Кодирование

{Кодирование информации в рыночных условиях}

Назначение

Материал подготовлен в 1995 году.

Кодирование – один из способов скрытия информации таким образом, чтобы избежать использование информации одной группы лиц и обеспечить это же использование иной группе. В то же время принципы кодирования должны быть известны третьей группе (и, соответственно, все коды). К первой группе можно отнести все виды бандформирований, созданные государством, ко второй – банки, к третьей – ФАПСИ. Построение такого треугольника является идеальным для ведения банковской деятельности. Бандформирования могут у ФАПСИ покупать коды доступа, банки могут переводить себе в карман любые средства под видом незаконного проникновения в их базы данных.

Таким образом, кодирование не является автономным и уникальным инструментом для хранения информации, а только средством для создания равновесной системы.

1. История кодирования.

В III веке до новой эры индийский император Ашока организовал “Общество девяти неизвестных”. В каждую из 9 книг собиралась определённая информация. Так, в книгу 1 – информация о способах ведения войны, в книгу 3 – кодирование информации. В то время в Индии уже было известно 64 способа кодирования информации. Первые зачатки блок-схем (особенно ВИВ-схем, к которым относятся **адамаровы конфигурации**) можно найти в этих книгах (некоторые элементы были опубликованы 80 лет назад).

За период до XXI века было столько разработок по кодированию, что только их перечень составит библиотеку.

2. Ссылки и справка.

Математический энциклопедический словарь. Москва, “Советская энциклопедия”, 1988, стр. 96: “...Среди ВИВ-схем наиболее изучены следующие подклассы: системы Штейнера... **адамаровы конфигурации**... аффинные и проективные конечные геометрии... Применяются в теории кодирования (при построении кодов)”.

То есть то, что **адамаровы матрицы** используются в кодировании информации, математике известно.

В 1991 году **Создан программный комплекс**, включающий программы по защите файловой и дисковой информации. Компьютеры – серии 386, 486, Системы – WINDOWs 95, 98. Полная стыковка на уровне супервизора, отсутствие признаков наличия программного комплекса на ЭВМ.

Создан одноразовый блокнот!

Особенности при кодировании файлов:

– Размер файла и контрольная сумма сохраняются.

– Файл при кодировании не переписывается, а кодируется “сам в себе”.

– Скорость кодирования совместима со скоростью чтения – записи на внешний носитель типа CD.

– При попытке чтения кодированного файла получаем “белый шум”.

– Размер файла для кодирования не ограничен.

Особенности при кодировании дисков:

– Диск закрывается полностью в течение микросекунд, получаем “белый шум” для всего диска.

– Без знания ключа вскрыть диск невозможно.

К основе – адамаровы матрицы были добавлены:

– система вращающихся уравнений;

– элементы теории “калейдоскоп” разработки А. Хатыбова (решения задачи о назначении).

Отметим, что добавленные структуры современной математике не известны и являются “НОУ – ХАУ” компании “РИТМ-фонд”.

3. В 1995 году вышел Указ N 334 Президента РФ “О мерах...”

В Указе Президента РФ от 3 апреля 1995 года N 334 “О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставлении услуг в области шифрования информации” (в дальнейшем “Указ N 334 о мерах”) говорится:

“Запретить использование государственными организациями и предприятиями в информационно-телекоммуникационных системах шифровальных средств, включая криптографические средства обеспечения подлинности информации (электронная подпись), и защищенных технических средств хранения, обработки и передачи информации, не имеющих сертификата ФАПСИ”.

“Предложить Центральному банку РФ и ФАПСИ принять необходимые меры в отношении коммерческих банков РФ, уклоняющихся от обязательного

использования имеющих сертификат ФАПСИ защищенных технических средств хранения, обработки и передачи информации при их информационном взаимодействии с подразделениями Центробанка.”

“…запретить деятельность юридических и физических лиц, связанную с разработкой, производством, реализацией и эксплуатацией шифровальных средств… предоставлением услуг в области шифрования информации без лицензий, выданных ФАПСИ”.

“ФСК и МВД совместно с ФАПСИ, Государственной налоговой службой РФ и департаментом налоговой полиции РФ осуществлять выявление юридических и физических лиц, нарушающих требования настоящего Указа.”

“Государственному таможенному комитету РФ принять меры к недопущению ввоза на территорию РФ шифровальных средств иностранного производства…”

Для того, чтобы оценить указ, надо вернуться к введению (стр.1).

После выхода указа все работы по кодированию были остановлены, получить какое-либо разрешение на ведение работ не представлялось возможным.

Результаты.

Разработанная система защиты информации с использованием **адамаровых конфигураций** (адамаровых матриц) до настоящего времени является идеальной системой защиты.

Система устанавливалась частным лицам и в структурах, где действительно была необходимость такой защиты.

4. Мнения сторонних организаций.

