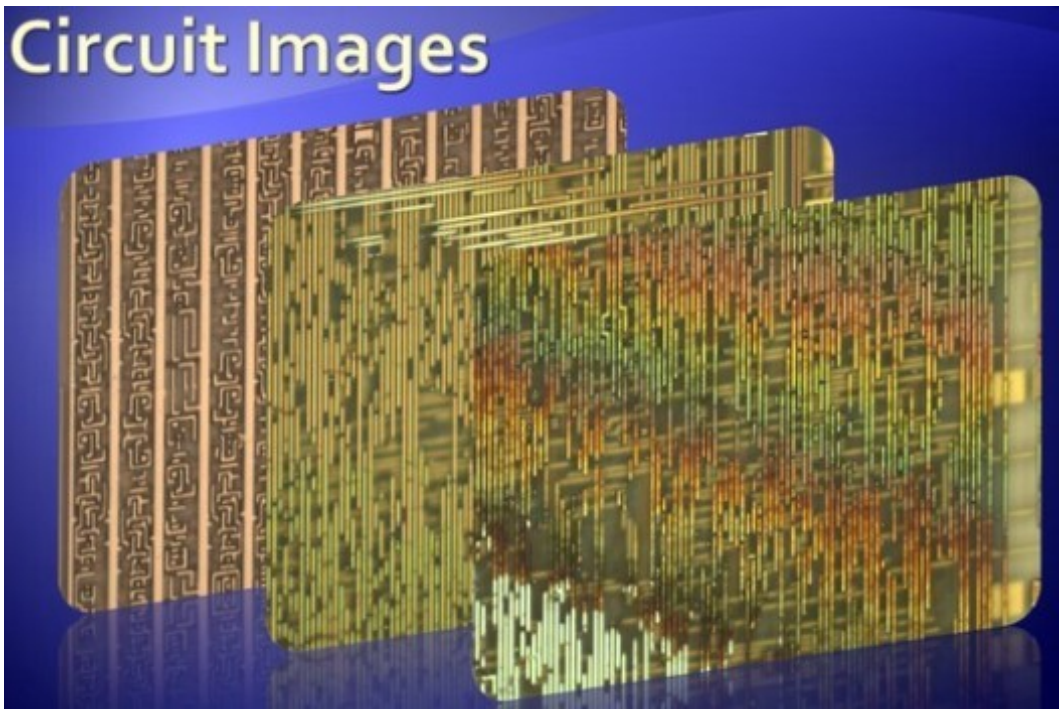
2. Каждая карта имеет свои собственные криптографические ключи. Для проверки ключей такой карты, картридер сначала должен определить, с какой именно картой начат обмен, а уже затем найти и вычислить связанные с ней ключи. Такая процедура именуется диверсификацией ключей и применяется в более разветвленных приложениях.

[ВРЕЗКА]

Хронология взлома

Взлом Mifare Ultralight. В мае-июне 2007 года два студента Амстердамского университета (Pieter Siekerman, Maurits van der Schee) проанализировали защиту самой простой версии RFID-чипов Mifare – в карточках Mifare Ultralight, используемых в качестве картонных одноразовых билетов на транспорте. Студенты выявили три серьезных проблемы, что позволило им на основе всего лишь единственной карточки сделать устройство для бесплатного проезда неограниченное число раз. Две из этих проблем решаются доработкой программы в считывателе турникета, что было вскоре и сделано голландскими транспортниками. Третья проблема решается только сменой архитектуры системы.

Германская атака на Mifare Classic. В декабре 2007 года германские исследователи Карстен Ноль и Хенрик Плётц (Karsten Nohl, Henryk Plötz) в рамках хакерской конференции 24th Chaos Communication Congress в Берлине продемонстрировали свои результаты по обратной инженерной разработке чипа карты Mifare Classic. Они применили технически один из самых сложных методов разрушающего анализа, последовательно удаляя слои чипа друг за другом и восстанавливая схематику по фотоснимкам слоев, сделанным с помощью микроскопа. Крайне трудоемкий процесс выделения и распознавания типовых элементов в схеме оказалось возможным автоматизировать с помощью специальной программы. В итоге же удалось найти участок, реализующий секретный криптоалгоритм CRYPTO1, и в общих чертах восстановить его работу. В марте 2008 Карстен Ноль опубликовал в Сети статью с итогами полного восстановления схемы CRYPTO1 и первичных результатов ее криптоанализа. Из этих результатов стало очевидно, что реализованный в Mifare Classic шифр имеет серьезнейшие слабости. Причем очень похоже, что схема ослаблена искусственно для облегчения вскрытия тому, кто знает «секрет».



Атаки университета Радбоуд. В январе 2008 Роэль Вердулт (Roel Verdult), студент голландского университета Radboud в Неймегене, вновь проанализировал на предмет слабостей модернизированную систему проездных билетов на основе Mifare Ultralight. И показал, что может изготовить портативное устройство клонирования ценой около 40 евро, с помощью которого одноразовая карточка позволят ездить неограниченное число раз. В марте 2008 коллектив исследователей этого же университета, работавший в контакте с немцами Нолем и Плётцем, с помощью собственных, неразрушающих методов повторил полное восстановление криптосхемы Mifare Classic. При этом было наглядно продемонстрировано, что знание слабостей шифра позволяет незаметно для владельца и с минимум затрат клонировать карточки-пропуска на охраняемые объекты или долгосрочные проездные билеты.

[КОНЕЦ ВРЕЗКИ]

Слабости в защите Mifare Classic

Голландская группа Digital Security обнаружила серьезные дефекты в механизме аутентификации карт Mifare Classic. Во-первых, как уже сказано, это позволило сделать полное обратное восстановление схемы CRYPTO1 и сконструировать собственную реализацию этого криптоалгоритма. Сделано это было с помощью известных в криптоанализе методов генерации сбоев.

Если атакующая сторона при аутентификации не в точности следует правилам обмена, предписываемым протоколом, то в принципе – по нештатным реакциям – имеется возможность получать дополнительную информацию об устройстве неизвестной схемы. Целенаправленно манипулируя сигналами на входе и комбинируя их с информа-

цией ответов, иногда можно восстановить устройство «черного ящика». Что и было сделано в данном случае.

Во-вторых, когда криптоалгоритм стал известен, стало возможным отыскать нужные секретные ключи. Например, усовершенствованным методом лобового вскрытия, т.е. тотального перебора всех возможных ключевых комбинаций. Ибо длина ключа в CRYPTO1 оказалась всего лишь 48 бит, так что при наличии подходящего быстрого вычислителя на полный «тупой» перебор в современных условиях требуется всего 9-10 часов работы.

Правда, стоит такая техника довольно недешево, однако голландским исследователям она и не понадобилась. Ибо CRYPTO1, как выяснилось, имеет не только короткую длину рабочего регистра (ключа), но и слабую функцию усложнения. Что позволило довольно легко отыскивать секретный ключ без лобового вскрытия.

Специально подобранный вид запросов на (заведомо неудачную) аутентификацию дает в ответах некоторую информацию о битах секретного ключа. Если один раз заранее собрать результаты всех таких ответов в большую просмотровую таблицу, коль скоро устройство CRYPTO1 уже известно, то атака на карту с неизвестным ключом становится быстрой и почти элементарной.

Надо просто опросить ее ложными запросами, по таблице установить одну часть ключа, а затем быстрым перебором остальных бит восстановить недостающую часть и получить ключ полностью.

Поскольку разработанная голландцами атака предназначена лишь для подтверждения концепции, а не для реальных хищений личности через клонирование карт, при демонстрации потребовалось многократное опрашивание карты-жертвы для конструирования просмотровой таблицы.

Для записи результатов всех этих попыток «неудачной» аутентификации в компьютер потребовалось несколько часов. Однако даже такой – не особо элегантный способ – можно реализовать и в жизни, если найти возможность незаметно расположить антенну картридера поблизости от карты жертвы на несколько часов.

Кроме того, вполне просматриваются способы оптимизации атаки и радикального сокращения числа опросов карты-жертвы, что делает атаку совсем простой и быстрой.

Эксплуатация слабостей и контрмеры

Как только секретный криптоключ извлечен из чипа карты, появляются самые разные возможности для злоупотреблений. Насколько тяжкими будут последствия злоупотреблений, зависит от конкретной ситуации.

Если все карты доступа имеют один и тот же ключ, то вся система контроля оказывается в высшей степени скомпрометирована и уязвима. Оценить масштабы такой уязвимости в цифрах, правда, не представляется возможным, поскольку открытой информации об объектах, охраняемых с помощью Mifare Classic, никто не публикует.

Но необходимо подчеркнуть, что именно для такой ситуации голландская группа продемонстрировала реальную атаку, когда карта-пропуск одного из сотрудников университета была «незаметно» для него опрошена и клонирована с помощью портативного картридера. Понятно, что человек, личность которого похищают, может быть совершенно не в курсе того, что здесь происходит.

В ситуациях, когда используются диверсифицированные ключи, простор для злоупотреблений существенно сужается. Атаки здесь более сложны, однако явно не выглядят невозможными. Впрочем, никаких реальных атак в данном направлении голландцами пока не демонстрировалось.

На техническом уровне никаких известных контрмер для данной атаки не просматривается. Экранирование карты в те моменты, когда она не используется, например в металлическом контейнере, сокращает, конечно, риски тайного считывания чипа. Однако в те моменты, когда карта используется, становится возможен и перехват сигналов, если скрытая антенна расположена неподалеку от поста контроля доступа.

По этой причине специалистами крайне рекомендуется усиление традиционных мер контроля. Доступ на охраняемые объекты необходимо защищать сразу несколькими способами, среди которых RFID-карта обеспечивает лишь один из механизмов контроля.

[ВРЕЗКА]

Результаты германских коллег

Когда немцы Карстен Ноль и Хенрик Плётц делали доклад на берлинской конференции 24CCC, они рассказали о своем вскрытии RFID-чипа Mifare Classic и восстановлении криптосхемы алгоритма CRYPTO1 лишь в самых общих чертах. Благоразумно решив не вдаваться в существенные подробности и не подставлять себя под обвинения о разглашении чужих коммерческих тайн и хищении интеллектуальной собственности.

Для голландских коллег из университета Radboud, к примеру, этой информации оказалось вполне достаточно, чтобы и подтвердить результаты немцев, и придумать собственную практичную атаку.

Однако другая голландская инстанция, TNO или национальная Организация прикладных научных исследований, по заказу правительства Нидерландов провела собствен-

ное изучение доклада немцев и сделала существенно иные выводы. В целом подтвердив результаты немцев, эксперты TNO в своем официальном заключении сделали вывод, что описанная атака не будет представлять реальной угрозы для Mifare Classic на протяжении еще лет двух, по крайней мере.

Отчет TNO был опубликован в последних числах февраля. А немцы к тому времени уже не только восстановили всю криптосхему полностью, но и выявили в ней очень серьезные статистические слабости. Что позволило им почти мгновенно по ответным реакциям чипа восстанавливать 12 из 48 бит секретного ключа.

Остальные биты приличный современный компьютер восстанавливает перебором за несколько минут, а специализированный вычислитель на основе FPGA, чипов с перепрограммируемой логикой, так и вообще за секунды. По этой причине заключение официальной экспертизы TNO для голландских властей с точки зрения немцев выглядело как серьезно вводящая в заблуждение неправда.

Единственно правильной реакцией в таких условиях была сочтена открытая публикация результатов криптоанализа шифра Mifare Classic в интернете. То, что выкладывание в Сеть этой работы («Cryptanalysis of Crypto-1» by Karsten Nohl) практически день в день совпало с публикацией очень созвучных результатов в университете Radboud – это, скорее всего, просто совпадение. Но совпадение очень выразительное.

[КОНЕЦ ВРЕЗКИ]

Проблемы и вопросы

Всякий раз, когда серьезные и ответственные исследователи обнаруживают дыры в защите распространенных систем, неизбежно встает сложная дилемма – как поступать с этой информацией.

Немедленная открытая публикация со всеми подробностями гарантированно простимулирует рост злонамеренных атак и очевидно нанесет обществу вред. Если же надолго задержать информацию в секрете, то практически наверняка никто сам не станет предпринимать дополнительных шагов для усиления защиты.

Поэтому раскрытие уязвимостей обычно сводится к компромиссу, который пытается сбалансировать все опасности тем, что критичные подробности публикуются с задержкой, предоставляющей время на исправление дефектов защиты.

Конкретно в ситуации со взломом Mifare Classic и голландские, и немецкие хакеры пошли именно по этому пути – своевременно предупредив сообщество безопасности и заинтересованные инстанции об угрозе, но удержав при себе принципиально важные детали об устройстве слабой криптосхемы.

При этом каждая из сторон, участвовавших во вскрытии, сочла необходимым в очередной раз раскритиковать пристрастие изготовителей к явно порочной концепции «безопасность через неясность». Ибо совершенно очевидно, что безусловно слабый алгоритм Crypto1 никогда бы не попал в повсеместно распространенные смарт-карты, пройди он через открытую независимую экспертизу.

Но проблему можно сформулировать и несколько иначе. Богатый опыт свидетельствует, что практически ни разу при вскрытии хакерами секретной проприетарной криптосхемы не обнаруживалось сильного алгоритма, превосходящего открытые и хорошо известные.

Из этого сам собой напрашивается вывод, что секретные схемы для того и удерживают в тайне, дабы их слабости, обеспечивающие быстрое вскрытие, были известны лишь тем, «кому надо». Но вот надо ли это обществу?

The End

[МЕЖКОЛОННЫЕ ВРЕЗКИ]

* * *

По данным аналитиков Gartner, бизнес на RFID-чипах стремительно растет. В 2007 году доходы здесь составили 917,3 млн. долларов, а в 2008 должны вырасти до 1,2 миллиарда или более чем на 30%. К 2012 году доходы прогнозируются в сумме 3,5 миллиарда долларов.

* * *

Контроль доступа исторически считается одним из самых старых применений бесконтактных карт. Среди наиболее крупных систем доступа на базе платформы Mifare фигурируют министерство обороны США и министерство транспорта США. Какого типа чипы используются в электронных пропусках американских правительственных структур, пресса не уточняет.

* * *

В транспортном секторе освоено наибольшее число проектов с использованием карт Mifare. Разной сложности проекты по оплате проезда реализованы во Франции, Германии, Польше, России, Турции, Великобритании, Австралии, Китае, Индии, Японии, Корее, Малайзии, Сингапуре, Аргентине, Бразилии, Канаде, Колумбии, Украине. Города США, как ни странно, в этот список стали входить лишь в последнее время.

\# \# \#

Суета заранее, или Пост-квантовые тайны криптографии

(*Октябрь 2016*)

В высших кругах криптографического мира наблюдается весьма оживленная активность. Почему так интенсивно все вдруг завертелось, никто толком не понимает. За кулисами явно знают больше – но помалкивают, как обычно. Да еще прячут концы…

Компетентные инстанции по обе стороны Атлантики, занимающиеся установлением всеобщих технических стандартов, в настоящее время очень заметно озаботились проблемами так называемой квантово-безопасной криптографии.

Под этим общим термином (в другой версии он же звучит как пост-квантовая криптография) в области защиты информации принято понимать широкий круг всевозможных алгоритмов, протоколов и устройств для коммуникаций, способных противостоять угрозам со стороны квантовых компьютеров.

Если знать, что настоящий квантовый компьютер – это пока еще техника сугубо гипотетическая, а реальные задачи по быстрому взлому шифров такие вычислители смогут решать (согласно прикидкам авторитетных экспертов) лишь только лет эдак через 20-30, а может даже 40, то вполне естественно и удивиться. Почему вдруг именно сейчас такая суета?

У высоких инстанций, конечно же, готовые ответы на подобные вопросы всегда имеются. Так что для поверхностных оценок несведущей публики представленные объяснения выглядят не только разумно, но и убедительно. Для специалистов, однако, картина куда менее ясна. Чем лучше эти люди понимают суть данного предмета, тем больше они видят неувязок и мутных умолчаний в предлагаемых объяснениях.

Ну а для того, чтобы стало понятно, отчего все это очень важно и интересно даже для неспециалистов, надо чуть подробнее разъяснить, что и как тут вообще происходит.

#

С 19 по 21 сентября 2016 в городе Торонто, Канада, проходил очередной международный симпозиум под названием «**Семинар ETSI/IQC по квантово-безопасной криптографии**».

Для подчеркивания значимости данного мероприятия надо пояснить, что ETSI – это Европейский институт телекоммуникационных стандартов (то есть отраслевой аналог американского НИСТ, главного органа стандартизации в США). А IQC, соответственно, это Институт квантовых вычислений при Университете Ватерлоо (или Уотерлу, как предпочитает выражаться англоязычная публика), то есть один из главных в мире научно-исследовательских центров, не первый десяток лет занимающихся проблемами криптографии в контексте квантовых компьютеров.

При столь солидных организаторах мероприятия уже не так удивительно, что среди участников симпозиума отмечены не только ведущие ученые академических структур и индустрии, но также важные люди из руководства транснациональных корпораций и правительственных ведомств Европы, Северной Америки, Японии, Китая и Южной Кореи. А кроме того, еще и большие начальники спецслужб, занимающихся защитой информации в таких государствах, как Великобритания, Канада и Германия.

И все эти сильно занятые люди, еще раз напомним, собрались ныне в Торонто для обсуждения того, каким образом пора всерьез укреплять криптографию для противостояния технологиям, которые даже по самым оптимистичным оценкам станут представлять реальную угрозу лет так лишь через двадцать, самое меньшее. А скорее всего, где-то еще дальше в будущем.

Если же принять во внимание тот факт, что без какой-либо взаимосвязи с этим мероприятием, но практически синхронно – в августе 2016 – НИСТ США **официально объявил** о запуске своей собственной крупномасштабной программы по переходу от традиционной криптографии к криптографии «пост-квантовой», то вывод будет вполне очевидным. В мире крипто уже явно затеяны большие перемены. Причем затеяны они как-то уж очень торопливо и даже с некоторыми признаками паники.

Что конечно же порождает вопросы, особенно у тех знающих людей, кто непосредственно занимается криптографией и регулярно соприкасается со всей данной средой.

#

В США первый официальный сигнал о том, что с укреплением и модернизацией традиционной криптографии надо срочно что-то делать, был отмечен год назад – в августе 2015 года. Именно тогда Агентство национальной безопасности, как главный авторитет государства в области шифров, опубликовало заявление о существенных переменах в своей базовой политике – в связи с необходимостью разработки новых стандартов для пост-квантовой криптографии или кратко PQC (*National Security Agency, Cryptography today, August 2015*).

Как и многие из других сторон этого процесса, АНБ заявило, что считает настоящий момент наиболее подходящим временем для того, чтобы вплотную заняться разработкой новых протоколов для криптографии с открытым ключом. Такой криптографии, где стойкость также будет зависеть от трудных задач математики, но только теперь это должны быть иные трудные задачи – не поддающиеся эффективному решению с помощью квантовых компьютеров.

Здесь можно пояснить, что для всех широко применяемых ныне алгоритмов и протоколов криптографии с открытым ключом (построенных на базе схем RSA и ECC, т. е. крипто на эллиптических кривых) стойкость выстроена на основе двух трудных в решении задач математики – разложения большого целого числа на пару простых сомножителей (что именуют факторизацией) и вычисления дискретного логарифма. Для обычных – классических – компьютеров обе задачи решить за приемлемое время считается невозможным. Или, выражаясь аккуратнее, никто и нигде таких методов пока не продемонстрировал.

Но случилось так, что когда в начале 1990-х ученые вплотную занялись теорией создания компьютеров существенно новых, «квантовых» (работающих на основе принципов квантовой механики), то очень быстро обнаружились и квантовые методы для быстрого решения именно этих двух задач криптографии – факторизации и дискретного логарифмирования… То есть большая проблема с надежностью засекречивания коммуникаций обозначилась уже весьма давно, свыше 20 лет назад.

Однако никаких мало-мальски конкретных шагов по решению этой проблемы никто все эти годы не предпринимал. Просто по той причине, что задача построения реального квантового компьютера для решения подобных задач сама по себе представляет гигантскую научно-техническую проблему. И каким образом эффективно данную проблему решать, никому было неведомо – ни в те времена, ни по сию пору…

Так, во всяком случае, было принято считать вплоть до начала нынешней суеты с неотложными шагами по разработке и внедрению пост-квантового крипто. Причем

шаги предприняты в таких условиях, необходимо подчеркнуть, когда мировая криптографическая наука все еще так и не нашла тех самых трудных математических задач, которые окажутся гарантированно «не по зубам» для компьютеров квантовых.

#

Все изложенное выше – это, так сказать, общеизвестный для криптографов базовый контекст, в рамках которого у специалистов сразу же возникает естественный вопрос. Что такого очень серьезного могло произойти в самые последние годы, из-за чего столь энергично вдруг завертелись шестеренки в «машине перемен»?

Естественно, в качестве возможного ответа первой же приходит идея о том, что кто-то где-то в тайне от остальных таки построил настоящий квантовый компьютер. И коль скоро наиболее заметную и решительную инициативу по скорейшему переходу к новой, квантово-безопасной криптографии демонстрирует АНБ США, несложно догадаться, какое именно государство приходит тут на ум в первую очередь. Обладающее не только самым огромным бюджетом для подобных инициатив, но и всеми нужными научно-техническими возможностями.

Однако, даже если гипотеза эта и выглядит для кого-то правдоподобной, принять её в качестве рабочей сообщество специалистов не может. Хотя АНБ, спору нет, организация в высшей степени засекреченная и умеющая в тайне применять наиболее мощные на планете суперкомпьютеры, имеется также и еще кое-какая достоверная информация. Благодаря сливам топ-секретных документов от Сноудена точно известно, что в 2013 году квантового компьютера у АНБ не то что не было и близко, но и интерес к этой теме был минимальный.

Как и все профессионалы, американская спецслужба тоже проявляет некоторое внимание к данному направлению. Однако собственные затраты на квантовые вычисления в бюджете АНБ занимают лишь небольшую долю в довольно скромной общей сумме (несколько десятков миллионов долларов), выделяемой в целом на перспективные исследования. Для сравнения, согласно экспертным прикидкам, под создание настоящего квантового компьютера, способного решать реальные задачи, потребуется сумма не менее миллиарда долларов – при условии, что уже будет в наличии подходящая технология. Но именно её-то пока что у ученых и нет…

В открытом сообществе криптографов, озадаченном поспешностью новых инициатив, для объяснения происходящего имеется, естественно, немало и других разнообразных домыслов. В отрыве от контекста каждый из них выглядит по-своему логично, однако при сопоставлении с другими известными фактами всякий раз обнаруживаются противоречия и нестыковки.

#

Наиболее содержательной, пожалуй, обзорной работой, обобщающей и сопоставляющей все подобные гипотезы и предположения без итогового ответа, можно считать известную статью «Головоломка, окутанная загадкой», подготовленную весьма известными криптографами Нилом Коблицем и Альфредом Менезесом в конце 2015 года (*Neal Koblitz and Alfred J. Menezes, “A Riddle Wrapped in an Enigma”*, **PDF**).

Дабы стало понятнее, почему имеет смысл сосредоточить внимание на фактах из именно этой аналитической работы, следует вкратце прояснить два момента. (а) Какое место занимают ее авторы в открытой академической криптографии; и (б) насколько тесно и загадочно их собственные научные разработки переплетены с нынешними инициативами АНБ США по ускоренному переводу используемых криптографических алгоритмов на другие рельсы.

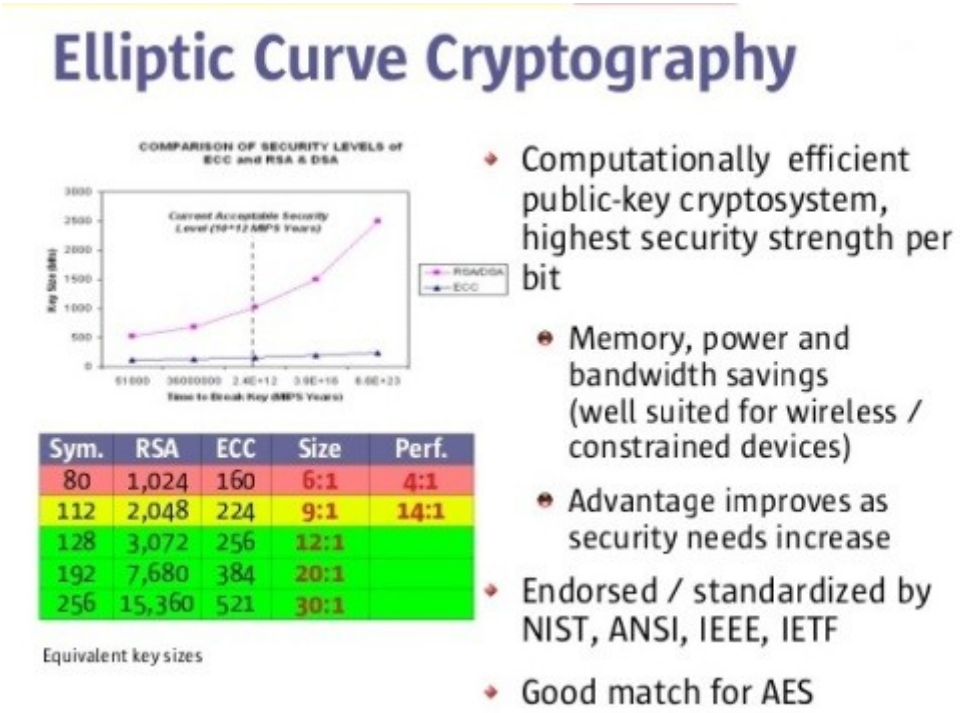
Американский математик и криптограф Нил Коблиц является (наряду с Виктором Миллером) одним из тех двух человек, которые в 1985 году одновременно и независимо друг друга придумали новую криптосхему с открытым ключом, получившую название ECC. Как сокращение от Elliptic Curve Cryptography, то есть «криптография на эллиптической кривой».

Здесь, ясное дело, совсем не место для углубления в технические детали этого метода и в его отличия от криптосхемы RSA, появившейся раньше и получившей наибольшее коммерческое распространение. Но следует подчеркнуть, что ECC с точки зрения практической эксплуатации обладает явными преимуществами, поскольку та же самая теоретическая стойкость алгоритма обеспечивается при намного меньшей длине ключа (для сравнения, 256-битные операции ECC эквивалентны работе с модулем длиной 3072 бита в RSA). А это, в свою очередь, сильно облегчает вычисления и существенно повышает быстродействие системы.

Второй важный момент (практически наверняка связанный с первым) заключается в том, что крайне скрытное АНБ США в своих криптографических предпочтениях с самого начала стало склоняться в пользу ECC. В первые годы и десятилетия это доносилось до академических и промышленных кругов в лишь неявном виде (когда, например, в 1997 году официальный сотрудник АНБ Джерри Солинас впервые выступил на открытой конференции Crypto – с докладом об их модификации известной схемы Коблица).

Ну а затем это было сделано отчетливо задокументированным образом, когда в 2005 АНБ США опубликовало свои рекомендации по криптоалгоритмам в виде так называемого Suite B (Набора B) – комплекса открыто опубликованных шифров для закрытия секретной и топ-секретной информации в национальных системах связи. Все базовые алгоритмы и протоколы этого «набора» были выстроены на основе ECC, а для RSA отводилась вспомогательная роль «первого поколения», нужного лишь для плавного перехода к новой более эффективной криптографии на эллиптических кривых…

На этом месте самое время вспомнить про Альфреда Менезеса, второго соавтора интересующего нас обзора про «Головоломку, окутанную загадкой». Ибо канадский математик-криптограф Менезес всю свою научную жизнь, начиная с середины 1980-х, работает в университете Ватерлоо – одном из заметнейших центров открытой академической криптографии. Именно здесь в 1980-е годы тремя профессорами университета была создана компания Certicom, занявшаяся разработкой и коммерческим продвижением криптографии на эллиптических кривых.



Соответственно, Альфред Менезес со временем стал не только видным разработчиком Certicom и автором нескольких авторитетных книг по криптосхемам ECC, но также и соавтором нескольких важных ECC-патентов. Ну а АНБ США, в свою очередь, когда запускало весь свой проект под названием Suite B, предварительно закупило у Certicom большой – на двадцать с лишним штук – пакет патентов, накрывающих «эллиптическую» криптографию.

Короче говоря, вся эта преамбула понадобилась для того, чтобы пояснить, почему Коблиц и Менезес – это именно те люди открытого сообщества математиков и компьютерщиков, кто по естественным причинам считал себя хорошо осведомленными о текущих делах и планах АНБ в области криптографической защиты информации. Однако и для них инициатива АНБ с резкой сменой курса на пост-квантовые алгоритмы стала полнейшей неожиданностью.

#

Особо, так сказать, задетыми из-за этой смены курса Коблиц и Менезес оказались по той причине, что они сразу же заметили и сопутствующие перемены в алгоритмах

«Набора B». Ибо тем же летом 2015 АНБ по-тихому – абсолютно никому не разъясняя причин – «выпилило» из своего комплекта ECC-алгоритм «P-256», одновременно оставив там его RSA -эквивалент с 3072-битным модулем. И более того, в сопутствующих заявлениях АНБ вполне отчетливо было сказано, что всем сторонам, внедряющим алгоритмы из Suite B, ныне уже нет никакого смысла переходить на ECC, а лучше просто увеличить длины ключей RSA и подождать, когда появятся новые пост-квантовые шифры…

Поскольку Коблиц и Менезес имеют все основания считать себя людьми, компетентными в области криптографии на эллиптических кривых, но при этом абсолютно ничего не слышали о новых методах взлома, скомпрометировавших «их» криптосхему, все тут происходящее вокруг ECC чрезвычайно математиков удивило. И заставило предпринять дополнительное расследование. Однако и оно не дало ничего.

Имея давние и тесные контакты с индустрией, ученые знают, что обычно все крупные корпорации, делающие криптографические задания и оборудование для правительства США, всегда получают некое заблаговременное предупреждение о смене планов. Но в данном случае ничего такого не было.

Еще более неожиданным сюрпризом оказалось то, что и к людям из НИСТ США, отвечающим за открытые криптографические стандарты государства, никто из АНБ по этому поводу не обращался. Ну и наконец (поскольку Менезес имеет связи и там), даже собственные математики-криптографы АНБ из Управления защиты информации (IAD) были крайне удивлены тем сюрпризом, что преподнесло им руководство со своей пост-квантовой инициативой…

Формулируя все собранные авторами свидетельства чуть иначе, вполне можно сделать вывод, что те весьма влиятельные люди, которые в недрах АНБ инициировали публичную смену курса, делали это без какой-либо обратной связи и консультаций не только со специалистами промышленности и академии, но даже и со своими собственными экспертами.

Именно к такому выводу, собственно, приходят в своих анализах и Коблиц с Менезесом. С готовностью признавая, что в итоге никто, получается, толком не понимает техническую подоплеку всего здесь происходящего.

#

Дабы столь странная и загадочная картина стала хотя бы отчасти более понятной, самое время отметить, что аналитическая статья Коблица и Менезеса выстроена по канонам пьес классического театра. То есть для всего в ней происходящего присущи единство места, времени и действия. Место – США и Канада, время – сейчас, действие – обозначенная криптографическая суета.

Однако реальная жизнь вообще и криптография в частности имеют куда более богатую, многослойную структуру и весьма нетривиальную историю, уходящую вглубь десятилетий и даже веков. Иначе говоря, объяснения для технической стороны происходящего ныне с пост-квантовом крипто можно увидеть довольно легко, если принимать в расчет полную историю открытой криптографии, особенно в аспектах её многослойной структуры, и обращать особое внимание на активность скрытых действующих лиц.

И хотя именно об этих вещах у Коблица-Менезеса нет ни слова, для адекватного восприятия интриги очень желательно знать, что на самом деле принципы криптографии с открытым ключом были открыты практически одновременно – в 1970-х годах – сразу в двух принципиально разных местах. Сначала, на несколько лет раньше, это сделали три секретных криптографа в стенах британской спецслужбы GCHQ, аналога и ближайшего партнера американского АНБ в задачах радиоэлектронной разведки. Но как это издавна заведено у шпионов, сделано все было в глубокой тайне и «только для себя».

Причем сразу же уместно отметить здесь и один тонкий нюанс. Открытие сделали не шпионы GCHQ, а математики подразделения CESG, отвечающего за национальные шифры и защиту правительственных систем связи Великобритании. С другой стороны, тесное взаимодействие между GCHQ и АНБ США происходит прежде всего по линиям совместной разведывательной деятельности.

Иначе говоря, поскольку в АНБ также есть собственное управление IAD (Information Assurance Directorate), специализирующееся на разработке криптоалгоритмов и защите информации, для математиков этого подразделения открытие британских коллег стало полнейшей неожиданностью. А впервые узнали они о нем от своих сослуживцев-шпионов, тесно общающихся с англичанами…

Как бы там ни было, однако, когда те же самые по сути алгоритмы «несекретного шифрования» – на основе факторизации и дискретного логарифмирования – независимо от спецслужб вскоре изобрели в США исследователи открытого сообщества (Диффи, Хеллман, Меркль, Райвест, Шамир, Адлеман), то АНБ приложило гигантские усилия, чтобы запихать этого джинна обратно в бутылку.

Никак не раскрывая, что спецслужба уже имеет у себя эту математику, начальники АНБ просто пытались всячески помешать ученым в широкой публикации данной информации. Напирая на то, что стойкая криптография – это слишком серьезное оружие, а их новые алгоритмы шифрования с открытым ключом позволяют устраивать скрытые от контроля коммуникации кому угодно, даже людям и сторонам, никогда друг с другом не встречавшимся.

Как всем известно, абсолютно ничего с запретом на знания и с затыканием ртов ученым тогда у АНБ США не получилось. В результате же открытое научное сообщество очень на АНБ разозлилось. А кроме того, под давлением ученых и индустрии ведать разработкой и внедрением коммерческой криптографии в стране стала в итоге вовсе

не шпионская спецслужба (как там ни старались), а гражданская структура, НИСТ США.

И хотя история эта весьма давняя, ныне она вполне наглядно повторяется. Если, конечно, смотреть внимательно и обращать внимание на характерные детали.

#

Нынешний международный симпозиум ETSI/IQC по квантово-безопасной криптографии, с которого начинался данный рассказ, имеет сразу несколько примечательных особенностей. Во-первых, на нем весьма солидно – руководителями важных структур – были представлены спецслужбы Великобритании, Канады, Германии. Все эти национальные спецслужбы – аналоги американского АНБ. Однако от АНБ США в явном виде не упомянуто абсолютно никого. И это, конечно же, не случайность.

Имеется масса свидетельств как от лидеров бизнеса, так и непосредственно от начальников разведструктур, что после разоблачительных сливов от Эдварда Сноудена практически вся ИТ-индустрия США (не говоря уже о других странах) реагирует на деятельность АНБ в высшей степени отрицательно. Ибо в своей гипер-активности вокруг компрометации стойкой криптографии шпионы серьезнейшим образом подорвали доверие общества не только к флагманам американского ИТ-бизнеса, но даже и к НИСТ США (навязав им искусственно ослабленный алгоритм в качестве стандарта). Иначе говоря, на международных форумах, обсуждающих пути к усилению криптографии в свете новых угроз, для АНБ США сейчас благоразумнее просто не светиться.

Другая примечательная особенность происходящего заключается в том, что нынешний «рабочий семинар» в Торонто – уже далеко не первый, а четвертый по счету. Первый был в 2013 в Париже, а второй – особенно для нас интересный – происходил осенью 2014 в столице Канады Оттаве. Интересным же данное мероприятие является по той причине, что там имел место в высшей степени необычный доклад от имени секретной британской спецслужбы GCHQ (*P. Campbell, M. Groves, D. Shepherd, «Soliloquy: A Cautionary Tale»*, **PDF**).

Точнее говоря, доклад был не от шпионов, а от подразделения защиты информации CESG, причем сделал его лично Майкл Гроувс (Michael Groves), возглавляющий криптографические исследования в этой спецслужбе. Тут обязательно надо подчеркнуть, что для людей из английских спецслужб совершенно не свойственно рассказывать о своих секретных разработках на открытых конференциях. Однако данный случай был воистину исключительным.

В своем докладе Гроувс не только рассказал, что британские криптографы уже давно, с начала 2000-х годов занимаются разработкой квантово-безопасных алгоритмов, но и в подробностях описал одну из особо удачных, как казалось, схем такого рода – построенную в 2007 году на основе так называемых числовых циклических решеток. К

сожалению, затем выяснилось, что данный криптоалгоритм – получивший от авторов имя Soliloquy – далеко не так силен, как предполагалось. В течение 2010-2013 для его эффективного взлома была придумана теоретическая атака с помощью квантового компьютера, а потому в итоге от алгоритма пришлось полностью отказаться.

При этом важно, что решение о полном отказе – а не об усилении-модернизации красивой конструкции – было в основном принято спецслужбой из-за очень мощной и сильно впечатлившей англичан атаки, разработанной в 2013 году группой исследователей открытого академического сообщества. В работе этих авторов (*K. Eisentraeger, S. Hallgren, A. Kitaev, and F. Song. «A quantum algorithm for computing the unit group of an arbitrary degree number field»*. In STOC ACM, 2014) описывается существенно новая квантовая атака весьма общего типа, накрывающая, в частности, широкий круг «пост-квантовых» криптосхем, включая и некому неведомый в ту пору Soliloquy…

#

С одной стороны, эффект от этого «полуоткрытого» выступления большого криптографа английской спецслужбы оказался именно таким, который очевидно и задумывался. Индустрия и академия, занимающиеся защитой информации, с готовностью приняли в качестве очень знающих консультантов людей из CESG (которые наглядно продемонстрировали не только свою «опережающую» компетентность, но и готовность делиться даже опытом неудач). На нынешнем форуме в Торонто, в частности, уже двум начальникам от CESG было доверено председательствовать на сессиях и модерировать дискуссии.

Но с другой стороны тут же проявился и совсем иной эффект, обычно сопровождающий любое сотрудничество со спецслужбами. Имеются в виду, конечно же, всяческое напускание секретности и попытки заглушить даже уже опубликованные результаты исследований. Мало того, что история про выступление гранд-криптографа CESG на открытом симпозиуме чрезвычайно скупо освещалась в СМИ, а статью и слайды презентации про Soliloquy можно отыскать в Сети лишь тем, кто очень четко знает, что именно ищет (на сайте ETSI, где эксклюзивно лежат данные файлы, прямых ссылок к ним не обнаруживается).

Самое неприятное, однако, тут даже в ином. Если кто-либо интересующийся захочет ознакомиться с той самой статьей ученых открытого сообщества, что сильно впечатлила английскую спецслужбу, то быстро выяснится, что и её отыскать не так-то просто. Данной статьи нет не только на сайте научных препринтов Arxiv.org, где уже давно наряду с физиками-математиками публикуются и компьютерщики-криптографы. Нет ее также и на специализированном сайте сугубо криптографических препринтов Eprint.iacr.org, принадлежащем IACR или Международной ассоциации криптографических исследований. (Каждый из авторов интересующей нас статьи имеет множество других публикаций на том, на другом, или даже на обоих из этих сайтов – нет только лишь нужной работы.)

Хуже того, если отправиться искать файл по личным веб-страницам исследователей на университетских сайтах, то и там поджидает засада. Наиболее известный из соавторов, Алексей Китаев, знаменит как супер-звезда на небосклоне квантовых вычислений, к криптографии имеет лишь сугубо касательное отношение, а ссылки на файлы своих публикаций вообще не накапливает. Ни на веб-страницах Калтеха и Института теоретической физики Кавли в Калифорнии, где постоянно работает, ни где-либо еще.

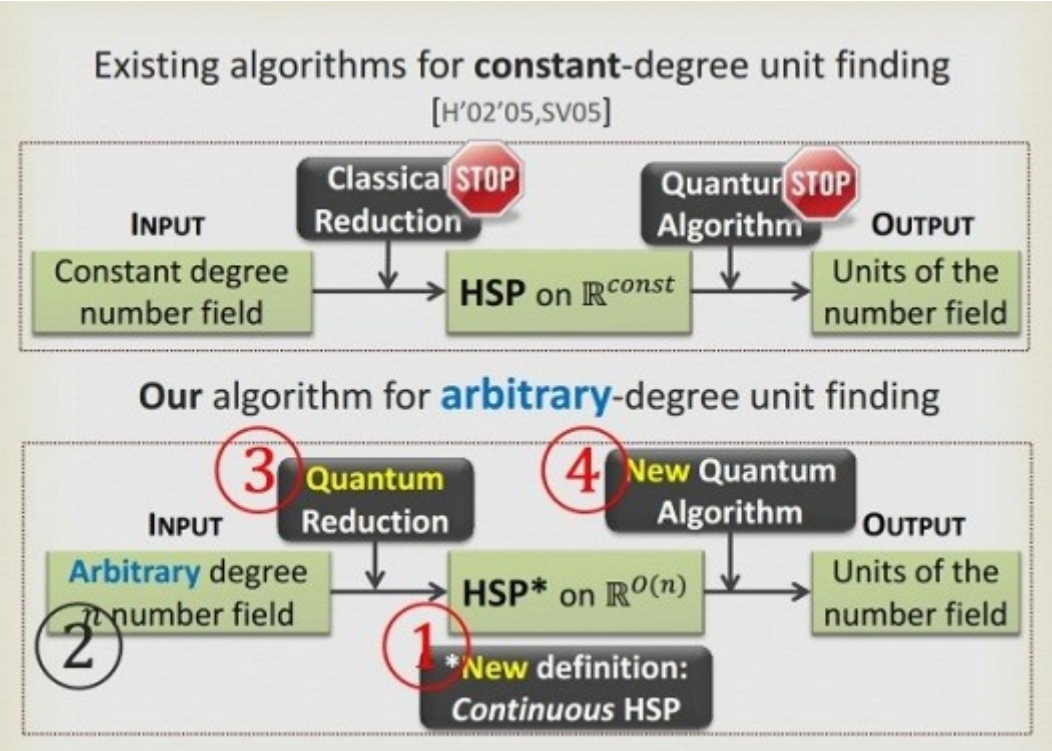
Другой соавтор, Шон Холгрен, действительно известный именно как криптограф, подобно многим другим исследователям имел прежде обыкновение выкладывать на университетской веб-странице ссылки на свои публикации. Но вот именно на интересующей нас статье это дело вдруг прекратилось. Для всех предыдущих статей файлы имеются, а для нужной – лишь название. Для всех же последующих публикаций 2015-2016 гг. нет даже названий. Хотя в архивах препринтов такие работы обнаруживаются…

Действительно полноценный перечень всего что было, есть и даже будет тут сделано (с подобающими ссылками на файлы) отыскивается лишь на сайте самого молодого из соавторов – по имени Фанг Сонг. Но что существенно, не на его университетских веб-страницах, а на персональном веб-сайте FangSong.info. Причем даже тут обнаруживаются странные потери. Нужный нам PDF-файл с вариантом искомой статьи таки имеется (**fangsong.info/files/pubs/EHKS_STOC14.pdf**), однако ссылки на примерно тот же файл, но с названиями типа «полная версия» и «Arxiv.org» оказываются битыми, зацикливая переход обратно на главную страницу. То есть файлы явно автором выкладывались, но и тут – как на сайте ArXiv – необъяснимо исчезли…

#

«Необъяснимыми» все пропажи такого рода (на самом деле подобных случаев довольно много) можно считать лишь при очень наивном и поверхностном взгляде на вещи. Потому что объяснение происходящему чаще всего содержится уже в заголовках статей, где авторы – в соответствии с давно заведенными у ученых правилами – обязаны указывать источники финансирования и грантов, на деньги которых проведены исследования.

Конкретно же в нашем случае «спонсором» однозначно выдающейся статьи о новом методе квантово-криптографической атаки является – сюрприз! – Агентство национальной безопасности США. Ну, а «кто за дэвушку платит, тот дэвушку и танцует», как известно. Понятно, что сами авторы исследования всегда заинтересованы в широком распространении своих результатов, однако у их спонсоров зачастую бывают прямо противоположные цели…



Единственно темным и действительно важным моментом, пока что оставшимся не освещенным во всей данной истории, является такой. Какая может быть взаимосвязь между новым, очень эффективным (и весьма впечатлившим спецслужбы) алгоритмом для вскрытия всевозможных криптосхем с помощью гипотетического квантового компьютера в далеком будущем и нынешними поспешными шагами АНБ по изъятию из обращения криптографии на эллиптических кривых?

