Криптография и свобода

Информация о книге

1. Название книги:
   Криптография и свобода
2. Описание целевой аудитории:
   Для широкого круга образованных читателей
3. Общий обзор книги:
   Слово криптография означает тайнопись.
   Российская криптография имеет многовековую историю, начинающуюся с указов Петра I о «черных кабинетах». До середины 80-х годов XX века криптография в России использовалась только для военных, дипломатических и правительственных линий связи и была строго засекречена. Даже употребление слов «криптография», «шифры», «ключи к шифрам» в открытых публикациях было недопустимо. Но в мире быстро назревала потребность в гражданской криптографии, стремительно развивались информационные технологии, стали появляться компьютерные сети, Интернет, денежные электронные расчеты. Для этого требовались надежные и общедоступные криптографические методы защиты информации.
   Была ли Россия готова к появлению гражданской криптографии? И да, и нет.
   Да, потому что еще с советских времен в России существовала прекрасная криптографическая школа и высококлассные специалисты-криптографы, которые долгое время на равных конкурировали с американским Агентством Национальной Безопасности и обеспечивали гарантированную защиту военных, дипломатических и правительственных линий связи.
   Нет, потому что синдром тотальной секретности всего, что касалось криптографии, восходил к сталинским временам и мало изменился за прошедшие десятилетия. А в подобных условиях очень хорошо себя чувствуют многочисленные чиновники от крипторафии.
   В 1992 году случился кризис: поток фальшивых авизо захлестнул Центральный Банк России и грозил обрушить всю финансовую систему. Потребовалась срочная помощь криптографов: в кратчайшие сроки создать, наладить и запустить в эксплуатацию систему криптографической защиты телеграфных и почтовых авизо в такой огромной структуре, как ЦБ РФ.
   Эта задача была выполнена за три месяца – неимоверно короткий срок.
   В России появился первый реальный пример гражданской криптографии.
   О том, что представляла из себя советская криптографическая школа, о ее специалистах и начальниках, о царившей тогда в стране атмосфере, о том, как была создана система защиты для Центрального Банка России, и, наконец, о том, почему же в России так трудно пробивает себе дорогу гражданская криптография – в этой книге.
4. Оглавление:

Freedom not free!

ПРЕДИСЛОВИЕ

Февраль 1993 г. Проблема фальшивых авизо в Центральном Банке России успешно решена. С 1 декабря 1992 года введена система защиты телеграфных авизо, использующая специализированный калькулятор «Электроника – МК-85 С». Калькулятор, изначально предполагавшийся для использования только в режиме шифрования, удалось приспособить для выработки некоего подобия электронной подписи авизо и тем самым гарантировать их подлинность. Сразу же стабилизировался курс рубля, а на директорате Центрального Банка Первый заместитель Председателя ЦБ Татьяна Парамонова официально заявила, что с момента введения этой системы защиты поток фальшивых авизо прекратился. Российскому государству сохранены огромные деньги…

*****

- Ты где вчера был?
- В Центральном Банке.

Начальник отдела как-то с подозрением посмотрел на меня, как будто я, пока еще действующий офицер ФАПСИ, продался врагам-конкурентам. Все, кто мешает бизнесу руководства ФАПСИ – враги. И с ними поступают по законам военного времени…

- Ты поучил новое удостоверение?
- Да, совсем недавно.
- Дай посмотреть.

Даю ему в руки свою новенькую красную книжецу с двуглавым Российским орлом. Смотрит, затем складывает и кладет к себе в карман.

- Значит так. Режим работы у тебя теперь будет такой: утром приходишь, отдаешь мне удостоверение, а в шесть вечера получаешь его обратно. И в Центральный Банк больше – ни ногой!
- Вы меня арестовываете?
- Нет, просто устанавливаю для тебя персонально особый режим работы.

Начальник отдела, в общем, неплохой человек. Сам бы он до такого никогда не додумался. Но есть начальники повыше, генералы. Их интересы в ЦБ были явно ущемлены. И кем: собственным подчиненным! Пользуясь тяжелым положением, в котором оказался ЦБ в результате неимоверного потока фальшивых чеченских авизо, они собирались навязать ЦБ кабальные условия поставки системы криптографической защиты: и по времени (два года) и по деньгам (около 2 млрд. руб. при тогдашней цене доллара примерно в 400 рублей). Вопрос о том, что это народные деньги подвергаются беззастенчивому разграблению, что затяжка на два года с поставкой системы защиты платежных документов Центробанка может привести к гиперинфляции и неимоверному обогащению криминала, их явно не волновал. Страна большая, нефти много, переживет. А ЦБ деваться некуда, ФАПСИ – единственная в то время организация, занимающаяся криптографической защитой, все специалисты – только там. Без ведома ФАПСИ никто и пикнуть не сможет. Система создавалась еще Иосифом Виссарионовичем, и с тех пор, по их мнению, ничего не изменилось. И вдруг – такой облом! Система защиты поставлена в ЦБ за два месяца, в обход начальников. Лакомный пирог упущен! Пора разобраться с теми, кто это сделал.

Но какой же примитивный метод разборки! Таков стиль работы многих российских чиновников. И объяснение очень простое – нефть, изобилие природных богатств, получаемые на этом «легкие» деньги расплодили и развратили российских чиновников. Сесть на трубу и перекрыть всем кран – вот основная цель их деятельности. И такой стиль работы переносится на криптографию, специфический раздел математики, занимающейся защитой информации. Появился спрос на криптографические алгоритмы, компьютерные программы, специализированные устройства – запретить! Приказать всем идти на поклон в ФАПСИ, а там чиновники уже решат, какой нужно отвесить поклон: в пояс или пасть в ноги. А непокорных - согнуть в бараний рог с помощью других таких же чиновников из различных налоговых, проверяющих и прочих инспекций. Это и есть реальная российская экономика.

Что делать в такой ситуации? Становится покорным вассалом, таким же чиновником, всю свою жизнь сочиняющим никому не нужные, оторванные от всякой реальной жизни распоряжения и инструкции? Тихий, спокойный способ существования, но противный. Противно убивать свое время, свою жизнь на бесполезные дела, часто приносящие просто откровенный вред другим людям. Противно ставить крест на своем образовании, на интереснейшей профессии математика-криптографа-программиста. Всю жизнь потом будет противно сознавать, что поддался слабости, уступил грубому нажиму, подчинился несправедливому решению, бросил на полдороге то, что действительно необходимо делать.

Свалить! Свалить из этого ФАПСИ, от этих начальников, от этих порядков! Пусть дальше будет трудно жить, пусть говорят, что надо было дождаться пенсии, не высовываться, не перечить начальству – все это пустое. Главное – получаешь шанс обрести то, чего никогда раньше не имел – свободы. А свобода не бывает бесплатной. Путь к обретению истинной свободы, особенно в России, с ее крепостными традициями, не может быть легким. При реальном социализме важны реальные блага: связи, протекции, чиновничьи должности, которые при переходе от социализма к капитализму (дикому) превращаются в акции, доходы, капитал, деньги. А можно ли прожить на свои знания, свою профессию без поддержки и блата? Можно ли инженеру прожить и прокормить семью не превращаясь в торговца-челнока или заурядного барыгу? Насколько соответствуют действительности все декларации о демократии в России, в изобилии сыплющиеся от разных российских политиков? Достижима ли в России реальная свобода и что это такое?

Больше десяти лет прошло с этого момента, в корне переменившего всю мою жизнь. И книга эта, в отличии от первой книги, «Практическая криптография», выпущенной издательством BHV-Петербург в 2002 году, пишется уже не в Москве, а в Южной Корее, стране, размером чуть больше Московской области, с численностью населения около трети российской, не обладающей такими несметными природными богатствами, как Россия, но достигшей такого уровня развития экономики, что южнокорейскими товарами завалены многие рынки, в том числе и российский. И я надеюсь, что если среди читателей этой книги окажутся люди, не знакомые с математикой и криптографией, то и для них найдется что-то полезное и интересное.

М.Масленников

Сеул, 2003 - 2008

4 ФАКУЛЬТЕТ

- Вот направление, во вторник пройдешь медкомиссию. Поступать-то твердо решил?
- Не знаю.
- Решай быстрее и если раздумаешь, сообщи мне. Кандидатов много, найдем другого.

Что я знал о 4 факультете Высшей Краснознаменной Школы КГБ СССР им. Ф.Э.Дзержинского в том далеком 1974 году? Практически ничего. Только то, что там очень трудно учиться, много математики, уровень подготовки сопоставим с мехматом МГУ. А еще то, что это военное учебное заведение, первые два года – казарма, придется носить военную форму, шинель и сапоги. Все, достаточно! Только казармы и сапог мне недостает для полного счастья. Все мысли направлены на то, чтобы после школы не попасть в армию, где правит «Здравствуй, дерево». Советская Армия – та сила, которая заставляет ребят браться за ум и всеми силами стремиться поступить хоть в какой-нибудь институт. Хочешь ли ты дальше учиться, какое в твоей жизни призвание, какая профессия больше нравится - все это вторично. Первично – не попасть в армию, не вычеркивать из жизни два молодых бесцельно прожитых года, не попадать в рабскую зависимость к армейским самодурам, не терпеть издевательств и унижений, не чистить по ночам зубной щеткой туалет. Даже в те годы было совершенно ясно, что всякие Максимы Перепелицы и Иваны Бровкины – не более, чем дешевая пропаганда. В реальной жизни все совсем не так, порядки в Советской Армии, дедовщина, издевательства над молодыми солдатами были хорошо известны, поэтому желающих попадать туда по собственной воле было мало. По крайней мере, среди ребят из нашего класса обычной московской школы № 154. Впрочем, нет, не совсем обычной. Над школой шефствовал институт атомной энергии им. И.В.Курчатова, отличавшийся от обычных НИИ советской эпохи чрезвычайно высоким интеллектуальным уровнем. У многих родители работали в Курчатнике, а частенько списывающая у меня контрольные по алгебре и геометрии одноклассница Катя Александрова была внучкой директора института академика А.П.Александрова. Отец работает в Курчатнике чуть ли не с момента его основания, так что мне уж сам Бог велел: после школы – МИФИ, а затем – в Курчатник. Сдалась мне эта ВКШ КГБ с ее военными порядками! Надо было сразу сказать об этом кадровику и не морочить больше голову ни себе, ни ему.

Но в руках бумажка, на которой сверху большими буквами: «Комитет Государственной Безопасности СССР». В моих руках – освобождение от школы на вторник, на целый день! Такая отмазка, наша классная руководительница, физичка, наверняка отпадет! Во вторник контрольная по физике, а в понедельник я выложу ей этот листочек и на таком изощренном основании прогуляю весь день, в том числе и эту гнусную контрольную. Отказаться еще успею, а пока – бери от жизни все!

Один школьный день я таким образом прогулял, понравилось. Основания – самые что ни на есть законные и весьма нетривиальные. Так ведь, наверное, такие возможности будут и еще несколько раз? Несомненно. Процедура оформления в КГБ долгая, отмазок от школы будет еще много. Так что же ими не воспользоваться? А уж решить: поступать или нет в Высшую Краснознаменную Школу КГБ, можно будет и попозже, ближе к вступительным экзаменам. Да и вообще, даже как-то интересно стало: таинственное учебное заведение, есть возможность сделать какой-то нестандартный выбор будущей профессии, вырваться из общей школьной стаи, длинным клином нацелившейся на МИФИ. Абсолютно никаких, даже самых приближенных представлений о будущей специальности после окончания ВКШ КГБ, у меня в то время не было, и вся эта затея напоминала авантюру. Прекрасно, обожаю авантюры!

Может, кто-то с детства мечтал стать летчиком или физиком и прямо с детского садика стал готовиться к будущей профессии. Но я уж точно никогда себе до окончания школы и близко не представлял, что буду криптографом.

Что же представляла из себя в то время полусекретная ВКШ КГБ? В ней было несколько факультетов, но математиков (биномов, яйцеголовых) готовил только один – 4 или Технический факультет. Остальные готовили, как правило, «истинных» чекистов. Биномов никто за «истинных», слава Богу, не считал, и для этого были все основания. Факультет был создан в начале 60-х годов, вскоре после того, как сбежавшие в СССР из американского АНБ – Агентства Национальной Безопасности, занимающегося в США вопросами криптографической защиты информации – американские криптографы Мартин и Митчел поведали советским коллегам об организации криптографической защиты в США. Криптография – точная наука, надежность шифра должна оцениваться не какими-то расплывчатыми рассуждениями, а точными математическими оценками, количеством двоичных операций, необходимых для взлома, и вероятностью успешного взлома. Криптограф может не знать какие-то лингвистические особенности языка, на котором осуществлялась шифрованная переписка, но он должен знать результаты Шеннона, быть математиком, в совершенстве владеть алгебраическими и статистическими методами анализа шифров. При таком подходе появляется возможность гарантировать надежность шифра от любого потенциального злоумышленника, и только такой подход является по настоящему профессиональным криптографическим анализом.

Догоним и перегоним Америку! По криптографии СССР должен быть не хуже, чем США, будем готовить своих профессиональных криптографов.

И, как ни странно, получилось! А, впрочем, ничего странного здесь нет. Криптография в те времена была чисто военной, обслуживала высшее руководство страны, а на такое дело денег и сил не жалели. Всемирно известный историк криптографии американец Дэвид Кан в своей книге «Криптографы» (изданной в России также под названием «Взломщики кодов») напрямую связывает поражение русских армий Самсонова и Ренненкампфа в Первой мировой войне со слабостью российских шифров. Пришедшие на смену царю большевики всегда были особыми конспираторами, любили секретность и, поэтому, не могли оставить без внимания криптографию. В 1921 году Ленин подписал декрет о создании специальной шифровальной службы при ВЧК-ОГПУ, которую возглавил один из близких соратников Ленина, старый большевик Г.И.Бокий. В эту спецслужбу пригласили всех лучших специалистов-криптографов того времени, чьи книги мы изучали на 4 факультете и 50 лет спустя. Но это была еще «традиционная» криптография, где основным орудием криптографа был остро отточенный карандаш и охотничье чутье на какие-то особенности во вскрываемом тексте. Результатов Шеннона в те времена еще не было, вскрытие шифров осуществлялось примерно такими же методами, какими Шерлок Холмс разгадывал загадку «пляшущих человечков» - в основном, за счет интуиции и опыта криптографа. Но тем не менее к началу Второй мировой войны у Советского Союза была достаточно эффективная шифровальная служба. «Явная неспособность немецких криптографов вскрыть советские стратегические системы, с помощью которых засекречивалась самая важная информация, вынудила одного немецкого криптографа признать, что, хотя Россия и проиграла Первую мировую войну в эфире, во время Второй мировой войны она сумела взять реванш за свое поражение» - цитата из Дэвида Кана.

Сталин, как старый большевик-конспиратор, прекрасно понимал значение шифровальной службы. В 1949 году было создано Главное Управление Специальной Службы при ЦК ВКП(б), многие криптографы того времени получили квартиры в «сталинских» домах, работать в ГУСС через райкомы комсомола направляли лучших молодых выпускников различных ВУЗов тех лет. «Читать всех, но наши шифры и переписку читать никто не должен» - такой лозунг выдвинул «лучший друг всех криптографов». Правда, насчет «читать всех» он, скорее всего, погорячился, ведь были в то время уже известны результаты Шеннона об условиях достижения абсолютной стойкости шифра. Как гласила одна из легенд, ходивших по 4 факультету, попытка одного человека объяснить Лаврентию Павловичу про абсолютную стойкость окончилась тем, что на выходе из здания Лубянки у него отобрали служебное удостоверение. После смерти Сталина шифровальную службу вновь вернули в КГБ, но, тем не менее, в 50-х годах сформировалась весьма сильная когорта советских специалистов-криптографов, которые в 70-х стали нашими лучшими преподавателями. Правда, большинство из них заканчивали обычные ВУЗы, а затем переучивались на криптографов. И вот, в начале 60-х – очередная криптографическая инициатива – готовить специалистов-криптографов сразу же после средней школы.

Создали 4 факультет ВКШ КГБ, пригласили туда лучших профессоров и преподавателей алгебры, математического анализа, теории вероятностей, теории чисел и многих других дисциплин. А самое главное, что основатели факультета сумели привнести на него дух университетской вольности, гордости за свою специальность, свою профессию, иммунитет от очковтирательства, лизоблюдства, безудержного чинопочитания, тупого преклонения перед разными начальниками, заложили традиции, которые оказались на удивление живучими. За годы существования факультета многие его выпускники сами стали прекрасными преподавателями и одновременно продолжали поддерживать атмосферу раскрепощенности и

высочайшей профессиональности во времена брежневского застоя-запоя. Да и отбор на факультет был весьма и весьма строгим: как правило, выпускники специализированных физико-математических школ, победители различных олимпиад, в общем те, кто уже доказал свою способность серьезно учиться.

Под военными погонами фактически существовало прежнее закрытое отделение мехмата МГУ, с раннего возраста целенаправленно натаскивающее молодых ребят на теорию конечных полей, вероятностные пространства, нормальное распределение и центральную предельную теорему, теорию конечных автоматов, комбинаторику и многое, многое другое, без чего невозможно представить себе современного криптографа.

И этот оазис существовал в структуре КГБ, где хватало славных начальников.

- В первую очередь нам нужны хорошие офицеры, а затем уже хорошие специалисты. Хороших специалистов мы можем набрать и из МГУ.

Такая точка зрения открыто высказывалась генералом - начальником факультета с высоких трибун на партсобраниях и активах. Особенно умиляло, конечно же, его отождествление себя с какой-то великой и невиданной силой – «мы». Наверное, это такие же важные генералы, для которых важнее всего – бодрый утренний рапорт дежурного офицера и регулярные строевые смотры, на которых генералы предстают во всем своем блеске перед подчиненными, а те едят их своими взглядами. Только вот представление о том, что же такое хороший специалист, у начальника 4 факультета не выходило за рамки его привычного генеральского кругозора: в первую очередь тот, у кого всегда поглажена форма и вычищены сапоги. И такой начальник был не одинок на факультете.

- На экзамен по алгебре нужно приходить четким строевым шагом, чтобы вся алгебра сразу видна была.

Так наставлял нас начальник рангом поменьше – всего лишь нашего курса. Ну, про своего начальника курса нельзя не вспомнить особо, в отдельной главе этой книги, а пока, говоря о самых общих чертах 4 факультета, стоит еще раз подчеркнуть наличие двух противоположных классов: начальников и преподавателей. Для начальников в первую очередь были важны хорошие офицеры, а для преподавателей – хорошие специалисты. И за все время моего пребывания на факультете я пришел к твердому убеждению, что это – альтернативы, из них нужно выбирать что-то одно: или хороший офицер, или хороший специалист. По крайней мере, на нашем курсе результатом воспитания хороших офицеров, как правило, становился стойкий иммунитет ко всем тупостям и глупостям военной службы и нетерпеливое ожидание очередного афоризма начальника курса, который полностью оправдывал эти надежды:

- В ваши годы Лазо уже ходил у топки паровоза, а японцы и белогвардейцы его туда бросали.

Ну разве можно в таких условиях не полюбить математику!

Глава 1

You are welcome

Этот простой плакатик (именно на английском языке) висел над входом в актовый зал, где состоялось мое первое знакомство с 4 факультетом ВКШ. И все, ничего более! Никак не ожидал: все же военное заведение. Где доска почета с отличниками боевой и политической подготовки, где плакаты с разными солдатами-буратино, с автоматами в руках защищающими от супостатов завоевания Октября, где призывы вождей учиться до посинения и экономить на экономике? Старое здание дореволюционной постройки по Большому Кисельному переулку, уютный дворик, тишина и патриархальность. И это в то время, когда парадность и показуха так и лезли изо всех щелей, а количество и дуракоемкость различных лозунгов и наглядной агитации была сопоставима разве что с современной рекламой. Со стен ПТУ на вас глядели типичные строители и строительницы коммунизма и хрипло зазывали: «Приходите к нам учиться!» И корова и волчица – хотелось добавить им в ответ. Лозунг всеобщего среднего образования означал на

практике, что учителя вынуждены были выдавать аттестаты любым двоечникам и лодырям, чтобы не портить показатели райкому КПСС. Потом пошла борьба за образцовый город, в котором должны быть образцовые институты, в них образцовые факультеты и кафедры. Борьба теми же способами, что и за всеобщее среднее образование. Одним словом – развитой социализм!

А ведь еще Ленин говорил: «Жить в обществе и быть свободным от общества нельзя». Не мог Технический факультет совсем оставаться в стороне от реальной действительности и исключить из повседневной жизни наглядную агитацию, политинформации, субботники, общественно-политические аттестации и прочую подобную чушь, составлявшую основы коммунистического мировоззрения. Но на факультете, встречая абитуриентов, всеми способами сразу же давали понять: не это здесь главное.

Уютный купеческий дворик, без всяких вывесок и рекламы, в самом центре Москвы, тихий, спокойный, располагающий к размышлениям, творчеству и фантазии – таким запомнился мне Большой Кисельный переулок, дом 11, изначальное место обитания советской криптографической альма-матер. А какие же были там в то время порядки?

Пять лет учиться на математика-криптографа посылали три ведомства: КГБ, Министерство обороны и Министерство радиоэлектронной промышленности (МРП). Каждое из этих ведомств само отбирало себе кандидатов на учебу и после окончания они должны были прийти туда на работу. Но с ребятами, отобранными МРП, поступали жутко несправедливо: пять лет нужно было ходить в военной форме, подчиняться всем военным порядкам, а после окончания им присваивалось звание офицеров запаса и они шли на работу в гражданское ведомство, не получая никаких льгот, положенных военнослужащим. Правда, их набирали только из Москвы и всегда после окончания оставляли в Москве, а вот выпускников от Министерства обороны ждала экзекуция в виде распределения. «Спасибо царю-батюшке, что Аляску продал» - основная их присказка за все пять лет учебы. Хабаровск, Чита, Алма-Ата, Рига, Минск, Калининград – мой адрес не дом и не улица, мой адрес Советский Союз, везде есть части радиоперехвата и дешифровальные службы при них. И набирали их со всего Советского Союза, сначала приглашая наиболее талантливых в специализированную физ-мат школу-интернат при МГУ, а затем – на 4 факультет. Выбор места распределения, как и полагается, - в зависимости от оценок в аттестате, но были и исключения, особо вольных москвичей могли и с красным дипломом заслать в Хабаровск. Тут уж вовсю торжествовали начальники, припоминая непокорным все грехи. Правда, такие ребята все равно через некоторое время пробивались в Москву, в аспирантуру, а начальники как были, так и оставались все теми же.

Но больше всего посылало на учебу 8 и 16 управления КГБ, шифровальная и дешифровальная служба, советский аналог американского АНБ. Довольно эффективный в то время аналог, о чем можно прочитать у Дэвида Кана. Посольства и дипломатическая переписка, правительственная и военная связь – все в ведении КГБ, нужны специалисты-криптографы, способные как разрабатывать свои, оригинальные шифры, так и взламывать чужие. Приехала как-то в Москву торговая делегация одной известной иностранной фирмы договариваться о строительстве в СССР крупного завода, узнала условия советской стороны и стала по шифрованной связи обращаться за инструкциями: до какого минимального предела можно торговаться? Получает опять же шифровками ответы. Советская сторона не спешит, гостеприимство проявляет: не хотите ли по Золотому Кольцу России проехаться, попить-погулять, достопримечательности и девушек русских посмотреть? Ну кто ж против такого соблазна устоит, переговоры серьезные, трудные, надо бы прерваться на недельку. А в 16 управлении в это время аврал, мозговая атака, штурм вражеской крепости. Зато потом наступил праздник греческой буквы дельта, которой в математике принято обозначать разность между двумя значениями: предполагаемым и минимальным.

Вот такую историю любили нам рассказывать на лекциях по основам криптографии. Подозреваю, что продукция построенного завода до сих пор колесит по всей России.

Но вернемся на Большой Кисельный. Вступительные экзамены на 4 факультет. Тут надо немного вспомнить существовавшую в те времена (середина 70-х годов) систему вступительных экзаменов в ВУЗы, поскольку стремление поступить в институт и избежать армии было тогда (да и сейчас тоже) практически поголовным. Почти во все московские ВУЗы вступительные экзамены начинались одновременно с 1 августа, поэтому желающие поступить должны были заранее выбрать себе институт и сделать на него всю ставку. Но в этом правиле были три явных исключения: МГУ, Физтех и МИФИ. Экзамены в эти институты считались более сложными, поэтому проводились они не с первого августа, как во всех остальных институтах, а в июле. Если не удалось поступить в один из этих трех институтов, то оставалась еще возможность попытать свои силы в августе. Причем даже в этой тройке были различия: первый и наиболее сложный экзамен – письменная математика – проводился, например, на факультете вычислительной математики и кибернетики МГУ буквально в первых числах июля, а первый вступительный экзамен в МИФИ – чуть попозже, 5-6 июля. Поэтому у абитуриента были реальные возможности попробовать свои силы в нескольких местах: сначала – в МГУ, затем, если не получилось на первом же и наиболее сложном письменном экзамене по математике, попробовать свои силы в МИФИ. Если и там неудача, то всегда в запасе был август, основная волна вступительных экзаменов.

Но было еще одно, четвертое исключение из этого правила – 4 факультет ВКШ КГБ. Вступительные экзамены туда начинались примерно в то же время, что и в МГУ – в самых первых числах июля, поэтому после неудачи на первой письменной математике оставалась еще возможность поступать в МИФИ. Так что для меня это был еще один, и весьма весомый аргумент за то, чтобы попробовать свои силы на 4 факультете.

Вступительные экзамены: математика (письменная и устная), физика и сочинение, самый трудный – первый, письменная математика, на ней сразу же отсеиваются около 60% абитуриентов. Надо сказать, что поскольку все абитуриенты на 4 факультет отбираются ведомствами, то они же и определяют конкурс при поступлении: примерно 3 человека на место. Сделать больше трудно для кадровиков: с каждым кандидатом много предварительной работы, тщательно проверяются все родственники, связи, привычки, характеристики. Как и в тридцатых годах, для поступления в ВКШ КГБ нужна рекомендация райкома ВЛКСМ. Не знаю, как там давали рекомендации в тридцатых годах, только в середине 70-х это, с первого взгляда отдающее почти революционной романтикой мероприятие, превратилось в будничную чиновничью процедуру. Никаких пламенных страстей, ничего существенного и интересного от всех этих процедур в моей памяти не осталось. Единственное – возможность несколько раз прогулять школьные уроки на таком изощренном и нетривиальном основании: оформляюсь в Высшую Школу КГБ!

А вот и первая радостная новость: казармы нет совсем! Еще за год до нас казарма была там же, в этом купеческом здании, но факультет расширился, добавилось отделение радистов, и все помещения казармы отдали им. Особых энтузиастов искать под казарму новое помещение видно не нашлось, поэтому москвичи теперь с первого же курса живут по домам, а все иногородние – в общежитии. По крайней мере, так официально объяснялось отсутствие в военном учебном заведении этого святого атрибута: на нет и суда нет.

От самих вступительных экзаменов на 4 факультет у меня сейчас осталось не очень много воспоминаний. Больше, пожалуй, о периоде подготовки к ним, о попытках объять необъятное и прорешать все задачи из всех учебников для поступающих в ВУЗы. Поэтому к самим экзаменам наступило состояние, близкое к безразличию, - скорее бы закончился этот кошмар. Да, пожалуй, еще припоминались страшилки про вступительные экзамены в МГУ, где время, отведенное для первого письменного экзамена по математике, измеряли чуть ли не с секундомером в руках, а при раздаче листов с вариантами экзаменационных задач от всех абитуриентов требовали держать руки за спиной. Но ничего подобного на первом письменном экзамене в ВКШ не было, обстановка была очень спокойная и даже где-то по домашнему уютная. Система простая: пять задач, сколько решил, столько и получаешь. Задачи попались не очень сложные, пришлось повозиться только с последней, пятой, из стереометрии. Ответ получился жутко уродливым и больше чем наполовину я был уверен, что где-то ошибся при рассуждениях или расчетах. Да и потом все время перед экзаменом меня преследовало раздвоение личности: основная, авантюрная часть, все время подзуживала: «Ну что, слабо?», а оставшаяся где-то в глубине, рассудочная, все время твердила: «Зачем тебе сдались эти военные порядки и сапоги? Иди в МИФИ, как все нормальные люди!». И вот когда я узнал, что на первом экзамене по математике успешно решил все пять задач и теперь перспектива нацепить на себя через месяц военную форму стала не какой-то эфемерной, а самой что ни на есть реальной, авантюрная часть, радуясь достигнутому успеху, опять вылезла вперед все с тем же вопросом и опять задавила во мне все хилые голоса разума. Но сейчас, спустя 30 лет после этой вступительной эпопеи, я опять по-прежнему согласен со своей авантюрной частью.

Еще одно воспоминание о вступительных экзаменах – это мандатная комиссия. Экзамены закончились, июль, жара, хочется отдохнуть последние денечки перед отправкой в военные лагеря, а тут надо терять целый день на какую-то мандатную комиссию, о которой я тогда не имел ни малейшего представления. А между тем это был важнейший ритуал для начальников, на который собиралась целая куча генералов во главе с начальником всей ВКШ КГБ. На мандатной комиссии начальники должны были живьем посмотреть каждого человека из нового пополнения, который, в свою очередь, должен был продемонстрировать свою подтянутость, дисциплину и стремление стать хорошим военным. Абитуриенты шли на мандатную комиссию в порядке набранных на вступительных экзаменах баллов, поэтому первые представшие перед комиссией люди должны были олицетворять собой потенциально лучшую часть будущего курса.

Я шел на мандатную комиссию в числе первых, поскольку мое общее количество баллов было почти максимальным – 24 из 25 возможных (к оценкам на экзаменах тогда еще приплюсовывался средний балл аттестата зрелости), поэтому когда методист факультета, готовившая нас к выходу на мандатную комиссию, увидела мою летнюю маечку-размахаечку безо всяких намеков на официальные пиджак и галстук, даже ее доброе сердце не выдержало такого надругательства над уважением к строгой комиссии. С идущего вскоре за мной Лехи М. был срочно снят пиджак, на пару размеров больший, чем того требовала моя отощавшая за время экзаменов фигура, и спешно водружен на меня с целью хоть как-то прикрыть непотребную для генеральского взора летнюю маечку. Про прическу говорить не приходится, поскольку, осознавая потенциальную угрозу поступления в военное учебное заведение, я последние полгода старался всячески насладиться всеми прелестями вольной жизни и, в частности, возможностью отрастить себе волосы подлиннее. Вот в таком импозантном виде началась моя военная служба.

- Решением мандатной комиссии Вы зачисляетесь на 1 курс 4 факультета Высшей Краснознаменной Школы КГБ им. Ф.Э.Дзержинского. Поздравляем Вас!

Начальником Высшей Школы КГБ в 1974 году был сравнительно молодой и подтянутый генерал-лейтенант. Окинув меня своим генеральским взором, он добавил

- А причесочку-то придется укоротить.

На выходе я побыстрее скинул пиджак и вернул его ожидавшему своей очереди Лехе М.

- Ну как?
- Все нормально!
- В правый карман пиджака положи 15 копеек.

Впоследствии из нашего курса Леха стал, пожалуй, одним из самых крутых бизнесменов.

*****

Итак, солдатские сапоги стали для меня, человека сугубо гражданского и не имевшего ни малейшей тяги к военной службе, самой что ни на есть настоящей реальностью. Но сразу честно признаюсь, что учеба на 4 факультете ВКШ КГБ все-таки сильно отличалась от обычной и овеянной разными страшилками службы в Советской Армии. Да и от обычного военного учебного заведения, даже от других факультетов ВКШ КГБ, Технический факультет отличался в первую очередь своим составом, своей спецификой, своими традициями. Но первые лагеря недалеко от Балашихи, под Москвой, на весь август месяц, почти сразу же после вступительных экзаменов, были пока еще довольно непривычными. Там уже все было по полной программе: казарма, строевая подготовка, солдатская столовая и распугивание грибников в окрестном лесу своими воинственными игрищами.

Первые военные впечатления. Толпа молодых и неуклюжих парней в новой и еще пахнущей вещевым складом повседневной военной форме высаживается из автобуса на пятачке перед главным корпусом балашихинских лагерей. Откуда-то появляется командир с какими-то другими погонами (старшина) и начинает командовать. Создается некоторое подобие толпы-строя, которая начинает свое шествие к бараку-казарме по асфальтовой дорожке. На пути – огромная лужа, которую все начинают обходить, но тут раздается командирский рык:

- Идти прямо! Что, лужи испугались?

Так, видимо, надо начинать готовить настоящих офицеров. Но это был один из немногих подобных эпизодов. Каждой из трех учебных групп математиков в этой самой первой Балашихе были назначены командиры из числа слушателей, поступивших на другие, истинно чекистские факультеты ВКШ КГБ, которые уже имели опыт службы в армии. Наш командир группы, к примеру, служил в Кремлевском полку и у нас с ним установились вполне нормальные человеческие отношения. И если бы не дикий рев дневального каждое утро ни свет ни заря

- Подразделение, подъем!

то самое первое месячное пребывание в Балашихе можно было бы назвать вполне сносным.

В конце первого и второго курса – опять туда же, только уже на пару недель, про это мы еще вспомним в этой книге. Но если сразу после поступления народ был еще немного напуган непривычной военной обстановкой и иногда даже пытался читать Устав гарнизонной и караульной службы и искать высокий смысл в классической уставной фразе: «Заслышав лай караульной собаки, часовой должен дать знать об этом начальнику караула установленным сигналом», то второе, а в особенности третье нашествие в Балашиху все больше походили на веселый пикник на природе, из которого можно натаскать для летних каникул холостых патронов, взрывпакетов и прочих бесплатных фейерверков. А что может быть лучше взрывпакета, плывущего в банке из-под тушенки по щучьему месту тихой лесной речки?

А говоря в целом о 4 факультете - заведение военное, со всеми военными атрибутами: хождением в военной форме, ежедневным утренним построением, на котором начальник курса придирчиво проверяет твой внешний вид, военной дисциплиной или, по крайней мере, ее видимостью. Кстати, а кто такой начальник курса? Это – отец-командир, организатор и вдохновитель всех наших побед, духовный наставник неопытной молодежи. Все слушатели (не курсанты, а именно слушатели, так официально называли нас в то время, хотя погоны были с буквой «К») 4 факультета разбиты на курсы, и у нескольких курсов - начальник. В то время было всего два начальника курса: один – для 1, 3 и 5 курсов, другой – для 2 и 4. Начальник курса – лицо, ответственное за своих подопечных: если кто-то попался, то виноват в этом в первую очередь начальник курса – недовоспитал своего попавшегося подопечного. А вообще-то по большому счету делать на работе начальнику курса (и еще его заместителю) было нечего. Слушатели первую половину дня – все на занятиях, их в это время не повоспитываешь. А вторая половина – чаще всего или разбегаются по домам (казармы-то нет!) или сидят занимаются в спецбоксах, в которые посторонним вход воспрещен. Так что видел и воспитывал своих ненаглядных чад начальник курса как-то урывками, на утреннем построении, да в перерывах между лекциями. А все остальное свое рабочее время он и его заместитель, наверное, копили силы для такого точечного воспитания, чтобы потом одним-двумя меткими ударами враз победить присущие любому молодому организму антивоенные пороки. Как это удавалось нашему начальнику курса – об этом особая глава в этой книге.

Первые два года на 4 факультете было некоторое подобие военной подготовки, впрочем, ненамного отличающееся от обычного гражданского вуза. Поначалу немного непривычно для человека, не испытывающего особой любви к военной форме, но потом выясняется, что таких как ты здесь подавляющее большинство и дальнейшая жизнь кажется даже интереснее, чем в обычном вузе.

Вот такое общее представление о 4 факультете и его обитателях. Пора к делу, к конкретике, детальному повествованию, написанному местным аборигеном на чужбине спустя почти 25 лет после его окончания. Веселая, светлая пора в моей жизни, масса впечатлений и друзей остались после нее!

Глава 2

Чуда!

Пятница, 8.00 утра. Весь курс построен и ожидает традиционного пятничного шоу – строевой подготовки. По рядам сначала шепотом, а потом все громче и громче разносится народный глас:

- Чуда!
- Чу-да!
- Чу-у-да!

И оно появляется: сначала в окне лестничного пролета на 5 этаже, а затем постепенно спускается все ниже и ниже и, наконец, ступает на грешную землю. Это наш начальник курса, отец-командир, подполковник. Начинается самое интересное, держи ухо востро, не прозевай и не забудь потом записать его чудесные мысли. Как величайшую реликвию храню я все эти годы записную книжку с почти тремя сотнями его афоризмов, дружно собранными за годы учебы всей нашей группой. Пятница – традиционный день, когда бывает наиболее богатый улов.

Шоу, как и положено, начинается с осмотра внешнего вида. По определению, почти все слушатели 4 факультета в этом смысле страшные разгильдяи, к тому же каждый божий день появляющиеся в таком виде на московских улицах, в метро, там где есть вероятность быть сцапанными обычным армейским патрулем. Единственный способ безопасного передвижения – не попадаться на глаза патрулю вообще, обходить все чумные места, стараться идти в толпе и только знакомыми маршрутами. Однако Чудо наивно верит в то, что с образцовым внешним видом патруль не найдет к чему придраться и, при невыполненном плане отлова, молча проводит глазами лакомный кусок сыра. Да и вообще, надо чем-то заниматься начальнику курса математиков. Не математикой же!

- Командирам групп докладывать о неприческах!

Командиры групп, безуспешно стараясь принять строгий вид, делают осмотр криптографического каре, и, естественно, докладывают, что непрически стремятся к нулю. Отец-командир поясняет:

- Прически, не соответствующие действительности, немедленно устранить! Сейчас мы с вами пройдемся друг по другу, точнее я по вам.

и начинает собственный таможенный досмотр. Курс замер в ожидании… конечно же, новых афоризмов!

- Стоящий рядом товарищ подчеркивает вашу неподстриженность.
- Что у вас там под шеей растет?
- У вас люфт на животе, в смысле ремня конечно, а живот надо уменьшать.
- Немедленно замените шапку-блин на шапку-шапку.
- Надо становиться в строй с чистыми сапогами, а то вы наматываете на ус, а наворачиваете только грязь.
- У вас спереди гармонь. Ой, у вас и сзади гармонь. В общем, баян!
- Что у вас с ногами? Поставьте их строевым способом!
- Я вам запрещаю в строю комедианничать, как допризывнику.
- Обрубите себе прическу!
- В строю должно быть однообразие, именно этим он отличается от бесстроия.

Строевая подготовка – это Чудино время. Чаще всего она проходила на небольшой площадке (язык не поворачивается выговорить слово «плацу») во внутреннем дворике нашей купеческой усадьбы. Часок разминки на свежем воздухе, разучивание «отходов и подходов», всегда сопровождаемое кучей анекдотов, приколов и Чудиных изречений.

- Выровняйте строй! А то привыкли на радиоэлектронике рисовать кривые.
- Ширше шаг! Что вы там шир-шир?
- Серов! Займитесь Гавриным. Постройте его и ведите строем.
- Добрынин! Не кульминируйте вокруг себя центр.
- Моторный! Вы почему обходите строй молчанием?

Но иногда ее переносили в аудиторию, для, если можно так сказать, теоретической подготовки. Здесь можно задушевно побеседовать с детьми малыми, неразумным, ничего в этой жизни не понимающими, кроме своей математики, о военной службе, учебе, отпуске и просто о разном.

Вот, например, про учебу.

- Вы вот не работаете в течение семестра, а когда подходит 30 июня, вы начинаете работать темпами «де же по де те», но «де же по де те» никакой производной не дает, поэтому у вас двойки.
- Нужно вытащить этих двоечников на бюро и спросить, сколько еще эти перлы будут блестеть изнутри.
- Комбинаторика – это ваш черный хлеб, который вы все время едите.

Иногда Чудо прямо на наших глазах делал потрясающие открытия в разных областях науки и техники, естествознания и человеческих возможностей. Оказывается, что:

- Осциллограф – не майка, его в комнате не сушат.

Это из области физики. А вот из области сначала арифметики, а затем и высшей математики:

- Ближайших метро три: Тургеневская, Колхозная, Площадь Свердлова, Площадь Революции, Дзержинская, Кузнецкий мост и так далее.
- Такая параллель, что ни один Лобачевский не исправит.

или смеси химии и математики:

- У Вас, Смирнов, полная химия данных.

или просто мистики и аномальных природных явлений:

- Происшествия не имеют происхождения, а имеют случайности!
- Происхождение Земли, происхождение жизни на Земле, происхождение человека от обезьяны… Происшествия не происходят, а случаются. Происходят чудеса!
- Перед кем он ходатайствует? Перед Вселенной ходатайствует.
- У вас что там, Святой Угол?
- Помогаете ему стать космоносцем?
- Ой, какие важные портфели! Прямо летающие тарелки.
- Все ходят нормально, а Вы идете через Луну, иначе Ваша пряжка не могла бы окислиться.
- Почему он начальника факультета не предупредил, что на Луну полетит к врачу?
- У Вас под ремнем лунный ландшафт проявился.

Чудино абстрактное мышление не знало границ. Его нетривиальный разум постоянно рисовал в его воображении некие фантастические картины, которые затем материализовывались в такие же нетривиальные высказывания и доставляли его подчиненным ничем неописуемую радость. О, сколько нам открытий чудных…!

- Он архиводы в рот набрал
- Вы должны запрограммировать в своем динамическом стереотипе, когда на себя посмотреть.
- Художественную литературу можно читать во сне, а не здесь.
- Создайте себе счетно-решающее устройство, чтобы знать, когда на какой трамвай и метро ногой наступить.
- Летом, даже если забраться на Эльбрус, нельзя сдать нормы ГТО по лыжам.
- Перчатки должны быть текстильные или шерстяные, а не кожаные из крокодила.
- Имейте в виду, что если холодная вода клонит куда-нибудь – не пейте ее.
- Многие товарищи идут на занятия с дебетом времени минусовым.
- Он повернулся и посмотрел на генерала, как будто это что-то эмеферное.
- У вас за строем то ли портфели, то ли базар. Надо либо убрать портфели в карман, либо самим залезть в портфели.
- Если у вас все аккуратно вверх ногами сделано, то сделайте неаккуратно.
- Трубу пароходную себе в рот положил и задымил.
- В праздники можно достать все, что угодно, даже черта лысого. Черта лысого – это может быть сильно сказано, но в последнее время прецеденты были.
- А он делает, что захочет, захочет сюда, захочет туда, куда его седьмая нога захочет. Восьмой вихрь в голове.
- И вы почувствуете, какой у нас длинный и толстый хвост. Как у доисторического ящура.

Но любимая тема – воинская дисциплина, опоздания, военная форма, outside - поведение доверенных его попечению чад. Чудо терпеливо и совершенно безнадежно пытается объяснить, как хорошо быть хорошим солдатом и как плохо быть плохим.

- Все ваши знания – это прилагательное. Существительное – это оружие и пулеметы.
- В чужих глазах вы и соринки замечаете, а в своих и бревна не замечаете. Нужно поднять работу по извлечению бревен из собственных глаз.
- Хватит ломаться и кривляться, пора выпрямляться в том смысле, что установлены порядки уставные.
- Вы такие творчества заделываете, что никто, даже крючкастый не разберется.

- С такой прической ходит как солдат спустя два месяца после демобилизации с Чукотки. Лучше бы на оленях ездил.
- Вы всегда найдете такую кривду, чтобы она смогла обволочь эту правду и представить ее в красивом виде.
- Прекратите давить информацию, в смысле разговаривать!
- Отец Корильо содержал целую камарилью парикмахеров, платил им по 1000 франков в день и стригся каждый день со своей семьей. Вот и вы можете стричься не для буржуазии, а для строя.
- Вы сами должны знать под кого стричься: под молодца, под воина или под артиста.

Как трудно сохранять спокойствие, сдерживать все рвущиеся наружу эмоции! Спокойствие, только спокойствие! Главное – математический подход: все запомнить, внести в базу данных, пронумеровать и сохранить. И когда-нибудь дать прочесть это своим детям и внукам: детки, учите лучше математику!

Контрасты – вот наилучший метод воспитания. Чудотворчества прививали нам любовь к математике гораздо быстрее любых других способов. После строевой подготовки наши преподаватели казались нам еще умнее, а все пропущенные лекции по алгебре и мат. анализу переписывались еще быстрее и старательнее. Все помнили об угрозе: в первую очередь нужны хорошие офицеры, а потом уже хорошие специалисты.

После утренней разминки – лекции. Здесь не до шуток, нужно максимальное внимание чтобы, записывая лекцию, еще и попытаться вникнуть в смысл доказанных теорем и облегчить себе дальнейшую подготовку к экзамену. Лекции по алгебре, мат.анализу, теории вероятностей – это особая глава в этой книге, пока же отметим, что эти лекции требовали максимальной сосредоточенности, внимания, напряжения, а, следовательно, и эмоциональной разрядки в перерыве. Перекуры – не очень хорошая разрядка, к тому же многие (включая автора этих строк) были абсолютно некурящими. И очень естественно такая разрядка была найдена – домино! Народный козел, не требующий особых умственных усилий, но очень эмоциональный и с элементами математики: умением считать до шести. И вот аудитория, где только что доказывали сходимости к различным предельным распределениям, оглашалась ответной реакцией:

- Конца взял!
- Руби шестерочный!
- С конца слез!
- Мочи!
- Рыба!

Естественно, с комментариями, присущими любому чисто мужскому коллективу.

В представлении Чуды это была ересь. Как могут эти головастики опускаться до уровня слесарей? А он, хранитель их математической невинности, должен это терпеть? Нет, нет и еще раз нет! Козловый дух должен быть изгнан, побежден любыми способами!

А какими? Играли ведь не на деньги, не всерьез, не на лекциях, а в перерывах. Первый способ, естественно, воспитательно-уморительный, с новыми афоризмами:

- Соберите всех козлов и на следующем перерыве зайдите ко мне

Козлы, как и положено, на следующем перерыве, вместо законного забивания фишки забиваются в кабинет Чуды.

- Любители козла и козьего молока! Там полстола, здесь полстола. Там, где козел посидел, полстола нет
- А почему нельзя играть?
- Потому что потому кончается на «у»

Ясное и понятное математическое объяснение. Не станешь же спорить и говорить что «потому» кончается на «ы» или «и». Но козлы по-прежнему плодятся, как кролики, и Чудо с огорчением констатирует:

- Теперь командир отделения стал главным козлеправом, а два самых главных учебных боевика учат как давить на козловые фишки и выдавливать из столов и его компонент козловый дух.
- Почему в ваше присутствие здесь витает козловый дух? И опять той же плеяды…

Заменить домино на шахматы! Вот в представлении Чуды игра, достойная математиков.

- Это хорошо, что он развивает свою память, делает шахматные и конские ходы.

Шахматная мысль в его воображении проникает на 4 факультет, завоевывает молодые умы, соединяется с математикой, порождает новых Алехиных и Ботвинников, затем вырывается на волю, в межпланетное пространство и … Дальше все где-то уже было описано. Но опять его не поняли.

- Козловый дух уберите! Замените его на шахматы. Это математическую мысль развивает.
- А домино в комбинаторике помогает
- В комбинаторике? Под пол-литру оно помогает!

Недолго велись мирные переговоры. Очень скоро козловому духу была объявлена война до последней доминошной кости.

- Ну-ка давайте сюда козла.
- Какого козла?
- Беленького, который жил-был у бабушки

Тихонько подойти к аудитории, застукать козловый дух и отобрать фишки с обещанием возвратить их после окончания факультета – вот такую наступательную тактику избрал наш padre, бесстрашно начав карательные операции в партизанской войне почти со всем курсом. А выиграть партизанскую войну, да еще в одиночку, заведомо невозможно. Новый комплект домино, продававшийся в спортивном магазине на соседней улице Кирова, стоил 99 копеек. Четверо играющих, у которых конфисковывалась фишка, скидывались по 25 копеек и тут же отсылали гонца за новым комплектом, выполняя таким образом магазину план по продаже домино лет на 5 вперед. А платяной шкаф в Чудином кабинете превращался в огромное фишкохранилище с перспективой вытеснения оттуда всего остального.

В конце концов было объявлено перемирие. На одном из Ленинских субботников Чудо попросил нескольких человек «прибраться у него в кабинете, в шкафу», заведомо осознавая, к чему это приведет. Арестованная фишка мигом разбежалась по всему курсу и весело застучала, празднуя свое счастливое избавление из ненавистного шкафа. Жалко, что на этом закончились и афоризмы про козловый дух.

Да, нелегкая задача досталась Чуде: сделать из нас хороших военных. По сложности примерно такая же, как сделать из него хорошего математика. Довольно скоро выяснилось, что традиционные методы кнута и пряника или разделяй и властвуй в применении к 4 факультету не шибко эффективны. Какой у начальника курса был основной кнут? Строевая подготовка по субботам, после занятий, где-то около часа. Обидно, но не смертельно, особенно если при этом еще удавалось разжиться очередными афоризмами на эту тему.

- Сейчас мы с вами на глазах у всей публики почистим зады
- Если в субботу вы входите в число желающих на строевую подготовку, то всякие свадебные и около того путешествия должны быть отложены.

Ну а пряники? Доска почета, благодарности и все прочие подобные кондитерские изделия зависели только от учебы, авторитетом пользовался тот, кто сильнее разбирается в задачах по алгебре и мат. анализу, а не тот, у кого бритый затылок и громкий командирский голос. Все попытки привить бациллу солдафонства изнутри, найти себе среди курса «друзей и помощников» заканчивались тем, что эти люди с трудом переползали экзаменационные сессии и в конце концов были либо отчислены за неуспеваемость, либо полностью дискредитированы перед остальным курсом своими двойками на экзаменах по математике. И вот в результате в борьбе за нашу образцовость и нравственность со всеми неприческами, козловыми

духами, зелеными и прочими змиями-искусителями и искусительницами остался только один преданный боец – Чудо, со своими цитатами бросившийся в отчаянный бой с этой танковой армадой.

- Когда горит под полом, надо отрывать ломом половые половицы.
- Вы почему опаздываете, вы что, последний из могикан?
- Лукьянцу тоже не хватило утюга на заднюю часть корпуса.
- Речь идет о том, чтобы показать умение и энергию, а не хвост.
- Вы не Дон-Кихот, чтобы разъезжать с индульгенцией где вам вздумается.
- Была показана архинизкая дисциплина.
- У вас что во рту: жевательная резинка или язык потолстел?
- Вы в Якутии были? Так вот, там живут такие шаманы, как нажрутся мухоморов и балдеют.
- Вы должны идти работать в театр мимикрии и там показывать носы, языки и прочие органы.
- И пыхнет своей цигаркой в лицо, считая что он Зевс … от слова зевать.
- У вас такой беспорядок в комнате, все равно что Тотоша и Кокоша мочалки жевали.
- Делайте маленькое, но дело. Не превращайте большое дело – политинформацию – в ересь.
- Командиры должны шевелиться и скрипеть, но не в плохом смысле, а в смысле первой скрипки.
- Касательство, встречи с бутылками и хождения вокруг них обходите.
- Зайдешь в вашу аудиторию и после надо чистить нос специальной чистилкой от грязи и бедлама.
- И эта реляция навечно осталась в скрижалях журнала.

Насчет реляции – это верно. На всех наших встречах после окончания факультета книжечка с Чудиными афоризмами неизменно пользовалась большим успехом. Но в целом это был довольно безобидный человек, дальше уморительных цитат его деятельность по нашему воспитанию, как правило, не шла. Правда, высказываемое им иногда выражение «Не шутите с военной службой!» сразу же воспринималось большинством из нас как предостережение: смотрите, к чему может привести излишнее усердие на военной службе. Но и это предостережение было, пожалуй, излишним: особо усердствоваших и увлекавшихся военной службой среди математиков 4 факультета не было. И это тоже легко объяснимо: среди математиков почти все поступили на факультет сразу же после школы, избежав службы в армии. Это была сознательная политика, которой придерживались кадровики, набиравшие абитуриентов: человек, прошедший армию, редко сохранял способности к математике. Но помимо математиков за год до нашего поступления на факультете открыли отделение радистов (военных радиоинженеров), вот там уже математика в таком объеме не требовалась, поэтому среди радистов соотношение служивших/не служивших в армии было примерно равным. Но численно это была лишь одна учебная группа на курсе, а математиков – три. Чудо всегда любил ставить нам радистов в пример, а на сборах в Балашихе после первого курса наши «родные» командиры групп были заменены радистами. Но кто кого в результате перевоспитал – неочевидно, один командир-радист, попадая, пусть даже и командиром, в среду математиков, не мог оставаться прежним носителем Чудиных идей.

Где-то на третьем курсе Чудина активность по нашему перевоспитанию стала спадать, у него появился новый объект для перевоспитания – молодые первокурсники. Но арьергардные бои продолжались почти до самого окончания факультета.

- Отцы, по моему, у всех есть, а то многие смотрят на меня и сомневаются

Много позже, слушая разных «слуг народа» по TV, я часто ловил себя на мысли: «Какие чудесные люди! Какое сходство!»

- Некоторые товарищи продолжают держать позицию недержания. Завяжите…узелком

Глава 3

Альбиносы

Вот, наконец, настало время рассказать и о том, чему и как учили на 4 факультете, о его преподавателях, выгодно отличавшихся от разных начальников, о том, как готовили в те времена

криптографов. На факультете существовало два, я бы мягко сказал, непохожих друг на друга класса: начальники и преподаватели. Представление о начальниках читатель уже получил в предыдущей главе. Конечно же, Чудо – явление уникальное, достопримечательность факультета, с ним мы сталкивались каждый день, но и остальные начальники, по рассказам и анекдотам из жизни различных поколений факультетских аборигенов, могли достойно побороться с ним за звание самого чудесного начальника. Но в этой главе речь пойдет о противоположном классе – преподавателях, из которых наиболее значимыми были преподаватели с кафедры математики. На факультете было несколько профильных кафедр: математики, криптографии, аналитики, вычислительной техники, все были тесно связаны с математикой, но кафедра математики – особая, ее преподаватели закладывали основы нашего образования.

Рассказать обо всех преподавателях с кафедры математики того времени сейчас просто невозможно, прошло уже почти 30 лет, многое из памяти стерлось, но общее мое впечатление о них осталось неизменным: это был блестящий коллектив настоящих профессионалов, людей, достойных всяческого уважения. Я постараюсь привести здесь лишь некоторые штрихи из их математических и не только математических портретов, позволяющие современному читателю оценить обстановку на 4 факультете в середине 70-х годов теперь уже прошлого века.

Первая лекция – математический анализ. Лекции по мат.анализу читает Георгий Павлович Толстов, седой пожилой полковник, всеобщий любимец. Они у него доведены до совершенства, до такого состояния, когда, кажется, что-то не понять просто невозможно. Начиная с простейших понятий точки и ее окрестности, он методично, маленькими шажками переходит ко все более и более сложным теоремам, связанным с функциями и пределами, а заканчивает теорией меры и интеграла, являющейся основой вероятностного пространства. Все даже самые мелкие факты занесены в различные леммы, теоремы, следствия и замечания, все пронумеровано и оприходовано, как в образцовом хозяйстве. Записывать его лекции легко и приятно, говорит ровно, не спеша, всегда укладывается в лекционное время, никогда не повышает голоса. Если уж только в аудитории становится совсем шумно, то Г.П. спокойно обращается: «Товарищи, тише. Теорема-то важная».

Спокойствие, невозмутимость, уверенность в себе, в своем богатейшем опыте, никакой излишней эмоциональности – таким навсегда запомнился мне, да я думаю и не только мне одному, Г.П., один из наших первых и лучших преподавателей с кафедры математики. Однажды на факультете была организована встреча с ветеранами, посвященная очередному дню Победы, на которой Г.П. в своей обычной манере, не спеша, без излишних эмоций, рассказывал нам, молодым курсантам, как он впервые попал на фронт под Сталинградом, как чудом уцелел при переправе через Волгу, как обстреливали и бомбили их тогда немцы. Нам же, узнав о его фронтовом прошлом, оставалось только по-хорошему завидовать нелегкому жизненному опыту этого человека, его характеру и знаниям.

На мой взгляд, Г.П. сумел привить многим из нас такое важное качество, как последовательное движение к цели step by step. В математике и криптографии никогда не следует спешить, пытаться перескакивать через какие-то шаги, кажущиеся на первый взгляд весьма простыми, лучше сделать несколько маленьких шажков, но каждый из них должен быть понятен и очевиден. Это же в полной мере относится и к написанию различных программ, которые затем соединяются в большой программный комплекс. Написание и отладка программы во многом сродни доказательству теоремы: и там и там необходимо получить требуемый результат. И в обоих случаях часто делаешь одну и ту же ошибку: пытаешься прыгнуть сразу подальше чтобы побыстрее завершить свою работу. Иллюзия! Вылавливать допущенные и в теореме, и в программе ошибки подчас бывает намного труднее, чем начать все сначала по методу Г.П.

И точно такой же подход оказывается наиболее эффективным при построении и анализе различных шифров. Что такое классический шифр? Это некоторое математическое преобразование, выполненное над открытым текстом, в результате которого он превращается в шифртекст. Преобразование зависит от ключа и часто является некоторой цепочкой более простых преобразований, зависящих от части ключа или даже только от отдельных его знаков. Посмотрите, например, на американский стандарт DES (Data Encryption Standart) – последовательно, за 16 шагов осуществляется преобразование блока информации. Но почему выбраны именно такие преобразования на каждом шагу? А что будет, если число шагов увеличивать до бесконечности? DES – это уже конечный криптографический продукт, всех мельчайших шажков, осуществленных при его создании, мы не знаем. Остается только слепо верить его создателям, а это не очень хороший подход.

По методу Г.П., создание шифра надо начинать с самых простейших преобразований, тщательно их изучить, просчитать, все несколько раз проверить и затем сделать следующий маленький шажок по пути их усложнения. А тщательное изучение предполагает получение ответов не только на лобовые вопросы типа: стойкий или нестойкий, но и любое другое дотошное копание до истины: что будет, если увеличивать длину ключа до бесконечности? какова мощность каждого слоя? какие операции лучше использовать? не будет ли повторений? И много, много других подобных вопросов. Для обобщения ответов на них в математике применяются такие алгебраические понятия, как группы, кольца и поля.

И вот наша подготовка к получению криптографического образования началась с алгебры, сначала с классической линейной, а затем постепенно, маленькими шажками, ко все более и более сложным теоремам, кончая красивейшей теорией конечных полей, разработанной еще в XIX веке молодым французом Эваристом Галуа. В криптографии теория Галуа легла в основу системы с открытым распределением ключей, предложенной американцами У. Диффи и М.Хеллманом в 1977 году. Но и до этого, в 1974 году на 4 факультете ВКШ КГБ прекрасно понимали всю важность и значимость для криптографии теории Галуа и уделяли ей первостепенное внимание при подготовке криптографов.

Алгебру обожали за ее красоту. Лекциям и задачам по алгебре большинство из нас всегда отдавало предпочтение перед другими предметами. Сан Саныч, молодой тогда еще преподаватель, сам недавно закончивший факультет, был окружен ореолом различных историй, в которых невозможно было отделить правду от вымысла. Одна из таких легенд гласила, что как-то в суточном наряде, будучи еще таким же слушателем, как и мы, Сан Саныч развлекался тем, что пытался научиться эффектно кидать штык-нож в одну из деревянных дверей. После нескольких безуспешных попыток дверь вдруг отворилась и из нее вышел … сам «боцман», зам. начальника ВКШ по строевой подготовке. «Боцман» был колоритнейшей фигурой во всей Высшей Краснознаменной Школе: капитан первого ранга, всем своим видом, голосом, поведением на 200% оправдывающий это народное прозвище. Все начальство, включая и «боцмана», обитало вдалеке от криптографов, в основном здании ВКШ КГБ на Ленинградском проспекте, но иногда, но все же редко, непотопляемый «боцман» заплывал и на Большой Кисельный. Полундра!

О том, что стало тогда с Сан Санычем, легенда умалчивала. Можно только попытаться ее легко домыслить: несколько суток ареста, но московские гауптвахты сильно загружены, мест нет. Какая жалость!

На лекциях Сан Саныча метод Г.П. сочетался с его боевым задором, стремлением подколоть своих слушателей, ненамного более молодых, чем он сам. «Тяжело в учении – легко в госпитале» - его любимая поговорка. А еще сама теория Галуа в устах Сан Саныча как бы говорила нам: смотрите, что смог сделать француз Галуа в 19 лет! А вы, такие же молодые, специально отобранные из лучших школ, собранные здесь все вместе, чем хуже? Цените красивые результаты, не выбирайте тривиальных путей! Один нетривиальный результат способен перевернуть все привычные представления, разрушить всю окостенелость и застой в математике и не только в ней. Пусть, на первый взгляд, это и труднее, но в любой ситуации пытайтесь найти нетривиальное, красивое решение, которое понравилось бы вам самим и заставило бы уважать вас окружающих. Не бойтесь быть белыми воронами, альбиносами, выделяющимися из общей стаи, это изначальное условие для творчества, для творческого успеха.

И эти зерна падали в почву, обильно удобренную Чудиными афоризмами, как бы добавляя: а если будете серыми, незаметными, тривиальными солдафонами, то будете такими же, как ваш начальник курса.

И вот, несколько лет спустя, казалось, что сама жизнь полностью подтвердила эти мысли: основанная на теории Галуа система с открытым распределением ключей Диффи-Хеллмана произвела переворот в криптографии, доказав, что несколько красивых и нетривиальных идей намного полезнее, чем сотни безропотных, бессловесных, безликих чиновников. Система рассылки ключей упрощается до предела, не нужны больше курьеры с опечатанными сургучной печатью пакетами, криптография становится дешевой, удобной, общедоступной. Система Диффи-Хеллмана оказалась незаменимой в коммерческой, свободной от чиновников криптографии. Но не в России! В России прапорщики, привозящие диппочтой в группу советских войск в Германии секретные ключи к шифрсистемам, везли обратно в контейнерах для диппочты дефицитные в то время покрышки к «Жигулям». Спрос, востребованность обществом – вот что необходимо приложить к красивой идее. А если в обществе всем заправляют Чудесные (а иногда к тому же – просто очень циничные) люди, то рассчитывать на такой спрос не приходится. Если вы такие умные, то почему строем не ходите?

Не высовывайся, будь как все, сиди тихо – вот атмосфера тех лет в СССР. В большинстве НИИ люди часами не вылезали из курилок, травили анекдот за анекдотом, обсуждали все, что угодно: хоккей, очередной фильм по телевизору, институтские сплетни, где что достать (свободно купить что-то приличное в те годы было невозможно), вязали носки и свитера, бегали по магазинам. Работы, как таковой, почти нигде не было, везде правили серость и скука, порождающие равнодушие и пьянство. Гарантированы какие-то самые минимальные жизненные условия, чтобы не помереть с голоду (на современном языке - около 120 – 150 долларов в месяц), и полная уравниловка везде и во всем. Это и есть тот развитой социализм, который рухнул за три дня. Но на смену ему пришел социализм загнивающий с истошным воплем «Обогащайся, кто как может!», и люди стали даже с умилением вспоминать свое прежнее болото. А разные изобретатели красивых идей и нетривиальных решений практически в любое время в нашей стране могут рассчитывать лишь на косые взгляды: «Шибко умный!», и хорошо, если только на простое непонимание, без оргвыводов. Нефти много, кому надо – тем хватит, а эти шибко умные бог знает, до чего могут додуматься. Вот она, замедленная отдача от залпа «Авроры».

Еще несколько слов о любимой мной алгебре. Кроме Сан Саныча, на кафедре математики было еще несколько преподавателей алгебры и все они пользовались огромным уважением у слушателей. Алгебра началась сразу же с первого курса, с самых первых дней пребывания на факультете, а экзамены по алгебре

были одними из первых и наиболее трудных. Алгебра сразу же произвела естественный отбор: лучшая часть курса – те, кто лучше разбирается в задачах по алгебре, кто уверенно чувствует себя на экзамене. Такие люди быстро становились неформальными лидерами, признанными авторитетами на курсе. Чудесные (назначенные Чудой) авторитеты – командиры отделений и групп – в первые годы обучения не всегда были одновременно и неформальными лидерами, однако постепенно, через год-два, значение неформальных лидеров возрастало даже в Чудиной «административной вертикали». Нормальная жизнь побеждала.

Но все-таки одних красивых идей в криптографии недостаточно. Должна быть еще какая-то рабочая лошадка, повседневная, будничная теория, которая всегда необходима так же, как заводу, выпускающему автомобили, необходимы не только полные полета фантазии дизайнеры, но и конвейер и обслуживающие его инженеры. И вот такой рабочей лошадкой в криптографии является теория вероятностей и математическая статистика или попросту ТВИСТ. Статистика текста – это одно из самых основных понятий криптографии, еще Шеннон подметил преобладания встречаемости отдельных знаков в любом открытом тексте, будь то разговорная речь, деловая переписка, телефонный сигнал или компьютерный файл. Любой криптографический анализ начинается с подсчета и анализа статистики перехваченного шифртекста,

Лекции по ТВИСТу начались на третьем курсе и их нам читал Вадим Евдокимович Степанов, начальник Теоретического (это слово всегда писали с большой буквы!) отдела 8-го управления КГБ. За его спиной были многие реальные, или как их еще называли, боевые шифры, он отвечал за их анализ, стойкость, отсутствие в них каких-то критических ошибок, просчетов, недостатков, которые позволили бы американскому АНБ их взломать. Как можно дать гарантию такой надежности? Очевидно, что для этого надо иметь коллектив из очень высококвалифицированных и независимых экспертов, которые смогли бы изучить и обосновать все возможные попытки потенциального взлома, вероятность его успешного проведения, а также предложить реальные способы защиты от него. А руководитель должен обладать такой квалификацией, которая позволит ему стать экспертом работ этих экспертов, вынести окончательное решение о стойкости шифра и взять на себя ответственность за безопасность обрабатываемой с его помощью информации.

Это был человек широчайшего кругозора, практик, стоявший по своему научному уровню на голову выше всех остальных. Его абсолютно все уважали, а экзамен по ТВИСТУ был той чертой, которая отделяла еще не до конца созревшего слушателя от уже почти готового специалиста-криптографа. Лекции напоминали отлаженный заводской конвейер, все теоремы не так красивы, как в алгебре, но чрезвычайно важны в криптографии, нельзя пропустить ни одной фразы, ни одного слова, чтобы не сбиться с ритма этого конвейера.

После окончания 4 факультета я попал на работу к Вадиму Евдокимовичу в Теоретический отдел, смог понаблюдать его не только как ученого, но и как администратора, как руководителя коллектива. Его высочайшая квалификация и авторитет были в отделе бесспорными, он досконально разбирался во всех выполненных криптографических анализах, статьях, посвященных различным проблемам анализа и синтеза шифров, был полностью в курсе всех проводившихся в отделе работ, дискуссий и споров. Да, все это так, его превосходство и авторитет как ученого не вызывали ни у кого из сотрудников ни малейшего сомнения.

Но у меня была возможность сравнить атмосферу и порядки, царившие в Теоретическом отделе, с Курчатником, в котором работал мой отец. По воспоминаниям многих людей, директор института академик А.П.Александров, или просто А.П., как часто называли его сотрудники, был очень демократичным человеком, любил раскрепощенную атмосферу, шутки, розыгрыши, вел почти пуританский образ жизни. Эти качества во многом были присущи и сотрудникам Курчатовского института, многие из которых были фанатично преданы своей работе, своему институту. Курчатник создал вокруг института огромную инфраструктуру, включавшую в себя дома для сотрудников, детские сады, поликлиники, школы, клуб и многое другое. При социализме 70 – начала 80 –х годов огромное значение для людей имела возможность купить машину, получить садовый участок, улучшить свои жилищные условия, и все это было реально в Курчатнике.

А здесь, в Теоретическом отделе 8 управления КГБ, можно ли назвать царившие тогда порядки демократичными? В обсуждении криптографических проблем – да, безусловно, а вот во всем остальном - сомнительно. Машина, винтики – вот, пожалуй, более точная характеристика. Военная дисциплина, применяемая в рамках научной среды, к теоретикам, для которых очень часто требуется раскрепощенность и свобода. Ежедневный обход контролера в 9.00 утра: все ли на месте? Социалистическое соревнование, в котором по положительным баллам защита диссертации приравнивается к отрицательным баллам за несколько опозданий на работу. Реальные жизненные блага – в основном руководству, рядовым сотрудникам – горы пустых обещаний и бесконечные списки, очереди, записи.

Но ведь ты же военнослужащий, офицер, получаешь за это солидную (по советским, но не по западным меркам) прибавку к окладу инженера. Ты работаешь на военную промышленность, твои знания, идеи, результаты идут на то, чтобы обеспечить защиту от очень сильного и опасного противника – американского АНБ, как большой пылесос всасывающего и досконально анализирующего советские

шифровки. Может быть в этом случае жесткая дисциплина, сталинская машина и винтики – наиболее приемлемая форма работы?

Да, безусловно, все это так. Но когда-то обязательно от всего этого наступает усталость: усталость от положения безропотного винтика, от ежедневного контролера, от пустых обещаний квартиры, машины, гаража, дачи и еще бог знает чего, что я в избытке получал за годы своей службы в КГБ, от общей обстановки в стране, которой ты служишь. Со сталинских времен вся наша промышленность работала практически только на оборону, вся страна являлась большим лагерем, а за опоздание на работу отдавали под суд. Но постепенно стало ясно, что танками и ракетами людей не накормишь, что те страны, где выпускают качественные и конкурентоспособные товары для людей, бытовую электронику, легковые автомобили, одежду, продукты и прочие товары ширпотреба быстро развиваются и богатеют, а сталинский стиль в конечном итоге приводит к застою и упадку экономики.

Сталинский стиль в криптографии – это когда вся криптография должна принадлежать государству и работать только на государственные и военные цели, когда все криптографы – это винтики в большой государственной криптографической машине, руководимой криптографическим вождем наверху и массой чиновников-подхалимов снизу. Свободная конкуренция, рынок криптографических идей и предложений – исключены.

А свободная, ориентированная на потребности людей, а не вождей, экономика требует и свободной криптографии, простой, понятной, доступной, надежной, не связанной с прихотями чиновников. К таким требованиям советская криптография в конце 80 годов была явно не готова и при безусловно высоком уровне ее развития в СССР все мировые рынки сбыта оказались захваченными американцами практически безо всякой конкуренции со стороны уже «свободной» России. Машина и винтики вчистую проиграли борьбу за мировое влияние, за немалые криптографические деньги.

О Вадиме Евдокимовиче Степанове еще пойдет речь в этой книге. Сейчас же, рассказывая о нем, как о преподавателе теории вероятности, я могу сказать только одно: нашему курсу посчастливилось учиться у такого человека. Это был Профессионал с большой буквы. На мой взгляд, это – первично.

Но вернемся на факультет. Преподаватели математики, да и сама обстановка на 4 факультете казались более раскрепощенными, демократичными, чем та, в которую я попал позже в Теоретическом отделе Степанова. С одной стороны, университетская среда, порядки и обычаи просто по определению должны сочетаться со свободой, свободой жизни и творчества. А с другой – наглядный пример «истинных» военных был всегда рядом, перед глазами, постоянно напоминал о трагических последствиях увлечения хождением строем.

И вот начались спецдисциплины, т.е. предметы, непосредственно связанные с криптографией: основы криптографии, теория дисковых шифраторов, теория электронных шифраторов, теория шифрующих автоматов. Многое из того, о чем шла речь на этих лекциях, сейчас открыто опубликовано и обсуждается в INTERNET, что-то уже безнадежно устарело, как, например, теория дисковых шифраторов. Однако в большинстве случаев, о которых нам тогда рассказывали, речь шла об аппаратной реализации шифраторов, об изучении реализуемых преобразований над полем GF(2), состоящем только из двух элементов – 0 и 1. Электронный шифратор – это аппаратная схема на типовых логических элементах, описываемых простейшими операциями математической логики: сложением и умножением по модулю 2, а также отрицанием. Такие логические элементы сплетаются друг с другом множеством проводов, образуя в результате преобразование некоторого двоичного вектора-ключа, из которого вырабатывается двоичная гамма наложения на опять же двоичный открытый текст. Но уже тогда, в середине 70–х годов, было ясно, что типовые логические элементы и провода устаревают, что на смену им приходят интегральные микросхемы, содержащие встроенный процессор с возможностью выполнения гораздо более сложных преобразований, чем это можно сделать с помощью множества плат с проводами и транзисторами. В интегральных микросхемах уже не возятся с отдельными *битами*, а вся информация одновременно обрабатывается в них векторами, содержащими по несколько (обычно по 8) бит, *байтами*. А все предыдущие криптографические результаты в теории электронных шифраторов получены в предположении, что основной единицей информации является бит. Если «битовую» криптосхему напрямую использовать для реализации с помощью интегрального микропроцессора, то это будет очень примитивно, тривиально, приведет к неполному использованию всех преимуществ процессора, в конечном счете – к потере эффективности, скорости работы криптосхемы. А скорость работы при шифровании, например, высокоскоростного канала, передающего телевизионное изображение, играет первостепенную роль.

И вот в далеком 1975 году кафедра математики 4 факультета ВКШ КГБ начинает серию научно-исследовательских работ, призванных заложить основы шифров на новой элементной базе, в которых основным элементом будет не бит, а сразу двоичный вектор, байт. Кафедра математики, ее преподаватели пользуются огромным уважением у студентов-слушателей, к этой НИР привлекаются лучшие из них, готовятся и защищаются многие дипломы и диссертации. Неторопливо, шаг за шагом, нанизываются цепочки теорем, призванных обосновать выбор криптосхемы, гарантировать криптографические свойства, доказываются предельные теоремы и групповые свойства.

Вообще-то, середину 70-х годов я бы обозначил как водораздел в криптографии. В Америке появляется криптография с открытым распределением ключей, все существовавшие до нее криптографические системы блекнут перед теми преимуществами, которые таят в себе открытые ключи. Простота обмена ключевой информацией при системе с открытым распределением ключей дает возможность использовать надежную криптографическую защиту не только для военных или правительственных линий связи, но и в повседневной жизни практически любому человеку. Через 20 – 25 лет, в 90-х годах, так и будет, появится общедоступная гражданская криптография. Такие события, как открытие систем с открытым распределением ключей, случаются в истории крайне редко, честь первооткрывателей здесь принадлежит американцам. Однако система с открытым распределением ключей (или, как ее называют иначе, асимметричная система шифрования) не позволяет шифровать данные с высокой скоростью. Для гражданской криптографии появляется потребность в общедоступной высокоскоростной системе традиционного, симметричного шифрования, а асимметричная система используется только для шифрования ключей к симметричному шифру.

В 1979 году американцы впервые открыто публикуют алгоритм симметричного шифрования DES, предназначенный не для военных целей, а для коммерческих шифров, к которым в мире начинает проявляться большой интерес. Возможность военного противостояния - вещь эфемерная, выигрывает не тот, у кого больше ракет и танков, а тот, у кого народ лучше одет и накормлен, живет в хороших домах, ездит на дорогих автомобилях и не мается в очередях за туалетной бумагой. И обеспечивают благосостояние не добрые дяди из Госплана, а коммерческие фирмы, коммерческие банки, дорожащие каждым своим клиентом.

Первый же беглый анализ показывает, что алгоритм DES – устаревший, ориентированный именно на биты, а не на байты. Следовательно, он не может обеспечить высокой скорости шифрования при использовании в интегральных микросхемах, в компьютерах при *программной* реализации. Ну а по части стойкости – не надо петь хвалебных песен, что он сильно стойкий. Схема, с точки зрения криптоанализа, действительно ломовая, но далеко не оптимальная по скорости и сложности программной реализации. Придумывать танки мы и сами умеем не хуже американцев, а здесь появляется уникальная возможность ответить на американский танк советской легковой гоночной машиной, ничем не хуже танка, и посоревноваться с американцами в коммерческой криптографии.

Реально в конце 70-х – начале 80-х годов, усилиями кафедры математики 4 факультета ВКШ КГБ, в Советском Союзе был весьма достойный ответ на американский DES: шифры на новой элементной базе. Их скорость шифрования была на порядок выше, чем у DES.

Что было дальше – искушенный в советской действительности читатель уже без труда догадался. Правда, вопрос о том, делать или не делать советский стандарт шифрования, в повестке дня не стоял: раз американцы выпустили свой DES, то мы должны дать свой ответ, несмотря на то, что само словосочетание «гражданская криптография» вызывало у тогдашних криптографических начальников аллергию. А какой ответ? Вариантов несколько.

1) Разломать DES и раструбить об этом на весь мир. Проехали. Не ломается.
2) Сделать общедоступный советский стандарт шифрования, еще лучший чем DES, например на основе шифров на новой элементной базе. «А каких-то важных секретов американцам не выдадим?
   Ну и что из того, что новая разработка, на всякий случай лучше подстраховаться…»
3) Советский вариант ответа, известный уже много лет: скопировать американское изобретение и малость его перекрасить.

Советским стандартом десять лет спустя, в 1989 году стал слегка перекрашенный DES, со всей чиновничьей тупостью названный «алгоритм ГОСТ 28147-89», а еще десять лет спустя чиновники ФАПСИ стали плакать: «Ну почему же мы упустили мировые криптографические рынки»? Наверное, зелененьких захотелось…

И все же эту главу нельзя заканчивать на такой минорной ноте. Шифры на новой элементной базе, математическая основа которых была заложена на 4 факультете во второй половине 70-х годов в рамках проводившейся тогда НИР по теме «Проба», хотя и не стали общенациональным стандартом, но внесли очень весомый вклад в развитие гражданской криптографии в России. Благодаря простоте и скорости реализации, с помощью шифров на новой элементной базе в начале 90-х годов была построена система защиты телеграфных и почтовых авизо для Центрального Банка России. И если бы не эта основа, этот математический и криптографический базис, то зеленое знамя ислама, сшитое на деньги, выкаченные из России с помощью фальшивых авизо, могло бы дойти в 90-х годах до Ставрополя, Астрахани или Волгограда. Впрочем, об этом речь еще впереди.

Глава 4

Бытие

Полузакрытые системы, к каким, без сомнения, можно отнести 4 факультет, всегда вызывают повышенный интерес. Какие там были внутренние порядки, писанные и неписанные правила? Что за люди обитали на нем? Как там кормили-поили и одевали-обували? Да и вообще, прошло уже много лет, отделяющих современного читателя от описываемой поры, и все подробности жизни того поколения юных криптографов становятся ему любопытны. Насколько помню, постараюсь изложить некоторые подробности нашего бытия, повседневной жизни аборигенов 4 факультета в те времена.