Фирма INTEL (Англия), 1999 г. Командировка в Дублин на симпозиум:

– “Продемонстрированная система защиты является лучшей и для фирмы является не досягаемой для понимания, однако матрицами адамара фирма занимается, и в ближайшие десятилетия будут разработаны аналоги…”;

– Германия, Эссен. 1995 г. Управляющий банком (встреча А. Хатыбова): “Как же работать с такой системой, если нельзя ничего перевести на свой счёт? И при этом сослаться на взлом.”;

– Москва, 1995г. Приезд специалиста от NATO по просьбе банкира из Эссена. Специалисту показали возможности программного обеспечения, уехал с разинутым ртом, реакции не было;

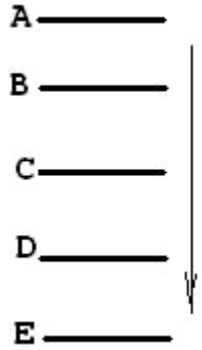
– Вновь созданная Налоговая Инспекция, Москва. 1995 г. Система была установлена на их компьютере. После демонстрации всех возможностей специалисты категорически отказались от использования иных систем кодирования. Поступил приказ убрать систему и использовать то, что предлагает ФАПСИ;

– Специалистам ФСБ было предложено дешифровать файл (Офис С. Кугушева). Файл дешифровать не смогли, но в официальном ответе есть фраза: “**Представленная система является старой и интереса не представляет**“.

Отметим, что до сих пор аналогичных систем защиты информации в мире нет!

Отдельно рассмотрим вопрос технического применения матриц адамара.

Звук



Для формирования звука имеем (числовые данные примерные):
A – эталон гравитационной частоты (10^{18}Гц)
B – тактовая частота мозга атмосферы (10^{16}Гц)
C – несущая частота мозга атмосферы (10^{15}Гц)
D – тактовая частота мозга гуманоида человека (10^{12}Гц)
E – несущая частота мозга гуманоида человека (7.2 – 22110 Гц)

Кодированию доступен только диапазон E, но любая звуковая информация сохраняется в диапазоне C (передача мысли на расстоянии). Если произвести незначительные изменения в диапазоне D, то несущая частота мозга гуманоида человека может измениться – либо полная потеря слуха, либо слышны “чужие голоса”, либо получим качественный особо чистый звук (разработки А. Бурлаченко). Технические средства для формирования искажений при передаче звуковой информации известны, но они работают только в диапазоне E.

Диапазон C шифрования не подлежит. Любое изменение внешних условий ликвидирует смысл шифрования звука, и без знания основ формирования звука – это искать что-то в тёмной комнате.

Спектральный анализ и кодирование спектров и сигналов

О спектрах химических элементов в настоящее время известно всё. Составлены подробные пухлые тома и требуется только использовать достижения науки для получения нужного результата, и чтобы результат остался тайной, можно использовать шифрование. Особенно важно в ПВО, системах наведения и так далее.

Однако. Для формирования любого спектра необходима эталонная (базовая) частота. Она “сформировалась” не так давно, и диапазон примерно 10^{16}гц.

В этом диапазоне – 2 базовых диапазона частот. Условно назовём их А и В.
Но в этих диапазонах в последние годы исчезло ряд частот (постоянные аварии на АЭС это подтверждают). Без знания принципов формирования радиационных частот заниматься их кодированием…(можно не продолжать).

Отдельные файлы – рекламы на программную продукцию
(желательно внимательно прочесть)

KODIPOVANIE **FAPSIA.RTF** **ITC-METH.DOC** **SHIFR6.RTF** **DCR_PREF.RTF** **FCR_pref.RTF** **SVC_PUBR.RTF**	**ТЕКУЩИЙ ФАЙД** **МНЕНИЕ ПО УКАЗУ N 334 (приложение к тексту)** **К заявке в РосАПО (приложение к тексту)** **Инструкция пользователю** **Система дисковой защиты** **Комплекс “СКАЛА” – система файловой защиты** **Сокращённый вариант описания (для ознакомления)**

P. S.
В планах работ по развитию системы *“INDEX-TWIST Cipherling”* предусматривалось: выпуск ЧИПА с готовой системой (ЧИП совмещён с операционной системой); разработка “брелков” для того, чтобы не работать с клавиатурой.

Приложение 1

25 декабря 1996 г.

ЗАЩИТА ОТ НСД

ШИФРОВАНИЕ, ЭЛЕКТРОННАЯ ПОДПИСЬ И КОНТРОЛЬ ДОСТУПА

Общие аспекты, российская специфика и вопросы защиты данных в системах прямой телекоммуникационной связи (в частности, в системах “клиент-банк”).

Защита от несанкционированного доступа (НСД) традиционно включает такие способы защиты от НСД, как шифрование, электронную подпись и контроль доступа к информации. Кроме того, возможно использование математических методов, которые сами по себе уже являются шифрозащитой (например, метод “Калейдоскоп” для решения в реальном масштабе времени NP -трудных и NP- сложных задач).

1. **Общий смысл шифрования.**

Шифрование электронной информации – нестандартная кодировка данных, исключающая или серьезно затрудняющая возможность их прочтения (получения в открытом виде) без соответствующего программного или аппаратного обеспечения

и, как правило, требующая для открытия данных предъявления строго определенного ключа (пароля, карты, отпечатка, и т. д.) – служит четырем основным целям.