Связь тут, как выясняется, имеется совершенно непосредственная. Но чтобы ее заметить, опять-таки, надо не только соображать в криптографии, но еще и очень внимательно следить за происходящим.

#

Когда на рубеже 2014-2015 только-только стало известно о пост-квантовом алгоритме Soliloquy от британской спецслужбы, о его последующей компрометации и о параллельно изобретенной квантовой атаке в открытом сообществе, один из очень компетентных и хорошо осведомленных криптографов, Дэн Бернштейн, сделал **интересное обобщение**.

Сопоставив все известные на тот момент факты, Бернштейн выдвинул предположение, что на самом деле новый квантовый алгоритм от Холгрена, Фанг Сонга и компании указывает также путь и к существенно более мощным атакам с помощью традиционных классических компьютеров. Причем на основе известных, но весьма туманных комментариев англичан Бернштейн сделал вывод, что и в британской спецслужбе об этом знают – но предпочитают держать ото всех в секрете…

Ото всех или не ото всех, этого никто достоверно не знает, естественно. Но зато прекрасно известно, что было потом. Когда еще через несколько месяцев, в августе 2015, АНБ США вдруг сильно удивило весь криптографический мир своим резким отказом от криптографии ECC с относительно короткой длиной ключа. Единственными, кто тут вряд ли удивился, были наверное криптографы британской спецслужбы.

Ну а еще через полгода, в начале 2016, уже и в открытом криптографическом сообществе появились две, как минимум, независимых публикации от ученых-исследователей, которые в самых общих чертах подтвердили предположение Дэна Бернштейна (*Ronald Cramer, Léo Ducas, Chris Peikert, Oded Regev. «Recovering Short Generators of Principal Ideals in Cyclotomic Rings»*. In Eurocrypt 2016; *Jean-François Biasse and Fang Song, «Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields»*. In 27th ACM-SIAM Symposium on Discrete Algorithms, 2016).

Иначе говоря, теперь уже строго и для всех показано, что да, действительно, новые и вроде бы сугубо «квантовые» подходы к решению трудных криптографических задач на самом деле позволяют ощутимо снижать трудозатраты также и при взломе криптосхем с помощью компьютеров классических.

Конкретно о компрометации схемы ECC пока нигде и ничего открыто не объявлено. Но это, похоже, уже лишь дело времени…

# # #

Дополнительное чтение

О множестве других случаев с незаметным изъятием спецслужбами существенных фактов и знаний: «**Выпиливание реальности**»

Об удивительной и отчасти мистической истории про одновременное открытие криптографии с открытым ключом в спецслужбах и в академических кругах: «**Параллельные миры**»

О том, как спецслужбы с помощью грантов и стипендий контролируют разработки открытой академической криптографии: «**Инженерия науки**»

Шизо-крипто, Ответственное крипто и другие формы патологического оккультизма

Шизо-криптография

(*Апрель 2015*)

Непосредственно сейчас на стыке большой политики и защиты информации из уст высокого государственного руководства по всему миру звучит просто-таки зашкаливающее количество неправды.

И если воспринимать всю эту ложь всерьез – как объективный показатель (не)честности тех людей, которые регулярно и повсюду становятся вождями человечества, – то вся цивилизация наша выглядит одной большой ошибкой природы, тупиком и безнадёгой.

Но с другой стороны, если смотреть на ситуацию с медицинской точки зрения, считая нынешнее состояние власти чем-то вроде тяжелой, но все-таки излечимой болезни, то появляется и некоторая надежда на выздоровление.

Ну а дабы суть происходящего – окруженного ощутимым полем психиатрического расстройства – стала понятнее и для тех, кто мало что смыслит в тонкостях медицины и защиты информации, первым делом полезно привести пару содержательных цитат.

Фрагмент первый – из стандартных справочников и словарей по терминологии современной психиатрии. Где тоже, если кто не в курсе, имеется термин «криптография», но означает он несколько иные вещи:

«***Криптография****: создание психически больными нового символического письменного кода. Наблюдается при шизофрении. Отражает в письменной речи явление криптолалии.* ***Криптолалия:*** *создание больными новой, нелепой «речи», сплошь состоящей*

из неологизмов и не могущей служить средством коммуникации между людьми. Наблюдается при шизофрении»…

Фрагмент второй – для наглядной демонстрации того, что на самом деле имеется не просто терминологическая, но и куда более глубокая-таинственная связь между «оккультным» (как считалось веками) искусством криптографии и психическим здоровьем человека. Данная цитата относится к жизни персонажа, своими блестящими достижениями весьма знаменитого в истории секретных спецслужб и криптографической науки XX века:

> *Хранение в себе такой массы государственных тайн не могло сильнейшим образом не сказаться на здоровье У.Ф.Ф. – как на психическом, так и физическом. Про моральную сторону главного дела всей своей жизни – чтения почты других людей – он написал такие слова: «Я часто задавал себе вопрос, а не была ли вызвана львиная доля моих психических проблем на протяжении всех этих долгих лет – хотя бы отчасти, по крайней мере – вот этой двусмысленностью моей работы»…*
>
> *Когда же один давний приятель как-то по случаю спросил его, а не является ли необходимостью быть сумасшедшим, чтобы быть криптографом, У.Ф.Ф. ответил ему так: «Необходимости в этом нет, но в работе это помогает»…*

Конкретнее о том, что за человек был У.Ф.Ф., о том, как звали его приятеля (тоже далеко не последнего человека в мировой индустрии криптографии), и о том, сколь интересен был исторический контекст, на фоне которого дружили эти люди, речь пойдет чуть позже. А пока самое время напомнить, чем же таким психиатрически-настораживающим удивляет текущая ситуация вокруг стойкого шифрования информации.

#

Рассуждая отвлеченно и абстрактно, крайне глупо было бы утверждать, будто на руководящие посты в наиболее мощных и влиятельных государствах планеты то и дело пробираются не просто психически неустойчивые люди, но и вообще натуральные шизофреники. Ведь понятно же, что руководить государством должны люди непременно со здоровой и стабильной душевной организацией.

Но вот если конкретно и повнимательнее прислушаться к тем вещам, что заявляют ныне первые государственные лица, то на данный счет закрадываются сильнейшие сомнения. А чтобы они стали понятны всем, достаточно лишь взглянуть на медицинское определение недуга:

Шизофрения *(от др.-греч. «расщепление рассудка») – психическое заболевание, связанное с распадом процессов мышления, рассогласованностью эмоциональных реакций и неадекватным восприятием реальности. Наиболее частыми проявлениями болезни являются галлюцинации, параноидный или фантастический бред.*

Если процитированное определение не вызывает протестов и возражений, то теперь уместно привести слова и аргументы большого человека в госадминистрации США, директора ФБР Джеймса Коми, с помощью которых он пытается сегодня убедить общество и законодателей в том, что стойкое шифрование файлов и коммуникаций – это абсолютное зло, которое вот-вот разрушит всю работу правоохранительных органов:

> *Мы сползаем к такой ситуации, когда очень многие люди начнут смотреть на нас со слезами на глазах и говорить нам: «Что это значит, что вы не можете? Моя дочь пропала. У вас есть ее телефон. Что это значит, что вы не можете мне сказать, с кем и о чем она переписывалась, прежде чем исчезла?»… Когда я слышу, как руководители ИТ-индустрии заявляют, будто (сильное крипто,) приватность и тайна личной жизни должны быть превыше всего, я закрываю глаза и говорю себе: «Только попытайся представить себе, как выглядит мир, где педофилов нельзя увидеть, где нельзя увидеть похитителей людей, нельзя увидеть наркоторговцев»…*

Сами по себе эти слова, конечно же, еще не доказательство, что у шефа ФБР «не все дома». Хотя для экспертов, знакомых с технической стороной проблемы, тут сразу же видно, что в подобной аргументации помимо чрезмерной эмоциональности нет никаких убедительных фактов и доказательств. Более того, специалисты, знакомые с историей вопроса, тут же припомнят, что по сути те же самые аргументы привлекал 20 лет назад другой директор ФБР, Луи Фри, когда надо было навязать «клиппер-чип» и запрет на стойкую криптографию при администрации Билла Клинтона. Короче, история известная и ничего особо нового тут вроде бы не звучит.

Существенно новым в нынешней ситуации является то, что и в других больших-влиятельных государствах власти ныне дозрели до похожей крипто-психологии – и открыто предлагают США сражаться с мировым злом совместно. В частности, власти Китая объявили, что тоже видят в сильной криптографии серьезную помеху для своей борьбы с террористами и преступниками. А потому отныне будут требовать встраивание «бэкдоров» («черного хода» для доступа правоохранительных органов к зашифрованной информации) в любых коммуникационных сервисах и устройствах, продаваемых на китайском рынке. Включая и все американские инфотехнологии, естественно.

Рассуждая хоть и наивно, но в духе здравомыслия, логично предположить, что при столь очевидном единодушии в выборе врагов и методов борьбы с ними, властям США и Китая тут было бы очень легко договориться. Однако в реальной жизни мы наблюдаем нечто диаметрально противоположное.

Президент США Барак Обама в самых решительных выражениях раскритиковал и отверг все подобные предложения Китая:

> *«(Эти их новые законы) по сути дела заставили бы все иностранные компании, включая и компании США, предоставлять китайскому правительству механизмы, с помощью которых они смогут шпионить и отслеживать деятельность всех пользователей… (На переговорах с*

китайским руководством) Мы заявили им очень ясно и отчетливо, что они должны изменить эту позицию, если намерены продолжать совместные дела с Соединенными Штатами»…

После столь решительной отповеди человеку постороннему было бы довольно легко предположить, что у лидеров некогда «самой свободной страны мира» что-то там опять поменялось в приоритетах и ценностях, они вдруг поняли, что «шпионить и отслеживать деятельность всех пользователей» – это же действительно как-то нехорошо и некрасиво (тотальная и постоянная слежка, отказ от презумпции невиновности, все такое прочее). А потому, вероятно, теперь у США здесь наметилась какая-то новая, более здравая позиция.

На самом деле ничего подобного нет и даже не намечалось. Власти США как и прежде решительно настроены ослаблять всю сильную криптографию – но только почему-то уверены, что это дозволено исключительно им. А в качестве укрепления этой странной позиции изобретается как бы новый, понятный лишь для них самих язык (см. психиатрическое определение криптолалии).

Теперь то, что прежде все именовали «бэкдорами», американские лидеры называют Front-door («парадная дверь», ибо государство – которому все граждане обязаны слепо доверять – имеет полное право входить в любой дом через парадную дверь, если сочтет это необходимым). Попутно для того же самого, по сути, появился и еще более витиеватый термин – «золотой мастер-ключ». Объяснять смысл термина, вероятно, не требуется. Но вот с какой стати власти США решили, что таким чудо-ключом смогут пользоваться лишь они одни, этого не знает никто.

Гигантскую американскую ИТ-индустрию, которая уже вполне ощутимо несет потери в доходах и репутации из-за непомерных аппетитов своих спецслужб, пытающихся следить за всеми сразу и разоблаченных в файлах от Эдварда Сноудена, эта позиция властей сильно беспокоит (выряжаясь помягче). На одной из недавних встреч капитанов индустрии с адмиралом Майком Роджерсом, нынешним директором АНБ США, соответствующие вопросы были заданы в совершенно конкретной форме:

«Если мы будем встраивать слабости / бэкдоры или золотые мастер-ключи для правительства США, то считаете ли вы, что мы должны делать то же самое – а мы (компания Yahoo!) имеем около 1,3 миллиардов пользователей по всему миру – делать то же самое для китайского правительства, для российского правительства, для правительства Саудовской Аравии, для Израиля, для французского правительства?»…

Принимая во внимание отчетливое «расщепление рассудка» в позиции американской госадминистрации по данной проблеме (как и по множеству других, впрочем), понятно, наверное, что на столь прямо поставленный вопрос адмирал Роджерс в принципе не мог дать столь же прямой ответ типа «да» или «нет». Естественно, он начал увиливать и уходить в абстрактные рассуждения «про надлежащие юридические рамки для доступа правоохранительных органов». Но аудитория ему попалась уже тертая, так что главу АНБ все же вынудили вернуться к сути вопроса и сформулировать свою позицию в более конкретном виде.

Однако и после нажима единственное, что смог тут выдать адмирал по сути, прозвучало в таком виде: «Я думаю, что мы сможем проложить наш курс в такого рода обстоятельствах». И все, на этом обсуждение темы было им закрыто…

#

Из всей этой истории несложно, наверное, понять, что власти и спецслужбы США совершенно определенно и категорически намерены и дальше следовать своему расщепленному крипто-курсу. Несколько труднее понять техническую сторону дела – а как же конкретно им мыслится воплощение подобных идей в условиях, когда все вокруг, казалось бы, уже вполне осведомлены про эту государственную шизофрению…

И вот чтобы хоть как-то прояснить эту сторону проблемы (полностью понять ее, к сожалению, даже людям с относительно здоровой психикой пока не по силам), будет очень полезно и поучительно обратиться к двум вещам. (1) К медицинскому определению криптографии – как «созданию особого кода, порождаемого психически больными». И (2), к истории жизни того самого У.Ф.Ф., который со своими странными идеями – о связях сумасшествия и криптографии – фигурировал в самом начале данного текста.

Звали этого человека Уильям Фредерик Фридман (1891 – 1969). В истории же XX века он наиболее известен как один из самых выдающихся криптографов и родоначальников криптологической науки, с одной стороны, а также, со стороны другой, как один из отцов-основателей крупнейшей на этой планете шпионской спецслужбы – Агентства национальной безопасности США, или кратко АНБ.

Еще одним примечательным моментом в личности данного человека – об этом по естественным причинам упоминают куда реже – следует считать довольно хрупкую и неустойчивую психику Фридмана, из-за чего он неоднократно оказывался в больницах для психиатрического лечения и реабилитации. Для нас же сейчас этот момент оказывается наиболее интересен, а в особенности – любопытны те конкретные причины и обстоятельства, при которых у великого криптографа происходили психические срывы и расстройства.

Первый эпизод такого рода имел место в конце 1941 года, сразу же после разгрома японцами тихоокеанского флота США в Пёрл-Харборе. Для Уильяма Фридмана, который в ту пору возглавлял криптоаналитическое подразделение армии США, это сокрушительное военное поражение его страны стало еще и тяжелейшей личной трагедией. Потому что он не только чувствовал личную ответственность за произошедшее, но и был абсолютно уверен, что его криптографы сделали все для предотвращения этой катастрофы.

Здесь надо пояснить, что очень успешное вскрытие шифров Японии было предметом особой гордости Фридмана и его команды. Американские криптоаналитики на регулярной основе обеспечивали массовое дешифрование как военной, так и дипломатической переписки этого потенциального противника, постоянно снабжая власти США наиболее достоверной информацией о намерениях японского руководства.

Но в делах высокой государственной политики, как известно, из-за вечных конфликтов интересов ничего не бывает просто. И очень непросто, в частности, выглядели расклады той поры в высших эшелонах власти США. По-прежнему оставаться нейтральной в полыхавшей мировой войне Америке становилось все труднее, но если президент Ф.Д. Рузвельт был очень решительно настроен против нацистов и видел будущее США только в союзе с Великобританией, то в американском Конгрессе, напротив, весьма и весьма сильными были прогерманские и антисоветские настроения.

В таких условиях у Рузвельта практически не было шансов «просто так» получить одобрение Конгресса на присоединение к антигитлеровской коалиции. А если бы он сделал это самостоятельно, в обход законодательной власти, то перед президентом, нарушающим конституцию, всерьез замаячила бы процедура отрешения от власти. С другой же стороны, поскольку Япония, как главнейший потенциальный враг США в тихоокеанском регионе, была военным союзником гитлеровской Германии, то жестокое и вероломное нападение японских милитаристов стало бы очень подходящим поводом или рычагом для решительного вывода страны из подвешенно-неопределенного состояния…

В истории США до сих пор остаются спорными и как бы туманно-неясными вопросы о том, где, как и почему задерживались дешифрованные японские телеграммы с важной информацией о явно готовящемся ударе по американскому флоту. Но зато достоверно известно, что после катастрофы в Пёрл-Харборе у шефа криптоаналитиков Уи-

льяма Фридмана натурально «поехала крыша» – он фактически перестал что-либо соображать и реагировать на окружающих, непрерывно повторяя только одно: «Но ведь они же знали, они же знали, они же знали»…

В общем, лично для У.Ф. Фридмана вступление США в мировую войну ознаменовалось его первым попаданием на койку в психлечебнице. А примерно еще через десяток лет история повторилась. И опять при весьма двусмысленных криптографических обстоятельствах.

Поскольку среди главных итогов победы антигитлеровской коалиции оказались не только беспрецедентно возросшие военно-политическая мощь и амбиции США на мировой арене, но также и соразмерно развившиеся аппетиты и возможности американских спецслужб, в делах шпионских стали происходить очень большие перемены. Сначала, в 1947, под сильным влиянием британских коллег была создана крупная и сильная разведструктура под названием ЦРУ. А еще через пять лет по аналогичной схеме несколько разрозненных криптографических и радиоразведывательных подразделений в составе вооруженных сил и правительства были объединены в мощную, единую и чрезвычайно секретную спецслужбу – АНБ США.

Естественным образом оказавшийся у истоков создания этого агентства, Уильям Фридман в тот период пребывал уже в весьма солидном предпенсионном возрасте (официально он уйдет на покой в 1955), занимая почетные должности помощника директора и консультанта по научно-исследовательским вопросам. Однако и в этом качестве ему довелось сыграть ключевую оперативную роль в одной очень важной, деликатной и по сию пору официально засекреченной миссии.

Для независимых историков криптографии, впрочем, эта тайная миссия давным-давно уже никакой не секрет, и в данной профессиональной среде она известна под условным наименованием «операция BORIS». Ибо именно так, Борис Хагелин, звали одного давнего приятеля Уильяма Фридмана. Этот шведский изобретатель и предприниматель в годы войны стал миллионером на поставках вооруженным силам США своего шифратора Hagelin, а после победы над нацистами сделал еще один гениальный ход – разместив штаб-квартиру своей фирмы Crypto AG в нейтральной Швейцарии, «надежной, как ее часы, банки и армейские ножи».

Специфическая аура нейтральности и надежности не только обеспечили Crypto AG быстрый и внушительный успех на мировом рынке шифраторов, но также сподвигли и еще несколько подобных фирм сделать своей базой Швейцарию. Поэтому именно туда в начале 1950-х был направлен Уильям Ф. Фридмен – дабы склонить к тайному сотрудничеству с разведкой США прежде всего Хагелина, а может и прочих, кого получится.

О деталях этих переговорах, ясное дело, ничего толком неизвестно, поскольку соответствующие отчеты до сих пор спрятаны в топ-секретных архивах спецслужб. Но благодаря проведенным в 1970-1990-е годы расследованиям журналистов было достоверно установлено, что АНБ, всячески запугивая «нейтральных» изготовителей шифраторов коммунистической угрозой, сумело склонить их к сотрудничеству. Итогом же этого сотрудничества стала разработка особых, «расщепленных» или шизо-криптографических схем, которые для всех представлялись как бы стойкими и надежными, а для криптоаналитиков АНБ позволяли без проблем вскрывать шифрпереписку, засекреченную такого рода алгоритмами…

Именно тогда, похоже, и родился знаменитый ныне принцип работы АНБ под названием NOBUS, расшифровываемый как «никто кроме нас» (Nobody But US). И именно тогда, скорее всего, в самом начале доверительных бесед Фридмана с давним приятелем, Хагелин, впервые услышав о столь фантастических замыслах американской разведки, сказал коллеге что-то вроде «Да вы там совсем уже рехнулись, что ли»…

Какие конкретно слова в тот момент звучали, впрочем, никто достоверно не знает. Но зато вполне достоверно, из письменного свидетельства жены Фридмана (тоже правительственной криптографини, кстати) известен тот финал диалога между У.Ф.Ф. и Борисом Хагелином, который приведен в самом начале настоящего текста – о том, что

сумасшествие для криптографа не обязательно, но может ощутимо помогать в работе…

Слова эти, наполненные горькой иронией, очень хорошо запомнились Элизбет Фридман по той, вероятно, причине, что по возвращении из служебной командировки в Швейцарию ее муж впал в сильнейшую депрессию, переросшую в психическое расстройство и закончившуюся очередным лечением в стационаре… Опять подлечившись, впрочем, Фридман еще не раз в 1950-е годы посещал европейских соратников.

#

Подводя итоги этой шизо-криптографической истории, обязательно следует отметить вот какую настораживающую вещь. В отличие от обычной шизофрении, которая, насколько известно медицине, не передается между людьми как инфекция, воздушно-капельным или половым путем, криптографическая форма той же болезни очевидно штука заразная.

И едва в США обозначилось обострение этого недуга (судя по характерным заявлениям директоров ФБР и АНБ), как тут же с очень похожими признаками инфекции стали выступать лидеры других стран и организаций – настаивая на ослаблении стойкого крипто и необходимости полного контроля за коммуникациями граждан: премьер-министр Великобриатнии Джеймс Камерон, шеф Европола Роб Вэйнрайт, первые лица Франции, власти Китая и России, ну и так далее, список зараженных прирастает с каждым днем.

Но есть, впрочем, и хорошие новости. В силу понятных причин (хвала Эдварду Сноудену), на данном этапе развития как большому так и малому ИТ-бизнесу гораздо выгоднее открыто выступать на стороне общества, а не ложиться под пресс тайных соглашений со шпионскими спецслужбами. Так что идеи и технологии стойкой, удобной в использовании криптографии востребованы на рынке куда лучше, нежели концепция спецслужб об обязательных бэкдорах (которыми смогут воспользоваться не только честные правоохранители, но и преступники любого сорта – что понимают все, кроме зараженных вирусом шизо-крипто).

Ну а кроме того, в обществе постепенно нарастает осознание, что в нынешних условиях тотальной ИТ-слежки применение людьми стойкого крипто становится не столько правом, сколько обязанностью всякого ответственного гражданина. Ибо только так и можно остановить сползание к тирании серьезно заболевшего государства… Но это впрочем, уже другая большая история.

# # #

Дополнительное чтение

О «хартии вольностей» для интернета и необходимости стойкого крипто для общества: «**Права и обязанности**»

О глубине болезни, поразившей государство, и о роли тут криптографии: «**Сноуден как повод**», «**Всего три слайда**»

О том, как интернет и программа PGP вызвали обострение шизо-крипто 20 лет назад: «**Клиппер, шкипер, фриц и …**»

О том, как шизо-крипто-вирус NOBUS подцепляла ИТ-индустрия: корпорация Apple – «**Никто кроме нас**»; и корпорация Microsoft – «**Хитрости крипторемесла**»

О крайне необычных страницах в биографии Уильяма Фридмана: «**Наука a la Ривер-бэнк**», «**Объяснимые слабости**», «**Крипто-акустика**»

«Ответственное крипто» и другие формы обмана

(*Ноябрь 2017*)

Мировому сообществу активно навязываются в качестве стандарта новые шифры от АНБ США. Имеет смысл разобраться, что в них действительно нового. И что, соответственно, старого…

Международная организация стандартизации ISO, как известно, насчитывает в своих рядах свыше 160 государств планеты и постоянно заботится о единых подходах человечества ко всем жизненно-важным вещам – от автодорожных знаков до упаковок для лекарств. Обычно все проблемы, сопутствующие этому кропотливому делу, решаются здесь без шумных скандалов и за закрытыми дверями.

Ныне, однако, один из традиционно тихих процессов такого рода – закрученный вокруг новых стандартов шифрования и длящийся уже три с лишним года – как-то вдруг перерос в столь горячие и оживленные дебаты, что шум от них даже выплеснулся на страницы служб новостей и прочих СМИ. Благодаря чему, собственно, всем и стало известно, какого рода любопытные вещи творятся сейчас с криптографией за спиной у широкой публики.

Если говорить о разыгравшемся скандале с шифрами совсем кратко, то суть конфликта тут вот в чем. Два новых криптоалгоритма, носящих названия Simon и Speck, активно продвигаются делегацией США в качестве очередного мирового стандарта индустрии для шифрования данных. Главных же проблем здесь две. Во-первых, у мирового сообщества сейчас нет потребности в новом крипто такого рода, так что никто ни американцев, ни кого-либо еще об этом не просил.

Ну а, во-вторых, самое главное, оба этих шифра разработаны знаменитой шпионской спецслужбой под названием Агентство Национальной Безопасности или АНБ США, что на сегодняшний день – в эпоху «после разоблачений Эда Сноудена» – ничего кроме подозрений вызвать не может.

Именно поэтому, собственно, делегации целого ряда влиятельных стран в ИСО, включая ближайших союзников США вроде Германии, Израиля и Японии, выступили активно против этих американских предложений. Вполне резонно предполагая, что АНБ энергично проталкивает свои новые алгоритмы в мировые стандарты не оттого, что это хорошие инструменты для защиты данных, а по той причине, что там знают, как эти шифры вскрывать…

#

Прежде чем переходить к выразительным техническим подробностям конфликта в ИСО, однако, весьма кстати будет также упомянуть и о совсем других событиях из текущих новостей. Для более объемного восприятия межнациональных стычек среди экспертов по стандартам и для погружения этого крипто-конфликта в соответствующий общественно-политический контекст, можно сказать.

На первый взгляд, эта пара иных новостей – про публичные выступления больших боссов из Министерства юстиции США – рассказывает о чем-то существенно другом, хотя и тоже очевидно связанном с криптографией. Однако на самом деле, если присмотреться повнимательнее, в свежих речах заместителя генпрокурора Рода Розенштейна и директора ФБР Кристофера Рэя, призывающих искусственно ослабить все коммерческие криптоалгоритмы и запретить по-настоящему сильные шифры, имеет место просто другая подача тех же самых государственных инициатив США, что и в ISO. Блюдо одно, только соусы разные.

Нет никакого смысла, в общем-то, пересказывать здесь подробности из нынешних докладов руководства американской генпрокуратуры и ФБР, ибо люди на высоких постах меняются, а одни и те же идеи озвучиваются ими на протяжении вот уже четверти века, как минимум. Примерно с тех пор, как к началу 1990-х у народа стали массово появляться персональные компьютеры, интернет-доступ и действительно сильные средства шифрования типа криптопрограммы PGP от Фила Зиммермана.

Для общего же представления о том, в чем здесь суть посыла властей к широкой публике, достаточно процитировать наиболее яркий момент из октябрьской, 2017 года речи Рода Розенштейна:

> *«Такое шифрование, которое не вскрывается по предписанию суда, подрывает конституционный баланс – ставя приватность граждан выше общественной безопасности. Те зашифрованные коммуникации, которые нельзя перехватить, и те запертые криптографией устройства, которые нельзя открыть, – всё это зоны беззакония, позволяющие преступникам и*

террористам действовать без их выявления полицией, без обязанности отвечать перед судьями и судами присяжных.»

Во всех подобных заявлениях, как это давно заведено, очень слабая логика аргументов с лихвой компенсируется мощным напором на эмоции слушателей. Ведь люди в массе своей не только крайне негативно, но и особо эмоционально относятся к деятельности террористов, наркоторговцев и прочих отвратительных педофилов. А потому под знаменем борьбы с этими разрушителями общества очень заманчиво проталкивать любые непопулярные меры – вроде тотального контроля за коммуникациями и личными записями граждан.

Но поскольку даже очень эмоциональные аргументы властей по сию пору так и не смогли убедить народ, что «во имя общественной безопасности» все поголовно обязаны принести в жертву свои права на тайну личной жизни, настойчивые потуги запретить сильное крипто повторяются вновь и вновь. Причем вместе с каждой новой попыткой для неизменно той же самой навязчивой идеи всякий раз власти пытаются изобрести какое-нибудь еще маскирующее название.

Поначалу, в прошлом веке, это называли «депонирование ключа». Затем решили, что ненавистный всем тайный «черный ход» (Backdoor, каковым и являлось депонирование) будет восприниматься лучше, если называть его иначе – «парадной дверью» для доступа властей. Еще одно недавнее лексическое изобретение мудрецов для того же самого – «золотой мастер-ключ». И вот теперь – когда все прочие замыслы бесславно провалились – изобретен новый термин «ответственное шифрование».

Как и прежде, высокие чиновники понятия не имеют, каким образом это самое их «ОШ-не-бэкдор» может быть эффективно реализовано в технических аспектах – сделать так, чтобы зашифрованные данные становились легко доступными лишь для одной «надзирающей за порядком стороны», но чтобы при этом ни аналогичные «надзиратели» других государств, ни злоумышленники-хакеры ничего подобного делать бы не могли…

Знающие профессионалы уверены, что это невозможно сделать в принципе. Если слабость в крипто заложена, то рано или поздно её непременно отыщут. Или просто украдут – была бы надлежащая мотивация. Однако власти (далеко не только в США, кстати) все время упорно декларируют, что если как следует подумать, то задача окажется решаемой.

Более того, тот же же зам-генпрокурора Розенштейн в своих речах для несведущей публики даже попытался создать впечатление, будто разного рода примеры «ответственного шифрования» на самом деле уже реально воплощены и вполне хорошо работают. Надо лишь сделать так, чтобы эти же вещи народ массово одобрил для применения в смартфонах и всех прочих цифровых устройствах.

Проблема с доводами большого босса из Минюста в том, что все приведенные в его докладе примеры «работающего ОШ» – это либо не раз уже разоблаченная ложь про надежные крипто-бэкдоры, либо про то, что вообще криптографией не является. Подробный и компетентный разбор конкретно этой лжи от Розенштейна – на английском языке – можно найти **тут** и **тут**, к примеру.

На языке же русском вполне убедительные опровержения для всего этого гранд-обмана в целом – причем исходящие примерно от таких же высокопоставленных госчиновников США, что интересно – можно найти в тексте «*Плохой носорог, хороший носорог*». Где бывшие начальники американской разведки, министерства обороны и госбезопасности уверенно и авторитетно всем доказывают, что сильное крипто – это очень хорошо для национального бизнеса, а значит, и для сильной процветающей страны. Ну а врагов общества сильное государство вполне способно нейтрализовать по-любому – невзирая на всех их шифры и коды…

#

Упоминание о существенно разных – а внешне так и вообще диаметрально противоположных – взглядах разных госначальников США на «сильную криптографию для народа и бизнеса» было сделано, конечно же, не случайно. Ибо в сюжете, начинавшем историю – о конфликте вокруг нового крипто-стандарта в ИСО – государство США позиционирует себя как сторона, настойчиво предлагающая всем и задаром подчеркнуто сильные новые шифры. Без всяких там бэкдоров, типа.

Любой человек, способный к аналитическим размышлениям, способен распознать тут очевидные логические нестыковки. Если руководство одного и того же государства – в независимости от находящихся у руля президентов и партий – давно и настырно борется со стойкими шифрами у широкой публики, а одновременно энергично навязывает всему миру «сильное крипто» собственного изготовления, то что-то здесь явно не так…

Если же начать копать эту тему поглубже – как о происхождении нынешних шифров Simon и Speck, так и вообще о сюжетах с участием спецслужбы США в «криптографии для всех» – то первичные подозрения относительно обмана быстро перерастают в твердую уверенность. Уверенность в том, что из источника под названием АНБ ничего такого, чему могли бы доверять остальные, не способно появиться в принципе.

Уже по той лишь причине, что в целях и задачах этого шпионского агентства такой вещи как «стойкое крипто для всех» никогда не было и вряд ли когда будет. Просто по определению. Помимо же абстрактных определений того, в чем заключается суть шпионской работы, имеется и вполне конкретный исторический контекст. С которым очевидно имеет смысл ознакомиться – для общего понимания происходящего.

#

Первые сигналы о появлении в АНБ новых интересных криптоалгоритмов Simon и Speck, которые это агентство вознамерилось безвозмездно подарить мировому сообществу, начали звучать в 2012 году. В частности, в **одном из докладов** на криптографической конференции индустрии, проходившей в тот год в Швеции, два знающих техасских эксперта со связями в спецслужбах рассказывали о текущих итогах и перспективах защиты информации в RFID-чипах. И среди упоминаний о примечательных новых шифрах, не только быстрых-надежных, но и компактных или «лёгких», чтобы работать в минималистичных условиях вроде чипов смарт-карт и «интернета вещей», прозвучала у них такая информация (со ссылкой на недоступный публике технический отчет АНБ):

> *«АНБ США недавно опубликовало [впечатлившие авторов] характеристики для Simon и Speck, двух семейств шифров их собственной разработки… Но для того, однако, чтобы эти шифры могли бы стать полезными коммерции, индустрии и широкой публике, также должны быть опубликованы и детали об устройстве алгоритмов. Это сделает алгоритмы пригодными для процедур стандартизации, поскольку без них международное сообщество в большинстве своем не торопится слепо доверять технологиям, исходящим из аппарата национальной безопасности любого государства»…*

Происходило это «первичное знакомство», еще раз подчеркнем, летом 2012 – примерно за год до публикации первых разоблачений от Эдварда Сноудена. То есть в тот период, когда все разговоры о тайных манипуляциях АНБ, ослабляющего в своих интересах любую криптографию, до которой удается дотянуться, звучали исключительно на уровне слухов и домыслов, не имея никаких документальных тому подтверждений.

Иначе говоря, в АНБ уже в ту пору был запущен небыстрый процесс подготовки шифров Simon и Speck к внедрению их в качестве мирового стандарта. Ну а то, что **общедоступная публикация** деталей об этих криптоалгоритмах летом 2013 совпала по времени с громким скандалом вокруг файлов от Сноудена – это, конечно же, оказалось не только очень неприятным сюрпризом для АНБ и США в целом, но и крайне неудачным совпадением для публичной презентации Simon и Speck в частности.

Как бы там ни было, шестеренки большой государственной машины в тот период уже вовсю крутились, так что на следующий год, в 2014, делегация США в ISO официально внесла шифры АНБ Simon и Speck в качестве своих кандидатов на новый мировой стандарт криптоалгоритмов, призванных «удовлетворить нужды в безопасных, гибких и поддающихся анализу облегченных блочных шифрах». Каждый из алгоритмов – образец превосходной производительности, причем Simon заточен для оптимальной работы в условиях аппаратной реализации на чипе, а Speck, соответственно, для удобных и компактных программных воплощений.

Несмотря на многочисленные достоинства этого счастья – щедро предлагаемого для всех и даром – сразу несколько национальных делегаций в ISO весьма решительно и сходу выразили, однако, свои категорические возражения против такого подарка от профессионалов спецслужбы США. Разоблачения от Сноудена впечатлили народ настолько глубоко и сильно, что представители Германии, Израиля и Японии – традиционных союзников США на политической арене – сочли необходимым подчеркнуть, что они работают в ИСО для обеспечения безопасности мировых стандартов, а не для их ослабления по рецептам АНБ.

Прямых доказательств, свидетельствующих о «не самой сильной» (скажем так) криптостойкости новых шифров, что надо подчеркнуть, ни у кого из противников Simon и Speck не было ни в первые годы инициативы, ни по сию пору. И вряд ли это должно кого удивлять. Криптографическая стойкость всякого подобного алгоритма определяется его способностью выдерживать «любые из известных крипто-атак». Если же какая-то из сторон изобрела принципиально новый способ анализа-взлома шифров, но никому о нем не рассказала, то для этой стороны, ясное дело, уровень криптостойкости начинает выглядеть существенно иначе, чем для остальных.

Примерно этого, собственно, и опасаются не-американские специалисты-криптографы, представляющие в ИСО национальные интересы своих стран, а заодно и всего мирового сообщества. Причем основания для подобных опасений не только вполне понятны, но и прочно подкрепляются множеством уже известных прецедентов из жизни.

#

Один из наиболее ярких, пожалуй, примеров среди прецедентов такого рода предоставляет история появления DES – самого первого и самого знаменитого блочного криптоалгоритма, в рождении которого непосредственно принимало участие и АНБ США. Причем уже тогда, в середине 1970-х годов, участие это имело весьма специфические формы, всегда характерные для этого шпионского ведомства и его знаменитого ныне девиза NOBUS или «никто кроме нас» (NObody But US).

Главным отцом-изобретателем, создавшим прототип всех нынешних блочных шифров, был Хорст Фейстел, никак не связанный с АНБ ученый корпорации IBM. Придуманная им схема повторяющихся криптографических преобразований над блоками данных, известная ныне как «сеть Фейстела», была заложена ученым в исходный вариант прототипа, получившего название «шифр Lucifer». Безусловно интересный, но редко вспоминаемый сегодня факт истории заключается в том, что уже самый первый вариант «Люцифера», представленный широкой публике в статье Хорста Фейстела для научно-популярного журнала Scientific American в 1973 году, имел весьма сильные – даже для современных шифров – базовые характеристики в своих параметрах: 128 битов для длины ключа и 128 битов для длины блока.

Когда же в IBM решили выдвинуть криптоалгоритм Фейстела в качестве всеобщего стандарта индустрии для шифрования компьютерных данных, то в качестве «многоопытного эксперта», способного модифицировать разработку любителей до надлежащего профессионального уровня, было привлечено Агентство национальной безопасности США. Результатом этого специфического сотрудничества, как известно, и стал первый глобальный криптографический стандарт DES. Получивший в итоге не только сокращенную до 64 битов длину блока, но и весьма странный размер ключа – длиной 56 битов.

В силу особенностей обработки двоичных данных в компьютерах, для алгоритмов и регистров более естественно оперировать такими блоками данных, длина которых выражена степенями двойки (32, 64, 128). В данном же случае даже уменьшенную вдвое, до 64 битов, исходную длину ключа по настоянию АНБ сократили еще на 8 разрядов. Существенно позднее от инсайдеров стало известно, что изначально эксперты АНБ настаивали на размере 48 битов, однако в IBM сочли столь малый ключ слишком уж сильным ослаблением шифра, так что 56-битная длина появилась в качестве своего рода компромисса.

Сегодня, когда вспоминают DES, обычно принято подчеркивать, что АНБ существенно укрепило криптостойкость шифра – модифицировав его модули преобразований (S-боксы) таким образом, чтобы DES не поддавался взлому методами «дифференциального криптоанализа». Хотя термина такого в те времена еще не было (его введут самостоятельно переоткрывшие данную вещь израильские ученые в 1990-е), суть этого очень мощного метода взлома была известна уже в 1970-е – причем не только специалистам АНБ, но и создателям шифра в IBM. Вот только информацию эту тогда же строго засекретили и от всех прочих оставили в тайне.

В итоге же всех таких манипуляций родился знаменитый шифр DES. Действительно сильный криптоалгоритм, на протяжении всего срока службы стойко противостоявший всем известным методам взлома – за исключением тотального перебора ключей. Этот лобовой – и очень недешевый – метод вскрытия стал доступен открытому сообществу криптографов лишь к концу 1990-х. Ну а в секретных недрах АНБ, опять же по свидетельству инсайдеров, лобовой взлом ключей DES был доступен изначально – по заранее составленным и отсортированным массивам шифрблоков, хранимых на магнитных лентах (ныне этот трюк именуется Rainbow Tables или «радужные таблицы»).

Именно поэтому, скорее всего, в АНБ и согласились на длину ключа 56 битов. По состоянию финансово-технических возможностей в 1970-80-е годы вряд ли кто еще мог иметь столь же дорогущий инструментарий вскрытия, какой был у самой богатой спецслужбы США. То есть перед нами классический пример опоры на принцип NOBUS во всей его исключительности…

Если же перенестись в день сегодняшний, к межнациональному конфликту стандартизаторов вокруг наследников DES под названием блочные шифры Simon и Speck, то здесь ныне происходят такие любопытные коллизии. Когда пресса (служба новостей Reuters), прознав про суть конфликта, напрямую спросила у АНБ, «а могут ли они сами вскрывать свои предложенные в ISO шифры?», то ответ спецслужбы прозвучал как образец двусмысленности: «Мы твердо верим, что они безопасны».

Глядя же иначе, это предельно честный ответ профессионалов, если вдуматься. Профессиональных шпионов, знающих реальную ситуацию, конечно, но обязанных всегда хранить её в тайне. Ведь абсолютно то же самое можно было не кривя душой говорить и про шифр DES на протяжении 20 лет его службы. Шифры безопасны, потому что никто не сумеет их вскрыть… кроме нас.

(Имеет смысл обратить внимание на использование слова «верим» – а не «знаем». Даже могущественное АНБ не может знать наверняка, что реально умеют делать не менее хитроумные спецслужбы других стран. Но поскольку и те держат свои умения в строгой тайне, данный нюанс – просто часть общей «игры в безопасность».)

#

Еще один выразительный пример из ряда «АНБ и крипто для всех» – это сравнительно недавняя история с алгоритмом Dual_EC_DRBG. То есть «генератором случайных битов на основе эллиптических кривых», который в 2000-е годы был очень настойчиво навязан американской спецслужбой мировому сообществу инфобезопасности и при этом имел в себе вполне отчетливый бэкдор. Среди делегатов ISO, ныне энергично выступающих против новых даров от АНБ, многие подчеркивают, что их недоверие и скептицизм в значительной степени базируются на бесславной истории с принятием Dual_EC в качестве всеобщего стандарта для генерации крипто-ключей.

На сегодняшний день уже достоверно известно, что во внутренних секретных документах АНБ, обнародованных благодаря сливам от Сноудена, официальное одобрение Dual_EC в качестве стандарта ISO рассматривалось как «большой успех» шпионского Агентства. В этих документах говорится, в частности, что спецслужба настойчиво «направляла дебаты по Dual_EC на протяжении четырех встреч ИСО – до тех пор, пока этот алгоритм не получил статуса глобального стандарта».

Справедливости ради следует подчеркнуть, что компетентные люди из открытого сообщества исследователей и тогда практически сразу выявили в этой операции обман. Свой криптогенератор ключей Dual_EC спецслужба начала продвигать в 2006 году, а уже летом 2007 два аналитика-криптографа из компьютерной индустрии (Dan Shumow и Niels Ferguson) продемонстрировали, что этот алгоритм содержит в себе такую математическую слабость, которую обычно принято именовать backdoor или «черный ход». Благодаря чему АНБ теоретически получает возможность предсказы-

вать генерируемые этим алгоритмом криптоключи, а значит – вскрывать всю зашифрованную с их помощью переписку…

Благодаря настойчивым закулисным манипуляциям АНБ, умело «направлявшим дебаты», мировое сообщество не смогло в тот раз оказать сопротивление нажиму со стороны США. Генератор Dual_EC не только формально одобрили в качестве международного криптостандарта, но и реально стали массово внедрять в криптоприложения. В частности, уже после утечек от Сноудена стало известно, что правительство США тайно заплатило 10 миллионов долларов известнейшей компании RSA Security лишь за то, чтобы она включила алгоритм Dual_EC в свой популярный программный «комплект разработчика» RSA BSAFE. Эту инструментальную библиотеку программисты всего мира используют при создании собственных криптоприложений на основе стандартных модулей индустрии.

Когда в эпоху «после Сноудена» стал общеизвестным целый комплекс свидетельств об умышленной компрометации этого гнилого «стандарта», то и ISO, и другие международные группы стандартизации, и даже NIST, национальный институт стандартов США, – все они были вынуждены «посыпать голову пеплом» и отозвать выданные ранее одобрения для криптогенератора Dual_EC. Что же касается АНБ США, то там просто отказались обсуждать данную проблему. Для шпионских спецслужб это совершенно обычное поведение. Никто даже не удивился.

#

Третий – заключительный и не менее существенный – аспект истории вокруг очередных криптодаров от АНБ сводится к тому, кто именно в недрах этой спецслужбы разработал новые шифры Simon и Speck. Очень важным этот нюанс является по той причине, что для обеспечения государственных и военных систем связи США действительно сильными средствами криптографии в спецслужбе АНБ давным-давно заведено специальное подразделение. Которое так и называется – IAD или Information Assurance Directorate, то есть «Управление защиты информации».

Так вот, совершенно достоверно и документально известно, что к созданию шифров Simon и Speck это управление IAD абсолютно никакого отношения не имело. Реально же разработаны они были совсем в другом подразделении АНБ, носящем название «Управление исследований» (NSA Research Directorate). Ну а практически все научно-технические исследования АНБ, как известно, остро заточены под основную миссию Агентства – электронный шпионаж.

Случайно так оно совпало или нет, точно нам никто не скажет, но события этой истории происходили таким образом, что период острых закулисных дебатов в ISO вокруг криптоподарков от АНБ (2014-2016 годы) хронологически полностью совпал с никак не афишировавшимся, но не менее острым конфликтом сторон и внутри самого Агентства национальной безопасности США. Главными итогами которого стали лик-

видация в составе АНБ Управления защиты информации и сопровождавший эту реформу уход – причем демонстративный и достаточно громкий выход – директора IAD Кертиса Дюкса (Curtis Dukes) вообще из состава сотрудников спецслужбы.

