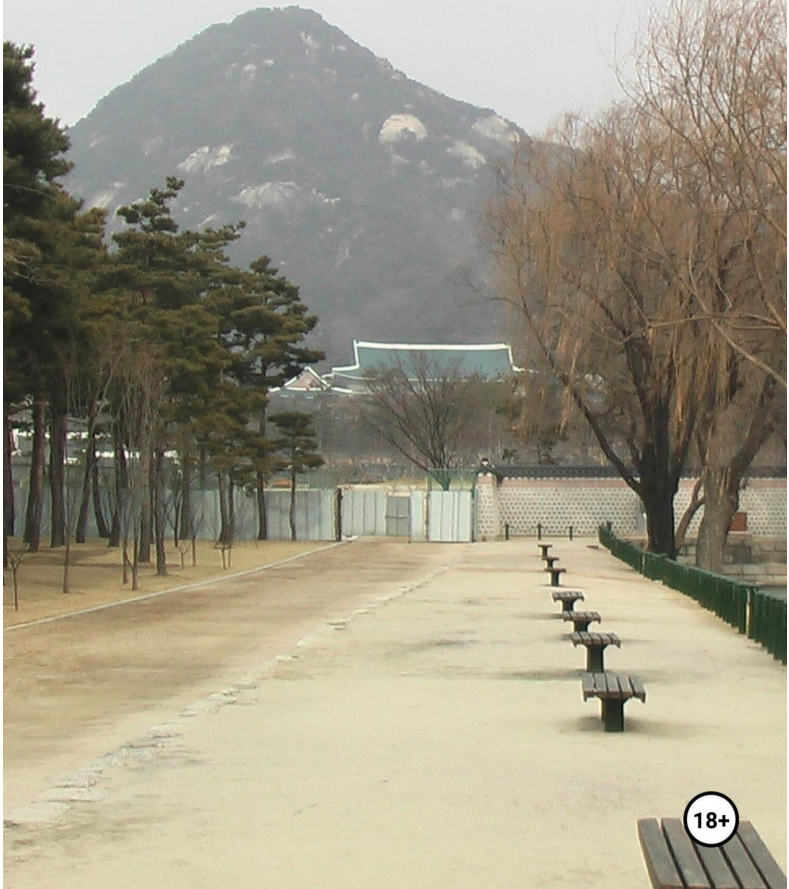
Масленников М.Е.

НЕВЕРОЯТНОЕ

Рассказ о работе советского криптографа
в Южной Корее



18+

Михаил Евгеньевич Масленников

Невероятное. Рассказ о работе советского криптографа в Южной Корее

http://www.litres.ru/pages/biblio_book/?art=71402335
SelfPub; 2024

Аннотация

Сейчас, к сожалению, профессия инженера, создателя материальных и интеллектуальных ценностей, не так популярна, как в 70-е годы: нефть, распределение нефтяных денег, торговля, юристы и экономисты куда понятнее и престижнее. Но тем, кто все же решил стать инженером и связать свою жизнь с производством, а не распределением, я хочу дать достаточно тривиальный совет: попробуйте свои силы за границей. И совсем не обязательно уезжать из России навсегда, иногда достаточно нескольких лет, после чего тянет назад. Но вырваться в иное измерение, иные условия труда, иные критерии оценки специалиста – необходимо.

Про то, как мне довелось постигать эти истины – в этой книге.

Все фотографии в книге взяты из личного архива автора.

Содержание

Михаил Масленников Невероятное. Рассказ о работе советского криптографа в Южной Корее

НЕВЕРОЯТНОЕ

Рассказ о работе советского криптографа за границей

Предисловие

Я сидел в Шереметьево-2 и все еще не верил в происходящее.

Сентябрь 1975 года.

«Никто, ни мать, ни отец, ни жена, ни дети – никто не должен знать, чем вы занимаетесь». Это – посвящение в специальность молодых слушателей 4 факультета Высшей Краснознаменной школы КГБ СССР имени Ф.Э. Дзержинского. В какую специальность? В криптографию.

Декабрь 2002 года.

«Вылет рейса на Сеул задерживается на три часа».

Казалось, что за эти три часа все вернется почти на 30 лет назад. Советского криптографа, собирающегося уезжать на постоянную работу, связанную с криптографией, в далекий и неведомый Сеул, остановят, проведут разъяснительную работу, дадут хороший пинок и вернут в 70-е годы. Что-либо иное представлялось просто невероятным. Ждать осталось недолго, всего три часа…

«Объявляется посадка на рейс до Сеула».

Не может быть! Сейчас что-то будет…

Началась антиобледенительная обработка самолета. Сижу в самолете у окна, чего-то жду…

Рулежка… Взлет. Невероятное свершилось!

Советская криптография

Когда в 1974 году я решил поступать учиться на 4 факультет Высшей школы КГБ, то мысленно смирился с тем, что всю жизнь буду невыездным. В 1974 году я еще не знал, что буду криптографом, даже не слышал такого слова, как криптография, но то, что дальнейшая работа будет связана с секретами, было нетрудно догадаться.