1. “Статическая” защита информации, хранящейся на жестком диске компьютера или дискетах (шифрование файлов, фрагментов файлов или всего дискового пространства) исключает или серьезно затрудняет доступ к (открытым) данным лицам, не владеющим паролем (ключём), то есть защищает данные от постороннего доступа в отсутствие владельца информации. Статическое шифрование применяется в целях информационной безопасности на случай похищения файлов, дискет или компьютеров целиком (жестких дисков компьютеров) и исключения возможности прочтения данных любыми посторонними (не владеющими паролем) лицами.
2. Разделение прав и контроль доступа к данным. Разные пользователи могут владеть своими личными данными (разными компьютерами, физическими или логическими дисками одного компьютера, просто разными файлами), недоступными никаким другим пользователям.
3. Защита отправляемых (передаваемых) через третьи лица, в том числе и по электронной почте, данных.
4. Идентификация подлинности (аутентификация) и контроль целостности переданных через третьих лиц документов.

Шифрование – наиболее общий и, при достаточном качестве программной или аппаратной системы, надежный способ защиты информации, обеспечивающий практически все его аспекты, включая разграничение прав доступа и идентификацию подлинности (“электронная подпись”).

С точки зрения качества защиты шифрование можно условно разделить на “сильное”, или “абсолютное”, практически нескрываемое без знания пароля, и “слабое”, затрудняющее доступ к данным, но практически (при использовании современных ЭВМ) вскрываемое за реальное время без знания исходного пароля.

Несмотря на заверения сотрудников отечественных служб государственной безопасности в том, что их “боевые методы” позволяют раскрыть любой шифр, так что абсолютных шифров не существует, теоретически это утверждение неверно, поскольку хорошо известен абсолютно надежный шифр, называемый “одноразовым блокнотом”, и существуют его достаточно качественные программные реализации, практически же пристальное законодательное внимание, проявляемое к системам шифрования в любой стране мира (а с 1995 года и в России) и накладывающие жесткие ограничения на использование шифров в коммерческих и государственных структурах (как правило, это ограничение на длину ключа, но Россия в этом вопросе пошла дальше), доказывает обратное: для борьбы (интересы госбезопасности требуют доступности абсолютно всей информации, находящейся на территории государства) с (некоторыми) системами шифрования государство использует не “боевые методы”

дешифрования, а законодательную базу, запрещающую их использование.

2. Электронная подпись.

Электронная подпись – вставка в данные (добавление) фрагмента инородной зашифрованной информации – применяется для идентификации подлинности переданных через третьих лиц документов (и произвольных данных). Сама передаваемая информация при этом никак не защищается, то есть остается открытой и доступной для ознакомления теми лицами, через которых она передается (например, администраторами и инспекторами почтовых узлов связи).

Кроме того, электронная подпись сама по себе не обеспечивает контроля целостности данных, так что если получатель убеждается в верности подписи, это еще не означает, что сами данные имеют к ней какое бы то ни было отношение (хотя воспитанная на бумажном делопроизводстве психология “подсказывает” пользователю, что раз подпись стоит, то с данными все в порядке). Многие программные системы дополняют электронную подпись функциями контроля целостности, однако если на электронные подписи (точнее – на шифровальные системы, применяемые в них) существуют определенные стандарты и, можно сказать, гарантии (сертификаты ФАПСИ), то контроль целостности никем, кроме разработчиков, не гарантируется. Последние же, в азарте творчества, часто преувеличивают свои достижения до абсурда, утверждая, например, что контроль целостности произвольных данных произвольного объема может быть обеспечен числом из 15 или 20 знаков, что противоречит теории информации так же, как вечный двигатель – законам термодинамики. На самом деле, для обеспечения стопроцентной гарантии целостности данных, объем “довешиваемой” информации должен составлять от 0.00…1 до 100% объема исходных данных в зависимости от шумового коэффициента исходного материала. Для текста электронная подпись, гарантирующая целостность исходного документа, составляет не менее 10% его объема, для архивного файла – не менее 70%. (Можете легко проверить, выполняется ли это условие в используемых вами подписях, если вы их используете.) Заметим, что, в отличие от электронной подписи, шифрование (с обратной связью) дает стопроцентную гарантию целостности данных без увеличения их объема вне зависимости от природы этих данных.

Достоверность собственно электронной подписи целиком и полностью определяется качеством шифрующей системы.

С точки зрения решения задачи идентификации подлинности полностью зашифрованный файл и открытый файл с добавочной зашифрованной информацией (“электронной подписью”) абсолютно эквивалентны.

3. Контроль права доступа

Контроль прав доступа – простейшее средство защиты данных и ограничения (разграничения) использования компьютерных ресурсов, предназначенное для ограждения определенной информации и системных ресурсов от лиц, не имеющих к ним отношения и не имеющих специального умысла получить к ним доступ или не обладающих достаточной для этого квалификацией. Сами данные хранятся на дисках в открытом (незащищенном) виде и всегда могут быть востребованы (похищены) в обход системы контроля, сколь бы изощренной она не была.