Итак, все слушатели факультета – военнослужащие, рядовые, сержанты и даже, для разнообразия, есть старшина курса. Но москвичи живут по домам в московских квартирах, а иногородние - в общежитии на Велозаводской улице, недалеко от метро «Автозаводская». Каждый учебный день утром вся эта стая в повседневной военной форме слетается на Большой Кисельный и предстает перед отеческим взором Чуды. Повседневная военная форма одежды – это, в первую очередь, сапоги, к которым полагаются летом хлопчато-бумажные, а зимой полушерстяные галифе и курточка-китель. И, в общем, не считая сапог, надо признать, что одежда достаточно практичная и удобная, с одним дополнительным и очень важным достоинством: ее не жалко, каждый год на вещевом складе выдают новый комплект, заставляя при этом сдавать старые обноски (наверное, для простых солдат или зеков). Самое неприятное, естественно, - это сапоги, целый день нужно сидеть в них на лекциях, громыхать ими по улицам и в метро, бегать по лестницам на Большом Кисельном. На складе всем выдают яловые, но они очень тяжелые и неудобные, поэтому многие покупают себе легкие хромовые офицерские сапоги и в самом прямом смысле слова значительно облегчают свою жизнь. Даже Чудо закрывает на это глаза, к хромовым сапогам не придирается, видимо, есть на этот счет негласное распоряжение. Но вот появляться без разрешения на факультете в более цивилизованной парадно-выходной форме, включающей в себя брюки с ботинками, не разрешается. И тут сразу же – противоречие с правилами Московского военного гарнизона, согласно которым появление военнослужащего (рядового или сержанта) в общественных местах в Москве допускается только в парадно-выходной форме, а в повседневной форме он должен сидеть в казарме. Но казармы на 4 факультете нет, и Чудо наивно рекомендует нам попытаться объяснить это армейскому патрулю, если у того возникнут подобные вопросы. Но никто из нас не испытывает по этому поводу никаких иллюзий, поэтому большинство старается всячески избегать встречи с патрулем. Мне, например, за все 5 лет обучения на 4 факультете посчастливилось ни разу не попасться в военной форме на глаза патрулю.

И еще одна гнусная особенность военной формы – момент перехода с зимней на летнюю форму одежды. Дело в том, что рядовому и сержантскому составу в зимней форме полагается носить шинель и шапку-ушанку, а в летней – можно без шинели и в фуражке. Приказ о переходе заранее издает начальник Московского гарнизона, обычно это – середина апреля, а какая при этом будет реальная погода – его не интересует. В 1975 году, в мой первый «шинельно-сапожный» год, весна была очень теплой и уже в конце марта температура доходила до 20 градусов тепла. Все нормальные люди ходили уже в одних рубашках, а слушатели 4 факультета при этом в шинелях и шапках-ушанках вспоминали про свою обязанность «стойко переносить все тяготы и лишения военной службы» и, естественно, начальника Московского гарнизона самыми теплыми и пропотевшими словами.

Но выдавались дни, когда мы обязаны были появляться на факультете в «гражданке». Это дни так называемых оперативных нарядов, связанных, как правило, с приездом или отъездом каких-то правительственных делегаций, встречать или провожать которые на улицы Москвы выводили толпы народа. А будущие чекисты, в том числе и биномы, должны были в гражданской форме незаметно находиться в самой гуще толпы и предотвращать возможные инциденты.

- Гражданская форма одежды – это пиджак с галстуком, а не одежда для пикника и джинсов с кисточкой

Читатель, несомненно, уже узнал автора подобных изречений. Чудо тоже должен был быть в толпе народа и даже в таких антисанитарных условиях руководить своими подопечными. И руководил!

- Если поступят указания свыше, то они поступят от 28 столба
- Если возникнут вопросы, надо подойти к близлежащему офицеру.
- Лебедев пришел с рыбной сумкой из-под океана.
- Быть в резерве – это значит ходить вокруг меня.
- Оперативный наряд – это не сказка и не контрольная, где можно творить.

Обычно оперативные наряды были одноразовыми мероприятиями: приехали–уехали делегации и на этом все закончилось. Но один раз в начале 1977 года в Москве произошел настоящий террористический акт – взрыв на Щелковской линии метро. У нас в это время была очень трудная зимняя сессия, после которой всем хотелось немного расслабиться и отдохнуть. И вот, перед последним экзаменом (хорошо еще, что это была философия), объявляют приказ начальника всей Высшей Школы КГБ: каникулы переносятся на неопределенное время, на следующий день после последнего экзамена начинается новый семестр, форма одежды – гражданская, занятия – через день: день учимся, а день катаемся в метро, предотвращаем подобные теракты.

«Осторожно, двери закрываются!» - эта противная фраза надолго запала нам всем в память, а Горьковско-Замоскворецкая и Таганско-Краснопресненская (тогда еще Ждановско-Краснопресненская) линии метро до сих пор вызывают у меня грустные воспоминания о тех пропавших каникулах. Больше месяца мы катались по ним из конца в конец, наблюдая (особенно в конце рабочей недели), как дежурная на конечной станции безуспешно пытается вытащить из вагонов всех пьяных. В конце февраля кто-то где-то принял решение, что опасность уже миновала, и этот наряд отменили, а нам с начала марта дали две недели отобранных каникул.

Еще одно воспоминание о внематематических сторонах жизни 4 факультета – это наряды на Красную Площадь во время праздников 1 мая и 7 ноября. Здесь, в отличии от оперативных нарядов, все наоборот – нужна парадно-выходная военная форма и быть на виду у всех. Цепочками из слушателей 4 факультета перекрывали все улицы, выходившие на Красную Площадь, и обеспечивали строгий пропускной режим.

Самое гнусное в этом мероприятии было его начало – около полшестого утра, когда на Красную Площадь еще не хлынули разные зеваки и просто праздношатающаяся публика. Но дальше, после того, как бодрящий воздух прогонял остатки недополученного сна, становилось даже интересно наблюдать некоторые подробности праздничных мероприятий в натуре, без глянцевого блеска телевизионных репортажей. Например, то, как уже прошедшие парадным строем солдаты начинают демонстративно чистить выданными им белыми перчатками свои сапоги, как «физкультурники и спортсмены» по внешнему виду (стриженным затылкам) мало чем отличаются от предшествовавших им солдат, как переносят часто бывавшую во время этих праздников непогоду участвующие в демонстрации трудящиеся и тому подобный социалистический реализм.

Ну и, наконец, последнее, но наиболее будничное употребление слова «наряд» при описании бытия на 4 факультете – это суточные наряды по объекту – Большому Кисельному. Факультет не был монопольным хозяином этой купеческой усадьбы, кроме нас там были еще некоторые ответвления Высшей Школы КГБ, включая курсы переподготовки офицерского состава, переводчиков и какие-то хозяйственные службы. И вот примерно раз в месяц каждому из нас (за исключением «блатных», типа старшины курса) выпадал суточный наряд по объекту. Два офицера (часто не с нашего факультета) и три патрульных из числа слушателей 4 факультета на сутки, с 16.00 до 16.00 следующего дня, становились единой командой, отвечающей за все и вся на объекте. Патрульных было три, но они сменяли друг друга через каждые 2 часа, а остальное время отдыхающая и бодрствующая смена отсыпались в отдельной каморке караульного помещения, иногда расписывая при этом пульку «с болванчиком». Дежурный патрульный днем должен был разгуливать по внутреннему купеческому дворику и всем своим видом подчеркивать, что это – военное заведение и порядки тут серьезные, а ночью постоянно проверять сохранность печатей на особо охраняемых помещениях типа склада арттехвооружений и спецбиблиотеки. Это в теории. На практике, естественно, дежурный патрульный страдал от безделья, ночью, как правило, старался вздремнуть где-нибудь в укромном уголке, а днем – поменьше попадаться на глаза разным начальникам.

В первые годы моей учебы патрульного еще вооружали автоматом без патрон – так, для боевого вида, припугнуть потенциального несведущего террориста. Потом даже этот декоративный автомат был заменен на обычный штык-нож, который надо было носить на поясе с грозным видом. Вообще про то, как математики обращались с боевым оружием, по факультету ходило несколько легенд. Легенду про то, как Сан Саныч в молодости использовал штык-нож, я уже рассказывал в предыдущей главе, в более поздние офицерские годы он неизменно входил в число «лидеров» по случайным выстрелам из пистолета в караульном помещении при сдаче боевого оружия. А одна история, связанная опять же с пистолетом при несении караульной службы, в качестве легенды долго ходила по факультету как пример того, к чему может привести горячее желание стать «истинным» чекистом.

В семье не без урода, и в здоровой атмосфере 4 факультета находились люди, желающие сделать себе карьеру на стукачестве. Особенно отличался этим один человек, назовем его просто Д., который в какие-то древние года, еще до моего появления на факультете, был старшиной курса, а потом, получив офицерское звание, был оставлен за эти заслуги на какой-то кафедре работать в своем прежнем амплуа. И вот довелось ему однажды попасть в суточный наряд самым главным, т.е. дежурным, которому, как и полагалось, был выдан для этого на сутки пистолет.

Пистолет в кобуре, прилаженный к задней части корпуса, вызывает неудобства, особенно в туалете. И вот Д., посетив это святое место, в котором равны генерал и рядовой, отстегнул мешавший ему пистолет вместе с кобурой, положил его на сливной бачок и забыл там. Через некоторое время молодой патрульный из числа отдыхающих не на шутку перепугался: в туалете он нашел бесхозный боевой пистолет! Молодому – простительно, наверное, слишком хорошо изучал Устав караульной службы и все время внимательно прислушивался, не гавкнет ли где караульная собака. Но Д., когда он принес ему найденный пистолет, сразу почувствовал себя героем: его наряд предотвратил нападение на охраняемый объект и завладел вражеским оружием! Мысленно прикидывая, какую награду он за это получит, Д. сразу же начал докладывать об этом по телефону дежурному по Высшей Школе КГБ:

- Товарищ дежурный, на объекте Большой Кисельный обнаружен оставленный без присмотра табельный пистолет Макарова, серийный номер…

И тут что-то в его мозгу щелкнуло. А может не в мозгу, а в какой-то иной части тела, только он наконец-то догадался хлопнуть себя по тому месту, где должен был болтаться его собственный пистолет. Страшная догадка поразила Д. и он вмиг раскрыл тайну несостоявшегося нападения неизвестного на охраняемый им объект. Хорошо, что дежурный по Высшей Школе КГБ оказался человеком с чувством юмора и не стал придавать последовавшему вслед за этим бодрым рапортом жалкому лепету серьезного значения.

Ну и вспоминая прочие нематематические развлечения на 4 факультете, нельзя не вспомнить наших преподавателей по физкультуре.

- Кросс 3 километра! Вырабатываем суровость!

Это были люди, удачно вписывающиеся в наше повседневное бытие тем, что позволяли сменить математическую среду на различные молодецкие забавы. От изобилия математики может быстро наступить переутомление, если это изобилие не прерывать чем-то, что математике абсолютно противоположно. И вот два раза в неделю такое прерывание наступало в виде занятий по физкультуре. Тут были самбо, легкая атлетика, плавание, лыжи, спортивное ориентирование, стрельба и, может быть, что-то еще. Много позже, уже после увольнения из КГБ, я очень часто вспоминал такой режим чередования умственного труда и физической разрядки: это, бесспорно, было очень полезно, помогало долгое время сохранять работоспособность и, как было принято говорить в то время, жизненный тонус. И, в общем, настроение у большинства слушателей 4 факультета было достаточно оптимистическое, и в такой обстановке учиться и постигать многие достаточно сложные математические премудрости, а также переваривать «тяготы и лишения военной службы» было даже интересней, чем в обычном ВУЗе.

Глава 5

Microsoft solution partner

Чрезмерное увлечение математикой чревато последствиями, как и в компьютере: если загрузить слишком много программ, то произойдет переполнение памяти и зависание. Мне приходилось слышать множество фантастических историй о том, как у излишне переусердствовавших студентов университета происходило зацикливание, какой-то сдвиг в психике. Так, например, один молодой человек задался целью выучить наизусть книгу Шабата «Комплексный анализ». Всем знакомым, кого встречал в читалке, он предлагал открыть эту книгу на случайной странице и проверить его. Потом его потянуло написать тезисы к новой Программе КПСС и лично отнести их в Кремль. «Где у вас тут принимают тезисы к новой Программе КПСС?» - спросил он на Красной Площади первого встречного милиционера-чекиста. Приняли по полной программе.

А как жили математики на 4 факультете, не было ли у них подобных сдвигов от большой нагрузки? На нашем курсе - не было, и в первую очередь благодаря тому коллективу, который сложился, притерся, спаялся и даже малость проспиртовался уже где-то через полгода после поступления на факультет.

Позже здесь, в Корее, пригласили меня однажды на семинар, который назывался «Microsoft solution partner». Надо заметить, что такие семинары весьма сильно отличаются от наших скучных симпозиумов и конференций. В холле – игровые автоматы, не хочешь слушать – иди замочи пару монстров или полюбуйся на пышногрудую каратистку, которая своими деревянными движениями напомнила мне наше Чудо. Обязательно накормят, напоят до отвала и преподнесут какой-то подарок с эмблемой Microsoft. На сей раз это был спортивный рюкзачок, забитый разными брошюрами, рекламой, фломастерами, CD – дисками. И

вот, разбирая эти сокровища, я вдруг обнаружил среди них … колоду игральных карт, еще одну нашу традиционную фишку! Настоящие, новые карты с надписью на рубашке «Microsoft office 2003». Вот ведь с юмором ребята, 10 очков им в пулю! Сразу стало ясно, чем они занимаются в офисах Microsoft.

Примерно тем же, чем и на 4 факультете. Преферанс мы любили за его «математичность», за точный подсчет вариантов, за элементы теории вероятности (прикуп), за возможность покарать зарвавшихся, пренебрегающих точными расчетами в угоду эмоциям и азарту. Он стал для нас своеобразным наркотиком, без пульки не обходились скучные лекции по марксистско-ленинской философии и политэкономии, основам радиоэлектроники, а также летние походы и московские пьянки. На факультете образовывались стойкие преферансные группы, любимым местом сбора которых были уединенные комнаты спецбиблиотеки, где разрешалось работать с секретными документами и куда был ограничен доступ посторонним, в том числе и нашему Чуде. Чаще всего игра шла не на деньги – это слишком тривиально. гораздо интереснее было придумывать различные наказания проигравшим – пропрыгать на одной ноге (одном сапоге) от аудитории до Чудиного кабинета, издать громкие ослиные крики, отжаться от пола, поднять несколько раз пудовую гирю. Летом, в походе на байдарках, традиционным наказанием было натаскать дров и приготовить еду.

В те времена было много великих свершений типа БАМа (на Б начинается, на Ь кончается, в мужиках нуждается – Байкало-Амурская магистраль), и, чтобы тоже быть причастными к чему-то грандиозному, монументальному, мы решили писать пулю на 1000, чтобы окончить ее вместе с 4 факультетом и получить в конце обучения нечто вроде диплома специалиста по преферансу. Долгих два года наша преферансная компания шла к намеченной цели, по крупицам собирая эти фантастические 1000 очков в пуле. Один раз, на сборище в честь 23 февраля, Витек, получив на мизере заслуженный паровоз, совершил святотатство: воспользовавшись некоторым замешательством остальных преферансистов, вызванного бурным обсуждением подробностей подцепления паровоза, он, как партизан на допросе в гестапо, попытался скомкать пулю и проглотить ее. Но остальные гестаповцы были еще настолько трезвы, что быстро скрутили ему руки, раскрыли рот и вытащили из него драгоценнейшую бумагу. Разгладив и проутюжив сей документ, общество единодушно дополнило традиционные правила преферанса: за попытку сжирания пули – 100 очков в гору.

Однако пора вернуться к летописи 4 факультета и описанию каких-то других, положительных черт его аборигенов, а то все время домино да карты. А где же что-то возвышенное, духовное? Где, например, театр?

На Таганке. И на 4 факультете сразу же оценили его. Это был один из немногих очагов раскрепощенности и свободы, отдушина в тухлой атмосфере брежневских лет. Даже Чудо не могло не отметить: «По Таганке и еще кое по чем заскучали».

Чтобы современный молодой читатель смог по достоинству оценить Таганку тех лет, надо сначала окунуться во времена застоя, попытаться понять мысли и чувства тех, кто жил тогда в СССР.

Это что за Бармалей
Нагло лезет в мавзолей
Брови черные, густые,
Речи длинные, пустые
Он и маршал, и герой,
Отгадай, кто он такой?
Кто даст правильный ответ,
Тот получит десять лет

Всем и вся безраздельно правит КПСС. Во главе партии – древние старцы, которым нужен уже только «покой, кефир и теплый сортир». Почти вся экономика, по традиции, работает только на выпуск танков и ракет, но в Сибири открыли много нефти и поток нефтедолларов позволяет еще поддерживать минимальный жизненный уровень народа. Но только в Москве! Километров 100 от Москвы – жуть с пистолетом! Практически ничего, кроме водки и хлеба, в сельских магазинах нет. «Длинная, зеленая и пахнет колбасой» - электричка из Москвы.

И во всех газетах, по радио и телевидению, по советской традиции одно и то же: коммунистическое пустозвонство, показуха, лозунги типа «сегодня работать лучше, чем вчера, завтра - лучше чем сегодня», откровенная ложь. Большинство людей уже не верит ни в какие идеалы, озабочены только тем, где, как и что достать, обменять, записаться в очередь, получить льготы, ухватить.

Планы партии – планы народа!

вещала аршинными буквами с крыш домов партийная пропаганда.

Расплеваться бы глиной и ржой
С колеей этой самой чужой…

доносился в ответ хриплый магнитофонный голос из открытых окон.

Песни Высоцкого – это песни того поколения, задавленного повседневными заботами о своем существовании, это отдушина, глоток свежего воздуха в атмосфере, отравленной ядовитыми парами развитого социализма.

Конечно же, в 20-летнем возрасте было другое понимание. Все мы были комсомольцами, ходили на комсомольские собрания и субботники, слушали политинформации, лекторов-пропагандистов. Но все это – чисто формально, раз так положено – значит проще подчиниться, чем выступать и наживать себе какие-то неприятности. А Таганка и Высоцкий – это по собственному желанию, от души.

Очередь за билетами на Таганку занимали с вечера. Всю ночь, сменяя друг друга, дежурили, боясь пропустить очередную перекличку. И вот – долгожданный момент, открытие касс. Сейчас ночные бдения будут вознаграждены долгожданными билетами. Как бы не так! Слишком большая была в то время ценность – билеты на Таганку. Перед самым открытием касс появляется театральная мафия и физически оттесняет всю очередь от заветного окошка.

Решение созрело быстро. Мы же КГБ! Оденем военную форму, организуем порядок и справедливое распределение духовных благ, попытаемся противостоять мафии. Наивные мысли! Первая же попытка их реализации кончилась провалом: все инициаторы кампании «за билетами - в военной форме» были наголову разбиты намного более могущественной театральной мафией и доставлены в милицию, а на факультет пришла соответствующая «телега». Как к ней относиться?

Чудо, по традиции, разродилось афоризмом:

- И они пошли на Таганку подряжаться администрации Высоцкого и других французов

и уже собиралось устроить шумную кампанию по искоренению «духа Таганки». Чему там могут научить будущих хороших военных? Только плохому, например:

- Всякое дело можно делать тремя способами: правильно, неправильно и так, как это делают в армии.

Сегодня носит «Адидас», а завтра Родину продаст. Сегодня слушатель ломится на Таганку, а завтра будет «сидеть к политинформатору абсолютным корпусом», носить «джинсики, пупсики, фупсики, показывая, какой он почти ковбой», не сумеет избежать «подстольного застолья», будет «смотреть на нехлебный квас», В общем, «все это говорит о недисциплинированности четвертого курса, о том, что он еще не дорос до четвертого и пребывает в эмбриональном состоянии до первого».

Но старшие товарищи быстро поправили Чудо. Если это дело шибко раскручивать, то виновными окажутся в первую очередь начальник курса и руководство факультета, не сумевшие привить будущим чекистам основ марксистско-ленинского мировоззрения и стойкости к проявлениям идеологических диверсий явными и тайными врагами всего прогрессивного человечества. Поэтому все ограничилось замечанием командира отделения: плохо погладили форму, перед тем как идти в ней на Таганку.

Но песни Высоцкого пели везде: в Балашихе и в походах, в общежитии и в аудиториях, на формальных и неформальных сборищах.

Солдат всегда здоров,
Солдат на все готов,
И пыль как из ковров
Мы выбиваем из дорог…

разносилось на лагерных сборах при шествии строя, напоминавшего случайное и равновероятное распределение.

Помаши рукой земле
Дяде мудрому в Кремле
Ведь ты летишь на фирменном сопле…

пугал окрестных гаишников ГАЗик, в котором нас вывозили поразмяться, побегать и пошуметь холостыми выстрелами на военных полевых игрищах в Балашихе.

Товарищ Сталин, Вы большой ученый
В языкознании познавший толк
А я простой советский заключенный
И мой товарищ серый брянский волк

доносилось в той же Балашихе из казармы-барака после отбоя.

Балашиха была чудесным местом. Древний еловый лес, свежий воздух, отдых от математики. Песни под гитару, фишки, вылазки за водкой, шумные и разудалые игры в войну, холостые патроны, припасаемые на лето, к походу на байдарках – все это разрядка, накопление сил перед достаточно сложной летней сессией.

Формально в Балашихе мы проходили курс военной подготовки. Каждому там выдавали персональный автомат АКМ, противогаз, офицерскую сумку-планшет, компас, карту и почти каждый день нас вывозили на какие-то полевые занятия, темами которых были: взвод в обороне, в наступлении, в засаде, ориентирование на местности, ночное ориентирование, стрельбы, боевое гранатометание и что-то еще.

К каждой учебной группе был приставлен военрук – обычно офицер в чине подполковник-полковник. От общения с этими людьми оставалось, в целом, приятное впечатление: они осознавали, что сделать из нас хороших военных нельзя, а можно вместе немножко поиграть «в войну» и дать возможность этим яйцеголовым побегать и порезвиться на свежем воздухе. Никаких неприятностей от этих людей у нас не было, они пользовались уважением и даже цитировались, как классики:

- А работа без плана это не работа, а так, муть!
- А начальник курса – это не женский половой орган, чтобы им прикрываться!

Единственное мое квази-печальное воспоминание – наш военрук не дал мне однажды прихватизировать для летнего похода мину-сюрприз. Вообще припрятывание «на сувениры» холостых патронов и боевых имитационных средств в Балашихе приняло повальный характер, в конце каждой полевой вылазки в противогазных сумках у большинства находились припрятанные неизрасходованные холостые патроны, взрывпакеты, сигнальные ракеты, в общем, все, чем удавалось разжиться. И вот один раз у меня в сумке уже лежала крупная добыча – настоящая мина-сюрприз! Это металлическая трубка длиной сантиметров 20, с детонатором. Если за него дернуть, то через несколько секунд мина начинает противно шипеть и свистеть, а затем из нее вылетает несколько сигнальных ракет. Для летнего похода – классная штука! Вечерком, когда стемнеет, дернуть у костра детонатор… Это не то, что тривиально кинуть в костер горсть холостых патронов. В общем, жажда припрятать эту мину у меня была огромная, но наш военрук, по-видимому, закрывая глаза на холостые патроны и взрывпакеты, посчитал (несправедливо!) что мина-сюрприз – это уже слишком и вел скурпулезный учет всех взорванных мин, благо их было немного, всего около десятка. Пришлось своими руками расправиться с этим сокровищем и отдать ему скелет от мины – пустую трубку.

Но это – наши военные начальники. А были еще и административные.

На втором курсе, опрометчиво посчитав, что в деле воспитания хороших военных достигнуты определенные успехи, Чудо отправил с нами в Балашиху своего заместителя, капитана. Этому товарищу следовало родиться лет на 40 пораньше. В 30-х годах из него бы получился хороший кум где-нибудь на Соловках, где кончалась власть советская и начиналась Соловецкая. Но в 1976 году он явно страдал на работе от ничегонеделания. Отправленный на 4 факультет как в наказание за какую-то пьянку, он сидел с Чудой в одном кабинете, и одно это уже развивало в нем садистские наклонности и желание отомстить всему свету. И вот такой случай представился: он во главе курса едет на сборы в Балашиху. Две недели он – царь и бог, может раздавать этим яйцеголовым направо-налево разные изощренные наказания, а они будут

скулить у его ног и просить о пощаде. И тогда он сможет насладиться тем, как падет с этих математиков их ореол учености, как они превратятся в обычных холопов, его холопов, которых он сможет казнить или миловать по любой своей прихоти.

Так сказка сказывается, а в реальности свое царствование надо начинать, конечно же, со строевой подготовки. Алгоритм следующий: учебная группа (около 25 человек) выстраивается по квадрату, в центре – Он, с прутиком-кнутиком в руке, небрежно постегивающий им по своему сапогу.

- Строевая подготовка – 45 минут хождения строевым шагом по квадрату, нога должна задираться на 20-25 сантиметров от земли. Если замечу, что задираете не так, накажу.

Ой, мужик, ты чего-то блефуешь. С нами так никто никогда не разговаривал. Сейчас обозлишь против себя всех, сумеешь ли потом справиться? Ведь даже Чудо, при всех его чудачествах и афоризмах, никогда не опускался до такого тона, до такой формы общения. Ты как в преферансе: решил упасть, играть мизер, а есть ли у тебя для этого фишки? Или надеешься на две семерки в прикупе?

- За разговоры тоже буду наказывать. Начали.

Прошло 30 минут, затем еще 10. Пора проявлять свою власть, наказывать.

- Низко ноги задираете. Всей группе – дополнительные полчаса строевой в личное время.

И с довольной улыбочкой похлопывает себя прутиком – я вам не Чудо, со мной шутки плохи.

Упал. Фишки на руках на мизер нет. На прикуп надеялся, на испуг? Напрасно. Дополнительные полчаса быстро пролетели, теперь пора делать паровоз.

- Личное время – лишнее время

Сначала отдельные возгласы, затем общий гул:

- Нам не нужно личное время!
- Хотим и дальше заниматься строевой подготовкой!
- Строевая подготовка – основа всех основ!

Не осознал еще наш незадачливый Цезарь всех последствий своих действий. Сидит у себя в комнатке, напротив плаца, готовится к каким-то экзаменам по марксистско-ленинской философии. А под окном у него – учебная группа, целиком и полностью, яростно задирая ноги, с лошадиным топотом и грохотом добровольно, в личное время, занимается строевой подготовкой. Зрители с интересом наблюдают это невиданное зрелище.

- Свободу 422 группе!
- Братья, мы с вами!
- Фашизм не пройдет!
- Даешь всеобщую строевую!

Стали собираться зарубежные гости – «истинные» чекисты, проходящие здесь же, в Балашихе, переподготовку. Бунт биномов – такое и представить себе невозможно! Время идет к вечеру, скоро ужин и отбой, как угомонить разошедшуюся группу? А вдруг начальство узнает? (Узнает, узнает, непременно. Уж «истинные»-то наверняка уже настучали.) Из окна, как белый флаг, высовывается капитанская голова: «Давайте поговорим!».

Паровоз – так по полной программе, всучить ему все, что только можно.

- Хотим строевую вместо ужина!

- Хотим строевую после отбоя!
- Ква-драт! Ква-драт! Ква-драт!

Темнеет. А вот и начальник лагеря показался.

- Что тут у вас происходит?
- Личное время – лишнее время!
- Хотим строевую!
- Готовимся к экзамену по строевой подготовке!
- Хотим готовиться и после отбоя!

Долгожданный миг победы! Наш капитан вынужден объяснять ему, почему вдруг у целой группы яйцеголовых математиков вспыхнула такая жгучая любовь к строевой подготовке. Жалкое мяукание, а ведь еще совсем недавно был таким орлом с прутиком в руке. Не зарывайся!

Потом, конечно же, были разборки, угрозы отчислить с факультета командиров группы и отделений, комсоргов и еще каких-то –оргов. Пошумело, пошумело и улеглось. Личное время – где, в каком уставе прописано, что в это время нельзя добровольно заниматься строевой подготовкой? А наш капитан нашего окончания факультета так и не увидел: вскоре после этой памятной Балашихи его куда-то перевели. Наверное, на повышение.

Зато дальше последняя Балашиха была на удивление тихой и спокойной. Капитан старался иметь с нами поменьше дел, воцарилось самоуправление, фишка и вылазки за забор. Легко было вылезти изнутри, где были горизонтальные перегородки, служившие ступенями к свободе. Однако путь обратно был намного сложнее. Гладкий и высокий деревянный забор, без щелей и ступеней, преодолеть который надо было аккуратно, не разбив и не растеряв драгоценной жидкости из офицерской сумки-планшета, в которую входило ровно 3 бутылки водки: две горлышком вверх, одна – вниз. Как и всяким партизанам, нам оказывало неоценимую поддержку местное население, часто прогуливавшееся вдоль этого забора.

- Ну что, курсантик, давай подсоблю!

Здоровый мужик своими сильными руками, как домкратом поднял меня до требуемой высоты забора, а там уже встречали свои братья по разуму.

В королевстве где все тихо и складно
Где ни войн, ни катаклизмов, ни бурь
Появился дикий вепрь огромадный
То ли буйвол, то ли бык, то ли тур.

И никакой математики!

Глава 6

Экзамены

Но вот наступает время, когда сжимаешься как пружина. Это – сессия. Здесь пора доказывать, что чего-то стоишь, что не хуже других, что учишься в элитном учебном заведении не зря. К экзаменам был подход весьма рациональный. Есть экзамены высшей категории – алгебра, мат.анализ, ТВИСТ, на них – не до шуток, запросто могут заклевать так, что в конце концов выгонят с факультета или переведут в группу к радистам. Готовились к ним, как правило, до посинения, пытаясь во всем разобраться, понять, прорешать все задачи, заучивая по несколько раз различные определения и исходные понятия, по которым затем уже можно что-то домыслить самостоятельно. Конспекты лекции были практически у всех, мало кто был настолько уверен в своих силах, что осмеливался их игнорировать.

Дни подготовки к этим экзаменам – дни ужасов и кошмаров. По факультету ходило неисчислимое количество историй, как предшествующие поколения пролетали на алгебре или ТВИСТе, как сыпались на

них в изобилии двойки, как потом выгоняли прямиком в Советскую Армию едва ли не четверть людей из учебной группы. Главное – не скатиться в примитивную зубрежку. Все вызубрить было абсолютно невозможно, а если разобраться, осознать, прочувствовать – уже легче, проще, увереннее. А дальше по аналогии можно что-то домыслить и в разумных пределах дофантазировать.

Г.П. Толстов всегда говорил: «Последний день перед экзаменом постарайтесь закончить заниматься пораньше. Посмотрите телевизор, погуляйте, развейтесь, выспитесь. Тогда на экзамен вы придете со свежей головой, а это очень важно». Да, действительно, ни у кого никогда не было уверенности, что выучил абсолютно все, да все, в том числе и преподаватели, понимали, что это невозможно. «Ответил на билет – экзамен только начинается» - еще одна любимая поговорка Сан Саныча, который больше всего на свете любил задавать на экзамене нетривиальные задачи. У В.Е. Степанова была своя манера принимать экзамен – сначала дополнительными вопросами и задачами определить верхнюю границу знаний и сообразительности, а затем потихоньку опускать ее до уровня, когда человек начинает чувствовать себя уверенно.

Но каждый сданный такой экзамен сразу же прибавлял уверенности в своих силах, гордости и авторитета. Это не какая-нибудь туфта типа Истории КПСС, на которой тройку можно было выпросить «за пролетарское происхождение». Это были экзамены по основам будущей специальности, специальности редкой и загадочной, их принимали талантливые люди, преданные своей профессии и увлеченные своим делом, на них практически никогда и никому не делали поблажек. И если ты прошел все эти чистилища – появляется самоуважение. ТВИСТ сдал – можешь жениться.

Математика – точная наука. На этих экзаменах нам твердо втолковали, что в ней лучше не блефовать, не говорить того, в чем не уверен, не злить преподавателя фразами типа «с точностью до наоборот». Если списываешь – то списывай с умом, так, чтобы потом сам смог разобраться в списанном и все детально разъяснить. Лучше не лезь в дебри, в которых не до конца разобрался, старайся всячески выпячивать и использовать то, что знаешь лучше. А самое главное – старайся всегда иметь запас прочности в виде знаний осознанных, основательно пропаханных несколько раз, прочно засевших в голове. Лучше помучиться один раз при подготовке в сессию, чем потом терять каникулы на подготовку к пересдаче. Никаких академических отпусков, задолженностей, особо длинных хвостов на 4 факультете не было: получил два балла – пересдаешь в каникулы или вскоре после их окончания. Три неудачных попытки – сразу же в Советскую Армию, все слушатели факультета – военнослужащие, уже принявшие присягу, так что отчисленный просто переводился за несколько дней в какую-нибудь обычную войсковую часть, и совсем не обязательно близко к Москве. Жесткая система естественного отбора.

Но готовиться к экзаменам можно дома. Сессия – это отдых от Чуды, не надо каждый день одевать военную форму и бежать сломя голову к утреннему построению. Хорошо известно, что куча народа мало способствует серьезной подготовке, лучше всего готовиться в уединенной обстановке, в тишине и спокойствии, подальше от общей массы. И здесь мы сразу же оценили отсутствие казармы. Первый курс – один из самых сложных на 4 факультете, больше всего идет отсев на первой и второй сессиях, к таким тяжелым экзаменам еще не привыкли, нет опыта. Если бы сюда еще добавилась казарма, постоянное скопище народа в одном месте, то это, несомненно, сильно усложнило бы нашу подготовку. А нам чуть ли не в открытую говорили: перед основными экзаменами по математике забудьте обо всем остальном. Естественно, не Чудо, он в сессию явно скучал.

Были и экзамены средней категории: физика, аналитическая геометрия, математическая логика, теория функций комплексной переменной и некоторые другие. На них, как правило, особых сложностей ни у кого не возникало, так, немного понервничаешь и все. Это все-таки не основные профильные предметы, все преподаватели это понимали и на них особо не зверствовали.

В 1976 году в Москве началась очередная шумная кампания по борьбе за образцовый город, в котором должны были быть образцовые институты и в них образцовые факультеты. И вот с какого-то бодуна чиновники придумали параметры образцового факультета: 15% отличников, 75% учатся только на хорошо и отлично, а двоечников нет вообще. Преподаватели на 4 факультете относились с юмором к подобным творчествам, особенно в преддверии сессии, но начальник факультета, генерал, взял под козырек и сказал «Есть». Партия прикажет – сделаем! А на чем поэкспериментировать? Попробуй, поборись за образцовый факультет на алгебре или на ТВИСТе, когда там принимают экзамены люди независимые и дуракостойкие, зубы себе только обломаешь и растеряешь все жалкие остатки своего авторитета. Поэтому в качестве подопытного кролика был выбран экзамен по физике, средняя весовая категория.

Про физику можно сказать несколько слов отдельно. Физика к криптографии имеет довольно косвенное отношение, для общего развития и культуры она у нас была два первых года. Лекции читал бессменный лектор Анатолий Тимофеевич Иванов, ласково прозванный в народе Собакиным. Он был человеком весьма увлеченным своим предметом, его лекции были очень эмоциональными, но записывать их было практически невозможно. Два часа он бегал с мелом около доски, торопливо что-то писал на ней и с жаром пытался объяснить аудитории написанное. Готовиться к экзамену по физике по конспектам было

невозможно, обычно подготовка сводилась к тому, чтобы пару раз пробежать какой-нибудь стандартный учебник. Экзамены он тоже принимал весьма эмоционально, иногда блистая перед экзаменующимися своей эрудицией и кругозором.

И вот Собакину довелось испить горькую чашу борьбы за образцовый факультет. В очередную сессию сверху, из учебной части, ему были спущены проценты отличников и хорошистов, которые по советской традиции надо было выполнить и перевыполнить.

Из нашей группы в 25 человек первые 20 – только пятерки! Запас прочности для образцового факультета создан. Еще немного – и можно разворачивать борьбу за сверхобразцовый факультет, в котором все 100% - одни отличники. А мы еще сдуру что-то читали, как-то готовились к этой физике! Главное – попасть в первую двадцатку, в первые проценты. Ближе к обеду, видимо, чувство голода стало побеждать у принимавших экзамен то воодушевление, с которым они восприняли очередное постановление партии и правительства, и лажа эта закончилась. Пошли четверки и в конце – даже одна тройка. Но все равно, поборолись хорошо, показали сомневающимся, что воодушевленное партийное слово способно творить чудеса.

Что-то пока маловато в этой книжке упоминался компьютер, может и не было его тогда на 4 факультете? Был, да еще какой! Советский компьютер «Рута-110», целая комната, уставленная шкафами с мигающими в них разноцветными лампочками.

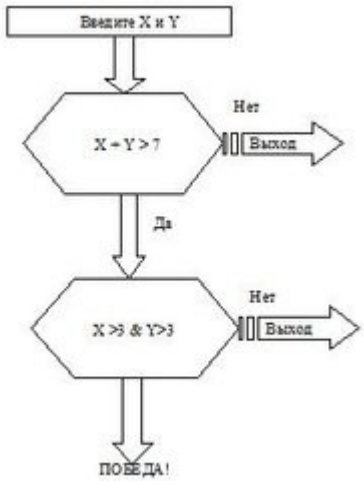
Первое посещение этой комнаты и очная ставка с компьютером состоялись у нас где-то на 2 курсе. Перед самой комнатой был небольшой предбанничек, где всем пришедшим туда слушателям предлагали одеть на сапоги музейные тапочки: от пыли и грязи компьютер часто ломался, от малейшего дуновения ветерка - тоже. Советская электроника, проводки и транзисторы в неимоверных количествах, огромные кастрюли с магнитофонной лентой, магнитные диски размером с автомобильное колесо, перфоратор для записи программы на перфоленту (ленточка обычной бумаги с кучей дырок на ней), спирт для протирки – вот основные характеристики первого увиденного мною компьютера. Про его производительность ничего сказать не могу, поскольку основную часть времени «Рута-110» была сломана, на профилактике или просто закрыта по техническим причинам. Язык программирования – машинные коды, набиваемые на перфоленту. Ошибся при набивке хоть в одном знаке – перебиваешь всю ленту.

Чтобы повергнуть в окончательный экстаз современных программистов, приведу одну фразу из ее технической документации:

«Все пакеты магнитных дисков устанавливаются на устройства, номера которых соответствуют номерам устройств в адресах секторов, записанных на пакетах.»

Эта фраза служила у нас в качестве достаточного (но ни в коей мере не необходимого!) теста на трезвость. Выдал, не запутался, язык не сломал – значит еще трезвый как стеклышко, продолжай дальше. Но это удавалось единицам, остальные же отрубались на этих секторах-устройствах-пакетах после первых пяти слов хоть трезвые, хоть «посмотревшие на нехлебный квас».

Чтобы реально подготовить и отладить на «Руте-110» какую-нибудь простенькую программу, типа:



требовалось около месяца. Сначала пишешь в ничем не повторимых машинных кодах программу, затем сломя голову рвешься после последней лекции в перфораторную успеть занять очередь на дятлоподобное чудо техники, на котором надо надолбать пару метров машинных кодов. Ближе к концу одно неверное движение руки – и ленточка превращается… В общем, все по новой. С N-ой попытки ленточка набита,

аккуратно скручена и как большое сокровище спрятана в баночку. Остается урвать момент, когда «Рута-110» будет на что-то способна и всунуть в нее свой дырявый серпантин.

Ежику понятно, что такой компьютер скорее отбивал всякую охоту иметь дело с ЭВМ. Теория - лекции по программированию - естественно были почти такими же, на них нам рассказывали про машинные коды для «Руты-110», кое-что про ассемблер, да про традиционные стрелочки-ромбики-прямоугольнички – блок-схемы. Отношение к этим лекциям было соответствующее, сделать какие-то задания по программированию удавалось единицам, остальные довольствовались теоретической подготовкой. Ехидный лектор, человек с юмором, часто любил строить разные каверзы на экзамене:

- Вы на машине были?
- Да, конечно.
- И что там запомнили?
- Перфоратор, накопители, считыватели.
- Не припомните, где там компилятор?

Человек судорожно пытается вспомнить назначение тех огромных шкафов, которыми уставлен машинный зал. Нереально. Остается надеяться на удачу.

- Как входишь, сразу же первый справа.

Мимо. Выходя из аудитории, сразу же попадает в окружение ожидающих своей участи.

- Что спрашивал?
- Где компилятор.
- Ну и где?
- Кто его знает! Я сказал, что первый справа, неверно.

Следующий уже учел этот опыт. На тот же вопрос уверенно отвечает, что слева. Опять мимо.

И только после нескольких неудачных попыток в какой-то голове, еще не окончательно задолбанной перфоратором, просыпаются знания:

- Мужики, так компилятор – это же программа!

«Прав был товарищ Сталин: кибернетика – буржуазная лженаука!» - такое резюме оставалось в душе у большинства из нас в результате общения с «Рутой-110», ее hardware и software. Попытаться запрограммировать на ней какой-то криптографический алгоритм – все равно что отправиться в кругосветное путешествие на горбатом «Запорожце», а если еще попробовать увеличить скорость…. Появления в ближайшем будущем персональных компьютеров, компьютерных сетей и INTERNET, никто тогда, в середине 70-х годов, на 4 факультете не мог себе и представить, а уж прогнозировать то, что будущая криптография будет тесно переплетена с ЭВМ, с операционными системами, с компьютерными коммуникациями было абсолютно нереально. Компьютер представлялся, в самом крайнем случае, как некий подсобный калькулятор, с помощью которого можно осуществлять тупые и трудоемкие криптографические задачи перебора ключей. Если есть возможность, думалось глядя на «Руту-110», то лучше с компьютером вообще напрямую не связываться.

Примерно через 10 лет, увидев впервые IBM PC XT, я невольно сравнил увиденное со своей первой компьютерной женщиной. И по выработанной за все это время математической привычке к обобщениям и поискам начальных аксиом, начал сразу же стал задавать себе кучу разных «А почему?».

- А почему советская большая интегральная схема самая большая в мире?
- А почему супостатский IBM PC XT практически не ломается и на нем так легко и приятно что-нибудь запрограммировать?
- А почему у них такой крохотный floppy-disk по сравнению с нашими колесами-кастрюлями?
- А почему на их компьютере можно играть в компьютерные игры, а на нашем из развлечений – только спирт для постоянной профилактики?

В результате один скромненький IBM PC XT моментально выветрил из моей головы остатки марксистско-ленинского мировоззрения, которые туда насильно вдалбливались все долгие предшествующие годы. А как они туда вдалбливались – это особая песня.

- Кто Ваш любимый герой из произведения Л.И.Брежнева «Целина»?

Это дополнительный вопрос на Государственном Экзамене по Научному Коммунизму. Экзамену, призванному подвести черту под воспитанием советского человека – строителя коммунизма. Всего на 5 курсе, перед самым выпуском, было два госэкзамена: по математике и научному коммунизму.

- Леонид Ильич Брежнев

Может и был на курсе хоть один человек, прочитавший Брежневские(?) опусы, но имя его неизвестно. И вот на госе начинают издеваться.

- Ну а еще, помимо Л.И.Брежнева, какой герой Вам запомнился?

Это уже проверка усвоения «правил игры», существовавших в то время: говоришь одно, думаешь другое, а делаешь третье.

- Это Партия, коллективный герой, своим разумом, целеустремленностью, энергией зажигавшая молодые сердца на подвиг, на построение нового общества, свободного от прежних предрассудков и пережитков.

Науку демагогии на 4 факультете усваивали быстро и, по сравнению с математикой, весьма легко. Для этого существовали история КПСС, марксистско-ленинская философия, политэкономия и теория научного коммунизма.

За эти экзамены с факультета никого никогда не выгоняли. Отношение к ним было соответствующее: вместо лекций по политэкономии (уже на 4 курсе) мы приноровились играть в баскетбол, а на остальных, по традиции – в преферанс. На 5 курсе, правда, когда началась теория научного коммунизма, иногда пытались что-то слушать и записывать: все-таки впереди госэкзамен. Забавные иногда удавалось услышать вещи. Рассказывая традиционные сказки про антагонистические (при капитализме) и неантагонистические (при социализме) противоречия, лектор вдруг сделал прямо у нас на глазах важнейшее открытие, заметно обогатившее марксистско-ленинскую науку. Оказывается, при современном развитом социализме основным стало такое неслыханное ранее противоречие, как противоречие между словом и делом. Разумеется, оно является неантагонистическим и временным: вожди поговорят, поговорят, наобещают коммунизм в 1980 году, а потом благополучно обо всем забудут, вот и нет противоречия. Но все же на госэкзамене про такое противоречие лучше не говорить: не хочется после 5 лет такой трудной учебы еще каких-то приключений на ровном месте. Пускай будут только традиционные противоречия, открытые еще товарищем Сталиным: между физическим и умственным трудом, между городом и деревней, а про коммунизм в 1980 году на госэкзамене по научному коммунизму в 1979 году лучше не вспоминать.

Глава 7

Каникулы

Последний экзамен сдан, впереди пьянка по этому поводу и каникулы! Забыть обо всем, сменить образ жизни, оторваться, порезвиться, попить-погулять впрок, на весь семестр до следующих каникул. Вперед!

Как и в любых других институтах, на 4 факультете каникулы были зимой (две недели) и летом (месяц). Зимние студенческие каникулы – чудесное время! Дома отдыха, пансионаты, различные турбазы оккупируются шумными молодыми компаниями, днем – лыжи, вечером – танцы-шманцы да пьянки-гулянки.

На втором курсе у нас уже организовалась своя компания и мы на зимние каникулы нагрянули в дом отдыха «Таруса». Изумительно красивое место на берегу Оки, лес, бесконечная лыжня, свежий воздух, полнейшее отключение от всякой математики и Чуды.

Мой напарник Вовка, с которым мы жили в одной комнате, был по своей натуре, как и я, авантюристом. Если на лыжах – то общий маршрут километров на 50, до местечка Велигож, там классная горка. Мне было интересно проделывать с ним такие марафонские забеги, приползая чуть живым обратно. Чтобы взбодриться по дороге – снежная ванночка: обтирание снегом. А та зима была весьма морозной, столбик термометра часто опускался ниже –30, самая что ни на есть бодрящая атмосфера.

Велигож нам тогда очень понравился своими горками, да еще приметили, что там есть своя турбаза. Поэтому, когда два года спустя я попал на турбазу «Алексин Бор» тоже на Оке, но выше, то сразу же стал подбивать своих новых компаньонов на аналогичные подвиги.

- Там у Велигожа классные горки! Поехали, сгоняем, покатаемся.

С ребятами мы познакомились там же, на турбазе, жили в одной комнате, вместе ели-пили и катались на лыжах. Их было двое, примерно того же возраста, что и я.

Сколько до Велигожа – никто толком не знал. По карте – три или четыре закорючки Оки, ничего страшного, главное – немного авантюризма, которого я к тому времени уже поднабрался в достаточном количестве. Правда, мои новые компаньоны как-то скептически воспринимали слова «Это здесь, рядом», но главное – ввязаться в бой, а там посмотрим.

И вот в один чудесный солнечный день, после завтрака, часов в 10 утра, мы выехали на лыжах на Оку. Свежая лыжня, тихая безветренная погода, легкий морозец, все способствовало лыжным авантюрам.

- Ну что, до Велигожа?
- Это, наверное, далеко.
- Нет, всего три поворота Оки, я по карте глядел.

Три поворота проехали очень быстро, однако Велигожа все нет и нет. Но теперь уже заработал принцип черепахи, перед которой, для того, чтобы она двигалась, вешают морковку.

- Вот за этим поворотом – точно Велигож!

До Велигожа мы все-таки добрались, но уже где-то к середине дня. Про классные горки к тому времени никто не вспоминал, жутко хотелось поесть и отдохнуть. Но мы выехали налегке, без денег и без еды, ведь сначала и не собирались делать никаких таких марафонских забегов. А заехали тогда от своей турбазы прилично: где-то километров 30-40.

В те времена были еще несколько иные отношения между людьми, чем сейчас. На турбазе «Велигож», видя трех голодных и обессилевших лыжников, сжалились над ними и бесплатно накормили обедом. Мы как смогли поблагодарили этих добрых женщин из столовой, собрали все остатки нашей воли в кулак и двинулись обратно.

Обратный путь проходил уже в сумерках и чисто на автопилоте: машинально двигаются руки и ноги, но мыслей в голове – никаких. Только фигура впереди идущего, главное – не отстать и не останавливаться, а то потом уже не будет сил снова начать движение.

Но я был доволен: моя авантюра удалась на славу! Будет, что вспомнить! Часам к восьми-девяти вечера мы приползли-таки в свой «Алексин-Бор», рухнули на кровати и сразу же отрубились.

На следующий день в соседней деревне Егнышевка мы отпаивались пивом. Я выслушал много теплых и ласковых слов, один человек после этого похода проклял лыжи страшным проклятием, а другой, наоборот, остался доволен:

- Да, мужики, я бы пошел с вами в разведку.

Зимние каникулы – это всего две недели, пролетали быстро. Основная радость, которую все ждали с нетерпением – это летний месяц август. Если сдал сессию без хвостов – весь август твой.

Правда, комсомольские вожди всей ВКШ как-то раз приняли решение, что за время обучения все слушатели должны один раз отработать летние каникулы в стройотряде, откусив тем самым от наших законных развлекаловок один смачный кусок. А стройотрядов было два типа: социалистический и коммунистический. В социалистическом работали за деньги, но в Москве, а в коммунистическом – бесплатно, но на Сахалине. Последний, естественно, для желающих романтики и экзотики, дорога туда и обратно – бесплатно, когда еще удастся увидеть столь экзотические места? Да и каникулы в этом случае были не месяц, а почти два – дорога неблизкая, возить туда народ только на месяц было невыгодно. Всем желающим ехать на Сахалин разрешалось сдать летнюю сессию досрочно и потом оторваться там по полной программе. И желающие были, достаточное количество людей, которые захотели поехать «за туманом и за запахом тайги». Вернувшись назад, они были полны впечатлений о различных «молодецких забавах» в этом стройотряде и в целом даже довольны.

Но все же основная часть предпочитала работать за деньги. Тут уж экзотики никакой не было: в Москве, на стройке госпиталя КГБ. Практически все тяжелые работы на стройках во времена развитого социализма осуществлялись или солдатами-срочниками, работавшими по принципу «солдат спит – служба идет», или студентами-стройотрядниками, или еще какой халявной и подневольной рабочей силой. Надежды на кадровых рабочих никакой не было, а с лимитчиками возиться было хлопотно.

Итак, вот она, типичная стройка, госпиталь КГБ. Строим подземный переход от хозблока к столовой. Наша задача – бетонные работы. Самосвал сваливает бетон, а мы растаскиваем его по всему переходу. Думать ни о чем особо не надо, нагружай носилки и таскай. Тут вроде все ясно. Следующая задача – сделать гидроизоляцию перехода. С раннего утра разводим костер под огромным баком с гудроном, плавим в нем это черное золото, обильно поливаем им бетонные плиты перехода и укутываем их рубероидом. Как надо по-нормальному делать гидроизоляцию – никто, естественно, не имеет ни малейшего понятия. Первый же дождик – весь переход течет как дырявое решето, а нас отправляют рыть траншею под какой-то кабель.

Командир стройотряда был из «истинных» чекистов, но человек разумный. Он знал реальную жизнь и четко представлял себе свою основную задачу в данной ситуации: пить с прорабом. Только так можно закрыть нарядов на приличную сумму и дать людям возможность немного подзаработать. В первую неделю, пока в стройотряде были одни яйцеголовые математики, все шло хорошо: мы делали всякую дурную работу, а командир договаривался с прорабом о хороших нарядах. Но через неделю к нам в стройотряд добавили «истинных» чекистов, основная профессия которых была закладывать всех и вся. Естественно, они сразу же стали закладывать командира, который не мог руководить иначе. В результате стройотряд превратился в Содом и Гоморру, мы по-прежнему делали всякую дурную работу, но уже почти за бесплатно, ибо официальные расценки на бетонные, земляные и прочие подобные работы похоже рассчитывались исключительно на зеков, которых кормят в тюрьме, а деньги им нужны только на пачку дешевых папирос «Беломор».

Но стройотряд – это только одно пропавшее лето, зато все остальные – свобода, отдых по полной программе. Республика САИД – союз анархии и демократии.

Отдых без байдарки – это не отдых. Тушенку запасали еще с зимы, а вообще все основные продукты – тушенку, крупы, сахар, муку для блинов – везли из Москвы, купить что-либо, кроме хлеба и водки-сучка (из древесного спирта) в деревенских сельпо было практически невозможно. Байдарочная кампания была стабильная, еще с первого курса, иногда с различными вариациями, от 3 до 5 байдарок, на 2 – 3 недели, километров 200 – 300 по течению тихой лесной речки типа Пра, Угра, Кабожа. Рыбалка, комары, веселье и раздолье – как теперь не вспомнить те незабвенные времена.

Самый первый поход был после первого курса. Опыта – ноль, молодые, необстрелянные, непривыкшие к самостоятельности. Собрав кое-как байдарки, проплыли километра 2-3, как вдруг ливень стеной. Теплый летний дождь, все попрыгали в воду, но продукты в байдарках – хлеб, сахар, макароны, крупы – все безжалостно промокло. Сразу же урок: имей под руками пленку, чтобы накрыть байдарку, не дай еде пропасть. Но в 18 лет смотришь на жизнь проще: промокла еда – съедим ее побыстрее, тушенка есть - значит не пропадем, что-нибудь придумаем. Зато красота-то кругом какая, живая природа, петляющая по лесу тихая речка Пра, народу на ней – никого, сам себе начальник и командир.

Целый день без устали надо махать веслом, идти вперед к намеченному конечному пункту. Обратной дороги нет, против течения не поплывешь, за день надо проплыть километров 25 – 30, тогда при режиме «день гребем – день стоим» за 2 – 3 недели можно проплыть весь маршрут. Гребной день – масса впечатлений: то куча белых грибов на глухом берегу, то ягоды, а то и какой-то дикий зверек вдруг испугано побежит прочь от плывущих по реке одичавших математиков. А на некоторых речках испытываешь острые ощущения на перекатах. Особенно богата перекатами была Кабожа. Это уже ближе к северу, на границе Тверской, Новгородской и Вологодской областей, там, видимо, в 30-е годы были лагеря и зеки, которые и возвели на этой лесной речке множество плотин. Их остатки до сих пор торчат полусгнившими бревнами из воды, создавая в крови у проплывающих по этой реке байдарочников дополнительный адреналин. Плывешь, плывешь себе спокойно, пригрелся, высох, почти дремлешь – а впереди обломки плотины, вода пенится, всюду бревна и камни, того и гляди пропоришь байдарку. Как не хочется прыгать в воду и тащить байдарку

руками! Эх, была не была, авось проскочим! Т-р-р-ах! И вот уже выгребаешь к берегу, а в корме полно воды. Клеимся! Лучше б все-таки было перед перекатом прыгнуть в воду и протащить свою ненаглядную резиновую пирогу на руках. А тут еще, как нарочно, проливной дождь с жуткой грозой. Но один глоток спиртосодержащей жидкости – и жизнь уже кажется интересной, какой же это поход без приключений! А байдарку заклеить – полчаса, чего расстраиваться из-за какой-то дырявой резиновой шкуры.

Ну и, конечно же, щучьи места. От одного вида кувшинок, вылезающих из воды невдалеке от берега, пробегает дрожь по телу. Там, там притаилась зеленая речная хищница. Главное – поточнее кинуть ей под самый нос блесну. Рывок – и вот уже леска натянута как струна, а на поверхности воды появляется зубастая морда, по форме напоминающая автомобиль VOLVO 740. Теперь главное – не дать сойти, резко не дергать, успокоить, дотащить до байдарки, а там уже загнать в подсачек. А потом – сварить из нее уху или поджарить на сковородке на костре, и хоть немного утолить постоянное чувство голода. От количества проглоченной еды это чувство в гребной день практически не зависит, сколько бы перед отплытием ни съел, к концу дня все равно будешь щелкать зубами не хуже голодной щуки.

Гребной день заканчивается выбором места для стоянки. Это особая песня, которую надо петь стоя.

- А здесь подход к воде плохой.
- Здесь какая-то дорога рядом.
- А здесь коров гоняли.
- Да тут дров совсем нет.
- Тут щучьих мест мало.
- Столько мест уже видели, так что ж, неужели здесь встанем?

В августе темнеет быстро. И вот в полутьме, устав от поисков того, не знаю чего, в конце концов причаливаем к первому попавшемуся берегу, по которому можно выбраться на сушу. Выбраться – смело сказано, обрыв высотой метров пять, по песчаной крутой тропке надо еще втаскивать на эту верхотуру байдарки. А наверху – чисто поле, только какой-то жалкий кустарничек невдалеке, количество потенциальных дров стремится к нулю. Луна и звезды уже на небе, желания плыть дальше уже ни у кого нет. Встаем!

К довершению всех приключений утром заявляется лесник, объявляющий, что мы встали в заповеднике. Наш рассказ о вчерашних приключениях весомо дополняется бульканиями в стаканах, в результате чего вся мужская часть нашего байдарочного колхоза отпадает в самом что ни на есть прямом смысле этого слова, а лесник как ни в чем ни бывало садится на свой мопед и уезжает. На следующий день заявляется уже другой лесник, который с горящим взором объясняет, что вчерашний лесник был неправильный, не из того леса, а он самый что ни на есть правильный и законный. Но этот братец кролик уже опоздал: мы собираемся и отплываем.

Ну а как же не вспомнить про грибы! Плавали же по диким местам, куда на машине добраться практически невозможно, народа (конкурентов) мало, кругом лес, должны же были быть грибы. Были, да еще какие! На речке Угре в одном глухом месте наша компания решила сходить за грибами.

Такого количества белых грибов я никогда раньше не видел, хотя мой грибной стаж к тому времени был уже весьма солидным. Белые грибы росли всюду: под елками и на полянках, во мху и в траве, на опушке и в глубине леса. Одно жалкое ведро было моментально заполнено одними белыми грибами, а ведь мы еще только вошли в основной лес. Пришлось снимать куртки и использовать их в качестве мешков. В конце уже можно было услышать такие диалоги:

- Серега, смотри, вон белый гриб прямо на дороге.
- Нагибаться неохота.
- Ногой его!

Белый гриб был красавец, Серегина нога на него так и не поднялась. Но что делать с такой уймой грибов, никто толком не знал. Ведь все их надо почистить, а потом как-то обработать: поджарить или сварить. В трезвом виде желающих чистить грибы не нашлось, поэтому была устроена пьянка. После принятия грибоочистильного допинга, все проблемы стали казаться простыми и разрешимыми. Грибы почистим и пожарим, дело нехитрое. Правда, с таким количеством грибов все это мероприятие может затянуться до утра, но водки должно хватить при любом раскладе.

Порезанные грибы насыпали на сковородку с большой горкой, чтоб побольше пожарить за один раз, костер развели что надо. Правда, потом выяснилось, что для жарки грибов еще надо подлить подсолнечного масла, но, наверное, это можно сделать и попозже. Пока – очередная порция допинга и очередная партия

грибов. А костер разгорается все сильнее, запахло горелым. Пора подлить масла. И вот, при попытке добавить в сковородку с грибами на шибко разгоревшемся костре подсолнечного масла, все это сооружение вдруг вспыхнуло ярким пламенем. Туши, а чем? Ногами! Все горящие грибы были самоотверженно затоптаны и приведены в прежнее жарящееся состояние, а доблестные пожарные получили заслуженное вознаграждение.

Много простора в России! Тихие и глухие лесные речушки, щучьи и грибные места, дикая и пока еще живая природа. Пока! Явно видно стремление человека все отравить и испортить.

На реке Кабоже один местный совхоз решил помыть цистерны из-под керосина. Километров на 20 вниз по течению от реки шел такой запах, что московский воздух стал казаться нам ароматом соснового леса. А ведь в байдарочном походе приходиться, в основном, пить воду из реки! Плывешь и думаешь: а какую еще отраву здесь могут спустить в реку местные начальники? Всякую. На той же Кабоже, к примеру, в начале реки вода была относительно чистой, но ближе к устью мы все заметили один ручеек, из которого хлестала какая-то мутная жидкость. Сразу же начались проблемы с питьевой водой, ибо брать воду для питья из реки стало невозможно. А как же речная фауна живет в таких условиях? Вымирает потихоньку, а вину за это сваливают на изобилие различных рыболовов. Да один такой ручеек страшнее всех сетей и удочек, установленных на этой речке. От рыбаков у рыбы есть шанс спастись, а от совхозного ручейка – нет, ибо это – химическое оружие в борьбе человека с природой.

А что говорить про реки покрупнее, например, про Оку? Наши первые походы в 70-х годах по реке Пре заканчивались на Оке, иногда невдалеке от поселка Кочемары, иногда ниже по течению в городе Касимове. В те времена Ока была сравнительно безвредной для здоровья рекой, можно было даже поймать крупную рыбу: леща или щуку. Поход в середине 80-х годов по Оке оставил тягостное впечатление. Берега от грязной воды заросли илом, а описание реки близ города Алексин больше напоминает сценарий какого-то фильма ужасов: по реке плывут хлопья пены от местного химкомбината, окрестные берега покрыты слоем цементной пыли, все живое в реке атрофировалось и находится на грани исчезновения. Так неужели продукция местных хим и цементного заводов важнее чистоты такой реки как Ока, неужели некому задуматься об отдаленных последствиях подобной хозяйственной деятельности?

Уже в 90-х годах, после победы демократии, большинство подобных совхозов-отравителей и заводов-убийц благополучно обанкротились и встали. И легче стало природе! Прекратилось бездумное удобрение почвы всякой гадостью, травящей почву и остатки живности, бегающей по ней, пересохли ядовитые ручейки, стравливающие в реки всякое дерьмо и отраву, закончилась (надеюсь, надолго) партийно-колхозная эпоха, оставившая после себя во всех деревнях средней полосы кучи ржавой сельхозтехники, тотальную алкогольную зависимость, нищету и разруху. Неужели когда-то в деревнях проживало большинство населения России?

- …но чтоб 30 августа все прибыли во-время: на самолете, на поезде или на другом четвероногом животном.

Есть, товарищ подполковник! Пора назад, на 4 факультет, в родные пенаты!

Глава 8

Криптография

Слово «криптография» впервые было произнесено перед нами только на 2 курсе. До этого – ни-ни, никаких упоминаний о будущей специальности. Полная секретность, все в точности так, как завещал товарищ Сталин: никому ни слова, ни жена, ни мать, ни отец – никто не должен знать о том, чем ты занимаешься. И вот на 2 курсе – посвящение в специальность, раскрытие (точнее, некоторое приоткрытие) тайны твоей будущей профессии.

После начались спецдисциплины, т.е. предметы, имеющие непосредственное отношение к криптографии. Первой была СД-7А – основы криптографии, там мы впервые познакомились с шифром простой замены и с методами его вскрытия, напоминающими разгадывание кроссвордов. Тоже предполагаешь некоторое вероятное слово, но подсказками и критериями истинности служат частота встречаемости знаков в шифртексте, расположение одинаковых знаков, пар, триграмм шифртекста. Первое практическое задание: надо вскрыть шифр простой замены по сравнительно небольшому тексту длиной около 100 знаков. Интересно было начало шифровки, в которой каждой паре цифр соответствовала одна буква русского алфавита: 45 32 18 45 32 18… Это означает, что в начале открытого текста первые три буквы повторяются, а такое начало не так уж часто бывает в обычной речи. Какие могут быть варианты?

- Две двери

- Про проценты
- При применении

и, наверное, читатель сможет сам придумать еще несколько вариантов, но не очень много.

По смыслу в нашем учебном задании в качестве открытого текста должна быть какая-то фраза, которая связана с шифрами и основами криптографии. Вряд ли из приведенных выше трех вариантов первые две фразы имеют отношение к криптографии, поэтому наиболее вероятен третий вариант. Он и оказался истинным:

При применении шифров простой замены статистика знаков открытого текста совпадает со статистикой знаков шифртекста.

Это как в рассказе про пляшущих человечков у Конан Дойля: не важно, как переобозначить некоторую букву алфавита – другой буквой, цифрами или каким-то иным символом, вроде человечка с флажками. Повторяемость буквы в тексте приведет к повторяемости того символа, которым обозначена эта буква. Считайте статистику шифртекста, сопоставляйте наиболее часто повторяющимся символам наиболее часто повторяющиеся буквы алфавита (в русском языке – СЕНОВАЛИТР), подбирайте вероятные слова, по ним расставляйте остальные буквы и проверяйте читаемость открытого текста – все, простая замена вскрывается быстро и элементарно. И никакой особой математики для этого не нужно, скорее сообразительность, логика, знание лингвистических особенностей языка.

Но простая замена в криптографии – примерно то же самое, что ламповые диоды в электронике, дело далекого прошлого, представляет интерес только для истории. В современных шифрах используют гаммирование, т.е. сложение букв или знаков открытого текста с гаммой наложения. И вот тут знание некоторого вероятного слова в открытом тексте приводит к тому, что становится известным кусок гаммы наложения, а это уже пища для криптоаналитика.

С каким юмором нам рассказывали на СД-7А про шифрованные телеграммы, отправляемые в некоторые ближневосточные страны. Почти каждая из них начиналась с перечисления многочисленных и всем известных регалий адресата, по которым вычислялось такое количество гаммы, которое иногда позволяло вскрывать шифр и читать телеграмму быстрее, чем она доходила до адресата. Конечно же, это свидетельствовало также о слабости их шифров, нормальный стойкий шифр должен обеспечивать безопасность даже в таких случаях, но в криптографии есть правила хорошего тона, одно из которых справедливо гласит: не предавай огласке сведения из шифртелеграмм, не давай возможности противнику вычислить кусок гаммы наложения, это облегчает ему задачу вскрытия долговременных ключей шифрсистемы.

- Вот шифртелеграмма, которую я получил накануне!

Это уже 1989 год, съезд народных депутатов. Генерал, стоя на трибуне, показывает прямо в телекамеру содержание шифртелеграммы, тот самый открытый текст, по которому легко вычисляется гамма наложения. И не в какой-нибудь ближневосточной стране, а в СССР. Мораль отсюда следует простая: советский военный шифр должен быть еще и стойким к проявлениям военного идиотизма.

На лекциях по основам криптографии нас последовательно подводили к мысли, что только строгий математический подход, основанный на результатах Шеннона, способен обеспечить гарантированную стойкость шифра. Всякие простые или чуть усложненные замены, коды, не обеспечивающие равновероятности шифртекста, перестановки знаков открытого текста без последующей перешифровки – это все ненадежно, нестойко, рассчитано на слабого противника. Хочешь быть спокойным за свои шифры – используй в них только то, что дает надежную гарантию стойкости при любом уровне подготовки криптоаналитиков-оппонентов. А уровень подготовки криптографов в США, по определению, не ниже, а даже может быть и выше, чем в СССР. Американцы давно следят за нашими линиями связи, знают общий характер переписки, умеют выделять служебные символы, используют протяжку вероятного слова, знают статистику языка и может быть еще многое другое. Хочешь иметь стойкий шифр - доверяй только строгим математическим оценкам!

Дисковые шифраторы – вот, пожалуй, первая попытка построить удобные шифры гарантированной стойкости. Для них можно выписать уравнения шифрования и более-менее точно подсчитать количество различных вариантов параметров, которые нужно будет опробовать для вскрытия ключа к такому шифру.

Дисковые шифраторы были изобретены очень давно, еще до второй мировой войны. Они предназначены для шифрования телеграфных сообщений, состоящих из обычных букв латинского алфавита.

Идея их построения очень простая. Каждой из 26 латинских букв ставится в соответствие один контакт на входе. При нажатии на клавишу, соответствующую этой букве, на данный контакт поступает электрический импульс, который начинает свое движение по цепочке дисков. Каждый диск представляет из себя колесо, на котором есть входные и выходные контакты, связанные между собой проводами-перепайками так, что одному контакту на входе соответствует строго один контакт на выходе. В математике такую конструкцию принято еще называть подстановкой. В результате после прохождения всей цепочки дисков на выходе появляется электрический импульс только на одном контакте. Буква, соответствующая этому контакту, является буквой шифртекста.

Диски в процессе шифрования вращаются друг относительно друга и тем самым обеспечивается отсутствие простой замены: одна и та же буква, зашифрованная в разные моменты времени, с большой вероятностью даст различные буквы в шифртексте.

Историю возникновения дисковых шифраторов, а также их подробное описание и характеристики нам рассказывали на СД-7Б. Сейчас все это можно прочитать в упоминавшейся уже ранее книге Дэвида Кана «Взломщики кодов». Здесь же мне хотелось бы упомянуть об одном весьма интересном эпизоде из лекций по СД-7Б, который я потом неоднократно вспоминал в своей дальнейшей работе.

У дискового шифратора есть два типа ключей. Одни ключи – долговременные, это перепайки между контактами дисков, т.е. те подстановки, которые соответствуют каждому диску. Их смена означает смену самого диска, и производится довольно редко, например, раз в месяц или даже в год. Другие ключи – начальное расположение дисков друг относительно друга. Их можно менять гораздо чаще, делать различными для каждой телеграммы в зависимости от ее номера. Такие ключи называются сеансовыми или разовыми. Количество долговременных ключей – всевозможных подстановок - огромно. Для каждого диска может быть всего 26! (26 факториал – произведение всех чисел от 1 до 26) различных вариантов его перепаек, а дисков несколько, иногда по 6, поэтому общее количество долговременных ключей получается совершенно фантастическим, $(26!)^6$, нечего даже и думать о возможности опробования такого числа вариантов. Разовых же ключей намного меньше, всего $(26)^6$ различных вариантов, даже во времена «Руты-110» было ясно, что такая работа по силам ЭВМ. Сюда еще добавляются разные заморочки, связанные с законом движения дисков друг относительно друга, но общий вывод можно сделать один: без знания подстановок надеяться дешифровать дисковый шифратор бесполезно. И вот тут лектор произнес одну замечательную фразу:

- Вы спросите, как вычисляются долговременные ключи? А никак, они покупаются.

Заходишь в магазин и покупаешь. На самом деле сейчас широко известно несколько детективных историй о том, как именно добывались долговременные ключи. Одна из таких историй – о немецкой подводной лодке U-571 времен второй мировой войны и находящемся на ней дисковом шифраторе «Энигма», захваченном американцами только для того, чтобы «купить» неизвестные подстановки.

Невозможность перебора долговременных ключей в дисковых шифраторах была равносильна признанию аксиомы в криптографии, аналогично той, что в геометрии прямая короче всякой другой линии, соединяющей ее концы, что в мат. анализе последовательность натуральных чисел бесконечна, что в физике справедливы законы Ньютона. Иметь дело с неизвестными факториальными ключами-подстановками, пытаться их определить, как-то вычислить – занятие малоприятное, в большинстве случаев просто бесполезное, их можно только «купить».

И вот тут начались вопросы и ответы.

- А почему нельзя сделать подстановку разовым ключом?
- Менять каждый раз диск в дисковом шифраторе долго, сложно и дорого.
- А не в дисковом? А, например, в шифре на новой элементной базе, работающем с байтами?

И уже много позже:

- А если мы реализуем шифр программно, то почему там нельзя использовать разовые факториальные ключи?

Можно, и еще как! Наличие факториальных ключей в криптосхеме, работающей с байтами по типу традиционного регистра сдвига, подрубает на корню все усилия криптоаналитика выписать и проанализировать уравнения шифрования, найти в них какие-то зависимости. Подстановка неизвестна – все, суши весла. Но если в дисковом шифраторе подстановки были долговременными ключами по объективным причинам, то в программном шифре все эти причины исчезли, запросто можно сделать факториальные ключи разовыми! Первый этап – схема работает вхолостую, выработанная генератором гамма идет на внутренние цели, выработку факториальных ключей-подстановок. А на втором этапе традиционный регистр сдвига, работающий с байтами и дополненный ключами-подстановками, начинает вырабатывать гамму наложения для шифрования открытого текста. За счет факториальных ключей схема может быть сильно упрощена и работать в дальнейшем с огромной скоростью, намного перекрывающей все небольшие издержки начальной холостой работы. Для такой схемы пусть хоть весь Генштаб каждый день трясет перед

телекамерами CNN своими шифрованными телеграммами, дразнит ими АНБ вволю, до факториальных ключей им все равно не добраться!

Идея факториальных ключей вызревала давно. Оценки стойкости схем с факториальными ключами колебались от 10^{100} до 10^{1000}, при желании можно сделать и больше, но это уже было бы изощрением. Скорости работы факториальных схем превосходили скорость программной реализации DES на порядок. К концу 80-х годов стало очевидно: факториальные схемы на новой элементной базе – это весьма перспективное направление развития шифров, сочетающее в себе высокую скорость и гарантированную стойкость. И что же дальше?

- Вы не выдвигали вашу схему на стандарт шифрования?

Да уж, чем-чем, а любовью к бумаготворческой деятельности Господь меня не наградил. Играть в бюрократические игры, состязаться в казуистике (а секретов врагам не выдадим?) – это не по мне.

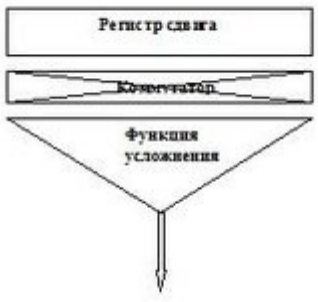
- Нет.

Конкурент в лице заместителя начальника Спецуправления 8 Главного управления КГБ СССР вздохнул спокойнее. Действительно, доказывать кагалу начальников, что советским стандартом шифрования должна быть новая и перспективная схема, а не допотопная копия DES, что заветы Сталина уже устарели, что кибернетика – это не буржуазная лженаука, а сегодняшний и уж тем более завтрашний день криптографии, - это бесполезный Сизифов труд. По крайней мере, в СССР в то время.

Да, честно говоря, в конце 80-х годов пропихнуть какую-то оригинальную криптосхему в качестве открытого стандарта шифрования было абсолютно нереально. Слишком силен еще был синдром тотальной секретности в криптографии, вряд ли какой начальник решился бы взять на себя ответственность дать добро на опубликование каких-то оригинальных криптографических результатов. Переделайте немного DES, придайте ему совковый вид, но никаких своих секретов при этом не раскрывать! Это уже позже шелест зеленых купюр немного приоткрыл у Сталинской криптографической системы ту таинственность, за которой подчас скрывались элементарное ничегонеделание, нежелание начальников брать на себя даже самую малую долю ответственности, тихое стоячее болото. Но про это мы еще поговорим попозже, а пока вернемся в 70-е годы, на 4 факультет.

Что такое электронные шифраторы? Это то, что пришло на смену дисковым шифраторам. Постепенно идеи механических колес, рукояток, вращаемых человеком, штифтов, перепаек и перемычек стали анахронизмом. Появились полупроводники, транзисторы и первые логические элементы, с помощью которых стало возможным реализовывать криптографические преобразования, в которых алфавитом открытого и шифрованного текстов является множество, состоящее только из двух элементов – 0 и 1. Любую букву любого алфавита можно представить в виде двоичного вектора, следовательно, электронный шифратор пригоден для шифрования любой информации. Как шифровать? Конечно же гаммированием, наложением двоичной гаммы на двоичный текст. Задача простая: придумать генератор двоичной гаммы, зависящий от ключа, в котором вычисление такого ключа при некотором известном отрезке гаммы было бы таким трудоемким, что делало бы эту задачу неразрешимой за реальное время. Ну и, естественно, чтобы такой генератор был не очень сложно реализуем с помощью имеющихся типовых логических элементов.

Ключевое слово в электронных шифраторах – балалайка. Так вполне естественно обозвали типовой и самый распространенный узел в генераторах двоичной гаммы.



Из подобных балалаек, соединяя их различными способами друг с другом, и стали создавать различные генераторы двоичной гаммы, предназначенные для электронных шифраторов. Тут уже никакой лингвистики, никаких кроссвордов, как в шифрах простой замены. Нужно скурпулезно и точно просчитывать различные математические свойства этих балалаек: периодичность, статистику, группу преобразований, вероятности перекрытия гаммы и т.п.

Балалайки дали сильный толчок к развитию статистических методов анализа шифров. Если в дисковых шифраторах объем шифрованной переписки был сравнительно небольшой, то при использовании электронных шифраторов объем двоичной гаммы мог уже достигать нескольких миллионов знаков. А тогда, при каких-то огрехах в функции усложнения, появлялась возможность строить различные статистические аналоги, т.е. находить сразу целые классы ключей, реализующих статистически близкие гаммы.

В типовой балалайке присутствует коммутатор. Это, как правило, механический элемент, набор перемычек между контактами регистра сдвига и функции усложнения, т.е. факториальный ключ, подобный диску в дисковом шифраторе. Но опять же, как и в дисковых шифраторах, это долговременный ключ, разовыми ключами, как правило, являлись начальные заполнения регистра сдвига. Здесь, конечно же, коммутатор в какой-то степени «сглаживался» функцией усложнения, которая за один такт из двоичного вектора выдавала только один двоичный знак, но тем не менее задача определения коммутатора была весьма нетривиальной.

Электронным шифраторам была посвящена отдельная спецдисциплина – СД-7В. Нолики и единички, балалайки справа и слева - все это добро аппаратно реализовывалось и запихивалось в довольно большие ящики в 60-х годах. И, естественно, часто ломалось, а посему следующей спецдисциплиной, СД-7Г, был инженерно-криптографический анализ электронных шифраторов. Закоротило где-нибудь в ящике с шифратором, отвалился контактик, полетел транзистор – не опасно ли? Не полезет ли в линию связи открытый текст? Как заблокировать потенциально опасные неисправности? Как оценить вероятность отсутствия опасных неисправностей? В общем, все рутинные вопросы, очень важные, конечно, но скучные. Элементная база, электроника в первую очередь, должна быть понадежней, культура ее производства повыше.

