"ЭНЦИКЛОПЕДИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ"

(сборник)

ГРОМОВ В.И., ВАСИЛЬЕВ Г.А.

Материалы, предлагаемые в этом разделе книги посвящены вопросам компьютерной безопасности (в том числе безопасности в сети Интернет).

Данное пособие рассчитано на подготовленного читателя. Если вы еще не совсем опытный пользователь персонального компьютера (ПК), то рекомендуем начинать его изучение с таких книг, как, например, замечательная книга Фигурнова: "Работа пользователя с IBM PC".

## Защита компьютеров от несанкционированного доступа к информации

Особенности защиты персональных компьютеров (ПК) обусловлены спецификой их использования. Как правило, ПК пользуется ограниченное число пользователей. ПК могут работать как в автономном режиме, так и в составе локальных сетей (сопряженными с другими ПК) и могут быть подключены к удаленному ПК или локальной сети с помощью модема по телефонной линии.

Стандартность архитектурных принципов построения, оборудования и программного обеспечения персональных компьютеров, высокая мобильность программного обеспечения и ряд других признаков определяют сравнительно легкий доступ профессионала к информации, находящейся в ПК. Если персональным компьютером пользуется группа пользователей, то может возникнуть необходимость в ограничении доступа к информации различных потребителей.

Несанкционированным доступом (НСД) к информации ПК будем называть незапланированное ознакомление, обработку, копирование, применение различных вирусов, в том числе разрушающих программные продукты, а также модификацию или уничтожение информации в нарушение установленных правил разграничения доступа. В защите информации ПК от НСД можно выделить три основных направления:

- первое ориентируется на недопущение нарушителя к вычислительной среде и основывается на специальных технических средствах опознавания пользователя;

- второе связано с защитой вычислительной среды и основывается на создании специального программного обеспечения по защите информации;

- третье направление связано с использованием специальных средств защиты информации ПК от несанкционированного доступа.

### 1.1. Специальное программное обеспечение по защите информации ПК

Для защиты персональных компьютеров используются различные программные методы, которые значительно расширяют возможности по обеспечению безопасности хранящейся информации. Среди стандартных защитных средств персонального компьютера наибольшее распространение получили:

- средства защиты вычислительных ресурсов, использующие парольную идентификацию и ограничивающие доступ несанкционированного пользователя;

- применение различных методов шифрования, не зависящих от контекста информации;

- средства защиты от копирования коммерческих программных продуктов;

- защита от компьютерных вирусов и создание архивов.

### 1.2. Средства, использующие парольную идентификацию

В простейшем случае вы можете воспользоваться аппаратными средствами установления пароля на запуск операционной системы ПК с помощью установок в CMOS Setup. При запуске ПК на экране монитора появляется сообщение (в зависимости от типа установленного у вас BIOS) вида: Press "DEL" if you want to run Setup или Press "Ctrl""Alt""Esc" if you want to run Setup (для некоторых видов BIOS).

Нажмите клавишу "DEL" или ("Ctrl"+"Alt"-"Esc") и на экране появится меню CMOS Setup. Выберите опцию Password Checking Option, введите пароль, сохраните новые установки Setup ("F10", "Y") и перезапустите ПК. Теперь перед каждым запуском компьютера на экране монитора будет появляться сообщение с требованием ввести пароль.

К сожалению, использование подобной парольной идентификации не является надежным. Достаточно ввести универсальный пароль (AWARD\_SW) или отключить аккумуляторную батарею, расположенную на материнской плате, и компьютер "забудет" все установки CMOS Setup.

Защита встроенного накопителя на жестком магнитном диске составляет одну из главных задач защиты ПК от постороннего вторжения.

Существует несколько типов программных средств, способных решить задачи защиты: защита от любого доступа к жесткому диску; защита диска от записи/чтения; контроль за обращением к диску; средства удаления остатков секретной информации.

Защита встроенного жесткого диска обычно осуществляется путем применения специальных паролей для идентификации пользователя (так называемая парольная идентификация). В данном случае доступ к жесткому диску можно получить при правильном введении пароля при загрузке операционной системы. В противном случае загрузка системы не произойдет, а при попытке загрузки с гибкого диска, жесткий диск становится "невидимым" для пользователя. Эффект защиты жесткого диска в системе достигается видоизменением загрузочного сектора диска, из которого удаляется информация о структуре диска. Такая защита весьма эффективна, и она надежно защищает жесткий диск от рядового пользователя.

## 2. Использование криптографии

##

Возможность использования персональных компьютеров в локальных сетях (при сопряжении их с другими ПК) или применение "модемов" для обмена информацией по телефонным проводам предъявляет более жесткие требования к программному обеспечению по защите информации ПК.

Потребители ПК в различных организациях для обмена информацией все шире используют электронную почту, которая без дополнительных средств защиты может стать достоянием посторонних лиц. Самой надежной защитой от несанкционированного доступа к передаваемой информации и программным продуктам ПК является применение различных методов шифрования (криптографических методов защиты информации).

Криптографические методы защиты информации - это специальные методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования.

Криптографический метод защиты, безусловно, самый надежный метод защиты, так как охраняется непосредственно сама информация, а не доступ к ней (например, зашифрованный файл нельзя прочесть даже в случае кражи носителя). Данный метод защиты реализуется в виде программ или пакетов программ, расширяющих возможности стандартной операционной системы. Защита на уровне операционной системы, чаще всего, должна дополняться средствами защиты на уровне систем управления базами данных, которые позволяют реализовывать сложные процедуры управления доступом.

В настоящее время не существует общепринятой классификации криптографических методов защиты информации. Однако, когда подвергается преобразованию (шифровке) каждый символ передаваемого сообщения ("симметричный" метод закрытия информации), можно условно выделить четыре основные группы:

- подстановка - символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее определенным правилом;

- перестановка - символы шифруемого текста переставляются по некоторому правилу в пределах заданного блока передаваемого текста;

- аналитическое преобразование - шифруемый текст преобразуется по некоторому аналитическому правилу;

- комбинированное преобразование - исходный текст шифруется двумя или большим числом способов шифрования.

Существует большое число программных продуктов шифрования информации, различающихся по степени надежности. Ниже мы рассмотрим наиболее надежные, проверенные временам программы.

### 2.1. Pretty good privacy (PGP)

Очень сильное средство криптографической защиты. Сила PGP не в том, что никто не знает, как ее взломать иначе как используя "лобовую атаку" (это не сила, а условие существования хорошей программы для шифровки), а в превосходно продуманном и чрезвычайно мощном механизме обработки ключей, быстроте, удобстве и широте распространения.

Существуют десятки не менее сильных алгоритмов шифровки, чем тот, который используется в PGP, но популярность и бесплатное распространение сделали PGP фактическим стандартом для электронной переписки во всем мире.

Обычные средства криптографии (с одним ключом для шифровки и дешифровки) предполагали, что стороны, вступающие в переписку, должны были в начале обменяться секретным ключом, или паролем, если хотите, с использованием некоего секретного канала (дупло, личная встреча и т.д.), для того, чтобы начать обмен зашифрованными сообщениями.

Получается замкнутый круг: чтобы передать секретный ключ, нужен секретный канал. Чтобы создать секретный канал, нужен ключ.

Разработанная Филипом Циммерманном программа PGP относится к классу систем с двумя ключами, публичным и секретным. Это означает, что вы можете сообщить о своем публичном ключе всему свету, при этом пользователи программы смогут отправлять вам зашифрованные сообщения, которые никто, кроме вас, расшифровать не сможет. Вы же их расшифровываете с помощью вашего второго, секретного ключа, который держится в тайне.

Свой публичный ключ можно разместить на Web странице, или послать его электронной почтой своему другу. Ваш корреспондент зашифруют сообщение с использованием вашего публичного ключа и отправит его вам.

Прочесть его сможете только вы с использованием секретного ключа. Даже сам отправитель не сможет расшифровать адресованное вам сообщение, хотя он сам написал его 5 минут назад. И самое приятное. На сегодня даже самым мощным компьютерам в ЦРУ требуются века, чтобы расшифровать сообщение, зашифрованное с помощью PGP!

Программа PGP широко доступна в сети. В связи с ограничениями на экспорт криптографической продукции, действующими в США, резиденты и нерезиденты США должны использовать разные места для загрузки программы.

Не так давно вышла новая freeware версия программы PGP 6.0i для Windows 95/NT (знак i после версии означает international). Ее можно скачать здесь (http: // www. pgpi. com).

Сам по себе экспорт PGP из США в 1991 году, распространение программы по всему миру, судебное преследование автора, юридические хитрости, недавно использованные для законного экспорта в Европу версии 5.5 в печатном виде, и другие связанные с PGP моменты представляют из себя историю весьма занимательную. Читайте об этом на официальном сайте в Норвегии или по-русски на отличном сайте Максима Отставнова в Русском Альбоме PGP:

http: // www. geocities. com/SoHo/Studios/1059/

Там вы найдете ответы на все связанные с PGP вопросы.

#### 2.1.1. Уязвимые места PGP

Ни одна система защиты данных не является неуязвимой. PGP можно обойти целым рядом способов. Защищая данные, вы должны задать себе вопрос: является ли информация, которую вы пытаетесь защитить, более ценной для атакующего, чем стоимость атаки? Ответ на этот вопрос приведет вас к тому, чтобы защитится от дешевых способов атаки и не беспокоиться о возможности более дорогой атаки.

Нижеследующее обсуждение по большому счету относятся не только к PGP но и ко многим другим системам шифрования и их уязвимым местам.

Скомпрометированные пароль и закрытый ключ Наверное, самую простую атаку можно осуществить, если вы оставите где-нибудь записанный пароль, защищающий ваш закрытый ключ. Если кто-нибудь получит его, а затем получит доступ к файлу с вашим закрытым ключом, он сможет читать адресованные вам зашифрованные сообщения и ставить от вашего имени цифровую подпись.

Вот некоторые рекомендации по защите пароля:

1. Не используйте очевидные фразы, которые легко угадать, например, имена своих детей или супруги.

2. Используйте в пароле пробелы и комбинации цифр, символов и букв. Если ваш пароль будет состоять из одного слова, его очень просто отгадать, заставив компьютер перебрать все слова в словаре. Именно поэтому фраза в качестве пароля гораздо лучше, чем слово. Более изощренный злоумышленник может заставить свой компьютер перебрать словарь известных цитат.

3. Используйте творческий подход. Придумайте фразу, которую легко запомнить, но трудно угадать: такая фраза может быть составлена из бессмысленных выражений или очень редких литературных цитат.

4. Используйте максимально длинные пароли - чем длиннее пароль, тем труднее его угадать.

5. При генерации ключей ВСЕГДА выбирайте максимальный размер ключа. В DOS версии на вопрос о размере ключа ответьте: 2048 (вместо выбора предлагаемых трех вариантов). В Windows версии выбирайте ключ размером 4096 и более.

Подделка открытых ключей Самое уязвимое место - это возможность подделки открытых ключей.

Вероятно, это самое серьезное слабое место любой криптосистемы с открытыми ключами, в частности, потому, что большинство новичков не в состоянии немедленно обнаружить такую подделку. О том, почему это важно и какие против этого следует предпринимать меры, подробно написано выше, в разделе "Как защитить открытые ключи от подделки".

Вкратце: когда вы используете чей-то открытый ключ, удостоверьтесь, что он не был подделан. Целостности нового чужого открытого ключа следует доверять, только если он получен непосредственно от его владельца или подписан кем-то, кому вы доверяете. Обеспечьте невозможность подделки открытых ключей на вашей связке. Сохраняйте физический контроль как над связкой открытых ключей, так и над своим закрытым ключом, по возможности сохраняйте их на своем персональном компьютере, а не на удаленной системе с разделением доступа. Сохраняйте резервную копию обеих связок.

Не до конца удаленные файлы Еще одна потенциальная проблема безопасности связана со способом, которым большинство операционных систем удаляет файлы. Когда вы шифруете файл и затем удаляете файл с исходным открытым текстом, операционная система не стирает данные физически. Она просто помечает соответствующие блоки на диске как свободные, допуская тем самым повторное использование этого пространства. Это похоже на то, как если бы ненужные секретные документы выбрасывались в мусорную корзину вместо того, чтобы отправить их в шреддер. Блоки диска все еще сохраняют исходные секретные данные, которые вы хотели стереть, и лишь со временем будут заняты новыми данными. Если злоумышленник прочитает эти блоки данных вскоре после того, как они помечены как свободные, он сможет восстановить ваш исходный текст.

Это может произойти и случайно: если из-за какого-нибудь сбоя будут уничтожены или испорчены другие файлы, для их восстановления запустят программу восстановления, а она восстановит также и некоторые из ранее стертых файлов. Может случится так, что среди последних окажутся и ваши конфиденциальные файлы, которые вы намеревались уничтожить без следа, но они могут попасться на глаза тому, кто восстанавливает поврежденный диск. Даже когда вы создаете исходное сообщение с использованием текстового редактора или Word-процессора, программа может оставить множество промежуточных временных файлов просто потому, что она так работает. Эти временные файлы обычно удаляются редактором при его закрытии, но фрагменты вашего секретного текста остаются где-то на диске.

Единственный способ предотвратить восстановление открытого текста - это каким-либо образом обеспечить перезапись места, занимаемого удаленными файлами. Если вы не уверены, что все блоки, занимаемые на диске удаленными файлами, будут вскоре использованы, нужно предпринять активные шаги для перезаписи места, занятого исходным открытым текстом и временными файлами, создаваемыми Word-процессором. Это можно осуществить, используя любую утилиту, которая способна перезаписать все неиспользованные блоки на диске. Такими возможностями, к примеру, обладают многие криптосистемы (Kremli, BestCrypt - см. ниже).

Вирусы и закладки Другая атака может быть предпринята с помощью специально разработанного компьютерного вируса или червя, который инфицирует PGP

или операционную систему. Такой гипотетический вирус может перехватывать пароль, закрытый ключ или расшифрованное сообщение, а затем тайно сохранять их в файле или передавать по сети своему создателю. Вирус также может модифицировать PGP таким образом, чтобы она перестала надлежащим образом проверять подписи. Такая атака обойдется дешевле, чем криптоаналитическая.

Защита от подобных нападений подпадает под категорию общих мер защиты от вирусных инфекций. Существует ряд коммерчески доступных антивирусных программ с неплохими возможностями, а также набор гигиенических процедур, следование которым серьезно снижает риск заражения вирусами. Общие вопросы мер борьбы с вирусами и червями находятся за пределами темы настоящего документа. PGP не содержит никакой защиты от вирусов, и ее использование предполагает, что ваш персональный компьютер является надежной средой. Если такой вирус или червь действительно появится, будем надеется, что сообщение об этом достигнет ушей каждого.

Другая аналогичная атака заключается в том, чтобы создать хитрую имитацию PGP, которая в работе выглядела бы точно так же, но делала не то, что предполагается. Например, она может обходить верификацию подписей, делая возможным принятие фальшивых сертификатов ключей.

Вы должны попытаться получить свою копию PGP непосредственно от PGP, Inc.

Существует также возможность проверить, не подделана ли PGP, с помощью цифровых подписей. Вы можете использовать другую заведомо целую версию PGP для верификации цифровых подписей на двоичных файлах подозрительной версии. Это не поможет, если вирусом инфицирована сама операционная система или если первоначальная версия PGP модифицирована таким образом, чтобы уничтожить в ней способность проверять подписи.

Такая проверка также предполагает, что у вас есть заслуживающая доверия копия открытого ключа, который можно использовать для верификации подписей на исполняемых модулях PGP.

Файлы подкачки (виртуальная память).

PGP первоначально разрабатывалась для MS-DOS, довольно примитивной по сегодняшним стандартам операционной системы. С ее переносом в другие, более сложные операционные системы, такие как MS

Windows или MacOS, возникло еще одно уязвимое место. Оно связано с тем, что в этих более хитрых операционных системах используется технология под названием "виртуальная память".

Виртуальная память позволяет вам запускать на своем компьютере огромные программы, размер которых больше, чем объем установленных на машине полупроводниковых микросхем памяти. Это удобно, поскольку с тех пор, как графический интерфейс стал нормой, программы занимают все больше и больше места, а пользователи норовят запускать по несколько больших приложений одновременно. Операционная система сохраняет фрагменты программного обеспечения, которые в настоящий момент не используются, на жестком диске. Это значит, что операционная система может записать некоторые данные, о которых вы думаете, что они хранятся только в оперативной памяти, на диск без вашего ведома.

Например, такие данные, как ключи, пароли, расшифрованные сообщения.

PGP не оставляет подобного рода секретные данные в памяти дольше, чем это необходимо, однако остается вероятность того, что операционная система успеет сбросить их на диск.

Данные на диск записываются в особую временную область, известную как файл подкачки. По мере того как данные становятся нужны, они считываются обратно в память. Таким образом, в каждый отдельный момент в физической памяти находится лишь часть ваших программ и данных. Вся эта работа по подкачке остается невидимой для пользователя, который лишь слышит, как щелкает дисковод. MS Windows перекачивает фрагменты памяти, называемые страницами, используя алгоритм замещения LRU (наиболее давно использованных страниц). Это означает, что первыми окажутся сброшены на диск страницы, доступ к которым осуществлялся наиболее давно. Такой подход предполагает, что в большинстве случаев риск того, что секретные данные окажутся сброшенными на диск, неощутимо мал, поскольку PGP не оставляет их в памяти надолго. Но мы не можем дать никаких гарантий.

К этому файлу подкачки может получить доступ каждый, кому физически доступен ваш компьютер. Если вас беспокоит эта проблема, возможно, вам удастся ее решить, установив специально программное обеспечение, стирающее данные в файле подкачки (например замечательная программа Kremlin 2.21 - ее можно скачать на многих серверах в том числе на http: // www. download. com и http: // www. shareware. com). Другим возможным средством является отключение механизма виртуальной памяти в операционной системе. Это позволяет сделать и MS Windows, и MacOS.

Отключение виртуальной памяти означает, что вам потребуется больше физически установленных микросхем оперативной памяти, для того чтобы в нее вошло все.

Нарушение режима физической безопасности Нарушение режима физического доступа может позволить постороннему захватить ваши файлы с исходным текстом или отпечатанные сообщения.

Серьезно настроенный противник может выполнить это посредством ограбления, роясь в мусоре, спровоцировав необоснованный обыск и изъятие, с помощью шантажа или инфильтрации в ряды ваших сотрудников.

Применение некоторых из этих методов особенно подходит против самодеятельных политических организаций, использующих в основном труд неоплачиваемых добровольцев.

Не стоит впадать в ложное чувство безопасности только потому, что у вас есть криптографическое средство. Приемы криптографии защищают данные, только пока те зашифрованы, и не могут воспрепятствовать нарушению режима физической безопасности, при котором скомпрометированными могут оказаться исходные тексты, письменная или звуковая информация.

Этот вид атаки дешевле, чем криптоаналитическая атака на PGP.

Радиоатака Хорошо оснащенным противником может быть предпринята атака еще одного вида, предполагающая удаленный перехват побочного электромагнитного излучения и наводок (сокращенно - ПЭМИН), испускаемого вашим компьютером. Эта дорогая и часто трудоемкая атака, вероятно, также является более дешевой, чем криптоанализ.

Соответствующим образом оборудованный фургон может припарковаться рядом с вашим офисом и издалека перехватывать нажатия клавиш и сообщения, отображаемые на мониторе. Это скомпрометирует все ваши пароли, сообщения и т.п. Такая атака может быть предотвращена соответствующим экранированием всего компьютерного оборудования и сетевых кабелей с тем, чтобы они не испускали излучения. Технология такого экранирования известна под названием Tempest и используется рядом правительственных служб и организаций, выполняющих оборонные заказы. Существуют поставщики оборудования, которые продают Tempest.

Кроме того можно использовать специальные генераторы "белого шума" для защиты от ПЭМИН, например: ГБШ-1, Салют, Пелена, Гром и др. Их можно приобрести во многих Московских фирмах торгующих спецтехникой (см. ПРИЛОЖЕНИЕ).