4. Указ N 334 Президента РФ “О мерах...”

В Указе Президента РФ от 3 апреля 1995 года N 334 “О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставлении услуг в области шифрования информации” (в дальнейшем “Указ N 334 о мерах”) говорится:

“Запретить использование государственными организациями и предприятиями в информационно-телекоммуникационных системах шифровальных средств, включая криптографические средства обеспечения подлинности информации (электронная подпись), и защищенных технических средств хранения, обработки и передачи информации, не имеющих сертификата ФАПСИ”.

“Предложить Центральному банку РФ и ФАПСИ принять необходимые меры в отношении коммерческих банков РФ, уклоняющихся от обязательного использования имеющих сертификат ФАПСИ защищенных технических средств хранения, обработки и передачи информации при их информационном взаимодействии с подразделениями Центробанка”.

“...запретить деятельность юридических и физических лиц, связанную с разработкой, производством, реализацией и эксплуатацией шифровальных средств... предоставлением услуг в области шифрования информации без лицензии, выданных ФАПСИ.”

“ФСК и МВД совместно с ФАПСИ, Государственной налоговой службой РФ и департаментом налоговой полиции РФ осуществлять выявление юридических и физических лиц, нарушающих требования настоящего Указа.”

“...Государственному таможенному комитету РФ принять меры к недопущению ввоза на территорию РФ шифровальных средств иностранного производства...”

Замечания.

4.1. Деятельность служб госбезопасности и некоторых родственных структур, В ЧАСТНОСТИ, ФАПСИ, по разработке, реализации и сертифицированию шифровальных средств, регламентируется лицензиями, выданными Гостехкомиссией при Президенте РФ – всего 80 временных лицензий, ***ОДНА ИЗ КОТОРЫХ*** **принадлежит ФАПСИ**.

4.2. В Указе отсутствует какая-либо информация о программных и аппаратных вирусах и методах борьбы с ними **(само по себе использование вирусов следует отнести к деятельности ФАПСИ в первую очередь**).

Вирусы можно использовать не только для уничтожения информации, но и для "прикрытия" шифросистем, впрочем, и наоборот. Отсутствие этого пункта в Указе говорит **о некомпетентности тех**, кто Указ готовил (если речь идет действительно о Государственной безопасности, а не об использовании Государственного аппарата отдельными структурами) и тем более, кто им прикрывается.

4.3. В Указе ни слова не сказано об ответственности ФАПСИ (включая финансовую) за:

– передачу третьим лицам и организациям полученную информацию;

– вред, нанесенный некомпетентностью ФАПСИ по конкретным пунктам Указа;

– не использовании современных разработок в Государственном масштабе, если эти разработки по качеству превосходят все, чем располагает ФАПСИ;

– необоснованный отказ от современных разработок.

4.4. В Указе отсутствует информация о контроле за деятельностью ФАПСИ.

4.5. В Указе отсутствует информация собственно о шифросистемах и математических методах, даже косвенное использование которых уже является защитой. В разъясняющих к Указу материалах нет ссылок на организации, более компетентных в вопросах рассмотрения используемых математических методов. Запрет использования методов проблемы не решает.

4.6. В Указе нет информации о сертификации программной продукции, которая могла бы быть предоставлена.

4.7. В Указе нет механизма исполнения Указа, поэтому **ФАПСИ создала собственные коммерческие структуры**, что само по себе уже противоречит смыслу Указа.

5. Практика использования средств защиты в России

(с точки зрения "Указа N 334 о мерах")

Несмотря на богатый научный потенциал России в области криптографии и особенно бурное ее коммерческое развитие в начале 90-х годов, на настоящий момент единственным лицензированным ФАПСИ (подчеркнем: ФАПСИ) шифром является ГОСТ 28147-89, самому же ФАПСИ и принадлежащий. Все остальные системы шифрования, предлагаемые зарубежными и отечественными фирмами

(RSA, Silent Running Software – PGP, ЛАН Крипто – “Веста”, Аладдин, Novex, Элиас и др.) в виде “библиотек” – начиная с зарубежных стандартов (DES, FEAL) и кончая новейшими оригинальными разработками – являются в равной степени незаконными и подводят наиболее активных инициаторов их разработки и использования на грань уголовной ответственности.

Ни одна фирма (кроме ФАПСИ) не имеет также права использовать и распространять где бы то ни было ГОСТ 28147-89, поскольку ГОСТ – в исполнении произвольного разработчика – уже не ГОСТ, и, главное, внедрение шифрования в организации предусматривает передачу ФАПСИ контроля над ключами доступа к информации.