Если же пользоваться более округлыми официальными формулировками, то в 2016 году глава АНБ адмирал Майкл Роджерс объявил, что «IAD как самостоятельное подразделение прекращает своё существование и сливается с направлением электронной разведки». Результатом чего стало появление в составе АНБ нового супер-мощного подразделения под названием Operations Directorate или «Оперативное Управление» в более-менее адекватном переводе на русский.

Поскольку и раньше на обеспечение разведывательно-наступательных операций АНБ приходились и порядка 90% бюджета агентства и подавляющая часть всего кадрового состава, то в новой реорганизации наблюдатели увидели лишь одно. Сигнал о теперь уже полной переориентации всех функций и задач АНБ – даже функций сугубо оборонительных – в направлении активных шпионских операций.

Ни для кого и никогда, в общем-то, не было секретом, что разведывательные усилия АНБ по ослаблению любой криптографии и любых сетей, до которых удается дотянуться, всегда находились в очевидном противоречии с оборонительными усилиями IAD, его же собственного Управления защиты информации. Специалисты которого вполне честно и наилучшим образом пытались защищать не только национальные сети государства, но и помогать делать то же самое национальной индустрии, американскому бизнесу, а также ближайшим военно-политическим союзникам США в других государствах.

Принимая в рассмотрение все эти тонкие нюансы и совсем недавно произошедшую ликвидацию IAD, имеет смысл повнимательнее прислушаться к комментариям Кертиса Дюкса, последнего директора Управления защиты информации, конкретно по поводу криптоалгоритмов АНБ, вызвавших нынешний конфликт в ISO. Отвечая на вопросы Reuters, Дюкс, во-первых, счел необходимым подчеркнуть, что его подразделение НЕ занималось разработкой шифров Simon и Speck. Ну а во-вторых, он в весьма дипломатичных выражениях дал понять, что новый стандарт нужен скорее АНБ, нежели мировому сообществу: «Здесь имеются, видимо, некоторые закономерные вопросы относительно того, а была ли в действительности нужда в этих самых шифрах. Ведь аналогичные по характеристикам алгоритмы шифрования уже существуют»…

#

Весной 2015 года, когда при прошлом президенте Обаме со стороны госадминистрации США пошла очередная волна призывов по ослаблению стойкого крипто в распоряжении широкой публики, главе АНБ адмиралу Роджерсу довелось выступать перед капитанами бизнеса и индустрии. И конечно же, адмиралу на этой встрече пришлось отвечать на очень неудобные вопросы слушателей, занимающих весьма заметные по-

сты в мировой экономике и желающих понять, что именно хочет от них государственное руководство со своими крипто-инициативами. Один из наиболее конкретных вопросов звучал так:

> *«Если мы будем встраивать слабости / бэкдоры или золотые мастер-ключи для правительства США, то считаете ли вы, что мы должны делать то же самое – а мы (компания Yahoo!) имеем около 1,3 миллиардов пользователей по всему миру – делать то же самое для китайского правительства, для российского правительства, для правительства Саудовской Аравии, для Израиля, для французского правительства?»*

На столь прямо поставленный вопрос директор АНБ не смог дать столь же прямого ответа и попытался перевести разговор в другое русло. Когда же его все-таки вынудили ответить на заданный вопрос, то из уст многоопытного шпиона прозвучала дословно такая фраза: «Я думаю, что мы сможем проложить наш курс в такого рода обстоятельствах»…

Сегодня, осмысливая текущие события в области криптографических инициатив США, вполне отчетливо можно видеть, как именно этот курс прокладывается. С одной стороны – заведомая ложь со стороны ФБР и руководства Минюста США про «ответственное шифрование». А со стороны другой – замечательно-хитроумные шифры типа Simon и Speck, разработанные умельцами шпионской спецслужбы АНБ в качестве всеобщего мирового стандарта…

# # #

Дополнительное чтение в тему:

Об одной известной полицейской игре в её приложениях к ослаблению криптографии: «**Плохой носорог, хороший носорог**»

Малоизвестные подробности о громком крипто-конфликте между корпорацией Apple и ФБР США: «**Что это было?**», «**Отрицание и обман**»

Про весьма специфический шизо-крипто-вирус NOBUS или Никто-Кроме-Нас: «**Шизо-криптография**»

Плохой носорог, хороший носорог

(*Август 2015*)

Практически все, наверное, в курсе, что у людей, волею судьбы или случая оказавшихся на высоких государственных постах, очень часто натурально «сносит крышу». То есть в мозгах у таких персонажей что-то там вдруг заклинивает, отчего идеи, которые раньше им просто нравились, теперь обретают статус «абсолютных истин».

Ну а другие идеи – сколь бы сильными и хорошо обоснованными они ни были – могут напрочь и в корне отвергаться уже по той лишь причине, что вождям они просто «не нравятся». Иначе говоря, еще недавно вполне разумные и гибкие люди буквально на глазах превращаются в тупых и агрессивных носорогов…

Но что самое любопытное, как только те же самые госчиновники покидают свои высокие посты во власти – дабы занять какое-нибудь сытное и заранее пригретое место в бизнесе (а это ныне происходит сплошь и рядом) – то к ним тут же возвращаются и здравомыслие вообще, и восприимчивость к рациональным доводам логики в частности.

То есть вчерашние носороги опять становятся похожи на почти нормальных людей. Пусть и не самых приятных из-за их очевидной беспринципности и алчности…

Хотя метаморфозы подобного рода происходят с политиками-бизнесменами повсеместно – в независимости от стран, континентов и политических режимов – особо наглядно это можно видеть на примере США. Где разгоревшиеся ныне дебаты вокруг

сильной криптографии в инфотехнологиях попутно, причем с редкой отчетливостью, проявили также и описанную выше закономерность.

Если кто-то вдруг смутно представляет себе, о чем тут идет речь, то суть происходящего совсем вкратце выглядит так.

Вскоре после прогремевших по миру разоблачений от Эдварда Сноудена, продемонстрировавших реальные масштабы слежки государства за всеми людьми без разбора, гиганты ИТ-индустрии решили по возможности подправить свою сильно подмоченную репутацию.

И теперь вместо безропотного и тайного сотрудничества со спецслужбами США такие влиятельнейшие корпорации, как Google и Apple, широко объявили, что в корне пересматривают принципы защиты информации в своих продуктах. Отчего данные пользователей станут не просто закрыты сильной криптографией, но и сама компания-изготовитель не будет в принципе иметь никакого доступа ни к криптоключам шифрования, ни собственно к данным.

Формулируя чуть иначе, новая защита информации мыслится так, чтобы разработчик программы или устройства не имел никакого доступа к зашифрованным данным клиентов по определению – даже если этого очень хочется компетентным государственным органам, вроде полиции или разведки…

Должно быть понятно, что смелая инициатива ИТ-гигантов, на которых ориентируется и вся остальная индустрия, в высшей степени не понравилась руководству правоохранительных органов и спецслужб США. Сначала от директора ФБР Джеймса Коми, а затем и от директора АНБ Майкла Роджерса последовала целая серия весьма эмоциональных публичных выступлений, в которых были красочно обрисованы масштабы опасностей, грозящих нации от подобных идей.

С точки зрения этих начальников, отсутствие у государства особых криптоключей-дубликатов, позволяющих властям при необходимости получать доступ к любым зашифрованным коммуникациям, – это прямой путь к хаосу и всеобщей погибели. Потому что под прикрытием сильной криптографии от правосудия и наказания смогут дескать ускользать все враги общества – от педофилов, бандитов и наркомафии до иностранных шпионов и террористов.

Позиция властей, столь остро заточенная для полемики, конечно же, вызвала в обществе массу возражений и критики. Наиболее содержательно на доводы силовиков ответили ученые эксперты, профессионально занимающиеся проблемами защиты информации и специально подготовившие развернутое многостраничное опровержение в виде коллективного «Технического отчета МТИ» (Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, MIT-CSAIL-

TR-2015-026, документ подписали полтора десятка наиболее авторитетных ученых страны).

Однако куда более любопытным опровержением представляется коллективная статья, написанная группой совершенно других известных людей и опубликованная одной из главных американских газет, столичной «Вашингтон Пост» (Why the fear over ubiquitous data encryption is overblown, Washington Post, July 28, 2015)

Авторами данного послания являются три бывших коллеги Коми и Роджерса, занимавшие столь же высокие госпосты в силовых структурах совсем еще недавно. Майк Макконнелл был директором АНБ в 1990-е и директором национальной разведки в 2000-е, в администрации Джорджа Буша. Майкл Чертофф при том же президенте возглавлял спецслужбу DHS или Департамент госбезопасности. Ну а третий автор, Уильям Линн III, был заместителем министра обороны уже при Обаме, только в первый срок его президентства.

Единственное отличие этих людей от нынешних директоров ФБР и АНБ заключается в том, что сейчас они занимают адекватно высокие посты в бизнес-корпорациях, плотно встроенных в военно-промышленный комплекс США и ежегодно оперирующих миллиардными суммами правительственных госзаказов.

Этого небольшого, на первый взгляд, отличия оказывается вполне достаточно, чтобы авторы имели в корне иную точку зрения на проблему. Оттого коллективная их статья носит выразительное название «Почему страхи перед повсеместным шифрованием данных сильно преувеличены», а все содержимое этого текста предоставляет куда более взвешенную и адекватную картину происходящего.

Суть базовых аргументов – в их самом кратком переложении – сводится в статье к следующему.

Во-первых, требования о наличии ключей-дубликатов (или технологий, их заменяющих), неизбежно вносят в любое шифрование такие уязвимости, которые увеличивают риски компрометации системы и хищения ключей злоумышленниками. Как показывают многочисленные примеры из жизни, ни одна сторона не может обеспечить идеальную безопасность хранения информации. А значит, хранилища ключей-дубликатов порождают особо опасный узел компрометации.

Во-вторых, требование о том, чтобы американские провайдеры инфотехнологий создавали ключи-дубликаты, никак не помешает злоумышленникам отыскать других провайдеров – предлагающих клиентам полное шифрование. В итоге же это приведет к обратному эффекту. Как результат, законопослушные организации и граждане утратят защищенные коммуникации, а вот у злоумышленников, напротив, этого хозяйства будет в достатке.

В-третьих, и это особо существенно, если США смогут настоять, чтобы компании делали доступными для властей ключи-дубликаты, то и другие государства, вроде Китая или России, будут настаивать на том же самом. И у бизнеса уже не будет принципиального базиса для того, чтобы сопротивляться подобным законным требования. Как результат, коммуникации буквально всех – бизнес-структур, политиков и просто частных лиц – станут легко доступны для великого множества правительств в самом широком спектре политических режимов.

И наконец, в-четвертых, уроки истории показали, что страхи перед повсеместным шифрованием, которое будто бы отбросит нашу безопасность во тьму неведения, оказываются сильно преувеличенными. В начале 1990-х годов, когда интернет, персональные компьютеры и криптография с открытым ключом предоставили для всех возможности дешевого и сильного шифрования, в руководстве нацбезопасности тоже были убеждены, что это катастрофа…

Однако небеса при этом не рухнули, а компетентные органы вовсе не ослепли и не оглохли. Скорее даже наоборот, в условиях цифровых технологий работа спецслужб во-многом стала даже более эффективной. Просто им пришлось научиться работать по-новому.

Подводя же итог своим аргументам, авторы заключают, что в конечном счете политическая и военная мощь государства всегда базируются на его экономической силе. То есть интересы бизнес-структур страны – это стратегически важная область при защите интересов национальной безопасности США. А для защиты бизнес-интересов едва ли не самое главное – успешно противостоять массированным атакам экономического шпионажа. Или формулируя чуть иначе, выходит, что безопасная инфраструктура коммуникаций на основе надежного и повсеместного шифрования – это великое общественное благо…

Все приведенные авторами аргументы, тут и спору нет, звучат разумно, логично и убедительно. Сильно настораживает лишь одно. Исходят эти доводы от тех же самых людей, которые совсем недавно – когда занимали высокие посты в госадминистрации США – оперировали в корне иной логикой «тупых носорогов». Все они лично и активно участвовали в самых жестких инициативах государства по усилению национальной безопасности, и при этом фактически никак не реагировали на призывы общественности к сбалансированным подходам…

Ну а самое, пожалуй, интересное, что происходят подобные метаморфозы с этими деятелями уже не первый раз. Если чуть поглубже поинтересоваться биографиями авторов, то несложно увидеть там вот что.

В 1990-е Майк Макконнелл был директором АНБ, затем с государственной службы перешел в руководство мощной корпорации Booz Allen Hamilton (BAH), затем в 2000-

е рулил уже всеми разведками США в совокупности, после чего опять вернулся в кресло одного из боссов ВАН.

Совершенно по аналогичной траектории Билл Линн III в 1990-е занимал руководящий пост в министерстве обороны, затем стал высокопоставленным лоббистом оборонной корпорации-гиганта Raytheon, затем он вновь большой чиновник, заместитель министра обороны, ну а теперь – глава крупной военно-промышленной фирмы DRS Technology.

Короче говоря, если завтра вдруг случится так, что кто-то из упомянутых (а также и не упомянутых) здесь высокопоставленных персонажей в очередной раз диаметрально изменит свою «жизненную позицию» и взгляд на важные государственные проблемы, то воспринимать это лучше всего как абсолютно естественную вещь.

Просто правила игры у них там такие…

# # #

Сигнал без шума, или Криптография как метафора

(*Впервые опубликовано – июль 2012*)

Новоиспеченный российский закон, вводящий для интернета черные списки (или реестр сайтов с запрещенным контентом), вызывает естественные вопросы. Слишком уж много признаков, что декларируется тут одно, а подразумевается нечто существенно иное.

О чем шумим?

Перед уходом на летние каникулы слуги народа в парламенте решили вдруг озаботиться защитой молодежи от тлетворного влияния интернета. И стахановскими темпами придумали-приняли новый закон – о внесении изменений в (другой, еще даже не начавший действовать) федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию».

Суть внесенных поправок, как все уже знают, сводится к созданию так называемых черных списков, на основании которых по всему государству будет блокироваться интернет-доступ к сайтам с противоправным и вредным контентом. К таковому отнесены детская порнография, пропаганда наркотиков и суицида.

Рассуждая абстрактно, ну что, казалось бы, в этом плохого? Кто, находясь в здравом уме, будет выступать против борьбы с такой мерзостью, как растление малолетних? Да и по прочим пунктам, всякие нормальные родители, наверное, будут только рады, если государство поможет им оградить своих чад от таких жутких напастей, как наркомания и самоубийство…

Проблема в том, что абстрактные рассуждения не годятся для анализа текущей жизни в конкретном государстве. И если в этой стране значительная часть интернет-сообщества, способная внятно и без мата формулировать свою позицию, совершенно определенно выступает против нового закона, то тому должны быть действительно серьезные причины.

Все, кто интересуется данной историей, наверняка уже не раз читали и слышали многочисленные доводы противников «черных списков». Доводы о том, в частности, что российское законодательство и так имеет вполне достаточно статей, позволяющих строго наказывать за преступления, связанные с растлением малолетних или наркобизнесом. Что введение цензуры нигде и никогда не делало общество лучше. Что в технических аспектах предлагаемые законом меры по блокированию запрещенных сайтов на деле эффективно не реализуются, а значит и закон работать не будет…

Примечательно, что одним из самых сильных контр-доводов, привлекаемых сторонниками нового закона в его защиту, стала формула «все так делают». Иначе говоря, к чему все эти бесплодные споры, если систематической фильтрацией интернет-контента ныне занимаются уже чуть ли не все государства. Не только авторитарные режимы в регионах Азии и Персидского залива, но также вполне демократические власти и в Европе (вроде Британии, Германии, Италии, Франции, стран Скандинавии), и в Австралии, и в Канаде, и в Южной Америке. То есть, можно сказать, Россия тут просто подтягивается к всеобщей мировой тенденции.

В общем, ясно, наверное, что проблема здесь обозначилась непростая. И для лучшего ее понимания хотелось бы иметь какой-нибудь еще аналитический инструмент, позволяющий выявлять дополнительные и/или скрытые аспекты происходящего.

Среди нестандартных подходов к анализу можно выбрать, к примеру, вот такой.

Теория информации и криптография

Одной из любопытных особенностей в истории развития прикладной математики XX века стало то, что теория информации и теория криптографии родились практически одновременно. Более того, родителем обеих наук является один и тот же человек – Клод Элвуд Шеннон.

Иначе говоря, имеются все – даже чисто медицинские – основания называть эту пару науками-близнецами, описывающими в общем-то одно и то же, но только с несколько разных сторон. Если теория информации занимается тем, каким образом в целостности и без искажений передавать сообщение по каналу, сильно зашумленному помехами, то криптография решает задачу, формулируемую с точностью до наоборот.

А именно, каким образом следует искажать сигнал искусственным шумом до такой степени, чтобы противник, подключившийся к каналу передачи, не смог бы понять содержание сообщения.

Особенно интересным разделом криптографии является криптоанализ – то есть специальный набор математических процедур и приемов для вскрытия шифров (ибо нельзя сконструировать сильный криптоалгоритм, не научившись прежде вскрывать шифры слабые). Понятно, что суть работы криптоаналитика – это получение доступа к сигналу, несмотря на все усилия тех, кто его «зашумлял». То есть можно говорить, что криптоанализ решает ту же самую задачу, что и теория информации, но только в условиях более специфического «шума в канале».

Но какое отношение (пора спросить) вся эта история имеет к принятому ныне в России закону о черных списках для интернета?

Связь тут следующая. Стандартный набор процедур, применяемых криптоаналитиками при вскрытии шифров, и в этом случае позволяет «отделить сигнал от шума», обеспечивая таким образом доступ к содержанию данного послания в его исходном, очищенном от помех виде. В криптографии такой сигнал называют «открытым текстом».

Конечно же, здесь это «дешифрование» будет проделано без той математической строгости, что присуща современной криптоаналитической науке. Криптография, можно сказать, в данном случае привлекается скорее в качестве наглядной метафоры.

Статистические аномалии

Одним из главных внешних признаков качественного криптоалгоритма обычно является статистически ровный шифртекст, похожий на случайную равновероятную последовательность. Всякая же статистическая аномалия в появлении символов и их комбинаций, как правило, указывает на имеющуюся в шифре слабость. Такого рода слабости, ведущие к легкому вскрытию защиты, были характерны, например, для криптографии в первых версиях ОС Windows.

Применительно к потоку законотворчества нашей Госдумы статистическая аномалия резко обозначилась в июле, когда в течение всего одной недели без каких-либо предварительных обсуждений были внесены, заслушаны и приняты сразу три закона. Причем все три – о клевете, об общественных организациях как «иностранных агентах», о черных списках для вредных интернет-сайтов – характеризуются одной и той же, собственно, особенностью.

Все эти инициативы направлены на ограничение имевшихся прежде прав, вводя дополнительную ответственность для всех, кто так или иначе зависит от власти. Говоря

подоходчивее, никаких дополнительных свобод эти законы не подразумевают. Речь там идет лишь о новых запретах и о наказаниях за «непослушание».

Если же вспомнить, что чуть ранее, в июне был принят и весьма созвучный этим трем новый закон об ограничении свободы собраний, то без всяких статистических расчетов становится вполне очевидно следующее. Власти в России заметно напуганы процессами, идущими в обществе, а потому начали поспешно закручивать гайки.

Частые повторения

Переходя к более конкретному рассмотрению нового закона о черных списках для блокирования запрещенных интернет-сайтов, полезно обратиться к специфическому криптоаналитическому приему под названием «выявление повторений».

Статистически неслучайные повторения в тексте послания нередко дают весьма мощный рычаг для взлома криптосистемы. Особенно в тех случаях, когда повторения одного и того же вида встречаются часто и именуются техническим термином «стандарты переписки» (любителям историй про Шерлока Холмса для иллюстрации метода можно напомнить сюжет о взломе им шифра пляшущих человечков). В анализируемом нами случае один из стандартов подобного рода очень хорошо известен заранее и выглядит как «детская порнография».

Законодатели практически всех стран мира каждый раз, когда надо протащить какой-нибудь очередной заведомо непопопулярный в обществе закон, снова урезающий гражданские права и свободы, первым делом норовят привлечь в качестве неотразимого аргумента борьбу с детской порнографией и чертовыми педофилами. До недавнего времени столь же безотказно работала нескончаемая война с угрозами терроризма, однако благодаря чрезмерной активности США на данном поприще и абсолютно невыразительным итогам этой борьбы на фоне общей усталости масс, террористическую угрозу ныне перевели в разряд горячего резерва.

Короче говоря, аргумент борьбы с «детской порнографией» пока что работает действительно безотказно, а потому привлекается вновь и вновь. Включая и беспощадную войну с плохими веб-сайтами. Длится вся эта борьба уже многие годы, но при этом, что характерно, количество историй о растлении малолетних ничуть не уменьшается.

На очень выразительных примерах из истории секс-скандалов в католической церкви и в высшем политическом руководстве целого ряда стран хорошо известно, что преступления в связи с растлением малолетних регулярно и в массовых масштабах замалчиваются. Дабы не порочить, типа, авторитет власти и духовенства. Как следствие, идеи борьбы с педофилами и собствено педофилы существуют раздельно и как бы сами по себе, пересекаясь лишь в отдельных эпизодических случаях. Когда заметают лишь каких-нибудь совсем уж незначительных извращенцев.

(Конкретно о российских реалиях НЕ-борьбы с этой напастью во власти можно почитать вот тут: «Непримиримые антипедофилы».)

Многократное использование одного ключа

Криптографической теорией и практикой установлено, что даже в тех случаях, когда для засекречивания сообщений используются весьма сильные шифры, обеспечивающие в канале сигнал, статистически никак не отличимый от случайной равновероятной последовательности, все равно имеется реальная возможность вскрытия защиты – если по какой-то причине отправитель для разных посланий использовал один и тот же секретный ключ.

Обращаясь к историческим примерам, наглядно иллюстрирующим данную слабость, можно вспомнить знаменитую историю взлома англичанами германского шифратора «Лоренц Шлюссельцузатц», закрывавшего особо секретную переписку высшего руководства Третьего рейха. Всего из-за одной, но очень серьезной ошибки немецкого шифровальщика, повторно применившего тот же самый ключ, британские криптоаналитики сумели восстановить по шифртекстам всю схему работы шифратора. После чего построили сначала один, а затем и десять «суперкомпьютеров» Colossus, несколько лет обеспечивавших постоянное чтение немецких секретов вплоть до победы над нацизмом (подробности см. тут: «Колосс британский»).

Применительно к той борьбе, которую нынешние власти демократических и не очень стран ведут в интернете с собственными гражданами, пытаясь перекрыть им доступ к сайтам с запрещенным контентом, роль важнейшего элемента системы – или «ключа» – играют так называемые черные списки, содержащие конкретные адреса подлежащих блокированию сайтов.

Понятно, что вся эта система хоть как-то способна обозначать свою работоспособность исключительно в условиях сохранения подобных черных списков в строжайшем секрете (поэтому, собственно, такие реестры и называют «черными»). Но понятно и то, что подобные списки невозможно применять однократно – напротив, они действуют постоянно, время от времени лишь пополняясь новыми строчками запретов. Отсюда-то проистекает и их ключевая слабость.

Как показывает опыт, рано или поздно непременно происходит утечка «черного списка» в интернет, обычно через сайты компромата типа WikiLeaks. И тут же любому становится видно, что все эти разговоры про борьбу с детской порнографией и педофилами – просто только повод для установления негласного и внесудебного контроля за доступом к информационным интернет-ресурсам.

Так было практически всюду, где «черные списки» сливались в сеть противниками цензуры. В Таиланде, скажем, где как и всюду обосновали сетевую цензуру необходимостью борьбы с детской порнографией, на самом деле свыше 1000 запрещенных

сайтов были связаны с критикой правящей королевской семьи. В Австралии лишь треть позиций секретного реестра относилась к запрещенным порносайтам. В Финляндии среди очень далеких от детской порнографии, но все равно запрещенных ресурсов, обнаружились сайты, критикующие антидемократическую практику цензуры. Ну и так далее в том же духе.

Короче говоря, каждая очередная публикация секретных черных списков стабильно подтверждает давно известную истину. Как только у людей, наделенных властью, появляется возможность своими властными полномочиями бесконтрольно злоупотребить, такого рода злоупотребления непременно происходят.

Открытый текст

Завершая данные упражнения в криптоанализе законотворческих посланий и отделив маскирующий шум от действительно содержательной информации, можно сделать следующий вывод.

И в российском, и в международном законодательстве без всяких черных списков давно существует вполне достаточный набор правовых инструментов, позволяющих пресекать и строго наказывать преступления, связанные с растлением малолетних и детской порнографией.

Конкретно в условиях физического расположения сайтов на территории России, в частности, госвласти имеют и вполне успешно применяют широчайший набор различных методов для блокирования любых интернет-ресурсов, расцениваемых ими как вредные. Закрытие сайтов может происходить как по решению судов, так и во внесудебном порядке: по представлениям прокуратуры, МВД или Минсвязи, через лишение доменного имени в зоне .RU и/или через физическую конфискацию серверов.

То есть, фактически, вся эта созданная новым законом система – с блокированием адресов через механизмы черных списков – для сайтов на российской территории и не требуется вовсе. Для чего же она может реально пригодиться, так это для быстрого и беспроблемного блокирования любого неугодного властям инфоресурса, находящегося за рубежом. Будь это хоть «Живой журнал», хоть YouTube, хоть сам Google.

Не факт, конечно, что такая потенциальная возможность будет часто применяться, однако собственно механизм цензуры для этого создан.

Причем создано все это в очевидном противоречии с Российской Конституцией, где в статье 29, пункт 5, в дословном виде прописана следующая строка: «Гарантируется свобода массовой информации. Цензура запрещается»…

Информация без смысла

Одна из важнейших особенностей теории информации (также как и криптографии) заключается в том, что наука оперирует исключительно информационными битами, никак не интересуясь смысловым содержанием этих битов. Все, что касается смысла информации, относится уже не к математическо-аналитической части, а к тому, кто именно этой информацией пользуется и ее интерпретирует.

Наглядной иллюстрацией этой особенности может служить информация о результатах скачек на ипподроме. Для кого-то набор символов с именем победителя может стать новостью о неожиданном получении целого состояния. Для кого-то еще – трагическим известием о крушении последних надежд. Ну а для подавляющей массы населения тот же самый фрагмент информации пройдет, скорее всего, абсолютно незамеченным – как будто его и не было вовсе.

Информация о повсеместных попытках насаждения внесудебного блокирования контента в интернете, что осуществляется вопреки духу и букве всех конституций свободного мира, запрещающих цензуру, относится к той же самой категории.

Для кого-то это явный сигнал тревоги, требующий немедленного вмешательства для восстановления утрачиваемых народом гражданских прав и свобод.

Для других – это благая весть. Означающая, что власти всех стран – в независимости от идеологии и религии – наконец-то вполне единодушны в своем желании иметь инструменты для эффективного контроля за информацией, доступной их гражданам.

Ну а для очень значительной массы населения эта новость вообще не означает практически ничего. Им, так сказать, все эти цензуры-несвободы в общем-то до лампады.

Если бы в России, в частности, дела обстояли иначе, то жили бы мы совсем в другой стране. И власть бы имели существенно иную. Ну а пока что мы имеем то, что имеем.

И ни теория информации, ни криптография тут совершенно ни при чем.

# # #

Темная сторона Силы

Серийные самоубийцы

(*Декабрь 2006*)

В течение последнего года целый ряд государств сотрясают весьма похожие по своей сути скандалы, связанные с широкомасштабным нелегальным прослушиванием сотовой связи.

О перехвате «неизвестно кем» мобильных телефонов высшего руководства Греции в писалось достаточно подробно (см. тут), за летние же месяцы добавилось еще несколько похожих историй из Италии и Южной Кореи.

Причем в этих странах картина с виновными в организации нелегальных прослушиваний далеко не столь туманна, как в Греции.

В частности, корейский суд разобрался и дал по три года тюрьмы начальникам национальной разведки NIS, возглавлявшим спецслужбу Южной Кореи в период с 1999 по 2003 год и руководившим незаконным перехватом разговоров политиков, видных бизнесменов и прочих граждан своей страны.

В Италии же следствие еще не закончилось, но и здесь арестованы замдиректора военной разведки SISMI, шеф безопасности крупнейшей компании связи Italia Telecom и владелец сети частных сыскных агентств, устроившие весьма прибыльный «кооператив» по массовому сбору компромата на сограждан от сетей мобильной связи.

С одной стороны, в этих скандалах нет, казалось бы, абсолютно ничего неординарного. В органах власти любого уровня работают вполне обычные люди со всеми их человеческими слабостями. И если современная техника в принципе позволяет спецслужбам организовать прослушивание интересующих их людей тайно, без волокиты с обоснованиями и получением санкций судебных органов, то наивно предполагать, что такими возможностями не будут пользоваться по причине «уважения законов».

Но вот с другой стороны, однако, за каждой из этих историй стоят не только элементарные нечестность и корыстолюбие, но также загадочные смерти людей и куда более глубокие тайны. А это делает ситуацию значительно серьезней.

Последняя из этих смертей случилась в июле в Италии.

Пост главного менеджера по безопасности в фирме Italia Telecom, освободившийся после ареста предыдущего шефа за преступные связи с руководством SISMI, занял некто Адамо Бове. В прежние годы Бове работал в полиции, слыл ведущим специалистом по спецвозможностям сотовой связи и в середине 1990-х прославился поимкой двух видных главарей итальянской мафии, отследив их перемещения по мобильным телефонам.

В совсем недавней шумной истории с расследованием прокуратурой дела о нелегальном похищении и вывозе из Италии человека сотрудниками американского ЦРУ, Адамо Бове был главным экспертом, восстановившим по лог-файлам сотовых операторов карту всех перемещений цэрэушников в процессе подготовки и проведения похищения.

Распутывание именно этой истории вывело затем прокуратуру на нелегальное сотрудничество американских спецслужб с итальянской разведкой SISMI, а далее – и на операции шпионов по сбору компромата в коммерческих целях.

На своем новом посту Адамо Бове стал для прокуратуры главным источником информации об устройстве системы нелегального прослушивания телефонов в сетях Italia Telecom. Но длилось это недолго, так как вскоре при весьма туманных обстоятельствах Бове «покончил жизнь самоубийством». Во всяком случае, так расценила произошедшее полиция.

Годом раньше в соседней Греции столь же загадочно оборвалась жизнь Костаса Цаликидиса, топ-менеджера компании мобильной телефонии Vodafone Greece. Лишь совсем недавно, в июне 2006, прокуратура Греции наконец признала очевидное – что эта смерть напрямую связана со скандалом вокруг нелегального прослушивания сотовых телефонов примерно сотни ведущих политических фигур страны.

Однако в выводах прокуратуры по-прежнему сохранена исходная версия полиции о «самоубийстве», несмотря на все доводы и доказательства адвоката семьи погибшего, убедительно опровергающие эту версию.

Организатор нелегальных прослушиваний до сих пор считается «неустановленным», поскольку все собранные улики указывают на разведку США, с которой тесно сотрудничают греческие спецслужбы, а среди ведущих политических сил Греции нет такой, которая была бы заинтересована в обострении отношений с Америкой.

Обо всех этих вещах чрезвычайно скупо упоминают ведущие мировые СМИ, а сколь-нибудь существенные подробности можно найти лишь в местной прессе Италии и Греции. Но и там по пальцам можно перечислить печатные издания, проводящие выразительные параллели между двумя загадочными и в некоторых существенных деталях очень похожими смертями топ-менеджеров.

Однако в действительности все обстоит куда более круто – и об этом не пишет вообще никто, даже в интернете.

Первое подробно документированное «самоубийство» из этой череды произошло в 1999 году в Швейцарии. Там в ту пору был в разгаре свой большой общенациональный скандал в связи со вскрытыми прессой фактами широкомасштабных прослушиваний мобильных телефонов, нелегально ведущихся «органами» без санкции суда.

Главным источником фактов для журналистов и парламента был некто Кристиан Массон, бывший информатор полиции, однажды узнавший реальную ситуацию с контролем сотовой связи и при помощи весьма содержательного веб-сайта начавший «личную войну» с противозаконной прослушкой.

Весной 1999 Массон сообщил друзьям, что постоянно получает угрозы, а вскоре «совершил самоубийство», бросившись с высокого пешеходного моста в Лозанне. Точно так же, падением с высокой эстакады на автостраду, недавно закончилась в Италии жизнь Адамо Бове.

Осуждение главных южнокорейских шпионов, о котором упоминалось в самом начале, – это, собственно, финал более ранней истории, главной фигурой в которой был совсем другой, ныне уже мертвый человек.

Похожий на все остальные, шпионско-политический скандал в Южной Корее разразился осенью 2005 года. Тогда журналисты добыли и опубликовали записи перехвата, который вела в сотовых сетях корейская национальная разведслужба NIS, нелегально следившая за ведущими гражданскими политиками страны и деятелями бизнеса.

Началось следствие, главным источником информации в котором стал бывший замдиректора разведки Ли Су Ир, непосредственно отвечавший за перехват. Но как только

он начал давать показания о приказах своего начальства и подробностях операции, его тут же нашли повесившимся в собственной квартире.

Точно в таких же обстоятельствах, повесившимся дома, был обнаружен в Греции Костас Цаликидис – за день до того, как директор Vodafone Greece известил власти об обнаруженной в их сети подсистеме для нелегального прослушивания.

Ни один из всех этих «самоубийц» не оставил записки, объясняющей причины содеянного, а по свидетельствам друзей и близких, никто из них не проявлял никакой склонности к суициду.

Но во всех четырех странах национальные спецслужбы очень тесно сотрудничают с США в противодействии «терроризму и организованной преступности», а каждый из погибших имел обширные сведения о специфике применяемых для этого технологий нелегального перехвата.

Понятно, какой из этого напрашивается вывод. Но именно поэтому никто не решается его сделать.

# # #

Вопросы на греческом

(Июнь 2006)

Утром 2 февраля 2006 года популярная в Греции оппозиционная газета Ta Nea опубликовала «темой номера» совершенно фантастическую, на первый взгляд, шпионскую историю.

История была о том, что сотовые телефоны кучи людей из высшего государственного руководства многие месяцы кем-то прослушивались с помощью шпионской программы-закладки в аппаратуре Vodafone Greece, одного из главных в стране операторов мобильной связи.

Буквально через несколько дней после обнаружения закладки в марте 2005 произошло загадочное самоубийство одного из топ-менеджеров Vodafone Костаса Цаликидиса.

Что случилось?

На официальной пресс-конференции, посвященной этим событиям, министр общественного порядка, министр юстиции и пресс-секретарь кабинета министров поведали (не ссылаясь на газету Ta Nea), что действительно, установлен факт нелегального прослушивания в сети Vodafone ста мобильных телефонов, многие из которых принадлежали ключевым фигурам правительства. Помимо премьер-министра и его жены, министров обороны, госбезопасности и других важных членов кабинета, в списке прослушиваемых лиц было и множество других крупных фигур.

В частности, представитель Греции в Евросоюзе, мэр Афин, министр обороны предыдущего правительства социалистов, высокопоставленные греческие военные, ведающие закупками вооружений, активисты и адвокаты правозащитного движения, известные журналисты (в том числе афинский корреспондент агентства новостей Аль-Джа-

зира), несколько анархистов, а также ряд бизнесменов с арабскими и пакистанскими именами. Список, что и говорить, выразительный.

Применявшаяся для прослушивания телефонов технология охарактеризована как «чрезвычайно изощренная». Самые же интересные вопросы – кто и зачем это делал – остались без ответа. Компания Vodafone, обнаружившая в своей аппаратуре шпионскую программу, сначала ее отключила (сделав невозможными быстрый поиск и арест владельцев четырнадцати телефонных номеров, получавших данные перехвата) и лишь потом доложила о находке. Причем в правительстве из этого сразу же сделали «военную тайну».

Подводя итоги этой истории на пресс-конференции, министр юстиции признал, что имеющейся информации пока не достаточно, чтобы решить, трактовать ли это преступление как покушение на тайну личной жизни или же как иностранный шпионаж.

Из крайне скудных сведений, найденных следствием, получалось, что подслушивающая техника, судя по всему, начала работать накануне летней Олимпиады 2004 года в Афинах. Весной следующего года закладку при плановом осмотре обнаружил техник фирмы Ericsson, чья аппаратура обеспечивает работу телефонной сети. 5 марта Ericsson сообщила о находке директору Vodafone Greece, а тот, ознакомившись со списком прослушиваемых номеров, 10 марта уведомил о происшествии аппарат греческого премьер-министра.

Кому это выгодно?

Длившееся около года «секретное расследование» не дало результатов лишь потому, что огромное количество косвенных улик сразу и недвусмысленно указывало на организатора столь широкомасштабного шпионского проекта.

Три антенны сотовой связи, обслуживавшие, как их назвали, «теневые телефоны» перехвата, находятся в центре Афин, и если соединить их на карте прямыми линиями, то внутри сравнительно небольшого треугольника оказывается здание посольства США.

Когда это стало известно, местные военные, ведающие закупкой оружия и техники, сразу же поняли источник поразительной, порой сверхъестественной осведомленности фирм американского военно-промышленного комплекса, продающих Греции вооружение на чрезвычайно выгодных для себя условиях. Греция является одним из самых заманчивых в Европе рынков для торговцев оружием, ежегодно расходуя на оборону не менее 3,5 млрд. долларов из бюджета.

Здесь же уместно напомнить, что лишь для обеспечения безопасности Олимпиады-2004 Греция затратила беспрецедентную сумму в 1,5 млрд. долларов на контракты, обеспеченные опять-таки фирмами США.

Как это было?

Еще одним пикантным нюансом в скандале оказалось то, что откровенно криминальный шпионаж осуществлялся с помощью «системы легального перехвата», разработанной самой компанией Ericsson и включаемой ею в состав программного пакета R9.1. Этот пакет был инсталлирован при модернизации оборудования греческой сети Vodafone осенью 2003 года.

Правда, принято считать, что официальный запуск системы перехвата сопряжен с очень сложным тестированием и перерывами в обслуживании клиентов, что в общей сложности стоит миллионы долларов. Однако в греческом варианте, как выяснилось впоследствии, поверх системы работала еще одна, тайная закладка, без проблем включавшая перехват лишь в те моменты, когда шли звонки по номерам из списка прослушки, а все остальное время остававшаяся «невидимой».

Для «массового обслуживания» сотни прослушиваемых номеров были задействованы всего полтора десятка мобильных телефонов, зарегистрированных в сети по анонимным контрактам. Когда шел вызов для номера «на контроле», одновременно проходил вызов конференц-связи для первого из незанятых номеров среди «теневых телефонов». Каждый из них, судя по всему, был снабжен магнитофоном, так что четырнадцати (иногда шестнадцати) номеров вполне хватало для постоянного присмотра за всем списком.

Георги Кориниас, директор Vodafone Greece, при разбирательстве в парламенте подчеркнул, что до марта 2005 он вообще ничего не знал о существовании подсистемы перехвата в составе R9.1. Лишь компания Ericsson владеет секретными кодами и параметрами, необходимыми для активации «легального перехвата».

Тайное же включение этой системы, по мнению Кориниаса, могла осуществить лишь «организация» с глубоким знанием специализированного ПО Ericsson, включающего 25 миллионов строк кода, 64 подсистемы и 1760 функциональных блоков.

Отметив, что программа перехвата может быть активизирована как непосредственно на месте, так и дистанционно, Кориниас сообщил, что Ericsson подсоединена к телефонным центрам Vodafone Greece через специальную систему безопасности, причем сама Vodafone не имеет доступа к этой системе.

После того, как всплыл скандал с прослушкой, компании Vodafone Greece тоже захотелось узнать, что же за программы работают в ее аппаратуре. Для этого 13 февраля 2006 года Кориниас написал в Ericsson письмо с просьбой предоставить код программы легального перехвата, на что штаб-квартира шведской компании ответила категорическим отказом, объяснив, что эти коды являются «стратегической ценностью», которой они не делятся ни с кем.

В ходе пятичасовой дачи показаний в греческом парламенте Кориниасу явно хотелось выглядеть белым и пушистым, однако впечатление портила явная неискренность директора Vodafone в его комментариях относительно смерти Костаса Цаликидиса.

Невзирая на известные факты и многозначительные совпадения, компания и ее директор упорно отрицают какую-либо связь между шпионским скандалом и гибелью своего сотрудника, по должности ближе всего находившегося к тайнам скрытной прослушки.

Среди сотни стоявших на прослушивании телефонов лишь один принадлежал представительству зарубежной державы – посольству США. Как выяснилось после небольшого журналистского расследования, на самом деле этим номером пользовались не американцы, а греки из службы внешней охраны посольства.

Другим выразительным примером оказался стоявший на прослушке телефон абсолютно ничем не выдающегося греческого электрика, единственная «слава» которого была связана с родственником по линии жены. Находящийся в бегах свояк электрика каким-то боком участвовал в делах террористической организации «17 ноября», среди кровавых дел которой значится убийство шефа афинской резидентуры ЦРУ Ричарда Уэлча.

Почему Костас?

Костас Цаликидис был техническим директором Vodafone-Greece, отвечавшим за развитие сети. Утром 9 марта 2005 года (за день до того, как Г. Кориниас отправился в аппарат премьера рассказывать об обнаруженной закладке) топ-менеджера нашли повесившимся в собственной квартире.

По заключению врачей смерть наступила примерно в семь утра, и, поскольку на дверях квартиры не было следов взлома, полиция классифицировала инцидент как самоубийство, не сделав ни вскрытия тела, ни даже криминалистической экспертизы места происшествия.

Никаких признаков суицида у человека, готовившегося к собственной свадьбе, близкие не замечали. Кроме того, семья обнаружила в домашнем ноутбуке Цаликидиса большое электронное письмо, которое он написал и разослал коллегам в 4:20 утра (то есть меньше чем за три часа до смерти), где составил перечень работ, которые он планирует выполнить с июля по сентябрь текущего года.

По свидетельству брата, Панайотиса Цаликидиса, за двадцать дней до смерти Костас подал заявление об уходе, которое руководство Vodafone подписывать отказалось. Поэтому инженер продолжал работать вплоть до последнего дня.

Кроме того, по признанию коллег, за день до смерти Цаликидис имел бурную разборку в дирекции компании. Своей невесте в самых обтекаемых выражениях он рассказывал, что на работе происходит нечто «очень неправильное» и если это раскроется, будет грандиозный скандал.

Понятно, что в подобных обстоятельствах семья Цаликидиса не поверила в версию полиции о самоубийстве и наняла адвоката для поиска правды и наказания виновных. Адвокат нашел множество дополнительных свидетельств, указывающих на преступление.

В частности, по журналу звонков в сотовом телефоне Цаликидиса было установлено, что его невеста, ушедшая из квартиры примерно в 23:00, была вовсе не последним человеком, с кем Цаликидис разговаривал перед смертью. В течение ночи Костасу несколько раз звонили, причем в первый раз он ответил, а два других вызова оставил без внимания.

Но самые важные данные появились после того, как загадочной смертью все же занялась – год спустя – прокуратура, и выяснилось, что накануне смерти Цаликидиса его домашний телефон по неясным причинам был поставлен на прослушивание компетентными органами.

Из записей лог-журнала прослушки видно, что с этого телефона 9 марта 2005 года был сделан звонок в 8 часов утра, то есть через час после смерти «самоубийцы», но до того, как тело обнаружили родственники.

Кто виноват?

Начиная с февраля этого года за собственное расследование истории энергично взялось недавно созданное независимое Управление по защите конфиденциальности телекоммуникаций (ADAE). За три месяца, невзирая на скрытое и явное сопротивление Vodafone, сотрудники ADAE нашли все то, что должны были, но «не смогли» раскопать греческие спецслужбы за предыдущий год.

Поскольку по жалобам абонентов была хорошо известна дата последней модификации прослушки (вызвавшая многочисленные глюки в сети и прибытие для ремонта техника из Ericsson), то по лог-журналу посещений в строго охраняемых телефонных центрах компании было установлено, что из пяти посетителей центра в интересующий день сотрудником компании был всего лишь один, а остальные – сопровождавшими его «гостями». Установить личности всех этих людей, правда, не удалось, поскольку «по недосмотру» данные записи журнала оказались случайно стерты.

Газета Ta Nea, имеющая сведущих информаторов в среде спецслужб (где явно не всем нравится происходящее), опубликовала имена шести сотрудников греческой разведки EYP, помогавших устанавливать и настраивать оборудование нелегальной прослушки.

