А.А. Кузнецов

# ЗАЩИТА ДЕЛОВОЙ ИНФОРМАЦИИ

## СЕКРЕТЫ БЕЗОПАСНОСТИ



*Издательство*
*«ЭКЗАМЕН»*
МОСКВА
2008

УДК 004.45
ББК 32.373-018.2
К89

**Кузнецов, А.А.**

К89 Защита деловой информации (секреты безопасности) / А.А. Кузнецов. — М.: Издательство «Экзамен», 2008. — 255, [1] с.

ISBN 978-5-377-00698-5

В доступной форме рассмотрены угрозы бизнес-секретам вашей фирмы, существующие при использовании компьютера, а также конкретные приемы, предупреждающие утечку важной информации из офиса. Проанализированы достоинства и недостатки программ, могущих помочь вам скрыть секреты от конкурирующих компаний.

Большинство глав книги делятся на две части: раздел «Полезная информация», в котором разъясняются принципы, заложенные в работе программ, и раздел «Необходимые навыки», рассказывающий о самих программах и условиях их эффективного использования.

Для студентов и преподавателей экономических и технических вузов, программистов, руководителей предприятий всех форм собственности.

**УДК 004.45**
**ББК 32.373-018.2**

Подписано в печать с диапозитивов 29.05.2007.
Формат 60x90/16. Гарнитура «Таймс». Бумага офсетная.
Уч.-изд. л. 10,10. Усл. печ. л. 16. Тираж 3000 экз. Заказ № 3811

**ISBN 978-5-377-00698-5**

# Содержание

# Введение

Безгрешных людей не бывает. В каждой семье есть свои «скелеты в шкафу», — маленькие и большие тайны, о которых не принято рассказывать посторонним. Что же тогда говорить о бизнесе? Стоимость покупки товара, цена его продажи, величина отката, размеры взятки за разрешающую подпись, адреса поставщиков, сведения о постоянных покупателях, база данных потенциальных потребителей, телефоны «своих» чиновников в местной администрации, налоговиков, осведомителей в фирмах-конкурентах и многое-многое другое, вплоть до имен сотрудников-секретоносителей, — все это составляет конфиденциальную информацию, предмет умолчания, тайну, секрет фирмы.

## Запомните

*Тайна крупных состояний, возникших неизвестно как, сокрыта в преступлении, но оно забыто, потому что чисто сработано.*

***Оноре де Бальзак***

В «доброе старое время», лет ...надцать назад (это у каждой фирмы по своему) сохранить секретность было сложно: многочисленные бумаги, сопровождавшие активную деятельность, терялись в столах у сотрудников, папки с документами забывались на скамейке в парке или на столике в пивной, документы с грифом «секретно» или «для служебного пользования» попадали в мусорные баки, послужив предварительно

кульком для конфет или оберткой для рыбы. Если пакет с бумагами был большой, он мог превратиться в томик Дюма или Чейза. Но чаще всего потерянные документы отправлялись прямо на помойку. Иногда они попадали в руки «нехороших людей», иногда нет. Любой тщательный обыск конторы давал повод для появления претензий к ее руководству (копии платежек, завалившиеся за стол, черновики договоров, придавленные грудой документов, оригиналы контрактов, случайно подшитые не в свои папки). Это время кончилось с появлением компьютера — «тайнохранилища», позволяющего вести практически безбумажный документооборот. Но появление компьютера, добавив удобства в работе, заменило старые проблемы на новые и многократно увеличило масштабы бедствия при утечке информации. Сотрудник не может потерять папку с договорами, но может посеять дискету, диск или флэшку с информацией о деятельности всей организации. Осведомитель недружественной фирмы не может украсть документ, но может, узнав пароли, обеспечить доступ своему реальному хозяину ко всем перспективным разработкам или коммерческим проектам компании. Наехавшая по заказу конкурента группа контролеров не найдет ваших набросков схемы распределения прибыли от сделки, послужившей причиной наезда. Но имея под рукой грамотного специалиста, она выпотрошит ваши компьютеры и получит информацию обо всех реальных успехах фирмы на ниве бизнеса (и, высоко оценивая ваш талант бизнесмена, предложит полюбовно разделить плоды этих успехов).

Когда ваш бизнес вырастет, вы сможете поручить защиту конфиденциальности информации в компании специалистам. Почему не сразу? Грамотный программист стоит $50, грамотный специалист по защите информации $200–300. Не в месяц, не в день, а в час. Вот и прикиньте свои возможности. Можно, конечно, найти «спеца» и за $300 в месяц (помните, как в старом мультике про царевну-лягушку две царские снохи прика-

зывали: «Эй, дед Кондрат, бывший солдат! Надо два ковра к завтрему вышить!»), но толку от него будет столько же, сколько от деда Кондрата в качестве дизайнера. Поэтому пока вы растете, либо сами должны присматривать за ручейками информации из вашей конторы, либо поручить это дело одному из своих партнеров (любой наемный работник никогда так серьезно не отнесется к вопросам обеспечения безопасности организации, как человек, могущий сам реально пострадать при потере бдительности).

## Запомните

*Когда события принимают крутой оборот, все сваливают.*

***Э. Мэрфи***

С чего начинать? С тщательной уборки помещения. И в прямом, и в переносном смысле. В прямом — с проведения под любым предлогом «субботника» и очистки офиса от любых лишних бумаг.

## Из жизни

*У одного из моих украинских друзей в столе на работе затерялись копии квитанций о покупке запчастей к его Мерседесу по кредитной карточке. Запчасти он покупал в Германии. Мелочь? Вроде бы, да. Но есть один нюанс: гражданам Украины не разрешено было в то время иметь кредитных карточек иностранных банков. А покупки-то он делал по кредитке одного широко известного на постсоветском пространстве прибалтийского банка. Вот во время обыска и погорел. Почему обыск был? Да по вине все того же банка. Он отчеты по карточным расходам клиентов отправлял в свои*

*украинские отделения по электронной почте открытым текстом. Налоговики с полгода почту копировали, потом клиентов сосчитали, оценили и как следует потрясли. Откупились вроде бы все, но сами представьте: обыск дома, обыск в офисе, несколько недель нервотрепки на допросах, затраты на прекращение дела. И из-за чего? Из-за нескольких бумажек, отсутствие которых лишило бы государственных рэкетиров основания для возбуждения дела (копии банковских писем по электронной почте — не документ, не было бы бумажек, сослаться не на что).*

В переносном — с очистки компьютеров фирмы от любых электронных версий старых документов. Проще всего это сделать радикально — скопировать с компьютеров действительно важную информацию, потом отформатировать диски и начать новую жизнь с чистого листа, учитывая существующие опасности информационного века и используя современные методы защиты своих секретов.

## Из жизни

*Во время обыска, произведенного в 1942 г. у немецких агентов, американская контрразведка обнаружила секретные задания, написанные симпатическими чернилами в журналах. Допрос показал, что ненужные журналы немцы продавали букинистам, вместо того чтобы сжигать их. Эта экономия оказалась роковой. Американские контрразведчики ринулись в лавки букинистов, скупили тысячи журналов, подвергли их обработке парами йода и восстановили буквально все задания, дававшиеся немецким шпионам в течение ряда лет. Это позволило американцам впоследствии уничтожить все немецкие шпионско-диверсионные организации.*

Эта книга об угрозах бизнес-секретам со стороны вашего помощника — компьютера. Она научит пользоваться приемами, предупреждающими утечку информации из офиса, познакомит с программами, которые помогут вам скрыть свои секреты от окружающих. Большинство глав книги делятся на: раздел «Полезная информация», в котором разъясняются принципы, заложенные в работе программ (чем больше понимаешь, как обеспечивается защита, тем спокойней спишь); раздел «Необходимые навыки», рассказывающий о самих программах и условиях их эффективного использования.

## Запомните

*Образование — это умение правильно действовать в любых житейских ситуациях.*

***Джон Хиббен***

На какой из описанных программ остановиться? Они все примерно равноценны по своим характеристикам, а их большое количество предназначено обеспечить возможности выбора наиболее удобной лично для вас. В каждом разделе упомянуты также две-три программы, выделяющиеся из общего списка по трем признакам «наиболее»: распространенная; простая в пользовании; многофункциональная.

Отдельно приведены списки бесплатных и платных версий программ. Чем они отличаются? Многие фирмы-разработчики выпускают наряду с платными бесплатные версии своих продуктов, несколько ограничив их функциональные возможности (например, длину пароля используемого ключа, число алгоритмов шифрования) или добавив в программу показ рекламных баннеров (и зарабатывают деньги не на вас, а на рекламодателях). Вероятно, что вас вполне удовлетворит

бесплатный вариант программы (программа дает возможность использовать только один алгоритм шифрования, но для защиты-то данных только один из нескольких и будет в реальности применяться, а если встроенный в программу алгоритм надежен, то не стоит и харчами перебирать, правда?), если же нет, то, опробовав бесплатную версию, вы всегда можете купить аналогичную платную у приглянувшегося производителя.


Вы бизнесмен? Вы заняты? У вас нет времени учиться? Подумайте. Только одно неверное движение руки разобьет ваш любимый джип о некстати появившийся трамвай. Ремонт же займет несколько дней и будет стоить несколько сотен долларов. Только одна некстати забытая в столе бумажка может забрать несколько недель вашей жизни и облегчит ваш карман уже на несколько тысяч все тех же условных единиц. Только одно перехваченное письмо с информацией о вашей предстоящей командировке может привести к ограблению ва-

шего дома или городской квартиры, похищению вас или кого-либо из ваших родственников, забрать вашу жизнь, наконец. Не жалейте времени на создание системы собственной безопасности.

### *Запомните* ~~~~~~~~~~~~~~

*Выживают только параноики.*

***Эндрю Гроув,***
***глава корпорации Intel***

# Техническое предисловие

*В великих делах нужно стараться не столько создавать события, сколько пользоваться теми, которые представляются.*

***Ф. Ларошфуко***

Все разработчики хвалят себя. И это естественно. Каждый оценивает успех по своим меркам, сравнивая полученные результаты со своими же достижениями вчерашними. Но это точка зрения специалистов-разработчиков. Точка же зрения потребителей на функциональные свойства и пригодность программы в реальной жизни может быть совсем иной. Только сравнения, сделанные сторонним наблюдателем, пользователем, потребителем, позволяют подобрать те решения, которые могут быть действительно полезны в бизнесе.

Выбор нужной программы из множества, встречающихся в сети, — занятие интересное, ответственное, но и утомительное. Интернет содержит ряд ссылок на программы, которые читателю самостоятельно просто затруднительно будет испытать (например, хорошо раскручена использующая стеганографию Invisible Secrets, но фирма-производитель предлагает только полюбоваться на интерфейс-программы и оплатить покупку), — эти программы в списки рекомендуемых не включались. Исключены также из числа рекомендуемых и программы, предлагаемые частными лицами, программы, помещенные на сайтах, которые не обновляются уже более года, а также с сайтов, не дающих опробовать программы без введения информации о пользователе, пытающемся скачать их пробную версию. Поэтому приведенные в книге списки рекомендуемых программ существенно меньше по размерам, чем встречающиеся в сетевых каталогах.


## *Анекдот в тему:*

~ ~ ~ ~ ~

*Нанял фермер работника. Трудится тот, не покладая рук, неделю, месяц, другой, хозяин не нарадуется, отличный работник попался! Как-то утром фермер и говорит:*

*— Слушай, Джон. Ты работаешь уже два месяца, а выходных не берешь. Я тебе сегодня поменьше работы дам, а после обеда и вовсе отдохни, съезди в город, развейся.*

*— Ладно, хозяин, а чего сейчас делать?*

*— Да вот картошку в сарае перебери. В дальний угол бросай совсем плохую, поближе — нормальную, а вот в этот ящик клади отличную, на посадку пойдет.*

*К обеду заходит хозяин в сарай. Сидит работник красный, взмокший, а картошка и на четверть не перебрана. Спрашивает хозяин:*

*— Джон, что случилось? У тебя же в руках всегда все спорится?*

*— Хозяин, Я И НЕ ЗНАЛ, ЧТО ТАК ТРУДНО ПРИНИМАТЬ РЕШЕНИЯ!*

# Глава 1

## По секрету всему свету...

*(как выбрать то, что нужно сделать секретом)*

*Умением говорить выделяются люди выделяется из мира животных; умением молчать человек из мира людей.*

***Г. Ландау***

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

**В этой главе:**

- Вы себя недооцениваете.
- Тайны коммерческие и некоммерческие.
- Кто-то теряет, а кто-то находит.
- Береженого Бог бережет.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Если ваш бизнес невелик, вы не представляете интереса ни для кого, кроме налогового инспектора, лишь изредка вспоминающего о вас в периоды «сбора урожая». Вы так думаете? Так вот, вы глубоко заблуждаетесь. То, что вы работаете «на себя», говорит о вашей инициативности. То, что вы не прогорели в течение нескольких лет, говорит о вашем трудолюбии и удачливости. Если при этом ваш бизнес растет, значит, у него есть перспектива и за вами надо понаблюдать. А если не растет? Значит, вы скрываете свои доходы... А раз скрываете доходы, значит, есть что скрывать. Есть что скрывать? Давайте-ка познакомимся поближе...


***ИЛЛЮСТРАЦИЯ***
***http://www.kv.by/index1999162201.htm***

*«Стоит упомянуть о вхождении в доверие к родственникам, друзьям, любовникам, детям, соседям или бывшему окружению, товарищам по учебному заведению, партнерам по бизнесу для выведывания информации. Может произойти навязывание псевдолюбовной интриги, дружеских отношений, религиозного единства, засылка проповедников и подготовленных «болтунов» для выведывания информации, отвлечения внимания философствованием, гороскопами, мистикой, разглагольствованием на житейские, морально-этические темы для создания шумовой завесы. На вас могут обрушить массу различных психологических «манипуляций», транзакционный анализ, «теорию игр», сценарный анализ по Берну, нейролингви-*

*стическое программирование и многие другие изощренные психотехники. Могут пригласить профессионального психолога для анализа ваших текстов или разговора. К агрессивным методам социальной инженерии можно, воздействие на патриотические, национальные, религиозные чувства, провоцирование ссор среди друзей и семьи, коллег и деловых партнеров для дестабилизации, отвлечения внимания, «выведения из игры». Другими словами, не стоит поддаваться на провокации...»*

Для сбора информации возможно использование справочников домашних телефонов, справочников предприятий для установления адреса, телефона, фамилии, названия предприятия, на котором вы работаете, для установления соседей, сослуживцев, для работы с вашим ближайшим окружением или последующей «социальной инженерии». Информацию о вас можно извлечь также из баз данных о предприятиях и их учредителях, о налогоплательщиках (для выяснения сведений о ваших доходах и деловых партнерах).

Впечатляет, правда? А теперь посмотрим, какие стороны вашей работы и жизни стоит сохранять в тайне от окружающих.

## Запомните ~~~~~~~~~~~~~

*Жизнь вынуждает нас многие вещи*
*делать добровольно.*

***NN***

Итак, тайны коммерческие:

**1. Производство**

- ✓ сведения о структуре и масштабах производства, производственных мощностях, типе и размещении оборудования, запасах сырья, материалов, комплектующих и готовой продукции;
- ✓ аналитические справки, отчеты о деятельности предприятия, материалы проверок.

**2. Управление**

- ✓ сведения о применяемых оригинальных методах управления организацией;
- ✓ сведения о подготовке, принятии и исполнении отдельных решений руководства организации по коммерческим, организационным, научно-техническим и иным вопросам;
- ✓ информация о персональных данных сотрудников предприятия.

**3. Планы**

- ✓ сведения о планах расширения или свертывания производства различных видов продукции и их технико-экономических обоснованиях;
- ✓ сведения о планах инвестиций, закупок и продаж;
- ✓ индивидуальные планы сотрудников, графики их работы и личный информационный фонд, персональные базы руководителей предприятия и структурных подразделений.

**4. Совещания, переговоры, контракты**

- ✓ сведения о фактах проведения, целях, предмете и результатах совещаний и заседаний органов управления организации;
- ✓ сведения о подготовке и результатах проведения переговоров с деловыми партнерами;
- ✓ сведения, условия конфиденциальности которых обусловлены в договорах, контрактах, соглашениях и других обязательствах.
- ✓ сведения об условиях конфиденциальности, из которых можно установить порядок соглашения и другие обязательства организации (перед клиентами и контрагентами).

**5. Финансы**

- ✓ сведения о кругообороте средств организации;
- ✓ сведения о финансовых операциях организации;
- ✓ сведения о состоянии банковских счетов организации и проводимых операциях;
- ✓ сведения об уровне доходов организации;

- ✓ сведения о состоянии кредита организации (пассивы и активы);
- ✓ сведения о балансах предприятия;
- ✓ сведения, содержащиеся в бухгалтерских книгах предприятия.

**6. Рынок**

- ✓ сведения о применяемых организацией оригинальных методах изучения рынка (маркетинга);
- ✓ сведения о результатах изучения рынка, содержащие оценки состояния и перспектив развития рыночной конъектуры;
- ✓ сведения о рыночной стратегии организации;
- ✓ сведения о применяемых организацией оригинальных методах осуществления продаж; об эффективности служебной или коммерческой деятельности организации.

**7. Партнеры и конкуренты**

- ✓ обобщенные сведения о внутренних и зарубежных заказчиках, подрядчиках, поставщиках, потребителях, покупателях, компаньонах, спонсорах, посредниках, клиентах и других партнерах, состоящих в деловых отношениях с организацией;
- ✓ сведения о конкурентах, которые не содержатся в открытых источниках (справочниках, каталогах, прессе);
- ✓ обобщенные сведения о внутренних и зарубежных предприятиях как потенциальных конкурентах в деятельности организации, оценка качества деловых отношений с конкурирующими предприятиями в различных сферах деловой активности.

**8. Цены, торги, аукционы**

- ✓ сведения о методах расчета, структуре, уровне реальных цен на продукцию и размеры скидок;
- ✓ сведения о подготовке к участию в торгах и аукционах, результатах приобретения или продажи на них товаров.

**9. Наука и техника**

- ✓ сведения о целях, задачах, программах перспективных научных исследований; ключевые идеи научных разработок;

- ✓ точные значения конструкционных характеристик, создаваемых изделий и оптимальных параметров разрабатываемых технологических процессов (размеры, объемы, конфигурация, процентное содержание компонентов и т.д.);
- ✓ аналитические и графические зависимости, отражающие найденные закономерности и взаимосвязи;
- ✓ данные об условиях экспериментов и оборудовании, на которых они производились;
- ✓ сведения о материалах, из которых изготовлены отдельные детали;
- ✓ сведения об особенностях конструкторско-технологического, художественно-технического решения изделий, дающих положительный экономический эффект;
- ✓ сведения о методах защиты от подделки товарных и фирменных знаков;
- ✓ сведения о применяемом программном обеспечении и используемых компьютерах.

**10. Технология**

- ✓ сведения об особенностях используемых и разрабатываемых технологий и специфике их применения;
- ✓ сведения об условиях производства и транспортировке продукции.

**11. Безопасность**

- ✓ сведения о порядке и состоянии организации защиты служебной или коммерческой тайны;
- ✓ сведения о порядке и состоянии организации охраны, системы сигнализации, пропускном режиме;
- ✓ сведения, составляющие служебную или коммерческую тайну организаций, предприятий партнеров и передаваемые ими в пользование на доверительной основе;
- ✓ сведения, раскрывающие отдельные аспекты системы защиты конфиденциальных сведений, содержание переписки и переговоров по вопросам их защиты;

- ✓ сведения о разработке и проведении мероприятий по обеспечению безопасности предприятия, в том числе об организации взаимодействия с правоохранительными органами;
- ✓ планы действий в чрезвычайных ситуациях.

**И личные секреты:**

- ✓ имущественное положение;
- ✓ состав семьи и место ее жительства;
- ✓ распределение имущественных прав в семье;
- ✓ отношения в семье или отношения с другими людьми;
- ✓ документально зафиксированный порядок перераспределения имущественных прав в случае гибели членов семьи;
- ✓ сведения о фактах биографии;
- ✓ состояние здоровья и скрытые физические недостатки;
- ✓ связи, пристрастия, увлечения, привычки и пороки;
- ✓ убеждения, оценки и взгляды;
- ✓ имеющиеся права наследования;
- ✓ имеющиеся права на интеллектуальную собственность;
- ✓ имеющиеся права на претензии к другим владельцам собственности.

## *Из жизни* ~~~~~~~~~~~~~~~~~~~~

*Мой друг, входящий в ТОП-менеджмент одного банка, уехал в регионы на проверку филиала. Естественно, по окончании — баня, стол, девочки. Делали фотографии, но ничего неприличного, а сам факт девиц на фотографиях был бы для него фатальным в отношениях с женой. Он просит директора филиала не делать ему фотографий, где есть хоть одна девица. Возвращается домой. На следующий день, вернувшись с работы, застает жену в полном гневе. Кидает конверт с фотографиями. Он выхватывает фотографии, судорожно перебирает — ни одной девицы, ВООБЩЕ! А ты конверт переверни! Он переворачивает конверт, и там от руки размашисто написано: «Сюда фото с девочками НЕ КЛАСТЬ!!!»*

Можно приводить сотни примеров появления угроз бизнесу и жизни его владельца при утечке конфиденциальной информации или ее легкодоступности. У любого человека, связанного с бизнесом, есть несколько приятелей, потерявших казавшиеся такими надежными источники дохода, каждый вспомнит леденящие душу истории про похищенных детей, многие слышали или читали про лесные кладбища «черных риэлторов».

В России ежегодно исчезают около 100 000 (ста тысяч!) человек. Не умирают, не уезжают, а исчезают. Да, некоторые бегут от долгов, родственников или меняют образ жизни, обрывая старые связи.

Но таких немного, а вот куда деваются остальные?!

## Запомните

*Трое способны хранить тайну, только если двое из них мертвы.*

***Бенджамин Франклин***

## Резюме

Просмотрите еще раз перечень того, что обычно считается коммерческой и личной тайной. Наверняка многим из перечисленных в списках пунктам вы не придавали значения. А напрасно! Информация о вас и ваших близких, вашем поведении и привычках, ваших делах и потенциальных возможностях накапливается в различных базах данных и в любой момент может стать средством манипуляции вашим поведением, вашим бизнесом, вашей жизнью.

## Не забывайте

*Последнее слово остается за теми, кто помалкивает.*

# Глава 2

## Лабиринт отражений
### (как закамуфлировать свою компанию)

*Прирождённый руководитель узнаётся по неразборчивой подписи.*

***Лео Фаррелл***

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

**В этой главе:**

- Как вас ищут.
- Что хотят о вас узнать.
- Зачем нужны ложные цели.
- Как создавать отражения реальности.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Информацию о ваших делах можно добыть, получив доступ к базам данных и войдя в контакт с вами, вашим окружением (родственниками, сотрудниками, партнерами, знакомыми) или вашей фирмой. Изменить что-либо в чужих базах данных вы уже не в силах.

***ИЛЛЮСТРАЦИИ:***

***http://www.newsru.com/finance/25nov2004/basejump.html***

*Российские пираты украли и растиражировали базу налоговой инспекции по подоходному налогу. В открытый доступ попали 36 млн. деклараций жителей Москвы и Подмосковья. За 2000 руб. любой желающий может узнать не только паспортные данные, но и доходы чиновников, бизнесменов и рядовых граждан. Там содержатся паспортные данные, домашний адрес получателя дохода, юридический адрес и телефон компа-*

*нии, в которой он работает. С помощью базы можно определить место работы любого лица Московского региона, проследить его финансовую историю, получить полный список сотрудников предприятия и акционеров с указанием полученных дивидендов. Там есть также данные о купле-продаже и строительстве недвижимости.*

***http://www.mclub.ru/pagenews-822.html***

*В продаже появились базы данных с личной информацией петербургских абонентов крупнейших сотовых компаний СПб, а также ведущих телефонных компаний города — «Северо-Западного телекома» и «Петерстара». Личную информацию миллионов людей продают за 1650 руб. В частности, к продаже предлагаются базы данных северо-западного филиала АО «Мегафон» (содержит данные почти о 1,3 млн. местных абонентов компании), петербургской сети «Мобильных телесистем» (около 500 000 клиентов), «Дельта телеком» (120 000 пользователей), Fora communications (15 000 клиентов). На другом компакт-диске разместились базы данных с личной информацией «Севзаптелекома» (около 1,9 млн. абонентов) и «Петерстара» (100 000 пользователей).*

***http://www.directmarketing.com.ua/news/243***

*Теперь в Москве можно беспрепятственно купить не только базы данных Московской городской телефонной сети или ГИБДД, но и список всех клиентов «Мобильных Телесистем». Сейчас практически открыто частную информацию о 5,5 миллиона абонентов МТС можно купить всего за 150 долл. Украденная база данных содержит информацию компании о личности клиента, его фамилию, адрес, номера контактных телефонов. Чтобы было проще найти в базе человека, его телефонный номер или проследить динамику платежей, разработчики создали системы поиска. Появлялись сообщения, что утечка базы данных могла произойти при содействии спецслужб. По закону подобные данные являются закрытыми.*

*Единственные, кому оператор мобильной связи должен их передать на условиях абсолютной конфиденциальности, — спецслужбы.*

Единственная возможность противодействия таким «случайным утечкам информации» чиновников или сотрудников телефонных компаний — добиться, чтобы ваши данные, внесенные в их базы данных, перестали соответствовать действительности, а впредь попадающие туда сведения о вас были ложными с самого начала.

## Запомните

*Самое верное средство остаться бедным — быть честным человеком.*

***Наполеон I***

Взвалившие на себя бремя ответственности за сохранность вашей конфиденциальной информации службы своей обязанности не выполняют. Поэтому с какой стати вы должны предоставлять им о себе верные данные? От этих сведений зависит ваше благополучие (возможно, жизнь), они же — в случае их потери — даже извиниться не соизволят?

### *ПОЛЕЗНАЯ ИНФОРМАЦИЯ*

Как изменить данные о себе в базах данных? Это зависит от вашей финансовой состоятельности и личной предприимчивости. Простая смена места жительства сделает информацию о вас устаревшей. Если же впредь ваше реальное место обитания не будет соответствовать официальному месту прописки, регистрация новых компаний будет осуществляться на подставных лиц, открытие счетов в банках на паспорта из стран, в которых вы оформили второе гражданство, а мобильные телефоны вы будете регистрировать по документам, содержащим искаженные сведения, вы сможете спать спокойнее.

***ИЛЛЮСТРАЦИЯ***

***Ли Яккока. Карьера менеджера (из рассказа о Генри Форде II).***

*Например, он терпеть не мог что-либо записывать на бумаге. Хотя мы с ним вдвоем руководили компанией на протяжении почти восьми лет, в моих архивах тех дней едва ли найдется документ, на котором стоит его подпись. Генри имел обыкновение хвастать, что никогда не хранил папок с материалами. Время от времени он сжигал все бумаги. «Все это может только навредить, — говаривал он мне. — Всякий, кто держится за свои бумаги, напрашивается на неприятности. Рано или поздно чужой человек прочтет их, и вам или компании придется за это расплачиваться».*

Если при этом и налоговая отчетность будет демонстрировать вашу вопиющую к состраданию бедность, вам можно будет только позавидовать. При заполнении декларации о доходах лучше всего учиться скромности у сильных мира сего.

***ИЛЛЮСТРАЦИИ***

***Ли Яккока. Карьера Менеджера. (из рассказа о Генри Форде II).***

*Однажды он спросил меня: «Вы платите какой-нибудь подоходный налог?»*

*«Вы шутите? — ответил я. — Конечно!» Нравилось мне это или нет, но я платил 50 процентов со всех своих доходов.*

*«А я обеспокоен, — сказал он. — В этом году я вношу налог в сумме 11 тысяч долларов. Впервые за шесть последних лет мне вообще приходится платить налог».*

*Это было непостижимо. «Генри, — сказал я, — как вам это удается?»*

*«Мои юристы все это улаживают», — ответил он.*

***http://www.day.az/news/ukraine/29069.html***

*Из декларации, поданной премьер-министром Украины, следует, что она живет весьма скромно. Тимошенко владеет квартирой площадью 32 квадратных метра, на ее счету в банке 900 гривен — это 178 долларов. У премьер-министра Украины маленький гараж, 18 квадратных метров, но машины у нее*

*нет. За прошлый год Тимошенко заработала порядка 12 тысяч долларов. Ее муж, Александр, вообще ничего не заработал. Недвижимостью он не владеет, но в иностранных банках у него 16 тысяч гривен и еще 900 в украинских.*

Вспомним о втором пути получения информации о вас — контактах с вами и вашим окружением. Какую информацию в процессе переговоров могут попытаться получить малознакомые люди, сидящие по другую сторону стола или совсем незнакомые лица на противоположном конце сети? Это:

- ✓ полное наименование предприятия, его место в структуре отрасли, почтовые реквизиты;
- ✓ данные о руководящем составе: фамилии, имена, отчества, номера служебных телефонов;
- ✓ профильные виды продукции, товаров и услуг, их характеристики, сведения об основных направлениях деятельности;
- ✓ стоимость основных и оборотных фондов;
- ✓ финансовое положение (размер уставного фонда, имена учредителей и их доли в уставном фонде);
- ✓ планируемые к освоению продукция, товары и услуги:
- ✓ их физические и стоимостные объемы;
- ✓ численность персонала и фонд заработной платы;
- ✓ потребности в сырье, материалах, комплектующих узлах и деталях, источники удовлетворения этих потребностей;
- ✓ транспортные и энергетические потребности.

На большинство из перечисленных вопросов зарубежные фирмы обычно ответов не дают, так как указанные сведения у них составляют коммерческую тайну. Предприниматели, желая продемонстрировать свою «крутизну», с легкостью расстаются со своими секретами:

- ✓ большинство сотрудников предприятия не понимают, что информация — одна из основных ценностей и нуждается в защите наряду с другими ресурсами;
- ✓ сотрудниками не учитывается, что «закрытость» тех или иных сведений выступает как важнейший элемент маркетинга и способ максимизации прибыли предприятия;

- ✓ всегда существует традиционное стремление к «обмену опытом» (а попросту — хвастовству) на встречах, семинарах и т.д.;
- ✓ на предприятии зачастую отсутствует иерархия доступа к сведениям конфиденциального характера;
- ✓ отсутствуют анализ и рекомендации по динамике перехода тех или иных сведений о работе предприятия из категории открытых в закрытые и обратно.

Стандартные рекомендации по предотвращению утечки информации при ведении переговоров:

- ✓ любой участник переговоров (с вашей стороны) должен четко представлять, какую информацию он имеет право передавать. Необходимо учить сотрудников работать по принципу «черного ящика»: есть входные параметры производимого фирмой изделия и полученные результаты, которые могут быть продемонстрированы. Как они получены — секрет фирмы;
- ✓ при попытках сторонних организаций установить с предприятием контакт следует выяснить, в чем состоят их намерения, если это не вытекает из самого обращения к предприятию. Необходимо, используя имеющиеся возможности, навести справки об организации, которая обратилась с запросом. Полезно также отправить в эту организацию встречный запрос и проанализировать реакцию на него;
- ✓ если обратившаяся организация заслуживает доверия, ее намерения отвечают интересам вашего предприятия и предполагается развивать намечающееся сотрудничество, необходимо выработать политику ведения переговоров. Не следует сразу передавать все запрашиваемые сведения в полном объеме. Необходимо убедиться, что запрашиваемые сведения соответствуют намерениям вашего потенциального партнера и действительно необходимы ему для дальнейшего сотрудничества с вашим предприятием. Особое внимание следует обратить, чтобы сведения, которые предприятие решило представить сторонней организации, не раскрывали коммерческих секретов предприятия;

- ✓ на стадии переговоров, когда суть взаимных намерений уже ясна, но юридически они еще не оформлены, было бы оптимальным ведение переговоров таким образом, чтобы ответы на вопросы потенциального партнера носили индикативный характер типа «да — нет», «можем — не можем» и т.д.;
- ✓ после юридического оформления взаимных намерений можно оперировать более широкими данными об основных фондах, потребностях и другими сведениями, необходимыми для развития сотрудничества.

### *НЕОБХОДИМЫЕ НАВЫКИ*

Представьте себя в ситуациях:

- ✓ Вам необходимо быстро подписать контракт с далеким партнером. Для начала работы его вполне устраивает электронная версия контракта с вашей подписью и печатью. Как ее создать?
- ✓ Вам предложили провести переговоры с компанией, достоверной информации о которой у вас нет. Вы не хотите сразу «светить» свою фирму. Как быть?
- ✓ Вам нужно срочно восстановить утерянные документы (хотя бы в копиях). Как это сделать?
- ✓ Вы хотите продемонстрировать своему банкиру (партнерам, сотрудникам), что ведете переговоры с крупной компанией и ваши дела вот-вот пойдут на лад; вам нужно дезинформировать конкурентов, подбросив их осведомителю парутройку документов, удостоверяющих серьезные связи вашей фирмы с крупными зарубежными компаниями. Как обзавестись набором необходимых бумаг?

### *Запомните*

*Ничто так не способствует успеху,*
*как видимость успеха.*

***Кристофер Лаш,***
***американский историк***

Начинать стоит с печатей. Существуют программы, позволяющие в течение нескольких минут сформировать красивые печати любого содержания в электронном виде (табл. 2.1).

*Таблица 2.1*

| Название программы | Где можно скачать |
|---|---|
| Stamp v0.85 | http://soft.li.ru/index.php?search=Stamp+v0.85+ |
| Pechat | http://lpm-soft.nm.ru/download/pechat.exe |
| Seal Win v1.0 | http://lpm-soft.nm.ru/download/Seal.exe |
| Штамп v1.0.R | http://softsearch.ru/pcgi/dl.cgi?t=2&id=148930 |
| MasterStamp 1.1 | http://www.alonewolfsoft.narod.ru/SOFT/mstamp.rar |

Рассмотрим процесс создания печати на примере программы Stamp v0.85, предназначенной для изготовления печатей и штампов любой формы. В программе предусмотрена возможность формирования печатей и штампов всех видов и стандартов Российской Федерации. При помощи Stamp можно быстро создать печать любой сложности, причём без всяких усилий. Программа проста в использовании; её может применять любой пользователь компьютера. Созданную в программе печать можно распечатать на любом документе при помощи принтера и наглядно убедиться в отличном качестве исполнения (для большей достоверности программа создана с функциями, позволяющими размазывать печать) или сохранить на диске как рисунок в формате BMP для последующего использования. Программа Stamp совместима с любым оборудованием для создания печатей и может быть применена для создания прототипов их материальных образцов.

Откроем окно программы, введем название компании, печать которой мы создаем и ее юридический адрес (рис. 2.1).

Программа позволяет регулировать параметры шрифтов (рис. 2.2) и относительное положение строк надписей в печати (рис. 2.3), выбирать размеры (рис. 2.4) и внешний вид рисунка в центральной части (рис. 2.5) как из базы образцов, уже имеющейся в программе, так и из других иллюстраций, понравившихся пользователю.

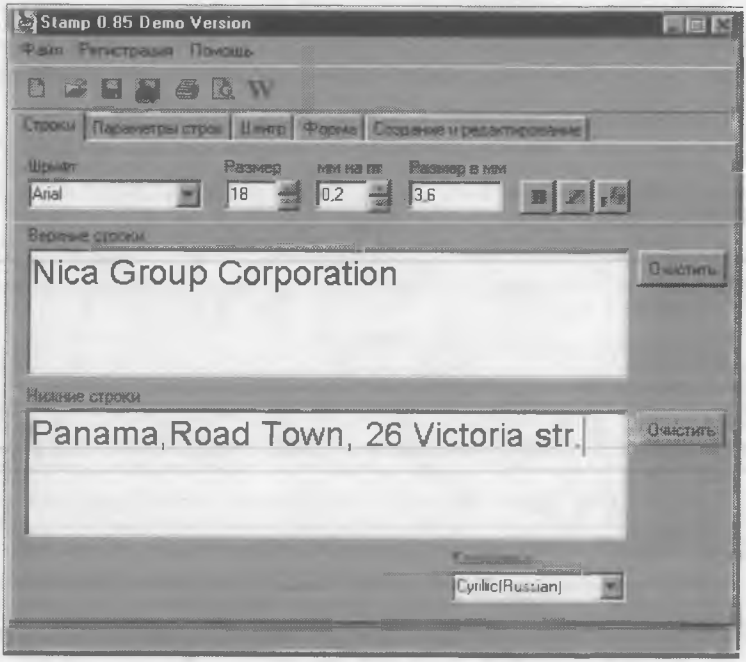



***Рис. 2.1.*** *Интерфейс программы Stamp*

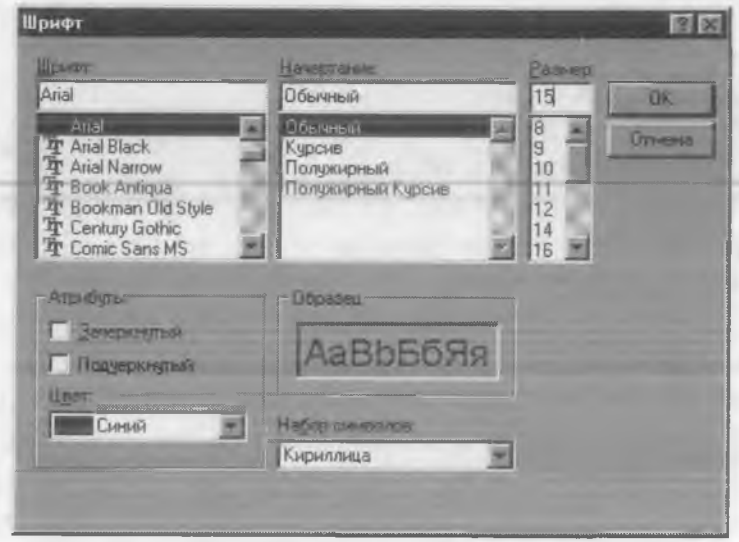



***Рис. 2.2.*** *Редактирование шрифтов печати*

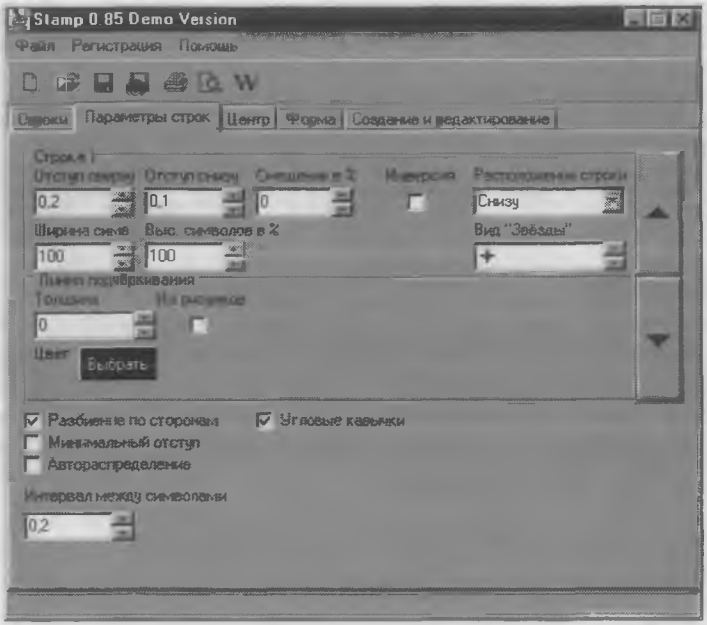



***Рис. 2.3.*** *Редактирование положения строк печати*


***Рис. 2.4.*** *Редактирование центральной части печати*


***Рис. 2.5.*** *Размещение рисунка в центральной части печати*

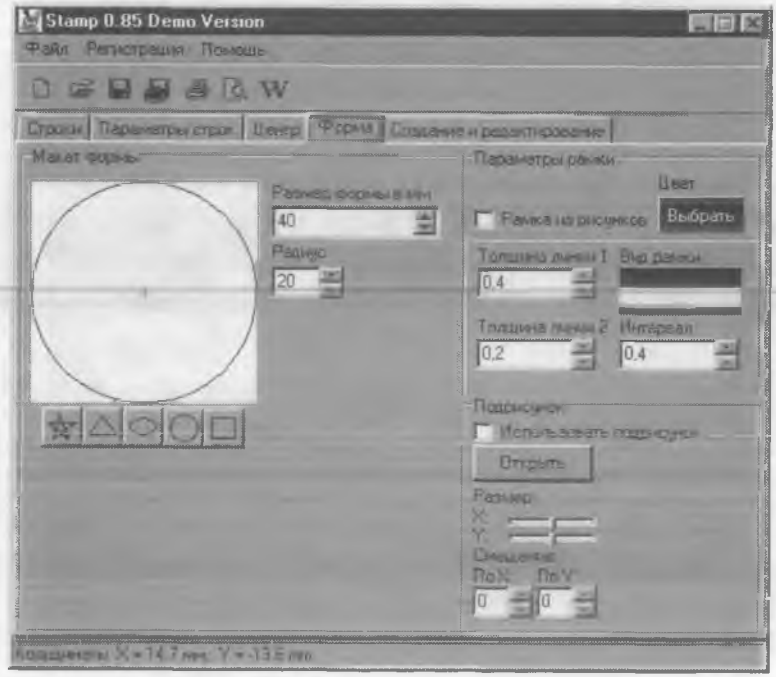



***Рис. 2.6.*** *Размещение рисунка в центральной части печати*

После размещения рисунка остается выбрать форму печати (рис. 2.6), и печать готова (рис. 2.7).

## Запомните

*Закон силён, сильней нужда.*

***И.В. Гёте***

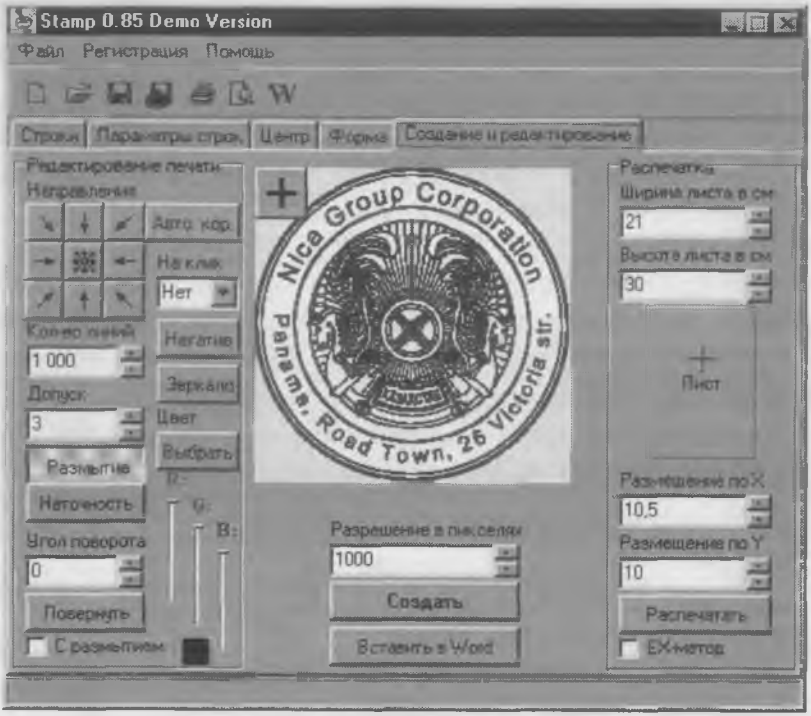



***Рис. 2.7.*** *Окончательный вид сформированной печати*

Сохранив ее как отдельный файл, вы можете ставить ее на любой нужный вам документ (рис. 2.8).


***Рис. 2.8.*** *Размещение сформированной печати в документе*

*Анекдот*
*в тему:*
~ ~ ~ ~ ~ ~ ~

*Инспектор ГАИ останавливает нового русского, едущего на «Мерседесе».*

*— Предъявите ваши права.*

*— Пожалуйста.*

*— Дорогой мой, у вас с головой все в порядке? Это же права на пилотирование самолета?*

*— Чего придираешься, начальник? Какие были, такие и купил.*

Сформировать и сохранить сразу с десяток образцов изготовленной печати с разной степенью размытости (когда понадобится проштамповать большое количество документов, слегка отличающиеся печати на них будут выглядеть как натуральные, проставленные рукой человека).

Итак, солидная печать иностранной фирмы-«партнера» у вас есть. Продолжим работать над ее имиджем.

*Анекдот*
*в тему:*
~ ~ ~ ~ ~ ~ ~

*Новый украинец своей новой секретарше поручает составить список необходимого для обустройства нового офиса по «евростилю». Получил список, читает:*

*1. Факс.*

*2. Ксерокс.*

*3. Принтер.*

*4. Компьютер.*

*5. Коврик для мышки.*

*Оборачивается к секретарше:*

*— Я понимаю, что стиль — это важно, но зачем так мелочиться? Вы бы ещё тапочки для таракана вписали!*

Теперь стоит обзавестись бланками придуманной компании. Для этого нужно создать ее логотип. Рассмотрим процесс его формирования.

## Запомните

*Всё легально, если сотня бизнесменов решит это делать.*

***Э. Юнг***

В повседневной жизни мы постоянно сталкиваемся с тысячами логотипов. Некоторые быстро забываются, другие откладываются в нашей памяти благодаря удачной композиции или имеющимся в них ляпам. По типу исполнения можно четко выделить три группы логотипов:

1. Только текст.
2. Только знак.
3. Комбинированное исполнение (знак + текст).

Остановимся на каждой группе подробнее.

***Только текст***

Логотип изготавливается путем написания названия фирмы выбранной шрифтовой гарнитурой. В зависимости от типа использованной гарнитуры данную группы можно разделить на две подгруппы: классическое и декоративное исполнение. К классическим шрифтам отнесем шрифты с засечками типа Times или Veranda:

Times New Roman **Verdana**,

а также аналогичные, отличающиеся шириной, толщиной и пропорциями букв или исполнением отдельных групп алфавита. Декоративными гарнитурами будем считать все остальные. Вот несколько примеров:

**Comic Sans MS** Matura MT Script Capitals

Это самый простой и быстрый способ изготовить логотип.

***Только знак***

Чтобы клиенты с первого взгляда на знак узнавали организацию, необходимо само название фирмы превратить в знак. Это реально, только если название организации короткое (как правило, 3–4 буквы и менее). Так слово **Sun** легче превратить в знак, чем название типа **Роспромпоставка**. Чем больше букв в слове, тем сложнее сплести их друг с дружкой и тем труднее получившийся знак читается (следовательно, запоминается), не говоря уж о размерах и количестве деталей. Вот примеры логотипов типа «только знак»:



***Текст + знак***

Этот тип логотипов объединяет в себе два предыдущих и наиболее распространен, так как использование изобразительного элемента в логотипе делает его более запоминаемым (чего не скажешь о текстовых логотипах) и позволяет сделать длинное имя вашей компании визуально более привлекательным. Как правило, знак либо располагается сверху, либо предшествует сопровождаемому слову



Безусловные лидеры при создании логотипов: векторные пакеты CorelDRAW, FreeHand, Xara, Adobe Illustrator. Вы можете изучить и использовать любой из них, но, так как вы все-таки не дизайнер, а бизнесмен, для создания простенького логотипа виртуальной фирмы вполне достаточно разобраться с обычным Adobe Photoshop, стоящим практически на каждом компьютере.

Создадим логотип для компании Nica Group Corporation, печать которой мы уже имеем. Запустив Photoshop, крупно напишем три первые буквы названия компании (рис. 2.9) и подчеркнем их сначала тонкой, затем более толстой линиями (рис. 2.10).

Наберем на этом же холсте полное название компании более мелким шрифтом (рис. 2.11), добавим пару линий сверху, выделим разными цветами отдельные участки логотипа и, подвигав по холсту надписи, разместим их так, как нам больше понравится (рис. 2.12).

Вы получили вполне приемлемый логотип, который можете использовать при создании бланков (рис. 2.13) или визиток (рис. 2.14).

## Запомните

*Человек может возвыситься лишь двумя путями — с помощью собственной ловкости или благодаря чужой глупости.*

***Ж. Лабрюйер***


***Рис. 2.9.*** *Интерфейс программы Adobe Photoshop*

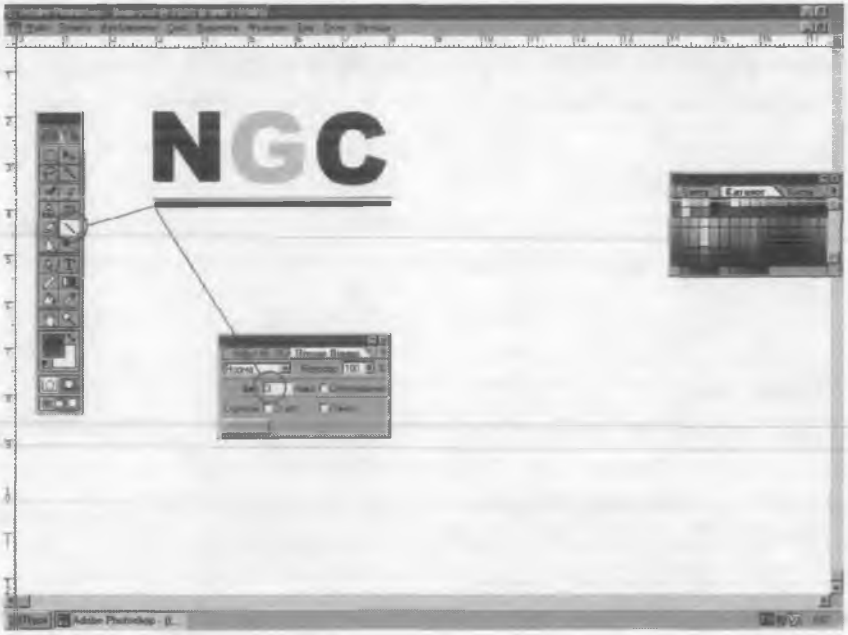



***Рис. 2.10.*** *Подчеркивание логотипа компании*


***Рис. 2.11.*** *Внесение в логотип полного названия компании*

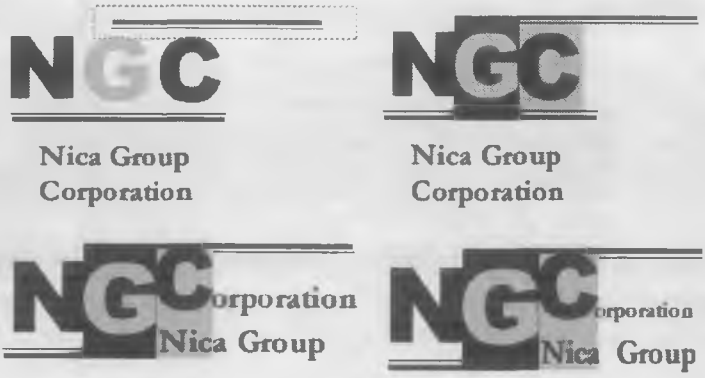



***Рис. 2.12.*** *Перемещение отдельных участков логотипа*


***Рис. 2.13.*** *Шапка бланка, изготовленного на базе разработанного логотипа*


**David Niles**

PROJECT DIRECTOR

E-mail: david@swissinfo.org

***Рис. 2.14.*** *Визитная карточка изготовленного на базе разработанного логотипа*

Adobe Photoshop — программа, удобная для работы с документами; позволяет, отсканировав документ (рис. 2.15), вырезать и увеличить печать с подписью (рис. 2.16), разделить их, улучшить качество печати и подписи отдельно (рис. 2.17) и использовать их в дальнейшем по своему усмотрению.