Вместе с тем (точнее, **ВСЛЕДСТВИЕ** позиции ФАПСИ, монополизировавшего рынок шифросистем), заявления многих авторов оригинальных криптосистем из известных в России фирм о наличии иностранных патентов, сертификатов и лицензий, подтверждающих высокое качество их разработок, является заведомо ложным, поскольку, во-первых, организация тестового полигона для серьезной проверки алгоритма шифрования стоит сотни тысяч долларов (в зависимости от страны, проводящей тестирование), которые, учитывая специфику рынка в этой отрасли бизнеса, никогда и ни в одной стране не окупятся без принятия соответствующей правительственной программы, и во-вторых, ни один автор оригинальной отечественной системы не может ОФИЦИАЛЬНО ВЫВЕЗТИ свою систему из России (в соответствии с приведенным выше указом), ВВЕЗТИ ее на территорию другого государства, зарегистрировать там, после чего ВЫВЕЗТИ ее за пределы этого государства и ВВЕЗТИ обратно в Россию. Если некоторые страны, например, и в отличие от России, США, еще допускают ИМПОРТ шифросистем, то в любой стране мира ВЫВОЗ шифросистемы является государственным преступлением.

С другой стороны, открытая публикация математических методов преступлением не является, поэтому различным зарубежным фондам не нужны готовые системы, достаточно изучить направление и сам опубликованный материал.

Реально существующие у нескольких российских фирм зарубежные сертификаты являются на самом деле патентами, свидетельствующими их АВТОРСТВО на систему.

Многие страны (в частности, США) выдают такого рода свидетельства вне зависимости от гражданства автора, стоит эта услуга около 2 тысяч долларов, никакого отношения к КОРРЕКТНОСТИ примененного математического аппарата и КАЧЕСТВУ программного обеспечения, равно как и к самому СУЩЕСТВУ защищаемого продукта, свидетельство не имеет (часто даже не требуется

предъявление полных исходных текстов и описания алгоритма), и действительность свидетельства распространяется не далее территории государства, его выдавшего. Таким образом, в России имеет смысл говорить только о свидетельствах РосАПО **(тоже никакого качества не гарантирующих).**

Итак, если физическое или юридическое лицо, вне зависимости от его статуса и ориентации, желает (полностью или частично) защитить свое информационное пространство, оно, согласно “Указу N334 о мерах”, ОБЯЗАНО использовать ГОСТ 28147-89.

Со всеми вытекающими последствиями. А последствия эти выражаются, прежде всего, в УСТАНОВЛЕНИИ СПЕЦИАЛЬНОГО КОНТРОЛЯ СО СТОРОНЫ СЛУЖБ ГОСБЕЗОПАСНОСТИ (ФАПСИ) над деятельностью упомянутого лица и, как следствие, существенном УВЕЛИЧЕНИИ ЧИСЛА АБСОЛЮТНО (с точки зрения все того же лица) ПОСТОРОННИХ СУБЪЕКТОВ, имеющих доступ к защищенной таким образом информации и проявляющих к ней повышенный, в целях государственной безопасности (не всегда), интерес.

Очевидно, государство физически не в состоянии обеспечить всех остро нуждающихся в требуемом уровне описанной информационной защиты, что приводит к типичной для России ситуации РАСХОЖДЕНИЯ установленной де юре, сложившейся де факто и еще раз (пере) установленной де юре практики, чему в немалой степени способствует нечеткость президентского “Указа N 334 о мерах”, в котором, например, не оговорено, что, собственно, понимается под шифрованием и какое отношение имеет сам Указ к некоторым российским законам и некоторым правительственным (же) решениям и резолюциям.

В настоящее время в России повсеместно используются архиваторы (pkzip, arj, lha, rar и др), уплотнители дискового пространства (Stacker, DoubleSpace) – все только ВВЕЗЕННЫЕ в Россию из за рубежа, – которые даже без учета заложенных в них непосредственно шифровальных функций (причем иногда с нигде не декларированными схемами шифрования) являются, в строгом смысле слова, шифрующими системами, поскольку используют нестандартную кодировку данных, серьезно затрудняющую возможность их прочтения (получения в открытом виде) без соответствующего программного обеспечения.

В этом смысле шифросистемами являются также известные редакторы ChiWriter, Word и даже Lexicon, поскольку каждый из них использует свою кодировку. Попытка четкого разделения стандартной и нестандартной кодировки заранее обречена на провал, поскольку невозможно заставить основных разработчиков мирового программного и аппаратного обеспечения использовать принятую тем или иным указом того или иного президента той или иной страны кодировку букв вверенной ему страны. Разумно предположить, что шифросистемами являются такие

программные продукты, в документации к которым явно написано, что это – шифросистема (заметим, однако, что последнее, то есть действительно ли это шифросистема или нет, и что под шифросистемой понимается, не может быть подтверждено никакими официальными документами кроме, с точки зрения “Указа N 334 о мерах”, лицензии ФАПСИ, которая не может быть выдана, потому что это противоречит интересам безопасности государства и, собственно, ФАПСИ).