Директор EYP категорически отверг обвинение, пообещав подать на газету в суд, однако был вынужден признать, что были названы реальные имена его сотрудников.

Управление ADAE тем временем проштудировало все записи о звонках, исходивших от «теневых телефонов» перехвата, и установило факты соединений с США, Англией, Австралией и Швецией. Первые три страны являются членами глобальной автоматизированной системы электронной разведки «Эшелон», участие же шведских спецслужб в этом предприятии тоже вполне объяснимо.

Особо примечательно, что один из американских номеров, на которые совершались эти звонки, зарегистрирован в городе Лорел, штат Мэриленд. Дабы стало понятно, что сие означает, достаточно привести официальный почтовый адрес штаб-квартиры Агентства национальной безопасности США: «Форт-Мид, Лорел, Мэриленд»…

Что будет?

Все вышеперечисленные факты, включая номера телефонов за рубежом и имена людей, предположительно замешанных в устранении Цаликидиса, стали известны прокуратуре к началу мая 2006, после чего наступили «жуть и тишина».

Хладнокровное убийство невинного человека лишь за то, что он узнал больше, чем ему полагалось, сделало шпионский скандал неразрешимой проблемой. Так или иначе все вынуждены признать, что при нынешней политической ситуации в стране назвать организаторов и исполнителей «операции» просто невозможно. А значит, будет сделано все, чтобы замять это дело.

За кулисами общеевропейской сцены явно происходят некие перемены, косвенным свидетельством чему стало ужесточение позиции Евросоюза в отношении США. Так, в течение мая было по меньшей мере два неожиданных демарша.

Во-первых, Еврокомиссия резко изменила свою проамериканскую позицию в отношении патентов на программы (в новом законе о патентах программ не будет). Во-вторых, Суд Европы аннулировал американо-европейское соглашение, обязывающее авиакомпании передавать властям США данные о своих пассажирах. Теперь решено, что для этого нет подобающего юридического базиса.

Кое-что изменилось и для компании Ericsson, но не сказать, что в худшую сторону. Ныне шведская корпорация допущена к «святая святых» – к жирным внутриамериканским тендерам на заказы в области национальной безопасности.

Так, в объявленном недавно конкурсе на создание хайтек-системы для охраны южной границы США с Мексикой в четверке главных претендентов на контракт среди главных монстров американского ВПК – Lockheed Martin, Raytheon и Northrop Grumman – оказалась и Ericsson. За лояльность, как можно понять, положено вознаграждение.

Если же говорить о Греции, то здесь специфика политической ситуации в общих чертах такова. Несмотря на чрезвычайно острое противостояние двух главных партий, сменяющих друг друга у власти, – «консерваторов» Новой Демократии и «социалистов» ПАСОК, – обе стороны занимают откровенно проамериканские позиции.

Поэтому должно быть понятно, что не только полное расследование, но даже открытое обсуждение всей этой криминально-шпионской истории не сулит ощутимых выгод ни одной из основных сил на политической арене. Фактически, политики Греции предпочитают делать вид, что ничего особенного не произошло…

# # #

Секс, ложь и шпионы

(*Май 2012*)

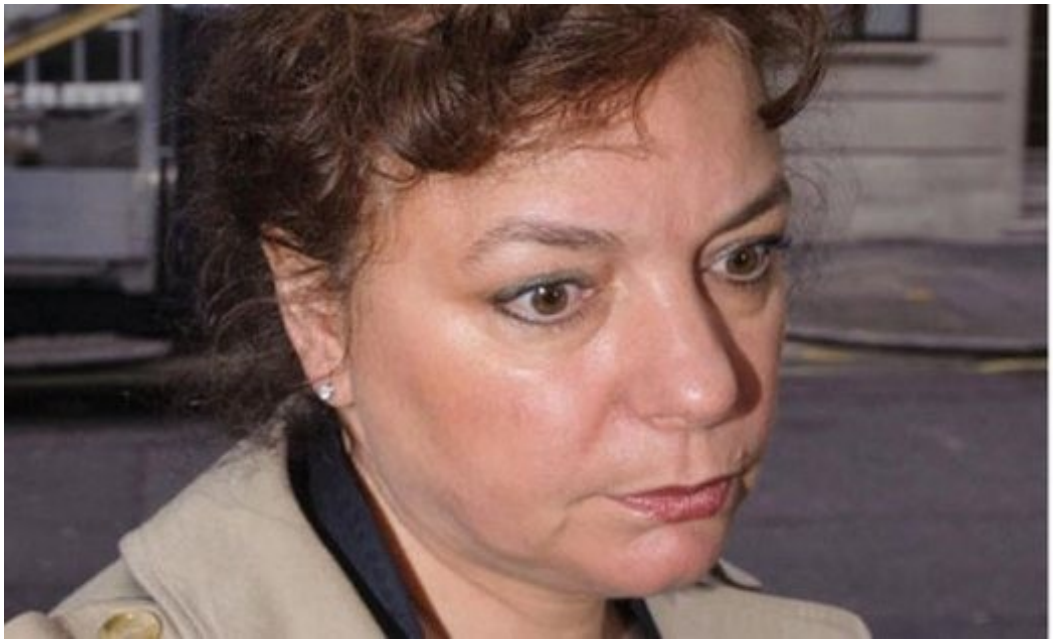
Самостоятельный фрагмент более крупного текста, посвященного таким сюжетам реальной жизни, которые выглядят «страньше, чем самое странное кино». Данный фрагмент – своего рода финальная глава в расследовании загадочной смерти английского шпиона Гарета Уильямса (см. ранее тут и тут).

Эта история куда более трагична и загадочна, нежели прочие, но при этом несет в себе столько черного юмора, что вполне могла бы лечь в основу какой-нибудь мрачной шпионской комедии в стиле братьев Коэнов.

Беда в том, что за сюжетом о комичной и абсурдной смерти сотрудника британской разведки Гарета Уильямса (Gareth Williams) стоит множество живых людей, потерявших самого близкого для них человека при абсолютно необъяснимых для следствия обстоятельствах. И черный юмор ситуации, к несчастью, только усугубляет горе родителей, родственников и друзей.

Тем не менее, дабы извлечь из этой трагедии хоть что-то полезное и поучительное, совершенно необходимо особо подчеркивать при рассказе наиболее странные моменты предпринятого властями разбирательства.

Итак, 2 мая этого (2012) года британский суд вынес вердикт по результатам слушаний дела о гибели Гарета Уильямса, сотрудника Секретной разведывательной службы, также известной как MI6. Подводя итог разбирательству, судья-коронер Фиона Уилкокс (Fiona Wilcox) пришла к выводу, что «смерть Уильямса невозможно однозначно объяснить исходя из имеющихся данных».



Более того, судья Уилкокс сочла необходимым также заявить, что смерть Уильямса вообще вряд ли когда-нибудь будет полностью объяснена, так как для этого недостаточно информации. Попутно, впрочем, судья-коронер отметила, что суд склонен считать смерть разведчика насильственной, но не может утверждать этого с достоверностью по той причине, что неоспоримых доказательств убийства нет…

Для тех, кто совсем не наслышан об этой престранной истории вокруг необъяснимой смерти одного из ведущих криптоаналитиков британской разведки, ключевые факты произошедшего выглядят так.

Тело совершенно голого Гарета Уильямса, компактно сложенное в «позе утробного плода» в спортивную сумку, было обнаружено полицией на ведомственной квартире MI6 в центре Лондона 23 августа 2010 года.

Погибший Уильямс проживал в этой квартире один – как кадровый сотрудник службы электронной разведки GCHQ, временно прикомандированный к MI6. Застегнутая на молнию сумка с его трупом была найдена аккуратно помещенной в ванну, однако следов постороннего проникновения в квартиру полиция не нашла.

Все экспертизы, проведенные криминалистами Скотланд Ярда, не дали следствию никакой содержательной информации об обстоятельствах смерти разведчика. Более того, судебно-медицинская экспертиза не смогла установить даже причину, из-за которой, собственно, умер этот молодой и здоровый человек в возрасте 31 года.

Но при этом в СМИ и бульварную прессу было сразу же слито немалое количество самой разнообразной информации о нестандартной сексуальной жизни погибшего. О том, в частности, что в квартире его нашли женские парики и кучу женской одежды на многие тысячи фунтов стерлингов. О том, что он посещал гейские бары, шоу трансвеститов и веб-сайты, посвященные всевозможным причиндалам для садомазохистских секс-утех.

Что в SIM-карте его мобильника обнаружены телефоны услуг «мужского эскорта», а в компьютере – следы посещения сайтов, посвященных клаустрофилии (поклонники этой небезопасной забавы наивысшее эротическое наслаждение получают от того, что оказываются запертыми в тесном ограниченном пространстве).

Короче говоря, практически все следствие по делу о смерти Гарета Уильямса на протяжении 21 месяца двигалось таким образом, что полиция безуспешно пыталась отработать версию о случайной гибели чудака-шпиона в результате его неудачных экспериментов с эротическим самоудовлетворением.

Делалось это очень упорно (специально приглашенные эксперты около 400 раз безрезультатно пытались сами запереть себя в саквояж, помещенный в ванну) и вопреки настойчивым возражениям родных и близких покойного, всегда подчеркивавших, что они хорошо знали особенности его личности, в которой не было признаков гея, трансвестита и садомазохиста-клаустрофила.

Единственным результатом бесплодных усилий Скотланд Ярда, собственно, и стало нынешнее судебное разбирательство коронера центрального Лондона Фионы Уилкокс. Английский коронер – это независимый представитель судебной власти, который расследует случаи насильственной или неестественной смерти, смерти по неизвестным причинам, а также случаи таких смертей, которые происходят во время пребывания человека в заключении или при задержании правоохранительными органами.

Основная особенность суда коронера в том, что это «суд дознания», а не «суд противостояния» обвиняющей и обвиняемой сторон. Главная же цель дознания – выявить те факторы смерти, которые можно изменить, дабы предотвратить подобные летальные исходы в будущем.

В случае с необъяснимой гибелью Гарета Уильямса коронеру предстояло разобраться с действительно непростой задачей. Но непростой отнюдь не потому, что фактов было мало, а скорее по той причине, что очень многие из известных фактов выглядели слишком «неудобно» и всячески игнорировались детективами полиции.

Суть всех этих неудобных проблем полезно изложить в виде неразрешенных следствием вопросов и сопутствующих им комментариев, поясняющих отсутствие удовлетворительных ответов.

- Находился ли кто-нибудь еще в квартире Гарета Уильямса в то время, когда оборвалась его жизнь? Официально считается, что никаких следов постороннего присутствия в квартире не обнаружено. В то же время эксперты признают, что ни на кафеле вокруг, ни на самой ванне не найдено никаких отпечатков рук или ног (голого) человека, найденного в сумке.

- Мог ли в принципе 30-летний мужчина самостоятельно упаковать себя в спортивную сумку, помещенную в ванну, застегнуть баул на молнию и, находясь уже внутри, еще и запереть молнию снаружи на висячий замок? Даже вне тесного объема ванны специально приглашенные эксперты не сумели продемонстрировать выполнимость подобного трюка. Ключи от замка, кстати, были найдены на дне саквояжа под трупом.

- Почему, когда на место происшествия прибыл специалист полиции по дверным замкам, способный установить признаки проникновения в дом посторонних, входная дверь квартиры уже была снята с петель, а замки с нее удалены? Странность этого факта усугубляется тем, что по свидетельству обслуги дома, дверь в квартиру было нельзя открыть снаружи, если замок был заперт изнутри. Однако местный констебль, обнаруживший в ванне труп, без проблем вошел в квартиру с помощью ключей уборщицы.

- Почему лучшие криминалисты Великобритании не смогли отыскать в квартире погибшего ни единого следа, по которому можно было бы идентифицировать

хоть каких-то людей, бывавших в квартире Уильямса – будь то по ДНК, отпечаткам пальцев или каким-то еще остаточным признакам? Здесь же уместно упомянуть, что за все время следствия полиция так и не смогла получить показания ни от кого из друзей по GCHQ или близких коллег Уильямса по MI6 (где друзей у него просто не было). Не было никого из них и на слушаниях в суде, где показания давали только начальники погибшего.

- От чего именно умер этот молодой, здоровый и спортивный человек? На теле Уильямса эксперты не обнаружили никаких внешних повреждений, а внутренняя экспертиза не выявила ничего необычного в крови и тканях тела. По свидетельству судмедэкспертов, установить точную причину смерти им сильно помешало далеко зашедшее разложение трупа, который нашли, как считается, через 8 дней после смерти Уильямса.

- Почему следствие упорно игнорирует показания констебля, обнаружившего труп, согласно которым сумка, в которой лежало тело, была кроме того наполнена какой-то специфической красноватой жидкостью, не похожей на воду или кровь? Этот же факт констебль повторил и на слушаниях в суде под присягой, однако и судью-коронера столь необычное обстоятельство почему-то не заинтересовало ни в малейшей степени. Еще одним странным обстоятельством, косвенно ускорившим разложение трупа, было очень сильное отопление в ванной комнате, почему-то включенное на максимум в жаркие дни августа 2010.

- Кто именно и по какой причине затребовал повторную судебно-медицинскую экспертизу трупа и каким образом служебная переписка между коронером и полицией по этому вопросу ныне оказалась необъяснимо «пропавшей»? Нынешний коронер Фиона Уилкокс вступила в эту должность 1 апреля 2011 года, поэтому все, что происходило до нее, предполагается как бы неведомым. А спросить, судя по всему, совершенно не у кого.

- Почему в спецслужбе MI6, где по инструкции положено начинать розыски сотрудника уже вечером того дня, когда он пропал, Гарета Уильямса даже не пытались всерьез искать больше недели? Причем звонок о пропаже человека поступил в полицию не из штаб-квартиры MI6, которая находится в нескольких сотнях метров от квартиры погибшего, а из штаб-квартиры GCHQ в графстве Глостершир, куда обратилась сестра Гарета Уильямса, обеспокоенная полной потерей контактов с братом. За столь вопиющее нарушение служебных порядков, как стало известно в суде, никаких наказаний или взысканий в MI6 не применялось.

- Почему в MI6 полностью спрятали от полиции не только служебные материалы покойного (раскрывавшие его чрезвычайно секретную шпионскую деятельность), но и множество личных вещей? Только на суде, находясь под присягой, один из следователей контрразведки, имеющий допуск в стены штаб-квартиры

MI6, признал, что на рабочем месте Уильямса под столом был обнаружен здоровенный саквояж с вещами погибшего, а также 9 принадлежавших ему флешек памяти. Ничего из этих вещей детективы полиции для исследования не получили, поскольку просто «не знали» об их существовании.

- Почему высокое руководство Скотланд Ярда настояло, чтобы в протоколе первичного осмотра места происшествия ни словом не упоминалось отсутствие (двух) личных ноутбуков Уильямса, хотя от близких было известно, что он с ними никогда не расставался? Через несколько дней эти компьютеры по-тихому всплыли в материалах дела. Вполне очевидно, что они находились на обработке в разведке, но вот как и когда именно они туда попали – осталось совершенно неясным. Коронерский суд этот крайне скользкий момент не заинтересовал абсолютно.

- Что содержала обнуленная память смартфона Уильямса, найденного в его квартире, и когда именно был сделан ресет содержимого аппарата до заводских установок? Технические эксперты Скотланд Ярда не только не смогли установить время, когда произошло это обнуление (до или после смерти владельца), но и оказались совершенно не в силах восстановить содержимое памяти аппарата. Хотя даже далекие от компьютеров люди давно в курсе, что за пределами компетентных органов имеется весьма развитая индустрия по восстановлению стертых данных в мобильных устройствах.

- Почему, наконец, руководство разведки с самого начала в заявлениях для прессы упорно настаивало, что смерть их чрезвычайно талантливого сотрудника абсолютно никак не связана с его служебной деятельностью? Но при этом (что показала запись разговора, предъявленная в суде) уже в самом первом звонке шпионов в полицию, где заявлялось об исчезновении их человека, начальница Уильямса на вопрос о морально-душевном состоянии пропавшего сообщила, что «его только что отстранили от работы, которой он занимался, и мы не знаем наверняка, как он это воспринял»…

Приведенная здесь дюжина неудобных вопросов – это, что называется, лишь небольшая, самая верхняя-заметная часть айсберга всей той огромной лжи, что уже нагромождена вокруг столь нехорошей кончины молодого человека, по всеобщим свидетельствам чрезвычайно одаренного в областях математики и компьютерных технологий.

Человека, главной жизненной ошибкой которого оказалась работа на разведслужбы своей страны. Потому что не видеть самой прямой связи между смертью Гарета Уильямса и его суперсекретной шпионской деятельностью не могут разве что совсем уж слепые и наивные.

Комментируя происходящее, британский эксперт Криспин Блэк (Crispin Black), в прошлом советник правительства по делам разведки, а ныне автор шпионских романов, говорит обо всем этом примерно так.

Для человека, близко знакомого с данной средой, сидящего на дознании по делу Гарета Уильямса и выслушивающего множество самых пикантных подробностей об особенностях частной жизни покойного, совершенно очевидно, что смерть шпионов при замысловатых обстоятельствах, включающих в себя изощренные секс-игры или женские наряды на мужиках – это отнюдь не есть что-то крайне необычное.

Избавиться от врага и обставить дело так, чтобы смерть выглядела как извращенная эротическая фантазия, пошедшая не по плану – это классический пример шпионской операции из учебных пособий всякой разведслужбы, от MI6 до Mossad.

Прикрытие секс-забавой – чрезвычайно удобный механизм при убийстве. Он не только обеспечивает маскировку для реально использованных при ликвидации средств и методов убийства, но также вдребезги разрушает репутацию жертвы, ощутимо подрывая энергию и инициативу людей, занимающихся последующим расследованием.

Все это хорошо известные в разведывательном мире факты. И они могут объяснить то поразительное число шпионов, а также прочих людей, по неосторожности вступивших в их опасный мир, которых обнаруживают мертвыми при обстоятельствах, похожих на смерть Гарета Уильямса.

Взять, к примеру, персонал основного места службы Уильямса, GCHQ или Штаб-квартиры правительственной связи, где занимаются перехватом и дешифрованием электронных коммуникаций.

В 1983 году 25-летний сотрудник GCHQ Стивен Дринкуотер (Stephen Drinkwater), работавший с документами в особо секретном подразделении, был найден у себя дома мертвым с пластиковым пакетом на голове.

В 1997 году другой сотрудник GCHQ, Николас Хасбенд (Nicholas Husband), 46 лет, был обнаружен дома мертвым, одетым в бюстгальтер и женские панталоны – и с пластиковым пакетом на голове.

Еще два года спустя, в 1999, лингвист-переводчик GCHQ Кевин Аллен (Kevin Allen), 31 год, был найден мертвым в своей кровати – с пластиковым мешком на голове и с маской-респиратором, заткнувшей ему рот.

В отличие от смерти Гарета Уильямса в центре Лондона, сразу же попавшей в криминальную хронику столицы и потому широко освещаемой, все упомянутые прежние случаи прошли совершенно тихо и классифицированы местной полицией Глостершира как «непредумышленные самоубийства».

В общей же сложности, если вести подсчет по британской разведке в целом, за последние полвека экспертами насчитывается по крайней мере 17 странных смертей подобного рода.

Хотя и эксперты по разведке, и тем более полиция предпочитают не выдвигать гипотез о возможных мотивах устранения Гарета Уильямса «по шпионской линии», нельзя сказать, что информация на данный счет отсутствует. Скорее даже наоборот.

Благодаря расследованиям журналистов из трудно контролируемых таблоидов, стало известно о некой трудноуловимой женщине-загадке, близко дружившей с Уильямсом в последний год его жизни и рассказавшей полиции много чего интересного о его личности и занятиях вне службы. Вот только в суде все эти показания по объяснимым причинам не прозвучали.

Из рассказов 27-летней американки Элизабет Гатри (Elizabeth Guthrie), которые были по частям зафиксированы в протоколах полиции под тремя разными именами (ее настоящим, а также как Миссы Гюнтер и как Мисы Гусейри) получалось вот что.

Гарет Уильямс определенно не был геем или трансвеститом, проявляя совершенно обычный мужской интерес к женскому полу. Также он сильно интересовался женской модой, часто покупал и дарил подругам дорогие вещи (то же самое подтвержают его сестра и другая близкая подруга, с которой Уильямс дружил с начальных классов школы).

Интерес шпиона-криптолога к моде был настолько велик, что в свободное время от основной службы – по вечерам и выходным – он закончил два курса по дизайну оде-

жды в одном из известных лондонских колледжей (также подтверждено администрацией курсов).

Кроме того, по свидетельствам женщин из близкого внерабочего окружения Уильямса, его стала сильно тяготить прикомандированная служба в MI6, так что он уже договорился о своем обратном переводе в GCHQ. А попутно, вместе с Элизабет Гатри и еще одним неназываемым сотрудником спецслужбы, они задумали организовать некий собственный бизнес, полностью оставив работу в разведке.

Незадолго до смерти, летом 2010 года, Гарет Уильямс заметил за собой слежку, о чем доложил руководству в MI6. Факт его доклада о сопровождающем «хвосте» (двое белых мужчин в возрасте около 40) стал известен прессе практически сразу после смерти из неофициальных источников в разведке, однако официальным руководством MI6 был категорически опровергнут.

В показаниях Элизабет Гатри эпизоды со слежкой всплыли опять, причем, по ее словам, Гарет был настолько обеспокоен этим эскортом, что стал менять обычные маршруты своих передвижений по городу.

Все эти факты, впрочем, в суде не прозвучали, а соответствующая статья таблоида Mirror с изложением рассказов Элизабет Гатри вскоре с сайта газеты бесследно исчезла…

Если же еще раз вспомнить главную цель судебного дознания коронера – выявить те факторы смерти, которые можно изменить, дабы предотвратить подобные летальные исходы в будущем – то можно считать, что суд свою задачу выполнил.

Молодым и умным людям, имевшим неосторожность глубоко погрузиться в большие шпионские тайны государства, не следует задумываться о переходе на другую работу.

Ибо это крайне опасно для жизни.


© REXMAILPIX

# # #

Стойкость к имитации

(*Февраль 2015*)

О загадках и странностях, окружающих феноменально успешную картину «Игра в имитацию» – как первую в истории кино биографию Алана Тьюринга, великого математика, криптографа и «отца» современных компьютеров. (*Своеобразное новое дополнение к более обширному исследованию «**Гостайна как метафора**».*)

В воскресенье, 22 февраля 2015, в США проходит ежегодная церемония вручения премии «Оскар» – формально американской, но с некоторых пор наиболее престижной награды среди кинематографистов всего мира (и это просто факт, в независимости от того, нравятся кому-то подобные расклады или нет).

Среди фильмов, выдвинутых на главные призы, есть и полный шлак – типа «Американского снайпера», прославляющего безмозглый патриотизм и боевое братство вояк, убивающих без разбору всех – мужчин, женщин, детей – в чужой, далекой и совершенно чуждой им стране. Есть картины неоднозначные, вызывающие жаркие споры и тяжкие раздумья – вроде российского «Левиафана» или польской «Иды». Есть произведения своеобразные и ни на что не похожие – как, например, последняя работа Уэса Андерсона «Отель Гранд-Будапешт».

Однако самым необычным явлением среди фильмов-номинантов (а может, и вообще во всем кинематографе 2014 года) определенно следовало бы считать картину «Игра в имитацию».

Когда сразу на 8 Оскаров – включая самые престижные (лучший фильм, лучшая режиссура, лучший сценарий и т.д.) – выдвигают кино, сделанное аутсайдерами с помо-

щью небольшой независимой компании и в рамках смешного для Голливуда бюджета, это уже интересно.

Но в данном случае мы имеем дело с неординарным событием, интересным втройне. С картиной, которая стала первым самостоятельным проектом молодых продюсеров, супружеской пары Норы Гроссман и Айдо Островски. Сценарий фильма написан еще более молодым автором, Грэмом Муром, для которого это первая в его жизни постановка. Ну а сделал этот шедевр норвежский режиссер Мортен Тильдум – как первый в своей жизни опыт полнометражного кино на английском языке.

Бенедикт Камбербэтч в роли Тьюринга и режиссер Мортен Тильдум

При столь скромных начальных условиях успех фильма оказался потрясающим – не только у критиков и коллег, но и среди широкой публики. Меньше чем за три месяца проката, к началу февраля 2015 «Игра в имитацию» собрала кассу порядка 140 миллионов долларов – практически в десятикратном размере возместив бюджетные расходы на съемку. И дабы любому человеку, далекому от кулуаров кинопроизводства, стало понятна степень необычности тут происходящего, надо кое-что пояснить.

Когда у сценариста появляется идея для постановки, он или она начинают искать тех, кто заинтересуется воплощением проекта. Ну а для общей характеристики замысла формулируется «гранд-концепция» – в нескольких словах, ёмко и предельно кратко излагающая суть сюжета. Нередко такая формула может звучать как полная дичь (без всяких там политкорректных реверансов), однако при умелом подходе к делу, бывает, в итоге получается очень успешное кино.

Например, сюжет известного всем фантастического фильма-блокбастера «День независимости» вполне адекватно сводится к следующей фразе: «О том, как два неудачника, еврей и негр (плюс еще один чокнутый алкаш), лихо спасли Землю от вторжения злобных инопланетян, заразив вражеский космофлот компьютерным вирусом»…

В нашем же случае, когда начинающий литератор Грэм Мур в поисках успеха и счастья переехал в Голливуд, то в кругах кинобизнеса он не раз пытался привлечь интерес к идее о фильме про Алана Тьюринга. Вот только формула его сюжета абсолютно никакого интереса в этих сферах поначалу не вызывала.

Что вряд ли удивительно, коль скоро суть концепции звучала примерно так: «О том, как гениальный математик-гомосек изобрел компьютер, взломал шифры нацистов и помог государству выиграть вторую мировую войну. После чего это же государство ученого и убило – потому что слишком много знал и был не такой, как все». Муру внятно и доступно дали понять, что в нынешние времена – да еще в Голливуде – на экранизацию столь подрывных идей никто и наверняка не захочет потратить ни единого цента…

Так что первые годы сценаристу приходилось зарабатывать на хлеб всякой ерундой типа халтурки в комедийных ТВ-сериалах, а возможности для творческой самореализации искать где-то еще – на поприще детективных романов, к примеру.

Ну а затем, когда к Муру пришел первый успех с романом «Шерлокиана», вдруг одно за другим начали происходить маленькие чудеса вокруг его давнего замысла про кино о Тьюринге. Знакомство с начинающими продюсерами, счастливая судьба сценария, выбор правильного режиссера, удачные актеры на главных ролях – все этапы рождения фильма как-то очень естественно уложили процесс кинопроизводства в русло, независимое от больших компаний. В итоге никто авторам не помешал, и они сделали именно то, что хотели. А зрители по достоинству оценили результат.

Вот только фоном для бесспорного успеха картины стали выступать не очень приятные вопросы и претензии людей, действительно сведущих в событиях и фактах жизни Алана Тьюринга.

Реально все было иначе

Успех любого произведения искусства у публики с необходимостью влечет за собой и его углубленный анализ. В случае же с «Игрой в имитацию» самое первое, что бросается в глаза специалисту – это чудовищное расхождение художественного вымысла с тем, что было на самом деле.

Ситуация здесь такова, что практически все сцены кинокартины так или иначе перевирают подлинные факты. Причем неправда зачастую носит принципиальный формообразующий характер. Начиная с того, что в действительности вовсе НЕ Тьюринг

придумал, как вскрывать шифр «Энигмы». И заканчивая тем, что в создании подлинного цифрового суперкомпьютера Colossus, построенного англичанами в Блечли-Парк для взлома германской шифрпереписки, лично Алан Тьюринг никакого участия не принимал.

Ну а действительно придуманную Тьюрингом дешифровальную машину, носившую название Bombe, даже с натяжкой называть компьютером весьма сложно. Ибо реально это был стенд для одновременной работы 36 электромеханических реплик «Энигмы», которые за счет оптимизированной параллельной обработки сильно ускоряли отыскание ключевых установок шифратора. Причем и базис дешифрования, и исходный прототип такой машины передали англичанам криптоаналитики Польши, начавшие вскрывать «Энигму» задолго до того, как ею занялся Тьюринг.

Из всего этого, впрочем, совершенно не следует, будто заслуги Алана Тьюринга на компьютерно-криптологическом поприще авторами фильма выдуманы. Вовсе нет. Просто реальная история криптографии и вычислительной техники намного сложнее и богаче, нежели это можно было бы уложить в 2-часовой художественный фильм жанра «шпионский триллер». Но вот зачем в этом кино изобильно придуманы такие конфликты, которых реально не было, и в то же время подлинные острые моменты, напротив, почему-то остались за кадром – это действительно большой вопрос…

Особую же отчетливость вопросы подобного рода обретают в ситуации, когда авторы фильма всячески настаивают на подлинности описываемых ими событий. В частности, сценарист и (что обычно для кинопроцесса не характерно) исполнительный продюсер картины, Грэм Мур, участвовавший в воплощении своего сценария на всех этапах производства, не только подчеркивает тщательную работу над сюжетом, но и такие вот вещи:

> *«Историческая точность была для нас гигантски важным делом. Мы чувствовали свою ответственность – сделать это правильно и сделать с уважением»…*

Своеобразное объяснение для столь очевидной логической неувязки можно найти в интервью Грэма Мура журналу WIRED (www.wired.com/2014/11/imitation-game-secrets/), явно не случайно опубликованному 28 ноября 2014, в день общенациональной премьеры «Игры…» в кинотеатрах США.

В этом интервью автор признается, что на самом деле его сценарий – это паззл, головоломка, которую аудитории предлагается решить самостоятельно:

> *«По жизни Тьюринг страстно увлекался кодами, паззлами и играми, – говорит Мур. – И я хотел, чтобы все наше кино было Игрой В Имитацию, где ответом к головоломке стала бы подлинная история Алана Тьюринга».*

В качестве подсказки к своей головоломке Грэм Мур предлагает обратить внимание на специфическую «прыгающую» структуру фильма. Рассказ все время перескакивает то назад, то вперед между разными периодами времени – то к финальными дням перед смертью Тьюринга, то к его работе в Блечли-Парке, то к его школьному детству.

Сценарист фильма Грэм Мур

Ну а другая очень важная подсказка Мура звучит так:

> *«Самые содержательные свидетельства о том, что происходило во взаимоотношениях между Аланом Тьюрингом и MI6 после того, как криптографы взломали германский шифр, в действительности почерпнуты из дневника Яна Флеминга – как это ни удивительно»…*

При чем тут Ян Флеминг?

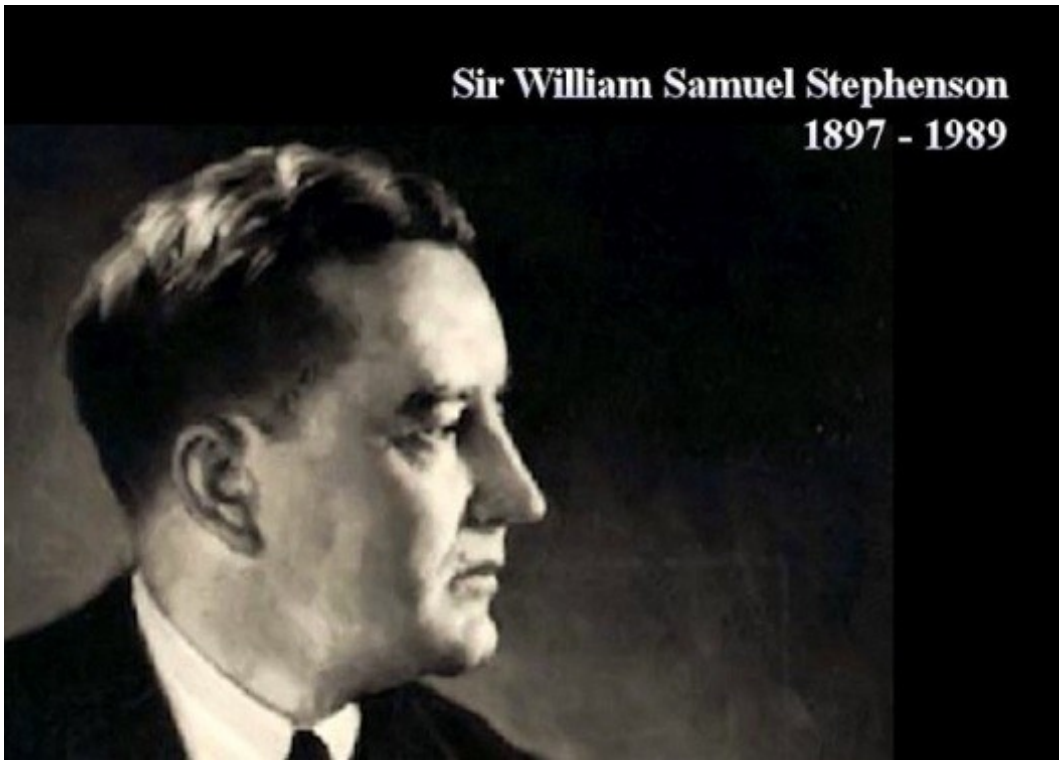
Из-за той безумной популярности, что выпала на долю самого знаменитого шпиона всех времен и народов, носящего имя Джеймс Бонд или агент 007, эпистолярное твор-

чество Яна Флеминга – как создателя столь грандиозного персонажа – давно изучено поклонниками бондианы от корки до корки. Так вот, в этой компетентной среде никто и никогда не только не видел, но и не слышал никаких упоминаний о таком источнике, как «дневник Яна Флеминга».

Иначе говоря, практически наверняка такой вещи в природе просто нет. А единственное, по сути, место, где словосочетание «Ian Fleming Diary» встречается в интернете (помимо «утки Мура») – это весьма специфический проект www.mi6-hq.com, в свое время возникший как побочное ответвление официального веб-сайта британской разведки SIS, также известной под названием MI6.

В 2008 году, по случаю 100-летия Флеминга и для формирования в народе привлекательного образа «шпионов с человеческим лицом», в разведслужбе завели особую веб-витрину под названием «MI6 – дом Джеймса Бонда». Ну а термином «дневник Яна Флеминга», соответственно, здесь окрестили расписание всевозможных юбилейных мероприятий в память о шпионе, ставшем знаменитым писателем и прославившем на весь мир оперативные подвиги британской разведки.

Подвиги эти, конечно же, Флемингом были выдуманы. Но за каждой шпионской фантазией, как известно, обычно скрываются те или иные реальные события и люди. В частности, реальным прототипом для Бонда, по признанию самого писателя, стала «сильно романтизированная» версия человека, носившего имя Уильям Стивенсон и псевдоним INTREPID (бесстрашный), полученный им от Уинстона Черчилля.



Про удивительную биографию Стивенсона и его весьма характерное отношение к убийствам людей можно почитать в других местах (несколько ссылок даны в конце

текста), здесь же нас интересуют лишь два конкретных момента, непосредственно связанных с военным периодом Алана Тьюринга и фильмом «Игра в имитацию».

Во-первых, сыграв ключевую роль в военно-стратегическом сближении США и Британии, а затем и в формировании тесного альянса англо-американских разведслужб, Уильям Стивенсон естественным образом стал центральной фигурой в делах, связанных с распределением среди союзников информации, получаемой англичанами из дешифрованной германской переписки.

Этот чрезвычайно тонкий момент – как воспользоваться добытыми сведениями, одновременно не скомпрометировав и не потеряв ценный источник – очень топорно отображен в нынешнем фильме про Тьюринга. Где сами криптоаналитики якобы решали, когда и что сообщать из добытой ими информации. На самом деле, конечно же, эта кухня работает совершенно иначе. А все решения здесь принимаются на куда более высоком политическом уровне.

Второй же момент, непосредственно связанный с первым, касается знаменитой истории с разбомбленным Ковентри. В своих мемуарах (или «дневниках Бесстрашного», если угодно) Стивенсон рассказывает, что из германской шифр-переписки, читавшейся разведкой, Уинстон Черчилль заранее знал о массированном авианалете армады Люфтваффе на город Ковентри, разрушившем свыше 50 тысяч домов и унесшем гигантское количество человеческих жизней.

Однако заранее предупреждать город и его население об авианалете власти сочли нецелесообразным, ибо здесь слишком высок был риск раскрытия тайны дешифрования немецких коммуникаций. Не без своеобразной профессиональной гордости Стивенсон попутно подчеркивает, что это именно он склонил к такому решению сильно колебавшегося Черчилля: «Война есть война – жертвы здесь неизбежны»…

Хотя этот очень мрачный эпизод из истории войны также подтверждается в книге «Тайна Ультра» от другого участника тех же событий, английского разведчика Фредерика Уинтерботема, официальная британская история по понятным причинам категорически данный факт отвергает. И ответственно заверяет, что «Черчилль ничего тут и знать не знал».

Примерно по тем же причинам – слишком уж неудобны для отлакированной версии истории циничные свидетельства шпионов – ни в США, ни в Великобритании власти по сию пору не решились на официальное раскрытие и издание топ-секретного разведотчета 1946 года под названием «The BSC Papers». Это, можно сказать, самые главные дневники Уильяма Стивенсона – о деятельности возглавлявшегося им «Британского центра координации безопасности», охватывавшего своей активностью оба американских континента в годы второй мировой войны.

Если характеризовать суть документа предельно кратко, то именно отчеты Стивенсона о шпионских операциях BSC на территориях самых разных нейтральных стран (операциях очень жестких, часто связанных с убийствами и однозначно трактуемых как тяжкая уголовщина по законам любого государства) в свое время и послужили источником вдохновения для творчества Яна Флеминга. Откуда, собственно, и родился мифологического масштаба герой MI6 по имени Бонд, Джеймс Бонд.

Внимание к деталям

После краткого экскурса в историю разведки и литературы «про шпионов», теперь самое время вернуться к картине «Игра в имитацию». И повнимательнее присмотреться к некоторым сценам из этого фильма. Причем рассматривать их не просто как художественный вымысел, а в сопоставлении с подлинными фактами из биографии Тьюринга. А также – самое главное – в сопоставлении с недавними событиями из жизни и смерти другого талантливого англичанина по имени Гарет Уильямс. Еще одного странноватого математика и компьютерщика, также имевшего неосторожность связать свою биографию с разведслужбами государства и с их темными ультра-секретами. Благодаря таким скачкам во времени легче заметить нечто важное и обычно ускользающее от внимания.

Вот, скажем, коротенькая сцена из самого начала фильма. В 1951 г. британская разведка перехватывает разговор полиции, из которого узнает, что дом Тьюринга ограблен. Поясняя суть происходящего более доходчиво, это означает, что спецслужба государства постоянно следит за своим же выдающимся ученым, расценивая его как потенциальный риск или угрозу национальной безопасности. (У историков имеются факты, согласно которым Тьюринг примерно за год до смерти сетовал в разговорах с друзьями, что за ним следят, а переписку читают, из-за чего срываются важные лично для него контакты.)

Реальная сцена из 2010. За несколько месяцев до своей смерти Гарет Уильямс обнаруживает, что за ним по Лондону регулярно следуют какие-то люди. Обеспокоенный «хвостом», он начинает менять обычные маршруты передвижений и докладывает об этом своему начальству в MI6. Впоследствии на суде, разбиравшемся с гибелью их сотрудника, руководство разведки будет всячески отрицать этот эпизод, несмотря на несколько независимых свидетельств.

Сцена из фильма. Полиции, расследующей подозрительное происшествие в доме Тьюринга, удается получить доступ к папке с его секретным досье времен второй мировой войны. Однако, когда папку открывают, то выясняется, что она пустая – все содержательные документы из нее уже кем-то изъяты… Попутно становится известно, что Тьюринг гей, и коль скоро официально это считается преступлением, из потерпевшего ученый превращается в обвиняемого.

Сцена из 2010. Когда полиция пытается найти зацепки к тому, что произошло в доме Гарета Уильямса, особый интерес следователей вызывают, ясное дело, его смартфон и ноутбуки. Однако и память телефона, и диски компьютеров оказываются уже зачищены «неизвестно кем»… При этом в доме холостяка обнаруживаются женские парики, куча женской одежды и признаки довольно необычных секс-забав. С этого момента главной версией следствия становится бытовая смерть гея-трансвестита, наступившая из-за его неосторожных сексуальных экспериментов.

Сцена из фильма (полностью выдуманная авторами картины): советский шпион из «кембриджской пятерки», Джон Кернкросс, узнав о гомосексуальной ориентации Тьюринга, тут же начинает его шантажировать и склонять к сотрудничеству… Факты реальной жизни (полностью отсутствующие в фильме) были таковы, что в 1951 году два других советских шпиона из «кембриджской пятерки», Гай Берджесс и Дональд Маклин, сбежали в СССР. Про одного из них, Берджесса, было известно, что он гей. И нет никаких сомнений, что в угаре холодной войны и шпионской истерии гомосексуальность слишком много знающего Тьюринга расценивалась в разведслужбах как очень серьезный риск для национальной безопасности. Особенно в свете того, что в годы перед смертью Тьюринг предпочитал проводить отпуски за рубежом, выбирая страны, толерантные к заведениям и сообществам геев. В частности, последний раз он ездил отдыхать в Грецию.

Сцена из 2010. Расклады истории легли так, что именно в этот год бурлящая политическая жизнь в Греции привела к очередному оживлению интереса к очень странной и нехорошей шпионской истории 5-летней давности. Тогда, напомним, телефонную сеть ведущего в стране оператора мобильной связи, Vodafone Greece, хакнула некая иностранная разведка, телефоны первых лиц государства прослушивались шпионами, а когда эти вещи стали всплывать, то один из топ-менеджеров сотовой компании, Костас Цаликидис, якобы «совершил самоубийство», причем расследование всего произошедшего по сути дела было спущено греческими властями на тормозах… В то же время Гарет Уильямс был известен в англо-американской разведке как ведущий технический специалист по шпионажу в сетях сотовой телефонии. По 3-4 раза в год он летал к коллегам в США, а кроме того – уже под чужим именем – не раз ездил в служебные командировки, среди прочего, и в страны средиземноморского региона.

В роковой же для него 2010 год Уильямса уже до такой степени стала тяготить шпионская работа, что он, по свидетельству близких, решил уйти из разведки в бизнес. В августе он последний раз побывал в США, по возвращении в Лондон его официально отстранили от дел в MI6, а еще примерно через неделю – и за несколько дней до начала нового парламентского расследования в Греции – труп Гарета Уильямса обнаружила лондонская полиция… При каких обстоятельствах и отчего именно оборвалась жизнь молодого и здорового человека, так и не смогли достоверно установить ни криминалисты полиции, ни коронерское судебное разбирательство…

Возвращаясь к фильму «Игра в имитацию», осталось отметить, что авторы картины совершенно умышленно, по их свидетельству, не показывают в финале собственно гибель великого математика (ибо ее тоже окружают свои загадочные обстоятельства). Вместо этого на экране идут заключительные титры с таким примерно текстом:

> *Алан Тьюринг убил себя в 1954 году, после того, как год подвергался государством принудительной гормональной терапии. Факты дешифрования Энигмы официально оставались государственным секретом на протяжении свыше 50 лет… Математические работы Алана Тьюринга вдохновляли несколько поколений ученых на исследования того, что в науке именуют «машинами Тьюринга», а в мире более известно как компьютеры…*

Это называется имитостойкость

В теории криптографии – как науки о защите информации – имеется специфическое понятие «имитостойкость». Формулируя подоходчивее, суть термина заключается в особом способе передачи сообщения. Так, чтобы содержащаяся в нем информация надежно доходила до получателя – несмотря на всяческие вставки или изъятия фрагментов, а также прочие искажения послания, которые противник может делать на канале доставки.

Иначе говоря, неприятель всегда старается в своих интересах исказить смысл доставляемого сообщения, имитируя его подлинность. Ну а отправитель (автор), в свою очередь, может сам заранее модифицировать свое послание таким образом, чтобы получатель на приемном конце все равно понял подлинную суть информации – несмотря на все ухищрения противника.

Все это, однако, возможно лишь при одном важном условии. Те, кто принимают сообщение, должны быть внимательны к деталям послания.