Если вы повторили на своем компьютере описанные выше операции, в вашем распоряжении оказались бланк и печать фирмы (подлинной или виртуальной) и вы можете написать в свой адрес послание с предложением о сотрудничестве, подписать с ней протокол о намерении заключить контракт, составить договор о совместной деятельности и т.д.

Для составления документов необходимо освоить еще одну программу — Microsoft Word — самый известный текстовой редактор. На практике Word — это наиболее часто использующаяся программа из комплекта Microsoft Office.

## Запомните

*Продукт, де-факто ставший стандартом, доминирует на рынке, даже если он не самый лучший с технологической точки зрения.*

***Кверти Дэвид***

Все должны уметь работать с Word. Когда новый сотрудник приходит устраиваться на работу, его спрашивают, умеет ли он работать на компьютере. В основном имеется в виду именно работа с Word. И уже во вторую очередь — работа с Excel, Интернетом, электронной почтой и т.д.

Microsoft Word — программный комплекс, объединяющий в себе простоту текстового редактора и мощь издательской системы с возможностью ведения большого количества различной документации.

С помощью Word можно:

- ✓ создавать, обрабатывать и распечатывать документы различной степени сложности;
- ✓ редактировать документы, используя буфер обмена;
- ✓ представлять документ в различных форматах: обычный, разметка, структура, веб-документ;

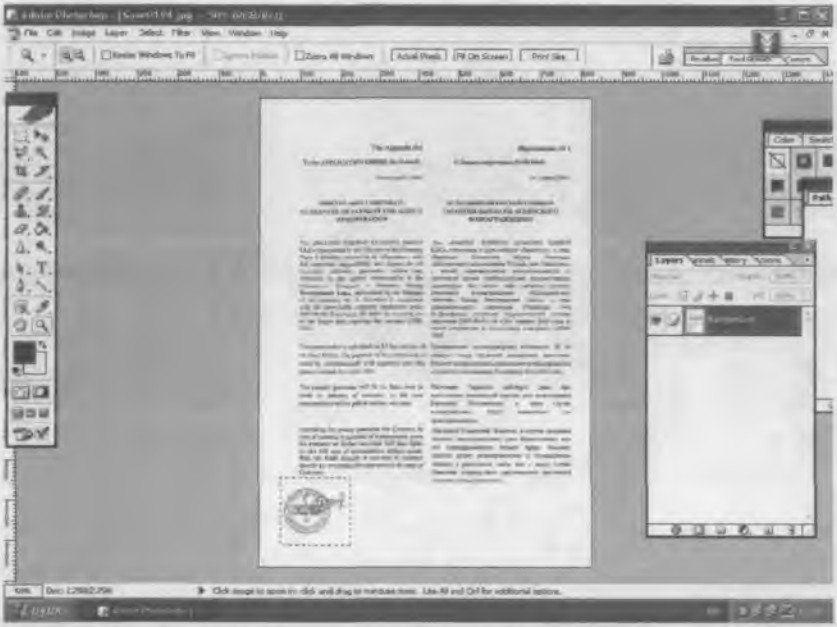
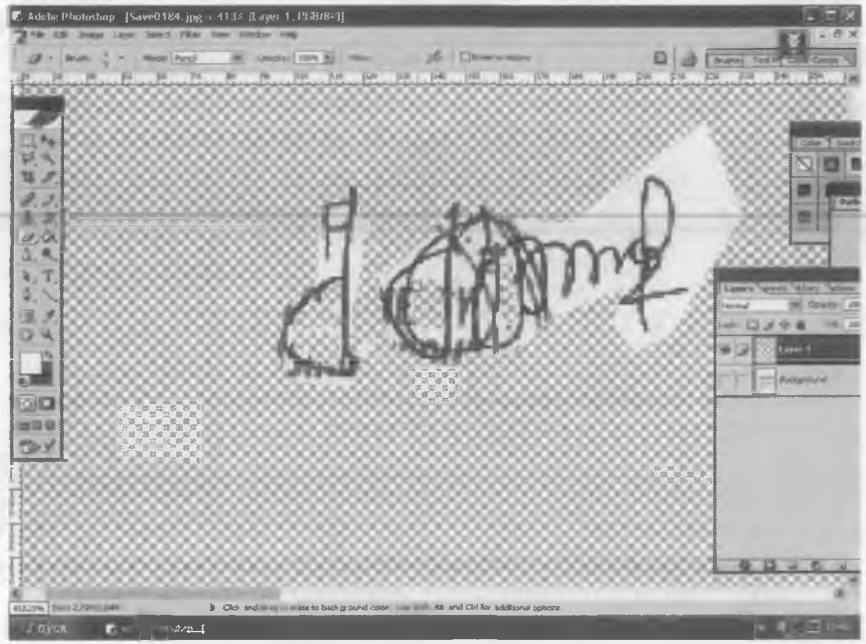


***Рис. 2.15.*** *Отсканированный документ в программе Photoshop*


***Рис. 2.16.*** *Увеличенное изображение печати и подписи с отсканированного документа*


THE STATE OF KENTUCKY
BALTIC ENERGY
LEASING GROUP
LLC
LIMITED LIABILITY COMPANY



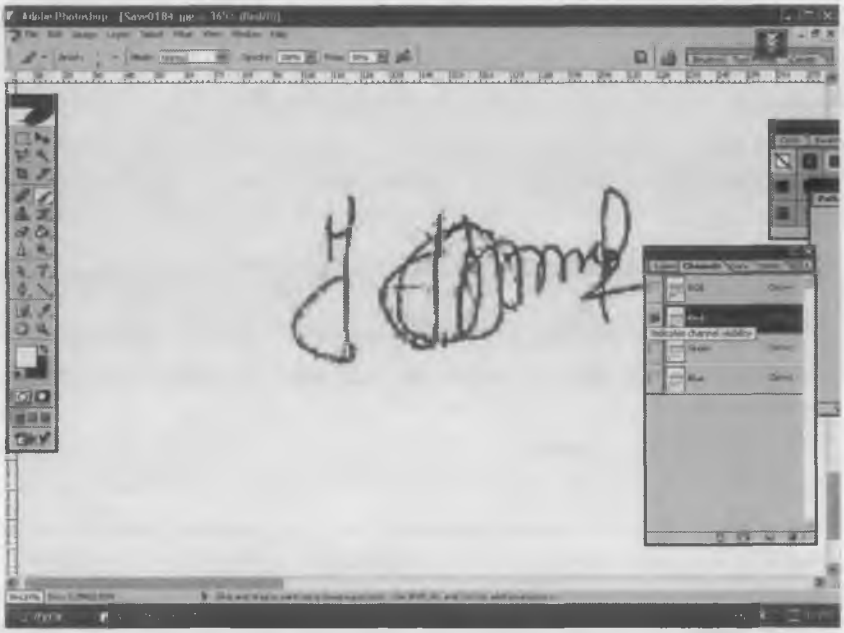


***Рис. 2.17.*** *Разделение печати и подписи с отсканированного документа*

- ✓ создавать в документе специальные поля: колонтитулы, колонцифры, сноски и примечания;
- ✓ отслеживать в документе все изменения, сделанные различными пользователями, а также хранить все эти изменения прямо в документе, чтобы можно было вернуться к предыдущему состоянию редактирования;
- ✓ использовать при редактировании различные средства автозаполнения полей;
- ✓ иллюстрировать документ рисунками, изображениями и фотографиями;
- ✓ снабжать документ специальными значками и символами;
- ✓ использовать мощные средства настроек шрифтов и абзацев;
- ✓ создавать и использовать стили, позволяющие почти мгновенно изменять внешний вид целой группы абзацев документа;
- ✓ использовать автоматическое форматирование по заданным параметрам текста при вводе;
- ✓ в удобной форме проверять правильность написания слов в различных языках;

- ✓ собирать по документу различную статистику;
- ✓ создавать авторефераты для документа;
- ✓ создавать документ совместно несколькими пользователями;
- ✓ пользоваться мощной системой макросов для автоматизирования многих процессов, необходимых при создании документов;
- ✓ автоматически создавать оглавления и указатели;
- ✓ работать с таблицами различного вида, в том числе производить в этих таблицах всевозможные сортировки данных;
- ✓ получать подробные сведения и справки по всем возможностям редактора.

И это перечень далеко не всех возможностей Word. Перейдем к практике. Пересказывать стандартные руководства пользователя бессмысленно, их издано множество. Чему стоит научиться в первую очередь? Вводить и редактировать текст, помещать в него рисунки и управлять их положением относительно текста. Давайте вместе составим заявку на покупку у вас партии металла иностранной фирмой. Выберите подходящий образец документа из массы имеющихся в сети (таблица 2.2), скачайте, откройте его в Word, замените название фирмы на нужное вам (рис. 2.18), поместите над текстом *логотип* фирмы (рис. 2.19), а под текстом печать и подпись директора (рис. 2.20) и… все.

*Таблица 2.2*

| Типы контрактов | Адрес сайта |
|---|---|
| Контракты на английском и русском языках — типовые формы | http://www.inservice.ru/documents/eng-contract/1.html |
| Каталог типовых форм договоров по различным направлениям (на английском языке) | http://www.onecle.com/index.shtml |
| Международные договоры поставки (купли-продажи) на английском и русском языках | http://www.miripravo.ru/sale_index.htm |
| Каталог международных контрактов на русском и английском языках | http://www.miripravo.ru/forms/distrib/distrib_index_0.htm |

*Окончание табл. 2.2*

| Типы контрактов | Адрес сайта |
|---|---|
| Каталог типовых контрактов на английском языке | http://www.jurisint.org/en/con/index.html |
| Контракты купли-продажи на русском языке | http://www.krona-spb.ru/info/cont/ldpko.htm |
| Примеры контрактов по экспорту материалов | http://www.wood.ru/ru/index.php3?reg=1&pag=ldpkopr |
| Каталог контрактов на русском языке | http://a500doc.narod.ru/businessoft.htm |
| Сборник типовых форм договоров на русском языке | http://www.idioma.ru/cgi-bin/b_wiev.pl?id=358&page=1&rzd=2 |
| Соглашения о перепродаже | http://www.polimaster.ru/download/agreements/reseller.doc |
| Библиотека типовых документов | http://gis.tyumen.ru/mycollection/mybookmarks.html |

Распечатанный на хорошем принтере результат ваших трудов может демонстрировать окружающим ваш потенциал и скорое улучшение благосостояния.

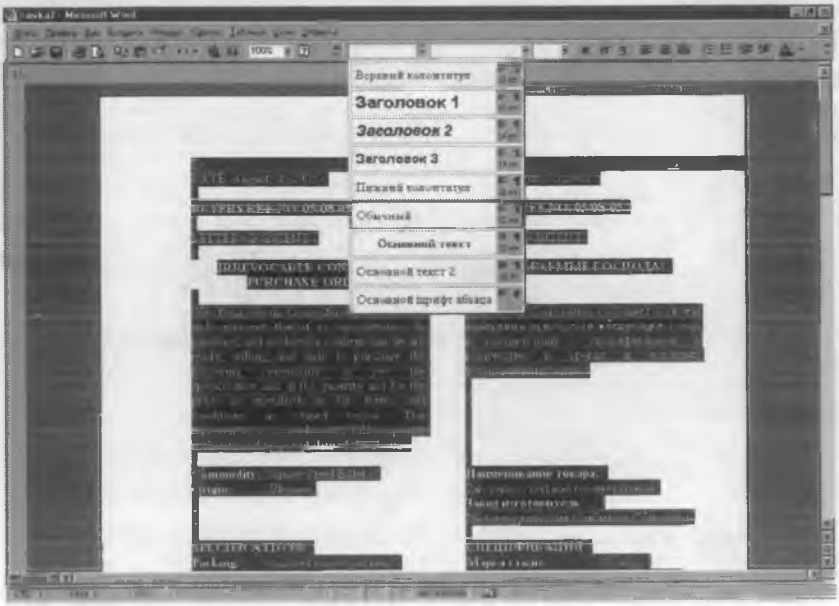



***Рис. 2.18.*** *Формирование заявки на закупку товара из образца*

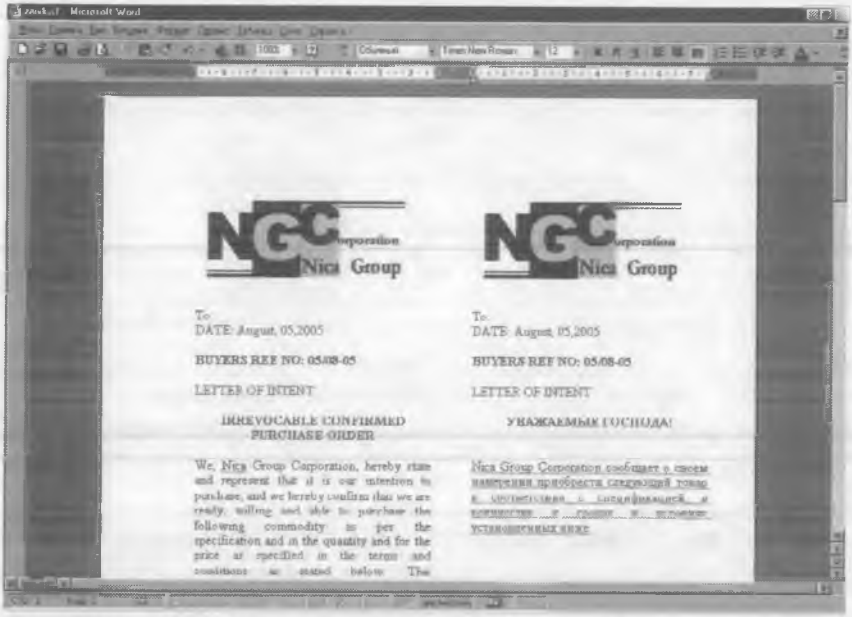



***Рис. 2.19.*** *Размещение логотипа фирмы над текстом*


***Рис. 2.20.*** *Размещение печати фирмы и подписи директора под текстом*

## Запомните

*Если у тебя нет денег — делай вид, что у тебя они есть. Если у тебя есть деньги — делай вид, что у тебя ни гроша.*

***«Пшекруй»***

Абсолютно аналогично вы можете формировать электронные версии своих договоров и писем, не забывая при этом устанавливать защиту (рис. 2.21) путем ввода пароля (рис. 2.22), без знания которого изменения в документах, копирование вашей печати и подписи будет достаточно затруднительным для большинства ваших корреспондентов.

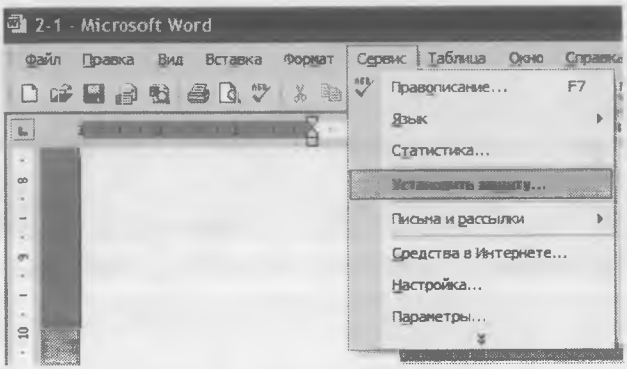



***Рис. 2.21.*** *Установка защиты на отправляемый текст*

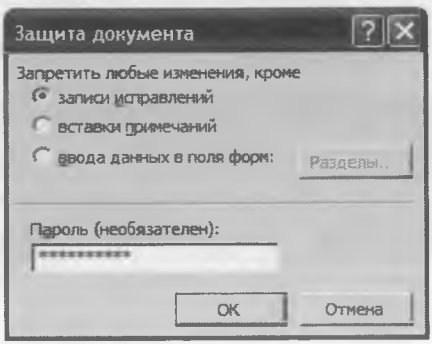



***Рис. 2.22.*** *Введение пароля при установке защиты*

Научившись азам пользования всего тремя программами, вы получаете возможность готовить самостоятельно конфиденциальные документы и создавать их электронные версии, необходимые для реальной работы.

## Кстати ~~~~~~~~~~~~~~~~

*Когда этот бизнес начинает идти на спад, мы распространяем слухи о том, что наши леденцы будто бы действуют как возбуждающее средство, усиливающее половое чувство. Это очень эффективно. Разумеется, слухи, а не леденцы.*

***Уоррен Баффет,***
***самый богатый в мире инвестор***

Если вы потратите на учебу хотя бы еще несколько дней, разобравшись с основными функциями программ по справочным пособиям, приведенным в списке литературы, ваши достижения в бизнес-политике будут ничем не ограничены (поверьте, большинство менеджеров весьма слабо представляют себе возможности современной офисной техники).

## Анекдот в тему:
~ ~ ~ ~ ~ ~

*Молодого человека недавно назначили заведовать отделом. Пытаясь ублажить начальника, он работает до поздней ночи. Уходя как-то домой около полуночи, он увидел своего босса, стоящего возле машины по уничтожению документов с какой-то бумагой в руке.*

*— Послушай, — обратился к нему босс, — это очень важный документ, а моя секретарша уже давно ушла. Ты не знаешь, как эта штуковина работает?*

*— Разумеется, — ответил молодой зав.отделом. Весь дрожа от возможности выслужиться перед боссом, он включил машину, вставил в нее документ и нажал кнопку старта. Документ медленно исчез.*

*— Прекрасно, прекрасно, — воскликнул босс, — не знаю, что бы я делал без тебя. Да, я забыл тебе сказать, что мне нужна лишь одна копия...*

## Резюме

Рассмотренные выше программы установлены практически на всех компьютерах. Их умелое использование позволяет камуфлировать реальную информацию о предприятии в ходе переговоров с пока еще незнакомыми фирмами, проводить кампании дезинформации при возникновении подозрений о появлении в компании чужих «кротов», осуществлять манипуляцию слухами путем организации утечки «достоверной» информации, сфабрикованной вами.

# Глава 3

## На сладкое слетаются не только мухи
### (как защитить свои секреты)

*Деньги любят тишину.*
***Девиз швейцарских банкиров***

**В этой главе:**

- Что такое шифрование.
- Виды алгоритмов.
- Ключи шифрования.
- Хорошие пароли.
- Какими программами шифровать.
- Шифруем файлы.
- А теперь расшифровываем.
- Когда можно использовать полученные навыки.

Когда дела у вас пойдут успешно, число лиц, проявляющих интерес к ним, возрастет многократно. Но даже сейчас (раз уж вы занимаетесь бизнесом) круг желающих заглянуть в ваш компьютер довольно широк. Это могут быть и пока еще верные друзья (но говорят ведь, что «предают только свои»): будущий Соловей-разбойник (ныне — верный помощник, — Алеша Попович), будущая Баба Яга (ныне — секретарша Василиса Прекрасная, или бухгалтер Василиса Премудрая), будущий Кощей Бессмертный (ныне — надежнейший партнер по бизнесу, — Добрыня Никитич), и сегодняшние претенденты на заработанную вами собственность (бандиты, чиновники, родственники), наконец, ваши конкуренты.

Как же оградить от них свои секреты?

## Запомните ~~~~~~~~~~~~~

*Опыт — это такая вещь, которая появляется сразу после того, как была нужна.*

*NN*

### *ПОЛЕЗНАЯ ИНФОРМАЦИЯ*

Чтобы защитить информацию, ее шифруют. Шифрование выполняется преобразованием скрываемого текста по каким-либо математическим закономерностям, которое делает восстановление исходного положения символов этого текста предельно сложным процессом для всех, кто не является законным владельцем информации. Шифрование информации гарантирует вам, что она будет в безопасности, даже если попадет в чужие руки. Например, если вы переставите буквы в строке о расходах за текущий день, она будет выглядеть так:

ОТКАТ СИДОРОВУ 25000 = ТТР0К0ВВС0О2УО5ОИА

Если же вы символы не только перемешаете, а еще и замените (а на клавиатуре их гораздо больше, чем букв в нашем алфавите), эта строка может выглядеть вот так:

ОТКАТ СИДОРОВУ 25000 = %G-9345Pu#12!!-9Ap:H}

Согласитесь, что добраться до ее смысла стало совсем сложно.

## Анекдот в тему:

~~~~~~

*Лектор в колхозе произносит речь:*

*— В настоящее время некоторые пессимистически настроенные элементы катастрофически мистифицируют патологическую абстракцию. С точки зрения банальной концепции, это явление возможно. А вы как считаете, товарищи колхозники?*
~~~~~~

*Встает колхозник, навоз с валенка скинул и отвечает:*
*— Так-то оно так, но потому как быть того не может, кабы чего-нибудь да не было. И не потому, что оно вообще, а когда оно что, вот тогда оно и пожалуйста.*

Но заменять символы на другие и менять их местами нужно по определенному, заранее установленному правилу, иначе восстановить исходный текст было бы невозможно. Порядок перестановки символов или замены их другими, т.е. набор логических правил, определяющих процесс преобразования информации из открытого состояния в зашифрованное, называется алгоритмом шифрования. Алгоритмы делятся на два типа: алгоритмы с открытым ключом, использующие различные ключи для шифрования и расшифрования (о программах, использующих эти алгоритмы, мы поговорим попозже); алгоритмы с секретным (или, как его еще называют, симметричным) ключом, использующие один и тот же ключ как для шифрования, так и для расшифрования. В программах, применяемых для шифрования информации, хранящейся в компьютере, обычно используются именно алгоритмы с симметричным ключом. Список наиболее часто встречающихся в программах шифрования алгоритмов с симметричным ключом, зарекомендовавших себя как надежные, приведен в табл. 3.1.

*Таблица 3.1*

| **Алгоритм** | **Максимальная длина ключа** |
|---|---|
| DES | 56 бит |
| 3DES | 112, 168 бит |
| Blowfish | до 448 бит |
| IDEA | 128 бит |
| AES | 128, 192, 256 бит |
| ГОСТ 28147-89 | 256 бит |

Шифрование выполняют с помощью ключей. Ключ шифрования — это специальным образом сформированная последовательность бит (единиц информации), являющаяся переменным

параметром алгоритма шифрования. Если вы зашифруете одну ту же информацию по одному и тому же алгоритму, но разными ключами, результаты получатся разные. Ключ шифрования имеет одну существенную характеристику — длину, которая, как правило, измеряется в битах. Сложность перебора всех возможных ключей растет с увеличением длины используемого ключа. Добавление только одного бита к ключу удваивает количество возможных вариантов ключей, добавление 10 бит — увеличивает число этих вариантов более чем в 1000 раз (если быть точным, то в 1024 раза). Поэтому, выбирая программы для шифрования, обращайте внимание на длину ключей, которые они используют. Лучше всего применять программы с длиной ключей не менее 128 бит. Ориентировочное время взлома ключей разной длины основными группами претендентов на знание ваших секретов, обладающими разными финансовыми возможностями, приведено в табл. 3.2.

*Таблица 3.2*

| **Тип нападающего** | **Затраты на технические средства** | **Время взлома ключа** | | **Длина ключа, достаточная для защиты** |
|---|---|---|---|---|
| | | 40 бит | 56 бит | |
| Хакер | $400 | 5 часов | 38 лет | 50 бит |
| Малый бизнес | $10 000 | 12 минут | 556 дней | 55 бит |
| Средний бизнес | $300 000 | 0,18 секунды | 3 часа | 60 бит |
| Крупная компания | $10 000 000 | 0,005 секунды | 0,6 минуты | 70 бит |
| Спецслужбы | $300 000 000 | 0,0002 секунды | 12 секунд | 75 бит |

### *ИЛЛЮСТРАЦИЯ*

Bruce Schneier, Applied Cryptography

*На сегодняшний день для симметричных алгоритмов шифрования достаточной длиной ключа шифрования считается 128 бит (16 байт). Для полного перебора всех возможных клю-*

*чей длиной 128 бит (атака* **brute force***) за один год необходимо наличие 4,2 × $10^{22}$ процессоров производительностью 256 миллионов операций шифрования в секунду. Стоимость такого количества процессоров составляет 3,5 × $10^{24}$ долларов США. Существует международный проект distributed.net, целью которого является объединение пользователей Интернетом для создания виртуального распределенного суперкомпьютера, занимающегося перебором ключей шифрования. Последний проект по взлому ключа 64 бит завершен в течение 1757 дней, в нем приняло участие более трехсот тысяч пользователей, а вычислительная мощность всех компьютеров проекта была эквивалентна почти 50 000 процессорам AMD Athlon XP с тактовой частотой 2 ГГц. Увеличение длины ключа шифрования на один бит увеличивает количество значений ключа, следовательно, и время перебора, в два раза. То есть, исходя из вышеприведенных цифр, за время 1757 × 2 дней можно взломать не 128-битный ключ, как может показаться на первый взгляд, а всего лишь 65-битный.*

Если раньше лихим героям-разведчикам приходилось шифровать вручную, затрачивая на подготовку маленькой радиограммы массу времени, компьютеры сделали процесс шифрования простым, легким и быстрым.

*Анекдот*
*в тему:*

~ ~ ~ ~ ~ ~

*Приходит как-то Гитлер на совещание, а поперек комнаты стоит огромный железный ящик. Гитлер спрашивает у Мюллера:*

*— Это что такое?*

*— А это Штирлиц установил новейшее советское миниатюрное компьютерное устройство, которое подслушивает и передает шифровками в Москву все наши разговоры.*

*— А чего же вы его не вытащите отсюда, если уж обнаружили? — раскричался Гитлер.*

*— Мы бы, мой фюрер, с удовольствием! Только его никто поднять не может, — ответил Мюллер.*

Особенность компьютерного шифрования в том, что даже незначительное увеличение стоимости вычислений (несколько лишних секунд работы вашего компьютера) может обеспечить огромное увеличение качества защиты. Очень стойкое шифрование сообщений (например, с 256-битным ключом) обычно требует чуть больше вычислений, чем шифрование слабое (с 56-битовыми ключами). Вследствие этого появилась возможность использовать сильное шифрование для защиты практически любого объема информации, сохраняемой вами на компьютере.

Ключи шифрования формируются из паролей, которые задаете вы сами (ключ — набор символов, его вы вряд ли запомните, а вот пароль — «1 000 000 баксов», отложится в памяти легко). Поэтому пароли все еще играют важную роль при организации системы защиты информации. Проблема в том, что именно они — простейший путь для взлома защиты. Почему? Да потому, что многие пользователи (так как возможности памяти среднестатистического человека ограничены) часто в качестве паролей используют год своего рождения, имена друзей или родственников, клички животных и т.д. (т.е. шифруют информацию с помощью «плохих» (простых для подбора) паролей. Задача подбора пароля оказывается значительно проще, чем подбор ключа шифрования. Но задача расширения возможностей памяти пользователя выходит за рамки данной книги, поэтому давайте рассмотрим способы, позволяющие значительно усложнить злоумышленнику процесс такого подбора. Какие пароли можно считать «хорошими»? Хорошим считается пароль, который крайне трудно угадать или подобрать, но очень легко запомнить. Он должен быть достаточно длинным (не меньше 7 символов), состоять из букв, цифр и символов, но в то же время легко и безошибочно набираться на клавиатуре.

Лучшая техника для создания сложных, но легко запоминаемых паролей — использование сочетаний слов, цифр и символов, которые мы хорошо знаем (например, имя самого богатого человека в мире + URL вашего любимого сайта или имя вашего первого начальника + email вашего партнера. Еще лучше использовать слова, написанные с «ошибками», вставлять посреди слова буквы в верхнем регистре, цифры, тире, знаки подчеркивания и пробелы. Даже для высококвалифицированного взломщика это затруднит процесс вскрытия информации в несколько сот тысяч раз, а для низкоквалифицированного сделает его просто невозможным). Старайтесь не записывать используемый пароль (некоторые пользователи хранят свои пароли записанными на листке, лежащем в ящике стола или наклеенном на монитор, так что быстрый поиск паролей героями зарубежных триллеров — часто горькая правда жизни), а если решили записать, пишите его только частично и храните подальше от компьютера.

Надежное шифрование ваших секретов зависит от триады: надежный алгоритм — длинный ключ — хороший пароль. Слабость любого элемента из этой тройки недопустима.

### *НЕОБХОДИМЫЕ НАВЫКИ*

При шифровании симметричным ключом используются одинаковые ключи для шифрования и расшифровывания сообщений. Ключ этот имеют (если он используется для шифрования сообщения) только отправитель и адресат, он не должен быть известен третьему лицу. Поэтому главная проблема симметричной криптографии состоит в предварительной передаче секретного ключа одним абонентом другому по надежному каналу. Это неудобство, однако, не мешает в случае, когда создатель и получатель сообщения одно и то же лицо (т.е. вы шифруете свою информацию на компьютере, храните ее какое-то время в зашифрованном виде, а затем расшифровываете, чтобы использовать). Кроме деловой переписки у вас есть ведь, конечно, и личные секреты, о которых нежелательно знать другим: список телефонов «нужных людей»; каталог избранных сайтов; письма информатора из фирмы конкурента; план рекламной компании; бизнес-план производства нового продукта и т.д. Нет ничего некорректного в том, что вы хотите сохранить в тайне свою конфиденциальную информацию.

*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*Едет новый русский на джипе «Чероки» по проселочной дороге. Скорость под 120. И, вылетая из-за крутого поворота, со всего размаху врезается в телегу, которой управляет мужик. Джипу хоть бы хны, телега же — в одну сторону, лошадь — в другую, мужик — в третью.*

*Лежит мужик на обочине, смотрит краем глаза — машина крутая, и начинает размышлять:*

*Так: лошадь — 8000.*

*Телега — 1000.*

*За здоровье попросить — 5000.*

*За моральный ущерб — ....*

*В этот момент из джипа выскакивает новый русский и подбегает к лошади. Та бьется в конвульсиях. Новый русский, недолго думая, достает пушку и двумя выстрелами в голову пристреливает ее. После этого с пистолетом в руке поворачивается и кричит:*

*— Мужик, а ты как себя чувствуешь?*

*Мужик (убегая на четвереньках в поле) — Лучше!!! Значительно лучше!!!*

Но как этого достичь? Ответ прост — всегда шифровать важную для вас информацию. Это Штирлицу приходилось маяться с шифровками и кодовыми книгами. Вам же в мгновение ока защиту практически любых объемов документации осуществит компьютер. Имеется довольно большое количество бесплатных программ (табл. 3.3), обеспечивающих надежное и быстрое шифрование сертифицированными алгоритмами (AES, 3DES, Blowfish, ГОСТ).

*Таблица 3.3*

| Программа | Характеристики |
|---|---|
| **AES Free**<br>519 Kb<br>http://www.abensoft.com/free.htm | Очень простая в пользовании программа. Использует алгоритм шифрования AES, длина ключа 128 бит, максимальная длина пароля — 7 символов. Имеет шредер, архиватор, позволяет создавать самораспаковывающиеся шифрованные файлы, изменять расширение шифруемых файлов, шифровать целиком папки со всем содержимым. |
| **FineCrypt**<br>4.06 Mb<br>http://www.finecrypt.net/index.htm | Очень мощная, но довольно сложная в пользовании программа. Предлагает на выбор 10 алгоритмов шифрования, имеет шредер и архиватор, позволяет создавать самораспаковывающиеся файлы. |

*Окончание табл. 3.3*

| Программа | Характеристики |
|---|---|
| **Dpcrypto**<br>437 Kb<br>http://www.dpaehl.de | Очень простая в использовании программа для шифрования отдельных файлов. Использует 8 алгоритмов. Не имеет никаких дополнительных функций. |
| **EasyCrypto Deluxe**<br>1.85 Mb<br>http://www.handybits.com | Отлично оформленная программа для шифрования отдельных файлов. Использует алгоритм BlowFish с длиной ключей от 40 до 128 бит и паролями до 8 букв. |
| **Crypto-Lock**<br>408 Kb<br>http://www.rtsoftware.org | Очень простая программа для шифрования отдельных файлов. Использует алгоритм Blowfish. Способна создавать самораспаковывающиеся файлы. |
| **Iron Key**<br>1,0 Mb<br>http://www.bestcrypto.com/products | Не очень удобная в пользовании программа. Использует алгоритм DES, длина ключа 56 бит. Не имеет никаких дополнительных функций. Пригодна для шифрования отдельных файлов. |
| **SafeGuard PrivateCrypto**<br>5,6 Mb<br>http://www.utimaco.com | Отлично оформленная и очень простая программа для шифрования отдельных файлов. Использует алгоритм AES. Способна создавать самораспаковывающиеся файлы. |

Большинство их настолько просты в пользовании, что любой ребенок, владеющий компьютером, является нынче лучшим шифровальщиком, чем знаменитые математики и разведчики прошлого. Давайте посмотрим, как осуществляется защита документов на примере одной из перечисленных в таблице программ — бесплатной программы AES Free. После ее установки (фактически заключающейся в серии последовательных нажатий кнопки Next) и запуска открывается интерфейс с тремя окнами. Под ними написано, что нужно делать для шифрования или расшифровки информации. Прочитаем эту инструкцию по

шифрованию (Шифрование: выберите файлы в левом окне и перетащите их в контейнер (центральное окно). Введите имя для зашифрованного файла. Введите и подтвердите пароль. Нажмите кнопку «Encrypt» («Зашифровать»)) и последуем ей (рис. 3.1). Эта программа, что позволяет шифровать как отдельные файлы, так и папки со всем содержимым. Поэтому перетащим в контейнер какие-нибудь файлы и папку, присвоим будущей шифровке имя (test), введем (и постараемся не забыть!) пароль и нажмем кнопку «Encrypt». Проходит секунда, содержимое центрального окна исчезает, а в правом окошке появляется файл «test». В нем и содержится в зашифрованном виде содержимое выбранных документов и папки (рис. 3.2).

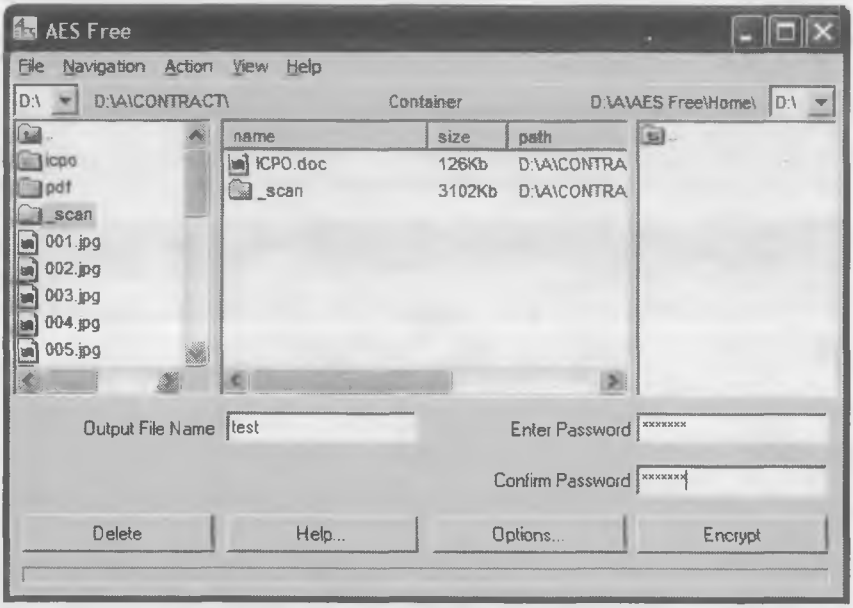



***Рис. 3.1.*** *Ввод шифруемых документов*

Процесс расшифровки также легок. Нужно просто перетащить из правого окошка зашифрованный файл в контейнер (центральное окно), ввести пароль и нажать кнопку «Decrypt» («Расшифровать») (рис. 3.3). В правом окошке тут же появится расшифрованная информация (рис. 3.4).

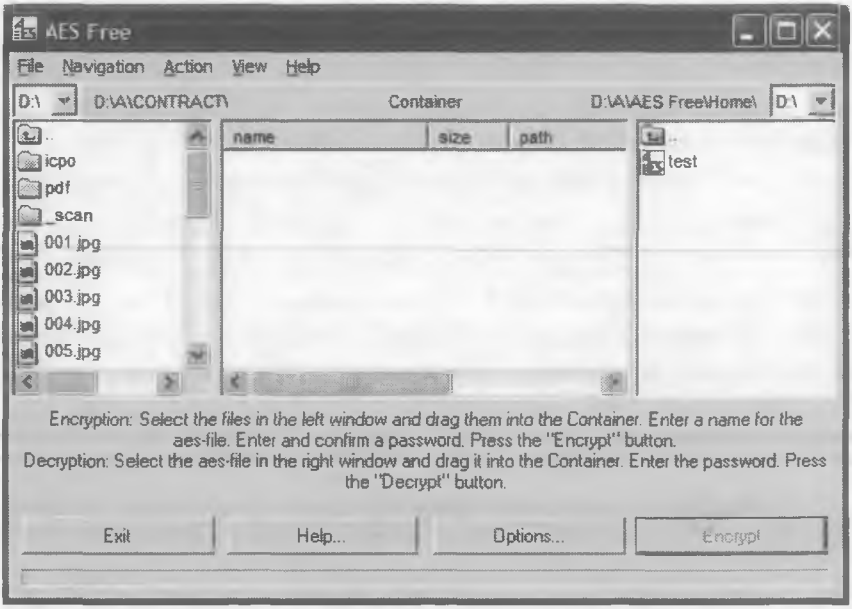



***Рис. 3.2.*** *В правом окне появился файл с зашифрованной информацией*

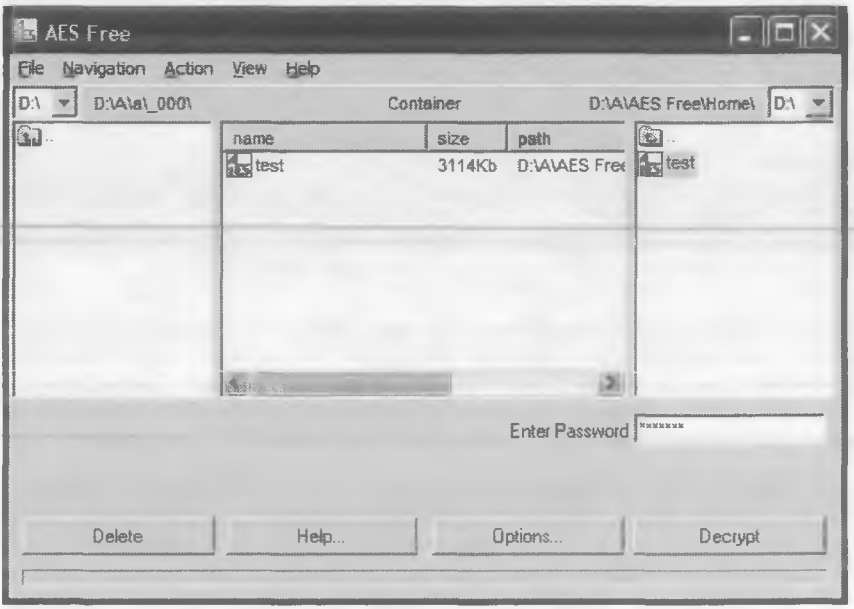



***Рис. 3.3.*** *Расшифровка файла*

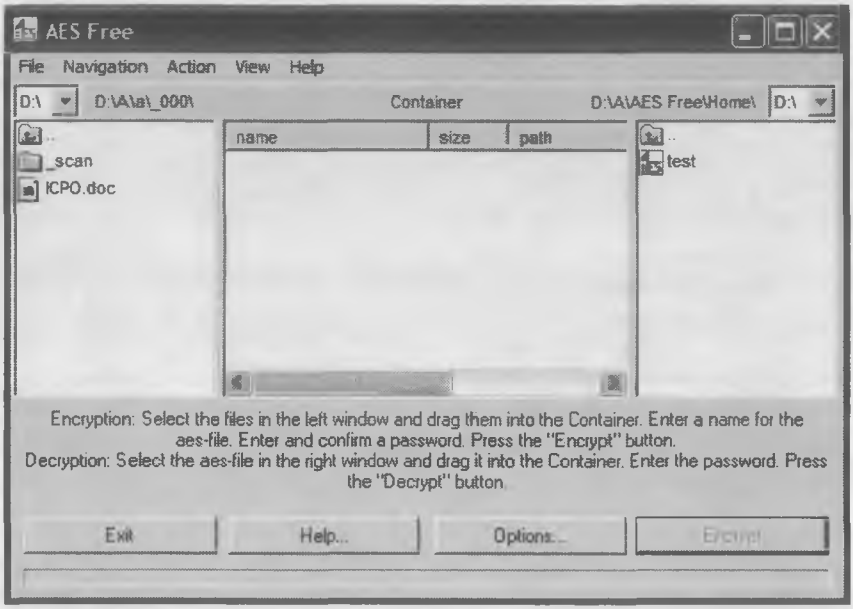



***Рис. 3.4.*** *В левом окне появилась расшифрованная информация*

У этой программы есть еще несколько полезных свойств. Вы можете выбрать расширение закодированного файла так, чтобы он внешне ничем не отличался от большинства файлов на вашем компьютере (рис. 3.5). В этом случае найти, какой же из множества файлов зашифрован, будет отдельной проблемой для заинтересованных лиц

## *Анекдот в тему:*

~ ~ ~ ~ ~ ~ ~

*Новый русский справляет новоселье. Собирает всех друзей, знакомых, подельников и везет к себе домой. На подъезде у него с недоумением спрашивают:*

*— Слушай, какое, к черту, новоселье? Ведь это и так был твой дом.*

*— Ну и что же? Адрес-то новый. Я ребятам из городской управы забашлял, они мне улицу переименовали.*

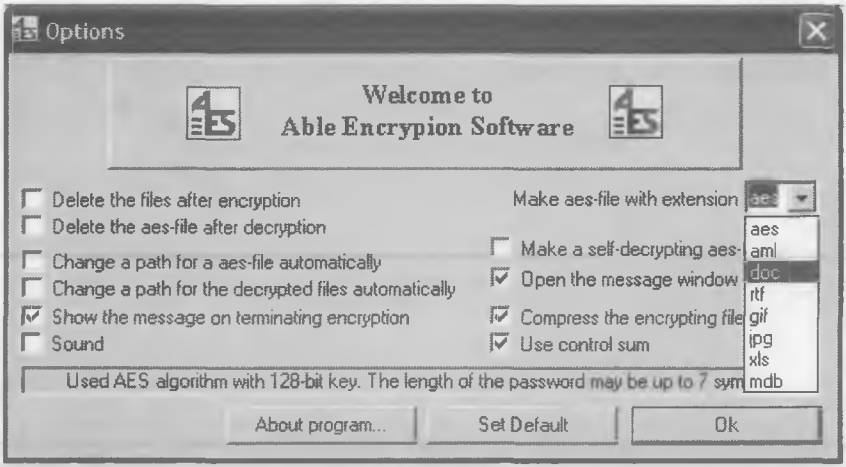



***Рис. 3.5.*** *Выбор расширения для зашифрованного файла*

В некоторых программах для шифрования информации (в частности, и в рассматриваемой) встроены шредеры, позволяющие уничтожать файлы, которые шифруются, автоматически (рис. 3.6). Дополнительной функцией использования встроенного шредера является уничтожение расшифрованных документов после их просмотра (расшифровали вы папку с документами, изучили нужные, затем уничтожили ее, — зашифрованный файл со всей папкой у вас-то имеется).

Отметим возможность создания программой самораспаковывающихся зашифрованных файлов, которые можно расшифровать на тех компьютерах, на которых сама программа не установлена. Допустим, вы отправляетесь в путешествие. Вам необходимо прихватить с собой некоторые конфиденциальные записи. Не везти же с собой программу для их расшифровки? Да и гостиничный компьютер может быть настроен так, что просто не разрешит вам устанавливать новое программное обеспечение. Как быть? Взять с собой самораспаковывающийся файл. Для его создания в настройках программы поставьте птичку возле записи «Make a self-decrypting aes-file» («Создавать самораспаковывающийся файл») (рис. 3.7). А дальше все делаете так же, как и раньше (вы можете сопровождать зашиф-

рованные файлы комментариями, для этого просто поставьте птичку возле надписи «Open the message window» («Открыть окно для сообщения»).

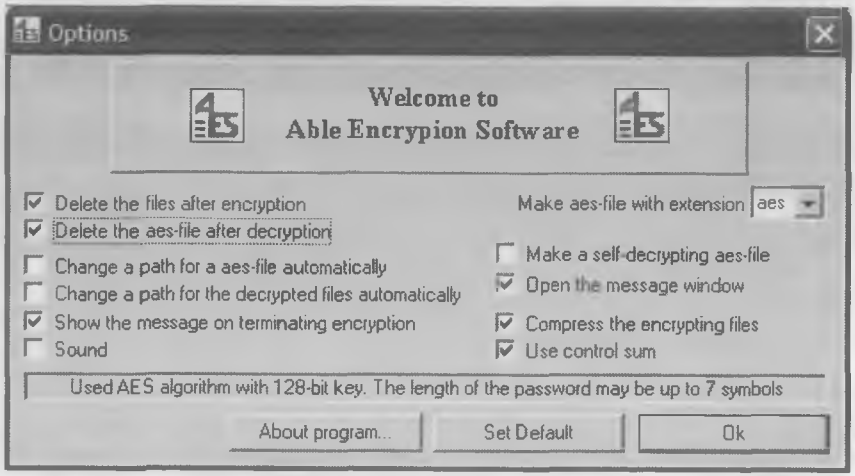



***Рис. 3.6.*** *Включение режима шредера (уничтожения исходных файлов при шифровании/расшифровке)*

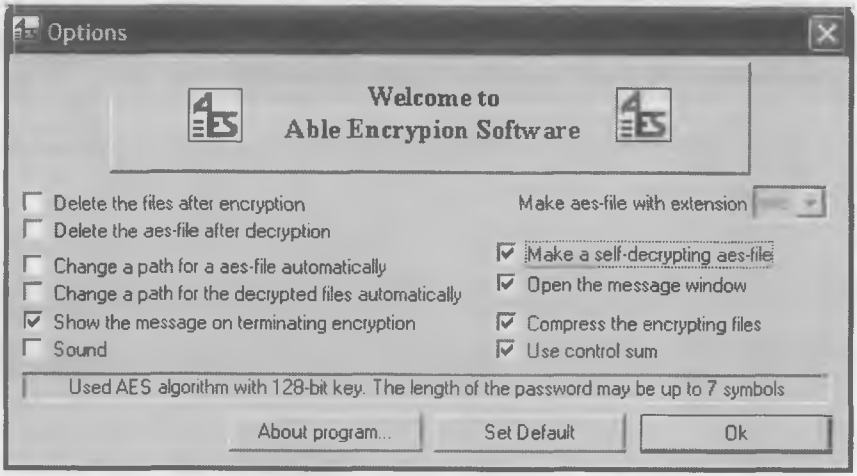



***Рис. 3.7.*** *Создание самораспаковывающихся зашифрованных файлов*

Теперь файл с закодированной информацией будет иметь расширение .exe и при запуске на любом компьютере перед ва-

ми будет появляться окошко, позволяющее выбрать место размещения расшифрованной информации, а после введения пароля прочитать комментарии к ней и получить доступ к документам (рис. 3.8, 3.9).

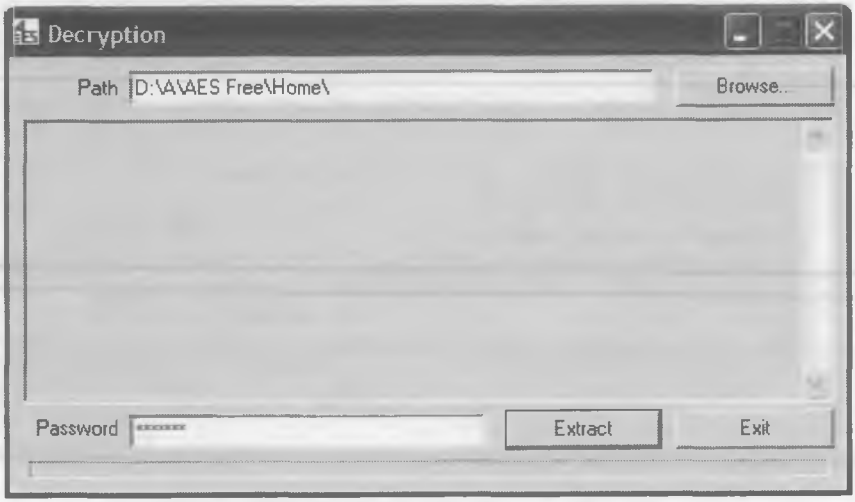



***Рис. 3.8.*** *Запуск самораспаковывающегося файла*

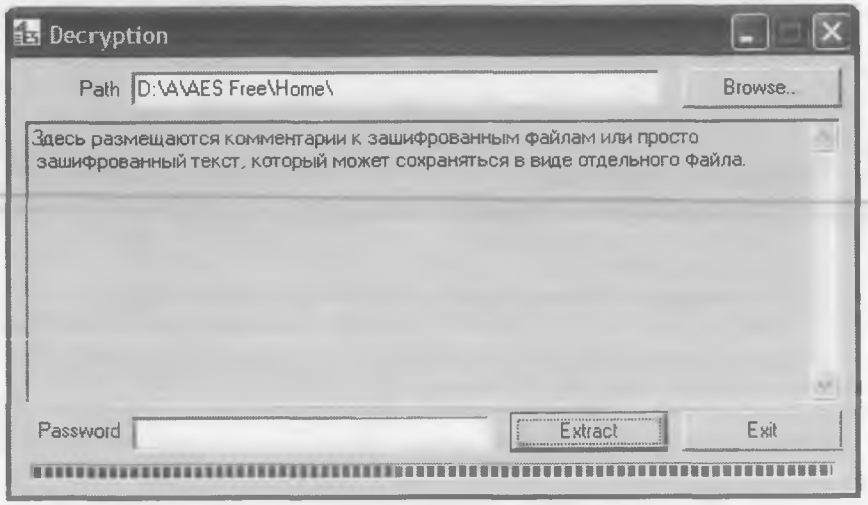



***Рис. 3.9.*** *Расшифрованные документы сохранены в директорию, указанную в верхнем поле, а комментарий появился в центральном окне*

Вы можете пересылать такие файлы вашим партнерам (с которыми заранее оговорили пароль для связи), брать их с собой в путешествие, да и просто, перемещаясь от домашнего компьютера к рабочему после трудового воскресного дня или бессонной ночи.