В 70-х годах криптография в СССР занималась только существующими в то время шифрами. Она была целиком ориентирована на обслуживание военно-промышленного комплекса и иных государственных структур, типа министерства иностранных дел, где возникала потребность в шифровании информации, передаваемой по различным линиям связи. Также советские криптографы пытались взломать, и небезуспешно, шифры других стран, где криптографии не уделяли достаточного внимания.

В 1974 году всем молодым слушателям 4 факультета вручили памятные значки, посвященные 25-летию факультета.

Если, взглянув на этот значок, читатель подумал, что в 1974 году исполнилось 25 лет IV факультету, то это не совсем так.

В 1949 году никакого IV факультета не существовало.

После войны стало известно, как немцы опростоволоси-

лись со своей шифровальной машиной «Энигма». Товарищ Сталин тоже очень заинтересовался этим, особенно когда отношения с бывшими союзниками испортились и началась холодная война. «Читать всех, но наши шифры и переписку читать никто не должен» – такой лозунг провозгласил он. И под этот лозунг создал ГУСС – Главное управление специальной службы при ЦК ВКП(б). Создал широко и основательно, ибо пример немецкой Энигмы был очень впечатляющим и свежим. Чего только не было в функциональных обязанностях ГУСС, прописанных в специальном секретном дополнении к Постановлению Политбюро ЦК ВКП(б) от 19 октября 1949 года о создании ГУСС! Это чтение иностранной дипломатической, военной, коммерческой и агентурной шифропереписки, разработка и контроль аппаратуры для отечественной шифрованной связи, радиоперехват шифрованной переписки иностранных государств. Создавался НИИ для разработки теоретических основ дешифрования главным образом машинных шифраторов Америки и Англии; теоретических основ и анализа стойкости отечественных шифров; проблем по созданию и использованию быстродействующих счетно-аналитических машин и проблем по новым методам перехвата сообщений.

Этим же постановлением создавались Высшая школа криптографов (ВШК) и закрытое отделение механико-математического факультета Московского государственного университета.

По своим целям и задачам ГУСС сопоставимо только со всемогущим американским АНБ – Агентством Национальной Безопасности, которое как огромный пылесос всасывает в себя все, что передается по различным каналам связи, обрабатывает, сортирует, пытается дешифровать с тем, чтобы получить от этого пользу для США. С одним небольшим дополнением: ГУСС было создано значительно раньше АНБ, появившегося на свет в соответствии с секретной директивой Трумена от 24 октября 1952 года.

После смерти Сталина наступила оттепель, в которой ГУСС растаяло 24 апреля 1953 года, но не бесследно. Растаять бесследно не позволяла набиравшая силу холодная война и ставшее заклятьем немецкое слово «Энигма». Название «ГУСС» исчезло, но криптография в СССР осталась. ВШК свое существование фактически прекратила вместе с ГУСС, а вот закрытое отделение мехмата МГУ – осталось.

Люди, специалисты-криптографы – вот главное богатство, которое оставили после себя ГУСС и ВШК. А сколько в истории СССР того времени было обратных примеров! Вспомним генетику, «академика» Т.Д. Лысенко с его превращениями пшеницы в рожь. Помним и «философов», объявивших кибернетику «буржуазной лженаукой».

В 1955 году по предложению ректора МГУ академика И.Г.Петровского было ликвидировано закрытое отделение мехмата МГУ.

«Раздробили», «реорганизовали», «переподчинили»

и прочие подобные административные меры в 50-х годах вряд ли шли на пользу криптографии в СССР. А у главного противника в холодной войне – США – наоборот, АНБ постоянно набирало силу и вес.

В 1960 году произошёл инцидент, имевший колоссальное влияние: специалисты АНБ Вильям Мартин и Бернон Митчелл бежали в СССР, где поведали сотрудникам КГБ о работе агентства.

Пока в СССР всю криптографию дробят, реорганизуют и переподчиняют, АНБ не теряет время даром. Про Энигму-то еще не забыли? Ведь холодная война в самом разгаре. А что, если у американцев уже есть своя «бомба Шеннона», аналогичная по назначению «бомбе Тюринга», но для советских шифров?

Быстро заткнули «философов», объявивших кибернетику «буржуазной лженаукой». Наоборот, новой криптографической философией стала такая: «Криптографический анализ нельзя проводить без ЭВМ, только на кончике пера». Ну и, конечно же, вспомнили про бессмертный сталинский наказ: «Кадры решают все!».

Возродить ГУСС тогда, в начале 60-х, так и не решились, а воссоздать заново ВШК – необходимо. Необходимо подготовить специалистов, способных создать такие советские шифры, для которых потом можно будет аргументированно доказать, что никакой «бомбы Шеннона» у американцев для них нет и не будет.

Криптографию во многом спасла ее секретность и те люди, которые пришли в криптографию в период ГУСС и затем, в 70-х годах, стали нашими любимыми преподавателями. И главным из этих людей, своего рода «криптографическим Королевым», многие совершенно справедливо считают Ивана Яковлевича Верченко.