Попыткой некоторого обобщения понятия шифратор, своего рода криптографической абстракцией, была теория шифрующих автоматов. В ней как бы намечались основные требования, которым должен удовлетворять современный шифратор: большая группа реализуемых преобразований, гарантированный период, стойкость к различным методам гомоморфизмов и т.п. Здесь, естественно, было полное царствование математики, а посему эта СД (кажется, СД-7Е) пользовалась большим уважением. Там нас впервые познакомили с таким свойством шифра, как имитостойкость, т.е. стойкость к попыткам целенаправленного искажения шифртекста и навязывания ложной информации. Историю возникновения самого понятия имитостойкости приводили следующую. В 60-е годы, во время войны во Вьетнаме, поставленные вьетнамцам советские ракеты класса «земля-воздух» управлялись с земли с помощью шифрованных команд. Американцы, имея мощные станции подавления таких радиосигналов, научились подавлять истинные команды управления ракетой и посылать вместо них ложные, заменяя некоторые знаки в перехваченных шифрованных сообщениях. В результате наши ракеты стали летать не в ту степь, а криптографы схватились за голову. Имитостойкость – это как бы отдаленная родственница электронной подписи, цели, которые преследует имитозащита шифра и система электронной подписи, весьма близки.

Ну и конечно теория информации, теория кодирования, коды исправляющие ошибки, энтропия, избыточность текста и все связанные с этим теоремы и задачи. Хотя большинство результатов по теории информации были в то время опубликованы в открытых изданиях (основополагающая книга Шеннона, многие книги по теории кодирования), у нас по инерции теорию информации причислили к спецдисциплинам со всеми вытекающими отсюда последствиями: секретными тетрадями и подготовкой в спецбоксе (совместно с преферансом).

Весь четвертый курс был посвящен практически одним спецдисциплинам. Все самые зверские экзамены (ТВИСТ и алгебра) остались позади, на экзаменах по СД уже обстановка была намного спокойнее, никого, как правило, за них не выгоняли, двойки ставили редко. Пахло окончанием факультета.

Глава 9

Прощание с факультетом

Грустно, ох как грустно было расставаться с 4 факультетом! Ясно было, что этот процесс – необратимый, что ему отданы лучшие молодые годы, что здесь был очень сильный коллектив, прекрасные преподаватели, интересная и полная впечатлений жизнь. Когда еще удастся окунуться в такую атмосферу?

Что ждет впереди? Повседневная рутинная работа, одно и то же каждый день с 9 до 6 вечера. И так на всю оставшуюся жизнь, до седых волос, до самой пенсии. Так хоть на последнем, на 5 курсе надо успеть насладиться всеми остатками свободы, остатками молодой и беззаботной жизни в университетской атмосфере 4 факультета.

Впрочем, говоря об университетской атмосфере, нельзя не отметить, что над ней все больше и больше сгущались солдафонские тучи. Давно, еще чуть ли не со 2-го курса, генерал - начальник факультета нам постоянно обещал:

- Скоро переедем в новое здание, хорошее, большое, там для вас будут все удобства, включая шоферские курсы и лодочную станцию.

Особенно умиляла, конечно же, лодочная станция: водка, лодка и молодка. Шоферские курсы были и раньше в старом здании на Большом Кисельном, однако их почему-то прикрыли и не собирались открывать вновь. Не было никаких оснований верить сказкам про них в новом царстве, что и оказалось истиной. А реальной перспективой последствий от переезда было усиление милитаризации, закручивание гаек, борьба с вольнодумством и раскрепощенностью, возникновению которых способствовала вся атмосфера Большого Кисельного.

Как говорил Чебурашка, строили мы строили, и наконец построили. Мрачное кирпичное здание на Юго-Западе Москвы, вместо окон - узкие проемы, бойницы. Наверное, для того, чтобы палить из шифрующих автоматов по засевшим в соседней Олимпийской деревне супостатам. Название соответствующее – МУЦ, в переводе – Межведомственный Учебный Центр. Пожалуйте на новоселье!

Казалось, что никому, кроме генерала, этот переезд на МУЦ был не нужен. Все были довольны Большим Кисельным: в центре Москвы, легко добираться практически из любого района, отдельно от всякого начальства, жизнь на нем уже успокоилась, стабилизировалась, устраивала абсолютно всех. Ну, начальник, будь немного поумнее, упрись рогом:

- Нельзя нам быть в общем здании, мы же криптографы, особая специальность, повышенная секретность. Мы же учим молодых специалистов: никто, ни жена, ни мать, ни отец не должны знать, чем мы занимаемся. А в общем здании одни наши стены без окон уже будут привлекать повышенное внимание всех, кто ездит на автобусах по Мичуринскому проспекту. Ну ни к чему это, нам лучше жить, как и раньше жили, незаметно, на Большом Кисельном, вдали от этой суеты.

Если бы начальник был поумнее! Тогдашний генерал явно не относился к подобной категории, Большой Кисельный, этот уютный купеческий дворик, был сдан практически без сопротивления, даже с радостью. В первую очередь нам нужны хорошие военные!

Этот прискорбный факт застал нас уже в середине 5 курса. Все понимали, что переезд на МУЦ – это не просто перемещение шкафов и сейфов на новое место. Это конец целой эпохи, заложенной основателями факультета, конец многим традициям и неписаным правилам, существовавшим со времен основания факультета, это победа доблестных вояк над математиками, над нашими любимыми преподавателями, над всеми, кто не хочет ходить строем. Не умеешь – заставим!

Но все-таки большую часть своей жизни на 4 факультете мы провели на Большом Кисельном. Теперь уже трудно вдолбать в наши головы серьезное отношение к плакатам типа «в бою граната – роднее брата», трудно заставить слушать лай караульной собаки или принимать во внимание проповеди начальника курса:

- Не шутите с военной службой!

Хождение строем – этому можете воспитывать следующие поколения криптографов. Наш курс счастливо избежал подобной участи, не осолдафонился, не стал курсом «истинных» чекистов с их постоянным закладыванием друг друга, сохранил верность математике и криптографии, университетским традициям, заложенными основателями факультета. Может, генералу и нужны были в первую очередь хорошие военные, но это его личные проблемы. Таких людей можно найти во многих других военных училищах, а хороших специалистов-криптографов готовили только на 4 факультете ВКШ КГБ и нигде более. И подготовить хорошего специалиста намного труднее, чем хорошего военного, научить человека думать головой гораздо сложнее, чем топать по плацу ногами и беспрекословно воспринимать всякие солдафонские тупости и глупости. Главный итог обучения на 4 факультете: всегда думай, прежде, чем что-то делать, не верь ничему, кроме бесспорно доказанных фактов, не слушай демагогии и пустозвонства, не

верь только одному авторитету, требуй доказательств. «Очевидно – это то, что легко доказывается» - еще одна поговорка нашего любимого Сан Саныча.

А еще факультет дал примеры того, что сейчас бы назвали наивным идеализмом, а раньше – честностью и порядочностью. Блат на экзаменах по основным предметам в наше время был практически исключен, только реальные ценности, только знания принимались в расчет. И от этого учиться было интересно, строго соблюдался принцип истинной демократии: все равны перед законом (экзаменом). Одно малейшее отступление от этого закона сразу же влечет за собой искушение сделать еще одно отступление, затем еще и еще. Маленькое ржавое пятно на кузове автомобиля очень скоро превращается в зияющую дыру, и весь автомобиль, какой бы замечательный он ни был изнутри, теряет свою цену. Не доводите автомобиль до ржавых пятен, следите за ним, не эксплуатируйте в экстремальных зимних условиях, чистите, промывайте, проводите профилактику – и он будет в прекрасном виде много лет.

К сожалению, условия развитого социализма, в которых существовал 4 факультет, можно сравнить разве что с зимней ездой по обильно посыпанной едкой солью дороге, к тому же с водителем-генералом, который слабо представлял себе истинную цену автомобиля и частенько путал его с телегой. Вместо поддержки университетского духа, заложенного его предшественниками, он тупо выполнял все идиотские инициативы, спускаемые сверху такими же генералами, устраивал борьбу за образцовый факультет, за повышение успеваемости, всячески усиливал на нем роль различных своих советчиков и соглядатаев, не обремененных математической логикой. Ведь на факультете училось много сынков различных генералов и потихоньку начинало проникать телефонное экзаменационное право. Этому праву всеми силами старались препятствовать преподаватели, но часто силы были слишком неравными, а надеяться на поддержку начальника факультета в этой борьбе было бесполезно.

Но все-таки в наше время, благодаря наивному идеализму преподавателей с кафедры математики, простой экзаменационной демократии, когда все равны, 4 факультет поддерживал свою высокую цену. А такой пример, показываемый в раннем возрасте, приводит к осознанному руководству в своей дальнейшей жизни простыми заповедями о реальном равенстве всех перед законом, по которым живет большинство людей в цивилизованных странах. И существовавший на факультете университетский дух служил своеобразным иммунитетом от проникновения бацилл «телефонной демократии». Разрушая прежние традиции, начальник факультета, может быть сам того не ведая, разрушал и этот иммунитет. Ну разве можно ставить двойку на экзамене сыну, чей отец-генерал позвонил начальнику факультета и попросил «последить» за ненаглядным чадом?

Милитаризация факультета усиливала в нем позиции любителей ходить строем и беспрекословно выполнять любые приказы (и прихоти) всяких начальников. Осознав свою силу, они стали иногда диктовать свои условия и кафедре математики, у которой, кроме наивного идеализма, веры в справедливость и в реальные знания, часто не было больше никакой поддержки.

В середине 80-х годов, будучи аспирантом-очником 4 факультета, я смог воочию наблюдать плоды такой политики на реальном живом примере.

Кафедра математики попросила нас, нескольких аспирантов, помочь им принять на первом курсе коллоквиум по линейной алгебре. Коллоквиум – это некоторый промежуточный экзамен, со всеми атрибутами экзамена: билетами, задачами, дополнительными вопросами. Отличие только в том, что это как бы «неофициальный» экзамен, за двойки на нем с факультета не выгонят, но у преподавателей складывается определенное впечатление об экзаменуемых слушателях.

Еще не испарились из памяти все подробности собственного обучения, таких же ситуаций, в которых я сам был экзаменующимся слушателем, поэтому настроение мое было самое что ни на есть благожелательное. И первый же мой подопечный усилил его еще больше: отвечает спокойно, без запинки, чувствуется, что парень серьезно подготовился, все дополнительные вопросы схватывает на лету, нет ни одного промаха. С большим удовольствием я поставил ему заслуженные 5 баллов и постарался, как мог, похвалить и пожелать успеха на экзамене.

Сидевший впереди другой слушатель внимательно вникал во все подробности нашего общения и делал какие-то свои выводы. Не успел еще первый парень выйти из-за стола, как он сам побыстрее напросился ко мне.

Я не могу описать полностью наше общение. Его метод был простой – на любой вопрос (в билете или дополнительный) – куча длинных и часто бессмысленных формул и в конце – результат по принципу «ткнуть пальцем в небо».

- Сколько всего векторов длины M над кольцом Z/N?
- Бесконечное число.
- Докажите.
- Это фундаментальный факт из мат. анализа

Мое благодушие смыло как рукой. Совершенно ясно, что человек пришел абсолютно неготовым, не знающим элементарных вещей, и при этом наивно пытающийся обвести меня вокруг пальца своей демагогией, пусть даже выраженной длинными и бессмысленными формулами. Дополнительный вопрос: прошу его посчитать ранг матрицы размера 3x3 в которой два столбца – линейно независимы, а третий – результат простого сложения первых двух. Завис минут на 10, исписал около страницы, в конце резюме: = 3.

- Ну расскажите, как считали.

В голове – полная мешанина, кое-что из алгебры, кое-что из мат. анализа, а основная часть – чушь собачья. И огромный апломб.

- Вы дали неверный результат. Ранг равен 2.
- Я тоже получил ранг 2, это просто описка.

Тут же, у меня на глазах, переправляет свой результат.

- Но Вы мне так и не объяснили, как Вы считали.
- Я все верно посчитал, это вы меня не поняли.

Другой дополнительный вопрос – тот же результат, те же сцены: я посчитал все верно, неверный результат – это просто описка, Вы меня не поняли. Ну просто еще и наглый парень, ко всему прочему!

- Хорошо, вот еще один дополнительный вопрос, но я прошу Вас ответить на него в присутствии еще одного преподавателя.

Иду за другим аспирантом, Серегой, который пока скучает. Вместе наблюдаем очередную абсолютно аналогичную сцену. Теперь его уже не поняли двое.

- Достаточно. Я вынужден поставить Вам 2.

Взвейтесь соколы орлами! Что с ним стало! Несправедливо, я все правильно отвечал, меня не поняли и все по новой с удвоенной силой. Меня этот тип очень заинтересовал, и я спросил о нем у Сан Саныча. Сын заместителя министра обороны одной из тогда еще небывших советских республик. Направляя его на учебу, это министерство строго наказало: обеспечить, чтобы он доучился до конца и был выпущен офицером, в противном случае служить на горную границу отправят кого-то из москвичей.

- Сейчас Вы ему совершенно справедливо поставили 2, а вот на экзамене…

Сан Саныч понуро посмотрел на меня, а я сразу же вспомнил первого парня, судя по всему москвича, и представил себе, что его после окончания факультета пошлют на горную границу только из-за того, что отчислят за двойки сынка замминистра обороны. Нет, нет и еше раз нет!

Против лома нет приема. На словах отношение начальства к преподавателям математики было корректным, а на деле – как всегда в нашем государстве относятся к шибко умным. Университетский дух 4 факультета держался на голом энтузиазме преподавателей первой волны, а еще – на любви подавляющего большинства слушателей к математике и тем, кто целиком посвятил себя ей. Но слушатели приходят, учатся и уходят, постепенно пропадают традиции, а образовывающийся вакуум заменяют хорошие военные.

Жалко, чрезвычайно жалко было покидать Большой Кисельный. Но нам через полгода предстояло покинуть и всю Высшую Школу КГБ, со всеми ее порядками и премудростями. Так где же провести выпускной банкет? Конечно же, на Кисельном!

Много поколений выпускников Высшей Краснознаменной Школы КГБ из года в год лелеяли одну и ту же мечту: напоить на выпускном вечере боцмана. Все пять лет, что мы учились, слово «боцман» было в устах наших начальников универсальной страшилкой, такой же, как у родителей, которые пугают милиционером непослушных детей. Приплытия боцмана на строевой смотр боялся даже наш генерал, начальник факультета. Но чаще всего боцман любил наводить шухер в общаге, где, по определению, его душе было наиболее привольно и всегда ждала обильная добыча в виде очередных суток ареста, выписываемых направо-налево. Все повидавшие по милости боцмана московскую гауптвахту потом обязательно клялись напоить его до бесчувствия на выпускном вечере, пусть даже ценой самопожертвования.

Наш курс, конечно же, почти целиком мечтал напоить Чуду. Но тут он проявил себя тонким стратегом, не стал ввязываться в одиночные бои, стойко держал круговую оборону, иногда исполняя свою любимую песню про Родину, которая щедро поила, но только одним лишь березовым соком. В общем, этой мечте не суждено было сбыться. А где-то в конце вечера к нам наконец-то пожаловал боцман.

- Леонид Григорьевич, давайте выпьем на прощание.

Общага, собрав остатки сил и извлекая из самых зашифрованных источников тщательно сберегаемый для такого случая коньяк, потянулась к боцману.

- Это у меня сегодня уже третий вечер.

Далеко еще молодым офицерам до его закалки, тщетны оказались надежды! Боцман лихо забулькал в себя N-грамм огненной жидкости и поплыл дальше. А общага малость подустала и тихо сдалась на милость победителя.

Все, окончен бал, погасли свечи. Впереди – другая жизнь, другие впечатления, другая операционная система. На следующий день Чудо решил устроить нам прощальное построение, на котором сказать свое отеческое напутствие перед дальней дорогой в самостоятельную жизнь. Но уже, конечно же, на МУЦе, в этом медвежьем углу, собрав там, на настоящем плацу, и молодых офицеров, и первокурсников, которые должны на таких мероприятиях набираться солдатского ума-разума. И вот на наши еще слегка шумящие головы посыпались от специально натренированного первокурсника пионерские клятвы: брать пример со старших товарищей, хорошо учиться, любить свою Родину, не пить, не курить и матом не ругаться.

Старшие товарищи ехидно усмехались:

- Мы верим в тебя, малыш!

Прощальная песня математиков 4 факультета Высшей школы КГБ СССР. Музыка общеизвестная, слова народные.

Раскинулось поле по модулю 5
В углах интегралы стояли
Студент не сумел производную взять
Ему в деканате сказали.

Анализ нельзя на халтуру сдавать
Профессор тобой недоволен
Ты должен критерий Коши доказать
Иначе с мехмата уволим.

Он вышел доказывать, знаний уж нет
В глазах у него помутилось
Увидел стипендии меркнущий свет
Упал, сердце больше не билось.

К нему подбежали со шпаргалкой большой
Хотели привесть его в чувство
Декан подошел, покачал головой
Не в силах здесь ваше искусство.

Три дня в деканате покойник лежал
В штаны Пифагора одетый
В руках Фихтенгольца он томик держал
Что сжил молодого со света.

Марксист свое веское слово сказал
Материя не исчезает
Загнется студент – на могиле его
Огромный лопух прорастает.

Профессор последнее слово сказал
Матрицами труп обернули
К ногам привязали тройной интеграл
И тело с мехмата спихнули.

Напрасно студенты ждут друга в пивной
Им скажут – они зарыдают
А синуса график волна за волной
По оси абсцисс убегает…

Колея

1979 год. Брежневская эпоха надоела всем до чертиков. Масса анекдотов, частушек, сплетен на эту тему, а товаров в магазинах все меньше и меньше. Все последние годы заметно невооруженным взглядом: система катится вниз. Про победу коммунизма, записанную в действующей в то время Программе КПСС, уже почти не вспоминают, хотя все вступающие в партию пишут: «Устав и Программу КПСС признаю и обязуюсь выполнять». Людей, которые бы искренне верили во все эти сказки, практически нет, система натужно пытается эксплуатировать несмышленую молодежь, засылая ее с большой помпой и показухой то на БАМ, то на еще какую-нибудь «стройку века», и оставляя там без человеческих условий жизни. Газеты, радио и телевидение забиты «Ленинскими университетами миллионов», «Трудовыми рапортами ударников пятилетки», «Вестями с полей», «Хрониками трудовых вахт» и прочей подобной чепухой, от которой хочется напиться, что большинство и делает. Нормальный труд забыт, к работе отношение как к обязательному отбыванию положенного срока, скучному и бесцельному.

Это были мрачные, какие-то предгрозовые годы. Полно предчувствий, что несоответствие между словом и делом в проводимой в стране политике должно закончиться чем-то печальным. Чем именно, никто тогда предсказать не мог, но все шептались: куда мы катимся? Почему так стремительно отстаем от Запада? Везде невиданный ажиотаж вокруг качественных иностранных товаров: мебели, одежды, телевизоров, магнитофонов, просто купить практически ничего путного невозможно, везде очереди, списки, каждое утро надо бегать в магазин отмечаться, ловить момент, когда «выкинут» товар. Лучше живут те, у кого есть связи в торговле, кто может что-то достать, договориться, замолвить словечко. Слово «коррупция» еще под

запретом, но фактически она уже расцвела пышным цветом. При реальном социализме важны реальные блага!

Что в таких случаях нужно, чтобы взбодрить страну? Масштабное шоу или маленькая победоносная война. А можно и то, и другое в одном флаконе. И вот, вместо обещанного наступления в 1980 году коммунизма, СССР готовится к проведению в 1980 году XX летних Олимпийских игр в Москве, а в конце 1979 года советские войска входят в Афганистан.

В связи со всеми этими событиями офицерам КГБ прибавили зарплату. Мы, молодые лейтенанты, только что выпущенные из 4 факультета ВКШ КГБ, сразу же получаем оклад 250 рублей, а это довольно много по советским меркам того времени. Выпускник обычного института, попадая на должность младшего научного сотрудника в каком-нибудь НИИ, как правило, получает 120-130 рублей. Но наш оклад состоит из двух частей: оклад по должности (130 руб.) и оклад по офицерскому званию (120 руб.), хотя военной формы в управлениях КГБ не носят.

Вот в таких условиях начиналась моя офицерская военная служба, хотя, конечно, «военного» в ней было очень мало. Больше все это походило на работу в обычном НИИ, в котором за счет специально подобранного состава сотрудников и относительно высоких окладов еще была иногда какая-то осмысленная работа, очень сильный коллектив математиков и обязательное отбывание на рабочем месте с 9 до 6.

Глава 1

Спецуправление

В КГБ начала 80-х годов было три управления, так или иначе связанных с криптографией и испытывавших потребность в выпускниках 4 факультета Высшей школы КГБ: 8 Главное управление, 16 не Главное, а просто управление, и управление правительственной связи, УПС без всякого номера и главности. Распределение обязанностей было такое.

УПС – эксплуатация шифровальной аппаратуры на правительственных линиях связи, чаще всего – на спецмашинах, на которых члены Политбюро ЦК КПСС со страшной скоростью проносились по Рублевскому шоссе, на спецлиниях, связывающих Кремль с дачами на Черном море и в других местах. Про УПС многие узнали после путча 1991 года, когда оно оперативно отключило все каналы спецсвязи у Горбачева, изолированного в Форосе.

16 управление – дешифровальная служба, взлом шифров наших потенциальных противников, а также ненадежных друзей-союзников и просто всех тех, кто не придает должного значения криптографии.

8 Главное управление – обеспечение безопасности всех отечественных линий, где используется шифрованная связь, т.е. та криптографическая сила, которая должна была противостоять могучему американскому АНБ – агентству национальной безопасности, занимавшемуся сбором шифрованной информации по всему миру и взломом нестойких шифров. 8 ГУ КГБ СССР состояло из трех больших подразделений – управлений А, В и С, из которых управление А отвечало за безопасность дипломатической переписки, управление В – за безопасную выработку ключей и своевременное обеспечение ими всех нуждающихся, а управление С – Спецуправление – за все остальное: за контрольный криптографический анализ старых шифров, за разработку новых перспективных шифров, за инженерно-криптографическую защиту, за нормативную базу при работе с шифрами, за связь с промышленностью и прочая, прочая, прочая.

Вот здесь, в Спецуправлении, началась в 1979 году моя офицерская служба в КГБ, которая там же драматически и закончилась в 1993 году, не дотянув нескольких месяцев до заветных общих 20 лет выслуги, дающих право сравнительно молодому человеку 37 лет от роду на получение офицерской пенсии. Но, право, получать в 37 лет сравнительно высокую (по советским меркам!) офицерскую пенсию не за боевые заслуги, не за какие-то выдающиеся достижения, а за работу фактически в обычном НИИ, часто просто за просиженные штаны, за безропотность и послушание, в нашей стране несколько стыдно.

Основная часть Спецуправления (это слово всегда писали с большой буквы!) размещалась в Кунцеве, в здании, напоминавшем известное здание Совета Экономической Взаимопомощи на Арбате – раскрытую книгу. Только «страницы» этой книги были не выгнутыми, как в оригинальном СЭВе, а прямыми, и их было не две, а три, да и этажей поменьше. А так, по конструкции и по стилю – схожи, все из стекла (за что и прозвано было в народе стекляшкой), летом жарко, а зимой – холодно.

В Спецуправлении 8 ГУ КГБ СССР было несколько отделов, каждый из которых специализировался на каком-то определенном круге криптографических задач. Но давняя мечта руководства Спецуправления была одна – своя небольшая производственная база, свой «свечной заводик», который позволил бы хоть немного избежать зависимости от советской промышленности. Шифраппаратуру того времени никак не отнесешь к товарам народного потребления, она выпускалась по спецзаказам для специальных целей, но в ней все равно использовалась стандартная элементная база, стандартная советская электроника со стандартными советскими проблемами. Идея наладить выпуск «спецэлектроники» для

перспективной шифраппаратуры овладевала умами руководства Спецуправления, порождая проекты один грандиознее другого. А начать эти проекты, как и полагалось в советское время, следовало со строительства.

Стекляшка занимала сравнительно небольшой по площади треугольничек на пересечении Молодогвардейской и Ельнинской улиц и в самом остром углу этого треугольника оставалось еще свободное место. Вот здесь-то и решили начать возводить криптографический «свечной заводик».

Это, как и многое другое при социализме, стало «народной» стройкой. В том смысле, что профессиональных строителей, как всегда, не хватало, и для выполнения самой тяжелой и низкооплачиваемой работы спускали (в приказном порядке) разнарядки офицерам Спецуправления. И вот молодые и полные энтузиазма выпускники 4 факультета Высшей школы КГБ начинали свою трудовую деятельность с того, что воочию наблюдают примерно такие картинки советской действительности.

Картинка первая. Паркет. Дефицитнейший материал, когда-то им устилали полы в жилых домах, но это было очень давно. Сейчас паркетом устилают полы только в элитных местах, к которому, просто по определению, должно относиться возводимое здание собственного «свечного заводика» Спецуправления. Но настилают паркет не рабочие-профессионалы, а солдаты срочной службы из какого-то строительного батальона. А офицеры Спецуправления им этот паркет подносят. Дело это было весной и то ли солдаты при этом больше о дембеле думали, чем о паркете, то ли вместо дуба, который, как известно, «годится на паркет, так ведь нет…», в нем использовали иные породы древесины, но только той же осенью уже молодые солдаты-салаги этот паркет отдирали, а те же офицеры его отодранный относили на свалку. Неправильно весной уложили, вздулся и рассыпался.

Картинка вторая. Экскаватор. Предназначен для копания котлована. Ну как тут не вспомнить бессмертное изречение: «У тебя работа в рублях, а у меня – в сутках». Работа экскаваторщика явно оценивалась в сутках и солярке, сожженной за эти сутки. Пока офицеры Спецуправления разносили и укладывали подвезенный бетон, экскаваторщик завел мотор на своем экскаваторе и бесследно испарился. Полдня непрерывно тарахтящий мотор экскаватора изображал его работу, а сам экскаваторщик занимался при этом видимо какими-то более важными делами. И все – практически в открытую, на глазах у офицеров КГБ, разносящих в это время бетон на носилках.

Наверное каждый, кто жил в то время, таких картинок насмотрелся достаточно, это, может быть, интересно для нынешнего молодого поколения, проявляющего интерес к социализму советских времен. Самый лучший способ насытить подобный интерес – попробуйте покопать канаву от забора и до обеда.

В конечном итоге это строительное произведение вылилось в дополнительный трехэтажный корпус («пункт приема стеклотары»), вся территория Спецуправления стала треугольной и полностью соответствовала магическому русскому числу три: три стороны у стекляшки, три этажа у «пункта приема стеклотары», и треугольный забор с колючей проволокой, все это хозяйство огораживающий.

Это были уже не первые мои уроки реальной жизни, реального социализма, его реальных строек. Еще при строительстве нового здания Высшей школы КГБ на Мичуринском проспекте нас, слушателей 4 факультета, несколько раз использовали в качестве подсобной рабочей силы на «воскресниках». Но в Высшей школе был учебный процесс, часто отрывать от которого слушателей было все-таки сложно (тогда, а как сейчас – ничего определенного по этому поводу сказать не могу) . А здесь, в стекляшке, никакого учебного процесса уже нет, все являются военнослужащими, которые обязаны безропотно выполнять приказы начальства. Так и велись все стройки на объектах в управлении В на проспекте Вернадского и в стекляшке, а молодые офицеры, полные сил и энергии, еще раз вспоминали на них описанную Александром Солженицыным в романе «В круге первом» криптографическую шарашку.

Но по сравнению с 4 факультетом была все-таки одна существенная разница: глупостей, вроде «в первую очередь нам нужны хорошие офицеры, а потом уже хорошие специалисты» здесь уже в открытую не говорили и уровень интеллекта руководства Спецуправления был намного выше. Не было, как на 4 факультете, четкого разделения на преподавателей и начальников, все начальники – это, как правило, тоже математики, только делающие при этом такую работу, которую везде принято называть карьерой. И в треугольнике «офицер – чиновник – специалист» еще неизвестно, какая сторона должна быть больше, во всяком случае, для большинства этот треугольник был явно не равносторонний. Люди, попадая на руководящие должности, понемногу менялись, становились более важными и вальяжными, любили давать руководящие указания, выступать с общими рассуждениями на партийных собраниях (все сотрудники КГБ должны были быть коммунистами), постоянно находили недостатки у подчиненных. Но если на 4 факультете эти недостатки все время выражались в «неприческах» и плохо почищенных сапогах, то в Спецуправлении начальники очень любили до бесконечности вносить мелкие стилистические поправки в подготовленные их подчиненными статьи для издававшегося в 8 ГУ КГБ внутреннего научно-технического сборника.

У меня была возможность сравнивать 4 факультет и Спецуправление: и в одном и в другом месте я провел достаточно времени. 4 факультет – резко выраженный контраст между преподавателями и начальниками и в целом более свободная, раскрепощенная атмосфера. Здесь меньше думают о карьерных

интересах, здесь более популярны профессионалы, люди, выделяющиеся по своим качествам из общей массы. Здесь, наконец, много молодых людей с еще не закостеневшими мозгами, не успевшими растерять свой идеализм, какие-то неуловимые и нетривиальные черты, по которым практически любой преподаватель, общаясь с ними, становится сам моложе и раскованнее. А Спецуправление – это уже машина, механизм, производство. Здесь нет начальника курса, подобного нашему Чуде, нет и такого коллектива, легкого на подъем, свободного, демократичного, раскованного, какой сложился в нашей учебной группе на 4 факультете. Все в Спецуправлении уже сами за себя, больше думают о карьерном росте, о начальственных перспективах, о смысле жизни и реальных ценностях в ней. Сказывается и возрастное неравенство: старшие коллеги более опытные и имеют больше прав, молодому специалисту еще предстоит доказывать, чего он стоит на самом деле. Обстановка в Спецуправлении показалась мне все-таки более скучной и серой, чем на 4 факультете, постоянные сплетни в курилке, одни и те же темы: кто и как делает себе карьеру, кого назначат начальничком, чего ожидать в ближайшем будущем… Да не хочу я ничего ожидать и расписывать свою жизнь заранее на 20 лет вперед: через три года выбиться в руководители группы, еще через пять – в руководство отделения и карабкаться в этой тихой и заезженной колее до седых волос. Хочется каких-то нетривиальных поступков, нестандартных решений, неординарных действий, не хочется быть таким, как все. Но это все, наверное, несбыточные мечты, реальность – вот она, гораздо проще и прозаичнее: разнарядка на стройку, дежурство по продовольственным заказам, высиживание каждый день с 9 до 6 за одним и тем же столом, глядя на одни и те же лица, политучеба после работы, одна и та же скучная и унылая обывательщина. И так – до пенсии? Ну уж нет, может быть, кому-то такая колея и по душе, но не мне. Год, два, а затем – искать выезд из нее.

Один отдел в Спецуправлении занимал особое положение в самом что ни на есть прямом смысле слова: находился не в стекляшке, а в обособленном старинном здании тюремного типа минутах в 15-20 ходьбы от стекляшки. Это был Теоретический отдел, в котором начальником был уже известный нам по лекциям по ТВИСТу Вадим Евдокимович Степанов. К нему-то я и попал сразу же после окончания факультета.

Глава 2

У Степанова

В 5 (Теоретическом) отделе Спецуправления работало около 50 человек, три отделения по 15-20 человек в каждом. Основной задачей отдела было проведение контрольных криптографических анализов действующей шифраппаратуры, выявление ее возможных слабостей и потенциальных опасностей, связанных с постоянным развитием вычислительной техники и криптографических методов анализа шифров. По действующим в те времена положениям, любая реально эксплуатируемая шифраппаратура должна была быть подвергнута контрольному криптографическому анализу не реже, чем один раз в 5 лет. Это довольно разумное положение, поскольку дать 100% гарантию стойкости на все времена никто не мог, криптографический анализ постоянно развивался, появлялись новые методы, новые люди, свежие взгляды. Сам криптографический анализ длился, как правило, около года и проводился следующим образом. Группе экспертов из 3 – 5 человек давали все предыдущие отчеты по анализу данной аппаратуры, подробное описание ее криптографической схемы, условий эксплуатации, требований, предъявляемых заказчиком аппаратуры, и за год надо было попытаться найти какие-то новые методы криптографического анализа этой схемы, которые позволили бы скинуть с предыдущих оценок стойкости 1-2 порядка. Работа почти всегда чисто абстрактная, самой этой аппаратуры эксперты часто вовсе не видели. Конечно же, качество проведенного криптографического анализа очень сильно зависело от квалификации экспертов, от их криптографического кругозора, эрудиции, умения найти и применить какие-то нетрадиционные, нетривиальные подходы, заметить то, что было пропущено на предыдущих экспертизах.

В основном в 5 отделе работали сравнительно молодые ребята, еще не потерявшие вкуса к криптографии как к науке. Всячески поддерживались и поощрялись различные семинары, диспуты, споры, здоровая конкуренция за лучшую идею, за скинутые порядки с оценок стойкости. Степанов старался придерживаться баланса: половина людей в отделе заканчивала 4 факультет ВКШ КГБ, другая половина - МГУ, вроде как две разные команды, в которых «школьники» (4 факультет) обладали тем преимуществом, что были уже знакомы с криптографией, а приходящему на работу человеку со стороны требовался год-два на то, чтобы вникнуть во все тонкости криптографических методов.

Но одними контрольными криптографическими анализами занять столько людей было невозможно. Отдел вел еще несколько перспективных НИР, в которых пытались предугадать возможности развития криптографии и вычислительной техники в будущем, появление новых направлений в анализе и синтезе шифров, проблемы искусственного криптографического интеллекта. Тут было огромное поле для различных дискуссий, для проявления остроумия и юмора (ТИКИ – КИКИ – теория искусственного криптографического интеллекта – конкретный искусственный криптографический интеллект), но сейчас,

спустя почти 25 лет, стало ясно: с перспективами наша криптографическая наука явно промазала. Американцы, с их идеями открытых ключей и электронной подписи, с их коммерческой криптографией оказались куда более практичнее. Конечно же, идеи системы с открытым распределением ключей У. Диффи и М. Хеллмана, впервые опубликованные в 1977 году, были известны, но отношение к ним тогда, на рубеже 80-х годов, было весьма настороженное. По привычке считали их какой-то уловкой американских спецслужб, своего рода «криптографической провокацией», призванной сбить с толку развивающиеся страны, внедрить у них эту систему, которую американцы, зная «потайной ход» в ней, затем смогут вскрывать. Про развитие электронной коммерции в то время думать никому не приходило в голову: для советской экономики вполне хватало коммерции по блату или с черного хода. Основная забота была о военных шифрах, а в них использование сравнительно новых американских идей было абсолютно нереальным.

Еще один вызов, который бросили американцы в то время – это DES, Data Encryption Standart. Открыто опубликованная криптографическая схема, в то время, как в СССР все, что было прямо или косвенно связано с криптографией, подвергалось тщательному засекречиванию. Такая система была заложена еще Сталиным и сохранялась до 90 годов практически в неизменном виде. Доходило до анекдотов. В 1986 году издательство «Радио и связь» в плане изданий на 1987 год опубликовало анонс книги Д.Конхейма «Основы криптографии». Книга зарубежного автора, в ней содержались только общеизвестные понятия, описание американского DES, самые тривиальные подходы к его криптографическому анализу. Реакция 8 ГУ КГБ СССР была однозначной: запретить. Весь тираж был объявлен ДСП (Для служебного пользования) и направлен в закрытые спецбиблиотеки управлений КГБ. Но план издательства был уже широко опубликован и в издательство начали приходить заявки на эту книгу. Все эти заявки издательство пересылало в 8 ГУ КГБ СССР, где, прямо на моих глазах, происходили следующие сцены.

- Так, Дальневосточный военный округ. Ну, тут все ясно.
- А это что? Мурманское морское пароходство? Ну-ка, разберитесь, кто это там так шибко заинтересовался криптографией, что они лезут, куда не следует!

Как мотыльки на ночной свет, полетели на анонсированную книгу все подпольные и полуподпольные криптографы. А в 8 ГУ КГБ СССР только и оставалось, что наладить их учет и контроль.

Почти такая же история, только уже с несколько другим сценарием, повторилась почти 10 лет спустя. В 1995 году был принят Указ Президента России № 334, в котором на любое использование криптографических средств требовалась лицензия ФАПСИ. К тому времени в России уже было множество коммерческих банков, использовавших различные системы шифрования и электронной подписи. Дальнейшее продолжение этой истории слишком тривиально, чтобы уделять ей здесь внимание, система и через 10 лет осталась практически той же.

Но вернемся к DES. Взломать DES предлагали всем желающим, и уж Теоретический отдел не мог остаться от этого в стороне. «Если вы найдете способы взлома DES, то я сразу же буду докладывать об этом на очень высоком уровне» - так выступал перед нами генерал, заместитель начальника Главка. Но, к чести 5 отдела, сильно напрягаться над попытками взлома DES никто не стал. Ломовая и тупая схема, которой не коснулись ни красота, ни изящество, ни оптимальность выбранных параметров, ни простота реализации. Но к ней было приковано высочайшее внимание! Получить какие-то красивые результаты и написать диссертацию на анализе DES было очень трудно, а завоевать внимание начальства – очень легко. И вот с конца 70-х годов в 5 отделе стали заниматься «криптографической теологией»: как малость приукрасить DES, чтобы немного скрыть его уродства, но в то же время (не дай бог!) не раскрыть при этом каких-то своих криптографических тайн.

В те времена – начало 80-х годов – расклад «криптографических сил» в 5 отделе был примерно следующим:

1 отделение – «криптографические законотворцы», те, кто занимался разработкой новых требований к перспективной шифраппаратуре (об этом речь пойдет впереди), а также разработкой советского стандарта шифрования, основанного на схеме типа DES. Кузница кадров для будущих криптографических чиновников.

2 отделение – вероятностники, то есть те, кто, в основном, специализировался на статистических методах анализа шифров. Их любимыми объектами были «балалайки», традиционные электронные шифраторы, работающие с битами на элементной базе 60-х годов, состоящей из типовых логических элементов.

3 отделение – алгебраисты, те кто специализировался на алгебраических методах криптографического анализа. Здесь, помимо анализа традиционных «балалаек», были люди, занимавшиеся разработкой шифров

на новой элементной базе, а также, те, кто изучал и анализировал появившиеся новые американские идеи открытых ключей.

Мне посчастливилось попасть к алгебраистам.

Между алгебраистами и вероятностниками всегда шли острые дискуссии на тему, чья же вера более истинная, и кто приносит больше пользы в криптографии. К «криптографическому законотворчеству» отношение во 2 и 3 отделениях было примерно такое же, как к политинформациям: спущено сверху, значит кому-то надо. Никто не верил, что разрабатывая новые требования или приукрашивая DES, можно получать какие-то красивые и полезные научные результаты, но приказ начальства – закон для подчиненных.

«Криптографическое законотворчество» не было доминирующим в Теоретическом отделе. Большинство людей стремилось к самостоятельной научной работе, писали и защищали диссертации, искали новые, оригинальные решения. Мне кажется, что Степанов был более расположен к таким людям, поскольку его собственный интеллект и кругозор был необычайно широк. Он досконально вникал во все отчеты, выполненные в отделе, поэтому все написанное, прежде чем попасть к Степанову, проходило через неоднократные обсуждения, проверки, споры. Наверное, любой другой подход неизбежно привел бы к фикции, к имитации бурной деятельности, к обесцениванию криптографического анализа, ведь даже если американцы и нашли какую-то слабость в наших шифрах, то вряд ли об этом станет известно. Вопрос о «критерии истинности» выполненных в 5 отделе работ, как правило, решался окончательным мнением Степанова, а придумать тут что-либо другое было невозможно. С другой стороны, наличие сильного лидера всегда благоприятно влияет на коллектив, вызывает естественное желание подтягиваться до его уровня, нацеливает на более трудные задачи. Сколько подобных примеров известно в нашей истории: С.П.Королев, И.В.Курчатов, А.П.Александров, М.В.Келдыш и многие другие. А если взять не науку, а, к примеру, спорт, то и здесь влияние одного человека, неординарной личности, трудно переоценить. Как не вспомнить советскую хоккейную сборную времен А.В.Тарасова, редко знавшую поражения, а все больше победы, добываемые тяжелым трудом.

И начальник Теоретического отдела тоже был из тех людей, кто явно выделялся из общей массы, кто был на голову выше своих подчиненных, причем выше именно в силу своего интеллекта, образованности, знаний, а не административного положения.

Мой приход в 5 отдел очень символично совпал с одним событием: в здании, где располагался отдел, в это время начали ломать советскую ЭВМ «Весна». Весь двор был заставлен мусорными контейнерами с платами и схемами (которые не микро), составлявшими раньше hardware этого очередного чуда техники. Увлекаясь в детстве сборкой транзисторных радиоприемников, я с ужасом прикидывал количество выкинутых транзисторов, диодов, конденсаторов и сопротивлений, которые всегда были дефицитом и предметом моего неутомимого поиска по разным радиомагазинам. Здесь же были совершенно иные единицы измерения, не штуки, а ящики, контейнеры, кубометры. Душа не выдержала, и не только у меня одного. Около этих сокровищ стали появляться и другие люди с плоскогубцами и кусачками и одна из последних моделей чисто советских ЭВМ приняла чисто советскую смерть.

Примерно через год какими-то неведомыми путями Спецуправление умудрилось закупить американский компьютер (тогда еще не персональный, а многопользовательский) Hewlet-Packard и установить его в стекляшке. И сразу все почувствовали разницу! Цивилизованные клавиатура и монитор, диалоговый режим работы, нет никаких перфолент и перфокарт, простой язык программирования BASIC, вместо машинных кодов и примитивного ассемблера, с которыми мы имели дело на «Руте-110» на 4 факультете. Этот компьютер сразу же стал центром всеобщего притяжения, а уж в 5 отделе – тем более, ибо располагался в стекляшке, где не было своего «отдельского» начальства. Фраза «Я пошел на машину» стала любимой для многих сотрудников, желающих обрести некоторую свободу творчества, особенно после обеда.

Но все же основная работа в Теоретическом отделе была с карандашом и бумагой. Строгие математические факты, доказанные теоремы и вытекающие из них оценки стойкости шифров – вот та продукция, которая требовалась от теоретиков. Разобраться с криптосхемой, вникнуть во все ее особенности, сильные и слабые стороны, а затем попытаться взглянуть на нее по-новому, свежим взглядом, с другой стороны. Этого уже нельзя прописать ни в каких инструкциях и приказах, это процесс творческий, решение может прийти неожиданно и внезапно, а можно и «зациклиться», гонять взад-вперед одни и те же идеи, не двигаясь с места. И вот тут важна обстановка, та атмосфера, в которой приходится работать теоретику. «Сидя все время на рабочем месте, работать по-настоящему невозможно» - такими словами меня встретили в отделе. Собрав полсотни математиков в одном месте, установив жесткий режим работы: с 9 до 6 вечера, невозможно добиться от них свежих идей. Очень часто самые красивые результаты получались не благодаря, а вопреки такому режиму: кто-то приноровился работать дома вечерами и ночами, отсыпаясь днем на работе, кто-то старался почаще брать больничный, библиотечные дни или аспирантский отпуск. Степанов все прекрасно понимал, но ничего поделать не мог или не хотел. Не мог он объявить во всем отделе свободный график работы, потому что все мы были действующие офицеры КГБ и подчинялись общему распорядку, установленному в Конторе.

Приход на работу – ровно в 9.00. Ежедневный обход контролера: все ли реально присутствуют на своих рабочих местах? Первые два часа, до 11.00 – творческое время. Все всегда дружно пытались договориться: ну давайте хоть первые два часа, пока голова еще свежая, никто никого не будет дергать, пусть будет возможность хоть немного спокойно поработать. Все эти благие намерения про творческое время быстро забывались, верх брали повседневные житейские проблемы: распределение продуктовых заказов, сдача партийных и комсомольских взносов, обсуждение бурных дебатов на последнем партсобрании, слухи о возможных новых назначениях и перемещениях людей и многое, многое другое в том же духе. Ровно в 11 – пятнадцатиминутная физкультурная пауза, которую, по традиции, в первые годы моего пребывания в отделе использовали под шахматные блиц-партии, а позже, после появления персональных компьютеров, – под компьютерные игры. Ожидание обеда, и обед в столовой, после которой многие вознаграждались хроническим гастритом. Военная часть, столовую обслуживали солдаты из местной роты охраны, практически никаких контролеров, интеллигентная обслуживаемая публика, которая не будет поднимать скандала из-за некачественной пищи. Примерно через год я пришел к твердому убеждению: а ну ее в болото! Проще приносить из дома бутерброды и термосы с горячим бульоном, чем добровольно, за свои деньги, загибаться в этой травиловке.

Ну а после обеда – мучительное ожидание конца рабочего дня. Как же медленно ползет время! Все проблемы уже обсуждены и переговорены с утра, все мысли в голове начисто перебиваются буйным обедом в желудке, перед тобой раскрытая тетрадь, гора предыдущих отчетов и часа четыре времени, оставшегося до финального свистка. Самое ненавистное время, ни разу ничего путного за это время мне в голову не приходило. И так каждый день, одно и то же, за редкими исключениями. Тоже ведь своеобразная школа выживания, в которой самое главное – не опуститься до уровня, когда эти повседневные проблемы вытолкнут все остальное из головы, когда забудешь о своем образовании, квалификации, призвании, займешься одной общественной или партийной работой, превратишься в заурядного сплетника и пустомелю из курилки.

Довольно быстро я понял, что такой образ жизни – не по мне, хотелось живой, интересной работы, хотелось видеть реальные результаты своей работы, которые можно выразить не только абстрактными теоремами, а чем-то иным, более приземленным, более понятным, более очевидным. Чтобы критериями успешного завершения работы были не одобрительные слова даже такого авторитетного человека, как Степанов, а что-то другое, тоже простое и понятное практически любому. У авиаконструктора, например, есть такие критерии: если его самолет успешно прошел летные испытания, значит он все сделал правильно, если у агронома вырос хороший урожай, значит он тоже сделал все верно. Да в том же 16 управлении, если вскрыли шифр, прочитали открытый текст – безусловный успех, заслуженная награда. Но в Теоретическом отделе 8 управления КГБ таких критериев чаще всего не было, случаи, когда удавалось «колонуть» какой-то свой действующий шифр были, во-первых, крайне редки, а, во-вторых, расколоть шифр с помощью абстрактного его анализа – это одно, а реально прочитать шифрованную переписку – это совсем другое. Отдел плодил кучи отчетов, статей в закрытые научно-технические сборники, проводил массу фундаментальных и прогнозных исследований, казалось, что собранные в одном месте сильные математики способны предложить новые оригинальные идеи, которые будут конкурентоспособны с последними американскими достижениями в криптографии. Но часто приходилось слышать такие речи:

- На самом деле мы здесь в резерве, на случай непредвиденных обстоятельств. А все эти теоремы – это так, чтобы не было скучно сидеть.

В триаде «специалист-офицер-чиновник» далеко не очевидно, что специалиста надо было ставить на первое место.

Но все же основное мое впечатление от времени, проведенном в отделе у Степанова – это очень сильный коллектив, в котором есть общепризнанный лидер, а у большинства сотрудников есть желание походить на такого лидера, достичь его уровня, составить ему конкуренцию. Такого коллектива мне, к сожалению, за всю последующую жизнь встречать больше не довелось. И любой молодой выпускник 4 факультета, попадая к Степанову, невольно впитывал в себя такие качества, как строгая логика в рассуждениях, подчинение их какой-то определенной цели, умение сразу же отличить реальные аргументы от пустой фразеологии, оценка человека по реальным результатам его деятельности. И эта степановская школа оказалась очень полезной во всей моей дальнейшей биографии, а прошедших ее людей потом приходилось встречать в таких организациях, как Газпром и Сбербанк.

Глава 3

Оперативные наряды

В 1980 году на Москву надвигалось не стихийное, а заранее задуманное бедствие – летняя Олимпиада.

Появилась эта рожа – сразу стало все дороже

Так в народе окрестили забавного олимпийского мишку, эмблему XX летних Олимпийских Игр. Любое мероприятие, раздуваемое советской пропагандой, вызывало настороженное отношение, а Олимпиада рекламировалась со всей удалью и прытью. Все традиционные советские массовые шоу, типа парадов на Красной площади и съездов КПСС уже приелись, не вызывали никаких эмоций, стали привычными спектаклями. А здесь впервые международное событие такого масштаба, призванное показать достижения развитого социализма (большей частью фиктивные), авторитет и признание ведущей роли СССР в мире (держащиеся исключительно на страхе перед ракетами и танками). Политическое событие, впервые Олимпиада проходит в социалистическом государстве, где расцвели свобода и демократия, нет эксплуатации и насилия (а также товаров в магазинах). Накануне Олимпиады в центральном клубе КГБ СССР лектор на полном серьезе около двух часов сравнивал перед офицерами КГБ условия жизни в США и СССР. Их зарплаты в 3000 – 5000 $ - это ничто, блеф, мистика, все деньги уходят на налоги, оплату жилья, медицину, да и вообще жизнь в Штатах невыносима, в два счета могут ограбить и убить. То ли дело в СССР, тишь да гладь, да божья благодать, живи себе и радуйся на свою зарплату, в 10 раз меньшую, чем в США.

Не могу сказать, что в то время подобные байки вызывали ярость. Нет, скорее полное равнодушие, собачка лает – ветер относит, провели мероприятие, поставили галочку в отчете – всем хорошо, и лектору и его слушателям. Коммунистическая система казалась вечной, ну подумаешь, дошли лидеры до старческого маразма, «сосиськи сраные» вместо «социалистические страны» произносят, нечего забивать себе этим голову. Все равно ничего не изменишь, а к тому же есть хорошее образование, работа, кусок хлеба, живешь как все, может даже в чем-то чуть-чуть лучше. Пусть все катится и дальше по наезженной колее, пока молодой, полон сил, энергии, чего думать о каких-то абстрактных проблемах и противоречиях. Пускай врут и дальше все эти лектора и пропагандисты, политинформаторы и агитаторы, мне от этого ни холодно, ни жарко.

Точно так же, в то время практически безразлично, отнеслось большинство народа к вводу советских войск в Афганистан в декабре 1979 года. Солдаты отправились защищать какую-то там апрельскую революцию, дело святое, или мы, или американцы – вот типичные настроения тех лет. Гораздо интереснее было наблюдать за всей затеей с Олимпиадой.

А Афганистан отразился на Московской Олимпиаде самым прямым образом. Американцы и их союзники, в знак протеста против ввода советских войск в Афганистан, призвали к бойкоту Олимпиады. Шоу грозило стать урезанным, неполноценным, неким немного расширенным вариантом спартакиады народов СССР. На пропаганду и агитацию были брошены все силы, в журналах публиковались карты боев, в которых страны, присоединившиеся к бойкоту Московской Олимпиады, закрашивались черным цветом, а обещающие приехать – красным.

На обеспечение проведения Московской Олимпиады были мобилизованы все без исключения сотрудники КГБ. Это называлось оперативный наряд. Главное – не допустить какой-нибудь провокации, под которой понимали в первую очередь антисоветские лозунги, митинги и демонстрации. «СССР – вон из Афганистана» - самый что ни на есть антисоветский лозунг, возмущенные советские граждане (капитаны да майоры) должны были сразу же дать ему решительный отпор и быстро доказать всему миру, что Советский Союз – самая миролюбивая страна в мире.

Не стало исключением и 8 ГУ КГБ СССР. Но польза от яйцеголовых, как от оперативников, была практически нулевая, поэтому большая часть сотрудников нашего отдела всю Олимпиаду провела на стадионе в Лужниках. Солнце всходит и заходит…, а болельщики – все те же.

Мне, к сожалению или к счастью, не довелось сидеть до посинения на стадионе. Небольшую группу сотрудников нашего отдела направили «на обеспечение безопасности и порядка» в гостиницу «Космос», куда съехалось множество иностранных туристов.

- Ребята, вы здесь совершенно не нужны, тут без вас уже тьма народа. Но раз уж вас прислали, то мне гораздо проще вас вообще не замечать, чем пытаться что-то изменить в такой ситуации.

Так нас приветствовал начальник оперативного штаба гостиницы, созданного на время Олимпиады. Доброе напутствие, а мужик, видно, хорошо знает реальную жизнь! В конце концов нашли оптимальный вариант для всех: мы парами дежурим в холле гостиницы, изображая из себя праздную публику, которой там и так хватало, но поскольку народа от отдела прислали много, «с запасом», а большой кучи народа в холле не нужно, то режим дежурства – день (с 10 утра до 8 вечера) дежуришь, а потом 3 (три!) дня – отдыхаешь. С таким режимом я был бы согласен на то, чтобы Олимпиаду в Москве проводили как можно чаще, хоть летнюю, хоть зимнюю.

В холле стоял большой телевизионный экран, весь ход Олимпиады можно было смотреть из удобного кресла, а не с галерки на трибунах. Советская пропаганда всячески заискивала перед приехавшими

иностранцами, и вместо того, чтобы попытаться получить с Олимпиады максимальный финансовый доход, старалась вовсю дудеть в идеологические дудки: мы не гонимся за прибылью, мы социалистическая страна.

- Завтра для зарубежных гостей столицы состоится теплоходная экскурсия по Москве и Подмосковью. Экскурсия бесплатная.

Зарубежные гости были немало удивлены подобной халяве. Наверное, такое было указание: занять иностранцев чем-нибудь, а то начнут еще по магазинам советским ходить (хотя и приукрашенным к Олимпиаде), с простыми людьми встречаться, беседовать о жизни… Забавный случай произошел на моих глазах с японцами. Наслушавшись вражьих голосов о проблемах с продуктами в СССР, они решили привезти все с собой. Упаковали еду в огромные баулы и вот с этими баулами предстали перед службой входного контроля гостиницы «Космос». А в этой службе были молодые ребята с собачками, натренированными на запах взрывчатки. Пока дежурный проверял паспорта, эти ребята подводили собачек к багажу и проводили свою проверку. И вот к баулу, забитому японской копченой колбасой, подводят такую собачку. Взрывчаткой не пахнет, пахнет чем-то другим, гораздо более вкусным, собачка не лает, но уходить от баула явно не хочет. Багажа много, проводник пытается силой оттащить ее, а она сопротивляется, и в конце концов решает это место пометить. На всякий случай, вдруг пригодится!

Бойкот Олимпиады – это была внешняя реакция мира на развязанную кровопролитную войну в Афганистане. Но совершенно неожиданно советская система получила уже во время Олимпиады наглядное отражение отношения к ней своего собственного народа. Это произошло в результате такого печального события, как внезапная смерть Владимира Высоцкого 25 июля 1980 года.

Официальная советская пропаганда старалась его не замечать, слишком нетривиальная и неудобная для властей это была личность. Признанный государством кумир должен был обязательно хоть раз в жизни (а то и чаще) похвалить партию и правительство за счастливую жизнь, сказать что-нибудь типа того, что его самая яркая роль – это чтение по TV книжек Л.И.Брежнева, прыгать от радости по поводу полученного от Генерального секретаря ЦК КПСС приветствия, ну на худой конец – спеть на праздничном концерте:

Малая земля – геройская земля
Братство презиравших смерть.

Ну и что с того, что у Высоцкого было много прекрасных военных песен, которые знала наизусть вся страна? Они не были одобрены в идеологическом отделе ЦК КПСС, хотя их слушали внуки Брежнева. Неуправляемый это был человек, чувствительный к той лжи, которая потоками лилась изо всех партийных щелей, не променявший свое истинное народное признание на дешевую мишуру официальных званий и наград.

Ни единою буквой ни лгу…

вот мотив его творчества, его выступлений с концертами перед тысячами простых людей в Сибири, на Камазе, на нефтяных промыслах, по всей стране.

Некролог о смерти Высоцкого напечатали только в одной газете, «Вечерней Москве», в нижнем углу на последней странице. Но на следующий день тысячи людей, презрев Олимпиаду, пришли проститься с ним к театру на Таганке. Власти растерялись и по привычке сделали вид, что ничего особенного не произошло, продолжая радоваться долгожданной Олимпиаде.

Москва была в шоке. Вся Олимпиадная помпезность и показуха сразу же как-то поблекли и выветрились, ясно стало видно циничное отношение правителей к своему собственному народу, к его горестям и потерям. Вот только изменить что-либо в той системе в то время было невозможно. Пройдет еще много лет, война в Афганистане станет суровой реальностью с многочисленными загубленными или искалеченными молодыми жизнями, только тогда общество начнет понемногу переходить к реальным действиям по избавлению от коммунистического дурмана.

Нам же Олимпиада ясно показала одно: математиков в системе КГБ считают за людей «второго сорта», рассчитывать на какое-то разумное использование полученного образования и навыков при подобных мероприятиях не приходится. Эта система в таких случаях работает по принципу «навались, ребята», без разбору посылая кого угодно и куда угодно, а после начальники раздают сами себе ордена и награды. Но особого сожаления о том, что не являюсь «истинным» чекистом, я почему-то не испытывал.

После Олимпиады за время моей службы в КГБ в Москве прошло еще несколько подобных мероприятий, на которых нас использовали в качестве «оперативников». Но все они, как правило, оставляли одно и то же тусклое впечатление: бесконечное и бесцельное высиживание, не требующее ни ума, ни знаний, ни образования, а только терпения и умения как-то подавлять скуку. Правда, в 1986 году одно такое мероприятие немного выделилось из этого серого ряда. Это был чемпионат мира по хоккею с шайбой, проходивший в Москве во дворце спорта «Лужники».

Хоккей с шайбой – это любимая игра моего детства, у него были миллионы поклонников, достать билеты на матчи с участием советской непобедимой сборной было для многих несбыточной мечтой. Усилиями выдающегося тренера, фаната своего дела Анатолия Владимировича Тарасова сборная СССР почти всегда побеждала, игроки поражали своим виртуозным мастерством, а во дворах на многочисленных хоккейных «коробках» мальчишки старались подражать Фирсову, Харламову, Старшинову, Рагулину, без конца комментировали каждый забитый ими гол, их финты и обводки.

И вот теперь у меня появилась возможность не просто посидеть на трибуне во время матчей чемпионата мира по хоккею, а проникнуть за кулисы, в фойе перед раздевалками команд, увидеть своих кумиров живьем, поговорить с ними, взять автографы. Оказалось, что большинство наших хоккейных звезд – совершенно нормальные ребята, гораздо менее заносчивые, чем КГБшные генералы, тренирующиеся до седьмого пота, добывающие свою славу и награды очень тяжелым трудом. И находящиеся под пристальным вниманием различных людей, не всегда преследующих только честные и благородные цели.

Примерно за два часа до начала финального матча за золотые медали СССР-Швеция один иностранный корреспондент, который стоял на улице и его не пускали к раздевалкам, стал просить о встрече с Игорем Ларионовым. Корреспондент говорил только по-английски, обычные охранники не могли его понять и попросили меня, как человека, слегка объясняющегося по-английски, узнать, чего он хочет от одного из лучших игроков сборной СССР.
Он показал мне пачку фотографий.

- Это сборная СССР после прошлогоднего чемпионата мира, проходившего в Праге. После окончания игр был прием в Ратуше. Это советская команда на приеме, а это серебряное ведерко для шампанского, которое было полное водки и советская команда его выпила.

Ничего особенного на этих фотографиях не было – молодые ребята после трудного чемпионата, совершенно нормальные. Но в Советском Союзе того времени разрешалось изображать советских кумиров только положительно, а полное водки серебряное ведерко для шампанского явно не укладывалось в эти стереотипы. Все было до предела очевидно – перед решающим матчем корреспондент хотел испортить настроение нашим хоккеистам. В хоккее чехи были нашими давними заклятыми друзьями и не гнушались никаких методов.

Но советская сторона тоже не оставалась в долгу. Спонсором того чемпионата мира было чешское отделение компании «Пепси-Кола», они развесили везде свою рекламу и установили в фойе перед раздевалками два автомата для бесплатной раздачи этого напитка. Народу в этом фойе было немного, но народ попадался иногда очень даже боевой. У автоматов дежурили две куколки-чешки, которые иногда отлучались со своего поста. И вот тут российский народ показывал, на что он способен, давал чехам свой, асимметричный ответ на их происки.

В мирное время, т.е. во времена обычных соревнований, в этом фойе дежурили две бабули – то ли администраторши, то ли билетерши. На время чемпионата мира все их контрольные функции взяло на себя КГБ, а бабули первое время сидели безо всякого дела. Но это продолжалось недолго. Вскоре они, как только куколки-чешки покидали свои автоматы, стали делать таинственные знаки и тотчас же из близлежащих кустов появлялись другие такие же бабули с трехлитровыми банками, которые бабули-агенты тащили к чешскому автомату.

Не прошло и половины чемпионата, как представитель чешской «Пепси-Кола» стал взбудораженно бегать по фойе и удивляться, почему такой большой расход у этих двух автоматов. Практически все запасы фирмы на весь двухнедельный чемпионат мира были израсходованы меньше чем через неделю и чехословацкому отделению Пепси-Кола стал грозить международный скандал.

Да, это был, пожалуй, единственный оперативный наряд за всю мою КГБшную практику, на память о котором остались яркие воспоминания, красочный альбом с автографами практически всех советских хоккейных звезд, канадская шайба и шведская клюшка.

Глава 4

Шифры на новой элементной базе

Про шифры на новой элементной базе я уже несколько раз упоминал в этой книге, но в основном абстрактно: были заложены основы, велись теоретические разработки. А как пощупать их руками? Что в них было действительно нового?

Здесь надо немного окунуться в ту «докомпьютерную» эпоху. Что такое микропроцессор – представление об этом было весьма расплывчатое. Что-то такое, что реализовано с помощью никому тогда не ведомого процессора, но только очень маленького, размером с копеечную монету. Живьем микропроцессор мало кто видел, только общие сведения: способен выполнять некоторые операции с двоичными векторами, достаточно быстро по сравнению с типовыми логическими элементами. Один раз,

еще в Высшей Школе КГБ, нам, рассказывая про микропроцессоры того времени, сказали, что их стоимость сравнима со стоимостью золота, сопоставимого по весу с микропроцессором.

Сначала, как только я пришел на работу в отдел Степанова, там загорелись идеей создать специализированный криптографический процессор, ориентированный на выполнение определенных криптографических преобразований. Что это должны быть за преобразования – тоже не было единого мнения. Преобразования для системы с открытым распределением ключей? Или для симметричного шифрования, без которого система с открытым распределением ключей теряет всю свою эффективность? В общем, начальный период создания криптографического процессора прошел в абстрактных криптографических спорах, которые были спущены на грешную землю одним простым вопросом, заданным спорщикам инженером, приглашенным из Зеленоградского завода Ангстрем, на котором предполагалось изготавливать эти процессоры:

- А какой толщины должен быть слой лакового покрытия вашего процессора?

Все криптографы сразу же выпали в полный осадок. Ответить на вопрос о толщине слоя лакового покрытия никто не смог, абстрактный криптографический процессор, рожденный в умах теоретиков, так там и остался.

Но идеи шифров, реализуемых с не с помощью какого-то надуманного криптографического микропроцессора, а с помощью начинавших появляться в то время самых обычных микропроцессоров для портативной бытовой электроники, оказались весьма живучими. Все очень просто: есть выпускаемые промышленностью микропроцессоры, выполняющие стандартные арифметические операции, их производительность невелика, но они очень дешевы. Задача криптографов - приспособить эти стандартные процессоры для выполнения криптографических преобразований. Не гора должна идти к Магомету, а Магомет к горе.

Однажды к нам в гости пожаловали ребята из НИИ Автоматики. Это был один из ведущих институтов Министерства радиоэлектронной промышленности, который занимался разработкой шифрующих устройств и в котором работало много выпускников 4 факультета. В теории 8 управление КГБ должно было выполнять только экспертные функции, разработку шифраторов должна была проводить промышленность, но в реальной жизни все тесно переплеталось, наш отдел постоянно выдавал какие-то идеи для новых схем, масса людей писала на этом диссертации, поэтому провести четкую грань между разработкой и экспертизой часто было невозможно.

Эти ребята тоже занимались разработкой шифров на новой элементной базе. Но они были практиками, для них первичным было «железо», реально существующие в то время микропроцессоры, под которые надо было придумать криптосхему, в которой все преобразования осуществляются не с традиционными битами, а сразу с байтами, 8-мерными двоичными векторами.

- Мы постарались придумать максимально простую для реализации криптосхему. Вы можете прикинуть оценки ее стойкости?

Ребята молодые, может быть старше меня года на 3 - 4. Один из них уже начальник сектора, пишет диссертацию. Эта тема – шифры на новой элементной базе – интересует многих. На 4 факультете кафедра математики подготовила два солидных отчета о проведенных исследованиях по аналогичной теме, несколько человек уже защитились. Новое, перспективное направление, что же оно из себя представляло?

Здесь я вынужден извиниться перед читателем этой книги, не имевшим ранее никаких дел с математикой. Сейчас придется немного залезть в теорию групп и теорию подстановок, со своими специфическими терминами: симметрическая группа, циклическая подстановка, свойство 2-транзитивности и т.п. Может быть неискушенный читатель пробежит эту часть «по-диагонали», не вдаваясь особо в подробности и не забивая себе в голову всех этих премудростей. Но в математике, как и в любой другой области науки, иногда удается получить красивый результат, и, чтобы оценить его красоту, надо немного вникнуть в детали, подробности, предшествующие его получению. Так что читатель, окунувшийся в начинающиеся ниже математические дебри (не такие уж и сложные, как может показаться на первый взгляд!), в конце концов будет вознагражден одной красивой «изюминкой».

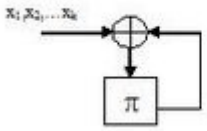
Большинство традиционных электронных шифраторов реализовано с помощью «балалаек», работающих с битами. В этих «балалайках» в ячейки регистра сдвига могут быть записаны только два элемента – 0 или 1, такой регистр сдвига называется регистром сдвига над полем GF(2) - полем Галуа из двух элементов. Операции с битами тоже весьма простые: сложение и умножение по модулю 2, а также отрицание. Все методы анализа подобных «балалаек» ориентированы на двоичные операции, на операции в поле GF(2).

Если же мы вместо битов переходим к байтам, то появляется много нового. Традиционные операции с байтами можно осуществлять несколькими способами. Например, сложение и вычитание могут быть с переносом или без переноса, т.е. или это будут операции в кольце вычетов по модулю 256, или покоординатное сложение бит. Но самое интересное обобщение происходит с операцией отрицания.

Отрицание (инверсия) бита – это фактически подстановка на множестве из 2 элементов. Когда всего 2 элемента, то мощность симметрической группы S_2 составляет всего 2! = 2, всего две подстановки: тривиальная единичная (ничего не меняется) и инверсия, когда 0 переходит в 1, а 1 – в 0. Мощность же симметрической группы S_{256} составляет 256! – совершенно фантастическое число. Введение подстановки в регистр сдвига, работающий с байтами, а не с битами, переворачивает все привычные методы криптографического анализа. Совершенно другие операции, а следовательно, нужны и другие подходы к анализу и оценке стойкости таких схем, чем те, которые использовались в традиционных двоичных «балалайках».

С чего начала кафедра математики на 4 факультете? С самого простейшего преобразования, осуществляемого с n-мерными двоичными векторами, с преобразования типа $(Gp)^k$, где G – группа, порожденная циклическим сдвигом ($G = \langle g \rangle$, $g = (0,1,\ldots,2^n-1)$-циклическая подстановка), p - некоторая фиксированная подстановка из S_2^n, а k – некоторое целое число.

Если здесь перейти от математических терминов из теории групп к обычной криптографической терминологии, то преобразование типа $(Gp)^k$ – это следующий узел.



Преобразования типа $(Gp)^k$ - это, фактически множество подстановок вида $g_{x1}p\ g_{x2}p\ldots\ g_{xk}p$, и задачей кафедры математики было обосновать какие-то свойства подобного множества, найти их зависимости от подстановки p. Типичная криптографическая ситуация – когда в таком узле *входное слово* $x_1,x_2,\ldots x_k$ является ключевым параметром, требуется найти подходы к его определению по нескольким известным переходам в реализуемой подстановке.

Кафедра начала с изучения группы $\langle g, p \rangle$, т.е. группы, порожденной двумя подстановками: циклическим сдвигом g и фиксированной произвольной подстановкой p. Это естественное обобщение преобразования $(Gp)^k$, предельный случай. Свойства группы $\langle g, p \rangle$ дают ответ на вопрос, что в принципе можно ожидать от нашего преобразования при увеличении длины k до бесконечности. Можем ли мы таким путем получить все подстановки или же есть какие-то запреты?
Оказалось, что если случайно и равновероятно выбрать из всей симметрической группы фиксированную подстановку p, то с вероятностью, близкой к 1, группа
$\langle g, p \rangle$ будет совпадать со всей симметрической группой, т.е. запретов не будет. Те подстановки p, для которых это не так, очень часто легко определяются, например,
p=g, а также любая линейная подстановка, реализующая преобразование вида
$p(x) = ax+b$, где a и b – фиксированные элементы из $Z/2^n$.

Дальше, естественно, стали возникать вопросы: а как скоро мы сможем достичь симметрической группы? Какова будет мощность *слоя* $(Gp)^k$ при некотором значении k, например, при k=2 или при k=3? При каком k множество $(Gp)^k$ станет
2-транзитивным, т.е. по имеющимся в нем подстановкам любая пара (y_1,y_2), в которой $y_1{}^1y_2$, сможет перейти в любую пару (z_1,z_2), в которой $z_1{}^1z_2$? Что в общем случае можно будет сказать про обобщение 2-транзитивности – m-транзитивность?

За свойство 2-транзитивности взялись основательно, чувствовалось, что здесь могут быть интересные криптографические зацепки: если 2-транзитивность отсутствует, то появляются запреты переходов биграмм текста, широкое поле деятельности для криптоаналитика. Например, если p - упомянутая выше линейная подстановка, то для любой пары (y_1,y_2) будет справедливо соотношение:

$$p(y_1)- p(y_2) = (ay_1+b) - (ay_2+b) = a(y_1-y_2)$$

В этом случае при применении подстановки p сохраняется соотношение между разностями знаков, а поэтому кратной транзитивности заведомо не будет.
А если p - не линейная, а произвольная подстановка? При каком минимальном значении k множество $(Gp)^k$ может достичь свойства 2-транзитивности? Всего имеется $2^n(2^n-1)$ различных пар (z_1,z_2), в которых $z_1{}^1z_2$, а количество различных подстановок в $(Gp)^k$ не превосходит $(2^n)^k$. Следовательно, свойства 2-транзитивности можно достичь только при $k^3 2$. Можно ли при k=2?

Рассмотрим множество подстановок $(Gp)^2$. Это множество реализует всевозможные преобразования произвольного значения t в значение s по формуле
$s = p(p(t+x_1)+x_2)$ при всевозможных x_1,x_2. Если бы это множество было 2-транзитивным, то для любых заранее фиксированных s_1,s_2, t_1,t_2, в которых $s_1{}^1s_2$ и $t_1{}^1t_2$, система уравнений:

$s_1 = p\,(p\,(t_1+x_1)+x_2)$
$s_2 = p\,(p\,(t_2+x_1)+x_2)$
имела бы решение относительно x_1,x_2, а, следовательно, поскольку p - подстановка, то и система
$s_1 = p\,(t_1+x_1)+x_2$ (1)
$s_2 = p\,(t_2+x_1)+x_2$
имела бы решение для любых заранее фиксированных s_1,s_2, t_1,t_2, в которых $s_1 \neq s_2$ и $t_1 \neq t_2$
Отсюда, вычитая одно уравнение из другого, мы приходим к одной очень важной криптографической характеристики подстановки p - матрице частот встречаемости разностей переходов ненулевых биграмм P(p) размера $(2^n-1)\times(2^n-1)$, а именно, на пересечении i-ой строки и j-го столбца в этой матрице стоит значение p_{ij} - число решений системы уравнений относительно x и y:
$x-y = i$ (2)
$p(x) - p(y) = j$
где $i, j \neq 0$.

Если при каких-то $i, j \neq 0$ $p_{ij} = 0$, то это означает, что при заранее фиксированных s_1,s_2, t_1,t_2, в которых $s_1 \neq s_2$ и $t_1 \neq t_2$, а также $t_1-t_2 = i$, $s_1-s_2 = j$, система (1) заведомо не имеет решения, ибо в противном случае имела бы решение и система (2).

Заметим, что $p_{ij} = p_{(2^n-i)(2^n-j)}$. Действительно, каждому решению (x_1,y_1) системы (2) можно поставить во взаимно однозначное соответствие решение $(x_2,y_2)=(y_1,x_1)$ системы
$x-y = 2^n-i$
$p(x) - p(y) = 2^n-j$
если домножить на –1 оба уравнения (2).
Из системы (2) очевидно вытекает, что число ее решений равно числу значений y, при которых
$p(y+i) - p(y) = j$ (3)
Если каждому решению (x_1,y_1) системы (2) поставить во взаимно-однозначное соответствие пару $(x_2,y_2) = (p^{-1}(x_1),p^{-1}(y_1))$, то такая пара будет решением системы
$x-y = j$ (4)
$p^{-1}(x) - p^{-1}(y) = i$
Следовательно, число решений системы (2) будет равно числу значений y, при которых
$p^{-1}(y+j) - p^{-1}(y) = i$ (5)
Из (3) очевидно вытекает, что сумма всех элементов p_{ij} в i-ой строке при любом i равна 2^n. Аналогично, из (5) вытекает, что сумма всех элементов p_{ij} в j-ом столбце при любом j равна 2^n.
Поскольку размер P(p) равен $(2^n-1)\times(2^n-1)$, то из условия, что сумма всех элементов p_{ij} в i-ой строке при любом i равна 2^n следует, что если бы P(p) не содержала нулей, то в любой ее строке все элементы были бы равны 1, кроме одного, равного 2. Аналогично получаем, что в этом случае в любом столбце должны быть все элементы 1, кроме одного, равного 2.
Если при некотором y выполняется
$p(y+2^{n-1}) - p(y) = 2^{n-1}$, (6)
то, поскольку $2^n-2^{n-1} = 2^{n-1}$, то (6) будет справедливо и при значении $y_1 = y+2^{n-1}$. Таким образом, элемент $p_{(2^{n-1})(2^{n-1})}$ не может быть нечетным.
Предположим, что некоторая i-я строка целиком ненулевая. Это означает, что среди значений $j_0,j_1,\ldots,j_{2^n-1}$, получаемых по формуле
$j_k = p(k+i)- p(k)$ (7)
содержатся все ненулевые элементы из $Z/2^n$, а какой-то один элемент встретился ровно 2 раза.

Просуммируем соотношение (7) по всем k от 0 до 2^n-1. Поскольку p - подстановка, то в правой части суммы получается 0, следовательно, сумма всех значений j_k также должна быть нулевой.

Но среди $j_0,j_1,\ldots,j_{2^n-1}$ содержатся все ненулевые элементы из $Z/2^n$, а какой-то один элемент встретился ровно 2 раза. Поскольку сумма (по модулю 2^n) всех ненулевых элементов кольца $Z/2^n$ равна $2^{n-1}(2^n-1) = 2^{n-1}$, то элементом, встретившимся два раза, должно быть 2^{n-1}.
Тогда, в силу свойства $p_{ij} = p_{(2^n-i)(2^n-j)}$ для любого значения i должно выполняться
$p_{i2^{n-1}} = p_{(2^n-i)2^{n-1}} = 2$
и при $i \neq 2^{n-1}$ получается, что в 2^{n-1} столбце как минимум 2 элемента равны 2. Следовательно, если некоторая i-я строка при $i \neq 2^{n-1}$ целиком ненулевая, то 2^{n-1} столбец заведомо содержит хотя бы один нулевой элемент, т.е. множество $(Gp)^2$ не является 2-транзитивным ни при какой подстановке p.
И еще отсюда сразу же вытекает, что общее число нулей в матрице P(p) не может быть меньше, чем 2^n-3. В этом случае в матрице ровно две ненулевых строки, расположенных симметрично друг от друга, а в средней строке с номером 2^{n-1} ровно одно нулевое значение посередине: $p_{(2^{n-1})(2^{n-1})} = 0$.

Подобными же методами легко показать, что в общем случае множество $(Gp)^k$ является 2-транзитивным при $k>2$ в том и только том случае, когда матрица $P(p)^{k-1}$ не содержит нулей. В частности, множество $(Gp)^3$ является 2-транзитивным тогда и только тогда, когда матрица $P(p)^2$ не содержит нулей.

Стало ясно, в каком направлении вести математические раскопки теории шифров на новой элементной базе: изучать матрицы P(p) для различных подстановок p. Здесь сразу же выделялись плохие подстановки – это линейные преобразования вида

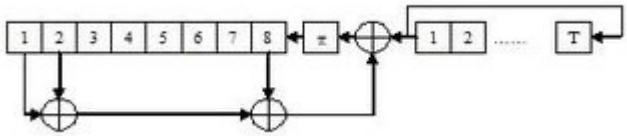
$$p(x) = ax+b$$

В этом случае при любом фиксированном $i^1 0$ система (2) имеет решение только при одном значении $j^1 0$, такая матрица заведомо не будет положительной ни в какой степени и свойство 2-транзитивности недостижимо. Число нулей у такой матрицы будет *максимальным*.

А можно ли построить подстановки с *минимально* возможным числом нулей в матрице P(p)? Этот вопрос уже гораздо интереснее, простого и тривиального ответа на него нет. Пока. Но в следующих главах этой книги ситуация прояснится и в конечном итоге получится очень красивый результат.

Но это больше теоретические дебри. С точки зрения практического применения гораздо важнее знать, чего можно ожидать от матрицы P(p) при случайном и равновероятном выборе p. И здесь были доказаны очень важные теоремы о том, что в среднем ненулевых элементов в этой матрице будет примерно 2/3, что с вероятностью, близкой к 1, при случайном и равновероятном выборе p матрица $P(p)^2$ небудет содержать нулевых элементов, а группа <g,p> будет совпадать с симметрической. В общем, все то, что требуется для использования подстановки p в качестве случайного разового ключа.

Вот такая была предыстория работ по шифрам на новой элементной базе. А ребята из НИИ Автоматики, по мотивам всех этих результатов, придумали следующую схему блочного шифра, работающего на основе байтового регистра сдвига и использующего только самые типовые операции с байтами, которые заложены в архитектуру появлявшихся тогда микропроцессоров. Эту схему назвали «Ангстрем-3».