Де факто, российские пользователи, при необходимости защиты информации ИСПОЛЬЗУЮТ средства шифрования, применяя архиваторы с парольной защитой (меняющей кодировку сжатых данных, а не устанавливающей права доступа), Diskreet /fast proprietary method/ из Norton Utilities, многочисленные shareware-программы (например, PGP – Pretty Good Privacy), системы, продаваемые теми же фирмами ЛАН Крипто, Аладдин и др, собственные разработки, а также вообще неизвестно откуда взявшиеся программы. В частности, криптозащита (и отнюдь не ГОСТ-шифрование) широко используется при обмене электронной почтой, о чем можно прочитать в документации к любой EMAIL-системе, поддержи-ваемой на территории России. Де юре такое поведение российских пользователей подлежит осуждению и даже некоему (согласно “Указа N 334 о мерах” – неизвестно точно, какому) наказанию, однако необходимая для наказания юридическая база отсутствует, и реальной альтернативы для российских физических и юридических лиц не предусмотрено.

6. Обзор и общая характеристика доступных средств шифрования

Вне зависимости от метода шифрования, любой шифр является слабым (то есть вскрываемым за реальное время), если длина пароля недостаточно велика.

Приводимая ниже таблица показывает время, требуемое на подбор пароля на AT-486/66MHz в зависимости от длины пароля и допустимых при его формировании знаков.

Число знаков пароля	4	5	6	7	8	9	10
Только цифры		0.08 с	0.8 с	8.3 с	1.4 мин.	13.9 мин.	2.3 час.
Лат. буквы без регистра	0.38 сек.	9.9 с	4.3 мин	1.9час	48.5 час.	52.5 лет	3.7 лет
Лат.буквы б/р и цифры	1.4 сек.	50.5 с	30мин	18час	27.2 дней	2.7лет	97 лет
Лат. буквы с регистром и цифры	12.4 сек.	13 мин.	13час	34 дня	5.8 лет	357 лет	22 204 лет

Все возможные символы	1 час	10.6 дней	7.4 лет	1908 лет	487 000 лет	120 млн.лет	32 млрд. лет

Pentium/200MHz превосходит AT-486/66MHz по производительности не более чем в 10 раз, использование супер-эвм позволяет сократить время перебора не более чем в 1000 раз, что, учитывая порядок приведенных в таблице чисел, абсолютно не принципиально.

Таким образом, если пароль включает только латинские буквы без различения регистра, то (любой) шифр является слабым при длине пароля менее 10 знаков (и "очень слабым" при длине пароля менее 8 знаков); если пароль включает только латинские буквы с различением регистра и цифры, то шифр является слабым при длине пароля менее 8 знаков ("очень слабым" при длине пароля менее 6 знаков); если же допускается использование всех возможных 256 знаков, то шифр является слабым при длине пароля менее 6 знаков.

Что же касается надежности непосредственно шифрования, то практически ВСЕ используемые в частных коммерческих структурах шифры являются СЛАБЫМИ.

Компания Access Data (87 East 600 South, Orem, Utah 84058, phone 1-800-658-5199) продает за $185 программу взлома шифров WordPerfect, Lotus 1-2-3, MS Excel, Symphony, Quattro Pro, Paradox, MS Word 2.0 и другие.

Существуют коммерческие версии дешифраторов для всех известных архиваторов (pkzip, arj и др.) зарубежные "стандарты" шифрования (с учетом многообразных предлагаемых модификаций), ЭКСПОРТИРУЕМЫЕ некоторыми технологическими развитыми странами (в частности, США-DES, Япония-FEAL) на самом деле являются стандартами соответствующих разведслужб, предлагаемыми и внедряемыми на территориях дружеских государств. Исключения в списке заведомо ненадежных систем шифрования, потенциально доступные для российского пользователя, составляют лишь некоторые (две или три) оригинальные российские разработки, однако, ввиду воздвигнутой государством информационной блокады в этой области, можно лишь строить предположения, какие именно.

Разделение систем шифрозащиты на сильные и слабые (как по длине используемого пароля, так и по надежности самой системы) имеет принципиальное значение, обуславливающее возможность реального применения как слабых, так и сильных шифров в условиях их юридического запрета. Дело в том, что если вы используете заведомо слабую шифрозащиту (например, pkzip с паролем), для которой существует эффективный взлом, то невозможно наверное утверждать, что выбранное вами средство является криптосистемой, скорее речь идет о ШИФРООБРАЗНОМ

ограничении и контроле прав доступа. С другой стороны, ЛЮБАЯ программа шифрования может потенциально рассматриваться как слабый шифр, то есть шифрообразный контроль доступа к данным, поскольку в обусловленных “Указом N 334 о мерах” и проинтерпретированных ФАПСИ условиях наличие официальных данных и характеристик по той или иной шифросистеме исключается в принципе. Наконец, каким бы шифром вы не пользовались, применение коротких паролей безусловно переводит их в разряд слабых, не представляющих опасности для интересов (какого бы то ни было) государства.

7. Защита данных в системах прямой телекоммуникационной связи

(системах типа “клиент-банк”)

В системах прямой телекоммуникационной связи (модем-модем) используется контроль прав доступа – проверка входного имени (иногда его называют входным паролем) – и это безусловно необходимая, безусловно допустимая и, в (данном) случае удаленной связи, то есть при отсутствии непосредственного контакта с физическими носителями информации, действенная защита.