Иван Яковлевич был человеком, навсегда преданным математике и криптографии, какие бы перипетии судьбы ему не приходилось при этом преодолевать. Как утверждается в его биографии, в апреле 1953 года на одном из высоких совещаний он вступил в полемику с самим Берия, за что был тут же уволен.

Представляю себе эту полемику!

– Товарищ Сталин поставил советским криптографам задачу: читать всех, но наши шифры и переписку читать никто не должен!

– Товарищ Берия, американский криптограф Клод Шеннон недавно доказал, что при наложении на открытый текст случайной и равновероятной гаммы такой шифр является абсолютно стойким, вскрыть его теоретически невозможно.

– Товарищ Верченко! Вы коммунист? Считаете, что Вас указания товарища Сталина не касаются?

– Товарищ Берия, но ведь криптография – это точная наука, один из разделов математики. В ней есть свои законы, так же, как законы природы, не зависящие от людей.

– Товарищ Верченко! У нас незаменимых людей нет. Если

для Вас результаты какого-то американского империалиста важнее указаний товарища Сталина, то попрошу Вас покинуть это совещание. Вы уволены!

Тут же, на выходе из здания МГБ, дежурный офицер отобрал у Ивана Яковлевича служебное удостоверение.

После публичного возражения Берии ведущего советского криптографа, чуть было не был провозглашен лозунг о том, что криптография – это «буржуазная лженаука», а криптографы – «приспешники американского империалиста Шеннона». Почему этот топор тогда так и не был запущен, а все ограничилось лишь увольнением Верченко, остается неясным до сих пор. Возможно, помешали секретность, немецкая Энигма или арест Берия. Скорее всего – все вместе, а может и еще что-то, скрываемое и сейчас.

И вот в 1960 году – перебежчики из АНБ, Мартин и Митчел.

Иван Яковлевич, помоги! Спаси и сохрани нас от АНБ! Так Отдел науки ЦК КПСС обратился к Верченко, с которым Берия расправился несколько лет назад. В 1962 году руководство КГБ предложило воссоздать Высшую школу криптографов на базе Высшей Краснознаменной школы КГБ. Воссоздать на базе ВКШ КГБ ликвидированную ВШК, назвав ее 4 (техническим) факультетом ВКШ КГБ. Как это? Ведь ВШК – это яйцеголовые математики-криптографы, почти что люди с другой планеты, у которых в голове одни теоремы и их математическое доказательство. А ВКШ – это во-

енное учебное заведение с казармой, хождением в военной форме и сапогах, с заместителем начальника школы по строевой подготовке, капитаном первого ранга, прозванным за это «боцманом». Как их совместить в одном учебном заведении?

История советской криптографии так причудливо повернулась, что сам факт открытого возражения Берии стал тогда для Ивана Яковлевича лучшим орденом. В отделе науки ЦК КПСС и в руководстве КГБ тогда еще при СМ СССР могли не разбираться в криптографии, но открытый спор с Берия – это понимали абсолютно все! Вот человек, который сможет создать оазис математики и криптографии в ВКШ КГБ под носом у ее руководителей типа «боцмана».

И Иван Яковлевич смог! Его назначили на должность начальника факультета 17 мая 1963 года и одновременно он был начальником кафедры математики.

В первом отчете о работе факультета в июле 1963 года Иван Яковлевич предложил программу развития, которая касалась практически всех сторон жизни факультета. Об этой программе можно узнать из биографии Верченко, выпущенной ИКСИ к 100-летию со дня его рождения. Здесь же мне хотелось бы выделить из нее такую цитату: «По мнению И.Я.Верченко, технический факультет со временем должен был стать центром научной мысли в определенных областях специальных исследований. … И.Я.Верченко сам подавал пример, активно участвуя … в научном анализе рабо-

ты специальной техники.»

Верченко заложил на 4 факультете ВКШ КГБ университетские традиции и всячески поощрял связи с МГУ. Слушателям первых наборов на 4 факультет руководство факультета во главе с Верченко организовало оформление постоянных пропусков в МГУ для посещения спецкурсов и спецсеминаров ведущих профессоров университета.

В итоге СССР получил уникальное учебное заведение – 4 факультет ВКШ КГБ – готовившее высокообразованных, квалифицированных и весьма редких в 60-80 годах прошлого века математиков-криптографов.

Приехали!

«Русские вознесли достижения своей страны в криптологии до высоты полета ее космических спутников» – это оценка американского историка Дэвида Кана, человека из противоположного лагеря в проходившей тогда холодной войне, высказанная им в 1967 году.

«Поехали!» – сказали в советской криптографии такие люди, как Верченко и воспитанная им плеяда замечательных специалистов, математиков-криптографов, ставших на 4 факультете в 70-е годы нашими любимыми преподавателями.

Университетские традиции, заложенные на 4 факультете Иваном Яковлевичем, предполагали не только образование университетского уровня, но и воспитание свободолюбивых граждан, мыслящих самостоятельно и не горящих желанием ходить строевым шагом.

Но с уходом с 4 факультета Ивана Яковлевича на должность начальника факультета назначили генерала, любившего хождение строевым шагом.