В ней два регистра сдвига, работающих с байтами. В первый регистр сдвига длиной 8 байт записывается 8-байтовый блок открытого текста, во второй – ключ, или как его еще можно здесь назвать входное слово, длины T для первого регистра. Схема крутится T тактов, после чего заполнение первого регистра выдается в качестве 8 байтового блока шифртекста. Типичный блочный шифр, все операции сложения – в кольце Z/256, реализация – изумительно простая, если писать программу, то это буквально две-три строки.

Но программы будут позже, а пока, в 1980 году, эту схему предполагалось реализовывать аппаратно, с помощью типовых микропроцессоров, работающих с байтами. Идеи подстановки-ключа тоже появятся позже, первоначально предполагалось p выбрать и зафиксировать. А главный вопрос, который интересовал НИИ Автоматики – до какого предела можно уменьшать значение T, количество тактов, которые должна отработать схема для зашифрования одного блока. Чем меньше T, тем выше скорость шифрования, а это было для них определяющим фактором.

- Нельзя ли выбрать T=16?

Нужно подумать.

Так начиналась моя осмысленная работа в Теоретическом отделе. Перед глазами - чистая тетрадь, отчеты 4 факультета и НИИ Автоматики, сиди и думай, нельзя ли выбрать T=16.

Глава 5

Взломаем?

Итак, читатель, давай себе представим, что мы – высококвалифицированные криптоаналитики из американского АНБ. Собственный загородный трехэтажный особняк, жена-красавица, три машины, одна из которых джип для воскресных поездок к морю, ежемесячный оклад тысяч так 5 – 6 USD.

На этом месте мое воображение представлять что-нибудь еще просто отказывается. Так и хочется воскликнуть, немного перефразируя крылатые слова Жеглова – Высоцкого:

- Ну посмотри, какой из тебя американский криптоаналитик? У тебя же зарплата 250 рублей на лбу написана!

Так что лучше представить себе что-нибудь другое, ближе к нашей Российской действительности. Например, вот такую вот сценку, свидетелем которой мне довелось быть уже намного позже, в 1993 году в период активной работы с Центральным Банком России.

Это было вскоре после успешного внедрения системы защиты телеграфных авизо. Руководство ЦБ решило устроить селекторное совещание со всеми крупнейшими расчетно-кассовыми центрами (РКЦ) и пригласить на него разработчиков системы защиты с тем, чтобы все смогли напрямую высказать свое мнение о системе и предложения по ее совершенствованию. Но помимо системы защиты телеграфных авизо все старались воспользоваться благоприятным моментом и донести до центробанковского начальства свои заботы и печали. Так мне невольно пришлось стать свидетелем реальных будней из жизни Российской глубинки. Один момент из жизни инкассаторов (они должны были развозить секретные ключи для системы защиты авизо) запомнился особо.

- Недавно в нашем РКЦ произошло ЧП. Один из инкассаторов, будучи в нетрезвом состоянии, на спор пробил ломом бронированное лобовое стекло инкассаторской машины.

Вот это уже родное, а то какие-то американские криптографы с их роскошной жизнью! Так что давайте представим, что один советский криптограф на спор взялся взломать «Ангстрем-3» при T=16. А другой (начальник) пообещал, что если взломает, то ему прибавят к ежемесячному окладу в 250 руб. еще 20 руб.

Здесь я еще раз хочу извиниться перед читателями за ту криптографическую рутину, которая сейчас последует. Что поделаешь: сказывается многолетняя привычка никогда и ничему не верить на слово, требовать ясных и четких доказательств. Заявлено: шифры на новой элементной базе, новое перспективное направление, математические результаты… Хватит общих слов! Нужны конкретные результаты! Что там было нового и как анализировались эти шифры? И здесь, признаюсь, началось с того, что первый пример шифра на новой элементной базе был самым тривиальным образом взломан. Так, как в этом примере.

Вот шифровка, которую надо прочитать.

D8 C7 83 EF F9 CA 71 FA 07 55 16 9B 3A 1A 99 53 87 CC 83 9D FA 1D D6 D8 35 98 FA 84 A2 57 EE 67 F2 F1 B7 63 2D AC 6C EB 76 08 38 99 B3 D5 83 A9 31 CB 5C 03 9A 2A 3C 23 8A 8F DC 62 CD 72 C5 DE 5C E2 0C 7B A8 1E B4 96 D9 77 28 30 EA CD F9 38 89 BB 30 71 08 EC 01 50 2C E0 E2 C4 2B 03 8B 30 35 C3 10 A5 86 92 B8 06 F7 F2 00 21 BF 28 4E 0A 04 67 11 07 B6 7E 7C 5D AA 25 7F 68 1B 09 F2 81 FF E4 31 A5 41 4D CA BE D1 58 85 1F 76 F3 DE 89 03 40 9D B4 00 50 29 99 EC C9 DF BB 66 86 6D CC CA 2F 0E 93 E7 2D AB 38 F3 1B AD EE 55 09 44 B3 D6 D3 CC 4F 0A 01 0D 63 78 FA 9D D4 A1 C9 84 85 CC B5 4C D4 99 5C 4D CB 2E 92 F0 29 19 7B 85 7F 7C 9E FD 63 7F 9B 95 5A 4D D7 AF A5 CD 6E 80 5F A5 B8 9E E5 C9 AB 6F 0F CD 33 46 98 6A D5 66 21 D4 E9 19 20 3E AD 03 6E F6 6D 8A 73 F6 B2 CE 60 F1 AE 87 A7 11 18 36 46 E8 C5 3A 30 9A 24 F2 65 55 8D 49 90 BD 0D F5 FD 29 D2 56 D9 D0 A9 92 22 16 76 D9 69 67 C2 B7 6A 42 CB E2 82 36 94 ED C0 91 2E A0 9D CD B0 9B FC 5C 77 15 5A C4 ED 17 54 22 22 F2 E3 26 39 A5 4A E6 91 63 7F 60 A0 F2 EA 5C 6A FF 9F D3 0F E0 63 0E 69 97 A8 05 5A 91 07 65 52 65 E0 6C DF EA EB 28 4E B4 34 FF AC B1 36 35 C8 19 DE 44 02 8B F1 50 6F CE 1C 6C 99 55 0E 2E 92 F0 29 19 7B 85 7F E8 D3 CB 3B 84 79 D7 8E 62 88 D6 2F D1 D9 2E 9F EE B1 D6 54 85 D2 65 ED 3A 73 F8 C5 90 E5 ED DB 6F B8 A2 0F 01 D6 CA B6 B7 9C B1 31 12 EA 45 48 F6 D0 D4 A2 F0 45 3B E9 AE D1 14 04 22 2C 15 FB CA 3E 58 99 14 3F 51 29 49 43 4D 95 48 FD 6C 2F ED 48 0C C9 6B F6 BC F9 5A EE 79 E9 0C 35 A2 F4 A6 C7 4E 1E B1 2B CB F9 A3 4B 30 9F 57 51 6A 90 97 72 45 90 72 95 BE 19 7B F3 D2 41 34 18 9D E1 BA 7C EF 07 35 B3 A1 D9 CF 2D 6B 80 5C F4 73 93 A8 3B 78 B5 3D 09 00 BE 85 09 B7 98 B6 74 BE 45 40 29 43 0E 92 92 C2 AA B1 50 94 AB FD CE 2D B5 8D 4E CD 35 DD 05 EA C2 6E C0 CE 45 3F 29 4D E8 49 8C D9 7B A7 D9 2A 59 C8 50 25 F3 29 29 F0 D2 27 3B BB E7 1D 7C 58 8C 7C D4 0E E2 7F 55 16 A1 89 2D A0 8D EC 82 2B C5 6B 88 2C 45 10 D9 46 55 4B 26 CC 25 21 8E 7D D7 4C CD 7C DE A5 A1 25 15 C4 52 5D 81 66 B6 6B 48 97 F2 A7 A1 8C E4 ED 39 82 E9 7C 6A AE 4A 8A 7F B0 32 43 57 F2 E4 EB 2A 13 14 51 5E CF 03 F7 02 F2 C2 38 5A 00 79 7C 04 6D 4E 50 46 E1 8D 55 9F 98 E5 04 F4 03 8F DF 28 DC 09 AB 9C C2 9C 36 24 A9 93 43 F2 C7 2C 01 EE F6 3D 63 74 EC 04 4F 2A 64 11 69 E2 F2 BE 50 F4 46 D3 6E AA CD EE F2 87 9E 6B 46 8F 27 7D B2 9A 73 4E DB 02 64 29 90 C7 00 28 A6 3F 0A 3E 06 62 C3 76 D9 BA 75 CD AC 05 3C 51 DF 7D 29 16 44 80 0C 8B DF 53 EB C0 1E 48 04 B6 40 4F 77 75 88 D0 28 76 EE 70 B6 D5 3C 44 77 AD 6C 13 55 AC 8D 15 18 C4 6B DD FF 0C 32 60 7B 52 2F B8 0E 57 E2 01 0F A5 85 C9 69 DD DC 5D D0 60 27 64 28 43 AD 11 19 B1 25 6D AF 36 F5 80 F3 CB 54 91 F0 B6 08 B8 11 FD 5C A3 C9 41 BD 70 86 27 AB 26 AB 31 BA FE F7 36 0B 06 69 8B 65 24 B0 54 6A A0 CD F9 19 CC E3 E2 77 5F F3 D5 1B 39 99 64 0A 69 F0 B4 BF E4 6D 9B B4 63 28 B1 1C DD E5 A1 B1 87 E8 83 3D 99 C2 E0 09 3C 70 96 61 7E 9E FE FA 47 CE 91 16 FF AA 11 EA 20 A1 7E 5A BB 43 47 33 0E C4 B8 34 78 EE AF 74 EF 23 81 B3 EE 47 44 05 18 2A CB 6D 4E A4 0C 2B 2F 8D 2D 93 03 3C 91 F4 48 08 50 FB DC 91 BC 5F 7B B4 C1 2F BC 81 9E FA 57 2E 20 AB 38 0D 8D 92 A0 87 6D 58 8A B6 86 DE 31 60 94 2C D7 41 8C E8 99 CA 2E 63 D8 0E 0A A4 7C 6A FB A8 76 E1 B8 A9 4F 75 41 08 CA 74 24 9C 6F D2 86 49 E4 DF D8 88 CD BC 79 AE DE 5C 1D D1 6E 23 61 FE 38 08 C1 6E 0B 4A F5 F3 75 61 95 04 D2 8A 4F 35 4F 96 D1 9F CC F7 63 33 AB D0 75 29 74 82 68 84 5A 3A 50 1A 55 D4 37 6A 9B 12 49 C9 6F 9C 2A 83 D7 12 5C 87 0D F3 AB 67 32 BF 0A 9B 9D 9E 50 74 BD BC 75 87 E9 19 21 92 C5 C6 A8 0A 0C 6F 9E D9 09 C8 1A F4 11 81 E8 A3 52 6D 06 48 FE 04 AF 31 1C 3D 51 2B 33 B5 2F 21 85 08 F4 13 C2 8D C2 C8 7B D9 0E EC D8 F5 30 C0 0E AB D8 AB ED F5 38 3D 4A E6 06 C6 84 89 4B 29

A4 B2 56 E7 FE D3 6C 82 62 3A 1F F8 93 5A 41 EC F6 4C 1C 7E 72 91 E0 67 FD 92 9A 94 B3 45 63 FC BC 6E 3B BD 41 F7 A4 DA 0E 6B 48 E1 61 5A 7A 7F 4A 50 1E 85 99 CA 8C 47 64 5A A6 1F 5C EC BF 5D 5B 12 A3 13 D6 4A 4D CC E0 AC C7 52 CA 2B E4 1F E5 76 22 9C 91 7F AF 94 21 D6 BC F1 6E CC AA AD E7 15 77 09 10 36 8A 8D F5 35 95 41 30 43 62 C8 09 46 D3 6E AA CD EE F2 87 F0 4B E2 7C DE 71 96 58 CF 24 AF 9F 57 0E 7E 97 FC 73 06 4B 91 3C 5B 12 5E D6 E7 94 E3 4B 91 C9 2E 55 FF 64 00 7F 08 36 05 0F 1C 33 BB A6 3A C2 02 FC 5F B8 B9 4B 92 ED 8A 69 CF 37 F8 2A EA E1 6A AB A4 6F AF 6E C3 D0 B8 92 39 56 C0 38 FA 07 AD 8F 21 79 4E 95 EF B5 13 A1 59 64 70 64 D1 8A 35 1D 25 F6 C6 D5 0D 01 4E FF 62 D4 D5 50 8E A4 C3 EC C1 C0 A0 0C F8 AE 11 60 DE 21 11 8C CB A1 04 F6 04 05 6F 72 4A 27 F2 3E C0 0C 39 11 61 4B F3 CA F0 E6 0A 8C 52 A3 C3 F3 F8 21 18 0B 28 AF 47 55 03 88 A4 03 D5 B6 F0 75 EB BD E2 7C 49 56 22 76 F8 1D EA B8 5B 1A 7F CE 84 00 D5 97 84 B9 74 B3 AD 3D 13 EE F2 60

Эта шифровка в ASCII-символах, т.е. в элементах по модулю 256, представленных в шестнадцатиричной записи. Известно, что она была получена с помощью схемы «Ангстрем-3» при T=16 и известна подстановка p:

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
B4	BA	3C	CB	F6	7E	09	3F	57	51	98	EE	31	89	E9	27

10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
BD	0A	86	24	35	0F	C1	77	2D	3A	2A	B2	33	DB	4E	56

20	21	22	23	24	25	26	27	28	29	2A	2B	2C	2D	2E	2F
A6	7D	B7	FE	D4	B8	21	CC	58	32	F9	14	B3	F4	1C	48

30	31	32	33	34	35	36	37	38	39	3A	3B	3C	3D	3E	3F
28	F8	CD	25	DC	E8	F7	1A	2E	38	A5	00	53	6A	BF	FA

40	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E	4F
37	9C	07	A0	91	59	54	7B	45	92	0D	A1	FF	0E	EA	A2

50	51	52	53	54	55	56	57	58	59	5A	5B	5C	5D	5E	5F
10	CE	E5	BE	7C	F3	85	4B	78	C3	50	5F	DD	F1	87	C0

60	61	62	63	64	65	66	67	68	69	6A	6B	6C	6D	6E	6F
1F	2F	26	0B	64	F5	1B	29	D8	8D	CF	EB	52	6B	C7	0C

70	71	72	73	74	75	76	77	78	79	7A	7B	7C	7D	7E	7F
2B	A3	C5	4C	55	C9	E3	E2	C2	FB	22	2C	04	11	1D	81

80	81	82	83	84	85	86	87	88	89	8A	8B	8C	8D	8E	8F
17	4D	06	93	88	30	EF	A4	C8	3B	34	46	DE	A7	36	5C

90	91	92	93	94	95	96	97	98	99	9A	9B	9C	9D	9E	9F
39	8F	66	3D	8E	01	8A	B9	C6	E4	12	B0	05	4A	FC	18

A0	A1	A2	A3	A4	A5	A6	A7	A8	A9	AA	AB	AC	AD	AE	AF
D6	13	A8	90	3E	8B	44	CA	D0	B1	40	15	E0	5A	9A	6D

B0	B1	B2	B3	B4	B5	B6	B7	B8	B9	BA	BB	BC	BD	BE	BF
D2	AB	C4	A9	6E	41	F0	AA	42	AC	19	5B	1E	4F	94	5D

C0	C1	C2	C3	C4	C5	C6	C7	C8	C9	CA	CB	CC	CD	CE	CF
16	8C	FD	5E	95	B5	97	6C	AD	08	BB	AE	96	20	7F	23

D0	D1	D2	D3	D4	D5	D6	D7	D8	D9	DA	DB	DC	DD	DE	DF
D5	43	D1	47	49	02	99	80	D9	60	61	65	70	AF	62	63

E0	E1	E2	E3	E4	E5	E6	E7	E8	E9	EA	EB	EC	ED	EE	EF
9B	DF	03	67	F2	68	69	6F	71	72	D7	73	74	75	76	79

F0	F1	F2	F3	F4	F5	F6	F7	F8	F9	FA	FB	FC	FD	FE	FF
EC	D3	82	E1	7A	ED	DA	83	84	9D	9E	9F	B6	BC	E6	E7

Что известно об открытом тексте? Это военная телеграмма, в которой содержится какой-то приказ. Начало телеграммы – стандартное: «Совершенно секретно. Приказ №», или в шестнадцатиричной записи соответствующих ASCII-символов
D1 EE E2 E5 F0 F8 E5 ED ED EE 20 F1 E5 EA F0 E5 F2 ED EE 2E 20 CF F0 E8 EA E0 E7 20 B9

Приступим к взлому, т.е. к определению неизвестного ключа $x_1,x_2,\ldots x_{16}$, записанного во втором регистре сдвига.

Давайте сначала выпишем уравнения зашифрования, реализуемые этой схемой. Если $(y_1,y_2,\ldots,y_8)$ – блок, записанный в первом регистре сдвига «Ангстрем-3», то за один такт работы схемы он перейдет в блок $(y_2,y_3,\ldots,y_9)$, где $y_9 = p(y_1+y_2+y_8+x_1)$, x_1 – первый байт неизвестного ключа. В общем случае, если последовательность всех заполнений первого регистра сдвига обозначить как $y_1,y_2,\ldots,y_{23},y_{24}$, где $(y_1,y_2,\ldots,y_8)$ – блок открытого текста, $(y_{17},y_{18},\ldots,y_{24})$ – блок шифртекста, то для любого $i^3 9$ будет справедливо:

$$yi = p(y_{i-8}+y_{i-7}+y_{i-1}+x_{i-8})$$

Преобразование блока $(y_i, y_{i+1},\ldots y_{i+7})$ в блок $(y_{i+1},y_{i+2},\ldots,y_{i+8})$ за один такт обозначим как d_{xi}. Очевидно, что это взаимно-однозначное преобразование, поскольку p - подстановка:

$$d_{xi}(y_i, y_{i+1},\ldots y_{i+7}) = (y_{i+1},y_{i+2},\ldots, p(y_i+y_{i+1}+y_{i+7}+x_i))$$

d_{xi} - это подстановка на множестве $Z/2^{64}$. Тогда все преобразование, осуществляемое схемой «Ангстрем-3», будет выглядеть как произведение подстановок:

$$d_{x1,x2,\ldots,x16} = d_{x1}d_{x2}\ldots d_{x16}$$

Рассмотрим преобразование $q(y_1,y_2,\ldots y_8) = (p(y_1), p(y_2),\ldots, p(y_8))$. Заметим, что
$q^{-1}(y_1,y_2,\ldots y_8) = (p^{-1}(y_1), p^{-1}(y_2),\ldots, p^{-1}(y_8))$.
Имеем

$$q^{-1}d_{x1,x2,\ldots,x16}\, q = q^{-1}d_{x1}d_{x2}\ldots d_{x16}\, q = q^{-1}d_{x1}qq^{-1}d_{x2}qq^{-1}\ldots qq^{-1}d_{x16}\, q = j_{x1}j_{x2}\ldots j_{x16} = j_{x1,x2,\ldots x16},$$

где $j_{xi} = q^{-1}d_{xi}q$
Если блок открытого текста $(y_1,y_2,\ldots,y_8)$ переходит в блок шифртекста $(y_{17},y_{18},\ldots,y_{24})$ с помощью преобразования $d_{x1,x2,\ldots,x16}$, т.е.
$d_{x1,x2,\ldots,x16}(y_1,y_2,\ldots,y_8) = (y_{17},y_{18},\ldots,y_{24})$,
то

$$q^{-1}d_{x1,x2,\ldots,x16}(y_1,y_2,\ldots,y_8) = q^{-1}(y_{17},y_{18},\ldots,y_{24}) = (p^{-1}(y_{17}), p^{-1}(y_{18}),\ldots, p^{-1}(y_{24})).$$

Тогда

$$(p^{-1}(y_{17}), p^{-1}(y_{18}),\ldots, p^{-1}(y_{24})) = q^{-1}d_{x1,x2,\ldots,x16}\, qq^{-1}(y_1,y_2,\ldots,y_8) =$$
$$q^{-1}d_{x1,x2,\ldots,x16}q\,(p^{-1}(y_1), p^{-1}(y_2),\ldots, p^{-1}(y_8))$$

Итак, вот она, первая зацепка для анализа «Ангстрем-3»: заменяем позначно все буквы шифрованного и известного открытого текста по подстановке p^{-1} и дальше используем вместо d_{xi} преобразования j_{xi}. А теперь давайте посмотрим на эти преобразования повнимательнее.

$j_{xi}(y_i, y_{i+1},\dots y_{i+7}) = q^{-1}d_{xi}q(y_i, y_{i+1},\dots y_{i+7}) = q^{-1}d_{xi}(p(y_i), p(y_{i+1}),\dots p(y_{i+7})) =$
$q^{-1}(p(y_{i+1}), p(y_{i+2}),\dots,p(p(y_i)+p(y_{i+1})+p(y_{i+7})+x_i) =$
$(y_{i+1}, y_{i+2},\dots, p(y_i)+p(y_{i+1})+p(y_{i+7})+x_i)$

Жизнь прекрасна и удивительна! Какие уравнения получились!

$y_{i+8} = p(y_i)+p(y_{i+1})+p(y_{i+7})+x_i$

Возьмем-ка теперь парочку блоков открытого текста $(y_1,y_2,\dots,y_8)$ $(z_1,z_2,\dots,z_8)$ и соответствующие им блоки шифртекста $(y_{17},y_{18},\dots,y_{24})$ $(z_{17},z_{18},\dots,z_{24})$ и выпишем уравнения одни под другими…

$y_{i+8} = p(y_i)+p(y_{i+1})+p(y_{i+7})+x_i$
$z_{i+8} = p(z_i)+p(z_{i+1})+p(z_{i+7})+x_i$

Это же криптографический Клондайк! Вычитаем одно уравнение из другого и ключ пропадает!

$u_{i+8} = v_i+v_{i+1}+v_{i+7}$ (1)
где $u_i = y_i-z_i$, $v_i = p(y_i)- p(z_i)$.
Из (1) имеем:
$v_i = u_{i+8} -v_{i+1}-v_{i+7}$ (2)
Линейное уравнение – мечта криптографа! Тут только надо найти все такие решения, при которых для каждой пары (u_i,v_i) соответствующий элемент $p_{ui,vi}$ в матрице P(p) был бы ненулевым. Поехали!
При T=16 из (1) и (2) имеем:
$u_1,u_2,\dots u_8$, $v_1,v_2,\dots v_8$ – известны – это открытый текст
$u_{17},u_{18},\dots u_{24}$, $v_{17},v_{18},\dots v_{24}$ – известны – это шифртекст
Из (2) последовательно находим:
$v_{16} = u_{24}-v_{17}-v_{23}$
$v_{15} = u_{23}-v_{16}-v_{22}$
……
$v_9 = u_{17}-v_{10}-v_{16}$

а затем уже из (1) – все u_i. Система (1) полностью решена!

Дальше – раздолье. Ключ опробуем позначно. Для первого байта ключа x_1 оставляем допустимыми только те значения, при которых пара (y_9,z_9) является решением системы
$y_9-z_9 = u_9$
$p(y_9)- p(z_9) = v_9$

Если таких значений будет несколько, то возьмем еще одну пару и истинным будут только те значения, которые содержатся в пересечении этих множеств и так поштучно определяем весь ключ.

Вот теперь пора и почитать, что там наша доблестная армия нашифровала. Военный приказ будем взламывать по-военному четко: делай раз, делай два, делай три.

1. Берем первые 24 знака известного нам открытого текста, соответствующие им знаки шифртекста и составляем две пары переходов из открытого текста в шифрованный.

Открытый текст	Шифртекст
Первая пара	
D1 EE E2 E5 F0 F8 E5 ED	D8 C7 83 EF F9 CA 71 FA
ED EE 20 F1 E5 EA F0 E5	07 55 16 9B 3A 1A 99 53
Вторая пара	
D1 EE E2 E5 F0 F8 E5 ED	D8 C7 83 EF F9 CA 71 FA
F2 ED EE 2E 20 CF F0 E8	87 CC 83 9D FA 1D D6 D8

2. Все байты в этих парах заменяем по подстановке p^{-1}

D2 0B 77 52 B6 31 52 F5	68 6E F7 86 2A A7 E8 3F
F5 0B CD 5D 52 4E B6 52	42 74 C0 E0 19 37 D6 3C

D2 0B 77 52 B6 31 52 F5 68 6E F7 86 2A A7 E8 3F
E4 F5 0B 38 CD 6A B6 35 5E 27 F7 F9 3F 7E A0 68

3. Для каждой из этих двух пар составляем и решаем систему линейных уравнений (1)

Первая пара
Открытый текст

	1	2	3	4	5	6	7	8
u_i	DD	00	AA	F5	64	E3	9C	A3
v_i	E4	00	C2	F4	0B	0E	F5	08

Шифртекст

17	18	19	20	21	22	23	24
26	FA	37	A6	11	70	12	03
D1	72	6D	54	BF	B0	D8	A7

Сначала с помощью уравнений (2) вычисляем промежуточные значения $v_{16},v_{15},\ldots,v_9$
$v_{16} = u_{24} – v_{17} –v_{23} = 03 –D1-D8 = 5A$
$v_{15} = u_{23} – v_{16} –v_{22} = 12 –5A-B0 = 08$
$v_{14} = u_{22} – v_{15} –v_{21} = 70 – 08-BF =A9$
$v_{13} = u_{21} – v_{14} –v_{20} = 11 – A9-54 = 14$
$v_{12} = u_{20} – v_{13} –v_{19} = A6 – 14 -6D = 25$
$v_{11} = u_{19} – v_{12} –v_{18} = 37 – 25 -72 = A0$
$v_{10} = u_{18} – v_{11} –v_{17} = FA – A0 -D1 = 89$
$v_9 = u_{17} – v_{10} –v_{16} = 26 – 89 -5A = 43$

Затем с помощью (1) вычисляем $u_9,u_{10},\ldots,u_{16}$
$u_9 = v_1+v_2+v_8 = E4+00+08 = EC$
$u_{10} = v_2+v_3+v_9 = 00+C2+43 = 05$
$u_{11} = v_3+v_4+v_{10} = C2+F4+89 = 3F$
$u_{12} = v_4+v_5+v_{11} = F4+0B+A0 = 9F$
$u_{13} = v_5+v_6+v_{12} = 0B+0E+25 = 3E$
$u_{14} = v_6+v_7+v_{13} = 0E+F5+14 = 17$
$u_{15} = v_7+v_8+v_{14} = F5+08+A9 = A6$
$u_{16} = v_8+v_9+v_{15} = 08+43+08 = 53$

Таким образом, получилась табличка промежуточных значений

Промежуточные значения для первой пары

9	10	11	12	13	14	15	16
EC	05	3F	9F	3E	17	A6	53
43	89	A0	25	14	A9	08	5A

Теперь проделываем все то же самое для второй пары.

Открытый текст

	1	2	3	4	5	6	7	8
u_i	EE	16	6C	1A	E9	C7	9C	C0
v_i	DF	01	F4	B7	D0	29	F5	05

Промежуточные значения

9	10	11	12	13	14	15	16
E5	B5	85	0C	05	23	1D	07
C0	5F	97	6E	1F	7A	B0	EB

Шифртекст

17	18	19	20	21	22	23	24
0A	47	00	8D	EB	29	48	D7
51	FB	00	52	FF	AD	9B	22

Чуток осталось! Для определения первого знака ключа x_1 надо найти y_9, поскольку $x_1=y_9-p(y_1)- p(y_2)- p(y_8)$, а все значения $y_1,y_2,\ldots,y_8$ – известны. Значение же y_9 находим исходя из следующих условий:
$p(y_9)- p(y_9\text{-EC})= 43$ (для первой пары) и
$p(y_9)- p(y_9\text{-E5})= C0$ (для второй пары)
Честно перебрав все 256 значений, находим: $y_9 = 9B$, тогда
$x_1 = 9B – D1 – EE – ED = EF$
Далее – все аналогично. Для второго знака ключа
$p(y_{10})- p(y_{10}\text{-}05)= 89$ (для первой пары) и
$p(y_{10})- p(y_{10}\text{-}B5)= 5F$ (для второй пары)
откуда $y_{10} = 98$, тогда $x_2 = 98 – EE – E2 – B0 = 18$

Точно таким же путем можно вычислить и все остальные знаки ключа. Небольшое затруднение возникнет лишь при определении x_{11}, поскольку в этом случае система получится такая:
$p(y_{19})- p(y_{19}\text{-}37)= 6D$ (для первой пары) и
$p(y_9)- p(y_9\text{-}00)= 00$ (для второй пары)
Вторая пара здесь ничего не дает, но зато первая отсеяла все отлично, только одно допустимое значение остается: F7.

Вот он, полностью вычисленный ключ к «Ангстрему-3» при T=16:
EF 18 9E C8 7B B9 0F A1 8E BC 71 6F D1 07 94 92
А вот и телеграмма, расшифрованная с его помощью:

Совершенно секретно. Приказ №362 по Дальнему военному округу. Все воины Дальнего военного округа, активно включившись в борьбу за достойную встречу XXV съезда КПСС, принимают на себя повышенные социалистические обязательства. Танкисты и артиллеристы, летчики и ракетчики, мотострелки и инженерные войска стремятся повышать свою боевую и политическую подготовку, быть преданными социалистической Родине и советскому народу. Но, к сожалению, в некоторых подразделениях нашего славного округа еще имеются отдельные случаи несерьезного отношения к такому важнейшему мероприятию, как достойная встреча партийного съезда. Так в 8 отделе технической службы в качестве повышенных социалистических обязательств решили разработать программу выработки простых чисел. В то время, как все бойцы и командиры стараются освоить новую, сложную технику, техническое подразделение ищет легких путей и простых чисел. В 8 отделе длительное время наблюдается снижение воинской дисциплины, многие офицеры этого отдела получили замечания на прошедшем строевом смотре и не сделали из них для себя должных выводов. ПРИКАЗЫВАЮ: 1) 8 отделу технической службы в недельный срок завершить разработку простых чисел и перейти к выработке программы для сложных чисел. 2) Все выработанные к настоящему моменту простые числа считать сложными. 3) Разработчикам простых чисел указать на необходимость повышения воинской дисциплины и выучки в их дальнейшей работе. 4) Приказ объявить во всех подразделениях Дальнего военного округа. Командир ДВО генерал-майор Безверхов.

Была ли такая телеграмма на самом деле – ничего определенного сказать не могу, дальних военных округов в России много, за всеми не уследишь. Но легенда про армейский приказ считать все группы абелевыми очень долго ходила по 4 факультету ВКШ КГБ.

А вообще-то «Ангстрем – 3» при T=16 вполне можно поставлять развивающимся странам в качестве братской бескорыстной помощи.

Назад, к балалайкам?

Глава 6

Там выезд есть из колеи…

Итак, с шифрами на новой элементной базе первый блин получился комом. И что же дальше? Отказаться от той простоты их реализации, которая сразу же бросалась в глаза любому криптографу, знакомому с DES или со старыми советскими шифрами? Создавать различных монстров типа специализированного криптографического процессора, который по стоимости будет сопоставим с танком? Или же напрячься и попытаться довести до криптографического ума «Ангстрем-3»?

«Криптографический танк» в конце концов появился, правда гораздо позже, уже после появления первых персональных компьютеров. Забегая вперед и снимая шляпу перед читателем, который хотя бы бегло просмотрел то, что было написано в предыдущей главе, я хочу рассказать историю появления специализированной компьютерной платы «Криптон».

Что бы ни пыталась производить советская военная промышленность, перешедшая на мирные рельсы, все равно в итоге получались танки («Москвич-412»). Криптография, переведенная на нужды простого народа, произвела советский стандарт шифрования - алгоритм ГОСТ 28147-89, скопированный с американского DES и немного переделанный. Но даже сами американцы (Брюс Шнайер в своей книге «Прикладная криптография») признавали, что DES – не самое лучшее произведение криптографического искусства.

«Никогда до этого оцененный NSA (National Security Agency) алгоритм не был опубликован... NSA считало, что DES будет реализовываться только аппаратно. В стандарте требовалась именно аппаратная реализация… Не для печати NSA охарактеризовало DES как одну из самых больших своих ошибок…»

С появлением первых персональных компьютеров IBM PC XT – 86 появились и первые попытки реализовать с их помощью криптографические процедуры, основанные на ГОСТ 28147-89. Но тут, даже несмотря на те фантастические (по тем временам) возможности, которые открывал перед криптографами персональный компьютер, скорость работы советского стандарта оказалась настолько медленной, что было принято решение создавать специализированную плату для IBM PC, на которой ГОСТ реализовывался бы аппаратно. Так появился советский криптографический танк «Криптон».

Конечно же, с ростом производительности персональных компьютеров менялись взгляды и на возможности реализации с их помощью криптографических алгоритмов. С появлением IBM PC AT – 286 скорость ГОСТа оказалась уже не столь актуальна, но маховик советской промышленности был запущен, Зеленоград начал выпускать «Криптоны», вложены деньги, нужна отдача. Все на танки!

Все это произошло спустя несколько лет после описываемых здесь событий. Те люди, которые были в курсе криптографических баталий в Теоретическом отделе Спецуправления в начале 80-х годов, могли с сожалением констатировать в стиле чудесного Виктора Степановича Черномырдина: «Хотели как лучше, а получилось как всегда».

Но вернемся в 1980-й год. Первый вариант «Ангстрема-3» разломан, но не выброшен на свалку. Ребята из НИИ Автоматики весть о его взломе восприняли даже с энтузиазмом: у них, разработчиков этой схемы, появились достойные оппоненты, с которыми будет интересно иметь дело, устраивать своего рода творческие соревнования на самую оригинальную идею для шифров на новой элементной базе. Закладывался базис, основа для будущих схем, здесь очень важно было не упустить что-то существенное, что исправить в дальнейшем будет очень сложно, но не менее важно было не скатиться до примитивного уровня американского DES, наворотив на схему всяких накруток в ущерб простоте, изяществу и скорости ее реализации.

Ясно, что длины T=16 для обеспечения стойкости схемы явно маловато, ее надо увеличивать. Но насколько? Каждое увеличение – это потеря в скорости шифрования, нужно найти оптимальную границу между безопасностью и эффективностью.

Широко раскинулось поле деятельности для Теоретического отдела, так что здесь я, получив свой честный двадцатник, попал в струю. Вот только за два с лишним года, проведенных в отделе у Степанова, этот полутюремный режим работы с контролером времени прихода и ухода с работы уже порядком надоел.

Сейчас здесь, в Корее, у меня уже есть возможность сравнивать. Однажды корейцы свозили меня в научно-исследовательский центр в городке Дей-Джоне. Нечто вроде небольшого коттеджного поселка в горах, ухожен так, что хоть картины пиши. Хочешь – сходи в горы, подумай там в одиночестве о своих проблемах, хочешь – отвлекись, посмотри на цветных декоративных рыбок, весело плавающих в пруду. Вид из окон – очаровывающе красив, величественные горы, слегка тронутые цивилизацией в виде линий электропередач, лес, декоративные деревья, все цветет и благоухает, корейцы неторопливо что-то обсуждают, сидя под ними.

5 отдел Спецуправления 8 ГУ КГБ СССР, 1981 год. Тюремное 3-этажное здание из красного кирпича, забор, обнесенный колючей проволокой, контрольно-следовая полоса, солдаты с автоматами. Вид из окна – на этот тюремный двор, в нем гараж, в котором стоят машины службы радиоперехвата. Около машин – солдаты-срочники, всем своим видом показывающие, сколько им осталось до дембеля. Сколько раз я ловил себя на мысли, что эта гнетущая обстановка часто просто парализует всякое желание нетрадиционно мыслить, искать новые решения. А просиживать там надо было строго с 9 до 6. Утром в 9 – обход контролера, не дай бог опоздать на 5 минут, хотя потом часа два можно вообще ничего не

делать или дружно ловить всей комнатой залетевшую осу. Постоянная суета, не имеющая ничего общего с криптографией, сплетни, продовольственные заказы, общественная работа – все, все это легко затягивает в колею, из которой не выбраться до самой пенсии. Энтузиазм проходит, на его месте появляется будничная рутина, год, два – и нет специалиста, полностью втянулся в эти типичные в те времена «правила игры», стал сереньким чиновником. Не высовывайся, не перечь начальству, не проявляй инициативы, будь как все – и получишь тихую, спокойную жизнь на много лет вперед.

Правила игры простые: не замечай несоответствия между словом и делом, не пытайся найти рациональное объяснение вещам заведомо иррациональным, почти мистическим. Ну зачем теоретикам нужен такой строгий режим присутствия в этом здании? Не является ли ежедневный обход контролера в 9.00 унизительным? Что важнее: результаты или присутствие на рабочем месте? А как влияют результаты работы на твое материальное благосостояние?

Не задавай ни себе, ни другим этих и многих подобных вопросов, ответа все равно не получишь. Так завелось еще с давних времен, времен Вождя Всех Народов. Закрытые системы, подобные шифровальной службе, легче перенесли все бушевавшие затем страсти, волнение улеглось, лозунги и названия поменялись, а порядки и «правила игры» во многом восстановились.

И что, в такой ситуации губить все лучшие молодые годы жизни, чтобы к 30 годам стать законченным старым ворчуном, отсчитывающим дни до пенсии? Всю жизнь торчать в этом тюремном здании, натужно досиживать там каждый день до 6 вечера заведомо зная, что от этих посиделок нет ни малейшей пользы, только вред?

Самый реальный выход из этой колеи – очная аспирантура при том же 4 факультете ВКШ КГБ. Теоретический отдел, кому как не теоретикам поставлять туда аспирантов-очников. А тут как раз завязалась эта эпопея с шифрами на новой элементной базе, там можно будет все основательно обдумать, взвесить и выдать какие-то разумные предложения. А самое главное – сменить эту ненавистную обстановку, эти высиживания до 6, этот тюремный двор с колючей проволокой.

Степанов косо посмотрел на меня, когда я заявил ему о своем желании поступать в очную аспирантуру.

- Ну Вы еще молодой, у Вас все впереди. У нас сейчас напряженные планы, Вы поработайте еще годик-другой, сдайте экзамены кандидатского минимума, создайте хороший задел для своей диссертации, а там посмотрим.

В отдел пришла разнарядка: выделить одного человека в очную аспирантуру. Очередные претенденты на нее отказались, поскольку учеба в аспирантуре на три года «замораживала» карьерный рост в 5 отделе. Степанов уже собирался отрапортовать, что желающих нет, когда я, по совету своих боевых товарищей, так нахально перечеркнул проповедуемый им «патриотизм к отделу».

- Вадим Евдокимович, у нас каждый год напряженные планы. А очная аспирантура для того и создана, чтобы человек мог, обучаясь в ней, сдать экзамены кандидатского минимума и написать диссертацию.

Степанов действовал в этом случае как прагматичный начальник. Ему нужен уход из отдела на три года молодого, перспективного сотрудника? Конечно, нет! Он – хозяин отдела, сотрудники – это его рабочая сила. Всеми способами надо постараться эту рабочую силу удерживать, не раздавать просто так направо-налево. Хотя здесь разнарядка была спущена сверху, из Главка, но ее, если бы не нашлось желающих, можно было тихо спустить на тормозах: напряженные планы, найдем человека в аспирантуру попозже, в другой раз. А тут молодой, два с небольшим года проработавший птенец все это ломает!

- В аспирантуре у Вас не будет возможности для служебного роста. Да и диссертацию за три года, я думаю, Вам защитить не удастся.

Этим словам я тогда, по молодости, не придал особого значения. Да, действительно, за три года очной аспирантуры редко кому удавалось защититься. Люди возвращались обратно в отдел и Степанов явно или неявно как бы укорял их: «Ну что, сынку, помогла тебе твоя очная аспирантура?» Для того, чтобы понравиться Степанову, надо было быть «патриотом» отдела, не воротить нос на сторону, на предложения об очной аспирантуре гневно отвечать: «Мне дорог мой отдел, я лучше буду обучаться заочно».

Но ребята, прошедшие очную аспирантуру, дружно говорили: «Плюнь ты на то, что там говорит Степанов. Это три года свободной жизни!»

Степанов был очень умным человеком, блестящим математиком. Но это был начальник, любивший крепостные порядки, сталинскую машину и винтики. Он не любил, когда люди поступали вопреки его мнению. И мне, к сожалению, еще пришлось испытать это на собственной шкуре.

Но это позже. А пока – успешно сданы вступительные экзамены в аспирантуру, впереди – новая жизнь, встреча со старым знакомым – 4 факультетом ВКШ КГБ, но уже в ином качестве. Прочь из этой колеи!

Пятилетка пышных похорон

4 факультет изменился. Те энтузиасты-идеалисты, которые закладывали его основу в начале 60-х годов, уже состарились и отошли от дел. Зато больше стало «хороших военных», чем-то похожих на наше Чудо. После переезда на МУЦ тихая и уютная обстановка, подчеркивающая обособленность и уникальную специфику криптографов, сменилась на тривиальную мишуру и иногда откровенную глупость. Боцман запросто мог выставить в находящейся по соседству Олимпийской деревне духовой оркестр и под его бравурную музыку, слышную аж у метро «Юго-Западная», устроить всеобщий лыжный кросс: смотрите, вот они, бойцы невидимого фронта. Старались не отставать от него и в изобилии появившиеся бог ведает откуда начальники и начальнички 4 факультета, не обремененные знаниями математики, но рьяно бросившиеся выполнять указание генерала готовить в первую очередь хороших военных. Наглядная агитация, социалистическое соревнование, пускание пыли в глаза другим подобным, но еще более надутым начальникам, которые теперь всегда рядом, - вот что стало важнее всего. Посещение Высшей школы каким-нибудь зампредом КГБ превращалось во всеобщее стихийное бедствие: а вдруг глянет как-нибудь косо или замечание сделает! И вот чуть ли не за месяц начинается подготовка к показухе, которая в криптографии противопоказана как нигде еще. На всех этажах у лифтов выставляется по офицеру, чтобы высокий гость не утруждал себя нажатием кнопки, начальники кафедр заучивают и репетируют свои роли, а сам генерал-начальник факультета с раннего утра, часа за 4 до возможного приезда вельможного барина, как дворецкий торчит у входа на факультет. Но барин туда даже не заглянул, ему до этих яйцеголовых нет абсолютно никакого дела, побыстрее бы закончить с нудной официальной процедурой - и в генеральскую столовую, к коньячку поближе. Изобильно откушав, идет этот большой начальник по холлу Высшей Школы КГБ, а его холоп, начальник этой школы, тоже генерал, упоенно рассказывает, как молодые ребята, выпускники «истинно» чекистских факультетов, свои головы в Афганистане кладут. «Мы своих слушателей готовим к подвигу!» - исторгая коньячные пары, визжит это homo soveticus.

Рождались сомнения.

Образцом для подражания у нашего генерала всегда было Орловское военное училище связи, где курсанты строем и с песнями бодро маршировали в столовую и все делали только по команде. Вот она, генеральская цель! Все математики построены на плацу в ровные шеренги, форма вычищена и выглажена, сапоги блестят как зеркало. И вот он появляется перед строем в генеральской форме, все взгляды – только на него, на его лампасы.

- Здравствуйте товарищи!
- Здравия желаем, товарищ генерал!

Он обходит строй, а подчиненные гложут его своими математическими взглядами. И воцаряются на 4 факультете настоящие офицеры…

- Ты представляешь себе нашего генерала без формы? Типичный слесарь-водопроводчик. Вот поэтому он сам всегда ходит в военной форме и всех уже достал здесь своими порядками.

Преподаватели с кафедр математики и криптографии – в большинстве выпускники 4 факультета. Строгие генеральские приказы давно уже считают «мобилизующими» со всеми вытекающими из этого практическими выводами. Хоть и плодятся новые начальники, как кролики, но университетский дух 4 факультета еще не удалось полностью истребить. Еще теплится!

Глава 1

…на все время праздников

- Что будет, когда умрет Брежнев?
- Ему будет малая земля, а нам всем возрождение.

Это случилось неожиданно. Но внутренне ждали: законы природы – едины для всех, их не обманешь. Можно сколько угодно пытаться обманывать свой народ беззастенчивой ложью про коммунизм, развитой социализм, но все это в конечном итоге вырождается в фарс и глухое презрение к власти.

- Где проходит граница между коммунизмом и развитым социализмом?

- По Кремлевской стене.
- А где между развитым и простым социализмом?
- По московской кольцевой автодороге.

Застой страшен своей безысходностью, безразличием, духовным опустошением, осознанием, что живешь напрасно, жизнь проходит впустую, а сделать ничего невозможно. Как ни работай, а твое благосостояние от этого не зависит. А какой тогда смысл работать?

Все газеты, телевидение, радио каждый день только и твердят: товарищ Леонид Ильич Брежнев направил приветственную телеграмму строителям Атоммаша, шахтерам Кузбасса, хлопкоробам Узбекистана, земледельцам Украины… Да что же это за стиль управления огромной страной, когда весь пар в гудок идет! От телевизора тошно, а пойдешь в магазин – зверинец. Толстые тетки-продавцы неспешно режут и фасуют колбасу, а огромная очередь уже вожделенно взирает на нее. И вот настал момент: тетка с тележкой подкатывается к прилавку и выбрасывает, самым натуральным образом выбрасывает пакетики с колбасой в толпу. Ажиотаж, давка, крики, все норовят ухватить кусок получше. А тетка довольна: посмотрела бесплатный спектакль, лишний раз осознала себя важным человеком, властителем этой очереди из очкастых интеллигентов, которых еще великий вождь называл словом на букву г.

Унижение, постоянное унижение испытывало огромное множество людей от всего этого дефицита, наглых продавщиц и очередей. Достать, урвать, поймать момент, когда выкинут товар, записаться, бегать отмечаться, получить по блату – вот каждодневное бытие большинства простых советских людей того времени. При огромных природных богатствах людям доставалась от них, как от бублика, одна дырка.

Пропаганда всегда старалась уходить от прямых ответов, создавать наукообразие на ровном месте. Находилась масса причин, временных трудностей, виновными оказывались агрессивные империалисты, война, закончившаяся более 30 лет назад, погода, пережитки прошлого, кто и что угодно, но только не руководство страны, которое твердо и последовательно вело борьбу за мир во всем мире. Но пропаганда работала практически впустую, все давно уже поняли, что это лишь цветная обертка, в которую завернут прогнивший и протухший товар.

Не можешь управлять страной – уйди. В отставку, на пенсию, на дачу, к детям и внукам, пиши мемуары, доживай спокойно свой век, тогда ты заслужишь большего уважения. Каждодневное мелькание и упоминание престарелого вождя, с трудом шевелящего языком, порождало только насмешки и анекдоты, опускавшие его авторитет ниже нулевой отметки.

- Все во имя человека, все для блага человека!
- Чукча видел этого человека!

Его смерть народ не воспринял как конец света, как когда-то восприняли смерть Сталина. Скорее было ощущение неизбежности перемен. В Высшей Краснознаменной Школе КГБ (успевшей к тому времени получить орден Октябрьской революции, и ставшей по этому поводу рычащей ВООРКШ КГБ) по традиции была объявлена повышенная готовность (к чему?), обязательное присутствие всех (включая аспирантов) на своих рабочих местах, ожидание чего-то такого, о чем никто ничего толком не знал.

- И такой режим сохранится на все время праздников!

Такую бессмертную оговорку-афоризм выдал один из начальников 4 факультета, разъясняя текущий момент.

Молодые аспиранты, вынужденные целыми днями торчать без дела в аспирантской комнатушке, естественно живо принялись обсуждать то, что происходит в стране и что будет дальше. Быстренько был выведен коммуно-биологический «закон 29 лет», по которому все коммунистические перемены совершаются раз в 29 лет после смерти очередного вождя.

1895 год. Умер Энгельс. Коммунизм зачем-то пожаловал из Европы в Россию.
1924 год. Умер Ленин. Коммунизм стал усатым.
1953 год. Умер Сталин. Коммунизм побрился наголо.
1982 год. Умер Брежнев. Коммунизм не умер.
2011 год. ???

Были извлечены на свет божий Хрущевские речи, ибо, как научила нас марксистско-ленинская философия, развитие происходит по спирали, а потому скоро начнут поминать Ильича-2 нехорошими словами. В этом не было сомнений. Все споры, как и должно быть у математиков, углубились в детали: через сколько лет это начнется, какими именно нехорошими словами, кто скажет первое слово. Дверь отворилась и к нам в комнату заглянул Сан Саныч, правда не тот, с которым мы уже встречались в этой книге, а другой, с кафедры криптографии.

- Товарищи, в вашей стенгазете есть одна маленькая ошибка. Посмотрите, пожалуйста, повнимательнее и исправьте ее.

Ошибка была быстро обнаружена и исправлена. Слова «как отмечал Л.И.Брежнев» были замазаны белой замазкой, а на их месте, от руки, было коряво нацарапано: «на XXVI съезде отмечалось». Сам Сан Саныч исправил ошибку чуть покрупнее: содержание большого стенда, посвященного 75-летию Брежнева, было заменено на серию статей из «Комсомольской правды» под общим названием «Таежный тупик».

На смену Брежневу без шума и пыли пришел Юрий Владимирович Андропов, бывший председатель КГБ. Популярности у него было, пожалуй, побольше, чем у Брежнева: не особо часто нес всякую ахинею с высоких трибун, был поскромнее, не увешивал себя орденами, как новогоднюю елку. КГБшные начальники засияли, а с рядовыми сотрудниками провели воспитательные беседы на тему: «юноше, обдумывающему житье, делать жизнь с кого….» Провели и провели, отметились в отчете о воспитательной работе, успокоились и забыли. Все вернулось на круги своя, жизнь продолжалась.

Глава 2

Каждый чекист - коммунист

Если раньше, в период моей учебы в качестве слушателя 4 факультета, основными единицами измерения нашей жизни были «учебная группа» и «начальник курса», то теперь, попав почти через три года после окончания факультета на него снова в качестве аспиранта, я одновременно попал в иное измерение, где основными понятиями были уже «кафедра» и «инспектор отдела аспирантуры». Вот тут самое время познакомить читателя с этими изначальными, иногда математическими, а иногда и нет, понятиями.

На 4 факультете было несколько профильных кафедр, из которых наиболее видное и значимое место занимали кафедра математики и кафедра криптографии. Впоследствии к этим двум лидерам примкнула еще кафедра вычислительной техники, но это все же произошло несколько позже, а тогда, в середине 80-х годов, соотношение было именно таким. Очень многие преподаватели с этих кафедр сами в прошлом окончили 4 факультет и насквозь пропитались теми традициями, которые были заложены его основателями, поэтому мое появление в качестве аспиранта кафедры криптографии не было для меня какой-то резкой сменой обстановки: многие знакомые лица, бывшие сокурсники – теперь уже аспиранты. На кафедре криптографии было около 10 аспирантов-очников, каждое ведомство: 8 ГУ, 16 управление КГБ, Министерство обороны – каждый год направляло в среднем по одному человеку на учебу в трехгодичную очную аспирантуру, а кафедра математики старалась отбирать себе аспирантов из наиболее способных слушателей, заканчивающих факультет. Аспиранты этих двух кафедр составляли, как правило, свободолюбивое сообщество, жившее по университетским традициям, не всегда совпадавшими с распоряжениями начальника той или иной кафедры, к примеру, с распоряжением отмечаться каждый день в специальном журнале прихода и ухода, или с распоряжением ходить в военной форме. Практически у всех аспирантов кафедры криптографии военная форма (облегченный вариант) висела на вешалке в аспирантской комнате и в редкие присутственные дни там же происходило переодевание, ибо желающих разгуливать в военной форме по городу практически не было.

У аспирантов теоретически было два начальства: руководство кафедры и руководство специального отдела аспирантуры, которому должны были подчиняться вообще все аспиранты Высшей школы КГБ, в которую в те времена 4 факультет, еще не добившийся тогда независимости, входил на правах «союзной республики». Но поскольку 4 факультет составлял все же сравнительно небольшую часть всей Высшей школы, то и отдел аспирантуры интересовался аспирантами-математиками «сквозь пальцы», ограничивая, как правило, свое влияние тем, что мы должны были раз в месяц посещать проводимое им общее собрание аспирантов Высшей школы, да присутствием на 4 факультете специального инспектора отдела аспирантуры. Но этот человек сильно отличался от прежнего, знакомого уже читателю, нашего бывшего начальника курса Чуды тем, что до мозга костей был бюрократом, которого не интересовало ничего, кроме выполнения индивидуального плана работы аспиранта-очника. Тут уже не было таких красочных афоризмов, такого страстного желания сделать невозможное – из математиков - хороших военных, одна лишь скучная повседневность:

- Сколько процентов диссертации у Вас готово?

Так что такой начальник справедливо считался аспирантами, прошедшими чудесную школу, несерьезным, а руководству кафедры всегда была готова отмазка: «Мы подчиняемся распорядку, установленному отделом аспирантуры». Вот она, долгожданная свобода!

Но аспиранты по-прежнему оставались военнослужащими, офицерами и получали соответствующее денежное довольствие. Аспирантура называлась целевая, на практике это означало, что то подразделение, которое направило офицера в очную аспирантуру, сохраняло за ним все денежное довольствие – оклады по должности и званию, ежегодную компенсацию за неиспользованную военную форму, тринадцатую зарплату, компенсацию за продовольственные пайки и может быть даже что-то еще, что сейчас, по истечении 20 лет с того времени, я уже мог и подзабыть. Все вместе аспирантское денежное довольствие получалось по тем советским временам достаточно приличным: где-то около 300 рублей в месяц, при этом появлялась масса свободного времени, фактически не было ежедневного обязательного отбывания в аспирантуре, все офицерские мероприятия вроде суточных нарядов и партийных собраний были разовыми и казались не слишком обременительными. Про партийные собрания, да и вообще про партийную жизнь в специфических условиях КГБ, стоит, пожалуй, сказать несколько слов подробнее.

По определению, данному кем-то из революционных вождей, все офицеры КГБ должны были быть коммунистами. Офицер КГБ, достигавший предельного комсомольского возраста, чуть ли не автоматом принимался в КПСС, случаи отказа означали почти что измену Родине и, поэтому, на практике были только в очень экзотических ситуациях. По крайней мере. в 8 ГУ и в Высшей школе КГБ таких ситуаций (беспартийный офицер) я сейчас вспомнить не могу. Какой в этом был смысл? По-видимому, дополнительный рычаг влияния на человека. Любое движение по службе, защита диссертации, оформление в загранкомандировку и всякое иное действие офицера всегда сопровождались написанием служебно-партийной характеристики, в которой непременно должна была присутствовать фраза: «Делу Коммунистической Партии и социалистической Родине предан». Эта фраза была одним из многочисленных социалистических обрядов, которым, по большому счету, мало кто придавал значение, но в конечном итоге смысл был один: без положительной служебно-партийной характеристики в КГБ работать нельзя. Но, помимо обрядов, для чего еще нужна была партийная организация, например, в Теоретическом отделе Спецуправления? Тут я постараюсь привести на этот счет свои «заметки фенолога», хотя этот вопрос также иногда дискутировался между любителями дискуссий и споров, но, правда, в те времена не особо шибко.

Во-первых, в любом научном, да и не только научном, коллективе всегда есть какие-то конфликтующие группы, непримиримые оппоненты, вечно всем недовольные, просто любители поговорить. Обычно выяснением отношений занимаются в курилках, в каких-то изолированных местах, по дороге на работу и с работы, иногда даже в выходные дни, особенно если на эти дни выпадает субботник или воскресник. Но это все – товарищеские игры, неофициальные выступления, тренировочные матчи. Партийное собрание – это официальный чемпионат отдела, со своей турнирной таблицей - протоколами партийных собраний, регулярно подшиваемыми в специальное дело. Не всякий прием, отрабатываемый в тренировочных матчах, может затем быть с успехом использован в официальных встречах, но общий показатель настроений в умах сотрудников Теоретического отдела Спецуправления протоколы партийных собраний отражали достаточно верно. А судейская коллегия – руководство отдела, отдел кадров – затем всегда могла выставить свои, финальные оценки и назвать имена победителей и проигравших.

Во-вторых, над руководством отдела стоит руководство Спецуправления, которому, в свою очередь, нужно оценивать руководителей отделов и для такой оценки есть очень простой и понятный критерий – количество «черных шаров», поданных против начальника отдела на закрытых выборах в партбюро. Здесь несколько слов для современных читателей о том, что такое партбюро. Все сотрудники отдела, достигшие (или даже еще не достигшие, но очень шустрые) предельного комсомольского возраста – 28 лет, были коммунистами. А коммунисты, согласно Уставу КПСС, образовывали на каждом предприятии первичную партийную организацию, которая обязательно раз в месяц проводила партийное собрание, а раз в год выбирала тайным голосованием партбюро – наиболее достойных коммунистов, которые затем руководили всей партийной работой в течение года. Что такое партийная работа? Это, в первую очередь, подготовка месячных партийных собраний (чтобы дискуссия на них велась в рамках заданной темы и в пределах партийных приличий), а также составление многочисленных планов и отчетов, направляемых в вышестоящие партийные инстанции. Во-вторых, это сбор партийных взносов, превращавшийся в стихийное бедствие для сотрудников, сидящих в одной комнате с осуществлявшим этот сбор секретарем партбюро. В Теоретическом отделе Спецуправления к партийной работе неизбежно примыкали различные криптографические дискуссии, выносимые затем на очередное партсобрание, поэтому начальник отдела по определению должен был состоять в партбюро.

При социализме всенародные выборы депутатов были безальтернативными, за кандидатов нерушимого блока коммунистов и беспартийных всегда голосовало 99,99% избирателей (марксистско-ленинская философия учит, что развитие происходит по спирали, все повторяется, но на более высоком уровне). Однако выборы в партийное бюро Теоретического отдела Спецуправления хоть и были всегда безальтернативными, но «черных шаров» Степанову на них кидали достаточно. Начальник отдела – это арбитр в различных внутриотдельских спорах, если все 100% сотрудников им довольны, то это означает одно – он не имеет собственной точки зрения и соглашается со всеми. Но если количество «черных шаров» приближается к 25%, то это означает, что авторитаризм начальника перевалил через опасную черту. Вот на таких простых и понятных критериях строилась вертикаль власти в Спецуправлении, да и, наверное, во всем КГБ. А партийная организация играла в этом случае роли «измерительного прибора».

Ну и, наконец, третья, но по значимости едва ли не основная роль партийной организации – устрашающая. Любой проступок офицера всегда приводил к разбору его персонального дела на партбюро или партсобрании. Правда, в Теоретическом отделе народ был слишком интеллигентный и до задержания милицией в пьяном виде дело обычно не доходило. А вот на 4 факультете и коммунистов было поболее, и «истинных» начальников хватало, и закалка у них была покрепче, рабоче-крестьянская, так что там уж бывало и ловили по пьянке, и аморальное поведение встречалось, и даже совершалось самое большое преступление – потеря офицерского удостоверения. Вот тут-то уж и разворачивалась вовсю работа партийной организации.

У меня, да и, наверное, у любого другого нормального человека, партийные собрания, если на них не было каких-то экзотических подробностей, вызывали скуку и сон. Но, к счастью, в период моего первого пребывания в отделе Степанова, я еще не дорос до партийного уровня и ходил в комсомольских штанишках - там тоже были собрания, но покороче и поспокойнее. Однако перспектива защиты диссертации и дальнейшего служебного роста привели меня в партийные ряды по категории «шустрый», т.е. чуть раньше положенных 28 лет.

Вступление в партию очень красочно описал Михаил Шолохов в «Поднятой целине», мне тут посоперничать с признанным мастером социалистического реализма явно не удастся. Одно утешает – здесь у нас как бы разные весовые категории. Он описывал вступление в тяжеловесную ВКП(б) времен тридцатых годов, мое же вступление – в легкую весовую категорию КПСС середины 80-х, да и герой Шолохова был абстрактный, комплексное число с ненулевой мнимой частью, а мои воспоминания – самые что ни на есть действительные, я бы даже сказал рациональные значения.

Итак, вступление в КПСС начинается с заявления и рекомендаций, причем все это добро надо написать обязательно перьевой ручкой с фиолетовыми чернилами. Партийная загадка: почему именно фиолетовыми, а не синими, которые более распространены? Нет рационального ответа, по умолчанию предполагаем, что фиолетовые чернила дольше сохраняются в партийных архивах для потомков из третьего тысячелетия, поэтому поиск фиолетовых чернил в советских канцелярских магазинах можно считать первым партийным поручением. Выполнено.

Далее. Текст заявления. Подавляя голос внутреннего разума, приходится писать: «Прошу принять меня в члены КПСС. Хочу быть в первых рядах строителей коммунизма. Устав и Программу КПСС признаю и обязуюсь выполнять». Хорошее это дело – первые ряды строителей коммунизма. Только в соответствии с признаваемой мною Программой КПСС коммунизм должен был быть построен еще 1980 году, а я датирую свое заявление 1983 годом. Три года уже живем при коммунизме? А как выполнять такую Программу? И что делают первые ряды строителей того, что уже построено? Наверное, как и на любой советской стройке – сдали объект, а потом еще три года устраняют недоделки. Но это такие всеобщие партийные игры, видишь черное – пиши белое, иначе не видать защиты диссертации. Да бог с ним, с этим коммунизмом, пусть себе будет, как в сказке про Илью Муромца, уже тридцать лет и три года. Когда эту Программу КПСС принимали, я даже в детский садик еще не ходил и кукурузу за полярным кругом не сеял, нет моей вины в том, что теперь, 22 года спустя, надо писать фиолетовыми чернилами, что признаешь и обязуешься выполнять разные глупости.

Ну а Устав КПСС, продекларированные в нем демократический централизм (современное название – властная вертикаль) и выборность снизу доверху (или сверху донизу, сейчас уже не упомнишь, вроде все-таки снизу, хотя по жизни чаще сверху), все это запоминать? Хороший человек был Костя Максимов, веселый, компанейский, а один абзац из Устава еще можно запомнить.

- Костя, задай мне вопросик по Уставу на партсобрании.
- Какой?
- А вот, про демократический централизм.

Вот так проходила моя подготовка к вступлению в КПСС. Заявление фиолетовыми чернилами, трое рекомендующих меня преподавателей с кафедры криптографии, Костин нужный вопросик в нужное время - и за принятие меня в ряды КПСС партийное собрание 4 факультета Высшей Ордена Октябрьской Революции Краснознаменной школы КГБ СССР им. Ф.Э.Дзержинского проголосовало единогласно.

От всей дальнейшей партийной жизни на 4 факультете осталось одно воспоминание: аудитория, в которой проходили факультетские партийные собрания. К тому времени факультет расширился, очень бурно развивались кафедры, связанные с вычислительной техникой, народу на факультете заметно прибавилось по сравнению с временами Большого Кисельного. Поэтому на факультетском партсобрании в аудиторию, рассчитанную человек на 100, надо было вместить несколько большее количество коммунистов. Какая же это оказалась удача!

Дело в том, что эта аудитория была наклонным залом, идущим с нижнего этажа на верхний. Внизу был основной вход, дальше – боковые лестницы, ведущие к верхним рядам, а на самом верху – дверь, являвшаяся запасным выходом. Во время партсобраний зал переполнялся и открывали верхнюю запасную дверь, через которую не успевшие занять основных мест тащили себе из других аудиторий стулья, чтобы

сидеть на них в проходах. Математическая мысль аспирантов, просидевших пару раз в этой толчее и духоте несколько часов, живо нашла оптимальное криптографическое решение.

Главное в нем было – прийти в нужное время, когда зал уже полон и надо идти за стульями. Отметившись у секретаря о своем присутствии, взгляды аспирантов тоскливо пробегали по переполненному залу и с изображением тяжкой необходимости на лице, но ликующие в душе, мы поднимались на самый верх и отправлялись на поиски дополнительных сидячих мест. Здесь тоже не нужно спешить, партсобрание – не волк, в лес не убежит, к моменту возвращения со стульями в руках забитыми оказывались и все проходы на лестнице. Оставалось (какая жалость!) сесть на принесенные стулья уже около запасной двери, но с другой ее стороны, и не с той, где зал с партсобранием. Но душой мы оставались с коммунистами факультета, с их партийной бескомпромиссностью и пламенным энтузиазмом. Иногда даже аплодировали, чтобы зал, если и не видел, то хотя бы слышал, что и за запасным выходом идет партийная жизнь. Когда же большая часть зала засыпала или просто одуревала от духоты и пустых речей, аспиранты тихонечко покидали свою обособленную галерку.

Это был 1984 год, период правления Черненко. Партия и партийные функционеры доживали свои последние золотые денечки.

Глава 3

Логарифмические подстановки

В этой главе давайте отложим в сторону лирические и понятные всем отступления про обстановку в стране в то время. Мои рассуждения об этом субъективны, кто-то может соглашаться с ними, кто-то, наоборот, считать те времена образцом для подражания на фоне современной криминализации страны. В этой книге я старался следовать криптографически-философскому принципу Шеннона: в шифре чередовать не похожие друг на друга операции перемешивания и сдвига. В качестве операций сдвига – главы, отображающие общую ситуацию в СССР и в КГБ в те, теперь уже далекие времена, а в роли перемешивания выступают главы, в которых много говорится о математике, криптографии или программировании. Сейчас начнется очередная «перемешивающая» глава.

Шифратор «Ангстрем-3» был построен в полном соответствии с этим принципом Шеннона: регистр сдвига над Z/256 (операции сдвига), усложненный подстановкой из S_{256}, типичным перемешивающим преобразованием. Перемешивающее преобразование дает столь необходимое в криптографии размножение различий в блоках открытого текста. В общефилософских книгах по криптографии, типа упоминавшейся выше книги Брюса Шнайера «Прикладная криптография», употребляется даже термин «лавинный эффект». Вот соответствующая цитата оттуда.
«… Это называется лавинным эффектом. DES спроектирован так, чтобы как можно быстрее добиться зависимости каждого бита шифртекста от каждого бита открытого текста и каждого бита ключа.»

Насколько я представляю себе DES, нигде, ни в одной книге, не было дано точных математических оценок этого «лавинного эффекта». DES так спроектирован и все. А почему он так спроектирован? Остается лишь догадываться, да строить статистические эксперименты, которые подтверждают: да «лавинный эффект» безусловно есть.

Вся прелесть «Ангстрема-3» в том, что в нем для оценки подобного «лавинного эффекта» на 4 факультете и в Спецуправлении еще в конце 70-х годов был разработан строгий математический аппарат, опирающийся на алгебру, на теорию групп, колец и полей. Об этих результатах я уже упоминал в предыдущей главе, посвященной шифрам на новой элементной базе, вот, вкратце, их суть.

1. В шифрах, использующих операции в кольце Z/256 и подстановки p из S_{256}, лавинный эффект определяется матрицей частот встречаемости разностей переходов ненулевых биграмм P(p) размера 255x255.
2. Лавинный эффект будет тем лучше, чем меньше нулей в этой матрице. Хорошими следует считать такие подстановки, матрицы которых, возведенные в квадрат, не содержат нулей.
3. При случайном и равновероятном выборе подстановки из всей симметрической группы S_{256}, общее количество подстановок в которой составляет огромную величину 256! – произведение всех чисел от 1 до 256, вероятность выбрать хорошую подстановку стремится к 1.
4. Существуют примеры самых плохих подстановок, это линейные подстановки.
5. Теоретически подсчитано минимально возможное количество нулей в матрице P(p).

Вопрос же о том, существуют ли подстановки с минимально возможным числом нулей в матрице P(p), оставался открытым до конца 1983 года.

*****

- Работайте дома. Если Вы будете часто здесь появляться, то диссертации не напишите.

Так напутствовал меня мой научный руководитель Б.А., который сам заканчивал 4 факультет в числе первых его выпускников, а сейчас уже защитил докторскую диссертацию и жил в мире групп, колец и полей. Это был бальзам на мою душу! Нет этого бессмысленного высиживания до 6 часов вечера, пустых разговоров ни о чем, нет смертельно опасной столовой-травиловки. Мысли раскрепощены, нет интеллектуального насилия, все проблемы, казавшиеся неразрешимыми, вдруг как-то сами стали успешно разрешаться. А что за проблемы?

Итак, мои творческие планы связаны с шифрами на новой элементной базе. Это новая тема и непаханое поле для деятельности. Основное отличие этих шифров от традиционных балалаек – наличие в них подстановки (или даже нескольких подстановок) из S_{256}. Эти подстановки определяют криптографические качества шифров, они же дают возможность строить очень простые и высокоскоростные схемы, поэтому фундаментальные исследования шифров на новой элементной базе нужно начинать с изучения подстановок. Нужно постараться получить наиболее полную картину их свойств, ответить на типовые вопросы, например:

- какие подстановки считать приемлемыми, а какие неприемлемыми для использования в шифрах на новой элементной базе и почему;
- как описать какие-то особенные классы подстановок и в чем будет их особенность;
- как лучше использовать подстановку в схеме, где ее целесообразнее расположить и почему;

И, наконец, надо попробовать дать ответ на конкретный практический вопрос: а что же делать со схемой «Ангстрем-3»? Как ее модернизировать, чтобы, сохранив простоту и высокую скорость реализации, обеспечить гарантированную стойкость?

Когда я поведал о своих замыслах Б.А., он сразу же стал пытаться приделывать к подстановкам теорию групп. Он витал в групповых облаках, а моей задачей было приземлять его фантазии на грешную подстановочную землю. И, в общем, такой дуэт оказался достаточно успешным.

Для начала мы попытались описать какой-нибудь класс подстановок p, для которого было бы гарантировано, что показатель 2-транзитивности множества Gp минимален и равен 3. Я надеюсь, что читатель припоминает упоминавшуюся ранее в этой книге матрицу частот встречаемости разностей переходов ненулевых биграмм P(p) и условие достижения 2-транзитивности за 3 шага: эта матрица, возведенная в квадрат, не должна содержать нулей. Я пытался описать класс подстановок, у которых полностью ненулевые средние строка и столбец, наличие такого «креста» дает гарантию того, что квадрат матрицы будет полностью положительным, без нулей. Б.А. сразу же стал пытаться найти и пристроить к этой ситуации какие-то аналогии из известных ему экзотических групп. Несколько попыток оказались безрезультатными и моей задачей было обоснование того, что этот класс групп совсем непригоден. Своего рода тотальное опробование всех подстановок, каким-то пусть даже косвенным образом связанных с изначальными. Б.А., как умудренный опытом рыболов, выискивал места, где могли водиться хорошие подстановки, а я закидывал в этих местах свою блесну.

И вот однажды клюнула такая подстановка, о которой даже сейчас, спустя 20 лет, я вспоминаю с нескрываемым удовольствием. Читатель, наверное, помнит про мое обещание привести один очень красивый результат про подстановки с минимальным числом нулей в матрице P(p). Настало время исполнить обещанное.

Пусть N – такое число, что N+1 – простое, q - примитивный элемент в поле Галуа GF(N+1), т.е. образующий элемент циклической мультипликативной группы этого поля.
Пусть p - преобразование множества Z/N вида:

$$p(x) = \log_q(q^{x+r} Å r), \text{ если } q^{x+r} Å r \neq 0,$$
$$p(x) = \log_q r, \text{ если } q^{x+r} Å r = 0,$$

где r - произвольный ненулевой элемент поля GF(N+1), r – произвольный элемент из Z/N, Å - операция сложения в поле GF(N+1). Тогда преобразование p является взаимно-однозначным на множестве Z/N, т.е. является подстановкой из симметрической группы S_N.
Это утверждение достаточно очевидно, поскольку q - примитивный элемент поля GF(N+1), т.е. множество значений $q,q^2,\ldots,q^N$ совпадает со множеством $\{1,2,\ldots,N\}$ – мультипликативной группой поля GF(N+1), а логарифмирование – операция, обратная возведению в степень. Все проблемы с нулем подправляются вторым условием: $p(x) = \log_q r$, если $q^{x+r} Å r = 0$.
Такие подстановки естественно назвать *логарифмическими*, а точку x_0, при которой $p(x_0) = \log_q r$ – *выколотой* точкой логарифмической подстановки p.

Здесь и всюду далее нам будут встречаться два разных типа арифметических операций сложения и вычитания: в кольце Z/N и в поле GF(N+1). Операции в кольце Z/N будем обозначать обычными символами “+” и “-“, а операции в поле GF(N+1) – Å и ▪ соответственно.

Теорема 1.
Пусть p – логарифмическая подстановка, $x_1 \neq x_2$, $x_1,x_2 \in Z/N$, i – произвольный ненулевой элемент кольца Z/N. Тогда если ни одна из точек x_1+i,x_1,x_2+i,x_2 не является выколотой, то $p(x_1+i)- p(x_1) \neq p(x_2+i)- p(x_2)$.
Доказательство.
Предположим, что $p(x_1+i)- p(x_1)= p(x_2+i)- p(x_2)$, тогда $q^{p(x1+i)- p(x1)}=q^{p(x2+i)- p(x2)}$.
Поскольку все точки не являются выколотыми, то отсюда вытекает, что $(q^{x1+i+r}Ar)(q^{x2+r}Ar)=(q^{x2+i+r}Ar)(q^{x1+r}Ar)$.
Раскрывая скобки и сокращая одинаковые члены в левой и правой частях равенства, получаем
$r (q^{x1+i+r}Åq^{x2+r})= r(q^{x2+i+r}Åq^{x1+r})$
Поскольку r - ненулевой элемент, то отсюда вытекает, что
$q^{x1+r}(q^i ▪ 1)= q^{x2+r}(q^i ▪ 1)$
Поскольку i – произвольный ненулевой элемент Z/N, а q - примитивный элемент GF(N+1), то $q^i \neq 1$, откуда вытекает, что $x_1=x_2$.■

Теорема 2. Пусть p – логарифмическая подстановка.
Тогда для любого ненулевого значения $i \in Z/N\backslash\{0\}$ из условия, что ни одна из точек x, x+i не является выколотой вытекает, что $p(x+i)- p(x) \neq i$.
Доказательство.
Пусть $p(x+i)- p(x) = i$. Тогда $q^{p(x+i)- p(x)}= q^i$, откуда $q^{x+r+i}Ar=q^i(q^{x+r}Ar)$, следовательно, $r=rq^i$. Отсюда следует, что i=0. ■

Раскинулось поле широко! Операции возведения в степень и логарифмирования в конечном поле позволили ловко избавиться от неопределенности в разности значений подстановки и легко, просто элементарно решить задачу построения матрицы P(p) с минимальным числом нулей. Заметим, что если в определении логарифмических подстановок отказаться от условия, что r - произвольный ненулевой элемент поля GF(N+1), то при r=0 мы получаем обычные линейные подстановки, у которых число нулей в P(p) максимально!
Осталось совсем чуть-чуть: разобраться с выколотой точкой.
Для произвольного ненулевого фиксированного $i \in Z/N$ рассмотрим отображение множества Z/N в Z/N вида:
$m_i(x) = p(x+i)- p(x)$,
где p - логарифмическая подстановка. Тогда, в силу теоремы 1, количество различных значений в множестве $\{m_i(x), x \in Z/N\backslash\{x_0,x_0-i\}\}$ равно мощности этого множества, т.е.N-2, причем, в силу теоремы 2, это множество в точности совпадает с $\{Z/N\backslash\{i\}\}$. В частности, при любом $i \neq N/2$ существует такое значение x, $x \in Z/N\backslash\{x_0,x_0-i\}$, что $m_i(x)=N/2$.
Теорема 3. Пусть p – логарифмическая подстановка.
Тогда если при некотором $i \neq N/2$ в i-ой строке матрицы P(p) справедливо $p_{iN/2}>1$, то эта строка не содержит нулевых элементов.
Доказательство.
В силу теоремы 2 достаточно доказать, что $p_{ii} \neq 0$. Условие $p_{iN/2}>1$означает, что либо $m_i(x_0)=N/2$, либо $m_i(x_0-i) =N/2$. Зафиксируем то, которое равно N/2, а другое оставшееся значение обозначим через m. Суммируя, как и ранее мы уже делали в этой книге, значения $m_i(x)$ по всем $x \in Z/N$, получаем:
$N/2(N-1) – i + m + N/2 = 0$.
Отсюда вытекает, что m=i, следовательно, $p_{ii} \neq 0$. ■

По коням! Пора заняться средней строчкой.
Начнем с самого любимого элемента – $p_{N/2,N/2}$. Ранее мы уже отмечали, что этот элемент должен быть всегда четным (рассуждения для случая $N=2^n$ легко обобщаются для произвольного четного N). Следовательно, в логарифмической подстановке возможны только два значения $p_{N/2,N/2}$: 0 или 2. Допустим, что $p_{N/2,N/2}=2$. В силу теоремы 2 эти значения может давать только выколотая точка x_0 и $x_0+N/2$, т.е.
$p(x_0+N/2)- p(x_0)= p(x_0+N/2+N/2)- p(x_0+N/2)= p(x_0)- p(x_0+N/2)=N/2$.
Отсюда вытекает, что $2p(x_0+N/2)=2p(x_0)$.
Рассмотрим два случая.