Наверняка вам случалось смотреть голливудские боевики, в которых герои лихо подключают к системам защиты свои ноутбуки и быстренько подбирают пароли, вскрывающие эти системы («Настоящая Маккой», «Рыба-меч» и т.п.).

*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*Из отчета службы безопасности «По поводу взлома китайцами сервера Пентагона»:*

*1) Каждый китаец попробовал один пароль.*

*2) Каждый второй пароль был «maodzedun».*

*3) На 657983241-й попытке сервер согласился, что у него пароль «maodzedun».*

К счастью, это только фантазии продюсеров, сценаристов и режиссеров, не имеющих представления о простейших мерах, предотвращающих возможность такого подбора. Если вы заметили, экспериментируя с описанной программой, она обладает одним несколько раздражающим свойством, — медлит примерно секунду перед началом шифрования или расшифровки. Чем это вызвано? Ключ, которым осуществляется шифрование документа, формируется из введенного вами пароля. Разработчики сделали простую вещь — ввели в процесс формирования ключа ряд математических операций, **усложняющих и,** тем самым, **замедляющих** это формирование. Выбросьте их, и вы, даже имея правильный пароль, никогда не расшифруете зашифрованный с его помощью текст. А вы-

полняясь, они не дают проверять больше нескольких паролей в секунду (дополнительные математические операции замедляют процесс подбора пароля в несколько миллионов раз, т.е. в несколько миллионов раз уменьшается и вероятность его взлома). Взломщик может подбирать пароли, используя самые скоростные компьютеры, однако даже при этом он не сможет перебирать более нескольких десятков паролей в секунду.

*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*Встречаются два новых русских у касс трансагентства. Выясняется, что оба едут в один и тот же далекий город, однако первый — самолетом, а второй — поездом.*

*Тот, что — самолетом, спрашивает у второго:*

*— А че поездом-то??? Долго, тяжело, неудобно...*

*Второй:*

*— Боюсь самолетом-то: столько террористов развелось, только и слышишь, там самолет взорвали, здесь взорвали. Поездом надежнее.*

*— Ерунда! Я тут у знакомого математика спросил, какова вероятность того, что в самолет подложат бомбу. Он прикинул — мизер, что-то типа 0,0001... Тогда я спросил, а какова вероятность, что я окажусь в самолете с двумя подложенными бомбами на борту? Оказалось, и вовсе ничтожная величина: 0,00000001. С тех пор я вожу с собой бомбу и летаю спокойно...*

Платные программы обладают теми же характеристиками, что и бесплатные, но не имеют ограничений по длине паролей и позволяют использовать максимально допустимые алгоритмами размеры ключей шифрования (табл. 3.4).

*Таблица 3.4*

| Программа | Характеристики |
|---|---|
| **CHAOS Messenger**<br>698 Kb<br>$54,95<br>http://www.safechaos.com/cm.htm | Очень простая в пользовании программа. Предлагает на выбор пять алгоритмов шифрования (AES, 3DES, Blowfish, GOST, поточное шифрование). Имеет шредер, архиватор, позволяет создавать самораспаковывающиеся шифрованные файлы, активные файлы, изменять расширение шифруемых файлов, шифровать целиком папки со всем содержимым. |
| **AES Home**<br>708 Kb<br>$39,95<br>http://www.abensoft.com/home.htm | Очень простая в пользовании программа. Предлагает на выбор три алгоритма шифрования (AES, 3DES и Blowfish). Имеет шредер, архиватор, позволяет создавать самораспаковывающиеся шифрованные файлы, активные файлы, изменять расширение шифруемых файлов, шифровать целиком папки со всем содержимым. |
| **USA Shield**<br>560 Kb<br>$49,95<br>http://www.usa.safeworld.info | Очень простая в пользовании программа. Предлагает на выбор три алгоритма шифрования (AES, 3DES и Blowfish). Имеет шредер, архиватор, позволяет создавать самораспаковывающиеся шифрованные файлы, шифровать целиком папки со всем содержимым. |
| **Folder Lock**<br>1.8 Mb<br>$35,00<br>http://www.newsoftwares.net/folderlock | Великолепно оформленная и сравнительно простая в использовании программа. Использует один алгоритм шифрования (Blowfish). Позволяет шифровать папки со всем содержимым. |

*Продолжение табл. 3.4*

| Программа | Характеристики |
|---|---|
| **ABI-CODER**<br>1.48 Mb<br>$12,99<br>http://www.abisoft.net/bd.html | Сравнительно простая в использовании программа. Предлагает на выбор три алгоритма шифрования (AES, 3DES и Blowfish). Позволяет создавать самораспаковывающиеся шифрованные файлы и шифровать целиком папки со всем содержимым. |
| **PC-Encrypt**<br>480 Kb<br>$49,00<br>http://www.pc-encrypt.com | Не слишком простая в пользовании программа (на любителя). Использует один алгоритм шифрования (Blowfish). Позволяет шифровать файлы и содержимое папок. Имеет шредер. Не позволяет применять пользователям за пределами США пароли длиннее 7 символов. |
| **PowerKey**<br>1.0 Mb<br>$35<br>http://www.elcor.net | Не слишком простая в пользовании программа. Использует 8 алгоритмов шифрования (Blowfish, 3Des, Des, Gost, RC2, Rijndael, Twofish). Имеет шредер, архиватор, позволяет создавать самораспаковывающиеся шифрованные файлы. |
| **CryptoMite**<br>1.58 Mb<br>$29,00<br>http://www.baxbex.com | Достаточно сложная в использовании программа. Использует семь алгоритмов шифрования (AES, Twofish, Mars, Cast 256, Blowfish, Gost, SCOP). Имеет шредер, архиватор, позволяет создавать самораспаковывающиеся шифрованные файлы, шифровать целиком папки со всем содержимым. |
| **Super File Encryption**<br>919 Kb<br>$39,95<br>http://www.fileencryption.org | Простая, но не очень удобная в пользовании программа. Предлагает на выбор пять алгоритмов шифрования (AES, Blowfish, Hash, Des и 3Des). Способна шифровать отдельные файлы и папки. |

*Окончание табл. 3.4*

| Программа | Характеристики |
|---|---|
| **Kremlin**<br>1,08 Mb<br>$35<br>http://www.kremlinencrypt.com | Простая, но не очень удобная в пользовании программа. Предлагает на выбор пять алгоритмов шифрования (Blowfish, CAST, Safer, RC4 и 3Des). Способна шифровать отдельные файлы и папки. |

Некоторые из них (AES Home или Chaos Messenger, например) позволяют создавать «активные» файлы. Это такие же самораспаковывающиеся шифрованные файлы, удобные для переброски информации, как и в приведенном выше примере, но имеющие встроенную мини-программку, обеспечивающую возможность шифрования ответного послания. То есть получили вы зашифрованный файл, сидя в своем гостиничном номере где-нибудь в Лондоне или Воронеже (как приложение к письму, или через свою ячейку сетевого депозитария, например), ввели пароль, прочитали послание, написали ответ, щелкнули по кнопке «Reply» (ответ) (рис. 3.10) и обеспечили себе возможность зашифровать как ответ, так и приложенные к нему файлы, рисунки, папки с документами (рис. 3.11). И все это, заметьте, без установки программ на гостиничном или «где вы там находитесь по своим делам» компьютере.

*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*Новый русский уехал на Канары и звонит оттуда в свою пейджинговую компанию оператору:*

*— Ну, пацаны, крутая у вас компания, всю жизнь теперь буду только у вас пейджера покупать и братанам посоветую!*

*— ???*

*— Да я даже здесь, на Канарах, сообщение от вас на пейджер получил!*

*— Какое сообщение?*

*— «Замените батарейку!»*

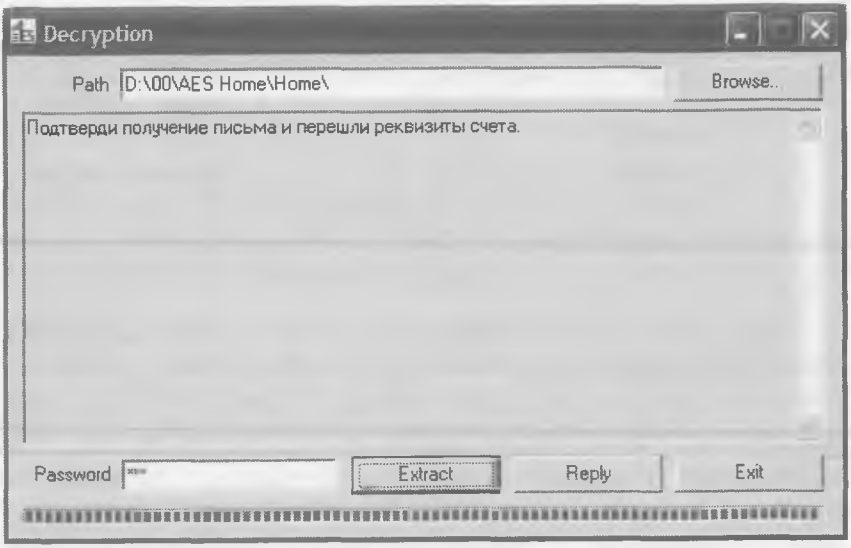



***Рис. 3.10.*** *Расшифрованные документы сохранены в директорию, указанную в верхнем поле, сообщение появилось в центральном окне, а ответ можно написать, щелкнув по кнопке «Reply»*

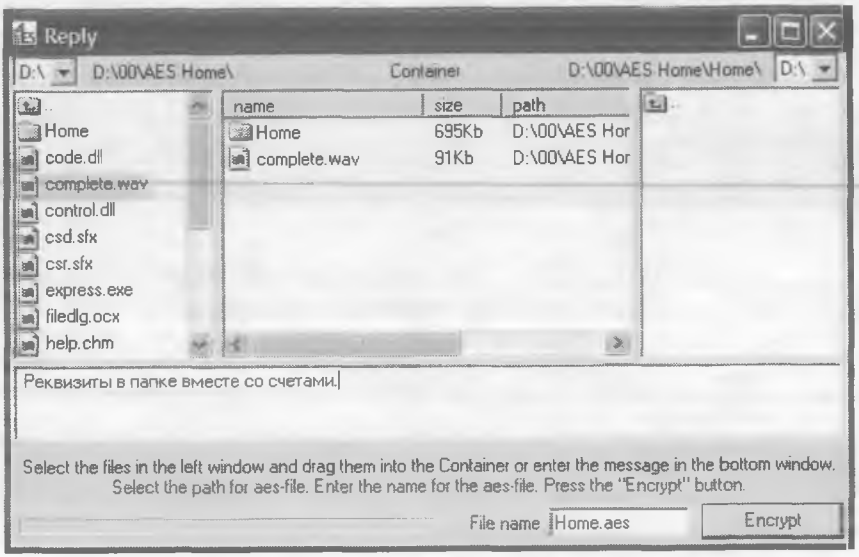



***Рис. 3.11.*** *Интерфейс активного файла*

## Резюме

~ ~ ~ ~ ~

Как военные самолеты каждого типа применяются для решения ограниченного круга поставленных перед ними задач, так и программы для защиты информации могут быть оптимально использованы только в заданных для них границах, выход за которые грозит снижением уровня безопасности. Когда имеет смысл применять описанные программы? Они, безусловно, надежны, но не прячут шифрованные файлы от постороннего взгляда. Поэтому использовать их стоит для защиты данных, когда информация о наличии у вас секретов некритична или не может представлять для вас угрозы, например:

- ✓ когда вы храните свою личную переписку на рабочем или домашнем компьютере и не хотите, чтобы ее просматривали другие сотрудники или родственники;
- ✓ когда вы храните домашнюю бухгалтерию на подключенном к сети компьютере и не хотите, чтобы в нее заглянул какой-либо праздношатающийся хакер;
- ✓ когда вы берете работу на дом и не хотите, чтобы утечка информации произошла при потере носителя (дискеты, диска, флешки);
- ✓ когда вы отправляетесь в путешествие и берете с собой ноутбук (в дороге он может быть потерян или украден, зачем же вору давать возможность читать конфиденциальную переписку с бизнес-партнерами, хранящуюся в этом ноутбуке?);
- ✓ когда вы шифруете и отправляете свою информацию в электронный депозитарий на удаленном сервере по открытому каналу связи.

*Не забывайте защищать ваши секреты,*
*они вам еще пригодятся!*

# Глава 4

## Хамелеона трудно отличить от стены

*(как скрыть свои секреты)*

*«Сограждане!» — начал он взволнованным голосом, но так как речь его была секретная, то весьма естественно, что никто ее не слыхал.*

***М. Салтыков-Щедрин, «История одного города»***

**В этой главе:**

- Зачем делать наличие секрета тайной?
- Что такое стеганография?
- Какие бывают контейнеры?
- Учимся размещать и извлекать информацию.
- Как все это лучше использовать?

Теперь, когда вы научились шифровать свои документы, поговорим о приемах сокрытия того факта, что вы вообще это делаете. Утечка информации о том, что вы используете программы для защиты своих секретов, может вызвать интерес к вам различных служб и организаций (как официальных, так и неофициальных), априори убежденных (и часто небезосновательно), раз уж у вас есть компьютер и вы храните в нем информацию, не предназначенную для чужих глаз, то эта информация финансового характера, и, добравшись до нее, их сотрудники сумеют разделить с вами результаты ваших финансо-

вых успехов, пополнив как свои карманы, так и кошельки ведомств, которые они представляют. Самое простое средство сокрытия самого факта существования у вас конфиденциальной зашифрованной информации — смена формата расширения у зашифрованного файла (например, формата расширения .aes на .rtf или .doc) и помещение его в каталог с аналогичными файлами (как показано в предыдущей главе на примере программы AES Free). В этом случае попытка его просмотра окажется неудачной (по всем внешним признакам это будет обычный файл), и он будет идентифицирован любопытным исследователем как файл, случайно испорченный.

*Анекдот в тему:*

~ ~ ~ ~ ~ ~ ~

*Встреча новых русских.*

*Каждый привел с собой громадину-охранника. И только у одного — щуплый, низкорослый, болезненного вида.*

*— Он у тебя крутой боец?*

*— Да нет, совсем никакой.*

*— Снайпер?*

*— Никогда оружия в руках не держал.*

*— Так зачем ты его за собой таскаешь?*

*Хозяин, поглаживая охранника по лысине:*

*— А он у меня уже четвертый, все его за меня принимают.*

Такой прием защитит вас от любопытного сотрудника, вора, укравшего ноутбук или хакера, проникшего в компьютер через сеть. Меры безопасности, могущие ввести в заблуждение специалистов, имеющих время и некоторую квалификацию (например, изучающих содержимое вашего компьютера после его конфискации), требуют больших усилий.

Существует простой способ прятать зашифрованную информацию от любопытных глаз — использование программ,

применяющих для защиты информации, кроме шифрования стеганографию. Слово «стеганография» в переводе с греческого означает «тайнопись» (steganos — секрет, тайна; graphy — запись). К ней относится огромное множество секретных средств для организации связи или хранения информации. Это невидимые чернила, микрофотоснимки, условное расположение знаков, тайные каналы связи и т. д. В отличие от криптографии, которая защищает суть секретной информации, стеганография скрывает само существование этой информации как таковой.

*Кстати*

*Как я люблю свою прекрасную фигуру, свою узкую талию, свой подтянутый животик. И как я ненавижу слой жира, который все это скрывает.*

*NN*

Компьютерные технологии значительно упростили и усовершенствовали стеганографию (появилось даже новое направление в области защиты информации — компьютерная стеганография).

### *ПОЛЕЗНАЯ ИНФОРМАЦИЯ*

Компьютерная стеганография — сокрытие сообщения или файла в другом сообщении или файле — основана на том, что органы чувств человека не способны различать малые изменения в цвете, изображении или звуке. Это свойство и применяют к данным, несущим избыточную информацию: изменение значений битов, отвечающих за цвет пикселя, не приводящее к заметному изменению цвета, малозаметные искажения в очертаниях букв, звучании музыки или речи.

Файл, который необходимо скрыть, называют *информационным*. Файл, используемый для сокрытия информации, называют *файлом-контейнером*. Объём файла-контейнера должен в восемь–десять раз превышать объём информационного файла. Где можно спрятать информационный файл? Оказывается, практически где угодно.

*Анекдот*
*в тему:*

~ ~ ~ ~ ~ ~

*Следователь:*

*— Расскажите, как было дело?*

*Щуплого вида интеллигент:*

*— Он наступил мне на ногу, а когда я сделал ему замечание, он меня кулаком ударил.*

*Следователь:*

*— А вы?*

*— У меня в руках была газетка, так я не удержался и ударил его по лицу газеткой. Ну и дальше пошло: он меня еще раз кулаком, я его — газеткой, газеткой, газеткой...*

*Следователь:*

*— Откуда же у него такие травмы?*

*— Да я забыл, что у меня в газетке шахтерский ломик был завернут...*


Можно использовать пробелы в документах, аудиофайлы (особенно формата MP3), картинки и фотографии. Самыми рас-

пространенными носителями и стали именно изображения. Например, обычная картинка 640×480 формата BMP позволяет скрыть в себе примерно 300 Кбайт текстовой информации, а размером 1024×768 — до 2 Мбайт. В настоящее время существуют три тесно связанных между собой и имеющих общие корни направления приложения стеганографии: сокрытие данных (сообщений); нанесение на произведение цифровых водяных знаков; введение заголовков. Рассмотрим варианты использования для своих нужд первого направления.

### *НЕОБХОДИМЫЕ НАВЫКИ*

Существуют бесплатные (табл. 4.1) и платные (табл. 4.2) программы, использующие стеганографию для защиты информации.

*Таблица 4.1*

| Программа | Характеристики |
|---|---|
| **Invisible CHAOS**<br>930 Kb<br>http://www.safechaos.com/ic.htm | Очень простая в пользовании программа. Позволяет прятать файлы и целые папки в рисунки (BMP), тексты (TXT), звуки (WAV) и HTML файлы. Использует алгоритм шифрования AES, имеет шредер и архиватор. |
| **4t HIT Mail Privacy LITE**<br>964 Kb<br>http://www.4t-niagara.com/hitmail.html | Очень простая в пользовании программа. Позволяет прятать короткие записки в рисунках формата JPG, GIF, TIFF и BMP. По утверждению разработчиков, шифрует их ключом длиной 128 бит. К сожалению, алгоритм шифрования ни в программе, ни на сайте не указан. |
| **ImageHide**<br>1.1 Mb<br>http://www.dancemammal.com/imagehide.htm | Очень простая в пользовании программа. Позволяет прятать короткие записки в рисунках формата BMP и PNG. Шифрует их по алгоритму RC4. К сожалению, длина ключа ни в программе, ни на сайте не указана. |

*Окончание табл. 4.1*

| Программа | Характеристики |
|---|---|
| **Encrypt Text in Picture**<br>1.95 Mb<br>http://www.acezip.net | Очень простая в пользовании программа. Позволяет скрывать информацию в рисунках формата BMP, JPG и JEPG. Шифрование отсутствует. |
| **SecurEngine Professional**<br>2.76 Mb<br>http://securengine.<br>isecurelabs.com | Неудобная в пользовании программа. Предлагает на выбор 4 алгоритма шифрования: AES, Blowfish, 3DES, GOST. Позволяет шифровать и прятать файлы в рисунках формата BMP, GIF, PNG и в HTML файлах. |
| **wbStego4.3**<br>447 Kb<br>http://wbstego.wbailer.com | Неудобная в пользовании программа. Позволяет скрывать информацию в файлах формата BMP, TXT, HTM и PDF. Шифрование отсутствует. |

*Таблица 4.2*

| Программа | Характеристики |
|---|---|
| **CHAOS Universal**<br>1 Mb<br>$74,95<br>http://www.safechaos.com/<br>cu.htm | Очень простая в пользовании программа. Позволяет прятать файлы и целые папки в рисунки (BMP), тексты (TXT), звуки (WAV) и HTML файлы. Использует алгоритмы шифрования: AES, 3DES, Blowfish, GOST. Имеет шредер и архиватор. |
| **Cloak**<br>7.5 Mb<br>$34,95<br>http://insight-concepts.com | Отлично оформленная, но очень неудобная в пользовании программа. Позволяет прятать файлы в рисунки (BMP, GIF, PNG) и шифровать их с помощью одного из трех алгоритмов (Arcfour, Blowfish или Rijndael). Имеет встроенный шредер и архиватор. |
| **WbStego4**<br>1.07 Mb<br>$20,00<br>http://www.wbailer.com/<br>wbstego | Так же, как и бесплатная версия, весьма неудобна в пользовании. Позволяет скрывать информацию в файлах формата BMP, TXT, HTM и PDF. Шифрование отсутствует. |

*Окончание табл. 4.2*

| Программа | Характеристики |
|---|---|
| **Steganography Premium**<br>2.47 Mb<br>$18,00<br>http://www.clickok.co.uk/steg/index.html | Неудобная в использовании программа. Позволяет скрывать отдельные файлы в рисунках формата BMP, JPG и файлах ZIP или DBF и шифровать их с помощью одного из трех алгоритмов (Arcfour, Blowfish или Rijndael). |
| **Puffer**<br>1.06 Mb<br>$34,95<br>http://www.briggsoft.com/puffer.htm | Не очень удобная в пользовании программа. Позволяет прятать файлы в рисунках формата BMP и PNG. Использует AES алгоритм шифрования. Имеет шредер и архиватор. |
| **Hermetic Stego**<br>1.85 Mb<br>$29,00<br>http://www.hermetic.ch/hst/hst.htm | Неудобная в использовании программа. Позволяет скрывать отдельные файлы в рисунках формата GIF, JPG и PNG. Шифрование отсутствует. |

Программа CHAOS Universal по оформлению и порядку операций шифрования похожа на уже рассмотренную программу AES Free (они и выпущены одной фирмой — Safe Soft Corporation). Поэтому перейдем сразу к рассмотрению режима ее работы, позволяющему прятать зашифрованную информацию в файлах-контейнерах.

Данная программа позволяет скрывать вашу документацию в рисунках, текстах, музыкальных записях и веб-страницах, осуществляет архивирование данных, выполняет шифрование с использованием алгоритмов AES, 3DES, GOST, Blowfish (по вашему выбору).

Открыв окошко «Options» («Настройки»), поставьте галочку в левом верхнем углу возле надписи «Steganography enabled» («Стеганография включена») (рис. 4.1).

Вернувшись в основное окно программы, откройте окно для выбора файла-контейнера (рис. 4.2). В этом окне подберите иллюстрацию, текст или файл, в который вы собираетесь разместить информацию (рис. 4.3).

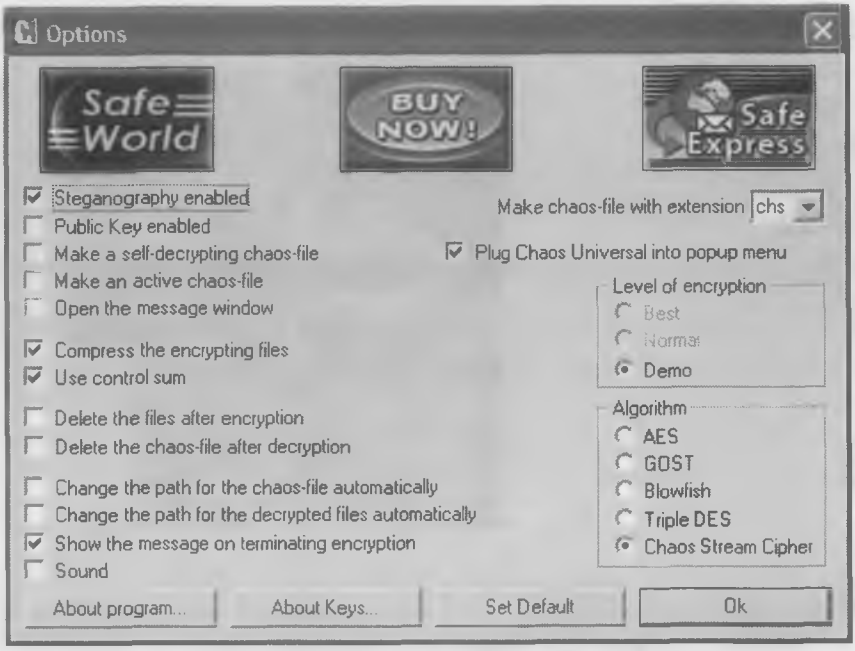



***Рис. 4.1.*** *Включение режима стеганографической защиты*

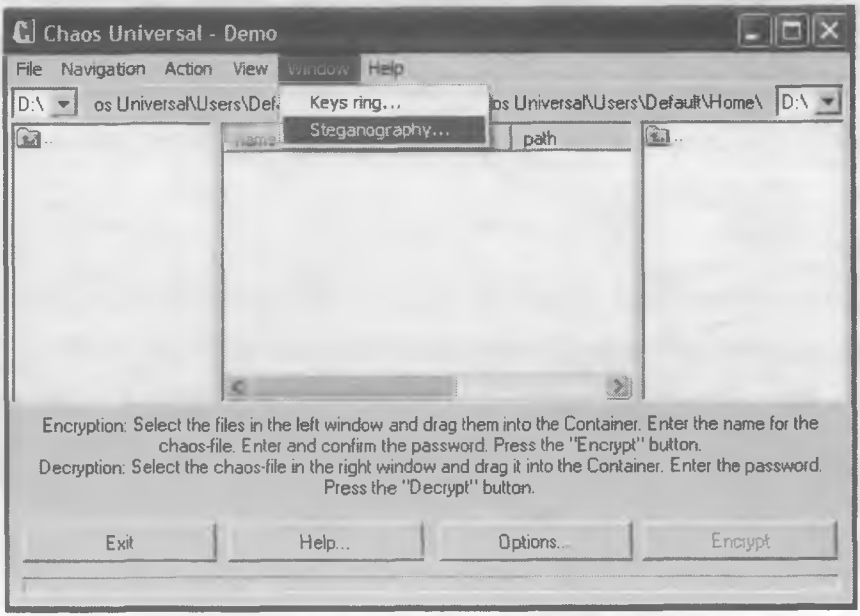



***Рис. 4.2.*** *Переход в окно выбора файла-контейнера*


***Рис. 4.3.*** *Выбор файла-контейнера*

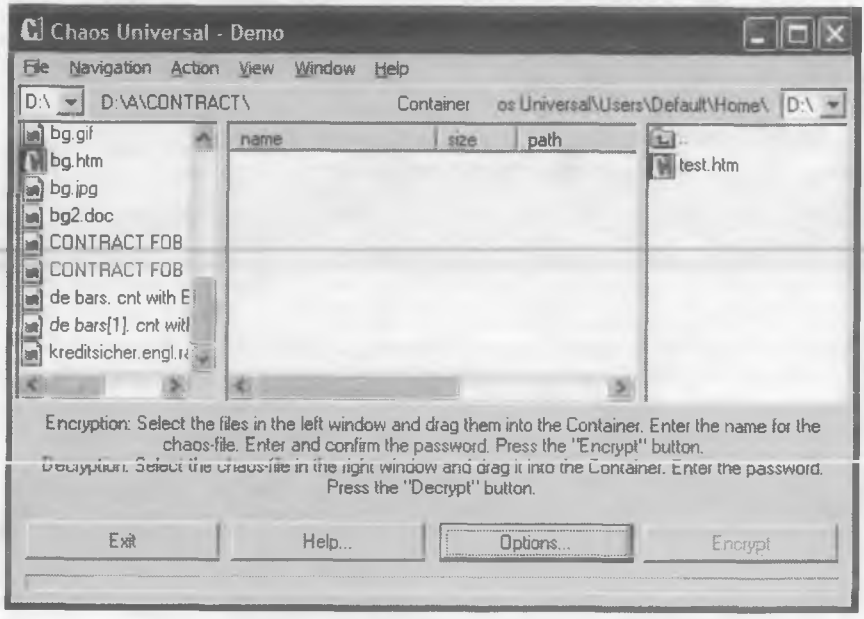



***Рис. 4.4.*** *Информация зашифрована и помещена в файл-контейнер test.htm*

Теперь шифруйте свои файлы абсолютно так же, как это описывалось в предыдущей главе. Зашифрованные файлы (рис. 4.4) имеют то же расширение и внешний вид, что и исходный файл, выбранный вами.

Если программа определит, что изменения во внешнем виде исходного файла (например, сочетание цветов в фотографии) при вводе шифрованной информации будут слишком велики (т.е. файл, который вы хотите зашифровать, слишком большого размера для выбранного вами контейнера и его искажение будет заметным), она предупредит вас об этом и предложит выбрать файл-контейнер большего размера.

Кроме программ, использующих приемы стеганографии по своему прямому назначению (т.е. для сокрытия шифрованных файлов в файлах-контейнерах), имеется несколько программ (табл. 4.3), присоединяющих зашифрованные файлы к файлу-контейнеру (в этом случае нельзя говорить о стеганографии в чистом виде). При реализации такой схемы отсутствуют ограничения на соотношения объемов скрываемой информации и файла, который служит для нее прикрытием.

*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*В ресторане:*

*— У вас в меню котлеты из рябчиков... Что, неужели прямо из рябчиков?*

*— Да, но если честно, то мы туда немного конины добавляем...*

*— Сколько это немного?*

*— Один к одному...*

*— Килограмм рябчиков на килограмм конины?*

*— Нет, один рябчик — один КОНЬ!*

*Таблица 4.3*

| Программа | Характеристики |
|---|---|
| **Chaos Chameleon**<br>760 Kb<br>http://www.safechaos.com/cc.htm | Очень простая в пользовании программа с удобным интерфейсом. Позволяет скрывать как отдельные файлы, так и папки со всем содержимым. Разработчики не скрывают, что файл-контейнер является только «шапкой» для блока зашифрованной информации. Использует AES алгоритм шифрования, имеет шредер. |
| **Steganography**<br>1.02 Mb<br>$24,95<br>http://www.securekit.com | Простая в пользовании программа с удобным интерфейсом. Позволяет скрывать отдельные файлы. К сожалению, форматы файлов, в которых можно скрывать информацию и алгоритм шифрования, не указываются ни на сайте, ни в самой программе Подозрительным является то, что нет ограничений по объему скрываемой информации в файле-контейнере. Создается впечатление, что зашифрованный файл просто добавляется к файлу-контейнеру, а не скрывается в нем. |
| **Stealth Files**<br>1.6 Mb<br>$50,00<br>http://www.froebis.com/english/sf40.shtml | Неудобная в пользовании программа. Позволяет прятать файлы в рисунках формата EXE, DLL, OCX, COM, JPG, GIF, ART, MP3, AVI, WAV, DOC, BMP, WMF. Разработчики утверждают, что скрываемые файлы шифруются. Алгоритм шифрования ни на сайте, ни в программе не указан. Оценок изменения вида файла контейнера после размещения в нем информации из программы провести невозможно. |

Программы этого типа — прекрасная защита от хакеров и подавляющего большинства специалистов, сумевших получить

доступ к содержимому вашего компьютера. Главное — не увлекайтесь, не объединяйте явно небольшой рисунок с огромным по размеру массивом данных.

## Резюме

~ ~ ~ ~ ~

Рассмотренные стеганографические программы позволяют:

- ✓ надежно скрывать существование у вас секретов, хранящихся в компьютере;
- ✓ пересылать в скрытом виде информацию своим партнерам по бизнесу;
- ✓ делать скрытное массовое оповещение клиентов о касающихся их событиях;
- ✓ но не слишком удобны при оперативной работе с информацией, требующей в течение дня многократного обращения к зашифрованным данным. Поэтому такие программы используются в основном при создании скрытых архивов для длительного хранения важной информации.

# Глава 5

## Запас карман не тянет
### (как и где хранить свои секреты)

*Хранить свой секрет — мудро, но ждать, что его будут хранить другие, — глупо.*

***С. Джонсон***

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

**В этой главе:**

- Шифрованные виртуальные диски.
- Создаем шифрованные диски.
- Прячем и ищем шифрованные диски.
- Учимся размещать и извлекать информацию.
- Удаленные хранилища информации.
- Как все это лучше использовать?

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Еще один метод, скрытия ваших секретов — это применение программ, позволяющих создавать на компьютере виртуальные шифрованные диски.

***ПОЛЕЗНАЯ ИНФОРМАЦИЯ***

Представьте себе, что вы ждете гостей. Стол накрыт, торт нарезан. Вы — любитель сладкого. Зная, что гостей будет много и после них вряд ли чего вкусненького останется, вы кладете кусочек торта на блюдце и суете подальше в холодильник.


Разумная предусмотрительность. Аналогичная ситуация. Вы работаете на компьютере, к которому имеют доступ и другие пользователи (сотрудники, родственники, друзья). Вы не хотите, чтобы важная для вас информация была случайно затерта, а личные письма прочитаны. Что делать в этом случае? То же, что и с кусочком торта. Зарезервировать на жестком диске пространство для себя (скажем, в один гигабайт) и защитить доступ к нему паролем. Такое защищенное место называется шифрованным виртуальным диском. Почему шифрованным? У такого диска есть одна интересная особенность, делающая его использование крайне удобным. Информация, заносимая на него, мгновенно, а информация, которая считывается, также мгновенно расшифровывается. Ключи, которыми выполняется шифрование, формируются из пароля, разрешающего доступ к диску. То есть открыли вы своим паролем диск и пользуйтесь им на здоровье сколько угодно как обычным диском. Выключили вы компьютер, диск автоматически отключился, и никто, кроме вас (владельца пароля), подклю-

чить его не может. Такая зарезервированная на жестком диске область называется файлом-контейнером. Операция подключения диска (файла-контейнера) может быть произведена либо вручную, либо автоматически (при загрузке Windows), но в любом случае только после введения вами пароля. На таком диске могут храниться любые файлы данных или программы, операционная система предоставляет возможность работать с ним так же, как с обычным диском. Для постороннего же человека, проникшего в компьютер, контейнер выглядит как обычный файл, а вот узнать, что внутри у него, нельзя, так как вся хранящаяся в нем информация зашифрована. Такой файл-контейнер можно переместить в любую директорию на своем компьютере, переписать на CD или флэшку, а затем открыть и использовать на другом компьютере (на нем должна быть установлена та же программа для работы с шифрованными дисками, которой воспользовались вы). Программы, создающие шифрованные диски, обычно используют те же алгоритмы, что и программы, описанные в первой главе. Поэтому требования к ним (надежный алгоритм, ключ достаточной длины) и к вам (использование хорошего пароля) аналогичны.

### *НЕОБХОДИМЫЕ НАВЫКИ*

Поговорим теперь о самих программах, позволяющих формировать шифрованные диски и работать с ними. В настоящее время существует достаточно большое количество как бесплатных (табл. 5.1), так и платных (табл. 5.2) программ, т.е. выбирать есть из чего. Основные отличия некоторых бесплатных программ: существование ограничений на число используемых алгоритмов, количество создаваемых дисков и их максимальные размеры. В остальном же (качество работы и применяемые алгоритмы) они обычно аналогичны. Если секретов у вас пока немного, вас вполне удовлетворит какая-либо из бесплатных версий (заодно вы привыкнете к ее постоянному использованию и оцените удобства, которые она привносит в вашу работу).

*Таблица 5.1*

| Программа | Характеристики |
|---|---|
| **Able Disk**<br>135 Kb<br>http://www.abensoft.com/disk.htm | Очень простая в пользовании программа. Использует стандартный алгоритм шифрования AES. Позволяет создавать виртуальные диски, невидимые и самой программой без прямого указания пользователем на них. Имеет встроенный шредер для быстрого уничтожения виртуальных дисков, режим автоотключения, возможность самостоятельного выбора комплекта горячих клавиш. |
| **BladeBox Iron Edition**<br>2.3 Mb<br>http://www.liveye.net/bladebox | Удобная и простая в пользовании программа с приятным интерфейсом. Использует стандартный алгоритм шифрования AES. |
| **Dekart Private Disk Light**<br>394 Kb<br>http://www.dekart.com/free_download | Простая в пользовании программа с очень простым интерфейсом. Использует стандартный алгоритм шифрования AES. Внимание! При инсталляции не создает собственной папки, не имеет средств для деинсталляции. |
| **PGP**<br>6,7 Mb<br>http://www.pgpi.org | Достаточно простая в пользовании программа с не очень удобным интерфейсом. Использует алгоритмы шифрования CAST, IDEA, 3DES. Имеет режим автоотключения через заданный промежуток времени. |
| **Cryptainer LE**<br>2.65 Mb<br>http://www.cypherix.co.uk | Достаточно простая в пользовании программа с не очень удобным интерфейсом. Использует алгоритм шифрования Blowfish. В бесплатной версии предельный объем виртуального диска ограничен размером в 25 Mb. |

*Окончание табл. 5.1*

| Программа | Характеристики |
|---|---|
| **TrueCrypt**<br>1,35 Mb<br>http://www.truecrypt.org | Достаточно простая в пользовании программа с не очень удобным интерфейсом. Использует алгоритмы шифрования: AES, 3DES, Blowfish, CAST, Serpent и Twofish. Разработчики оригинально решили проблему формирования скрытых виртуальных дисков. Очень интересно видеть в окне программы указание, что созданный диск невидим. Ситуация напоминает сюжет известного анекдота «Скажи пароль!» |

*Таблица 5.2*

| Программа | Характеристики |
|---|---|
| **Safe Disk Pro**<br>1 Mb<br>$19,95<br>http://www.safechaos.com/sd.htm | Очень простая в пользовании программа. Использует стандартные алгоритмы шифрования: AES, Blowfish, 3DES и GOST. Позволяет камуфлировать виртуальные диски и скрывать их, делая невидимыми для самой программы без прямого указания пользователем на их адрес. Имеет встроенный шредер, режим автоотключения, возможность самостоятельного выбора комплекта горячих клавиш. |
| **CryptoExpert**<br>1.9 Mb<br>$59,95<br>http://www.cryptoexpert.com/std | Простая в пользовании программа с отличным интерфейсом. Использует алгоритмы шифрования: AES, 3DES, Blowfish и CAST. Имеет шредер, режим автоотключения, возможность самостоятельного выбора комплекта горячих клавиш. |

*Продолжение табл. 5.2*

| Программа | Характеристики |
|---|---|
| **Dekart Private Disk**<br>1.07 Mb<br>$45<br>http://www.dekart.com/free_download | Достаточно простая в пользовании программа с хорошим интерфейсом. Использует алгоритм шифрования AES. Имеет шредер и режим автоотключения. |
| **BestCrypt**<br>4,03 Mb<br>$59,95<br>http://www.jetico.com | Достаточно простая в пользовании программа с хорошим интерфейсом. Использует алгоритмы шифрования: Blowfish, Twofish, Rijndael и GOST. Имеет шредер, режим автоотключения, возможность самостоятельного выбора комплекта горячих клавиш. В сети встречаются указания на ее российские корни. |
| **Secure Disk**<br>1.64 Mb<br>$29,95<br>http://www.wekasoft.com/securedisk | Достаточно простая в пользовании программа с не слишком удобным интерфейсом. Использует алгоритм шифрования Blowfish. |
| **Virtual Encrypted Disk**<br>490 Kb<br>30 EUR<br>http://www.susels.com | Достаточно простая в пользовании программа. Используемый алгоритм шифрования ни на сайте, ни в программе не указывается. |
| **StrongDisk Pro**<br>1.9 Mb<br>$80,00<br>http://www.strongdisk.com | Отличная программа с большим количеством дополнительных функций и возможностью камуфляжа создаваемых виртуальных дисков. Использует алгоритмы шифрования: 3DES, IDEA, CAST, RC5, Safer, Blowfish, AES и GOST. Может быть рекомендована опытным пользователям. Разработчики не скрывают своего российского местоположения (PhysTechSoft Ltd). |

*Окончание табл. 5.2*

| Программа | Характеристики |
|---|---|
| **Steganos Safe**<br>16 Mb<br>49,95 EUR<br>http://www.steganos.com | Отлично оформленная программа с очень большим количеством дополнительных функций. Может быть рекомендована очень опытным пользователям. К сожалению, ни на сайте, ни в программе не указаны алгоритмы, которые используются для шифрования информации. Имеет встроенный шредер. |

Able Disk — небольшая программа для создания шифрованных виртуальных дисков объемом до 2 Gb (рис. 5.1). С ними можно работать как с обычными (дисков может создаваться несколько, причем зашифрованных разными паролями; создание нескольких дисков позволяет фактически обходить ограничение на предельный размер диска, — создайте три диска по два гигабайта, вот вам и шестигигабайтный сейф).


***Рис. 5.1.*** *Интерфейс программы Able Disk*

Для создания нового виртуального диска достаточно выбрать в меню пункт «New Disk» («Новый диск») в левом верхнем углу окна (рис. 5.2), ввести желательное место размещения диска и пароль (рис. 5.3), который будет требоваться для доступа к материалам, помещенным на диск.

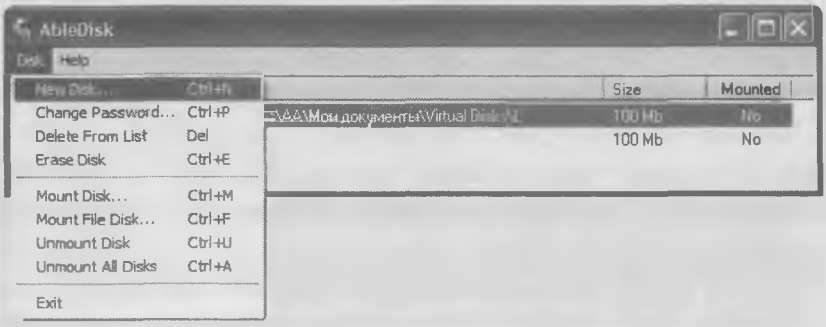



***Рис. 5.2.*** *Создание нового диска*

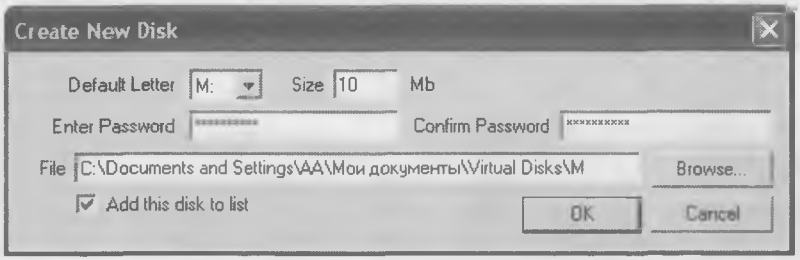



***Рис. 5.3.*** *Выбор характеристик нового диска*

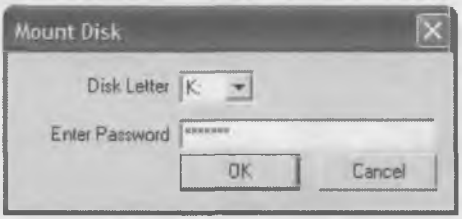



***Рис. 5.4.*** *Ввод пароля при входе в виртуальный диск-контейнер*

Виртуальный диск — это фактически обычный зашифрованный файл-контейнер, помещаемый на жестком диске. В дальнейшем все файлы, отправляемые на виртуальный диск, автоматически шифруются ключом, сформированным из пароля, а просмотр их и перенос на другие диски возможен только при правильном введении этого же пароля (рис. 5.4). После разре-

шения доступа виртуальный диск становится доступен для всех программ Windows (рис. 5.5) на время, необходимое пользователю для работы с ним.

После окончания работы с диском он может быть отключен либо непосредственно из самой программы, либо выключится автоматически сам при завершении работы компьютера. Отключенный диск становится невидимым для средств Windows (рис. 5.6) и для получения доступа к нему необходимо снова ввести правильный пароль.


***Рис. 5.5.*** *Работа с виртуальным диском*

Недостаток большинства программ, создающих скрытые диски, их автоматический запуск при включении компьютера. Не заметить в окне работающей программы наличия скрытых дисков просто нельзя. После этого получение от вас пароля для доступа к виртуальным дискам — дело сравнительно небольшого времени.


***Рис. 5.6.*** *После отключения виртуальный диск становится невидимым для Windows*

## *Анекдот в тему:*

~ ~ ~ ~ ~ ~ ~

*У нового русского спрашивают:*

*— Что вы чаще используете для получения информации: газеты, компьютер, телевизор...?*

*— Утюг.*

Для решения этой проблемы в Able Disk предусмотрена возможность делать диски невидимыми и для самой программы. В этом случае достаточно выбрать скрываемый диск и выбрать пункт меню «Delete from List» («Убрать из списка»). После этого он исчезает из списка дисков, доступных для просмотра. Перевести диск в рабочее состояние теперь можно, только вручную найдя его в своих папках, подтвердив про-

грамме, что это именно он, и введя пароль (рис. 5.7). После этого он станет доступен и для программы, и для средств Windows (рис. 5.8).

*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*Как-то вождь всех народов товарищ Сталин смотрел очередной кинофильм перед выпуском его в массы. После просмотра Сталин раскурил свою трубку, попыхтел и, наконец, изрек:*

*— А что это у главного злодея усы, как у товарища Сталина? Это что, заговор? Товарищ Берия, расстрелять актера, гримера, сценариста и режиссера.*

*— Есть!*

*Насмерть перепуганный режиссер:*

*— А может быть, мы ему просто усы сбреем?*

*— ...Или так.*


***Рис. 5.7.*** *Идентификация невидимого диска и введение пароля*

Такой невидимый виртуальный диск может иметь вид файла с любым расширением и быть спрятан в укромном уголке жесткого диска (главное, чтобы вы сами не забыли, где).

*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*— Скажите, это институт по отработке ориентации ракет в безвоздушном пространстве?*

*— А-а-а!*

*В институте упала телефонная трубка и раздался выстрел. Застрелился начальник третьего отдела. На следующий день куча опавших листьев, под которыми ревели грузовики, переместилась в тайгу. На старом месте только ветер шевелил оставшийся кусок парового отопления.*

*Звонок.*

*— Скажите, пожалуйста, это институт по отработке ориентации ракет в безвоздушном пространстве?*

*— А-а-а! Опять! А-а-а!*

*Ба-бах! Застрелился опытный сотрудник-секретчик, гордость организации.*

*На следующий день вся тайга вместе со снегом переехала в Каракумы.*

*Звонок.*

*— Простите, пожалуйста, это опять я, я вам, наверное, надоел... Это институт по отработке ориентации ракет в безвоздушном пространстве?*

*— Да. Чего тебе?*

*— Надю можно?*

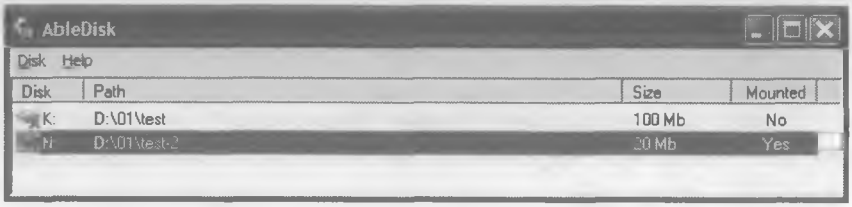



***Рис. 5.8.*** *После идентификации невидимый диск становится доступным*

Еще одно дополнительное достоинство этой программы — наличие «горячих клавиш», позволяющих практически мгновенно уничтожать как зашифрованную информацию, так и саму программу на компьютере (представьте себе ситуацию: неизвестные, но неприятные люди ломятся в дверь, а вам необходимо срочно уничтожить пароли и адреса, записанные на виртуальном диске, да и от самой программы, размещение которой на компьютере предполагает наличие у вас секретов, неплохо было бы успеть избавиться).

### *ИЛЛЮСТРАЦИЯ*

**Джеффри Робинсон. Всемирная прачечная. Альпина бизнес букс. М. 2004.**

*«Ранним утром 1996 года сотрудники ФБР постучали в дверь Джона Мэтьюсона. На следующий день он передал дискеты с данными по переводам средств около 1000 клиентов Guardian по 1600 счетам, осуществлявшимся в течение 14 месяцев. Все клиенты банка, за исключением 73, были американцами. Кроме того, Мэтьюсон передал ФБР свою электронную записную книжку Rolodex, в которой содержались сведения о фактических владельцах счетов...»*

Свидетельством возможного присутствия в компьютере секретной информации является ряд признаков, могущих привлечь внимание заинтересованных лиц и побудить их к тщательному поиску размещенного на жестком диске файла-контейнера.

Рассмотрим эти признаки и варианты их устранения.

- ✓ **Наличие программы для работы с виртуальными дисками.**

Естественным способом демонстрации отсутствия программы для управления виртуальными дисками на компьютере является удаление как ее самой, так и ее инсталляционных файлов. Оно может быть как мнимым, так и реальным. Первый вариант легко осуществить простым переименованием инстал-

ляционного файла и сменой его расширения, либо присоединением этого файла к файлу-контейнеру, обеспечивающему ему внешнее прикрытие.

Второй вариант предусматривает хранение инсталляционного файла программы либо в сети, либо на одном из CD дисков (естественно, среди множества других программ). Всегда существует возможность отслеживания информации, передаваемой на ваш компьютер через Интернет; может также вызывать подозрение наличие у вас специализированных CD с программами для защиты информации. Поэтому скачивать программы для защиты информации рекомендуется либо из нейтральных мест, например компьютерных клубов, либо с сайтов, поддерживающих SSL канал связи с пользователями (например, поместите важные для себя программы в свои же почтовые ящики на Gmail или ячейки Netarhiver и имейте защищенный доступ к ним из любой точки земного шара). Использовать CD лучше всего не специализированные, сконцентрировавшие в себе сливки последних выпусков программ для защиты, а солянку с набором различных утилит, среди которых мелькают и нужные вам программы.

Спрятав инсталляционный файл, можно быть готовым в любой нужный момент без сожаления либо деинсталлировать программу для работы с виртуальными дисками обычным порядком, либо выполнить ту же операцию с помощью нескольких «горячих клавиш», предусмотренных в некоторых из программ.