– В первую очередь нам нужны хорошие военные, а потом уже – хорошие специалисты.

И потихонечку, полегонечку, строевым, шаг за шагом, начались попытки вытравить на 4 факультете те университетские традиции и вольности, которые были заложены Верченко.

В 2008 году я выложил в свой LiveJournal книгу «Криптография и Свобода». (https://mikhailmasl.livejournal.com/4852.html), версии которой для чтения с помощью различных устройств можно скачать на Литрес (https://www.litres.ru/book/mihail-evgenevich-maslennikov/kriptografiya-i-svoboda-71369458/?lfrom=1205764204). В этой книге я иногда буду вспоминать о ней, называя ее для краткости просто КиС.

Чтобы конкретно представить себе процесс создания «хороших военных» вместо специалистов-криптографов, достаточно прочитать в КиС несколько высказываний нашего начальника курса, подполковника, прозванного Чудой.

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

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

И так далее, в том же духе.

Но не тут то было! Отбор слушателей на 4 факультет был очень строгий. Отделы кадров 8 и 16 управлений КГБ искали среди школьников старших классов победителей различных олимпиад, причем не только по математике. С каждым проводилось индивидуальное собеседование и предлагалось поступать на 4 факультет. Конкурс тоже регулировался отделами кадров. В 1974 году – примерно 3 человека на место. И одно очень важное замечание: почти все, кто учился тогда на математиков-криптографов, поступили на 4 факультет сразу

же после школы, избежав срочной службы в Советской Армии. Негласно, но вполне справедливо, считалось, что после армии человек к серьезной математике уже неспособен. Были исключения, но для того, чтобы под них попасть, от человека требовалось доказать свой недюжинный талант.

В таком коллективе университетские традиции Верченко впитывались и надолго оставались в нем гораздо лучше, чем хождение строевым шагом. А анекдотичные высказывания Чуды только усиливали любовь к математике, как бы говоря:

– Вот, смотрите, что такое хороший военный! Хотите быть такими же? Нет? Так учите получше математику!

Более детально останавливаться на особенностях обучения на 4 факультете я сейчас не буду, интересующемуся читателю могу предложить почитать об этом в КиС.

В 1979 году я закончил 4 факультет и был направлен на работу в 5 (Теоретический) отдел Спецуправления 8 ГУ КГБ СССР.

В то время вся криптография в СССР еще была окутана плотной завесой секретности. Долгое время АНБ придерживалось такой же точки зрения: все, что связано с криптографией – секретно! Но оказалось, что в США АНБ не всесильно. В 1977 году правительством США был утвержден DES – Data Encryption Standard, который был открыто опубликован 17 марта 1975 года в федеральном реестре. Разработкой DES занималась компания IBM. Сенат США в 1978 году проверил действия АНБ и признал, что «представители АНБ ни-

когда не вмешивались в разработку алгоритма DES».

Первая реакция в СССР, где вся криптография секретна: коварные американцы. Сейчас мы найдем американскую закладку в DES, все разломаем, все прочитаем, покажем им кузькину мать.

В 1979 году, когда я только-только пришел на работу в 5 отдел, к нам в гости пожаловал заместитель начальника 8 ГУ КГБ СССР генерал-майор Владимир Николаевич Сачков. Говоря про DES, он поставил всем сотрудникам Теоретического отдела СУ 8 ГУ КГБ СССР такую задачу:

– Проведите криптографический анализ DES и найдите в нем какую-нибудь уязвимость. Если у вас получится найти уязвимость в DES, то я буду докладывать об этом на самом высоком уровне.

Найти уязвимость в DES не удалось. О чем же докладывать на самом высоком уровне? Да мы сделаем свой стандарт шифрования! А как же тотальная советская секретность в криптографии? А мы его сделаем из американского DES!

Так в СССР в начале 80-х появились криптографические чиновники. Первой их задачей было создание советского стандарта шифрования из американского DES. На это ушло почти 10 лет, советский криптографический стандарт шифрования получил корявое название «алгоритм ГОСТ 28147-89».

Известный американский криптограф Брюс Шнайер в своей книге «Прикладная криптография», выпущенной в

1994 году, сравнил DES и ГОСТ 28147-89

«Вот главные различия между DES и ГОСТ:

DES использует сложную процедуру генерации подключей из ключей. В ГОСТ эта процедура очень проста.

В DES 56-битовый ключ, а в ГОСТ – 256-битовый. Если добавить секретные перестановки S-блоков, то полный объем секретной информации ГОСТ составит примерно 610 бит.

У S-блоков DES 6-битовые входы и выходы, а у S-блоков ГОСТ – 4-битовые входы и выходы. В обоих алгоритмах используется по восемь S-блоков, но размер S-блока ГОСТ равен одной четвертой размера S-блока DES.

В DES используются нерегулярные перестановки, названные P-блоком, а в ГОСТ используется 11-битовый циклический сдвиг влево.

В DES 16 этапов, а в ГОСТ – 32.»