Защита от фальшивых дат подписей Несколько менее очевидным слабым местом PGP является возможность того, что нечестный пользователь создаст электронную подпись на сообщении или сертификате ключа, снабженную фальшивой датой. Если вы пользуетесь PGP от случая к случаю, вы можете пропустить этот раздел и не погружаться в дебри сложных протоколов криптографии с открытыми ключами.

Ничто не помешает нечестному пользователю изменить системную дату и время на своем компьютере и создать сертификат своего открытого ключа или подпись, содержащие другую дату. Он может создать видимость того, что подписал что-то раньше или позже того времени, когда он это действительно сделал, или что его пара ключей была создана раньше или позже. Из этого могут проистекать различные юридические или финансовые выгоды, например, за счет создания некоего оправдания, позволяющего ему затем отрицать свою подпись.

Мы полагаем, что проблема фальшивой даты на электронной подписи не более серьезна, чем проблема фальшивой даты, стоящей рядом с подписью ручкой. Никого не волнует, что кто угодно может поставить любую дату рядом со своей подписью на договоре. Иногда "некорректная" дата рядом с подписью не предполагает никакого мошенничества: возможно, она означает время, с которого подписывающий признает этот документ, или время, с которого он хочет, что бы его подпись вступил в силу.

В ситуациях, когда вопрос доверия к тому, что подпись выполнена именно в определенное время, является критичным, люди могут просто обратится к нотариусу, чтобы он засвидетельствовал момент подписи и заверил это своей печатью. Аналогично, при использовании цифровой подписи для заверки даты подписи документа можно обратится к пользующейся доверием третьей стороне, чтобы она сертифицировала эту подпись своей. Никакого экзотического или чрезмерно формализованного протокола для этого не требуется. Подписи свидетелей издавна используются как юридическое доказательство того, что документ был подписан в определенное время.

Пользующийся доверием уполномоченный сертификатор или нотариус может создавать достойные доверия подписи с заведомо корректной датой.

Такой подход не требует централизованной сертификации. Возможно, эту роль может выполнять любой пользующийся доверием посредник или незаинтересованная сторона точно так же, как действуют сегодня обычные нотариусы. Когда нотариус заверяет своей подписью подпись другого лица, он создает заверенный сертификат другого заверенного сертификата, который может служить подтверждением подписи, выполненной от руки. Нотариус может вести собственный реестр, добавляя в него отдельные сертификаты с цифровыми подписями (не копируя в него сами подписанные документы). Этот реестр можно сделать общедоступным. Дата на подписи нотариуса должна пользоваться доверием, и она может являться более веским доказательством и юридически быть более значимой, чем дата на сертифицируемой подписи.

Последующие версии PGP, вероятно, будут предусматривать возможность простого управления нотаризованными сертификатами подписей с достойными доверия датами.

Утечка данных в многопользовательских системах PGP была создана для использования на персональном компьютере, находящимся под физическим контролем лишь одного пользователя. Если вы запускаете PGP дома на своем собственном PC, ваши зашифрованные файлы находятся в безопасности, пока никто не ворвался в ваш дом, не украл компьютер и не заставил вас открыть ему свой пароль (или не отгадал пароль, если он слишком прост).

PGP не предназначена для защиты исходных открытых данных в скомпрометированной системе. Она также не может предотвратить использования злоумышленниками изощренных способов доступа к закрытому ключу во время его использования. Вы должны просто знать о существовании этих опасностей при использовании PGP в многопользовательской среде и соответствующем образом изменить свои ожидания и свое поведение. Возможно, ваши обстоятельства таковы, что вы должны рассмотреть возможность использования PGP только на изолированной однопользовательской машине, находящейся под вашим непосредственным физическим контролем.

Анализ активности Даже если атакующий не сможет прочитать содержимое вашей зашифрованной корреспонденции, он может извлечь по крайней мере некоторую полезную информацию, наблюдая, откуда приходят и куда уходят сообщения, отмечая их размер и время дня, когда они отправляются. Это похоже на то, как если бы злоумышленник смог взглянуть на счет за междугородные телефонные переговоры, чтобы узнать, кому вы звонили, когда и сколько времени разговаривали, даже если содержание телефонных разговоров остается ему неизвестно. Это называется анализом активности. Решение этой проблемы требует введения специальных коммуникационных протоколов, разработанных для повышения сопротивления анализу активности в вашей коммуникационной среде. Возможно, при этом потребуется применение ряда криптографических приемов.

Криптоанализ. Возможно, кто-то, обладающий суперкомпьютерными ресурсами (например, правительственная разведывательная служба) предпримет дорогостоящую и чудовищную криптоаналитическую атаку. Возможно, ему удастся сломать ваш ключ RSA, используя новые засекреченные знания в области разложения чисел на множители. Но гражданские ученые интенсивно и безуспешно атакуют этот алгоритм с 1978 года.

Возможно, правительство обладает каким-либо секретным методом взлома обычного шифра IDEA, использованного в PGP. Это - самый страшный кошмар для криптографа. Но абсолютных гарантий безопасности в практическом приложении криптографии не бывает.

И все же осторожный оптимизм кажется оправданным. Разработчики алгоритма IDEA - одни из самых сильных криптографов Европы. IDEA подвергался интенсивной проверке на безопасность и экспертировался лучшими гражданскими криптографами мира. В том, что касается устойчивости к дифференциальному криптоанализу, он, вероятно, лучше DES.

Кроме того, даже если этот алгоритм обладает каким-то до сих пор не замеченными слабыми местами, опасность сильно уменьшается из-за того, что PGP сжимает открытый текст до шифрования. Стоимость необходимых для взлома вычислений скорее всего будет больше ценности любого сообщения.

Если обстоятельства, в которых вы находитесь, оправдывают предположения о том, что вы можете подвергнутся столь чудовищной атаке, возможно, вам следует обратится к консультанту по вопросам безопасности данных для выработки особого подхода, соответствующего вашим чрезвычайным требованиям.

В общем, без надежной криптографической защиты ваших данных от противника не требуется практически никаких усилий для перехвата ваших сообщений, и он может делать это на повседневной основе, особенно если они передаются по модему или электронной почтой. Если вы используете PGP и соблюдаете разумные меры предосторожности, злоумышленнику потребуется затратить намного больше усилий и средств для нарушения вашей приватности.

Если вы защищаете себя от простейших атак и чувствуете, что на вашу приватность не собирается посягать целеустремленный и обладающий огромными ресурсами противник, вы, вероятно, будете защищены PGP. PGP

дает вам Почти Полную Приватность.

#### 2.1.2. Интернет-ресурсы PGP

В сети можно найти огромное количество связанной с PGP

информации. Неплохие ее каталоги расположены на страницах:

- PGP, Inc. (www. pgp. com);

- PGP. net (www. pgp. net);

- международный сервер PGP (www. pgpi. com);

- конференция пользователей PGP (pgp. rivertown. net);

- "Русский Альбом PGP" (www. geocities. com/SoHo/Studios/1059/).

### 2.2. Зашифровка информации в изображении и звуке

Этот класс продуктов, называемых стеганографическими, позволяет прятать текстовые сообщения в файлы. bmp,. gif,. wav и предназначен для тех случаев, когда пользователь не хочет, чтобы у кого-либо создалось впечатление, что он пользуетесь средствами криптографии.

Пример подобной программы - S-tools:

ftp: // ftp. kiae. su/pub/windows/crypto/s-tools4. zip

Программой очень легко пользоваться. Внешне графический файл остается практически неизменным, меняются лишь кое-где оттенки цвета.

Звуковой файл также не претерпевает заметных изменений. Для большей безопасности следует использовать неизвестные широкой публике изображения, изменения в которых не бросятся в глаза с первого взгляда, а также изображения с большим количеством полутонов и оттенков. Использовать картину Танец Матисса - идея плохая, т. к. все знают, как она выглядит, и, кроме того, она содержит большие зоны одного цвета.

Программа может использовать несколько разных алгоритмов шифровки по выбору пользователя, включая довольно сильный алгоритм 3DES.

### 2.3. Зашифровка с помощью архиваторов

Arj, Rar, WinZip и им подобные архиваторы позволяют создавать защищенные паролем архивы. Этот способ защиты значительно слабее описанных выше. Специалисты по криптографии утверждают, что в методах шифрования, применяемых в архиваторах, содержаться "дыры", позволяющие взломать архив не только подобрав пароль, но и другими способами. Так что не стоит пользоваться этим методом шифрования.

### 2.4. Защита паролем документов MS Office

Не используйте этот метод никогда! Взлом настолько прост, что изготовитель коммерческого пакета для восстановления паролей, забытых незадачливыми пользователями, включил в программу пустые циклы, чтобы замедлить ее работу для создания впечатления сложности поставленной задачи. Изготовитель же некоммерческого пакета:

http: // www. geocities. com/SiliconValley/Vista/6001/pwdremover. zip

пустых циклов в программу не включал, так что взлом занимает меньше секунды. Взламываются документы MS Word 6.0 и 7.0, MS Excel 5.0 и 7.0, причем созданные как английской версией продукта, так и несколькими национальными, включая русскую.

### 2.5. Защита данных с помощью программы NDEC

NDEC простая и в то же время чрезвычайно надежная программа, в который были применены оригинальные алгоритмы многоступенчатого полиморфного кодирования с использованием двух ключей. Это означает что например один и тот же файл зашифровываемый одним и тем же ключом, каждый раз будет иметь новый, отличный по всем байтам вид.

Пользователям NDEC при шифровании/расшифровке данные необходимо вводить ДВА пароля. Длинна каждого пароля не может быть больше 256 символов.

section 1 of file ndec. com < uuencode 1.0 by FRIENDS Software >

filetime 614831580

begin 644 ndec. com

M4+AU' [HN! 3O$<WF+Q"U"`R7P\_XOXN: $`OHX! \_/. EB] BQ! - /KC-D#V5,SVU/+

MD`$"3F] N($1E8V] D: 6YG($5M86EL($-R>7! T; W(@=F5R<VEO; B`Q+C`@0F5T

M82`M(#0N,2`J\*BHJ3F] T(&5N; W5G: "! M96UO<GDD("`@("`@("`@("`@N``)

MNF8! S2'-(/V+^$] /OLX"`\_\*+RM'I\Z7\A\_=&1K\``: V5NA``ZS\*0K96R$. L [

MK96R$. L\K96R$. M! K96R$. MCK96R$. MDK96R$. MEK96R$. MFK96R$'((I-'M

M2G3T<\_@SR3/; T>U\*=+\_1T] 'M2G2^T=.%VW07T>U\*=+G1TX# [! G(+T>U\*=02M

ME; (0T=,NBH\; `8#Y"G0Z,] N#^0) T) M'M2G27<A\_1 [4ITEM'3T>U\*=) 71T] 'M

M2G24T=. `^P) S'BZ\*ORL! K(K85HOW\*\_/SI% [KB\*P"R(#5`#S\_=; SK,] 'M2G4$

MK96R$-'3@/L(<M+1 [4IU! \*V5LA#1TX# [%W+"T>U\*=02ME; (0T=. ! X] \`AM\_K

MM%@&NRX) 4S/; B\N+TXOKB\_. +^\L#``(\*! `4````````&! P@) `0(```,$! 08`

M``````````<("0H+#`T\*0#X! \*$, I2&E-04XN`8`! =F5R>2! S: 6UP; &4@8X) 4

M"W! T; W(6/````0!.; VXM1&5C; V1I; F<@1<`) +6UA: 6P@0R(H=&VR"BD@. C@D

M(#$`D"XP($) E=&$@+2`T#0H%%%L2.3DW+3(P`2`\*5$UI5&] S; V9T. H&$-G! A

M<F%T,BP@06P"BDM2: 6=H=','97,J! 4A+9#I4: &F\_4G-59B\@BE) X=`YN82MU

MBL0C(! 1L>6) N; W0N8! R5<W1R: 6) U5IE0. T5GI5`01B"=(%M0H%1); &EP(%K5

M; 4"AF+=N; ETB"D99E36F&V4%LV`A8V5N<] KTJB! D`TZ>; J(4; W1H! '<! +JB$

M<VAO=W1(8WDN8 [\*K"`U("2AJFF%CB7=I) ZM2\*F$Z\*') \*5CIW170\A! 55]: A`

M<&) \*22=G+"X$=H(46215<PYE. NFU4"`:; $66.2UE>-\*69: HJ/@P3/E6\*. N2H

M8R(@5) 0X&D89($] U`2<(6W! A<W,Q70@R. ^] =22M) \^P(2@(. =$EDM11\*6V$D

M%R0M; V5SH0) D? `HE$RX9! R131'5!%==Y('! H<BXE,4@". B1/; O,@; 154%^$M

M) `\_/) R@. ? 1MQ#D50%<4@^BSH\*%@$2F%G826] 5#H&88! W,16Y'4YF9@@%] V%4

MHRT&`) &Y\_P`SP"XJ! 3+@`L3@! /; 81^+TPQ("! 2K@95(R$M02Y$! 451 [D01`(

M) `$`'\_X`,N3-%CP-=`. JXO4`9#+`JKI\_!. @V`,-7. `$`#O. J7\/W%8OWK8O0

MN7T4@`"M\*D+0\_LHRP@K`=02"`E [2R\*K2#=; 0Y@(``/`JUO; >XN##M`G-(<. L

M/"``H'3 [3L,\87(&/'IW`B3? H) ! D0`"L@6@! =`M. "1L': ^YKPU5N"#) K; F] W

M,VUM2$! J. @! M`&] H\_`'\! \_QLT@W\$P$`90$J`C("\*C(`N``] S2&+V`"AP [0\

M,\GK] ; 1`3`GAM#\%/@7\NBB`,`'H"? N^@`"L$P`\*" [IY`NC [^KC\_3! OH^! (`

M^JP,+J) ^! #Q%=`D\1```=`6Z; @3KX. C@^K^"!%? HZQ0`^NC6"L,$Z. +Z6NB:

M\_P`2<QU2NA4#Z+ [Z7DET"T`! Z,'ZBM"T`D? K\+H; `Z@$ZZJC! #XL>O] RV``(

MHP8%@'S\_#70] Z); Z@P) \*-K\(! 4Z=^E] 7%! 16Z%4^7^C] ^70(8\*,) +OX&/P,H

M;. AN\*$5H"`8D>23H\@\*%'0D) Z: $`S!,'Z! L$BAD%Z! 7ZNB] Z1/I25"+S'H`^

ML\*F2JQRK$C(%5! XDW\_F+SX'I": H"#+XMG/. F7W04%`BZD! \3^NNZ,^\*E%\_E5

MBP! R) @@D) NC%^6\_HO\_E6 [OF: ^9Q6&K) D5MP>) (E64GH(\*\] 4! @%4P=XUZ [WH

M3J2@E#1%=$\*Z4A>H3$) 2``: B! A`) N0$`BQX%L`2U>\_ZZ=0RY``0! H`UN\_@O`

M=! 90B\CH=P"4@A<0%`845? Y8/0+\*'W39ZT^Z8#QF! BA"8/GH`\_D\A70$5,VE

M=/5E3BI,NE) 8Z"4"41W? [U'%403>;%$A`? X41@#Z\_2T) ^<T@"E! 1OSXNBB8(

M"3/; "@`'A] 4N`"4N] ATN\*`4N! 4`P`P`%TLSVW#+@1T-0@24"(N+<6>L`. =4R

M+29] -$(R! 5. ! - ! #K\RX"! O [2YU0V/$(E%%`\_,L0] XM=9,L"^! 50V.1! 14\*Q1

MNS2$4J,\) P6@'! OXJEE84+L-"=<`5=>S"UC^P#P#: 0B4+>+869=APV [J%3@\*

B. . L#J5<XGQ`0GY/GGP"? T@V? #0\U`P86-``,) 0F<#0:? \_P

`

end

sum - r/size 33185/2491 section (from "begin" to "end")

sum - r/size 51962/1789 entire input file

### 2.6. Защита данных с помощью программы "Кобра"

"Кобра" - это программа, о которой даже зарубежные специалисты говорят как о самой совершенной и научно обоснованной криптосистеме.

Ежегодно проводятся семинары и научные конференции, где сотни уважаемых математика всех стран обсуждают перспективы "Кобры" и оригинальный алгоритм, разработанный российскими программистами. Так что "Кобра" это пожалуй лучший вариант, но она стоит денег.

Справки по телефонам в Питере: (812) - 234-0415, 245-3743, 234-9094, 245-3693.

### 2.7. Защита дискет с помощью программы DiskHide

DiskHide это программа которая позволяет сделать любую дискету (после того как вы записали на нее информации) абсолютно пустой. Вряд ли например у таможни или у вашего начальника хватит ума просматривать с помощью DiskEditor`а содержимое пустой дискеты.

section 1 of file dh. zip < uuencode 1.0 by FRIENDS Software >

filetime 614831580

begin 644 dh. zip

M4$L#!! 0````(```(?! OBTQ\*(Z`4``#H&```,````1$E32TA) 1$4N15A%79- [

M4% -W%L=\_] ^; >/`GAD6A] WYAP>20$0M! `B#%@@@P2&@&A^&``! >211) (`1B$D

MC6#K5<"V5\*WMB`A%@=@6'%0TJXN/] ;%8LEB'+>WJ5-?! LG5QJ19! R0\*=SFC/

M'Y\_O] \_SFG-\? Y\_Q^FHTR@``(D,%: R. /9! @`,`(#&/"DSXN4; M"88TZ2MP31Y

MVPKU6PTZ3! PI%D>$8\_%&2\ZN0KTA=`66:] B) B<. CL) 0RDZDP! \,P"G@SSIV&

M>K,`"D`,&0: FA: $8F\*P; F`I=`. HN: \\_\_#4@\&7] 10: \_&6V^? H? 5&0/W<? BS9

M8,; R] (: R@NV8+D] G,%KXK\_</ISJNB$C? [^\G^FR/6-\@Q/\&'Q-WW$^2DXEI

MP8A@J. Y: W?! XZZNZ'RGD2P"2O'`V] OJ`T; `&9V.7SVC4'\*/GJ) AC] AQSYI@ [

M2R. C,Z\*OW? U+HOF9Z; GDIF1XUO: Y! V? EK^ [! FF'S\_%E [T3UHFR(; &3. ^#) GM

M<P^\*] M7G0 [: 7=+-9,NQX"9M#9NL^,\_) FY<CO%QR>DS\:;%. PB2/: =ZD<ZMPW

ME$ [\) AB? ',=; IK) & [6\548W#; ^7SC;?? R. T/ [X/: ^Z. N3OB& [3L@] Y2] OXD8

M=5SQ(0; K^IQ\*LV^"^; >#SD,XM.2GE\_8^#VOTB9-T96; N3N+! E),TE. K4S@SL

M1\EE8HBX00P0(\08,7&;! &`Z@OZ^-3\*%2H-F7@() 0<E\_; '+FB, [P8H(\_A^-.

M3RV#Z [ZHN<V\_&`? 7`\_4-^YUG/0RZ"V\*=I4,`. <M@B. Y%QIN@+O@) Q8\MU%"I

MCJ%N9$$-&'F\VSW>YY! G,%Q:! `\*H2+\*ZFB) =967A'X [9]: G3JP4\_" [: (@P5 [

MO06U,8RF"WZ [5IQUT)""S672`B52L%&ZR88T/&-9: - T,=3M\*N0#8P\*? F'6O, M] "U. S01: \_I\@=H>! Z<RX [XJ\_>D5KZSCFS?); S) 7#. UCG [KIB5TF [-) =(U&`K

MQ<I! $$ [: \> [MS%\_I%. E0FS>4RF,#7H##VK! #&AN [$Z\*\*XC2E\,D] @MHDOXX<

M9\*+\_9%Q&NG<7E2EO07\_@<: /=CK% [\_\_XN,\_L1F=\3"H"\_E=:; V: Y#%\%G%Q+J

M@TNE=K [7U,TFAQ"B^? 5$`U$\*? &%Q) - Q$J>'DT/=`Q>1%F6G/60(6'RK\*G89=

M] -5`^ [%PXB:] FO; @`\H [=7YW [TGM/M(5BSB3S/8M)"WC7T#UZ: \_=0I4QVC<V

MS5\>H; +R [0D-88] WH>2') N0IM0G+#%Z9R+;: 'J%P/17/\_3J/ [GCU4+(!? 9V5

MV^PBD8#Y: '] K [: VFI%%/-XG4ZSK. () ="] (S [L/J$EWJ) ZX\*? FBF;! N<! 2)%?