✓ **Наличие на жестком диске крупных файлов, не открывающихся имеющимися в компьютере программами, что позволяет идентифицировать такие файлы как предполагаемые файлы-контейнеры.**

В этом случае существует несколько способов сокрытия существования виртуальных дисков в компьютере.

**А.** Самое очевидное решение при появлении опасности — удаление файла-контейнера. Такое поведение вполне разумное

при наличии резервных копий скрываемой информации, хранящихся в надежном месте. Однако при традиционном удалении файла сама информация, находившаяся в нем, на жестком диске остается. Ее можно легко восстановить, определить, что восстановленный файл — виртуальный диск, и попросить пользователя сообщить пароль для работы с ним.

Это означает, что необходимо также физически удалить эту информацию с жесткого диска. Существуют специальные программы — шредеры, позволяющие затереть информацию в файлах перед их удалением. Однако они не способны справиться с задачей затирания файла размером в несколько гигабайт за считанные секунды. Поэтому при уничтожении виртуальных дисков некоторыми разработчиками применяется следующий прием: для выработки ключа шифрования используется не только пароль, вводимый пользователем, но и модификатор ключа шифрования размером 128 бит. При необходимости срочного предотвращения доступа к виртуальному диску нажатие «горячих клавиш» приводит к затиранию встроенным шредером в первую очередь именно этого модификатора, после чего файл-контейнер удаляется обычным образом. Без модификатора ключа, который был надежно уничтожен, даже при наличии правильного пароля восстановить зашифрованную информацию оказывается невозможно (этот прием используется при затирании файлов шредером описанной выше программы).

**Б.** Другое решение — сокрытие наличия на диске файлов-контейнеров методами стеганографии, т.е. размещение файла-контейнера, скажем, в серии изображений, сборнике музыкальных записей или в аудиокниге.

*Анекдот*
*в тему:*

~ ~ ~ ~ ~ ~ ~

*Умирает старый еврей, созывает свою родню и говорит:*
*— Я зарыл клад...*

*— Где?*
*— В земле...*
*— Точнее, точнее!*
*— Земля — это третья планета от Солнца.*

Учитывая, например, что изображение в формате BMP может практически без потери качества содержать до трети своего объема дополнительной информации, необходимое для хранения файла-контейнера дисковое пространство превышает его размеры в этом случае примерно в три раза.

Такой способ хорош для использования в домашних условиях, когда количество скрываемой информации сравнительно невелико (в этом случае ее можно просто ввести в рисунок или аудиофайл все той же стеганографической программой), однако наличие репродукций галерей Эрмитажа с высоким качеством разрешения на рабочем компьютере может вызвать вполне законное подозрение.

**С.** Третий вариант — камуфляж файла-контейнера его модификацией и размещением среди большого количества других подобных файлов. Существует множество различных форматов данных. Можно дать файлу-контейнеру имя с расширением, скажем, DOC или XLS, а затем разместить его среди подобных файлов (удобным местечком является, например, системный каталог Windows). При попытке открыть такой файл он будет казаться просто поврежденным. Однако этой меры зачастую бывает недостаточно. При просмотре файлов стандартных форматов с помощью простых текстовых редакторов (таких, как блокнот или редактор файлового менеджера Far) легко обнаружить, что большинство из них имеют стандартные «заголовки», находящиеся в начале файла. Отсутствие такого заголовка и может привлечь внимание к скрываемому файлу-контейнеру.

✓ **Наличие в имеющихся на диске папках файлов, дата создания которых существенно отличается от дат создания самой папки и прочих файлов, помещенных в ней.**

Обычно работа с файлами из той или иной папки выполняется в течение какого-то определенного времени, и файлы из

нее имеют сравнительно близкие даты создания или модификации. Просмотр содержимого компьютера позволяет легко выделить файлы, время модификации которых не характерно для их окружения, и идентифицировать их как потенциально интересные для изучения. Избежать такой идентификации можно, переустановив при записи модифицированного файла время в компьютере.

Анализ перечисленных выше признаков хранения секретной информации в файлах-контейнерах и средств их камуфляжа позволил сформулировать основные требования, которые желательно учитывать при выборе программам, формирующих виртуальные диски:

1. Созданный виртуальный диск должен представлять собой набор файлов-контейнеров случайного размера.
2. Файл-контейнер не должен иметь собственного заголовка, позволяющего его идентифицировать.
3. Должна быть обеспечена возможность снабжения файлов-контейнеров стандартными заголовками файлов других форматов.
4. Должна быть обеспечена возможность установки искусственных дат создания, модификации и времени последнего доступа к файлу-контейнеру.
5. Вся дополнительная информация, необходимая для работы с виртуальным диском, должна быть зашифрована паролем пользователя.

Кроме вышеперечисленных приемов может быть полезным введение в программы для работы с виртуальными дисками режима отсроченного подтверждения пароля (при отсутствии правильно введенного пароля в течение определенного времени после загрузки системы производится автоматическое удаление заданных виртуальных дисков и самой программы). Пароль должен вводиться пользователем по собственной инициативе, а не по запросу программы. Эта функция крайне необходима при существовании угрозы потери физического доступа к компьютеру с конфиденциальной информацией.

Программы, формирующие виртуальные диски и позволяющие хранить на них информацию в зашифрованном виде, отлично справятся с ее защитой как при угрозе ее случайной утечки (кража или потеря ноутбука, несанкционированный доступ к компьютеру случайного человека и т.п.), так и при серьезном изучении вашего компьютера заинтересованными лицами. Однако зная о возможном интересе к вашим файлам организаций, имеющих значительные финансовые и интеллектуальные ресурсы, лучше воспользоваться таким приемом, как удаленное хранение архивов. Рассмотрим, зачем нужны такие «сложности».

Вы зашифровали и спрятали свою конфиденциальную информацию. Казалось бы, теперь можно вздохнуть спокойно. Вы защитили свои секреты от постороннего взгляда. Остается одно: обеспечить возможность собственного свободного пользования ими. Рассмотрим сначала, как вы можете потерять доступ к собственной информации.

Шифрованные файлы хранят обычно либо на внешних носителях (дискеты, CD, DVD, флэшки, магнитооптические диски и т.п.), либо на жестком диске компьютера. В первом случае вы можете потерять свою информацию в результате:

- ✓ потери носителя;
- ✓ кражи носителя;
- ✓ естественной порчи носителя;
- ✓ случайного разрушения носителя;
- ✓ возникновения случайных или преднамеренных искажений в файле, содержащем зашифрованную информацию, что препятствует его расшифровке;
- ✓ присутствия вирусов, повреждающих вашу информацию при просмотре в компьютере, в который помещается носитель для просмотра;
- ✓ потери доступа к компьютеру с программой, обеспечивающей возможность расшифровки информации;
- ✓ утраты доступа к ключу, позволяющему расшифровать информацию;

- ✓ утраты доступа к программе, обеспечивающей расшифровку информации.

Во втором случае к вышеперечисленным причинам добавляются возможность:

- ✓ кражи компьютера;
- ✓ разрушения компьютера (например, при пожаре);
- ✓ естественной порчи жесткого диска;
- ✓ повреждения или удаления зашифрованной информации при включении компьютера посторонними лицами во время вашего отсутствия;
- ✓ повреждения или удаления зашифрованной информации при несанкционированном доступе хакера к содержимому вашего компьютера во время вашей работы в сети;
- ✓ случайного повреждения или удаления зашифрованной информации при вашей работе на компьютере.

На основании анализа перечня вышеперечисленных причин потери информации сформулированы требования к форме хранения конфиденциальной информации, обеспечивающие возможность свободного доступа к ней даже при одновременном действии совокупности ряда негативных факторов:

1. Зашифрованный файл должен быть сохранен при случайных или преднамеренных попытках его уничтожения с помощью программных или физических средств воздействия.
2. Должна быть обеспечена возможность расшифровки информации без обязательного применения программных средств, использованных при ее шифровании.
3. Зашифрованный файл не должен, видимо, отличаться от других файлов, среди которых он помещен.

Рассмотрим практические методы преобразования и хранения информации, удовлетворяющие этим требованиям.

Предотвратить потерю важных файлов при неконтролируемом воздействии на носители информации (компьютер или внешние носители) можно путем размещения достаточного числа резервных копий в местах, недоступных одновременному проявлению совокупности неблагоприятных факторов. Напри-

мер, если созданный шифрованный файл хранится на домашнем компьютере, желательно иметь его копию: на внешнем носителе, хранящемся отдельно от компьютера (это предотвратит потерю информации при заражении компьютера вирусами); в рабочем компьютере или на внешнем носителе, хранящемся в офисе (это предотвратит потерю информации при пожаре или краже имущества); на внешнем носителе, хранящемся в депозитной ячейке банка (эта мера защитит, например, при конфискации имущества); на компьютере, не имеющем к вам никакого отношения (всегда можно сбросить важный для вас файл на компьютер приятеля, пока он готовит кофе). Эти приемы дают вполне достаточную степень сохранения информации при малоподвижном образе жизни ее владельца.

Необходимость перемещений (зачастую вынужденных) на дальние расстояния значительно увеличивает вероятность потери информации, записанной на взятом в дорогу материальном носителе (кражи в аэропортах, потеря багажа, слишком придирчивый таможенный досмотр и т.п.). Избежать таких потерь можно размещением зашифрованной информации в сети (в простейшем случае, например, отправкой ее себе же на бесплатные почтовые ящики, открытые в разных странах, при большем опыте работы в сети, — загрузкой на собственные сайты, имеющие нейтральное содержание (например, сайт выпускников ПТУ № 17 города Урюпинска и т.п.) и не вызывающие интереса прочих пользователей Интернета.

*Анекдот*
*в тему:*

~ ~ ~ ~ ~ ~

*Требуется опытный хакер.*
*Резюме оставлять на рабочем столе нашего сервера.*

Кроме утраты самой информации, потерять доступ к ее содержимому можно при сочетании таких неблагоприятных факторов, как одновременное прекращение существования фирмы,

выпустившей программный продукт, которым зашифрована, информация, и случайное (или преднамеренное) уничтожение этой программы на вашем компьютере. Этого случая можно избежать, используя при шифровании программы, позволяющие создавать самораспаковывающиеся зашифрованные файлы (пример описан в первой главе). Превратив свою конфиденциальную информацию в файл такого типа, вы можете всегда получить доступ к ней вне зависимости от внешних обстоятельств.

Размещение секретных файлов на компьютерах родственных фирм или на вашем сайте — хороший трюк, позволяющий сохранить ее при форсмажорных обстоятельствах, но… Вспомните дело «Юкоса». Компьютеры для изучения их содержимого изымались даже из школ, спонсировавшихся фирмой. Ее сетевые контакты тоже наверняка изучались досконально (провайдер хранит информацию о вашей деятельности в сети от трех до пяти лет).

*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*Путин он-лайн:*

*— Только что через Интернет пришел хороший вопрос:*

*«А не западло тебе, Вова, отвечать на анонимные вопросы по Интернету?»*

*Отвечаю задавшему этот вопрос обладателю IP (такой-то), хост (такой-то), провайдер (такой-то) Иванову Сергею Васильевичу, проживающему в городе Оренбурге, ул. Пирогова, дом 13, квартира 2.*

*НЕ ЗАПАДЛО!*

Как быть? Оказывается, сфера услуг для бизнесменов предусматривает и этот случай. В сети существуют электронные архивы (табл. 5.3), которые всего за несколько долларов в месяц

будут хранить вашу конфиденциальную информацию (естественно, перед помещением в архив не забудьте ее зашифровать) (рис. 5.9).

*Таблица 5.3*

| Название системы | Объем места | Стоимость (в год) | Адрес |
|---|---|---|---|
| Net Depositary | 100 Mb | $29,55 | http://www.netarchiver.com |
| StrongFolder | 20 Mb | $120 | http://www.dekart.com/home |
| NetDocuments | 1 Gb | $115,2 | http://www.netdocuments.com/ |
| Xdrive | 5 Gb | $120 | http://www.xdrive.com |
| InfinityDrive | 6 Gb | $180 | http://www.infinitydrive.net |


***Рис. 5.9.*** *Вход в электронный депозитарий*

В арендованной ячейке вы можете раскладывать информацию по созданным вами же папкам (рис. 5.10), подгружать новые файлы и уничтожать их, делать краткие комментарии. В общем, все то, что вы делаете на диске своего компьютера.

Передача файлов в ячейку осуществляется по защищенному каналу связи, использующему SSL протокол, который автоматически подключается при вашем входе в депозитарий. Если же вы будете помещать секретные (зашифрованные!) файлы в де-

позитную ячейку не со своего компьютера, а из интернет-кафе или компьютерного клуба, отследить ваши действия и использовать информацию о них против вас будет невозможно.


***Рис. 5.10.*** *Ячейка электронного депозитария*

Государственные службы и секретные агентства имеют доступ к новейшей криптографической технологии. Такой же технологией пользуются террористы, поставщики оружия и наркотиков. Ее имеют нефтяные компании и другие корпорации-гиганты. Обычные же люди и общественные организации в своем большинстве до сих пор не имели доступа к криптографическим технологиям высокого уровня. Времена изменились, теперь они доступны и вам.

## Запомните

*Старайся быть умнее других и старайся, чтобы они этого не заметили.*

***Филипп Честерфилд,***
***английский дипломат***

## Резюме

Рассмотренные программы позволяют скрывать существование у вас секретов, хранящихся в компьютере, но не слишком удобны в путешествиях, так как воспользоваться шифрованным диском можно, только имея уже установленную программу для работы с ним (но ведь далеко не всякий гостиничный или клубный компьютер позволит вам проинсталлировать привезенную с собой или скачанную из сети программку). Поэтому традиционно программы для работы с шифрованными дисками используют:

- ✓ когда вы часто работаете дома, а на вашем домашнем и рабочем компьютерах установлены идентичные программы;
- ✓ когда существует угроза доступа к вашему компьютеру со стороны лиц, могущих принудить вас тем или иным способом сообщить пароль для получения доступа к зашифрованной информации;
- ✓ когда существует угроза внезапного появления лиц, заинтересованных в получении от вас секретной информации, хранящейся в компьютере.

# Глава 6

## Уходя, гасите свет

### (как спрятать следы своей работы)

*Лучшее время сделать что-либо —*
*время между вчера и завтра.*
***«Принцип оптимального***
***промежутка»***

**В этой главе:**

- Почему забирают компьютеры.
- Как работают шредеры.
- Учимся уничтожать файлы.
- Учимся уничтожать следы своей работы.
- Напоминание.

С завидным постоянством любой современный конфликт сопровождается изъятием у оказавшейся более слабой стороны компьютеров. Просто наваждение какое-то. Взгляните только на заголовки статей в сети за любой день прошедшей недели (когда бы вы ни читали эти строки).

***ИЛЛЮСТРАЦИИ:***

***http://accoona.ru/news/index.php?id=4631***

*Генпрокуратура изъяла компьютеры у главного юриста «ЮКОСа»*

***http://831.ru/0-40-7154-0/20050314-20050314/1292240-120-0***

*У «Трансинкора» изъяты компьютеры*

***http://www.rosbalt.ru/2004/07/28/171695.html***

*В «Центральном московском депозитарии» изъяты компьютеры и документы*

***http://www.moscow2000.com/news/view2.asp?Id=11175&IdType=5***

*У подозреваемого по «делу Чубайса» изъяли компьютер и записи*

***http://07nov2003.interport.ru/world/vesti.html***

*В Латвии полиция изъяла компьютеры у крупнейшей русскоязычной газеты*

***http://www.1917.com/index.html***

*Малайзия: из штаб-квартиры сайта оппозиции изъяты компьютеры*

***http://www.ntann.ru/?id=62038***

*Сотрудники УФСБ изъяли компьютер фирмы «Комплексная безопасность» с «убийственными файлами, которые поставят крест на политической карьере Савельева»*

***http://krsk.kp.ru/news/print/98830***

*Московская прокуратура проводит обыск и изымает компьютеры в офисе интернет-издания «Грани.ру»*

Казалось бы, наверняка были более ценные вещи в офисах, но забирают именно компьютеры. Чем же они так приглянулись победителям? Ведь с уверенностью можно сказать, что это были не самые последние модели. Присмотримся же к этой компьютерофилии следственных органов поближе.

## *ПОЛЕЗНАЯ ИНФОРМАЦИЯ*

Сохранение секретности информации зачастую сталкивается с одной проблемой. Компьютер обычно не уничтожает сразу удаляемые вами документы, а ограничивается тем, что скрывает их имена (при удалении файла средствами операционной системы всего лишь помечается место, ранее занимаемое файлом, как свободное, а удаляется только часть заголовка файла), физически же файл продолжает существовать, пока не будут

перезаписаны данные в занимаемых им секторах диска. Огромные объемы памяти современных машин гарантируют, что такая запись произойдет очень и очень нескоро.

### Запомните ~~~~~~~~~~~~~

*Народная мудрость: чем больше диск, тем больше риск.*

Это позволяет с помощью специальных программ восстанавливать вроде бы уничтоженную информацию и получать доступ к документам, о которых их авторы уже давным-давно забыли. Например, написали вы несколько черновиков, составили итоговый документ, потом стерли черновики (и даже не забыли удалить их из корзины). Документ вы аккуратно зашифровали и успокоились. А напрасно. Черновики-то (пусть и невидимые для вас) на жестком диске остались. Это похоже на тот случай, когда ненужные секретные документы выбрасываются в мусорную корзину вместо того, чтобы отправиться в шредер.

### Анекдот в тему:

~~~~~~

*Распоряжение босса:*

*— Все ненужные бумаги уничтожить, но сначала сделать копии!*

Если компьютер попадет в чужие руки (или кто-либо грамотно скопирует его содержимое), просмотр черновиков даст почти полную информацию о ваших интересах, контрактах и планах. Даже когда вы пишете исходное сообщение без всяких черновиков с использованием текстового редактора, программа создает на диске множество промежуточных временных файлов. Эти временные файлы обычно удаляются при закрытии редактора, но фрагменты того текста, который вы писали, все равно остаются
~~~~~~

где-то на диске. Единственный способ предотвратить возможность восстановления написанного текста — создать новую запись на том месте диска, которое занимали удаленные файлы. Как быть? Не от руки же писать, сжигая пометки?

*Анекдот в тему:*

~ ~ ~ ~ ~ ~ ~

*Новый русский подъезжает к своему офису, где час назад взорвалась бомба. Все оцеплено, пожарные суетятся, ментов полно, дым валит из окон. Мимо проносят на носилках окровавленного охранника. Он говорит:*

*— Шеф, у вас большое горе! Когда рвануло, в офисе ваша жена была... Погибла...*

*— Это все фигня! А бухгалтер, бухгалтер где??!*

Так вот, для полного уничтожения электронной документации и устранения следов деятельности на компьютере и применяют программы-шредеры, многократно записывающие поверх уничтожаемой информации наборы случайных чисел.

### *НЕОБХОДИМЫЕ НАВЫКИ*

В некоторых программах для шифрования информации (в частности, и в тех, которые мы рассматривали в качестве образцов в предыдущих главах) такие шредеры уже встроены, что позволяет уничтожать файлы, которые шифруются автоматически.

*Анекдот в тему:*

~ ~ ~ ~ ~ ~ ~

*В Голливуде один режиссер для сцены сражения пригласил десятитысячную массовку.*

*— Вы разорите меня! — стал кричать на него продюсер.*

*— Не беспокойтесь. Я приказал во время съемок стрелять настоящими снарядами.*

Это удобно при работе с законченными документами, но для уничтожения черновиков нужно либо не забывать запускать шифровальную программу и применять ее в режиме шредера, либо использовать специализированную программу-шредер (список наиболее популярных бесплатных программ приведен в табл. 6.1, а платных — в табл. 6.2).

*Таблица 6.1*

| Программа | Характеристики |
|---|---|
| **CHAOS Shredder**<br>259 Kb<br>http://www.safechaos.com/cs.htm | Очень простая в пользовании программа. Позволяет вычищать практически все мыслимые места появления временных файлов. Особенно удобна при удалении файлов и папок, выбираемых самим пользователем. |
| **12Ghosts Wash**<br>1.49 Mb<br>http://www.12ghosts.com | Отличная программа для опытного пользователя. Позволяет вычищать практически все мыслимые места появления временных файлов. К недостаткам можно отнести только некоторые неудобства при удалении файлов, выбираемых самим пользователем. |

*Окончание табл. 6.1*

| Программа | Характеристики |
|---|---|
| **Eraser**<br>751 Kb<br>http://www.tolvanen.com/eraser | Хорошая программа для опытного пользователя. Позволяет удалять временные файлы. К недостаткам можно отнести неудобства при удалении файлов, выбираемых самим пользователем. |
| **HandyBits File Shredder**<br>1,6 Mb<br>http://www.handybits.com | Очень простая, но не слишком удобная программа. Позволяет удалять отдельные файлы. |

*Таблица 6.2*

| Программа | Характеристики |
|---|---|
| **Privacy Eraser Pro**<br>1.92 Mb<br>$29,95<br>http://www.privacyeraser.com | Отлично оформленный шредер с подробным перечнем программ, временные файлы которых необходимо удалять. Так как эти перечни полностью попадают в разделы некоторых бесплатных программ, дешевле и быстрее воспользоваться ими. |
| **ShredIt**<br>1.17 Mb<br>$19,95<br>http://www.mireth.com | Простая, но неудобная в пользовании программа. Позволяет удалять отдельные файлы, выбранные пользователем. |
| **Eugene Shredder**<br>680 Kb<br>$29,95<br>http://www.eugenesoft.com/EugeneShredder.php | Неудобная в пользовании программа. Позволяет удалять отдельные файлы, выбранные пользователем. |
| **DriveScrubber**<br>736 Kb<br>$29,95<br>http://www.iolo.com | Очень неудобная программа, словно сделанная для большого любителя поморочить себе голову за свой счет. Но если у вас на кредитке есть лишние деньги... |

Программа CHAOS Shredder, как и прочие, устанавливает файлам случайные дату и время модификации перед их удалением, затем уничтожает файлы и многократно записывает на этом же участке жесткого диска белый шум. Таким образом обеспечивается секретность удаляемой информации. Использовать эту программу крайне просто. Вы должны перетащить файлы и папки, подлежащие уничтожению, из левого окошка в правое и нажать кнопку «Erase» («Стереть»). Файлы исчезнут из правого окошка и из вашего компьютера (рис. 6.1). Поверх их будет несколько раз записан и стерт набор случайных чисел. Теперь, воспользовавшись какой-либо программой для восстановления информации на диске, заинтересованное лицо сможет добраться только до этих цифр.

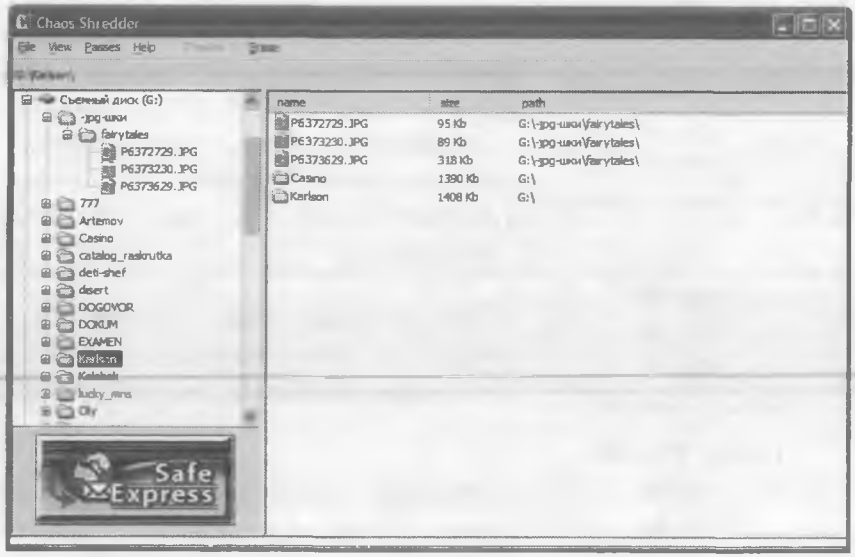



***Рис. 6.1.*** *Интерфейс программы CHAOS Shredder*

Сколько раз нужно перезаполнить числовым мусором то место диска, на котором были ваши документы? В принципе достаточно одного, но при желании это число можно увеличить. Открыв выпадающий список «Passes» (рис. 6.2), вы сможете ре-

гулировать количество циклов перезаписи данных случайными числами, а из списка «View» (рис. 6.3) управлять порядком размещения программы в контекстном меню операционной системы и формой представления каталогов файлов.

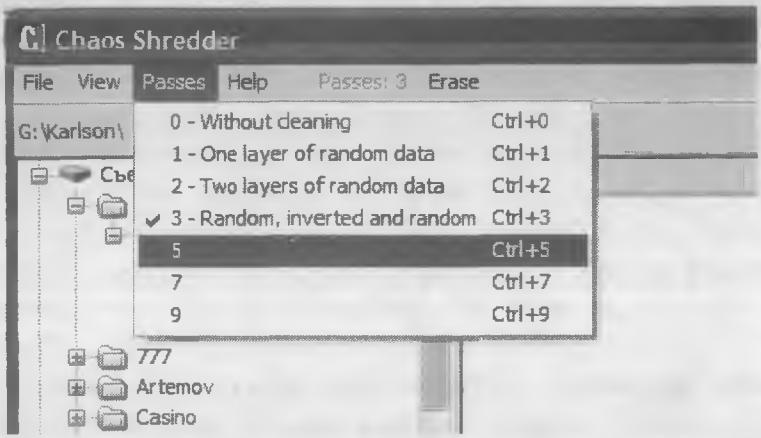



***Рис. 6.2.*** *Установка числа циклов «очистка/заполнение мусором»*

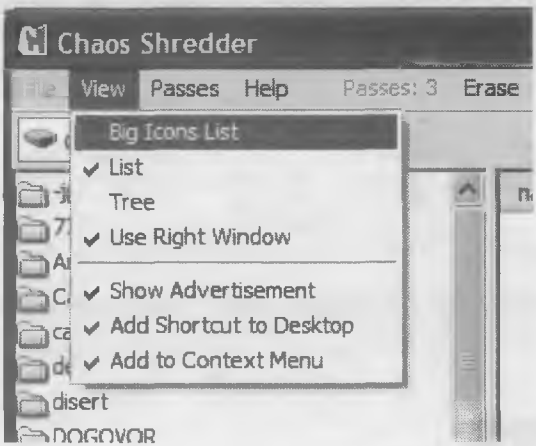



***Рис. 6.3.*** *Настройки программы CHAOS Shredder*

Многие программы (текстовые редакторы, например) создают временные файлы, заголовки которых они удаляют после

окончания работы с документами, не уничтожая на диске содержимое самих файлов. При этом часть конфиденциальной информации остается записанной на диске и становится в критической ситуации доступной специалистам, а вы об этом даже не подозреваете. Вот тут вам и поможет специализированный шредер. Когда в конце рабочего дня вы переносите в правое окошко корзину, каталоги с временными файлами и разрешаете шредеру «протереть» сами диски (рис. 6.4), он уничтожит не только остатки временных файлов в отведенных для них местах, но и почистит все свободное пространство на жестких дисках. Что это дает? Вам не нужно вспоминать. Следы каких файлов могли сохраниться в компьютере, — удаляя все подряд при зачистке свободного пространства жестких дисков, шредер уничтожает полностью содержимое любых остатков, записывает и вытирает несколько раз на их месте случайные числа, т.е. выполняет обязанности хорошего дворника без необходимости регулярного обращения к нему во время работы.

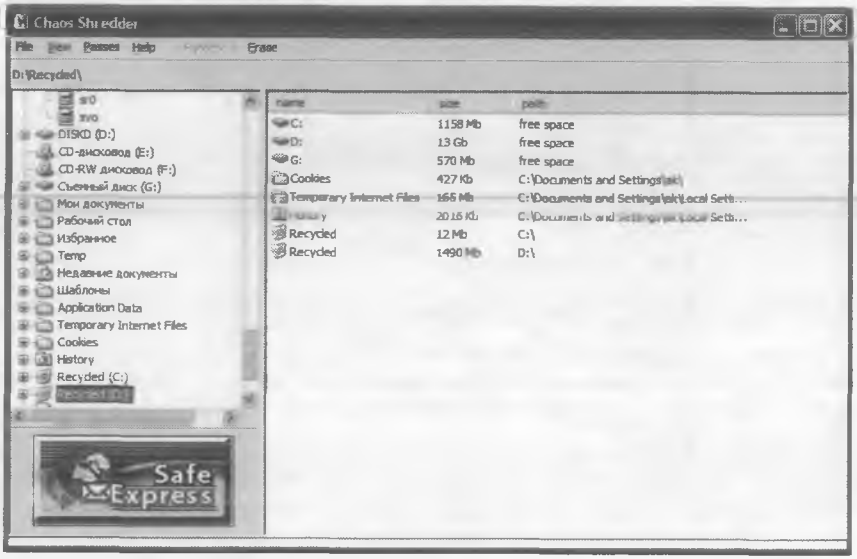



***Рис. 6.4.*** *Очистка дисков с помощью программы CHAOS Shredder*

## Резюме

~ ~ ~ ~ ~

Рассмотренные программы позволяют удалять следы своей работы на компьютере. Какую из них вы выберете, дело ваше, лишь бы выбрали, установили, научились и НЕ ЗАБЫВАЛИ пользоваться.

## Запомните ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

*Человек, которому повезло, — это человек, который делал то, что другие только собирались сделать*

# Глава 7

## Кто стучится в дверь ко мне?
### (как вступать в контакт с внешним миром)

*Открытыми картами лучше всего*
*играть при закрытых дверях.*

***Януш Ковальчик***

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

**В этой главе:**

- Трудности первого знакомства.
- Что такое асимметричное шифрование.
- Чем хорош открытый ключ.
- Учимся знакомиться.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Первое знакомство... Пусть даже не очное, а заочное. Вы пишете по электронной почте письмо Большому Боссу с рационализаторским предложением о методах экономии скрепок в конторе; вы посылаете в банк весть о том, что намерены разместить в нем свои сэкономленные на сигаретах и успешно припрятанные от жены активы; вы связываетесь с риэлторской конторой в Ницце и извещаете ее о желании поменять свою двухкомнатную «хрущевку» в Наро-Фоминске на симпатичный домик вблизи Марселя. Почти возможные (правда, с некоторыми поправками) ситуации. При этом вам совсем не хочется делиться идеей изобретения с другими сотрудниками и непосредственным начальником, деньгами — с налоговиками, а информацией о том, что вы можете себе позволить содержать виллу на Лазурном берегу, — с бандитами. Всегда существовала проблема защиты конфиденциальности контактов, обусловленная необходимостью согласования между сторонами ис-

пользуемых средств связи, паролей, методов шифрования информации, навыков сторон в этом самом шифровании. Эта проблема разрешалась обычно только при личных встречах сторон или при наличии надежных посредников, т.е. решение ее было доступно лишь государственным чиновникам или весьма состоятельным согражданам.

*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*Агент ФСБ Петров приехал из Америки. Ну, его расспрашивают, как там дела, как остальные агенты живут.*

*Петров:*

*— Вы специальному агенту Иванову давали задание взломать компьютер Пентагона?!*

*База:*

*— Ну да, давали.*

*Петров:*

*— Ну, так, он просил передать вам, что уже две недели шифровки пишет, а вы все не отвечаете! Пошлите ему, наконец, крестовую отвертку!*

Сейчас все изменилось. Интернет сделал доступной связь, а асимметричные алгоритмы шифрования — ее защиту. Но если Интернет уже стал привычным инструментом, то слова «асимметричные алгоритмы шифрования» для большинства бизнесменов пока еще звучат тарабарщиной.

### *ПОЛЕЗНАЯ ИНФОРМАЦИЯ*

Как бы ни были надежны криптографические системы с симметричным алгоритмом шифрования (описанные в первой главе), они имеют одно слабое место при практической реализации — проблему передачи пароля (ключа). Чтобы был возможен обмен конфиденциальной информацией между двумя сторонами, кто-то первым должен выбрать пароль (сформировать ключ) для шифрования, а затем каким-то образом в конфиденциальном по-

рядке передать его другой стороне. В общем, получается замкнутый круг: для передачи пароля, позволяющего выполнять шифрование при переписке требуется, использование какой-то другой криптосистемы или секретного канала связи. То есть симметричные методы шифрования удобны, когда заранее определен круг лиц, участвующих в обмене информацией, подлежащей шифрованию и дешифрованию, установлены протоколы шифрования и согласованы используемые пароли.

*Анекдот в тему:*

~ ~ ~ ~ ~ ~ ~

*Как-то попал новый русский (НР) на «Поле Чудес». И выпал ему сектор «приз». Выносят в студию черный ящик, и Якубович начинает торговаться.*

*— Не хочу я ни денег, ни приза, — говорит НР, — я лучше в микрофон свистну. Берет НР микрофон и свистит.*

*— Вы только что просвистели ВАЗ-2110! — объявляет ведущий и вынимает из ящика ключи от автомобиля.*

*— А на кой мне твой драндулет, — говорит НР, — я вот вчера поспорил с Вованом на 600-й «мерс», что на всю страну свистну.*

Существуют алгоритмы работы с информацией, использующие различные ключи для ее шифрования и расшифрования. Эта идея предложена в 1976 г. американскими специалистами по вычислительным наукам У. Диффи и М. Хеллманом и стала началом современного периода в развитии криптографии. Появилась возможность реализации нового принципа организации засекреченной связи без предварительного снабжения абонентов ключами (помните, в случае симметричного шифрования обе стороны должны были знать пароль?).

Общие принципы работы асимметричных алгоритмов:

- ✓ участник информационного обмена генерирует пару ключей. При этом данные, зашифрованные одним из ключей,

могут быть расшифрованы только другим ключом. Один из этих ключей является открытым (общедоступным), другой — закрытым (секретным). Секретный ключ участник хранит у себя, а открытый распространяет всем желающим отправлять ему шифрованные сообщения. Открытый ключ — это функция, при помощи которой отправитель может зашифровать свое сообщение, но ни он сам, ни кто-либо другой не может расшифровать это сообщение, используя открытый ключ. Для расшифрования сообщения (т.е. осуществления обратной операции — вычисления значения аргумента по значению функции) необходимо знать некоторый параметр указанной функции, который, по сути, и является закрытым ключом;

- ✓ отправитель сообщения шифрует информацию открытым ключом и передает ее получателю по открытым каналам связи;
- ✓ получатель расшифровывает сообщение, используя свой закрытый ключ.

То есть асимметричные алгоритмы шифрования позволяют получателю расшифровывать информацию, получаемую им от любого количества отправителей. Представьте себе, например, что у вас есть ключ и неограниченное количество красивых висячих замочков. Вы раздаете открытые замочки всем желающим. Теперь каждый из них может написать вам письмо, положить в шкатулку, закрыть ее и отправить вам. Замочек устроен так, что открыть ее может только ваш ключ и никакой другой. Кроме того, даже тот, кто закрыл замочек, уже не сможет больше открыть его, так как не имеет ключа. Замочков множество, но ключ только один, и он у вас! Вот такие «замочки» и есть аналогия открытых ключей. С их помощью можно зашифровать информацию, но расшифровать уже нельзя. Для расшифровки и требуется секретный ключ, владельцем которого являетесь вы. Вы можете распространять свой открытый ключ («замочек»), поместив его на сайт (и тогда любой желающий сможет написать вам секретное послание) или отправив его всем друзьям по переписке с помощью электронной почты.

Основное преимущество криптографии с открытым ключом — упрощенный механизм обмена ключами (при осуществлении коммуникации по каналу связи происходит обмен открытыми ключами, позволяющими только шифровать информацию).

Но у каждой медали есть две стороны. Из-за особенностей алгоритмов, лежащих в основе систем с открытым ключом, их быстродействие при обработке единичного блока информации обычно в десятки раз меньше, чем быстродействие систем с симметричным ключом на блоке той же длины. Хорошо, если вам нужно зашифровать и отправить только платежку в банк. Десяток-другой секунд можно и подождать. Но гораздо хуже придется, если возникнет необходимость переслать чертеж или кипу проектной документации. Тут уж дело затянется на часы. Поэтому для повышения эффективности систем с от-

крытым ключом обычно применяют смешанные методы шифрования, реализующие криптографические алгоритмы обоих типов. При шифровании информации программой задается случайный симметричный ключ, выбирается алгоритм с симметричным ключом для шифрования исходной информации, а затем алгоритм с открытым ключом для шифрования самого симметричного ключа. По каналу связи передается текст, зашифрованный симметричным ключом и сам симметричный ключ, зашифрованный открытым ключом. Для расшифровки действия производятся в обратном порядке: сначала при помощи секретного ключа получателя расшифровывается симметричный ключ, а затем при помощи симметричного ключа — полученный по каналу связи зашифрованный блок информации. Не бойтесь, все это совсем не сложно, за вас эти операции сделает компьютер.

*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*В контору, которая занимается ремонтом сотовых телефонов, входят двое: здоровый новый русский, весь обвешанный золотом, и ма-а-аленький, плюгавенький интеллигентишка. Новый русский подходит к окошку, на котором написано «Прием и выдача заказов», вытаскивает из кармана телефон и бросает его в окно со словами:*

*— Что это за ботва!!!*

*Из-за его спины выбегает интеллигентишка, засовывает голову в окошко и говорит:*

*— Простите, Николай Петрович спрашивает, почему телефон не работает?*

*Девушка, обитающая по ту сторону окошка, берет телефон и несет его проверить. Через некоторое время*

*она возвращается и протягивает новому русскому другой телефон, мол, тот сломан, посмотрите этот.*

*Новый русский берет в руки телефон:*

*— Что это за ботва?!?!?!?*

*Интеллигентишка:*

*— Николай Петрович интересуется, как он работает?*

## *НЕОБХОДИМЫЕ НАВЫКИ*

Шифрование конфиденциальной информации, пересылаемой по сети, стало привычной операцией для многих корпоративных и индивидуальных пользователей, желающих сохранить свои коммерческие тайны или подробности личной жизни. Появилось огромное количество прикладных приложений, использующих открытые ключи в неявном для пользователя виде (интернет-пейджеры, почтовые программы, протоколы связи). Так как рынок услуг по предоставлению открытых ключей практически полностью монополизирован PGP, встречается сравнительно небольшое число программ, пытающихся составить конкуренцию PGP Corporation в этой области. Несколько бесплатных (табл. 7.1) и платных (табл. 7.2) программ, дающих примерно одинаковую степень защиты (все они используют 5–7 стандартных проверенных алгоритмов), позволяют выбрать среди них наиболее удобную для себя (по оформлению интерфейса, минимуму нажатий кнопок для получения желаемого результата и усилий по освоению программы, максимуму дополнительно предоставляемых функций).

*Таблица 7.1*

| Программа | Характеристики |
|---|---|
| **FineCrypt**<br>4,06 Mb<br>http://www.crypto-systems.com | Простая в пользовании, но не слишком удобная программа с хорошим интерфейсом. Может использоваться как при переписке, так и для шифрования файлов на компьютере. Имеет шредер, архиватор, предлагает на выбор 10 алгоритмов шифрования. |

*Окончание табл. 7.1*

| Программа | Характеристики |
|---|---|
| **DeltaCrypt Public Key File Encryption**<br>975 Kb<br>http://www.deltacrypt.com/english/home/index.htm | Использует открытый ключ длиной 1024 бита, созданный по алгоритму RSA. Может шифровать как отдельные файлы, так и папки. Основной недостаток — полное отсутствие шифрования по симметричному алгоритму. В связи с этим шифрование файлов большого размера занимает очень много времени. |
| **Eureka Public Key**<br>1,02 Mb<br>http://www.datasecuritysolutions.com | Простая в пользовании, но очень неудобная программа. |
| **DeepCoder**<br>821 Kb<br>http://www.devotechs.com | Простая в пользовании, но очень неудобная программа. |

*Таблица 7.2*

| Программа | Характеристики |
|---|---|
| **PGP (Pretty Good Privacy)**<br>19 Mb<br>$518<br>http://www.prodmag.ru/catalog/info/1036/0 | Самая старая, самая распространенная, самая раскрученная, самая многофункциональная, практически ставшая стандартом программа. Нет смысла говорить о характеристиках — размер программы говорит сам за себя, а подробными инструкциями заполнены полки в книжных магазинах. Если у вас появилось время — учитесь, учитесь и учитесь. |
| **AES Pro**<br>1031 Kb<br>$ 59,95<br>http://www.abensoft.com/pro.htm | Очень простая в пользовании программа. Использует асимметричный алгоритм El Gamal и симметричные алгоритмы шифрования AES, 3DES и Blowfish. Имеет шредер, архиватор, позволяет создавать самораспаковывающиеся шифрованные файлы, шифровать целиком папки со всем содержимым. |

*Окончание табл. 7.2*

| Программа | Характеристики |
|---|---|
| **Active CHAOS**<br>996 Kb<br>$ 59,95<br>http://www.safechaos.net/ac.htm | Очень простая в пользовании программа. Использует асимметричный алгоритм El Gamal и симметричные алгоритмы шифрования AES, 3DES, Blowfish и GOST. Имеет шредер, архиватор, позволяет создавать самораспаковывающиеся шифрованные файлы, шифровать целиком папки со всем содержимым. |
| **Crypto Anywhere**<br>3,83 Mb<br>$39,95<br>http://www.bytefusion.com/download/index.htm | Отлично оформленная программа. Использует асимметричный алгоритм RSA и симметричный Towfish. Может шифровать текстовые сообщения и приложенные к ним файлы и отправлять их по электронным адресам получателей (почти полный email клиент). К недостаткам можно отнести неприспособленность к локальному шифрованию информации на компьютере. |

На практике из всех предлагаемых на рынке вариантов можно выделить две программы: PGP и AES Pro. Первая программа замечательна своей широкой распространенностью (она присутствует на рынке уже полтора десятка лет, о ней написаны сотни книг и пособий, или, как говорят в ее рекламе: «фактически она стала стандартом шифрования»). Из ее недостатков следует упомянуть жалобы многих пользователей на сложность освоения, большие размеры, имевший место несколько лет назад скандал, связанный с обнаружением в ней оставленного разработчиками люка и уход из компании, предлагающей ее на рынке, Филиппа Зиммермана, — человека, придумавшего PGP.

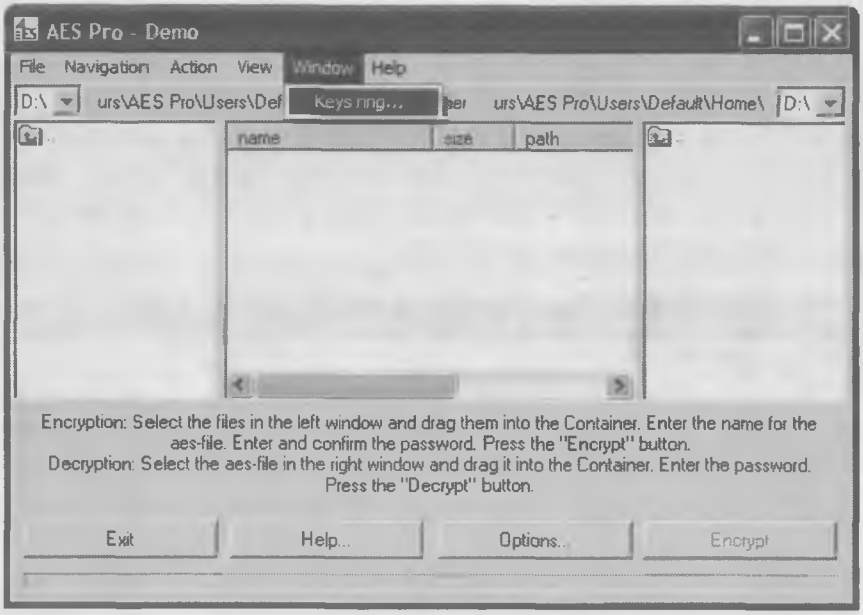



***Рис. 7.1.*** *Вход в поле для создания ключей в программе AES Pro*

Вторая программа позволяет формировать наряду с обычными еще и так называемые активные открытые ключи, дающие возможность вести защищенную переписку с абонентами, не имеющими установленных на компьютере программ для шифрования (эта возможность может быть использована вами в интересах собственной фирмы, ведь, разместив активный открытый ключ на ее сайте, вы сможете обеспечить всем своим потенциальным клиентам конфиденциальность переписки с вами). Рассмотрим эту возможность подробнее. Активный открытый ключ — это мини-программа, уже содержащая ключ для шифрования. Она может зашифровать информацию, предназначенную для пересылки, но не может расшифровать ее (т.е. она не может использоваться самостоятельно, например, для шифрования файлов, предназначенных для хранения на этом же компьютере). При этом она расшифровывает файлы, зашифрованные базовой программой. Скачав такой ключ с сайта или получив его по почте, пользователь может шифровать и от-

правлять владельцу программы информацию (например, запрос на открытие счета или вопрос о стоимости конфиденциальных услуг). Давайте создадим такой ключ и научимся использовать его. Запустив программу AES Pro, нужно открыть окошко для работы с ключами (рис. 7.1), присвоить будущему ключу имя, ввести адрес своей электронной почты и нажать кнопку «Create keys» («Создать ключи») (рис. 7.2).

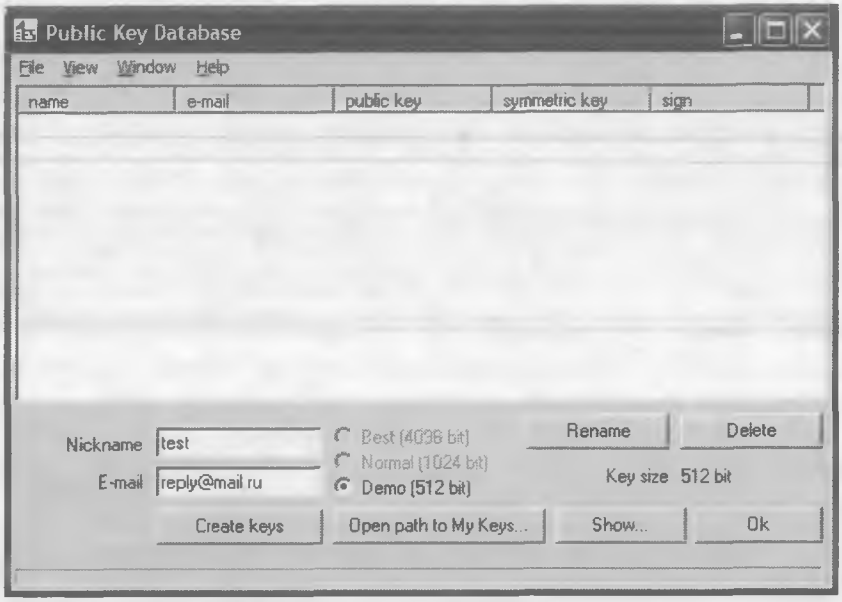



***Рис. 7.2.*** *Создание открытых ключей в программе AES Pro*

Программой одновременно создается обычный открытый ключ (порядок работы с ним такой же, как и у PGP) и активный ключ. Добраться до ключей, присоединить какой-либо из них к письму или поместить на сайте можно, нажав кнопку «Open path to My Keys» («Открыть путь к моим ключам»). В открывшемся окошке будет указан путь к обычным ключам и открыт доступ к ним (рис. 7.3). Теперь можно любой из этих ключей поместить у себя на сайте или отправить своим корреспондентам (если у них в компьютере нет установленной программы AES Pro, то лучше отправить именно активный ключ).

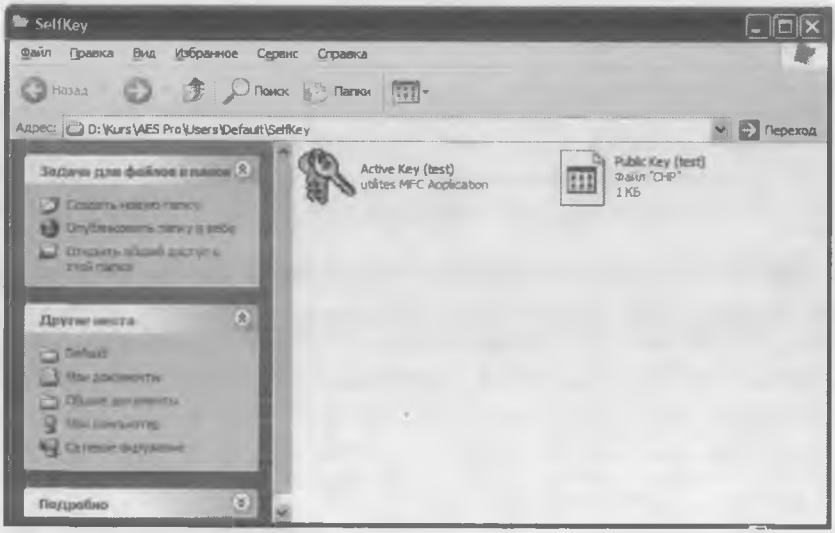



***Рис. 7.3.*** *Обычный и активный открытые ключи*

Скачав такой активный ключ с вашего сайта и запустив его (просто щелкнув по скачанному файлу), пользователь может закрепить его за собой, присвоив любое кодовое имя и закрыв доступ к нему от посторонних паролем (рис. 7.4). После этого он сможет пользоваться именно этим, имеющимся у него ключом.


***Рис. 7.4.*** *Вход в активный открытый ключ*

*Из практики:*

*— Алло! Техотдел?! Я пароль набираю, а меня не пускают!*

*— Значит, правильно набирать надо.*

*— Я правильно набираю! Пять звездочек!*

Щелкнув в этом окошке по кнопке «Ок», пользователь открывает окно для работы с файлами (рис. 7.5) и может шифровать их точно так же, как это описывалось выше (в главе 1). Единственное отличие — ему нет необходимости вводить пароль, так как ключ для шифрования документов уже находится в активном открытом ключе. Зашифровав документы (рис. 7.6), пользователь может отправить их владельцу программы (банк, адвокатская контора, страховая компания) как обычное приложение к письму. Получив это приложение, можно расшифровать его (рис. 7.7, 7.8), как это описывалось на примере в главе 3. В этом случае также не нужно вводить пароль, так как ключ для расшифровки сообщения (секретный ключ) уже содержится в программе.