В самом начале картины «Игра в имитацию» закадровый голос Алана Тьюринга, обращаясь к зрителям, говорит с экрана примерно такие весьма загадочные фразы:

> *«Вы обращаете внимание на детали? Хорошо. Если вы будете невнимательны, то вы кое-что упустите. Важные вещи. Я не буду делать паузы, я не буду повторять, а вы не будете меня перебивать. Вы полагаете, будто из-за того, что вы сидите там, где вы сидите, а я нахожусь тут, где я, то это вы управляете тем, что будет происходить. Так вот, вы ошибаетесь. Это я здесь управляю. Потому что я знаю такие вещи, которых вы не знаете.*
> <…>
> *Но вот все то, что будет происходить далее, начиная с данного момента – это уже не моя ответственность. Это ваша. Обратите на это внимание»…*

Ни кинофильм «Игра в имитацию», ни текст данной статьи, тем более, не могут навязать человеку ответственное восприятие информации, ясное дело. Имитацию правды навязать можно, а вот ответственность – нет.

Но собранных здесь материалов, думается, уже достаточно, чтобы зрители и читатели не только могли бы отличать достоверные факты истории от авторского вымысла, но и понимали бы, с какой целью эти искажения были внесены.

# # #

Дополнительное чтение

О крайне загадочной смерти Гарета Уильямса, ведущего специалиста британских спецслужб GCHQ и MI6: «**Секс, ложь и шпионы**»;

Редко упоминаемые и просто необычные факты вокруг истории шифратора ENIGMA: «**Загадка загадок**»;

Факты и фактоиды о яркой, очень короткой и чрезвычайно секретной жизни первого цифрового суперкомпьютера разведслужб: «**Колосс британский**»;

Про знаменитого, но неизвестного разведчика Уильяма Стивенсона: «**Шпионы и мафиози**», «**Правда жизни**»;

О множестве неясных по сию пору страниц в ранней истории компьютеров и в биографиях их создателей: «**Тайны внутри секретов**»;

Про характерные события и весьма специфический контекст, определявшие развитие науки в разгар холодной войны: «**Бунт ученого**»;

О цепи преступлений, сопровождавших шпионские скандалы последних лет: «**Вопросы на греческом**», «**Серийные самоубийцы**».

Универсальная модель для усвоения уроков

Всего три слайда

(*Июль 2013*)

Что можно почерпнуть из истории Эдварда Сноудена, если анализировать ее с позиций компьютерной безопасности и защиты информации.

В драматичной череде событий, сопровождающих разоблачительные сливы Эда Сноудена о тайнах спецслужб, особо интересными представляются как бы «побочные» эпизоды этой саги.

Эпизоды, которые на самом деле – при надлежащем к ним внимании – раскрывают суть происходящего в мире куда более адекватно, нежели весь тот трескучий и малосодержательный шум в СМИ «о шпионах, которые шпионят».

Вот лишь два типичных примера навскидку.

Когда Эдвард Сноуден озвучил официальное обращение к двум десяткам стран с просьбой о предоставлении ему политического убежища, а в качестве наиболее пред-

почтительного пристанища была названа Исландия, там тут же обозначился генеральный секретарь ООН Бан Ки Мун.

Выступая в Рейкьявике перед членами исландского парламента, глава важнейшей на планете международной организации счел нужным не просто персонально упомянуть Сноудена (что для главы ООН в высшей степени странно), но и всячески его осудить «за безответственное раскрытие» секретов разведывательных спецслужб. То есть публикацию правды о нелегальной возне шпионов, по убеждению Муна, следует расценивать не иначе, как «злоупотребление» информацией, создающее для мирового сообщества больше проблем, чем пользы…

Эпизод второй – это злосчастное возвращение на родину президента Боливии Эво Моралеса, когда Франция-Испания-Португалия-Италия дружно (и с вопиющим нарушением общепринятых международных норм) перекрыли воздушное пространство Европы, заставив президентский самолет вынужденно приземлиться в Австрии.

А на земле венского аэропорта борт главы суверенного государства, находящегося при исполнении официальной миссии, был подвергнут унизительному досмотру – на предмет выявления «посторонних лиц». (Раз Моралес летел из Москвы, а там одобрительно отозвался о смелости Сноудена, то «кто-то» – не шибко умный, но очень могущественный – подобным способом решил, очевидно, помешать перемещению беглеца-разоблачителя в Южную Америку.)

Понятно, наверное, что все такие вещи являются полнейшим дипломатическим беспределом. Фактически, криминалом на государственном уровне и примером того, как не могут и не должны быть устроены международные отношения в цивилизованном мире. Но куда менее понятными выглядят собственно те механизмы, с помощью которых и руководством ООН, и властями далеко не последних государств планеты можно, оказывается, манипулировать, словно безмозглыми марионетками…

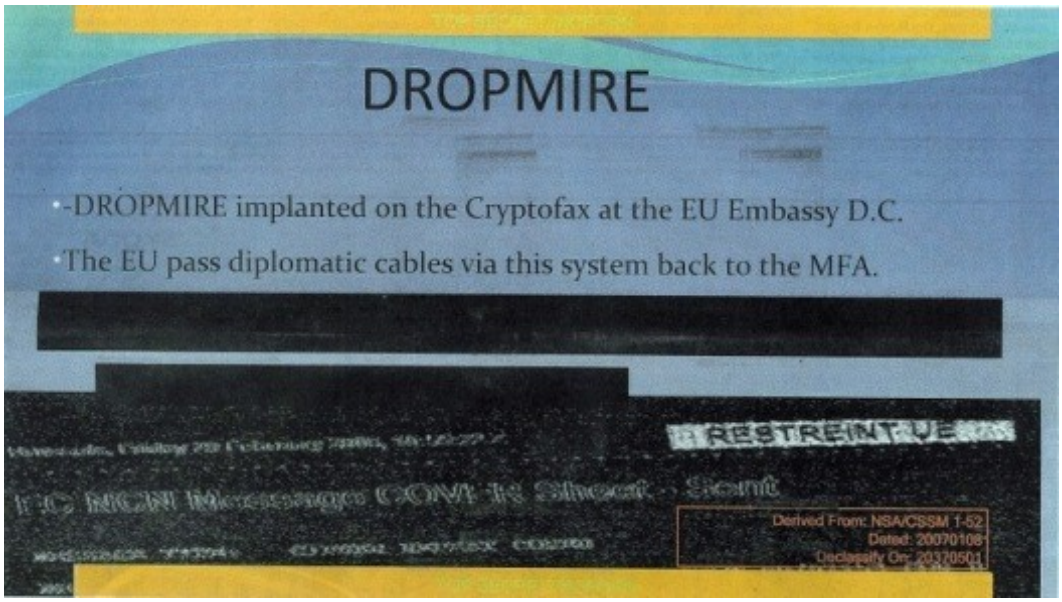
Так вот главная, пожалуй, суть топ-секретных документов, которые благодаря Сноудену появляются ныне в прессе для всеобщего ознакомления, заключается именно в этом. Данные материалы одновременно являются и документальными свидетельствами, и своего рода «шпионскими метафорами», наглядно поясняющими, каким образом в действительности устроена вся жизнь в нашем странном мире.

Иными словами, почти любой из слайдов внутренних презентаций АНБ США, оказавшихся ныне на страницах СМИ, можно трактовать двояко. С одной стороны, как содержательную информацию о реальных технологиях и масштабах компьютерного шпионажа. А с другой стороны – как аллегорию, отражающую ту или иную грань почти всеобщей слепоты общества, не имеющего практически никакого представления о реальных механизмах власти и тайных делах спецслужб.

[*В конце каждого подраздела приводятся ссылки на дополнительные материалы и расследования, дающие более адекватную картину происходящего.*]

СЛАЙД # 1: «ГРЯЗЬ ПО КАПЛЯМ»

Начать иметь смысл с наименее выразительного, на взгляд многих, слайда. На котором нет ни впечатляющих блок-схем о работе систем перехвата АНБ, ни таблиц с перечислением ведущих ИТ-корпораций, как провайдеров, снабжающих разведку США данными и коммуникациями всех своих клиентов.



На этом же невзрачном слайде чуть ли не единственно содержательная информация говорит о том, что технология перехвата под названием DROPMIRE внедрена американской спецслужбой в факсимильный шифратор Cryptofax, засекречивающий переписку посольства Евросоюза в Вашингтоне.

Чтобы сразу стало ясно, насколько взгляд специалиста отличается от взгляда несведущего человека, далее полезно привести рассказ Маркуса Куна, которого именно этот слайд – среди всех прочих разоблачений Сноудена – заинтриговал наибольшим образом.

Причина обостренного интереса в том, что в открытом академическом сообществе Маркус Кун является одним из главных специалистов в области TEMPEST. Этим кодовым словом уже довольно давно принято называть особые шпионские технологии, которые через побочные компрометирующие излучения аппаратуры позволяют похищать информацию о содержании тех документов, которые данные аппараты обрабатывают.

Тему TEMPEST принято считать очень большим секретом спецслужб. Так что о том, как подобные вещи делаются ныне у шпионов, информации в открытой литературе почти что нет. Но на рубеже 1980-90 годов это направление исследований было само-

стоятельно «переоткрыто» академическим сообществом ученых и специалистов по компьютерной безопасности. От них-то постепенно публика и узнала про возможности TEMPEST много интересного.

И вот, поскольку Куну, работающему в Компьютерной лаборатории Кембриджа, в свое время доводилось лично проводить массу экспериментов по перехвату компрометирующих сигналов-утечек от офисного оборудования, то в слайде про Евросоюз и DROPMIRE он тут же распознал хорошо знакомую ему картинку.

Сильно зашумленное изображение в нижней трети слайда – это то, что исследователь может получить из эфира, если станет целенаправленно прослушивать его с помощью качественного радиоприемника на предмет выявления компрометирующих излучений. В частности, очень похожим образом выглядит перехватываемый видеосигнал от дисплея с изображением страницы текста.

В ходе своих исследований Маркус Кун больше всего занимался побочными утечками от катодно-лучевых кинескопов и LCD-дисплеев компьютеров, а излучения факсимильной техники в его круг интересов прежде как-то не попадали. Кроме того, Кун особо подчеркивает, что не знает больше ничего о данном конкретном случае, кроме освещаемого в газетах.

Однако, тщательное рассмотрение зашумленного сигнала со слайда дает ему несколько существенных подсказок о работе конкретно этой шпионской технологии.

Давайте приглядимся, предлагает он, к тому, как именно выглядит текст заглавными буквами «EC NCN»:

Можно заметить, что только вертикальные края этих букв обозначены как яркие линии. В то время как соответствующие горизонтальные края по сути дела отсутствуют (например, в буквах E и N).

Теперь представим себе, что устройство, от которого перехватывается сигнал – это факс-машина на основе движка лазерного принтера. В таком аппарате луч лазера последовательно, один за другим, экспонирует пиксели изображения на светочувствительный электрически заряженный барабан.

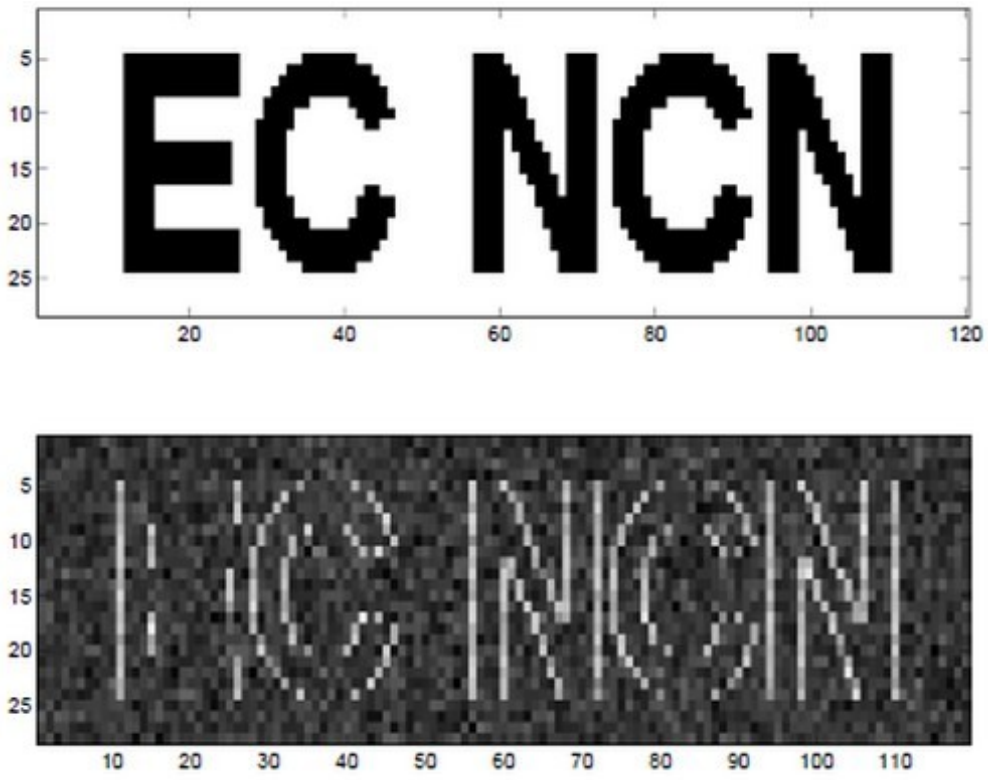
Если лазер «включен», то в той точке, где он освещает барабан, происходит снятие заряда статического электричества, так что порошок тонера не прилипнет, и в результате это будет белый пиксель. Если же лазер выключен, то поверхность барабана остается заряженной, тонер прилипнет, затем перейдет на бумагу, результатом чего на отпечатке становится черный пиксель.

Типичный принтер такого рода имеет единственный лазерный диод, который последовательно и по одному наносит пиксели на печатаемую страницу – строка за строкой. Теперь пора отметить, что всякий раз, когда лазерный диод включается и выключается, то от кабеля, который его питает, происходит электромагнитный всплеск сигнала или «клик». И вот этот клик можно услышать с помощью радиоприемника, который настроен перехватчиком на множество таких частей радиоспектра, где обычно бывает тишина.

При частоте пикселей порядка нескольких мегагерц (в зависимости от разрешения картинки и скорости печати), стандартный AM радиоприемник, предназначенный для прослушивания обычных радиопередач, не способен к восприятию такой быстрой последовательности кликов. Однако хороший лабораторный приемник с диапазоном рабочих частот, охватывающих много мегагерц, данную задачу решает.

Полученную в результате волновую форму затем можно оцифровать и конвертировать в растровую картинку (о том, как именно это делается, в подробностях исследуют несколько статей и технических отчетов Маркуса Куна, а ссылка на рассказ об этой работе по-русски приведена в конце раздела).

Ну а теперь, предлагает Кун, давайте устроим моделирование-симуляцию того, как может выглядеть результат эфирного перехвата сигнала от лазерного принтера, который печатает на бумагу уже знакомую нам последовательность букв «EC NCN». В верхней части иллюстрации – собственно текст, который перехватывается, а внизу – то, что перехватчик увидит как результат своей работы:



По мере того, как лазерный луч сканирует избражение текста строка за строкой, каждый раз, когда он включается или выключается, то есть всякий раз при переходе между белой и темной частями картинки, оказывается возможным визуализировать сопутствующий широкополосный «клик» в эфире – как яркий пиксель.

Таким образом, любой вертикальный край буквы превращается в яркую вертикальную линию. В то же время горизонтальные края остаются невидимыми. Плюс к этому, вы получаете на картинке фоновый шум – от множества всевозможных других вещей, которые в это же время происходят в той же самой части радиоспектра.

Кун подчеркивает, что на приведенной выше картинке он просто смоделировал достаточно типичный TEMPEST-процесс. В реальной картинке, приводимой на слайде газетами, конечно же имеются некоторые отличия от модели Куна. Во-первых строки сканируемого изображения могут не быть строго горизонтальными, во-вторых, появляются отличия из-за других шрифтов печати или иной разрешающей способности. В-третьих, …

Впрочем, дальнейшие подробности из технической части анализа Куна именно здесь уже вряд ли важны и уместны (все интересующиеся могут найти оригинал этого исследования по адресу lightbluetouchpaper.org). И без того, наверное, уже всем ясно, что шпионская технология DROPMIRE представляет собой одну из разновидностей Tempest-атак.

Куда же более содержательным представляется переход к «аллегорической» компоненте топ-секретного слайда. Причем начать тут удобно с примечательного слова-названия DROPMIRE, которое в обычных и стандартных англо-русских словарях не встречается.

Более существенный (согласно лингвистическим правилам) второй корень MIRE означает «болото» или «грязь». А корень DROP, соответственно, «каплю» или «кидать» (брызгать). Иначе говоря, в вольно-ироническом переводе на русский эту технологию можно трактовать как нечто такое, что связано с копошениями шпионов в «брызгах грязи из болота»…

Подобная аллегория именно в данном случае представляется особо уместной по той причине, что шпионят тут за посольством Евросоюза. То есть, грубо говоря, за такой организацией-говорильней без армии и спецслужб, решения которой не имеют никакого обязательного характера для стран-участниц. Однако подслушивание закулисных обсуждений и разборок в этой говорильне позволяет шпионам выявлять узлы противоречий, претензий и склок между членами ЕС, а затем использовать это «грязное бельишко» в интересах США.

Понятно, конечно, что подобная нечистоплотная возня не имеет абсолютно никакого отношения ни к борьбе с международным терроризмом, ни к «делу мира во всем ми-

ре». Однако копошение в грязи – это один из давних и весьма важных компонентов в работе не только американских, но и практически всех прочих секретных спецслужб.

Именно через этот, в частности, канал обычно отыскиваются слабые места политиков и прочих «объектов разработки», за которые их можно зацепить, как следует прищемить, а затем через беспощадный шантаж манипулировать людьми, словно послушными марионетками.

Ведь никто же, наверное, не думает, что генеральный секретарь ООН без серьезных на то причин вдруг становится страшно озабочен не ситуацией в каком-нибудь там неблагополучном регионе планеты, а сугубо личным демаршем некоего молодого компьютерщика, сильно обидевшего разведслужбы США…

Дополнительные материалы:

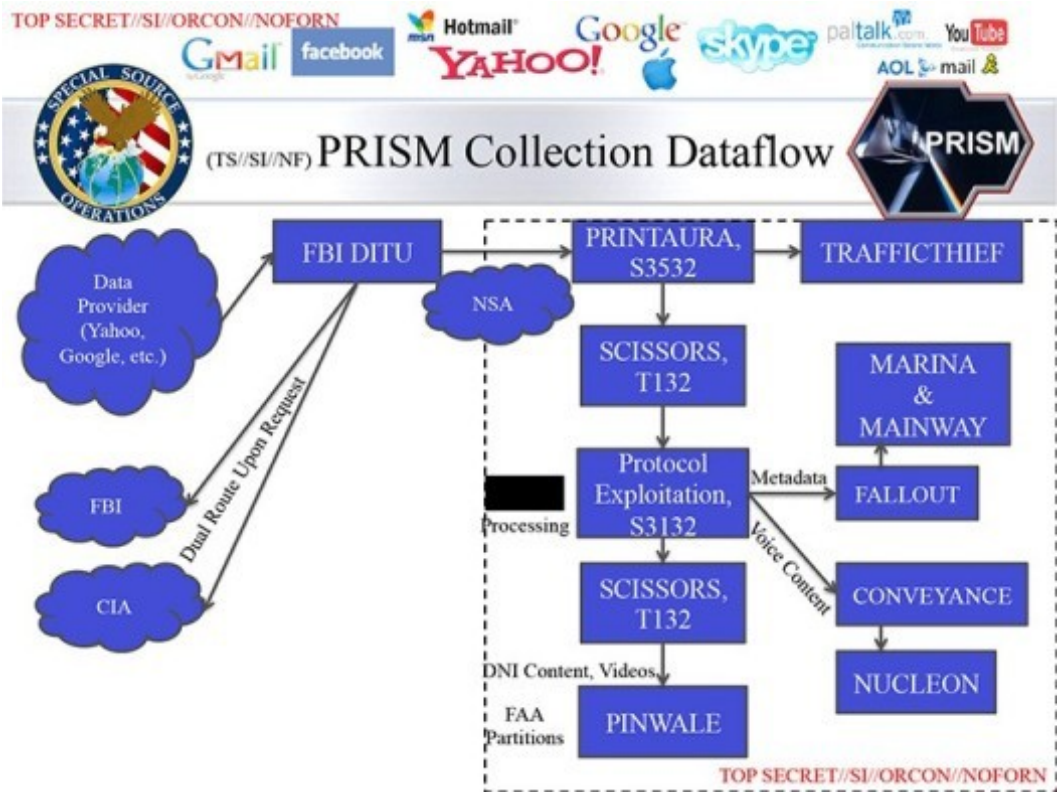
- Об истории рождения технологий Tempest в недрах спецслужб: «Секреты дальночувствия»;

- О темпест-исследованиях Маркуса Куна, позволяющих дистанционно снимать информацию с дисплеев компьютеров и экранов ТВ: «Волны компромата»;

- О специфических особенностях непотопляемого шефа ФБР Дж. Эдгара Гувера, снискавших ему титулы «сточной ямы, накапливающей грязь» и самого худшего политического деятеля за всю историю США: «Страницы жизни героя».

СЛАЙД # 2: «ОБЛАЧНОСТЬ И ТУМАН»

Второй топ-секретный слайд из коллекции Сноудена посвящен разведывательной программе АНБ под названием PRISM и с помощью наглядной блок-схемы отображает общие принципы, на основе которых функционирует эта система-пылесос для тотальной слежки за интернетом.



Дабы суть этой любопытной картинки стала понятнее, следует выделить ее главные элементы: [a] собственно базу данных PRISM (очерченный пунктиром бокс, занимающий основную часть слайда); [b] множество ведущих провайдеров данных (Google, Yahoo, Apple, Facebook, Microsoft, Skype и так далее), наполняющих базу АНБ коммуникациями своих пользователей и совокупно обозначенных облаком в левой верхней части изображения; [c] важный блок под названием FBI DITU, выступающий в качестве своего рода «прокладки» между облаком провайдеров и облаком АНБ (плюс шпионскими облаками ЦРУ и самого ФБР).

Название блока FBI DITU расшифровывается как «Data Intercept Technology Unit» или по-русски «Подразделение технологий перехвата данных в составе ФБР». Важнейшая особенность технических средств этого подразделения в том, что они непосредственно и на абсолютно законных основаниях встроены непосредственно в серверное оборудование всех провайдеров США.

Благодаря именно этому оборудованию DITU, как принято считать, ФБР США имеет возможности для беспрепятственного обеспечения правоохранительной деятельности в интернете – получая о провайдеров доступ к электронной почте, файлам хранения, чатам и всем прочим коммуникациям интернет-пользователей.

В отличие от ФБР, разведслужбы США формально не имеют у провайдеров столь мощной технической базы. Поэтому считается, что они получают от провайдеров данные перехвата лишь по индивидуальным запросам, санкционированным специальным судом FISC, который надзирает за законностью шпионажа на американской территории.

Но одно дело, как это выглядит на бумаге, и совсем другое, как реализовано на самом деле. Формально провайдеры вроде Google или Facebook сообщают публике, что да, они обязаны по закону сотрудничать с разведкой, но делают это в очень ограниченных масштабах, время от времени пересылая в АНБ запрошенную информацию по FTP, старомодному каналу перекачки данных. Но ни о какой такой широкомасштабной программе PRISM никто из провайдеров и не слышал-то никогда.

На самом же деле, как выясняется, база данных АНБ фактически напрямую подключена к серверам провайдеров, но только через каналы DITU ФБР. А это означает, как свидетельствуют опубликованные Сноуденом документы, что в АНБ имеют возможность не только тотально перекачивать себе все, что нужно, но и в реальном времени контролировать онлайновую жизнь своих «объектов» – сразу же получая сигналы об их заходе, скажем, в аккаунт электронной почты или об отправке очередного послания…

Отсюда понятно, наверное, что все эти ритуалы с «санкциями суда» и с пересылкой файлов через ftp служат, по сути, лишь в качестве прикрытия гигантской индустрии слежки. Или, образно выражаясь, в качестве тумана, скрывающего шпионские «облака», плотно накрывшие провайдеров.

И дабы отсюда плавно перейти к обобщенно-метафорической значимости рассмотренного слайда, полезно вспомнить впечатляющую историю с компрометацией сотовой связи в Греции.

Если кто не в курсе или забыл, то в период 2004-2005 годов крупнейшему в Греции провайдеру GSM-телефонии, Vodafone Greece, некие загадочные и по сию пору «неустановленные силы» внедрили в аппаратуру чрезвычайно хитрую шпионскую закладку.

Технически эта закладка для скрытного прослушивания абонентов была реализована на основе совершенно легального ПО, используемого в следственной работе правоохранительных органов и созданного самим поставщиком связного оборудования для Vodafone Greece, шведской фирмой Ericsson. Иначе говоря, техническая схема доступа тут была примерно та же, что и в истории с PRISM.

Главной же фишкой закладки было то, что оператор связи Vodafone Greece эту программу легального подслушивания для себя не приобретал и не устанавливал, а в сети компании шпионская подсистема работала как бы невидимо и неведомо для обслуги Vodafone. Но при этом на постоянной прослушке стояли телефоны премьер-министра Греции, его жены, ключевых фигур правительства, включая министров обороны и госбезопасности, а также многих других заметных лиц в государстве общим числом около 100.

Самым неприятным аспектом конкретно для Греции в этой истории оказалась невозможность признать правду. Обе ведущие партии страны, поочередно сменяющие друг друга у власти, в международных делах придерживаются откровенно проамериканской позиции. А независимые расследования истории с закладкой, как их ни тормозили и ни запутывали, все равно упорно указывали на США как на организатора выявленной прослушки. Хуже того, в прессе всплыли и четкие – вплоть до имен исполнителей – данные о том, что помогали устанавливать и настраивать эту закладку для американцев сотрудники греческой разведслужбы EYP.

Немало неприятностей доставил этот скандал и руководителям по уши замешанных в него компаний, английской Vodafone и шведской Ericsson. Во-первых, потому что «теневые» телефоны сети, через которые прослушка ретранслировалась за рубеж, сливали этот материал на номера, расположенные не только в США, но также в Британии и Швеции (прозрачно указывая на замешанность «в деле» национальных разведслужб этих государств).

Во-вторых, потому что Ericsson категорически отказалась предоставить для изучения исходные коды программ, обеспечивающих «легальный перехват». А в-третьих, непосредственно с выявлением закладки оказалась связана таинственная смерть топ-менеджера Vodafone Greece, Костаса Цаликидиса.

Хотя официально эту смерть расценили как самоубийство с неясными мотивами, в прессу Греции просочилась масса фактов, свидетельствующих о хладнокровном устранении спецслужбами невинного человека, оказавшегося неудобным и несговорчивым свидетелем преступления. Однако расследовать все эти факты власти Греции не пожелали.

Весьма похожий сценарий за последние годы разыгрывался во множестве стран, секретные спецслужбы которых тесно сотрудничают с США. Сначала в обществе разгорается громкий скандал в связи с разоблачением нелегальной прослушки, а затем неожиданно и без мотивов кончает самоубийством какая-нибудь ключевая фигура этого скандала.

Так было в Швейцарии с информатором полиции Кристианом Массоном, затеявшим слив в прессу материалов о нелегальном шпионаже в местных сетях GSM и вскоре якобы совершившим суицид путем прыжка с высокого моста. Так было в Италии с полицейским Адамо Бове, помогавшим прокуратуре выявить систему нелегальной прослушки, устроенной разведкой SISMI в сетях Italia Telecom. После этого разоблачения Бове – для наведения порядка у связистов – был назначен в Italia Telecom на пост главного менеджера по безопасности, однако вскоре и он фатально «прыгнул с моста» в безлюдном месте.

Другой типичный вариант «самоубийства» в такого рода сценариях – это повеситься в собственной квартире (если человек живет один). Так произошло в Греции с топ-

менеджером Vodafone Цаликидисом. И в точности так же оборвалась жизнь одного из руководителей разведслужбы Южной Кореи.

Замдиректора разведки Ли Су Ир, непосредственно отвечавший за перехват, был привлечен к ответственности в связи с аналогичным национальным скандалом о тайной прослушке спецслужбами политиков, журналистов и прочих сограждан. Но как только генерал начал давать показания о приказах своего начальства и о подробностях операции, он тут же стал еще одной «жертвой суицида».

Для того, чтобы иметь более адекватное представление об общей картине, на фоне которой происходит вся эта откровенная и абсолютно безнаказанная уголовщина, можно напомнить о так называемых «экстраординарных перемещениях». То есть о своеобразных формах борьбы ЦРУ США с международным терроризмом, в ходе которых людей, не нравившихся «борцам», просто похищали в той стране, где они проживали, и нелегально вывозили за границу на арендованном самолете.

Ну а дальше, как ныне хорошо известно, похищенных помещали либо в тайные тюрьмы местных спецслужб где-нибудь в Восточной Европе, либо в тюрьмы дружественных спецслужб в странах Ближнего Востока и азиатского региона, либо, наконец, в заморскую тюрьму США типа Гуантанамо. Где многих из этих людей подвергали жестоким пыткам, не говоря уже о беззаконном многолетнем заключении без суда и адвокатов.

Понятно, наверное, что все эти случаи «экстраординарных перемещений», исчислявшиеся по меньшей мере сотнями, с юридической точки зрения однозначно являются тяжкими преступлениями. Но реальность такова, что происходили эти преступления в глобальном масштабе и при сотрудничестве национальных разведслужб, на территории которых людей похищали, нелегально вывозили воздушным транспортом и тайно держали в тюрьмах.

Формулируя чуть иначе, применительно конкретно к Европе, в подобных преступлениях так или иначе оказались соучастниками спецслужбы чуть ли не всех европейских государств. А потому следует ли удивляться, сколь дружно и послушно все воздушное пространство Европы ныне было перекрыто для самолета президента Боливии – только лишь потому, что заокеанскому Большому Брату померещился на борту ненавистный Сноуден…

Дополнительные материалы:

- О системе глобального перехвата и о систематическом шпионаже США против своих союзников: «Служба гибкой морали»;

- О тотальной компрометации защиты информации в системе сотовой связи GSM: «Что показало вскрытие».

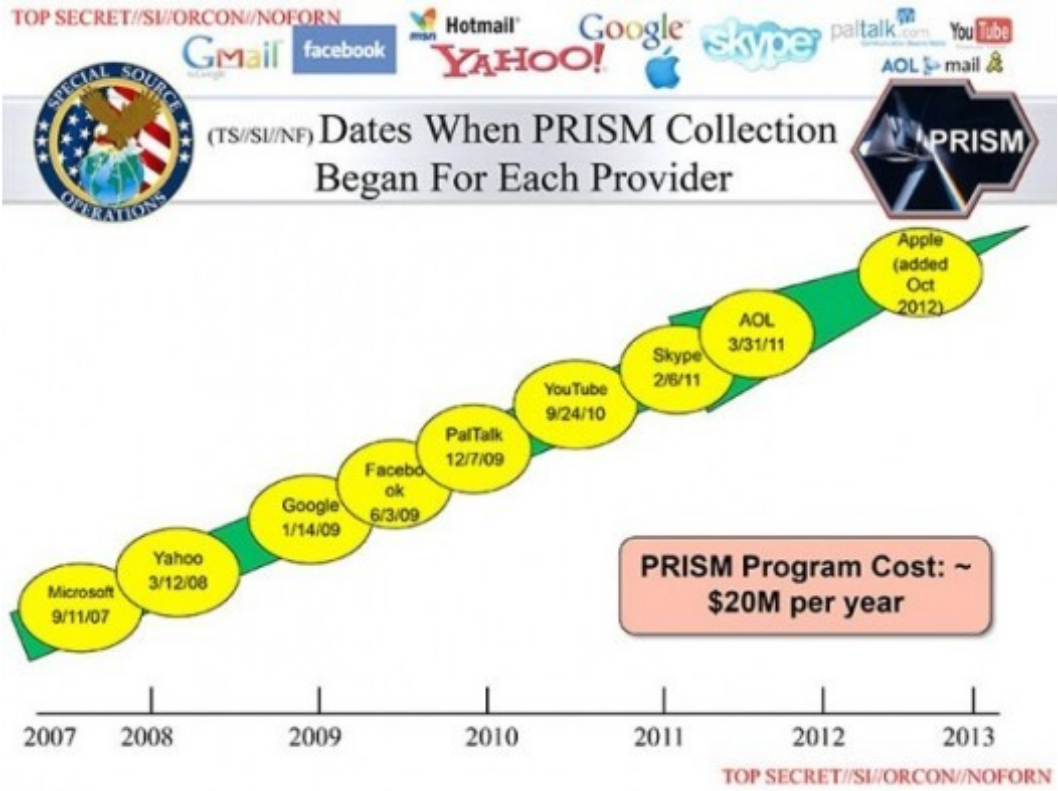
- О крупномасштабной шпионской операции США против властей Греции: «Вопросы на греческом»;

- О множестве «загадочных» смертей, окружающих истории с массовым нелегальным прослушиванием телефонов: «Серийные самоубийцы»; «Секс, ложь и шпионы»;

- Об истоках традиций спецслужб в области чистой уголовщины и физической ликвидации людей: «Правда жизни».

СЛАЙД # 3: «МАСШТАБЫ ЗАРАЖЕНИЯ»

Последний из рассматриваемых здесь топ-секретных слайдов хронологически оказался слитым в прессу одним из самых первых. И по содержанию своему, пожалуй, представляется наиболее понятным для постороннего человека. Ибо суть картинки вполне внятно передает уже название слайда: «Даты, когда сбор данных в базу PRISM был начат от каждого из провайдеров» (11 сентября 2007 – Microsoft, 14 января 2009 – Google, 6 февраля 2011 – Skype, и так далее).



Пространно комментировать здесь глубоко интимные для каждой из перечисленных компаний истории о том, как все они по очереди ложились под разведывательно-индустриальный комплекс США, здесь вряд ли будет уместно (для интересующихся, впрочем, в конце раздела помещены ссылки на исследования данной темы применительно к наиболее известным ИТ-корпорациям).

Можно сказать, что по этой картинке и без всяких слов уже понятно, что база данных АНБ под названием PRISM имеет в интернете все, что хочет (или, эквивалентно, всех, кого хочет)…

А потому от конкретного слайда можно сразу переходить к его метафорической составляющей. Которую в данном случае наилучшим, пожалуй, образом может представить известная среди специалистов по компьютерной безопасности книга под названием «Арсенал руткитов» (*«The Rootkit Arsenal» by Bill Blunden, Wordware Publishing, 2009*).

Точнее говоря, нас здесь будет интересовать не собственно эта толстенная, на 900 с лишним страниц монография о наиболее изощренных методах компрометации компьютерных систем, а ее самая последняя глава, которую издательство в печать не пропустило. По той причине, что в ней автор книги, Билл Бланден, признается не то чтобы в розыгрыше читателей, а скорее в завуалированном донесении до них через этот большой технический текст очень важной, но крайне неприятной правды. Причем правда эта отнюдь не о компьютерах…

В первых же строках этой главы (опубликованной в Сети как отдельное эссе) автор работы «официально свидетельствует, что его книга The Rootkit Arsenal – это аллегория, замаскированная под техническую компьютерную книгу». Ибо под всей этой теорией о компрометации драйверов устройств и под исходными кодами программ лежит куда более глубокое послание – об очень серьезном заражении всей политической системы государства.

Любой человек, занимавшийся исследованием вредоносных программ, пишет Бланден, ныне знает, что для руткитов оказывается совершенно реальным поставить под контроль и целиком весь компьютер, и те машины, что с ним связаны. То есть внешне невинное и сравнительно небольшое приложение (размером меньше 500 килобайт) оказывается способно тихо и незаметно скомпрометировать всю систему, масштаб которой измеряется порядками гигабайт и в миллионы раз больше, чем собственно вредоносная программа.

Скомпрометировав компьютер, злоумышленник может встроить руткит глубоко внутри инфраструктуры машины, а затем постепенно укреплять и усиливать эту основу, чтобы манипулировать всем множеством ключевых подсистем конструкции. Конечным же результатом этих тонких манипуляций становится то, что руткит обретает очень значительную степень скрытного влияния на работу всей системы.

Все, что требуется для такого рода компрометации системы – это правильно организованный доступ к ключевым функциям системы и детальное понимание того, как работают все эти вещи.

Отойдя чуть-чуть назад от деревьев, чтобы увидеть лес, поясняет Бланден, можно констатировать, что нечто очень похожее уже произошло с политической системой и структурой власти в Соединенных Штатах (а также, можно добавить здесь, в разной степени и с политической системой всех тех государств, которые оказались поражены той же самой заразой).

В своем эссе автор развернуто обосновывает, естественно, этот вывод с позиций эксперта по защите информации и просто наблюдательного человека. И если непредвзято смотреть на реальное состояние дел, с выводами Бландена трудно не согласиться.

Политическая система «демократии западного образца» действительно глубоко скомпрометирована, причем в самом своем корне («system is rooted», как выражаются на английской интерлингве компьютерщики).

Дополнительные материалы:

- Об индустриальном размахе разведки и о совместных делах шпионов с корпорациями Microsoft и Booz Allen Hamilton (на которую работал Эд Сноуден): «Большая ЖрАТВА»;

- О том сколь «давно и естественно» ведущие ИТ-корпорации сползают в мир секретных спецслужб: «Хитрости крипторемесла» (Microsoft); «Если спишь с собаками» (Google); «Все ходы записаны» и «Два кольца и два планшета» (Apple); «Игры в слова» (Skype).

В ЗАКЛЮЧЕНИЕ

Дабы не заканчивать материал на совсем уж унылой ноте, хотелось бы признать, что и политика, и бизнес, и даже работа спецслужб (как ни странно) в принципе могут быть гораздо честнее и чище, нежели то, как они выглядят сейчас.

Разведкой, например, вполне возможно заниматься как весьма благородным, рафинированным и изощренно-интеллектуальным делом. Но для этого надо учить шпионов не воровству секретов и способам ликвидации людей, а правильной работе с открытыми источниками информации. Особенно в нынешнюю эпоху информационного изобилия.

То, что политикой и бизнесом в принципе можно заниматься и по-честному, прекрасно известно, наверное, всем. Хотя с учетом нынешних раскладов в мире звучит это чрезвычайно наивно и старомодно. Слишком уж ситуация запущена.

Но начинать лечить все это дело, как ни крути, надо все-таки со спецслужб. Именно там сосредоточены самые глубокие и болезненные тайны, пускающие метастазы по всей системе.

И пока все эти тайны остаются скрытыми, не извлеченными на свет для всеобщего ознакомления, вылечить систему от поразившего ее руткита не получится.

Именно поэтому самыми важными для здоровья общества людьми становятся такие герои, как Эдвард Сноуден или Брэдли Мэннинг. Те, кто в одиночку решается бросить вызов всей этой насквозь прогнившей и очевидно преступной системе, массово раскрывая ее «страшные тайны». Именно оттого система их дико боится и яростно преследует с нарушением всех общепринятых правовых норм.

Но есть сильное ощущение, что людей таких будет становиться все больше и больше.

Иначе не выздороветь.

Дополнительные материалы:

- О том, что представляет собой чистая разведка и о роли открытых источников информации: «Модель OSINT»;

- О том – для примера – как выглядит OSINT-расследование истории с антракс-атакой, осуществленной против американского народа осенью 2001 года: «Следствие окончено, забудьте».

# # #

Сноуден как повод

(*Август 2014*)

Годовщина событий 9/11 и биография человека по имени Эдвард Сноуден дают специфический фон для картины того, что происходит ныне с миром и какова здесь роль инфотехнологий.

От Гавайев до Москвы

Августовский выпуск ИТ-журнала WIRED в качестве темы номера разместил на своих страницах большущий материал про Эдварда Сноудена (http://www.wired.com/2014/08/edward-snowden/).

В материале этом — без преувеличения — интересно все: и множество колоритных фактов из жизни героя; и писатель, приезжавший недавно в Москву, чтобы взять у Э.С. обстоятельное интервью; и снимки от знаменитого фотографа, придающие текстам весьма особенное ощущение «присутствия». Короче, работа мастерская.

Для тех, кто не владеет английским, все эти вещи наверняка должны появиться где-то на просторах Рунета и в русском переводе. Поэтому здесь будет не столько пересказ содержательного, спору нет, и на сегодня самого большого интервью Сноудена за весь период его жизни в России, сколько обзор некоторых важных или примечательных моментов вокруг данной истории.

Таких моментов, которые в исходном тексте либо вообще не присутствуют, либо упоминаются мимоходом. Но если смотреть на эти вещи под правильным углом, то можно извлечь из истории Э.С. много, много больше того, что там видно на первый взгляд.

В качестве элементарного — для затравки — примера, можно, скажем, упомянуть такой занятный факт «случайного совпадения».

Для приезжавшего к Сноудену в Москву писателя Джеймса Бэмфорда, автора главного текста в WIRED, его первый близкий контакт с организацией под названием Агентство национальной безопасности США произошел на Гавайских островах. (В годы вьетнамской войны Бэмфорд по призыву попал служить в ВМС, однако за сообразительные мозги в итоге оказался не столько военным моряком, сколько «разведчиком-аналитиком» на одной из гавайских баз АНБ, занимающихся радиоперехватом.)

И случилось так, что именно там же, на Гавайях, почти полвека спустя закончилась работа в АНБ для Эдварда Сноудена — когда в мае 2013 он с кучей флешек, залитых файлами с топ-секретным компроматом, сел в самолет, улетающий в Гонконг…

«Это делается просто»

Начать историю, однако, лучше всего издалека. С 1946 года, когда в Нюрнберге, Германия, прошел суд над людьми, ответственными за чудовищные преступления нацистов (а в США, по другому случайному совпадению, тогда же родился Джеймс Бэмфорд).

Помимо представителей правосудия, в рамках беспрецедентного судебного процесса практически полный доступ ко всем обвиняемым, недавней элите нацистской Германии, имел человек по имени Густав Гилберт — в качестве переводчика и доктора-психолога (а также как сотрудник американской разведки, что не афишировалось). Год спустя, в 1947, у Гилберта вышла книга «Нюрнбергский дневник» — с обстоятельными рассказами о том, с кем конкретно и о чем именно ему там доводилось беседовать (*Gilbert, G.M., «Nuremberg Diary». New York: Farrar, Straus and Company, 1947*).

На сегодняшний день самым знаменитым, пожалуй, фрагментом этой книги продолжает оставаться совсем небольшая цитата из откровений Германа Геринга, официального «преемника фюрера», рейхсмаршала третьего рейха и одного из ближайших соратников Гитлера по нацистской партии.

Именно этому деятелю удалось выразить в общедоступных понятиях очень простую, циничную и всегда работающую формулу того, каким образом политикам или «лидерам нации» в собственных целях удается столь успешно манипулировать народными массами. Вплоть до вовлечения наций в ужасные войны, приносящие лишь смерть, горе и разруху для всех нормальных людей.

Цитируя Геринга дословно:

> *Естественно, обычные люди не хотят войны. Ни в России, ни в Англии, ни в Америке, ни в Германии. Это понятно. Но ведь в конечном-то счете*

политику определяют лидеры страны, а для них это всегда простое дело — увлечь за собой массы людей. Будь это демократия или фашистская диктатура, парламент или диктатура коммунистов.

Есть у народа голос или нет, неважно, — массы всегда можно склонить на поддержку лидеров. Это просто. Все, что для этого надо, это сказать людям, что они атакованы. Попутно прищучив за отсутствие патриотизма пацифистов, подвергающих страну еще большей опасности…

Казалось бы, ну куда доходчивее — вот же он, извечный рецепт манипуляций. Прочтите, люди, и поймите, наконец, как вас все время обманывают ваши лидеры. Ну сколько можно быть послушным стадом, которое постоянно то склоняют на ненависть к «не таким, как мы», то хладнокровно и без всякой жалости отправляют на убой…

Так нет ведь, рецепт Геринга мало того что постоянно применяется, но и безотказно продолжает работать по сию пору — в любой точке планеты.

Когда, скажем, в конце 1990-х Джеймс Бэмфорд (уже знаменитый в ту пору журналист, писатель и исследователь разведслужб) работал над Body of Secrets, своей очередной книгой о разведке США, то в руки ему попал поразительный документ. Среди множества бумаг, недавно рассекреченных из закрытых госархивов администрацией Клинтона, он наткнулся на материалы об операции Northwoods, прежде совершенно неизвестной историкам.

В этом документе начала 1960-х годов содержался план действий, разработанный спецслужбами и принятый высшим генералитетом США. В результате этих действий американское население должно было массово одобрить военное вторжение на Кубу с последующей долгосрочной оккупацией острова. Ради этой цели в рамках Northwoods планировалось осуществить взрывы и затопления кораблей, угоны самолетов и несколько кровавых террористических актов в городах США — представив происходящее как дело рук кубинских революционеров, атакующих Америку по указанию Фиделя Кастро.