M#; 'G4^81UXD? QMJ6MO\_CZ) ! /XN\*'"`P'7HV^. >6D@Y<+$=T"QVOL`! 1P375Y

MC^\_8,X%WY6) D\MN\*$84-+4X'XN\_) D6@#XDI&H@8LWI:! U: C). \_`%\*<E? <^"+

MZT@Y% -\*3\(F,YD6CP!! 7! O [9) X\*Z4"9^B2^(#0H"X7$; DQ'=5D-Q08F! JUP?

MKI#) 5T7+? (LJ@): U4U1=6,(/3BZKWF: U-2\_+YD4)"\_-\*ET? &O&#\*%,+ZS@<U

M\*; UX: T<SVF: [2CKZ] \*>. $VUMH2W"7] \*UH4\Y89'A$6Q] 40R/PA>+%;: 4M/RJ

M?%6NOH0? HE6KPN0KN) HEX<N/] <Z'% -^&3; @2@4\*I\*31FE\_/R371\_BZ4ZOZ22

M&: \*DEX=GDQ. P"- [RX^<: 0Z,#ON('<TWXJABYTNO,T [MA+'PE<1K%5T: IJ'AX

M] W,V+E/@$6S\2",+YU65OPL"Y-1UKA$<"8B) $-,F]: 51; - P''5@O#`'+C) 7F

M] LUH8``DML&108\*LG\*7\/) T) 65^EWQ53L4. WT(Y6@LW\*PF\*3<6=-R\2&DMR0

M4YSWLM5%.1\U<2V: K. ! UH? \*6YOBUHMVR@@K\*$+. L; 7O1SY^SPZ+X; &V5<K<X

M7Q] 8G%WXY=^YY; X; UPCC3B7J#"%%%0SF? T] 8BHNVME1WS!,8DRJAO'ED]%!%

M. GN$N?? P`J8&\L"`! +R`QU,%; LS] ^\_\#4$L#!! 0````(```(?! ON151$N04`

M`\*4,```,````1$E32TA) 1$4N5%A4G59-; Q-7% -TC\1] NNZB"Y`RQ\T78A9`\*

MA") 5E`7; EE@T\*B4HB6CIJLJ\*! 55; J=M\*+\\_S\ // ,O. <] [0] H%\_T/\V''22?)

M\_(6>. YX/. V"0L) 1HQK [OW\*] SSWU7KU#QV=A]] F) OY\_$W! S2W<8VV'FS05GM [

MY^FCW>^HN;: VZ-#ZDR=TGPWVZ7Y [O [WWO+WM7+U2`] S>V? \_VSLYVFYK. @D. \_

MA+83BB`0Y/H9! 2+R=&BEITF; @0T#<: PU&? RH(T\_%8CB%=$A&>3: V83JDR$] &

M(AL2216=`<VHU\H7L? \*5H7YHH\#&(? 5M! &MKC`XT^? I8! +I`J [TUB+JBKR-A

MC. VQZ] HW(5I-Y [$-X"; \*1@K! \*J) DJ$] #971&48%VH@=(0ABM`G(! A/A&`JX1

M%<76/\_/RI [X-; $=<Q`U"? N\*UHD"=X) 62J\*]. C`V2`BVRPU`8. +@@BD7/I` []

M`2RR1\_] ED<E4'&7X004-&O'7D0CPWPA? CQ"=47UKLABYO) 4I49Y>E1\>9=I-

MI5`Q'A/\Y843<: BEN#A5'<O'8<: 5\*] ``'RKK6E\'%J7@FB-KBCS; YSZ\*^`Q'

MB$(1%37A+Q0LM<^5EN2&24</RTS'36SDCI$+&A&J6.,,OI"VFQ^CO@I5E/I>

M4D3N@`BQ\'1%@@\*M8T/1=3GH\\%`>; &6ACV3#! 2#3 [0IX\2B/CK3+4\*LF9B\

M@R&QHYRJ; HA-5Q0#/HKQVO"W5G>E=3EZV5<C$8. \*6E4] E2H\4>`8C32BZ:%\*

M42R,\*T+T"KV-<V] Q7D1FHD,O@] R<Q^2<#QPKOV0OJN0: T35BI,: >BY$J1ZU!

M^9B(#) P) `0J"! (ALH(] UF\*#; XTPJOM6YJEY>V2`\_U [4EQ: P99^U? '&$6ZMQE

MZC) Y^@EG5\*! Y-C1\*(E [R1"Q\VT'; BP+\*M. -G\*! #SB/WY9^],O<$\_SZJ; 4\M!

M+26UQH! Y1S;. &<U<1\"81690A! S@C] \\&\_3/+F(5BF&C=L,DT0$K"] V] M45?

M;! "M/ [C^\`'8%JH@\*PKHY8. D2=J(VV<E-SDK"II60\(=DND) QX$ZP6>DO,2X

MP((4\<3<S,/KBI) V2#RY\*/L"`#`S\*] 'TB$<Q%ZF4V? K) I";. ^OR: UP') E. S(

M2U>?: SKTJJ2\F"# [1'T/D: $\BQ55<0%NBBN8YYP3>. I; =VC= [%3WQN887Q? &

M! 1J"! T<TL)"V3#%YK&^\*! J+GT^V [7] Z [<\_? VIK/Y<-. AGP6=>ZQ\_I+LY"S7T

M [N9DZ/\_\^ [&? /VN0-V^O,VHN-9NM! =K: W7^T^SWMM1\ [] /G>BZ] ^W'FZ. [], M7^\_^0,V%&\_1F$J0X\LI&GH. A\1WJ. /1 [F'6UL3@CKF? Y&6C67&MYY1HMS; >6

MY] =6ID$F-R11Z\9\LSF\_MD@? \_$R`\_/W1-? EKLK2; 3P\_: > [2] M\_. \34\_:! \_PR

MMTZ [>W3KVE0+#GEL) =C-+(8ZQ7F+H0LDI7\*YSX1Q,2",#J3U: 1Y4P`Q5S! `-

MDI5>\(H. >%Y! (&YVI<:)"D16Z2 [KB($3': @0S^L0%"9+P992M6=P! G1? =EK+

MGS: \*Y! 97%N [A&87G+ // 7VKAUR; CIM+9F&B^^WWBU-6F\] 'YC? JV-EQV`U [:, M-! - X9=JVZ2PMS8YB] ? W&^? N [. ?%9; 77PXEF; YIJ. XZQ>XD;) @,CF'(EBF5R<

M0MV(CK&`DUPU0! >I00ZL? <U<JO8Q>FX [I? I7=. $ [1: &Q6$GB%. @R8E4$]] "O

M! BV-KPJKXSL; &,(+`\_>&+O2W%\*&Q! J=DL0Z@7U. W3X2#/<. T<: 9X<#BI\^H#

M. CE+SB6K8R&. E3; J\*5$LT"Y+XR5MA"M%\*%F^R5B750\_5Y>O,/. Z9(] ZFGO"J

MT>) K0NHFI [B5YC<E [. "790(9'24N! GARD8FI#? &3KSS<BMV0? K. >]: W$QM! #

MH? WJ? 6\*\WI+! \*1ULE$\*([\_F\*/K#FDA [BEE. @,89,49ZYA; 652R;% [9%X5\/ [

M\_U! +`0(4`! 0````(```(?! OBTQ\*(Z`4``#H&```,````````````(```````

M``! $25-+2$E$12Y%6$502P$"%``4````"```"'P; [D541+D%``"E#```#```

M`````````"`````2! @``1$E32TA) 1$4N5%A44$L%! @`````"``(`=````/4+

$``````

`

end

sum - r/size 16086/4433 section (from "begin" to "end")

sum - r/size 28110/3199 entire input file

### 2.8. Защита жестких дисков с помощью программы BestCrypt

Проблема защиты данных на жестких дисках ПК, является, пожалуй, самой актуальной в области защиты информации.

Программа BestCrypt, на наш взгляд является лучшей (из доступных бесплатно в Интернет) программой для создания шифрованных логических дисков. Есть версии для Dos, Win 3. XX, Windows 95/98, Windows NT. На таких дисках целесообразно хранить не только всю секретную информацию но и другие программы шифрования (в т. ч. PGP со всеми секретными ключами).

Программа на ваш выбор предлагает три алгоритма шифрования (DES, GOST, BlowFish) - рекомендуем выбирать проверенные алгоритмы – GOST или BlowFish.

Кроме создания шифрованных дисков (и всего сервиса связанного с ними) программа позволяет полностью на физическом уровне производить шифрование дискет, что очень удобно для передачи секретной информации.

Эту замечательную программу вы можете скачать на сервере разработчика, Финляндской фирмы Jetico:

http: // www. jetico. sci. fi Вот серийный номер, необходимый для регистрации бесплатной версии программы:

User name: Sonixx

Organization: [AnThraX]

Serial number: BC-35D1-EAA6-027F

### 2.9. Защита жестких дисков с помощью программы seNTry 2020

Программа seNTry 2020 (версия 2.04) на наш взгляд является одной из лучших программ для создания шифрованных логических дисков под Windows NT. На таких дисках целесообразно хранить не только всю секретную информацию но и другие программы шифрования (в т. ч. PGP со всеми секретными ключами).

Эту замечательную программу вы можете скачать на сервере разработчика:

http: // www. softwinter. com

А вот генератор ключей, необходимый для регистрации программы:

section 1 of file sentry. com < uuencode 1.0 by FRIENDS Software >

filetime 619930778

begin 644 sentry. com

MZ(``M`FZY0'-(; I\*`K0\*S2&T"; HY`LTA,\"Y`@"^3`\*\_=`: KJZRK04$\#77X

MOG0&9KK62G\*SZ"8`9H'R17 [! \*F:)%G0&Z(8`9H'R17 [! \*F:)%G0&Z'<`ND<"

MM`G-(</\9O? 2K&: +VF;! Z@AF@>/\_````,MAG9C,4G70"``#BY&; WTL/] OW`&

MNO\`N0@`9@^WPF; 1Z',&9C4@@ [CMXO-FJTIYY\_S#4,'H". @! `%A@4,#H!. @&

M`%CH`@! APR0/! #`\. G("! `=2BM"T`LTA6L. ^=`: Y`@"MAN#HR\_] 2LB"T`LTA

M6N+PPPT\*<V5.5') Y(#(P,C`@=C(N,#0@: V5Y9V5N97) A=&] R+B`H8RD@,3DY

M. "!!: R! +; W) T(%M33U,@9W) O=7! =#0H-"D5N=&5R('EO=7(@; F%M93H@) `T\*

14V5R: 6%L(&ES. B`D#0HD'@`

`

end

sum - r/size 34466/486 section (from "begin" to "end")

sum - r/size 2375/332 entire input file

### 2.10. Защита жестких дисков с помощью программы SafeHouse

Еще одна программа для создания шифрованных логических дисков.

Есть версии для Dos, Win 3. XX, Windows 95/98, Windows NT. На таких дисках целесообразно хранить не только всю секретную информацию но и другие программы шифрования (в т. ч. PGP со всеми секретными ключами).

Международная версия слабая (40/56 бит ключ), а американская вполне достойная. С их сайта http: // www. pcdynamics. com/SafeHouse/ в Интернете просят не переписывать ее не жителям США. Но только просят.

Загрузить можно без проблем. Пароль для инсталляции - us. checkpoint

### 2.11. Защита данных с помощь программы Kremlin

Программа Kremlin является как бы логическим дополнением программы BestCrypt. Она позволяет шифровать файлы и электронную почту по многим алгоритмам, на ваш выбор (IDEA, 3DES, CAST и др.). Но главным ее достоинством является возможность (в заданные промежутки времени, или, например, при каждом выключении компьютера)

НЕВОССТАНОВИМО стирать все файлы истории, лог-файлы, временные файлы Интернет а также все те файлы что вы укажете. Кроме того вы можете указать НЕВОССТАНОВИМОЕ обнуление информации на свободном месте жесткого диска и в файле виртуальной памяти (своп-файле) Windows.

Программа доступна для скачивания, на многих бесплатных сервера, в том числе на:

http: // www. shareware. com

http: // www. download. com

А вот серийный номер, необходимый для регистрации бесплатной версии программы (проверялся на версии 2.21): 4040053298

### 2.12. Защита ПК с помощью аппаратных средств

Назначение данного устройства - удаление информации при попытке изъятия накопителя, при похищении компьютера, при проникновении в зону обслуживания компьютера (сервера) или при нажатии определенной кнопки.

По сути дела данное устройство является аналогом бумаго-уничтожительной машинки.

Принцип действия данного устройства - форматирования накопителя.

Известно, что в начале каждого накопителя расположены таблицы разделов, таблицы размещения файлов, каталоги - поэтому уничтожение информации начинается именно с них и даже после нескольких секунд работы данного устройства на накопителе остается информация, которую очень тяжело восстановить. Если же устройство отработает несколько минут, то вся информация будет уничтожена. После первого цикла уничтожения начинается второй и так далее (до разряда автономного источника питания), поэтому информация нельзя восстановить даже по остаточной намагниченности. Подобный метод стирания есть в утилитах WipeFile и WipeDisk, однако для их запуска компьютер должен быть включен, да и многие операционные системы не представляют непосредственный доступ к диску и соответственно эти утилиты могут не сработать.

Подобный метод уничтожения информации может показаться "варварским", однако если правильно организовать работу (резервное копирование каждый день, ведение полного протокола работы за день и т.п.), то стертую информацию можно восстановит с минимальными потерями времени (диск не страдает).

Для идентификации администратора, имеющего доступ к охраняемым компьютерам компьютеру) применяются электронные ключи с длиной кода 48 бит. Небольшое время, отведенное для предъявление данного ключа – 10 секунд, полностью исключает возможность его подбора. Датчики, при срабатывании которых происходит уничтожение информации, пользователи выбирают сами. Наиболее часто используются концевые выключатели (вскрытие компьютера, открытие комнаты, тревожная кнопка), звонок телефона (пейджера), датчики срабатывающие при изменении объема.

Устройство представляет собой блок, монтируемый в отсек 3,5" дисковода и имеет автономное питание. Устройство включается в разрыв IDE шлейфа и не требует установки никаких драйверов. Данное устройство можно установить в любой компьютер, имеющий накопители типа IDE.

Обеспечивается монтаж и годовая гарантия.

Подробную информацию об уничтожителе можно получить по телефону в Питере: (812) - 259-5018 в АОЗТ "БАЙТ". Применяемый метод уничтожения информации не приводит к порче накопителя и не противоречит законодательству (как и любая бумаго-уничтожительная машинка).

E-mail: byte@infoservice. spb. ru

### 2.13. Криптография и политика

Крупнейшие специалисты в области защиты информации сегодня откровенно заявляют: правительство США, как и любое другое, включая Россию, принимая законы об обязательной защите информации в государственных и частных коммерческих фирмах, на самом деле пытается получить доступ к конфиденциальной информации о своих гражданах. Что происходит?

Большой брат с американским акцентом Любая западная фирма, желающая расширить свой бизнес за счет рынков третьих стран, рано или поздно сталкивается с ограничениями на экспорт некоторых технологий, имеющих двойное применение или просто слишком хороших для слаборазвитых стран.

Но если эта фирма согласится соблюдать определенные правила игры, подобный экспорт будет разрешен. Главное условие - засекречивание всей сопутствующей документации. Секретность достигается использованием специальных компьютерных программ, называемых криптографическими.

Специальные государственные службы следят за тем, чтобы фирмы не скупились на покупку такого программного обеспечения и постоянно использовали его в своей работе. В заявлениях для прессы и открытых инструкциях делается упор на самые новейшие достижения криптографии, алгоритмы и программы, сертифицированные правительственными службами.

Нас ежедневно уверяют, что именно эти программы гарантируют стопроцентную защиту от любого несанкционированного доступа. И напротив, говорится о том, что программы, созданные в частных или независимых от государства предприятиях, "взломает" даже ребенок.

Это преувеличение, на практике приводящее к большой лжи.

Стремление государственных секретных служб ввести свои правила шифрования частных и коммерческих данных означает лишь желание Большого брата выведать их. Для этого есть два подхода, и оба они активно применяются на практике.

"Стопроцентная защита"

Совсем затюканный западными странами Саддам Хуссейн потерпел поражение задолго до войны в заливе. Имеющиеся в его распоряжении самолеты "Мираж" были поставлены французами. Коварные лягушатники уверяли покупателя, что электроника этих самолетов имеет стопроцентную защиту от несанкционированного доступа. Однако, когда дело дошло до войны, эта защита была сломана немедленно - одним кодовым сигналом, пущенным в обход хитроумной системы. Бортовые системы самолетов были отключены, и диктатор остался без авиации.

Подобный "черный вход" в якобы защищенную систему имеется в ЛЮБОЙ СЕРТИФИЦИРОВАННОЙ ГОСУДАРСТВОМ ПРОГРАММЕ, но об этом не принято распространяться вслух.

Билль сената США S266 от 1991 года откровенно требует, чтобы американское криптографическое оборудование содержало ловушки, известные лишь АНБ - Агентству национальной безопасности. В 1992 году ФБР предложило конгрессу закон, - облегчающий подслушивание телефонных разговоров, но он был провален. Тогда в 1993 году Белый Дом начал кампанию за утверждение в качестве государственного стандарта криптографической микросхемы CLIPPER для употребления при засекречивании в телефонах, факсах и электронной почте. Однако разработчики, компания AT&Т, не скрывают, что у правительства есть ключик от "черного входа" в систему вне зависимости от того, какой сложности пароль назначит наивный пользователь.

"Общественные гарантии".

Второй подход в обжуливании потенциальных клиентов основан на системе так называемых открытых ключей, только полная совокупность которых может позволить владельцу расшифровать любое сообщение в системе.

Пользователь читает только свои сообщения, но если дело доходит до серьезных и законных причин (например, решение суда или интересы национальной безопасности), стоит собрать, скажем, десять уважаемых граждан, которым розданы части главного ключа, как тайное станет явным.

Подобный подход был справедливо раскритикован большинством специалистов. По мнению Аллена Шиффмана, главного инженера фирмы Terisa Systems, Калифорния, технология "ключ у третьей стороны" не только не будет использоваться за рубежом, но и вообще представляет собой еще один ход правительства США для удержания технологии шифрования в стороне от прогресса. "А разве применил бы Форд систему защиты, разработанную в фирме Toyota, если бы ключи от системы были у японского правительства? " - вопрошает Джим Бидзос, президент авторитетной корпорации RSA Data Security.

Среди корпоративных пользователей, ищущих гарантий того, что важные данные не будут перехвачены, даже сама возможность поверить правительству полностью исключается. И это в Америке, где спецслужбы регулярно получают увесистые оплеухи за малейшие попытки проникнуть в частные дела гражданина. Кто же в России поверит правительству, которое ни разу не было откровенно со своими гражданами?!

Зачем ФАПСИ такие большие уши Федеральное агентство правительственной связи и информации России - структура, аналогичная американской АНБ. Но поскольку работает она в России, для удовлетворения своего профессионального любопытства использует методы попроще. Например, дискредитацию систем защиты, разработчики которых сознательно исключают возможность "черных входов", а также все программы, в разработке которых ФАПСИ не участвовало.

Дело в том, что сейчас во многих городах страны ФАПСИ созданы некие научно-технические центры, занимающиеся внедрением собственных защитных систем. Эти разработки немедленно получают необходимые для продвижения на рынок сертификаты качества, выдаваемые, разумеется, ФАПСИ. И независимые конкуренты бьются жестко - ФАПСИ отказывается лицензировать чужую продукцию, сколь хороша бы она ни была. К тому же последнее - надежность, как вы уже поняли, - традиционно лишнее качество для Большого брата любой национальной принадлежности.