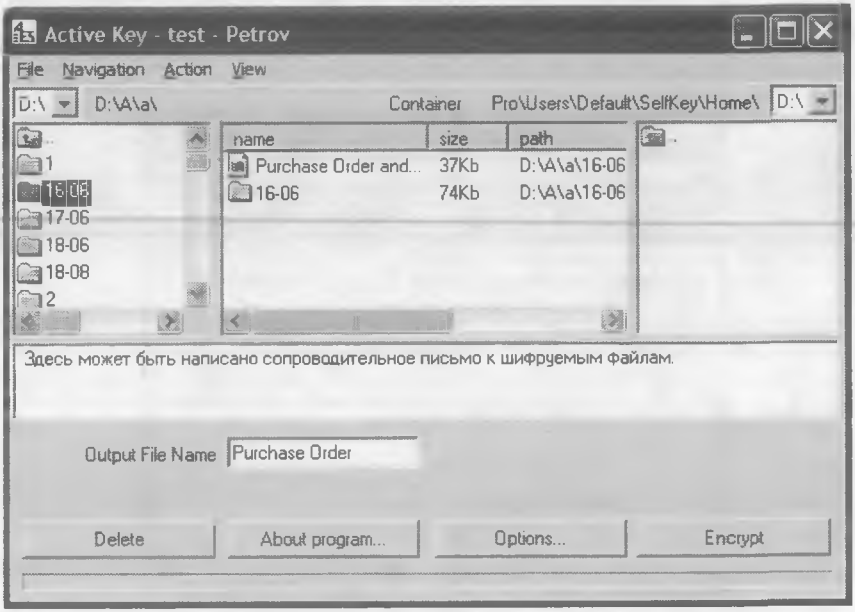



***Рис. 7.5.*** *Шифрование активным открытым ключом*

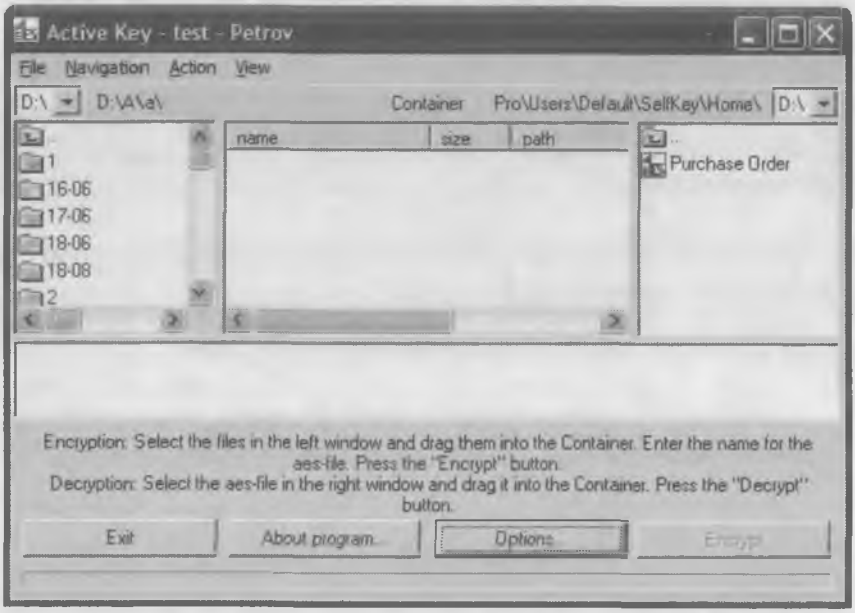



***Рис. 7.6.*** *Информация, зашифрованная открытым ключом (в правом окошке)*

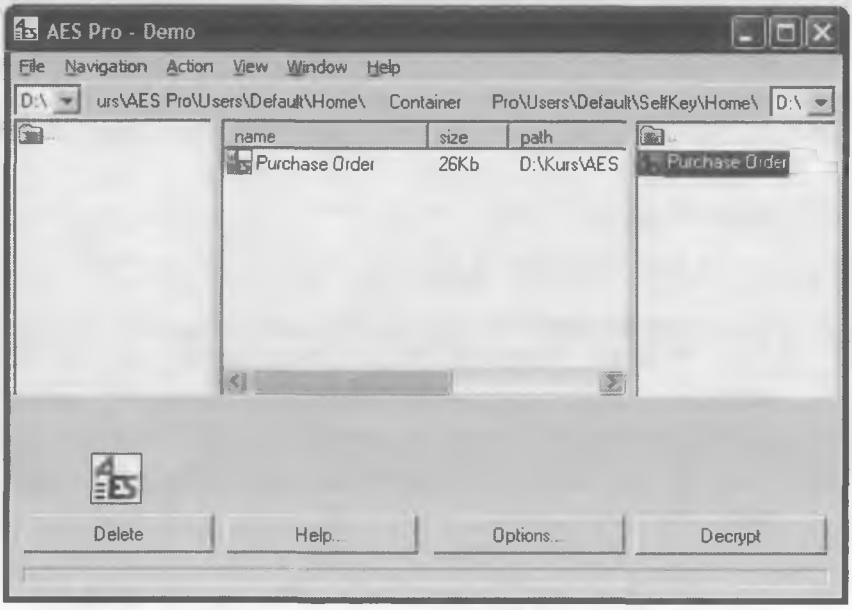



***Рис. 7.7.*** *Расшифровка полученной информации базовой программой*

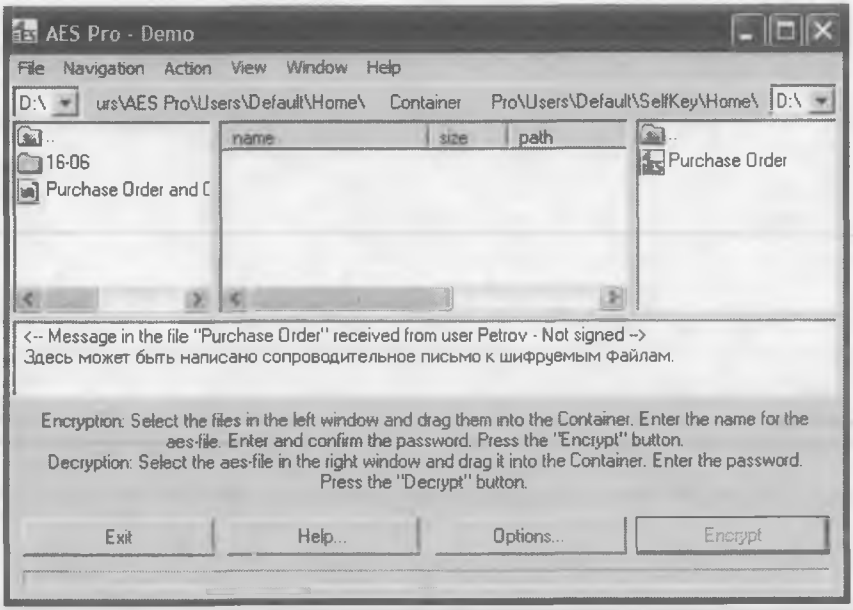



***Рис. 7.8.*** *Информация, расшифрованная базовой программой, появилась в левом окне*

Автор сообщения и ключи для переписки с ним автоматически заносятся в базу данных программы (рис. 7.9), и впредь шифровать сообщение тому или иному пользователю можно, просто щелкнув по его имени из выпадающего списка (рис. 7.10).

## *Из практики:*

*Звонок в Техотдел:*

*— Почему, когда программа доходит до места, где написано «нажмите любую клавишу», я нажимаю, а компьютер начинает перезагружаться?*

*Полчаса выясняются возможные причины, затем программист невзначай спрашивает:*

*— А какую кнопку вы нажимаете?*

*— Ну, там же написано «любую», вот я и нажимаю большую круглую на системном блоке!*

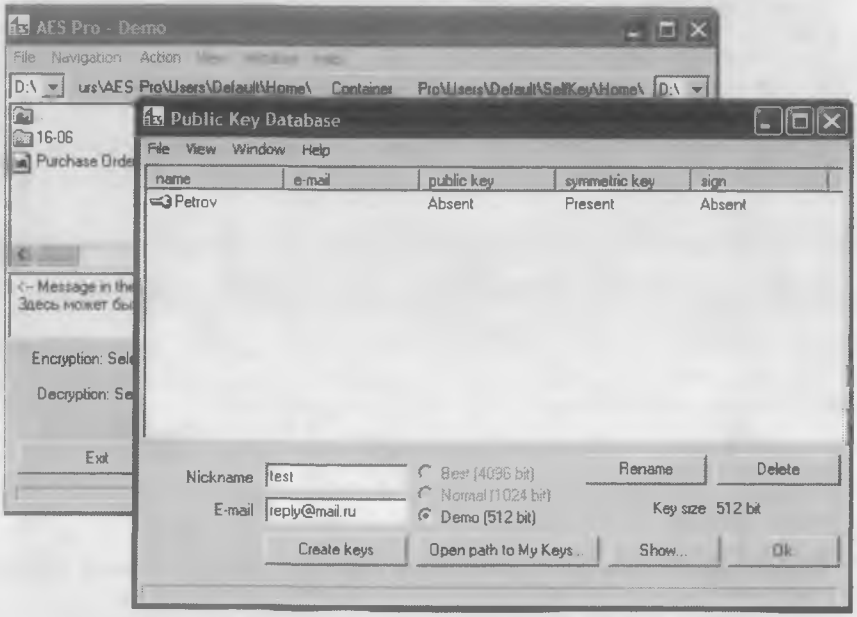



***Рис. 7.9.*** *Добавление автора сообщения в базу данных*

После первого обмена сообщениями базовая программа и активный ключ переходят на шифрование сообщений по одному из симметричных алгоритмов шифрования. Это значительно повышает надежность защиты перехватываемых сообщений от попыток взлома. Активный ключ практически позволяет превращать открытый канал связи в защищенный. Казалось бы, зачем? Ведь уже существует SSL? Но SSL можно использовать, если компьютеры обоих абонентов подключены к сети. А кто может поручиться, что в компьютере у вашего удаленного друга по переписке не сидит вирус-информатор, тут же пересылающий набираемый им текст заинтересованным лицам? При использовании же активных ключей письмо можно писать, шифровать его и приложенные файлы на одном компьютере, а отправку зашифрованного сообщения осуществлять с другого.

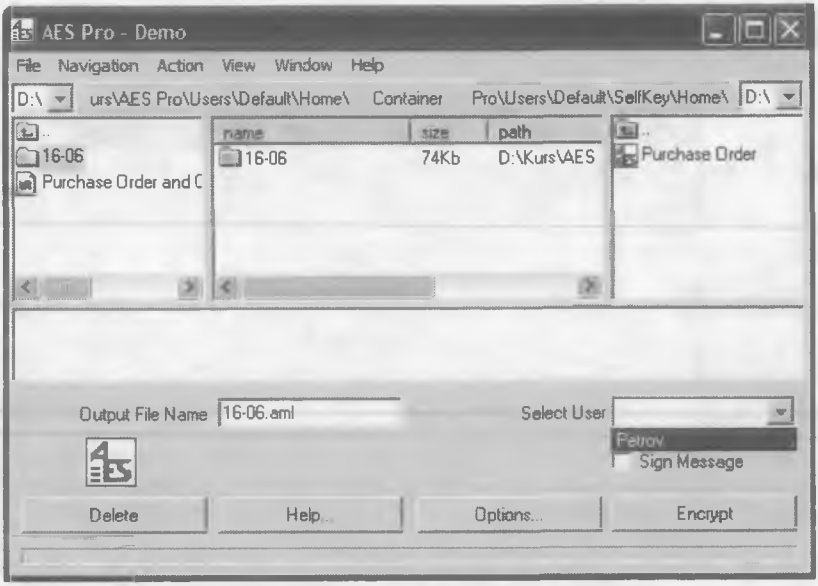



***Рис. 7.10.** Выбор пользователя, которому шифруется сообщение*

## Резюме

На базе алгоритмов асимметричного шифрования основаны все основные современные средства коммуникации, обеспечивающие защиту информации при ее пересылке по открытым сетям. Они находят применение в приложениях для создания защищенных каналов связи (технология SSL) и защиты электронной почты. Использование же программ, применяющих открытые ключи в явном виде (т.е. заставляющих вас выбирать ключ, которым будет выполняться шифрование), значительно сократилось и находит применение в тех случаях, когда требуется:

- ✓ обеспечить свободный доступ к своему ключу максимальному числу пользователей, например, размещая его на сайте компании;
- ✓ иметь возможность удостовериться в личности корреспондента, получив подтверждение подлинности его ключа у третьей стороны.

# Глава 8

## Вам письмо, распишитесь в получении...
### (как скрыть свои контакты)

*Хорошо лишь то беспокойство, благодаря которому мы впоследствии обретаем покой.*

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

**В этой главе:**

- Кто-то теряет, а кто-то находит.
- Кое-что о работе почты.
- Зачем иметь несколько почтовых ящиков?
- Чем может быть полезен спам?

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Интернет, открыв практически неограниченные возможности для быстрой и конфиденциальной связи, обеспечил любому желающему условия для анонимного создания предприятий, дистанционного управления их персоналом и координации работы с деятельностью смежников. Как средство связи Интернет традиционно применяется для пересылки электронной почты, уже упомянутой выше интернет-телефонии и быстрого текстового общения через интернет-пейджеры типа ICQ. В этой главе рассмотрены основные требования к организации защищенной переписки по электронной почте.

Навыки организации защиты своих контактов давно освоили хакеры.

***ИЛЛЮСТРАЦИЯ***

***http://lib.web-malina.com/getbook.php?bid=58&page=16***

*Человек, располагающий ценной информацией, посылает в одну из телеконференций через анонимный почтовый узел самоадресуемое текстовое почтовое сообщение, исходящий адрес IP (Internet Protocol) которого проследить невозможно. Заинтересованный покупатель отвечает зашифрованным сообщением. Если продавец согласен на сделку, он отвечает другой шифровкой. Это тот случай, когда связь осуществляется «втемную» — полностью анонимно. «Выражаясь военным языком, это как черный туннель, шифрованный канал, — поясняет один хакер. — Никаких открытых сообщений. Обе стороны ничего не знают друг о друге. Они не знают даже, с каким континентом они общаются».*

И забота о собственной безопасности приносит им уже сейчас ощутимую прибыль.

***ИЛЛЮСТРАЦИЯ***

***http://emigration.russie.ru/news/3/7482_1.html***

*По подсчетам экспертов исследовательской фирмы «Компьютер экономикс» из Калифорнии, совокупный материальный ущерб американских компаний от нападений хакеров в 2004 году достигает 17,5 миллиарда долларов. А ведь еще год тому назад сумма потерь от вторжения компьютерных взломщиков составляла 13 миллиардов долларов. Недаром ФБР считает борьбу с хакерами третьим из своих приоритетов — после противостояния террористам и шпионам.*

При этом доход одной стороны (хакеров) напрямую формируется из убытков другой стороны (обычных бизнесменов). Не стоит забывать, что хакеры — только незначительная (и самая маловероятная в нашей суровой действительности) часть претендентов на ваши накопления. Подумайте об этом.

*Надо делиться!*

***Александр Лившиц,***
***министр финансов РФ***

## *ПОЛЕЗНАЯ ИНФОРМАЦИЯ*

Доставка корреспонденции в стародавние времена была делом длительным, хлопотным и опасным, дорога, знаете ли, а в пути чего только не случается (вспомните одно только путешествие д'Артаньяна в Лондон из Парижа). Писали мало, отправка гонцов была делом дорогим и доступным лишь коронованным особам, да банкирским домам. Девятнадцатый век несколько упростил жизнь почтовых служащих и так уменьшил время доставки писем, что общение через перо и бумагу привело даже к появлению в английском языке выражения pen friends (друзья по переписке). В двадцатом веке телеграф, телефон и факс реализовали мечту бизнесменов о мгновенной связи и превратили планету в один большой потребительский, торговый и производственный одновременно кооператив. Радио и телевидение добавили перца, и мы оказались рыбками в огромном аквариуме, где все знают все обо всех, а понятие конфиденциальности стало понятием условным (кому нужно, все равно все узнает) и временным (раз уж сохранить секрет все равно невозможно, утечку информации нужно оттянуть во времени, глядишь, она уже никого и не заинтересует). Но, давая больше технических возможностей для осуществления связи и средств для ее контроля, прогресс, сделав виток, вернулся на исходную позицию: если пятьсот лет назад отнятое у гонца грабителями письмо не давало им ничем поживиться ввиду элементарной безграмотности членов тогдашних «бандформирований», то появление программ для защиты корреспонденции, применяющих надежные алгоритмы шифрования, сделало недоступным содержание переписки лиц, их использующих. Правда, возможность защиты конфи-

денциальности породила еще один эффект: люди стали опасаться шифровать свою переписку (Шифрует? Ага, значит, есть что скрывать. Террорист или денег много имеет. Надо присмотреться повнимательнее...) Короче, клубок проблем. За какую же ниточку потянуть?

Сегодня появляется все больше программных и аппаратных средств защиты информации при доставке ее через сеть. Решения поставщиков варьируются от простых средств, шифрующих электронную почту, до аппаратно-программных комплексов для создания виртуальных частных сетей (VPN — virtual private network). При этом большинство решений требует установки специализированных программных или аппаратных средств на обоих концах защищаемого соединения. Но иногда для защиты информации компании уже достаточно простой гарантии того, что данные не будут скопированы на сервере местного провайдера теми, кто его контролирует.

Поэтому давайте начнем рассмотрение вариантов приемлемых для вас решений по сохранению конфиденциальности переписки с открытия обычного почтового ящика.

Ваша электронная почта проходит через множество узлов связи и обычные телефонные линии, а поэтому абсолютно доступна для перехвата и чтения.

*Анекдот в тему:*

~ ~ ~ ~ ~ ~ ~

*У директора одной провайдерской фирмы спросили:*

*— Почему Вы так активно создаете сервисы бесплатного e-mail?*

*— Ну, как Вам сказать... А Вы читали когда-нибудь чужую почту?*

Поэтому, пользуясь электронной почтой, прежде всего сделайте невозможным официальное доказательство принадлеж-

ности получаемой корреспонденции именно вам (по крайней мере той, которая может представлять для вас угрозу: текущая информация из банков о состоянии ваших счетов, письма из трастовых фондов, управляющих вашими капиталами, и т.п.). Как этого можно добиться?

Имейте несколько почтовых ящиков. Один или несколько из них должны быть официально открыты у местного провайдера и принадлежать вам и/или вашей фирме (в этом случае вы всегда можете сослаться: да, я веду переписку по электронной почте, вот, мол, мои ящики, их содержимое мне знакомо, а больше знать ничего не знаю).

Откройте несколько почтовых ящиков на бесплатных серверах в разных странах (открывая ящики на бесплатных серверах, вы не производите платежей в сети своей кредитной карточкой, то есть не оставляете финансовых следов, позволяющих идентифицировать эти ящики как ваши, при этом вы не должны, естественно, указывать, открывая их, своего реального имени). Эти почтовые ящики открывайте не со своего компьютера (лучше всего делать это из интернет-кафе или компьютерного клуба). Для конфиденциальной переписки используйте только эти, не имеющие к вам официального отношения почтовые ящики.

### *НЕОБХОДИМЫЕ НАВЫКИ*

В табл. 8.1 указаны адреса некоторых бесплатных почтовых служб. Кстати, чтобы не просматривать ежедневно все ящики, используемые для связи с разными адресатами, вы можете установить на каждом из них режим автоматической пересылки на один, служащий сборным пунктом для вашей почты, и в дальнейшем считывать информацию только с этого ящика.

Важную для вас информацию при отправке почтой желательно шифровать. Некоторые почтовые службы (Moment Secure Mail, Safe-mail, Secure email) обеспечивают шифрование вашей переписки с клиентами этих же служб. Открытие поч-

тового ящика занимает всего несколько минут и не требует введения какой-либо информации, позволяющей вас идентифицировать (рис. 8.1). Оно заключается в выборе для себя имени (например, baks), пароля для входа в свой почтовый ящик (например, $1 000 000) и указания какого-нибудь почтового адреса (можно тоже бесплатного) для переписки с вами в случае, если вы забудете свой пароль и обратитесь с просьбой его восстановить.

*Таблица 8.1*

| **Название почтовой службы** | **Где размещается** |
|---|---|
| Safe-mail | http://www.safe-mail.net |
| Mail.com | http://www.mail.com |
| Bluebottle | http://www.bluebottle.com |
| FreeMail | http://freemail.aussiemail.com.au |
| WebMail | http://www.webmail.co.za |
| Moment Secure Mail | http://www.momentmail.com |
| TheMail | http://www.themail.com |
| Postmaster | http://www.postmaster.co.uk |
| MyPersonalEmail | http://www.mypersonalemail.com |
| EmailAccount | http://mail.emailaccount.com |
| Secure email | http://www.s-mail.com/index.shtml.en |
| Address | http://www.address.com |
| FastMail | http://www.fastmail.fm |
| Swiss Info | http://swissinfo.org |
| Soft Home | http://www.softhome.net |
| hotPOP | http://www.hotpop.com |
| GAWAB | http://www.gawab.com |
| Tmicha | http://www.tmicha.net |

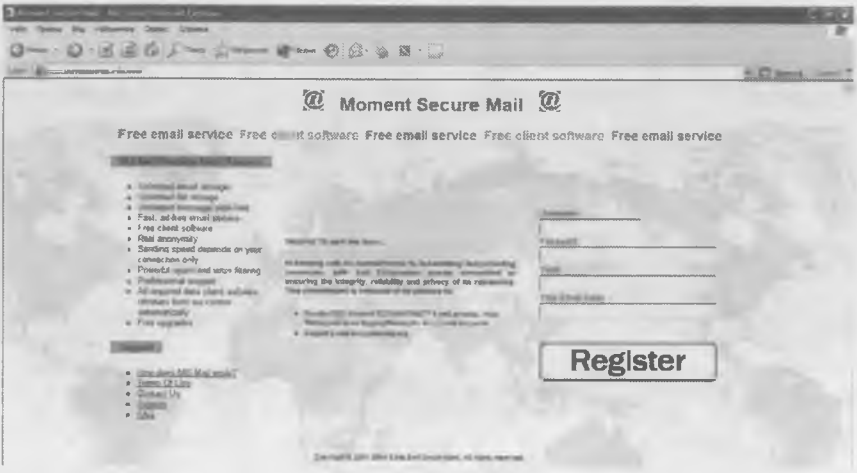



***Рис. 8.1.*** *Открытие почтового ящика в почтовой службе Moment Secure Mail*

Выполнив эти операции, вы получаете возможность обмениваться конфиденциальными документами в зашифрованном виде со своими деловыми партнерами (имеющими почтовые ящики в той же службе) с помощью любого гостиничного компьютера.

*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*Программист звонит в справочную.*
*— У вас можно телефон по адресу узнать?*
*— Да, можно.*
*— Тогда, пожалуйста: vasja@mail.ru*

Этот способ хорош при осуществлении связи с корреспондентами, открывшими почтовые ящики на том же почтовом сервере, что и вы. Но не можете же вы заставить пойти по этому пути все организации, с которыми вы контактируете? Как быть?

***ПОЛЕЗНАЯ ИНФОРМАЦИЯ***

Существуют протоколы обмена информации, позволяющие создавать временные защищенные каналы связи в открытых сетях. Одним из самых распространенных таких протоколов является SSL (secure socket layer), разработанный фирмой Netscape. Вы узнаете, что SSL начал использоваться в тот момент, когда видите, подключившись к какому-либо серверу, в адресной строке своего браузера URL, начинающийся с аббревиатуры https (рис. 8.2).

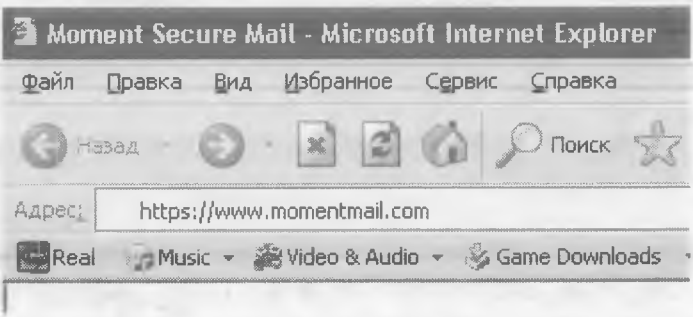



***Рис. 8.2.*** *Подключение к серверу по защищенному каналу связи*

В процессе подключения ваш браузер посылает серверу приветственное сообщение (hello message). В свою очередь сервер также посылает браузеру свое приветственное сообщение. Эти сообщения являются первичными, инициализирующими, и содержат информацию, используемую при дальнейшей настройке открываемого секретного канала: версию протокола, идентификатор сессии, способ шифрования, метод компрессии, а также два специально сгенерированных случайных числа; и сервер, и клиент генерируют такие числа независимо друг от друга, а затем просто обмениваются ими друг с другом. При получении приветственного сообщения от клиента сервер отсылает свой сертификат. После этого выполняется еще ряд промежуточных обменных операций, в процессе которых производится окончательное уточнение выбранного алгоритма шифрования, ключей и секретов. Затем сервер посылает клиен-

ту некое финальное сообщение, после чего обе стороны приступают к обмену зашифрованной информацией. Все это происходит практически мгновенно и незаметно для вас. Просто знайте, что если в адресе сервера вместо аббревиатуры http//... вы увидите набор букв https//..., ваш компьютер уже создал защищенный канал связи. Вы видите на экране нормальный текст, но шел-то до вас он в зашифрованном виде и при перехвате выглядит для стороннего наблюдателя как обычная абракадабра. Шифровали пересылаемую информацию не вы, вы даже не можете дать распоряжение отменить шифрование при пересылке, просто протокол связи у сервера такой, а то, что вы этим почтовым сервером пользуетесь, — дело случая. Таким образом, защищенное соединение устанавливается между вашим компьютером и почтовым сервером, на который собирается почта. Выбор удаленного сервера (подальше за границей) обеспечит хорошую защиту ваших данных при передаче через местные сети (рис. 8.3).

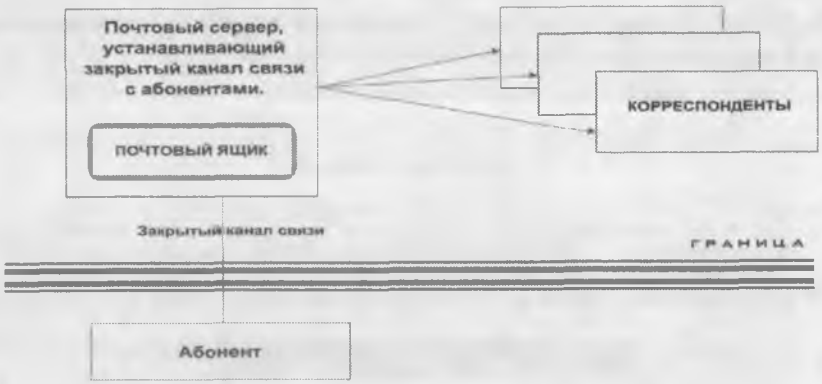



***Рис. 8.3.*** *Организация связи через почтовый сервер, поддерживающий закрытый канал связи с абонентами*

Что реально дает такая схема, какие у нее есть преимущества? Во-первых, пользователи, имеющие защищенные почтовые ящики на сервере, шифруют переписку друг с другом. Во-

вторых, они получают гарантию защиты данных при их передаче через местные сети в условиях, когда нет полной уверенности в том, что данные не будут скопированы в этих сетях, т.е. в том самом месте, где их проще всего перехватить. Кроме того, когда пользователь работает со своей электронной почтой по закрытому каналу, извне невозможно перехватить не только текст письма, но и его адресную часть. Таким образом, нельзя выяснить, с кем общается абонент; более того, невозможно даже определить, что по закрытому каналу работают именно с почтой.

При этом от корреспондентов, с которыми переписывается абонент, не требуется установки какого-либо дополнительного программного обеспечения, поскольку между почтовым сервером и корреспондентом информация передается в открытом виде. Для этого может быть использован уже существующий почтовый ящик либо ящик, зарегистрированный на одной из вышеупомянутых почтовых служб. Если же и отправитель, и получатель пользуются электронными адресами, открытыми на таком почтовом сервере, то участки, на которых информация передается через Интернет в открытом виде, и вовсе отсутствуют (рис. 8.4).


**Рис. 8.4.** *Организация связи через почтовый сервер, шифрующий переписку между своими абонентами*

### *НЕОБХОДИМЫЕ НАВЫКИ*

В табл. 8.2 указаны адреса ряда почтовых служб, поддерживающих протокол SSL для связи со своими клиентами. Как это можно использовать? Откройте почтовый ящик (на который будут пересылаться письма с других адресов) на одной из таких служб и спокойно читайте свою почту, собранную в этом ящике, хоть браузером, хоть с помощью почтовой программы. И в том, и в другом случае на этапе доставки ваша почта будет защищена от посторонних глаз.

*Таблица 8.2*

| **Название почтовой службы** | **Где размещается** |
|---|---|
| Moment Secure Mail | http://www.momentmail.com |
| Safe-mail | http://www.safe-mail.net |
| Secure email | http://www.s-mail.com/index.shtml.en |
| Gmail | http://www.gmail.com |
| RunBox | http://www.runbox.com |

Используя этот прием, помните: некоторые почтовые службы время от времени изменяют условия обслуживания, идя на поводу у правительств места своей регистрации. Например, Gmail, продолжая поддерживать пересылку почты по SSL каналу при использовании почтовых клиентов, отказалась от защиты корреспонденции при просмотре ее с помощью браузера.

*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*Почтовый сервер присылает служебное сообщение о задержке доставки посланного по электронной почте письма «...из-за отсутствия на месте сотрудника ФСБ, контролирующего вашу почту...»*

Как еще можно закамуфлировать свою переписку? В этом неоценимую помощь вам окажут спаммеры. Опубликуйте свой почтовый адрес на нескольких форумах, откликнитесь на не-

сколько писем с предложением виагры, короче, «засветитесь», попадите в каталоги рассылок спаммеров и получайте 100–200 писем в день с предложениями виагры, фотографий молодых девочек, счета на eBay, миллионов нигерийских наследников, счетов в интернет-банках, бонусов казино и т.д.

### Запомните

*Где умный человек прячет лист? —*
*в лесу.*
*А если леса нет, он сажает его,*
*чтобы спрятать в нем лист.*

***Цитата из рассказа Г. Честертона***
***«Сломанная шпага»***

Ваша реальная корреспонденция в буквальном смысле утонет в спаме, а выбрать ее из мусора с помощью простейших фильтров на своем почтовом клиенте вам труда не составит.

В табл. 8.3 приведен список бесплатных, а в табл. 8.4 платных программ, позволяющих фильтровать корреспонденцию, скачиваемую вашим почтовым клиентом с сервера. Установите одну из них, настройте фильтр на перечень разрешенных адресов и получайте свою корреспонденцию с почтового сервера по защищенному каналу.

*Анекдот*
*в тему:*

~ ~ ~ ~ ~ ~

*25 мая было проведено бета-тестирование новой антиспамовой программы в российском Интернете. Результаты превзошли все ожидания. Поток спама в течение всего дня на всей территории России сократился примерно в 3–4 раза. Разработчики предлагают не обращать внимания на мелкие сопутствующие эффекты типа прекращения работы метро и общественного транспорта в Москве и других крупных городах.*

*Таблица 8.3*

| **Название программы** | **Размер** | **Где можно скачать** |
|---|---|---|
| SPAM Shredder | 1,5 Mb | http://safechaos.com/ss.htm |
| SPAMfighter Standard | 0,97 Mb | http://www.spamfighter.com/default.asp |
| PP MailCheck | 3,5 Mb | http://www.ppsoft.dk/Mailcheck_eng.htm |
| MailEnable Standard | 5,1 Mb | http://www.mailenable.com |
| SpamAware | 4,4 Mb | http://www.jam-software.com/freeware/index.shtml |
| Bounce Bully | 1,2 Mb | http://www.bouncebully.com |
| ChoiceMail Free | 9,2 Mb | http://www.digiportal.com |

*Окончание табл. 8.3*

| Название программы | Размер | Где можно скачать |
|---|---|---|
| Messenger Spam Block | 248 Kb | http://www.pingram.com |
| Spam-Aid | 1,01 Mb | http://www.versasoft.com |
| Anti Spam Boy | 2,61 Mb | http://www.acezip.net |
| Matador Spam Fighter | 938 Kb | http://blogs.clearscreen.com/migs |
| POPFile | 4,77 Mb | http://popfile.sourceforge.net |
| Elgr anti-spam | 700 Kb | http://7tec.com/en |
| E_Cloaker | 230 Kb | http://www.codefoot.com |
| Junkanoo | 640 Kb | http://junkanoo.kw-online.com/index.html |

*Таблица 8.4*

| Название программы | Размер | Цена | Где можно скачать |
|---|---|---|---|
| Zaep AntiSpam | 1,4 Mb | $ 39,95 | http://www.zaep.com |
| Out Spam | 553 Kb | $ 19,00 | http://www.brigsoft.com/outlook-spam-filter |
| SpamRemover | 2,08 Mb | $ 19,95 | http://www.productsfoundry.com/spamremover |
| A FamilyMail | 6,2 Mb | 29,90 EUR | http://www.familymail.com/en |
| SpamWeed | 2,1 Mb | $29,95 | http://www.spamweed.com |
| SpamBurner | 3,16 Mb | $ 29,95 | http://www.spamburner.com |
| IPS Spam Filter | 4,58 Mb | $ 19,00 | http://www.ipsspamfilter.com |
| Spam Monitor | 3,2 Mb | $29,95 | http://www.pctools.com/spam-monitor |
| InBoxer | 4,1 Mb | $ 29,95 | http://www.inboxer.com |
| Spam Bully | 1,68 Mb | $ 29,95 | http://www.spambully.com |

## Резюме

Рассмотренные приемы обеспечения защиты корреспонденции позволяют:

- ✓ осуществлять шифрование переписки с корреспондентами без применения специальных программ для шифрования;
- ✓ скрывать адреса и имена своих корреспондентов при отсылке и получении почты через сервер, использующий закрытый канал связи для контакта со своими абонентами;
- ✓ скрывать факт получения шифрованной корреспонденции.

# Глава 9

## В каждой строчке только точки...

*(как спрятать свои планы)*

*В этом мире нет гарантий, есть только возможности.*

***Дуглас Макартур,***
***американский генерал***

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

**В этой главе:**

- Еще раз об открытых ключах.
- Как шифруют электронную почту?
- Сам себе шифровальщик.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Сокрытие реальной почты в спаме, скачивание ее по защищенному каналу, шифрование между абонентами одного почтового сервера, — все это хорошо, но хочется чего-то большего. Хочется твердо знать, что написанное вами **очень важное письмо** не будет прочитано. Да, технические детали проекта, кое-какие пункты договора, сроки и прочие немаловажные, но и не самые важные мелочи. Все это можно доверить и защищенному каналу, и шифрованию на сервере. Но имена (!), доли (!), роли (!) участников проекта! Ведь при использовании защищенных каналов связи с сервером или шифрующего внутреннюю переписку почтового сервера ваша почта все равно доступна его администратору. Пока ваш бизнес невелик, инте-

реса к нему нет, можно пользоваться и этими бесплатными и простыми в использовании средствами, но ведь он вырастет... Тут уж невольно вспомнишь: «Береженого Бог бережет», и захочешь перед отсылкой все-таки зашифровать информацию. О том, как это сделать, мы и поговорим в этой главе.


### *ПОЛЕЗНАЯ ИНФОРМАЦИЯ*

Вы не забыли еще об открытых ключах, которые рассматривались в первой главе? Вот технологию их применения и стали активно использовать программисты при разработке почтовых программ, обеспечивающих защиту доставляемой корреспонденции. Существует два основных способа организации связи между почтовыми программами, использующими открытые ключи. Первый — прямой обмен ключами между пользователями (рис. 9.1), второй — получение пользователями ключей корреспондентов из удаленной базы данных (рис. 9.2).

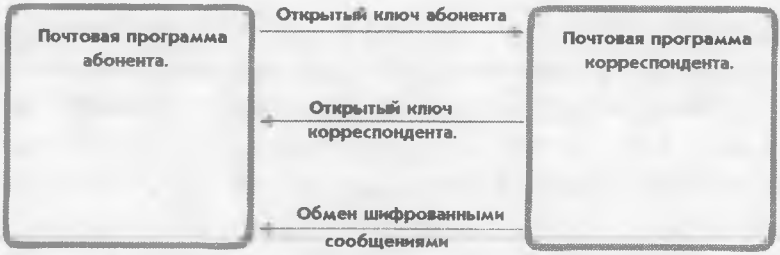



***Рис. 9.1.*** *Организация связи с помощью почтовой программы, напрямую обменивающейся ключами с аналогичными программами*

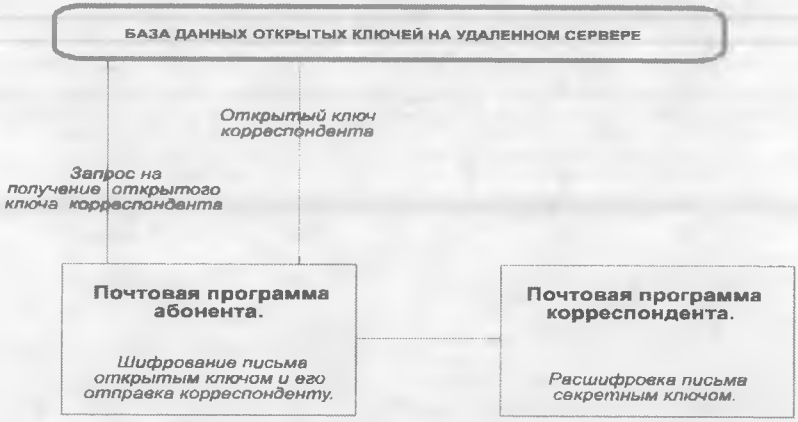



***Рис. 9.2.*** *Организация связи с помощью почтовой программы, использующей открытые ключи, помещенные в удаленную базу данных*

Система для работы с открытым ключом стала использоваться и в почтовых программах, поставляемых компанией Microsoft. При работе с MS OutLook или OutLook Express вы можете получить комплект ключей в одном из центров сертификации. Эта процедура совершенно бесплатна и доступна любому желающему. Для получения ключей необходимо выбрать в настройках программы закладку Security и с помощью кнопки Get Digital ID («Получить цифровой сертификат») перейти на страницу Удостоверяющего Центра Микрософт (Сервера Сертификатов). Выбрав тип ключа (фактически вы-

бирается его длина, от которой зависит надежность шифрования) и выполнив необходимые действия, по которым вас проведет Мастер создания ключей, вы получите необходимый комплект. Полученные ключи следует поместить в хранилище сертификатов (в Windows 2000 хранилище находится в Active Directory). Сделать это можно также через закладку Security. Разослав открытые ключи своим корреспондентам и получив в ответ их ключи, вы будете готовы к обмену шифрованной корреспонденцией.

Для шифрования передаваемых по электронной почте сообщений и документов многие пользователи применяют PGP. Этот продукт применяется для шифрования корреспонденции и встроен в некоторые почтовые программы.

### *НЕОБХОДИМЫЕ НАВЫКИ*

Учитывая печальную славу образцов продукции Microsoft, как весьма уязвимых для взлома (при прекрасных макроэкономических показателях компании трудно все-таки координировать работу нескольких тысяч программистов), и тень, брошенную на разработчиков PGP историей с люками в программе, стоит обратить внимание на почтовые программы или приложения к ним, позволяющие шифровать переписку, предлагаемые другими производителями. Перечень ряда бесплатных программ этого типа приведен в табл. 9.1, а платных — в табл. 9.2.

*Таблица 9.1*

| Программа | Характеристики |
|---|---|
| **Safe Express Free**<br>1.48 Mb<br>http://www.netsafesoft.com | Очень простая в пользовании почтовая программа. Для шифрования текста сообщения используется алгоритм шифрования AES (длина ключа 128 бит), для шифрования ключа, которым шифруется сообщение, используется алгоритм Эль Гамаля (длина ключа 1024 бита). Имеет встроенный архиватор и шредер. |

*Окончание табл. 9.1*

| Программа | Характеристики |
|---|---|
| **Cypherus Free Basic Encryption**<br>4,58 Mb<br>http://www.cypherus.com | Очень неудобное приложение для шифрования сообщений по электронной почте. При шифровании текста сообщения, используется ключ в 128 бит, а для шифрования ключа, которым шифруется сообщение, используется ключ длиной 1024 бита. К сожалению, алгоритмы, по которым выполняется шифрование, не указываются ни в программе, ни на сайте. |
| **SecExMail**<br>2,56 Mb<br>http://www.bytefusion.com | Приложение к почтовым программам, позволяющее шифровать отправляемые сообщения. Для шифрования текста сообщения используется блочный алгоритм шифрования Twofifh (длина ключа 256 бит) и ISAAC (длина ключа 64 бита), для шифрования ключа, которым шифруется сообщение используется алгоритм RSA (длина ключа 2048 бит). Недостатками можно считать известную сложность в использовании и необходимость предварительно обмениваться открытыми ключами с корреспондентами, защита переписки с которыми осуществляется. |
| **Top Secret Crypto Gold**<br>3.23 Mb<br>http://www.topsecretcrypto.com | Приложение к почтовым программам, позволяющее шифровать отправляемые сообщения. Для шифрования сообщения используется алгоритм RSA с длиной ключа до 16384 бит. Недостатками можно считать сложность в использовании и необходимость предварительно обмениваться открытыми ключами с корреспондентами, защита переписки с которыми осуществляется. |

*Таблица 9.2*

| Программа | Характеристики |
|---|---|
| **Safe Express Pro**<br>1.66 Mb<br>$ 99,95<br>http://netsafesoft.com | Очень простая в пользовании почтовая программа. Для шифрования текста сообщения предлагает на выбор пять алгоритмов шифрования (AES, 3DES, Blowfish, GOST, RC4), для шифрования ключа, которым шифруется сообщение, используется алгоритм Эль Гамаля (длина ключа до 4096 бит). Имеет встроенный архиватор и шредер. При желании позволяет шифровать сообщения заранее согласованным паролем, не используя открытый ключ. |
| **CYPHER MILLENIUM**<br>3.44 Mb<br>$ 270,00<br>http://www.cypher.com.br/cypher/oasys_tecnologia__cypher_e.htm | Простая и красиво оформленная программа. Для шифрования текста сообщения предлагает на выбор пять алгоритмов шифрования (Rijndael, Twofish, DS2, Blowfish, GOST and RC4). К сожалению, больше пригодна для шифрования файлов на компьютере, чем для защиты электронной почты. |
| **The Bat!**<br>9.8 Mb<br>$ 27<br>http://www.ritlabs.com | Отличная почтовая программа, позволяющая шифровать сообщения с помощью PGP. |
| **PMMail 2000 Professional**<br>4.77 Mb<br>$ 49,95<br>http://www.blueprintsoftwareworks.com | Добротная почтовая программа, позволяющая шифровать сообщения с помощью PGP. |

Давайте ознакомимся с какой-нибудь из них, оценим ее достоинства и степень пригодности для вашей цели (защиты электронного документооборота с клиентами и партнерами).

Safe Express по внешнему виду и техническим возможностям как почтовой программы практически соответствует известной Outlook Express (рис. 9.3). Ее основное достоинство: она **всегда** шифрует пересылаемые письма к адресатам, у которых аналогичная программа уже установлена (прочим адресатам она отправляет, естественно, открытые письма, предупреждая вас об этом). Применяя Safe Express, вам не придется объяснять окружающим, зачем вы шифруете свою переписку, — это делаете не вы, а используемая программа. Почему вы ею пользуетесь? Так она же хорошо еще и от спама защищает (кстати, это действительно правда).

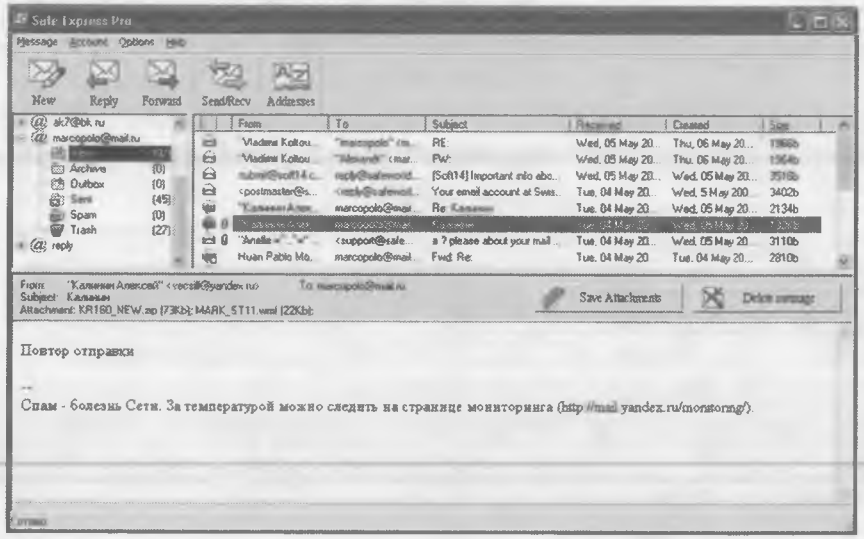



***Рис. 9.3.*** *Интерфейс программы Safe Express*

Кроме обычных почтовых настроек вы можете защищать ваши почтовые ящики паролем (рис. 9.4), выбирать алгоритм шифрования и размеры ключей, которыми программа будет шифровать вашу переписку (рис. 9.5), имеете доступ к собственным ключам (рис. 9.6), что позволяет устанавливать идентичные ключи на разные почтовые ящики.


*Рис. 9.4. Защита паролем почтового ящика*

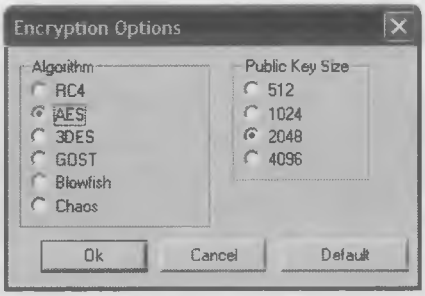



*Рис. 9.5. Выбор алгоритма шифрования и длины ключа*


*Рис. 9.6. Интерфейс окна доступа к ключам программы*

После написания адреса получателя программа самостоятельно разыскивает на удаленном сервере и скачивает его открытый ключ за то время, пока пользователь пишет текст сообщения. Когда же письмо окончено и дана команда на его отправку, программа автоматически шифрует сообщение и приложенные к нему файлы. Версия Safe Express Pro дополнительно позволяет шифровать письма заранее согласованным между пользователями паролем (рис. 9.7).

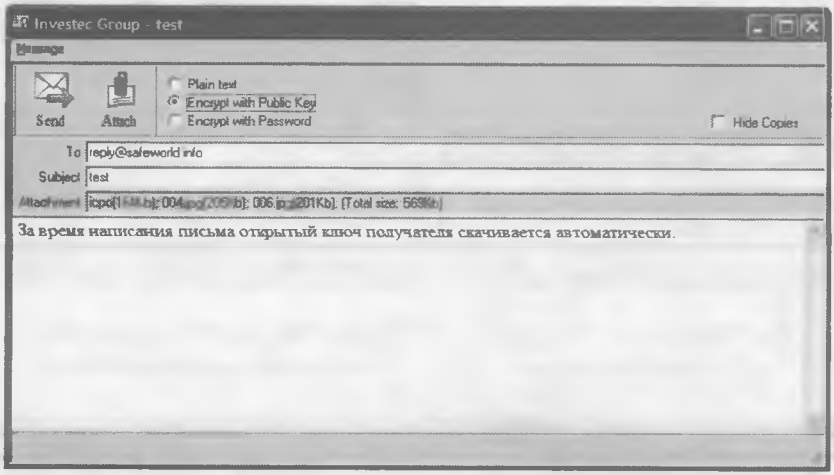



***Рис. 9.7.*** *Интерфейс окна для подготовки письма*

К письму можно присоединять в качестве приложений не только отдельные файлы, а и целые папки со всем содержимым (рис. 9.8), так как программа при пересылке не только шифрует, а архивирует все приложенные документы.

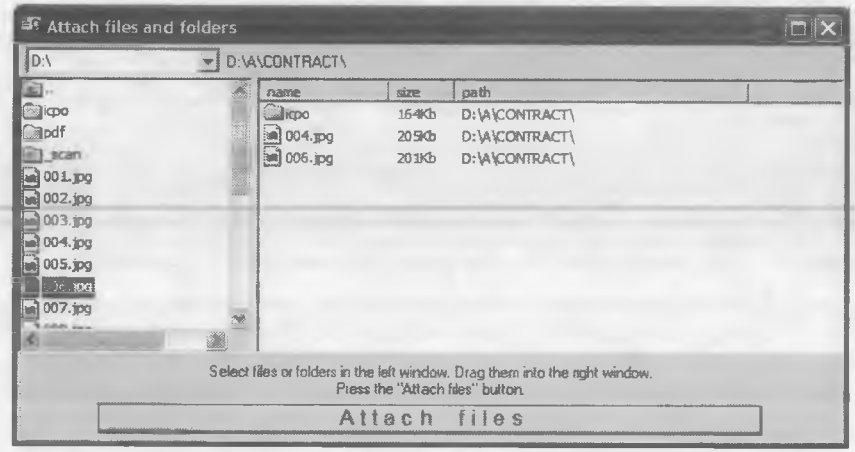



***Рис. 9.8.*** *Присоединение документов к письму*

В общем, если вы уже умеете пользоваться Outlook Express или The Bat, переход на эту или подобную программу для вас не составит труда.

## Резюме

Рассмотренные программы для шифрования электронной почты позволяют:

- ✓ устанавливать защищенную связь с новыми корреспондентами без личных встреч и согласования паролей, используемых для шифрования;
- ✓ шифровать большие объемы пересылаемой информации, используя надежные алгоритмы шифрования.

# Глава 10

## Написано пером, не вырубишь и топором...
*(как утаить свои мысли)*

*Спокойно спится только тому, кто лучше вооружен.*

*NN*

**В этой главе:**

- Интернет-пейджер — ваш сетевой мобильник.
- История ICQ.
- Как работает интернет-пейджер.
- Как шифруют чат.

Отдельной темой является использование интернет-пейджеров, или так называемых асек, позволяющих обмениваться сообщениями в режиме реального времени с любым человеком в сети. Их повсеместное распространение среди пользователей совпало по времени с триумфальным нашествием мобильников, да, по сути, интернет-пейджер и явился сетевым аналогом мобильного телефона.