Единственной, по сути, причиной того, что уже утвержденный военными план не привели в действие, стало категорическое несогласие президента Джона Кеннеди, целиком отвергнувшего эту операцию как неприемлемую…

По случайному, ясное дело, совпадению книга Бэмфорда Body of Secrets, рассказывающая среди прочего и про операцию «Нортвудс», появилась в продаже весной 2001, когда к власти только-только пришел Джордж Буш-сын. А уже в сентябре 2001 Америку и мир потрясли известно какие ужасные террористические атаки, в глазах обывателей оправдавшие все последовавшее — и вторжение в Афганистан, и войну в Ираке, и все остальное в рамках «борьбы с терроризмом» (детали об этой операции см. в текстах «9/11 — десять лет спустя», «Правда и ложь»).

Примечательная череда случайностей

Теперь пора, наконец, обратиться к фактам биографии главного героя.

По случайному, конечно же, стечению обстоятельств, Эдвард Сноуден был зачат его родителями в 1982 году — в год выхода первой и самой знаменитой книги Джеймса Бэмфорда об АНБ, «Дворец Загадок» (*The Puzzle Palace by James Bamford*, подробности об истории рождения этой выдающейся исследовательской работы см. в тексте «Анатомия бывает разной»).

По другому случайному совпадению, Эдвард Сноуден родился в семье, проживающей в штате Мэриленд — недалеко от места, где находится военная база Форт-Мид, известная как штаб-квартира АНБ США. А в семье Сноуденов, где работой и для отца, и для матери была служба в ведомствах федерального правительства, как бы само собой всегда подразумевалось, что по этому же пути со временем пойдут и их дети.

Наконец, благодаря еще одному совершенно случайному совпадению, первым же местом работы Сноудена — еще до окончания учебы — оказалась небольшая ИТ-фирма, офис которой был в здании, располагавшемся на территории под названием Форт-Мид… Утро же трагического дня, 11 сентября 2001, Сноуден запомнил так: «Я вел машину по пути на работу и по радио услышал о первом ударе авиалайнера в небоскреб»…

Как и для многих других патриотично настроенных американцев, атаки 9/11 и тут же развернутая в национальных СМИ пропаганда оказали на Сноудена сильнейшее воздействие. Поэтому весной 2004, когда боевые действия в Ираке вновь обострились, юноша записался добровольцем в войска спецназа США. Сейчас об этом периоде наивности он рассказывает так:

> *«Для разъяснений, исходивших от правительства — по сути пропаганды — я был совершенно открыт, когда речь шла о вещах типа Ирака, о его закупках алюминиевых труб для ракет и о его спорах антракса. У меня была очень сильная вера в то, что правительство не стало бы нам врать, что у наших властей благородные намерения, и что война в Ираке будет именно такой, как о ней нам рассказывают. То есть целевым и ограниченным усилием, направленным на освобождение угнетенных. И я был настроен исполнить свою часть этой благородной задачи».*

Благодаря хорошим результатам Сноудена на приемных испытаниях, его без проблем зачислили в войска. Однако требования к физической подготовке спецназовцев оказались куда более сложным вызовом. Вскоре, на одной из тренировок Сноуден получил переломы сразу обеих ног. И спустя несколько месяцев, когда кости срослись, его уволили с военной службы по состоянию здоровья.

Наверное, и такой житейский расклад можно считать чистой случайной чередой событий. Но можно, однако, начать усматривать здесь и вполне отчетливую закономерность — линию судьбы, если угодно, направленной на миссию…

Банальность зла, или ложь как работа

Глубинная суть того, что совершил в итоге Эдвард Сноуден, заключается в совершенно уникальном стечении внешних или государственных обстоятельств, наложившихся на редкое сочетание личных качеств этого человека.

Реальность жизни и работы спецслужб США в начале 2000-х годов оказалось такова, что (а) огромное количество задач разведки оказалось переложено на частные коммерческие структуры и, как следствие, (б) сотрудники этих бизнес-структур смогли получать быстрый допуск к очень серьезным государственным тайнам.

Почему это было сделано, догадаться, наверное, несложно. Под задачи национальной безопасности — особенно, когда «нация атакована» — легче всего выбивать астрономические суммы из бюджета. Ну а осваивать или пилить все эти огромные бабки гораздо сподручнее, ясное дело, если подключить в дело шустрые коммерческие структуры (см. тексты «Бизнес в помощь», «Чтоб Кафку сделать былью»).

Принимая же в учет масштабы финансирования и размах амбиций разведслужб самой мощной державы на планете, столь же несложно постичь, насколько серьезная мина замедленного действия была при этом заложена под сами основы тайной работы секретных органов. Потому что в основе шпионажа — так уж сложилось по давней традиции — лежат три главные вещи: ложь, обман и неправда. Или вранье, короче говоря.

Но только напрямую и как есть эта истина никогда не произносится, а облекается во множество благородно звучащих формул и вдохновляющих оберток. Ну а молодые сотрудники, начинающие карьеру в спецслужбах, постигают нутряную лживую суть их работы очень и очень небыстро, по мере подъема по служебной лестнице.

Эдвард Сноуден, попав на эту глубоко секретную кухню из коммерческих структур, уподобил происходящее тому, что делается с лягушкой, которую варят заживо без всякого ее сопротивления. Лягушка спокойно сидит в холодной воде кастрюли, поставленной на огонь, не замечая, что вода постепенно разогревается. И продолжает сидеть до тех пор, пока кипяток ее не убьет.

Очень похожим образом ложь выжигает честь и совесть кадровых сотрудников спецслужб. Цитируя интервью Эда Сноудена:

> *«Вас ставят в ситуацию, где зла совсем немножко, лишь чуть-чуть нарушаются установленные правила, приходится быть нечестным самую*

малость, кого-то там слегка обмануть, немного поступиться интересами общества — и вот вы уже тоже согласны это принять, вы можете найти оправдание для этого. Но если вы делаете так раз за разом, то этим порождается скользкий для сползания склон, который со временем становится все круче и круче. И к тому моменту, когда подобные вещи продолжаются 15 лет, 20 лет, и вы все это видели не раз, то вас уже вообще ничего из творящегося не шокирует»…

Сноуден же приобщился к великой лжи намного быстрее. Поэтому за несколько лет своей успешной и весьма прибыльной работы (коммерческое сопровождение инфосистем, обеспечивающих суперсекретную деятельность шпионов) он сумел сохранить не только ум, но также и честь, и совесть. А переломный момент в этой насквозь пропитанной обманом работе лично для него наступил 13 марта 2013, когда он решил «выпрыгнуть из кастрюли».

В тот день, сидя за своим рабочим столом в гавайском подземном бункере, Сноуден прочел в новостях очередную порцию бесстыжей брехни об их нелегкой службе во славу отчизны. На этот раз это был отчет о выступлении директора национальной разведки США Джеймса Клаппера в Конгрессе США, где глава всех шпионов страны «искренне заверил» парламент и нацию, что АНБ не занимается систематическим сбором информации о миллионах американцев.

Когда статьи о выступлении Клаппера появились в газетах, Сноуден тут же — и в который раз — завел разговоры с коллегами, поражаясь, как люди могут верить во все это лживое дерьмо… Ну а поскольку тема такая — про обман вокруг реальных масштабов шпионажа АНБ — в их кругу возникала уже неоднократно, Сноуден даже и не удивился особо тому, что в этой специфической среде не было по сути вообще никакой реакции на слова их начальника в Сенате.

Именно об этой ситуации в государстве, сползающем в тоталитаризм, написала в свое время философ Ханна Арендт, анализировавшая повседневную работу бюрократии в нацистской Германии и назвавшая такие вещи «банальностью зла» (Eichmann in Jerusalem: A Report on the Banality of Evil, by Hannah Arendt, 1963). Сноуден увидел очень четкие параллели между нынешней ситуацией и знаменитой работой Арендт полувековой давности:

«Это было больше чем просто принятие заведомой лжи… Происходящие вещи уже воспринимаются как совершенно нормальные. Именно в этом и заключается главная проблема, именно в этом суть того, что было с ложью Клаппера в Сенате. Он рассматривал обман американского народа — когда он это делал — просто как свою работу, как нечто совершенно обычное и естественное. И он был прав, полагая, что никто его за это не накажет. Потому что впоследствии, когда ему пришлось признать, что да, он лгал находясь под присягой, то никто не дал ему за это дело ни по

рукам, ни по шапке. Это говорит очень многое обо всей данной системе и очень многое о наших лидерах»…

Что нам со всем этим делать?

Для всякого человека, мало-мальски знакомого со спецификой работы национальных спецслужб в разных странах, ничуть не секрет, что примерно по той же схеме работают и все прочие разведки. Только «дым пожиже, да труба пониже», как говорится.

Иными словами, практически любая спецслужба в своих подходах к решению поставленных задач так или иначе тяготеет к тоталитарным методам и ко лжи о реальной ситуации. Просто потому, что так им работать и удобнее, и проще. Соответственно, если бы в других странах спецслужбам давали столько денег, сколько дают в США, то масштаб тотальной слежки и обмана был бы наверняка ничуть не меньше. А может и поболее того.

По этой причине, когда мировая пресса в очередной раз начинает сегодня обсуждать очередные файлы с компроматом из гигантского архива, переданного Сноуденом журналистам, имеет смысл все время помнить одну незамысловатую вещь. В действительности тут обсуждаются не столько тайные операции АНБ и их ближайших союзников, сколько вообще технический уровень и подходы современных спецслужб, получивших принципиальную возможность для тотальной слежки за всеми. Слежки постоянной и непрерывной.

И ныне, получив уже достаточно внятное представление, что конструкция обоснований для массового шпионажа за народом в качестве своего фундамента имеет только ложь и ничего иного, кроме лжи, всякий человек, способный соображать, должен, по идее, понимать и то, что так быть не должно. Причем возможности для изменения ситуации определенно имеются.

Сам Сноуден, к примеру, видит адекватный ответ общества в массовом применении надежного шифрования:

«У нас имеются средства и у нас имеются технологии для того, чтобы положить конец массовой слежке — вообще без каких-либо законодательных шагов со стороны государства, и без ощутимых перемен в политике. Мы сами, на массовом уровне можем нести перемены — вроде того, чтобы сделать шифрование общепринятым стандартом, когда все коммуникации зашифрованы по умолчанию. Таким путем мы способны положить конец массовой слежке — не только в США, но и по всему миру».

Ну а до тех пор, пока такой момент всеобщего и сильного шифрования не наступил, говорит Сноуден, обнародование компромата о тайных действиях спецслужб должно

и будет продолжаться. Причем ныне для аналитиков, штудирующих подобные «сливы», уже вполне очевидно, что серьезные топ-секретные документы под широкой «крышей Сноудена» явно стали передавать журналистам и другие источники в спецслужбах.

И есть ощущение, что количество таких людей будет расти. Причем не только в США. Потому что во всех спецслужбах, ясное дело, должны находиться честные сотрудники с общечеловеческими понятиями о правде и лжи, о том, что правильно, а что нет.

Можно сказать, что пример Сноудена — это еще один очень сильный антидот для оздоровления современного общества, пораженного опаснейшим ядом тотальной слежки.

И хотя сегодня нередко можно услышать голоса радикалов, страшно раздраженных, что владеющие сноуденовым компроматом журналисты выдают публике «в день по чайной ложке», а не вываливают в интернет все и сразу, на суть и решение проблемы это уже вряд ли сможет существенно повлиять.

Эдвард Сноуден, в частности, считает, что информация, содержащаяся в любых других сливах из «его» архива, почти наверняка никакой особой роли уже не сыграет:

> *«Вопрос для нас не в том, что за новая история появится следующей. Вопрос в том, что мы будем со всем этим делать?»*

# # #

Дополнительное чтение

Более содержательный контекст для файлов от Эдварда Сноудена: «**Всего три слайда**», «**Бизнес в помощь**».

Об абсолютно достоверных, но редко обсуждаемых фактах вокруг самых знаменитых терактов: «**9/11 — десять лет спустя**», «**Правда и ложь**».

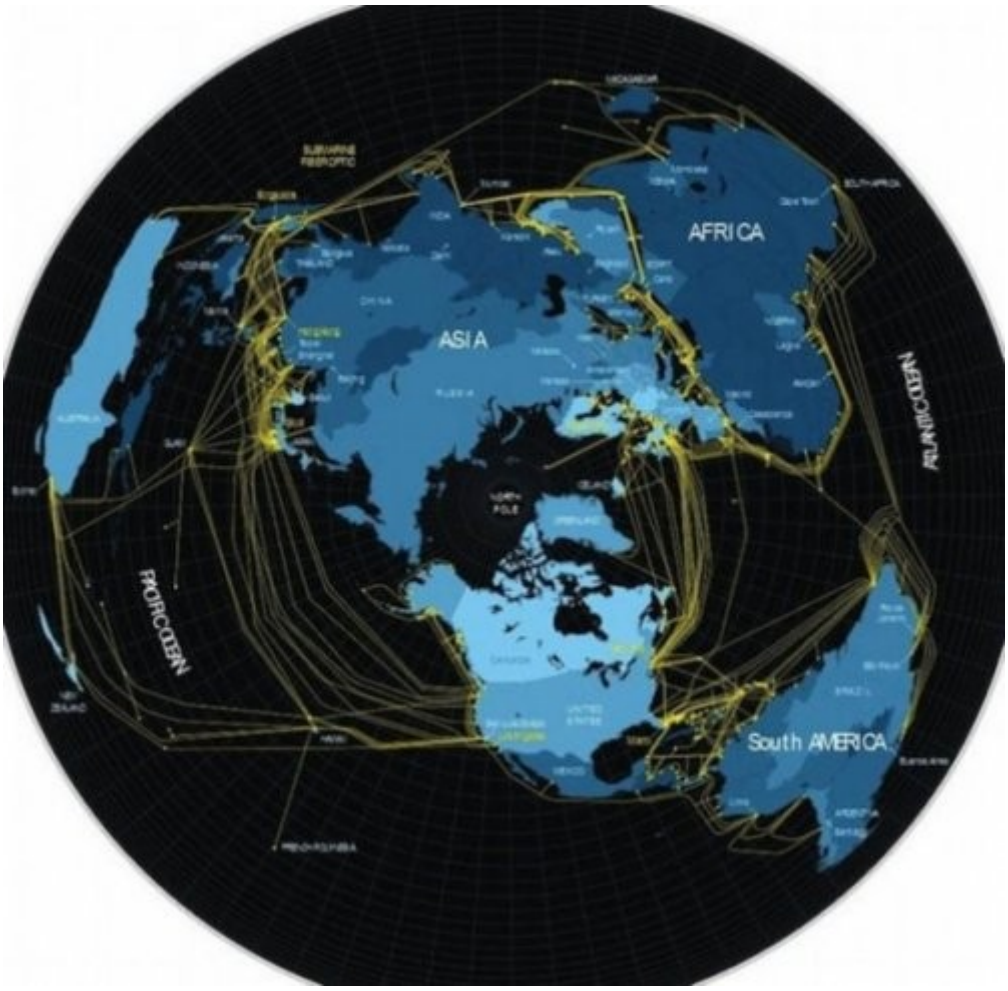
Про тайны бизнеса шпионов вокруг тотальной слежки: «**Большая ЖрАТВА**», «**Чтоб Кафку сделать былью**».

Про исследования писателя и журналиста Джеймса Бэмфорда: «**Анатомия бывает разной**».

Бизнес в помощь

(*Сентябрь 2013*)

Шум прессы вокруг гранд-слива компромата от Эдварда Сноудена все время норовят опустить до мелочей и пустяков. То есть «понизить уровень дискуссии», выражаясь профессиональными терминами. Именно поэтому здесь хотелось бы уровень повысить. И поговорить о вещах действительно серьезных.



К мелочам и пустякам относятся не только концентрация на личности Сноудена или на проколах людей, занимающихся анализом и публикацией полученных от диссидента тысяч файлов.

Столь же несущественной, строго говоря, является и другая тема, обсуждаемая бурно и абсолютно бесцельно – о том, что «шпионы шпионят». Поскольку шпионят де чересчур много, без всякого стыда, совести и уважения законов.

А чем еще, интересно, им следует заниматься, если работа у них такая? Причем именно за эту бесстыжую шпионскую работу государство совершенно официально и платит своим разведкам деньги налогоплательщиков…

Но вот очень важный и близко связанный с этим вопрос – о больших деньгах, крутящихся вокруг шпионажа и национальной безопасности, а также о том, кто и как эти деньги «пилит» – все время как-то в поле дискуссий не попадает. А если и попадает, то быстро забалтывается и переводится в общее русло типа «борьбы с терроризмом».

Но вопрос на самом деле очень интересный.

И проиллюстрировать это помогут следующие три цитаты.

В середине августа 2013, в самый разгар скандала вокруг разоблачений от Сноудена, развернутый комментарий к ситуации дал генерал Майкл Хейден (Michael Hayden), директор АНБ США с 1999 по 2005, а затем директор ЦРУ в последние годы президентской администрации Джорджа Буша-сына.

То есть человек, более чем компетентный в делах национальной разведки, комментируя только что данные обещания президента Обамы – провести реформу в «нехороших» методах шпионажа АНБ – выдал такую витиеватую конструкцию:

> *«Президент пытается ныне предпринять некоторые шаги, дабы американцам было более комфортно жить с тем, чем мы занимаемся. Но осуществить подобное будет сложно, поскольку, честно говоря, делать шаги к тому, чтобы американцам жилось более комфортно – это на самом деле делать американцев менее защищенными»*…

Для справки, ныне отставной многозвездный генерал Майкл Хейден является одним из главных руководителей консалтинговой фирмы Chertoff Group, специализирующейся на проблемах национальной безопасности и заказах федерального правительства.

Еще одна, уже более конкретная цитата в тему – от другого многозвездного адмирала, Майка Макконнела (Mike McConnell), в недавнем прошлом директора национальной разведки, а еще ранее директора АНБ США. Аналогично Хейдену, Макконнел в своих публичных выступлениях тоже всегда нагнетает в обществе страхи, напрямую связывая утечки от Сноудена с возрастанием террористических угроз для нации.

Выступая в июле 2013 на конференции бизнес-подрядчиков федерального правительства, Макконнел подчеркнул, что разглашенные Сноуденом документы уже нанесли «необратимый ущерб» возможностям США в деле предотвращения терроризма:

> *«Все это ослабляет наши способности понимать ядерные инициативы Северной Кореи, понимать то, что происходит в Сирии, то, что возможно происходит с Талибаном в Афганистане»*…

Опять-таки для справки, ныне Майк Макконнел является вице-президентом одной из крупнейших в мире консалтинговых фирм Booz Allen Hamiltion (BAH), имеющей многомиллиардные и суперсекретные контракты с правительством США в области

обеспечения безопасности (подробности о шпионском бизнесе ВАН можно найти в материале «Большая ЖрАТВА»).

Небезынтересно, наверное, отметить, что системный администратор Эдвард Сноуден непосредственно до своего ухода в диссиденты тоже был сотрудником ВАН, и в этом качестве имел доступ к документам настолько высокого уровня секретности, какого не имеют даже высокие чины разведслужбы АНБ.

Еще более интересно, быть может, то, что на пост директора национальной разведки в администрации Буша-сына адмирал Майк Макконнел пришел из бизнеса – из кресла вице-президента Booz Allen Hamiltion. А послужив несколько лет родине на ответственной и важной государственной должности, затем вновь вернулся на давно пригретое место руководителя ВАН.

Наконец – третья цитата в тему – дабы всем уже абсолютно отчетливо стало ясно, насколько важны страшные угрозы терроризма для финансового благополучия определенного типа бизнес-структур, полезно привести высказывание генерала военно-воздушных сил США Джона Джампера (John P. Jumper). По его личным экспертным оценкам, террористическая угроза – это:

> *«Это более великая опасность чем нацизм, это страшнее чем коммунизм. Та угроза, что нависла теперь над нами от террористических фанатиков – она самая опасная среди всех. Потому что для этих людей жизнь не значит ничего»…*

Из общего контекста уже несложно, наверное, догадаться, что Джон Джампер – это далеко не обычный американский генерал, а весьма большой человек специфического окологосударственного бизнеса. В настоящее время Джампер является исполнительным директором корпорации SAIC – еще одной очень крупной хайтек-корпорации, имеющей с разведслужбами США и Пентагоном тысячи контрактов на многие миллиарды долларов (подробнее о специфической истории и бизнес-модели этой фирмы см. материал «Закрытое акционерное общество власти»).

Иначе говоря, все перечисленные люди энергично участвуют в очень популярной (и весьма прибыльной, ясное дело) игре под названием «вращающаяся дверь». Когда попавшие в высшую элиту персонажи то и дело пересаживаются с важных государственных постов в кресла руководителей частного бизнеса, а затем – при удобном случае – ненадолго возвращаются обратно. На госпостах они обеспечивают жирными контрактами «свои» бизнес-структуры, а с капитанских мостиков бизнеса сытно подкармливают «своих» людей в правительстве.

Надо ли говорить, что все подобные штуки, от которых за милю разит коррупцией, предпочтительнее всего обделывать в обстановке секретности. А что может быть делом более секретным, чем защита национальной безопасности?

В общем, в США как-то само собой все сложилось так, что «защита страны от постоянно нависающих страшных (и мифических, естественно) угроз» стала у них чем-то вроде нашей «нефтегазовой трубы». То есть источником самых изобильных в государственной казне денежных потоков, к которым жадно присосались, увы, такие организмы, насытить которые невозможно в принципе…

При этом все они заняты в высшей степени благородными делами – не только укреплением национальной безопасности и спасением мира от угроз терроризма, но попутно также борьбой с иностранной коррупцией и взяточничеством в международной торговле (немало пикантных подробностей на данный счет можно найти в материале «Служба гибкой морали»).

Иностранная помощь

Неисчерпаемая, но почему-то очень скупо освещаемая в прессе тема о занятных отношениях между спецслужбами США и миром бизнеса особо интересна в аспектах своего «международного сотрудничества», назовем это так.

Потому что одно дело, когда американские ИТ-компании типа Google или Microsoft помогают бороться с врагами отчизны родным спецслужбам своей страны, и совершенно другое дело, когда национальные фирмы других государств – скажем операторы связи в Европе или Азии – помогают американской разведке шпионить за собственными согражданами…

В последнюю декаду августа 2013 уважаемая газета Wall Street Journal вышла с большим материалом-расследованием, содержащим всякие новые подробности о разведывательных программах АНБ США. В отличие от основной массы последних разоблачений, так или иначе опирающихся на файлы Сноудена, журналисты (точнее журналистки) WSJ выстроили свой материал на основе личных свидетельств сотрудников АНБ. Все эти люди по ясным причинам делились информацией анонимно, однако рассказали немало действительно интересных вещей.

Например, именно в этой статье было раскрыто, что у АНБ ныне имеются возможности получать прямой доступ примерно к 75% всего интернет-трафика, идущего через оптоволоконные кабели на территории США. Эта гигантская цифра, ясное дело, была поспешно и очень решительно опровергнута официальными представителями АНБ. Однако факт опубликован, а думающие люди уже сами решат, кому тут больше верить – сотрудникам спецслужбы, пытающимся хоть как-то очистить совесть от соучастия в беспределе домашнего шпионажа, или же пиар-подразделению шпионской «корпорации».

Вполне естественно, что информация о 75% привлекла основную долю внимания американских читателей и прочих СМИ. Но при этом (или даже из-за этого) подавляющее большинство тех, кто обсуждал материал, очевидно проглядело в той же самой статье,

но чуть дальше, другой очень важный абзац (упоминаемый в СМИ чрезвычайно скупо), где говорится о куда более примечательном методе, массово применяемом АНБ для сбора информации:

> *«Агентство национальной безопасности США начало заниматься перехватом интернета задолго до 2001 года, свидетельствуют бывшие сотрудники разведки. Проводимые секретным подразделением АНБ Special Services Office (Отдел Особых Сервисов), такого типа программы перехвата были поначалу разработаны для доступа к коммуникациям с зарубежных постов – через договоренности с иностранными интернет-провайдерами. Как рассказывает бывший сотрудник спецслужбы, АНБ и сегодня все еще имеет такого рода соглашения во множестве стран, в частности, на Ближнем Востоке и в Европе»…*

Дабы стало более понятно, до сколь гигантских масштабов разрослось ныне тайное сотрудничество национальных и международных провайдеров связи с разведслужбами США и их ближайшими партнерами, имеет смысл скомпилировать информацию, опубликованную на сегодняшний день в разных источниках.

Наиболее надежная информация на данный счет появлялась в файлах Сноудена – относительно семи британских и американских (транснациональных) интернет-компаний, которые тесно сотрудничают с британским аналогом АНБ, спецслужбой GCHQ или Штаб-квартира правительственной связи. (В силу географического расположения Великобритания является чрезвычайно важным узлом для многих оптоволоконных сетей, объединяющих континенты.)

Интересно, что английская газета The Guardian, часто выступающая как главный «рупор» для разоблачений Сноудена, не решилась опубликовать названия этих фирм, сочтя информацию чересчур взрывоопасной. Однако два германских издания, куда более мелких по масштабу и фактически региональных, газета Süddeutsche Zeitung и телеканал NDR, опубликовали компромат «как есть».

То есть, получив от одного из представителей Сноудена доступ к топ-секретным документам GCHQ за 2009 год, эти издания рассказали и о конкретных провайдерах связи, обслуживающих англо-американскую разведку, и о присвоенных им шпионами кодовых наименованиях:

– Verizon Business (DACRON)
– British Telecom (REMEDY)
– Vodafone Cable (GERONTIC)
– Global Crossing (PINNAGE)
– Level 3 (LITTLE)
– Viatel (VITREOUS)
– Interoute (STREETCAR)

Из внутренних документов спецслужбы следует, что GCHQ имеет секретные соглашения с этими семью компаниями, которые именуются в одном из документов как «партнеры по перехвату» и в соответствии с договоренностями предоставляют разведке доступ к своим сетям подводных кабелей.

Причем делается это отнюдь не безвозмездно. Данные компании получают соответствующую оплату за свою техническую помощь и снабжение необходимой логистикой. Более того, некоторые из них даже разработали свое собственное оборудование спецдоступа – для более эффективного сбора интернет-данных.

В GCHQ эти работы проводятся под названием «Освоение интернета» (Mastering the Internet) и в качестве компонента входят в более широкую программу TEMPORA.

В разведслужбах всегда прекрасно понимали, что конкретные названия участвующих в этой затее компаний являются информацией, чрезвычайно чувствительной к разглашению. Во внутренних документах разведки об этом говорится как об ECI или «Exceptionally Controlled Information» (исключительно ограниченной информации) – дабы реальные названия фирм повсюду заменялись кодовыми словами. Ибо раскрытие названий способно привести не только к «политическому скандалу на высоком уровне», но также может оказаться крайне разрушительным в смысле доверия клиентов к этим компаниям.

Коль скоро теперь столь беспокоившие шпионов и их партнеров утечки реально начали происходить, замаравшимся компаниям связи – хочешь не хочешь – приходится как-то реагировать. Естественно, первым делом хочется все-все горячо отрицать.

Или сделать так, как фирмы Vodafone и Verizon, которые особо вообще не мудрили и прибегли в точности к той же схеме, по которой свое тесное партнерство со шпионами «опровергают» интернет-компании США, засветившиеся участием в программе PRISM (см. материал «Всего три слайда»). То есть было заявлено, что они подчиняются законам всех тех стран, в которых работают со своими кабелями. И что они не раскрывают никаких данных своих клиентов ни в какой юрисдикции, пока не получат от властей официальный законный запрос на такую информацию.

Главный трюк этого «юридически честного» ответа в том, что от фирмы-провайдера связи по условиям соглашения требуется, в первую очередь, установить правильное оборудование для «законного перехвата» – скрытным и безопасным образом. А что уж там дальше делается с этим оборудованием, ведомо только спецслужбам. Которые иногда прикрывают свой «пылесос» бумажками официальных запросов – дабы было что предъявить при проверках законности.

Нельзя, однако, сказать, что реальные масштабы перехвата от оптоволоконных кабелей являются особой тайной. Еще в 2003 году техник компании AT&T Марк Кляйн (Mark Klein) обнаружил «секретную комнату АНБ» в одном из калифорнийских узлов

своей компании-оператора и рассказал о тех совершенно фантастических (для посторонних) возможностях интернет-шпионажа, что предоставляло работавшее там оборудование Narus (ныне подразделение Boeing).

Несколько позднее эту информацию компетентно подтвердил Билл Бинни (Bill Binney), высокопоставленный сотрудник АНБ, покинувший разведслужбу в знак протеста против массового и беззаконного наращивания шпионажа в отношении сограждан. По свидетельству Бинни, уже тогда одно устройство Narus, подключенное к оптоволоконной линии, могло каждую секунду брать от кабеля 1,2 миллиона писем электронной почты длиной по тысяче знаков. Или иначе, 100 миллиардов электронных писем в день. И техника эта за прошедшие годы в своем развитии отнюдь не стояла на месте…

Возвращаясь к нынешней компрометации семи оптоволоконных компаний, управляющих гигантской долей от всех широкополосных подводных магистралей на основе оптоволокнных кабелей, можно без преувеличения говорить, что все их хозяйство в совокупности образует тот самый скелет, что лежит в основе общепланетной интернет-архитектуры.

Пока что в точности неизвестно, как много узлов в сетях этих провайдеров оборудованы техникой Narus, Verint или им подобными средствами перехвата от оптоволоконных магистралей. Но из документов разведки, опубликованных газетой Guardian следует, что в 2012 году GCHQ брала информацию от более чем 200 оптоволоконных кабелей и была способна обрабатывать данные по крайней мере от 46 из них одновременно. Полное содержимое перехваченных коммуникаций обычно сохраняется для анализа и фильтрации в течение 3 дней, а более компактные метаданные хранятся до 30 суток…

Все известные прежде свидетельства и документы о специфике работы АНБ позволяют уверенно говорить, что аналогичные «соглашения о сотрудничестве» с национальными операторами связи имеются у разведок Канады, Австралии и Новой Зеландии. Ибо службы электронной разведки этих государств имеют очень тесные взаимоотношения по обмену информацией с АНБ и GCHQ в соответствии с договором о разведках UKUSA от 1946 года. Во всем, что касается разведки средств связи, эти страны считаются ближайшими союзниками США вообще и АНБ в частности.

Ступенькой ниже имеется группа других государств, общим числом около 30, именуемых в документах АНБ «партнерами третьей стороны». Пока что из файлов Сноудена достоверно известно, что одной из этих близких стран является Германия. На основе общей информации о близком сотрудничестве разведслужб, вполне можно предполагать, что к тому же ряду относятся страны Скандинавии (прежде всего Швеция), Израиль, Южная Корея, Нидерланды, Испания, Италия, Греция.

Интересная специфика работы у разведчиков такова, что спецслужбы этих государств «третьей стороны» могут весьма тесно сотрудничать с АНБ и ЦРУ, среди прочего и в важном деле окучивания национальных провайдеров связи, но при этом американцы энергично шпионят как за правительствами этих стран, так и за собственными «коллегами» из местных спецслужб.

Документально известно, в частности, что Израиль – несмотря на очень тесные контакты с США – считается одной из главных целей американской разведки, наряду с Ираном, Китаем и Россией. Да и Израиль, что тоже не секрет, располагает одной из самых активных разведсетей на территории США.

Наконец, есть еще одна группа стран в Европе и на Ближнем Востоке, где по свидетельству источников WSJ национальные провайдеры связи также «помогают» АНБ из-за особых отношений США с властями этих государств. Главным внешним признаком подобного рода «особых отношений» можно считать так называемую Оборонную телефонную линию – или Defense Telephone Link – напрямую соединяющую эти страны с властями США.

Известно, что в Европе к этой группе относятся следующие страны: Албания, Австрия, Болгария, Латвия, Литва, Македония, Польша, Румыния, Словакия, Словения, Чехия, Эстония.

На Ближнем Востоке: Бахрейн, Кувейт, Оман, Катар, Саудовская Аравия, Объединенные Арабские Эмираты, (плюс, конечно же, еще раз Израиль).

В большинство своем эти страны по тем или иным причинам оказались в сильной зависимости от американской военной помощи, а потому часто сами желают сотрудничать с разведслужбами США. Но конечно же, наличие прямой «горячей линии» совершенно не означает, что буквально во всех этих странах АНБ непременно имеет соглашения с местными интернет-провайдерами.

Однако данный перечень дает вполне четкое представление о том, где еще, наиболее вероятно, следует ожидать сотрудничающих с американской разведкой операторов связи. Потому что не только с политической, но даже с чисто технической точки зрения понятно, что заключать секретные бизнес-соглашения с зарубежной разведслужбой – это в высшей степени деликатное и чреватое большими проблемами дело. Иначе говоря, в подобных шпионских сделках провайдеры связи обязательно должны иметь прикрытие от своих госвластей. Или хотя бы от национальных спецслужб.

И конечно же, совсем не случайность, что именно в перечисленных выше странах Восточной Европы и Ближнего Востока в эпоху президента Буша-сына появились секретные тюрьмы ЦРУ, где прятали и пытали, бывало, похищаемых спецслужбами США людей. Которых поначалу считали террористами, а затем либо отпускали по-

тихому, либо по сию пору держат без суда где-нибудь на базе Гуантанамо вот уже второй десяток лет.

То есть речь идет о чистой уголовщине и серьезнейших преступлениях, за которые еще никто не понес заслуженного наказания.

Вместо послесловия

Если после всего здесь рассказанного у кого-то вдруг осталось непонимание – типа, а как же необходимость борьбы с настоящими террористами? – то здесь может помочь самый тривиальный тест.

Начиная с сентября 2001 года (про раньше и говорить не о чем) попробуйте отыскать в истории хоть один настоящий судебный процесс над реальными главарями террористов Аль-Каиды. Чтобы было следствие, чтобы был суд, чтобы этим злодеям хоть раз дали возможность рассказать, как все было на самом деле. Ведь как было бы поучительно – арестовать и судить Осаму Бен Ладена…

Реальность такова, что судов подобных не бывает. Потому что если хоть раз довести настоящее правосудие до конца, то тогда откроется и реальная ситуация с терроризмом.

Но именно это есть очень большая (и чрезвычайно прибыльная) государственная тайна…

# # #

Bitcoin как знак перемен

(*Декабрь 2013*)

Очень любопытные и важные дела происходят вокруг цифровой криптовалюты Биткойн. Еще вчера об этих экзотических виртуальных деньгах, анонимно родившихся в сетевом андеграунде, почти никто, кроме продвинутых пользователей интернета, и понятия-то не имел. А ныне Bitcoin обсуждают и – что особо поразительно – одобряют власти ведущих государств планеты.

Кто тут рулевой?

Глядя на происходящее со стороны и без подготовки, действительно весьма сложно постичь, каким образом происходят столь быстрые и удивительные перемены.

Когда в октябре этого года ФБР и другие правоохранительные спецслужбы США под корень вырубили в интернете Silk Road, крупнейший в мире онлайн-рынок наркотиков, то попутно много недобрых слов досталось и Bitcoin – как анонимной платежной системе, на основе которой были устроены взаимные расчеты у пользователей «Шелкового пути».

От представителей американских властей в прессу то и дело стали просачиваться мнения и оценки примерно такого содержания:

> *Завеса анонимности, предоставляемая виртуальными валютами, помогает опасной преступной деятельности, такой как торговля наркотиками, отмывание денег, нелегальные продажи оружия и детская порнография…*

Иначе говоря, вполне отчетливо давалось понять, что правоохранительные органы и структуры власти уже всерьез намерены разобраться со всеми этими анархическими цифровыми деньгами и навести в данном деле порядок – как понимают его на государственном уровне…

Ну а затем стало известно, что на 18-19 ноября с.г. назначены специальные слушания в Сенате США – причем не просто посвященные виртуальным сетевым валютам вообще и Биткойну в частности, но именно в свете последних событий вокруг Silk Road.

То есть по итогам подобного мероприятия вполне можно было ожидать каких-то новых законодательных инициатив, направленных на ужесточение контроля, пресечение и наказание любой самодеятельности масс в отношении цифровых наличных и обезличенных взаимных расчетов.

И вот тут-то, когда сенатские публичные слушания пошли и завершились, вдруг неожиданно выяснилось, что американское государство не только не намерено «запрещать Bitcoin», но и совсем даже напротив. В системе усмотрена масса положительных аспектов, стимулирующих развитие рынка и бизнес-инноваций. Да и вообще – дело это в принципе неплохое.

Ну а что касается контроля за злоупотреблениями и пресечения преступной деятельности, так на этот счет у государства уже имеются все необходимые инструменты и полномочия. То есть никаких дополнительных мер по закручиванию гаек тут, судя по всему, не планируется…

Дабы загадочность этого удивительного события в Сенате стала еще более непонятной, необходимо подчеркнуть, что ни одна из ветвей власти США пока еще даже не определилась, как вообще следует трактовать Bitcoin. Как еще одну валюту? Как товар? Как ценные бумаги? Как-то, может быть, вообще иначе?

Мало того, что здесь нет понимания. Конкретно у законодателей, по большому счету, нет еще даже и интереса к этой проблеме. Об этом красноречиво свидетельствует уже тот факт, что на «слушаниях по Биткойну» в Сенате 18 ноября реально от конгрессменов присутствовал всего один-единственный человек – председатель соответствующего сенатского комитета, рассылавшего запросы-приглашения по инстанциям и экспертам, чтобы от них услышать компетентное мнение специалистов по проблеме.

Иными словами, на слушаниях в Сенате собралось немало сведущих и заинтересованных людей. Однако собственно законодателей среди этих людей не оказалось.

Что же касается исполнительной ветви власти, то президенту США и его аппарату – в свете околошпионских скандалов вокруг файлов Сноудена и массы прочих разнообразных проблем – сейчас явно не до того, чтобы делать еще и какие-то стратегические решения или заявления по Bitcoin.

И тем не менее, представители практически всех ключевых структур американского государства – министерства юстиции, министерства финансов, банка федерального резерва и так далее – на редкость дружно и согласованно выступили в Сенате в едином ключе: что система Bitcoin это вполне серьезно; что поставить ее под свой контроль власть не может; что пытаться её искоренять, однако, не следует; а надо, напротив, пытаться обращать подобные системы на пользу обществу и государству…

Короче говоря, за всем этим спектаклем «официального одобрения» совершенно отчетливо чувствуется рука опытного и сильного режиссера. Но вот только кто именно срежиссировал данную постановку – на такой вопрос вряд ли кто сейчас ответит.

Но и не зная ответов на подобные вопросы, вполне можно – даже нужно и наверняка пора – поближе познакомится с собственно системой.

Как это устроено

По мнению компетентных специалистов, профессионально разбирающихся в тонкостях математической криптографии, программирования пиринговых сетей и экономики финансово-платежных систем, технология Bitcoin по праву носит титул «золотого стандарта» цифровой валюты.

При этом никому достоверно не известно, что за человек или команда людей стоит за изобретением Bitcoin. А работа системы устроена так, что ни у госвластей, ни у банков, ни у сетей кредитных карт и прочих традиционных структур, занимающихся финансовыми транзакциями, нет – строго говоря – абсолютно никаких резонов любить и приветствовать Bitcoin.

Потому что Bitcoin – как пиринговая или одноранговая система с открытым исходным кодом – это не просто новая технология для обеспечения взаимных денежных расчетов на основе цифровых монет-Биткойнов, но и гораздо больше. Есть все основания говорить, что суть Bitcoin – это в концентрированном виде совершенно иная модель функционирования общества.

Для людей, использующих Bitcoin, работа механизмов данной системы делает в общем-то несущественными такие вещи, как банки, финансовое регулирование и правительственное вмешательство в их денежные дела.

По сути дела, обращение монет-Биткойнов не может быть объектом контроля и манипулирований со стороны правительств или финансовых институтов, а взаимные денежные расчеты происходят непосредственно между двумя сторонами без всяких посредников.

При этом, поскольку здесь изначально нет никакой центральной базы операций или операторов, функционирование данной системы нельзя остановить в принципе – пока есть люди, желающие продолжения ее работы.

С технической стороны это обеспечено тем, что система Bitcoin характеризуется полностью децентрализованной структурой, в которой нет и в принципе не требуется никакого центрального сервера или доверяемых сторон для гарантированного обеспечения честных платежей.

Пользователи системы сами генерируют и держат у себя криптоключи к цифровым кошелькам со своими деньгами, расплачиваясь непосредственно друг с другом через прямые транзакции.

При этом математико-криптографическая основа системы устроена так, что здесь вся сеть прочих пользователей Bitcoin обеспечивает честность каждой конкретной транзакции – обладая надежными проверочными средствами для недопущения подделки денег и мошенничества с повторным использованием одних и тех же средств.

О конкретных деталях относительно устройства и функционирования столь любопытной системы подробнее можно прочесть в материале «**Деньги будущего**». Ну а здесь, для завершения краткого описания Bitcoin, осталось подчеркнуть такие вещи.

Эта система была задумана и реализована таким образом, чтобы все мы не нуждались в доверии к каким-то конкретным личностям, к компаниям или к правительствам. В этой системе кто угодно может проверить код программы, а собственно сеть не контролируется никем конкретно. Именно в этих факторах заключается то, что вдохновляет на доверие к данной системе.

Иными словами, Bitcoin выживает и набирает сил по той причине, что именно вы здесь можете увидеть и чего видеть не можете. Все пользователи скрыты, однако все транзакции выставлены напоказ. Код доступен для всех, однако его происхождение остается загадкой. Валюта Bitcoin одновременно вполне реальна и при этом неуловима – также как и ее создатель.

Короче, уровень живучести Bitcoin таков, что эта система способна пережить хоть ядерную атаку…

Так, во всяком случае, выглядит теория. На практике же, как известно, все сводится к делам тех или иных конкретных людей. И вот тут сразу начинаются проблемы…

Соглашатели и радикалы

Дабы нынешняя ситуация в движении Bitcoin стала понятнее, полезно вкратце напомнить всю недлинную пока хронологию этой системы.

Пять лет тому назад, в октябре 2008, анонимный «отец Биткойна», укрывшийся под японским псевдонимом Сатоши Накамото, опубликовал в интернете основополагающую статью под названием «Bitcoin: Пиринговая система электронных наличных» (https://bitcoin.org/bitcoin.pdf).

(То, что «Сатоши Накамото» – это вымышленный персонаж, никогда сомнений не вызывало. Японское имя вряд ли имеет отношение к национальности создателя или создателей системы, поскольку все тексты автора написаны на безупречном английском, а хотя бы отдаленно чего-то похожего на японский вариант Биткойна в интернете никогда не было.)

Уже в 2009 году сформировалось ядро программистов, которые создали реальное воплощение Биткойна в Сети. Примечательно, что никто даже из самых первых энтузиастов лично с Сатоши Накамото не встречался, а все их общение происходило исключительно по электронной почте.

На базе этого же ядра программистов-энтузиастов был создан Фонд Bitcoin, сосредоточившийся на развитии системы и ее продвижении в массы. Что же касается Сатоши Накамото, то в 2010 году, когда система Bitcoin реально заработала и начал набирать обороты, персонаж под этим именем полностью самоустранился от участия в движении и «растворился в интернете»…

Обменный курс Биткойна поначалу был, что называется, ниже плинтуса. Но, по мере распространения интереса к системе среди народных масс, довольно быстро обозначился отчетливый рост. Сначала это были центы, затем доллары, после чего десятки, сотни, а ныне многие аналитики абсолютно всерьез предсказывают, что за 1 Биткойн к началу 2014 года уже стабильно будут давать 1 тысячу долларов американских денег…

Естественно, все это очень похоже на ажиотаж вокруг очередной финансовой пирамиды. Также понятно, что умные-грамотные в целом люди с самого начала указывали на эту аналогию и предрекали Биткойну скорый крах – как и для любого мыльного пузыря на рынке.

Правда и то, что курс Биткойна растет далеко не стабильными темпами, а скорее напротив – то и дело скачет как безумный. Бывали ситуации, когда всего за пару недель он катастрофически обрушивался ниже доллара, а затем вновь взлетал в сотню раз выше. (Подробности о критике Bitcoin см. в материале «На звон БитМонет».)

Но как бы там ни было, системе Bitcoin определенно удается не только стабильно выдерживать все эти скачки курса, многочисленные попытки компрометации и недоверие властей-корпораций, но и продолжать свой постоянный рост.