1. r=1, следовательно, $p(x_0)=0$. Тогда $p(x_0+N/2)=N/2$. Имеем:
   $q^{p(x0+N/2)}= q^{N/2} \Rightarrow q^{x0+N/2+r}Ar=q^{N/2} \Rightarrow q^{N/2}(1 ▪ q^{x0+r})= r \Rightarrow q^{N/2}(1Ar)= r \Rightarrow 2q^{N/2} = 1$.
   Возводя обе части последнего равенства в квадрат и учитывая, что $q^N=1$, получаем такое равенство возможно только в тривиальном поле из 3 элементов.
2. $r \neq 1$, следовательно, $p(x_0) =N/2$, $p(x_0+N/2)=0$, откуда
   $q^{p(x0+N/2)}= 1 \Rightarrow q^{x0+N/2+r}Ar=1 \Rightarrow r(1 ▪ q^{N/2})= 1 \Rightarrow q^{N/2}= 1 ▪ r^{-1}$.
   Возводя это равенство в квадрат, получаем значение r:
   $r=2^{-1}$

С учетом условия $p(x_0) = N/2$ получаем: $\log_q 2^{-1} = N/2$, откуда $2^{-1} = q^{N/2} Þ 2^{-2} = 1$. Такое также возможно только в тривиальном поле из 3 элементов.
Следовательно, во всех реальных практически значимых случаях $p_{N/2,N/2}=0$. Тогда найдется по крайней мере одна строка i, в которой $p_{N/2,i}$ ³2, и по теореме 3 в ней не будет нулей. Общее число нулей в такой матрице, с учетом уже упоминавшейся ее симметричности, будет равно N-3. Это минимально возможное количество нулей и оно оказалось достижимым!
Заметим, что подстановка, обратная к логарифмической, также будет логарифмической. Действительно, если $p(x) = \log_q(q^{x+r} Ar)$, то $q^{p(x)} = q^{x+r} Ar$, откуда
$x = \log_q(q^{p(x)-r} Ar_1)$, где $r_1 = (\blacksquare\ r)q^{-r}$. Следовательно, $p^{-1}p(x) = \log_q(q^{p(x)-r} Ar_1)$. При этом $q^{p(x)-r} Ar_1 = (q^{x+r} Ar)q^{-r} Ar_1 = q^{x}$ 1
0. Для случая $x=x_0$ справедливо: $p(x_0) = \log_q r$, при этом $q^{x0} = (\blacksquare\ r)q^{-r}$, откуда $x_0 = p^{-1}p(x_0) = \log_q((\blacksquare\ r)q^{-r}) = \log_q r_1$

Осталось построить в явном виде логарифмическую подстановку. Заметим, что условие N+1 – простое число выполняется для практически очень важного случая N=256, следовательно, логарифмические подстановки заведомо существуют при N=256. Условию N+1 - простое число удовлетворяет также N=16 и именно для этого значения мы сейчас и построим логарифмические подстановки, предоставляя заинтересованному читателю возможность построить логарифмические подстановки при N=256 самостоятельно.
В качестве примитивного элемента поля GF(17) выберем q=3, а также положим r=1, r=0. Составим таблицу степеней значения q:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
q^i	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

Используя эту таблицу, построим логарифмическую подстановку p

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
p(x)	14	12	3	7	9	15	8	13	0	6	2	10	5	4	1	11

и ее матрицу P(p)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0	1	2	11	2	1	1	1	1	1	1	1	1	1	1
2	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1
3	2	1	0	1	1	1	1	1	1	2	1	1	1	1	1
4	1	1	1	0	2	1	2	1	1	1	1	1	1	1	1
5	1	1	1	2	0	1	1	1	2	1	1	1	1	1	1
6	2	1	1	1	1	0	1	1	1	1	1	1	2	1	1
7	1	1	1	2	1	1	0	1	1	1	2	1	1	1	1
8	1	2	1	1	1	1	1	0	1	1	1	1	1	2	1
9	1	1	1	1	2	1	1	1	0	1	1	2	1	1	1
10	1	1	2	1	1	1	1	1	1	0	1	1	1	1	2
11	1	1	1	1	1	1	2	1	1	1	0	2	1	1	1
12	1	1	1	1	1	1	1	1	2	1	2	0	1	1	1
13	1	1	1	1	1	2	1	1	1	1	1	1	0	1	2
14	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1
15	1	1	1	1	1	1	1	1	1	2	1	1	2	1	0

Это подстановка с минимально возможным числом нулей в матрице P(p).

Это был, пожалуй, мой самый красивый математический результат. Но, к большому сожалению, логарифмические подстановки так и не нашли достойного применения в криптографии. Почему? Да очень

просто – их мало. Помните фразу про долговременные ключи-подстановки в дисковых шифраторах: «Их не опробуют. Их покупают.» Если в схемы типа «Ангстрем-3» мы будем ставить только логарифмические подстановки, то опробование всевозможных вариантов подобных подстановок сведется к опробованию всего лишь трех элементов: q - примитивного элемента в поле Галуа GF(257), r - произвольного ненулевого элемента поля GF(257) и r – произвольного элемента из Z/256. Это – копейки, совершенно ничтожная, по криптографическим меркам, величина. Если же выбирать подстановку случайно и равновероятно из всей симметрической группы S_{256}, то общее число опробуемых вариантов будет совершенно астрономической величиной 256!, намного превосходящей психологически недосягаемую в криптографии величину 10^{100}.

Но для шифров на новой элементной базе логарифмические подстановки позволили полнее представить общую картину того «лавинного эффекта», к достижению которого так стремятся криптографы всего мира.

Для меня же это означало еще и то, что путь к защите диссертации был открыт, несмотря на пессимистические прогнозы Степанова и проповедуемый им «патриотизм к отделу». Но на Степанова они подействовали не как на ученого, а как на администратора: красивый математический результат получен вышедшим из под его контроля сотрудником «на стороне», на кафедре криптографии Высшей Школы КГБ. Незамедлительно последовали выводы: наказать, чтобы не высовывался и чтобы другим неповадно было изменять родному отделу! Впрочем, об этом чуть ниже.

Глава 4

Совхоз

События в стране стали развиваться экспоненциально быстро по сравнению с брежневским без малого 20-летним правлением.

Андропов – ЧК КПСС – дневные облавы – водка «Андроповка».

Раз в неделю мы встречались с Б.А. и я не мог сдерживать своих эмоций: раскрепощенная аспирантская обстановка, масса свободного времени, дома работается гораздо легче и продуктивнее.

- Вот подождите, поймают Вас где-нибудь в кинотеатре, на дневном сеансе, тогда и будет Вам «свободная обстановка».

Но, по правде говоря, мне это особо не грозило. Не до кинотеатров было, интересная тема диссертации, да и появилась возможность решить семейные проблемы: сидеть дома с маленьким ребенком, ибо устроить в те времена свое чадо в детский сад было, естественно, большой проблемой, а тем более в районе-новостройке.

Диссертация продвигалась достаточно быстро. После появления логарифмических подстановок стало ясно, что она выходит на финишную прямую: «Теоретико-групповые и комбинаторные методы анализа и синтеза блочных шифров, реализуемых с помощью неавтономного регулярного регистра сдвига», специальность 20.03.04 – теоретическая криптография. Б.А. меня всячески поддерживал и к концу первого аспирантского года стало ясно, что вполне реально успеть защитить диссертацию еще в аспирантуре и при этом насладиться всеми прелестями вольной жизни.

Хотя какие это прелести жизни? Утром, когда в магазине мало народу, суметь купить более-менее съедобный кусок мяса, или собирать кучу всяких справок, чтобы встать в бесконечную очередь на улучшение жилищных условий – вот типичные советские прелести. А еще моей страстью стало добывание книг, художественной литературы.

Как трубила пропаганда, Советский Союз – самая читающая страна в мире, и в этом, в отличие от многого другого, в чем-то была права. Но свободно купить интересную книгу в книжном магазине было невозможно. Ее можно было только достать: купить втридорога на черном рынке, обменять, купить по абонементу, сдав 20 кг макулатуры, причем полки книжных магазинов ломились от партийной макулатуры: работ Ленина и разных пустых брошюрок с речами современных партийных вельмож.

Собирание собственных книг, личных библиотек стало весьма распространенным увлечением у московской интеллигенции, своеобразной интеллектуальной отдушиной, способом уйти от навязчивой и противно-примитивной коммунистической пропаганды. Для того, чтобы сдать макулатуру на интересную книгу - собрание сочинений Джека Лондона, исторические романы Мориса Дрюона, и, конечно же, на Александра Дюма – люди по несколько дней отмечались и дежурили в очереди. И это только для того, чтобы сдать макулатуру и получить заветный абонемент!

Не шарь по полке хищным взглядом
Тут не даются книги на дом
Лишь безнадежный идиот
Знакомым книги раздает

Хотя после смерти Брежнева стал просыпаться интерес к политике. В основном – зрительский, наблюдательный: что там еще эта власть учудит и сколько протянет очередной правитель? А период ежегодной смены правителей окрестили «пятилеткой пышных похорон».

- Какие цари были после царя?
- Владимир мудрый, Иосиф грозный, Никита чудотворец, Ленька летописец, Юрий долгорукий и Костя тишайший.

Особенно остро чувствовалась полная деградация коммунистической системы при правлении Черненко. Практически ни у кого не было сомнений: должность руководителя такой огромной страны не по нему. Старый, больной канцелярист, всю свою жизнь работавший только с бумагами и с Брежневым, серая, бесцветная личность, никаких идей, никаких перемен. Год вся страна смеялась и ждала естественного окончания этой комедии. И в марте 1985 года дождалась.

В Высшей школе КГБ уже никто не паниковал, все эти пышные похороны воспринимались как будничная рутина, мол генсеки приходят и уходят… А аспирантам в те похороны вместо пустого времяпровождения в аспирантской комнате доверили дежурить на гостевых трибунах Красной площади. Там я впервые услышал живой голос нового, молодого генсека. Что-то он нам уготовил?

Да бог с ними, с генсеками! Диссертация готова, все отзывы и рецензии собраны, осталось только дождаться, когда будет утвержден новый Ученый совет, а то все полномочия старого закончились в 1984 году, а без нового совета диссертацию не защитишь. Период вынужденной бездеятельности.

Закончил диссертацию – поезжай поработать в совхоз! Так по-советски логично решило руководство аспирантуры, и меня вызвали на беседу к самому секретарю парткома Высшей школы КГБ.

- Я прошу Вас помочь нам. Нет у меня сейчас под рукой ни одного человека, а Вы, как молодой коммунист, должны понять меня и выполнить это партийное поручение. Поработайте в совхозе командиром отряда неделю, ну максимум две, а потом я найду Вам замену.

Сельское хозяйство в советские времена работало таким образом, что практически ни один колхоз-совхоз не мог обойтись без «шефской помощи», а попросту говоря без халявной рабочей силы, осуществляющей самые примитивные и трудоемкие операции. На поля выгонялись тучи студентов, рабочих, инженеров, которые целыми днями убирали картошку, морковку, свеклу, капусту и прочие овощи-фрукты. Эти дары природы свозились на овощебазы, где все то, что не успевало быть разворованным, благополучно догнивало до кондиции. Многие горожане для безопасности собственного здоровья старались выращивать почти все необходимое для себя на собственных дачных участках, прозванных по размеру щедрости родного государства «6 сотками», а ко всему этому круговороту государственного сельскохозяйственного производства относились как к неизбежному социалистическому ритуалу, сопровождаемому, как правило, обильной выпивкой и неограниченной бесплатной закуской.

Бог миловал в наше время 4 факультет от всей этой кутерьмы. Но времена изменились и ко времени моего возвращения в родную альма-матер в качестве аспиранта еще одним элементом в деле подготовки хороших военных стали периодические «трудовые десанты» в подмосковный совхоз: рядовых слушателей – на неделю, преподавателей и аспирантов – на день. Совхоз был без ума от счастья иметь таких шефов: военная дисциплина, по совхозным меркам практически все поголовные трезвенники, молодые здоровые ребята, работающие исключительно за идею – разве сравнять с каким-нибудь заводом или ПТУ, дружно отключающимся одновременно с открытием магазина.

По весне совхоз снова тряс «шефов»: пришлите людей перебирать картошку, а то сорвется посадочная страда. У совхоза было собственное большое подземное картофелехранилище, где в огромных буртах всю зиму хранилась картошка. Весной надо было все эти бурты перебрать и расфасовать картошку на крупную, среднюю, мелкую и гнилую. Для этих целей имелось несколько древних картофелесортировальных машин (КСМ) – обычный транспортер с валиками, различные зазоры между которыми позволяли производить требуемое разделение этого народного продукта на элиту, средний класс, пролетариат и алкоголиков. Два человека влезали на картофельные бурты и лопатами кидали картошку на транспортер КСМ, а еще три человека с корзинами сидели у разных ответвлений и, вылавливая руками гнилье, наполняли разные корзины разными сортами.

Вот на такие трудовые подвиги и направил меня партком Высшей школы КГБ. Работа тяжелая, противная и абсолютно бесплатная. Дело в том, что в социалистические времена в Высшей школе КГБ получать за работу деньги считалось ну, неудобно, что-ли. Работа за идею – вот какой был идеал, проповедовавшийся со времен то ли ленинского бревна, то ли китайских хунвейбинов. Да и расценки на подобный сельскохозяйственный труд были соответствующими: сортировка 1 тонны картошки стоила около 2,5 рублей советских денег. Бригада из 5 человек, уматываясь в усмерть, за день могла отсортировать максимум 5 тонн картошки и, следовательно, заработать за день 12,5 рублей, по 2,5 рубля на человека.

Поэтому даже логично было не связываться с такими деньгами: все, что оставалось после вычетов за питание и проживание с большой помпой перечислялось в детский дом.

Совхоз приставил к нашему отряду техника Виталика, задачей которого было обеспечение бесперебойной работы всех КСМ. Задачей, нужно прямо сказать, практически невыполнимой, что Виталик прекрасно понимал и делал из этого свои, соответствующие выводы. Виталикино тело, не подающее иных признаков жизни, кроме перегара, выносилось из укромного уголка и погружалось на трактор уже через два-три часа после начала работы, как раз к тому времени, когда все КСМ начинали ломаться. Осуществлялся разбор его наследства в виде гаечных ключей, отверток и плоскогубцев, после чего все будущие чекисты вспоминали кружок «Умелые руки» и КСМ каким-то чудом начинали снова крутиться.

Так прошла моя первая неделя в совхозе. Ребят, работавших со мной, сменили, а мне, естественно, смена не пришла. Ну ничего, ведь сам секретарь парткома Высшей школы КГБ обещал, что максимум через две недели меня заменят. Но через две недели очередной автобус привез мне вместо смены руководящие указания парткома: активизировать, мобилизовать, усилить работу. Я сразу вспомнил стройку госпиталя КГБ и все самые сочные выражения, услышанные там. Ведь все-таки основная моя задача – защита диссертации, никакой партком за меня ее не сделает, да и надоело уже бессменно торчать здесь, среди этой гнилой картошки и алкашей-совхозников. Не без труда отыскав в этой дыре телефон, я напрямую позвонил секретарю парткома и напомнил ему о его обещании.

Никакой любезности секретарь уже не проявлял. Похоже, что он вообще забыл про меня и про все свои обещания, поэтому мои напоминания вызвали в нем рычание. Поняв, что дальнейшие переговоры бесполезны, я бросил трубку и пошел по деревне в поисках человека, которому можно было бы излить свою душу. Тут же попался Шурик, секретарь парткома совхоза, который как нельзя лучше подходил для этой роли.

В процессе излияния-возлияния Шурик поведал мне сокровенные совхозные тайны. То, что в совхозе работают слушатели Высшей школы КГБ – страшная тайна. Но не от агентов иностранных разведок, а от одной шустрой бабы из соседнего совхоза, Героини Социалистического Труда, которая, если эта информация до нее дойдет, употребит все свои связи и влияние и перетащит такую непьющую халявную рабочую силу к себе, чтобы добиться новых высот в социалистическом соревновании знаменосцев пятилетки.

Излив Шурику душу, я, собрав последние силы, пришел в свою каморку и включил радио. Михаил Сергеевич Горбачев на очередном Пленуме ЦК КПСС объявлял о начале перестройки…

Глава 5

Ученый совет

Раз впереди замаячила защита диссертации, значит, пора устанавливать хорошие отношения с Сергеем Николаевичем, секретарем Ученого совета факультета. Про Ученый совет и его секретаря здесь надо сказать несколько слов особо.

Ученый совет – это такой специальный орган, который имеет полномочия рассматривать диссертации и ходатайствовать перед ВАК – Высшей Аттестационной Комиссией – о присуждении соискателю ученой степени кандидата или доктора тех или иных наук. Ученый совет 4 факультета имел полномочия рассматривать диссертации по двум специальностям: 20.03.04 – теоретическая криптография и 20.03.05 – инженерная криптография. Разница между этими специальностями была довольно условная, обе они были связаны с математикой и криптографией, но неофициально на практике более престижной считалось защитить диссертацию по специальности теоретическая криптография – это означало, что в ней содержатся интересные математические результаты, красивые теоремы и нетривиальные доказательства. Диссертация по инженерной криптографии содержала, как правило, какие-то важные практические результаты, возможно и не содержащие в себе математической красоты и изящества, но которые принесли уже реальную пользу. Эта специальность была очень популярна для соискателей из 16 управления КГБ, «колонувших» какой-нибудь зарубежный шифр и решивших расписать подробности его вскрытия. По специальности теоретическая криптография присваивали, как правило, ученую степень кандидата или доктора физ.-мат. наук, а по инженерной криптографии – технических наук.

Ученый совет 4 факультета состоял из ведущих советских криптографов того времени, в него входили и наиболее опытные преподаватели с кафедр математики и криптографии, а также наиболее значимые специалисты-криптографы из 8 и 16 управлений КГБ и Министерства обороны. Заседания Ученого совета проходили раз в месяц и на них рассматривались либо одна докторская, либо две кандидатских диссертации. На практике ВАК автоматически утверждал все решения Ученого совета 4 факультета, поэтому принятие на Ученом совете решения о присуждении ученой степени означало успешную защиту диссертации и окончание длинной и нудной бюрократической процедуры подготовки к ее защите.

Из трех лет, проведенных мною в очной аспирантуре, расклад был примерно такой – первый год – сдача экзаменов кандидатского минимума и получение основных результатов, второй год – написание и

оформление диссертации, ну а весь третий год – подготовка к защите, сбор отзывов и рецензий, «окучивание» Сергея Николаевича, секретаря Ученого Совета. С этим человеком мне уже приходилось сталкиваться во времена учебы на 4 факультете – он читал нам на третьем курсе лекции по марксистско-ленинской философии («бытие определяет сознание») и был прозван за это Фейербахом, хотя сам по образованию был математиком, кандидатом физ.-мат. наук.

Про философские изыскания Сергея Николаевича сейчас, по прошествии стольких лет, я ничего определенного сказать не могу, многое из той славной «науки всех наук» уже бесследно исчезло из моей памяти, да если когда что-то туда и западало, то, в основном, вместе с другой философско-преферансной истиной:

- Под вистующего – с тузующего, под игрока – с семерика.

Но это было почти 10 лет назад. Сейчас же, в 1985 году, Сергей Николаевич вернулся к своей основной специальности – математике, но общение с философией не прошло для него бесследно – он стал математическим бюрократом.

Для современного читателя будет наверняка очень скучным долгий перечень ВАКовских требований к оформлению диссертации, автореферата, рецензий и отзывов, которые Сергей Николаевич требовал скурпулезно соблюдать и в которых находил основной смысл своей деятельности. Но некоторые эпизоды из моего общения с ним, на мой взгляд, достаточно интересны, поскольку отражают ту атмосферу, обстановку в ученой криптографической среде тех лет.

Защита диссертации – это научный спор, в котором соискатель отстаивает правоту своих научных взглядов и результатов, изложенных в диссертации, а его официально утвержденные оппоненты их пристально изучают и анализируют, пытаясь найти в них ошибки, неточности, неоптимальные методы и любые иные недостатки. На Ученом совете эта дискуссия происходит уже в явном виде и по ее результатам совет выносит свое решение: присуждать или нет соискателю ученую степень. Оппоненты – это тоже живые люди, иногда на заседании совета происходили примерно такие диалоги.

- В этой теореме содержится ряд неточностей, однако в личной беседе с автором…
- Это в какой такой беседе? В ресторане, что ли?

Но это скорее исключение из правил. Защита диссертации – это серьезное мероприятие, а члены Ученого совета – это весьма и весьма уважаемые всеми люди. Защита диссертации почти никогда не превращалась на 4 факультете в театрализованное представление, любой соискатель должен был быть всегда готов к каким-то неожиданным вопросам, к критике, к выявленным его оппонентами ошибкам, в общем, к нормальной научной дискуссии. Так было в большинстве случаев, но на мою долю выпало один раз увидеть исключение из этого правила.

Аспирантов, всерьез помышляющих о защите диссертации, Сергей Николаевич привлекал в качестве подсобной рабочей силы для различных своих нужд: уничтожения (в печке, путем сжигания) устаревших документов, подготовке и дежурству на очередных заседаниях Ученого совета. Функции дежурного на заседании Ученого совета сводились к отметкам в специальном списке всех присутствующих и приглашенных, но, выполнив эти обязанности, дежурный затем получал возможность присутствовать на самом заседании и набираться там ума-разума, необходимого ему для подготовки к собственной защите. Несколько раз таким дежурным приходилось быть и мне, и одно дежурство было достаточно интересным.

Накануне Сергей Николаевич предупредил меня, что защищаться будет очень важный человек. Обычно на одном заседании совета рассматривают две кандидатские диссертации, а здесь – только одна. Тщательно проинструктировав, Сергей Николаевич еще раз подчеркнул особую важность завтрашнего заседания.

На следующий день, как и положено, в 8 утра, я уже был на своем боевом посту около аудитории, в которой проходили заседания совета. Почти сразу же в аудиторию зашел действительно большой человек с плакатами в руках, которые стал развешивать на доске, вместо того, чтобы, по традиции, исписывать ее мелом, дрожа от волнения. Интуитивно было ясно, что это и есть тот самый важный соискатель, я даже не просил его представиться.

Но примерно через полчаса к аудитории подошел еще один человек, почти такой же большой (нет, все же чуть поменьше), но уже безо всяких плакатов.

- Вы на защиту?
- Да
- Разрешите, я отмечу Вас в списке.
- Да это я сам и защищаюсь!
- А кто же тогда плакаты развешивал?
- Это Васька Сернов.

Оглядев хозяйским взглядом доску с развешенными на ней плакатами, соискатель милостиво предложил своему подручному

- Ну что, пойдем, покурим!

Стоит ли говорить, что «черных шаров» на этой защите не было, а с мест раздавались только хвалебные замечания по адресу соискателя, возмущение его скромностью («это материалы для докторской диссертации, а не кандидатской»), предложения выдвинуть ее на Государственную премию. Лишь один оппонент, подойдя к развешенным плакатам, отважился на некоторую завуалированную критику:

- Здесь были приведены очень интересные и убедительные результаты. Я бы отметил только одно: результаты первой главы были получены в 50-х годах, второй – в 60-х, третьей – в 70-х. Но это не значит, что они устарели, наоборот, прошли хорошую практическую апробацию.

Соискатель был, насколько мне сейчас не изменяет память, одним из советников зампреда КГБ. Биография боевая – до конца 40-х годов – истинный чекист, оперативник, а затем подался в криптографию. И вот стал, наконец, долгожданным кандидатом технических наук!

Но перед своей собственной защитой я все же сильно волновался. Как отнесется Ученый совет к такому сравнительно молодому (28 лет) соискателю, когда многие другие соискатели годами мучаются с диссертацией? Как, наконец, отнесется ко мне такой член Ученого совета, как Вадим Евдокимович Степанов, который перед моим уходом в очную аспирантуру предсказывал, что мне вряд ли удастся там защититься? Что скажут оппоненты?

Но все страхи оказались напрасными. Защита диссертации прошла успешно, никто не мог ничего сказать против логарифмических подстановок и метода кратной транзитивности для анализа шифров типа «Ангстрем-3». Многие вопросы, связанные с шифрами на новой элементной базе, прояснились. Подстановку р в шифрах типа «Ангстрем-3» нужно ставить до, а не после операции сложения с ключевыми знаками входного слова – в этом случае не будет того катастрофического упрощения уравнений зашифрования/расшифрования, которое привело к краху «Ангстрема-3» при Т=16. Точек съема с основного регистра надо выбирать не три, а четыре, а функцию усложнения использовать не $x_1+x_2+x_8$, а $x_1-x_2-x_7+x_8$. Длину же Т, при которой практически перестают работать методы, основанные на 2-транзитивности, следует выбирать порядка 40.

«После защиты диссертации устраивай банкет» - гласит одно из основных неписаных (хотя в нашей аспирантской стенгазете оно было прописано явно) правил. А как же начавшаяся недавно удалая антиалкогольная кампания, с ее «обществами трезвости» и «безалкогольными свадьбами»? Несколько слушателей 4 факультета, ради прикола, решили в общежитии «отметить» выход в свет антиалкогольного Указа Горбачева-Лигачева. Ребята явно не отдавали себе отчета в том, на какой риск они идут, ведь общежитие – общее, они жили там вместе с «истинными» чекистами. Их моментально заложили и уже на следующий день в 24 часа все были отчислены с факультета.

Этот Указ был опубликован в газетах сразу после 9 мая 1985 года и вступал в силу с 1 июня, т.е. с этого времени партия приказывала всем коммунистам «завязать». Но в мае, до 1 июня, этот партийный приказ еще не вступил в силу, хотя на желающих 30 мая, в день моей защиты, принять участие в «небезалкогольном» банкете по этому случаю уже тогда, заранее, могли посмотреть слишком трезвым взглядом. По крайней мере, примерно такие разъяснения я услышал от начальника кафедры криптографии. Но все же большинство моих аспирантских знакомых и друзей, с которыми довелось нести боевую службу все эти три аспирантских года, от вступления в общество трезвости воздержались. Доктора и кандидаты криптографических наук, как революционеры-подпольщики тайно собираются у меня на квартире в тесной комнатушке. На маевку. Пролетарии всех стран, соединяйтесь!

Глава 6

IBM PC XT

Все, цель достигнута, пора осмотреться и подумать, что же дальше. Высшая школа КГБ мне нравилась, несмотря на все изменения, произошедшие в ней за последние годы. Ведь не начальники определяют ее лицо, а слушатели, те ребята, ради которых она и существует. Отбор идет очень строгий, поэтому коллектив подбирается, как правило, очень сильный. С такими ребятами интересно общаться, читать им лекции, спорить, состязаться в остроумии и смекалке, да и примеры прекрасных преподавателей перед глазами. Это не то, что в Теоретическом отделе, доказывай абстрактные теоремы с 9 до 6 вечера, быстро превращаясь в закостеневшего чинушу, думающего только о карьере. Возможность сравнивать была, почти по три года я пробыл в отделе у Степанова и в Высшей школе, и вывод однозначный: вся обстановка, отношения между

людьми, характер преподавательской работы на 4 факультете для меня предпочтительнее, чем в 8 управлении КГБ. Кафедра криптографии готова была взять меня после окончания аспирантуры на преподавательскую работу…

- Назад!

Я был офицером, который безоговорочно обязан подчиняться приказам. Но можно приказать солдату рыть траншею, а как приказать математику придумывать и доказывать теоремы? Разве применим приказ, грубый нажим, граничащий с насилием, там, где речь идет о творческой работе, о поисках новых нетривиальных методов, о нестандартных подходах? Не будет ли в таком случае обратного результата?

И этот приказ исходил от Степанова, умнейшего человека, которого я очень уважал, как ученого. Но он был еще и жестким человеком. Хорошо это или плохо – вопрос спорный, может быть в каких-то ситуациях жесткость администратора и необходима, но в данном случае он затащил меня назад, к себе в отдел даже не спросив моего мнения, с помощью грубой силы приказа, как отступника от идеи «патриотизма к отделу», как диссидента, которого надо наказать, чтобы другим неповадно было. Это – стиль работы, на который наложила свои отпечатки вся история ВЧК-КГБ. Не хочешь – заставим: хоть канаву копать, хоть теоремы доказывать, при Сталине многие так работали. Была ли в таком приказе какая-то производственная необходимость? Вот уж вряд ли! Это, скорее, был результат каких-то внутриотдельских интриг, желание мелких начальничков, рангом пониже Степанова, не упустить случая и проучить строптивого молодого человека, не пожелавшего делать себе карьеру «как все», показать ему «истинные ценности», преподать наглядный урок на тему «Машина и винтики». Но Степанов был начальником отдела, командиром, администратором, без его собственного мнения такой приказ никогда бы не появился. И он поддерживал идею безоговорочного «патриотизма к отделу», помимо мелких начальничков он и сам приложил свою руку к тому, чтобы насильно затащить меня обратно и как следует проучить за строптивость. Не хочет винтик вворачиваться – советский слесарь по нему кувалдой!

- Диссертация – это твое личное дело. Здесь теперь тебе нужно начинать все сначала, завоевывать авторитет, доказывать, что ты достоин нашего отдела.

Интересная теория! Насильно затащили назад в это тюремное здание, а потом я должен еще доказывать, что сам туда рвался! А ради чего? Ради этой противной «игры в начальников», когда смыслом жизни становится не интересная работа, а стремление вылезти пусть в маленькие, но начальнички, надуть побольше щеки и поглядывать свысока на своих бывших сокамерников, командовать ими.

Большая обида осталась тогда у меня на Степанова и тех, кто шептал ему на ухо, как побольнее ударить этого строптивого. Но это, как выяснилось позже, были только цветочки той системы, а какими оказались ягодки – в то время мне не могло присниться даже в кошмарном сне. Но желание получать интересные результаты пропало. Какой смысл?

Я не скрывал своего недовольства, Степанову на это было наплевать. Интересные работы над шифрами на новой элементной базе в Теоретическом отделе практически прекратились, возможно по той причине, что в вопросе о советском стандарте выбор окончательно пал на переделанный DES, которым занимались «криптографические законотворцы» из 1-го отделения. Все разумные модификации «Ангстрема-3» я предложил в своей диссертации, написанной «на стороне», будучи аспирантом-очником кафедры криптографии 4 факультета Высшей Школы, и для Степанова это был еще один аргумент в пользу родных «законотворцев». Да и хлопот при этом меньше, проще объяснить руководству Спецуправления: взяли за основу американский стандарт, своих тайн не выдаем.

А еще одной особенностью, которую я заметил, вернувшись на степановском аркане обратно в его отдел, стало заметно усилившееся внимание к системам с открытым распределением ключей. В середине 70-х годов американцы предложили два принципиально разных подхода к построению таких систем: с помощью возведения в степень в конечных полях (система Диффи-Хеллмана) и с помощью умножения больших простых чисел (система RSA, названная по первым буквам ее авторов: Riverst, Shamir и Adleman). Первые кавалерийские атаки Теоретического отдела на эти системы к тому времени закончились, отношение стало серьезнее, уже не как к «провокации американских спецслужб», а как к новому направлению в криптографии. Степанов, надо отдать ему должное, понял это одним из первых, и к моменту моего возвращения у алгебраистов отдела основным предметом споров стали преимущества и недостатки умножения больших простых чисел и возведения в степень в конечных полях. Но, в отличии от американцев, гражданская, коммерческая криптография, ради которой и создавались системы с открытым распределением ключей, по-прежнему считалась идеологически вредной.

Но это была не моя тема. Открытые ключи и строящиеся с из помощью асимметричные системы шифрования – красивейшая математическая находка, но масть легла так, что я посвятил свои научные изыскания традиционному, симметричному шифрованию, хотя и на новой элементной базе. А дальнейшая судьба шифров на новой элементной базе была туманна: с одной стороны, «законотворцы» со своим советским крокодилом – DES, одобренным сверху, а с другой – открытые ключи, становившиеся главным

предметом внимания алгебраистов. Плюс ко всему – традиционные советские «балалайки», требовавшие контрольных экспертиз, особенно после того, как в них выявлялись какие-то криптографические «дыры», выпавшие из внимания 15 – 20 лет назад, в момент их создания.

Так, в бесцельной суете и обидах прошел год. Скучное высиживание над раскрытой тетрадкой за дежурным анализом древней «балалайки», сплетни, язвительная оценка окружающей меня действительности, осознание того, что, помимо своей воли, превращаюсь в серого чиновника, все интересы которого сводятся только к ожиданию руководящих указаний и повышений по службе. Одни и те же лица, одни и те же проблемы: кто каким начальничком вскоре станет, да кто куда намеревается уйти из отдела. Уйти из отдела – это оказывается тоже искусство, нужно заранее как следует «окучить» каких надо начальников, распустить, когда надо, слух о своем уходе из отдела, с кем надо договориться, а потом … никуда не уходить. Проверка на вшивость, нечто вроде одного из способов получить повышение по службе в своем родном колхозе.

Тоска зеленая, а что же дальше?

- Степанов собирает наше отделение у себя в кабинете.

Опять какие-нибудь разборки местного масштаба, типа согласования новых требований к шифраппаратуре. Совершенно бредовые требования, запутывающие до предела принятую и уже долгое время использующуюся практику считать стойкость шифратора, как отношение трудоемкости к надежности. Прошлый раз это шоу вылилось чуть ли не в поименное голосование с тем, чтобы потом, лет через 5, можно было бы прочитать эти записки из сумасшедшего дома и фамилии тех, кто был его пациентами. Пациентов хватало…

Но на этот раз я ошибся. На столе у Степанова стояло то, чего раньше никто никогда в отделе не видел - персональный компьютер IBM PC XT.

Loading…

Невиданное зрелище – говорящий без бумажки Генеральный секретарь ЦК КПСС! Народ обомлел: сам ходит, телохранители не поддерживают, молодой, шустрый и бойкий. Ну, что-то теперь будет!

Началось все, по-правде говоря, как-то не в кайф. С антиалкогольной компании.

- Взгляд звериный, хвост змеиный, что это?
- Очередь за водкой!

Потом пошли-полетели перестройка, демократия и гласность.

Товарищ, верь, пройдет она,
И демократия, и гласность,
Лубянка вспрянет ото сна,
И вот тогда госбезопасность,
Припомнит наши имена.

И замочит в сортире, хочется добавить в конце 2003 года. Но тогда, в 1987 году, политическая жизнь в стране (или, по крайней мере, в Москве) заметно оживилась. Очереди за газетами в которых (о, боже) – критика КПСС и Сталина, такие слова, которые раньше произносились только в узком кругу, в анекдотах и на кухнях.

В одном месте прибудет, зато в другом убудет. Вместе с появлением демократии и гласности из магазинов почему-то стали исчезать последние товары. Чем больше зрелищ – тем меньше хлеба. Одновременно и того, и другого в нашей стране не бывает.

- Цепь на метр удлинили, миску на два отодвинули, и гавкать разрешили.

Сначала казалось – несерьезно, ненадолго. Реальная власть как была, так и останется у Политбюро, у ЦК КПСС, так было, так есть, так будет. Всякие новации типа XIX Партийной конференции и Съезда Народных Депутатов – для отвода глаз, пар стравить, но прямые трансляции – новое захватывающее зрелище. Народ не отрывается от телевизоров и радиоприемников, все ждут одного – выступлений оппозиции. Накануне XIX партконференции стравить пар решили и в Теоретическом отделе

Спецуправления 8 ГУ КГБ СССР. Партком попросил всех коммунистов подготовить свои предложения для этой конференции в надежде на то, что все пройдет тихо, по старинке: примут несколько газетных лозунгов, а партком отчитается о проведенном мероприятии. А тут понеслось:

- Убрать могилы Сталина, Жданова, Брежнева, Суслова от Кремлевской стены!
- Установить общественный контроль за деятельностью органов КГБ!
- Установить памятник жертвам репрессий!

Сомнительно, чтобы все эти предложения пошли дальше парткома Спецуправления, которому ясно дали понять: идет брожение в еще относительно молодых математических умах. Но даже партком Спецуправления ничего уже не мог поделать…

Ну да бог с ней, политической ситуацией в стране, да с разными чудесами. Появились первые персональные компьютеры! Loading…

Глава 1

Rub berries body

«Из математика легко подготовить программиста, а вот из программиста математика – сложнее» - так любил говорить Б.А., мой научный руководитель. Истинно так! Только каков конкретный алгоритм подготовки программиста из математика-криптографа? С чего, по выражению Великого Вождя, начать?

С компьютерных игр. Пусть наиграется до посинения, до тех пор, пока пар из ушей не повалит, после этого – клиент готов. Дальше до всего остального, если есть голова на плечах, додумается сам. Главное – чтобы компьютер имел, как принято выражаться, дружеский интерфейс, а по-простому, по-советски – не заставлял бы тебя долбать дырки в перфоленте, не стращал бы своими кастрюлями-накопителями, не ломался и был бы доступен без записей и очередей практически в любое время, т.е. был бы на самом деле персональным. Математику, прошедшему через алгебру и ТВИСТ, разобраться в какой-то там DOS или языках программирования совсем нетрудно, а компьютер, после проведенных вместе с ним битв против шамуса или арканоида, - лучший боевой друг.

Несомненно, это была вражеская диверсия: в Теоретический отдел Спецуправления 8 Главного управления КГБ СССР практически одновременно с появлением там первых PC были запущены компьютерные игры. Работа встала, начался первый и самый основной этап освоения компьютерной грамотности – наиграться до посинения. Все теоретики, алгебраисты и вероятностники, молодые и старые, активные и пассивные, обсуждали одну и ту же научную проблему: как в Space Quest-2 пройти болото с кикиморой.

- Палку взять на берегу пробовали?
- Сколько раз, не помогает.
- Нырни поглубже и обойди ее.
- Глубже не ныряется.
- Должна же быть дорога в обход болота.
- Да нет там никакой другой дороги, только через болото!
- Пугнуть ее чем-то надо.
- Пробовали, не помогает.

Это была одна из первых игр-бродилок, в которых команды человечку-путешественнику по неведомой планете надо было набирать по-английски на клавиатуре. Успешно были пройдены все первые уровни, а вот на этом проклятом болоте кикимора всякий раз нагло проглатывала отважного странника. И весь 5 отдел никак не мог ничем ему помочь.

Забыты научные распри и споры, наступило всеобщее единение в борьбе с этой буржуйской вражиной. Научный подход: пронумерованы все предыдущие попытки, идет анализ возможных вариантов, дискуссии и дебаты, рисуются схемы проходимых лабиринтов, криптографы яростно пытаются применить самый известный и самый надежный метод криптографического анализа – метод тотального опробования, не остаются в стороне и другие достижения современной криптографической мысли – методы согласования, гомоморфизмов, статистических аналогов, и все они направлены против одного и того же противника, воспринимаемого уже не как абстрактный «вероятный противник», а как самый ни на есть настоящий – кикимора из болота в Space Quest 2 и те, кто ее придумал. В конце концов человеческий разум победил!

Где-то спустя примерно неделю после первой попытки, когда, казалось, тотально были опробованы все мыслимые криптографами методы, кто-то обратил внимание на кусты, растущие около болота.

- Ягоды с кустов есть пробовали?
- Не помогает.
- А если натереть ими тело?

Rub berries body. Волшебные слова, истина в последней инстанции! Человек, сказавший их первым, заслуженно стал героем дня, его поздравляли, жали руку, желали дальнейших творческих успехов. После этих слов запах ягод отпугнул кикимору и она сочла человечка несъедобным. Всеобщее ликование и радость: победа, добытая в трудной и упорной борьбе!

Это был, пожалуй, пик экстаза компьютерных игр в отделе. Ажиотаж пошел на спад, хотя тетрисоманы еще долго крутили-вертели свои загогулины, пытаясь установить новый абсолютный рекорд. Но в конце концов свершилось то, что и должно было свершиться: игры стали надоедать. Может, запрограммировать что-нибудь? Алгоритм какой или метод? Вот так персональные компьютеры стали лучшими друзьями всего прогрессивного человечества, в том числе и советских криптографов. По крайней мере, в Теоретическом отделе Спецуправления 8 ГУ КГБ СССР.

Глава 2

Бормотуха

Предсказателей и гадалок в 5 отделе хватало, особенно среди «криптографических законодателей». Прогнозные исследования – очень модная тема: как будет развиваться вычислительная техника? Как это отразится на криптографии? На оценках стойкости? Как будут развиваться методы криптографического анализа? И много иных подобных «как». В основном все сводилось к угадыванию желаний криптографического начальства. А оно пожелало, в частности, новые требования к шифраппаратуре.

Тут надо немного посвятить читателя в основы криптографического анализа. С чего он начинается? С предъявляемых к этой аппаратуре криптографических и инженерно-криптографических требований, т.е. нормативного документа, определяющего, в каких случаях результаты проведенного криптографического и инженерно-криптографического анализа считать опасными для дальнейшей эксплуатации аппаратуры, а в каких – нет. Например, когда удалось построить наглядный пример вскрытия шифра, подобный тому, который описывался для шифра типа «Ангстрем-3» при T=16 – это заведомо опасный результат. Но такие ситуации встречаются на практике очень редко, а в большинстве случаев результаты криптографического анализа носят абстрактный характер: трудоемкость Q метода определения секретного ключа составляет столько-то двоичных операций, при этом надежность P (вероятность правильного определения ключа) – такая-то. Минимальное отношение Q/P по всем рассмотренным методам криптоанализа является оценкой стойкости шифровальной аппаратуры.

С незапамятных времен (с начала 60-х годов) действовали единые криптографические и инженерно-криптографические требования, по которым опасной считалась оценка стойкости ниже, чем 10^{25}. По тем временам, да и по этим тоже, этого вполне хватало, чтобы говорить о гарантированной стойкости: опробование такого количества вариантов не по силам даже современным компьютерам. Но криптографическое начальство, напуганное страшилками про нейрокомпьютеры и эффект сверхпроводимости, а также бурным научно-техническим прогрессом на Западе, решило подстраховаться: создать новые требования к перспективной шифраппаратуре, в которых не было бы никаких четких оценок и в любом случае можно было бы сказать, что мы все знали и предвидели.

По новым требованиям оценка стойкости измерялась почти по Эйнштейну: не в Q/P, а во времени. Во времени максимальной эксплуатации. Ну, да это бог с ним, со временем, хоть в погонных метрах мерить эту стойкость, главное нововведение было в двух коэффициентах: a и b. b - ежегодные темпы роста производительности вычислительной техники, тут еще с натяжкой можно было как-то предположить конкретные цифры - 1-2 порядка в год, хотя, очевидно, не каждый год сохраняются подобные темпы. Вся хитрая чиновничья казуистика заключалась в коэффициенте a - ожидаемый ежегодный прогресс криптографических методов анализа. Это примерно то же, что и количество чертей на конце булавочной иголки, сколько это будет – одному Богу известно.

Одну старую «балалайку» в НИИ автоматики проанализировали по новым требованиям. Как там считали коэффициент a - не знаю, скорее всего откопали все старые отчеты и разделили общее количество сброшенных порядков на время, которое эта «балалайка» эксплуатировалась. В итоге общая оценка стойкости получилась 100 лет, эту цифру официально записали в отчете. На следующий год в 5 отдел пришел молодой парень, свежим взглядом нашел статаналог и по старым, добрым требованиям «уронил» оценку стойкости до 10^{21}. Больше старых «балалаек» по новым требованиям не анализировали, так спокойнее будет жить.

Но любимой темой для гаданий был прогноз развития ЭВМ. Под это дело была даже открыта специальная НИР «Экстракт», злыми языками, ничего не понимавшими в техническом прогрессе, окрещенная бормотухой. Как скажется на криптографии развитие ЭВМ – вот главный вопрос, на который должна была дать ответ эта НИР в середине 80-х годов теперь уже прошлого века. Источником

разведданных для НИР «Экстракт» служили, в основном, публикации в газете «За рубежом» про различные технические сенсации на Западе, которые аккуратно переписывались и, естественно, засекречивались.

Исходная точка отсчета в НИР «Экстракт» была такова: всемогущее американское Агентство Национальной Безопасности скупает все мировые компьютеры, распараллеливает их и запускает для перебора ключей к советским «балалайкам». Сколько они смогут сделать операций в год? Сколько еще порядков нужно накинуть для подстраховки?

Броня крепка и танки наши быстры. Советская криптография всю свою сознательную жизнь была исключительно военной, обслуживала только высшее руководство СССР, правительство, важные министерства типа министерства иностранных дел, войска. Психология и мышление советского высшего криптографического начальства также были исключительно военными, да к тому же еще идеологически кристально чистыми. Слова «коммерческая криптография», «рынок», «прибыль» для него даже во второй половине 80-х годов были контрреволюционными (по крайней мере, в официальных документах), за которые товарищ Сталин справедливо делал известно что. Так было, так есть, так будет всегда!

А жизнь-то менялась. Персональные компьютеры дешевели, их становилось все больше и больше, и не за горами было то время, когда они станут неотъемлемым бытовым атрибутом, наподобие телевизора или холодильника. Запрограммировать на PC криптографический алгоритм не так уж и сложно, а отсюда уже один шаг и до массовой, гражданской криптографии, была бы только в ней потребность. А тут модемы и первые компьютерные сети стали появляться…

Остановиться бы тогда, в конце 80-х годов, снять с глаз темные очки и оглядеться вокруг на окружающую действительность. Была же ведь реальная возможность побороться за мировые рынки сбыта наукоемкой криптографической продукции, программ и алгоритмов, была возможность даже в каком-то смысле стать законодателями криптографической моды. Были и идеи (те же шифры на новой элементной базе), были и отличные молодые специалисты, с ходу освоившие все нехитрые программистские премудрости и готовые выдавать конкурентоспособную продукцию. Не было одного: желания руководства реально поддержать это направление. Разговоров про необходимость использования компьютеров было выше крыши, море совещаний, партийных собраний, оперативок, но если речь заходила о каких-то реальных делах – глухая стена. Так тише, спокойнее, меньше ответственности.

Дело еще и в том, что советская электронная промышленность того времени просто по определению не могла выпускать ничего похожего на западные PC. Как, мы советские криптографы попадем в зависимость от враждебного нам запада? А если они нам закладок понаставят, или эмбарго какое введут? Наша электроника хоть и с танк размером, да и ломается постоянно, но это – своя, отечественная! А запад – загнивает и постоянно стоит над пропастью. Наверное, смотрит, что мы там делаем.

Но PC открывали перед криптографами колоссальные возможности. Программируешь самостоятельно любой необходимый алгоритм, нет этой противной и поглощающей все силы зависимости от промышленности, от заводов. Надежность западных персональных компьютеров намного выше, чем советской техники, поэтому сам собой почти отпадает вопрос об инженерно-криптографическом анализе: PC практически никогда не ломаются. Любое изменение в алгоритме – Upgrade – тоже нет необходимости связываться с заводом, достаточно перепрограммировать алгоритм. Универсальность, надежность, потенциально большой спрос – вот что сулило использование PC в криптографии, а точнее – решение криптографических проблем с помощью PC.

Дремучий консерватизм наверху и реальное понимание внизу – вот краткая характеристика отношений к PC в конце 80-х годов. А, впрочем, почему только в конце 80-х? Разве мало было затем предложений запретить использование импортного программного обеспечения? Спустя почти 20 лет по-прежнему какой-нибудь депутат иногда выступает с таким предложением. Чудесные люди! «Windows для чайников» – в массы!

Кроме того, учитывая универсальность задач, которые можно решать с помощью персонального компьютера, многие сразу же поняли, что это потенциальный «запасной аэродром» на случай каких-то непредвиденных перемен в тихой и спокойной жизни государевых криптографов. Ведь специальность криптографа весьма экзотическая, так ли легко будет найти другую работу в случае каких-то катаклизмов? Раньше, во времена полного господства государственной собственности, зарплата офицера КГБ была в среднем в 2 раза выше, чем у обычного инженера, но вот появились кооперативы, первые частные предприятия, на которых те же инженеры, не обремененные доходящей иногда до абсурда воинской дисциплиной, стали зарабатывать намного больше офицеров КГБ. Так что у высокого начальства был еще один повод опасаться PC: с ними слишком вольнолюбивыми могут стать подчиненные офицеры-математики, будут заглядываться на сторону. Как тут не вспомнить степановскую теорию патриотизма к отделу!

Вадим Евдокимович Степанов внезапно умер. Еще в пятницу я с ним здоровался, а в понедельник утром сообщили эту трагическую новость. Тромб сердечных кровеносных сосудов, почти мгновенная смерть. Это был, несмотря ни на что, человек, своим интеллектом и образованностью сильно выделявшийся среди остальных, даже среди начальников 8 ГУ. Его кончина не могла не вызвать перемен в жизни 5 отдела, административная удавка, которой он сдерживал многих, ослабла. Это сказалось, в частности, на мне: без лишнего шума, опять-таки, особо и не интересуясь моим мнением, меня отправили в другой отдел с повышением, на должность заместителя начальника отделения. Но тут уже я сильно не переживал, после

того насилия, в результате которого меня лишили возможности остаться в Высшей Школе КГБ, я был готов свалить из 5 отдела куда угодно.

Глава 3

Верхи не могут, низы не хотят…

Если какой-то человек обманывает тебя один раз, то начинаешь испытывать к нему недоверие, в другой раз – теряешь всякое уважение, а в третий – посылаешь вдогонку могучему русскому языку, не всегда печатаемому, и больше не имеешь с ним никаких дел.

А если обманывает государство и безраздельно правящая в нем КПСС? Послать, конечно, тоже можно, но больше не иметь с ними дел – невозможно. «Жить в обществе и быть свободным от общества нельзя. Всякая свобода в буржуазном обществе есть лишь замаскированная (или лицемерно маскируемая) зависимость от денежного мешка, от подкупа, от содержания» - В.И. Ленин, цитирую, как помню, работа называется, кажется, «Партийная организация и партийная литература», а номер тома и страницу в ПСС пусть читатель, если захочет, найдет самостоятельно.

В Советском Союзе нельзя было быть свободным от съездов КПСС, политинформаций, газеты «Правда» и выступлений Генерального секретаря ЦК КПСС. Ложь, ложь и еще раз ложь, безответственная, иногда вызывающе нахальная, настырная, навязчивая.

- Что будет бесплатным в 1980 году?

Это было в одном из первых моих школьных учебников. Там же, с картинками, давался ответ:

Жилье
Санатории и дома отдыха
Транспорт (нарисованы корабли, поезда и самолеты)
Городской транспорт (автобусы, троллейбусы, трамваи, метро)

И много чего еще было понарисовано в этой школьной книжке.

- Когда Продовольственная программа должна дать первые результаты?

А это уже посовременней, 1981 год, вопросы к ОПА (общественно-политической аттестации), посвященной недавнему Пленуму ЦК КПСС, на котором с большой помпой была принята Продовольственная программа. Тут же ответ: «Уже в этом году». Так сказал на Пленуме товарищ Леонид Ильич Брежнев.

Все видели эту ложь, мысленно посылали по известному направлению ее авторов, но делали вид, что все нормально, так оно должно и быть. Да просто дела не было большинству людей до всех этих руководителей и их очередных насквозь лживых высказываний. Верхи живут своей жизнью, а низы – своей: очередями в магазинах за колбасой, в которой половина бумаги и крысиного мяса.

Но раздражение копилось. Одна и та же ложь день за днем, месяц за месяцем, год за годом надоедала до изнеможения, жизнь беспросветная, трудная, не вызывающая никаких эмоций, только борьба за существование. Злость накапливалась долгое время и наконец, как и должно было случиться, полезла наружу. Горбачев попытался чуть приоткрыть клапан, стравить самое большое раздражение, но система моментально пошла вразнос, сметая все партийные инструкции.

Началось с гласности. Все давно привыкли к скучным и однотипным газетам и журналам, телевизионным новостям в программе «Время». «Бенефис Брежнева и немного о погоде» - так прозвали главный телевизионный информационный канал. И вдруг при Горбачеве начали появляться совсем другие статьи и новости: то статья экономиста Николая Шмелева «Авансы и долги» в журнале «Новый мир», посвященная разваливающейся социалистической экономике, то телевизионная программа «Взгляд» со ставшими впоследствии весьма известными молодыми людьми, которые говорили с экрана нормальным человеческим языком, то завоевавший жуткую популярность журнал «Огонек», где поведали то, о чем раньше только шептались. Политизация произошла мгновенно. В 5 отделе были раскопаны стенографические отчеты древних съездов ВКП(б), еще с выступлениями оппозиции, и они начали бурно обсуждаться вместо традиционных тем о том, кто каким станет начальником.

Приоткрылась завеса о том, что представляет из себя система КГБ и ее прошлое. Ведь когда в 1974 году я решился поступать в Высшую школу КГБ, то практически ничего этого не знал. Были, конечно же, какие-то обрывочные сведения о том, что в 30-х годах были репрессии, потом партия (имя Хрущева при этом не упоминалось) их осудила и после началась не жизнь, а сказка: Запад загнивает, а мы процветаем и идем к

светлому будущему. Давно бы уже дотопали, если бы не плохая погода да козни империалистов и их приспешников-диссидентов, вроде Сахарова и Солженицына.

А о том, что потери от репрессий сопоставимы с потерями в Великой Отечественной войне – ни слова. Что многие выдающиеся советские ученые – Королев, Вавилов, Туполев, Тимофеев-Ресовский – сидели в сталинских лагерях, что после революции была фактически уничтожена интеллигенция – тоже ни слова. И велика в этом «заслуга» ВЧК-КГБ, той организации, в которой приходится теперь служить. Хотя криптографы никогда не были «истинными» чекистами, но их влияния избежать невозможно, это было очевидно. По-другому стали восприниматься все повседневные проблемы, различные действия начальников, приказы, идущие с самого верха. Как относится к такому, на первый взгляд, весьма рутинному приказу, как приказ по КГБ о стаже и выслуге лет сотрудников? А в нем перечень сталинских лагерей, служба в которых засчитывается в стаж теперь, в конце 80-х годов: Воркута, Магадан, Колыма… И ты еще должен поставить свою подпись, что ознакомился с этой документальной географией ГУЛАГа, как бы согласен: да, нужна выслуга лет охранникам и вертухаям тех лагерей, где сгноили миллионы человеческих жизней.

Начальники все время пытались как-то сдерживать эти порывы, но скорее достигали обратного результата. Перед первыми свободными выборами народных депутатов, когда Ельцин баллотировался от Москвы, во всех отделах провели собрания, зачитали закрытое письмо ЦК КПСС, смысл которого сводился к одному: не голосуйте за Ельцина. Результаты голосования по закрытому избирательному округу, который составляло общежитие Высшей школы КГБ: за Ельцина – около 90%.

Сталинские времена безвозвратно ушли. Молчать и скрывать свою точку зрения уже никто особо не стремился, все неуклюжие действия различных парткомов, типа добровольно-принудительного участия в демонстрации «трудящихся» в честь праздника Великого Октября, открыто осмеивались и чуть ли не половина людей их попросту игнорировала. И это в 8 управлении КГБ, где все офицеры и коммунисты, где с раннего возраста все время вдалбливали: в первую очередь нам нужны хорошие офицеры, а потом уже – хорошие специалисты. Но тут очень четко срабатывал один из основных постулатов марксистско-ленинской философии: не указания начальства, а бытие определяет сознание. За что боролись, на то и напоролись. Лапшу на уши можно вешать людям недалеким, а если у тебя есть хорошее образование, заложенное прекрасными специалистами-преподавателями, то невольно привычка строгого математического анализа распространяется и на всю окружающую тебя действительность, начинаешь, по привычке, требовать доказательств, строишь контрпримеры, пытаешься все уяснить и во всем разобраться, хочешь иметь свою, осознанную точку зрения. Да так и к экзамену по ТВИСТу всегда готовились.

Вот, например, Горбачев все время говорит общие слова о демократии, а потом вдруг предлагает, чтобы первый секретарь партийного органа (райкома, обкома и прочего …кома) автоматически становился во главе соответствующего Совета народных депутатов. Доказательство такой необходимости – невнятное, неубедительное, неочевидное, за такое доказательство (да и теорему тоже) его бы с экзамена по алгебре или ТВИСТу быстро бы вынесли прямиком в Советскую Армию. А предложение назначать без выборов депутатов от КПСС? Явное противоречие с аксиомами демократии.

Потом, чуть позже, стало ясно, что за люди окружали Михаила Сергеевича. На снимке - самый первый лидер вновь образованной Коммунистической партии Российской Федерации закрыл голову волосатой рукой, а на ней татуировка: «Ваня». Математика тут бессильна.

Разные Кузьмичи правили великой страной, где, несмотря на все их старания, сохранилась еще интеллигенция, здравый взгляд на жизнь, оппозиционность власти. Оппозиция! Вот ключевое слово, гарантия от разных застоев, изгибов-перегибов, культов, антиалкогольных компаний. А в экономике – конкуренция. Если государство подмяло все под себя – это мыльный пузырь, все равно, что борьба за образцовый факультет в советское время – одна показуха, когда-нибудь обязательно лопнет. С таким государством можно сдать разве что экзамен по Истории КПСС. Если есть реальная оппозиция в политике и конкуренция в экономике – это свидетельство реальной прочности государства, с таким не страшно идти на алгебру или ТВИСТ.

Но в России все повторяется. В том числе и История КПСС.

Глава 4
Криптографические верхи не хотят, а низы не могут…

Кибернетика – буржуазная лженаука – вылезла из своего змеиного гнезда и в конце 80-х годов поползла травить своим ядом чистые умы математиков Спецуправления 8 Главного Управления КГБ СССР. Увлечение персональными компьютерами приобрело повальный характер, причем начальный игровой этап быстро прошел. Персональные компьютеры и программное обеспечение к ним были буржуазными, идеологически вредными, но очень удобными и доступными. Они произвели очередной взрыв в советском криптографическом омуте, но только гораздо более сильный, чем открытые ключи или схема DES. Людей невозможно стало оторвать от PC, теоремы и абстрактные споры - вторичны. Что делать криптографическому начальству?

Логичный ответ – создавать боевые шифры, реализуемые с помощью персональных компьютеров – отметаем не то, что с порога, а за много верст до него. Это с помощью персональных компьютеров наших

вероятных противников создавать военные шифры? Товарищ Сталин, слышите, что тут без Вас стало твориться в любимой Вами криптографии?

Ну а не военные? Например, коммерческие, как и американцы? Вроде бы и советский стандарт шифрования для этого сделали?

У меня есть своя точка зрения на то, для чего сделали советский стандарт шифрования. Как там говорил Никита Сергеевич Хрущев: «Покажем Кузькину мать Америке»? Кажется так. Долгое время в гонке вооружений между СССР и США действовал принцип: око за око, зуб за зуб. Сделали американцы новый стратегический бомбардировщик – дадим на него свой советский ответ. Сделали открытую криптосхему DES, взбудоражили советское криптографическое начальство, заставили его напрячься – получите в ответ советский открытый стандарт шифрования, слегка переделанный из вашего DES. Пусть теперь ваше криптографическое начальство напрягается! Вот вам наша криптографическая «Кузькина мать»! По крайней мере, если кто-то станет мне говорить, что тогда, в 1979 году, когда принималось решение о создании советского стандарта шифрования, заботились о коммерческой криптографии, то разрешите усомниться в такой трогательной и заблаговременной заботе о будущих российских банкирах.

Почти 10 лет создавали советский стандарт шифрования, в основном перестраховываясь от выдачи каких-то таинственных криптографических секретов. За эти 10 лет в стране много интересных вещей случилось, к концу уже зазвучали слова «перестройка», «хозрасчет», «гласность» и кое-что еще. Но мышление советского криптографического начальства по-прежнему оставалось идеологически кристально чистым: коммерческая криптография противоречит учению великого Сталина. А уж о том, чтобы с помощью «буржуазной лженауки» офицеры Спецуправления работали во благо каких-то коммерсантов, не могло быть даже самых отдаленных помыслов.

И вот, помимо воли начальства, в низах - повальное увлечение персональными компьютерами. Куда, в какое криптографическое русло его направить?

Первоначально, естественно, - на автоматизацию криптографического анализа советских балалаек. Пускай на PC считают различные статистики. Но очень скоро выяснилось, что импортные PC гораздо умнее советских монстров – ЭВМ, и на них можно делать намного более интересные криптографические задачи, а именно: использовать их в качестве шифровальной техники с практически неограниченными возможностями для реализации оригинальных криптосхем, для построения удобного интерфейса, для выработки ключей и т.п. А для чего и для кого? Кто будет конечным потребителем такой чисто программной продукции, использующей в качестве элементной базы стандартные персональные компьютеры зарубежного производства?

Начальство не могло дать на это никакого вразумительного ответа, только традиционные заклинания про криптографические результаты, которые сейчас «нельзя получить на кончике пера», имея в виду опять же использование PC для тупых задач перебора ключей или сбора статистики при анализе древних военных схем. А компьютерные фанаты плодились в Спецуправлении с ужасающей быстротой, это, в основном, были молодые ребята, закончившие Высшую Школу КГБ, и проводившие за компьютером все рабочее время, часто даже оставаясь и после работы. Необходимого выхода для их фанатизма тогда в Спецуправлении не находилось. Они находили себе друзей-программистов на стороне, в открытом мире, полулегально подрабатывали в появившихся коммерческих фирмах, но развернуться по-настоящему для создания серьезных коммерческих шифров, которые смогли бы быть конкурентоспособными на мировых рынках, никто так и не смог. Такое было невозможно в принципе во времена СССР.

Эти ребята вызывали у меня уважение и чувство зависти: они свои результаты видят на экране, могут их проверить и чуть ли не потрогать руками. А мои теоремы и методы криптографического анализа почти всегда абстрактны, удовольствия от их получения у меня в последнее время возникало все меньше и меньше. Тянуло в фанаты.

Глава 5

Фанат

Я наконец-то дорвался до компьютера! Еще первое знакомство с IBM PC XT привело меня в неописуемый восторг, стало ясно: вот именно то, к чему я привязался надолго, может быть на всю оставшуюся жизнь. Первый (игровой) этап обучения пройден, все чаще стало появляться желание реализовать все свои замыслы на PC. А это, в первую очередь, шифры на новой элементной базе, им было отдано почти десять лет жизни, появилась уверенность, какое-то подсознательное чувство, что на этом пути можно находить элегантные и очень надежные криптографические решения. С помощью PC легко сделать ключом случайную подстановку в шифре типа «Ангстрем-3», а тогда все мыслимые подходы к анализу такого шифра становятся невероятно трудоемкими, глухими, а все положительные качества – скорость и простота реализации – сохраняются. Такой регистр сдвига с неизвестной подстановкой можно использовать и для многих других криптографических целей, например, в качестве генератора случайных чисел или для функции хеширования.

Разные напыщенные начальники всегда вызывали у меня чувство неприязни, гораздо приятнее иметь дело со специалистами, людьми, отличающимися профессионализмом, преданностью своей

профессии, умом, талантом, настойчивостью. А тут самому пришлось стать пусть небольшим, но начальничком, у которого в подчинении свыше 20 человек. В условиях Спецуправления 8 Главного управления КГБ это значит только и делай, что руководи, давай указания, проверяй, ругайся, разделяй и властвуй. Ну уж нет, эта суета не по мне, я сам в такие начальники никогда не лез. Но должность маленького начальничка дала две неоценимые по тем временам вещи: свой, истинно персональный компьютер и отдельный кабинет, в котором кроме меня был еще один настоящий начальник, а я - его зам. Никакой кучи народа в комнате, никто не претендует на твой компьютер, начальник (настоящий) очень любит разделять и властвовать и избавил меня от этой напасти. Я остался наедине с PC, с самым что ни на есть персональным компьютером, в спокойной и почти уединенной обстановке, сам себе режиссер. Никакая сила уже не могла оттянуть меня от моей любимой игрушки.

Сначала я погрузился в язык Assembly. Какими-то правдами и неправдами был добыт оригинал книги Питера Нортона «Программирование на языке ассемблера» с кучей примеров. Толстенная книга, но когда наглядно видишь на экране, что все запрограммировал верно, результат совпал, появляется азарт. Методика одна и та же, что в математике, что в программировании: от простейших вещей ко все более и более сложным, стараясь не перескакивать через этапы и все досконально понять. Но программирование интереснее тем, что результат конкретен и нагляден, его можно чуть ли не потрогать руками, тогда как в математике теоремы абстрактные, в них очень легко упустить какую-то цепочку при доказательстве и не заметить, что движешься в неверном направлении. В программировании уход в сторону, какие-то непонятные «глюки» выявляются гораздо быстрее, этот процесс эмоционально более интересен.

Как изменилась жизнь! Вместо скучного досиживания до 6 вечера дежурный офицер чуть ли не насильно отгонял меня от компьютера в 9 вечера, когда объект закрывался. У меня был суперсовременный по тем временам Laptop с плазменным экраном, первое подобие нынешних Notebook, только без автономного питания, но размером почти такой же, чуть побольше. Его можно было даже засунуть в сумку – невероятно для тех времен, когда еще свежи были в памяти тапочки, надеваемые на сапоги в комнате, где стояло советское чудо вычислительной техники – «Рута-110». Поражали возможности: жесткий диск – 40 Мб, это же огромная величина! Сколько программ можно на него записать! 286 процессор – насколько более быстрый, по сравнению с IBM PC XT. Сколько же на нем всего напахать можно! Да здесь какой угодно шифратор сделать можно, не связываясь ни с каким заводом, все в твоих руках.

Заработали первые ассемблеровские программы: оказывается сравнительно легко сделать свои прерывания в DOS, программировать ввод-вывод, лазить по оперативной памяти. Наигравшись вдоволь с Assembly, я занялся его старшим братом – языком C, тогда еще без всяких плюсов.

Математик любит искать во всем логику, закономерности, разумность. Если ее не хватает в реальной жизни, то компьютер, операционная система, языки программирования дополняют этот дефицит, служат своего рода отдушиной, тем сказочным миром, который помогает легче переносить уродливость мира реального. Следовательно, чем более иррациональным будет повседневное бытие, тем больше будет тяга к компьютеру, к его удивительно логичному и разумному поведению, осмысленным действиям, внутренней логике, виртуальной действительности. Там нет тупых и невежественных генералов, очередей за мясом, совхозов и овощебаз, общественной работы и субботников, там только четкие и понятные критерии, TRUE и FALSE, единица и ноль. А специалист по компьютерам, хороший программист всегда будет востребован, при любом правителе, любой идеологии, любых начальниках. Отсюда уже недалеко и до свободы, до реальной свободы, когда пропадает этот инстинктивный трепет перед важными надутыми начальниками, не освоившими толком даже компьютерных игр.

Сидящий напротив мой начальник все время гадал: сколько нужно времени, чтобы я «сломался», ну или хотя бы мне надоел компьютер: месяц? полгода? год? Своего рода приложение к теме «Экстракт». Но все его прогнозы оказались с «глюками», компьютер засасывал меня все больше и больше. После того, как были запрограммированы и отлажены алгоритмы, реализующие шифры на новой элементной базе, захотелось сделать к ним удобный интерфейс. Ну а это уже такой простор, просто вселенная! И еще, конечно же, хотелось, чтобы мой компьютерный фанатизм принес кому-то реальную пользу, чтобы моими программами пользовались, чтобы вся эта огромная работа не пропала даром. А вот это уже в системе Спецуправления 8 ГУ КГБ СССР сделать было намного сложнее, ибо там с незапамятных времен действовали негласные правила: не высовывайся! будь как все! не проявляй лишней инициативы, она наказуема! Короче, в триаде чиновник-офицер-специалист можно было спорить только о том, что поставить на первое место: чиновника или офицера. В дальнейшем сама жизнь присудила золотую медаль (с зеленью) чиновнику, а все недовольные таким раскладом специалисты попросту разбежались кто куда. Тогда же, в конце 80-х годов, у меня еще была какая-то наивная вера в справедливость, в то, что эта система способна адекватно воспринимать те компьютерные программы и усилия по их внедрению, которые стали моим призванием, всем смыслом жизни. Как говорил Александр Солженицын, тоже, кстати, имевший отношение к криптографии, «Бодался теленок с дубом».

Глава 6

Умножение и деление

Помимо всяких идей и размышлений, человек должен еще каждый день питаться, что-то кушать, чтобы не протянуть ноги от одной духовной пищи. 90-91 года – это то время, когда очевидность этого утверждения стала проявляться особенно остро, а подземное бомбоубежище в стекляшке, основном здании Спецуправления 8 ГУ КГБ СССР, быстро превратилось в картофелехранилище. Пошел натуральный обмен: Спецуправление заключило с каким-то совхозом то ли явный, то ли неявный Договор, по которому обязалось поставлять совхозу бесплатную рабочую силу в виде офицеров Спецуправления для уборки урожая, а совхоз за это рассчитывался натурой – картошкой, капустой и еще какими-то нехитрыми сельхозпродуктами, которые закладывались на хранение на зиму в находящееся в подвале стекляшки бомбоубежище. Перезимуем!

Сейчас уже трудно сказать, насколько реальны были страшилки про возможный голод, про отсутствие государственных продовольственных запасов, которые регулярно распускались у нас в отделе на самом что ни на есть официальном уровне. То ли это была очередная пропаганда, призванная оправдать выделение людей в совхоз, то ли сермяжная правда, рассказ о которой должен лишний раз напомнить – не расслабляйтесь! Скорее всего, и то, и другое в одном флаконе. То, что положение в стране действительно тяжелое, было ясно и без всяких начальников.

Глупая антиалкогольная компания лишила бюджет одного из весьма существенных источников дохода, причем меньше пить русский народ все равно не стал. Сразу же пропал сахар, конфеты-карамельки, дрожжи и прочие ингредиенты, а также кастроли-скороварки, с помощью которых изготавливаются различные сорта самогона, «изюмовок» и «табуретовок». Это стало общенациональным народным промыслом, ушедшим в плохо скрываемое подполье. Зато впервые после войны появились талоны: на водку, на сахар, на табак, т.е. процесс приобретения этих товаров стал вдвое сложнее: сначала в ЖЭКе по месту жительства надо, отстояв огромную очередь, получить талоны за очередной месяц, потом в магазине, уловив момент, когда там «выкинут» товар, эти талоны еще и отоварить, естественно, тоже не без очереди.

Прочие товары постепенно тоже стали пропадать. Мука, различные крупы, не говоря уже о традиционно дефицитном мясе, как-то незаметно тоже стали дефицитными, их тоже нужно было «доставать», «хватать», ждать, когда «выкинут». Бакалейные отделы в магазинах подтянулись до уровня мясных в том смысле, что стали такими же пустыми. Доступным товаром оставался только хлеб, но и с ним иногда возникали перебои.

Но ведь ничего существенного в СССР за последнее время не произошло: не было ни войны, сравнимой по масштабам с Великой Отечественной, не было каких-то общенациональных стихийных бедствий, не считая антиалкогольной кампании. Куда же все подевалось?

Да ничего никуда не девалось. Не было никогда в СССР никакого изобилия, только Москва была показушной витриной первого в мире социалистического государства, а чуть подальше от Москвы, километров 100-200 – пустые прилавки. И существовало это самое передовое и самое справедливое в мире государство исключительно за счет богатейших природных ресурсов, в первую очередь нефти. Советская промышленность могла производить только военную технику, так повелось еще со времен Отца всех народов: мы в капиталистическом окружении, осажденной крепости, все для фронта, все для победы! А легковые машины, например, в СССР были огромным дефицитом, купить «Запорожец», «Москвич» или – предел мечтаний – «Жигули»-копейку для многих было несбыточной мечтой. Запчасти для автомобилей при социализме – это вообще гимн социализму и всей его автомобильной промышленности. Практически все необходимое – только по предварительной записи и только тем, у кого есть различные льготы, да и то сначала надо дожидаться несколько месяцев заветной открытки, извещающей о том, что очередь подошла, затем бежать сломя голову с этой открыткой через весь город за масляным фильтром, аккумулятором, покрышками и прочим дефицитом, без которого на автомобиле ездить невозможно.

В нормальной цивилизованной стране на первом месте стоит производство, приумножение общенационального богатства. Это в нормальной, а что же в СССР? Деление, распределение всех природных ресурсов, в первую очередь нефти, денег, полученных от ее продажи на западных рынках, раздача всех благ, и часто не по заслугам, а по принципу современной сороки-белобоки:

- Этому дала – он дров нарубил,
- Этому дала – он воды наносил,
- Этому дала – он и дров не рубил, и воды не носил,

  Но зато за него сам директор просил

Те страны, где операция умножения национального богатства стоит на первом месте, стабильны и мало зависят от каких-то политических баталий. Например, Италия: в 80-х годах там неоднократно происходили смены правительств, но качество итальянской бытовой техники – холодильников, стиральных машин, автомобилей, а также одежды, обуви, продуктов и прочая, прочая, прочая от этого почему-то не пострадало. Правительство (и его частые смены) – само по себе, а экономика – сама по себе. Просто в этой и многих других западноевропейских странах на первом месте стоит операция умножения, приумножения национального богатства путем производства качественных товаров народного потребления. А в СССР на первом месте всегда стояла и до сих пор стоит операция деления, распределения тех легких доходов,

нефтяных денег, которыми Бог наградил СССР, но которые не приносили и до сих пор не приносят счастья или хотя бы просто нормальной цивилизованной жизни советским, а затем и российским гражданам. Меняются лозунги, правители, стоящие на верхних этажах власти авторитеты, а деление, распределение нефтяных денег по-прежнему остается основным стимулом любых значимых усилий советской (российской) экономики. И такая экономика, точнее, экономика в кавычках, перевернутая с ног на голову, в которой большинство простых людей являются не производителями общенационального богатства, а потенциальными конкурентами на его большую нефтяную часть, не может не зависеть от борьбы за контроль над нефтяной трубой, завуалировано называемой в нашей стране политикой. Целью этой борьбы является не общее благо, не новые технологии, не развитие производства, а властная вертикаль, место под солнцем, в первую очередь поближе к нефтяным деньгам и их распределению.

В конечном итоге вся политическая борьба в СССР и в России всегда сводилась не к конкуренции каких-то идей, а к банальному выяснению «Кто кого главнее», кто будет издавать царственные Указы, у кого будет больше прав распределять национальное российское богатство. Народ при такой борьбе превращался как бы в болельщиков на стадионе: можно пошуметь и покричать, выпустить пар, но реально решать, кому стать затем нефтяным олигархом, а кому – работягой на полудохлом заводе, на котором месяцами не платят зарплату, будут правители, верховные делители природных богатств. Правители могут меняться, но стимулы, которыми они руководствуются, - нет, слишком много легких нефтяных денег. И не нужны такой системе никакие новые технологии, нетривиальные решения, научно-технический прогресс – нефтяных денег на наш век хватит.

Но любая смена правителей при такой системе – это смена владельца природных богатств, нефтяной трубы, крана, ее перекрывающего, и разделяющего людей на «плохих» и «хороших». Такая смена никогда не бывает безболезненной, здесь возможны всякие чудеса. И одно только желание: чтобы прошла подобная смена в верхах как можно спокойнее, без стрельбы и танков на улице, без истерики по поводу «завоеваний Великого Октября».

Борьба за контроль над операцией деления при брежневской Советской власти проходила тихо, кулуарно, о ее ходе многие могли судить лишь по косвенным признакам: в каком порядке вожди стоят на трибуне мавзолея, сколько раз упомянули имя члена Политбюро ЦК КПСС в газете «Правда», кто с кем пошептался в президиуме очередного торжественного заседания. Довольно скучные признаки, мало в них было азарта, напора, художественной выразительности. То ли дело во времена Горбачева и провозглашенной им перестройки - на всю страну по телевизору: «Борис, ты неправ!». Тут же появились в киосках значки с портретом Ельцина и подписью «Егор, ты неправ!». Меньше хлеба – больше зрелищ, такой была повседневная действительность в СССР в конце 80-х годов. Все бы хорошо, зрелища – интересная штука, да вот только бедная операция умножения, производство всего необходимого людям для повседневной жизни, загибалась при этом прямо на глазах. Даже убогие, советского производства телевизоры, холодильники, стиральные машины, мебель, одежда, обувь, не говоря уже о продуктах, стремительно исчезали из свободной продажи. Получалась цепная реакция: люди, занятые в производстве, вынуждены были в основном думать о том, как раздобыть самое необходимое для своего существования, как и где достать, урвать, выстоять, выстрадать какой-то жизненно необходимый минимум, как не пропустить свою долю во всеобщей операции деления.

Противное ощущение оставалось тогда от всей обстановки в стране. Видно самым что ни на есть невооруженным взглядом, что образование, интересная работа, желание делать что-то полезное – это анахронизм, надо всеми силами пробиваться к кормушке, к благам, к дефициту, заводить нужные связи, «дружить» с тупыми и никчемными людьми, ворочающими реальными социалистическими ценностями. Но это же противно! Один вид продавщиц из универсама, кидающих в толпу пакетики с колбасой, вызывал омерзение, а ведь это был самый низший уровень «делителей». Чуть повыше – их начальники и начальницы, все время сидящие на своих рабочих местах в дефицитных ондатровых шапках, подчеркивающих их важность. Офицеры Спецуправления, выделяемые на доставку продовольственных заказов в Новоарбатский гастроном, могли воочию понаблюдать этот сорт торгового люда, у которого в стране была реальная власть.

Но это внизу. А наверху делили (естественно, между собой) бабки побольше, иногда упоминая при этом «социализм с человеческим лицом», а иногда – «демократию, свободу и права человека». Делили, делили – не поделили.

Вот так и революция подоспела. Августовская, 1991 года.

EXECUTE!

- Зайди в 631 комнату, там Сережа чай раздает.

Советские магазины в 1991 году – это гимн развитому до предела социализму! Теннисные корты, только сеток не хватает: огромные по площади универсамы, когда-то служившие местом столпотворения народа, обезлюдели, пустые товарные полки убрали за ненадобностью, стало вольно и просторно,

занимайтесь спортом, граждане, и забудьте вы об этой гнусной еде. Делайте пробежки, берите, как советовали газеты, «энергию из свежего морозного воздуха», а всякое мясо и прочая калорийная пища – это злейший враг, и мы его победили!

Почти все продукты – только по талонам или через заказы на предприятиях. Здание Спецуправления 8 ГУ КГБ СССР превратилось в перевалочную продуктовую базу, во всех отделах выделены комнаты, где раздают продуктовые заказы. Так было давно, все время, что я там работал, только если раньше, год-два назад, в этих заказах были, в основном, «деликатесы» (по советским понятиям), то теперь – все что съедобно: картошка, крупы, консервы, а также соль, чай, мыло и спички. Хочешь мира – готовься к войне, запасайся, кто может!

Давно забыты те времена, когда кто-то не брал заказов. Теперь всем все нужно, деньги стремительно обесцениваются, копить их нет никакого смысла, а тратить в магазинах не на что. Как распределять те продуктовые крохи, которые выпадали в отделение? Естественно, поровну. А как разделить поровну на 20 человек пачку чая весом 200 грамм? И вот появляются аптекарские весы, на которых каждому отвешивается по 10 грамм чая. Развешивает в 1991 году – офицер КГБ, майор, специалист с высшим образованием, закончивший Высшую Школу КГБ. Эта картинка навсегда осталась в моей памяти, это – апофеоз социализма, финал его существования, ради которого миллионы людей отдали все свои силы и даже жизни. Нет, определенно, что-то будет, а вот что именно, никто ничего не знал. Но готовились, как всегда, к худшему…

Глава 1

17 пунктов

- Это коммунистический путч и он потерпит поражение!

Я не верил своим ушам. Еще только вчера объявили о создании ГКЧП, перекрыли все информационные каналы: газеты, радио, телевидение, а сегодня, 20 августа 1991 года в здании КГБ по своему обычному транзисторному приемнику на средних волнах я могу слышать такие слова! И это не какой-нибудь «Голос Америки», а самая что ни на есть советская радиостанция «Эхо Москвы». Впервые прозвучали такие резкие слова, что это значит? Видно, что-то совсем не в силах коммунистическая система, стремительно пошел ее развал, аксиомы и постулаты, казавшиеся вечными, рухнули в один миг. Публика, объявившая о создании Государственного Комитета по Чрезвычайному Положению, явно упивалась театральными эффектами и не знала, что делать дальше. И почти такой же театр был в Спецуправлении 8 ГУ КГБ СССР.