Со времени своего создания и поныне ФАПСИ развернуло грандиозную пропагандистскую кампанию против подобных фирм. Вот пример информации, опубликованной во многих СМИ.

"О шифросредствах, не гарантирующих защиты. По имеющимся в отделе лицензирования и сертификации ФАПСИ сведениям, ряд российских фирм - разработчиков и производителей средств защиты информации получили сертификаты на разработанные ими шифросредства в обход существующей системы...

ФАПСИ предупреждает потенциальных пользователей, что данные сертификаты не могут удостоверять соответствие указанных продуктов действующим России требованиям к шифровальным средствам и гарантировать обеспечение безопасности обработанной с их помощью информации".

В числе упомянутых программ - система "Кобра", программа, о которой даже зарубежные специалисты говорят как о самой совершенной и научно обоснованной криптосистеме. Ежегодно проводятся семинары и научные конференции, где сотни уважаемых математика всех стран обсуждают перспективы "Кобры" и оригинальный алгоритм, разработанный российскими программистами.

Чуть раньше в "Московском комсомольце" появилась статья, авторы которой заявляли буквально следующее "Шифры, созданные коммерческими структурами ФАПСИ расколет за обеденный перерыв".

### 2.14. Выводы

Теперь давайте сделаем выводы из всего прочитанного:

1. При планировании мероприятий по защите информации целесообразно применять комплексный подход:

- рядом с вашим компьютером в обязательном порядке должно быть установлено устройство для защиты от ПЭМИН (например ГБШ-1, Салют, Пелена или Гром);

- вся важная информация (в т. ч. и программы для шифровки электронной почты типа PGP) должна храниться на зашифрованном диске (разделе жесткого диска) созданного например с помощью программы BestCrypt или, что еще лучше - "Кобры";

- установите программу Kremlin 2.21 и настройте ее таким образом, чтобы при каждом выходе из Windows она обнуляла: свободное место на всех дисках, содержимое виртуальной памяти (своп-файл), все файлы истории, лог файлы и т.д.;

- вся ваша корреспонденция (E-Mail) должна шифроваться с помощью программы PGP (рекомендуем версии 2.6.3ia - для DOS и 6.0i для Windows). Шифруйте абсолютно всю корреспонденцию, нельзя давать повода расслабляться Большому брату;

- периодически (раз в месяц или раз в квартал) производите полную смену всех паролей;

- при передачи секретной информации через съемные носители информации (например через дискеты) целесообразно маскировать ее например с помощью программы DiskHide;

- для надежного шифрования файлов используйте программы: NDEC, "Кобра", Kremlin, PGP.

2. При выборе пароля руководствуйтесь следующими рекомендациями:

- не используйте очевидные фразы, которые легко угадать, например, имена своих детей или супруги;

- используйте в пароле пробелы и комбинации цифр, символов и букв. Если ваш пароль будет состоять из одного слова, его очень просто отгадать, заставив компьютер перебрать все слова в словаре. Именно поэтому фраза в качестве пароля гораздо лучше, чем слово. Более изощренный злоумышленник может заставить свой компьютер перебрать словарь известных цитат;

- используйте творческий подход. Придумайте фразу, которую легко запомнить, но трудно угадать: такая фраза может быть составлена из бессмысленных выражений или очень редких литературных цитат;

- используйте максимально длинные пароли - чем длиннее пароль, тем труднее его угадать.

3. Никогда не защищайте секретную информацию с помощью архиваторов и защиты предлагаемой MS Office.

4. Никогда не пользуйтесь криптосистемами сертифицированными ФАПСИ, АНБ и пр., ВСЕ они имеют так называемые "черные ходы" и легко взламываются как этими службами так и хакерами.

5. Для большей надежности иногда имеет смысл использовать не одну, а несколько системам шифрования (например шифровать E-Mail

сначала с помощью NDEC а затем с помощью PGP).

6. Всегда осуществляйте физический контроль за носителями информации. Лучше всего если они всегда будут при вас (например коробка дискет в дипломате).

7. Помните что в новых версиях даже надежных криптосистем (типа PGP) могут появиться "черные ходы" под давлением правительства и спецслужб, так что имеет смысл пользоваться известными и проверенными версиями.

8. Используйте сами и активно пропагандируйте среди своих друзей и знакомых применение самых лучших средств криптографии. Пусть шифрование станет одной из неотъемлемых частей вашей жизни. Подобным образом жизни вы внесете свою лепту в справедливое дело борьбы со всевозможными спецслужбами (АНБ, ФСБ, ФАПСИ и пр) защищающими интересы преступного олигархического режима, а не ваши интересы!

## 3. Создание архивов

При эксплуатации персональных компьютеров по самым различным причинам возможны порча или потеря информации на магнитных дисках. Это может произойти из-за физической порчи магнитного диска, неправильной корректировки или случайного уничтожения файлов, разрушения информации компьютерным вирусом и т.д. Для того чтобы уменьшить потери в таких ситуациях, следует иметь архивные копии используемых файлов и систематически обновлять копии изменяемых файлов. Для хранения архивов данных можно использовать внешние запоминающие устройства большой емкости, которые дают возможность легко скопировать жесткий диск (например, магнитооптика, стримеры, "Арвид" и др.)

Для копирования файлов можно, разумеется, использовать следующие средства:

- стандартные команды Сору, Xcopy, Diskcopy;

- программные средства PCtools, Norton Commander, Windows;

- программы непрерывного копирования Backup и Restore.

Однако при этом архивные копии занимают столько же места, сколько занимают исходные файлы, и для копирования нужных файлов может потребоваться много дискет.

Более удобно для создания архивных копий использовать специально разработанные программы архивации файлов, которые сжимают информацию.

При архивировании степень сжатия файлов сильно зависит от их формата.

Некоторые форматы данных (графические, Page Maker и др.) имеют упакованные разновидности, при этом сжатие производится создающей исходный файл программой, однако лучшие архиваторы способны поджать и их. Совсем другая картина наблюдается при архивации текстовых файлов, файлов PostScript и им подобных (текстовые файлы обычно сжимаются на 50-70%, а программы на 20-30%).

Наиболее популярны архиваторы ARJ, LHA, RAR и PKZIP (имеет отдельный распаковщик PKUNZIP).

Большинство из этих программ не надо специально покупать, так как они предлагаются как программы условно-бесплатные (Shareware) или свободного распространения (Freeware). Хорошую помощь при архивации программ (поскольку каждый пользователь имеет любимый архиватор) могут оказать вам специальные "оболочки" (так называемые PackerShells), такие как SHEZ или GUS, которые самостоятельно определяют компрессированный файл и помогают его распаковать (так называемый процесс разархивации); аналогичные средства имеются в современных оболочках общего назначения (Norton Commander, DOS Navigator и др.).

Подобные оболочки обычно лишь управляют имеющимися программами-архиваторами общего пользования. Архиватор RAR имеет собственную встроенную оболочку.

Принцип работы архиваторов основан на поиске в файле "избыточной" информации и последующем ее кодировании с целью получения минимального объема. Самым известным методом архивации файлов является сжатие последовательностей одинаковых символов. Например, внутри вашего файла находятся последовательности байтов, которые часто повторяются. Вместо того чтобы хранить каждый байт, фиксируется количество повторяющихся символов и их позиция. Для наглядности приведем следующий пример.

Упаковываемый файл занимает 15 байт и состоит из следующей последовательности символов:

BBBBBLLLLLAAAAA

В шестнадцатеричной системе 42 42 42 42 42 4С 4С 4С 4С 4С 41 41 41 41 41

Архиватор может представить этот файл в виде (шестнадцатеричном):

01 05 42 06 05 4С OA 05 41

Эти последовательности можно интерпретировать следующим образом: с первой позиции 5 раз повторяется знак В, с шестой позиции 5 раз повторяется знак L и с позиции 11 повторяется 5 раз знак А.

Согласитесь, очень простая демонстрация алгоритма архивации.

Очевидно, что для хранения файла в его последней форме требуется лишь 9 байт - меньше на 6 байт.

Описанный метод является простым и очень эффективным способом сжатия файлов. Однако он не обеспечивает большой экономии объема, если обрабатываемый текст содержит небольшое количество последовательностей повторяющихся символов. Более изощренный метод сжатия данных, используемый в том или ином виде практически любым архиватором, - это так называемый оптимальный префиксный код, и в частности, алгоритм Хаффмана, или кодирование символами переменной длины. Код переменной длины позволяет записывать наиболее часто встречающиеся символы и фразы всего лишь несколькими битами, в то время как редкие символы и фразы будут записаны более длинными битовыми строками. Например, анализируя любой английский текст, можно установить, что буква Е встречается гораздо чаще, чем Z, а Х и Q относятся к наименее встречающимся. Таким образом, используя специальную таблицу соответствия, можно закодировать каждую букву Е меньшим числом бит, используя более длинный код для более редких букв, тогда как в обычных кодировках любому символу соответствует битовая последовательность фиксированной длины (как правило, кратной байту).

Популярные архиваторы ARJ, РАК, LHARC, PKZIP работают на основе алгоритма Лемпела-Зива. Эти архиваторы классифицируются как адаптивные словарные кодировщики, в которых текстовые строки заменяются указателями на идентичные им строки, встречающиеся ранее в тексте.

Например, все слова этой книги могут быть представлены в виде номеров страниц и номеров строк некоторого словаря. Важнейшей отличительной чертой этого алгоритма является использование грамматического разбора предшествующего текста с разложением его на фразы, которые записываются в словарь. Указатели позволяют делать ссылки на любую фразу в окне установленного размера, предшествующем текущей фразе.

Этот размер определяет границы поиска соответствия; при его увеличении возрастает плотность упаковки, но снижается скорость работы программы.

Если соответствие найдено, текущая фраза заменяется указателем на ее предыдущее вхождение.

Программы-архиваторы позволяют не только сэкономить место на архивных дискетах, но и объединять группы совместно используемых файлов в один архивный файл, что заметно облегчает ведение архивов. К основным функциям архиваторов относятся:

- архивация указанных файлов или всего текущего каталога;

- извлечение отдельных или всех файлов из архива в текущий каталог (или в указанный каталог);

- просмотр содержимого архивного файла (состав, свойства упакованных файлов, их каталожная структура и т.д.);

- проверка целостности архивов;

- восстановление поврежденных архивов;

- ведение многотомных архивов;

- вывод файлов из архива на экран или на печать.

Все программы-архиваторы, как правило, снабжены подробными комментариями, поэтому их применение не вызывает особых затруднений.

Кроме того, в программах-архиваторах могут быть предусмотрены дополнительные функции по защите информации в архивном файле с помощью пароля, который используется как ключ алгоритма шифрования данных в архиве.

## 4. Защита от компьютерных вирусов

Компьютерный вирус - это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять различные нежелательные действия на компьютере. Программа, внутри которой находится вирус, называется "зараженной". Когда такая программа начинает работу, то сначала, как правило, управление получает вирус.

Вирус находит и "заражает" другие программы или выполняет какие-нибудь вредные функции: портит файлы или таблицу размещения файлов на диске, "засоряет" оперативную память, изменяет адресацию обращений к внешним устройствам и т.д. Более того, зараженные программы могут быть перенесены на другой компьютер с помощью дискет или локальной сети.

В настоящее время известно более двадцати тысяч вирусов. Условно они подразделяются на классы по следующим признакам.

По среде обитания:

- сетевые, распространяющиеся по компьютерной сети;

- файловые, внедряющиеся в выполняемый файл;

- загрузочные, внедряющиеся в загрузочный сектор жесткого диска или дискеты.

По способу заражения:

- резидентные, загружаемые в память ПК;

- нерезидентные, не заражающие память ПК и остающиеся активными ограниченное время.

По возможностям:

- безвредные, не влияющие на работу ПК;

- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими звуковыми и прочими эффектами;

- опасные, которые могут привести к серьезным сбоям в работе ПК;

- очень опасные, которые могут привести к потере программ, уничтожению данных, стереть информацию в системных областях памяти и даже преждевременному выходу из строя периферийных устройств.

Данная классификация объединяет, естественно, далеко не, все возможные вирусы; в каждой категории встречаются варианты, не названные в силу их экзотичности, например, CMOS-вирусы или вирусоподобные структуры, "обитающие" в среде Microsoft Word. Кроме того, встречается ряд программ, не обладающих всеми свойствами вирусов, но могущих представлять серьезную опасность ("троянские кони" и т.п.)

Для защиты и борьбы с вирусами применяются специальные антивирусные программы, которые можно разделить на несколько видов:

- программы-детекторы позволяют обнаружить файлы, зараженные вирусом. Работа детектора основывается на поиске участка кода, принадлежащего тому или иному известному вирусу. К сожалению, детекторы не гарантируют обнаружения "свежих" вирусов, хотя в некоторых из них для этого предусмотрены особые средства. Наиболее известными детекторами являются ViruScan, NetScan. У нас в стране используется детектор Aidstest;

- программы-доктора (или фаги)"лечат" зараженные программы или диски, уничтожая тело вируса. При этом в ряде случаев ваша информация может быть утеряна, так как некоторые вирусы настолько искажают среду обитания, что ее исходное состояние не может быть восстановлено.

Широко известными программами-докторами являются Clean-Up, M-Disk и уже упомянутый выше Aidstest;

- программы-ревизоры сначала запоминают сведения о состоянии программ и системных областей дисков, а в дальнейшем сравнивают их состояние с исходным. При выявлении несоответствий выдают сообщение пользователю. Работа этих программ основана на проверке целостности (неизменности) файлов путем подсчета контрольной суммы и ее сравнения с эталонной, вычисленной при первом запуске ревизора; возможно также использование контрольных сумм, включаемых в состав программных файлов изготовителями. Могут быть созданы, и встречаются, вирусы, не изменяющие при заражении контрольную сумму, сосчитанную традиционным образом - суммированием всех байтов файла, однако практически невозможно замаскировать модификацию файла, если подсчет ведется по произвольной, заранее неизвестной схеме (например, четные байты дополнительно умножаются на 2), и совсем невероятно при использовании двух (или более. .) по-разному сосчитанных сумм;

- доктора-ревизоры - это программы, объединяющие свойства ревизоров и фагов, которые способны обнаружить изменения в файлах и системных областях дисков и при необходимости, в случае патологических изменений, могут автоматически вернуть файл в исходное состояние;

- программы-фильтры располагаются резидентно в оперативной памяти компьютера, перехватывают те обращения к операционной системе, которые могут использоваться вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Программы-фильтры контролируют действия, характерные для поведения вируса, такие как:

- обновление программных файлов;

- запись на жесткий диск по физическому адресу (прямая запись);

- форматирование диска;

- резидентное размещение программ в оперативной памяти.

Выявив попытку совершения одного из этих действий, программа-фильтр выдает описание ситуации и требует от пользователя подтверждение. Пользователь может разрешить операцию, если ее производит "полезная" программа, или отменить, если источник данного действия неясен. К широко распространенным программам-фильтрам относятся FluShot Plus, Anti4Us, Floserum, Disk Monitor. Это достаточно надежный метод защиты, но создающий существенные неудобства для пользователя.

Некоторые антивирусные функции встроены в современные версии BIOS.

Выпускаемые антивирусные программные продукты, а их очень много, как правило, объединяют основные функции детектора-доктора-ревизора.

Следует отметить, что антивирусные программы постоянно обновляются, не реже одного раза в месяц, и способны защитить компьютеры от вирусов, известных программе на данный момент.

Прежде всего, необходимо подчеркнуть, что защитить компьютер от вирусов может только сам пользователь. Только правильное и своевременное применение антивирусных средств может гарантировать его от заражения или обеспечить минимальный ущерб, если заражение все-таки произошло. Необходимо правильно организовывать работу на ПК и избегать бесконтрольной переписи программ с других компьютеров, в первую очередь это касается развлекательных программ и компьютерных игр.

### 4.1. Действия при заражении вирусом

При заражении компьютера вирусом (или подозрении на это заражение) необходимо выполнить следующие операции.

1. Выключить компьютер, чтобы вирус не продолжал выполнение своих разрушительных функций.

2. Произвести загрузку компьютера с "эталонной" (системной)

дискеты (на которой записаны исполняемые файлы операционной системы и программы-детекторы) и запустить антивирусные программы для обнаружения и уничтожения вируса. Использование "эталонной" дискеты является необходимым, т. к. при загрузке операционной системы с жесткого диска некоторые вирусы могут переместиться в оперативную память из загрузочного модуля. При этом системная дискета должна быть защищена от записи, с помощью переключателя, расположенного на ее корпусе (для дискет 3,5") или наклейки (для дискет 5,25").

3. Далее следует последовательно обезвредить все логические диски винчестера. Если некоторые файлы на логическом диске невозможно восстановить и они не уничтожаются, то необходимо неповрежденные файлы скопировать на другой логический диск, а этот диск заново отформатировать. Затем восстановить все файлы на этом логическом диске путем обратного копирования и с использованием архивных копий.

### 4.2. Профилактика против заражения вирусом

Профилактика в основном состоит следующем.

Проверка информации, поступающей извне (дискеты, локальной сети, Интернет и т.д.), с помощью программ-детекторов или программ-ревизоров. Для этого желательно использовать программы, которые проверяют не длину файла, а вычисляют его контрольную сумму, так как многие вирусы не изменяют длину зараженных файлов, а изменить файл так, чтобы его контрольная сумма осталась прежней, практически не возможно.

Если принесенные программы записаны на дискете в архивированном виде, то следует извлечь файлы из архива и проверить их сразу, только после этого файлы можно пускать в работу.

Очень простой и надежной проверкой на наличие резидентных вирусов является отслеживание изменений в карте памяти компьютера, например, за прошедший день. Для этих целей можно использовать специальные программы, которые заносятся в командный файл autoexec. bat, выполняемый при начальной загрузке MS DOS. Весьма удачным выбором здесь может быть программа ADinf, которая умеет читать информацию с дисков без использования услуг DOS, так что ни один "невидимый" вирус не может ее обмануть. Это существенно сокращает время проверки, поскольку требуется проверить только вновь появившиеся или измененные файлы.

Из существующих на сегодняшний день антивирусов мы рекомендуем:

из зарубежных - Norton Antivirus (http: // www. symantec. com); из отечественных - Adinf, Adext, Doctor Web. Если вы захотите приобрести их, вот координаты:

антивирусный отдел АО "ДиалогНаука", Москва тел. (095) 135-6253, 137-0150, тел. /факс 938-2970

BBS (095) 938-2856 (28800/V.34)

FidoNet: 2: 5020/69

E-mail: antivir@dials. ru

WWW-сервер: http: // www. dials. ru, http: // www. dials. ccas. ru

## 5. Сохранение информации на магнитном носителе

Информация на жестком диске может разрушиться не только вследствие действия компьютерного вируса или злого умысла вашего недоброжелателя, но и в результате физических и логических дефектов.

Кроме того, неприятности могут возникнуть и по вашей собственной неосторожности - в случае ошибочного форматирования дисков или удаления файлов.

Для сохранения данных на диске необходимо:

- регулярное проведение профилактических работ;

- своевременное реагирование на первые признаки повреждения;

- соблюдение правил обращения с диском;

- систематическое резервное копирование.

### 5.1. Проведение профилактических работ

Регулярно проверяйте свой диск на наличие плохих (bad) секторов.

Для их обнаружения можно воспользоваться утилитой Disk Doctor из комплекта Norton Utilities.

Отметим, что входящая туда же утилита Calibrate может иногда сделать дефектный кластер на диске снова нормальным.

Если на вашем жестком диске достаточно места, то целесообразно из файла autoexec. bat (DOS) запускать утилиту Erase Protection, которая размешает удаленные файлы в специально выделенной области на диске, откуда они могут быть при необходимости извлечены. В других операционных системах имеются аналогичные средства.

Следует помнить, что единственным стопроцентно надежным способом уберечь вашу информацию от любых разрушительных случайностей является четкая, неукоснительно соблюдаемая система резервного копирования.