А своеобразным отражением проблем роста у новых цифровых денег оказывается весьма непростая ситуация вокруг Фонда Bitcoin и конкретных людей, этот фонд представляющих.

Среди ключевых фигур и своего рода евангелистов движения чаще всего называют таких деятелей, как Гэвин Андресен (Gavin Andresen), главный ученый Фонда; Питер Вессенс (Peter Vessenes), председатель Фонда; и Майк Хирн (Mike Hearn), член правления Фонда и до недавнего времени видный программист корпорации Google.

На протяжении последних лет все перечисленные и влиятельные в Фонде люди энергично ратовали за то, чтобы работать и сотрудничать с властями – дабы преодолеть

широко распространенный в государстве подход недоверия к подобным стихийно возникшим начинаниям.

Чтобы стало понятнее, почему это действительно важно, достаточно привести хотя бы такой факт. По свидетельству юристов Фонда, даже сегодня те молодые компании, что имеют в своем названии или в документах на регистрацию слово Bitcoin, зачастую сталкиваются с отказами банков…

При этом, однако, в жизни движения Биткойн вполне отчетливо наблюдаются и такие силы, которые выступают активно против позиции «соглашателей» в правлении Bitcoin Foundation. Причем радикальное крыло энтузиастов не только возражает против госрегулирования на словах, но и пытается прибегать к более действенным рычагам сопротивления.

Одной из заметных фигур этого крыла является Коди Уилсон (Cody Wilson), наиболее известный как лидер специфического проекта с открытыми исходными кодами, нацеленного на огнестрельного оружия с помощью 3D-принтеров. Другой известный лидер Bitcoin-сопротивления – программист Амир Тааки (Amir Taaki), называющий себя «крипто-анархистом».

Не так давно два этих активиста объявили о планах разработать программное обеспечение Dark Wallet (темный кошелек) – инструмент, который, как они надеются, сделает платежный сервис не только более легким для пользователей, но и обеспечит Биткойн-транзакциям еще большую анонимность.

Уилсон, Тааки и все их сторонники в движении Bitcoin уверены, что соглашательская деятельность правления Фонда выглядит очень подозрительно. Более того, уже звучат открытые обвинения в адрес тех членов руководства, которые предают принципы независимости и анонимности. Иначе говоря, те важнейшие принципы, что были изначально заложены Сатоши Накамото в самую сердцевину новой валюты.

Справедливости ради следует признать, что обвинения эти не лишены оснований. И позиция правления Фонда в отношении анонимности действительно является двусмысленной.

На недавних слушаниях в Сенате США, в частности, главный юрисконсульт Фонда Bitcoin, Патрик Мёрк (Patrick Murck), с одной стороны, среди минусов отметил, что пользователи системы уже столкнулись с проблемами сохранения своей анонимности. И при этом, с другой стороны, пообещал, что будущие версии программного обеспечения Биткойн позволят реализовать лучшую верификацию личности.

Если же подытоживать суть конфликта в целом, то Коди Уилсон и прочие радикалы категорически не одобряют тот путь, которым пошло правление фонда, соглашаясь на встречи с представителями федеральных властей. Особое раздражение, в частности,

вызвала презентация, которую в 2011 году главный ученый Фонда Гэвин Андресен давал в ЦРУ США.

Что же касается совсем недавних событий, то некоторые из радикальных энтузиастов Биткойн были сильно разочарованы в октябре, когда Майк Хирн с ликованием приветствовал известие про разгром властями сайта Silk Road, назвав это «фантастической новостью».

Помимо философско-идеологических разногласий – и очевидно вместе с ростом финансовых успехов Bitcoin – систему отчетливо начали потряхивать и скандалы существенно иного рода.

Например, под сильнейший огонь критики со стороны соратников не так давно попал председатель фонда Питер Вессенс. Параллельно со своим административным постом в правлении, Вессенс является основателем фирмы под названием CoinLab, цель которой – быть инкубатором для новых коммерческих приложений вокруг Bitcoin.

А там где коммерция, там же, естественно, и скандалы вокруг дележа денег. В мае нынешнего года CoinLab подала в суд на Mt. Gox, до недавних пор крупнейшую в интернете Биткойн-биржу, которую обвинила в нарушении контрактных обязательств – с требованием к ответчику заплатить 75 миллионов долларов в порядке возмещения ущерба.

По мнению CoinLab, веб-площадка Mt. Gox не выполнила своих обязательств по передаче им всех своих биржевых возможностей, имеющихся в США и Канаде – что было частью их бизнес-соглашения, и что должно было сделать CoinLab крупнейшим Биткойн-обменником в Северной Америке.

Победа CoinLab в суде вполне могла оказаться для Mt. Gox фатальным ударом, поэтому в ответ данная компания, базирующаяся в Японии, выдвинула против CoinLab встречный контр-иск. Обвинив их в том, что CoinLab завладела деньгами пользователей Mt. Gox на сумму свыше 5 миллионов долларов, но при этом не зарегистрировала себя как бизнес финансовых услуг – чем сделала недействительными их прежние контрактные соглашения…

По мнению критиков, вся эта некрасивая история – и судебный демарш Вессенса, и текущие юридические проблемы у CoinLab – представляет собой не просто наглядное свидетельство корыстных и злонамеренных помыслов у лидеров движения. Но и вообще – личную нечестность людей среди наиболее влиятельных фигур во главе Bitcoin-движения.

Впрочем, несмотря на атаки радикалов, пока не подлежит никакому сомнению, что Андресен, Хирн и Вессенс – как ведущие разработчики этого программного обеспечения – плюс все их единомышленники в правлении Фонда, обладают в сообществе на-

много большим весом и авторитетом. По сути дела, данная команда уже действует в мире Bitcoin так, как структура, де факто управляющая всей системой.

Причем для этого имеются и сугубо технические причины. Система и ее базовый код не являются чем-то навсегда застывшим. И поскольку запуск в работу абсолютно любых коррективов и изменений в правилах требует соответствующих изменений в эталонном (референсном) ПО, то ведущие разработчики программы держат свои руки на рычагах власти. Ибо в коде системы такие рычаги реально имеются. Иначе говоря, перечисленные люди оказываются известными и естественными лидерами всего сообщества…

Действительная важность такого лидерства стала очевидна для всех, когда в марте этого года иная группа добровольных программистов Биткойна попыталась сделать апгрейд базового ПО системы. Как результат, в течение непродолжительного периода времени пользователи системы работали с двумя разными и несовместимыми версиями Bitcoin. То есть произошел фактический раскол, который по природе различий в кодах вполне мог превратить Биткойн в две разные валюты.

Андресену и его единомышленникам достаточно оперативно удалось убедить пользователей нового ПО в том, чтобы переключиться обратно на предыдущие версии программы, предотвратив таким образом кризис. И вполне очевидно, что правление и далее будет энергично продолжать подобного рода усилия во всем, что касается ключевых вопросов программирования системы.

С точки зрения радикалов – Уилсона, Тааки и их сторонников – руководство фонда в лице Андресена и компании уже давно лишь скрывается под личиной либертарианцев, несущих миру новые анонимные наличные. На самом же деле, уверены они, правление мечтает «превратить Биткойн в PayPal Plus», а ради успеха этой своей затеи полностью готово и согласно делать все, что прикажет им правительство…

Глобальный фактор

Строго говоря, пока что нет – кроме голословных обвинений радикалов – абсолютно никаких свидетельств тому, что руководство Bitcoin уже вступило в некие тайные соглашения с властями США.

Однако не подлежит никакому сомнению факт очевидного «потепления» в отношениях к Биткойну со стороны американского правительства. Таким же неоспоримым фактом является и то, что ключевые фигуры в правлении Фонда Bitcoin являются гражданами США – со всеми вытекающими отсюда последствиями для их «независимости».

Но если посмотреть на бесспорные нынешние перемены вокруг Bitcoin в более широком – мировом – масштабе, то легко выявляются и совсем другие, ничуть не менее (а

может, и намного более) важные факторы. В первую очередь – страны азиатского региона и в первую очередь Китай.

Согласно статистическим данным веб-сайта Bitcoin Charts, ныне уже около трети всех Биткойн-транзакций в мире проходят через одну биржу, BTC China, которая в качестве обменника обслуживает только китайских пользователей. Как результат, стремительно растущая биржа BTC China по объемам торгов совсем недавно обогнала прежнего лидера, базирующийся в Токио сайт Mt. Gox.

На Bitcoin Singapore, международной конференции по криптовалюте, проходившей примерно одновременно со слушаниями в Сентае США, вице-президент BTC China Линке Янг так, например, объяснил секрет их небывалой популярности:

> *«Главная причина того, почему Биткойн стал таким хитом в Китае – это потому что китайцы по натуре люди бережливые, а в Биткойне все больше и больше людей видят привлекательный способ для хранения и инвестирования своих денег»…*

Имеются тут, впрочем, и куда более веские причины. Скажем, в прошлом месяце интернет-компания Baidu, известная как «китайский ответ Гуглу» и самый популярный поисковик в стране, начала принимать Биткойны в качестве оплаты за некоторые из сервисов, предлагаемых ее дочерней компанией Jiasule.

Не секрет и то, что предприимчивая доля китайцев, не особо довольная строгим государственным контролем властей за оборотом юаней, увидела в Биткойнах привлекательный способ для валютных спекуляций.

Вообще, для многих аналитиков финансовых рынков оказалось неожиданным сюрпризом – принимая во внимание жесткий контроль бизнеса в стране и отчетливый подпольный потенциал Биткойна – что власти Китая не вмешались и не начали строго регулировать Биткойн-операции…

Вместо этого телевизионная компания CCTV и газета Жэньминь Жибао – обе являющиеся главными государственными СМИ – на протяжении всего прошедшего лета давали весьма позитивные материалы о системе Bitcoin. Иначе говоря, неофициально одобрили новые цифровые деньги для повсеместного использования.

Ну а в завершение этой интересной картины осталось добавить, что сразу же после окончания слушаний по Биткойну в Сенате США, китайские власти сделали весьма многозначительное объявление.

Народный банк Китая 21 ноября этого года объявил, что страна больше не видит никаких выгод от увеличения своих запасов в иностранной валюте. Соответственно, Китай больше не стремится к накоплению валютных резервов, а финансовые власти Китая «в основном» заканчивают свое обычное вмешательство в регулирование валютного рынка и расширяют масштабы ежедневных торгов по юаню.

Для общего представления о том, насколько круто выглядят эти перемены, следует отметить, что валютные резервы Китая лишь за третий квартал года увеличились на 166 миллиардов долларов, достигнув рекордной суммы 3,66 триллионов долларов (это больше чем в три раза превышает валютные запасы любой другой страны мира).

Кроме того, Китая сегодня – это крупнейший в мире кредитор США, а сумма американского долга китайцам составляет ныне 1,294 триллиона долларов. Каким образом охлаждение интересов Китая к накоплению своих валютных запасов скажется на судьбе американских государственных долгов – это вопрос даже среди специалистов спорный.

Еще более спорным выглядит вопрос о том, имеет ли к этому хоть какое-то отношение благоприятная ситуация вокруг Биткойна, явно обозначившаяся в Китае. Но один вывод, однако, тут представляется вполне очевидным.

При любых разговорах о дальнейшей судьбе системы Bitcoin вопрос об отношении к ней со стороны государства США заведомо не будет определяющим.

Тут же уместно напомнить и то, что США на самом деле никогда и не были в центре мира Bitcoin. Хотя по сию пору неясно, кто именно изобрел Биткойн и откуда Сатоши Накомото вообще появился, по многим особенностям его английского видно, что это язык британских островов, а не американского континента.

Далее, ни одна из трех главных обменных Биткойн-бирж интернета не находится в Соединенных Штатах: наряду с BTC в Китае и Mt. Gox в Японии, третьим основным обменником является сайт Bitstamp, находящийся в Словении.

Ну и, наконец, что еще более важно по мнению многих экспертов и наблюдателей, так это неоспоримая значимость Bitcoin для стран развивающегося мира. Где эта система

уже по самой природе будет все больше и больше доказывать людям свою полезность и преимущества. Поскольку реально способна предложить им такой тип валюты, который обладает иммунитетом ко всем финансовым манипуляциям со стороны местных правительств.

А кроме того, Bitcoin способен совершенно естественным путем подключать и выводить в мир глобальной экономики те миллиарды людей, что пока не имеют доступа к традиционным финансовым сервисам (то есть речь идет о широчайших платежных возможностях для так называемых unbanked или «безбанковых» людей планеты).

# # #

Дополнительные материалы

Об истории появления, сути и критиках BitCoin: «На звон БитМонет»

Об идеологических и технических особенностях устройства системы: «Деньги будущего уже здесь»

О детективных розысках прессой реального изобретателя BitCoin: «Тайна отцовства»

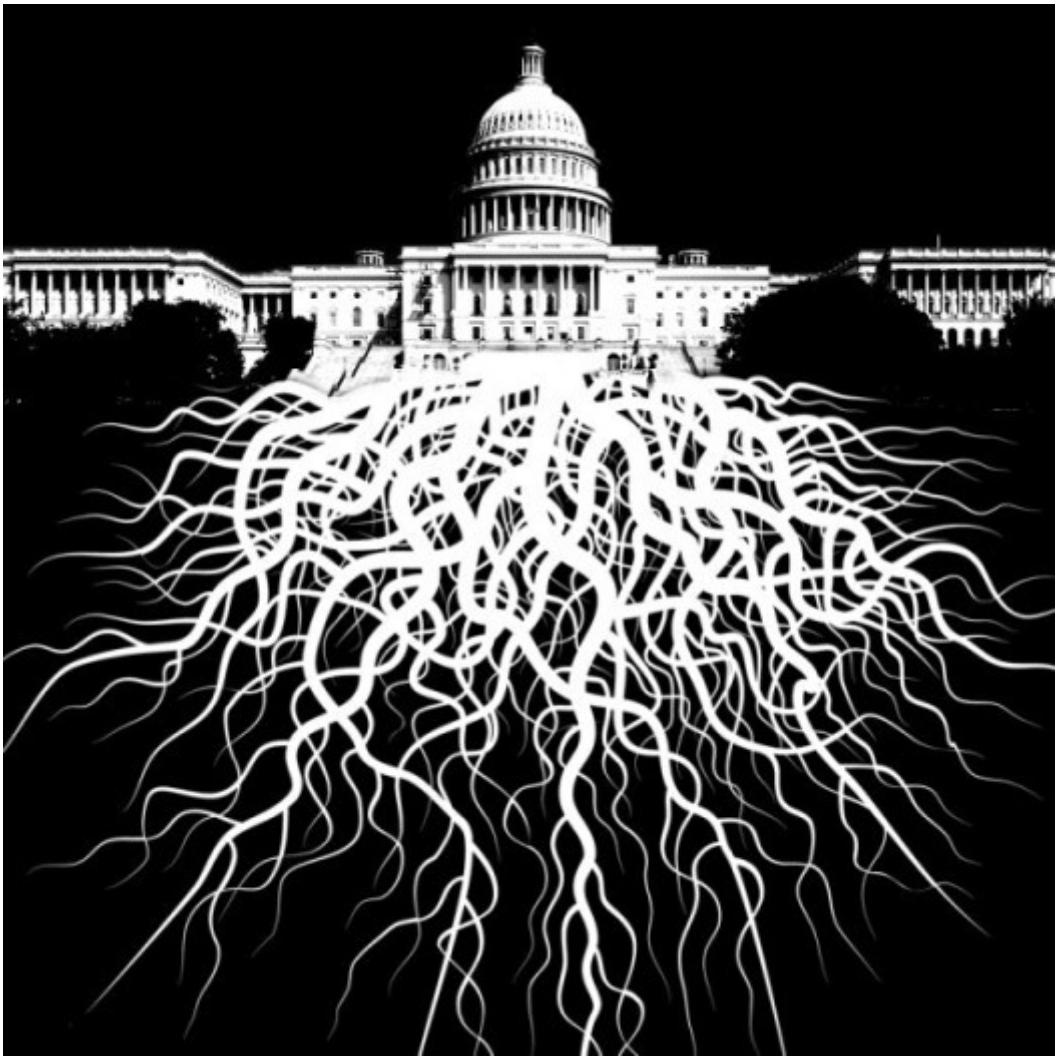
О применении BitCoin в организации честных, насквозь проверяемых выборов: «CommitCoin: Сделаем это по-честному»

О подпольном рынке Silk Road, работавшем на основе BitCoin: «Шелковый Путь в контексте»

Невыученные уроки истории

(*Март 2017*)

Одни говорят, что история повторяется дважды. Другие считают, что история вообще ходит все время кругами. Но так или иначе, невозможно хоть чему-то у истории научиться, если не замечать важные исторические параллелизмы.



Пролог: страхи и тайны

Одной из наиболее примечательных аналитических публикаций, появлявшихся в феврале 2017 на страницах ведущей газеты США The New York Times, стала статья под названием «*Утечки множатся, а с ними и страхи Глубокого Государства в Америке*».

Примечательна эта статья даже не тем, что в заголовки центральной газеты чуть ли не впервые попал термин Deep State применительно к специфике государственной власти в США (прежде столь открыто о параллельных тайных структурах, реально управляющих государством абсолютно без какого-либо контроля со стороны обще-

ства, обычно писали лишь презренные таблоиды и всяческие конспирологические издания). На фоне острого противостояния между президентом Трампом и традиционной госбюрократией термин «глубокое государство» быстро стал в прессе расхожим, так что Нью-Йорк Таймс лишь закрепила тенденцию.

Куда интереснее то, что очевидный факт «столкновения культур» и конфликт двух существенно разных подходов к ведению государственных дел представлен в газете как нечто совершенно новое для истории США:

> *Волна утечек из правительственных структур подрывает администрацию Трампа, что ведет к проведению параллелей с такими странами как Египет, Турция и Пакистан, где влиятельные теневые структуры в недрах правительственной бюрократии, часто именуемые «глубоким государством», всячески ослабляют и сдерживают демократически избранную власть. (А затем, при углублении конфликта, и нередко доводят дело до государственного переворота.)*
> . . .
> *Здесь нет никаких хороших долговременных последствий. Война между разведывательным сообществом и Белым Домом – это плохо для разведсообщества, это плохо для Белого Дома, и это плохо для безопасности нации…*

Иначе говоря, очевидно умные и знающие эксперты, цитируемые газетой, всяческими примерами пытаются создать впечатление, будто очень «влиятельные теневые структуры» в государстве – это давняя известная напасть где-то там, в других странах. Но уж конечно не в США с их отлаженными демократическими механизмами контроля, сдерживающих рычагов, противовесов и так далее.

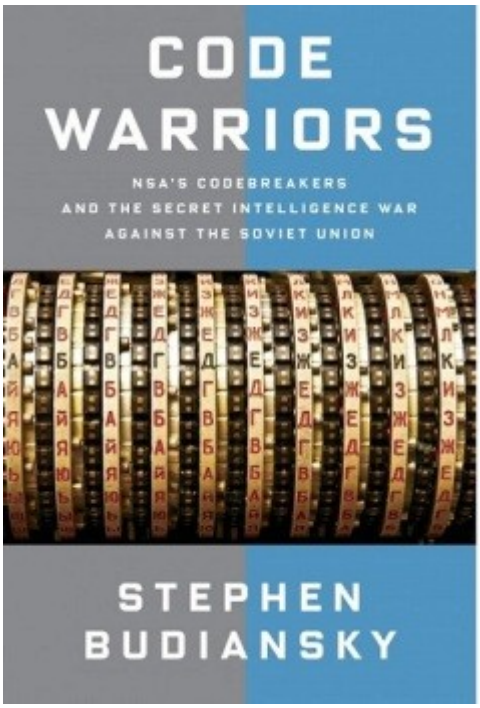
Ярчайшим примером чему, по идее, должна служить и совсем новая инициатива ЦРУ США – с выкладыванием в свободный онлайновый доступ гигантского архива своих рассекреченных документов, охватывающих историю разведслужбы с момента создания в конце 1940-х и вплоть до 1990-х годов.

Этот массив, насчитывающий около 1 миллиона документов на более чем 12 миллионах страниц, был в принципе доступен исследователям и ранее – но на очень неудобных условиях (чтобы получить доступ, требовалось лично приехать в Национальный архив в пригороде Вашингтона и успеть занять место за одним из 4 компьютерных терминалов, подключенных к нужной базе архива и работающих лишь строго по будням, с 9-00 до 16-30). Заставить же ЦРУ выложить эти документы в интернет удалось недавно и исключительно через суд. Причем поначалу срок выполнения работы оценивался в 6 лет, а затем – осенью 2016 – было дано обещание выложить все в онлайн к концу 2017.

Однако уже в январе 2017 (аккурат накануне въезда Трампа в Белый Дом) вдруг выяснилось, что ЦРУ США – это оказывается, чуть ли не главный в державе сторонник

открытого информирования общества о темных государственных секретах. Поэтому все работы по обеспечению онлайн-доступа к рассекреченным архивам ЦРУ уже ударно завершены – так что всем добро пожаловать в «*читальный зал ЦРУ*». Ну а попутно, как все наверняка наслышаны, из разведки пошли в прессу и анонимные сливы богатого компромата на людей из команды нового президента…

Изучение давних секретов из архивов ЦРУ, несомненно, принесет со временем множество содержательных статей и книг о малоизвестных страницах новейшей истории и её тайных войн. Ну а пока эти работы пишутся, имеет смысл свежим взглядом взглянуть на то, что уже подготовлено за последнее время исследователями данной области. И увидеть очень выразительные – можно даже сказать поучительные – исторические параллели с нынешними событиями. Особенно в контексте Глубокого Государства или кратко ГГ.



В частности, особого внимания заслуживает совсем свежая, опубликованная в конце 2016 года, книга американского журналиста и писателя Стивена Будянски «*Кодо-воины: Криптоаналитики АНБ и тайная разведывательная война против Советского Союза*» («Code Warriors: NSA’s Codebreakers and the Secret Intelligence War Against the Soviet Union» by Stephen Budiansky. Knopf 2016).

В книге с весьма широким охватом событий собрано великое множество фактов и документов не только о деятельности АНБ, естественно, но также и об операциях ЦРУ, космической разведки и прочих спецслужб США. Нас же – ради проведения отчетливых параллелей – особо будет интересовать глава восьмая, под названием «Дни кризиса»…

Тема «У»: U-2 и Украина

Для тех читателей, кто не очень уверенно ориентируется в ключевых исторических событиях второй половины XX века, следует напомнить, что планета никогда не оказывалась на грани мировой термоядерной войны столь же близко, как это случилось в дни так называемого Карибского кризиса осенью 1962 года. И что характерно, у руля власти в США стоял в ту пору президент Джон Ф. Кеннеди, а в империи СССР аналогичный пост Сына Неба занимал Никита С. Хрущев. То есть люди, в своих личных устремлениях больше всего желавшие мира во всем мире… (Благодаря чему, быть может, мы и не сгорели тогда в огне тотальной катастрофы.)

Еще одна очень характерная деталь из той же эпохи, на которую обращают внимание куда меньше, заключается вот в чем. Примерно через год после кризиса, осенью 1963 Джон Кеннеди был убит, а еще через год, в 1964 Никита Хрущев был принудительно смещен со всех постов и отправлен в отставку (причем есть свидетельства, что поначалу у заговорщиков имелись планы и его физической ликвидации). Ну а продолжением этих историй стали крупномасштабная война США во Вьетнаме, Лаосе и Камбодже, ввод советских войск в Чехословакию для подавления Пражской весны и, соответственно, совсем никаких надежд на скорый мир во всем мире…

Уже из этих примеров наглядно видно, что лидеры государств хотя и способны играть, несомненно, огромную личную роль в судьбах народов, однако и незримые структуры ГГ так или иначе все равно проявляют свои могущество и влиятельность. А также неистребимые властолюбивые интересы, которые в самой основе своей не имеют ничего общего с надеждами и чаяниями народных масс. И конечно же, эти скрытые, ни перед кем не отчитывающиеся структуры в недрах любых бюрократических государств имеются всегда. В независимости от эпохи или конкретной страны. Другой вопрос, сколь огромных степеней могущества эти теневые структуры могут достигать. И как, соответственно, их контролировать-нейтрализовать в условиях демократии.

В контексте нынешних российско-американских отношений кризис начала 1960-х особо поучителен по той причине, что здесь имеется целый букет тем-соответствий, не заметить которые довольно сложно. В первую же очередь следует выделить тот факт, что прежний президент Дуайт Эйзенхауэр был политиком-конформистом, полностью вписанным в уже существовавшую бюрократическую систему США и охотно делегировавшим свои полномочия в компетентные инстанции. Ну а Джон Кеннеди (в тесной связке с братом Робертом), относился к тому типу людей, которые очень энергично пытаются изменить систему к более прогрессивному и динамичному виду.

Степень «прогрессивности» нынешнего президента Трампа, конечно, – это тема весьма дискуссионная, однако его энергичные попытки поменять устоявшуюся в государстве систему управления сомнений не вызывают. Аналогично, вряд ли кто будет возражать, что его предшественник Обама был президентом, абсолютно ни в чем не посягавшим на традиции системы или области компетенции силовиков. Ну а что самое главное, и в ту, и в другую эпоху новый президент-реформатор унаследовал от прези-

дента-конформиста кучу серьезнейших политических проблем, разруливать которые по-любому надо. И одной из самых серьезных проблем в обоих случаях стали резко ухудшившиеся отношения с русскими. Причем даже название причины в обоих случаях начинается на одну и ту же букву «У»…

И точно так же, как сегодня история с госпереворотом (и сбитым авиалайнером) на Украине является наглядным примером вопиющего лицемерия, двойных стандартов и абсолютно бесстыжего вранья в делах высокой международной политики, в 1960 году нечто очень похожее продемонстрировала история со сбитым над Уралом самолетом-шпионом U-2 (подробности см. в тексте «*Море лжи и привет от Автобазы*»). Масштабы той драмы, конечно, были несравнимо меньшими, однако и такого инцидента вполне хватило, чтобы в хлам испортить трудно налаживавшиеся советско-американские отношения и сорвать уже согласованные многосторонние договоренности по линии ядерного разоружения.

Позднее, уже покинув свой высокий пост, Эйзенхауэр честно признавал, что если бы власти СССР нарушили американское воздушное пространство в той же манере, как это многократно делалось с применением U-2, то он сам бы первым обратился в Конгресс о немедленном объявлении войны. Однако для себя США, уверовав в собственную исключительность, считали такое поведение вполне приемлемым и безнаказанным. Ибо тогдашний директор ЦРУ Аллен Даллес всячески заверял президента, что U-2 летает настолько высоко, где русским его ни за что не достать. И даже если вдруг Советам удастся сбить самолет ракетой, то ни шпионское оборудование, ни пилот машины наверняка после этого не выживут, чтобы хоть что-то рассказать коммунистам…

В реальности, как известно, все вышло с точностью до наоборот. Ракета ПВО не только достала U-2, но и пилот, к счастью, остался жив, и шпионское оборудование уцелело. Хитрый Хрущев, однако, громко объявил миру лишь о сбитом самолете-шпионе США, нагло вторгшемся на тысячи километров вглубь СССР, но ни слова не проронил о подробностях – выжидая реакцию американцев. Ну а Эйзенхауэр и его Госдеп, по сути подставленные Алленом Даллесом и баснями от ЦРУ, в привычной для политиков манере начали гнать стопроцентную ложь. Нечто совершенно фантастическое про коварство погоды, турбулентность и недостаток кислорода у пилота, в помутнении рассудка улетевшего из Турции неведомо куда и невинно погибшего под Свердловском…

Выждав некоторое время и позволив всему этому официальному вранью от США как следует утвердиться в новостях СМИ, затем Хрущев не скрывая торжества объявил миру, что пилот самолета на самом деле жив и здоров, находится в советской тюрьме и уже все-все честно признал о своей сугубо шпионской секретной миссии… Этот ловкий ход, несомненно, стал триумфом советской пропаганды – однако последствия скандала для международного климата оказались весьма печальными.

На конференцию по разоружению в Париже, проходившую две недели спустя, Хрущев приехал, что называется, на взводе, с высокой трибуны выдал 45-минутную, в высшей степени эмоциональную речь, местами похожую на истерику, а в итоге фактически торпедировал все трудно достигавшиеся прежде договоренности по нормализации отношений и сворачиванию гонки вооружений…

Всяческие инциденты вокруг шпионажа происходили между СССР и США довольно регулярно, как до, так и после этой истории. Столь неадекватно же разъярили советского лидера вовсе не многократные разведывательные полеты U-2, а возмутительно упорная, с каждым витком конфликта все более наглая и беспардонная ложь со стороны американского руководства. Отчего Хрущев счел оскорбленным не только себя лично, но и решил, что в подобной ситуации гордость и достоинство его государства были бы в высшей степени унижены, если бы СССР сделал на конференции вид, будто ничего особенного не произошло.

Несложно постичь, что ни одна из сторон в итоге тут ничего для себя не выиграла – кроме резко ухудшившихся отношений. А это, по некоторым причинам естественного свойства, всегда укрепляет могущество тайного ГГ.

Тема «Р»: Раскрытие

Сегодня практически все уже, наверняка, наслышаны о человеке по имени Эдвард Сноуден и о том, в общих чертах, что он сделал для информирования публики о шпионских тайнах Агентства национальной безопасности США. Но при этом ныне практически никто и ничего не знает о молодых американцах под фамилиями Мартин и Митчелл, которые находясь в том же, что и Сноуден, возрасте сделали примерно то же

самое – но только на полстолетия раньше, летом 1960 года. То есть в такой исторический период, когда даже сам факт существования криптографической спецслужбы АНБ был великой государственной тайной.

Уже одно лишь то, что имена Уильяма Мартина и Бернона Митчелла (William H. Martin, Bernon F. Mitchell) ныне широкой публике неведомы, является наглядным свидетельством абсолютно никак не усвоенных уроков истории. Скорее можно даже утверждать обратное. Практически все государства (включая и СССР) предпочли побыстрее замять и забыть этот мимолетный эпизод, сделав вид, что его и не было вовсе. Отчего, собственно, впоследствии и должен был появиться Эдвард Сноуден – чтобы вновь напомнить миру о давно известных и заведомо нехороших вещах. Но только теперь уже с тучей неопровержимых в своей подлинности документов.

В отличие от Сноудена, явно не питавшего иллюзий в отношении России и осевшего здесь лишь в силу известных обстоятельств, Мартин и Митчелл тайно перебрались из США в Москву (через Мексику и Кубу) абсолютно целенаправленно, очевидно руководствуясь свойственными молодости романтическими мечтами о стране, строящей светлое будущее. (По иронии судьбы, фактически таким же маршрутом, но только в обратную сторону – из Москвы через Кубу в Латинскую Америку – собирался лететь беглец Сноуден. Помешала утрата паспорта, аннулированного американскими властями.)

Но как бы там ни было, общая суть происходившего в обоих случаях была примерно той же самой. В сентябре 1960 года советские власти устроили для неожиданно явившихся к ним Мартина и Митчелла масштабную пресс-конференцию – с трансляцией на весь мир через Radio Moscow, – где недавние криптоаналитики спецслужбы весьма подробно рассказали вот о чем:

> *«Мы были сотрудниками NSA, в высшей степени секретного Агентства национальной безопасности, которое в интересах правительства США занимается разведкой коммуникаций почти всех стран мира. Однако, просто сам факт того, что правительство США сует свой нос в секреты*

других наций, практически никак не повлиял на наше решение стать перебежчиками. Наше несогласие связано с теми конкретными методами, которыми США собирают разведывательную информацию.

[Далее следовали некоторые подробности о наиболее агрессивных методах сбора, включающих вторжения на территорию других государств и сопутствующую ложь для обмана общественного мнения…] Более того, особо мы были обескуражены практикой США перехватывать и дешифровать засекреченные коммуникации собственных союзников. Наконец, мы категорически против того факта, что власти США охотно вербуют агентов среди персонала своих собственных союзников»…

На вопрос прессы о том, секретные коммуникации каких именно из нейтральных и союзных стран регулярно перехватывает, дешифрует и читает АНБ США, Уильям Мартин ответил так: «Италия, Турция, Франция, Югославия, ОАР (Египет и Сирия), Индонезия, Уругвай – этого достаточно, я думаю, чтобы дать общую картину».

Поскольку три первых государства из упомянутых являлись членами блока НАТО, то есть ближайшими военными союзниками США, понятно, наверное, что широкое обнародование подобной информации в потенциале могло иметь весьма серьезные последствия – если бы хоть кто-то захотел всерьез разбираться с этой темой. Но никто, очевидно, не захотел, так что и поныне – когда всплывают очередные свидетельства о регулярной слежке АНБ за известными политиками и главами стран НАТО – все как бы возмущаются и делают вид, что слышат об этом впервые. Хотя на самом деле подругому тут и не было никогда…

Более того, на сегодня имеется внушительная масса документов и фактов, свидетельствующих, что спецслужбы множества государств – в Европейском, Азиатском и прочих регионах, – помимо тесного сотрудничества с коллегами из США, на регулярной основе еще и шпионят для американцев за собственными политическими лидерами. Потому что демократически избранные руководители государств приходят и уходят, а профессионалам спецслужб работать надо всегда. В независимости от партий и людей, находящихся сейчас у руля… Именно в этом, собственно, и заключается неистребимая стойкость Глубокого Государства.

Ну а то, что тайные структуры власти множества как бы независимых стран по сути обслуживают интересы ГГ в США – уж так оно само как-то сложилось давным-давно. И почему-то упорно сохраняется, несмотря на многократные известные попытки изменить этот порядок.

Тема «О»: Остров

Было бы в корне неверно думать, будто ГГ – это лишь военные и секретные спецслужбы (хотя, бесспорно, они формируют особо влиятельную – поскольку силовую – часть

структуры). В работе этой сети непременно участвуют и «просто» политики, и лидеры финансово-промышленных кругов, и прочие немаловажные люди, от которых что-либо критично зависит в государстве.

Но сколь бы разношерстным ни подбирался этот состав в той или иной конкретной стране, одна особенность имеется в существовании любого ГГ непременно. У каждого государства снаружи обязательно должны иметься сильные и агрессивные внешние враги, а также постоянно нарушающие мир и покой граждан опасные враги внутренние – в виде всевозможных террористов и прочих радикалов-экстремистов. Если же такие государства для общей обороны собрались в блок-союз, то и общий враг у них должен быть исключительно огромный и опасный.

И тут уже совершенно неважно, есть такие враги в реальности, или их надо сконструировать искусственно. Враги просто обязаны быть. Потому что иначе никак не удается как следует отвлекать внимание публики от никогда не надоедающих игр ГГ с их безграничной властью над обычными людишками… Ну а один из самых удобных способов сеять вражду между соседями и разжигать очаги напряженности внутри собственных стран – это создавать разного рода изолированные анклавы на основе компактно проживающих этнических групп или же островов в море-океане.

Вполне наглядный пример всей этой философии предоставляет тема Карибского кризиса вокруг Кубы – особенно, если ее рассматривать в сопоставлении с недавним кризисом вокруг Крыма. А также – что совершенно необходимо – еще и с учетом окружающего исторического контекста. Потому что именно контекст, объясняющий динамику и механизмы происходившего, в мировых СМИ почему-то всё время норовят исключить из обсуждения проблемы.

Неоспоримые же факты истории выглядят следующим образом. Когда в начале 1954 года новый советский Сын Неба Никита Хрущев, не пробыв на высшем посту еще и года, своим волевым решением (или дурной блажью – тут как посмотреть) отрезал Крым от России и включил его в состав милой ему Украины, то на международных

отношениях это не сказалось абсолютно никак. Народ Крыма или России тут никто не спрашивал, народ Украины – тем более. Сын Неба так решил, незримое советское ГГ решение одобрило, закон страны под это дело изменили, а международному сообществу прочих ГГ до этих наших дел было тогда вообще как до Марса.

Но вот когда в том же 1954 году СССР обратился с просьбой принять его в члены недавно созданного оборонительного блока НАТО, то вот здесь международное сообщество занервничало – и выдало Советам решительный отказ. Ибо вся идеология НАТО изначально была построена на принципах «Держать Америку внутри, Россию снаружи, а Германию под»… Другими словами, у военного союза Запада во главе с США иначе просто исчезал бы опаснейший противник на всем европейском континенте – а такой сценарий ГГ никогда не устраивал. (Здесь же надо непременно напомнить, что и при нынешнем Сыне Неба, уже в 2000-е годы, Россия вновь пыталась вступить в члены НАТО – и опять получила недвусмысленный отказ.)

Естественным итогом отказа полувековой давности стало то, уже в 1955 вокруг СССР сформировался военный блок Варшавского договора. Ну а к концу того же десятилетия США разместили в Турции, непосредственно у границ СССР баллистические ракеты средней дальности, вооруженные ядерными боеголовками и с минимальным временем подлета практически ко всем стратегически важным точкам страны. Именно этот ход американцев, как известно, и подтолкнул Хрущева к размещению аналогичных ядерных вооружений на острове Куба, непосредственно «в подбрюшье» у США. («Запустим ежа в штаны дяде Сэму», как выражался на данный счет наш незабвенный лидер).

Поскольку «строго секретная» тема ракет в Турции всегда выводилась за рамки открытой дискуссии о Кубе, при обсуждении Карибского кризиса в западных источниках по давней традиции принято всю вину возлагать на волюнтаризм Хрущева и агрессивность СССР. По совершенно аналогичной траектории, при нынешних дискуссиях вокруг возврата Крыма в Россию на Западе практически никогда не желают признавать, что никакой темы «аннексии» не возникло бы вообще, если бы страны НАТО не поддержали вооруженный госпереворот в Киеве. Хотя на словах, надо подчеркнуть, все власти Европы, США и Канады подобные насильственные действия решительно осуждают – применительно к себе и своим союзникам…

Под конец это странной темы, где все стороны конфликта публично говорили одно, тайно делали другое, а за кулисами договаривались о третьем, осталось напомнить лишь еще один факт. В результате мирного выхода из Карибского кризиса – благодаря готовности к компромиссам братьев Кеннеди, Хрущева и его ближайших соратников – в тайных рядах ГГ осталось очень много недовольных. Военные и спецслужбы США были в ярости, что Кеннеди помешал им раздавить режим Кастро на Кубе, а динозавры-сталинисты в СССР были уверены, что Хрущев сделал слишком много уступок американцам.

Но как бы там ни было, хотя ни Кеннеди, ни Хрущева вскоре у рулей управления сверхдержавами уже не стало, достигнутые ими договоренности все же продолжали работать. И никаких попыток вторжения из США на Кубу с тех пор больше не было. Смещая фокус этой истории с Карибского моря на Черное, довольно трудно не заметить своеобразную иронию повтора событий в обратную сторону.

Однажды Сын Неба отрезал Крым от России, затем Сыну Неба отказали в НАТО, а у Кубы в хлам испортились отношения с США. Спустя полвека другому Сыну Неба вновь отказали в НАТО, но затем он вернул Крым в Россию, а у Кубы начали налаживаться отношения с США… Ключевая же идея в этой интересной череде событий заключается в том, что Крым как был изначально, так и остался в России. И теперь уже крайне маловероятно, что какой-нибудь еще Сын Неба захочет этот факт изменить. Ну а еще более маловероятно, что на такой исторический итог хоть как-то смогут повлиять власти Кубы, Украины или каких-либо еще ГГ…

Тема «К»: Криптография

В тот же самый 1962 год, когда едва не разразилась катастрофа термоядерной войны, произошло одно очень тихое, совсем незаметное и практически никому неведомое событие. Однако некоторым весьма нетривиальным образом этот эпизод тоже отмечен как немаловажный в главе о «Днях Кризиса» книги Стивена Будянски про незримые войны спецслужб в годы Холодной войны. И более того, глубокая суть эпизода по-прежнему чрезвычайно актуальна и сегодня.

Собственно событием этим был доклад отставного ветерана АНБ Уильяма Фридмана, сделанный им на заседании Американского философского общества и носивший название «Шекспир, тайная разведка и государство». Формально историко-литературный доклад был посвящен делам отдаленной эпохи: некоторым секретным методам шпионажа, характерным для работы государственной Почты Британии в ранние годы правления династии Тюдоров. Несмотря на столь далекую, казалось бы, от современности тему, выступление Фридмана вызвало острое недовольство и раздражение у его бывших начальников в АНБ США. Но чтобы понять суть конфликта, надо немного углубиться в детали доклада и его предыстории.

В качестве начала для своего исследования Фридман выбрал следующую строчку из исторической хроники Шекспира «Генрих V»:

О заговоре королю известно, –
Их письма удалось перехватить…

Ну а далее специалист в развернутой форме и на исторических примерах показывает, сколь полезным и эффективным делом может быть для властей чтение секретной переписки всех – как оппонентов, так и союзников. Однако в заключение доклада профессиональный криптограф-аналитик, посвятивший всю свою жизнь чтению чужих писем, произносит вот какие неожиданные слова:

Имел ли Шекспир какое-то личное мнение относительно этичности перехвата корреспонденции, относительно сбора тайно собираемых таким образом разведданных, и относительно использования этих сведений для ведения общественных дел? Интересно было бы это знать.

Понимал ли он, насколько сложно соединять такого рода действия с демократическими идеалами свободного и открытого общества? Которое предпочитало бы, чтобы его правительство вело все свои внутренние дела настолько открыто, насколько это вообще возможно. А также, чтобы и все внешние или иностранные дела велись в подобной открытой манере.

И вообще, насколько далеко открытое ведение общественных дел может быть совместимо с национальной безопасностью демократического государства? Было бы очень интересно узнать, какими могли быть ответы Шекспира на такого рода вопросы…

Из столь неожиданного финала к исследованию монархий крайне давней эпохи несложно понять, что на самом деле Фридман в аллегорической форме говорил о чем-то своем, глубоко личном и наболевшем. Более того, историкам спецслужб ныне в подробностях известно, как именно и в какой конкретно форме «отец американской криптологии» Уильям Фридман был сильно унижен и оскорблен Глубоким Государством США.

Дабы очень большую и замысловатую историю изложить тут совсем вкратце (важнейшие подробности можно найти в разделе «*Дополнительное чтение*»), достаточно упомянуть лишь такие факты. В 1950-е годы именно Фридман был ключевой фигурой в суперсекретной операции АНБ, обеспечившей американской разведке «тайные бэкдоры» (как это назвали бы сейчас) в огромном количестве шифраторов, используемых множеством самых разных государств по всему миру. Причем без разницы, являлись ли власти этих государств противниками или союзниками США. Ну а неофициальное название у этого гранд-успеха шпионов по некоторым причинам звучало как «операция BORIS» (ибо американского криптографа связывала личная дружба с крупнейшим поставщиком шифраторов Борисом Хагелином).

Лично же для Фридмана столь блестящее достижение его спецслужбы быстро вылилось в глубокую личную драму. Вскоре после очередной служебной командировки в Швейцарию (где он обеспечивал договоренности по бэкдорам с изготовителями шифр-техники), в августе 1958 года Фридман написал личное письмо Говарду Энгстрому, который в тот момент только-только покинул высокий пост заместителя директора АНБ. И конкретно о рассматриваемой здесь спец-операции в письме имелись такие интересные пассажи:

> *«Также я должен вам сообщить – не зная толком, со смехом или со слезами – что наш Сэмми [тогдашний директор АНБ Джон Сэмфорд] донес до меня в предельно ясной форме, что он более не желает, чтобы я писал хоть что-то нашему другу Борису. Ничего за исключением чисто социально-бытовых тем. Собственно же вещь теперь находится в руках сами-знаете-кого и он полагает, что мы (включая в особенности меня лично) отныне не должны иметь со всем этим делом абсолютно ничего общего. И я вот начинаю удивляться, в связи со всем этим проектом, а чья тут собственно корова-то? В чьих интересах весь этот проект идет столь успешно?»*

Историкам криптографии и спецслужб, что любопытно, по сию пору так и не удалось достоверно установить, кого именно в письме именуют «сами-знаете-кто». Но зато отлично известно, что за события происходили вскоре после отправки этого послания. Руководство АНБ решило не просто полностью отстранить Фридмана от дел, но и в грубой форме – прислав на дом команду «чистильщиков» – конфисковало все его личные архивы. Не насовсем, конечно, а лишь для выявления, изъятия и засекречивания особо чувствительных к разглашению документов…

После этой истории понятно, наверное, что все оставшиеся десять лет своей жизни Уильям Фридман провел в тяжких размышлениях – что же за монстра он собственными руками помогал выращивать в своей стране, славившейся давними демократическими традициями и свободами…

Эпилог: в чем же У-Р-О-К?