***ИЛЛЮСТРАЦИЯ:***

***http://www.contentfiltering.ru/doc.asp?ob_no=585***

*Результаты исследования дают возможность утверждать, что интернет-пейджеры стали стандартом де-факто для деловых коммуникаций. Абсолютное большинство пользователей успешно применяют его для переговоров с коллегами, партне-*

*рами и заказчиками для решения оперативных бизнес-вопросов. Этот вывод подтверждается данными аналитического центра Radicati Group, согласно которому 85% компаний уже взяли на вооружение IM; на конец 2004 г. в мире было зарегистрировано около 130 миллионов пользователей IM различных платформ. Важно отметить, что интернет-пейджеры не являются конкурентом традиционным каналам общения (например, электронной почте), но средством коммуникаций нового уровня. Оно отличается большей оперативностью, удобством, простотой, символизирует высокую степень доверия между сторонами.*

Появление сотен модификаций интернет-пейджеров, привязанных фактически к одному стандарту порядка организации связи, породило множество угроз со стороны «теневых сил» сети.

***ИЛЛЮСТРАЦИИ:***

***http://www.antimalware.ru/index.phtml?part=news1&newsid=1&arc=0***

***Новый IM-червь приносит с собой целый букет вредоносных программ***

*Секьюрити-эксперты из компании FaceTime Communications, которая продает продукты для защиты сетей интернет-пейджеров, предупредили, что безымянный червь содержит коктейль из вредоносного ПО, включая так называемый rootkit — хакерский инструмент, который, проникнув в компьютер, прячется от защитного ПО и перехватывает управление системой.*

*Атаки IM-червей и вредоносного кода становятся все интенсивнее. Согласно недавнему отчету IMlogic в третьем квартале 2005 года число угроз, обнаруживаемых в сетях интернет-пейджеров и пиринговых сетях, выросло по сравнению с тем, что было год назад, на 3295%.*

***http://itware.com.ua/news/9157/print/***

***Защита интернет-пейджера Trillian дала трещину***

*Специалисты сообщили об опасной ошибке, обнаруженной в популярном продукте компании Cerulean Studios. Воспользо-*

*вавшись найденным в Trillian изъяном, злоумышленник может закрывать приложения на ПК пользователя и даже полностью перехватить управление системой.*

***http://www.webplanet.ru/news/software/2002/5/13/869.html***

***У пейджера MSN снова проблемы***

*Как выяснилось, интернет-пейджер MSN Messenger, пользующийся в США и других западных странах довольно высокой популярностью, предоставляет хакерам возможность для несанкционированного проникновения на компьютер пользователя этой программы. Обнаруженный «критический» недостаток в защищенности столь популярного ПО стал последним сообщением о неблагонадежности программ от Microsoft.*

Особые неприятности бизнесменам доставляет сочетание широкой распространенности интернет-пейджеров с практически полным отсутствием навыков защиты конфиденциальной информации у многих пользователей.

***ИЛЛЮСТРАЦИИ:***

***http://www.cnews.ru/reviews/free/security2005/articles/im.shtml***

*54% опрошенных заявили, что никогда не обменивались секретными данными по интернет-пейджерам. Соответственно, 46% честно признали, что такие факты имели место. Более того, каждый четвертый респондент (27%) считает, что его коллеги по работе обмениваются конфиденциальной информацией по IM.*

***ПОЛЕЗНАЯ ИНФОРМАЦИЯ***

В 1996 г. малоизвестная израильская компания Mirabilis, основанная несколькими студентами, выпустила первую программу интернет-пейджер — ICQ (известную у русскоязычных пользователей как «Аська»), совершив, тем самым, настоящую революцию в области общения в сети. ICQ совмещает возможности электронной почты и чата. Она позволяет общаться в режиме реального времени, но в то же время для связи с собеседн-

ником не требуется его обязательное присутствие в Интернете. В этом случае сообщение дойдет до адресата при его следующем выходе в сеть. Кроме того, при использовании ICQ не нужно каждый раз искать своего собеседника: после запуска программы сразу можно начинать общение (конечно, при условии, что у собеседника она тоже запущена). Поиск людей — это еще одна уникальная возможность, которая реализована в ICQ, позволяющая найти любого человека, подключенного к сервису. Плюс к этому программа поддерживает возможность обмена файлами и сетевые игры. ICQ непрерывно сообщает, кто из ваших друзей и партнеров находится в данный момент в сети. Программа работает в фоновом режиме и не занимает много памяти. Вы можете работать с другими приложениями, ICQ сообщит вам, когда кто-либо пытается выйти с вами на связь, если же вам некогда, запишет приходящие сообщения, не отрывая вас от работы. Оцените успех: всего год спустя после выпуска ICQ компания Mirabillis была выкуплена крупнейшим американским провайдером America On-Line за 287 миллионов долларов (на создание же программы авторами было истрачено около ста тысяч). В настоящее время пользователями ICQ является более двухсот миллионов человек.

***ИЛЛЮСТРАЦИЯ:***

***http://www.shopnot.ru/index.php?id_news=1088&page=54***

*Как показали результаты онлайнового опроса, проведенного компанией Infowatch, среди российских пользователей Интернета не пользуются на работе интернет-пейджерами лишь 13% респондентов, 45% опрошенных используют их постоянно, а 42% — время от времени. Почти половина опрошенных (46%) признали, что обмениваются через интернет-пейджеры конфиденциальной информацией.*

Столь впечатляющие результаты породили множество подражателей и продолжателей в разработке программ-коммуникаторов (наиболее известные: MSN Messenger, Miranda, Yahoo! Messenger, Trillian), развивших заложенные в ICQ идеи и воз-

можности (программное обеспечение этого типа получило название Instant Messaging, сокращенно IM, или IM-клиенты). Давайте разберемся в механизме работы программ этого типа.

Принцип работы ICQ довольно прост. Любому компьютеру, подключенному к Интернету, обязательно должна присваивается уникальная (в глобальном смысле) цифровая комбинация, называемая IP-адресом. Это позволяет различным программам, функционирующим в сети, работать друг с другом, обеспечивая единое информационное пространство. Но для обычных пользователей этот IP-адрес при входе в сеть изменяется. Чтобы осуществлять постоянную идентификацию абонентов были созданы специальные серверы, зарегистрировавшись на одном из которых, пользователь ICQ получает свой UIN (Universal Internet Number, — своеобразный постоянный адрес абонента), после чего может общаться с любым пользователем ICQ в реальном времени (рис. 10.1).

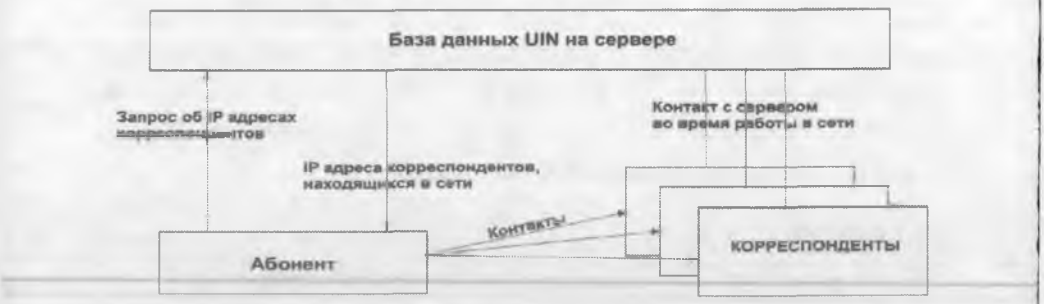



***Рис. 10.1.*** *Схема организации связи с помощью интернет-пейджера*

При подключении к сети программа, коммуникатор информирует сервер, что программа с таким-то UIN подключилась к сети, сообщает свой текущий IP-адрес и запрашивает информацию, находятся ли в сети ее корреспонденты (UIN которых в нее введен). Если кто-либо из корреспондентов к сети подключен, с сервера поступают сведения о его IP-адресе, а программа корреспондента информируется в свою очередь об IP-адресе абонента. Программы абонента и корреспонден-

та сообщают своим владельцам о том, что между ними установлен контакт и при желании они могут начинать прямое общение.

*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*Звонок в пейджинговую компанию:*

*— Девушка, вы конфиденциальность сообщений соблюдаете?*

*— Да, конечно!*

*— Точно?*

*— Точно.*

*— Тогда передайте абоненту № 8246: «Вася! Забери труп из багажника!»*

Использованию интернет-пейджеров в корпоративной сети сопутствует весь спектр традиционных угроз, которые трудно предотвратить обычными средствами защиты, пока еще не адаптированными для контроля IM-клиентов: заражение червями, проникновение троянских коней, утечка секретной информации, кража паролей и т.п. Блокирование для сотрудников доступа к IM-серверам (например, к http://www.icq.com) эффекта не дает — серверов стало слишком много, и сменить канал разговора труда не представляет, а, кроме того, интернет-пейджер — штука очень удобная. Если сотрудники используют его для делового общения, эффективность их работы существенно повышается.

Хорошим выходом из создавшегося положения является использование интернет-пейджеров, шифрующих сообщения. Это позволяет беспрепятственно общаться сотрудникам в рамках предприятия (включая удаленные филиалы), предотвращает случайную утечку информации, обусловленную неосторожностью работников, делает маловероятным попадание

каких-либо вредоносных программ через IM-клиенты. Такое решение, естественно, должно сочетаться с запретом на использование в компании интернет-пейджеров, не поддерживающих режима секретности и жестким контролем выполнения этого распоряжения.


Методы шифрования сообщений в интернет-пейджерах аналогичны методам, используемым в почтовых программах. Простота реализации защиты вызвала буквально взрывной рост числа предлагаемых версий пейджеров, обеспечивающих шифрование чата. Многие пейджеры, приближаясь по техническим возможностям к почтовым программам, обрастают также функциями программ IP-телефонии и средств шифрования файлов на локальных компьютерах, становясь в умелых руках мощным инструментом защиты потока деловой информации. Наиболее часто используются три способа скрытия сообщений от посторонних глаз:

- ✓ защита сообщений с помощью асимметричных алгоритмов шифрования (рис. 10.2);

- ✓ защита сообщений с помощью симметричных алгоритмов шифрования с передачей ключа шифрования по другому каналу связи (рис. 10.3);
- ✓ обмен сообщениями через удаленный сервер, формирующий защищенные SSL каналы связи с абонентами (рис. 10.4).

Каждый из этих методов имеет свои достоинства и выбор программы, использующей для защиты пересылаемых сообщений тот или иной прием, зависит только от конкретных условий, в которых оказался пользователь.

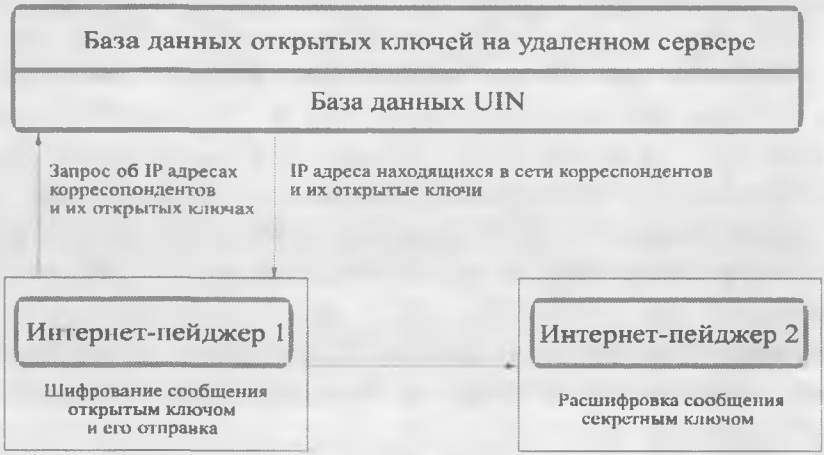



***Рис. 10.2.*** *Схема организации связи при защите сообщений с помощью асимметричных алгоритмов шифрования*

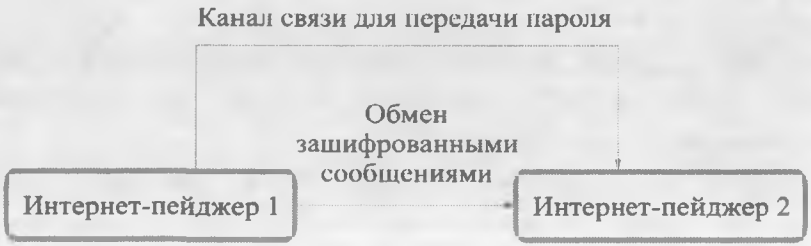



***Рис. 10.3.*** *Схема организации связи при защите сообщений с помощью симметричных алгоритмов шифрования*

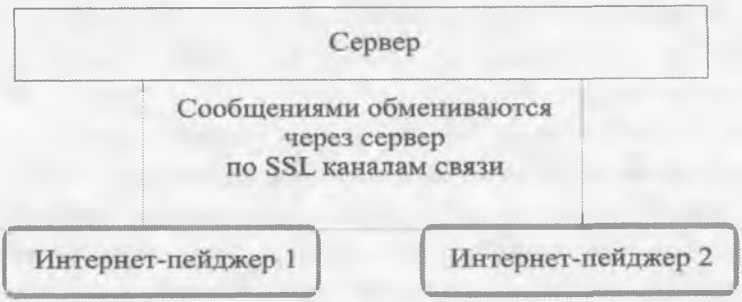



***Рис. 10.4.*** *Схема организации связи через удаленный сервер, формирующий защищенные SSL каналы связи с абонентами*

Первый метод защиты удобен при организации связи между абонентами, не имеющими других защищенных каналов связи, но использующие его пейджеры применяют в качестве уникального идентификатора электронный почтовый адрес пользователя и не могут поддерживать связь с традиционными интернет-пейджерами (ICQ, Miranda, AOL и т.д.). Поэтому основная область их применения — обмен шифрованными сообщениями внутри групп лиц, уже установивших первый контакт иными методами (например, через обычный незащищенный пейджер).

Использование второго способа защиты ограничено необходимостью согласования используемых при шифровании ключей. Это подразумевает либо предварительную личную встречу будущих друзей по переписке, либо наличие защищенного канала связи между ними, либо внесение изменений в программный код пейджера, присваивающих в скрытом виде тот или иной пароль каждому экземпляру программы (это удобно при организации внутрикорпоративных сетей).

Третий способ защиты более или менее гарантирует безопасность только при использовании во внутрикорпоративных сетях (что толку защищать каналы связи, если пересылаемую по защищенному каналу информацию можно скопировать на сервере? В этом случае получается, что тот, кто имеет контроль

над сервером, контролирует и проходящую через него информацию).

### *НЕОБХОДИМЫЕ НАВЫКИ*

Список наиболее распространенных пейджеров, обеспечивающих шифрование пересылаемых сообщений, приведен в табл. 10.1–10.4. Большинство из них дает примерно одинаковый уровень защиты, отличаясь в основном, комфортностью для пользователя и наличием дополнительных функций. Значительное число пейджеров бесплатно, что позволяет как беспрепятственно тестировать их в полном объеме, так и без материальных затрат заменять их, если при тестировании они не устраивают вас по каким-либо параметрам.

*Таблица 10.1*

| **Интернет-пейджеры, использующие асимметричные алгоритмы шифрования** | **Характеристики** |
|---|---|
| **CryptoHeaven**<br>9,6 Mb<br>$29,00–599,00 ежегодно (в зависимости от предоставляемого объема пространства на сервере)<br>http://www.cryptoheaven.com | Отлично оформленная программа, совмещающая функции интернет-пейджера и почтового клиента. Шифрует сообщения открытым ключом до 4096 бит и сеансовым симметричным ключом в 256 бит. |
| **Safe Chat**<br>1,02 Mb<br>Free<br>http://www.safechaos.com/sc.htm | Очень простой в пользовании интернет-пейджер, совмещающий свои функции с функцией почтовой программы. Шифрует сообщения открытым ключом до 4096 бит и сеансовым симметричным ключом до 448 бит. |
| **X-IM**<br>1.85 Mb<br>Free<br>http://x-im.net | Очень простая в пользовании и добротно сделанная программа. Шифрует сообщения открытым ключом в 2048 бит и сессионным ключом 256 бит. |

*Окончание табл. 10.1*

| Интернет-пейджеры, использующие асимметричные алгоритмы шифрования | Характеристики |
|---|---|
| **BitWise Chat**<br>3,15 Mb<br>Free<br>http://www.bitwisechat.com | Простой в использовании и непритязательный в оформлении интернет-пейджер. Использует 1024-битовый открытый ключ и 256 битовый сеансовый симметричный. |
| **iGo Incognito**<br>1,5 Mb<br>Free<br>http://www.igo-incognito.com | Очень простая, но не слишком удобная программа. Позволяет шифровать сообщения открытыми ключами в 512 и 768 бит. |
| **Blowsearch Secured Messenger**<br>3,754 Mb<br>http://www.blowsearch.com | Сложный в настройке и не слишком удобный пейджер. Бесплатная версия шифрует сообщения ключом в 56 бит, платные (по мере увеличения стоимости) до 4096 бит. |

*Таблица 10.2*

| Интернет-пейджеры, использующие симметричные алгоритмы шифрования | Характеристики |
|---|---|
| **TrilogyEC Pro**<br>5.35 Mb<br>Free<br>http://trilogyec.com | Современно оформленный интернет-пейджер, позволяющий шифровать сообщения симметричным ключом длиной 256 бит. Поддерживает интернет-телефонию. |
| **Filetopia**<br>1,77 Mb<br>Free<br>http://www.filetopia.org/home.htm | Хорошо оформленная, но не слишком удобная программа. Поддерживает 8 симметричных алгоритмов шифрования. |

*Окончание табл. 10.2*

| Интернет-пейджеры, использующие симметричные алгоритмы шифрования | Характеристики |
|---|---|
| **GlChat**<br>1.36 Mb<br>$9,95<br>http://www.glnetsoftware.com | Очень простой пейджер, использующий для шифрования сообщений симметричные ключи длиной до 256 бит. |

*Таблица 10.3*

| Интернет-пейджеры, использующие SSL канал связи с сервером | Характеристики |
|---|---|
| **Mirador Instant Messenger**<br>38,93 Mb<br>$333,50–1593,30 (в зависимости от числа пользователей)<br>http://e-securion.com | Многофункциональный и хорошо оформленный пейджер для поддержания связи в закрытых корпоративных сетях. Обеспечивает защиту сообщений путем передачи их через SSL каналы связи между центральным сервером и пользователями. |
| **DeskNow WebMessenger**<br>23,8 Mb<br>$49,00<br>http://www.desknow.com/desknowwm/index.html | Простой по оформлению интернет-пейджер с очень сложной подготовкой к началу работы. Декларируя себя как web-пейджер, требует перекачки с сайта большого файла. Обеспечивает защиту сообщений путем передачи их через SSL канал связи. |

*Таблица 10.4*

| Интернет-пейджеры, разработчики которых не сообщают об используемых методах защиты сообщений | Характеристики |
|---|---|
| **Chat Watch Professional**<br>2.4 Mb<br>$60,00<br>http://www.zemericks.com | Прекрасно оформленный интернет-пейджер с возможностью отсылки писем по электронной почте. Разработчики декларируют шифрование. |

*Окончание табл. 10.4*

| **Интернет-пейджеры, разработчики которых не сообщают об используемых методах защиты сообщений** | **Характеристики** |
|---|---|
| | пересылаемой корреспонденции. К сожалению, ни в программе, ни на сайте не указаны алгоритмы шифрования и размеры используемых ключей |
| **Trillian Basic**<br>8.58 Mb<br>Free<br>http://www.ceruleanstudios.com | Отлично оформленный интернет-пейджер с многочисленными функциями и настройками. Разработчики декларируют шифрование пересылаемой корреспонденции. К сожалению, ни в программе, ни на сайте не указаны алгоритмы шифрования и размеры используемых ключей. |
| **Yak!**<br>1,04 Mb<br>$6,50<br>http://www.digicraft.com.au/yak | Очень простой австралийский пейджер. Разработчики утверждают, что пересылаемые сообщения шифруются по алгоритму TwoFish. Так как алгоритм шифрования симметричный, а введение пароля при подготовке сообщения не требуется, наличие защиты у пересылаемых сообщений представляется сомнительным. |

Давайте запустим один из этих пейджеров и посмотрим, как он работает. В качестве опытного образца попробуем американский Safe Chat (рис. 10.5), отличающийся предельной простотой при запуске и в эксплуатации. Он автоматически инсталлируется одновременно с программой Safe Express, описанной в предыдущей главе, использует ее ключи и базу данных учетных записей (рис. 10.6). Интерфейс пейджера традиционен и сразу понятен пользователям, уже имевшим дело с программами аналогичного назначения.

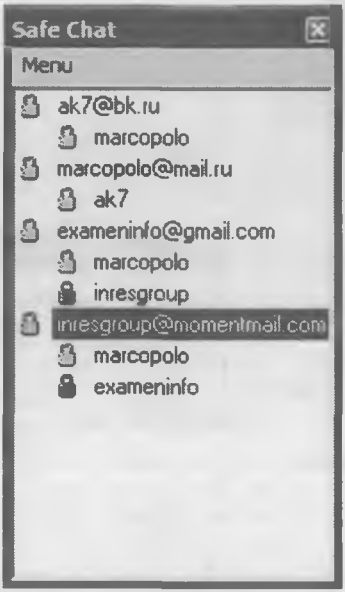



***Рис. 10.5.*** *Окно контактов интернет-пейджера Safe Chat*

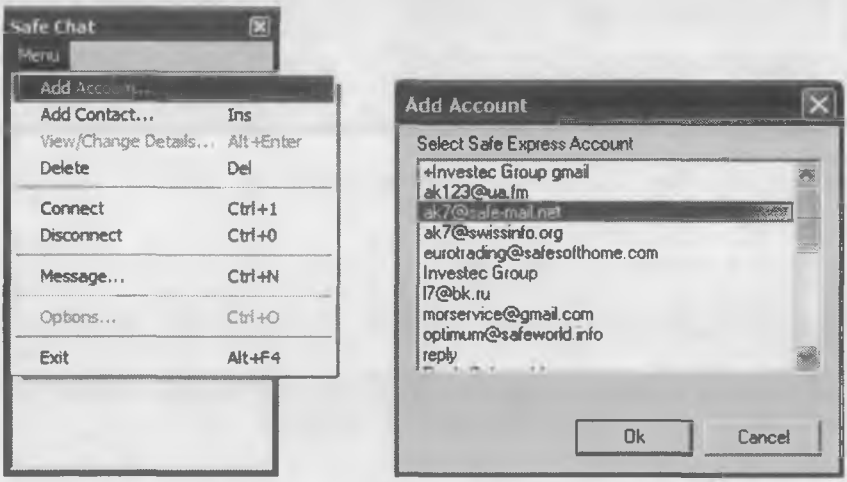



***Рис. 10.6.*** *Создание учетной записи в интернет-пейджере*

Внеся в базу данных контактов учетной записи (рис. 10.7) сведения об абонентах, с которыми будет осуществляться переписка, и присвоив им контактные имена, вы можете начинать обмен шифрованными посланиями.

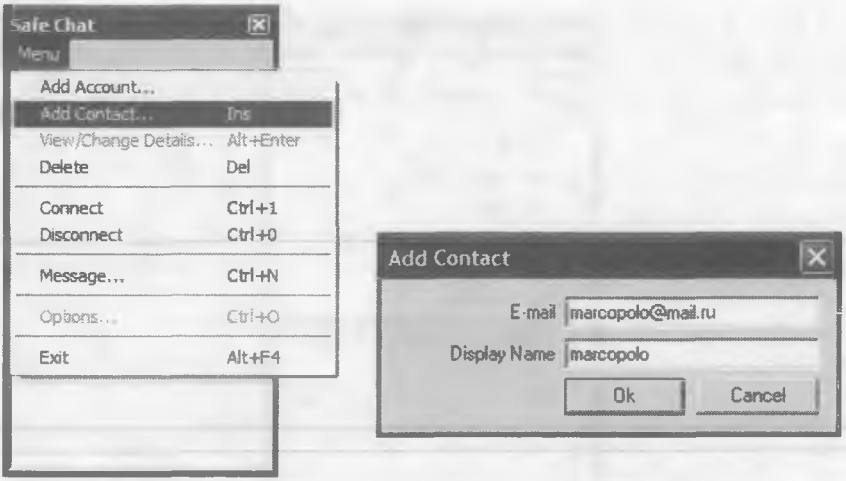



***Рис. 10.7.*** *Внесение нового корреспондента в базу данных интернет-пейджера*

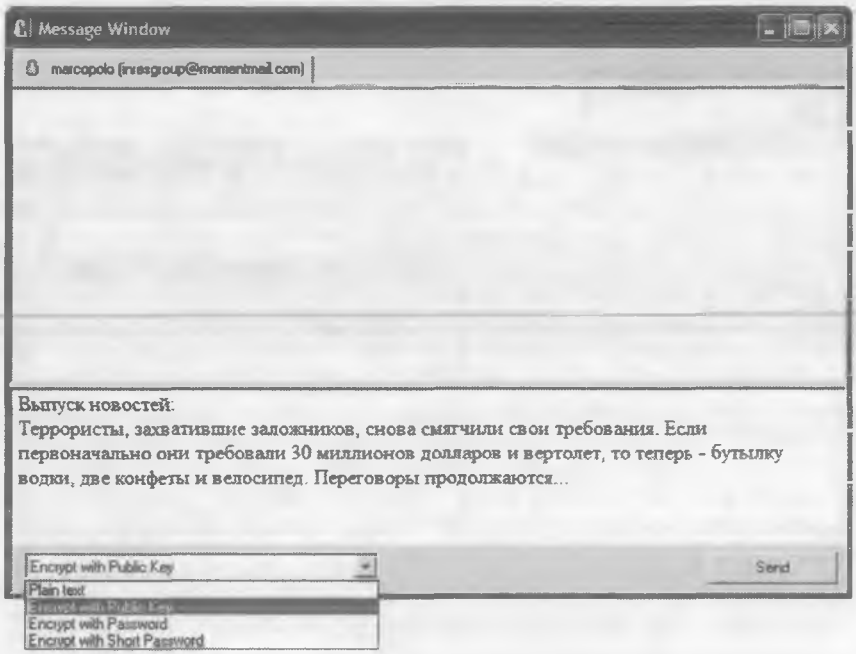



***Рис. 10.8.*** *Выбор режима шифрования передаваемой информации*

Сообщения вы можете шифровать открытым ключом получателя, симметричным ключом, созданным из согласованного между вами пароля, или не шифровать вовсе (рис. 10.8). Всю работу по шифрованию и расшифрованию ваших сообщений пейджер выполнит автоматически, и вы сможете пользоваться ним как привычной «аськой» (рис. 10.9).

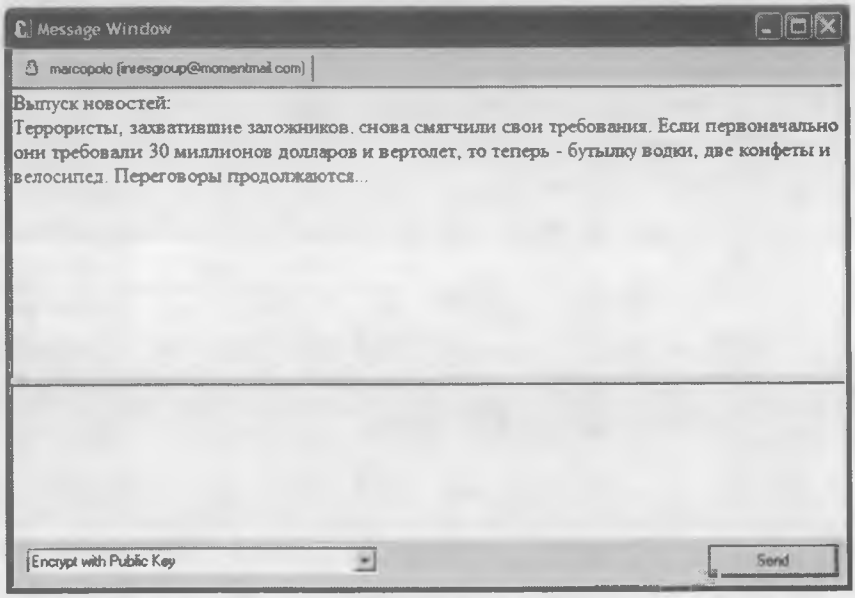



***Рис. 10.9.*** *Информация зашифрована, передана другому абоненту и расшифрована*

Размер ключей, которые использует пейджер для шифрования сообщений разным абонентам, соответствует размеру ключей, установленных при переписке с ними почтовой программы Safe Express.

*Анекдот*
*в тему:*

~ ~ ~ ~ ~ ~

*Восточная чайхана, к посетителю подбегает мальчик.*
*— Дядя Ахмед, вас ждет дядя Али.*
*— Спасибо, Пейджер-джан.*

## Резюме

Интернет-пейджеры в последние годы прошли путь от просто удобного средства общения в мощный инструмент организации информационных потоков. Какие дополнительные возможности приобрели их современные модели?

- ✓ пересылка приложенных файлов;
- ✓ интернет-телефония;
- ✓ полноценный чат;
- ✓ надежная защита содержания передаваемых сообщений.

Адаптация уже имеющихся программ для карманных компьютеров — дело недолгое. Можно ожидать, что интернет-пейджеры станут основным средством коммуникации ближайшего будущего.

# Глава 11

## Тихие заводи Сети
### (как защитить свой круг общения)

*Организация не терпит импровизации.*
***Генрих Леер, военный теоретик***

**В этой главе:**

- Как заставить сотрудников попридержать язык.
- Что такое виртуальная сеть.
- Как защищают информацию в частных виртуальных сетях.
- На какую секретность можно надеяться.

Сеть общедоступна. Пользуясь интернет-пейджером или электронной почтой, вы ежедневно оставляете в ней сотни следов своего пребывания, фиксируя которые, можно узнать многое о вас, ваших привычках, интересах, контактах, текущем состоянии дел и ожидаемых в них переменах. Можно ли в таких условиях обеспечить себя защитой? Да, можно, шифруя пересылаемую информацию или пользуясь почтовыми серверами, шифрующими переписку и обеспечивающими защиту канала связи с клиентами. Эти приемы хороши для небольших организаций и частных пользователей, понимающих важность конфиденциальности и необходимость защиты передаваемой информации. А как быть крупным фирмам? Играющий роль Большого Босса клерк центрального офиса пишет поручение подчиненному филиалу и отправляет его по открытой сети электронной почтой, даже не задумываясь, нет ли в тексте информации, могущей навредить его конторе. Журналист направляет в редакцию отчет с места проис-

шествия, не понимая, что своим «вниманием к деталям» он раскрывает тайны следствия. Главный редактор, быть может, это сообразит и не подпишет такую статью в печать, но прошедший по сети материал вполне может дать лишний шанс технически грамотным террористам уйти от ответственности. Как довести до каждого сотрудника необходимость шифровать передаваемую информацию? Как обязать, как заставить его это делать?

Ответ простой: как в армии. Солдат не выбирает цвета формы, меню на обед или марки личного оружия. Что дали, то и носи, что на стол поставили, то и лопай, а из того, что в руках оказалось, — стреляй (если жить хочешь, конечно).

## Запомните

*О вкусах не спорят. Их навязывают.*

***Г. Малкин***

Пытаться в крупной компании при существующей текучести кадров довести до каждого сотрудника необходимость поддерживать режим секретности, объяснить опасности, возникающие при отсутствии дисциплины его соблюдения, пробудить сознательность и патриотизм по отношению к фирме — дело затратное и бесперспективное. Вот тут-то и пригодится армейский опыт. Выдали каждому сотруднику программу-коммуникатор, которая сама автоматически шифрует его переписку с другими работниками, приказали ею пользоваться, пригрозили, что появление в его компьютере других программ этого типа лишит его премии, милости начальства, перспектив служебного роста, социального пакета и т.п., он и будет ее применять, ругаясь себе под нос, понимая или не понимая (это уже не важно), зачем и кому это нужно. Контроль за качеством выбранных программ и обучением персонала — на специалистах, контроль за применением этих программ работниками — на начальниках среднего звена, надеющихся пересесть в кабинеты попросторнее. Большинство служащих в этом случае и подозревать не будут, что их переписка зашифрована, а каналы общения надежно защищены.

## Запомните

*Будущее — это тщательно обезвреженное настоящее.*

***А. и Б. Стругацкие***

Этот вариант организации контактов в крупной компании возможен при использовании защищенных сетей связи между ее сотрудниками или подразделениями, партнерами и поставщиками. Что же собой представляет защищенная сеть? Давайте остановимся на этом подробнее.

***ПОЛЕЗНАЯ ИНФОРМАЦИЯ***

Погонять мячик с друзьями на ухоженном футбольном поле можно двумя способами, существенно отличающимися по затратам: купить, например, стадион и пользоваться им, когда заблагорассудится, или оплатить только время для игры, — т.е. арендовать стадион или даже одну футбольную площадку. Создать частную сеть для обмена информацией также можно двумя путями: проложив собственные линии связи между подразделениями компании или, оплатив время за пользование сетями, уже существующими. Понятно, что второй способ по деньгам гораздо предпочтительнее.

В Советском Союзе денег особо не считали и ставили всем более-менее значащим что-то в государстве людям на столы «вертушки» — телефоны качественной спецсвязи, обеспечивавшие для особо важных персон и защиту их переговоров. Какое-то время защищенная связь была прерогативой очень ограниченного круга лиц — государственных чиновников, высшего военного и партийного руководства. Бурная неконтролируемая телефонизация, начавшаяся во всех странах в конце 50-х г., облегчила доступ к телефонным сетям любым заинтересованным лицам: журналистам, частным детективам, любителям поболтать на халяву, неудачливым конкурентам, подозрительным мужьям и ревнивым женам, а миниатюризация средств прослушивания и подслушивания породила множество любителей извлечь выгоду из чужих слов, опрометчиво сказанных в телефонную трубку.

*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*Сидит мужчина в надувной лодке и рыбачит. Сидит уже три часа, но все не клюет.*

*— О Боже, — взмолился мужчина, — пошли хотя бы одну большую рыбу на обед!*

*Всплывает огромная тигровая акула:*

*— Ну?*

Этот взрывной рост числа ушей, прислушивающихся к словам, несущимся по линиям тогда еще только телефонной связи, вызвал появление в сфере услуг новой: частной защиты переговоров в телефонных сетях. Понятие Centrex (Central office exchange service) появилось в США как общее название способа предоставления услуг деловой связи абонентам нескольких компаний на основе совместно используемого оборудования одной учрежденческой станции PBX (Private Branch Exchange). Основное преимущество Centrex в том, что компании при создании выделенных корпоративных сетей экономили значительные средства, необходимые на покупку, монтаж и эксплуатацию собственных станций. Хотя для связи между собой абоненты Centrex частично используют ресурсы и оборудование сети общего пользования, сами они образуют так называемые замкнутые группы пользователей CUG (Closed Users Group) с ограниченным доступом извне, для которых реализуются виртуальные PBX.

*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*Звонок по телефону:*

*— Здравствуйте, это квартира Иванова Сергея Петровича?*

*— Нет, это квартира Каца Арона Самуиловича.*

*— Простите, это 550-3311?*

*— Нет, это 550-3312.*

*— Надо же, в седьмом знаке ошибка, а какой эффект...*

Если в 60–80-е гг. телекоммуникационные сети занимались в основном передачей голоса, а доставка данных была чем-то сопутствующим, то на сегодняшний день это соотношение из-

менилось на обратное. Уже к концу 90-х гг. передаваемый поток данных значительно превышал поток голосового трафика. На первый план вышли виртуальные сети VPN (Virtual Private Network), работающие на базе Интернета. VPN через Интернет соединяют множество удаленных пользователей или удаленные офисы с сетью предприятия. Некоторые предприятия внедряют аппаратные решения VPN с целью усиления защиты, другие используют только программные реализации. Аппаратные решения VPN выпускают различные производители, в том числе крупнейшие: Cisco, Nortel, IBM и Checkpoint. Схема соединения для связи со служащими или с представительствами компаний в других городах и странах очень проста (рис. 11.1). Удаленный пользователь посылает вызов в точку присутствия местного сервис-провайдера услуг Интернета (ISP). Затем вызов шифруется, проходит через Интернет и соединяется с сервером предприятия абонента.

При этом формируется канал VPN, обычно называемый «туннель», по которому можно производить защищенный обмен данными между двумя конечными узлами. Этот туннель «непрозрачен» для всех остальных пользователей, включая провайдера, т.е. VPN решения, вне зависимости от того, аппаратные они или программные, действуют как специализированные маршрутизаторы, расположенные на концах IP-соединений между пользователями. Когда клиент передаёт пакет, он посылает его через маршрутизатор или шлюз, добавляющий заголовок проверки подлинности (Authentication Header) с информацией о маршрутизации и подлинности. Затем данные кодируются и вместе с инструкциями по декодированию и обработке становятся инкапсулированными защищенными полезными данными (Encapsulating Security Payload). Получающий маршрутизатор VPN отбрасывает информацию заголовка, расшифровывает данные и направляет пакет по назначению (компьютеру или локальной сети). Таким образом, потребительская сущность VPN — создание

«виртуальных защищенных туннелей» в Сети, позволяющих организовать защищенный удаленный доступ через открытые каналы Интернета к серверам баз данных, FTP и почтовым серверам. Физическая сущность технологии VPN заключается в способности защитить трафик информационных систем, аудиовидеоконференций, систем электронной коммерции и т.п. На каком варианте организации виртуальной сети остановиться? Крупная компания, имеющая много удаленных офисов, может позволить себе более дорогое аппаратное решение проблемы; не слишком большая фирма, личный состав которой подвижен или работает на дому, предпочтет программный вариант. Она может либо примкнуть к одной из действующих сетей и пользоваться ее услугами как сторонней организации (ведь обслуживается же она в охранном агентстве, у местного провайдера или в сети проката оборудования?), либо купить и установить для внутреннего спокойствия ее хозяев собственный VPN сервер.

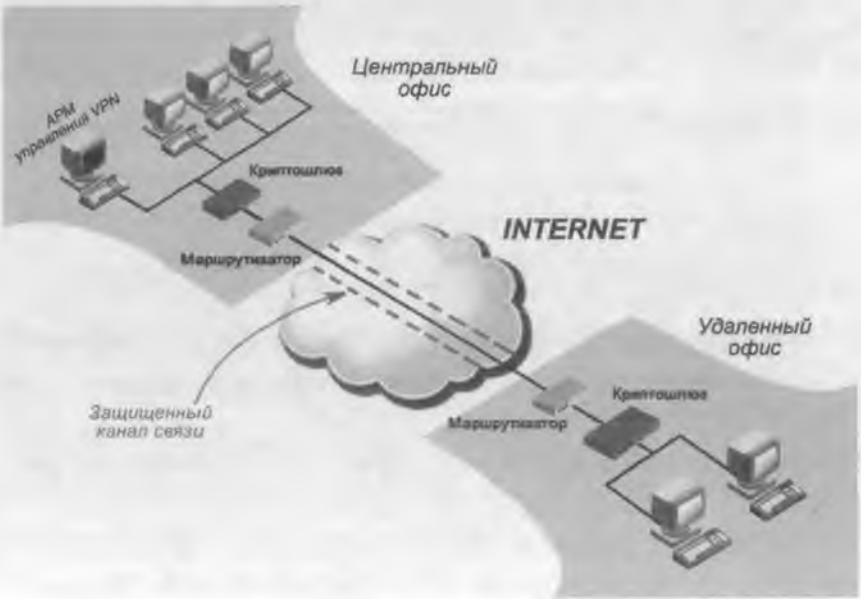



***Рис. 11.1.*** *Схема соединения для VPN связи*

*Анекдот в тему:*

*— Дорогой, ты кого больше любишь? Меня или эту дурацкую штуку, за которой ты ПРОВОДИШЬ ЦЕЛЫЙ ДЕНЬ, СВОЛОЧЬ!!!!!*

*— Ну, киса, как ты можешь сравнивать неодушевлённый предмет с КОМПЬЮТЕРОМ!*

Конфигурацию виртуальной частной сети в зависимости от конкретных потребностей можно легко менять. Например, работающему на дому рядовому сотруднику может быть предоставлен ограниченный доступ к базе данных предприятия, а менеджеру удаленного офиса или руководителю компании — широкие права доступа, командированного работника можно ограничить только каналом обмена информацией с непосредственным начальником, а путешествующего главу фирмы — возможностью удаленного контроля за действиями любого из сотрудников.

*Запомните*

*Правила для всех одинаковые, только исключения разные.*

***Д. Рудный***

Каналы VPN защищены обычными алгоритмами шифрования, заложенными в стандарты протоколов безопасности (IPSec, PPTP, L2TP и т.д.), самым распространенным из которых является IPsec (Internet Protocol Security). Протокол IPsec обеспечивает защиту на сетевом уровне и требует поддержки стандарта IPsec только от общающихся между собой устройств по обе стороны соединения. Все остальные устройства, расположенные между ними, просто обеспечивают обычный трафик

IP-пакетов. Протоколы безопасности не шифруют данные, а лишь определяют, как используются алгоритмы шифрования, контролируют порядок обмена ключами, их размеры и сроки службы, ряд других условий, необходимых для построения VPN (контроль целостности, аутентификацию абонентов и т.д.), короче, следят за четким выполнением программы работы виртуальной сети.

*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*Потерпел крушение круизный лайнер. Спаслись человек тридцать и высадились на необитаемом острове. Через несколько дней начался голод. Решили потянуть спички, кого съесть первым. Съели первого. Через несколько дней — второго. И так далее. Дошла очередь до нового русского.*

*— Ну все, друг. Снимай свой малиновый пиджак, будем тебя есть.*

*— Пацаны, да вы шо! Я щас братанов через спутник наберу, они на вертолете привезут еду, выпивку и девочек, а если надо, то и по домам развезут.*

*— Так чего же ты молчал? Столько народа съели!*

*— Но я же думал, что это все входит в программу круиза!*

### *НЕОБХОДИМЫЕ НАВЫКИ*

Возможность создания закрытых информационных сетей, в которых аудиовидеосвязь и передаваемые данные надежно защищены, привлекает многих корпоративных клиентов в нашей стране. Появились тысячи больших и не очень фирм, которые хотят общаться со своими далеко проживающими «дочками» или «братьями», эффективно ими управлять и взаимодейство-

вать, не обременяя информацией о своих методах работы, способах извлечения прибыли и полученных конечных результатах ни государственные службы, ни частных любителей сунуть нос в чужой карман.

### Кстати

*Немного о реинкарнации. Если ты родился в России — значит в прошлой жизни совершил что-то очень-очень плохое.*

Успешные компании, делающие бизнес в регионах, — самые первые и самые крупные клиенты операторов VPN. Прибыль, приносимая виртуальными сетями, в несколько раз превышает доходы от предоставления ставших уже обычными услуг интернет-провайдеров, объем работы при обслуживании клиентов практически не отличается, а величина первичных затрат ощутимо меньше, чем при создании клиентской сети интернет-провайдера. Это вызвало взрывной рост числа фирм, предлагающих свои услуги в качестве VPN операторов. За дело взялись сами провайдеры, представительства иностранных компаний, остатки электронных монстров советских времен, бывшие НИИ, КБ и фирмы-однодневки. Чьими же услугами воспользоваться? Какими критериями руководствоваться?

### Кстати

*Объявление в газете:*
*Быстро и качественно сделаем любую халтуру.*

В общем-то критериев два: размеры фирмы и давность ее существования. С одной стороны, слишком маленькая компания обычно новичок на рынке, набравший вчерашних студентов без опыта работы и пытающийся перепродать услуги и решения своих более крупных партнеров. С другой стороны, фирма, присутствующая на рынке достаточно давно, самим

фактом своего длительного выживания свидетельствует, что ее услуги востребованы, а продаваемые решения стоят затраченных на них денег. Несколько достаточно «старых» и крупных компаний, предлагающих свои услуги в секторе защиты частных сетей, приведены в табл. 11.1.

*Таблица 11.1*

| Название компании | Адрес сайта |
|---|---|
| **Инфотекс** | http://www.infotecs.ru |
| Aladdin Software Security | http://www.aladdin.ru |
| **Trend Micro** | http://www.trend-micro.ru |
| ДиалогНаука | http://www.antivir.ru |
| ЛАНИТ | http://www.lanit.ru |
| ТехноСерв А/С | http://www.technoserv.ru |

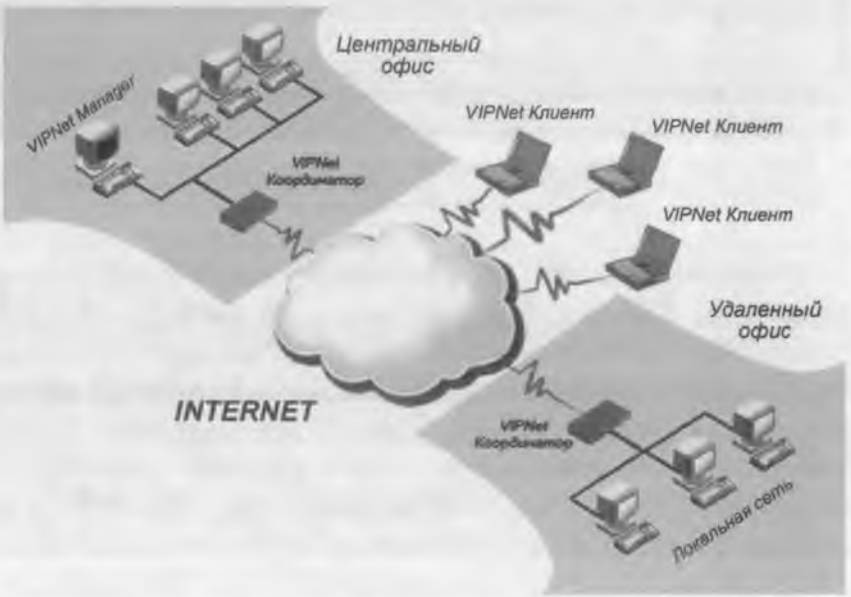



***Рис. 11.2.*** *Схема организации связи с помощью программного комплекса ViPNet компании «Инфотекс»*

Рассмотрим, как на основе программных решений создаются виртуальные сети на примере продукции компании «Инфотекс». Программный комплекс включает в себя (рис. 11.2) программы «Администратор» (в облегченной версии — «Менеджер»), «Координатор» (для подключения локальной сети) и «Клиент» (для локальных компьютеров).

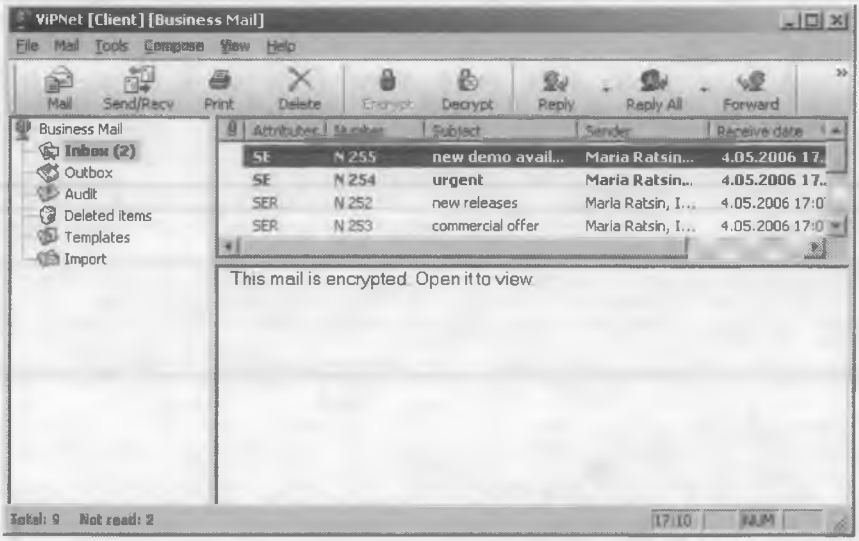



***Рис. 11.3.*** *Программа «Клиент» программного комплекса ViPNet*

Криптографическое ядро комплекса может использовать следующие криптоалгоритмы: AES (256 бит), ГОСТ (256 бит), 3DES (168 бит) и DES (56 бит). Алгоритмом по умолчанию является ГОСТ (256 бит), остальные алгоритмы могут быть по желанию выбраны самим пользователем. Длина ключа для асимметричной ключевой системы (открытый и секретный ключи) равна 1024 бит (ГОСТ Р 34.10-2001). Программное обеспечение устанавливается поверх существующей физической сети и не ухудшает ее показателей. После установки программ на все компьютеры, которые будут включены в виртуальную сеть, контакты их внутри самой

виртуальной сети (электронная почта, чат, обмен файлами) будут защищены, а связь с внесетевыми пользователями останется прежней. Используемый почтовый клиент (рис. 11.3) по внешнему виду максимально приближен к традиционным и только лишняя пара кнопок напоминает о его дополнительных возможностях.

Для оперативной связи между пользователями защищенной сети в программный комплекс включен интернет-пейджер (рис. 11.4).

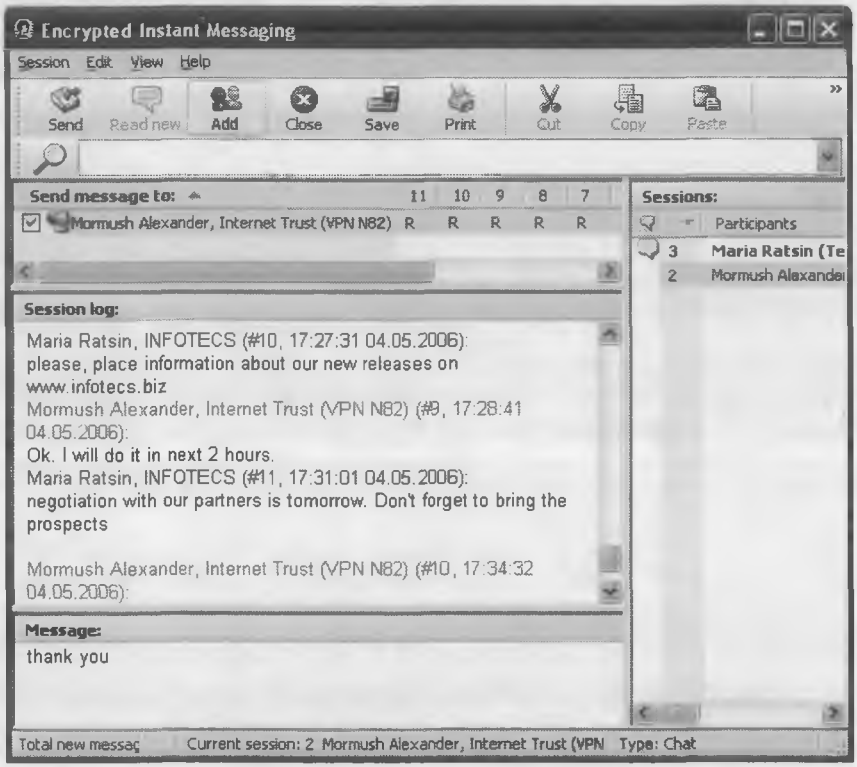



***Рис. 11.4.*** *Интернет-пейджер программного комплекса ViPNet*

Создание защищенной виртуальной сети с помощью системы ViPNet просто и дешево, а предлагаемый уровень защиты достаточно высок.