Многолетний опыт как частных лиц, так и крупных предприятии во всем мире показывает, что при грамотном подходе (несколько "поколений" копий для каждого из ряда временных интервалов - месяц, неделя, день, полдня) вы не потеряете более одного рабочего дня на восстановление утраченной информации; в случае же, если последние копии архива содержат уже поврежденные файлы, вы имеете возможность вернуться к более ранним. С появлением доступных носителей CDROM ведение архивов облегчилось, поскольку необходимо хранить только целевые файлы и небольшое количество программ, основная же масса программного обеспечения легко восстанавливается с лазерных дисков или фирменных дистрибутивов (стоит, правда, напомнить, что известны случаи обнаружения вирусов и в тех и в других). Существует доступная возможность переписать информацию длительного хранения на лазерный диск, тем самым предохранив ее практически от всех неприятностей.

### 5.2. Действия при первых признаках повреждения диска

Наиболее типичными симптомами, предшествующими возникновению серьезных дефектов на диске - следующие:

- отсутствие доступа к отдельному файлу или появление в текстовых файлах посторонних символов;

- замедление работы дисковода;

- появление при записи и чтении информации звука, напоминающего фырканье насоса;

- неустойчивость процесса загрузки DOS.

При появлении какого-либо из перечисленных симптомов в первую очередь перепишите на дискеты наиболее важную информацию (которая еще доступна). Затем попытайтесь восстановить разметку утилитой Calibrate

- для жесткого диска и Disk Tools - для дискет. Обе эти утилиты входят в состав Norton Utilities. Независимо от результатов переразметки завершите процесс восстановления обработкой диска утилитой Norton Disk Doctor.

Во многих случаях описанных действий достаточно для восстановления работоспособности диска. Однако иногда исправление дефектов в автоматическом режиме невозможно. В этом случае применяются специальные методы, описание которых выходит за рамки данной книги.

Для изучения этого вопроса вам следует обратиться к специальной литературе.

### 5.3. Эксплуатация и обслуживание дисков

Приводы жестких дисков обычно в обслуживании не нуждаются. Диски располагаются в герметически закрытом корпусе. У вас никогда не должно появляться мыслей об очистке винчестера от пыли - даже если внутри его находятся частицы пыли, все-равно срок его службы достаточно велик.

Разборка винчестера с высокой вероятностью (99,99%) приводит к его выходу из строя!

Для обеспечения безаварийной работы жесткого диска старайтесь воздерживаться от курения возле ПК. Особенно страдают дискеты. Частицы дыма и смол, оседающие на их поверхности, образуют слой, сравнимый с толщиной магнитного покрытия, и данные перестают читаться.

В отличие от жесткого диска, дисководы требуют регулярной очистки, поскольку в отверстие, предназначенное для установки дискет проникает пыль, табачный дым и др. Первичную очистку можно выполнять при помощи специальных пылесосов через мелкие щели. Не пользуйтесь мощными агрегатами, так как добычей пылесоса могут оказаться головка записи/чтения или другие небольшие механические части, находящиеся внутри дисковода. Если же вы возьметесь за дело таким рьяным способом, то это профилактическое мероприятие приведет только к необходимости приобретения нового дисковода!

К значительным проблемам приводят осаждения пыли на головке записи/чтения. В результате на экране появляются сообщения типа "Can't read disc in drive А: " и другие.

Однако прежде чем вы решите, что виноват дефектный или грязный привод, проверьте используемые дискеты. Дискеты, которые без проблем читаются на других дисководах, должны читаться и на вашем. Таким образом, можно сразу же определить, действительно ли виноват дисковод.

Очистку рабочих головок необходимо поручать специалистам, а если еще не истек гарантийный срок дисководов, то изготовителям или поставщикам.

Если вы непременно хотите очистить рабочие головки самостоятельно, лучше воспользоваться специальными чистящими дискетами.

В заключение еще несколько советов по обращению с дискетами.

- Наряду с рекомендациями, которые находятся на конверте каждой дискеты, нужно хранить дискеты в закрытом ящике, что обеспечивает следующие преимущества: вы найдете необходимые данные быстрее, если не будете разыскивать дискеты по разным углам; вы защищаете дискеты от механического и магнитного влияния извне, вы обеспечиваете определенную степень защиты и безопасности дискетам и хранимым на них данным.

- Извлекайте дискеты из дисковода только тогда, когда индикатор LED погашен.

- Храните 5,25" дискеты в их защитном конверте.

- Подписывайте дискеты только с легким нажатием. Не давите на защитный футляр и не сгибайте дискету.

- Никогда не касайтесь пальцами незащищенной области дискеты.

- Не держите дискеты в месте с очень низкими или высокими температурами.

- Никогда не располагайте дискеты вблизи от источников электромагнитных полей (акустических систем, телевизора и др.). Вы должны помнить, что данные, потерянные по причине воздействия электромагнитного поля, как правило, восстановлению не подлежат, хотя в принципе это возможно. При транспортировке дискет заворачивайте их в фольгу; в противном случае три-четыре поездки на троллейбусе или трамвае могут оказаться фатальными для ваших данных.

- При перемещении важных данных не поленитесь записать их на дискету дважды, в разные каталоги, чтобы не пришлось совершать утомительные путешествия из-за сбоя в одном из ста файлов.

- Записав данные на дискету, убедитесь в их читабельности командой типа "А: \ COPY \*. \* NUL".

## 6. Специальные средства защиты пк

Прохождение электрических сигналов по цепям ПК и соединительным кабелям сопровождается возникновением побочных электромагнитных излучений в окружающей среде. Распространение побочных электромагнитных излучений за пределы контролируемой территории создает предпосылки для утечки информации, так как возможен ее перехват с помощью специальных технических средств контроля. В персональном компьютере основными источниками электромагнитных излучений являются устройства ввода и вывода информации совместно с их адаптерами (монитор, принтер, клавиатура, печатающее устройство и т.д.), а также центральный процессор. Утечке информации в ПК способствует применение коротких видеоимпульсов прямоугольной формы и высокочастотных коммутирующих сигналов. Исследования показывают, что излучение видеосигнала монитора является достаточно мощным, широкополосным и охватывает диапазон метровых и дециметровых волн.

Для уменьшения уровня побочных электромагнитных излучений применяют специальные средства защиты информации: экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений и наводок при помощи различных резистивных и поглощающих согласованных нагрузок.

Специальная проверка ПК заключается в проверке выполнения установленных требований по защите информации, а также в выявлении и анализе источников - каналов утечки информации и разработке предложений по их закрытию. Специальную проверку, как правило, проводят организации (учреждения), являющиеся головными по защите информации в министерствах (ведомствах), разрабатывающих и изготавливающих аппаратуру контроля информации. Техническому контролю в ПК должны подвергаться следующие потенциальные и реальные каналы утечки информации:

- побочные электромагнитные излучения в диапазоне частот от 10 Гц до 1000 МГц;

- наводки сигналов в цепях электропитания, заземления, в линиях связи;

- опасные сигналы, образующиеся за счет электроакустических преобразований, которые могут происходить в специальной аппаратуре контроля информации. Эти сигналы должны контролироваться в диапазоне частот от 300 Гц до 3,4 кГц;

- каналы утечки информации, образующиеся в результате воздействия высокочастотных электромагнитных полей на различные провода, находящиеся в помещении, которые могут выступать в качестве приемной антенны. В этом случае проверка проводится в диапазоне частот от 20 кГц до 1000 МГц.

При контроле защиты информации ПК используются специально разработанные тестовые программы, а также специальная аппаратура контроля уровня излучения, которые определяют режим работы ПК, обеспечивающий совместно с другими техническими средствами скрытый режим работы для различных средств разведки.

Наиболее серьезной техникой оснащены те лица, которые стремятся получить несанкционированный доступ к банкам данных компьютеров. Для этого необходима специальная аппаратура с цифровой обработкой. Самое надежное внедрение можно осуществить путем непосредственного подключения к компьютерной сети. Это возможно лишь в том случае, если в здании компьютеры объединены в общую локальную сеть.

Снимать информацию с последующей обработкой можно, регистрируя излучения компьютера и его периферии, а также компьютерных линий. Во время работы компьютера в питающей сети наводятся сигналы, регистрируя которые после соответствующей обработки можно получить полную или частичную информацию о процессах, происходящих в памяти компьютера и его периферии. Для дистанционного снятия информации за счет побочного излучения компьютера и его периферии применяют высокочувствительные широкополосные приемники с последующей цифровой обработкой полученной информации. Проведите небольшой эксперимент: включите ваш компьютер и проведите перестройку радиоприемника в УКВ диапазоне. Практически весь диапазон будет забит помехами от работающего компьютера и, если ваш IBM-совместимый или любой другой компьютер без соответствующей защиты, никто не сможет дать гарантию, что его не контролируют. Системы съема компьютерной информации невероятно сложны и требуют специальной аппаратуры аналоговой и цифровой обработки с применением компьютеров и определенного программного обеспечения.

Для защиты можно использовать специальные генераторы "белого шума" для защиты от ПЭМИН, например: ГБШ-1, Салют, Пелена, Гром и др.

Их можно приобрести во многих Московских фирмах торгующих спецтехникой (см. ПРИЛОЖЕНИЕ).

## 7. Защита пк от сбоев

Порой различные программно-аппаратные сбои компьютера приносят больше вреда чем компьютерные вирусы. Вот самые общие рекомендации по их предотвращению.

### 7.1. Защита от аппаратных сбоев 1

Если позволяют финансы, то всегда приобретите и используйте блоки бесперебойного питания (UPS), лучше фирмы APC (модель Back или Smart). Если финансы не позволяют, то поставьте хотя бы простой Pilot;

- никогда не приобретайте (а если он у вас есть - то откажитесь от использования) т. н. Кэш-контроллеры (в особенности фирмы Tekram);

- никогда не приобретайте (а если он у вас есть - то откажитесь от использования) т. н. BackPack (жесткий диск - работающий через параллельный порт) - чрезвычайно ненадежное устройство;

- заземлите свой компьютер. Хорошим заземлением может например послужить металлическая арматура дома (но не батареи);

- никогда не доверяйте ремонт (сборку, разборку, подключение дополнительных устройств, апгрейд) - неквалифицированным лицам;

- покупку компьютера и комплектующих производите только в надежных и проверенных фирмах. Подробнее об этом можно например узнать в конференции Фидо - PVT. EXCH. BLACK. LOG. Приведу лишь несколько примеров фирм, где НЕ следует покупать компьютеры: Вист, Формоза, Р&К, Партия, Лэнд (Ток Интрнейшнл), Al Tech. Неплохие фирмы: НТ, Московский Негоциант, Клондайк, Компьюлинк.

### 7.2. Защита от программных сбоев 2

Пользуйтесь надежными операционными системами. На наш взгляд наилучшим выбором является - Microsoft Windows NT 4.0 (5.0).

Операционная система Windows 95 очень нестабильна и содержит множество ошибок;

- никогда не используйте программу кеширования дисков smartdrv. exe - всегда удаляйте ее из файлов config. sys и autoexec. bat, а также другие программы программного (к аппаратным кэш-контроллерам это так же относится) кэширования дисков (Norton Speed Drive, Rocket и др.). Как правило большинство сбоев жестких дисков происходит именно из-за них;

- никогда не пользуйтесь Norton Utilites для Windows 95 (если вы все же используйте эту операционную систему);

- не используйте функцию Direct Access в программе Dos Navigator, иногда она работает очень некорректно;

- и наконец самое главное - выполняйте периодическое резервное копирование (архивирование) всех важных данных. Причем желательно иметь не менее двух копий (разных дат) с вашими важными данными - помните скупой платит дважды а то и трижды! НЕ ЗАБЫВАЙТЕ О ШИФРОВАНИИ ВАЖНЫХ ДАННЫХ!

## 8. Что помнит ваш компьютер?!

Рассмотрим еще один аспект нашей безопасности. Это нехорошие функции многих программ: вести лог-файлы, протоколы, запоминать все, что делалось вами и т.д.

Защита от программ Microsoft.

Программы фирмы Microsoft обладают на редкость исключительным количеством всевозможных "черных ходов", "люков", "багов" и т.д. Вот лишь некоторые примеры:

- Microsoft Outlook Express 4.0 - все письма которые вы когда либо отправляли, получали или удаляли он все равно хранит в своей базе. Поэтому периодически рекомендуем удалять (лучше невосстановимыми методами, например с помощью программы Kremlin 2.1) эти файлы. Они расположены в директориях:

\Windows\Aplication\Microsoft\Outlook Express\Mail\ - почта - здесь необходимо удалить все файлы с расширениями IDX и MBX.

\Windows\Aplication\Microsoft\Outlook Express\News\ - новости - здесь необходимо удалить все файлы с расширениями NCH.

- Microsoft Internet Explorer 4.0 - в директориях:

\Windows\Cookies\ - хранит файлы Cookies (их лучше периодически удалять с помощью программы Kremlin 2.1).

\Windows\Temporary Internet Files\ - хранит там места где вы были в Интернет (их лучше периодически удалять с помощью программы Kremlin 2.1).

- Microsoft Windows 95 - в директориях:

\Windows\History\ - хранит все файлы истории (их лучше периодически удалять с помощью программы Kremlin 2.1).

\Windows\name. pwl - в этих файлах Windows хранит имена, телефоны и пароли для соединения с Интернет, все они легко (с помощью специальных программ) расшифровываются...

\Windows\Profiles\name\ - где name имя пользователя, хранит профили и все установки конкретных пользователей (это кстати справедливо и для Windows NT)

\Aplication\Microsoft\Outlook Express\Mail\ - почта \Aplication\Microsoft\Outlook Express\News\ - новости \Aplication\Microsoft\Address Book\ - адресная книга \Cookies\ - файлы Cookies

\Favorites\ - файлы закладок Интернет \History\ - файлы истории Windows user. dat - параметры пользователя user. da0 - резерв Это лишь малая часть из возможных примеров, большинство других программ (модемные, факсовые, FTP-клиенты, броузеры и т.д.) ведут лог-файлы (где и когда вы были, что делали), кэши и т.д. – ПРОВЕРЯЙТЕ И ОТСЛЕЖИВАЙТЕ ЭТО, БУДЬТЕ БДИТЕЛЬНЫ! И удаляйте их с помощью программы Kremlin 2.1.

К вопросу о CMOS SETUP.

Вот вам еще один наглядный пример лазеек для спецслужб.

Любой компьютер имеет возможность установить пароль на вход. Но мало кто знает что специально для спецслужб (разработчиками BIOS) были созданы универсальные пароли, открывающие вход в любой компьютер.

Вот примеры:

- AWARD BIOS: AWARD\_SW, lkwpeter, Wodj, aPAf, j262, Sxyz, ZJAAADC

- AMI BIOS: AMI, SER, Ctrl+Alt+Del+Ins (держать при загрузке, иногда просто INS)

Естественно, что вводить пароль нужно в соответствии с регистром букв.

Программы авторизующиеся в Online.

В последнее время все чаще стали появляться программы которые проводят проверку своей легальности посредством Интернет (вернее когда вы сидите в Интернет, они незаметно проверяются, а потом радуют вас сообщением о том что - мол это нелегальная копия - наглядный пример Bullet Proof FTP). Но это еще пол беды, существует мнение что такие программы, как например операционная система Windows, способны как бы следит за всем что происходит на компьютере (либо сами, либо по команде из Интернет) и отправлять все собранные данные своим разработчикам. Недавно был скандал, когда один известный FTP клиент оправлял все вводимые имена и пароли своим разработчикам. Так что будьте бдительны!

Клавиатурные шпионы Это программы предоставляющие возможность записи того, что вы печатаете на чужом компьютере, владельцем этого компьютера, или, если смотреть на это с другой стороны, ваше право посмотреть, что творилось на вашем компьютере, пока вас не было в офисе.

И то, и другое делается одним методом: все, что набирается на клавиатуре, заносится в текстовый файл специальной программой. Так что набранный вами текст на компьютере в бизнес-центре или интернет-кафе может легко стать достоянием владельца такого компьютера. Технически такая операция выполняется классом программ, называемых keyboard loggers. Они существуют для разных операционных систем, могут автоматически загружаться при включении и маскируются под резидентные антивирусы или что-нибудь еще полезное.

Самая лучшая из опробованных авторами программ, Hook Dump 2.5 (http: // www. geocities. com/SiliconValley/Vista/6001/hookdump. zip, для Win 3.1. и Win 95), написанная Ильей Осиповым (http: // www. halyava. ru/ilya/), может автоматически загружаться при включении компьютера, при этом никак не проявляя своего присутствия.

Набранный на клавиатуре текст, названия программ, в которых набирался текст, и даже скрытый пароль в Dial-Up Networking, который вообще не набирался - все записывается в файл, расположенный в любом директории и под любым именем. Программа имеет много настроек, позволяющих определять нужную конфигурацию.

## 9. Защита от вредных компьютерных факторов

Наша нынешняя жизнь немыслима без ПК, но при работе с ним необходимо учитывать ряд рекомендаций, которые помогут сохранить ваше здоровье.

1. Оптимальное расстояние между экраном и работающим ПК должно быть около 50 см.

2. В качестве монитора ПК лучше всего использовать новые цветные жидкокристаллические мониторы.

3. Идеальным (с точки зрения безопасности для здоровья) является компьютер типа "Notebook".

4. Если вы пользуетесь обыкновенным монитором с ЭЛТ, то в обязательном порядке необходимо использовать защитный экран класса -

полная защита. Мы рекомендуем: Русский Щит (Золотой или Платиновый).

5. Верх экрана должен быть примерно на уровне горизонтальной линии, проведенной от глаз к экрану.

6. Во время работы положение кистей рук должно быть горизонтальным, предплечья разогнуты в локтевых суставах под углом 90

градусов, спина должна быть прямой. Руки должны иметь опору на столе.

7. Во время нормальной работы голова не должна быть сильно наклонена, чтобы не беспокоили головные боли и боли в шее.

8. Клавиатура должна располагаться не ближе 10 см от края стола.

При длительной работе с клавиатурой нежелательно, чтобы кисти и предплечья опирались на угол стола.

9. Желательно чтобы компьютер был заземлен.

10. При длительной работе с ПК важны своевременный отдых, разминка.

11. Во время работы с монитором не следует сидеть "как столб", необходимо периодически менять позу, двигать плечами, поморгать глазами или закрыть их на несколько секунд. Дышать надо свободно.

После 30-45 минут интенсивной работы желательна пауза и гимнастика, в том числе для глаз.

12. Через 10 минут работы полезно на 5-10 с отвести глаза в сторону от экрана.

13. Следует ограничить время интенсивной работой с ПК; не более 4

часов в день.

14. Рабочие места с ПК должно определенным образом устанавливаться относительно светопроемов:

Дверь Іњњњњњњњњњњњњњњњњњњњњњњњњњњњ<њњњњњњњњњњњњњњ>њњњњњњњњњњњњњњњњњњњњњњњњњњњњ-

‹ Допускается Рекомендуется ‹

‹ Іњњњњњњњњњњњњњњ - Іњњњњњњњњњњњњњњ - ‹

‹ ‹ Стол ‹ ‹ Стол ‹ ‹

‹ Іњњњњњњњњњњ - ‹Іњњњњњ-Іњњњњњ-‹ ‹Іњњњњњ-Іњњњњњ-‹ Іњњњњњњњњњ - ‹

‹ ‹ Кресло ‹ ‹‹Кла - ‹‹ ‹‹ ‹‹ ‹‹ Кла-‹‹ ‹Кресло ‹ ‹

‹ ‹линия њњ> ‹ ‹‹виа - ‹‹ВДТ ‹‹ ‹‹ВДТ ‹‹ виа-‹‹ ‹<њњ линия‹ ‹

‹ ‹ взора ‹ ‹‹тура ‹‹ ‹‹ ‹‹ ‹‹ тура‹‹ ‹взора ‹ ‹

‹ њњњњњњњњњњ± ‹њњњњњ±њњњњњ±‹ ‹њњњњњ±њњњњњ±‹ њњњњњњњњњ± ‹

‹ њњњњњњњњњњњњњњ± њњњњњњњњњњњњњњ± ‹

‹ Окно Окно Окно ‹

њњњњњњњњњњњњ<њњњњњњњњњњњ>њњњњ<њњњњњњњњњњњ>њњњњњњ<њњњњњњњњњњ>њњњњњњњњњњњ±

- Схемы размещения рабочих мест с ПК должны учитывать расстояния между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора), которое должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов - не менее 1,2 м.

- Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей (размер ВДТ и ПК, клавиатуры, пюпитра и др.), характера выполняемой работы. При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики.

- Конструкция рабочего стула (кресла) должна обеспечивать поддержание рациональной рабочей позы при работе на ВДТ и ПК, позволять изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления.

- Рабочий стул (кресло) должен быть подъемно-поворотным и регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от переднего края сиденья, при этом регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию.

- Поверхность сиденья, спинки и других элементов стула (кресла)

должна быть полумягкой, с нескользящим, неэлектризующимся и воздухопроницаемым покрытием, обеспечивающим легкую очистку от загрязнений.

## 10. Безопасность при работе с ббс и ftn сетями

В этой главе мы рассмотрим основные рекомендации, целесообразные к применению в целях вашей безопасности при регистрации и работе с ББС и FTN сетями.

ББС - это программно-аппаратный комплекс обеспечивающий с помощью модема и необходимого ПО доступ к программам и информации.

FTN сети (например Фидо) - это любительские компьютерные сети, предназначенные для обмена сообщениями электронной почты.

Итак, наши рекомендации:

1. ПРОВЕРЯЙТЕ ОТСУТСТВИЕ АОН. Прежде чем звонить на ББС или FTN, удостоверьтесь (например путем звонка с сотового телефона, с телефона-двойника типа Panasonic, с таксофона или с телефона который гарантированно не определяется системой АОН) что на данном узле отсутствует система АОН. Если в списке ББС (или в рекламе) указан тип модема: Russian Courier, Zyxell или IDC - то можете не звонить туда, там с вероятностью 99% используется АОН. АОН засвечивает себя характерным щелчком и звуковым сигналом, как правило после первого гудка (т.е. он снимает трубку а далее уже идут гудки выдаваемые самими АОН, и по тональности как правило отличающиеся от первого гудка).

Если АОН есть, но вам все же надо остаться анонимным то воспользуйтесь АнтиАОНом, функции АнтиАОНа присутствуют практически во всех телефонных аппаратах с АОН (например в РУСЬ или в Phone Master).

Либо купите (их полно на радиорынке в Митино) приставку АнтиАОН, она вам еще не раз пригодиться! Функцию АнтиАОН лучше включать почти сразу после набора номера и удерживать ее некоторое время, экспериментируйте и умение придет к вам. Если АОН не может определить номер то вы, после снятия трубки АОНом слышите характерные тональные посылы (порядка 9 штук).

2. ПРИ РЕГИСТРАЦИИ ИСПОЛЬЗУЙТЕ ВЫМЫШЛЕННЫЕ ДАННЫЕ. Никогда не стоит регистрироваться под настоящим именем, ибо неизвестно к кому могут попасть ваши данные и для чего их могут использовать.

Возьмите любую телефонную базу, например КОТИК или ее Online версию: http: // www. xland. ru: 8088/tel\_win/owa/tel. form и введите любую выдуманную вами фамилию. Не стоит вводить тривиальные фамилии, вроде - Иванов, Петров, Смирнов, Андреев, Алексеев и т.д. Лучше что-то не совсем обычное, ну первое что приходить в голову: Левашов, Дубинин, Авдотин, Садовский и т.д. Далее, выпишите любого из выведенного списка (выпишите инициалы, адрес и телефон).

### 10.1. Интересные ББС

Ниже приводиться список наиболее интересных (на наш взгляд)

Московских ББС:

Іњњњњњњњњњњњњњњњњњњњњњњњњњњњљњњњњњњњњњњњњљњњњњњњњњњњњњњњњњњњњњњњњњњњњ-

‹ Название ББС ‹ Телефон ‹ Время работы ‹

‹ ‹ ‹в рабочие дни в выходные ‹

ЃњњњњњњњњњњњњњњњњњњњњњњњњњњњќњњњњњњњњњњњњќњњњњњњњњњњњњњљњњњњњњњњњњњњњЊ

‹ Anarhia BBS ‹095-948-6250‹ 06: 00-14: 00 ‹ <<< ‹

‹ DGN LTD BBS (AON) ‹095-582-4922‹ 24h ‹ 24h ‹

‹ Fantom BBS ‹095-907-0382‹ 24h ‹ 24h ‹

‹ Gnosis Occultus BBS (AON) ‹095-916-4042‹ 22: 30-07: 00 ‹ <<< ‹

‹ Hack's Station BBS Line#1 ‹095-430-4530‹ 22: 30-08: 00 ‹ <<< ‹

‹ Hack's Station BBS Line#3 ‹095-437-0960‹ 01: 00-09: 00 ‹ <<< ‹

‹ Hacker's Stone BBS ‹095-344-1227‹ 00: 00-12: 00 ‹ <<< ‹

‹ InfoScience BBS line 2AON‹095-923-0871‹ 24h ‹ 24h ‹

‹ InfoScience BBS line 4AON‹095-923-2003‹ 24h ‹ 24h ‹

‹ InfoScience BBS line 5AON‹095-229-7622‹ 24h ‹ 24h ‹

‹ InfoScience BBS line 6AON‹095-229-3985‹ 24h ‹ 24h ‹

‹ InfoScience BBS line 8AON‹095-913-9944‹ 24h ‹ 24h ‹

‹ InfoScience BBS line 9AON‹095-913-9945‹ 24h ‹ 24h ‹

‹ InfoScience BBS line 12AON‹095-742-1440‹ 24h ‹ 24h ‹

‹ InfoScience BBS line 13AON‹095-742-1441‹ 24h ‹ 24h ‹

‹ InfoScience BBS line 14AON‹095-742-1443‹ 24h ‹ 24h ‹

‹ MSAAB BBS ‹095-270-0237‹ 24h ‹ 24h ‹

‹ MAKET (AON) ‹095-263-1129‹ 24h ‹ 24h ‹

‹ Orl. Corp ‹095-152-9044‹ 23: 00-07: 00 ‹ 24h ‹

‹ Some Old Bullshit BBS(AON) ‹095-236-3424‹ 00: 00-07: 30 ‹ <<< ‹

‹ SoftLand BBS ‹095-932-9053‹ 24h ‹ 24h ‹

‹ Shadow Gluck BBS SG#1(AON) ‹095-452-4103‹ 24h ‹ 24h ‹

‹ The Videoman station ‹095-432-0257‹ 23: 00-08: 00 ‹ <<< ‹

˜њњњњњњњњњњњњњњњњњњњњњњњњњњњ™њњњњњњњњњњњњ™њњњњњњњњњњњњњ™њњњњњњњњњњњњњ±

Примечания:

АОН - наличие АОН на станции.

24h - станция работает 24 часа в день.

<<< - Станция работает так же, как и в рабочие дни (см. столбец weekdays).

### 10.2. Интересные конференции сети Фидо

Ниже приводится список наиболее интересных (на наш взгляд) конференций Фидо:

Mo. Advice - ответы на любые вопросы Mo. Books. Wanted - поиск и продажа книг Mo. Talk - Московские разговоры Mo. SoftExchange - поиск программ Mo. Wanted - поиск всего остального N5020. Point - поиск поинтовых вакансий в Московском Фидо Ru. Aon - об АОНах Ru. Anti. Ats о борьбе с АТС

Ru. Army - как откосить от армии Ru. Internet - вопросы по Интернет Ru. Internet. Chainik - аналогично но для чайников Ru. Internet. WWW - анонсы новых WWW сайтов Ru. Phreaks - фрикинг, взлом сотовых телефонов, карточек и т.д.

Ru. Crypt - криптография Ru. Security - безопасность Su. Chainik - вопросы по FTN технологии Su. Chainik. Faq - факи Su. Chainik. General - общие вопросы Ru. Hacker - о хакерах и для хакеров Su. Hardw. chainik - вопросы по железу (Hardware)

Su. Hardw. phones - о телефонах Su. General - обо всем понемногу Su. Spy - шпионская эха Su. Virus - компьютерные вирусы Su. Pol - политика Su. Pol. Theory - политика (теория)

Survival. Guide - выживание и безопасность XSu. Cellular - сотовые телефоны.

## 11. Безопасность в сети интернет

### 11.1. Выбираем провайдера

Выбор провайдер - это отправная точка с которой начинается ваш путь в увлекательный мир Интернет.

При выборе надо учитывать то обстоятельство что практически все провайдеры требуют идентификации вашей личности (ФИО, паспортные данные и т.д.).

Как преодолеть эту и другие проблемы, об этом читайте ниже.

1. ПРОВЕРЯЙТЕ ОТСУТСТВИЕ АОН. Если вы хотите сохранить свою конфиденциальность при работе с Интернет, то прежде всего необходимо удостовериться в отсутствии аппаратуры АОН у провайдера. Для этого производятся контрольные звонки на рабочие (именно рабочие а не тестовые линии - их телефоны необходимо узнать заранее у провайдера или из других источников) телефонные линии например с сотового телефона, с телефона-двойника типа Панасотовик, с таксофона или с телефона который гарантированно не определяется системой АОН. АОН засвечивает себя характерным щелчком и звуковым сигналом, как правило после первого гудка (т.е. он снимает трубку а далее уже идут гудки выдаваемые самими АОН, и по тональности как правило отличающиеся от первого гудка).

Если АОН есть, но вам все же надо остаться анонимным то воспользуйтесь АнтиАОНом, функции АнтиАОНа присутствуют практически во всех телефонных аппаратах с АОН (например в Русь или в Phone Master).

Либо купите (их полно на радиорынке в Митино) приставку АнтиАОН, она вам еще не раз пригодиться! Функцию АнтиАОН лучше включать почти сразу после набора номера и удерживать ее некоторое время, экспериментируйте и умение придет к вам. Если АОН не может определить номер то вы, после снятия трубки АОНом слышите характерные тональные посылы (порядка 9 штук).

Доподлинно известно, что аппаратура АОН имеется у всех провайдеров использующих модемы Zyxell (например Deol), а также у всех провайдеров производящих оплату в кредит (МТУ-Информ, ГОТ и др.).

2. ПРИ РЕГИСТРАЦИИ ИСПОЛЬЗУЙТЕ ВЫМЫШЛЕННЫЕ ДАННЫЕ. Никогда не стоит регистрироваться под настоящим именем, ибо неизвестно к кому могут попасть ваши данные и для чего их могут использовать.

Возьмите любую телефонную базу, например КОТИК или ее Online версию: http: // www. xland. ru: 8088/tel\_win/owa/tel. form и введите любую выдуманную вами фамилию. Не стоит вводить тривиальные фамилии, вроде - Иванов, Петров, Смирнов, Андреев, Алексеев и т.д. Лучше что-то не совсем обычное, ну первое что приходить в голову: Левашов, Дубинин, Авдотин, Садовский и т.д. Далее выпишите любого из полученного списка (выпишите инициалы, адрес и телефон). И плюс ко всему необходимо выдумать левые паспортные данные, ну серия, номер, кем выдан, когда.

Кстати по базе ОЗОМ можно определить принадлежность конкретной улицы к конкретному отделению милиции - для еще большей достоверности.

Теперь вам осталось изготовить какую-либо ксиву с вашей фотографией и вымышленными данными. Для убедительности надо достать печать (у друзей, или сделать ее - любая печать в Москве стоит порядка 50 долларов) - лучше государственного типа. Ксива может например гласить что вы: студент, охранник, работник прокуратуры, сотрудник ФАПСИ (ФСБ, МВД), или просто какой-либо сотрудник какой-либо фирмы.

Далее едете в контору к провайдеру (лучше с утра - с утра люди добрее) и говорите что хотите зарегистрироваться (стать их клиентом) а когда доходит до паспорта (иногда достаточно просто вписать паспортные данные не предъявляя его) говорите что не взяли его (мол никто и не говорил по телефону что нужен паспорт) - НО вы наизусть помните свои паспортные (вымышленные естественно!) данные - это скорее всего пройдет (так как клиентов нынче мало, а денег всем хочется). Для убедительности можете показать свое удостоверение (также при входе на некоторые конторы где требуют паспорт - оно вам может здорово пригодится).

Если хотите чтобы улик не было совсем, можете еще изготовить факсимиле вымышленной подписи и ставить его на договоре (незаметно разумеется).

Если не прокатит, то уходите с обиженным видом и пригрозите: мол ноги моей больше не будет в вашей гнилой конторе.

3. ПОЛЬЗУЙТЕСЬ ПРОВЕРЕННЫМИ ПРОВАЙДЕРАМИ. Трюк с левыми паспортными данными лучше всего может пройти в мелких конторах, а в крупные компании типа Демос и Релком даже лучше и не соваться (если конечно у вас не будет хорошо сделанного студенческого билета или паспорта).

Далее приводится список более-менее стабильных Московских провайдеров, который поможет вам сделать оптимальный выбор.

4. ИСПОЛЬЗУЙТЕ ТЕСТОВЫЕ ВХОДЫ. Некоторые провайдеры (например Корбина), если позвонить им и попросить проверить качество связи называют телефон по которому можно это сделать. Как правило время работы на тестовой линии составляет 15-60 минут, что вполне достаточно для проведения некоторых акция.

Вот некоторые примеры:

Провайдер "КАРАВАН"

тел.332-4486, факс 129-3500

a. Cерийный телефон 332-4768 (8 линий).

b. Отдельные телефоны:

332-4122, 332-4123, 332-4124, 332-4125, 332-4126, 332-4127, 332-4274, 332-4264, 332-4255, 332-4252, 332-4246, 332-4454, 332-4469, 332-4472, 332-4793.

c.129-1744, 129-3254, 129-3290.

d. Серийный телефон 931-67-88 (11 линий).

Прямые телефоны на серию:

931-6001, 931-6009, 931-6100, 931-6133, 931-6136, 931-6144, 931-6145, 931-6540, 931-6541, 931-6542, 931-6788.

e. Отдельные телефоны: 939-1475, 939-3084, 939-5213, 939-4270, 939-3275, 939-5118, 939-2635, 939-5237, 939-5236.

Бесплатно пользоваться каналом можно с 4 ночи до 10 утра ежедневно. По телефонам, которые начинаются с 332. Login: free, Password: caravan. Если не пускают, это значит, что все бесплатные модемные входы уже заняты.

Провайдер "СИТЕК". У этого провайдера можно получить бесплатный E-Mail!

На windoms. sitek. net

Tel: 742-9420(21)

963-3101

964-1301

964-1091

995-1090

DNS: (I) 195.212.225.2

(II) 195.212.225.162

Login: sitek

Password: sitek

5. ИСПОЛЬЗУЙТЕ РЕКЛАМНЫЙ ДОСТУП. Некоторые провайдеры (например Россия Онлайн) предлагают (или прилагают к купленному модему, компьютеру и т.д.) пакет ПО, документацию и некоторое количество часов бесплатной работы в Интернет (как правило 5-10 часов). Пользуйтесь этим, не забывая про общие правила безопасности описанные нами.

Другие провайдера (например СИТЕК) просто продают запечатанный конверт, в котором находится имя, пароль и определенное количество часов работы в Интернет. Это пожалуй самый безопасный вариант, где вы ни коим образом не засвечиваете свои данные. Такие конверты можно например приобрести на радиорынке в Митино или в самом СИТЕКе.

6. ИСПОЛЬЗУЙТЕ "ЛЕВЫЙ" DNS. Для того что бы спрятать свой IP-адрес, вернее даже не спрятать а использовать IP-адрес другого провайдера необходимо в параметрах установки связи поставить DNS другого провайдера (например, Демоса).

Вот например DNS провайдера Demos:

Primary 194.87.0.8

Secondary 194.87.0.9

А вот DNS провайдера Гласнет:

Primary 195.218.218.38

Secondary 195.218.218.37

7. МОСКОВСКИЕ ПРОВАЙДЕРЫ СЕТИ ИHТЕРHЕТ.Д.алее идет список наиболее известных Москвоских провайдеров.

Hазвание: АО Релком Почтовый адpес: 123098, Москва, yл. Маpшала Василевского, д.1, коpп.1.

Телефон/факс: 196-07-20. 196-08-20, 196-08-23/ 196-32-95

E-mail: support@relcom. ru

Home page: http: // www. relcom. ru

Сеpвис:

http: // www. relcom. ru: 80/Relcom-Moscow/OfficialDocs/Pricelist/

Hазвание: ООО "Компания Демос+"

Почтовый адpес: 113035, Москва, Овчинниковская наб., д.6/1

Телефон/факс: 956-60-80, 956-62-33 / 956-50-42

E-mail: info@demos. su

Home page: http: // www. demos. su

Сеpвис: http: // www. demos. su/eng/price-e. htm

Название: "Гот"

Почтовый адрес:

Телефон: 921-36-01, 923-21-27

Модемные телефоны: 925-3503, 925-3507, 925-7165, 924-5847, 923-8741, 925-1994

E-mail:

Home page: http: // got. mmtel. ru

Сервис:

Название: "Corbina Telecom"

Почтовый адрес: Рязанский пр., 30/15

Телефон: 755-5648

E-mail: sales@corbina. ru

Home page: http: // www. corbina. ru

Сервис:

Hазвание: InComa

Почтовый адpес: 125252, Москва, yл. Кyyсинена, д.21Б, офис 60.

Телефон/факс: 198-73-81 / 913-25-12

E-mail: info@incomma. com

Home page: http: // www. fastnet. ru

Сеpвис: http: // www. fastnet. ru/bnet/bnet. html

Hазвание: АО "Техно Центp Плюс"

Почтовый адpес: 115395, Москва, yл. Юности, д.13, коpп.2.

Телефон/факс: 374-76-63, 965-10-10, 465-90-25 / 374-00-02

E-mail: info@techno. ru

Home page: http: // www. techno. ru

Сеpвис: http: // www. techno. ru/koi/netgroup/netprice. html

Hазвание: ОАО "Московский междyнаpодный и междyгоpодный телефон"

Почтовый адpес: 119895, Москва, Зyбовская пл., д.3. и ул. Арбат, 46

Телефон/факс: 241-6232, 246-02-43, 338-00-11, 241-84-81 / 246-41-53, 241-71-01.

E-mail: commt@db. mmtel. msk. su

Home page: http: // www. mmtel. msk. su

Сеpвис: http: // www. mmtel. msk. su/koi8/mmtel/tarmmtel. html

Hазвание: СП "SOVAM TELEPORT" (Россия Онлайн)

Почтовый адpес: 111250, Москва, yл. Кpасноказаpменная, д. 12.

Телефон/факс: 258-41-75 / 258-41-69

E-mail: sale@online. ru

Home page: http: // www. online. ru

Сеpвис: http: // koi. www. online. ru/rservices/rinvite. xhtml

Hазвание: ТОО "Элвис+"

Почтовый адpес: 103460, Москва, Зеленогpад, Центpальный пpоспект, д.11.

Телефон/факс: 536-95-51, 531-46-33 / 531-24-03

E-mail: www@elvis. ru

Home page: http: // www. elvis. ru

Сеpвис: http: // www. elvis. ru/BBS/price. html

Hазвание: АО "РОСПРИИТ"

Почтовый адpес: 103375, Москва, Твеpская yл., д.7.

Телефон/факс: 201-68-90 / 923-23-44

E-mail: sales@sovmail. rosprint. ru

Home page: http: // www. rosprint. ru

Сеpвис:

Hазвание: Инститyт космических исследований РАИ

Почтовый адpес: Москва, Пpофсоюзная yл., д.84/32.

Телефон/факс: 913-30-41 / 913-30-40

E-mail: info@www. space. ru

Home page: http: // www. space. ru

Сеpвис: http: // www. space. ru/english/spacenet/plist. html

Hазвание: Акционеpная компания СЭЛФ

Почтовый адpес: 103617, Москва, Зеленогpад, коp.1412.