В 2014 году, т. е. задолго до начала последней президентской гонки в США, американский профессор-политолог Майкл Гленнон из Университета Tufts опубликовал большое, объемом почти с книгу, аналитическое исследование под названием «*Национальная безопасность и Двойное Правительство*» (National Security and Double Government, by Michael Glennon, PDF).

Цель исследования Гленнона – дать ответ на такой важнейший вопрос. Принимая во внимание, что Барак Обама получил широкую поддержку избирателей и пришел к власти благодаря мощной критике в адрес политики Буша и его администрации, как могло получиться так, что национальная политика США все равно осталась той же самой? Хотя вместо прежнего президента в Белый Дом пришел совсем другой человек, поначалу многократно и красочно обещавший фундаментальные перемены в этой политике…

Во множестве собранные Гленноном документы и свидетельства показывают, что традиционные институты демократической власти в США – Конгресс, президент и суды – в реальности давно подорваны и не работают. На самом же деле эффективно тут работает, как её называет Гленнон, «трумэновская сеть» бюрократов, которая и образует невидимое государство национальной безопасности. Ну а самое главное, автор показывает, что дальнейшее оставление политики безопасности в руках трумэновской сети очень серьезно угрожает традиционным американским свободам и демократической форме правления – ведя прямиком к тоталитарным порядкам.

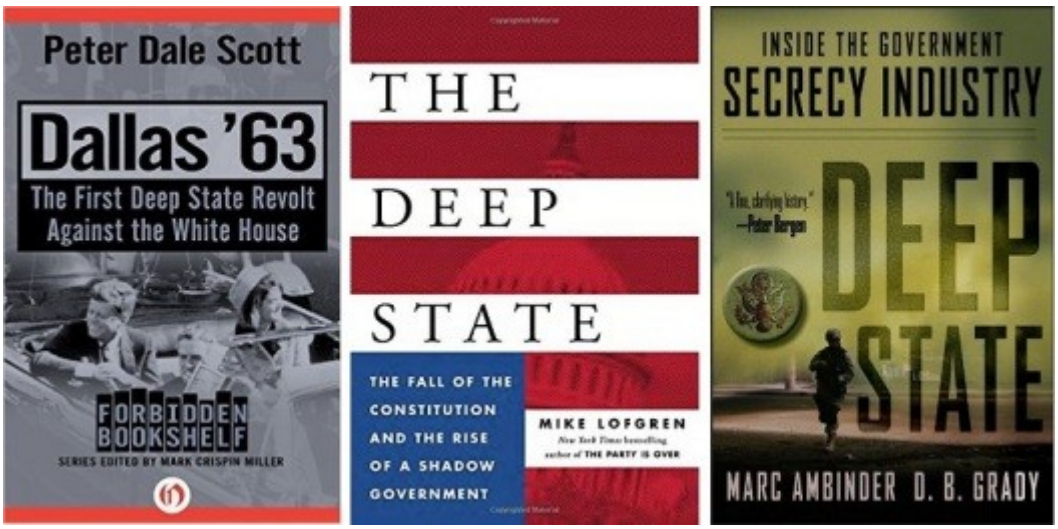
В связи с этими выводами никак нельзя не вспомнить давние предупреждения от Дуайта Эйзенхауэра, как президента США, непосредственно сменившего в Белом Доме Гарри Трумэна и унаследовавшего уже работающую «систему». В 1961, покидая свой

высокий пост и передавая бразды правления молодому-энергичному Джону Кеннеди, в обращении к нации Эйзенхауэр произнес такие слова:

> *[За годы Второй мировой, Корейской и Холодной войны] Мы были вынуждены создать постоянную индустрию вооружений гигантских масштабов. Связка гигантских вооруженных сил и огромной индустрии вооружений представляет собой нечто новое в опыте Америки. Суммарное воздействие этого – экономическое, политическое, даже духовное – ощущается в каждом городе, в каждом доме Штатов, в каждом ведомстве федерального правительства. Мы признаем, что так было нужно. Однако, мы не должны упускать из виду и серьезнейшие последствия этого для самих основ нашего общества.*
>
> *В правительстве мы должны препятствовать обретению того недопустимого влияния, которого добивается военно-промышленный комплекс. Потому что потенциал для погибельного роста этой неприемлемой силы существует и будет сохраняться в дальнейшем. Мы никогда не должны позволить, чтобы давление этого союза стало угрожать нашим свободам или демократическим процессам. Нам ничего не следует брать на веру. Только бдительное и хорошо осведомленное гражданское общество может обеспечить, чтобы безопасность и свобода могли процветать совместно…*

Дабы наглядно увидеть и понять, до какой степени и американский народ, и всё мировое содружество наций проигнорировали это предупреждение тогда и продолжают игнорировать ныне, достаточно для начала просто ознакомиться с официальной точкой зрения на убийство президента Джона Ф. Кеннеди в 1963 году – хотя бы в общедоступной Википедии.

А затем – для сравнения – внимательно прочитать о том же из достоверных свидетельств, которые за много десятилетий анализа и поисков собрали независимые исследователи. Библиотека из этих книг наберется огромная, но вот как – для примера – выглядят названия наиболее свежих исследовательских работ в тему.



- Питер Д. Скотт (2015), «*Даллас '63: Первый бунт Глубокого Государства против Белого Дома*»;
- Майк Лофгрен (2016), «*Глубокое Государство: Упадок Конституции и восход Теневого правительства*»;
- М.Эмбиндер и Д.Б. Грейди (2013), «*Глубокое Государство: Внутри индустрии правительственной секретности*».

Из этих и множества им подобных книг несложно увидеть, что проблема ГГ присутствовала в обществе всегда, но только как тема, которую в открытом обсуждении старались всячески избегать. И лишь нежданное появление Дональда Трампа в Белом Доме запустило давно употребляемый термин в заголовки центральных газет.

Нынешний президент США – это, конечно, совсем-совсем не Джон Ф. Кеннеди. Да и в России нынешний Сын Неба мало чем похож на Хрущева. Однако застарелых споров и конфликтов в отношениях между нашими странами остается ничуть не меньше, чем полстолетия назад. И коль скоро разруливать их по-любому надо, для всех должно быть только лучше, если бы при рассмотрении любой политической проблемы всегда принималось во внимание не только то, что на поверхности, но и мотивы-принципы-механизмы Глубокого Государства.

Естественно, речь идет о ГГ как в той, так и в другой сверхдержаве. Да и во всех остальных странах тоже. Иначе же никто и ничего тут просто не поймет в происходящем.

# # #

Дополнительное чтение в тему

О темных делах международной сети Глубокого Государства при организации прослушивания мобильной связи: «**Серийные самоубийцы**»; «**Вопросы на греческом**»

О жестком подавлении документального ТВ-сериала Би-Би-Си про деятельность ГГ в Великобритании: «**Правда о тайном правительстве**»

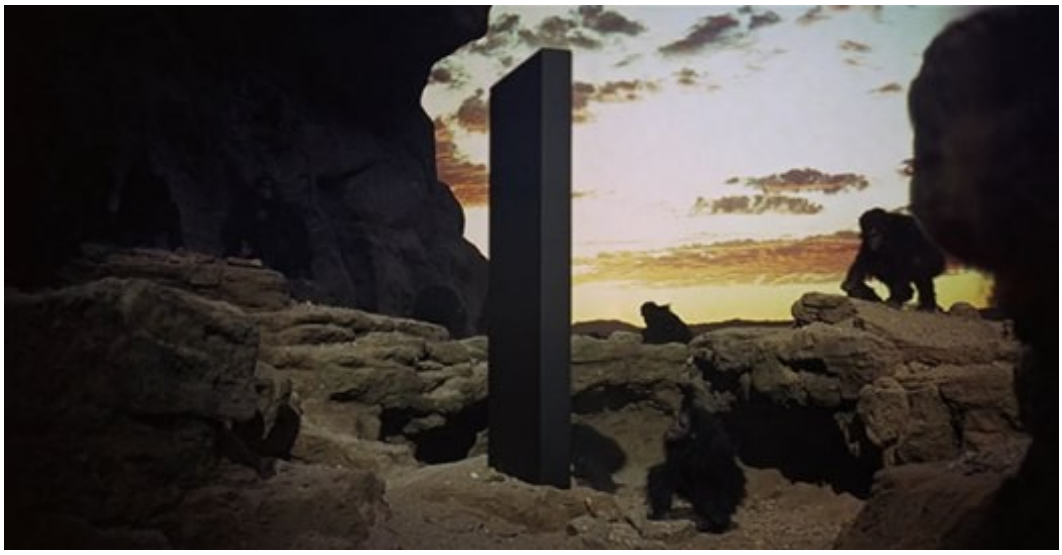
О своеобразном проявлении Глубокого Государства в США при синхронном запуске обсуждения BitCoin во всех трех ветвях государственной власти: «**Биткойн как знак перемен**»

Подробности о причудливых эпизодах и тайнах в биографии отца американской криптологии Уильяма Фридмана: «**Чтение между строк**», «**Шизо-криптография**», «**Выпиливание реальности**»

Криптография как универсальная модель для науки

(*Май 2019, idb*)

О том, почему для лучшего понимания настоящего и будущего полезно внимательно смотреть в прошлое. И о том, каковы взаимосвязи между проблемами фундаментальной науки, взломом черных ящиков и гражданским неповиновением ученых.



Несколько дней тому назад в блоге Брюса Шнайера, видного эксперта по проблемам безопасности и защиты информации, а также автора множества популярных книг на столь актуальную тему, появилась запись под таким названием: «*Почему криптографам отказывают во въезде в США?*» . Хотя суть проблемы, поднятой в публикации, довольна проста, причины происходящего остаются для народа совершенно неясными и вызывают всеобщее недоумение.

Для начала, естественно, надо пояснить простую суть.

В марте нынешнего года всемирно известному криптографу, профессору Ади Шамиру не дали американскую визу для очередного посещения RSA Conference, одного из крупнейших мероприятий мировой индустрии инфобезопасности, ежегодно проводимого в Сан-Франциско. Мало сказать, что первая буква фамилии ученого, Shamir, это «S» в названии как криптоалгоритма RSA, так и одноименной компании, устраивающей мероприятие. Помимо этого, Шамир является гражданином Израиля, ближайшего военно-политического союзника США. Сей факт также заслуживает подчеркивания.

Потому что теперь, в мае 2019, аналогичная история приключилась с другим известнейшим криптографом Россом Андерсоном, являющимся гражданином Великобритании. То есть другого главного союзника США на мировой арене. Кембриджский профессор Андерсон планировал слетать в Вашингтон для участия в торжественной

церемонии по поводу вручений – и ему самому в том числе – очередной почетной награды от сообщества инфобезопасности. Однако, как и Шамир чуть ранее, ученый не получил от американских властей визу, необходимую британцам даже для краткосрочных посещений страны.

Сообщая об этих странных новостях, Брюс Шнайер попутно отмечает, что наслышан еще о двух, как минимум, видных криптографах, которые оказались ныне точно в такой же ситуации. Причин для отказа в визе (точнее, для бесконечного затягивания процедуры без официального отказа) никто ученым не объясняет, но создается такое впечатление, что появился некий «черный список» тех криптографов, присутствие которых власти США считают в своей стране нежелательным…

Никаких достоверных сведений или документов, разъясняющих причины и механизмы происходящего, у озадаченного криптографического народа на сегодняшний день нет. Поэтому в комментариях – помимо печальных сетований и едких ругательств в адрес госбюрократов – звучат одни лишь слухи и домыслы.

Но что характерно, практически никто не предлагает оглянуться на сравнительно недавнее прошлое – и вполне отчетливо там увидеть, что всё это уже было, было. Причем происходило это также с известнейшими учёными и в том же самом государстве США. И происходило не без причин, естественно…

#

В начале 1950-х годов, в самый разгар Холодной войны и эпохи маккартизма, за просоветские или просто за левые-независимые взгляды в США серьезным репрессиям подвергались, как известно, не только госслужащие, деятели культуры или журналисты, но и многие ученые, включая знаменитых. Среди наиболее памятных сюжетов на данный счет можно отметить истории злоключений американских физиков-ядерщиков Роберта Оппенгеймера и Дэвида Бома, а с британской стороны – истории об отказе в американской визе для отца квантовой физики и нобелевского лауреата Поля Дирака или о превращении в «невыездного» гениального математика Алана Тьюринга.

Содержательные подробности обо всех этих эпизодах можно найти в материале «*Бунт ученого*», здесь же особо отметить следует два других момента – прямо связанных с отчетливыми историческими параллелями между прошлым и настоящим. Точнее, между историями физиков-математиков прошлого и компьютерщиков-криптографов настоящего.

Момент первый – это тесное переплетение темы давления на ученых с темами национальной безопасности и шпионажа в интересах врагов. В 1950-е годы, в угаре борьбы с «атомным шпионажем», были казнены на электрическом стуле супруги Этель и Юлиус Розенберги. На сегодняшний день уже достоверно известно, что это была акция устрашения. Ибо казнили Розенбергов не столько за тяжесть их преступления,

сколько в назидание остальным – за их решительный отказ признать вину и сотрудничать со следствием.

Примерно за то же самое – отказ каяться, называть имена «неблагонадежных» и давать показания против своих коллег – выдающийся физик Дэвид Бом в те же годы был жестко наказан вообще без признаков каких-либо преступлений. Для начала его отправили в тюрьму за неуважение к следствию, разбиравшемуся с «анти-американскими» взглядами ученого на политику, а затем тут же уволили из университета и лишили возможности работать по специальности – как на родине, так и в Британии. Когда же ученый нашел работу в Бразилии и получил бразильское гражданство для свободы передвижений по миру, Бому аннулировали его американский паспорт и лишили гражданства США.

Ныне на дворе год 2019, или иначе, шесть лет спустя после знаменитых разоблачений от «государственного хакера» Эдварда Сноудена (которому власти США тоже первым делом аннулировали американский паспорт, чтобы заблокировать перемещения по миру). Благодаря России, Сноудену посчастливилось остаться на свободе, однако повезло так далеко не всем. Заметно обострившаяся за последние месяцы, глобальная война американской администрации с многочисленными «хакерами как шпионами» привела к тому, что за решеткой ныне оказались и Джулиан Ассанж, и уже в который раз Челси Мэннинг. То есть те, кто с опорой на интернет дали первые примеры массового раскрытия темных государственных тайн в интересах информирования и оздоровления общества.

Ассанжа пока держат в Британии, однако власти США решительно настроены добиться экстрадиции смутьяна-австралийца. Чтобы уже самим и по полной программе расправиться с журналистом и хакером как с особо опасным и вредоносным шпионом.

Ну а Челси Мэннинг под это дело снова угодила за решетку в точности по той же траектории, как когда-то Дэвид Бом. Как узник совести, исключительно из-за своего принципиального отказа давать показания судебным инстанциям – в данном случае, против Ассанжа и WikiLeaks.

Другой важный момент в исторических параллелях – это настойчивое пригибание тех строптивых ученых, кто не согласен с политикой государства в области управления наукой. Совсем не секрет, что после окончания второй мировой войны влияние военно-промышленного комплекса и спецслужб США на развитие национальной науки не только не ослабло, а напротив, многократно усилилось. Практически во всех главных областях научной работы заниматься распределением финансовых средств и диктовать приоритетные направления для исследований стали так называемые «администраторы», представляющие интересы военных, разведки, прочих силовиков и тесно связанной с ними индустрии.

Как естественное следствие этого, в научном мире мощно закрепился и стал быстро нарастать обширный пласт «секретной науки», о результатах и достижениях которой всем прочим, не имеющим допусков, было знать «не положено». Конечно же, очень многим из настоящих ученых подобные перемены сильно не понравились. Однако открыто выступать против новых порядков и «научных администраторов» – ставя этим под угрозу собственную карьеру и материальное благополучие – решались очень и очень немногие.

Что примечательно, среди знаменитых физиков не нашлось тогда практически никого, кто открыто и активно не согласился бы с новыми порядками. Наиболее же яркие – и при этом отчетливо разные – примеры научного неповиновения государству дали в ту пору два особо выдающихся ученых-компьютерщика: отец кибернетики Норберт Винер и отец теории информации Клод Шеннон.

Один из них, Винер, по сути первым дал сигналы об очень нехороших тенденциях и уже в 1947 году выступил с публичным «манифестом восстания» (как назовут это в прессе) – не только объявив об отказе сотрудничать с милитаристами в их секретной «науке мегабаксов» (как назвал это ученый), но и призвав всех остальных коллег последовать его примеру. Другой же великий ученый, Шеннон, не делал никаких громких заявлений, но просто последовал призыву Винера. Полностью оставив большую, щедро финансируемую государством науку, перейдя на тихую преподавательскую деятельность и занявшись интересными лично для него научными исследованиями в собственной домашней лаборатории…

Подробнее о неординарных эпизодах в жизни Винера, Шеннона и других зачинателей компьютерной эпохи можно прочесть в материалах «*Тайны внутри секретов*» и «*Хакинг реальности*». Здесь же остается лишь с грустью констатировать, что отважные инициативы этих ученых мировое научное сообщество не поддержало тогда абсолютно никак. И если в США по сути полное контролирование государством националь-

ной науки в интересах военных и нацбезопасности стало несомненным уже к середине 1960-х годов, то аналогичная картина для Европы и прочих регионов планеты стала фактом научной жизни примерно в начале 1970-х.

#

Но самое интересное тут, однако, что всего через несколько лет – в середине 70-х – произошло великое научное чудо, грандиозные последствия которого для всей истории нашей культуры и прогресса не поняты и не осмыслены человечеством как следует вплоть до нынешнего дня. Чудом таким стало рождение существенно новой, изначально свободной от государства науки, получившей название «открытая криптография». Причем рождение это – как и положено делам чудесным – сопровождали обстоятельства воистину удивительные и мистические.

Фактически одновременно и сразу во множестве разных мест у незнакомых друг с другом людей появилась крайне необычная концепция «несекретного шифрования», иначе именуемая «криптография с открытым ключом» и прежде считавшаяся делом просто невозможным в принципе. На протяжении веков и тысячелетий все сведущие люди знали, что для конфиденциального зашифрованного общения двух сторон они непременно должны обладать общим секретом – ключом шифрования.

Теперь же вместе с новым открытием вдруг выяснилось, что все эти традиционные представления человека о шифрах и тайнах являются в корне неверными. И на самом деле всё тут обстоит существенно иначе. То есть надежно зашифрованная связь между двумя совершенно незнакомыми сторонами, никогда прежде не имевшими общих секретов, оказывается не только возможна в принципе, но и способна отлично работать на практике.

В научной сердцевине открытия оказалась идея об Асимметричных – то есть существенно разных – ключах для зашифрования и расшифрования послания. Все же прежние представления о защите информации базировались на идее Симметричного ключа – когда ключ для зашифрования и расшифрования строго один и тот же. О том, почему подобный взгляд – со сменой симметричных подходов на асимметричные – чрезвычайно полезен для прогресса не только в криптографии, но и во всех науках вообще, удобнее пояснить ближе к финалу. Здесь же сосредоточимся лишь конкретно на асимметричных событиях недавней истории.

#

Итак, концепция криптографии с открытым ключом родилась по сути одновременно в Британии, в стенах секретной спецслужбы GCHQ, и в университетах США среди молодых ученых-компьютерщиков, никак с государственными криптослужбами не связанными (колоритные детали этой истории см. в тексте «*Параллельные миры*»). Глав-

ная и принципиальная разница в последствиях от этих синхронных открытий была в следующем.

Хотя в АНБ США и прочих англоязычных спецслужбах-партнерах новые удивительные методы шифрования от британцев были восприняты профессионалами с интересом и энтузиазмом, далее их тут же и строго засекретили – как еще одну перспективную крипторазработку на будущее. Так что весь остальной мир не только не узнал от GCHQ ничего нового, но вообще ведать не ведал про это замечательное открытие секретной науки еще четверть века.

Что же касается академического сообщества, то здесь независимо сделанные открытия от Диффи, Хеллмана, Меркля, Райвеста, Шамира и Эдлмана произвели воистину фурор и революцию. Породив не только внушительный поток открытых криптографических исследований и учебные курсы по криптографии/защите информации в университетах, но и вообще став предметом особой гордости академических ученых. Ибо прежде криптография по традиции была занятием сугубо секретным, в университетах этому делу не учили, но все мало-мальски сведущие люди и так достоверно знали, что ничего, хоть как-то похожего на алгоритмы Диффи-Хеллмана и RSA, никогда в области защиты информации просто не существовало.

Иначе говоря, новая наука открытая криптография буквально с момента рождения начала опираться в первую очередь на сугубо собственные разработки. Да еще на те обрывочные сведения, что были известны «из прошлого и будущего», выражаясь образно. То есть из книг-статей о криптографической истории, с одной стороны, и из футуристических трудов, со стороны другой, от двух отцов компьютерной науки – Клода Шеннона и Норберта Винера, опережавших своё время как минимум на четверть века.

Благодаря Шеннону, знаменитому не только как отец теории информации, но и отец научной криптографии, открытая крипто-наука фактически с первых дней стала работать с двоичными битами, вполне отчетливо представляя себе, сколь тесно и неразрывно – через двоичные коды – переплетены друг с другом защита коммуникаций от искажений и защита информации от доступа противника. Что же касается наследия Норберта Винера и тихо увядшей после его смерти науки кибернетики, то революционные идеи этого ученого – о важности обратной связи и о компьютерных системах с поведением живых организмов – обретут особую ценность для проблем криптографического анализа несколько позже.

А поначалу важнейшей проблемой для открытой криптографии стало активное противодействие секретных спецслужб, в первую очередь, со стороны Агентства национальной безопасности США. Государственные органы, компетентные в делах радиоэлектронного шпионажа и защиты информации, абсолютно не желали, чтобы профессиональные знания на этот счет распространялись свободно и без их жесткого контроля. Поэтому ко всем энтузиастам, изобретателям и исследователям из мира академи-

ческой науки стали применять разнообразные меры воздействия и давления, направленные на то, чтобы «загнать криптографического джинна обратно в бутылку».

Но поскольку и люди в науке, и времена в политике тогда уже были сильно другие (уотергейтский скандал и бесславный конец завравшегося президента Никсона, еще более бесславный конец вьетнамской войны, масштабное расследование противозаконных операций спецслужб и так далее), абсолютно ничего из затей АНБ против открытой криптографии тогда не вышло. Ни нагнуть всех к безропотному подчинению, ни даже продавить лидеров на тайное сотрудничество у государства не получилось ни физически, ни морально.

Так что далее «научным администраторам» пришлось учиться жить и работать в условиях новой реальности. Параллельно с новой открытой наукой, не только быстро и постоянно наращивающей компетентность, но и самостоятельно переоткрывающей и развивающей для всех те секретные вещи, которыми когда-то безраздельно владели исключительно в элитной науке государственных тайн.

#

Среди множества важных достижений и (пере-)открытий, самостоятельно сделанных учеными академического сообщества в 1980-е годы, особо отметить здесь следует два. В 1985 голландец Вим ван Экк опубликовал первую в открытой науке работу о компрометирующих побочных излучениях электронной аппаратуры – чем невольно раскрыл страшную тайну спецслужб, обобщенно именуемую кодовым словом Tempest. А в самом конце 1980-х израильтяне Ади Шамир и Эли Бихам придумали и развили чрезвычайно эффективный общий метод для вскрытия шифров, получивший от авторов не самое удачное название «дифференциальный криптоанализ». Спустя годы станет известно, что и этот мощный инструмент у секретных аналитиков и шпионов государства тоже давно имелся – под другим кодовым названием и исключительно для себя, конечно же.

Ну а на совершенно особое для истории десятилетие 1990-х пришелся и самый, пожалуй, насыщенный интересными-драматичными эпизодами комплекс событий в криптографической науке. Да и во всей науке человечества в целом, если научиться смотреть пошире.

Дабы суть гигантской картины перемен была ясна и в её самом сжатом виде, имеет смысл выбрать три наиболее характерных эпизода крипто-десятилетия.

Во-первых, это персональные компьютеры и начало массового распространения интернета как принципиально новой, простой и удобной формы цифровых коммуникаций. И в теснейшей взаимосвязи с этим – появление свободно доступной для всех и реально очень качественной программы шифрования PGP от Фила Зиммермана. Для народа «Весьма приличная приватность» стала своего рода нежданным бесплатным

подарком от профессионального программиста и криптографа-любителя, тщательно сконструировавшего свой криптопродукт на основе самых лучших достижений открытой криптографии.

Ну а для государственных спецслужб программа PGP стала своего рода фокусной точкой и символом всего того, что следует любыми способами давить и выкорчевывать. Символом реально сильных знаний и технологий, распространяемых свободно для всех и полностью без контроля со стороны государства. Которое нутром и инстинктами ощущает, что подобного рода процессы угрожают важнейшим основам самого его существования.

Поэтому, конечно же, с программами типа PGP государство развернуло «криптографические войны», попытавшись в новых условиях возродить дух Холодной войны, начать жесткое судебное преследование независимых криптографов вроде Зиммермана и поставить под свой контроль общедоступные средства шифрования. Однако, в условиях развалившегося СССР и отсутствия на мировой арене другого «мирового пугала», абсолютно ничего похожего на контроль открытой криптографии и тут у государства не получилось.

Во-вторых, существенно другим и тоже важнейшим крипто-событием десятилетия стало замечательное открытие Питера Шора, придумавшего квантовый алгоритм для быстрой факторизации – то есть для разложения на множители – очень больших чисел. На огромной вычислительной сложности этой задачи в условиях компьютеров обычных, как известно, выстроена вся криптографическая стойкость криптоалгоритма RSA. Ну а в условиях гипотетического квантового компьютера, как показал Питер Шор, появляется удобная возможность опробовать все варианты сомножителей в параллели и одновременно, что приводит, соответственно, к быстрому и эффективному вскрытию RSA. В теории, по крайней мере.

На практике же всё сложилось так, что алгоритм Шора стал и первым, и сразу очень интересным в своих приложениях квантовым алгоритмом. Таким алгоритмом, который перевел всю область квантовых вычислений из плоскости абстрактно-теоретических рассуждений об общей привлекательности метода в плоскость новой технологии, предоставляющей совершенно конкретные и значительные преимущества в сравнении с теми компьютерами, что имеются ныне.

По сути дела, именно благодаря алгоритму Шора направление квантовых компьютеров получило очень мощный стимул к практическому развитию и освоению – сначала в лабораториях, а ныне и в коммерческой сфере. Но самое главное, что практические достижения ученых в освоении манипуляций хрупкими квантовыми состояниями материи в итоге привели исследователей к весьма неожиданному выводу. По всему выходит так, что и природа на своих самых глубинных уровнях действует как невообразимо огромный и в высшей степени надежный квантовый компьютер…

В-третьих, наконец, еще одним чрезвычайно важным научным достижением криптографии в 1990-х годах стали существенно новые подходы ко вскрытию «черных ящиков». Новые до такой степени, что принципиально изменилось и само понимание весьма давней концепции «черный ящик».

Если вы посмотрите в словарях определения этого понятия, общего и традиционного для многих областей науки, начиная с квантовой физики и вплоть до поведенческой психологии, то суть там вкратце такова. Изучается неведомый в своем устройстве объект, имеющий нечто на входе и выдающий нечто на выходе. Информация о содержимом на входе и выходе в том или ином объеме считается доступной и поддаётся измерениям-сопоставлениям. Однако внутреннее устройство черного ящика остается неизвестным, поэтому все объекты, дающие один и тот же выход при одинаковых сигналах на входе, считаются эквивалентными.

Иначе говоря, неважно, что там у ящика внутри, важна лишь формула, наилучшим образом соотносящая вход и выход. Вполне возможно, что когда-то это была хорошая концепция, помогавшая открыть ученым немало важных и полезных вещей в делах формального описания «черных ящиков». Но с таким подходом наука сама себя искусственно ограничивает, даже не задаваясь вопросами о внутренних механизмах и жизни устройства.

А вот если вопросами такими начать задаваться и, более того, считать конкретно изучаемый «черный ящик» в некотором роде живым организмом – с собственной историей рождения, с собственным специфическим метаболизмом и индивидуальными особенностями функционирования – то можно, оказывается, узнать тут и несравненно больше с точки зрения «анализа и взлома». Вплоть до восстановления общего устройства и главных рабочих параметров системы…

Именно такой – существенно новый – подход к анализу шифрсистем и появился в открытой криптографии к середине 1990-х годов. Как это обычно бывает, мощная новаторская идея возникла сразу во множестве мест, причем главным образом среди молодых-пытливых хакеров, активно экспериментировавших со взломом криптозащиты в системах платного телевидения. В солидной же академической криптографии новый подход ко вскрытию черных ящиков появился благодаря Полу Кочеру. Поначалу тоже хакеру-взломщику компьютерного андеграунда, но в конечном итоге – грамотному специалисту с хорошим университетским образованием.

Причем особо следует отметить, что свой первый диплом по специальности Кочер получил в области биологии. Такой поворот событий в некотором смысле обеспечил возврат крипто-компьютерной науки к кибернетическим идеям Норберта Винера – о взглядах на электронную технику как на живой организм и о важности систем обратной связи.

Профессиональные навыки Кочера как биолога не могли не сказаться и на его хакерских подходах к решению задач криптоанализа. Всякая криптосхема в конечном счете имеет конкретную физическую реализацию, а любое такое физическое устройство – как и живой организм – имеет не только формальный вход и выход, но и множество других параметров жизнедеятельности, поддающихся исследованиям и измерениям. Таких, в частности, параметров, как время реакций на разные внешние сигналы. Или, скажем, перемены в потреблении питания при выполнении разных внутренних функций.

В целой серии публикаций, получивших мощный резонанс в криптографическом сообществе, Кочер и его коллеги продемонстрировали комплекс существенно новых и чрезвычайно эффективных методов для извлечения криптоключей из «черных ящиков» шифровальных устройств. Все эти методы, получившие названия типа «таймерная атака» или «дифференциальный анализ питания», были своего рода развитием уже известной темы о побочных компрометирующих сигналах. Революционная суть новых работ была в том, что «биологический» подход к криптоанализу черных ящиков оказался не только весьма дешевым и эффективным, но и органично включал в себя активный компонент – когда исследователь для решения своих задач может нужным образом влиять не только на формальный внешний вход, но и на внутренний «метаболизм» системы.

Среди великого множества интересных работ и исследований, порожденных новым подходом, можно отметить, в частности, такие. Тогда же, в середине 90-х, Ади Шамир и Эли Бихам опубликовали примечательную статью «Дифференциальный анализ сбоев», где по сути дела объединили свой фирменный метод «чистого математического анализа» с хакерскими приемами взломщиков криптосхем, искусственно порождающих в устройстве те или иные сбои для извлечения из него битов криптоключей. Как показали израильтяне, при грамотном сочетании этих методов возможно не только эффективное извлечение ключей из криптосхем известных, но также и восстановление криптосхем в «черных ящиках» неизвестной конструкции.

Другой важной вехой того же периода стала Компьютерная лаборатория Кембриджского университета, которую возглавил Росс Андерсон. Благодаря Андерсону и его научным сотрудникам-хакерам эта лаборатория стала одним из важнейших для открытой криптографии центров, занимающихся весьма продвинутыми экспериментальными исследованиями в области анализа и взлома реальных шифрсистем…

#

Наступившие далее 2000-е годы принесли для мира открытой криптографии существенно новые проблемы и беды – как и для всего остального мира, впрочем. Под знаменем борьбы со злом «мирового терроризма» государственные спецслужбы куда более масштабно смогли продавливать на сотрудничество и ослабление инфозащиты практически всех. Не только сети инфраструктуры и изготовителей коммуникацион-

ной аппаратуры, но и производителей криптообрудования, и органы стандартизации, и даже кого-то из ученых академического сообщества криптографов.

Все эти вещи, однако, происходили в условиях глубокой государственной тайны. Сигналы от честных и компетентных специалистов, выявлявших искусственно вносимые слабости в коммерческую криптографию, время от времени появлялись, конечно же, но очень мало кто обращал на них внимание. Скандально общеизвестными и широко обсуждаемыми они вдруг стали лишь в 2013 году, благодаря Эдварду Сноудену и множеству топ-секретных файлов АНБ, раскрытых им для информирования общества о масштабах происходящего.

Но скандалы приходят и уходят, как известно, а государственные спецслужбы остаются – причем такими же, как они и были, обычно. Мощнейший удар по репутации, нанесенный файлами от Сноудена, так или иначе, но вполне удалось пережить. Компании ИТ-индустрии, сильно расстроенные компроматом о тайном и нелегальном сотрудничестве со спецслужбами, так или иначе удалось успокоить и вернуть к общим проектам. Даже вся как бы независимая пресса вполне успешно вновь поставлена тут под контроль и уже совершенно не интересуется ни изучением файлов от Сноудена, ни даже их нынешней судьбой (хотя изучено и опубликовано тут было не более 1 процента массива).

Единственными, по сути, кто по-прежнему активно заинтересован в подлинно сильной криптографии и в настоящей инфобезопасности для всех, остаются лишь ученые и исследователи открытого криптографического сообщества. По причине чего их наиболее видные-независимые лидеры и имеют нынешние проблемы с государством в делах перемещения между странами.

#

Финалов у этой истории должно быть два. Криптографический и общенаучный.

Для завершения темы криптографической осталось лишь рассказать, что думают и говорят по поводу происходящего сами главные герои всей этой саги .

Британский профессор Росс Андерсон, не сумевший прилететь в Вашингтон на церемонию вручения наград для авторов самых лучших книг по инфобезопасности (среди которых предсказуемо оказалась и его знаменитая среди спецов монография), выступил перед участниками мероприятия через видео-обращение. В содержательной части этого выступления, продублированной также и в блоге Кембриджской Компьютерной лаборатории, говорится о том, что как раз сейчас Андерсон готовит третье, существенно дополненное издание своей книги-бестселлера «*Инжиниринг безопасности*» (подробности об этой весьма неординарной работе см. в материале «*Искусство защиты по Андерсону*»).

Главы новой версии книги будут выкладываться в онлайн по мере их подготовки автором – для критического прочтения и комментариев читателей. Среди уже готовых фрагментов, в частности:

> *Только что выложена в онлайн глава «**Кто противник?**» . В ней собраны содержательные сведения из файлов Эда Сноудена и других подобных им документов, рассказывающих о реальных возможностях государственных спецслужб. Причем сразу в сопоставлении с тем, что мы узнали об актерах киберкриминальной сцены благодаря работе нашего Кембриджского Центра киберпреступлений. Представляется очень странным и любопытным, что по прошествии почти уже шести лет после раскрытий от Сноудена никто так и не попытался сложить вместе всё то, что нам теперь известно, в виде согласованного аналитического обзора.*

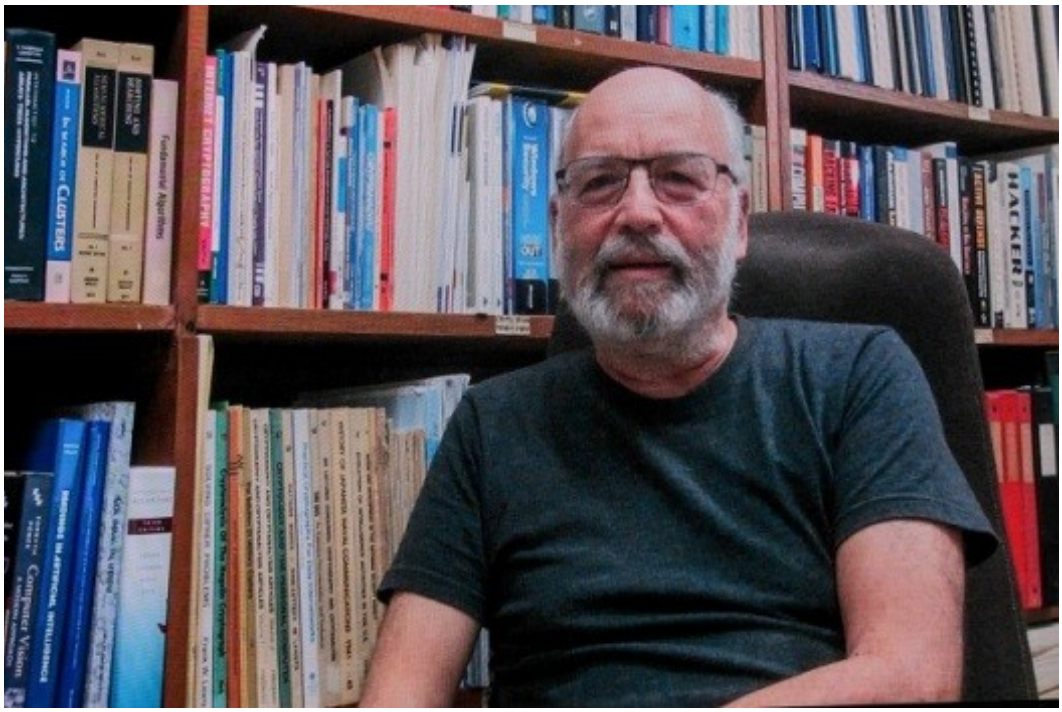
Слова Андерсона про «странно и удивительно» – это здесь, скорее всего, просто риторическая фигура. Ибо причины для отсутствия серьезных аналитических разборов «всего того, что нам теперь известно» на самом деле вовсе не удивительны. Слишком уж неприятно и пугающе выглядит открывающаяся тут для народа картина. Развернутые комментарии к этой картине можно найти в текстах «*Сноуден как повод*» и «*Всего три слайда*». Ну а если подытожить суть совсем кратко, то получается вот что.

Два существенно разных и в то же время подозрительно похожих противника для обитателей киберпространства – это две разные стороны по сути одного и того же феномена. Государственные спецслужбы очень часто крышуют киберкриминал точно так же, как это происходит у госчиновников с криминалом и хищениями в банковско-финансовой сфере или в промышленности, как это происходит с наркоторговлей и терроризмом, наконец. Всюду, где крутятся гигантские криминальные деньги, а государство абсолютно не способно с этой напастью справиться, причина, как правило,

одна и та же. Представители государства сами находятся здесь «в доле» и шкурно заинтересованы в сохранении своих доходов. Именно поэтому побороть такую преступность внутри системы просто нереально.

Но вполне можно сделать нечто иное. Не участвовать в этом самим.

Примерно об этом – только без каких-либо отсылов к криминальным аспектам происходящего – вполне внятно говорит и израильский профессор Ади Шамир. В своем видео-послании к участникам RSA-конференции, участвовать в которой американские власти ему не позволили, Шамир сказал так:



«Я являюсь членом Национальной академии наук США, иностранным членом британского Королевского общества, членом французской и израильской Академий наук. Меня награждали премией Тьюринга, научными премиями Японии, Израиля и другими многочисленными наградами. И если кто-то вроде меня не может получить туристическую визу от США для того, чтобы сделать приглашенный доклад на одной из главных конференций в нашей области – причем, похоже, и у других участников возникли такие же проблемы – то, быть может, пришла пора подумать о другом месте для проведения наших научных конференций»…

#

Ну а теперь финал общенаучный. Чему нас может научить вся эта история в её широкой ретроспективе.

По меньшей мере три важных момента должны быть тут ясными вполне.

Во-первых, на примере открытой криптографии отчетливо видно, что мощный прогресс возможен в науке абсолютно без помощи государства. Более того, даже вопреки его противодействию. По той, прежде всего, причине, что все достижения исследователей публикуются открыто и выносятся для обсуждения и развития всего научного сообщества.

Второй момент – или важнейший фактор успеха – не ограничивать себя давно утвердившимися догмами. Ибо любая догма – будь то в религии или науке – это не то, что бесспорно, потому что надежно доказано. А то, что доказать не могут, но по традиции считают воистину верным. На самом же деле это чаще всего оказывается в итоге еще одним человеческим заблуждением.

И третий момент. Во всяком деле продвижения очень полезна «асимметричная» точка зрения – как на решение проблем, так и на общее устройство системы. По давно утвердившейся традиции науку физику привыкли воспринимать как учение о Симметриях Природы. Однако симметрии важны прежде всего для стабильности и устойчивости системы, но очень мало помогают для понимания того, как система живет и движется. Для понимания же этих вещей полезно и необходимо в первую очередь выявлять главные Асимметрии системы. Именно благодаря им и происходит собственно жизнь – как движение материи, энергии, сигналов, битов информации, неважно чего, из одной точки в другую.

Нынешние расклады знаний и барьеров в науке таковы, что именно открытая криптография – с её специфическими «крипто-биологическими» подходами к анализу и вскрытию черных ящиков – предоставляет наиболее перспективный инструментарий для «взлома» и проникновения в наиболее загадочные из научных тайн. От голографии в основах материи-пространства или эволюционного конструирования биологической клетки и вплоть до механизмов и структур, связывающих эти вещи в единое разумное целое.

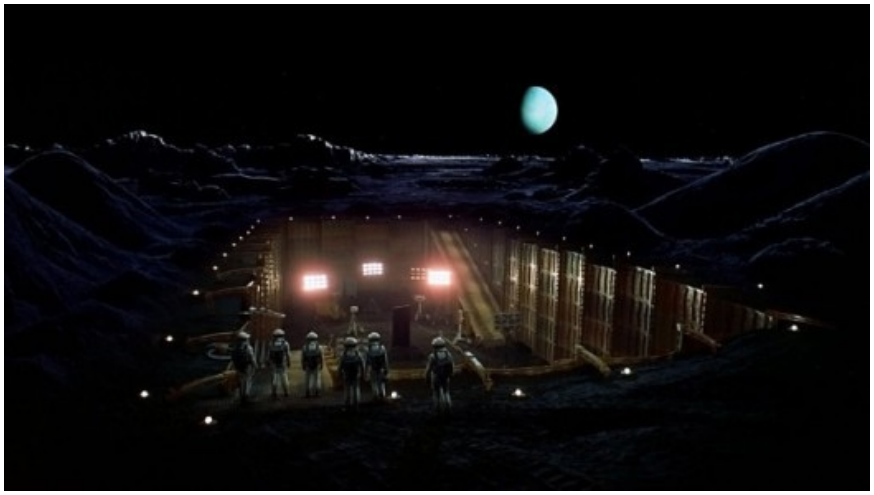
В частности, если на основе крипто-биологических подходов анализировать Асимметрии в устройстве атомов материи окружающего нас мира, то становится несложно сообразить одну простую, но очень важную вещь. Все мы – в любой точке пространства и в буквальном смысле – сидим на источнике неисчерпаемой, чистейшей и абсолютно даровой энергии. Той самой энергии в основе жизни асимметричной природы, которая бесконечно подпитывает электрические заряды частиц и обеспечивает их вечное вращение внутри атомов.

И если эта энергия постоянно идет через нас всю жизнь, то и мы вполне можем использовать её для собственных жизненных нужд – осознанно и с пользой.

Да-да, конечно, идея о принципиальной доступности и легком-практичном использовании человеком этой даровой энергии возмутительно противоречит всем догмам науки – от начал термодинамики до законов сохранения. Однако очень полезно помнить,

что практически любая догма рано или поздно оказывается суть ложь. Или помягче, очередной символ нашего непонимания природы.

Так что явно пора учиться понимать и принимать природу вообще без догм. Ибо ей для бесконечной жизни и творчества никакие из наших догм не требуются абсолютно.



# # #

Дополнительное чтение

*О широко- и мало-известных подробностях того, как в разгар Холодной войны интересы и секреты государства стали подменять саму суть науки: «**Годы когда потеряли погоду**», раздел в большом тексте «Бунт ученого»; «Гостайна как метафора».*

О гражданском неповиновении Норберат Винера и Клода Шеннона: «Тайны внутри секретов», «Он занимался хакингом реальности» .

О глубоко мистических и просто занятных обстоятельствах, сопровождавших рождение открытой криптографии: «Параллельные миры»

О крипто-исследованиях Ади Шамира в 2000-е годы: «Особенности национальной забавы», «Неслучайные случайности», «Подбит на взлете»

О научно-общественной деятельности Росса Андерсона и его примечательной книге: «Инженерия Науки», «Искусство защиты по Андерсону», «Скрепка и булавка», «Лаборатория и жизнь», «Unus Mundus»

О тесных взаимосвязях между здоровьем государства и защитой информации: «Сноуден как повод», «Всего три слайда»

Основные источники

«Why Are Cryptographers Being Denied Entry into the US?», Schneier on Security, May 17, 2019.

«RSA Conference 2019: Cryptographers' Panel Decries Adi Shamir's Visa Issues», by Tom Spring. Threatpost, March 6, 2019.

«Security Engineering: Third Edition», by Ross Anderson, Light Blue Touchpaper, May 17, 2019.

THE END