Утром 19 августа всех руководителей отделений собрал у себя в кабинете начальник отдела, объявил о ГКЧП и сказал, что у нас вводится усиленный режим несения службы: уходить домой можно только после специального разрешения руководства, дома всегда быть доступными, не занимать домашний телефон посторонними разговорами, быть готовым к срочным вызовам на службу. Традиционные и даже ритуальные заклятия, такие вещи уже приходилось слышать не раз, но здесь ситуация иная. Чрезвычайное положение объявлено неожиданно, объявили его люди, утверждающие, что Горбачев серьезно болен и не может выполнять свои функции, а это весьма неочевидно. Что у них на уме, насколько правомочны их действия, почему мы должны безропотно им подчиняться – вот куча вопросов, которыми сразу же закидали начальника отдела. Самое главное требование было одно – все приказы и разъяснения по поводу ГКЧП отдавать в письменной форме. Весьма логичное требование. «Разъяснения будут» - пообещал начальник отдела, хотя мало кто в это поверил. Всем уже не раз приходилось бывать в так называемых «оперативных нарядах», типа того, что был в 1980 году во время московской Олимпиады, и все четко представляли себе ту неразбериху и бестолковщину, которой неизбежно сопровождалось участие математиков в подобных шоу-представлениях. Но одно дело наблюдать на Олимпиаде за собачкой, мирно писающей на японскую копченую колбасу в фойе гостиницы «Космос», и совсем другое – выступать на защиту каких-то сомнительных личностей, решивших провозгласить себя «спасителями» отечества от своего собственного народа.

Но письменные разъяснения неожиданно появились. Утром 21 августа с пометкой «Ознакомить личный состав» на нескольких страницах были приведены 17 пунктов разъяснений текущей ситуации. Были ли эти разъяснения спущены сверху или являлись плодом возбужденной фантазии наших местных генералов – сказать сейчас трудно. Похоже, что все-таки местная инициатива, но смысл был один и тот же, что и везде в КГБ: поддержим ГКЧП в наведении порядка в стране. Только жизнь-то развивалась гораздо стремительней генеральских бумаг: в то время, как эти 17 пунктов были получены у нас в отделении, по радио уже шли такие передачи, из которых было ясно, что дело ГКЧП проиграно. И буквально полдня спустя – новая

директива руководства: немедленно вернуть все бумаги с 17 пунктами назад, чтобы никто не догадался о поддержке ГКЧП. Это называется марксистско-ленинская диалектика!

Коммунистическая система сломалась за три дня. Такое событие удается наблюдать лишь раз в жизни! Кухонные сплетни и анекдоты брежневских времен, еле двигающие языком генсеки, тотальный дефицит, наглые продавщицы, кидающие пакеты с колбасой в толпу, непросыхающие колхозы-совхозы, партийные секретари, пропагандисты и политинформаторы, антиалкогольная компания и разные Кузьмичи, чай, развешиваемый аптекарскими весами, и талоны на продукты - все это капля за каплей переполняли считавшуюся бездонной бочку народного терпения. И вот - лопнуло, прорвало, понеслось, сметая на своем пути памятники коммунистическим вождям и коммунистических активистов.

А офицеры Спецуправления 8 ГУ КГБ СССР при этом ждали, когда их с шифрующими автоматами наперевес, под красным флагом и с криками «За ГКЧП! За Янаева!» бросят на штурм Белого дома, или что-то в этом роде. И это ожидание привело к тому, что буквально на следующий же день после провала путча начальника 8 ГУ КГБ СССР завалили рапортами об увольнении. Даже в КГБ терпение людей иссякло.

Мне уже тоже порядком надоела эта контора. Всю жизнь, как сознательный чиновник, я в ней точно торчать не буду. Если бы было куда – свалил бы прямо сейчас, но с компьютером я совсем потерял голову, просиживая около него целыми днями, не задумываясь больше ни о чем ином. Конечно, теперь у меня есть за плечами основательная компьютерная грамотность и даже, наверное, побольше этого. Но чтобы свалить из КГБ надо иметь еще место, куда свалить, каких-то влиятельных друзей в открытом мире, да и просто какой-то опыт работы не в закрытой, а в вольной организации, где свои правила, свои нравы, где есть конкуренция и зарплата зависит от выполненной работы. Обо всем этом у меня было очень смутное представление, служба в закрытой структуре КГБ – это своего рода искусственный инкубатор, птенцы которого часто не имеют ни малейшего понятия о жизни на общем птичьем дворе. Да еще к тому же недавно вышел закон о статусе военнослужащего, по которому офицер, отслуживший 20 лет, получал право на офицерскую пенсию. Для меня эта лафа наступит только в далеком 1994 году, это еще целых три года! А вдруг все-таки как-то удастся проторчать здесь до этого времени, тогда хоть не так жалко будет лучшие молодые годы, отданные службе в КГБ.

Только отношение к начальникам теперь стало уже совсем другое. Исчез священный трепет перед генералами, они, вон, сами теперь, после своего выступления «мимо цели» во время путча, попрятали головы в песок, разом спала спесь и надутость, заговорили человеческим языком: «Надо развивать коммерческую криптографию, вы же умные ребята, надо бороться за рынки, за заказчиков». Эка их понесло! Это, наверное, напугали слухи о том, что разгонят контору под горячую руку, тогда придется и о хлебе насущном подумать. В открытую стало поддерживаться создание подконтрольных коммерческих фирм и заключение с ними от лица Спецуправления различных договоров, сулящих финансовые дивиденды. Пошел стихийный раздел рынка сбыта криптографической продукции…

Ровно в полночь на стрелку слетелась братва
Продинамить никто не решился
Перетерли вопрос про четыре ларька
Но консенсус пока не сложился…[1]

Но где-то примерно к маю 1992 года испуг прошел, новое демократическое правительство вывело всю шифровальную службу из системы КГБ (уже переименованной к тому времени), обозвало ее ФАПСИ – федеральное агентство правительственной связи и информации - и посадило во главе ФАПСИ такого директора, в котором недоразбежавшиеся офицеры Спецуправления сразу же почувствовали твердую руку, способную навести порядок и выправить допущенные за последние полгода перегибы и искривления Генеральной линии. Он сразу же получил прозвище «папа». А уж в коммерческой криптографии политика стала совсем ясной и понятной. Как там говорил медведь из детской сказки?

- Все шишки в лесу - мои!

---

[1] Песня времен гражданской войны 90-х годов в исполнении группы «Профессор Лебединский»

Глава 2

Криптоцентр

- Толя, я не знаю в Спецуправлении ни одного человека, который бы хорошо о тебе отзывался.

Славик был опытным человеком, успел побывать советником в Афганистане и сейчас работал в нашем отделении. А говорил он так о К., инженере тоже из нашего отделения, но человеке достаточно странном и уж явно не из выпускников 4 факультета.

Где-то в 85 или в 86 году молодые ребята во главе со Славой решили сделать шифратор на базе портативного микрокалькулятора «Электроника МК-85», который серийно выпускался на заводе «Ангстрем» в Зеленограде. Какую выбрать криптосхему для такого шифратора, учитывая, что ресурсы калькулятора (память и скорость процессора) крайне ограничены? Само собой разумеется, что не американо-советского крокодила DES-ГОСТ, это все равно, что двигатель от танка пытаться в горбатый «Запорожец» поставить. Они пришли в Теоретический отдел (в то время я еще был там), где им рассказали про шифратор «Ангстрем-3» и как в нем нужно выбирать параметры. Эта схема их вполне устроила и модернизированный «Ангстрем-3» лег в основу программы, предназначенной для реализации с помощью калькулятора «Электроника МК-85». Эту программу надо было записать в ПЗУ калькулятора вместо серийной программы, предназначенной для бытовых целей. Запись и перепайка серийного ПЗУ была возможна только в заводских условиях, да и к тому же немного изменился дизайн и название клавиш на панели, поэтому нужен был человек, который возьмет на себя эту гнуснейшую функцию: связь с советским заводом конца 80-х годов.

Таким «заводским толкачом» стал К., человек, не имевший специального криптографического или математического образования, не бывший никогда офицером, но обладавший иными качествами, которые мне, к сожалению, пришлось познать позже на своем горьком опыте. А по части отношений с людьми Слава был намного опытнее меня, но его словам о К. я, к сожалению, не придал тогда значения.

Модернизированный калькулятор назвали «Электроника МК-85 С». Он уже не выполнял никаких функций калькулятора, но в него можно было ввести секретный ключ длиной 100 десятичных цифр и с его помощью осуществлять симметричное зашифрование и расшифрование текстовой или чисто цифровой информации, вводимой с клавиатуры, а шифровка или открытый текст высвечивались на экране. Никакие периферийные устройства, кроме сетевого адаптера, к этому калькулятору не подключались.

Этими калькуляторами изначально предполагалось оснастить Советскую Армию, где долгое время использовались очень громоздкие и неудобные переговорные таблицы, предназначенные для засекречивания переговоров на низовых уровнях: отделение, взвод, рота. Но постепенно планы использования «Электроники МК-85С» все разрастались и потребовалась программная реализация этого калькулятора на персональном компьютере, а также программная система для выработки секретных ключей к калькулятору.

К. был в нашем отделении и, следовательно, формально находился у меня в подчинении. Но он не был офицером, к тому же подробности его работы «заводским толкачом» мне были абсолютно неинтересны, они, как я понял позже, сводились в основном к шушуканью с «нужными» людьми, не всегда, естественно, бескорыстному. Как специалист он был никакой, не мог сам написать или даже грамотно проверить написанную кем-то программу, о криптографии имел представление на уровне солдата из части радиоперехвата, где когда-то служил и, по его словам, красил траву перед приездом в часть генералов-начальников 8 ГУ КГБ. Но у него были те качества, которыми не обладало большинство людей в Спецуправлении: пронырливость, хитрость, жадность, легкость, с которой он раздавал направо-налево различные обещания, а потом обязательно под разными предлогами обманывал связавшихся с ним людей, полное отсутствие такого понятия, как честь и доброе имя в глазах окружающих. На понимание этих простых житейских фактов у меня, к сожалению, ушло несколько печальных лет общения с этой мерзкой личностью.

Но поначалу мне даже нравилась его активность. К. выделался из общей полусонной массы людей, всегда куда-то спешил, был все время «при деле», производил впечатление делового человека, полного грандиозных замыслов. Казалось, сам бог велел мне попробовать вылезти из КГБшного инкубатора через общение с ним. Какое мне дело до его темных сторон, программировать я научился, теперь пора учиться свои программы рекламировать и продавать, чтобы они не оставались «вещью в себе», а реально работали и приносили взаимное удовлетворение разработчику и потребителю.

Первыми на свет божий появились программные реализации калькулятора «Электроника МК-85С» и системы выработки секретных ключей к нему. На идею программы выработки секретных ключей меня натолкнули женщины нашего отделения. В Спецуправлении работали, в основном, мужчины, и для того,

чтобы коллектив не становился чрезмерно «мужским», начальство старалось в каждой рабочей комнате держать по крайней мере одну женщину. Их функции сводились, в основном, к техническим операциям: подготовкам отчетов, программированию каких-то простых задач и, естественно, раздаче продовольственных заказов, соблюдению очередности дежурства «по заказам» и тому подобное. С появлением компьютеров их основным времяпровождением в нашем отделении стала одна из самых первых и очень популярных компьютерных игр TETRIS. Но ведь это же готовый генератор случайных чисел! Моменты времени при нажатии на клавиши во время игры – это и есть случайная последовательность, которую можно использовать для генерации секретных ключей для «Электроники МК-85С».

Сказано – сделано. Несложно было подготовить простенькую программку, которая фиксировала моменты времени при нажатии на клавиши и затем я, руководитель отделения, стал просить женщин в рабочее время играть в TETRIS: для проверки генератора надо было набрать статистику вырабатываемых знаков и просчитать ее характеристики. Просчитали: все нормально, практически случайное и равновероятное распределение.

Но все-таки калькулятор «Электроника МК-85 С» был весьма примитивным устройством, разрабатываемым для низовых звеньев Советской Армии. Его первоначальная программная реализация тоже не отличалась богатством функциональных возможностей: зашифровать и расшифровать, результат выдать на экран, такие программы для меня уже были неинтересны. Ведь возможности компьютера позволяли реализовывать практически все мыслимые в то время криптографические фантазии, я уже почувствовал вкус к программированию, к хорошему и удобному интерфейсу, была огромная жажда сделать что-то свое, нетривиальное, но в то же время понятное для пользователя, даже самого непросвещенного в криптографии. Например, используя в качестве прототипа популярный интерфейс типа Norton Commander, сделать систему шифрования и электронной подписи файлов, заложить туда возможности как симметричного, так и асимметричного шифрования, ввести систему выработки секретных и открытых ключей, а также учет использования криптографических функций. Такую систему естественно было назвать *Криптоцентр*.

Это был конец 1991 года. Жуткое время: магазины пустые в самом что ни на есть прямом смысле этого слова, вечно полуголодное состояние, что будет впереди – непонятно, КГБ, называемое теперь по-другому, но сохранившее все прежние порядки, надоело до чертиков. Надежда только на компьютер, даже скорее не надежда, а почти религиозная вера в него, в его возможности, в то, что когда-нибудь с его помощью удастся вырваться на волю, ощутить себя свободным человеком, не думающим только о том, где и как достать, раздобыть, урвать то, что жизненно необходимо человеку. И вспоминать пережитое, как страшный, кошмарный сон.

Но все это после… А пока, в конце 1991 года, нужно было самому найти себе интересное дело, которое целиком бы поглотило, помогло бы оторваться от жуткой реальности, забыть вечно полуголодное состояние и страх перед будущим. Таким делом стал для меня Криптоцентр, моя первая реальная программа, которая предполагалась для широкого применения. Конечно же, никакие мои начальники не давали насчет Криптоцентра никаких указаний, это было время безвластия в Спецуправлении, когда каждый мог заниматься практически всем, чем пожелает. Кто-то стал подрабатывать в различных коммерческих структурах, кто-то просто слонялся целыми днями без дела, кто-то политизировался до посинения, но мне все это было неинтересно. Гораздо интереснее было писать Криптоцентр, осваивая при этом еще глубже мой любимый компьютер, все его неограниченные интерфейсные возможности, восхищаясь его простотой и надежностью. К тому времени у меня уже появился настоящий Notebook, который я стал таскать к себе домой, и вместо просиживания в своем кабинете допоздна, я стал пораньше уходить с работы, и дома, на кухне, тоскливо глядя на пустой холодильник, пытался окунуться в придуманный и реализуемый мною в абстрактном виртуальном мире Криптоцентр. И это помогало, сильно помогало продержаться в эти труднейшие месяцы, не давало выхода накапливавшемся чувствам безысходности, злости, обиды и несправедливости. Да и, пожалуй, многим в стране уже приелись зрелища, а все больше хотелось хлеба и хоть какой-то стабильности. Хоть какая-то стабильность наступила (впрочем, она и раньше была): самым стабильным в это время в России стало воровство.

Глава 3

Криптографическая приватизация

Социализм умер, СССР развалился, все стали растаскивать социалистическую собственность. Ее и раньше таскали, но сравнительно понемногу и потихоньку - вспомним продавщиц из советского гастронома или прорабов на стройках социализма. А еще очень часто то, что не могло быть утащено, просто сливалось или зарывалось в землю. Водители грузовиков, приписав себе в путевой лист несколько значащих цифр, вынуждены были избавляться при этом от предававшего их лишнего бензина, ударное Олимпийское

строительство сопровождалось ударным закапыванием в землю оставшихся неиспользованными бетонных плит и прочих стройматериалов, ну а уж сельское хозяйство просто по определению всегда было близко к земле. «Не доставайся же никому, а то возродится капитализм!» - вот основной принцип социализма в подобных случаях.

И вот ненавистный капитализм, который столько раз поминали нехорошими словами различные партийные и комсомольские активисты, стал возрождаться с начала 90-х годов, и в первых рядах его строителей встали те же активисты, быстро выучившие диалектику не по Гегелю, а по Чубайсу. А кто не был активистом и диалектиком, тому в этой приватизации доставался, как правило, кукиш с маслом.

Легко понять, как приватизировать, к примеру, гастроном или автосервис. А как приватизировать бывшее 8 ГУ КГБ СССР, шифровальную службу? Что нужно, чтобы урвать от нее хотя бы какой-то кусочек, желательно полакомнее? Какие основные особенности криптографической приватизации?

Офицеры-математики из Спецуправления 8 ГУ в правовом отношении были почти теми же ГУЛАГовскими зеками из криптографических шарашек, описанных Александром Солженицыным в романе «В круге первом». Огромная интеллектуальная собственность, основательно проверенные и проанализированные криптографические алгоритмы были, как сначала казалось, ничейными, их разработчики не имели реальной возможности запатентовать или каким-то иным образом засвидетельствовать свои имущественные права на разработки, которым приходилось отдавать не один год поисков, сомнений, споров и дискуссий. Офицер, по определению, не имеет свободного времени, все время он находится на Государевой службе, даже когда спит, ест или попивает пивко все мысли должны быть направлены только на одно: как там страна любимая, все ли в ней спокойно и хорошо? А уж если вместо пивка ему вздумалось какой-то алгоритм придумать или программу написать – это тоже государственная собственность, такая же, как нефть или газ, только интеллектуальная. И все низменные помыслы о деньгах за эту собственность офицером сразу же должны быть выброшены в пропасть.

Что стало с государственными нефтью и газом – хорошо известно. А что же стало с государственной интеллектуальной собственностью? Вот наглядный пример из моей реальной жизни.

Разработка шифров на новой элементной базе потребовала около 10 лет работы многих талантливых людей, были написаны огромные тома отчетов, кандидатские и докторские диссертации на эту тему, все было очень основательно пропахано, проверено, теоретически и практически обосновано. Подготовлен реальный пример шифра на новой элементной базе – программа для калькулятора «Электроника МК-85 С». Вопрос к российскому читателю (зарубежные, если таковые когда-нибудь будут, ни за что не смогут дать правильный ответ): кому достанутся все дивиденды от продаж этого калькулятора?

Российский читатель, прочитавший предыдущую главу, наверняка сразу же даст правильный ответ: К., заводскому «толкачу», имевшему примерно такое же отношение к разработке шифров на новой элементной базе, как людоед из центральной Африки к разработке операционной системы Windows, но который знает толк в подобных делах. Ответ настолько очевиден, что даже не хочется обсуждать эту тему: это аксиома, в России всегда так бывает просто по определению. Гораздо интереснее, с точки зрения математика, проследить конкретные механизмы подобного чудодействия, описать этот замечательный алгоритм step by step.

Step 1. Родина в опасности! Наша армия не имеет удобных шифровальных средств! Необходимо оснастить ее портативными шифраторами «Электроника МК-85 С»!

Comment. Все согласны: в этом есть большая доля истины. Это все происходило у меня на глазах, когда К. был всего лишь инженером в моем отделении. И подобные мысли высказывались не только им, но и многими другими сотрудниками, причастными к разработке «Электроники МК-85С». Только К. строил насчет нее слишком конкретные планы. По своим понятиям.

Step 2. Наша экономика в кризисе! Денег нет! Для оснащения армии портативными шифраторами надо много денег!

Comment. И опять же все согласны, возразить на это нечего, все именно так и есть. Только криптографы-математики, как правило, не были так сильно связаны с заводами, со спецификой их советской работы, с «проталкиванием» заказов. Здесь уже не абстрактная математика нужна, а опять же все конкретно, по понятиям. А математики – это слишком интеллигентная для такой работы публика, а потому их интересы в данном случае не столь важны. Да и к тому же они все офицеры, достаточно договориться с одним-двумя генералами и все подчиненные им офицеры возьмут под козырек.

Step 3. Для оснащения армии портативными шифраторами надо пустить их в открытую продажу и заработать на этом деньги для оснащения армии.

Comment. Ну, ну. Какие-то колхозные напевы: все мы делаем одно, общее дело, и не важно, кого при этом погладят по головке и дадут за это конфетку. В подобном колхозе очень легко все коврижки достаются обласканным Председателем колхоза «доставалам» дефицита, а рядовые колхозники, как правило, получают одни пустые трудодни. Но на всех митингах – плакаты: «Хлеб – Родине!»

Step 4. Я могу взять на себя функцию зарабатывания денег. Для армии, только для армии, ну и еще для развития отечественной криптографии!

Comment. Дети, только дети, как говорил Остап Бендер. Правда, в этом конкретном случае современный Остап Бендер говорил это не на общем собрании, а в узком кругу начальников-генералов, строя перед ними грандиозные планы: на заработанные деньги мы организуем широкий криптографический ликбез, вы будете читать лекции по криптографии во всех крупнейших городах Советского Союза и не только Советского Союза. Лесть, грубая и в большинстве случаев абсолютно нереальная, но задевавшая какие-то тайные генеральские струны. Ведь КГБ был абсолютно закрытой структурой, а многие начальники, сравнивая себя с американцами У.Диффи и М.Хеллманом, тоже мечтали о мировой известности.

Step 5. Я создам для этого малое предприятие и от его имени буду продавать портативный шифратор «Электроника МК-85 С».

Comment. Ближе к телу. Главный упор делался при этом на слово «малое». Какой-то новый вариант давней генеральской мечты - своего собственного свечного заводика, как тогда многим казалось. Вся эта демократия и малые предприятия казались в те времена (еще до путча 1991 года) какими-то несерьезными, временным явлением. Чем бы дите не тешилось, лишь бы не плакало.

Step 6. От имени малого предприятия я заключу Договор со Спецуправлением, по которому мне будут разрешены продажи портативного шифратора.

Comment. Момент истины. Но опять же всерьез никто не задумывался о юридических последствиях подобных действий. Все мыслили прежними категориями: К. – коммунист, если будет делать что-то не так, то вызовем его на партбюро и там проработаем как следует. Что такое Договор одного юридического лица (Спецуправления) с другим (кл-овским малым предприятием), какие из него могут последовать реальные результаты, никто в то время не имел четкого представления.

Step 7. Я честный! Я хороший! Я никогда никого не обманываю!

No comment.

Это было смутное время, золотая пора для разных жуликов и проходимцев. Юридической проработки подобных Договоров практически никакой не проводилось, достаточно было подобному пробивному человеку охмурить, окучить пару начальников, от которых зависело принятие решения, наобещать с три короба, навесить всякой лапши на уши – и все, готов Договор, фактически передающий права интеллектуальной собственности, добытой трудом многих людей, одному подобному К., который после этого принимает важный вид, осознает себя причастным к руководящему кругу, и начинает делать с этой бесхозной собственностью все, что душа его пожелает.

Правда, эта собственность казалась тогда не ахти какой и ценной. Хотя внутри шифратора был заложен алгоритм шифра на новой элементной базе, но его интерфейс, сервисные возможности полностью соответствовали самому низовому звену Советской Армии. Вводи информацию с убогой клавиатуры, получай выход только на экране, переписывай его вручную, алгоритм шифрования – только симметричный, ввод ключа – 100 знаков и 10 проверочных цифр – тоже только вручную, солдату можно приказать, а как убедить, например, банкира возиться с этим, как называл его сам К., «Шуриком», к тому же ломающимся с такой же частотой, что и любая советская электроника? Особо много желающих не было, к тому же К. по своей натуре установил на них совершенно астрономические цены: что-то около $400 за один калькулятор, в то время, как такой же серийный калькулятор со стандартной микросхемой стоил в обычном магазине «Электроника» около $10. Эту огромную разницу в цене К. объяснял исключительно новизной заложенных в «Электронику МК-85 С» криптографических идей, к которым он сам не имел никакого отношения.

Непременно загнулась бы организованная им фирма типа «Рога и Копыта», если бы не фальшивые авизо в Центральном Банке России…

Глава 4

Фальшивые авизо

В 1992 году в России произошло очень много интересных событий. Накануне, в декабре 1991 года, распался СССР. Хотя многие потом приписывали причину его распада тройке Ельцин – Кравчук – Шушкевич, сообразившей в Беловежской Пуще, но на самом деле все еще очень сильно определялось позицией Украины, где намного раньше был референдум, на котором большинство высказалось за незалежность. СССР умер, новый, 1992 год страна встречала с новым – старым названием – Россия и с демократически избранным и близким к народу (особенно по спиртосодержащей части) Президентом.

С 1 января 1992 года были выпущены на волю цены. Стала очевидна причина ужасающей пустоты в магазинах накануне Нового Года: все торгаши придерживали товар, чтобы потом продать его подороже. Сразу стали вспоминаться сказки про зверства капитализма, где возмущенные трудящиеся объявляли забастовки при повышении цен на 20%. Дети, салаги, не видали настоящего повышения, раза в три меньше чем за месяц. Но тут, справедливости ради, надо сделать одно замечание: условия эксперимента были разные. У них, за бугром, товары при этом никуда не исчезали, а у нас, в самой справедливой и прогрессивной стране, вся власть принадлежала торговому народу, который волен был силою этой власти отменить на некоторое время всякую еду вообще.

И вдруг оказалось, что с 1 января 1992 года власть торгового народа рухнула! Враз не стало наглых продавщиц, кидающих в толпу пакетики с колбасой, теперь эта колбаса свободно лежит целый день на прилавках и никто ее не покупает. Денег таких нет, ибо цены – коммерческие. Как забавно было видеть неприступных еще вчера теток за прилавком, теперь вынужденных улыбаться и чуть ли не зазывать к себе покупателей. Только деньги подавай! Вот где их только взять в таком количестве?

Где-то примерно в июне 1992 года впервые произошло еще одно знаменательное событие: появился свободный курс доллара по отношению к рублю. Он, правда, был и при советской власти, что-то около 90 копеек за 1 доллар, но тех, кто пытался доллары купить или продать сажали в тюрьму: все операции с валютой были «свободным» гражданам СССР запрещены, вся иностранная валюта, по определению, принадлежала государству. Граждане довольствовались только валютой жидкой. И вот с июня 1992 года любой человек в России получал реальную возможность купить или продать американскую валюту, не опасаясь быть отправленным за это за решетку. В момент появления биржевых валютных торгов курс доллара составлял около 125 рублей, и он почему-то сразу же стал очень быстро расти, чуть ли не на 30-40% каждый месяц. Инфляция, неработающая экономика, разборки во властных верхах, негативные экономические последствия распада СССР – все это, конечно же, напрямую влияло на состояние нашей национальной валюты. Экономика и раньше потихоньку загибалась, но таких простых критериев оценки этого процесса не было. Теперь же появился очень четкий, объективный и не зависящий от правящей элиты критерий: курс доллара по отношению к рублю. Он сразу же стал очень популярным в народе, наравне с прогнозом погоды, а резкое повышение этого курса вызывало заметное раздражение всего населения.

Но была еще одна причина столь резкого роста курса доллара – фальшивые чеченские авизо. Фактически отделившаяся от России мятежная республика быстро нашла способ легкого добывания больших денег с помощью изготовления фальшивых платежных поручений, передаваемых по обычным телеграфным каналам в системе платежей Центрального Банка России. Оказалось, что эти каналы практически никак не защищены от доступа к ним криминала, это самые обычные почтовые отделения связи, по которым любой человек может послать своей бабушке в другой город телеграмму с поздравлениями с Новым Годом. А может и платежное поручение для зачисления на подставную фирму суммы с достаточным числом нулей. Правила составления таких телеграмм были очень простыми и в них в то время практически не использовались какие-то серьезные методы проверки их подлинности.

В ноябре 1992 года курс доллара составлял уже около 400 рублей. Из них, по оценкам ЦБ, 200 рублей – реальная цена доллара, 100 рублей добавляло ближнее зарубежье, активно избавлявшееся от еще советских рублей, а 100 рублей – фальшивые авизо. Для преступников часто курс доллара не играл существенной роли, полученные по фальшивым авизо деньги надо было как можно скорее перевести в доллары, твердую валюту, и это, естественно, приводило к стремительному падению рубля.

Центральному Банку России потребовалась профессиональная, криптографическая система защиты от подделок телеграфных авизо. Но с одним существенным замечанием: она требовалась не просто быстро, а практически немедленно, любая задержка с ее внедрением приводила к колоссальным денежным потерям, раскрутке инфляции, росту курса доллара. А кто мог предложить ЦБ поставить какую-нибудь систему защиты за 2-3 месяца? Генералы ФАПСИ? Да кто из них захочет брать на себя такую ответственность и хлопоты! Да и не было в тот момент за душой у ФАПСИшных генералов ничего, кроме общих разговоров, теоретизирования и лозунгов, а здесь срочно нужно действовать, невзирая на начальственные указивки, не уламывая по несколько дней очередного генерала подписать очередную бумагу, не бегая по нескончаемому

бюрократическому кругу. А надавить на них сверху? Но ЦБ – самостоятельная структура, надавить на ФАПСИ не может, а в верхах идет ожесточенная борьба за власть, им не до фальшивых авизо.

Это было по своему замечательное время. Сама жизнь, критическая ситуация, в которой оказался Центральный Банк, вынудили его искать для защиты от фальшивых авизо все возможные средства. Критериями поиска были быстрота внедрения и криптографическая надежность, устойчивая работоспособность и простота в эксплуатации. Первая же моя встреча со специалистами ЦБ, которая произошла в начале сентября 1992 года, сразу же прояснила для меня ситуацию: вот то, реальное и очень нужное дело, где появилась уникальная возможность применить на практике все то, чему нас, математиков, учили на 4 факультете, чему я посвятил столько лет своей жизни.

Execute! ЦБ спасли шифры на новой элементной базе.

Глава 5

Подробности…

Сейчас, спустя пятнадцать лет, вся эта история с оснащением в 1992 году Центрального Банка России системой криптографической защиты телеграфных авизо, обрастает массой различных слухов и вымыслов. ФАПСИ, называющееся уже по-другому, естественно, все криптографические заслуги приписывает себе. Вот, например, что говорил г-н Матюхин в 2007 году.

«В конце ноября (2007 года – ММ) в Москве состоялся первый форум CNews. Он собрал представителей ключевых игроков ИТ-рынка и был призван определить будущее развития информационных технологий в России и в мире, понять роль ИТ в государстве и бизнесе завтрашнего дня.»

Это цитата с сайта http://safe.cnews.ru/reviews/index.shtml?2007/12/17/279874. Далее там говорится следующее.

«Чтобы определить будущее, полезно осознать наше сегодняшнее местонахождение "на карте развития ИТ". Оценки роли России в эволюции ИТ-индустрии и роли ИТ в жизни нашего государства, данные спикерами форума, были весьма неоднозначными. Например, руководитель Федерального агентства по информационным технологиям Владимир Матюхин не согласился с популярным мнением о том, что в области ИТ Россия постоянно догоняет Запад. По его словам, в нашей стране всегда были системы, аналоги которых западные страны так и не смогли разработать. Правда, эти решения были "страшно далеки от народа" и от реализации задач, в наибольшей степени востребованных населением. В качестве примера г-н Матюхин привел использование уникальной технологии, разработанной в 1993 году ФАПСИ и ставшей препятствием на пути распространения фальшивых авизо из Чечни. Данное решение фактически сделало этот преступный бизнес бессмысленным.»

Я, по правде говоря, так и не понял, в качестве чего привел г-н Матюхин пример «уникальной технологии, разработанной в 1993 году ФАПСИ»: в качестве решения, которое «страшно далеко от народа», или наоборот, в качестве «реализации задач в наибольшей степени востребованных населением». Но это можно отнести к издержкам редактирования данного выступления, по смыслу, все-таки, «препятствие на пути распространения фальшивых авизо из Чечни», которое «сделало этот преступный бизнес бессмысленным», не так уж далеко от народа. Скорее наоборот, судя по тому вниманию, которое сейчас, спустя столько лет, вызывают эти вопросы в Интернет.

Вот только хотелось бы услышать от руководителя такого высокого ранга хоть какие-нибудь подробности создания и внедрения этой уникальной технологии, а то в том же Интернете, в интервью информационному агентству REGNUM годом раньше, в декабре 2006 года (http://www.regnum.ru/news/749825.html), некий «эксперт, боровшийся с фальшивыми авизо», утверждает прямо противоположное и уже кое с какими подробностями.

«Мы разработали уникальную криптографическую систему защиты. Некоторые элементы этой системы не имеют аналогов в мире. Каждый финансовый платеж авизо защищался мини электронной цифровой подписью. Авизо пересылались по специальным средствам связи между РКЦ. Подделать такой финансовый платеж невозможно.
Когда началась эта работа, Центробанк вообще никому не доверял. Для государственной организации это было беспрецедентно, но, вероятно, для этого были основания. Руководство чувствовало, что кто-то и в самом Центральном банке работает на криминал, поэтому было принято решение на первом этапе изготавливать "ключи" (определенная последовательность цифр, которая вводится в шифратор; зная эту последовательность и имея шифратор, можно производить дешифрование информации - прим. ИА

REGNUM) непосредственно в нашем офисе. На последующих этапах ЦБ РФ самостоятельно изготавливал ключи. Здесь, где мы с вами разговариваем, находились около двадцати охранников Центробанка - с автоматами, в бронежилетах, и под их защитой наши сотрудники делали эти "ключи". Можно сказать, что мы в тот момент держали в руках "ключ" от всех финансов России.
Таким образом, всю техническую сторону дела выполняла только компания "Анкорт". Необходимо было в течении нескольких месяцев поставить шесть тысяч шифраторов, разработать уникальные криптографические решения для защиты 1800 абонентов сети, правила функционирования защищенной сети и многое другое для обеспечения необходимого уровня информационной защиты сети ЦБ РФ. Наша компания выполнила свою задачу, и с 1 декабря 1992 г. защищенная система ЦБ РФ начала функционировать. Уже на протяжении более 14 лет никому не удалось технически подделать авизо ЦБ РФ.
Естественно, это было очень и очень небезопасно. У нас не было оружия, но мы ходили в бронежилетах. Мы столкнулись лицом к лицу с нашими противниками. Криминал приезжал с оружием, блокировал производство шифраторов, так что нам пришлось перевозить их в безопасное место, приносили огромные суммы денег, чтобы подкупить, угрожали и требовали "ключи". Но они опоздали, и им было сказано: "Что бы вы ни сделали, господа, все это будет бесполезно: система уже запущена, и изменить ее вы не сможете". С другой стороны, спохватились государственные органы: как же без их ведома производится защита государственного банка, а вдруг что-то случиться, могут снять с должности... И на всякий случай стали заводить уголовное дело на руководителя компании за несанкционированное оснащение ЦБ РФ»

И ни слова о ФАПСИ. Так, намеки, на какие-то «государственные органы», которые «на всякий случай стали заводить уголовное дело за несанкционированное оснащение ЦБ РФ» на героя – руководителя компании. Какие-то таинственные «наши сотрудники», которые в бронежилетах, под защитой около 20 охранников Центробанка, «держали в руках ключ от всех финансов России». Но имя главного героя, спасителя России, у читателей REGNUM не вызывает сомнений.

Эта публикация, с подробностями голливудского боевика, пошла гулять по всему Интернету, практически никто не усомнился в том, что есть еще на Руси такие криптографические богатыри, как компания «Анкорт», которая «выполнила всю техническую сторону» дела оснащения огромной сети ЦБ РФ надежнейшей защитой, разработала «уникальную криптографическую систему», не имеющую аналогов в мире. Обычная электронная подпись, основанная на системе с открытым распределением ключей, по сравнению с «мини электронной цифровой подписью», просто отдыхает.

Восторженных почитателей героя – «эксперта» мне хочется немного приземлить. Простеньким сравнением заголовка из этой статьи, опубликованной в конце 2006 года, с предисловием к моей книге «Практическая криптография», вышедшей в свет в начале 2003 года.

Практическая криптография	Публикация REGNUM
ПРЕДИСЛОВИЕ АВТОРА Россия, 1992 год. Переход к рынку. Динамика роста курса доллара: 01.07.92 1$ = 125 руб. 01.08.92 1$ = 161 руб. (рост за месяц почти на 29%) 01.09.92 1$ = 205 руб. (+ 27%) 01.10.92 1$ = 254 руб. (+24%) 01.11.92 1$ = 398 руб. (+57%) 01.12.92 1$ = 447 руб. (+12%) Наш родной рубль в стремительном падении. И вдруг… 02.12.92 1$ = 417 руб. (- 7% за день!) …… 31.12.92 1$ = 415 руб. Весь декабрь рубль оставался стабильным, несмотря на проходившие в то время бурные политические события: Съезд Народных Депутатов, на котором было отправлено в отставку правительство Гайдара. "Рубль аплодирует правительству Гайдара! " - заголовки газет того времени. Конечно же, на курс рубля влияет огромное	Нагляднее всего ситуацию иллюстрирует динамика инфляции во второй половине 1992 года: 01.07.92 - 1$ = 125 руб. 01.08.92 - 1$ = 161 руб. (рост за месяц почти на 29%) 01.09.92 - 1$ = 205 руб. (+ 27%) 01.10.92 - 1$ = 254 руб. (+ 24%) 01.11.92 - 1$ = 398 руб. (+ 57%) 01.12.92 - 1$ = 447 руб. (+ 12%) В разгар этого обвала **Георгия Матюхина** на посту председателя Банка России сменил **Виктор Геращенко** (назначен 4 ноября 1992 года). Экономическая ситуация в России ухудшалась лавинообразно. Следствием этого стал острый политический кризис, разразившийся в ходе VII съезда народных депутатов России (1-14 декабря 1992 года). В острой конфронтации со Съездом президент **Борис Ельцин** едва не лишился своего поста и был вынужден согласиться на замену **Егора Гайдара** на посту главы правительства **Виктором Черномырдиным**. Между тем, уже 2 декабря стремительное падение российского рубля внезапно остановилось: 02.12.92 - 1$ = 417 руб. (- 7% за день)

множество факторов. И все же… Наверное ЦБ что-то такое предпринял. Тем более, что Председатель Центрального Банка России Виктор Владимирович Геращенко делает доклад на Съезде, отчитывается о мерах по стабилизации финансового рынка. Откроем этот доклад и прочитаем внимательно. И в одном абзаце найдем фразу о том, что с начала декабря во всех расчетно-кассовых центрах ЦБ РФ стали применяться криптографические устройства для защиты от подделок почтовых и телеграфных авизо.	31.12.92 - 1$ = 415 руб. Выступая на Съезде, Виктор Геращенко констатировал, что банковские расчеты России были поставлены на грань полного паралича, однако неизбежный крах удалось предотвратить, благодаря оснащению расчетно-кассовых центров ЦБ шифровальными устройствами, что позволило свести к минимуму риск мошенничества при совершении телеграфного авизования платежей.

Мне кажется, что, забывая упомянуть всех, кроме самого себя, «эксперт» мог бы все же не опускаться до такого явного плагиата.

Впрочем, в сторону эти примитивные криптографические сказки. Я надеюсь, что читателю будет интересно узнать истинные подробности того, как в 1992 году появилась система защиты телеграфных и почтовых авизо в Центральном Банке России, от непосредственного участника тех событий. Сразу же оговорюсь: никаких бронежилетов я на себя ни разу в жизни не одевал и около 20 охранников Центробанка меня не охраняли, когда я распечатывал на двустороннем лазерном принтере ключевые таблицы. Ключ, правда не от всех финансов России, а всего лишь от системы выработки всех ключевых таблиц, в руках действительно держал: это была дискета 1, 44 Мб. И вынужден констатировать, что никто огромные суммы денег за эту дискету мне не предлагал. Да и за разработку всей системы тоже.

Итак, обо всех тех событиях по порядку в хронологической последовательности.

Первый портативный шифратор «Электроника МК - 85 С» появился на свет в конце 1990 года. И его роды были трудными, как всегда бывает, когда впервые используется новый тип шифра. А новизна заключалась в следующем: работал этот шифратор не с битами и не с байтами, а с обычными десятичными цифрами. Помните, в семнадцати мгновениях весны: «От предчувствия удачи у Мюллера заболела голова». Заболела потому, что он обнаружил одинаковые цифровые пятизначные группы в шифровке от русской радистки Кэт и в донесении, перехваченном от Штирлица в Берне. А еще в Советской Армии с очень давних времен использовались очень громоздкие и неудобные переговорные кодовые таблицы, в которых разные приказы, команды, военные сведения заменялись на цифровые кодовые обозначения. И если их не перешифровывать с помощью такой же десятичной гаммы наложения, то голова может заболеть не только у абстрактного Мюллера.

Причиной появления «Электроники МК - 85 С» стала война в Афганистане, когда неудобные переговорные кодовые таблицы в критических ситуациях вынуждали солдат передавать данные вообще открытым текстом, что приводило к трагическим событиям. Я уже упоминал ранее одного из инициаторов этой разработки, Славу, который к тому времени успел побывать в Афганистане и знал об этих проблемах не по наслышке. Тот отдел, куда я попал после степановского Теоретического отдела, как раз и занимался в том числе разработкой кодовых таблиц для Советской Армии и методами их перешифровки. Он и еще двое молодых ребят, все – математики, выпускники Высшей Школы КГБ, придумали первый вариант криптосхемы для «Электроники МК – 85 С».

Основным критерием была скорость шифрования. «Электроника МК – 85 С» это, фактически, бытовой программируемый калькулятор «Электроника МК – 85», в котором был реализован простейший язык BASIC. У меня даже сохранился его снимок.

Теоретически можно было бы вообще ничего в нем не переделывать, а запрограммировать на этом родном языке алгоритм шифрования и использовать в качестве шифратора дешевый бытовой калькулятор. Но проблема заключалась в том, что никаких периферийных устройств к нему не подключалось и ввести готовую программу шифрования было просто неоткуда. А дойти до такого садизма, как заставлять солдат Советской Армии вводить вручную написанную на BASIC программу шифрования, никто не мог даже в

КГБ. Требовалось создать специализированную микросхему, реализующую алгоритм шифрования аппаратно, но алгоритм должен быть простой и быстрый, ресурсы калькулятора – весьма ограничены.

В борьбе за скорость разработчики алгоритма за основу взяли шифратор типа «Ангстрем-3», естественно переделанный по сравнению с тем первым вариантом, который я приводил в этой книге. Пришлось увеличивать длину входного слова, теряя при этом в скорости, и тогда ребята сначала решили использовать «Ангстрем-3» только для выработки разового ключа, а быструю раскрутку гаммы осуществлять с помощью простенькой балалайки. В Теоретическом отделе эта балалайка была быстро разломана, а у начальства тогда отложилось в голове, что калькулятор – нестойкий.

Балалайку выкинули, стали использовать «Ангстрем-3» для раскрутки гаммы. На грани между допустимым компромиссом между скоростью и стойкостью, давая повод для теоретических дискуссий на тему «стойкий – нестойкий» и нервируя начальство. Но дело в том, что для каких-то разумных подходов к снижению трудоемкости определения неизвестного ключа требовался огромный материал, огромное количество открытого и соответствующего ему шифрованного текста: если мне сейчас не изменяем память, порядка 10^6 - миллиона знаков. Теоретически такое допускалось, практически же, глядя на калькулятор, в то, что по его кнопкам можно нажать миллион раз и он при этом не сломается, верилось с трудом.

К чему я сейчас рассказываю об этом «криптографическом базаре»? Цена его оказалась слишком высокой. Но об этом чуть позже.

Все околокриптографические подробности, связанные с проталкиванием выпуска «Электроники МК – 85 С» на заводе Ангстрем в Зеленограде, я уже приводил выше. Финал таков: правдами и неправдами, в основном за счет усилий К., выпуск был налажен. В этом надо отдать ему должное. И действительно, для этого требовались деньги. Это было уже в 1991 году, еще до путча, полного паралича в Спецуправлении еще не было, опять же какими-то правдами и неправдами (окучиванием начальников) К. сумел добиться снятия с «Ангстрема-3» грифа секретности и разрешения продавать «Электронику МК – 85 С». Нельзя не признать, что это решение было разумным, иначе этот единственный реальный пример шифра на новой элементной базе так бы и сгнил в сейфах КГБ – ФАПСИ.

Августовский путч парализовал Спецуправление. Все ждали, что контору вот-вот разгонят, практически все работы встали, спасайся, кто может. Все стали патриотами коммерческой криптографии, включая руководство. Я тоже был тогда маленьким начальничком, правда не настоящим, как мне прямо говорили мои подчиненные, а компьютерным фанатом. К. тоже не считал меня за своего полноценного начальника, но мой компьютерный фанатизм, по-видимому, внушал ему уважение, и я тоже попал по его окучивание, правда, не как начальник, а как математик – криптограф - программист.

Для продажи «Электроники МК – 85 С» в 1990 году К. создал малое предприятие «Анкорт». Это предприятие было малое в самом прямом смысле слова: постоянно в нем работали только два человека – сам К. и его бухгалтер. К. начал заманивать в «Анкорт» офицеров Спецуправления, но желающих было мало, К. не вызывал к себе доверия у офицеров. Те ребята, которые разрабатывали криптосхему для «Электроники МК – 85 С», работать в «Анкорте» отказались. Практически все мои друзья не советовали мне связываться с К., но в Спецуправлении в конце 1991 года был хаос, всякая осмысленная работа, требующая знаний криптографии, практически встала, будущее – более чем неочевидно. Мысли о том, что кушать самому и кормить семью надо каждый день, заставляли искать пути к выживанию в то время. А контакты с «Анкортом», несмотря на негативные отзывы большинства людей о К., казались мне в то время меньшим из зол. Сейчас, по прошествии стольких лет, мне приходится признаваться самому себе: это была большая ошибка, нельзя было идти на «сделку с дьяволом» вопреки моральным принципам, которые в те времена существовали в среде математиков – криптографов.

Итак, К. соблазнил меня работать на «Анкорт», рисуя перспективы всяких «райских наслаждений». К тому времени, помимо фанатизма, у меня уже был достаточный опыт написания программ, поэтому подготовить программную реализацию шифратора «Электроника МК – 85 С» на компьютере не составляло большого труда. Кроме того, первая версия системы Криптоцентр стала приобретать товарный вид, и мне было даже интересно, как она будет воспринята в открытом мире.

Где-то с начала 1992 года К. стал активно рекламировать «Электронику МК-85 С». У нас с ним сложился своеобразный дует, в котором К. играл роль зазывалы-торговца, а я – технического специалиста, способного объяснить дотошным покупателям все криптографические нюансы портативного шифратора и своей программы. Мы стали с ним ездить по разным выставкам и выставлять на них эту криптографическую продукцию. И вот где-то в августе 1992 года на одной из выставок калькулятор приметили специалисты из ЦБ.

Здесь, упомянув про первые контакты с ЦБ, мне хочется сделать еще одно отступление про обстановку в Спецуправлении в то время. Период, когда слова «коммерческая криптография» были допустимыми, закончился где-то в мае 1992 года. В это время вышел Указ Президента Ельцина о запрете коммерческой деятельности в государственных структурах (точное название сейчас не помню, но смысл был именно такой). 8 и 16 управления КГБ, а также управление правительственной связи были выведены из структуры КГБ и объединены в ФАПСИ – Федеральное Агентство Правительственной Связи и Информации. Новый генеральный директор ФАПСИ рьяно бросился выполнять Указ: «Всякую коммерческую деятельность запретить, заключенные к тому времени Договоры – разорвать!» Вроде как

выдавили из тюбика зубную пасту, а теперь приказано вдавить ее обратно. «Мобилизующий» приказ, такие не раз приходилось слышать и от генерала - начальника 4 факультета. Но времена уже были не те, грозные приказы не вызывали священного трепета. Лозунг – лозунгом, а жизнь – жизнью. К тому же поговорка «рыба гниет с головы», как показала дальнейшая история ФАПСИ, представленная сейчас в разделе уголовно-криминальной хроники на сайте компромат.ру, оказалась удивительно точной.

Мое сотрудничество с «Анкортом» продолжалось и в конце концов оно привело меня в Центральный Банк для разработки в минимально возможные сроки системы криптографической защиты платежных поручений. Сейчас, спустя 15 лет, когда всем стало ясно, что в 1992 – 1993 годах для Центрального Банка России была создана эффективная система защиты банковских авизо, у руководства бывшего ФАПСИ нет желания вспоминать какие-нибудь подробности того, как изгибалась «Генеральная линия» в то время, и какой хаос творился тогда в Спецуправлении. А подробности такие: эта система создавалась полулегально, в обход руководства ФАПСИ, под прикрытием малого предприятия «Анкорт», ибо любые попытки каким-то образом «легализовать» проводимые тогда работы неизбежно привели бы к их затягиванию.

Подробности состоят также в том, что сначала Центральный Банк пытался официально обратиться в ФАПСИ с просьбой разработать систему криптографической защиты банковских авизо. К тому времени у руководства ФАПСИ уже выработался условный рефлекс: коммерческая криптография должна использовать только алгоритм ГОСТ 28147-89, потому что с него давно сняты все подозрения в секретности. А как конкретно коммерсанты будут использовать этот алгоритм – их проблемы. Завод «Ангстрем» в Зеленограде начал выпускать специализированные платы «Криптон» для персональных компьютеров, вот пускай покупают и используют. Как и всегда было в СССР: что бы ни выпускала промышленность, все равно получается танк или автомат Калашникова. Калькулятор «Электроника МК – 85 С» явно не укладывался в этот стереотип, в нем не было криптографического танка – алгоритма ГОСТ, а по виду и по размерам он больше напоминал продукцию загнивающего запада, откуда, кстати, и вел свою родословную. Поэтому, хотя К. и протолкнул разрешение на его продажу, но это было еще в «прошлой жизни», до прихода нового руководства ФАПСИ. Выдавленная зубная паста должна быть загнана обратно в тюбик!

Под системой криптографической защиты для ЦБ в ФАПСИ понимали что-то такое, что в первую очередь минимизировало бы всякую ответственность. Только ГОСТ, ответственность за него минимальна и за десять лет согласований и утверждений «размазана» по такому количеству чиновников, что найти ответственного уже невозможно. Во вторую очередь, Указ Ельцина о запрете коммерческой деятельности в госаппарате понимался как запрет для подчиненных, но не для начальников. Вкус к получению денег уже пришел. Вот поэтому в 1992 году, в ответ на запрос Центрального Банка, ФАПСИ в свою очередь запросило на разработку системы криптографической защиты около двух лет, чтобы попытаться найти за это время, как и к какой элементной базе пристроить танк ГОСТ, поскольку во многих расчетно-кассовых центрах ЦБ в то время компьютеров попросту не было, и около двух миллиардов рублей.

Центральный Банк, надо отдать должное его руководству, не пошел на поводу у ФАПСИ. Два года затяжки грозили непредсказуемыми последствиями для всей финансовой системы России, фальшивые авизо вылавливались исключительно благодаря интуиции и опыту молодых девушек-операционисток из РКЦ практически ежедневно. А сколько не вылавливалось? Ответ на этот вопрос давал стремительный рост курса доллара.

Решающим оказался сентябрь 1992 года. Первая же встреча в ЦБ показала, насколько они заинтересованы в поисках тех, кто мог бы оказать хоть какую-то конкуренцию ФАПСИ. Срочно нужна криптографическая защита телеграфных авизо, все остальное – вторично. На первый взгляд, нет проблем, калькулятор – вот он, перед вами, шифруйте и защищайте, но дьявол, как всегда, скрывался в криптографических деталях.

Не требовалось шифровать, а нужна была короткая проверочная комбинация, код подтверждения достоверности, КПД, который бы гарантировал подлинность платежного поручения. Никто и никогда при разработке криптографических алгоритмов для «Электроники МК – 85 С» не предполагал, что калькулятор может потребоваться для выработки какого-то КПД. Поэтому, несмотря на всю заманчивость возможного контракта с ЦБ, К. сначала решил от него отказаться. Во-первых, калькулятор неприспособлен для выработки КПД, во-вторых, мало привлекала перспектива конкурировать с ФАПСИ, в котором он к тому времени был инженером, а я – действующим офицером, одним из его начальников.

И вот дернул же меня тогда какой-то черт с ним не согласиться! Точнее – посоветовать немного подождать с ответом: может быть что-то удастся придумать. Для меня это решение было абсолютно нелогичным, иррациональным, оторванным от всякой реальной жизни. Нужно ли мне портить отношения с ФАПСИ, кода остается всего два года до заветных 20 лет выслуги, дающих право на офицерскую пенсию? Такое ли безграничное доверие вызывал к себе К., от которого шарахались все офицеры Спецуправления? Нужно ли было отдавать в его руки такой уникальный контракт, как разработка системы защиты для всего Центрального Банка России? Такой ли большой я имел к тому времени опыт общения не с интеллигентными математиками – криптографами, а с циничным дельцом, с которым можно иметь дело только по принципу: не верь, не бойся, не проси?

В общем, мой первый опыт реального бизнеса оказался примерно таким же, как и первый вариант шифратора «Ангстрем-3», то есть не просто плохим, а прямо никудышным. В результате в 2006 году на всю страну публично заявляется: «…всю техническую сторону дела выполняла только компания "Анкорт"».

Нет, не всю. Компания «Анкорт» в лице ее директора выполняла безусловно важную функцию: выбивание из зеленоградского завода в кратчайшие сроки большого числа калькуляторов «Электроника МК – 85 С». Точка. Но этого недостаточно для оснащения такой организации, как Центральный Банк. Нужна еще криптографическая инфраструктура: разработка способов использования калькулятора для выработки КПД, создание и наладка системы выработки и смены ключей, нормативные инструкции, обучение персонала, модернизации системы и т.п. Нормальные компании, планирующие долгосрочный бизнес, подбирают для таких работ специалистов, заключают с ними юридически выверенные до мельчайших подробностей контракты, ведут прозрачную финансовую политику, со специалистами обращаются чрезвычайно бережно, всеми силами стараются вовлечь их в дела компании, заинтересовать в получении прибыли за счет заключенных контрактов и многое, многое другое, что гораздо позже я наблюдал в Корее.

Но мой первый опыт в коммерческой криптографии в виде контактов с «Анкорт» я сейчас не могу назвать иначе, как варварский. Огромный объем проделанной работы, удачный контракт с Центральным Банком, в результате – не просто ноль, а глубокий минус без пенсии офицера.

Это все философия жизни, пора перейти к прозе. К криптографическим раздумьям в сентябре 1992 года о том, как приспособить калькулятор для выработки КПД. Сначала – о том, что же вообще мог делать этот калькулятор.

Он изначально разрабатывался для Советской Армии, для засекречивания переговоров ни самом низовом уровне: отделение, взвод, рота. Два режима работы: буквенно-цифровой и чисто цифровой. В первом случае с клавиатуры вводилось нормальное сообщение на русском языке, которое затем засекречивалось и высвечивалось на экране в виде пятизначных цифровых групп. Этот режим считался основным, в перспективе предполагалось, что существовавшие долгое время в армии кодовые переговорные таблицы будут отменены, все сообщения будут вводиться открытым текстом с клавиатуры, засекречиваться, а затем полученные пятизначные группы будут продиктованы в канал связи. Но такое могло произойти очень нескоро, отмена переговорных кодовых таблиц – дело будущего, а пока предполагалось, что калькулятор может быть использован для их перешифровки, чтобы избежать опасных повторов кодовых обозначений, как об этом очень популярно поведали Штирлиц и Мюллер. В этом режиме с клавиатуры вводились только цифры, которые затем перешифровывались и на экран опять же выдавались цифровые пятизначные группы.

Ничего этого Центральному Банку не требовалось. Им не требовалось шифровать платежное поручение, лишний раз усложнять и без того непростую работу операционисток из РКЦ. Количество авизовок, обрабатываемых каждой из них, доходило до нескольких сотен за день, это не экзотические шифровки Юстас – Алексу, отсылаемые раз в месяц. Требовалось добавить к авизовкам какой-то короткий КПД, который бы зависел как от содержания платежного поручения (от кого, кому, какая сумма, дата и т.п.), так и от ключа, известного только в РКЦ. Нет ключа – вычислить КПД нельзя. И более того, нет ключа – нельзя в уже готовом платежном поручении изменить хоть какие-то данные (например, сумму перевода), ибо тогда КПД должен быть совсем другим, никак не связанным с первоначальным.

Самое печальное заключалось в том, что естественные методы защиты, например, зашифровать в цифровом режиме сумму перевода, были абсолютно неприемлемы. Во-первых, при шифровании в шифрованный текст автоматически добавлялся десятизначный маркант, а одним из требований ЦБ было то, что длина КПД не должна превосходить 10 цифр. Этот маркант являлся простым набором случайных чисел и гарантировал отсутствие повторов гаммы наложения, которое могло бы привести к повторениям в шифровках а-ля 17 мгновений весны. Но с точки зрения выработки КПД для ЦБ он был абсолютно бесполезным, не нес в себе никакой информации о платежном поручении и съедал отпущенный лимит по длине КПД. Во-вторых, и это самое главное, шифрование не давало гарантированной защиты от подделки. Шифрование – это простое гаммирование, сложение цифр открытого текста со знаками зависящей от ключа гаммы наложения. И если вычислить КПД было нельзя, то изменить в готовом платежном поручении сумму перевода можно было очень просто: сумма известна, зашифрованная сумма тоже известна из КПД, вычитаем одно из другого, получаем гамму наложения, складываем ее с измененной суммой, получается новый КПД, который будет принят получателем как истинный. В криптографии это было давно известно, еще со времен войны во Вьетнаме, когда зашифрованные шифром гаммирования команды управления советскими ракетами изменялись американскими системами перехвата. Советские ракеты стали летать не в те вьетнамские джунгли, а криптографы схватились за голову. В 70-е годы появилась теория шифрующих автоматов, одним из разделов которой стала имитостойкость, т.е. способность шифра противостоять целенаправленному навязыванию ложной информации. И первым постулатом, первой аксиомой стало: шифры гаммирования не являются имитостойкими. Калькулятор «Электроника МК – 85 С» был простейшим устройством шифрования именно по принципу гаммирования, никакие имитоприставки в нем не предполагались, ресурсов было по минимуму, да и для низовых звеньев Советской Армии они не требовались. Ведь там в цифровом режиме перешифровывались кодовые переговорные таблицы, их содержание потенциальному противнику предполагалось неизвестным, требовалось всего лишь гарантировать отсутствие повторений.

Попечалившись над этими проблемами пару дней, я стал искать нетривиальное решение. И оно в конце концов нашлось, простое и понятное, которое, с одной стороны, полностью устроило Центральный Банк, поскольку КПД получился коротким, не более 10 цифр, как того и требовал заказчик, а с другой – полностью исключило всякие возможности подделок. Только «покупай» ключи, как нас и учили в Высшей Школе КГБ, рассказывая о дисковых шифраторах.

Суть в следующем: шифровать ничего не будем. Займемся маркантом. Если поглядеть на снимок калькулятора, то среди его черных кнопок в верхнем ряду вторая справа - генератор случайного марканта. Он необходим в шифрах гаммирования для обеспечения уникальности вырабатываемой при каждом шифровании гаммы. С помощью марканта обеспечивается отсутствие повторений в шифртексте, даже если какие-то повторения встречались в открытом тексте. В «Электронике МК – 85 С» маркант многократно шифровался с помощью долговременного секретного ключа, но уже в режиме блочного шифра, и полученный таким образом результат становился разовым криптографическим ключом шифратора «Ангстрем-3», действительным только для данного сообщения. Своеобразный аналог session key в современных компьютерных системах, использующих протокол SSL. И вот тут то уже вовсю использовался «лавинный эффект» размножения различий, которым обладали блочные шифры. Измени хоть один символ в марканте – разовый ключ будет уже абсолютно другим, и каким конкретно – невозможно вычислить без знания долговременного ключа.

Но на приемном конце для расшифрования сообщения должны были ввести сначала маркант и затем вычислить с его помощью разовый ключ данного сообщения. Так и было, первые 10 знаков в любой шифровке, полученной с помощью калькулятора, всегда были маркантом. Пользователи этого практически не замечали, они вводили все подряд: маркант и шифртекст, а калькулятор сам отбирал первые 10 знаков, вычислял по ним разовый ключ и с его помощью расшифровывал остальной текст. Но эта была та зацепка, то нетривиальное решение, которое в конечном итоге и позволило спасти Центральный Банк от фальшивых авизо. Ничего не шифруем, а в цифровом режиме расшифрования в качестве марканта (первые 10 знаков) вводим банковскую информацию, которую необходимо защитить от подделок. Из этой информации калькулятор автоматически вычисляет разовый ключ для расшифрования непонятно чего, но нам расшифровывать ничего и не надо: вводим, например, в качестве ширтекста одни нули, тогда получаем чистую гамму наложения, кусочек нужной длины используем в качестве КПД. Хоть 5, хоть 7, хоть 10 знаков, это безразлично, всю имитозащиту выполнил маркант, точнее – алгоритм его преобразования в разовый ключ.

Эта неожиданная идея сразу перевернула все пессимистические взгляды на возможность использования калькулятора в ЦБ. КПД вырабатывать на калькуляторе можно, и способ выработки удовлетворяет всем банковским требованиям. Банк реально получал надежнейшую криптографическую защиту, для реализации которой не требовалось разрабатывать заново какие-то шифровальные средства, все уже готово и серийно выпускается в Зеленограде. Следовательно, в кратчайшие сроки можно решить проблему защиты от фальшивых авизо.

Решение есть, запатентовать бы. И выставить бы «эксперту, боровшемуся с фальшивыми авизо», как это и принято во всем цивилизованном мире, условия: решение – есть, хочешь – покупай. И потребовать оформить юридически Договор на передачу интеллектуальной собственности с указанием в нем своих роялти. Печально сейчас, 15 лет спустя, вспоминать об этом. Нет, не было тогда никаких реальных возможностей запатентовать это решение. Я был в то время действующим офицером ФАПСИ, т.е. юридически совершенно бесправным лицом, для любого патентования нужно было разрешение руководства. Один патент у меня к тому времени уже был – на алгоритм шифрования типа «Ангстрем-3», в нем – все по честному, только реальные разработчики из НИИ Автоматики и Спецуправления. Оформляли этот патент около двух лет. Проку с него, как показала практика, – ноль, все вопросы передачи прав на продажу «Электроники МК – 85 С» решались начальниками – генералами, про этот патент никто и не вспомнил. Криптографический ГУЛАГ оставался неизменным со сталинских времен.

Вот так «Анкорт» и получил «уникальную криптографическую систему защиты», у которой «некоторые элементы не имеют аналогов в мире», практически даром, как впоследствии практически даром были приватизированы многие природные ресурсы России. Но современные олигархи хотя бы не выступают публично с заявлениями типа: «Мы создали нефть и газ».

Итак, в середине сентября 1992 года стало окончательно ясно, что калькулятор можно использовать в ЦБ. Там сразу же за нее ухватились, как за соломинку, первоначально планируя использовать в течение полугода, до появления чего-то более серьезного, чем казавшийся примитивным калькулятор. «Анкорт» где-то в конце сентября заключил официальный контракт с Центральным Банком на поставку большой партии калькуляторов «Электроника МК – 85 С».

Но в ЦБ еще нужно с нуля создавать криптографическую инфраструктуру: систему выработки ключей к калькулятору, нормативные документы для банковского персонала, никогда до этого ни с какими шифровальными устройствами не работавшего, программную реализацию алгоритма выработки КПД на компьютере для больших РКЦ и многое другое. Про это в контракте не было речи по понятным соображениям: не хотели лишний раз дразнить ФАПСИ. И без этого реакция криптографических генералов, считавших себя единственными монополистами на все, что связано с криптографией, была однозначной:

запретить! Во-первых, никто не хотел брать на себя никакой ответственности, а во-вторых, фактически уплывал богатый клиент. Но как запретить? Это был октябрь 1992 года, никаких официальных поводов для запрета еще нет, Указ Ельцина № 334 «О лицензировании и сертификации в области защиты информации» будет принят гораздо позже, в 1995 году. И вот тогда вспомнили «криптографический базар» в Теоретическом отделе о том, стойкий или нестойкий калькулятор «Электроника МК – 85 С», и запустили в ЦБ «пену»: сомневаемся в его криптографической надежности. Доллар растет, как на дрожжах из-за фальшивых авизо, а ФАПСИ в это время пускает в Центральный Банк, предпринявший реальные шаги для защиты своих платежей, криптографические «пенные волны». И самое интересное в том, что эти волны совершенно беспочвенны. Ведь для выработки КПД в калькуляторе, во-первых, ничего не шифруется, а во-вторых информация, обрабатываемая с помощью «Ангстрема-3» на одном разовом ключе, крайне мала, несколько знаков, тогда как все сомнения в криптографических качествах возникали при миллионе знаков.

Несколько эпизодов из этих событий мне особенно запомнились. В конце октября 1992 года Центральный Банк пригласил меня и К. на довольно представительный симпозиум по проблемам информатизации, который проходил в здании бывшего СЭВ на Арбате. У меня с собой был довольно экзотический по тем временам Notebook, выдававший разработчика, к тому же там было заявлено, что мы с К. разрабатываем систему защиты для ЦБ. И вот в перерыве на меня буквально налетел какой-то важный господин, по виду – высокопоставленный чиновник.

- А Вы знаете, что Ваша система нестойкая?

- Откуда у Вас такие сведения?

- Я знаю!

- А Вы сами по образованию кто, криптограф?

Господин не был криптографом по образованию, но то, что система защиты для ЦБ – нестойкая, почему-то не вызывало у него сомнений.

Но результатом этих «пенных волн» была задержка с внедрением системы защиты примерно на две недели. Это было в начале октября 1992 года и читатель легко сможет прикинуть стоимость двухнедельной задержки по динамике роста курса доллара в то время.

Ну а мне в это время надо было подумать о криптографической инфраструктуре для ЦБ. Как вырабатывать ключи? Как вообще переложить на компьютер максимально возможную работу по защите телеграфных авизо? Идей была масса, все сводились к тому, чтобы в будущем попытаться максимально автоматизировать эту систему кодирования. В октябре 1992 года все начиналось с простейших программ – первых версий системы «Криптоцентр – авизо» для выработки КПД на компьютере и выработки ключей для такой огромной сети, как Центральный Банк. Первые две недели октября из-за «пенных волн» выдались спокойными, в ЦБ их переваривали, а у меня появилось время написать первую версию «Криптоцентра – авизо».

В начале ноября 1992 года в ЦБ было принято окончательное решение, несмотря на все возражения ФАПСИ, использовать калькулятор для защиты банковских платежей. Окончательная точка была поставлена на совещании у первого заместителя Председателя Центрального Банка Р.А.Ситдикова, которое проходило 7 ноября на Неглинке, неподалеку от Красной площади, на которой в этот день шумела то ли демонстрация в честь Великого Октября, то ли что-то еще. Первый же вопрос, который г-н Ситдиков задал разработчикам системы защиты, был, естественно, о криптографической стойкости.

- А Вы уверены, что Ваши калькуляторы стойкие?

У меня в голове уже вертелись длинные рассуждения про имитостойкость, маркант, советские ракеты во Вьетнаме, но К., знающий методы общения с высокими начальниками, опередил.

- Да, уверены. Мы оснастили ими Советскую Армию.

Вопросов о стойкости больше не было.

Изготовление и рассылка секретных ключей – деликатнейший криптографический вопрос. В 8 ГУ КГБ СССР существовало специальное управление «Б», которое занималось исключительно этими проблемами: как изготавливать и рассылать ключи. И вот ЦБ в годовщину Великого Октября идет на революционный шаг – отказывается от услуг управления «Б». Ключи для системы кодирования авизо первоначально будут изготавливаться в «Анкорте», а рассылаться с помощью службы инкассации ЦБ. Это был вызов проповедуемой со сталинских времен религии секретности в криптографии, которая способна завалить любое живое дело. А мне, как разработчику, эта новость давала пищу для размышлений: сейчас ЦБ отказывается от услуг управления «Б», так в дальнейшем может быть удастся внедрить и современную систему рассылки ключей по типовым каналам связи, шифруя их перед рассылкой с помощью системы с открытым распределением ключей. Это будет намного дешевле, чем услуги службы инкассации.

И, наконец, естественно был поднят вопрос о программной реализации системы кодирования авизо с помощью персональных компьютеров. Очень энергичная женщина, главный бухгалтер Центрального Операционного Управления, работать с калькуляторами наотрез отказалась.

- У нас столько авизовок проходит каждый день, а здесь экранчик и клавиатура такие миниатюрные, на выработку КПД для каждой авизо уходит слишком много времени, мы не справимся! Дайте нам программную реализацию алгоритма выработки КПД на персональном компьютере.

No problem! Через день я уже в ЦОУ, на своем Notebook объясняю девушкам-операционисткам, как кодировать авизо с помощью «Криптоцентр-авизо». Но в ЦОУ в этот день компьютеров еще не было, так что мои первые объяснения были чисто умозрительными. И потом, глядя на то, как работают эти девушки, заваленные кипами «входящих – исходящих», часами не отрывающиеся от своих рабочих мест, невольно закрадывались мысли: ну вот, у них и так здесь работы невпроворот, а я тут еще появляюсь со своей системой кодирования, усложняю их и без того непростую жизнь. Но когда они поведали мне некоторые подробности, то все сомнения сразу же отпали.

- У нас здесь постоянно в соседней комнате следователь МВД дежурит, мы чуть ли не каждый день фальшивые авизо вылавливаем и относим ему. А суммы-то в них какие: 800-900 миллионов рублей в каждой. Вы уж нам помогите!

На одной лишь интуиции молоденьких девушек-операционисток держалась вся система защиты платежных поручений Центрального Банка до декабря 1992 года! И то, что тогдашнее руководство ЦБ пошло наперекор догмам ФАПСИ, взяло на себя ответственность за спасение финансовой системы страны, не могло не вызывать у меня уважения. Появлялось желание доказать, что советская криптографическая школа – это не пустой звук, что те университетские традиции, которые существовали на 4 факультете вопреки начальникам, могут пригодиться в критической ситуации. Для Центрального Банка ситуация, несомненно, была критической, вынуждала к нестандартным решениям ради одной цели: в кратчайшие сроки защитить банковские платежи. В конце совещания 7 ноября Р.А.Ситдиков достает свою визитку и дает ее К.

- Вот моя визитка, а в ней – мой прямой телефон. Если кто-то будет мешать – звоните мне напрямую, на следующий день этот человек будет уволен.

В моей жизни было несколько случаев, когда возникало ощущение бессилия перед бюрократической стеной. В России три раза мне посчастливилось наблюдать ситуацию,

когда в ответ находился решительный человек, начальник, который фактически заявлял: «Работайте, создавайте, Вам верят. Всю ответственность я беру на себя».

На внедрение системы защиты был дан карт-бланш. Но что же делать с программной реализацией? Тут опять я хочу посвятить читателя в некоторые нюансы существовавших в то время правил работы с шифровальной техникой.

Криптографическая стойкость – способность шифра противостоять математическим методам анализа – это только одна, хотя и важнейшая характеристика системы защиты. Шифр, как правило, реализуется с помощью каких-то электронных устройств, в которых есть побочные излучения. Да и простое нажатие на клавиши при вводе открытого текста или ключа вызывает миниатюрные звуковые волны, которые могут быть перехвачены чувствительным прибором. Все эти вопросы рассматривались в рамках так называемых специсследований, результаты которых, как правило, приводили к усложнению эксплуатации аппаратуры: требовались генераторы шумовых излучений, специальные звукоизолированные камеры, развязки по сети питания и многое, многое другое. Калькулятор «Электроника МК – 85 С» был хорош еще и тем, что все эти проблемы были в нем минимизированы: есть автономное питание, энергопотребление минимально, а следовательно минимальны побочные излучения. Но когда речь заходила о программной реализации, то, строго следуя инструкциям ФАПСИ, каждый компьютер нужно было в течение долгого времени исследовать на специальном стенде, чтобы выявить все опасные побочные излучения, а затем ужесточить и без того непростые условия работы операционисток из РКЦ. При этом, как правило, в ходе подобных тестов пытались найти хоть какие-то побочные излучения, заведомо считая все их опасными, и не вдаваясь в детали, насколько они опасны реально.

Это все было из разряда требований к военным и важнейшим правительственным линиям закрытой связи. Но здесь, в Центральном Банке, ситуация совсем иная. Защита практически отсутствует, нужно срочно внедрять криптографические методы, а любые контакты с ФАПСИ неизбежно приведут к затягиванию внедрения.

И здесь опять же ЦБ проявил реализм. Программная реализация «Криптоцентр-авизо» в 1992 году реально была внедрена в двух крупнейших РКЦ: Центральном Операционном Управлении и в Оперу – 1. Формально считалось, что кодирование осуществляется с помощью калькуляторов, а «Криптоцентр-авизо» работает в режиме тестирования. На самом деле калькуляторы валялись в сейфах и ни одного дня ими никто не пользовался в течение многих лет эксплуатации «Криптоцентра-авизо». А мне даже пришлось в 1999 году подписывать акт о том, что «Криптоцентр-авизо» стойкий к «проблеме 2000 года». Привет тем, кто придумал эту нетривиальную бизнес-акцию!

Итак, Центральный Банк получил элегантную криптографическую систему при минимальных затратах по времени и стоимости. Это стало возможным благодаря тому, что в течение почти 15 лет велась разработка теории шифров на новой элементной базе, которые позволили создать калькулятор «Электроника МК – 85 С», быстро подготовить систему выработки ключей и всю остальную криптографическую инфраструктуру. Причем не благодаря, а вопреки усилиям руководства ФАПСИ.

Что же касается «эксперта» К. - Бог ему судья. Сильный менеджер в таком деле необходим, одних усилий яйцеголовых математиков-криптографов в нашей стране явно недостаточно. Но после той интеллигентной среды, в которой я существовал всю свою сознательную жизнь, общение по принципам: «не верь, не бойся, не проси», моральный дискомфорт, постоянное ощущение: сейчас обманут, напрягись, не раскрывайся, - показались мне дикими. К., как всегда, занялся окучиванием центробанковских начальников, мне же гораздо интереснее было работать с простыми девушками – операционистками из расчетно-кассовых центров банка. Именно они были уже не абстрактными, а вполне конкретными потребителями моих криптографических идей и программ. И если для них, впервые в жизни услышавших слово «криптография», это слово оказалось с нормальным, человеческим, а не бюрократическим лицом, то я был этому очень рад. Именно они, эти молодые девушки, и являются истинными героинями, спасшими в 1992 году Россию от фальшивых авизо.

На их интуиции и ответственности функционировала вся система платежей и до, и после внедрения системы криптографической защиты.

Ну и, наконец, последнее. У читателя, внимательно прочитавшего начало этой главы, неизбежно возникнет вопрос: система защиты авизо была внедрена в Центральном Банке с 1 декабря 1992 года, так почему же тогда г-н Матюхин говорит об «использовании уникальной технологии, разработанной в 1993 году ФАПСИ»? Что за временные чудеса, когда разработанная в 1993 году технология внедряется с 1 декабря 1992 года? Может быть в 1993 году ФАПСИ разработало какую-то принципиально другую технологию? Или же это просто опечатка в тексте?

В 1992 году ФАПСИ похвастаться было нечем. Неожиданно появился алгоритм, использующий маркант для выработки КПД, реакция – чисто рефлексная: запретить! В декабре 1992 года этот алгоритм на деле доказал свою стойкость: поток фальшивых авизо прекратился, доллар упал. Это официально признали в январе 1993 на Директорате Центрального Банка. Реакция ФАПСИ – это наша разработка! В январе 1993 года, на ежегодном отчете отдела, в котором я был заместителем начальника отделения, открытым текстом было заявлено: гендиректор ФАПСИ распорядился считать разработку для ЦБ проделанной не каким-то малым предприятием, а ФАПСИ. Формально – на 100% именно так. Калькулятор «Электроника МК – 85 С» - разработка ФАПСИ, вся инфраструктура разработана действующим офицером ФАПСИ. С одним маленьким добавлением: полулегально, без разрешений руководства. Вот и одна из возможных причин временных чудес: разработка внедрена с 1 декабря 1992 года, а указание считать ее разработкой ФАПСИ поступило в январе 1993 года.

Другая причина – да, действительно в 1993 году ФАПСИ приложило свою руку и к разработке. Острота проблемы спала, Центральный Банк не спеша стал обращаться в ФАПСИ с просьбой об официальном разрешении на использование уже реально действующей системы защиты банковских авизо. ФАПСИ, руководствуясь указаниями своего руководства, внесло некоторые косметические изменения в способ построения информационного блока авизо, подлежащего кодированию, ничего не меняя по существу: тот же калькулятор «Электроника МК – 85 С», в котором для выработки КПД используется маркант в режиме расшифрования. Этот алгоритм получил название «алгоритм ФАПСИ», на него было дано официальное разрешение, реально использоваться в банке он начал с начала 1994 года. К тому времени ЦБ уже заказал новую разработку – специализированный калькулятор «Электроника МК – 85 Б», только для Центрального Банка, и в нем было всего три алгоритма: старый, с 1992 года, новый, придуманный ФАПСИ, и оригинальный, только для этого нового калькулятора, не совместимый с «Электроникой МК – 85 С». Новый алгоритм я придумывал уже с учетом всех особенностей защиты авизо в Центральном Банке, в основе его по-прежнему лежали шифры на новой элементной базе, безо всяких монстров - ГОСТов, фактически это была специализированная хеш-функция, зависящая от ключа. Завод в Зеленограде выпустил несколько тысяч калькуляторов «Электроника МК – 85 Б», их разослали по всем РКЦ ЦБ, но разрешения на работу с третьим, оригинальным, придуманным только для ЦБ алгоритмом ФАПСИ так и не дало. Ни да, ни нет.

Глава 6

Итого

Итак, оснащение Центрального Банка криптографической системой защиты на базе портативного калькулятора «Электроника МК-85 С» произведено, система введена в эксплуатацию с 1 декабря 1992 года и сразу же дала весьма ощутимый эффект. Значимость этого события явно выперала за рамки ФАПСИ. Математика и криптография кончаются, начинается политика: кто и как это сделал, как к этому относиться, кого казнить, а кого помиловать.

Мои дальнейшие рассуждения о событиях того времени достаточно субъективны, я, как непосредственный их участник, не могу быть абсолютно объективным. Но все же постараюсь минимизировать эмоции, а больше внимания уделять не вызывающим сомнения истинам.

Итак, истина 1: Договор на оснащение системой криптографической защиты Центральный Банк заключил не с ФАПСИ, а с малым предприятием «Анкорт».

Истина 2. Предприятие «Анкорт» имело какие-то юридические отношения с ФАПСИ. Эти отношения в конце 1992 года были весьма запутанными, с одной стороны, из-за шараханий «Генеральной линии» ФАПСИ в отношении коммерческой криптографии (разрешить – запретить), а с другой – из-за личности руководителя «Анкорта».