Телефон/факс: 530-26-00 / 530-34-44

E-mail: Support@CompNet. RU

Home page: http: // www. compnet. ru

Сеpвис: http: // www. compnet. ru/news-bin/news/compnet. prices

Hазвание: АО "Оpгланд"

Почтовый адpес: 103527, Москва, Зеленогpад, коp.833.

Телефон/факс: 532-10-40, 532-00-06, 532-56-33 / 532-90-90

E-mail: admin@orgland. zgrad. su

Home page: http: // www. orgland. ru

Сеpвис: http: // www. orgland. ru/orgland/orgprice. html

Hазвание: Компания "Элвис-Телеком"

Почтовый адpес: 125190, Москва, а/я 211.

Телефон/факс: 152-97-00 / 152-46-61

E-mail: pau@telekom. ru

Home page: http: // www. telekom. ru

Сеpвис: http: // www. telekom. ru/rus/rprice. html

Hазвание: Коpпоpация LMS

Почтовый адpес: 115573, Москва, а/я 211.

Телефон/факс: 323-90-76, 324-44-40 / 323-90-24

E-mail: info@express. ru

Home page: http: // www. express. ru

Сеpвис:

Hазвание: Сообщество Финансовых Телекоммyникаций Почтовый адpес: 117806, Москва, Пpофсоюзная yл., 65.

Телефон/факс: 334-89-71, 913-30-76, 334-37-96, 330-56-85 /

330-37-96

E-mail: sales@sft. fact400. ru

Home page: http: // www. sft. fact400. ru

Сеpвис: http: // www. sft. fact400. ru/down/sft\_ip. zip

Hазвание: Компания 2КОМ

Почтовый адpес: 117342, Москва, yл. Бyтлеpова, 17Б.

Телефон/факс: 330-80-74, 330-45-47/ 330-45-56

E-mail: adm@mail. com2com. ru

Home page: http: // www. com2com. ru

Сеpвис: http: // www. com2com. ru/koi8/support/intlet1. html

Hазвание: Rinet

Почтовый адpес: Москва, 1-й Хвостов пеp., д.11а.

Телефон/факс: 238-39-22

E-mail: info@rinet. ru

Home page: http: // www. rinet. ru

Сеpвис: http: // www. rinet. ru/price/price. html

Hазвание: ООО "Zenon N. S. P"

Почтовый адpес: Москва, 1-я yлица Ямского поля, д. 19.

Телефон/факс: 251-57-02, 250-46-29

E-mail: www@aha. ru

Home page: http: // www. aha. ru

Сеpвис: http: // sunny. aha. ru/users/prices. htm

Hазвание: ЗАО "Гаpант-Паpк"

Почтовый адpес: 119899, г. Москва Воpобьевы Гоpы, МГУ, Иаyчный Паpк Телефон/факс: 932-91-50, 932-91-51 / 932-91-50

E-mail: info@park. ru

Home page: http: // www. park. ru

Сеpвис: http: // www. park. ru/INFO/info? k+net/price

Hазвание: Ассоциация пользователей компьютеpных сетей "Гласнет"

Почтовый адpес: 103009, Москва, Газетный пеp., д.9, стp.2.

Телефон/факс: 222-09-90 / 229-00-43

E-mail: support@glasnet. ru

Home page: http: // www. glasnet. ru

Сеpвис: http: // www. glasnet. ru/brochure/rusprice. html

Hазвание: Компания "NetState Communications"

Почтовый адpес: Москва, yл. Твеpская, д.5/6, подъезд 4.

Телефон/факс: 292-73-17 / 292-76-35

E-mail: info@goldnet. ru

Home page: http: // wwwnet. ru/

Сеpвис:

Hазвание: Компания "CENTRONET"

Почтовый адpес: 123424, Москва, Волоколамское ш., д.112

Телефон/факс: 491-85-76 / 491-30-66

E-mail: eugenie@astro. ru

Home page: http: // www. astro. ru/

Сеpвис: http: // www. astro. ru/docum2. htm

Hазвание: АОЗТ "ИС ГЕИЕЗИС"

Почтовый адpес: 127276, Москва, yл. Ботаническая, д.14

Телефон/факс: 903-94-94, 903-94-82 / 903-94-25

E-mail: root@genesis. msk. ru

Home page:

Сеpвис: BBS 401-41-74 (файл genesis. exe)

Hазвание: Online Resource Center

Почтовый адpес: Москва, Ленинский пp., д.32/а Телефон/факс: 938-29-83 / 938-29-81

E-mail: admin@orc. ru

Home page: http: // www. orc. ru/

Сеpвис: http: // www. orc. ru/price/pricerus. html

Hазвание: ЗАО "РФК"

Почтовый адpес: 107076, Москва, Пpеобpаженская пл., д.6/68, стp.3

Телефон/факс: 964-03-73, 964-03-91 / 964-25-19

E-mail: support@transit. ru

Home page: http: // www. transit. ru

Сеpвис: http: // www. transit. ru/koi8/priceip. htm

Hазвание: Компания "CITYLINE"

Почтовый адpес: 119034, Москва, Коpобейников пеp., д.1/2, стp.6.

Телефон/факс: 245-88-68 / 245-88-77

E-mail: webmaster@cityline. ru

Home page: http: // www. cityline. ru

Сеpвис: http: // www. cityline. ru: 8083/prices. html

Hазвание: ООО "Data Express Corp. " (Deol)

Почтовый адpес: 117279, Москва, yл. Остpовитянова, д.37а.

Телефон/факс: 932-72-01, 932-76-01 / 932-74-10

E-mail: sysop@deol. ru

Home page: http: // koi8. deol. ru

Сеpвис: http: // koi8. deol. ru/service/instr. htm

Hазвание: QuasiWest Ltd.

Почтовый адpес: 119899, Москва, Воpобьевы гоpы, Иаyчный паpк МГУ, коpп.7.

Телефон/факс: 247-62-08 / 932-91-04

E-mail: info@netclub. ru

Home page: http: // www. netclub. ru

Сеpвис: http: // koi. www. netclub. ru/Russian/netprice. html

Hазвание: ООО "МАСТАК-ИИФО" (Ситек)

Почтовый адpес: 111020, Мoсква, а/я 100. (yл. Стоpожевая, д.

23).

Телефон/факс: 964-12-01 / 964-11-83

360-6909, 334-4406

E-mail: postmaster@sitek. net

Home page: http: // www. sitek. ru

Сеpвис:

http: // www. koi. sitek. ru/sitek\_inform/price/serviseprices. html

Hазвание: АО "Ропнет"

Почтовый адpес: 103084, Москва, Мясницкая yл., 47.

Телефон/факс: 207-75-56 / 207-32-01

E-mail: root@ropnet. ru

Home page: http: // www. ropnet. ru/

Сеpвис: http: // www. ropnet. ru/koi/internet/inter\_pr. html

Hазвание: ТОО ГАММА

Почтовый адpес:

Телефон/факс: 939-39-07 / 938-21-36

E-mail: mailto: postmaster@gamma. ru

Home page: http: // www. gamma. ru

Сеpвис: http: // www. gamma. ru/cgi-bin/prices/koi? rates=comm:

http: // www. gamma. ru/cgi-bin/prices/koi? rates=noncomm

Hазвание: TERRA RUTHENIA

Почтовый адpес:

Телефон/факс: 924-20-28 /

E-mail: mailto: info@ru. com

Home page: http: // www. ru. com/

Сеpвис: http: // www. ru. com/services. koi. html

Hазвание: Data Force

Почтовый адpес: 3-й Самотечный переулок, 11

Телефон: 288-9340

E-mail: info@dataforce. net

Home page: http: // www. dataforce. net/

Сеpвис:

Hазвание: Global One

Почтовый адpес: Тверская ул., 7

Телефон: 201-9285

E-mail:

Home page: http: // www. global-one. ru/

Сеpвис:

Hазвание: NetPass

Почтовый адpес: Садовническая ул., 76, стр.2

Телефон: 961-2460

E-mail: sales@netpass. ru

Home page: http: // www. netpass. ru/

Сеpвис:

Hазвание: Plug Communication

Почтовый адpес: Мерзляковский пер., 3-1-1

Телефон: 795-0955

E-mail: info@plugcom. ru

Home page: http: // www. plugcom. ru/

Сеpвис:

Hазвание: GoldNet

Почтовый адpес: Тверская ул., 5/6, подъезд ј4

Телефон: 292-7317

E-mail: mailbox@goldnet. ru

Home page: http: // www. goldnet. ru/

Сеpвис:

Hазвание: Инфотел Почтовый адpес: Пресненский вал, 19, офис 911

Телефон: 252-0701, 252-1212

E-mail: info@infotel. ru

Home page: http: // www. infotel. ru/

Сеpвис:

Hазвание: Коммбелга Почтовый адpес: Мытная ул., 3, вход 2, 14-й этаж Телефон: 931-9950

E-mail: sales@co. ru

Home page: http: // www. co. ru/

Сеpвис:

Hазвание: Комстар Почтовый адpес: 3-я Тверская Ямская, 39/5

Телефон: 956-0000

E-mail: request@comstar. ru

Home page: http: // www. comstar. ru/

Сеpвис:

Hазвание: Мегабит7

Почтовый адpес: ВВЦ (ВДНХ)

Телефон: 234-5065

E-mail: support@megabit7. ru

Home page: http: // www. megabit7. ru/

Сеpвис:

Hазвание: Микродин Почтовый адpес: Новозаводская ул., 18

Телефон: 145-9755, 145-9380

E-mail: office@microdin. ru

Home page: http: // www. microdin. ru/

Сеpвис:

Hазвание: МТУ-Информ Почтовый адpес: Смоленская-Сенная пл., 27-29, стр.2

Телефон: 258-7878

E-mail: info@mtu. ru

Home page: http: // www. mtu. ru/

Сеpвис:

Hазвание: Редлайн Почтовый адpес: Цветной бульвар, 30, комн.517

Телефон: 200-2475, 291-6132

E-mail: redline@redline. ru

Home page: http: // www. redline. ru/

Сеpвис:

Hазвание: ФТ-Центр Почтовый адpес: Покровский бульвар, 3

Телефон: 208-3300, 917-5232

E-mail: info@ftcenter. ru

Home page: http: // www. ftcenter. ru/

Сеpвис:

Hазвание: Центральный телеграф Почтовый адpес: Тверская ул., 7, подъезд 4

Телефон: 201-6884, 201-9262

E-mail: spu@m400. ctel. msk. ru

Home page: http: // www. ctel. msk. ru/

Сеpвис:

Hазвание: Элкател Почтовый адpес: ул. Бутлерова, 15, офис 150

Телефон: 424-1811

E-mail: info@elkatel. ru

Home page: http: // www. elkatel. ru/

Сеpвис:

### 11.2. По www без следов

Путешествуя по Интернету, мы не часто задумываемся о том, что оставляем следы своих посещений каждый раз, когда заходим на какой-либо сайт. Пожалуй, об этом и не стоило бы беспокоиться, если бы не был так велик тот объем информации, который потенциально могут добыть о нас владельцы сайта. Стандартные log-файлы, хитроумные скрипты и прочие ухищрения любопытных владельцев способны узнать о вас многое: тип компьютера и операционной системы, страну пребывания, название и адрес провайдера, и даже зачастую адрес электронной почты и ваше имя.

Существуют много причин, по которым пользователь может не захотеть оставлять следы своего пребывания. Тут и нежелание раскрыть свой адрес электронной почты, чтобы не стать жертвой спама, и необходимость получить информацию с сайта, который варьирует ответ в зависимости от страны, из которой отправлен запрос. Или, например, вы частенько заходите на Web узел ваших конкурентов, и хотите делать это анонимно.

Кроме того, существуют такие бяки, как cookies, да и дыры в безопасности в MSIE обнаруживаются все новые и новые... В общем, не послать ли нам в путешествие по WWW кого-нибудь еще? Идея трезвая, и достаточно легко выполнимая, причем несколькими способами.

Способ 1: Анонимайзер Осуществить подобный анонимный серфинг позволяет служба Anonymizer. Зайдите на их сайт (http: // www. anonymizer. com или http: // www. iproxy. com), наберите нужный URL, и вперед! Отправляясь по ссылке, помещенной на странице, которую вы просматриваете с помощью Анонимайзера, вы попадаете на очередную страницу снова через Анонимайзер, так что процесс автоматизирован, и набирать новый URL

снова не нужно. Были хорошие времена, когда Анонимайзер отправлялся по указанному адресу немедленно, теперь же для тех, кто пользуется этой службой бесплатно, существует 30-секундный период ожидания. Кроме того, Анонимайзер позволял использовать как HTTP, так и FTP ресурсами.

Теперь же использовать FTP могут лишь зарегистрированные пользователи.

При использовании этой службы след в log-файлах оставляете не вы, а Анонимайзер, что исключает возможность сбора всей той информации, о которой было написано выше. Никакие cookies до вас не доходят.

Некоторые сайты, например (например, Hotmail), через него недоступны, что, очевидно, объясняется желанием их владельцев следить за посетителями. Анонимайзер также не работает с безопасными узлами, использующими SSL протокол.

Анонимайзер имеет еще две приятные особенности. Во-первых, некоторые сайты WWW бывают недоступны из одного места, но доступны из другого. Во-вторых, некоторый сайты выдают вам информацию в зависимости от того, откуда поступает ваш запрос.

Способ 2: Прокси Анонимизировать путешествие по сети можно также с помощью прокси сервера. Прокси сервер работает, по сути, как Анонимайзер, т.е. документ с сайта "забирает" он, а не вы. Правда, есть некоторые немаловажные отличия, а именно:

- от cookies вас прокси не избавляет (избавьте от них себя сами, сделайте файл cookies. txt read-only или отключив (Disable All Cookies, Запретить использование Cookiese) их использование в Internet Explorer 4.0 и все дела!);

- прокси сервер работает как с HTTP, так и с FTP, что дает возможность анонимизировать посещение не только Web сайтов, но и FTP архивов;

- IP адрес вашего родного прокси сервера, т.е. того, пользование которым обеспечивает ваш провайдер, все равно отражает имя вашего домена или, по крайней мере, его примерное географическое положение.

Последний пункт приводит нас к следующему выводу: если вам очень важно остаться анонимным при работе с каким-нибудь сайтом, или при чтении и отправке почты с использованием браузера (т.е. тип сервиса, предлагаемый Hotmail), используйте не свой прокси сервер, а чужой.

Большинство прокси серверов ограничивают доступ на основании IP адреса, с которого происход обращение. Иными словами, если вы пользуетесь провайдером Demos, то прокси сервер Glasnet вас к себе попросту не пустит. Но к счастью, в сети всегда можно найти "добрый" прокси, владельцы которого либо открыто заявляют о его доступности для всех желающих (например этот), либо прокси, который по той или иной причине не ограничивает доступ только своим доменом, о чем широкой публике не известно, например:

noc. uncu. edu. ar: 8080

proxy. co. rmit. edu. au: 8080

conan. gocis. bg: 8080

proxy. intermedia. cl: 8080

webcache. ms. mff. cuni. cz: 8080

proxye1-atm. maine. rr. com: 8080

infosun-fd. rus. uni-stuttgart. de: 8080

linux. softec. es: 8080

nivel. ttaol. fi: 8080

proxy. galactica. it: 8080

www. go. com. jo: 8080

zip-translator. dna. affrc. go. jp: 30001

cvs2. kyunghee. ac. kr: 8080

magicall2. dacom. co. kr: 8080

proxy1. jaring. my: 3128

mpls. cache. mr. net: 3128

w3cache. us. edu. pl: 8080

sunsite. icm. edu. pl: 8080

proxy. qatar. net. qa: 8080

bill. ostrabo. uddevalla. se: 8080

proxy1. turnet. net. tr: 8080

proxy2. turnet. net. tr: 8080

episd. elpaso. k12. tx. us: 8080

proxy. telekom. yu: 8080

proxy. cybergate. co. zw: 8080

svc. logan. k12. ut. us: 8001

www. archmate. com. tw: 3128

www. anonymizer. com: 8080

http: // proxy. emirates. net. ae/proxy. pac (AUTOCONFIG)

Обновленный список анонимных Proxy серверов можно всегда найти на http: // www. lightspeed. de/irc4all/eindex. htm.

Для настройки браузера в Netscape Navigator зайдите в Options=>Network Preferences=>Proxies=>Manual Proxy

Configuration=>View и введите указанные значения. В MS Internet

Explorer аналогично. Проделав эту нехитрую операцию, вы сможете путешествовать по сети, оставляя след например как болгарский или американский пользователь, но... тут есть один очень важный момент.

Далеко не все прокси серверы являются полностью анонимными.

Некоторые из них позволяют администратору сайта, который вы посещаете с использованием прокси, при желании определить IP адрес, с которого происходит обращение к прокси, т.е. ваш реальный IP адрес.

Проверьте свой прокси на предмет его полной или неполной анонимности:

http: // www. tamos. com/bin/proxy. cgi Если вы получите сообщение Proxy server is detected! - ваш прокси имеет "дыру", и вам будет предоставлена информация о вашем реальном IP адресе, как впрочем и об IP адресе прокси сервера, который вы используете. Если же сообщение гласит Proxy server is not detected - все в порядке! Рекомендуется периодически (не реже чем раз в месяц) проверять те прокси с которыми в работаете на анонимность.

В заключение еще несколько соображений касательно использования прокси серверов. Работа через далеко расположенный прокси снижает скорость передачи данных и время ожидания. Кроме того, автор НЕ рекомендует использовать приведенные выше адреса прокси, поскольку если все читатели станут их использовать, то очень скоро удовольствие кончится и доступ к ним будет закрыт (если уже не закрыт). Найдите свой прокси сами, это несложно. Автор нашел эти адреса за 5 минут. В Альтависте наберите ключевые слова, что-нибудь вроде proxy+server+configuration+Netscape, и вы получите список страниц, где провайдеры рассказывают своим пользователям, как настроить их браузеры для работы с прокси. Пробуйте все подряд, на пятый или седьмой раз вас ждет удача - прокси согласится с вами работать.

Способ 3: Стирайте кэш Большинство WWW клиентов сохраняют в специальной директории (кэше) все те места в Интернет где вы были.

В целях вашей безопасности целесообразно периодически (скажем либо каждый день, либо раз в неделю) стирать содержимое кэша (лучше использовать невосстановимые методы стирания информации, например с помощью программы Kremlin 2.21). В Internet Explorer 4.0 (лучшем на наш взгляд WWW клиенте) он располагается в директории:

\Windows\Temporary Internet Files\

Специально для параноиков А ведь разные анонимизаторы можно выстраивать в цепи! Конечно, нельзя через прокси сервер обратиться к другому прокси серверу, чтобы тот зашел за вас на какой-нибудь сайт, но вот через прокси к Анонимайзеру обратиться можно. А можно еще через Анонимайзер опять к самому Анонимайзеру... Ух, даже дух захватывает от обилия комбинаций.

Фантазируйте!

СОЗДАНИЕ WWW-САЙТОВ

WWW-сайты, или проще домашние странички пользователей могут создаваться с разными целями. Одни например захотят разместить фото своей любимой девушки, а другие (как например мы) будут использовать их с целью пропаганды и распространения полезных материалов (в т. ч. и для акций информационной войны).

Но чтобы избежать неприятностей от власть имущих (или банально -

от своего провайдера) целесообразно придерживаться некоторых рекомендация, перечисленных ниже.

1. ВЫБИРАЙТЕ ТОЛЬКО ЛУЧШЕЕ

На сегодняшний день для создания своих сайтов представляют интерес следующие бесплатные службы:

http: // www. weekend. ru (ftp: // ftp. weekend. ru) - Отечественный узел, дают 10 Мб бесплатного места, обновление по FTP, необходим существующий адрес E-Mail.

http: // www. bar. ru (ftp: // ftp. bar. ru) - Отечественный узел, дают 10 Мб бесплатного места, обновление по FTP, необходим существующий адрес E-Mail.

http: // www. geocities. com (ftp: // ftp. geocities. com) - дают 6 Мб бесплатного места, обновление по WWW или по FTP, требуется существующий адрес E-Mail. Пожалуй это самый надежный и популярный узел. Но здесь не так просто получить адрес, т. к. приходится часами бродить по разным директориям в поисках заветного слова vacant.