Можно ли было сделать первый советский стандарт шифрования как-то по-другому, не из американского DES? Ведь алгоритмы DES и ГОСТ 28147-89 были сравнительно медленными, для практической реализации ГОСТ 28147-89 на первых персональных компьютерах типа IBM PC XT пришлось создавать специализированную плату «Криптон» с аппаратной реализацией этого алгоритма, поскольку программная реализация работала слишком медленно.

На одном из совещаний в СУ 8 ГУ КГБ СССР, проходившем примерно в 86 или 87 году, стоило мне сказать о том,

что чисто советская разработка – алгоритм «Ангстрем – 3» – работает примерно в 10 раз быстрее, чем алгоритм «Магма», ставший впоследствии ГОСТ 28147-89, как курировавший продвижение «Магмы» в ГОСТ заместитель начальника СУ Анатолий Иванович Куранов испуганно спросил меня:

– Вы не пробовали подавать документы на оформление «Ангстрема-3» в качестве национального стандарта шифрования?

Про «Ангстрем-3» я уже писал в КиС. Это была красивая и простая криптографическая схема. На ней многие (я в том числе) писали диссертации. Но писать горы всяких чиновничьих бумаг на оформление в качестве национального стандарта шифрования желающих не нашлось. Да и представлялась тогда вся эта затея с национальным стандартом какой-то несерьезной. А как же быть с грифами секретности? А кому он нужен, этот национальный стандарт шифрования, при развитом социализме? Всё – государственное, частная собственность – ругательное слово. Надо было начальству позлить американцев, создавших свой DES с помощью частной фирмы IBM, и объявившими его открытым стандартом. Напрягли они советское криптографическое начальство – пусть теперь сами напрягаются с нашим ГОСТом.

Боюсь утомить читателя подробностями того, как постепенно советская, а затем и российская криптография усилиями криптографических чиновников сползала с космической орбиты в земное болото. Ведь от меня ждут описания

Южной Кореи, их образа жизни, их девушек. Ждут красивых фотографий корейских гор, достопримечательностей и многого другого.

Поэтому постараюсь вкратце рассказать, как в России в 90-х годах сказали «достигшей высоты полета космических спутников» криптографии:

– Приехали!

Это сказали криптографические чиновники. Внезапно в 90-х годах криптография из науки, специфического раздела математики, стала полем для слишком вольного выпаса на нем чиновников, для создания безграмотных законодательных документов, в которых постарались запретить все, что связано с криптографией. Зачем? Для приватизации всего криптографического, для устранения конкурентов. На смену лозунгу «Читать всех, но наши шифры и переписку читать никто не должен» пришел более простой и понятный лозунг времен НЭПа: «Обогащайтесь!»

Оставалось только одно – уехать работать за границу.

Что произошло в Южной Корее

В детстве я любил читать газеты, и в то время (конец 60-х годов) о Южной Корее писали не иначе, как о марионеточной проамериканской стране. Возможно, какая-то доля истины в этом и была: страна жила на американские дотации, которые зачастую банально разворовывались – некий аналог легких нефтяных денег в современной России. Но затем власть в Сеуле захватили военные и, как теперь стало ясно, они навели порядок в экономике. Вместо банального разворовывания деньги стали вкладываться в закупку новых технологий и развитие производства. Через 10 – 15 лет о Южной Корее заговорили как об азиатском тигре и южнокорейские товары стали завоевывать мир. Вот такая краткая и поучительная история со счастливым концом про корейское экономическое чудо. Ну а мне предстояло увидеть это чудо своими глазами и даже принять некоторое участие в том, чтобы оно стало еще чудеснее.

Причина, по которой корейцы в 2002 году стали искать зарубежного криптографа, была простая: у них накануне по Интернету утащили из одного банка $50 000 (см. http://www.dslreports.com/forum/remark,13621296). Вот перевод этой статьи на русский язык.

«Корейский хакер украл 50 000 долларов из онлайн-банка

СЕУЛ: 20-летний бросивший школу подросток взломал систему онлайн-банкинга и украл около 50 000 долларов, что вызвало тревогу по поводу безопасности широко используемых в Южной Корее услуг интернет-банкинга. В пятницу полиция арестовала мужчину, опознанного только по фамилии Ли, и его неустановленного сообщника за кражу 50 миллионов вон (50 000 долларов) с банковского счета 42-летней домохозяйки в мае. Это был первый случай взлома и ограбления счета онлайн-банкинга в Южной Корее, лидере по количеству пользователей высокоскоростного Интернета. По состоянию на апрель количество подписчиков онлайн-банкинга составляло 23 миллиона, что составляет около половины населения страны. По данным полиции, Ли прикрепил хакерское программное обеспечение к сообщению, которое он разместил на сайте сообщества. Женщина нажала на нее, непреднамеренно загрузив хакерскую программу «key stroke», которая позволила Ли получить пароли и код безопасности для ее учетной записи. Полиция заявила, что пользователи Интернета должны избегать загрузки незнакомых программ в Интернете и устанавливать защитное программное обеспечение, предоставляемое банками.

Международные новости»

Эта заметка написана малазийцем Гекке Краай, дата – 2003-03-21. Но поскольку в ней упоминаются апрель и май, то описанное происшествие было в 2002 году или ранее.