В ЦБ мне потом приходилось слышать такую оценку тех событий: систему защиты установили «двое лысых». Под одним из них понимали г-на К., под другим – автора этих строк. Но.

Истина 3. В конце 1992 года оба лысых являлись сотрудниками ФАПСИ.

Математика и логика окончательно закончились.

Истина 4. В конце 1993 года оба лысых уже не являлись сотрудниками ФАПСИ.

Истина 5. В 2007 году руководство переименованного ФАПСИ приводит пример разработки «уникальной технологии, ставшей препятствием на пути распространения фальшивых авизо из Чечни», как результат работы ФАПСИ. «В нашей стране всегда были системы, аналоги которых западные страны так и не смогли разработать».

Что и какие мысли крутились в головах руководства ФАПСИ в начале 1993 года по этому поводу – одному Богу известно. Могу только предположить: амбиции. Как это так: без нашего разрешения? Типичный пример «директорской психологии», которую мне потом неоднократно приходилось наблюдать. Логика и результаты – по боку, упрется рогом, нальет глаза кровью, и в ответ на логику только одно: а мне плевать!

В конце 1992 - начале 1993 года руководство ФАПСИ было в ярости. Слова «Центральный Банк», «защита авизо» были контрреволюционными и контриков ждала неминуемая расплата. Про математические и криптографические задачи никто не вспоминал, никаких даже самых отдаленных намеков на обсуждение метода использования марканта для выработки КПД в Спецуправлении тогда не проводилось, о традиционных в таких случаях «мозговых атаках» забыли. Почему? А может быть потому, что в октябре 1992 года, когда в ФАПСИ просочились первые слухи о том, что ЦБ хочет использовать калькулятор, реализующий обычный шифр гаммирования, там стали ехидно потирать руки: сейчас они что-нибудь на нем зашифруют, а мы им в ответ – криптографический ликбез. Знаете ли вы господа-банкиры про имитостойкость? А про то, куда летали с шифром гаммирования советские ракеты во Вьетнаме? Так что не рыпайтесь, выкладывайте побольше денежек и слушайтесь умного «папу» из ФАПСИ. Ситуация казалась на 100% беспроигрышной.

Разработка любой криптографической системы защиты начинается с разработки требований к ней: от кого и как она должна защищать. Портрет абстрактного вероятного противника. У меня же в сентябре 1992 года с этим проблем не было: система защиты телеграфных авизо в первую очередь должна защищать от чиновников ФАПСИ, от самых что ни на есть конкретных. Гаммирования не дождетесь! Вот вам маркант, с ним и ковыряйтесь до посинения, если возникнет желание. Желаний ковыряться с маркантом не возникло, но зато возникло желание разобраться с изобретателем. «Ксиву – на стол, в Центральный Банк больше – ни шагу!». Вот такую своеобразную оценку стойкости системе защиты телеграфных авизо выдало ФАПСИ в феврале 1993 года.

Ярость – это с одной стороны. А с другой – коммерческий прагматизм. Много ли заработаешь на военных и правительственных линиях связи? Нужно ближе к деньгам. Центральный Банк – одна из ключевых финансовых организаций, от него тянутся ниточки ко всем коммерческим банкам. Если протолкнуть какую-то систему защиты в ЦБ, то дальше можно навязывать ее и всем остальным. Коммерческая криптография становится ясной и понятной: сесть на трубу, перекрыть всем кран, заставить идти на поклон. Вскоре все так и будет, появится Указ Ельцина «о лицензировании и сертификации в области защиты информации», все пойдут на поклон к ФАПСИ. Но это произойдет через два года, а тогда, в начале 1993 года, успешное внедрение полулегальной и относительно независимой системы защиты в ЦБ явно шло вразрез с далеко идущими замыслами генералов ФАПСИ.

Такова была криптографическая политика, грязная и неблагодарная. Но я старался поменьше думать о ней. Ведь действительно, в ЦБ было сделано очень большое и нужное дело, все криптографические решения использовали только идеи шифров на новой элементной базе, тот математический аппарат, который разрабатывался с помощью кафедр математики и криптографии 4 факультета Высшей Школы КГБ, Спецуправления, НИИ Автоматики. Разработка этого аппарата велась около 15 лет, на эту тему было написано много отчетов и диссертаций, содержащих действительно новые, оригинальные результаты. Эта работа сильно отличалась от проталкивания в стандарты советского варианта DES, в которой требовались, в основном, согласования и разрешения. И вот в тот момент, когда, казалось, DES-ГОСТ окончательно перечеркнул все усилия, затраченные на разработку шифров на новой элементной базе, эти шифры, хотя и полулегально, вопреки усилиям руководства ФАПСИ, нашли себе достойное применение и стали «препятствием на пути распространения фальшивых авизо из Чечни, фактически сделали этот преступный бизнес бессмысленным».

Это был уже второй мой урок по теме «Криптография и свобода». Первый преподал мне Степанов, насильно затащив после защиты диссертации обратно к себе в отдел. Смысл везде один и тот же: начальник – царь и бог, выступил против – не жди ничего хорошего. Свобода может быть только санкционированной сверху. Не осознанная (как, помнится, учили философы), а указанная необходимость. Властная вертикаль – отнюдь не новое изобретение, она существовала и при Сталине, и после него. Точная наука математика здесь кончается, начинается философия жизни. И все мои попытки подходить к жизненным околокриптографическим проблемам с теми же подходами, что и

к доказательству теорем, неизменно оканчивались одним и тем же: дважды два получалось равным пяти. Досрочно защитил диссертацию в аспирантуре – плохо, диссертация – это твое личное дело, назад, к Степанову, начинай там все с начала. Но это были просто невинные шалости. Через семь лет, после защиты ЦБ, никто уже не говорил подобных глупостей, все было проще: пиши рапорт об увольнении по собственному желанию.

Спорить с этим начальством? В очередной раз доказывать, что ты не верблюд? Бодаться теленку с дубом? Ну уж нет! Играйте в эти игры сами, мне они противны. Дело сделано, а как к этому отнесутся начальники – их проблемы. Карьерный рост в ФАПСИ мне был абсолютно безразличен, чиновничьи должности противны. Окучивание начальников, слезные челобитные – дайте хотя бы досидеть полгода до пенсии – низко и мерзко. Я лишь попросил объяснить, почему мне запрещают работать с ЦБ, отбирая утром служебное удостоверение. Не получив на это никакого внятного ответа, в рапорте с просьбой уволить по собственному желанию я постарался высказать все, что думаю по этому поводу.

СВОБОДА?

Погоны сброшены, я стал вольным. Вот она, долгожданная свобода! Вечная аспирантура! Сколько раз за все время моей службы в КГБ я ловил себя на мысли: как же угнетает эта противная зависимость от разных иногда компетентных, но чаще просто напыщенных, надутых от собственной важности начальников, положение бесправного холопа, которого могут послать в совхоз, на субботник-воскресник, на стройку социализма выполнять там самую черную работу абсолютно бесплатно. Ведь та система КГБ, в которой я служил, породила ГУЛАГ, в котором миллионы бесправных заключенных своими костями выстраивали советскую промышленность, работавшую в основном на армию. Все родимые пятна этого ГУЛАГа сохранились в неприкосновенности и во времена моей службы в КГБ: контролеры за приходом и уходом с рабочего места, обязательное высиживание с 9 до 6 вечера даже в том случае, если работаешь в теоретическом отделе, где такой режим оказывает прямо противоположное воздействие на получение требуемого от тебя результата, отлученность от результатов своего труда, дающая широкое поле деятельности разным криптографическим проходимцам. Все официально запрещено: офицеру запрещено подрабатывать на стороне, отлучаться без разрешения начальства из Москвы, самому сменить себе работу, если она стала неинтересной и есть предложения из других мест. Но реально все можно, только втихаря, по партизански, где пошептавшись с нужными людьми, где просто наплевав на грозные приказы и распоряжения начальства. Как в том анекдоте про попа и мужика.

- Батюшка, дозволь в Великий Пост кусочек мяса съесть?
- Не дозволяю!
- Но ты же сам ешь.
- Так ведь я об этом ни у кого не спрашиваю!

Реально можно и подрабатывать, пытаясь хоть как-то прокормить семью в трудное время «рыночных преобразований». Но так устроена система: нарушителями является абсолютное большинство, поэтому начальникам легче управлять такими людьми. Чуть что – сразу припоминаются все «грехи» скопом: опоздания на работу, несанкционированные отъезды из Москвы, отсутствие «патриотизма к отделу». На 4 факультете у начальников, собирающихся отчислить слушателя за неуспеваемость, всегда был готов следующий аргумент

- Ходит в неглаженной форме, да и вообще, он в наряде уснул.

И вот – свобода, формально начальников больше надо мной нет. Свобода? Нет тупых начальников? Это в России то?

Russia. Example.

После победы демократии в России все разрешено. Если перейти на простой язык, то это, в частности, означает, что всем водителям не грех иногда и «подбомбить», т.е. немного подзаработать частным извозом. Это стало общенародным хобби, по крайней мере в Москве и окрестностях, а поскольку в моих пристрастиях автомобиль стоит на втором месте после компьютера, то вечерком, после дневного сидения за компьютером, я частенько выезжал «на охоту». Помимо чисто меркантильных целей, здесь еще удавалось иногда увидеть наглядные примеры из жизни простых россиян, люди, встречающиеся тебе в первый и последний раз, часто бывают очень откровенны и не сдерживают своих эмоций.

И вот один раз ко мне в машину села молодая и привлекательная женщина лет 30-35. Мы с ней разговорились о том, о сем, по виду – интеллигентная, образованная, приятно побеседовать. И надо же было быть в это время в машине включенным радиоприемнику! Там через некоторое время в выпуске новостей сообщили, что Пенсионный фонд России решил проявить какую-то очередную заботу о россиянах. При слове «Пенсионный фонд» моя собеседница, оказавшаяся бухгалтером какого-то ОАО, враз преобразилась, интеллигентность сняло как рукой, и она стала напоминать разъяренную фурию. Такого отборного трехэтажного мата я, пожалуй, не слышал со времен стройотряда, где мы работали на стройке госпиталя КГБ. Только сейчас он лился из уст этой очаровательной женщины, которая таким образом всю оставшуюся дорогу красочно описывала свои интимные отношения с Пенсионным фондом: как там приходится сдавать отчеты и принимать все возможные позы перед инспектором, доказывая, что ты не верблюд и пени на тебя накладывать не за что, сколько там требуют бумаг по всякому поводу и без повода, какое там столпотворение народа в дни сдачи отчетов, как придираются к заполнению каждой клеточки в каждой бумажке и многое другое, причем ее рассказ был весьма эмоционален и передаваем дословно только в непечатном издании. А ведь это один лишь Пенсионный фонд! Кроме него для возбуждения женщин-бухгалтеров еще есть налоговая инспекция, статуправление, фонды социального и медицинского страхования, в общем, множество поводов для различных впечатлений и встреч.

Это – реальная российская свобода. Свобода чиновничьего бизнеса, ущемляющего миллионы людей, собирающего толпы народа у кабинетов инспекторов из разных регистрационных палат, налоговых инспекций и множества обязательных фондов, бизнеса, основанного исключительно на взятках. Это какая-то совершенно извращенная свобода и демократия, при которой лучше живут не те, кто приносит больше пользы остальным людям, а те, кто делает им больше вреда. Самый богатый человек в мире – основатель Microsoft Билл Гейтс – создал операционную систему Windows, компьютерные сети, Internet, то, что позволило людям во всем мире жить лучше, общаться друг с другом, вывело все человечество в новый, компьютерный век. А что сделали самые богатые люди в России? Купили чиновников и сели на трубу. Как же это тривиально и примитивно!

После увольнения из КГБ у меня появилась масса возможностей почувствовать себя простым россиянином, например, побывать в районной поликлинике. Результатом общения с нашим «бесплатным» здравоохранением стал партизанский стиль мышления: «Живым не сдаваться!». Жизнь по принципу «волка ноги кормят» быстро отрезвила, помогла сбросить розовые очки, сквозь которые мне часто приходилось смотреть на нашу действительность, познакомила со многими новыми людьми, из которых честных и порядочных оказалось все-таки намного больше, чем жуликов и проходимцев, однако последние очень часто оказывались в роли различных начальников. Глядя на пышный расцвет чиновничьего бизнеса в России я невольно сравнивал увиденное со знакомой мне системой КГБ. Сколько общих черт! Те же тупые начальники, подчас нисколько не задумывающиеся о последствиях принимаемых ими решений (в КГБ, пожалуй, даже чуть поумнее были), та же рабская зависимость от них. Например, полностью заплатить все налоги в России в принципе невозможно, а посему практически каждый россиянин зависит от налоговой инспекции, в любой момент ему можно предъявить обвинение. От взяточного геноцида спасает только большое количество и нищета россиян. Про любимых всеми гаишников лучше и не вспоминать, когда я был офицером КГБ, то от них спасала красная книжица и закон о статусе военнослужащего, по которому офицера нельзя было штрафовать. И вот на «свободе» наконец-то дошло: это же клан охотников за людьми, основной задачей членов этого клана являются засады с радарами, каждый удачный выстрел – полтинник или стольник, в зависимости от инфляции.

Принцип «Не верь, не бойся, не проси!» давно уже стал национальной российской идеей, которую столько раз пытались найти правители, живущие на Олимпе. А кто не хочет жить по такому принципу, кто слишком буквально воспринимает декларированную свободу и права человека – тем лучше из России свалить.

Вот такая жизненная позиция выработалась у бывшего офицера КГБ.

Глава 1

Гениальный директор

Вернемся в 1993 год. Куда податься после увольнения из ФАПСИ? Вроде ясно: к К., с которым мы на пару окучивали Центробанк. Но больно уж заметные перемены произошли с ним после успешного завершения эпопеи с системой защиты телеграфных авизо для ЦБ. Хотя нет, скорее это была моя наивность, неумение разбираться в людях, когда я пытался искать в нем положительные черты, слишком уж сильно на меня действовала его показная деловитость и напористость, граничащая с нахальством. Критерием, который помог мне взглянуть на него другими глазами, были деньги, которые Центробанк заплатил за внедрение системы защиты авизо. В 1992 году работы по защите авизо не закончились, потом еще два года мы делали различные специализированные модернизации калькулятора специально для ЦБ и в результате за все эти работы ЦБ перечислил его малому предприятию где-то около миллиона долларов.

Первые же относительно крупные деньги моментально преобразили этого человека. Наши прежние отношения с ним «на равных» сразу же перешли в категорию «начальник – подчиненный», где начальником, естественно, мыслил себя К. Ну на то, кем он там себя мыслил, мне было абсолютно наплевать, мы с ним работали, не заключая никакого контракта, мне же хотелось довести до коммерческого внедрения мою систему «Криптоцентр» и, кто знает, может быть и каким-то образом внедрить ее в ЦБ. Идеи К. были гораздо проще: прихватизировать себе все деньги, получаемые от ЦБ, не допуская в этом деле никаких конкурентов. Обычная и очень банальная история, в которой мне досталась незавидная роль спарринг-партнера в различных махинациях этого «Гениального директора».

Сразу же разорвать наши отношения К. не мог: при общении с ЦБ было слишком много чисто технических проблем, в которых он был абсолютно некомпетентен, а найти мне замену было довольно-таки сложно. Поэтому его задачей на начальном этапе нашего сотрудничества было платить поменьше, а обещать и пускать пыли в глаза – побольше. Одним из способов пускания пыли в глаза был миф о создании имиджа фирмы.

Часто «деловые» переговоры с участием К. больше походили на записки из сумасшедшего дома. Вместо реальной и взвешенной оценки своих возможностей следовал поток словоблудия:

- Я крупнейший производитель шифровальной техники в Европе!
- Я вхожу в двадцатку ведущих мировых авторитетов по криптографии!
- Каждый день я приношу государству экономию в 30 тысяч долларов!

и так далее в том же духе. Неудивительно, что многие потенциальные заказчики, вежливо выслушав эту ахинею, делали от ворот поворот. Эти же бредни (скорее всего, на Центробанковские деньги) публиковались и в печати.

Мания величия охватила этого человека. Ему, как солдату-дембелю, хотелось нацепить на себя все, что блестит: чтобы о нем писали газеты, показывало телевидение, в советские времена он, наверное, был бы без ума от счастья, если бы на высокой трибуне юные пионеры повязали его красным галстуком. И вот захотелось ему однажды стать победителем конкурса «Золотой бизнес» и повесить на стенку соответствующую грамотку в рамочке. Стоило это удовольствие в те времена где-то около 5 тысяч долларов: грамотка в рамочке и торжественный вечер со шведским столом в фойе гостиницы «Россия» в придачу.

Но поскольку К. одновременно захотел покататься по заграницам, то так получилось, что в момент этого торжественного вечера он был в Италии, а почетное право попить-погулять в гостинице «Россия» ему пришлось предоставить мне и еще одному Толе, Анатолию Григорьевичу, бывшему офицеру, высокому и стройному, который заканчивал 4 факультет года на 4 раньше меня. У нас с ним сложился прекрасный дуэт.

Шведский стол состоял исключительно из коньяка и водки, которыми встречали прямо в фойе. «Победители» слегка разогревались, а затем началась по-советски нудная процедура вручения грамоток в рамочке, отличавшаяся от награждения победителей соцсоревнования только нахальными попытками раскрутить разогретых победителей «на бабки», т.е. стать спонсорами чего-то. Желающих раскручиваться было немного и вскоре попойка продолжилась, только уже за столиками. Одновременно начались выступления артистов, некое подобие новогоднего Голубого огонька 60-х годов. Очаровательная Клара Новикова с микрофоном в руке стала прогуливаться между столиками и нацелилась на сидевшего рядом со мной красавца Анатолия Григорьевича. Прямым ходом она направилась к нашему столу, а мы с Толей заворожено глядели на нее. И тут…

И тут подали горячее мясо. С картошечкой. Мясо – это святое, при его появлении я забываю обо всем остальном, душа уходит куда-то в другое место, а руки сами начинают тянуться к ножу и вилке. К моему стыду, в выборе между духовным и съедобным я тогда выбрал последнее. А Клара Новикова, увидя, как сосед ее красавца предал все светлые идеалы искусства, сразу же сделала разворот на 180 градусов и больше такой возможности увидеть вблизи звезду российской эстрады у меня уже не было.

За нашим столиком был еще один молодой человек, который, как оказалось, - сын одного из сотрудников Спецуправления 8 ГУ КГБ. Торгует импортной мебелью: простой и понятный бизнес, никаких научных заморочек, договорился, купил, продал, потом еще и еще. Мы с ним сразу же нашли общий язык, общение продолжилось в самых что ни на есть демократических условиях и после того, как официальное мероприятие в гостинице «Россия» закончилось. В общем, когда я наконец-то добрался до дома, выяснилась одна любопытная вещь: грамотка, которая была в рамочке, по дороге потерялась. Рамочка есть, а грамотки в ней нет, видно прикрепили плоховато, не рассчитывали, что у нее будет такая нелегкая жизнь.

Вручение рамочки без грамотки К. напоминало сценку из мультика, в котором Вини Пух и Пятачок дарили ослику Иа-Иа подарки на день рождения. Нам с Толей (который Анатолий Григорьевич) было очень трудно сдержать свои ехидные эмоции, глядя на то, как К. воспринимает всерьез эту мишуру, хотя и весьма недешевую.

Жизнь в его конторе очень часто напоминала какой-то дурдом, в котором К. постоянно с кем-то ругался: с уборщицами, с завхозом, с бухгалтерами, с молодыми программистами. Такая уж у него была натура – склочной бабы, которая всегда и всем недовольна. Ту мизерную зарплату, которую он выплачивал, считал верхом благодеяний, за которые все должны быть обязаны ему до гроба. «Я вас кормлю» - любимое высказывание этой «кормящей матери», занятой целый день склоками, пустым трепом, сплетнями и завистью. Его высокомерие становилось все больше и больше с каждым очередным Центробанковским вливанием.

Сколько раз я упрекал себя за ту наивность, с которой связался с ним! Практически ни один человек не мог проработать с К. больше года, все, кто приходили и уходили, были плохими, хорошим – один К. Пределом его мечтаний была торговля: водкой, гербалайфом, его убогими «Шуриками», всем, где есть возможность обмана, легкие деньги, общение с жуликами и проходимцами и все остальные прелести из жизни в «свободной» России в начале 90-х годов. После службы в КГБ, где, несмотря на все остальные перипетии, я общался с людьми порядочными, интеллигентными, образованными и честными, переход к общению с К. все чаще начинал вызывать омерзение. Быстро дошло, что никаких денег мне здесь не видать, как своих ушей, одна только начальная школа реальной жизни. Все-таки подобных типов в России достаточно много и надо один раз переболеть этой болезнью, чтобы к ней выработался устойчивый иммунитет. А в период болезни стараться не забывать своей основной специальности – математика-криптографа-программиста, не опускаться до торгашеского уровня и относиться ко всему этому с юмором. Так легче переносится эта неприятная, но не смертельная бацилла.

- Господин Гениальный директор, а какое место Вы занимаете в двадцатке ведущих мировых авторитетов по криптографии?

Но одно дело было реальным и бесспорным – это Центробанк, единоличную заслугу в оснащении которого К., естественно, присвоил сам себе. В его контору стали иногда заглядывать весьма нетривиальные личности, во встречах с которыми доводилось поучаствовать и мне. Правда, чаще всего во время словоблудия Гениального директора хотелось просто покрутить пальцем у виска, но утешало одно: собеседники, наверное, тоже обладают чувством юмора. Но один раз К. укатил в какую-то очередную заграницу, и встречать японскую делегацию довелось мне и Анатолию Григорьевичу, без Гениального, к нашей обоюдной радости. Эта была делегация из какого-то японского университета, которая изучала условия ведения бизнеса в России, и направила ее к нам партия «Яблоко».

Эта встреча запомнилась мне по одному эпизоду, о котором чуть ниже. А началась она с каких-то дурацких вопросов, которыми эти инопланетяне стали пытать нормального советского человека.

- Какая на Вашей фирме проводится финансовая политика?
- Упало – обналичили.
- А какая часть доходов идет на выплату заработной платы?
- По ведомости или черным налом?

Ну и все в том же духе. Водка, закуска – все в холодильнике, ждут своего часа, а они тут про какую-то финансовую политику! Да в России может быть только одна финансовая политика: приплыли деньги – прячь их поскорее, пока родное государство их не умыкнуло. Это у них там в Японии рабочий час работает на государство, а все остальное время – на себя и на фирму. А в России государство хочет, чтобы 110% всех доходов уходило на налоги и прочие явные и неявные поборы, а люди при этом жили за счет святого духа и еще оставались должны государству. Но не может: нет у святого духа таких денег. Поэтому вместо святого

духа в России появился «черный нал» и блестяще справился с поставленными ему демократическими партией и правительством нелегкими задачами. И вот все это я постарался популярно объяснить японцам.

Насколько они поняли все мои объяснения – не берусь судить. Но по некоторым косвенным признакам нечто подобное, изложенное в несколько иной форме, им, скорее всего, уже приходилось слышать.

Тривиальные истины всегда неинтересны. Поэтому, по-возможности поскорее закончив дискуссию о «финансовой политике» в России, я предложил гостям менее тривиальное зрелище – посмотреть свою систему «Криптоцентр». Японцы, гуманитарии, о криптографии услышали впервые, и показ живой, работающей криптографической системы произвел на них впечатление. Ведь это был 1993 год, тогда еще не было встроенных криптографических функций в операционные системы компьютеров и рынок криптографической продукции был экзотичен и свободен.

И вот потом произошел тот эпизод, который навсегда остался в моей памяти. Праздношатающейся публики, захаживающей в контору, было достаточно, десятки раз я показывал и пытался объяснить разным личностям свою систему «Криптоцентр», они с умным видом все выслушивали и сматывались, раздавая направо-налево кучу обещаний все это купить, внедрить в своем регионе, стать нашими дилерами и т.п. Японцы же, вежливо выслушав все мои рассказы криптографа-фанатика, вкусив после этого русского гостеприимства, сделали весьма нетривиальный жест.

- Спасибо за очень интересную встречу. Мы отняли у Вас очень много времени, которое Вы могли бы посвятить своей работе. Но мы готовы компенсировать эти потери. В этом конверте 200 долларов, которые, как мы поняли, дополнят тот «черный нал», который есть на вашей фирме.

Немая сцена. Такого в новейшей истории России я еще не встречал. По инерции ближайшие 10 лет я голосовал исключительно за партию «Яблоко», которой симпатизировал и без японцев. Но теперь на вопрос: «А почему ты голосуешь именно за них?» у меня всегда был простой и понятный ответ: «За 200 долларов!».

По моим наблюдениям, у всех личностей, подобных К., есть вера в чудо. Кропотливый повседневный труд инженера – это не их удел. Одним махом они намерены решить все мировые проблемы, мелкие технические детали – не в счет. Такой идеей–fix у К. было сотрудничество с иностранным партнером, который начнет продавать по всему миру его ломающиеся от малейшего дуновения ветерка «Шурики». Таких желающих почему-то не нашлось, но на Центробанковской инерции удалось установить деловые контакты с одной южноафриканской фирмой, которая предложила нам продавать в России свою продукцию – телефон и факс, обеспечивающие шифрование передаваемого сигнала. Аналоговый сигнал в этой аппаратуре преобразовывался в цифровой и, следовательно, появлялась возможность гарантированного зашифрования передаваемого цифрового сигнала. Для этих целей необходимо было установить в эту аппаратуру свой алгоритм шифрования и, естественно, выбор пал на схему типа «Ангстрем-3».

К. подписал контракт с этой фирмой, по которому их инженеры оказывали нам содействие в проведении модернизации этой аппаратуры и таким образом мне удалось впервые познакомиться с зарубежными специалистами, с уровнем их квалификации и стилем работы.

Тут и впоследствии мне еще не раз приходилось вспоминать добрым словом родную криптографическую alma-mater, 4 факультет. Те качества, которые нам прививали с раннего возраста вместе с математикой, это теперь те козыри, с которыми можно общаться по крайней мере на равных с иностранной фирмой и ее инженерами. А у них ведь тоже не все бывает гладко, часто возникают чисто технические проблемы, в процессе решения которых и познается, кто есть who.

Поставленный нам телефон не работал. Приехавшие в первый раз с фирмы ребята были веселыми и общительными, но сделать так ничего фактически и не смогли. Телефон по-прежнему не работал, несмотря на все заверения, что причина этого вот-вот будет найдена. После нескольких месяцев бесплодных обменов мнениями по факсу, фирма наконец-таки прислала к нам своего ведущего инженера Дэви.

На каждой фирме есть люди, составляющие ее золотой фонд и Дэви, несомненно, был именно из этой категории. Сравнительно молодой парень лет 30-35, веселый, общительный и досконально разбирающийся во всем, что было связано с этим телефоном. Для него не было никаких проблем, он запросто перепрограммировал и перешивал ПЗУ, прекрасно разбирался в алгоритмах оцифровки аналогового сигнала, был одарен замечательным слухом и, кроме всего прочего, поражал своим ответственным отношением к делу. Мне было жутко интересно общаться с ним, а ему, как я подозреваю, было интересно послушать про криптографию, о которой он раньше не имел большого представления. За несколько дней мы с ним на пару смогли подготовить программу для записи в ПЗУ, в которой был реализован алгоритм шифрования типа «Ангстрем-3». Я на Notebook писал различные тестовые программы, Дэви переписывал их на имитатор ПЗУ в компьютере, а затем мы сравнивали результаты работы. В конечном итоге возникла идея

провести полное тестирование не на имитаторе, а на реально подготовленном ПЗУ и сравнить результаты с моими тестовыми программами на компьютере. Но для этого Дэви нужен был специальный прибор – Digitaser, который он смог бы подключить к ножкам-контактам ПЗУ и получить на его экране снимаемую с них цифровую последовательность. Это достаточно сложный прибор и у Дэви его с собой не было.

И тут у К. возникла идея: свозить Дэви на завод в Зеленоград, где были эти Digitaserы, там можно будет все протестировать, а заодно показать иностранному инженеру ведущее советское предприятие электронной промышленности. Если бы К. побольше общался не с разными зеленоградскими начальниками, а с простыми работягами, то наверняка бы десять раз подумал о возможных негативных последствиях показа зеленоградского «социалистического реализма» перед тем, как тащить туда прекрасного зарубежного специалиста.

С Серегой, работавшим в Зеленограде небольшим начальничком, мы накануне договорились о пропусках на 10 часов утра. Серега все это перепоручил какой-то девочке, которая про них то ли забыла, то ли что-то перепутала, в общем, пропусков в 10 утра не было. Пока с помощью советского внутреннего телефона (мобильников тогда практически ни у кого еще не было) удалось дозвониться до вечно где-то бегающего Сереги, прошло полчаса. Еще с полчаса Серега ругался с девочкой, снова перепоручал все ей, короче говоря, на сам завод мы попали уже ближе к обеду.

Я никогда не был на фирме у Дэви, но по моим более поздним корейским представлениям, иностранная фирма – это в первую очередь сотрудники, работающие на своих рабочих местах. Серегина зеленоградская контора в 1993 году – это куча рабочих мест, заваленных всякими чудесами советской электроники, но без всяких признаков человеческого присутствия. И вот в этих необитаемых завалах мы с Дэви начали искать заветный Digitaser. Его радость по поводу сравнительно легко найденного первого Digitasera оказалось преждевременной: сие чудо техники не работало. Найти второй оказалось уже посложнее, но и он мало чем отличался от своего первого собрата. На поиски третьего мы уже отправились вместе с Серегой по нескончаемым и абсолютно необитаемым зеленоградским лабиринтам и где-то на втором или на третьем уровне этой realty-бродилки наконец-таки наткнулись на то, что надо. Радости Дэви не было предела – этот Digitaser работал! Он тут же стал подключать его к ножкам ПЗУ, а Серега с вдруг откуда-то появившимися сотоварищами сразу же вспомнили, что настало время обеда и пора отметить российско-южноафриканское сотрудничество, что все уже в холодильнике и ждет заветного часа.

Дэви дорвался до работы, его уже больше не интересовало ничто на свете. Все серегины напоминания про обед остались без ответа, так что российско-южноафриканское сотрудничество приобрело вполне привычные очертания: русские зеленоградцы пьют–гуляют, мы с Дэви – работаем. Первое знакомство зеленоградской публики с Дэви состоялось, народ разбежался, наконец-то наступила рабочая атмосфера, только вот результаты у Дэви на экране Digitasera почему-то не совпадали с теми, что у меня на экране Notebook. Могла быть куча разных причин: неправильно подключили Digitaser, не та ножка ПЗУ, не тот сигнал, не то подали на вход, не те ключи и т.п. Дэви последовательно, step by step стал перебирать всевозможные варианты, а мне пришлось все время отгонять от него вдруг откуда-то вылезших во время обеда зеленоградских коммерсантов. Они наперебой предлагали ему купить партию сникерсов, гербалайфов, шмоток и чего-то еще.

В поисках причины несовпадения результатов прошел весь день. Дэви все это время был с головой в работе, никак не реагировал на очередные серегины призывы «прерваться и перекусить», его ничего больше не интересовало на зеленоградском заводе (по моему, того что он там увидел в первые часы, было достаточно), важен был лишь конечный результат, ради которого он, знающий себе цену специалист, прекрасный и очень ответственный инженер, прилетел за тысячи километров из Южной Африки в Москву. И Дэви в конце концов победил! Победил этот бардак на зеленоградском заводе, победил советские Digitaserы, советские пьянки-гулянки, советских назойливых коммерсантов. К вечеру, когда весь завод уже окончательно вымер, результат на экране Digitasera у Дэви совпал с моим на Notebook. Это было бесспорное доказательство того, что схема «Ангстрем-3» запрограммирована в ПЗУ верно и работа выполнена успешно. Голодного, но довольного проделанной работой Дэви, я повез к себе домой, в свою двухкомнатную квартиру покормить и показать условия жизни советского инженера.

Не поверил. Нельзя, говорит, жить в таких условиях: 5 человек в двух комнатах. А где же гостиная? Я спросил про его условия жизни – двухэтажный дом в пригороде Кейптауна, три машины: Volvo – его, для поездок на работу, Wolkswagen – для поездок жены по магазинам, джип – для воскресных поездок к морю.

- А сколько стоит такой дом?
- Около 20 тыс. долларов.
- Дешевле моей квартиры в Москве. Давай меняться!

Порассказав Дэви о наших реалиях, я узнал от него некоторые подробности о жизни в Южной Африке. Рассказ Дэви немного отличался от того образа Южно-Африканской Республики, который так красочно описывала в течение многих лет советская пропаганда: расизм, апартеид, белые убивают черных, а те горят справедливым возмездием. «Да я когда из дома ухожу, то даже двери не запираю» - поведал Дэви. Тихая, спокойная страна, уважающая труд инженера, труд человека, приносящего общественную пользу. Попробуй-ка в Москве не запереть на три замка квартиру, уходя на работу, или, хотя бы для начала, не вытащить магнитолу из машины! Сколько раз мне потом приходилось убеждаться, насколько далека наша пропаганда от реальной жизни, как она примитивна, выпячивая у других то, что там может быть и есть, но незаметно, незначительно, и не замечая успехов в экономике. Ибо если говорить об экономике, то тут уж всем советским пропагандистам приходится совсем туго. Огромная страна Россия, куча природных ресурсов, все, абсолютно все условия для того, чтобы быть экономически высокоразвитой страной, быть на самом деле ведущей мировой державой не только по количеству танков и ракет, но и по товарам «ширпотреба», товарам для людей. Например, вся Южная Корея просто завалена китайскими товарами, дешевой китайской электроникой, одеждой, продуктами. А есть ли там российские товары? Один раз, увидев на корейском рынке армейский бинокль с серпом и молотом, я из любопытства купил его. Вот он, единственный российский товар в Корее! Но моя радость была преждевременной: под кучей чисто российских брэндов – автоматов Калашникова и ракет – в конце концов нашлась и простенькая надпись: made in China. Впрочем, о тех чувствах, которые испытывает советский человек, вырвавшись на волю из самой справедливой на свете страны, я постараюсь рассказать попозже и, может быть, даже не в этой книге. А сейчас пора назад, в Москву 1993 года, в контору г-на К..

Что же стало с этим телефоном дальше? А ничего. Он, конечно же, обладал гарантированной криптографической стойкостью, но достигалось это за счет сложности его реализации, откуда вытекали частые сбои при связи по не очень-то надежным советским телефонным каналам, различные неудобства для пользователя и, конечно же, высокая цена. К. по привычке заломил за него совершенно астрономическую цену: свыше 5 тыс. долларов за один аппарат и всем нагло врал про то, что этот телефон производится в Зеленограде. Надежды окучить по второму разу Центробанк не оправдались, там уже были сыты по горло его «Шуриками», а остальные потенциальные покупатели, едва узнав про цену, быстро делали от ворот поворот.

Менеджер предприятия должен трезво взвешивать свои возможности, прикидывать не только сиюминутные, но и отдаленные шаги. А К. все время наивно верил в разные чудеса. Один раз такое чудо свершилось с его допотопными калькуляторами, но все надежды на второе чудо (заграница нам поможет) были совершенно безосновательны. Потребности в подобных телефонах на российском рынке не было.

Глава 2

Тучи ходят хмуро…

Russia. Examples.

Есть в России старинный город Тверь, а в нем – Комсомольская площадь. Даже не площадь как таковая, а так, небольшой скверик в стороне от развилки дорог: налево свернешь – на Ржевское шоссе попадешь, прямо поедешь – так это прямо на Питер. А дороги с этом месте в славном городе Твери такие, как будто прошли по ним совсем недавно фашистские танки и отутюжила их в мирное время вражеская авиация. Но видать уже после войны будочка гаишника появилась на самой развилочке и светофорчик, да еще где-то в небе, на трамвайных проводах – маленькая табличка «СТОП». Метров за 5 до светофорчика.

А ездят по этой дороге теперь часто машины с московскими номерами, которые хоть и останавливаются у светофорчика, но не под самой табличкой «СТОП», а проехав вперед эти самые 5 метров, поближе к повороту на Ржевское шоссе. Да и поди заметь ее, эту табличку: если едешь там впервой, то только успевай канавы объезжать, эти достопримечательности тверские, вверх-то уже и смотреть некогда. И вот только иноземный водила поворачивает на стрелочку в светофочике, как тут же выскакивает к нему из будочки гаишник с волшебной палочкой и, придав челу своему строгий Государственный вид, вещает:

- Почему нарушаем Правила Дорожного Движения?

Недоумевает водила: только что он демонстрировал чудеса фигурного вождения, пытаясь объехать все канавы на дороге Республиканского значения, превысить скорость здесь в принципе невозможно, на красный свет не ездил, терпеливо ждал стрелочки, где, какие пункты этих священных Правил он нарушил? И тут гаишник, сияя от распирающего его удовольствия, показывает своей волшебной палочкой на болтающуюся как одинокий листочек на трамвайном проводе табличку «СТОП» и как вдумчивый педагог объясняет нерадивому водиле:

- Правила предписывают остановиться у таблички «СТОП», а Вы заехали за нее.

Мне в тот раз повезло: гаишник попался молодой и еще не окончательно растерявший простые человеческие чувства. Я попросил его оценить по любой мыслимой шкале состояние охраняемого им дорожного полотна, к тому же ехал на дачу с семьей, и он после 20-минутной душевной беседы поведал мне местные гаишные тайны.

- На эту точку наше начальство всегда спускает повышенный план по протоколам. Все прекрасно знают, что иногородние машины эту табличку, как правило, не замечают, вот и приходится здесь быть ударником труда. Если я этот план не выполню, то меня же потом лишат всех благ.

В первый раз я видел, как гаишник стыдился своей работы. Это уже было явно аномальное явление в российской действительности, ну а дальше последовало еще аномальней:

- Давайте я составлю протокол, что Вы переходили улицу в неположенном месте. Штраф за это мизерный, 0,1 минимальной зарплаты, в Москву его даже присылать не будут – накладные расходы дороже. А для меня этот протокол пойдет в мой дневной план.

Так я стал пешеходом-нарушителем.

End of example

Эйфория патриотизма быстро прошла. В ЦБ система защиты телеграфных авизо работала стабильно уже около года, самая интересная пора прошла, все вернулось на свои чиновничьи круги. Заниматься эксплуатацией системы защиты авизо в ЦБ стали уже не те люди, с которыми мы ее внедряли, все опять вернулось к многочисленным бумагам, согласованиям и перестраховкам. Со скрипом ФАПСИ дало «добро» на эту систему, внеся, естественно, свои косметические модернизации, но по тому тягомотному процессу, которым сопровождалось получение этого разрешения, стало ясно: о внедрении системы «Криптоцентр» в ЦБ, какой бы хорошей она ни была, нечего и мечтать. Не дадут. Даже работающую в таких крупных подразделениях ЦБ, как ЦОУ и ОПЕРУ, программную систему «Криптоцентр-АВИЗО», моделирующую работу с калькулятором на персональном компьютере, ФАПСИ не признавало. Нашли универсальное решение: эта программа используется в «тестовом» режиме, а основная работа якобы осуществляется с помощью калькулятора. На самом деле калькуляторы валялись в сейфах без дела, а вся реальная работа осуществлялась с помощью «Криптоцентра-АВИЗО».

Стена, бетонная чиновничья стена, совершенно непробиваемая. Иногда дело доходило до полного абсурда. С самого начала использования этой системы Центробанк хотел провести такую модернизацию калькулятора, чтобы алгоритм выработки КПД для телеграфных авизо был бы оригинальный, разработанный специально для ЦБ, и реализован в специальной версии калькулятора, которую назвали «Электроника МК - 85 Б». Это разумное требование, поскольку калькулятор «Электроника МК-85 С» был предназначен для армии, для широкого применения, и не исключалось, что он мог попасть в руки криминала. Применение же специализированного калькулятора, изготовленного специально для ЦБ и содержащего уникальный алгоритм выработки КПД, заведомо повышало надежность системы защиты авизо. И вот в конце 1993 года ЦБ заключил с кл-овской конторой Договор на разработку «Электроники МК-85 Б», в котором всю техническую часть – разработку оригинального алгоритма выработки КПД и программирование модели калькулятора на компьютере – пришлось выполнять мне. Но поскольку в таких огромных системах, как сеть РКЦ Центробанка, самая большая проблема – переходный период, т.е. обеспечение устойчивой работы системы при внесении в нее изменений, то одним из требований ЦБ было, чтобы калькулятор также поддерживал все прежние алгоритмы, на которые к тому времени уже было получено разрешение ФАПСИ. А в назначенный день «Х» по команде все переводят калькулятор на новый режим работы.

В это время у меня уже было намного больше понимания о том, что необходимо ЦБ и какие есть для этого возможности в калькуляторе. Нужно было реализовать хеш-функцию, в которую подмешиваются знаки секретного ключа, причем в процессе подмешивания и знаки ключа и хешируемая информация принимают участие в выработке новых подстановок, которые в свою очередь используются в схеме типа «Ангстрем-3».

Детальное описание подобного способа построения хеш-функций (только без подмешивания знаков ключа) я приводил в книге «Практическая криптография», по такому же принципу строились хеш-функции для асимметричной электронной подписи в системе «Криптоцентр».

Подробное описание этого нового алгоритма я по просьбе ЦБ сразу же отправил в ФАПСИ с тем, чтобы получить разрешение на его использование в ЦБ. Но поскольку такое разрешение возможно только после криптографической экспертизы этого алгоритма, а она может продлиться достаточно долго, то было принято решение начать создание калькуляторов «Электроника МК-85 Б» со старыми и новым алгоритмом, наладить их выпуск, оснастить ими все РКЦ, которые вначале будут работать на прежнем, широко распространенном алгоритме, а переход на новый уникальный алгоритм отложить до получения на него разрешения ФАПСИ.

И вот завод «Ангстрем» в Зеленограде выпустил несколько тысяч калькуляторов «Электроника МК-85 Б», в каждом из которых был уже реализован новый, уникальный, разработанный специально для ЦБ алгоритм выработки кода подтверждения достоверности телеграфных авизо. Калькуляторами «Электроника МК-85 Б» оснастили все РКЦ, люди стали работать ни них, используя прежний, старый и общеизвестный алгоритм. А от ФАПСИ по поводу нового алгоритма нет никакого ответа: ни положительного, ни отрицательного. Все как в воду кануло! Затрачена масса усилий на разработку этого калькулятора, решены все технические проблемы, огромная банковская сеть готова к переходу на уникальный алгоритм. Но чиновники ФАПСИ – важнее всего!

Так и остался этот уникальный алгоритм «вещью в себе». А я получил еще одно наглядное подтверждение прописной истины: вся власть в России принадлежит чиновникам. Могут меняться лозунги, вчера были «Вперед, к победе коммунизма!», а сегодня – «Вперед, к победе рынка!», но чиновничья власть в нашей стране неизменна. А отсюда легко вытекает основная мотивация действий многих людей – выбиться в чиновники. Не производство товаров и услуг, а упрямое карабкание по чиновничьей лестнице – вот высший смысл жизни.

А причина – изобилие нефти и прочих природных богатств. Это легкие деньги, доходы от которых и распределяют чиновники, они и дают эту чиновничью независимость и практически полную безответственность за принимаемые чиновничьи решения. Основная масса населения, в глазах чиновников, - это потенциальные конкуренты на их долю природных богатств, на их собственность, называемую иногда еще почему-то «общенародной».

Чиновники ФАПСИ – это особая песня, которую надо петь стоя. В подобных закрытых системах намного больше сохранился ядовитый дух сталинизма и стремление к бесконечным запретам. В 1991 году, после неудачного путча, из 8 ГУ КГБ уволилась масса народа, начальники были в панике, но примерно через полгода этот шок прошел и чиновники воспряли духом. В смысле стали придумывать, какие бы запреты и неприятности заготовить тем, кто решил покинуть систему КГБ. Первое предложение было очень характерным: законодательно закрепить, что человек, уволившийся из ФАПСИ, 10 лет не имеет права работать по специальности. Различные Конституции и Права человека – это все где-то там, далеко, а здесь свои нравы и обычаи, как при Сталине – 10 лет по рогам. В явном виде это предложение не прошло, все-таки такой сталинизм по ту сторону забора с колючей проволокой уже отошел в прошлое. Но неявно, не мытьем, так катанием, ФАПСИ методично перекрывало кислород всем своим бывшим сотрудникам, которые не захотели оставаться в «действующем резерве». Апофеозом чиновничьих усилий явился Указ Президента РФ № 334, согласно которому любой криптографический «чих» требовал разрешения ФАПСИ. Указ, абсолютно оторванный от реальной жизни, допускающий неограниченное множество трактовок, пытающийся объять необъятное криптографическое пространство. Мне доводилось уже комментировать его в книге «Практическая криптография». Но этот Указ был принят в 1995 году, а вся описываемая выше эпопея с калькулятором «Электроника МК-85 Б» происходила двумя годами раньше, на Центральном Банке ФАПСИ тогда еще только оттачивало свое чиновничье мастерство.

Все больше и больше сгущались тучи. И не только над криптографией, но и в целом по стране становилось все яснее, что декларированные в 1991 году свобода и демократия – мираж, что в реальной жизни произошла всего лишь смена лозунгов и чиновников. Зависимость же от них простого человека, которым я теперь с полным основанием мог себя называть, отнюдь не уменьшилась, если не сказать большего. Все чаще и чаще приходила в голову крамольная мысль: и стоило ли связываться с этим Центральным Банком? Что в результате? Выгнали за полгода до офицерской пенсии, работа по специальности под вопросом, Гениальный директор, с которым я связался, такой, что на него надеяться нельзя, а у меня трое детей, кормить их чем-то надо. Что там в анекдоте говорил Иосиф Виссарионович Лаврентию Павловичу, глядя на портрет Пушкина?

- Души прекрасные порывы!

Глава 3

Break

Russia. Examples.

Есть в Тверской области чудесный уголок – Лесной район. Это на самом севере области, везде – леса, вековые ели и сосны, тихая речка Мологa вдали от цивилизации, на ней еще можно порыбачить, великолепные песчаные пляжики для купания, в окрестных лесах бесконечное множество грибов и ягод, иногда даже можно встретить лесных зверей из детских сказок: зайца, лису, волка и медведя. От Москвы – 400 километров, на машине – 6 часов езды, и ты попадаешь в совершенно иной мир, где нет суеты, где чистый воздух и родниковая вода без хлорки. Здесь, как нигде еще в России, я мог почувствовать себя свободным, а стоящая на берегу Мологи старинная русская деревня Гузеево стала местом моего летнего паломничества. Я построил в ней деревенский дом, и все время, пока я находился в Москве, все мысли – только о том, как летом поехать отдохнуть в Гузеево.

А как живут там местные жители? Существовавший при Советской Власти совхоз …. нет, не развалился. В нем просто уже несколько лет никому не платят денег, а так – Председатель, Правление – все есть. Народ давно уже перешел на самое что ни на есть натуральное хозяйство в российских условиях. А именно: все молодые и работоспособные уехали в райцентр, остались одни пенсионеры – старики и старухи, да местные алконавты, которые летом собирают и продают заезжим кооператорам за копейки грибы, ягоды или рыбу и тут же пропивают полученное, а зимой – христарадничают перед старухами, притаскивая им за кусок хлеба или стакан самогона воды и дров. Все стараются сажать картошку, а вот коров в этой благодатнейшей для них местности уже практически не осталось: заготавливать на зиму сено некому.

Зимой деревня – словно вымершая, голодные волки по ночам рыскают по деревенским улицам в поисках непривязанных собак. Зато летом, за счет приезжих из Москвы и Питера, деревня оживает, все местные жители относятся к «дачникам» хорошо, простора, леса и реки на всех хватает с избытком.

До ближайшей деревни – совхозного центра Борисовское – около 16 километров по лесу, до районного центра Лесное – около 47 километров по той же лесной дороге, которая, по нашим российским понятиям, вполне приличная для езды по ней даже на легковой машине. А для местных аборигенов 47 километров – мелочь, пешком пройти можно, хотя раз в неделю ходит автобус.

Есть даже электричество, высоковольтка протянута по просеке через дремучие леса. А посему местные алконавты или даже заезжие коммерсанты любят воровать с нее провода. Это же цветной металл, его можно, как грибы или ягоды, сдать в пункте приема «лома цветных металлов» и заработать. А несколько окрестных деревень после этого несколько недель сидят без света. Крадут, в основном зимой, когда все вокруг вымирает, но бывает, когда год на грибы-ягоды неурожайный, то и летом.

И вот в одно прекрасное лето сидим мы в Гузеево без света неделю, затем другую… Жарко, еда у всех без холодильников быстро портится, нашлась в деревне одна энергичная женщина, Алина Александровна, которая поехала на автобусе в райцентр Лесное чтобы узнать, когда можно на него хотя бы надеяться. А обратно пешком отправилась, эти самые 47 километров – российский вариант марафонской ходки. Мы в это время с детьми как раз возвращались на своей машине из райцентра, по дороге встретили ее и подвезли до деревни. А она нам поведала о деталях своей миссии.

Недалеко (сравнительно) от райцентра Лесное есть Удомельская АЭС, которая обеспечивает электроэнергией и райцентр Лесное, и совхозный центр Борисовское. А вот Гузеево, которое от Борисовского всего-то в 16 километрах, обеспечивают электроэнергией Бежецкие энергосети, которые на другой стороне Мологи и высоковольтка от которых тянется до Бежецка многие километры по глухим лесам. Почему так получилось – теперь уже никто не знает, давно это было, еще при социализме. А сейчас, в эпоху демократического капитализма, протянуть 16 километров проводов по довольно приличной лесной дороге от Борисовского до Гузеева – большая проблема, которую местные Чубайсы решить не в состоянии. Они без проблем могут только цены на электроэнергию увеличивать.

- Пишите прямо Путину!

Так посоветовали ей в районной энергоконторе.

Зачем Путину? Мелко! Лучше сразу Генеральному Секретарю Организации Объединенных Наций!

Уважаемый господин Генеральный Секретарь!

Есть ли у вас там, в Объединенных Нациях, столбы и провода? Если есть, то снарядите, пожалуйста, батальон миротворческих сил и пошлите их к нам, в Лесной район, провести 16 километров высоковольтки между Борисовским и Гузеево. И поставьте, пожалуйста, охрану у каждого столба, а то через месяц опять все провода порежут и будем мы снова сидеть без света и холодильников.

End of example.

Чувствовалось, что мое пребывание в конторе у К. подходит к естественному финалу. К. решил, что Центробанк уже выполнил роль дойной коровы, больше с него в таких масштабах не урвать, а посему основной его задачей стала прихватизация добытого. Ведь формально, в период работы с ЦБ, его контора считалась хоть и малым, но государственным предприятием, которое учредил зеленоградский завод. Следовательно, Центробанковский лимон тоже формально был пока государственным, хотя в Уставе, естественно, были соответствующие финансовые полномочия у Гениального директора. А при прихватизации конторы все имущество переходило к «трудовому коллективу». Поскольку этот трудовой коллектив менялся со скоростью кометы, то из потенциальных претендентов оставался чуть ли не один К. Поэтому его естественной для такого человека задачей был переход от условного «чуть ли» к безусловному «один К.». И я был ему в этом заметной помехой.

Не могу сейчас сказать, были ли тогда у меня реальные шансы бороться с ним за свою долю Центробанковских богатств. Ведь в момент заключения многих Договоров с ЦБ я был на действительной военной службе, т.е. совершенно бесправным. У меня не было никакого контракта с ним и с его конторой, не было четко оговоренных прав и обязанностей. Официальная зарплата соответствовала уровню мелкого клерка, готовящего исходящие документы, иногда с «барского» плеча К. дополнительно подкидывал по сомнительным Договорам подряда, а потом полгода вспоминал о совершенных им благодеяниях. Мне же хотелось самостоятельности, к его глупостям и выходкам очень скоро стало испытываться стойкое отвращение. Единственное, что радовало – те программы, которые мне удалось за это время подготовить. Это система «Криптоцентр» для широкого применения и «Криптоцентр-АВИЗО» для кодирования авизо в ЦБ. Программы собственные, оригинальные, «Криптоцентр-АВИЗО» успешно работал в ЦБ, а обычным «Криптоцентром» заинтересовались некоторые банки, причем люди, интересовавшиеся этими программами, были, как правило, интеллектуально намного выше примитивного К., его байки про «ведущего мирового авторитета в криптографии» вызывали у них, мягко говоря, непонимание, мне после таких пассажей приходилось с удвоенной силой разъяснять им, что не все здесь такие. И вот в какой-то момент пришло понимание того, что надо сделать выбор: или заниматься тяжбами с К. по поводу его прихватизации, или отдать предпочтение криптографии, развитию того, что уже было сделано, внедрению новых идей, новым разработкам.

Заказчик, срочно нужен был заказчик на эти идеи, который готов был бы меня поддержать, который бы поверил, проявил нетривиальный подход, как тогда, в1992 году в ЦБ. А найти такого заказчика – большая проблема, особенно с учетом того, что ФАПСИ вовсю закручивало криптографические гайки, стремясь придавить всех, кто вышел из под контроля. «Криптоцентр» - это только моя визитная карточка, за ним ведь могут последовать и другие, еще более интересные системы. Южноафриканцы, посмотрев «Криптоцентр», оценили возможности его продажи на рынке Южной Африки. Пришла бумага: 6 миллионов долларов. Но попробуй получи на это разрешение ФАПСИ! Государство в награду за все мои труды наградило меня статусом «невыездной» непонятно на сколько лет. На 5 – это минимум. Но в ОВИРовской анкете почему-то требуется указывать места работы за последние 10 лет. А уж секретностью я был вымазан по самые уши, 5 лет точно нет никакого смысла даже рыпаться.

И вот где-то в конце 1994 года другой мой настоящий коллега, Анатолий Григорьевич, который успел поработать торговым менеджером где-то около полугода в конторе у К. и которого я уже упоминал в этой книге, вышел на один очень крупный банк, который даже сейчас я не могу назвать своим именем: ведь драконовский криптографический Указ №334 Президента РФ еще никто не отменял. Пусть это будет просто W-банк. Этот банк закупил сравнительно большую партию установок программы «Криптоцентр» и сразу же зашла речь о дальнейших шагах нашего возможного сотрудничества. Банк имел множество филиалов во всех крупных городах России и поддерживал связь с ними по электронной почте Sprint-Net. Требовалось, используя систему «Криптоцентр» как основу, разработать, наладить и запустить в промышленную эксплуатацию автоматизированную систему защищенного электронного документооборота между филиалами банка и Центром.

Как я был рад вновь общаться с нормальными и интеллигентными людьми! Вместо полубезумных реплик К. – диалог технических специалистов, составление технических заданий, проектирование, разработка, отладка, проверка, - все то, что составляет основу реальных дел, а не пустого фантазерства. Но неужели опять все финансы отдавать К.? Он же не способен ни на что, кроме демагогии, подрывающей авторитет инженера, его участие в этом проекте – гибель проекта.

Однако сам К. почему-то считал, что я являюсь его полным вассалом и все мои работы будут проходить только через его фирму. С соответствующими финансовыми отчислениями – 50% ни за что, только за то, что он сам провозгласил себя великим. А узнав, что такие условия меня не устраивают, устроил, как всегда, театр одного актера: я тебя кормлю-пою, а ты такой неблагодарный.

Он мне уже надоел до чертиков. Но вот-вот должны были поступить Центробанковские деньги за программы, которые я писал специально для ЦБ около года и К., по широте своей душевной, обещал мне с них аж целых 30%. Причем обещал не только устно, но даже письменно. И вот деньги пришли, но вместо моей честно заработанной доли я опять получил только его демагогию.

Break! Пора прерывать гениальность Гениального директора. Выслушав в очередной раз его словоблудие, я на сей раз как можно спокойнее сказал:

- А знаешь что, К., иди-ка ты на х…!

Больше я никогда не видел этого человека.

Глава 4

Next step

Russia. Examples.

Опять милый моему сердцу Лесной район Тверской области. Лес там – всему голова, это основа благосостояния жителей райцентра и окрестных деревень. Лесопилки и различные деревообрабатывающие кобинатики – вот единственная жизнеспособная промышленность, способная там прокормить народ. Бревна, срубы, доски, вагонка, летние дачные домики – все это затем отвозится на продажу в Москву, а иногда даже и в Финляндию – она сравнительно недалеко. Бензопила, острый, как бритва, топор, стамески, долото и всякие другие столярные премудрости – все это в крови у местных жителей, искусство строить избы, колодезные срубы, бани и все прочее из дерева передается из поколения в поколение. Леса вокруг много, но и вырубают его тоже по-черному. А ведь дерево – не трава, за одно лето не вырастет. Но пока еще вырубить весь лес в Лесном районе не удалось. Слишком уж много его там.

Где рубить лес – так называемые порубочные билеты - это определяет местное начальство, районная администрация - бывший райком КПСС. Есть места для рубки получше, туда и подъехать проще, и деревья там прямые и стройные, а есть и похуже – туда проехать можно лишь зимой по замерзшему зимнику и деревья там на болотине похуже, с гнильцой.

И вот один раз, в базарный день – пятницу, идем мы с местным аборигеном Юрой, помогавшим мне строить дом, по центральной базарной площади райцентра Лесное. И вдруг Юра поведал мне одну из маленьких местных хитростей.

- Вон видишь на обочине черная Волга? Это машина главы администрации.
- А зачем она здесь стоит?
- Из нее наблюдают, кто где хлеб покупает. В палатке – наш местный хлеб, он похуже и подороже. А с фургончика продают хлеб из Твери, он получше и подешевле. Но все местные стараются покупать только местный хлеб, потому что если кто-то пойдет покупать хлеб в фургончике, глава администрации его запишет и потом припомнит это, когда будут распределять порубочные билеты.

Вот с этой забавной сценкой из жизни российской глубинки у меня теперь всегда ассоциируется наукообразный термин «административный ресурс».

End of example

- Хороший ты разработчик, но все делаешь сам, в одиночку. А если с тобой что-то случится?

Такие речи мне часто приходилось слышать от чиновников ЦБ, когда речь заходила о внедрении программы «Криптоцентр-АВИЗО». В их представлении разработка программного обеспечения обязательно должна вестись коллективно, большим колхозом, в котором есть Председатель, Правление, Партийная организация, Местком и множество иных начальников. Так привычнее, но это, как правило, система коллективной безответственности. Такие системы, наверное, хороши в каких-то иных областях деятельности, но только не в математике и программировании, где конечный результат не зависит от начальства. Не может генерал приказать программе перестать выдавать неверный код подтверждения достоверности авизо, избавить ее от «глюков». Это может сделать только программист, который писал эту программу. А сделать ему это будет тем легче, чем меньше постороннего народа совало свой нос в программу. В идеале – если все основные процедуры делал один человек, используя, может быть, только очень хорошо проверенные результаты других людей. А если большую программу одновременно пишет целый колхоз, все модули еще как следует не проверенные, с возможными ошибками, затем все это добро собирается в одну кучу – все, гиблое дело, такой программе нельзя доверять выполнение серьезных задач: непременно «заглючит», а программисты-колхозники будут до бесконечности обвинять в этом друг друга. Мне такое программирование не по душе, поэтому, по возможности, все жизненно важные процедуры в программе я стараюсь делать сам или использовать только то, что уже неоднократно испытано и чему можно доверять (но и все равно обязательно проверять!).

И вот огромный W-банк встал перед выбором: а не страшно ли связываться с программистом-одиночкой? Если бы в этом банке были одни чиновники, то наверняка вместо реальной разработки автоматизированной системы электронного документооборота получились бы бесконечные дебаты на эту тему, но тут мне опять повезло: нашелся в W-банке человек, который отмел все эти дебаты простым и понятным аргументом:

- Всю ответственность я беру на себя!

Это был Владимир Константинович Тяпкин, бывший полковник Советской Армии, инженер, кандидат технических наук.

Что же требовалось W-банку?

Первый раз, когда я появился там, мне запомнилась одна картинка. Старинное здание напротив Кремля, комнаты не то что дореволюционной, а прямо доисторической постройки, типа тех, что можно увидеть в фильме «Петр I» или «Иван Васильевич меняет профессию». Одна комната была похожа на боярскую кладовку: размером примерно 5x5 метров, но самое интересное – наклонный потолок. С одной стороны комнаты – сравнительно высокий, а с противоположной – не больше, чем метра полтора, встать и выпрямиться невозможно. Работало в этой комнате управление информатики W-банка, с одной стороны (с высоким потолком) сидела мужская часть, а с другой, где встать невозможно – в рядок три молодых девушки, которые целый день отправляли по Sprint-Net в многочисленные филиалы банка различные распоряжения, балансы, сводки, статистические отчетности и всю прочую документацию, составляющую основы жизнедеятельности любого банковского организма. И вот требовалось высвободить этих девушек, вытащить их из этой кладовки на свет божий, а всю нудную и однотипную работу переложить на автоматизированную систему защищенного электронного документооборота.

Криптоцентр позволял только шифровать и подписывать файлы, но он не был приспособлен для их рассылки. К тому же у W-банка были свои, специфические требования к рассылке: при получении адресат должен автоматически посылать отправителю подтверждение получения, заверенное своей электронной подписью. Это требование было основано на нескольких реальных случаях из жизни банка. Один раз девушка ошиблась и при отправке платежных документов по Sprint-Net указала неверный адрес получателя. Пока с этим разобрались, произошла задержка платежа и клиент выставил банку штрафные санкции. В другой раз наоборот, банк выставил по Sprint-Net клиенту по каким-то основаниям штрафные санкции, но клиент отказывался их оплачивать, впоследствии уверяя, что не получал их.

Общая причина этих и других подобных недоразумений – изобилие ручных операций при существовавшем в то время электронном документообороте, отсутствие четкого разграничения, когда и в какой момент времени ответственность за электронный документ переходит от отправителя к получателю, большая нагрузка на обслуживающий персонал, который, как и все люди, может иногда и ошибаться. И тут я еще раз смог убедиться, что криптография – это хоть и важная, но только одна составляющая в банковской системе электронного документооборота. Другая составляющая, хоть и не такая изящная, но не менее важная – электронная бюрократия, программа-чиновник.

А не получится ли так, что программа-чиновник оставит без куска хлеба человека-чиновника? Одну подобную сцену мне довелось в явном виде наблюдать в ЦБ. Первая версия программы «Криптоцентр-АВИЗО» была очень простой: девушка набирала с клавиатуры все реквизиты авизовки, программа высчитывала по ним код подтверждения достоверности и выдавала его на экран. В таком виде эта программа первоначально работала в ОПЕРУ – крупном подразделении ЦБ, где ежедневно обрабатывали

несколько сотен авизовок. Под кодирование авизо была создана специальная группа, около 10 человек, но на самом деле подготовку исходящих авизо осуществляла совсем другая группа, а подготовленные пакеты авизо в виде базы данных в формате DBF передавались на дискете в группу кодирования. Здесь их распечатывали и для кодирования заново вводили в компьютер все реквизиты вручную. Когда мне впервые поведали эту таинственную Центробанковскую технологию, то я позволю себе здесь не приводить свои эмоции по этому поводу. Вскоре я принес в ОПЕРУ новую версию «Криптоцентра-АВИЗО», в которой уже был автоматический ввод всех необходимых для кодировки реквизитов из DBF-файла. Девушка – операционистка, запустив эту программу, нажала одну клавишу «ENTER» и на экране через секунду высветился результат:

Успешно закодировано авизо – 50

Первая реакция девушки:

- Ну все, теперь нас всех разгонят!

Но, странное дело, никого не разогнали. Просто вместо дурной и бестолковой работы они стали заниматься анализом баз данных, получением сводных характеристик, повышением своей компьютерной грамотности. А система «Криптоцентр-АВИЗО» тоже при этом развивалась, я все время добавлял туда по просьбе ОПЕРУ все новые и новые возможности. Одна задача оказалась достаточно нетривиальной, но в то же время жизненно очень важной.

Речь зашла о блокировке возможности повторного приема одного и того же авизо. Это был реальный случай из практики работы ЦБ и начальство потребовало срочно принять меры. Эти меры в первую очередь касались крупных РКЦ, где очень большой объем обрабатываемых авизо. Если РКЦ работало с калькулятором, то тут, опять же, оставалось надеяться только на человеческую интуицию. Но в ОПЕРУ ни одного дня с калькулятором не работали, программа «Криптоцентр-АВИЗО» там использовалась уже давно, к ней все привыкли и настало время сделать ей очередной Upgrade. Проверку на повторяемость можно было осуществить с помощью базы данных, но вся беда была в том, что при кодировании авизо по каким-то прихотям ФАПСИ категорически запрещалось пользоваться компьютерными сетями, хотя работали одновременно несколько человек на разных компьютерах. Компьютер при кодировании должен работать в автономном режиме, следовательно, об использовании общей базы данных в режиме on-line не могло быть речи. Пришлось вводить локальные системы учета для каждого рабочего места, все записи в которых в конце рабочего дня подписывались операционисткой с помощью «Криптоцентра» и затем сливались в общую базу данных, в которой и происходила проверка на повторяемость.

Но одной вещи в ОПЕРУ мне так и не удалось сделать – это избавить их от необходимости таскать дискеты из комнаты в комнату при общении с группой, которая готовит исходящие авизовки. Все были согласны: система общения должна быть автоматизирована: подготовил, зашифровал, подписал, послал по сети – принял, проверил подпись, расшифровал, использовал – все в автоматическом режиме, никаких разгуливаний с дискетами по комнатам. Но получить на это разрешение ФАПСИ – это было выше всех моих усилий! И так почти 10 лет все эти девушки своими ножками оттаптывали чиновников ФАПСИ, которым все эти проблемы были глубоко безразличны.

Но хождение из комнаты в комнату в ЦБ – это всего лишь капля в огромном океане вреда, который нанес тысячам людей чиновничий монополизм ФАПСИ. Вспомним очереди в налоговую инспекцию, регистрационную палату, во всякие обязательные фонды, живущие на деньги налогоплательщиков, но не создающих для этих налогоплательщиков никаких, даже самых элементарных удобств. Здесь же сама напрашивается автоматизированная система защищенного электронного документооборота! Вместо инспекторов – сервера, вместо поездок людей с различными бумагами – пересылка файлов по электронной почте, в зашифрованном виде и с электронной подписью. Так, глядишь, и времена настанут, когда «черного нала» и взяток поменьше будет. Технически сложно? Да, безусловно, причем не только технически, но и организационно сложно сделать первые шаги. Но все эти проблемы постепенно решаемы, это я могу сказать по своему собственному опыту работы с W-банком. Но при одном непременном условии: если такая госструктура как ФАПСИ будет заниматься только тем, что ей положено по ее статусу – ПРАВИТЕЛЬСТВЕННОЙ связью, и не будет совать свой ушлый нос туда, где нет военных и государственных секретов.

К счастью, W-банк трезво оценивал ФАПСИ. Разрешено все, что не запрещено законом, а если чиновники не могут грамотно составить закон, то это их проблемы. Первая версия автоматизированной системы электронного документооборота для W-банка была создана примерно через полгода. Конечно, первый подобный блин всегда получается немного неуклюжим, не совсем оптимальным, но он заработал! Это была

еще DOS-версия, но даже в таком первобытном виде эта система устроила банк намного лучше, чем работа до одурения молодых девчонок. А в моей криптографической эпопее наступил Next step – разработка автоматизированных криптографических систем под конкретного заказчика. Я наконец-то получил долгожданную самостоятельность!

Глава 5

Бомбила

Russia. Examples.

Тот год выдался в Лесном районе изобильным на клюкву. Окрестные леса полны болот, а на болоте, на кочках, растут эти красненькие бусинки, которые, кажется, кто-то рассыпал по зеленому болотном мху.

Сбор каждого сорта ягод имеет свои особенности. Малина растет на довольно высоких кустах, поэтому за ней надо меньше нагибаться, но и лазить по этим непролазным кустам сложно. Черника или брусника – в лесу, обычно в сухом, сосновом, но за этими ягодами надо нагибаться, садиться на землю или вставать на колени. А вот клюква – та на болоте. Под ногами постоянно хлюпает вода, на землю не сядешь, а нагибаться надо так же, как за черникой или брусникой. Да и ходить по болоту труднее, чем по сухому сосновому лесу, похлюпаешь часа три-четыре – и все, сил больше нет, хочется поскорее вылезти на твердую землю.

Мне очень нравится собирать клюкву, уж больно красиво она рассыпана по болотистым кочкам, но больше, чем сравнительно небольшое 8-литровое пластмассовое ведерко, за день набрать никогда не удавалось. Да и дойти до болота – путь довольно неблизкий: сначала до леса, а потом еще по лесу до самого болота. А по самому болоту еще надо походить, чтобы найти места, где клюква покрупнее и собирать ее полегче. В общем, одного дня сбора клюквы мне хватало на то, чтобы потом еще пару дней от этого сбора «отходить».

Местные жители собирают клюкву, в основном, на продажу. Кооператоры покупают у них ее по 3 рубля за килограмм, а в Москве на рынках килограмм клюквы стоит уже 30 рублей и то не такой свежей и крупной, какой я ее видел в натуральном виде. И вот один раз, где-то уже ближе к концу сентября, я возвращался на машине в Москву со своего Гузеевского поместья и по лесной дороге до райцентра подсадил подвезти одного местного мужичка. Он-то и поведал мне о том, как и в каких масштабах собирают окрестные сельские жители клюкву. Я не могу ручаться за то, что все в его рассказе было правдой, но по некоторым другим признакам, которые мне доводилось видеть своими глазами в той местности, особо сильно он не выдумывал, да и не было ему никакого смысла выдумывать.

В начале сентября к нему в гости приехали брат и сват. Где-то примерно с 10 сентября в тех краях официально открывается сезон сбора клюквы, и они, как только открыли сезон, втроем за неделю собрали около 3 центнеров клюквы.

- Мужики вдвоем на болоте черпаками ее собирали и в мешки, а я эти мешки домой таскал. Вечером еще даже силы оставались, чтобы телевизор посмотреть. И мы столько денег заработали!

По 3 рубля килограмм, 3 центнера – это 900 рублей, около тридцати долларов. По тем краям за неделю - огромные деньги. А у меня никак не укладывается в голове даже сама возможность такой адской работы - набрать столько клюквы. Но местный народ, видимо, уже доведен безденежьем до такого состояния, что согласен даже на такие каторжные условия. И это всего в 400 километрах от Москвы!

End of example

Встать, не доезжая метров 5 до светофора, в крайний правый ряд. За 3 секунды до зеленого – рви, педаль газа в пол до упора. Только так на перекрестке можно вырваться вперед и обогнать конкурентов, а призом в этой гонке – очередной клиент рублей на 50, а если повезет – то и на 100. Это – народная забава, называемая «подбомбить», т.е. выехать на своей машине в роли частного и никем не контролируемого такси. В Москве вечерком, часов в 8, поймать «бомбилу» нет никаких проблем: поднял руку и меньше чем через минуту можешь даже выбирать варианты.

При новой демократической жизни бомбилы начисто переиграли государственные такси: по несметному количеству, по ценам, по доступности. Государственное такси должно еще кормить чиновников: начальников, бухгалтеров, налоговую инспекцию, различных проверяющих и прочая, прочая, прочая. Бомбила, чаще всего, кормит только сам себя, сам себе начальник, бухгалтер, автослесарь, сват, кум и брат.

А поэтому и цены у бомбилы намного ниже, чем у шашечного такси, все давно уже поняли эту очевидную истину. Пытаться государству (в лице заинтересованных чиновников) запретить «подбомбить» - это все равно, что объявить войну, которую, как и партизанскую, выиграть невозможно. Слава богу, что чиновники это поняли, и никаких ощутимых актов агрессии по отношению к бомбилам не проявляли.

Ну а меня-то, образованного человека, что потянуло на эти игрища? Во-первых, конечно, мальчишеское желание погонять по городу на машине, как когда-то в детстве на велике. Тем более, что Москва, усилиями Главной Московской Кепки – Юрия Михайловича Лужкова – преображалась прямо на глазах. «Единственное, что простой народ получил от этой демократии – московскую кольцевую автодорогу» - так достаточно просто и понятно объяснил мне текущий политический момент один клиент. Центр города стал чистым и красивым, признаки цивилизации стали проникать и на окраины. Посмотреть на все своими глазами, порадоваться хоть каким-то светлым сторонам в довольно-таки беспросветной жизни – это тоже стало возможным в результате «бомбежек». Во-вторых, естественно, сугубо прагматические цели – подзаработать денег. Хоть и был у меня теперь постоянный клиент – W-банк, но его финансовая поддержка не была особо щедрой. На уровне среднего программиста банка, где-то 400-500 долларов в месяц. Правда, в отличие от программиста банка, я не состоял в штате банка и работал дома в удобное для меня время. Обычно весь день я непрерывно просиживал у компьютера, а к вечеру, чтобы немного развеяться и хоть как-то отдохнуть от монитора, выезжал подбомбить, так сказать, на вечерний выгул железного коня, хотя иногда, когда финансовые проблемы сильно поджимали, приходилось выезжать на бомбежку и среди бела дня.

И, в третьих, это была школа реальной жизни, общения с простыми людьми, тренировка умения быстро отличать жуликов от порядочных людей. Здесь у меня выработались свои особые критерии, свои правила поведения: ведь водитель-бомбила – это одиночка, рассчитывать может только на себя. Естественно, что бывают случаи обмана, нетривиальные ситуации, поэтому важно правильно спрогнозировать развитие событий, в первый раз видя человека, подсевшего к тебе в машину клиентом. Эти правила достаточно простые и естественные: не возить пьяных, шумные компании, лиц кавказской национальности, при дальних поездках требовать предоплату, не верить слишком заманчивым обещаниям при назначении цены, по возможности, «бомбить» в своем знакомом районе, более удачная бомбежка всегда бывает в праздники и выходные, стараться не ездить в будни в центр города – там гиблое место, застрянешь в пробках, и т.п.

Все доходные бомбильные места – вокзалы и аэропорты – оккупированы мафией. У меня была возможность один раз поглядеть на нее «в натуре». Клиент попросил довезти его из Строгино до аэропорта «Шереметьево-1». Не заезжая на платную площадку перед аэропортом, он вышел, а я развернулся и уже здесь, на шоссе, остановился перед голосующим человеком. Судя по всему, ему не хотелось связываться с шереметьевскими «таксистами», вот он и прошел пешком в сторону от их «сервиса» метров 100. Мы с ним быстро договорились о цене, и только я собрался отъезжать, как дорогу мне перегородили две машины – одна спереди, другая – сзади. Из передней вышел мужик уголовного вида и подойдя к моей машине развязно спросил:

- Ты что, работаешь здесь?

Это была уже не стоянка перед аэропортом, а обычное шоссе, по которому все машины едут в сторону Ленинградского шоссе. Мафия уже считает и это шоссе своим, осталось только поставить на нем турникет и брать со всех плату за проезд.

- Я просто ехал по шоссе и остановился подвезти человека.
- Мы здесь работаем.
- Ну забирайте его, если хотите.

Мой пассажир был здоровенным мужиком килограммов под 100 весом. Когда они назвали ему цену, он просто обложил их трехэтажным матом и мафиози (а их было всего двое), еще раз напомнив, что они здесь «работают», уехали.

«Бомбильный» бизнес был очень простым и распространенным, но получить с его помощью денег, достаточных для содержания семьи, было невозможно. Я всегда считал его своим хобби, способом смены обстановки, своего рода отдыхом после дневного общения с компьютером. Вечерние 3 – 4 часовые вылазки до кризиса 1998 года приносили, в среднем, 15-20 долларов нечистого дохода, из которого потом нужно было вычитать взятки гаишникам и оплачивать газ пропан-бутан, служивший топливом для моей «пятерки», а также покупать различные запчасти, которые по крайней мере раз в неделю приходилось заменять в ней. После кризиса доходы населения резко упали и, следовательно, упали и «бомбильные» доходы. Примерно в два раза. Плюс к тому стали расти цены на бензин. Вообще, по поводу цен на бензин ситуация в России весьма забавная. Низкие мировые цены на нефть – населению России плохо, случился кризис 1998 года,

многие потеряли в нем все свои сбережения. Высокие цены на нефть – опять же плохо, начинается внутренний рост цен на бензин (мировые же цены на него повышаются!) и, как следствие, рост цен на все остальное - продукты, одежду, предметы первой необходимости – стоимость доставки возросла! Причем подобный рост еще сопровождается и типично советским ажиотажем. Примером тому может служить газ пропан-бутан, к которому я привык и всегда использовал только его в качества корма для своего железного коня.

Повышение цены на пропан-бутан всегда проводилось «по просьбам трудящихся». Эти просьбы появлялись после того, как вслед за подорожанием бензина пропан-бутан … нет, не дорожал, а просто становился дефицитом. Бензиновых мафий (бензоколонок) в Москве было много, а газовых – раз два и обчелся. И вот на всех этих раз два и обчелся одновременно пропадает газ, ну не подвозят его в тех количествах, как всегда. У каждой газозаправочной станции образуются неимоверные очереди, многие уже привыкли к газу, который в среднем в два раза дешевле бензина, в очередях на газозаправочную станцию у пересечения Волоколамского шоссе и МКАД мне приходилось иногда выстаивать по 5 – 7 часов в ожидании заветного газа. Естественно, что после таких мероприятий появлялись «просьбы трудящихся»: пусть уж лучше подорожает, чем такие очереди. Лучшие люди газовой отрасли страны шли им навстречу: газ дорожал, причем не на скромные 3-5%, а зачуток поболее, раза этак в полтора-два, и как по мановению волшебной палочки все очереди пропадали.

У газа была еще одна весьма существенная в российских условиях особенность: его труднее разбавить, чем бензин. Если незабвенный Василий Алибабаевич из «Джентльменов удачи» разбавлял бензин одной лишь ослиной мочой, то это, несомненно, был честнейший работник бензоколонки, передовик производства, ударник коммунистического труда. Много ли у него было этой ослиной мочи? Ведро, два? Один раз я подвозил двух не совсем трезвых «королев бензоколонки» и они, проникнувшись ко мне чувством сострадания, всю дорогу советовали никогда не заправляться у них тем, что называется «бензином». И это в Москве, столице нашей Родины. А на периферии еще проще: один бензовоз, сегодня он возит мазут для печного отопления, а завтра в него заливают бензин АИ-92. Промыть от мазута.