Единственное слабое звено такой защиты – возможность перехвата информации в процессе ее прохождения по телефонному каналу. Для исключения такой возможности следует применять шифрование передаваемых данных, то есть ГОСТ 28147-89. Однако НАИБОЛЕЕ ВЕРОЯТНЫМ (ПО КРАЙНЕЙ МЕРЕ – НАИБОЛЕЕ РЕАЛЬНЫМ) организатором телефонного перехвата являются именно государственные службы безопасности, и некоторые родственные структуры, владеющие всеми ключами ГОСТа. Как правило, это в дальнейшем используется далеко не для государственных целей. Следовательно, целесообразность (сертифицированного ФАПСИ) шифрования в прямой телекоммуникационной связи, скажем так, неочевидна.

Существует уже способ дешифровки СВИФТА, и владение монополией телекоммуникационных связей приведет только к одному следствию.

Помимо телефонного перехвата самих данных возможен перехват входных имен, что особенно опасно для систем типа “клиент-банк”, так как похищенные имена могут использоваться для проведения реальных денежных операций совершенно посторонними лицами. Однако как раз этой опасности можно избежать, если использовать шифрованные, с участием оригинальных для каждого сеанса связи синхропосылок (обратных открытых ключей), входные имена. Организация такой защиты абсолютно законна, поскольку речь идет не о шифровании и даже не об электронной подписи, а о развитии механизма контроля доступа. На сегодняшний день описанный механизм нигде практически не применяется, и его отсутствие

представляет реальную угрозу для любого крупного банка, использующего телекоммуникационный обмен реальными данными.

Шифрование "удаленных входных имен" заложено в CBTELE12, согласно общему проекту, начиная с версии 04.02, и это на сегодняшний день ЕДИНСТВЕННАЯ ПО КРАЙНЕЙ МЕРЕ НА ТЕРРИТОРИИ РОССИИ СИСТЕМА КЛИЕНТ-БАНК, которая будет обладать описанным механизмом защиты.

Практика применения в прямых телекоммуникационных системах электронной подписи не имеет под собой никаких оснований.

Во-первых, прямая связь (модем-модем) не предполагает участия третьих лиц при передаче данных, так что обмен электронными подписями напоминает беседу двух склеротиков, которые через каждую минуту забывают, что они уже поздоровались, и снова скрепляют факт своей встречи рукопожатием и представляются друг другу.

Во-вторых, и как уже отмечалось ранее, сама по себе электронная подпись может быть похищена (в том числе при передаче данных) и использоваться похитителями для придания видимости "правильных" абсолютно "неправильным" документам. Наконец, представление, что поставленная на документе электронная подпись может служить для решения юридических споров и установления какой бы то ни было истины, в корне ошибочно: действие электронной подписи распространяется на психологическую сферу, но никак не на юридическую. Сертификаты ФАПСИ дают право фирмам-разработчикам продавать электронную подпись, но не имеют никакого отношения к правовым аспектам ее использования. Если я заявлю, что никогда не посылал документа, заверенного моей электронной подписью, никакой суд не докажет обратное, и мне даже не потребуется наличие свидетелей или алиби. И это правильно, потому что существует слишком много возможностей подделки или похищения подписи, о чем уже говорилось выше. Кроме того, никто не возьмет на себя ответственность за надежность и безопасность самой программной системы, обеспечивающей электронную подпись. Сертификаты ФАПСИ, как уже упоминалось, являются лишь относительными гарантиями, основное их назначение – регулировка рынка.

В РЕАЛЬНО СЛОЖИВШЕЙСЯ ЮРИДИЧЕСКОЙ ПРАКТИКЕ (см. Решение Высшего Арбитражного Суда РФ N С1-7/ок-587 от 19.08.94) сама по себе электронная подпись, какими бы сертификатами она не подтверждалась, в качестве доказательства подлинности документа не принимается.

Возвращаясь к изложенным выше "сомнениям" относительно надежности той или иной электронной подписи: ЕЩЕ В 1994г.

БЫЛИ ОБНАРУЖЕНЫ ЗАКЛАДКИ, В ЧАСТНОСТИ ПРОТИВ СИСТЕМ, ПОСТРОЕННЫХ НА ОСНОВЕ ПАКЕТА PGP (Pretty Good Privacy), ПРИ ПОМОЩИ КОТОРЫХ БЫЛИ ПОДДЕЛАНЫ ЭЛЕКТРОННЫЕ ДОКУМЕНТЫ [журн."Частный сыск" N 1 за 1995 г., статья

А.Щербакова]

Между тем PGP построен на наиболее распространенном во всем мире (и в том числе в России) методе шифрования RSA, канонизированным в США (для, опять же, НЕПРАВИТЕЛЬСТВЕННЫХ и, желательно, "Outside USA", сфер). Что после этого можно сказать об отечественных "подписях", ОПИРАЮЩИХСЯ НА ТОТ ЖЕ МЕТОД RSA либо наши ГОСТ Р 34.10-94 и ГОСТ Р 34.11-94, которые бесконечно далеки от практики всемирного использования и, соответственно, массированных атак со стороны компьютерных пиратов? Но – в этом плане у нас все еще впереди…

Учитывая состояние современного математического аппарата, технических средств и способов защиты информации, следует отметить:

1. Существуют научные, учебные и прочие центры, кафедры, где разрабатываются математические методы (в том числе и частным путем). Эти методы, как правило, публикуются и становятся достоянием любой страны, пожелавшей воспользоваться разработкой не только для научных целей, но и организации системы безопасности.