## Резюме

~ ~ ~ ~ ~

Создание собственной VPN обеспечивает:

- ✓ основанную на криптографии защиту трафика;
- ✓ возможность коммуникации с любой точкой мира, гарантирующей защиту доступа к внутренним ресурсам локальных сетей и баз данных компании;
- ✓ развитие коммуникационных систем без вкладывания значительных средств в строительство собственных выделенных линий.

# Глава 12

## Говори, говори, да не заговаривайся
### (как не бросать слов на ветер)

*Сначала трижды подумай, а потом промолчи.*

***Анри де Ренье,***
***французский писатель***

**В этой главе:**

- Телефон — источник информации о вас.
- Что такое интернет-телефония.
- Как защищают речь при использовании интернет-телефонии.
- Как правильно говорить по телефону
- Как скрыть факт наличия секрета в телефонном разговоре.

Любая армия, линии связи которой контролируются врагом, представляет собой лакомый кусочек для показательной порки и демонстрации силы противника. Это утверждение в полной мере относится и к вам. Вы, предприниматель, борющийся за успех, как и полководец, вошедший с войсками на вражескую территорию, постоянно находитесь во враждебном окружении чиновников, конкурентов и преступных группировок.

## Запомните ~~~~~~~~~~~~~~

*Закрытый рот помогает сохранить зубы.*

***Пословица***

Телефон до последнего времени являлся одним из основных средств, обеспечивающих возможность быстрого общения между удаленными партнерами или ведения переговоров с клиентами и в то же время как каналом прямой утечки информации (при прослушивании), так и косвенным источником сведений об уровне и разветвленности ваших знакомств (по фиксируемым на узле связи номерам телефонов, с которыми вы контактировали).

***ИЛЛЮСТРАЦИИ:***

***http://palm.newsru.com/world/20aug2003/proslushka.html***

*В Перу разгорается политический скандал, начало которому положил телефонный разговор президента страны Алехандро Толедо, который был незаконно записан на пленку, а затем воспроизведен в одной из программ перуанского телевидения, сообщает ИТАР-ТАСС.*

***http://www.nta-nn.ru/?id=67963***

*В Нижнем Новгороде арестованы преступники, обворовавшие квартиры, используя прослушивание телефонов. По данным следствия, члены преступной группы, подключаясь к телефонным линиям с помощью спецаппаратуры, записывали на диктофон голоса хозяев, и после проникновения в их жилье снимали квартиру с сигнализации.*

***http://www.sedmoykanal.com/news.php3?id=16347***

*...израильская полиция вела прослушивание всех разговоров, ведущихся с телефона премьер-министра Израиля Биньямина Нетаниягу, а также управляющей его канцелярии Рохамы Аб-*

*рахам. Записи подлежали все (без исключения) телефонные разговоры, включая и частные.*

***http://www.lenta.ru/world/2001/03/01/estonia/***

*В Эстонии вступило в силу постановление правительства страны, разрешающее правоохранительным органам прослушивать телефонные разговоры жителей и просматривать их электронную почту, сообщает РИА «Новости».*

**http://www.ntn.tv/ru/news/ukraine/05/07/05/1018.html**

*Заместитель министра внутренних дел Александр Фокин обвинил своего руководителя министра Юрия Луценко в шантаже и незаконном прослушивании телефонов.*

Перу, Россия, Израиль, Эстония, Украина — география случайно замеченных прессой событий. Да и можно ли называть событием то, что стало уже массовым явлением?

## *Анекдот в тему:*

~ ~ ~ ~ ~ ~ ~

*Приходит как-то журналист к новому русскому, и во время интервью замечает, что у того на столе лежат четыре сотовых телефона.*

*Не понимая юмора, он начинает осторожно расспрашивать:*

*— Скажите, пожалуйста, для чего этот аппарат?*

*— Международный!*

*— А этот?*

*— Междугородний!!*

*— А этот?*

*— Городской!!!*

*— А этот?*

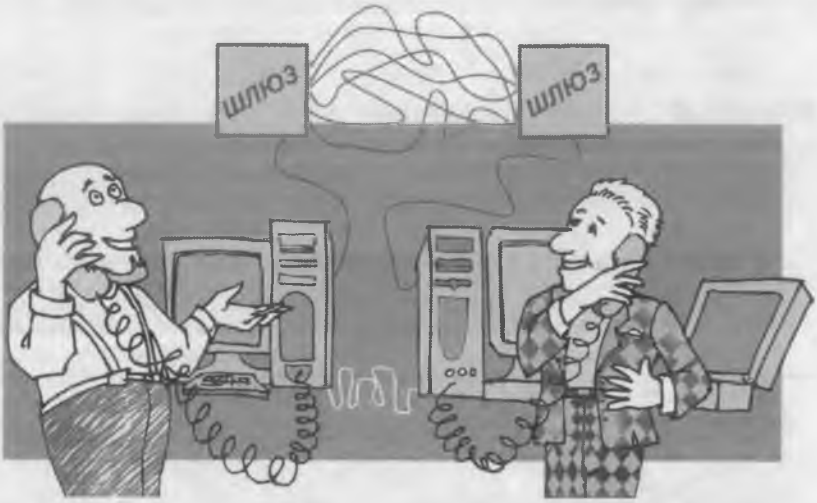
*— Да забодал ты меня, мужик, местный это, местный!!!*

Несколько облегчило защиту конфиденциальности телефонных переговоров появление IP-телефонии, все больше вытесняющей из обихода связь по обычным телефонным каналам.

### *ПОЛЕЗНАЯ ИНФОРМАЦИЯ*

При отправке электронной почты или любого online запроса, вы посылаете пакеты данных через Интернет. Эти пакеты попадают туда, куда их отправили потому, что все программы, участники общения через сеть, «разговаривают» на одном языке. Этот язык называется Интернет-протокол (Internet Protocol, или IP). IP-пакеты могут нести данные, графику, голос или видеоизображение. Под IP-телефонией понимается технология, позволяющая использовать Интернет или любую другую IP-сеть в качестве средства организации и ведения международных и междугородных телефонных разговоров.

В телефонной сети голос передается в виде аналогового или цифрового сигнала по предварительно установленному при вызове каналу связи, а при работе интернет-телефона трансформируется в пакеты цифровых данных, которые затем пересылаются по сети и расшифровываются на другом конце соединения, но только в этом случае речь идет не о прямом канале передачи. В случае использования интернет-телефона передача пакетов данных осуществляется по той же сети, по которой идет передача и других данных файлов, электронной почты и т.п. Но в сети ведь никто не знает, когда и как дойдут передаваемые данные до пункта назначения. Иногда они запаздывают, тогда происходят паузы в разговоре — ваш собеседник не услышит предложения целиком, пока не передадутся все пакеты, в которые оно было помещено. Если в сети происходит потеря пакетов, то бывает, что из предложений выпадают слова, а из фраз — целые предложения.




Существуют три варианта осуществления интернет-телефонии:

- ✓ компьютер — компьютер
- ✓ компьютер — телефон
- ✓ телефон — телефон

По технологии Компьютер — Компьютер звонки производятся с одного компьютера на другой с помощью специальных программ (табл. 12.1), которые могут быть установлены на любую пару компьютеров.

*Таблица 12.1*

**Список наиболее известных программ для интернет-телефонии**

| Программа | Адрес сайта |
|---|---|
| Google Talk | http://www.google.com/talk |
| **NetMeeting** | http://www.netmeeting-zone.com |
| Skype | http://www.skype.com |
| **Internet Phone** | http://www.vocaltec.com |
| **MediaRing Talk 99** | http://www.mediaring.com |
| **Net2Phone** | http://www.net2phone.com |
| **PhoneFree** | http://www.phonefree.com |

Схема Компьютер — Телефон позволяет совершать звонки с компьютера на любой телефон в мире через многочисленные службы, предлагающие свои услуги (табл. 12.2).

*Таблица 12.2*

**Список крупных служб, обеспечивающих возможность звонков с компьютера на обычные телефоны**

| Компания | Адрес сайта |
|---|---|
| Deltathree | http://www.zvonitut.ru |
| **IP-Calls** | http://www.ip-calls.ru/support.htm |
| **CALL2PHONE** | http://www.call2phone.org |
| **Alterphone** | http://www.alterphone.ru/pc2phone.shtml |
| Neotel | http://www.transneogrup.md/?ln=ru |
| OCC | http://www.oss.ru/service/individual/pc-call |
| Multinet | http://multinet.com.ua |
| InnoMedia | http://www.innosphere.net |
| Net2Phone, Inc. | http://www.net2phone.com |
| Dialpad Communications, Inc. | http://www.dialpad.com |
| CrystalVoice Communications | http://www.crystalvoicelive.com |
| Go2Call Com, Inc. | http://www.go2call.com |

Технология Телефон — Телефон позволяет производить соединение обычных телефонов, но при этом голос передается через Интернет. Порядок вызова абонента в этом случае практически не отличается от порядка при обычной телефонной связи. Просто на обычном телефонном аппарате вместо привычной восьмерки набирается номер местной компании, обеспечивающей связь (который является номером ближайшего телефонного сервера), идентификационный номер, указанный на карточке IP-телефонии, а затем номер вызываемого абонента. После набора номера система IP-телефонии (через второй сервер) соединяет вас с телефоном вызываемого абонента. Таким образом, звонящий совершает традиционные операции дозвона и слышит привычные сигналы телефонной сети. Обычный телефонный звонок удерживает канал связи открытым на протяжении всего разговора, даже если собеседники молчат. Интернет-телефония устраняет эту неэффективность, заполняя каналы только голосовыми пакетами, а во время пауз используя эти же каналы для пересылки пакетов других звонков, т.е. один канал делится между несколькими пакетизированными разговорами. Поэтому пакеты данных от разных запросов и даже различные их типы могут перемещаться по одной и той же линии в одно и то же время.

По мере увеличения числа людей, использующих технологию IP-телефонии, проблема безопасности становится всё серьезнее. Крупные компании и государственные организации особенно озабочены вопросами защиты конфиденциальной информации при вводе в эксплуатацию сервисов VoIP (Voice over IP). Например, 97% новых телефонов, которые планируется установить в Северной Америке в ближайшие годы, будут использовать технологию VoIP. В случае же передачи голосовых данных с использованием протокола IP по беспроводным Wi-Fi сетям криптографическая защита вообще должна присутствовать в обязательном порядке. Что же касается ныне существующих программных средств, реализующих возможности IP-телефонии, то компании-разработчики даже в рекламе не

указывают, применяется ли при передаче голосового трафика хоть какой-нибудь механизм защиты от прослушивания (это, конечно, говорит в пользу того, что такие средства не применяются).

Для защиты речевой информации, передаваемой в IP-сетях, разрабатывают специальные программы, использующие криптографические алгоритмы шифрования исходных пакетов и сообщений, которые позволяют обеспечить гарантированную конфиденциальность IP-телефонии. Существующие криптографические алгоритмы при использовании 256-битных секретных и 1024-битных открытых ключей шифрования (например, по ГОСТ 28147-89) делают практически невозможным дешифрование речевого пакета.

Проблемой защищенной IP-телефонии является обмен криптографическими ключами шифрования между абонентами сети. Как правило, используются криптографические протоколы с открытым ключом с применением протокола Диффи-Хеллмана, который не дает тому, кто перехватывает разговор, получить какую-либо полезную информацию о ключах и в то же время позволяет сторонам обменяться предварительной информацией для формирования общего сеансового ключа, который применяется в дальнейшем для шифрования и расшифрования речевого потока.

Таким образом, IP-телефония может обеспечивать вполне качественную защищенную связь между абонентами, грамотно использующими предоставляемые им возможности.

*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*Суровым сибирским мужикам прислали американский дереворубочный станок.*

*— Ээээ, — сказали суровые сибирские мужики и вставили в станок щепку.*

*— Хрусь, — ответил станок.*

*— Оооо, — сказали суровые сибирские мужики и вставили полено.*

*— Хрууусь, — ответил станок.*

*— Оооо, — сказали мужики и вставили вековую сосну.*

*— Хр-ррру-сьь, — ответил станок.*

*— Оооо, — сказали мужики и вставили в станок железный ломик.*

*— Кр-яя-к, — сломался станок.*

*— Аааа, — сказали суровые сибирские мужики, — дрянь всякую присылают...*

## *НЕОБХОДИМЫЕ НАВЫКИ*

Как же достигнуть сохранения конфиденциальности при ведении телефонных разговоров с абонентами, связь с которыми вы не хотите афишировать? (к таким абонентам можно отнести иностранный банк, в котором вы открываете или имеете счет, фирму, оказывающую вам посреднические услуги при открытии офшорной компании и т.п.). Можно рекомендовать несколько вариантов организации связи для обеспечения анонимности вашего телефона и невозможности документарно связать ваши звонки с вами:

1. Звонки из телефона-автомата (лучше из соседнего города или с помощью карточек IP-телефонии).
2. Покупка дубликата sim карты для сотового телефона на радиорынке (да, это некрасиво, но реальному абоненту кроме потери нескольких долларов ничем не угрожает, ваши же реальные планы останутся для заинтересованных лиц неизвестными).
3. Покупка анонимной карты sim-sim за пределами России (например, на Украине при покупке карты sim-sim не требуется даже предъявления паспорта, звонить по ней вы сможете только с территории Украины, но зато принимать звонки (и оставлять ее номер телефона в качестве контактного) на

всей территории России). Этот прием, хотя и ограничивает возможности для исходящих звонков, позволяет вам быть все время на связи для входящих.

4. Ну и, наконец (самый экзотический вариант), заключается в покупке спутникового телефона. При его выборе следует обратить внимание в инструкции на особенности организации связи (например, «Иридиум» при наличии сети сотовой связи подключается прямо к ней и работает в зоне действия сети как обычный сотовый, что вам, разумеется, для сохранения конфиденциальности не нужно).

## Запомните

*Бог думает о нас. Но он не думает за нас.*

***Жан Кокто,***
***французский драматург***

При ведении телефонных разговоров с собеседниками даже по анонимному телефону также следует придерживаться некоторых простых правил (вам ведь неизвестно, установлен ли контроль над телефоном вашего собеседника):

1. Если вы еще не установили личный контакт с фирмой или банком, которые собираетесь посетить, сводите разговор просто к договору о встрече («Добрый день. Можно ли к вам подойти? В какое время удобнее?»).
2. Если у вас спрашивают, кто звонит (для выписки пропуска, для записи на прием и т.п.), называйте не свою фамилию, а фамилию, близкую по звучанию к вашей (например, Ежов вместо Ершов). Вы всегда сможете сослаться потом на плохое качество связи или невнимательность секретаря.
3. Не сообщайте в телефонном разговоре никакой дополнительной информации (я, мол, по рекомендации господина Сидорова), помогающей вас впоследствии идентифицировать.

4. При установке первичного контакта с фирмой или банком, которые вас будут обслуживать, лично знакомьтесь с оператором или сотрудником, получившим распоряжение поддерживать связь с вами. Постарайтесь запомнить его голос и манеру разговора. Договоритесь (а лучше внесите в контракт на обслуживание на случай смены сотрудника) об условном имени, которым вы будете называться при телефонных звонках и об условной фразе, наличие или отсутствие которой будет означать, что вы находитесь под чужим контролем и ваши распоряжения недействительны).
5. В дальнейшем используйте в телефонных разговорах с данной организацией только обусловленные имена.
6. Не используйте условные имена в повседневных телефонных переговорах (это позволяет раскрыть вашу маскировку).


*Запомните*

*Торопись, не спеша.*

***Любимая поговорка императора Октавиана Августа***

Конечно, эти правила можно и не соблюдать, но в этом случае вы не гарантированы от утечки характеризующей вас и ваши дела информации к заинтересованным лицам. Как вы думаете, приятно было увидеть в печати премьеру Украины Юлии Тимошенко распечатки своих разговоров с некоторыми из местных олигархов?

***ИЛЛЮСТРАЦИЯ***

**Фрагмент из телефонного разговора И. Коломойского и Ю. Тимошенко**

***http://www.puls.org.ua/news/2005/09/20/96***

*И.К. Привет Луи Витон. Как дела?*

*Ю.В. Беня, ты окончательно оборзел. Помни, с кем говоришь: за базар отвечать надо.*

*И.К. Юля, я не понял. Ты что, уже следующую коллекцию прикупила? Я тебя последний раз в Витоне видел. И вообще не дёргайся: помни, кто оплачивает ваши апельсиновые расходы. А то у вас революции, контрреволюции, а у меня что — Федеральное казначейство. Твоему президенту Боря Березовский миллионов десять дал, а ты с меня уже сколько вытянула?*

*Ю.В. Ваша еврейская беда в вашей жадности. Борис дал не десять, а тридцать и ещё дал бы. И просил за это не завод, а только встретиться в Киеве и официально в совместном заявлении осудить преступный кэгэбистский режим Путина. Витя мог бы и согласиться — Путин его всё равно на дух не переносит. Хуже не было бы. Вон Мишико кибенизирует его по полной программе и ничего — все уважают.*

*Запомните* ~~~~~~~~~~~~~

*Болтун — находка для шпиона!*

***Лозунг — предостережение сталинских времен***

Ведение телефонных разговоров с партнерами и фирмами, связь с которыми вы не скрываете (вы связаны, например, постоянными взаимными поставками или осуществляете совместные проекты), также можно и нужно защитить от прослушивания (зачем заинтересованным лицам знать о ваших оборотах, местах складирования или сроках поставки грузов?). Для этого достаточно:

1. Использовать скремблер для защиты разговора и факсимильных сообщений. К достоинствам скремблеров можно отнести малые размеры (с обычную книгу) и цену (от $50 до 300$), к недостаткам — относительную слабость криптографической защиты (http://www.mascom.ru/katalog/skremblers.htm). Применение скремблеров целесообразно при защите телефонных переговоров от бандитов, собирающих информацию о вас и вашей фирме и не обладающих серьезными техническими возможностями для проведения информационных атак на ваши жилые и рабочие помещения.
2. Использовать интернет-телефонию, применяя в процессе разговора программы для защиты речи, например **PGPfone** (http://www.pgpi.org/products/pgpfone) или **Speak Freely** (http://sourceforge.net/project/showfiles.php?group_id=87107). К достоинствам этого приема следует отнести абсолютную надежность защиты, обусловленную большими размерами используемых для шифрования речи ключей, к недостаткам — вашу «привязанность» к компьютеру (хотя размер небольшого ноутбука не больше размеров скремблера). Применение защищенного интернет-канала для ведения телефонных разговоров способно не только полностью обезопасить ваши беседы (кроме того случая, естественно, когда жучки будут установлены в вашем собственном офисе), а и значительно сократить ваши расходы на междугороднюю и международную телефонную связь (платите-то вы все равно только за пользование сетью, а уж какую информацию принимаете и передаете — дело ваше).

## Запомните

*Когда мы тратим время на планирование, его становится больше.*

***Бенджамин Франклин***

## Резюме

Рассмотренные приемы организации голосовой связи и средства защиты разговора позволяют существенно снизить риск утечки деловой информации и предотвратить возможность использования против вас сведений, упоминающихся в перехваченных беседах.

# Глава 13

## Свой среди чужих, чужой среди своих
### (как контролировать сотрудников)

*Не задавай вопросов, и тебе не будут лгать.*

***Английская пословица***

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

**В этой главе:**

- Работники теряют время, а вы — деньги.
- Зарубежный опыт наведения порядка.
- О сложности контроля умников.
- Стальная рука в мягкой перчатке.
- Сижу высоко, вижу далеко...

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

На вашей улице праздник. Вы открыли собственное дело. Начались приятные будни самостоятельной работы, омрачаемые лишь трениями с заказчиками, поставщиками, банками, посредниками, контролирующими органами и бандитскими группировками, алчными родственниками и завидующими вам соседями. Но с вами есть единомышленники, помогающие своим упорным трудом преодолеть все препятствия на пути в светлое будущее, — ваши сотрудники! Вы так думаете? А присмотритесь-ка повнимательнее, что делают на работе те из них, о ком можно собрать более-менее достоверную информацию?

***ИЛЛЮСТРАЦИИ:***

***http://old.computerra.ru/offline/2001/406/11679/for_print.html***

*Злоупотребление доступом в Интернет на рабочем месте ежесекундно крадет из бюджета американских компаний*

*2000 долларов. Всего же за прошлый год потери составили 63 млрд. долларов. Компания Websense, в чьем исследовании содержатся эти полуфантастические цифры, объясняет так их происхождение: в США 57 млн. человек имеют доступ в Интернет на рабочем месте. По статистике, около 40% времени, проводимого работником в Интернете, не связано с выполнением служебных обязанностей. Теперь остается только умножить среднюю заработную плату на 1 час гуляния по Сети в неделю да на 57 млн. человек — и астрономическая цифра готова.*

***http://www.mariland.ru/modules.php?name=News&file=article&sid=23***

*Оказалось, что почти каждый четвертый сотрудник, имеющий доступ в Интернет, посещает порносайты, перманентно заседает в чатах или обменивается романтическими посланиями. 43% респондентов полагают, что сексуально-ориентированная онлайновая активность отражается на продуктивности работы. В то же время 24% признались, что используют служебные компьютеры именно в означенных целях.*

***http://sp.sz.ru/00_04_04_05_.html***

*Исследование показало, что 79% опрошенных выявляли на рабочих местах злоупотребление доступом в Интернет со стороны своих работников.*

***http://www.russianboston.com/archive/j-article.php?id=21586***

*В ходе проведенных опросов и исследований было установлено, что как минимум в 70% британских организаций были отмечены злоупотребления «несоответствующим» использованием доступа к Сети в рабочее время.*

Впечатляет? А это ведь только вершина айсберга — злоупотребления при работе в сети. Чем же они занимаются в остальное время?

*Анекдот*
*в тему:*

~ ~ ~ ~ ~ ~

*В фирму для рутинной работы на компьютере устраиваются три претендента. Первого зашедшего на собеседование спрашивают:*

*— Вас интересуют порносайты в Интернете?*

*Тот подумал, если сказать, что интересуют, то примут за сексуального маньяка:*

*— Нет, не интересуют.*

*— Свободны!*

*Заходит второй, ему тот же вопрос. Он подумал, если сказать, что не интересуют, то сочтут за ненастоящего мужика:*

*— Да, интересуют.*

*— Свободны!*

*Наконец заходит третий:*

*— Вас интересуют порносайты в Интернете?*

*— А что такое Интернет?*

*— Оформляйтесь на работу!*

Задача контроля разгильдяев тесно примыкает к проблеме вычисления кротов, информирующих конкурентов о вашей деятельности. Когда в фирме существует раздолье для бездельников, решающих свои личные задачи на рабочем месте, появление информаторов, получающих дополнительный доход за совмещение основной профессии и стукачества, является делом времени.

Многие компании пытаются принимать жесткие меры, регламентирующие работу и поведение своих сотрудников

***ИЛЛЮСТРАЦИИ:***
***http://zhensovet.com/ut/index.php?s=2a68d1f28961f6cdddd923434552c7df&showtopic=3901***

*«...я работала на крупную корейскую корпорацию у себя в городе. Ничего хорошего. Камеры везде — в кабинетах, кори-*

*дорах. Требовали доносить обо всем руководству. Бывшим сотрудникам вход запрещен. На верхнем этаже президент приказал построить «аквариум» — это у кабинетов вместо стен — стекла. Так что нельзя было даже в носу поковыряться — увидят. Отдел маркетинга посадили напротив абонентского и сделали большие проемы в стенах. Так что наши маркетологи весь день работали на всеобщее обозрение посетителей абонентского. Беременных девочек лишали (до сих пор лишают) премии. Все наши беременнушки до последнего втайне держали беременность. Лишают премии за все. Ни в коем случае нельзя есть, а тем более пить алкоголь даже после работы на рабочем месте. Мы работали очень часто по ночам по одному, было скучно, поэтому принесли магнитофон, чтобы хоть радио слушать. Запретили. Так же президент сам лично проехал по подразделениям и изъял поттеры-электрочайники. Чтобы пожар не наделали. Помню, кто-то все-таки включил чайник, президент увидел — лишил премии...»*

***http://www.rostrud.info/10/45/894***

*«Мой муж устроился в японскую компанию в Москве. Зарплата — в 2 раза выше, чем на той же должности в российской. Ну и, конечно, престиж: все-таки Япония, ё-моё! Кто ж знал, что Сергей попадет в лагерь по подготовке самураев! Опоздание на одну минуту карается объяснительной. 3 опоздания — вычитается дневная зарплата. В японской фирме это может быть больше $100. На обед и прочее покидание офиса выделяется 1 час. Нужно больше? За 2–3 недели до этого пишете заявление. Даже если его удовлетворят, отлучку придется отработать! Печатная корреспонденция просматривается. Прочитав, начальник, если посчитает нужным, передаст ее тебе. Телефонные разговоры записываются и прослушиваются. Никаких мобильных внутри офиса! В столовой незаметные сотрудники заходят, делают вид, что пе-*

*рекусывают. На самом деле они фиксируют коллег, «прохлаждающихся» в столовой! Если в течение дня ты замечен более двух раз, то попал в черный список. Нужно быть предельно осторожным, когда объясняешь начальнику, почему ты хочешь в отпуск. Иначе, вернувшись, можешь с удивлением узнать, что уволен. Японцу трудно поверить, что вместо зарабатывания денег человек почти месяц тратит их на теплое пиво и потных женщин. Они думают, ты был у конкурентов и договаривался о более высокой зарплате. Любой чих в офисе доводится до сведения руководства. Один коллега совершенно серьезно спросил мужа: что думает напарник Сергея о новом замдиректора и вообще нравится ли напарнику руководство? Услышав в ответ «Не знаю, не спрашивал», коллега намекнул, что босс очень удивляется, почему Сергей не докладывает о своем напарнике, да и вообще не наведывается поговорить по душам...»*

Как вы думаете, казарменное положение сотрудников будет стимулировать появление новых гениальных идей? Вряд ли. Сможет ли оно предотвратить утечку информации при негативном отношении сотрудников к руководству компании? Маловероятно. Скорее всего, в организации работы, как и в жизни, стоит соблюдать правило 20/80.

***ИЛЛЮСТРАЦИЯ***

***http://www.wood-invest.ru/russian/articles/article_1.htm***

*Правило 20/80 означает, что в любом процессе малое число причин (20%) жизненно важны, а 80% не оказывают существенного влияния на результат. Менеджеры проектов знают, что 20% работы (первые и последние 10%) отнимают 80% времени и ресурсов. Правило 20/80 можно применить практически к любой сфере деятельности и знаний, начиная от науки управления и до физики.*

- ✓ *20% товарных запасов занимают 80% склада,*
- ✓ *80% товарных запасов поставляются 20% поставщиков,*

- ✓ *80% объема продаж обеспечивается 20% менеджеров по продажам,*
- ✓ *20% персонала провоцируют 80% связанных с персоналом проблем,*
- ✓ *20% персонала обеспечивают 80% вашего производства,*
- ✓ *80% времени ваши сотрудники убивают на то, что принесет 20% приходов,*
- ✓ *80% от суммы вашего счета за телефонные переговоры истрачены впустую.*

*Из всего, что вы делаете в течение дня, только 20% действительно важно. Из этих 20% проистекает 80% ваших будущих результатов. Найдите и направьте ваше внимание на эти 20%. Сторонники теории утверждают, что поскольку 20% ваших сотрудников обеспечивают 80% результатов вашей компании, вы должны посвятить время управлению только этими 20% сотрудников, называемых «суперзвездами».*

То есть 80% сотрудников, занимающихся текучкой, нуждаются в прямом принуждении и открытом контроле, а 20% выполняющих самую квалифицированную и важную часть работы (бухгалтеры, экономисты, дизайнеры, программисты, менеджеры и т.д.) от такого публичного недоверия просто примутся за мелкие пакости в стиле «итальянской забастовки» (для тех, кто не слышал: «итальянская забастовка» — работа с соблюдением всех норм и законов (освещенности рабочего места, уровня шума, уровня загрязнения воздуха и т.п.), а знатоки Трудового кодекса и ГОСТов знают, при необходимости же всегда готовы будут их соблюдать...) Как, не унижая публично квалифицированные кадры, контролировать их поведение и регистрировать контакты, а при возникновении нужды в индивидуальном порядке «ставить на место» или срочно удалять из числа сотрудников компании?

### *ПОЛЕЗНАЯ ИНФОРМАЦИЯ*

Существует целый ряд программных приложений-шпионов (spyware), которые, будучи установлены на компьютере, соби-

рают и сохраняют информацию о пользователе, работающем на нем, а затем пересылают ее по указанным разработчиками адресам.

Программы-шпионы делятся на несколько групп, различающихся прежде всего своим назначением.

**Internet-spyware**. Эти программы собирают информацию о качестве связи, способе подключения, скорости модема и т.д.

**WWW-spyware**. Это приложения, следящие за вашей деятельностью в сети: посещаемыми сайтами, покупаемыми продуктами, информацией, которую вы вводите в формы при совершении покупок в электронном магазине.

**Cookie-spyware**. Данные приложения не попадают на компьютер пользователя. Эти программы анализируют информацию, содержащуюся в cookies (небольших текстовых файлах), создающихся во время посещения сайтов. Они используются для запоминания личных предпочтений пользователя и записи его регистрационной информации.

**HDD-spyware**. Программы этой группы занимаются сбором информации о содержании жесткого диска. Чаще всего речь идет о контроле списка программного обеспечения, установленного на компьютере.

**Логгеры приложений**. Некоторых наблюдателей (чаще всего работодателей) интересует список приложений, с которыми работал пользователь. Эта информация может также быть собрана специальными программами.

Неприятно ощущать, что за вами наблюдают, но перечисленные выше группы программ-шпионов не создают вам проблем и не делают явных гадостей, а вот программы, относящиеся к группам, перечисленным ниже, вполне могут испортить вам аппетит.

**E-mail spyware.** Эти приложения могут внести изменения в вашу электронную переписку, снабжая исходящие от вас письма графическими баннерами или рекламными текстами. Информация о характеристиках вашего почтового ящика может быть передана другим спаммерам для рассылки рекламы.

**Snoopware.** Это одна из разновидностей программ-шпионов, специально разработанных для удаленного наблюдения за тем, чем занимаются пользователи на своих компьютерах.

**Keylogger**. Эти программы фиксируют информацию о каждой нажатой вами клавише; впоследствии хозяин программы может ознакомиться с содержанием всех текстов, набранных на вашем компьютере.

Для наблюдения за деятельностью сотрудников вам вполне достаточно освоить и постоянно применять какой-нибудь из логгеров приложений или keylogger-ов, позволяющих неявно (или, наоборот, явно) контролировать их работу на компьютере.


## *НЕОБХОДИМЫЕ НАВЫКИ*

Существует ряд программ (табл. 13.1), предназначенных для контроля процесса работы «белых воротничков», их активности в Интернете или на рабочем месте и сообщающих по локальной или внешней сети информацию, которая интересует шефа, ему лично или назначенному им лицу.

*Таблица 13.1*

| Программы | Характеристика |
|---|---|
| **Able Box**<br>http://www.abensoft.com/box.htm | Очень простая бесплатная программа. Позволяет регистрировать и анализировать деятельность и активность работы пользователя на компьютере, фиксирует содержимое набираемых в редакторах текстов и писем. |
| **Boss Agent**<br>$29,95<br>http://www.safechaos.com/ba.htm | Очень простая программа. Позволяет регистрировать и анализировать деятельность и активность работы пользователя на компьютере, фиксирует содержимое набираемых в редакторах текстов и писем, позволяет пересылать собранную информацию в адрес руководителя. |
| 007 **Keylogger** Spy<br>$39,95<br>http://www.waresight.com | Программа записывает подробную информацию о посещенных веб-сайтах, интернет-чатах, открытых окошках, запущенных приложениях, набранных символах (в том числе логинах и паролях), а, кроме того, умеет делать снимки экрана с заданным промежутком. |
| **SpyBuddy**<br>$69,99<br>http://www.buy-spybuddy.com | Хорошая программа для слежения за деятельностью сотрудников. Позволяет контролировать как операции на компьютере, так и манипуляции в сети. Может осуществлять контроль как в видимом, так и в невидимом для пользователя режимах. |
| **PC Activity Monitor Net**<br>$89,95<br>http://www.keyloggers.com | Отличная программа. Позволяет контролировать выполняемые на компьютере операции дистанционно. |
| **Spector Pro**<br>$99,95<br>http://www.spectorsoft.com | Отличная программа. Не только регистрирует запущенные на компьютере программы, но и фиксирует содержимое написанных в редакторах текстов и писем. |

*Окончание табл. 13.1*

| Программы | Характеристика |
|---|---|
| **INVISIBLE KEYLOGGER** $39.99 http://www.invisiblekeylogger.com | Простая программа для слежения за деятельностью пользователя на компьютере. |
| **NetVizor** $295 http://www.netvizor.net/ | Очень мощная программа для тотального контроля за сетью компьютеров в офисе. |
| **View My Logs** $10 в месяц http://www.1spysoftware.com/viewmylogs.shtml | Предлагается сервис по дистанционному слежению за указанным вами компьютером. Может быть удобен при необходимости эпизодического контроля деятельности сотрудников в сети. |

Посмотрим, как работают такие программы на примере простейшей (Able Box), установка которой не требует никакого опыта в настройке сетевых соединений. Able Box предназначена для наблюдения за пользователями компьютера: детьми, сотрудниками, да и вообще кем угодно (рис. 13.1). Программа фиксирует всё, что делает пользователь и записывает собранную информацию на жестком диске.

В настройках (рис. 13.2) можно установить срок хранения накопленной информации (3, 5, 30 дней) и форму ее представления (сокращенная или расширенная статистика). Полная информация о работе пользователя (рис. 13.3) больше будет интересна системному администратору, а вот сокращенная форма может наглядно продемонстрировать боссу, чем же реально занимался сотрудник. Она не только информирует, какие программы запускались в течение рабочего дня, но и сообщает о характере их использования (было ли открытое окно активным, какова частота нажатий клавиш или кликов по мышке при работе с ним).

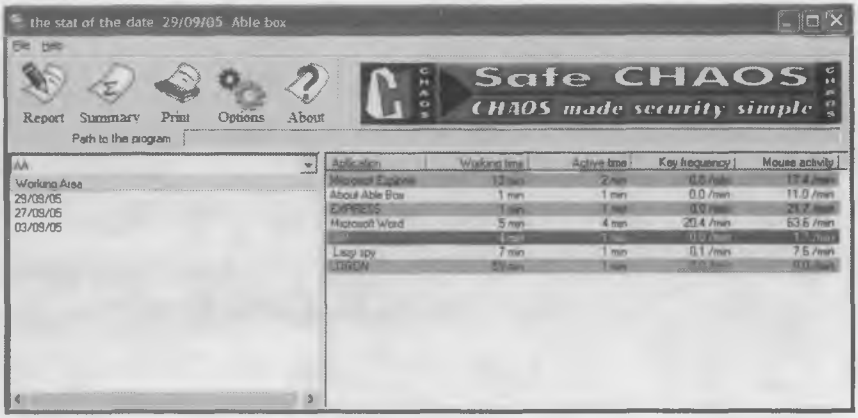



***Рис. 13.1.*** *Интерфейс программы Able Box*

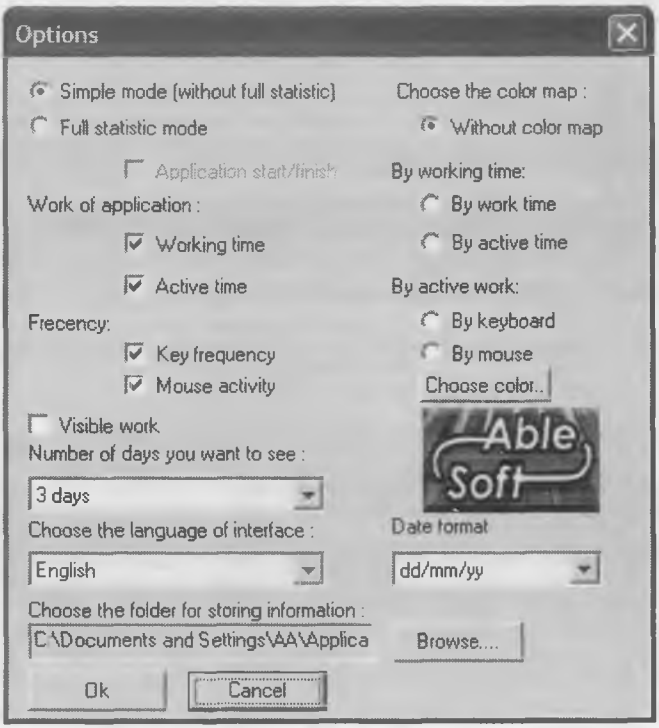



***Рис. 13.2.*** *Настройки программы Able Box*

Кроме того, программа обратит внимание хозяина на ключевые моменты рабочего дня, выделив приложения, которые

пользователь использовал наиболее активно (на что именно обращать внимание, естественно, нужно сначала установить в «настройках») и может позволить просмотреть, каким же был реальный вклад работника в тот или иной документ (рис. 13.4), над которым он работал.

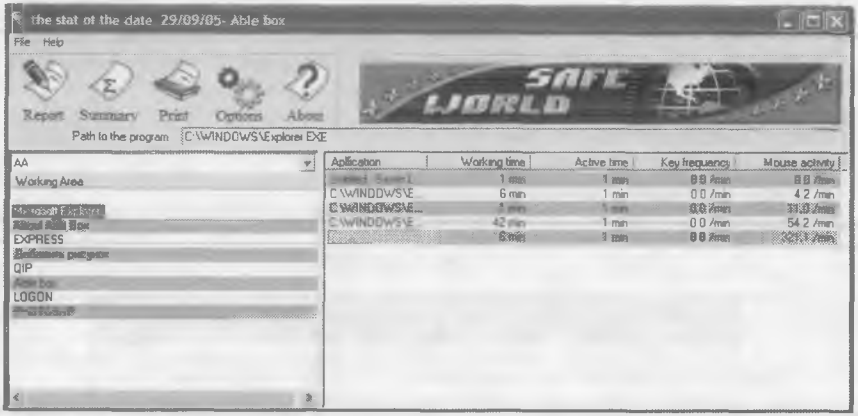



***Рис. 13.3.*** *Подробная статистика по работе с одной из программ*

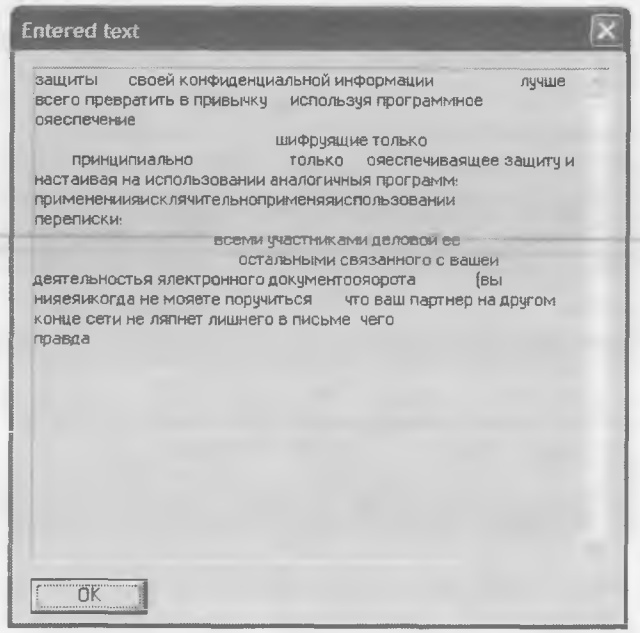



***Рис. 13.4.*** *Содержание написанного сотрудником текста*

В настройках предусмотрена возможность как невидимого, так и видимого для сотрудника режима работы (в этом случае справа на панели задач (это в нижней части экрана) появляется иногда подмаргивающий глаз). Хотите проследить за работой сотрудника втайне от него, — включаете режим невидимой работы. Если же вам некогда заниматься повседневным контролем, включаете видимый режим работы и, зная, что глаз хозяина не дремлет, работник хочет не хочет, займется делом, а там, глядишь, ему и понравится.

### *Кстати* ~~~~~~~~~~~~~~~~

*Надпись на воротах завода: «Каждый, кто любит работать, сможет развлечься здесь по полной программе».*

*NN*

Программа позволяет делать выборку результатов работы по отдельным дням, формировать отчеты за выбранные периоды, суммировать информацию и давать усредненные данные. Добраться до собираемой информации без пароля нельзя, так что, установив программу на компьютерах конторы и просматривая еженедельные или ежемесячные отчеты, можно оценивать вклад каждого из работников в результаты их совместной деятельности.

### *Анекдот в тему:*

~~~~~~

*— Внимание, земля! Говорит борт 13! У нас отказал бортовой компьютер. Что делать? — Борт 13! Борт 13! Это диспетчер! Слышите меня? Играйте пока на резервном! Играйте на резервном.*

Это возможности простенькой бесплатной программы. Использование же платных версий аналогичных программ суще-
~~~~~~

ственно расширит варианты организации контроля вами работы своей фирмы и будет особенно эффективным при наличии у предприятия филиалов или нескольких офисов.

## Резюме

Рассмотренные программы позволяют скрытно или явно контролировать деятельность сотрудников, вычислять предателей, оценивать личный вклад работников в реализацию осуществляемых компанией проектов. Программы этого типа приносят особенно большой эффект, когда:

- ✓ часть сотрудников фирмы работает дома, связываясь с головным офисом через сеть;
- ✓ подразделения предприятия размещены в разные, зачастую удаленные помещения;
- ✓ компания имеет удаленные филиалы в разных концах страны;
- ✓ существует вероятность наличия в рядах сотрудников осведомителей — конкурентов;
- ✓ в коллективе существует напряжение, вызванное неадекватной оценкой некоторыми сотрудниками своего вклада в общее дело, и появилась настоятельная необходимость выполнить объективную оценку их усилий;
- ✓ появилась неотложная задача и требуется встряхнуть коллектив, расслабившийся от спокойной жизни.

# Глава 14

## Форма — это уже содержание
### (как контролировать свой компьютер)

*Порядок учит сберегать время.*
***И.В. Гёте***

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

**В этой главе:**

- Возможно, вы уже под колпаком.
- Откуда ждать неприятностей.
- Что могут шпионы-невидимки.
- Компьютерная контрразведка.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Контролируя работу других людей, будьте готовы к тому, что кто-нибудь попытается проконтролировать и деятельность вашей компании. Легче всего это сделать, получив доступ к содержимому информации, обрабатываемой на компьютере. Компьютер — это центр активности любой работающей фирмы. Подобно сердцу он пропускает через себя потоки информации, преобразует и перераспределяет ее, превращая из набора данных на удаленных серверах во вполне понятные графики, таблицы, иллюстрации. Изучая ваши пристрастия, круг общения, содержимое писем, условия контрактов и географию контактов, можно поставить под контроль и вашу личную жизнь, и работу вашей компании.

***ИЛЛЮСТРАЦИЯ***
***http://dn-weekly.kiev.ua/news.php?newsid=3411***

*Для рядового обывателя дело о мошенничестве некоего жителя Нью-Йорка Джу Джиянга (Juju Jiang) известно как*

*«дело Kinko». Однако программы удаленного администрирования и сбора информации о пользователе удаленного компьютера (snoopware) стали вызывать серьезную обеспокоенность в мире специалистов, занимающихся обеспечением безопасности пользователей в сети.*

*Программы подобного рода могут угрожать потерей или разглашением важной информации. В уходящем году этот самый Джу Джиянг установил на 13 компьютерах всемирно известной компании Kinko, занимающейся созданием различного рода копий с документов, программу, позволяющую захватывать и отсылать на компьютер злоумышленника все пароли, введенные на «зараженном» компьютере. В итоге нарушителю удалось завладеть информацией о денежных счетах и личных данных более 450 человек. Затем, используя полученную таким образом информацию, хакер перевел деньги со счетов жертв на созданные им счета, якобы принадлежавшие жертвам.*

Не рассчитывайте, что попытаться добраться до ваших секретов может только агент спецслужб или опытный хакер. Доступность информации о средствах взлома делает потенциально опасным для вас любого современного пользователя компьютера.

***ИЛЛЮСТРАЦИЯ:***
***http://www.mk.ru/numbers/185/article6134.htm***

*На диске, изъятом у продавца, находилось несколько сотен программ, предназначенных для уничтожения, взлома и кражи информации из компьютеров пользователей сети Интернет.*

*— Представьте, вот вы сидите в Интернете, бродите спокойненько по сайтам, болтаете в чате. А в это время любой более-менее знакомый с компьютерами человек может при помощи такого диска залезть в ваш компьютер, скопировать, удалить или изменить там информацию, — рассказывает специалист Управления по борьбе с преступностью в сфере высоких технологий («Р»). — Кроме этого без особого труда владелец «Хакера» может украсть ваш пароль для пользования*

*Интернетом. Есть и программы, позволяющие физически испортить некоторые детали компьютера.*

*Как стало известно «МК», диск «Хакер» пользуется особой популярностью у начинающих компьютерных злодеев, которые — по примеру своих более опытных товарищей — хотят постигнуть азы искусства взламывания и уничтожения информации.*

*— Диск этот регулярно обновляется, — вздыхают специалисты. — Его авторы внимательно следят за всеми последними антивирусными разработками и достижениями в сфере защиты информации. Поэтому неопытный пользователь практически не может защититься от обладателя «Хакера».*

Не думайте, что программы-шпионы могут проникнуть в ваш компьютер только с сайтов сомнительного содержания или с помощью сотрудника-предателя. Занести их можете и вы сами, поработав с документами, хранящимися в вашей флэшке на чужом компьютере (например, вместе с руководством фирмы-партнера) или просто открыв приложение к письму, полученному с электронного адреса старого друга.

***ИЛЛЮСТРАЦИЯ***

***http://www.cnews.ru/newtop/index.shtml?2004/06/24/160564***

*На компьютер пользователя программы-шпионы могут попасть при запуске программных продуктов, посещении вебсайтов или получении электронных писем. Активировавшись, они начинают неусыпную слежку за компьютером и его владельцем. Злоумышленники получают уникальную возможность перехватывать вводимые с клавиатуры тексты, копировать файлы и при этом оставаться незамеченными.*

*По словам Мэтта Серджента (Matt Sergeant), старшего специалиста по антиспамовым технологиям в MessageLabs, жертвы спаммеров, скорее всего, откроют письмо, в теме которого будет содержаться информация, непосредственно касающаяся их самих или их работы. «Идея состоит в исполь-*

*зовании знакомых слов и фраз, таких, как пароли, клички домашних животных или названий компаний, — такое письмо адресат, скорее всего, откроет».*

Не рассчитывайте, что, раз уж в мире несколько сотен миллионов компьютеров, интерес именно к вашему маловероятен. Даже если вы пока еще не настолько богаты, чтобы заинтересовать кого-либо содержанием своего банковского счета, ваш компьютер можно использовать (не беспокоя вас, естественно) для массовых рассылок спама или совершения мошеннических операций в сети (претензии, конечно, предъявят в первую очередь вам, а там уж отмывайтесь сами, как знаете). Кроме того, вы не застрахованы от внезапно свалившегося богатства или полосы удач в делах. Так почему бы предусмотрительному хакеру не иметь в архиве лишний шанс (в виде возможности доступа к вашему компьютеру) помочь потратить появившиеся излишки капитала? Как там говорится в известном фильме: «...запас карман не тянет, а в хозяйстве и пулемет пригодится».

***ИЛЛЮСТРАЦИЯ***

***http://www.mt-v.ru/php/public/comp.php?p=182&more=1***

*Сканирование миллиона ПК, осуществленное в прошлом квартале интернет-провайдером EarthLink и разработчиком систем компьютерной безопасности Webroot Software, показало, что на каждый персональный компьютер приходится в среднем 28 активных «шпионских» приложений. В целом* ***более 300 тысяч программ*** *позволяют злоумышленникам красть содержащуюся в компьютерах информацию и открывать к ним доступ.*

Так что привыкните к мысли, что угрозы вездесущи, а приемов взлома вашего компьютера — множество. Есть два пути борьбы с этой напастью: один — смириться и продолжать кормить своими деньгами паразитов, исповедуя известный принцип «пусть подавятся». Преимущества этого варианта: не нужно учиться и не нужно заниматься скучным каждодневным

контролем компьютера. Основной недостаток — ваши деньги могут быстро кончиться.


*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*Выступает председатель колхоза:*

*— В позапрошлом году засеяли сто гектаров пшеницы — долгоносик всю съел!*

*— В прошлом году засеяли триста гектаров пшеницы — опять долгоносик всю съел!*

*— В этом году засеем пятьсот гектаров пшеницы — пусть подавится!*

Второй путь — бороться, по возможности минимизируя потери и создавая трудности противнику. Победа в этой борьбе не гарантирована, но возможна.

*Запомните* ~~~~~~~~~~~~~

*Тот, кто мечтает заработать миллион долларов, вряд ли его заработает, тот, кто не мечтает, не заработает никогда.*

*NN*

Какой вариант поведения избрать — дело ваше. Но помните, что отсутствие желания решать какую-то проблему зачастую еще не избавляет от необходимости все-таки ею заниматься.

*Анекдот в тему:*

~~~~~~

*На плацу стоит часть. Командир части:*

*— Так! Кто едет на картошку, два шага вперед.*

*Из строя выходит три человека.*

*— Хорошо... вы трое — в машину, остальные идут пешком!*

***ПОЛЕЗНАЯ ИНФОРМАЦИЯ***

Существуют три основные группы действий, которые осуществляются программами-шпионами:

- ✓ копирование информации пользователя компьютерной системы (паролей, криптографических ключей, кодов доступа, электронных документов);
- ✓ изменение алгоритмов функционирования системных, прикладных и служебных программ;
- ✓ навязывание заданных извне режимов работы.

Получив с помощью программы-шпиона доступ к компьютеру, злоумышленник может считывать информацию не только с него, но и с компьютеров, подключенных к пораженному компьютеру по локальной или глобальной сети, изменять права
~~~~~~

доступа к компьютеру удобным для себя образом, устанавливать режимы работы компьютера, способствующие утечке с него информации.