Ну и, конечно же, описывая трудовые бомбильные будни, нельзя не вспомнить про гаишников, которых тоже можно в какой-то степени отнести к бомбильным начальникам. Одно радовало: огромный численный перевес бомбил перед гаишниками, в результате которого у гаишников иногда просто нет физической возможности слупить со всех по максимуму. Но за все мое бомбильное время мне очень редко удавалось видеть на дороге гаишника, простаивающего на дороге без дела, т.е. без уже пойманной и теперь раскручиваемой жертвы.

Один раз какой-то гаишный начальничек, будучи без формы и «на отдыхе», оказался моим клиентом. Клиентом довольно своеобразным: сначала, откушав прямо в моей машине водочки, он затем решил «заработать» немного денег. Первым делом мы поехали на квартиру к какому-то бедолаге, у которого ГАИ за что-то отобрало права. Там мой клиент пытался уговорить его все уладить, естественно за определенную мзду. Не стесняясь меня, постороннего человека, этот гаишный начальничек пересказал мне потом детали своих деловых «переговоров», из которых, насколько я понял, следовало, что его там послали куда подальше. Тогда он решил устроить «объезд» своих подчиненных, несущих трудную службу на дорогах столицы нашей Родины. Как говорил один высокопоставленный российский чиновник, «делиться надо». Первую точку он накрыл сравнительно легко, его подчиненные не ожидали приезда своего начальника на водиле-бомбиле. Пришлось за это платить, но зато эти ребята быстро разнесли по всем своим друзьям-сотоварищам весть о необычном обходе, который совершает их начальничек и последующие набеги были уже не столь успешными. Обо всех своих впечатлениях он, опять же нисколько не стесняясь, делился со мной, незнакомым ему человеком, которого он видел в первый раз, но это все были довольно очевидные истины о нравах, творящихся в его ведомстве. В конце концов водочные пары взяли свое, его потянуло «на девочек», а мне он уже порядком надоел, поэтому когда он под каким-то предлогом куда-то отлучился из машины, я не стал его больше дожидаться.

Вообще-то Москву я бы назвал «краем пузатых ментов», т.е. таких, которые уже насытились жизнью и напоминают ленивого кота: «Мне бы иномарочку остановить и подороже…». А вот периферия, провинция – это «край голодных ментов», они кидаются на всех без разбору. По крайней мере, гаишники в часто посещаемой мною Тверской области именно такие. Чуть ли не в каждой деревне после пересечения границы Московской и Тверской области по Ленинградскому шоссе – гаишные засады с радарами, которые кормят и поят эту несусветную ораву чиновников с большой дороги. И больше всего обидно, что эти гаишники, молодые люди, обычно прошедшие армию, пытаются перенести армейскую «дедовщину» на всех без разбору. Он (гаишник) всегда прав, он обладает всеми государственными полномочиями, он в конечном итоге принимает окончательное решение, от которого намного дешевле откупиться на месте. А чтобы раскрутить клиента «на бабки» идут в ход разные методы, например страшилки про опасности на дорогах, театрально рассказываемые клиенту, пойманному в глухой деревушке за скорость 80 км/час. Но чаще всего трезвомыслящий клиент начинает свое общение с гаишником сразу же с его основного философского вопроса:

- Сколько денег надо?

Ибо, к примеру, в моей бомбильной практике сложилась определенная шкала перевода времени в деньги. Взятка гаишнику – это, примерно, полчаса бомбежки, зачем же терять лишнее время?

Самое интересное, что и время гаишника тоже легко переводится в деньги. Поэтому, после некоторого времени, необходимого для усвоения этих простейших бомбильных истин, я стал относиться к ним философски спокойно и математически расчетливо. А позже корейцам объяснял особенности российской действительности так

- In Russia each policeman – businessman.

Но гаишные засады и канавы на дорогах – это еще не полный перечень опасностей, подстерегающих вольнолюбивого бомбилу.

Одна безобразнейшая сцена, которую мне довелось наблюдать на дороге, осталась надолго в моей памяти. Это было в конце июня 2000 года, обычный рабочий день, около 11 часов дня. Я ехал по московской кольцевой дороге и где-то невдалеке от пересечения с Рублевским шоссе движение прекратилось, все машины встали. Наверное, авария, сейчас разберутся, приедет милиция, оформят протокол, поедем дальше. Но милиции там было уже достаточно, а авария была не с транспортом, а с отношением верховных правителей к своему народу. Это Президент Российской Федерации Владимир Владимирович Путин решил проехаться по МКАД от своей дачи до Ясенево, где он в тот день представлял Службе внешней разведки ее нового директора.

Затор на МКАД был неимоверный, причем в обе стороны. Общее время ожидания проезда монаршего кортежа составило свыше полутора часов. Рядом я заметил автобус с авиапассажирами, направлявшийся в какой-то аэропорт, бетономешалку, которая все это время крутила свой бетон, а приводить все слова, которые были высказаны в адрес властей, здесь нет никакой возможности – слишком уж откровенны они были. Ведь МКАД – это общая дорога, дорога для всех, а не только для всенародно избранных. Для царских забав есть же специальные трассы, есть в конце концов специальный вертолет. Отрубать на полтора часа важнейшую транспортную артерию Москвы – это значит приносить убытки тысячам людей безо всякой надежды получить за них хоть какую-то компенсацию, наносить убытки сотням промышленных компаний, городу, преобразующемуся усилиями московских властей. Многокилометровые «правительственные» пробки – это позор России, наглядное проявление реальных нравов и обычаев, реальной российской «демократии». Царь правит, а дело холопов царю повиноваться, он Богом (всенародно) избранный. Но даже в настоящие царские времена настоящие цари не были столь высокомерны по отношению к своему народу. Во время первой мировой войны царица и царские дочери работали в госпитале сестрами милосердия. А кем работали современные царские дочери во время первой и второй чеченских войн?

И еще отличие современных царей от настоящих царей прошлого в том, что те, настоящие цари чувствовали себя истинными и рачительными Хозяевами земли русской, ибо основным мотивом их действий было передать наследнику Государство Российское процветающим и богатым. Да и наследник с юных лет набирался государственной мудрости, участвовал в заседаниях Государственного Совета, вникал в дела отца-монарха, готовился стать ему на смену. Культурный и интеллектуальный уровень тех царей также был очень высоким. Так, например, цесаревич Александр III несколько раз проверял с орфографическим словарем свои письма к отцу – царю Александру II, поскольку тот очень строго наказывал за неуважение к русскому языку, за грамматические ошибки в письмах. Ну как тут не вспомнить про Брежнева, который не мог без ошибок написать название своей любимой хоккейной команды – ЦСКА.

Система власти, созданная свергнувшими настоящих царей большевиками, очень скоро стала по сути такой же царской, но с одним существенным отличием: если раньше отбора в цари не было, был наследник, знал свое предназначение и к нему готовился, то теперь управлять государством стала любая кухарка, пробившаяся в Генеральные секретари или в Президенты, и отнюдь не за счет своего ума и талантов. Но уж дорвавшись до власти – все, все тормоза начисто отказывают. Дозволено все! Высшее существо! Никакой ответственности, ни перед Богом (которого сначала не было, а потом, когда потребовалось, опять появился), ни перед народом, называемым в последнее время модным заморским словечком «электорат». Перед всеми последними шоу-выборами мне почему-то частенько вспоминаются известные слова Вождя Всех Народов, который, глядя с трибуны мавзолея на демонстрацию трудящихся, замечал для своего, узкого круга: «Вот бараны пошли».

А ведь были времена, когда Россия была по-настоящему великой страной, давшей всему миру уникальную русскую культуру, науку, общественных деятелей, беззаветно преданных своей Родине. Но все – в прошлом,

очень и очень далеком, лучший культурный слой, российская интеллигенция были безжалостно вырезаны после Великого Октября.

На одном фанатизме можно решить какие-то тактические задачи, просуществовать исторически короткое время. А дальше на смену фанатизму должно прийти что-то другое. Например, в Китае пришла экономическая реформа, в результате через несколько лет пол-мира завалено дешевыми китайскими товарами. В России же на смену революционному фанатизму сначала пришли репрессии и страх, затем, когда страх прочно засел в подсознании у большинства людей - безразличие. Власть – сама по себе, народ – сам по себе, хорошо еще, если друг другу не мешают. У власти есть нефть и газ, дающие основной доход. Получить доход от какой-то трудовой деятельности людей – долго и хлопотно, нефть и газ дают его быстро и много. Все просто и понятно, только вот жить в такой стране и с такой системой взаимоотношений власти и народа очень трудно. Ибо, даже если у тебя есть хорошее образование и большое желание работать, ты знаешь, что этого здесь не требуется. Не тот случай. Торговать, обманывать, пробиваться в чиновники или в мафию, к нефтяным деньгам – это ближе к истине.

Можно ли изменить эту абсурдную ситуацию? В ближайшее время – вряд ли, слишком много в России природных ресурсов, дающих легкие деньги. А увещевать правителей: «Не надо проедать всю нефть и газ, надо развивать промышленность» - бесполезно. Не тот уровень. Надежда может быть только на чудо: откроют ученые (скорее всего, не российские) новые виды топлива и резко упадут мировые цены на нефть и газ. Или инопланетяне прилетят и все у нас наладят.

Сколько трагических случайностей привели Россию к такому состоянию! Сама Октябрьская Революция (по простому – переворот) была цепью случайностей. Если бы в царской семье не был болен наследник… Если бы Временное Правительство проявило чуть больше решительности… Если бы, в конце концов, союзники России – страны Антанты – проявили чуть больше понимания к тому, что тогда произошло в России и к каким последствиям это приведет для всего мира… Если бы Белые Армии зацепились за Урал, Крым, Сибирь, создали бы свою, независимую Республику. Ведь вот же наглядный пример – Южная Корея. Не поддалась коммунистическому натиску, отстояла свою свободу и независимость, а теперь, через 50 лет, легко сравнить, кто был прав: Северная или Южная Корея, где лучше жить.

На примере России почти весь мир понял: так делать нельзя! В одной только России правители, одурманенные легкими нефтяными деньгами, не усвоили элементарных уроков демократии, дающей в конечном итоге и экономически стабильное государство.

Вот такие мысли частенько одолевали меня во время вечерних бомбежек. От них накапливалась усталость, но и без них, как без наркотика, я уже не мог жить. А дальнейшая судьба представлялась еще более хмурой. Перспектив работы по специальности мало, доходов мало, расходы растут вместе с детьми, мои Жигули – пятерка от почти каждодневной езды по городу постепенно умирали естественной смертью, свалить за границу пока нельзя – невыездной. Один лишь компьютер, как мог, помогал мне пережить это нелегкое время.

Глава 6

TeleDoc

Russia. Examples.

Сразу предупреждаю: сам не видел, а только слышал от местных жителей. Своими глазами видел только ту глухомань, по которой течет река Молога, да ту деревню Горки, километров 20 выше по течению от моего Гузеево, о которой пойдет речь.

Молога счастливо избежала участи многих подмосковных речек, превратившихся в сточные канавы для отходов советских промышленных предприятий. Наверное, просто потому, что и предприятий-то таких там особо и нет, кое-что, конечно, сливают, но сравнительно немного. А потому и рыба пока еще водится, хотя ловят ее иногда не с помощью примитивных удочки, мережи, сети, а электроудочкой. Выезжают ночью на лодке с аккумулятором, от которого питается автомобильная фара, и свет от этой фары направляют на воду. Рыба, в том числе и крупная, плывет на свет, тут и бьют по ней колом, оглушают и ловят подсачеком. Просто и понятно, снасти тоже доступные для местных жителей. С обычной удочкой после такой ловли на реке неделю делать нечего.

Но даже при такой ловле еще остается на Мологе достаточно рыбы и иногда можно поймать крупный экземпляр щуки, судака, леща, язя. Но речь сейчас пойдет не о них, а о соме.

Около деревни Горки на Мологе были омута, в которых водились сомы. Сом – это нечто вроде поросенка, всеядный, ему можно скармливать любые отходы, и вот вся деревня Горки дружно взялась откармливать одного сома. Все знали место, куда он приплывает на откорм, и сом всегда находил там чем поживиться. Так прошло все лето, а ближе к осени сома решили выловить.

На трактор «Беларусь» приспособили лебедку с крюком от тракторного прицепа, насадили на нее наживку и закинули в омут, в место сомовьего откорма. Доверчивый сом, не ожидая от людей такой подлости, по старинке схватил съестную подачку, а трактор «Беларусь» взревел своим мотором.

Сома ели всей деревней. Голова у него была такой, что в пасть к нему спокойно мог засунуть свою голову человек, что многие и делали. А еще с ужасом представляли себе возможность встречи с этим чудовищем при традиционной ловле «электроудочкой», но все равно ловить на нее не перестали.

End of example.

Автоматизированная система электронного документооборота прижилась в W-банке. Начальство и простые сотрудники почувствовали ее удобство и постепенно она стала охватывать все новые и новые сферы деятельности в банке. Сначала ей доверяли самые простые банковские документы – статистические отчетности, балансы, различные банковские формы, затем перевели на нее платежные документы, подтверждения векселей, паспорта валютных сделок и еще много всяких других документов, о существовании которых мне, непосвященному в тонкости банковских технологий человеку, никогда не приходилось раньше слышать. Для нее придумали специальное название – TeleDoc – и оно также прижилось в банке. Название это появилось не сразу, сначала были различные варианты: Криптоцентр-V, Омега, но в конце концов выбрали TeleDoc. Тут еще приходилось учитывать российскую специфику: сертификата ФАПСИ на эту систему, естественно, не было, приставку «крипто» в названии лучше не упоминать. Десятки раз мы обсуждали эту проблему с В.К. Тяпкиным, но всякий раз единогласно приходили к выводу – соваться в ФАПСИ по этому поводу – бесполезно. Финансовые затраты на проведение подобной экспертизы будут сопоставимы со стоимостью ее разработки, а гарантии положительного результата никакой нет. И не потому, что система плохая, нестойкая, с какими-то «дырами» и т.п., нет, здесь банк был сам заинтересован в гарантированной стойкости, поэтому все криптографические и программные решения, перед тем, как их использовать в TeleDoc, неоднократно обсуждались и проверялись с Тяпкиным и управлением безопасности банка. Проблема была в другом – сертификатов в то время (1996 – 1998 гг.) не выдавали практически никому, кроме Московского филиала Пензенского НИИ Автоматики, которому патронировал Генеральный директор ФАПСИ, сам выходец из Пензы. Сертифицированные конкуренты были ни к чему, а создать систему зажима для чиновников, особенно в такой сфере, как криптография – привычное дело. Поэтому даже постановка вопроса в ФАПСИ о сертификации TeleDoc вынудила бы меня длительное время заниматься подготовкой различных справок, описаний, разрешений и прочих чиновничьих премудростей, а развитие самой системы при этом бы застопорилось. Но самое главное, что вся эта суета оказалась бы бесполезной и даже вредной: сертификата получить заведомо нельзя, можно только «засветиться», раздразнить ФАПСИшных «гусей».

Систему TeleDoc, под именем Омега, я подробно описал в книге «Практическая криптография», и если читатель заинтересуется связанными с ней техническими подробностями, то там он сможет найти полную документацию по этой системе. Здесь же я постараюсь описать наиболее интересные перипетии ее создания в условиях суровой российской действительности.

Первая DOS-версия TeleDoc (TeleDoc-1) просуществовала в банке с 1995 по 1998 года, она, конечно же, была немного неуклюжей, но честно отрабатывала положенные ей функции. Следующая версия (TeleDoc-2) разрабатывалась уже под Windows 32 и была намного более совершенной: в ней появились специализированные базы данных входящих и исходящих документов, специальный интерфейс для работы с ними, различные автоматические режимы, системы централизованного управления и прочая, прочая, прочая. Все это шаг за шагом добавлялось, накапливалось в реально действующей, «боевой» системе без нарушения производственного цикла банка, без задержки документооборота хотя бы на день. Мне нравилась система взаимоотношений, установленных с банком: составляется Техническое задание на год, в котором прописываются самые общие требования к разработке. Все конкретные текущие вопросы, возникавшие у меня при написании программ, оперативно решались с Тяпкиным по телефону без дополнительных бумаг. Примерно раз в неделю – встреча в банке, я привожу им свои программы, они их проверяют, дают свои замечания. В конце года ТЗ принимается, после чего реально работающая в банке версия TeleDoc обновляется. В такой схеме взаимоотношений чиновничьих извращений было по-минимуму, а поэтому работать с банком мне было интересно. Ну а банк, в свою очередь, получал уникальную, разработанную под его требования систему по весьма низкой цене.

Как я уже отмечал выше, я никогда не состоял в штате банка. Все работы с банком осуществлялись от имени моей частной фирмы ИЧП «Альба», в которой самое главное было – наличие банковского счета. Других признаков предприятия - наличия офиса, секретарши, бухгалтера и вообще какого-то иного персонала, кроме директора, там не было. Но существенно было другое: такая схема взаимоотношений позволяла мне сохранять за собой права интеллектуальной собственности на разрабатываемые программы. Банк финансировал разработку, получал за это право неограниченного тиражирования программ, но у меня

оставалась возможность самостоятельной продажи этих программ другим заказчикам. Более того, В.К.Тяпкин неоднократно повторял, что он всячески готов поддерживать мои поиски других заказчиков на TeleDoc, и реально оказывал мне в этом посильную помощь. Ведь самое трудное – объяснить потенциальному заказчику все особенности и преимущества подобной системы, а сделать это можно лучше всего на примере реально работающей системы в реальном банке.

Сколько раз я предлагал TeleDoc Центральному Банку! Не те времена, не те люди теперь там были. «Несертифицировано!» - вот и весь разговор. Чиновники везде одинаковы, минимум перемен, минимум новизны, минимум ответственности. Вообще-то банковская структура должна быть разумно консервативной, но где провести ту грань разумности? Некоторые эпизоды из жизни ЦБ, которые мне пришлось наблюдать, были явно за этой гранью.

Упоминавшаяся выше моя программная система «Криптоцентр-АВИЗО», не имевшая сертификата ФАПСИ, успешно работала уже около 3 лет в двух крупных подразделениях ЦБ: Центральном Операционном Управлении (ЦОУ) и в ОПЕРУ-1. Но навязчивая идея руководства ФАПСИ прибрать к рукам ЦБ постепенно привела к мысли заменить все несертифицированное программное обеспечение сертифицированным. Казалось бы, нет ничего проще: опробованная, успешно работающая программа посылается на сертификацию, проводится ее экспертиза, по результатам которой делаются возможные доработки, устраивающие как экспертов, так и реальных пользователей. Но это – в теории, на практике, в реальной жизни все не так. «Сделаем свою программу и насильно заставим всех в ЦБ ее использовать» - так решило это могучее Ведомство.

ОПЕРУ-1 ломать налаженные технологии и использовать ФАПСИшное творение отказалось наотрез. В конце концов чиновники ЦБ уступили напору этих девушек, обслуживающих счета всех крупнейших государственных организаций, в том числе и самого ФАПСИ. А вот ЦОУ (точнее, его руководство) сдалось, безропотно разломало все что я у них налаживал за эти годы. Потом мне довелось встретить в ЦБ девушку-операционистку из ЦОУ, которая работала с моей программой, и она, чуть не плача, поведала мне о своей новой жизни в условиях ФАПСИшного сервиса.

Ни разу и ни от кого за все мое посткгбэшное время я не слышал положительных отзывов о ФАПСИ. Везде одно и то же: запретить, навязать свое, которое работает хуже, зато сертифицировано. А от ребят, оставшихся дослуживать в этой Конторе, приходилось слышать: «Гниет там народ, интересной работы нет, многие просто спиваются». Зато административного ража, желания «всех пригнуть», подчинить, заставить кланяться – хоть отбавляй. Один раз газета «Московский комсомолец» в коротенькой заметке поведала, что ФАПСИ активно проталкивает идею оснащения всех контрольно-кассовых машин (любимых всеми торговцами ККМ) автоматической системой электронной подписи. Якобы меньше будет уклонений от налогов. А мне сразу представляется такая картина: по какому-нибудь вещевому или продуктовому рынку под ручку с розовощеким милиционером шагает ФАПСИшник с полными сумками. Электронную подпись проверял.

Не было у меня ни малейшего желания идти с системой TeleDoc на поклон к ФАПСИ. Я вложил в нее уйму труда, делал ее с удовольствием, ради удобства людей, ради внедрения своих идей, которым посвятил практически всю сознательную жизнь. Ведь, естественно, никаких криптографических алгоритмов типа ГОСТ или DES я в ней не использовал, только то, что выросло из «Ангстрема-3». Это все хорошо просчитано, основательно проверено, оригинальные криптографические решения. А такие оригинальные решения – это еще один рубеж защиты от потенциального злоумышленника, от различных продвинутых хакеров, научившихся воровать секретные ключи из оперативной памяти компьютера. И теперь объяснять все это чиновникам, мечтающим о контроле за вещевыми рынками?

Сейчас прошло уже почти 10 лет с момента появления первой версии TeleDoc и можно оценить, что же в ней было сделано правильно, а что, наоборот, не выдержало проверки временем и немного порассуждать о перспективах развития подобных систем. На мой взгляд, первая основная особенность TeleDoc – нестандартный криптографический интерфейс. Что это означает?

Работы по созданию мировых стандартов криптографического интерфейса велись с начала 90-х годов, и где-то к середине 90-х уже появились первые результаты. Если разработчик программного обеспечения хочет использовать в своих программах криптографические функции шифрования и электронной подписи, то для этих целей Microsoft подготовил и внедрил в Windows начиная с Windows-95 специальный интерфейс – CAPI – Cryptography Application Programming Interface. Этот интерфейс использует для выполнения криптографических операций динамические библиотеки, удовлетворяющие определенным требованиям Microsoft. Такие библиотеки принято называть еще CSP – Cryptography Service Provider. Для разработчика программного обеспечения вся прелесть технологии CAPI-CSP в ее универсальности, возможности выбора различных CSP от различных производителей, и возможность использования всех других богатых интерфейсных возможностей, предоставляемых пользователям Microsoft. Например, для организации закрытой электронной почты (когда письма отправляются в зашифрованном виде и с электронной подписью) достаточно, например, в таких известных почтовых программах, как Microsoft Outlook или Microsoft Outlook Express использовать встроенные в них возможности технологии CAPI-CSP. Таким образом,

простейший путь к созданию системы защищенного электронного документооборота – использование уже готовых решений Microsoft и стандартного интерфейса CAPI-CSP.

Но в первых двух версиях TeleDoc технология CAPI-CSP не используется. Первая версия – это DOS-версия, для DOS эта технология была еще в зачаточном состоянии, а вторая версия для Windows-32 разрабатывалась на основе первой версии TeleDoc, наследуя все ее свойства. Да и по времени разработки второй версии (98 год) – в то время технология CAPI-CSP не была еще так широко распространена.

Была и еще одна весомая причина, по которой в TeleDoc я стал использовать оригинальный криптографический интерфейс. Это – надежность, устойчивость работы системы в огромной сети W-банка. Собственный криптографический интерфейс – это исходные тексты программ, с помощью которых затем можно разобраться практически в любой сбойной ситуации, понять причину сбоя и устранить ее. Такие ситуации неоднократно возникали на практике, во время повседневной эксплуатации TeleDoc в W-банке. Одну такую ситуацию в банке прозвали «черной дырой» и для того, чтобы понять и устранить ее причину, потребовалось больше года. Дело в том, что к тому времени почтовые «аппетиты» W-банка выросли, дорогостоящая Sprint-Net перестала его удовлетворять, TeleDoc уже достаточно прижился и потихоньку созревал для собственной почтовой системы с использованием протоколов SMTP и POP3. Но пока он созревал, W-банк закупил специальную почтовую систему Pegasus mail, которая также использовала эти же протоколы. Когда же TeleDoc дозрел, то в качестве наказания за долгое дозревание ему была поставлена задача: обеспечить совместимость с Pegasus mail. Все бы ничего, дело нехитрое, протоколы-то одни и те же, но только вот тогда и появилась эта проклятая «черная дыра».

Вся информация, передаваемая из Центра в филиалы, отправлялась с помощью почтовой системы Pegasus mail (TeleDoc осуществлял только подготовку к отправке, включая шифрование и подпись), а в филиалах принималась по протоколу POP3 с помощью внутренней почтовой системы TeleDoc, а критерием успешного приема была проверка электронной подписи. Все принималось успешно, за исключением «черных дыр», которые регулярно возникали в разных филиалах примерно один раз в три месяца. На этих «черных дырах» проверка подписи давала отрицательный результат, повторная отправка, проводимая как в автоматическом, так и в ручном режиме, давала то же самое, случайные искажения на линии связи были исключены, управление информатики звонило мне домой, как к главному экстрасенсу, специалисту по черной программной магии, и просило, по возможности, расколдовать эти заколдованные мессаджи.

Вылавливать и исправлять различные программные глюки - это занимает едва ли не 90% времени разработчика-программиста. Но для того, чтобы это успешно сделать, необходимы какие-то исходные точки анализа: глюк должен быть устойчивым, регулярно повторяться, обладать какими-то закономерностями. Причинами глюка, чаще всего, являются ошибки в программе (программ без ошибок, так же как и абсолютной истины, не бывает), но иногда могут быть и конфликты с какими-то другими работающими программами, неверное распределение памяти, некорректное использование внешних устройств и куча всяких иных причин. Здесь же глюк был какой-то случайный, проявлялся редко и в различных ситуациях. Банк по-своему находил из него выходы: информация, содержавшаяся в «черных дырах», перекладывалась в другие пакеты и в них уже благополучно доставлялась по назначению. А я на все вопросы о возможных причинах этого глюка просил дополнительной конкретной информации: содержания пакета при отправке и при приеме (это сложно сделать, все автоматизировано и доступен только конечный результат), чем он отличается от других пакетов (ничем – такой был стандартный ответ), каких-то других «зацепок», по которым можно было бы понять причину глюка. Банку проще было раз в три месяца смириться с глюком, чем ковыряться с причинами его возникновения, и так прошел почти год.

В конце концов одна энергичная девушка из какого-то филиала все-таки дожала управление информатики банка по поводу этого глюка. Какими-то правдами или неправдами в банке смогли выловить то, что выдавал при глюке в канал связи Pegasus mail и что принимали в филиале. И оказалось, что есть различия! Тут уже у меня появилась конкретная пища для размышлений и в конце концов причина была выявлена: несоответствие в одном редком случае результатов кодировки MIME, осуществляемой Pegasus mail и внутренними процедурами, используемыми в моем любимом Borland C++ Builder v.3.0. Немного домыслив, мне пришлось слегка модернизировать процедуру приема, чтобы исправить эти огрехи.

Программист никогда не может считать себя застрахованным от подобных ситуаций.

Готовые чужие программы, к которым нет исходного текста, - это, как говорят в математике, «черный ящик», слепо верить тому, что все в нем работает так, как утверждается в его документации – можно, но осторожно. А вообще, при таких ситуациях лучше руководствоваться этически может быть и не совсем корректной, но математически очень правильной и надежной логикой: никому и ничему не верю, пока не проверю все сам. Даже если под словом «чужие программы» понимаются программы, созданные столь уважаемой и даже, более того, обожаемой мною фирмой Borland.

А в целом, оригинальный криптографический интерфейс позволил, как это ни странно, ускорить разработку TeleDoc и быстрее добиться его устойчивой работы. Ведь технология CAPI-CSP в то время также была еще

новой, хорошую документацию по ней найти было очень сложно, поэтому то время, которое потребовалось бы мне чтобы разобраться во всех ее тонкостях и деталях, могло бы оказаться весьма и весьма значительным.

Но оригинальный криптографический интерфейс требовал и оригинальной ключевой системы: системы выработки секретных и открытых ключей, системы подтверждения подлинности открытых ключей, их рассылки и смены. Здесь Microsoft также предлагает всем разработчикам использовать свои стандартные решения: различные форматы файлов с секретными ключами, сертификаты открытых ключей и сертификационные центры для распределения открытых ключей. Но во время разработки первых двух версий TeleDoc все это также находилось еще в зачаточном состоянии, а поэтому, пожалуй, единственным способом обеспечения устойчивой работы системы распределения ключей в огромной сети W-банка была разработка оригинального программного обеспечения для менеджера системы распределения ключей.

Эта система честно отрабатывала установленные ей W-банком функции: примерно раз в полгода в час «X» проводила полную смену всех ключей у всех пользователей TeleDoc в банке. И это было довольно разумное требование: банк – большой организм, какие-то сотрудники, работавшие с TeleDoc, за полгода могли уволиться, потерять свои секретные ключи, ценность самой информации, обрабатываемой с помощью TeleDoc, за полгода менялась, в общем периодическая полная смена всех ключей была одним из весьма существенных элементов информационной безопасности банка. И в конце концов эта весьма непростая операция стала проходить в банке спокойно, без сбоев и нарушений непрерывного процесса электронного документооборота. Но одну интересную возможность системы TeleDoc при смене ключей банк так и не использовал – это рассылку по электронной почте новых секретных ключей.

При смене ключей все эмоции отбрасываются, работают чисто математические рассуждения и модели. Зачем проводится смена ключей? Для ликвидации возможных последствий компрометации каких-то ключей. А можно ли при смене ключей новый секретный ключ шифровать с помощью старого? Эмоции в сторону, считаем все ключи скомпрометированными и вся информация, обрабатываемая с их помощью, доступна потенциальному злоумышленнику. А тогда ему становятся доступными и новые ключи, зачем же в этом случае затевать столь дорогостоящую и трудную операцию по их смене? Следовательно, шифровать новый ключ с помощью старого нельзя, в этом случае смена ключей не может дать 100% гарантии безопасности.

Но банк большой, ключевая система, по его требованию, централизована, т.е. выработка почти всех секретных ключей осуществляется в Москве, в центральном офисе банка, а филиалы есть во Владивостоке и на Камчатке. Как бы удобно было не посылать людей за дискетами с новыми секретными ключами из Владивостока в Москву, а выработать ключи на месте или, на худой конец, выслать им файлы по электронной почте! Но выработка секретных ключей на местах почему-то не устраивала W-банк, управление безопасности считало централизованную выработку более безопасной и надежной. И вот тогда появилась идея рассылки секретных ключей по электронной почте, при которой новые ключи шифруются с помощью абсолютно стойкого шифра – случайной и равновероятной одноразовой гаммы. Здесь, конечно же, тоже возникали организационные сложности, связанные с одноразовой гаммой, но одной дискеты с такой гаммой должно было хватить филиалу на все смены ключей в течение 50 лет. Идея была очень заманчивой, более того, уже реализованной в виде специального программного обеспечения, которое оставалось только применить на практике. Но тут энтузиазм банка почему-то угас, до практического внедрения рассылки секретных ключей дело так и не дошло. Видимо, успешно работающая система защищенного электронного документооборота стала для банка большой ценностью, которую он не хотел подвергать каким-то дополнительным испытаниям, опасаясь при этом возможных сбоев и нарушений производственного процесса.

Дефолт подкрался незаметно и проверил на прочность российские банки. Система взаимоотношений (и денежных расчетов) между банками свелась к простейшей формуле: «Никто никому не верит». А как быть в такой ситуации с прямыми электронными расчетами? Вот тут-то W-банку очень пригодилась система TeleDoc, автоматически посылающая подтверждение получения, заверенное электронной подписью получателя. W-банк окончательно поверил в TeleDoc.

Глава 7

Частное предприятие

Russia. Examples.

То лето выдалось в Гузеево жарким и сухим. Дождей не было чуть ли не два месяца, болота в лесу все высохли и, как обычно, начались пожары. Потушить горящее торфяное болото практически невозможно,

огонь уходит вглубь, тлеет, а затем разгорается вновь. Так и будет это болото тлеть до осени или даже до зимы, пока осенние дожди или снег основательно не пропитают его водой. Люди в такой ситуации могут лишь немного притушить огонь, не давать ему выйти на поверхность, не допустить верхового пожара. Но все равно, ходить по лесу невозможно, дым разъедает глаза, нечем дышать, ветра нет. Этот дым окутывает и близлежащие деревни, но там днем все-таки появляется ветерок и хоть немного его рассеивает. Но на ночь все равно приходится плотно закрывать все окна. Лучшее спасение – у реки, там ветра побольше, дыма поменьше.

И вот в один такой день мой 10-летний сын Антон со своим приятелем поехали на великах на рыбалку. Дорога на самые лучшие места шла вдоль реки, места им были хорошо знакомые и даже обжитые современной детворой. Каждый вечер они собирались здесь на тусовки, разводили костер, пекли картошку, приносили различные консервы. И вот в одном таком месте впереди метрах в 20 от их великов прямо на дорогу выбежал зверь, похожий, как он мне потом сам говорил, «на большую лохматую собаку». Это был медвежонок, настоящий, дикий. Они с медведицей, по-видимому, жили на болоте, но пожары вынудили их покинуть места своего привычного обитания и отправиться на поиски менее дымных мест. А река их очень даже устраивала: не так много дыма и на берегу – еда, остатки консервов от человечьих тусовок.

Человечьи дети затормозили и стали заворожено глядеть на настоящего медвежонка. Но тут из ближайших кустов раздался такой рык его медведицы-матери, что они попрыгали на свои велики и газанули в противоположную сторону со скоростью гоночного мотоцикла.

Потом примерно с неделю мой сын, заядлый рыболов, боялся близко подходить к реке. Но вскоре страхи улеглись, его снова потянуло на рыбалку и даже на тусовки. И какое воспоминание осталось: своими глазами видел живого дикого медведя!

End of example.

При социализме частная собственность была запрещена: все предприятия – только государственные, все добро – народное, общественное. Гражданам иногда разрешалось иметь небольшую личную (но не частную!) собственность. В чем разница между личной и частной собственностью? По марксистско-ленинской теории, личная собственность – это то, что нажито личным трудом, а частная – путем эксплуатации кого-то еще. Это в теории. А как на практике?

А на практике различных «цеховиков», т.е. людей, организовавших небольшое подпольное предприятие, например, по пошиву дефицитной одежды, сажали в тюрьму на несколько лет: возрождение капитализма, страшное преступление! А один случай, рассказанный мне моей матерью, работавшей преподавательницей физики в ПТУ, поражает своей жуткой дремучестью, в которой пребывало наше государство каких-то 20 лет назад.

Один парень из их ПТУ решил подарить своей девушке импортные сапоги. Это, как и многое другое, в то время было страшным дефицитом, но чего не сделаешь ради любимой. И вот в один прекрасный день он, отстояв в ГУМе почти 5 часов в очереди, с боем сумел достать отличные итальянские женские сапоги. Прекрасная покупка, но его радость была преждевременна: сапоги оказались малы. Что делать? Расстроенный парень потащил сапоги обратно в ГУМ, чтобы продать их там «с рук», т.е. из рук в руки, минуя государственный прилавок, почти за ту же цену, чуть-чуть увеличив ее, чтобы компенсировать себе моральные потери от 5 часового ажиотажа их законного добывания.

«Спекуляция» - по такой статье он был задержан и осужден на год тюрьмы, в которой и просидел от звонка до звонка. Когда он вновь появился в ПТУ, это был уже совсем другой человек: прошедший тюремные «университеты», с исковерканной судьбой.

Что можно иметь человеку, а что нельзя – все определяло коммунистическое начальство. Например, в Тверской (тогда еще Калининской) области в конце 70-х – начале 80-х годов горожанам не разрешалось иметь дом в деревне. Обком КПСС принял постановление: хочешь купить дом в деревне – прописывайся там, работай в местном колхозе или совхозе. К чему это привело? К вымиранию остатков жизни в деревне. И только после прихода к власти Горбачева этот абсурд был ликвидирован.

Но все социалистические традиции - побольше у человека отнять и побольше ему позапрещать - оказались очень живучими. Они в полной мере проявились и после официально провозглашенной отмены социализма и перехода к светлому настоящему всего человечества – капитализму с рыночным лицом. Лаконичный анекдот советской эпохи:

- Имею ли я право?
- Имеете.
- Могу ли я?

- Нет, не можете!

оказался весьма актуальным в постсоветские времена. Имеет ли человек право на частное предпринимательство? Имеет. А можно ли было реально заниматься им, не нарушая существовавших законов? Нет, однозначно нет, невозможно было в ельцинской России ничего не нарушать, ибо армада чиновников сразу же наплодила такую кучу различных постановлений, методических указаний, разъяснений и инструкций, что все декларируемые свободы враз накрылись этими килотоннами бумаг.

Я создавал свое частное предприятие с самыми благими намерениями: оно должно было дать мне желанную свободу деятельности, под которой в первую очередь понималась разработка и внедрение новых компьютерных программ. Торговля, различные финансовые махинации, челночный бизнес меня не привлекали, к тому времени у меня уже было осознание себя, как специалиста в области криптографии, и терять эту специальность, разменивать ее на «купи-продай» мне не хотелось. Буду писать и продавать свои программы, честно платить все налоги, жить поживать и добра наживать.

Мысль «честно платить все налоги» улетучилась почти сразу же после создания ИЧП «Альба». По тогдашним законам предприятие должно было заранее предположить свою прибыль и из расчета этой предполагаемой эфемерной прибыли отстегивать родному государству каждый месяц реальные бабки. Называлось это чудодействие как авансовые платежи налога на предполагаемую прибыль. Реальных денег еще нет, а налоги с них надо платить уже каждый месяц.

Да и как я могу запланировать прибыль от своих программ! Кто знает, сколько надо времени на то, чтобы найти заказчика, все ему объяснить, убедить, договориться о реальных механизмах установки, наладки и запуска сложного программного комплекса. Вроде бы логично вести разговор о деньгах и прибыли только после того, как решены все технические вопросы, на которые требуется масса времени. А платить авансовые платежи налога на прибыль мне просто нечем, не буду же я под это дело брать кредит под неимоверные проценты.

Следовательно, в моих условиях начать работу предприятия и при этом честно платить все налоги, в частности, авансовые платежи налога на прибыль, в принципе невозможно.

А что такое прибыль? Это разница между реальными затратами на производство продукции, называемыми себестоимостью, и ее продажной ценой. А кто определяет реальные затраты на производство моих программ? Инструкция о порядке определения затрат, включаемых в себестоимость продукции, которую писали чиновники, которые, возможно, о компьютере, кроме редактора Word, ничего больше не знают. Я работаю дома, стол с компьютером занимает полкомнаты в двухкомнатной квартире, где живет семья из 5 человек. Те неудобства, которые он причиняет, те ресурсы, которые потребляет, подлежат включению в себестоимость? По инструкции – нет, ничего там про это не сказано, точнее сказано, но такими общими словами, которые можно толковать по всякому. «А Вы заключите сами с собой договор аренды помещения под Ваше предприятие, вот тогда все будет по инструкции» - так мне разъяснили в налоговой инспекции. Это как – сам с собой? От юридического лица подписываться левой рукой, а от физического – правой? А с мифических доходов, получаемых от такой «аренды», еще и платить подоходный налог?

А раздел «Использование личного автотранспорта для служебных поездок»? Чиновники милостиво разрешили включать в себестоимость расходы по этой статье. В сумме, эквивалентной стоимости что-то около 10 литров бензина в месяц, т.е. за месяц я могу наездить по служебным поездкам не более 100 км при условии, что в моей машине ничего не сломается, на канавах около налоговой инспекции не полетит шаровая опора или рулевая тяга, в двигателе не израсходуется машинное масло, не износятся покрышки, не проржавеет кузов и т.п.

В общем, понимание того, что законы – сами по себе, а жизнь сама по себе, пришло очень быстро. Помимо чиновничьих инструкций человеку нужны еще элементарные условия для существования: еда, одежда, расходы на семью, минимальный комфорт. Только после того, как все это обеспечено, государство вправе что-то требовать в виде налогов. А сложившаяся абсурдная система, не учитывающая реальные особенности российской действительности того времени, не могла не привести к ответной реакции – теневому бизнесу и черному налу. Зато какая армия людей занята в различных инспекциях, обязательных фондах и прочих чиновничьих конторах! Они все прекрасно понимают полную абсурдность этой системы, но это их хлеб насущный, их кормушка, часто с отвращением, но они уже привязались к ней.

Каждое чиновничье ведомство обеспокоено только одним: как получить для себя побольше прав, побольше людей поставить в рабскую зависимость от себя. Например, где-то до конца 90-х годов налоговая инспекция и различные обязательные фонды имели право выставлять банку обязательные инкассовые поручения на списание задолженности со счета предприятия. Что сие означало на практике? Налоговая отчетность такова, что в ней сам черт ногу сломит, учесть все законодательные закорючки простому человеку физически невозможно, для этого надо ничем другим больше не заниматься, а только целыми днями штудировать тоскливую «Финансовую газету» или еще что-нибудь подобное. Возможны ошибки, неточности, что-то не в соответствии с какой-то мудреной инструкцией, оформлено не по той форме и т.п. Сдавать годовой отчет в

налоговую инспекцию – это не программы писать, тут надо все высидеть, выстрадать, выслушать, откланяться, осознать себя мелкой букашкой, дрожащей перед Государственными Интересами. Но вот отчет (и все с каждым годом постоянно увеличивающиеся сопровождающие его бумажки) сдан, наконец-то можно заняться основным делом – программами. Проходит месяц, два, пора наведаться в банк, узнать про состояние своего счета. А там неприятная новость: налоговая инспекция втихаря, не ставя в известность, по обязательному инкассовому поручению списала почти все, что на этом счету было. Для налоговой инспекции – это копейки, мелочь, ради которой никто не будет рыпаться, а для меня, для предприятия в единственном лице – не совсем.

Что делать в такой ситуации? Писать слезное прошение в налоговую инспекцию: разберитесь, пожалуйста, не может у нас быть такой задолженности. Налоговая инспекция разбирается и даже возвращает деньги. Какая радость – получить что-то от государства! Но радость – с двойным дном. Кто кому в этой ситуации что должен – понять практически невозможно. Налоговая инспекция, сделав еще через какое-то время очередной перерасчет, начинает трактовать возвращенные деньги как недоимку, на которую почти год после этого начисляются банди…, простите, официально утвержденные Государственными Органами пени.

В конце каждого квартала надо бросать работу и заниматься откровенно бесполезной работой – составлением по большей части липовых отчетов и справок. А потом еще развозить их по разным концам Москвы во всякие обязательные фонды, налоговую инспекцию, статуправление. Да почему же надо ради благополучия нескольких чиновников гонять по этому цирковому кругу тысячи людей? Почему я должен возить одни и те же отчеты и в налоговую инспекцию и в статуправление? Разве эти два ведомства не могут между собой договориться? Какое мне дело до их ведомственных проблем, почему я, свободный (как все время декларируется) человек должен безропотно отстаивать многочасовые очереди для сдачи отчетов в принудительные фонды? Ведомства получают право контролировать огромные массы людей, а люди не могут потребовать от ведомств в ответ каких-то разумных рамок их чиновничьей деятельности, а поэтому бесконечно плодятся никому не нужные бумаги в отчетности, различные справки, сведения, формы, растут очереди и взятки.

Почти 10 лет я созерцал эту чудовищную систему подавления горсткой чиновников человеческого достоинства тысяч людей. Нет, горбатого могила исправит, чиновничью власть в России просто так победить или хотя бы немного приструнить невозможно. Остается только ее созерцать и фиксировать в своей памяти, как Чудины высказывания в период учебы на незабвенном 4 факультете. Итак, картинки с натуры.

У меня за все время моей предпринимательской деятельности сложилось убеждение, что налоговая инспекция – это орган, работающий в соответствии с Государственными планами. Планами по штрафам, как, например, и ГАИ. Чем ниже цена барреля нефти на мировом рынке – тем больше разных проверок. Например, единственную проверку моего ИЧП «Альба» налоговая инспекция провела как раз накануне дефолта – весной 1998 года. Вообще мне всегда был очень симпатичен синьор Черника из детской сказки Джанни Родари «Приключения Чипполино». На своей крохотной хижине он повесил такое объявление: «Господа воры! Будьте добры, заходите, и вы сами убедитесь, что брать здесь нечего». Но это совершенно абстрактные ассоциации, не имеющие абсолютно никакого отношения к повествованию про проверку в налоговой инспекции.

Две серьезных и непроницаемых женщины попросили привезти им через неделю всю документацию ИЧП «Альба». Это куча всяких квартальных и годовых отчетов, различные ведомости, приходные и расходные ордера, авансовые отчеты. Вот последнее то как раз и самое гнусное. Предприятие состоит из одного человека, доходы – только бы прокормиться, да и то это доходы не человека, а предприятия. Чтобы стать доходами человека, их надо почти ополовинить (налоги в Пенсионный фонд, разные соц и мед страхи, подоходный налог). Да что же я, мазохист что ли? Есть статья расходов предприятия «Хозяйственно-операционные нужды», вот по этой статье и можно получить реальные деньги в банке. А потом долго собирать всяческие чеки – подтверждение расходов, осуществленных якобы на нужды предприятия, да еще чуть ли не на каждый такой чек писать авансовый отчет.

Чеков я к тому отчету набрал целый мешок, а вот писать ко всем авансовые отчеты по всем чиновничьим правилам было просто противно, написал какие-то общие цифры, а при желании в этом мешке можно было найти под них достаточное количество чеков. Сам же мешок притащил в налоговую инспекцию как часть отчетной документации.

Примерно так же, как я готовил авансовые отчеты, налоговая инспекция подготовила акт проверки. Лист, на котором куча каких-то непонятных цифр, а в конце вывод – недоимка, штраф в размере где-то около $100. Видимо, плановая цифра. «У нас еще низкие штрафы» - так мне прокомментировали результаты проверки эти две женщины.

При высоких же ценах на нефть появилась другая напасть: лавинообразно стало нарастать количество бумаг, сдаваемых в Органы, и чуть ли не каждый квартал стали меняться сдаваемые формы. Да и перерегистрация подоспела. При слове «перерегистрация» меня до сих пор начинает трясти мелкой дрожью,

ибо почти полгода я ничем другим не занимался, кроме как высиживанием, выстаиванием, собиранием разных бумажек, непредвиденными расходами.

Конечно же, сейчас, по второму заходу, я бы ни за что не решился на такой подвиг. Но тогда во мне еще не угас исследовательский пыл - посмотреть живьем на постсоветскую систему реальной власти, да и платить денег разным барыгам за «услуги по перерегистрации предприятия» не хотелось. Будь что будет, попробую окунуться с головой в чиновничий омут.

Вообще сама эта перерегистрация была мне непонятна. Госдума приняла новый Гражданский Кодекс, в котором такой формы предприятия, как ИЧП (индивидуальное частное предприятие) не предусмотрено. Ну и что мне делать? «Все по новой» - так популярно объяснили в налоговой инспекции: регистрационная палата, налоговая инспекция обязательные фонды, статуправление – везде нужна новая регистрация. Но ведь я же не прекращал деятельности, каждый квартал сдавал отчеты, за что мне теперь такая напасть? Да и в свидетельстве о регистрации моего ИЧП «Альба» ничего не сказано, что оно действует какой-то ограниченный срок. Если законодатели приняли новый закон, затрагивающий интересы всех граждан, то не мешало бы позаботиться о механизмах его запуска. Пожалуйста, я согласен называться по-другому, вместо ИЧП, например, ООО, но почему ради смены трех букв в названии я должен бросать всю свою основную работу и полгода кланяться чиновникам?

Впрочем, это вопрос риторический. На него есть универсальный вопрос-ответ: «В какой стране живем?». Поэтому компьютер – только для подготовки бумаг, необходимых для перерегистрации.

Первый рубеж – регистрационная палата. Это та контора, где регистрируют вновь созданное или перерегистрируют ранее долбанное-передолбанное предприятие. Я опять со своим наивным вопросом: деятельности не прекращал, отчеты регулярно сдавал, нельзя ли просто сменить три буквы в названии? Это было воспринято как покушение на чиновничью Власть. Если все так легко будут менять только по три буквы, то и чиновников не послали бы после этого тоже на какие-то буквы в количестве, равном трем. Нет, тут надо просечь ситуацию, смириться и не рыпаться, все равно от регистрационной палаты никуда не деться. Итак, сперва нужен новый Устав. А старый не подойдет? Нет, там ничего не сказано про общее собрание акционеров (состоящих из одного человека), про распределение их доли в Уставном фонде и еще про кучу каких-то мудреных вещей вроде выпуска акций.

Криптография и свобода. Свобода? Глава 7. Частное предприятие. Часть 2.

Устав я переписывал раза четыре и каждый раз инспекторша находила в списанном из какой-то типовой книжонки Уставе только ей одной ведомые погрешности. Но это не было еще самой большой проблемой. У ИЧП «Альба» был юридический адрес, совпадающий с моим домашним адресом, что было истиной на все 100%: я все время работал дома. А согласно – минуточку внимания – распоряжения Председателя Регистрационной Палаты, регистрация предприятия с юридическим адресом, совпадающим с адресом постоянного местожительства, осуществляется только при условии, что такое предприятие зарегистрируется в Комитете Поддержки Малого Предпринимательства при Правительстве Москвы. При социализме точно так же собирали взносы на ДОСААФ и Красный Крест, а незабвенная Нона Мордюкова в «Бриллиантовой руке» изрекла вечно актуальную фразу: «А не будут брать – отключим газ!».

Комитет для моей поддержки располагался в гостиничном номере отнюдь не самой плохой гостиницы. Комитетчиков двое: Председатель и Секретарь, мужчина примерно моего возраста и молоденькая девочка. Ну и, естественно, очередь, но хиленькая, всего каких-то часа полтора, не то, что в Регистрационную Палату, куда надо ездить записываться с утра. Мужчина, бегло пролистав мой Устав, вдруг изрек

- А Ваш отец не в Курчатовском институте работал?
- Да, там.
- Я его знал, мы с ним вместе работали.

Видимо, тоже когда-то, в той еще жизни, был инженером. А потом вдруг занялся поддержкой доходяжного малого предпринимательства. Самая подходящая работа для инженера из курчатника. Естественно, пошла раскрутка «на бабки»:

- юридическая консультация (фактически обязательная);
- пакет бланков для заполнения при регистрации;
- пакет каких-то нормативных и прочих документов, типа журналов учета проверок предприятия, которые я почти сразу же забросил куда подальше;

- проверка на уникальность названия предприятия: старое – Альба - уже кем-то занято, надо новое, пусть это будет Альба-Софт;
- пошлины за регистрацию в этом Комитете.

Да и прием ведет эта лавочка, естественно, не каждый день. В общем, где-то пару недель я ошивался в этом заведении, пока наконец-то мне не выдали заполненное на бланке, напоминающем сталинские облигации обязательного займа, свидетельство, что мое теперь уже ООО «Альба-Софт» находится под бдительным присмотром Комитета (за мои же деньги). Пора опять в Регистрационную Палату.

Регистрационная Палата – это как отчий дом: из него уходишь, но потом вновь и вновь туда возвращаешься. Ибо после первой «ходки» дают всего лишь временную регистрацию на три месяца, за которые надо встать на учет в налоговой инспекции, обязательных фондах, статуправлении, открыть счет в банке. И только после всех этих ритуальных обрядов временную регистрацию меняют на постоянную. Но поскольку за три месяца все это провернуть часто бывает просто нереально, то приходится еще не раз заглядывать в эту чиновничью альма-матер за продлением временной регистрации.

Вообще-то дальнейшие похождения бывшего подполковника КГБ по перерегистрации в обязательных и примкнувших к ним фондах следовало бы описывать вверх ногами или задом наперед. Слишком уж сюрреалистическая картина, никак не укладывающаяся ни в какие рамки ни математической логики, ни простого здравого смысла. Неразумное объяснение может быть только одно: как на Украине обозвали ГАИ? Очень правильно: ДАИ – державна автомобильна инспекция. Гнусно не лицемеря, ясно и понятно. А как расшифровывается ГИБДД? Гони Инспектору Бабки и Двигай Дальше. Но это опять же совершенно абстрактные ассоциации.

Начнем со статуправления, ибо без кодов ОКПО любое предприятие будет как солдат без офицера. А еще бравый солдат Швейк, устами одного из своих многочисленных героев – майора Блюгера, отмечал, что «каждый офицер есть есть существо необходимое, - в то время как вы, рядовые, являетесь случайным элементом и ваше существование допустимо, но не обязательно». Офицеров-статуправлений в Москве много, есть и недалеко от моего дома. Но для перерегистрации надо идти в Центральный офис – к самому генералу, ибо офицеру заменить три буквы в солдатском имени не по силам. Штраф какой выписать – это запросто.

Старинное здание напротив Детского Мира напоминало пчелиный улей, а очередь уже с утра змеиным хвостом извивалась с третьего этажа до первого. Я практически никогда не интересовался, что же означают присвоенные мне кем-то и когда-то коды ОКПО. Попав за 5 минут до закрытия конторы в заветный кабинет, в котором сидели три уже абсолютно безразличных ко всему девушки, я только и смог произнести: «Все то же» и сунул девушке листок со своими старыми кодами. Она машинально взяла его и квитанцию об оплате и по ее лицу было видно, что ее состояние явно не лучше моего. Такое впечатление, что чиновники никак не могут жить без ажиотажа, очередей, шума и гама. При социализме такие же очереди были за выкидывавшимися в соседнем Детском Мире дефицитными товарами, а теперь сменивших идеологию правителей периодически охватывают приступы ностальгии по ним. Вот и устраивают они иногда такие искусственные шоу-представления с большой массовкой. Но хоть эта процедура проходит без взяток (?) - отвечаю только за себя, за всех – не знаю.

Ну а дальше пошли песни о Главном. Обязательные фонды.

Нормальное предприятие, где есть нормальные работники, начисляет им каждый месяц зарплату, с которой надо отстегивать определенные проценты в Пенсионный фонд, фонды обязательного социального и медицинского страхования, фонд занятости. Величина отстегиваемых процентов определяет отношение к тебе со стороны чиновников этого фонда: чем она больше, тем больше снобизма и желания раскрутить клиента по максимуму. Самый тихий и безобидный фонд – фонд занятости, туда отчисляется всего 1% от суммы заработной платы, самый гнусный - Пенсионный фонд, в который отчисляется 28% за счет предприятия и плюс еще 1% из самой зарплаты. Все разговоры про то, что каждый россиянин сам жутко заинтересован в легальном получении зарплаты, поскольку тогда к пенсии он сможет накопить себе на достойную жизнь – лукавые. На специальный пенсионный счет россиянина идет всего лишь этот 1%, а основная часть – 28%, уплаченных фонду предприятием, идут самому фонду и россиянину этих денег больше не видать, как своих ушей.

Налоговая инспекция не трясла мое предприятие столько, сколько Пенсионный фонд. Идеи простейшие: найти расходы предприятия, не попадающие под раздел «Себестоимость» в соответствии с незабвенной инструкцией о порядке определения затрат, включаемых в себестоимость. Такие расходы автоматически трактуются как скрытые выплаты работникам (?) и с них взимаются отчисления 28% в Пенсионный фонд плюс штраф за скрытые доходы. В общем, без особых усилий Пенсионный фонд может потопить практически любое частное предприятие.

Первый раз Пенсионный фонд проводил проверку ИЧП «Альба» года через два после его создания. Проводившая проверку женщина-инспекторша работала в нем недавно, а потому была еще в каком-то

смысле идеалисткой. Я ей честно (насколько возможно!) рассказал про специфику работы ИЧП «Альба», что я бывший офицер, перешедший на вольные хлеба. И сначала мне казалось, что свершилось чудо – по результатам проверки она написала Акт, в котором говорилось, что нарушений (а следовательно и штрафов) нет. Моя идиллия длилась около недели. Затем, видимо, старшие и более опытные товарищи объяснили ей, что План – закон, его выполнение – долг, перевыполнение – честь. Через неделю она позвонила мне и попросила приехать.

- У нас было совещание, на котором давали разъяснения по порядку включения затрат в себестоимость, и я поняла, что мы с Вами составили Акт неправильно.

Ну еще бы, Акт без штрафов (и без взяток!) просто по определению неправильный. В общем, все свелось к раскрутке на стандартные 100 баксов.

Но это было сравнительно давно, идеалисты из Пенсионного фонда повывелись, а мне надо теперь там перерегистрироваться.

- Для перерегистрации я должна произвести у вас проверочку.
- Что для этого нужно?
- Приносите всю вашу документацию.

Привожу ей огромную сумку со всей бухгалтерией предприятия, догадываясь, что надо готовить бабки. Но сколько?

- У меня очень много работы, много больших предприятий. Вашу документацию мне придется брать к себе на дом и там с ней вечерами работать.

Какая самоотверженная женщина, прямо патриот своей профессии! Не жалеет своего личного времени, не отходит от станка ни днем, ни ночью!

Проходит месяц, затем другой, беготня с этой перерегистрацией уже порядком надоела. Пора закругляться, а без справки из Пенсионного фонда все дальнейшие шаги застопорились. Лето наступает, пора отдохнуть, съездить в Гузеево, покупаться, позагорать, а не торчать в этой пыльной Москве, бегая по чиновничьим конторам. При сдаче очередного квартального отчета в Пенсионный фонд интересуюсь у этой женщины насчет проверки.

После нескольких лицемерных монологов про загруженность наконец-то наступает момент истины: $300.

Когда наконец-то вся эпопея с перерегистрацией закончилась и я в первый раз от лица вновь созданного ООО «Альба-Софт» принес квартальный отчет в налоговую инспекцию, то там удивились.

- А что это вы начали все сначала? Вы продолжайте отчетность своего ИЧП «Альба», ведь ничего практически не изменилось, только три буквы в названии.

Глава 8

Тупик

Фельдъегерь долго удивлялся, когда вместо офиса увидел простую квартиру.

- Я, наверное, не туда попал? Здесь находится ООО «Альба-Софт»?
- Здесь, здесь, проходите.
- А Михаил Евгеньевич Масленников это кто?
- Это я.
- Вам пакет из Федерального Агентства Правительственной связи и информации. Получите и распишитесь.

Повеяло прежними запахами: таинственностью, важностью, Государственностью. Так и кажется, что сейчас снова призовут на службу Царю и Отечеству те, кто не поддался тлетворному влиянию капитализма и сохранил в неприкосновенности самые ценные социалистические идеалы: всем все запрещать. Только боюсь, что для такой службы я уже непригоден.

Оказалось, что я сам теперь стал объектом оперативной разработки (или, может быть, пока еще «профилактики») ФАПСИ. Высунулся на их взгляд чуть больше, чем положено.

Тест сего послания из прошлого привожу дословно, сохраняя его стиль и орфографию.

Федеральное Агентство Правительственной связи и информации при Президенте Российской Федерации. Лицензионный и сертификационный центр. 13.03.2001 № ЛСЦ/К – 827.

Генеральному директору общества с ограниченной ответственностью «Альба-Софт» Масленникову М.Е.

О лицензировании деятельности в области защиты информации.

Уважаемый Михаил Евгеньевич!

Согласно распространяемой по глобальной телекоммуникационной сети «Интернет» рекламе ООО «Альба-Софт» осуществляет разработку и распространение автоматизированных систем «Криптоцентр» и «VTELEDOC», реализующих функции шифрования и электронно-цифровой подписи.

В соответствии с Указом Президента Российской Федерации от 3 апреля 1995 года № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» деятельность, связанная с разработкой, производством, реализацией и эксплуатацией шифровальных средств без лицензий, выданных Федеральным агентством правительственной связи и информации при Президенте Российской Федерации, запрещена.

Одновременно Федеральным законом «О рекламе» реклама товаров, реклама о самом рекламодателе, если осуществляемая им деятельность требует специального разрешения (лицензии), но такое разрешение (лицензия) не получено, не допускается.

В связи с изложенным предлагаем привести деятельность ООО «Альба-Софт» в соответствии с действующим законодательством Российской Федерации. В противном случае к Вашему предприятию могут быть применены меры, предусмотренные российским гражданским и уголовным законодательством.

О принятых мерах просим сообщить в месячный срок.

Заместитель начальника Центра В.Н.Мартынов

«Вчера котов душили, душили…»

Документальное подтверждение статуса «враг народа». А насчет отсутствия лицензии – не совсем все так, как расписал г-н Мартынов. Лицензия у меня была, только не от ФАПСИ, а от Гостехкомиссии. Что это за зверь такой? Это вроде как обидно стало Минстерству Обороны, что его обошли в криптографическом Указе № 334. Как же так: при социализме жили вместе, КГБ и Генштаб МО имели свои шифровальные службы, а теперь, при рынке – все криптографические деньги отдать без боя КГБ? Ищите дураков в стране буратино! Быстренько бравые воины соорудили Гостехкомиссию и снабдили ее правами выдавать лицензии на деятельность, связанную с защитой от несанкционированного доступа (НСД), вопреки всяким Указам всегда трезвого Б.Н.Ельцина – попробуй докажи, что защита от НСД и криптография никак не связаны! Вот туда-то и решили податься мы с В.К.Тяпкиным за легализацией моей полулегальной криптографической деятельности в период расцвета взаимной любви с W-банком.

Алгоритм получения лицензии в Гостехкомиссии был прост, как правда: около $2000 "спонсорской помощи" и неделя беспробудного пьянства с отставными армейскими полковниками. Детали (Криптоцентр и TeleDoc) их абсолютно не интересовали, наливали до краев, потом лакировали пивком. Но в результате заветную бумажку с гербом и печатью я получил и в ней черным по белому было написано, что «Государственная техническая комиссия при Президенте Российской Федерации разрешает выполнять работы (оказывать услуги) по защите информации, указанные в пунктах 2.1 а, б; 3 г-ж настоящей Лицензии на всей территории Российской Федерации.», а в этих самых пунктах 2.1 а, б, которые сидели на трубе, и 3 г-ж (нецензурные ассоциации заменяем многоточием …), в частности, содержались «Разработка (3.1.), производство (3.2.), реализация (3.3.), установка (3.4.), монтаж (3.5.), наладка (3.6.), испытания (3.7.), ремонт (3.8.), сервисное обслуживание (3.9.) программных средств защиты от НСД, защищенных программных

средств обработки информации от НСД, программных средств контроля защищенности информации от НСД, программных средств по требованиям безопасности». Нормальный человек, прочитав сей бюрократический шедевр, наверняка будет смеяться, а мне, спустя много лет после описываемых здесь событий, кажется невероятным, то, что сохранилось в этих файлах, как напоминание о том, что такое совок. Потом, уже в Корее, корейцы много раз приставали ко мне с идеями криптографического бизнеса в России. Я открывал им сайт, к примеру, Крипто-Про, показывал иконостас лицензий (что-то около 16) и популярно объяснял алгоритм их получения, обязательно добавляя, что у меня нет ни малейшего желания опять участвовать в этом многомесячном алкогольном заплыве. Русская водка – это не корейская 24% соджа, у корейцев просыпалось чувство самосохранения и вопрос о криптографическом бизнесе в России отпадал естественным путем.

Но все это потом, намного позже, а пока у меня не было ни малейшего желания вступать в теологический спор с ФАПСИ насчет того, является ли лицензия на «защиту от НСД» криптографической индульгенцией. Прав тот, у кого больше прав. Насчет «мер, предусмотренных российским гражданским и уголовным законодательством», все ясно – напустить на предприятие кучу проверок. Ребята из одного банка, в котором использовался «Криптоцентр», писали мне, что ФАПСИ напрямую не предъявляло им никаких претензий. Зато налоговая полиция моментально обвинила в укрывательстве от налогов «сверхдоходов», полученных банком от использования программ клиент-банк с «Криптоцентром», как средством осуществления электронной подписи. А вообще-то даже проверки (после мук перерегистрации) не стали меня сильно пугать. Проверяйте, штрафуйте, получить что-либо от ООО «Альба-Софт» - проблематично. Движимости или недвижимости нет, торговлей не занимаемся, товаров на складе и самого склада тоже нет, наедут – прикрою к чертовой матери эту лавочку и свалю за границу. Да если и не наедут (хотя это письмо – уже наезд) все равно постараюсь куда-нибудь свалить, куда подальше от всех этих ФАПСИшников, регистрационных палат, налоговых инспекций, Пенсионных фондов, ГАИшников, которые стали реальными хозяевами в стране. Это их страна и в ней надо жить по их законам: кланяться, толкаться в очередях, давать взятки, унижаться. И ко всему прочему еще и не работать по своей любимой профессии. Если страну (чиновников) переделать невозможно, остается ее поменять. Вот только сколько времени надо мной будет висеть это проклятие – невыездной? Через 10 лет после увольнения из КГБ я смогу в ОВИРовской анкете даже не указывать эти темные страницы из моей жизни. Но для этого надо ждать еще целых 3 года, как долго! А если попробовать пораньше, ведь по закону по рогам дают всего 5 лет? Закон законом, а в реальной жизни откажут без объяснения причин, занесут в «черный список» - специальную базу данных ФСБ, и потом из нее уже не выбраться до конца жизни. Повышенная секретность, особый участок – всего этого мне пришлось глотнуть с избытком. Да и для того, чтобы найти интересную работу за границей, нужно время, нужно иметь представление, какие специалисты там наиболее востребованы, нужны ли криптографы.

Криптографы нужны, несомненно! Электронные расчеты, электронная торговля, банковские услуги – везде нужна криптография. Все нормальные страны постепенно снимают ограничения на использование криптографии, а фирмы, занимающиеся разработкой криптографических программ, стараются не упустить перспективные возможности, завоевать открывающиеся рынки сбыта. И только в России в компании с Северной Кореей и Ираком каждый криптографический чих сопровождается «мерами, предусмотренными российским гражданским и уголовным законодательством».

Но пока, в данный момент, мне еще сваливать некуда, а в месячный срок надо отвесить очередной поклон ФАПСИ в лице г-на В.Н. Мартынова.

Заместителю начальника лицензионного и сертификационного Центра Федерального Агентства Правительственной Связи и Информации при Президенте Российской Федерации г-ну Мартынову В.Н.

На Ваш исх. № ЛСЦ/К-827 от 13.03.2001 *19.03.2001 г.*

Уважаемый г-н Мартынов В.Н.!

В соответствии с Уставом ООО «Альба-Софт», зарегистрированным Московской Регистрационной Палатой в реестре за № 572840-РП 03 апреля 2000 г., предметом деятельности ООО «Альба-Софт» является в том числе «разработка научно-технических решений для создания информационно-поисковых систем, систем связи и информационной безопасности». При осуществлении этой деятельности ООО «Альба-Софт» разработаны несколько пакетов прикладных программ, ориентированных на использование в широко применяемых в настоящее время операционных и прикладных системах (Windows-32, Microsoft Outlook, Lotus Notes и т.п.) и предназначенных для упорядочивания и контроля за электронным документооборотом, осуществляемым с их помощью. Программы,

разработанные ООО «Альба-Софт», допускают встраивание в них дополнительных модулей, в том числе и модулей, осуществляющих шифрование и электронно-цифровую подпись.

Поскольку разработка подобных программ требует их тщательного и длительного тестирования, нашей компанией были подготовлены программы-иммитаторы операций шифрования и подписи, в которых не используются принятые в Российской Федерации стандарты шифрования и электронно-цифровой подписи (ГОСТ Р 34.10-94, ГОСТ Р 34.11-94), а также известные алгоритмы DES, PGP,RSA, IDEA, ГОСТ 28147-89 и им подобные. Наша компания не считает эти программы-иммитаторы (которые мы именуем MCS-модулями) средствами криптографической защиты информации, а рассматривает их как инструмент для тестирования интерфейсной оболочки. Слова «Шифрование» и «Электронная подпись» на сайте компании «Альба-Софт» предназначены для квалифицированных программистов, которым потребуется, имея описание MCS-модулей, заменить их на реальные операции шифрования и подписи.

Согласно ст.2 раздела 1, а также п.1 раздела 5 главы 2 Федерального Закона о рекламе, «реклама - распространяемая в любой форме, с помощью любых средств информация о физическом или юридическом лице, товарах, идеях и начинаниях (рекламная информация), которая предназначена для неопределенного круга лиц» «Реклама должна быть распознаваема без специальных знаний». Информация, помещаемая на сайте ООО «Альба-Софт» в INTERNET, носит технический характер, предназначена для узкого круга специалистов в области электронного документооборота, требует специальных знаний (знаний языков программирования, информатики). Исходя из этого, мы не считаем содержание нашего сайта рекламой.

С уважением,

М.Е.Масленников, Генеральный директор ООО «Альба-Софт», кандидат физ.-мат. наук

Знать ничего не знаю ни про какую криптографию, а слова «шифрование» и «электронная подпись» произношу по привычке так же, как по привычке наше государство все еще называю советским. А сколько и в каких условиях заказчик будет «тестировать» MCS-модули – про это ни в каком законе ничего не сказано. Сколько надо, столько и будет. В ОПЕРУ ЦБ «Криптоцентр-АВИЗО» тестировали около 10 лет.

А вообще-то все чаще и чаще стало появляться ощущение тупика. Что дальше?

Отношения с W-банком после того, как оттуда ушел В.К.Тяпкин, изменились, в них появилась новая для меня черта: TeleDoc работает успешно, больше ничего не надо. Переходить в штаты этого банка и заниматься там текущими банковскими проблемами мне не хотелось: теряется самостоятельность, а самое главное - работа банковским клерком меня не прельщала. Найти новых заказчиков на мои программы в условиях криптографического геноцида было очень трудно, почти нереально, я убедился в этом за последние 2 – 3 года. Переквалифицироваться? В кого? В специалиста по 1С бухгалтерии? Спрос на эту программу действительно большой, ибо она – плод общения с чиновниками, попытка автоматизировать ту кипу бумаг, которые каждое предприятие должно готовить и сдавать во время квартальных и годовых отчетов. Но у меня эти бумаги вызывают отвращение, я сам заполнял и сдавал их с большой натугой, исключительно по необходимости. А здесь теперь надо разбираться со всеми этими формами и справками, их обновлениями и изменениями в соответствии с чиновничьими прихотями. Нет, на 1С бухгалтерию меня явно не тянет. Надо что-то другое, а что?

Вот в таких раздумьях проходил день за днем, а кушать-то хочется каждый день. Вместо бомбильни по вечерам я отчаянно пытался сделать этот источник существования чуть ли не основным, целыми днями разъезжая на своей видавшей виды пятерке по окрестным «охотничьим угодьям». Но таких бомбил тучи! А пятерка, прошедшая к тому времени около 300 тыс. км, разваливалась прямо на глазах. Двигатель дымил, грелся, чтобы мотор не заглох, приходилось жарким летом на полную открывать кран отопителя. Сцепление, коробку передач и прочие машинные части я уже менял на ней несколько раз, и все равно постоянно приходилось ждать каких-то подвохов. Один раз мне показалось, что что-то подозрительно гремит в левом переднем колесе. Потихоньку я доехал до гаража и когда уже встал перед воротами, чтобы въехать в него, отвалилась левая рулевая тяга. Это было как предупреждение: в следующий раз что-то может отвалиться прямо на ходу.

Хорош итог прожитой больше чем наполовину жизни: денег нет, работы нет, перспектив нет, так и кажется, что все прожито впустую. Торговать надо было идти, спекулировать чем-то или сесть на должность,

сулящую взятки. Один парень, выпускник Высшей школы КГБ с нашего курса, устроился на работу в таможню.

- Серега, как тебе не стыдно! Ты же математик!

Так воскликнул, узнав об этом при встрече с ним, бывший командир его учебной группы.

- Понимаешь, Толян, там же невозможно не брать. Такая обстановка.

Легкие деньги, привыкание к ним – необратимый процесс. Приходится выбирать: или интересная работа, или таможня, совместно эти два понятия существовать не могут. А у меня все еще оставалась надежда найти когда-нибудь интересную и высокооплачиваемую работу по специальности. По крайней мере, хотелось хотя бы немного за нее побороться.

Но в России это практически невозможно.

Свалить, свалить из этой России к чертовой матери, свалить за границу, куда угодно, но только не оставаться больше в этой опостылевшей Москве без работы, без денег, без перспектив, сменить, срочно сменить всю окружающую обстановку, не видеть больше этих налоговых инспекций, Пенсионных фондов, наглых гаишников, считающих себя начальниками всех и вся, и потерявших даже самую малость стыда, не гнушающихся ездить за поборами со своих подчиненных на водиле-бомбиле.

Нет, еще три года высиживать в России у меня уже нет сил. Все, хватит, есть Internet, поисковые сервера, с их помощью - все силы, всю энергию я буду теперь тратить только на поиски работы за границей.

Глава 9

One way ticket

Russia. Last example.

Конец ноября 2002 года, почти ночь. По заснеженной и узкой Живописной улице я занимаюсь своим привычным делом – бомблю. Но настроение уже совсем другое: в декабре я наконец-то сваливаю из России в Южную Корею, работа по специальности, по криптографии. Денег, как всегда, не хватает, но теперь появилась надежда вырваться из этой мрачной страны и попробовать свои силы в зарубежной компании. Моими пассажирами являются трое молодых ребят, это программисты из какого-то банка, засидевшиеся допоздна на работе, интеллигентные и порядочные. Идущая впереди меня машина дает правый сигнал поворота и притормаживает, а я, естественно, чисто машинально объезжаю ее слева и левыми колесами чуть-чуть выезжаю за сплошную разделительную линию. И только тут замечаю милицейскую засаду.

Сержант - гаишник по возрасту был, наверное, вдвое младше меня, а по объему – вдвое больше. Но он тут – хозяин этой тайги, сейчас пойдут ритуальные заклинания, которые в разные времена прерывались полтинником или стольником.

- Вы совершили одно из самых опасных нарушений Правил Дорожного Движения – выезд на встречную полосу.
- Сколько?
- Пятьсот.

Наглость этих работников большой дороги способна любого, даже самого уравновешенного человека, вывести из себя. Я намного старше его и по возрасту и по званию, у меня за плечами уже достаточный жизненный опыт, я стараюсь честно заработать немного денег, а он взмахнул своей волшебной палочкой – и надеется, что я просто так отдам ему свой двухдневный заработок! Напрасно!

- Согласно Закону, я отберу у Вас права и рассматривать Ваше дело будет суд.

Согласно Закону! Да он даже не удосужился толком прочесть свой основной закон-кормилец – Правила Дорожного Движения. Для трактовки пересечения разделительной полосы как выезда на встречную полосу

дорога должна иметь по 4 полосы движения в каждую сторону. А тут всего одна. Согласно Закону нужны также независимые свидетели, показания которых заносятся в Протокол. Потом, год спустя, когда я приехал в командировку из Сеула в Москву и показал этот Протокол милиционеру из Административной группы ГАИ, даже его беглого взгляда на него было достаточно: «Все – липа».

Теоретически перед Законом все равны. Не нравится мне решение гаишника – его можно обжаловать через суд. Но механизмы применения Закона далеко не одинаковые. Для гаишника, чтобы испортить мне последние впечатления от покидаемой Родины, достаточно всего лишь махнуть своей палкой. Мне же, чтобы добиться справедливости, надо бегать по судам и чиновникам, чего мне только и не хватает для полного счастья.

Пока гаишник, напрягая все свои извилины, составлял протокол, я записывал на отдельном листе номера всех машин, которые, объезжая мою стоящую пятерку, тоже заезжали за сплошную полосу.

- А почему Вы их не штрафуете?
- Не надо за других, отвечайте за себя!

Когда все эти ритуальные церемонии закончились и я извинился перед поджидавшими все это время в моей машине ребятами, мои нервы не выдержали.

- Это их страна, их порядки, их блатные нравы! Нормальному человеку в их стране делать нечего! Здесь нет ни законов, ни элементарного человеческого уважения! Почему я, достаточно взрослый человек, бывший офицер, должен как солдат-салага подчиняться прихотям сержанта-самодура? Эта страна такой была, такой и останется еще долгое время, а поэтому в ней лучше не жить!

Молодые ребята-программисты, узнав, что я вскоре уезжаю в Южную Корею и в своей основной жизни тоже компьютерный фанат, сразу же заинтересовались: что? как?, и всю оставшуюся дорогу мы разговаривали на общем языке. А меня потом, уже в Корее, целый год мучал один и тот же вопрос: ну почему разная шпана в России обладает реальной властью? Верхи – это особый разговор, простой человек чаще всего сталкивается именно с гаишниками, налоговыми инспекторами, различными чиновниками и прочими шишками на ровном месте. И – бессилен перед ними, не по закону, а по реальным механизмам его применения. «Имею ди я право? Имеете. Могу ли я?…» Нет ли здесь старого давнего основного противоречия развитого социализма: между словом и делом?

Сколько раз потом мне было стыдно перед корейцами за порядки в России!

- Я в Москве пока дошла от Пушкинской площади до гостиницы Россия, у меня милиция три раза паспорт проверила.

Так поведала мне одна побывавшая в России корейская девушка. За все время моего пребывания в Сеуле, - а это уже почти пять лет – никто не останавливал меня на улице для проверки документов.

- У нас есть закон, по которому полицейский должен обращаться к иностранцу на английском языке, а поскольку многие полицейские английский язык знают не совсем хорошо, то они стесняются.

Стесняются! Их бы в Москву, к российским коллегам, на перевоспитание. Слон я, слон, только ногами не бейте!

Я устал, просто смертельно устал от своей родной страны и творящихся на ней порядков. Желание жить честно, делать полезное дело, приносить людям пользу – аномальное явление. Понятие человеческого достоинства существует только для избранных, простым же смертным – очереди, унижения, издевательства, взятки. Блатной жаргон, блатные нравы, блатные порядки, «все как на зоне», как говорит сатирик Михаил Задорнов. Мои программы, в которые была вложена огромная масса труда, остались здесь во многом невостребованными, они не обеспечили мне более-менее достойное существование.

Я покидал Россию с легким сердцем: хуже не будет. Свободы, реальной и материально обеспеченной свободы, мне здесь не видать. Пролетариату нечего терять, кроме своих цепей, дали бы только отсюда свалить. А поэтому в тот день, когда в моих руках оказалась бордовая книжица с двуглавым орлом и надписью «Заграничный паспорт», я наконец-то поверил в реальность сделать очередной крупный Upgrade в своей жизни.

***

Вылет рейса «Аэрофлота» Москва-Сеул задержали на три часа. Спокойствие, только спокойствие, олимпийское спокойствие: я почти 10 лет ждал этого момента, так что лишних 3 часа – это капля в море, пивка попью. Вот только позвонить домой не удалось: единственный в Шереметьево-2 телефон-автомат, принимавший монеты-рубли, был сломан. Когда же в Duty-free я выгреб из карманов всю оставшуюся неизрасходованной на телефонные звонки мелочь и высыпал ее перед продавщицей с наивным вопросом: «Что на это здесь можно купить?», она в ответ продала мне на нее последний кусочек моей Родины – крохотную шоколадку.