Это, конечно, не чеченские авизо, но что-то на ту же тему. История получила широкую огласку и, перефразируя популярную песню Андрея Макаревича, корейский исполком забил в колокола.

Меня в этом сообщении привлекла строка: «По состоянию на апрель количество подписчиков онлайн-банкинга составляло 23 миллиона, что составляет около половины населения страны.» В 2002 году половина жителей Южной Кореи уже пользовались онлайн-банкингом!

Как конкретно корейцы стали бороться за безопасность своего онлайн-банкинга и что он представлял из себя в начале нулевых – обо всем этом я постараюсь рассказать в этой книге.

Ну и, конечно же, – много красивых фотографий Сеула, корейских гор и не только их.

Сеул. Дворец.

Знакомство

У читателя наверняка уже масса вопросов к автору:

– Как ты узнал о том, что в Южной Корее требуется криптограф?

– А корейцы знали, что в прошлом ты был сотрудником КГБ?

– Корейцы знали что-нибудь о проблемах с фальшивыми авизо у Центрального Банка России в 1992 году?

– Как и кто тебя встретил в Сеуле?

И таких вопросов – бесконечное множество. Постараюсь постепенно, step by step, ответить на них.

Желание искать работу за границей появилось не сразу. Во время службы в КГБ СССР я, естественно, был невыездным. Увольнение со службы было весьма драматическим и оставило в моей памяти незаживающий рубец на всю жизнь. При моем непосредственном участии была создана и начала успешно функционировать с 1 декабря 1992 года система криптографической защиты от фальшивых авизо для Центрального Банка России. Обо всем этом я писал в КиС, а затем и в отдельной своей книге «Маркант», которая сейчас доступна на Литрес. (https://www.litres.ru/book/mihail-evgenevich-maslennikov/markant-71339377/)

Было огромное желание продолжить заниматься криптографией, писать криптографические программы, но неза-

висимо от чиновников ФАПСИ, которые в 90-х годах откровенно стремились к абсолютной монополии на все, что так или иначе было связано с криптографией. Усилиями этих чиновников были приняты невразумительные нормативные документы, основной целью которых был тотальный запрет всего и всех, кто стремился остаться независимым от ФАПСИ. Моя система электронного документооборота V.TeleDoc, введенная в эксплуатацию в крупнейшем российском банке «Возрождение», вызвала ярость чиновников. В 2001 году я получил письмо из ФАПСИ с требованием «привести свою деятельность в соответствии с действующим законодательством Российской Федерации». Это письмо опубликовано в книге «Маркант» и в КиС.

Пора искать работу за пределами Российской Федерации.

Осенью 2002 года поиск зарубежного работодателя в Интернете завершился успешно. Предложение из Южной Кореи, требуется специалист-криптограф. Для чего – я тогда еще не знал.

Я сразу же сказал на проводившемся по Интернету собеседовании, что до 1994 года был на военной службе подполковником КГБ, а на криптографа учился на 4 факультете Высшей школы КГБ СССР. Работодателя это нисколько не смутило. Гораздо больше его интересовали мои работы по криптографической защите Центрального Банка России и банка «Возрождение». Собеседование прошло успешно.

Самолет «Аэрофлота» подлетал к Сеульскому аэропорту

Инчхон. Кто и как меня там встретит? Как мы будем общаться, на каком языке? Где я буду жить? Как начнется моя работа в корейской компании? Что делать в выходные? А вдруг в Южной Корее тоже есть какие-то законодательные запреты в области криптографии?

Эти и многие другие вопросы вызывали некоторое волнение и опасения. Все они оказались напрасными, это сказывалась привычка к «советскому образу жизни» с его запретами и проблемами на каждом шагу.

Мое первое очное знакомство с корейским работодателем прошло успешно. Мы общались с ним по-английски, моих познаний в этом языке со времен экзаменов кандидатского минимума оказалось вполне достаточно. Никаких запретов в области криптографии в Южной Корее нет, условия жизни – нормальные, отдельный номер в гостинице, оплачивает жилье компания. Я с головой погрузился в свою любимую работу, а по выходным – лазил по корейским горам.

Они расположены тут же, в Сеуле, и в них развернуты национальные парки для отдыха. Южная Корея – территориально весьма небольшая страна, ее размер сравним с размером Московской области, 70% территории – горы. Дачных участков практически ни у кого нет, по выходным жители Сеула в большинстве своем отправляются в национальные парки лазить по горам. До этих парков легко добраться на метро.

Вершина корейской горы Добонгсан

KISA

Иногда в России мне приходилось спрашивать у криптографических чиновников:

– Как вы относитесь к международным криптографическим стандартам?

Типовой ответ:

– У нас свои стандарты.

А один на стене своего служебного кабинета в ФАПСИ даже повесил плакат

– Тот, кто встроил RSA, тот проныра и лиса.

Вот такие в России «идеи чучхе». Почему-то криптографические чиновники считают оторванность российской криптографии от цивилизованного мира за благо. «Мы сами себе придумываем свои криптографические стандарты, нам Америка не указ!»