Никаким указом эту практику не запретишь.

ФАПСИ не располагает информацией о существующих математических методах решения задач, а также информацией о возможном использовании математических методов для организации шифрозащиты.

2. Существуют такие организации, как РОСАПО, которое выдает патенты и свидетельства на программные продукты, причем задолго до появления "указа". Любой программный продукт на основании свидетельства или патента может быть реализован в любой стране без санкции ФАПСИ. ФАПСИ не может, естественно взять на себя роль патентного ведомства.

3. Ни один математик, серьезно занимающийся проблемами информационной безопасности, никогда не обратится в ФАПСИ – за время работы мы не встретили там НИ ОДНОГО ГРАМОТНОГО СПЕЦИАЛИСТА (в современных информационных потоках нельзя работать с "шорами" на глазах).

4. Ни одна организация не будет действовать согласно "указа" в связи с тем, что там не определены ответственность ФАПСИ (включая и финансовую) за утерю конфиденциальной информации (или передаче ее третьим лицам).

5. Для реализации "указа" необходимо:

– запретить в России разрабатывать какие-либо математические методы;

– запретить разработки программных средств;

– запретить деятельность РОСАПО по выдаче патентов и свидетельств на программную продукцию;

– запретить выезд (математиков – в первую очередь) за границу;

– запретить деятельность иностранных компаний, скупающих как программную продукцию, так и математиков в России;

– запретить реализацию программ сетевого обмена информацией,
и так далее.

В дополнение к вышесказанному следует:

Разработаны программные средства на базе метода “Калейдоскоп”, которые позволяют кодировать любую информацию простейшими средствами.

Шифросистема НЕ ИМЕЕТ ПАРОЛЯ и не может быть в принципе раскрыта.

Математический аппарат опубликован и, конечно, может быть использован для целей кодирования любой информации. В явном виде этот метод предназначен для решения традиционных задач.

Разработанная система защиты “Скала” не вскрываема никакими методами, так как построена на системе вращающихся уравнений с использованием теории “Калейдоскоп”.

Метод “Калейдоскоп” предназначен для решения задач из класса “Системный анализ и исследование операций” в реальном масштабе времени и предназначен для оперативной обработки информации.

К используемой системе кодирования добавлены шнур Фибоначчи и маска золотого сечения.

Приложение 2

3. Свидетельства.

17 февраля 1994 г. авторское свидетельство N 940054 (Российское агентство по правовой охране программ для ЭВМ, баз данных и технологий интегральных микросхем – РосАПО), Программа Система шифрозащиты электронной информации “INDEX-TWIST Cipherling” (“INDEX-TWIST Cipherling”). Страна – Российская Федерация, авторы: Тарарухин И. В., Румянцев А. И., Заявка N 940045.
Зарегистрировано в реестре программ для ЭВМ. Собственник программы – АО “Ритм-Фонд”, Москва.

5 июня 1995 года авторское свидетельство N 950201 (Российское агентство по правовой охране программ для ЭВМ, баз данных и технологий интегральных микросхем – РосАПО), “Резидентская палитра” (RPLI). Страна – Российская Федерация, авторы: Тарарухин И. В., Румянцев А. И., Заявка N 950130.
Зарегистрировано в реестре программ для ЭВМ. Собственник программы – АО “Ритм-Фонд”, Москва.

5 июня 1995 года авторское свидетельство N 950202 (Российское агентство по правовой охране программ для ЭВМ, баз данных и технологий интегральных микросхем – РосАПО), “FORMS DESIGNER” (FDESIGN). Страна – Российская Федерация, авторы: {Хатыбов А.М. и др., Заявка N 950131.
Зарегистрировано в реестре программ для ЭВМ. Собственник программы – АО “Ритм-Фонд”, Москва.

28 февраля 1995 года авторское свидетельство N 950811 (Российское агентство по правовой охране программ для ЭВМ, баз данных и технологий интегральных микросхем – РосАПО), MVC (“Manual Visual File Comparison”). Страна – Российская Федерация, авторы: Тарарухин И.В., Румянцев А,И., Заявка N 940521.
Зарегистрировано в реестре программ для ЭВМ. Собственник программы – АО “Ритм-Фонд”, Москва.

5 июня 1995 года авторское свидетельство N 950200 (Российское агентство по правовой охране программ для ЭВМ, баз данных и технологий интегральных микросхем – РосАПО), “Процессор частотных словарей” (“AUTODICT”). Страна – Российская Федерация, авторы:
Тарарухин И. В., Хатыбов А. М. Заявка N 940129.
Зарегистрировано в реестре программ для ЭВМ. Собственник программы – АО “Ритм-Фонд”, Москва.

Все необходимые Программные продукты были зарегистрированы до выхода Указа о мерах…