### *ИЛЛЮСТРАЦИЯ*

**Как я хакал американосов в их же школе.**
***http://www.diwaxx.ru/hak/hakamericos.php***

*«Она потом еще сказала, что тебе пароль придется менять каждые 3 месяца, да плюс еще на следующий год пароль твой по умолчанию изменится на password и его надо будет опять сменить. Я подумал про себя, что эта леди действительно хочет, чтобы я чего-нибудь нехорошее с их системой сделал! Ну, вот начал я расспрашивать у друзей, как зовут тех учеников, которые ушли из школы в прошлом году — ну они мне сказали пару человек — ну я и подумал, что надо почву прозондировать. Логин формируется из «$первая_буква_имени_фамилия. Ну вот я собрал все логины чуваков, которые перешли в другие школы — залогинился с паролем password — бум. Порнуху могу в школе смотреть почти без боязни быть пойманным.*

*Второй этап — учительские привилегии (а это оценки и все такое). То же самое, что и с учениками — тока надо узнать имя учителя, который уволился! Узнал — зашел — уже могу даунлоудить файлы и могу читать все НЕТВОРК_ПАПКИ. И у меня есть доступ к программам выставления оценок и посещаемости (у них там нет журналов — все на компах, да на Форточках). Ну затем я подумал, что неплохо бы мне достать ДОФИГА аккаунтов, ну зашел я на компутер под названием \\ student2 (там хранится вся инфа об учащихся — в разных случаях он называется по разному, узнать можно это по ярлычку в Мой Компьютер — там будет написано что-то вроде этого: $some_login on \\students2\yr2004. Вот там и путь прописан. Так вот я зашел туда и обнаружил, что там есть папки, называемые yr2001 yr2002 — а ведь учащиеся 2002 и 2001 годов уже нафиг давно ушли со школы И их логины остались, и их пароли*

*поменялись на password! Теперь у меня много логинов и я могу терроризировать админа вешаньем компъютеров и всякими подлостями».*

В иллюстрации сохранен стиль и убраны самые только самые, грубые ошибки. Как видите, чтобы доставлять неприятности, высшее образование и четкие цели совсем не обязательны.

## *Анекдот в тему:*

~ ~ ~ ~ ~ ~

*Поймал Иван-дурак в проруби щуку. Та ему:*

*— Отпусти ты меня, Иван, и любое твое желание по-щучьму велению, по твоему хотению будет исполнено!*

*Обрадовался Ванюха, кинул щуку обратно в прорубь и говорит:*

*— Хочу знать, не слезая с печи, все, что в мире творится за лесами-за горами, за морями-окиянами. Хочу под музыку балдеть, на голых девок день и ночь пялиться, с заморскими дураками переписываться и все новые анекдоты про Царя-батюшку первому в мире узнавать!*

*Так Иван-дурак стал первым на Руси пользователем Интернета.*

Чтобы обнаружить проявления чужого присутствия в вашем компьютере на возможно более ранней стадии и по возможности защитить себя от них, существуют специальные программы-антишпионы, сканирующие содержимое компьютера и извещающие пользователя о появлении непрошенных гостей. Они регистрируют работающие программы компьютера и сигнализируют при появлении отклонений от разрешенной хозяином нормы их поведения.


Правда, ни одна из известных антишпионских утилит все-таки не гарантирует стопроцентного распознавания и уничтожения программ-шпионов. Остается пользоваться старым правилом: «защиты много не бывает» и понимать, что, чем больше антишпионских программ используется, тем лучше ваша защита.

### *НЕОБХОДИМЫЕ НАВЫКИ*

Рассмотрим характеристики некоторых из программ-антишпионов и возможности их наиболее эффективного использования в своих интересах. В табл. 14.1 приведен список наиболее распространенных программ, используемых для компьютерной контрразведки. Принципиальных отличий, по которым можно было бы дифференцировать программы по качеству и возможностям, они не имеют. В основе большинства лежит процесс сканирования памяти, реестра и файлов с целью обнаружения уже известных вариантов программ-шпионов. Так что различаются они в основном по функциональности, оформлению интерфейса и частоте обновлений базы данных программ-вредителей фирмой — разработчиком.

*Таблица 14.1*

| Программа | Характеристики |
|---|---|
| **Ad-Aware SE Personal Edition**<br>2.72 Mb<br>23,92 EUR<br>http://www.lavasoft.nu | Простая в пользовании и удобная утилита производит поиск шпионских программ на основе собственной базы данных. Поиск выполняется в разных областях системы: в реестре, в памяти, на дисках. Кроме того, программа анализирует работу оперативной памяти и отыскивает те программы, к которым система не должна достаточно долго обращаться, учитывая характер текущей деятельности. Если такие процессы специально не запускались, но проявляют активность, Ad-Aware предупреждает пользователя. Таким образом удается выявить паразитические программы (трояны, вирусы, шпионские модули и т.п.). В программе доступен русский интерфейс. |
| **X-Cleaner**<br>679 Kb<br>$29,95<br>http://www.xblock.com | Простая в пользовании программа. Кроме обычных задач поиска программ-шпионов, Xcleaner имеет несколько дополнительных полезных функций, помогающих обеспечить защиту информации: шредер и встроенный генератор паролей. |
| **SpyStopper Pro**<br>1,94 Mb<br>$29,95<br>http://www.itcompany.com | В реальном времени программа блокирует пытающиеся проникнуть в систему модули, а также те программы-шпионы, которые уже попали на ваш компьютер и пытаются вместе с передаваемой вами информацией переправиться на другие компьютеры сети. К сожалению, такие разновидности шпионских программ, как клавиатурные шпионы, SpyStopper не отлавливает. |

*Продолжение табл. 14.1*

| Программа | Характеристики |
|---|---|
| **Webroot Spy Sweeper**<br>8,52 Mb<br>$29,95<br>http://www.webroot.com/consumer/products/spysweeper | Простая, удобная и очень мощная утилита для выявления и удаления троянских программ, шпионских модулей, кейлоггеров и прочих нежелательных программ. Утилита поддерживает регулярное обновление базы данных через Интернет. К недостаткам следует отнести очень сильное торможение системы при работе программы. |
| **Able Monitor**<br>820 Kb<br>Free<br>http://www.abensoft.com/am.htm | Утилита запускается после установки системных программ в компьютере и впредь не допускает работы любых программ, установка которых не была санкционирована пользователем. Это позволяет детектировать и деактивировать все программы-шпионы, попадающие в компьютер. |
| **Spybot-S&D**<br>4,8 Mb<br>Free<br>http://www.safer-networking.org | Утилита осуществляет поиск и ликвидацию программ-шпионов и рекламных агентов (небольших модулей, предназначенных для прокручивания рекламных сообщений и баннеров). Найдя подобные «вкладыши», SpyBot-S&D удаляет их или, если удаление невозможно, заменяет их на пустые блоки. Кроме того, программа умеет очищать списки посещенных сайтов, открытых файлов и запущенных приложений. В программе доступен русский интерфейс. |

Одной из лучших программ-антишпионов является Ad-Aware SE фирмы Lavasoft (рис. 14.1). Давайте для начала русифицируем ее интерфейс.

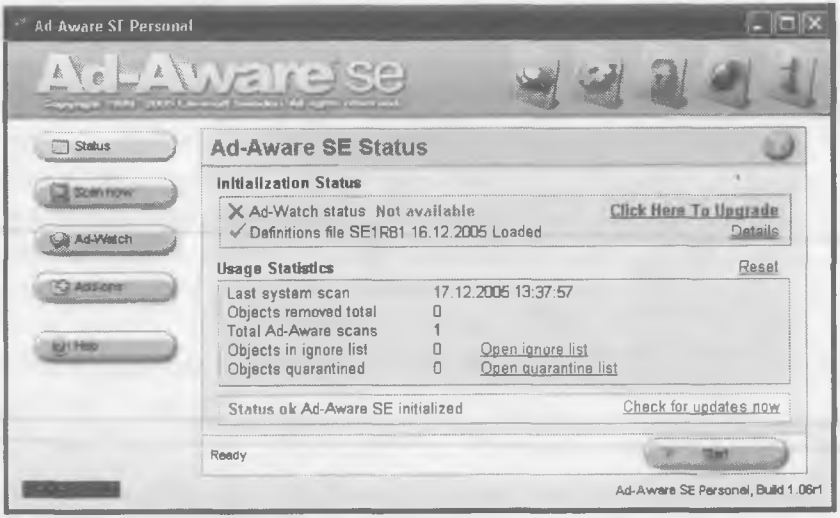



***Рис. 14.1.*** *Интерфейс программы Ad-Aware SE*

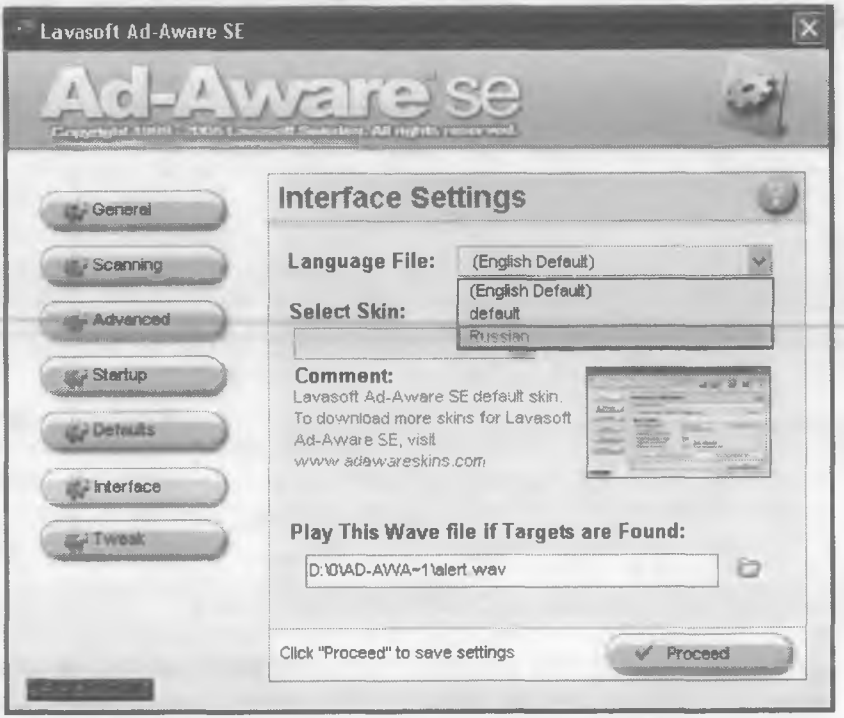



***Рис. 14.2.*** *Русификация программы Ad-Aware SE*

Вы можете поискать в Яндексе массу ссылок на ее русификатор, а можете сразу перейти по ссылке http://adaware.ru/download.htm и скачать его отсюда. После этого проинсталлируйте файл Ad-Aware-SE-Language-Pack.exe. В директории «Lang» папки Lavasoft\Ad-Aware SE Personal появится файл Russian.awl. Запустите программу, загляните в раздел «Опции» (на кнопке нарисована шестеренка) и щелкните в открывшемся окне по кнопке «Interface». Выберите русский язык и щелкните по кнопке «Proceed» (рис. 14.2, 14.3).

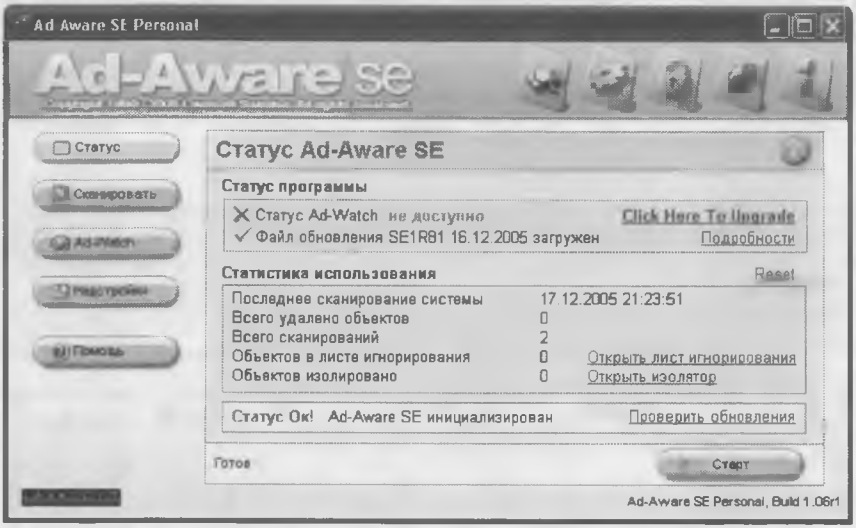



***Рис. 14.3.*** *Русифицированный интерфейс программы Ad-Aware SE*

Теперь, перейдя в основное окно программы, можно приступить к поиску программ-шпионов. Щелкните по кнопке «Старт» и выберите режим сканирования (рис. 14.4). После этого, нажав кнопку «Далее», остается наблюдать за ходом сканирования (рис. 14.5) или, свернув окно программы, заняться своими делами, предоставив программе самостоятельно проводить «контртеррористическую операцию» в вашем компьютере. После окончания сканирования программа покажет вам, сколько «кибертеррори-

стов» обнаружено (рис. 14.6). Щелкнув по кнопке «Далее», вы перейдете в окно, позволяющее выбрать из обнаруженных объектов те, которые подлежат уничтожению (вы же установили на компьютер и свои программы контроля, правда?).

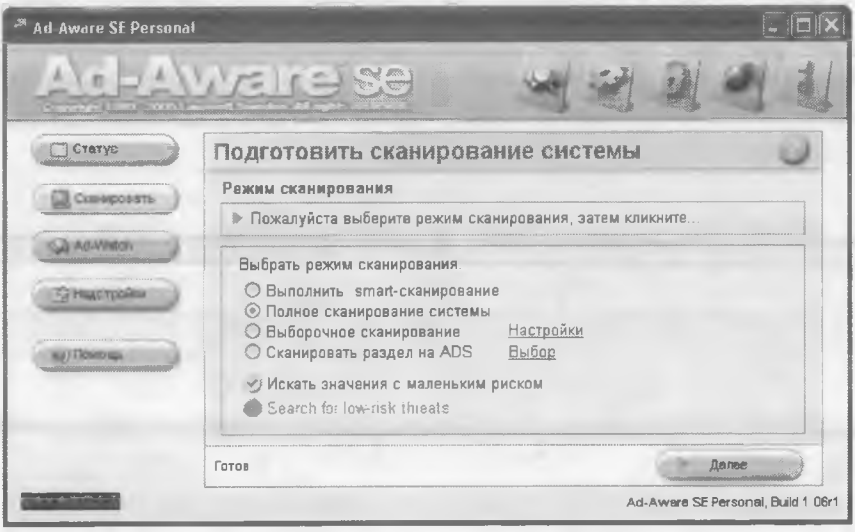



*Рис. 14.4. Подготовка к сканированию системы*

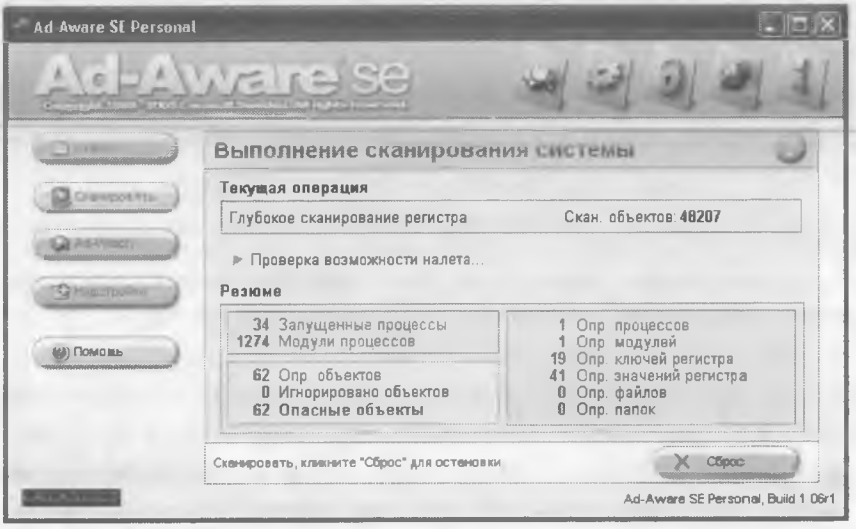



*Рис. 14.5. Выполняется сканирование системы*

*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*— Вот КАМАЗ — хорошая машина! Я купил — и не жалею. НИКОГО...*

Пометив чужих шпионов, удалите их, щелкнув по кнопке «Далее».

Вот, собственно говоря, и все. Ваш компьютер очищен от шпионов (по крайней мере тех, которые хранятся в базе данных программы Ad-Aware SE).

При запуске нового или тщательно вычищенного от шпионов компьютера целесообразно запустить программу Able Monitor (рис. 14.8). Работая в фоновом режиме, она продетектирует и запомнит установленные в компьютере на момент ее запуска программы и впредь просто не допустит работы утилит, установка которых не была санкционирована лично вами.


***Рис. 14.6.*** *Результаты сканирования системы*


*Рис. 14.7. Выбор объектов для удаления*

## *Анекдот в тему:*

~ ~ ~ ~ ~ ~

*Новый русский на 600 «мерсе» останавливается на красный свет. Вдруг с ходу ему в зад впечатывается (как всегда) запорожец. Бортовой компьютер «мерса» выдаёт сообщение: «Обнаружено новое устройство. Установить?»*

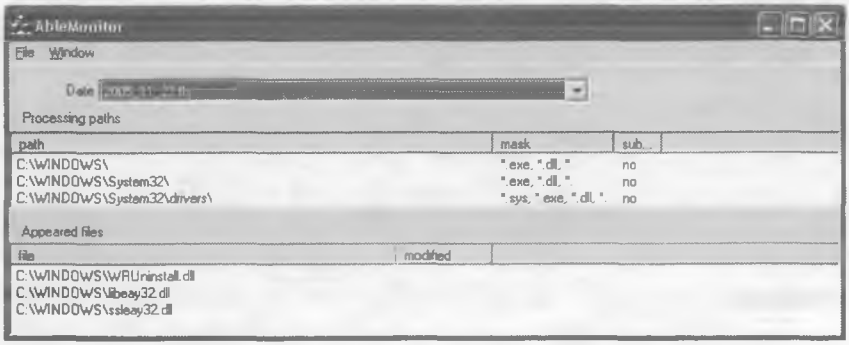



**Рис. 14.8.** *Интерфейс программы Able Monitor*

## Резюме

Рассмотренные программы позволяют детектировать работу системы, выявлять и уничтожать программы-шпионы. Обнаружив в компьютере шпиона, не стоит торопиться с его уничтожением, ведь самим фактом отключения программы-шпиона вы предупреждаете ее владельца о том, что программа найдена и вы знаете о слежке. Если этот владелец — хакер, в этом нет ничего страшного. Но если существует вероятность запуска к вам в компьютер программы-шпиона из конкурирующей фирмы, подумайте, может быть стоит ее использовать как канал отправки дезинформации ее хозяину?

# Глава 15

## Эх, дороги, пыль да туман
### (как путешествовать без риска)

*В каждом, даже самом плохом человеке, можно найти что-то хорошее. Нужно только как следует его обыскать.*

***Из инструкции милиционерам***

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

**В этой главе:**

- Джентльменский набор бизнесмена.
- Беззащитный путешественник.
- Упрямый гостиничный компьютер.
- Кто-то теряет, а кто-то находит.
- Мал золотник, да дорог!

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Последние десятилетия принесли нам информационную революцию, сформировавшую новый тип бизнесмена, — бизнесмена физически мобильного, но постоянно связанного средствами коммуникаций со своими предприятиями, партнерами, клиентами и сотрудниками. Теперь, перемещаясь на тысячи километров, можно регулярно контролировать работу подчиненных, вести секретные переговоры, согласовывать и подписывать соглашения, создавать и уничтожать юридические структуры, т.е. руководство превращается из эпизодического явления, происходящего в основном при вашем личном появлении в конторе, в процесс непрерывный, не обусловленный та-

кими факторами, как место вашего пребывания или время суток. Давайте же поговорим о том, как сохранить ваши секреты во время путешествия.

Когда вы дома, вас окружают родные и сотрудники, адвокаты и помощники, прикормленные правоохранительные органы и крышующие бандиты. Ваши секреты охраняются стенами фирмы и сигнализацией, системным администратором и охраной, связями и положением в обществе. В вашем процветании все заинтересованы, вы делаете благополучной жизнь многим, а кто же будет плевать в источник финансирования?

*Анекдот в тему:*

~ ~ ~ ~ ~ ~

*Разговаривают двое новых русских. Вдруг один изрекает:*

*— Моя милиция меня бережет...*

*Другой чешет в затылке:*

*—И мне купить, что ли...*

Но вот вы собираетесь в дорогу. Один или с двумя-тремя охранниками. Что будет в вашем багаже? Обычный перечень вещей — само собой. Но что еще входит в «джентльменский набор» бизнесмена? Информация. Проекты контрактов, номера счетов (вряд ли вы все их помните на память), электронные, почтовые и обычные адреса, телефоны, партнеров, представителей компании, сотрудников, родственников, просто друзей, наконец. Кто-то везет с собой ноутбук, кто-то КПК, кто-то флэшку. Но в дороге бизнесмен практически беззащитен. Адвокат и помощники далеко. Вокруг посторонние, не заинтересованные в нем люди. Задержать бизнесмена пусть даже на короткое время для формальных процедур «установления личности» (Ой. Простите, обознались!) и разлучить его с носителем информации проблем нет.

***ИЛЛЮСТРАЦИИ:***

***http://old.cry.ru/text.shtml?200408/20040819220414.inc***

*По подозрению в незаконной торговле оружием в аэропорту Праги задержан российский бизнесмен.*

***http://www.nr2.ru/ekb/13_76330.html***

*В аэропорту «Кольцово» задержан бизнесмен.*

***http://news.mirsofta.net/detali/all/618/33447.html***

*Президент азербайджанской нефтяной компании задержан в аэропорту.*

***http://www.rosbalt.ru/2006/6/2/249522.html***

*Во время делового визита в Тель-Авив предприниматель задержан в аэропорту Бен-Гурион израильской полицией.*

***http://news.pravda.ru/main/2001/02/24/23518.html***

*Два сирийских бизнесмена задержаны в аэропорту Каира.*

Хорошо, если подвод для задержания надуман, а информация надежно зашифрована. Помурыжили часок-другой, да и отпустили восвояси. Потеряно только время. Ну а если это серьезный заказ конкурентов, или бандитов, или рэкетиров в погонах, или жены, решившей добраться до ваших активов?

## *Кстати*

*Параноики только думают, что на них ополчился весь мир, а я это точно знаю.*

*NN*

В этом случае шифруй не шифруй, а пароль и программу, которая поможет прочитать изъятые у вас документы, предоставить придется. Уликой против вас будет само наличие носителя с зашифрованной информацией в прихваченных с собой вещах, а уж средств убедить вас оказать помощь задержавшим вас личностям в прочтении ваших документов хватает.


Как избежать такого варианта развития событий?

## Запомните

*Умный человек найдет выход из любого сложного положения. Мудрый в этом положении не окажется.*

***Ю. Рихтер***

В пятой главе мы рассматривали как один из вариантов размещение необходимых данных в зашифрованном виде на удаленном сервере. Это удобно, если вы просто хотите перебросить себе копии документов. А если, поработав с документами

и внеся в них коррективы, вам необходимо снова спрятать их? Вы можете, конечно, скачать какую-нибудь шифрующую программу из Сети. Но гостиничные компьютеры (как, впрочем, и компьютеры в интернет-кафе или интернет-клубах) существа не слишком гостеприимные и обычно не разрешают инсталляции новых программ без согласования с системным администратором. Как быть?

*Запомните*

*Жизнь — это то, что случается с нами, пока мы строим планы на будущее.*

***Томас Ла Манс***

### *ПОЛЕЗНАЯ ИНФОРМАЦИЯ*

Общедоступные компьютеры в обязательном порядке имеют набор стандартных программ, входящих в состав Microsoft Office. Грех было бы не использовать некоторые из них для своих целей в путешествии. Если возня с заменой цвета букв или размещением конфиденциальной информации под рисунком (рисунок выносится на передний план, а текст прячется за ним) в Microsoft Word не слишком продуктивна (большой многостраничный документ будет слишком заметен), то использование Power Point обеспечивает возможность скрытой перевозки даже небольших архивов. Рассмотрим пример практического использования этой программы. Давайте создадим слайд, демонстрирующий успехи вашей компании, и наполним его конфиденциальным содержимым. Открыв уже имеющийся или создав новый слайд, внесите в него конфиденциальную информацию (рис. 15.1). Объем текста, который может быть помещен в слайд, практически не ограничен.

Измените цвет шрифта, которым записана информация, на цвет фона плаката (рис. 15.2), а затем сожмите рамку поля, в котором вы ее записали до минимального размера (рис. 15.3).

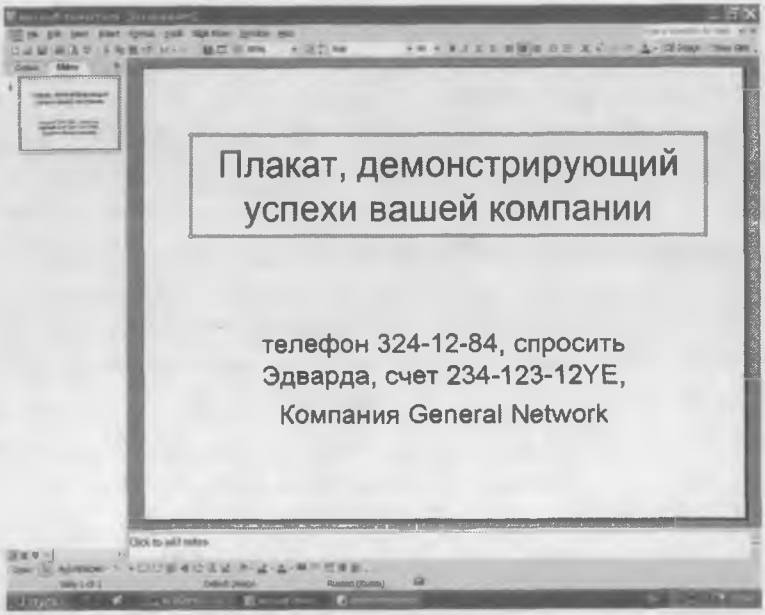



***Рис. 15.1.*** *Демонстрационный слайд с конфиденциальной информацией*

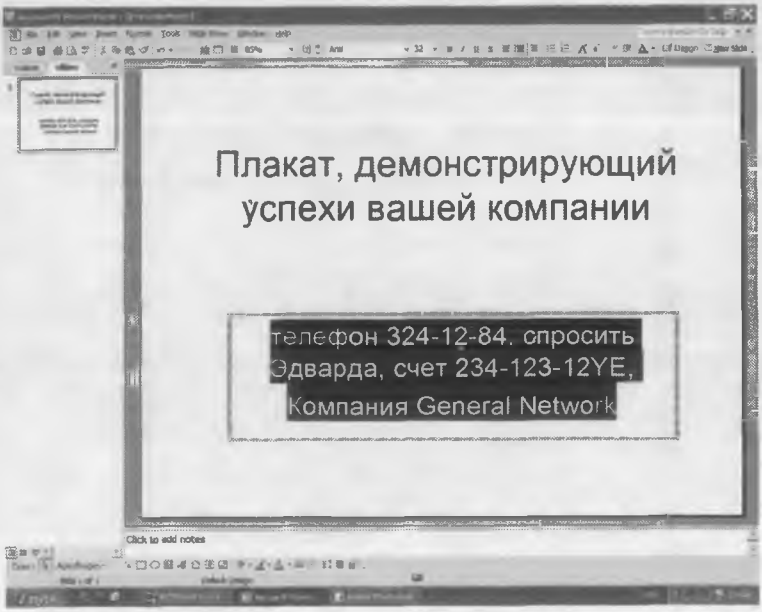



***Рис. 15.2.*** *Выделение конфиденциальной информации и смена цвета шрифта, которым она записана*

Такой способ защиты секретной информации называется «техника микроточки». Он активно использовался разведчиками во время второй мировой войны (правда, тогдашним шпионам было посложнее: они использовали фотоаппараты для пересъемки документов, мощную оптику для уменьшения и чтения текста, материальные носители для переноса и камуфляжа уменьшенного изображения).

Теперь вы можете поместить сформированную «микроточку» на любом месте слайда и прикрыть его, например рисунком (рис. 15.4). Этот слайд ничем не будет выделяться среди других аналогичного (рекламного, например) содержания и вряд ли привлечет внимание лиц, получивших доступ к вашему компьютеру. Вы же, добравшись до конечного пункта своего путешествия, на любом компьютере сможете удалить рисунок-прикрытие, увеличить размер поля с конфиденциальной информацией и получить доступ к ней.

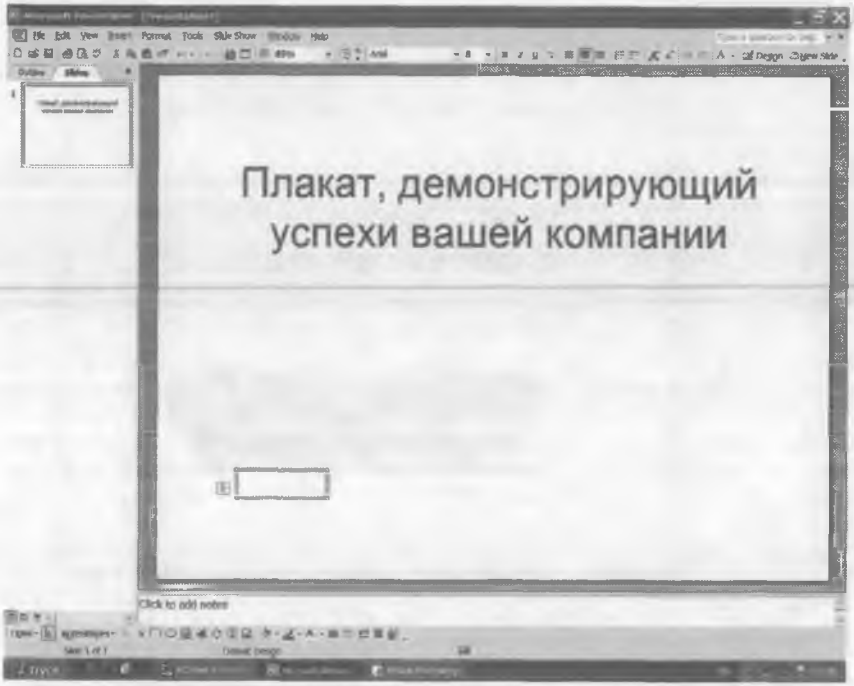



***Рис. 15.3.*** *Уменьшение размеров поля, в котором записана информация*

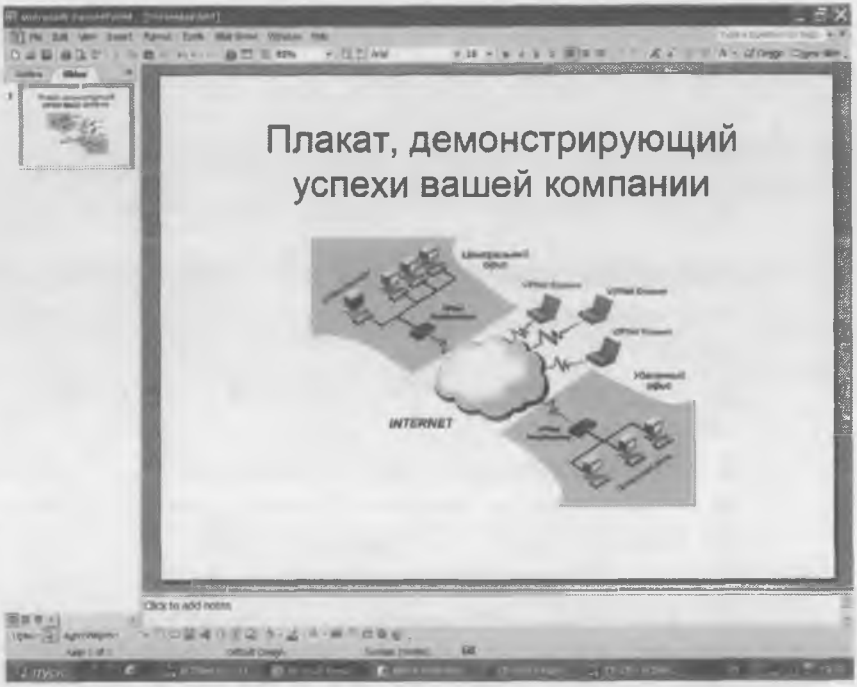



***Рис. 15.4.*** *Рисунок, помещенный поверх невидимой микроточки*

Этот способ самозащиты прост и надежен, но не всегда достаточен. Для исключительных случаев (вы подозреваете, что уже находитесь под наблюдением) бывают нужны дополнительные меры безопасности. Что можно предпринять?

Практически любая программа при установке на компьютере нуждается в предварительной настройке, без которой она либо вообще не будет работать, либо ее работа будет происходить совсем не так, как ожидает пользователь. Часть этих настроек выполняется при инсталляции программы: она выспрашивает у пользователя его имя и место работы, тип установки, путь к месту размещения программы, проверяет, нет ли в предполагаемом месте размещения уже такого файла, иногда при этом сразу указывает каталоги для временных файлов, для сохранения проектов и т.д. Вот против всех этих манипуляций и возражают «компьютеры общего пользования» (зачем обслуживающим их системным администраторам лишняя головная

боль и выяснение, какие из установленных пользователями программ послужили причиной сбоя?).

*Анекдот в тему:*

*Хакер орет на жену:*

*— Ты изменяла?*

*Жена:*

*— Ах ты паскуда, кобелина, да как ты такое мог подумать!*

*Х: — Нет, лучше сразу скажи, ты изменяла?*

*Ж: — Да хорош тебе, просто чушь!*

*И: — Если я узнаю, что изменила — урою!*

*Ж: — Скажи мне, что случилось?*

*И: Что-что! В сеть войти не могу, сервак выдает: «Проверьте имя пользователя и пароль»! Не мог же он сам измениться! Стерва! Ты изменяла?*

Применив программу для шифрования и удалив затем без использования специальных средств следы своей работы с конфиденциальными документами, вы далеко не всегда можете быть уверены, что действительно полностью от них избавились. Временные файлы, остатки файлов со стертыми заголовками на жестком диске, следы использования шифровальных программ в виде некоторых не удаленных при деинсталляции папок, — эти и многие другие элементы могут позволить заинтересованным лицам восстановить информацию, с которой вы работали, определить программное обеспечение, применяемое вами для защиты, оценить его стойкость, проследить пути получения и места хранения ваших секретов.

*Кстати*

*Из рассказа менеджера банка:*

***Оператор**: Представьтесь.*

***Клиент**: Вам мою настоящую фамилию назвать?*

Этих неприятностей можно избежать, воспользовавшись программами, инсталляции не требующими. Когда-то все программы были инструментами прямого действия, потом инсталляторы продемонстрировали, что они могут быть полезны как разработчикам (собирая сведения о пользователях и предотвращая их ошибки при установке программы), так и самим пользователям (выполняя за них часть рутинных операций по созданию каталогов и размещению в них необходимых файлов), и стали неотъемлемым атрибутом современных программ. Конфликт между желаниями пользователей (иметь под рукой привычные программы на любых компьютерах) и системных администраторов в местах общественного пользования побудил разработчиков средств защиты информации выпустить ряд программ, не требующих инсталляции, но позволяющих надежно шифровать и пересылать данные, а затем удалять следы своей работы на компьютере. Порядок работы с документами на общедоступном компьютере при использовании таких программ приведен на рис. 15.5.

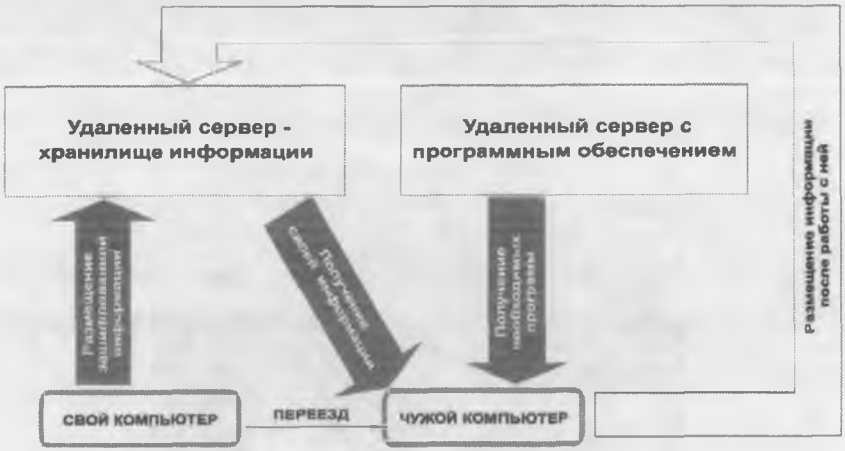



***Рис. 15.5.*** *Организация работы на общедоступном компьютере*

Отправляясь в путешествие, стоит зашифровать и поместить нужную вам в дороге информацию на удаленном сервере. Устроившись в гостинице, можно легко скачать свою инфор-

мацию и программы для ее расшифровки. Поработав, снова зашифровать и разместить обновленный комплект документов в удаленном хранилище. Следы своей деятельности на компьютере целесообразно уничтожать таким же, не имеющим инсталлятора шредером. При такой организации работы вы становитесь перекати-полем, не привязанным ни к конкретному компьютеру, ни к носителям информации, и можете осуществлять управление своим бизнесом, свободно перемещаясь по свету.

## *НЕОБХОДИМЫЕ НАВЫКИ*

Существует несколько программ серии «tiny» (кроха), обеспечивающих защиту информации (табл. 15.1), специально предназначенных для путешественников, испытывающих затруднения при инсталляции программного обеспечения на общедоступных компьютерах. Программы свободно распространяются в сети и используются в качестве рекламной продукции выпустившей их компании.

*Таблица 15.1*

| Программы | Характеристика |
|---|---|
| **Tiny Cipher** http://www.safesofthome.com/tc.htm | Очень простая бесплатная программа. Позволяет шифровать любые объемы документации. Использует AES алгоритм, длина ключа 128 бит. |
| **Tiny Shredder** http://www.safesofthome.com/ts.htm | Очень простая программа. Позволяет надежно уничтожить все следы работы на компьютере. |
| **Tiny Chat** http://www.safesofthome.com/tch.htm | Очень простой интернет-пейджер, позволяющий вести шифрованную переписку при предварительном согласовании применяемых паролей. Использует AES алгоритм шифрования, длина ключа 128 бит. |

Программа Tiny Cipher (рис. 15.6) по уровню защиты и оформлению интерфейса аналогична AES Free, рассматривавшейся в первой главе. К ее недостаткам можно отнести то, что она не архивирует шифруемую информацию и не позволяет создавать самораспаковывающиеся архивы, правда, эти функции разработчики опустили, вероятно, сознательно с целью уменьшения размера файлов, которые приходится скачивать пользователю.

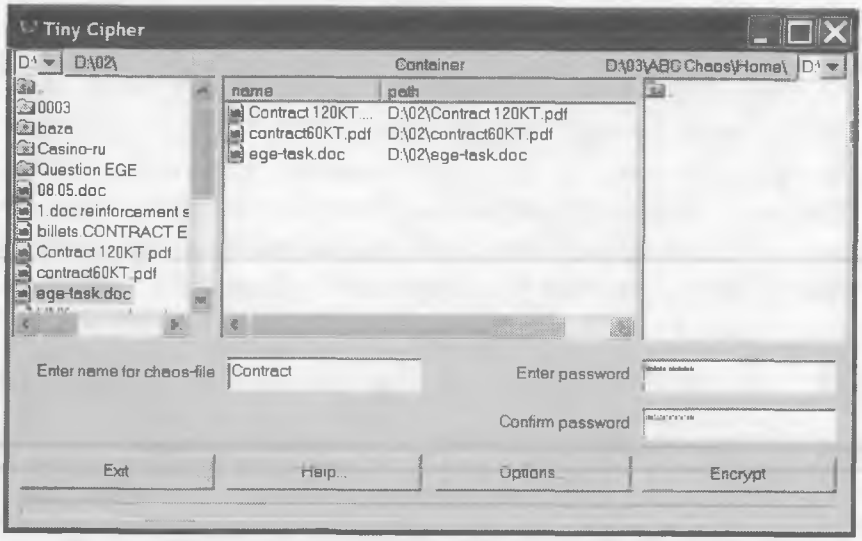



*Рис. 15.6. Интерфейс программы Tiny Cipher*

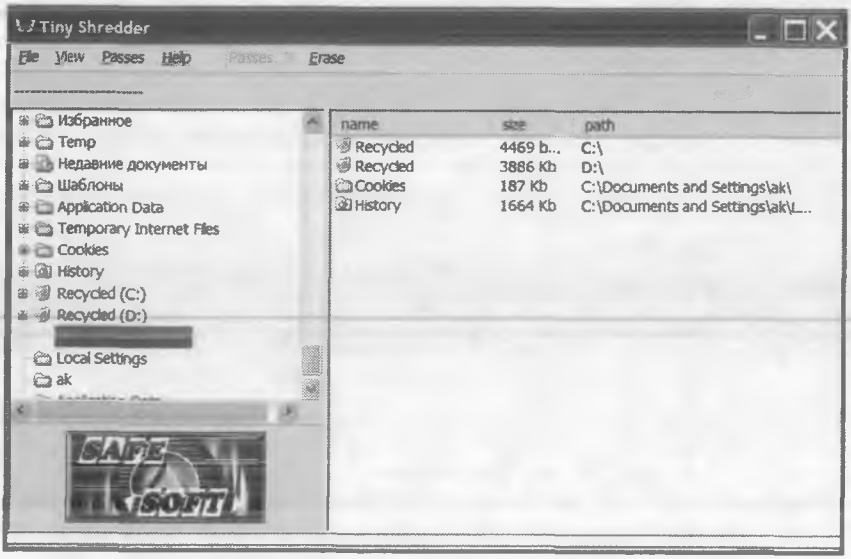



*Рис. 15.7. Интерфейс программы Tiny Shredder*

Программа Tiny Shredder (рис. 15.7) по своим возможностям полностью аналогична программе CHAOS Shredder, описанной в четвертой главе, но имеет втрое меньший размер. После первого же запуска она уютно устраивается на рабочем столе, исправно чистит «авгиевы конюшни» компьютера, а потом бесследно удаляется, чтобы снова при необходимости возникнуть из сети, как джинн из бутылки.

Программа Tiny Chat (рис. 15.8) — упрощенная модификация упомянутого в восьмой главе интернет-пейджера Safe Chat. Tiny Chat позволяет мгновенно обмениваться открытыми ключами с другими удаленными абонентами, находящимися в сети, шифровать передаваемые сообщения и надежно обеспечивает защиту связи путешественника.

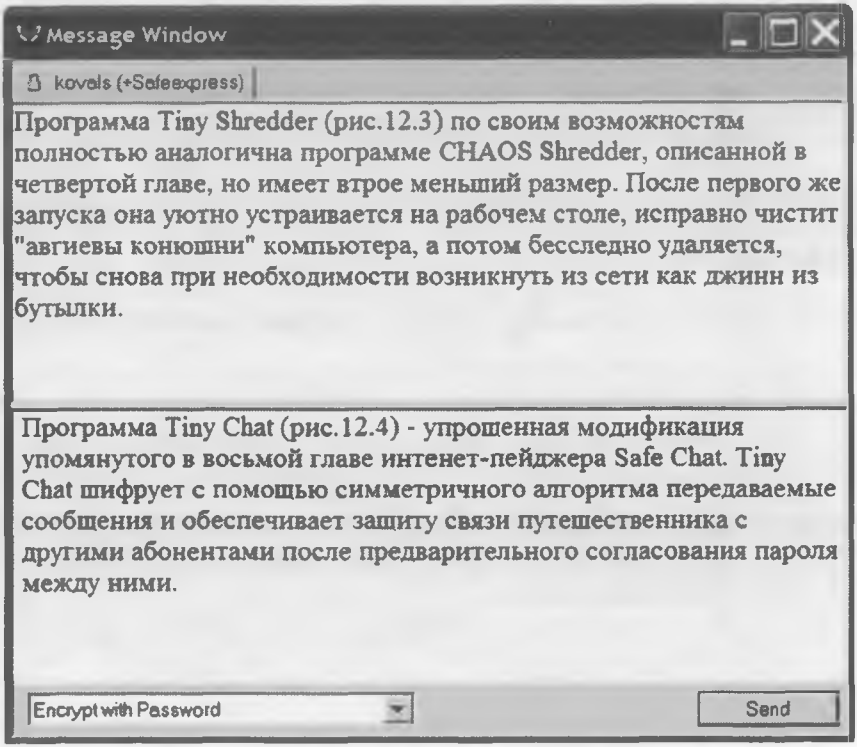



***Рис. 15.8.*** *Интерфейс программы Tiny Chat*

## Кстати ~~~~~~~~~~~~~~~~

*Из рассказа менеджера банка:*

***Оператор**: — Придумайте и назовите слово, которое будет паролем, не менее чем из 5 букв.*

***Клиент**: — Вася.*

***Оператор**: — «Вася» — это 4 буквы, а нужно не менее 5...*

***Клиент**: — А-а-а, тогда Коля.*

***Оператор**: — «Коля» — это тоже 4 буквы, а нужно НЕ МЕНЕЕ ПЯТИ!*

***Клиент**: — А-а-а-а-а, ну давайте тогда мое имя — Таня.*

## Резюме

~ ~ ~ ~ ~

Рассмотренные программы позволяют работать с конфиденциальными документами на общедоступных компьютерах и поддерживать защищенную связь с другими пользователями. Программы этого типа крайне полезны, когда:

- ✓ вам часто приходится работать на чужом компьютере и вы не хотите, чтобы со следами этой работы ознакомился его хозяин;
- ✓ существует вероятность попытки копирования конфиденциальной документации, необходимой вам в путешествии;
- ✓ вам необходимо поддерживать защищенную связь со своими сотрудниками или клиентами с общедоступных компьютеров.

# Техническое послесловие

*В своих бедах вы всегда виноваты сами.*

*NN*

Общие рекомендации и напоминания.

1. Саддам Хусейн потерпел поражение задолго до начала войны в заливе, закупив самолеты «Мираж» французского производства. Продавцы уверяли, что электроника этих самолетов имеет стопроцентную защиту от несанкционированного доступа. Однако когда война началась, эта защита была немедленно отключена одним кодовым сигналом, любезно предоставленным французами американцам. Бортовые системы самолетов были отключены, и армия Ирака осталась без авиации.

Подобный «черный ход» в защищенную систему всегда существует в любой сертифицированной государством программе, но об этом обычно не принято распространяться вслух. Поэтому, шифруя информацию, не используйте программы, разработанные в стране своего местопребывания. Ведь какая тем же французам или американцам разница, что именно вы шифруете их программами? Вот если вы переберетесь к ним...

2. Рекомендации по защите пароля:

а) не используйте очевидные слова или наборы слов, которые легко угадать, например имена или год рождения. Если ваш пароль будет состоять только из одного слова, его очень просто определить, заставив компьютер перебрать все слова в словаре;

б) используйте в пароле пробелы и комбинации цифр, символов и букв. Фраза в качестве пароля гораздо лучше, чем слово. Придумайте фразу, которую легко запомнить, но трудно

угадать: лучше, если такая фраза будет составлена из бессмысленных выражений или очень редких цитат;

в) используйте максимально длинные пароли — чем длиннее пароль, тем труднее его подобрать;

7) периодически (не реже раза в квартал) меняйте свои пароли.

3. При выборе размеров ключей в программе шифрования выбирайте максимальный размер ключа.

4. Не забывайте использовать шредеры при удалении информации из компьютера.

5. Не забывайте шифровать информацию при передаче ее через съемные носители.

6. Конфиденциальную информацию храните только на виртуальных шифрованных дисках.

7. Шифруйте переписку и чат.

8. Используйте бесплатные почтовые ящики.

9. При любых регистрациях в сети (например, при открытии почтового ящика) указывайте только вымышленные данные.

10. Регулярно сканируйте свой компьютер программами-антишпионами.

11. Контролируйте контакты своих сотрудников.

*Кстати* ~~~~~~~~~~~~~~~~~

*Счастье — это когда тебе все завидуют,*
*а нагадить не могут.*

# Заключение

*Крупный успех составлен из множества предусмотренных и обдуманных мелочей.*

*NN*

Картина, написанная художником, и программа, написанная программистом. Что в них общего? Они созданы из множества мелких, подчас незаметных неискушенному наблюдателю элементов мозаики, сложение которых в единое целое дает нам прекрасное произведение. В чем их отличие? Царапина или пятнышко на картине не меняют для нас впечатления от нее. Неверный символ в коде программы делает ее уязвимой, а зачастую и неработоспособной. Создание системы безопасности компании сродни написанию кода программистом. Один маленький сбой в ее работе или заранее не предусмотренная нештатная ситуация и деньги, потраченные на обеспечение безопасности, оказываются выброшенными на ветер. Как говорится в детском стишке:

*Не было гвоздя — подкова отпала,*
*не было подковы — лошадь захромала.*
*Лошадь захромала — командир убит.*
*Конница разбита, армия бежит.*
*Враг вступает в город, пленных не щадя*
*Оттого, что в кузнице не было гвоздя!*

Помните об этом.

**Кузнецов Александр Александрович**

# ЗАЩИТА ДЕЛОВОЙ ИНФОРМАЦИИ (СЕКРЕТЫ БЕЗОПАСНОСТИ)

Издательство ***«ЭКЗАМЕН»***

Гигиенический сертификат
№ 77.99.02.953.Д.008330.09.06 от 14.09.2006 г.

Научный редактор *В.И. Осипов*
Корректор *Л.И. Иванова*
Дизайн обложки *И.Р. Захаркина*
Компьютерная верстка *А.Л. Бабабекова*

105066, Москва, ул. Нижняя Красносельская, д. 35, стр. 1.
www.examen.biz
E-mail: по общим вопросам: info@examen.biz;
по вопросам реализации: sale@examen.biz
тел./факс 641-00-30 (многоканальный)

Общероссийский классификатор продукции
ОК 005-93, том 2; 953005 — книги,
брошюры, литература учебная

Отпечатано в ОАО «ИПК «Ульяновский Дом печати»
432980, г. Ульяновск, ул. Гончарова, 14

**По вопросам реализации обращаться по тел.:
641-00-30 (многоканальный).**