Лукавят! Не все российские криптографические стандарты придуманы в России. Все, что касается открытых ключей и электронной подписи, придумали американские криптографы. Я писал об этом в книге «Маркант».

Но главное не в том, кто и что придумал, а в том, как использовать криптографические алгоритмы.

Если вы создаете какой-то сложный программный комплекс, например, систему Интернет-банкинга, ориентированную на неопределенный круг потребителей (помните –

«количество подписчиков онлайн-банкинга составляло 23 миллиона, что составляет около половины населения страны»), то ваш программный комплекс должен будет работать с типовыми устройствами и типовой операционной системой, которыми пользуется этот неопределенный круг потребителей в своей повседневной жизни. Если в свободной стране вы начнете создавать какие-то надуманные проблемы миллионам пользователей, то они просто не будут использовать ваш Интернет-банкинг и закажут его создание другой фирме.

Типичный пример надуманных проблем, создаваемых в России криптографическими чиновниками, – это запрет общепринятых международных стандартов и, в первую очередь, запрет асимметричного алгоритма RSA. Разумных объяснений этим запретам нет, так захотели чиновники и все тут. И, к огромному сожалению, эти чиновники получили практически неограниченные права все запрещать, не неся при этом ни малейшей ответственности за последствия, вызываемые этими необоснованными запретами.

В Южной Корее я наконец-то выбрался из российского криптографического «королевства кривых зеркал». Полстраны пользовались Интернет-банкингом не потому, что разрешили чиновники, а потому, что это было удобно. Хотя криптографические чиновники в Южной Корее тоже есть, но само название их организации – Korean Information Security Agency (KISA) – для уха российского криптографа

звучало ласково и по-домашнему тепло. Они не создавали никаких идиотских запретов, а наоборот, иногда очень даже помогали. Далее в этой книге я расскажу, когда и при каких обстоятельствах мне пришлось иметь дело с KISA.

Естественно, что никто в Южной Корее не считал криптографию и создание криптографических программ чем-то особенным, требующим каких-то лицензий и сертификатов от KISA. Используй при этом все, что необходимо и удобно, главное – чтобы работало и было востребовано конечным пользователем. Создать как-то иначе Интернет-банкинг, которым пользуется полстраны, просто невозможно. Нужно для создания более безопасного Интернет-банкинга привлечь иностранного криптографа – пожалуйста, никакого разрешения KISA для этого тоже не требовалось.

Олимпийский парк в Сеуле. Скульптура «Указующий перст».

Пьяный алгоритм RSA

Взявшись за написание этой книги, я сам себе дал слово писать ее как можно более простым языком, по возможности избегать сложных математических формул и терминов. Книга должна быть интересной обычному читателю, который не должен напрягаться от чего-то непонятного. Непонятно – значит надо разъяснить как можно более простыми словами и примерами.

Как я упоминал выше, в 2003 году малазиец Гекке Крайай пишет про Интеренет-банкинг Южной Кореи: *«Это был первый случай взлома и ограбления счета онлайн-банкинга в Южной Корее, лидере по количеству пользователей высокоскоростного Интернета»* Сам случай произошел в 2002 году. А когда в Южной Корее запустили систему Интернет-банкинга?

Корейский Интернет-банкинг был тесно связан с криптографией. В нем использовалась криптографическая аутентификация и электронная цифровая подпись. В свою очередь, эти два понятия тесно связаны с асимметричной криптографией и цифровыми сертификатами.

Когда какой-то человек приходит в отделение банка, то его просят представиться: кто вы и что вам здесь надо. Если тот же человек пытается зайти на банковский сервер, то сервер делает фактически то же самое – пытается про-

верить подлинность и цели обратившегося к нему клиента. А как это сделать? Одним из распространенных методов проверки подлинности клиента является его криптографическая аутентификация, т.е. проверка подлинности с помощью криптографических методов.

Криптографическая аутентификация предполагает проверку электронно-цифровой подписи (ЭЦП) клиента. А нормальная ЭЦП, в свою очередь, предполагает наличие у клиента ключа для подписи, а у сервера – ключа для проверки подписи клиента. Ключ, с помощью которого клиент осуществляет подпись, называется private key, а ключ, с помощью которого сервер осуществляет проверку подписи клиента – public key. По-русски – закрытые и открытые ключи. Закрытый ключ иногда именуют секретным, а открытый – публичным.

Вопросы и ответы.

Есть ли у клиента его открытый ключ?

Есть.

Есть ли у сервера закрытый ключ клиента?

Нет.

Связаны ли между собой закрытые и открытые ключи?

Да, связаны, каждому закрытому ключу соответствует строго определенный открытый ключ.

Можно ли по закрытому ключу определить открытый ключ?

Да.

Можно ли по открытому ключу определить закрытый? Нет.

Теперь о сертификате. Открытый ключ еще называют публичным, потому что он у всех на виду. А появляться на публике голому открытому ключу просто неприлично. Вот его приодевают и приукрашивают в специальной организации, называемой Центром Сертификации (ЦС) или, по терминологии Microsoft, Certification Authority (CA). Приодетый и приукрашенный открытый ключ, получивший в ЦС персональную ЭЦП, и принято называть сертификатом.

Как приодевают и приукрашивают в ЦС открытый ключ – особая песня. Различных атрибутов в сертификате может быть великое множество: фамилия, имя, отчество владельца, его должность, место работы, место жительства, электронная почта и т.д. и т.п. Указывается также назначение ключа (key usage или extended key usage): для подписи или шифрования электронной почты, для идентификации пользователя на сервере, для подписи программных кодов, для EFS (Encrypted File System) и прочая, прочая, прочая. В сертификате обязательно присутствуют срок действия ключа и электронная подпись ЦС. Здесь опять же, пробегая галопом по такой необъятной теме, как состав информации, включаемой в сертификат, я руководствовался принципами гуманизма к обычному читателю, стараясь не перегружать далекого от криптографии человека всеми нюансами, связанными с созданием в современных информационных систе-

мах персональных сертификатов. Вкратце: это «одетый» открытый ключ, получивший «паспорт» – персональную ЭЦП в ЦС. «Одежд» может быть много, иногда и самых экзотических: корейцы, например, включают в свои сертификаты хеш-функцию от национального ID и некоторого случайного числа – это их персональный атрибут, который называется KR, по-видимому, Korean Random.

Читаем Википедию.

«Инфраструктура открытых ключей (ИОК, англ. PKI – public key infrastructure) – набор средств (технических, материальных, людских и т. д.), распределённых служб и компонентов, в совокупности используемых для поддержки криптозадач, на основе закрытого и открытого ключей. В основе PKI лежит использование криптографической системы с открытым ключом»

В Интернете я наткнулся на интересную презентацию, которую приготовил mr. Jae-IL, Lee, Vice President of Korea Information Security Agency and Secretary General of Korea PKI Forum. В ней дается краткое представление о PKI наиболее развитых стран азиатско-тихоокеанского региона: Южной Кореи, Китая, Японии, Сингапура, Тайваня, Таиланда и Индии. В частности, с момента появления PKI в феврале 1999 года в Корее было выдано примерно 11 миллионов сертификатов, а в Китае – 5 млн. с августа 2004. По остальным странам даются только даты появления PKI: в Японии – апрель 2001, Сингапур – 1998 год, Тайвань – апрель 2002, Та-

иланд – 2001 год, Индия – июнь 2000. Россия в этой презентации даже не упоминается.

В самой Корее действует 6 национальных сертификационных центров. Около 70% выданных сертификатов используются для Internet Banking.

Тут меня немного смутило расхождение в количестве пользователей Интернет-банкинга у Гекке Краай (23 миллиона) и mr. Jae-IL, Lee, Vice President of KISA (70% от 11

миллионов). У одного из них данные не совсем верные. По-моему, прав вице-президент KISA. Но в любом случае, счет идет на миллионы пользователей.

Итак, предварительной оценкой начала работы Интернет-банкинга в Южной Корее можно считать февраль 1999 года, когда появилась первая PKI. Эта PKI была представлена в виде специализированного программного обеспечения XecureWeb, разработанного корейской фирмой SoftForum. Вот что сказано про XecureWeb в японской Википедии (https://ja.wikipedia.org/wiki/Xecureweb)

«XecureWeb – система, разработанная в Корее. Это программное обеспечение (программное обеспечение PKI), которое обеспечивает взаимное доверие и надежную связь в сети»

Читатель, видимо уже заинтересовался: а какая асимметричная криптография используется в Корее? Можно ли рассказать о ней поподробнее?

Рассказываю поподробнее.

Как-то в апреле 1977 года три еврея собрались выпить. Напились и придумали алгоритм с открытым распределением ключей RSA – первые буквы их фамилий: Rivest, Shamir, Adleman. Не верите? Напрасно. Читайте Википедию.

«Рон Ривест, Ади Шамир и Леонард Адлеман из Массачусетского технологического института в течение года предприняли несколько попыток создать одностороннюю функцию, которую было бы трудно инвертировать. Ривест и

Шамир, будучи компьютерными учеными, предложили множество потенциальных функций, а Адлеман, будучи математиком, отвечал за поиск их слабых мест. Они опробовали множество подходов, включая "ранцевый" и "перестановочные полиномы". Какое-то время они думали, что то, чего они хотели достичь, невозможно из-за противоречивых требований. В апреле 1977 года они провели Песах в доме одного из студентов и выпили много манишевицкого вина, а затем вернулись к себе домой около полуночи. Ривест, не в силах заснуть, лег на диван с учебником математики и начал думать о своей односторонней функции. Остаток ночи он провел, формализуя свою идею, и к рассвету большая часть статьи была готова. Алгоритм теперь известен как RSA – инициалы их фамилий в том же порядке, что и в их статье.»

И стал этот пьяный алгоритм RSA мировым асимметричным стандартом. Очень удобным и практичным. С его помощью легко осуществлять асимметричное шифрование и электронную подпись. И в корейском Интернет-банкинге тоже используется алгоритм RSA.

Конец ознакомительного фрагмента.