Недавно в одной из телеконференций Usenet мы узнали способ как обойти такое ограничение. Итак, все что от вас требуется так это загрузить вот этот URL (в одну строчку естественно):

http: // www. geocities. com/cgi-bin/homestead/new\_app? hood=Athens/Academy

&addr=2470

Далее система предложит Вам зарегистрироваться, а в конце скажет что мол этот адрес (2470) занят и в замен предложит на выбор кучу других свободных, вот и все дела. Более того, чтобы попасть в желанное место - hood и addr могут быть любыми на ваш вкус!

http: // xoom. com (ftp: // ftp. xoom. com) - дают 5 Мб бесплатного места, обновление по FTP, необходим существующий адрес E-Mail.

http: // www. tripod. com (ftp: // ftp. tripod. com) - дают 5 Мб бесплатного места, обновление по FTP, необходим существующий адрес E-Mail.

2. ДУБЛИРУЙТЕ СВОИ САЙТЫ

В особенности это касается тех кто собирается распространять материалы противоречащие законам власть имущих.Т. е. лучше всего создавать несколько (2-5) своих страничек с одинаковым содержанием, но на разных серверах. Тогда вас будет труднее прикрыть. Помните что хакерские сайты как правило живут не больше недели. Но опять-таки уже имея сайт не составит особых проблем выложить его в другом месте.

3. ИСПОЛЬЗУЙТЕ БЕСПЛАТНЫЙ E-MAIL

Практически на всех узлах, при регистрации своего сайта необходимо иметь существующий E-Mail адрес. Поэтому следует заранее запастись десятком-другим разных адресов у разных бесплатных провайдеров (например в USA. NET и (или) в Hotmail). Здесь следует учитывать те рекомендации что мы давали в разделе ВАШ ВТОРОЙ АДРЕС.

4. ПРИ РЕГИСТРАЦИИ ВВОДИТЕ ТОЛЬКО ВЫМЫШЛЕННЫЕ ДАННЫЕ

Во всех системах для того, чтобы получить бесплатное место необходимо ввести много всяких данных о себе (ФИО, пол, возраст, страну, адрес, хобби и т.д.). Правда надо сказать что РЕАЛЬНО никто эти данные скорее всего не проверяет, мы всегда вводили самые нелепые данные и все проходило. НО лучше всего выдумать какую либо фамилию (лучше конечно не Иванов и Петров и скажем Никольский, Левашов или что-то еще) и использовать телефонные базы типа КОТИК, или их Online версию для узнавания недостающих данных:

http: // www. xland. ru: 8088/tel\_win/owa/tel. form

Выберите любого Левашова (или кого там еще) и смело вписывайте его данные при регистрации. Более того необязательно указывать что вы из Росси, можете указать что вы например John Smith из Штатов или из Албании... Советуем при каждой новой регистрации использовать новые имена, адреса, страны и т.д.

5. ИСПОЛЬЗУЙТЕ АНОНИМНЫЙ ПРОКСИ-СЕРВЕР ИЛИ АНОНИМАЙЗЕР.

Этой рекомендации целесообразно придерживаться всегда, даже при обычной работе с Интернетом. Подробнее см. выше.

6. ИСПОЛЬЗУЙТЕ АНОНИМНЫЙ ПРОКСИ-СЕРВЕР ПРИ РАБОТЕ С FTP.

При загрузке (обновлении) своего сайта по FTP необходимо также использовать анонимный proxy-сервер. Как правило в установках FTP-клиента его надо устанавливать в так называемый режим Passive.

7. ОТКЛЮЧИТЕ ИСПОЛЬЗОВАНИЕ COOKIES

Этой рекомендации целесообразно придерживаться всегда, даже при обычной работе с Интернетом. Подробнее см. выше.

8. РЕГИСТРИРУЙТЕСЬ В ПОИСКОВЫХ СИСТЕМАХ

Для того чтобы о вашем сайте смогли узнать другие люди есть два верных способа. Первый: необходимо в какой-либо (в одной или в нескольких) конференции Usenet (FidoNet) периодически давать рекламу своего сайта (например в конференции FIDO7. RU. INTERNET. WWW). Второй: необходимо зарегистрировать свой сайт в известных поисковых системах, как правило, необходимый пункт регистрации называется Add URL (добавить URL, добавить ресурс и т.д.). При регистрации у вас могут либо спросить только URL и система сама проиндексирует его за несколько дней, либо еще и название ресурса, владельца, тематику и т.д. В любом случае все данные о владельце ресурса целесообразно давать вымышленные, полученные например из телефонных баз типа КОТИК, либо можно воспользоваться Online версией этой базы:

http: // www. xland. ru: 8088/tel\_win/owa/tel. form

Примеры поисковых систем и каталогов ресурсов достойных внимания:

http: // www. search. ru/ - Поисковая система по русским ресурсам Интернет.

http: // www. rambler. ru - Русская поисковая система (и каталог ресурсов) RAMBLER.

http: // www. stars. ru - Каталог ресурсов Созвездие Интернет. При регистрации требуют имя и телефон владельца ресурса, но т. к. никто его проверять не будет достаточно воспользоваться любым, полученным из систем типа КОТИК.

http: // www. ru - Каталог ресурсов Russia on the Net.

http: // www. altavista. digital. com - одна из самых популярных буржуйских поисковых машин. При регистрации требуется только URL.

http: // www. infoseek. com - популярная буржуйская поисковая машина.

При регистрации необходимо по E-Mail выслать свой URL.

Вместо того чтобы оповещать каждую поисковую машину вручную, не помешает зарегистрировать свой сайт при помощи бесплатной службы представления. Попробуйте обратиться в службы Submit It

http: // www. submit-it. com/, AddURL http: // www. addurl. com/ или 123

Add-It http: // www.123add-it. com/.

9. СОВЕТЫ ПО СОЗДАНИЮ ДОМАШНИХ СТРАНИЦ

1. Не больше пяти позиций на каждом уровне! Количество вариантов на каждом уровне каталога не должно превышать пяти. Если их получается больше, сгруппируйте позиции и создайте подкаталоги.

2. Не больше трех уровней! Каждый элемент информации должен быть доступен с трех щелчков мышью.

3. Не больше 30K! Размер каждой загружаемой страницы не должен превышать 30К. Если ваша страница требует длительной загрузки, предупредите об этом посетителей. Избегайте крупных изображений и апплетов, иначе они потеряют терпение и уйдут на другой сайт.

4. Не раздувайте цветовую палитру! Следует воздержаться от широкого использования цвета в текстовых документах. Каждый дополнительный цвет увеличивает размер файла. Начните с нескольких цветов и добавляйте новые только по мере необходимости.

5. Делайте изображения гладкими! Пользуйтесь функцией anti-aliasing, чтобы придать изображениям привлекательность и уменьшить размер файлов.

6. Соблюдайте меру! Избегайте пестрых, многоэлементных фоновых изображений: они сильно затрудняют чтение ваших страниц. Если необходимо следовать определенному стилю, существенно ослабьте контрастность и увеличьте яркость.

7. Не используйте много шрифтов! Использования огромного количества шрифтов сильно затрудняет чтение ваших страниц, а также создает впечатление вашего непрофессионализма.

8. Придерживайтесь стандартного размера! Составляйте крупные изображения из более мелких. Несколько маленьких картинок загружаются значительно быстрее, чем одна большая.

9. Не загадывайте! Если ваша страница пока еще в стадии разработки, не акцентируйте это. Вид дорожного знака Under Construction всем давно приелся. Если вы вносите что-то новое, просто добавьте это - без плоских шуток.

10. Давайте эскизы! Если вы помещаете на свой сайт каталог изображений, пользуйтесь не текстовыми описаниями, а эскизами. Они быстро загружаются и несут в себе больше информации, чем слова.

11. Пользуйтесь тегами! Для ускорения загрузки страниц применяйте в изображениях теги HEIGHT, WIDTH и ALT.

12. Пользуйтесь MS Front Page 98! Для создания своего сайта лучше всего использовать самый популярный и интуитивно понятный редактор - Microsoft Front Page 98. Помните - когда вы делаете ссылку (hyperlink) с одной странички на другую (или на какой-либо файл), то все что должно быть в этой ссылке - это имя странички или файла (например name. htm) а структуру которую ставит Front Page, типа file: // путь\_к\_файлу/name. htm надо удалять, иначе ничего не будет работать.

13. Помните об именах! Помните что index. htm INDEX. HTM Index. Htm разные файлы с точки зрения операционной системы UNIX (стоящий у большинства бесплатных служб). Поэтому чтобы избежать путаницы при создании сайтов рекомендуем придерживаться для всех файлов сайта - имен с маленькими буквами (index. htm).

### 11.3. По FTP без следов

Путешествуя по Интернету, мы часто не думаем о том, что оставляем следы своих посещений каждый раз, когда заходим на какой-либо ftp сайт. Стандартные log-файлы любопытных владельцев способны узнать о вас многое, и прежде всего ваш IP адрес, что равнозначно например тому что узнали ваш телефон.

Существует несколько способов защиты от подобных посягательств.

Способ 1: Прокси Анонимизировать путешествие по сети можно с помощью прокси сервера. Прокси сервер работает, по сути, как Анонимайзер, т.е. документ с сайта "забирает" он, а не вы.

Большинство прокси серверов ограничивают доступ на основании IP адреса, с которого приходит обращение. Иными словами, если вы пользуетесь провайдером Demos, то прокси сервер Glasnet вас к себе попросту не пустит. Но к счастью, в сети всегда можно найти "добрый" прокси, владельцы которого либо открыто заявляют о его доступности для всех желающих (например этот), либо прокси, который по той или иной причине не ограничивает доступ только своим доменом, о чем широкой публике не известно, например:

noc. uncu. edu. ar: 8080

proxy. co. rmit. edu. au: 8080

conan. gocis. bg: 8080

proxy. intermedia. cl: 8080

webcache. ms. mff. cuni. cz: 8080

proxye1-atm. maine. rr. com: 8080

infosun-fd. rus. uni-stuttgart. de: 8080

linux. softec. es: 8080

nivel. ttaol. fi: 8080

proxy. galactica. it: 8080

www. go. com. jo: 8080

zip-translator. dna. affrc. go. jp: 30001

cvs2. kyunghee. ac. kr: 8080

magicall2. dacom. co. kr: 8080

proxy1. jaring. my: 3128

mpls. cache. mr. net: 3128

w3cache. us. edu. pl: 8080

sunsite. icm. edu. pl: 8080

proxy. qatar. net. qa: 8080

bill. ostrabo. uddevalla. se: 8080

proxy1. turnet. net. tr: 8080

proxy2. turnet. net. tr: 8080

episd. elpaso. k12. tx. us: 8080

proxy. telekom. yu: 8080

proxy. cybergate. co. zw: 8080

svc. logan. k12. ut. us: 8001

www. archmate. com. tw: 3128

www. anonymizer. com: 8080

http: // proxy. emirates. net. ae/proxy. pac (AUTOCONFIG)

Обновленный список анонимных Proxy серверов можно всегда найти на http: // www. lightspeed. de/irc4all/eindex. htm.

Для настройки FTP клиентов как правило прокси-сервер надо установить в passive режим. Проделав эту нехитрую операцию, вы сможете путешествовать по сети, оставляя след как болгарский или американский пользователь, но... тут есть один очень важный момент.

Далеко не все прокси серверы являются полностью анонимными.

Некоторые из них позволяют администратору сайта, который вы посещаете с использованием прокси, при желании определить IP адрес, с которого происходит обращение к прокси, т.е. ваш реальный IP адрес.

Проверьте свой прокси на предмет его полной или неполной анонимности:

http: // www. tamos. com/bin/proxy. cgi Если вы получите сообщение Proxy server is detected! - ваш прокси имеет "дыру", и вам будет предоставлена информация о вашем реальном IP адресе, как впрочем и об IP адресе прокси сервера, который вы используете. Если же сообщение гласит Proxy server is not detected - все в порядке! Рекомендуется периодически (не реже чем раз в месяц) проверять те прокси с которыми в работаете на предмет анонимности.

В заключение еще несколько соображений касательно использования прокси серверов. Работа через далеко расположенный прокси снижает скорость передачи данных и время ожидания. Кроме того, автор НЕ рекомендует использовать приведенные выше адреса прокси, поскольку если все читатели станут их использовать, то очень скоро удовольствие кончится и доступ к ним будет закрыт (если уже не закрыт). Найдите свой прокси сами, это несложно. Автор нашел эти адреса за 5 минут. В Альтависте наберите ключевые слова, что-нибудь вроде proxy+server+configuration+Netscape, и вы получите список страниц, где провайдеры рассказывают своим пользователям, как настроить их браузеры для работы с прокси. Пробуйте все подряд, на пятый или седьмой раз вас ждет удача - прокси согласится с вами работать.

Способ 2: Стирайте содержимое кэша Большинство FTP клиентов сохраняют в специальной директории все те места в Интернет где вы были (а иногда сохраняют и нешифрованные имена и пароли).

В целях вашей безопасности целесообразно периодически (скажем либо каждый день, либо раз в неделю) стирать содержимое кэша. Например в Bullet Proof FTP (лучшей на наш взгляд программе, ее можно скачать на http: // www. bpftp. com) он располагается в директории: Cache.

Лучше производить невосстановимое стирание, например с помощью программы Kremlin 2.21.

### 11.4. Безопасность e-mail

Электронная почта, как впрочем и обычная, является важным атрибутом нашей безопасности, инструментом обмена информацией частного характера. Но она немедленно перестает быть таковым, если нарушаются три важных условия. Первое: текст сообщения доступен только отправителю и адресату. Второе: уверенность в том, что полученное письмо принадлежит тому человеку, чья подпись стоит под этим письмом.

Третье: возможность отправить письмо, оставшись, в случае необходимости, анонимным. Обсуждение первого вопроса выходит за рамки этой статьи, поскольку относится к области гражданской криптографии, что требует отдельного разговора. Мы же рассмотрим последние два вопроса.

Но сначала мы предлагаем вашему вниманию статью Леонида Коника "ФСБ приглядит за электронной почтой" чтобы вы сами могли убедиться в реальной необходимости защиты своей безопасности:

"Вслед за сотовыми и пейджинговыми операторамиї Петербурга органы ФСБї добрались и до компаний, предоставляющих услуги доступа к компьютерным сетям (провайдеров).

Компании обязаны обеспечить спецслужбам возможность контроля любых передаваемых данных, в частности - сообщений, посылаемых по электронной почте. Так же, как и в случае с сотовыми и пейджинговыми фирмами (см. "ДП" N 43/96), провайдеры обязаны за свой счет создать такие возможности и предоставить Федеральной службе безопасности соответствующую аппаратуру для перехвата информации. Эта аппаратура (выносной пульт) выводится непосредственно в органы ФСБ, поэтому какой-либо контроль со стороны компаний невозможен.

Представители компаний-провайдеров в один голос говорят о "возврате к старым временам" и с сожалением констатируют, что отныне не смогут декларировать конфиденциальность пересылки данных.

Так назначено судьбой В отличие от сотовых и пейджинговых собратьев, провайдеры пока не получили директивы от Минсвязи. Но, по словам генеральных директоров компаний Александра Григорьева ("Дукс") и Сергея Федорова ("Нева Линк"), "люди в штатском" уже наведывались к ним в офисы.

Собственно, в лицензиях провайдеров всегда присутствовала фраза:

"Сеть должна отвечать эксплуатационно-техническим требованиям по обеспечению и проведению оперативно-розыскных мероприятий в соответствии с Законом "Об оперативно-розыскной деятельности (ОРД) в РФ". Однако реально до сих пор никто не требовал соблюдения этого пункта.

Сейчас Госсвязьнадзор - ведомство, контролирующее деятельность компаний связи, ведет переоформление лицензий провайдеров. Условием переоформления лицензии является строгое выполнение всех ее пунктов, в том числе и о внедрении аппаратуры контроля.

Некоторые компании уже выполнили все требования лицензии. Они внесли доработки в используемое программное обеспечение, а также снабдили органы ФСБї выносным пультом в виде компьютера. Формально компьютеры отдаются не безвозвратно, а во "временное пользование".

Компании надеются, что им компенсируют хотя бы часть затрат.

Служба дни и ночи Генеральный директор компании "Петерлинк" Анатолий Листвинский заметил, что многие провайдеры в Петербурге используют каналы связи сети Relcom. Поэтому проще и дешевле было бы не озадачивать каждого провайдера проблемами розыскной деятельности, а в складчину подсоединить один выносной пульт прямо к петербургскому узлу Relcom на Марсовом поле.

Технические специалисты компьютерных фирм говорят, что перехвату поддается лишь электронная почта (идущая в режиме off-line). Для того чтобы "поймать" сообщение, посылаемое по сети Internet в режиме прямого доступа (on-line), необходимо вести контроль постоянно: никто не может предсказать, в какой момент времени отправит сообщение именно интересующий спецслужбу человек. Постоянный контроль требует мобилизации огромных сил, к тому же он противоречит Закону об ОРД. В нем говорится о том, что проведение оперативно-розыскных мероприятий, затрагивающих охраняемые законом тайну переписки, телеграфных сообщений, телефонных и иных переговоров, допускается лишь для сбора информации о лицах, подготавливающих, совершающих или совершивших тяжкие преступления, и только с санкции прокурора или при наличии судебного решения.

Алекс - Юстасу Помимо законов РФ "Об ОРД" и "О связи" в открытой печати не было опубликовано ни одного приказа Минсвязи или ФСБї об организации работ по обеспечению оперативно-розыскных мероприятий на сетях связи. Между тем Конституция РФ (ст.15 разд.3) гласит: "Любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения".

В сложившейся ситуации у провайдеров существует три варианта действий: отказаться от бизнеса, пытаться отстоять свои права (хотя бы на компенсацию расходов) или подчиниться. Практически все предпочитают третий путь. Провайдеры уверены, что весть о доступе спецслужб к электронной почте не отпугнет клиентов. "В отличие от абонентов сотовых и пейджинговых компаний, наши клиенты вряд ли передают какие-либо секреты. Компьютерные сети - это просто средство общения", - ответственно заявляют они. "

А теперь от теории перейдем к практике.

1. ПОЛУЧЕНИЕ E-Mail

Иногда у пользователя возникает ситуация, в которой ему хотелось бы выявить реального автора полученного сообщения. Например, вы получили сообщение от вашей жены, в котором она пишет, что уходит к другому. Вы можете либо вздохнуть с облегчением, выпить на радости рюмку-другую, и отправиться с друзьями на дачу праздновать это событие, либо попытаться выяснить, не является ли это шуткой ваших друзей.

Ваши умные друзья могли легко изменить поле From в отправленном сообщении, поставив туда вместо своего обратного адреса хорошо известный вам адрес вашей жены, например masha@flash. net. Как это делается, можно прочесть ниже, в разделе "ОТПРАВКА E-Mail". Так что стоящая перед нами задача сводится к следующему: соответствует ли указанный адрес отправителя адресу, с которого в действительности было отправлено сообщение.

Итак, каждое электронное сообщение содержит заголовок (header), представляющий из себя служебную информацию о дате отправления сообщения, названии почтовой программы, IP адресе машины, с которой было отправлено сообщение, и т.п. Большинство почтовых программ по умолчанию не отражают эту информацию, но ее всегда можно просмотреть, либо открыв файл, содержащий входящую почту, с помощью любого текстового редактора, либо использовав функцию почтовой программы, позволяющую просматривать служебные заголовки, которая, как правило, называется Show all headers. Что же мы видим? А вот что:

Received: by geocities. com (8.8.5/8.8.5) with ESMTP id JAA16952

for; Tue, 18 Nov 1997 09: 37: 40 - 0800 (PST)

Received: from masha. flash. net (really [209.30.69.99])

by endeavor. flash. net (8.8.7/8.8.5) with SMTP id LAA20454

for; Tue, 18 Nov 1997 11: 37: 38 - 0600 (CST)

Message-ID: <3471D27E.69A9@flash. net>

Date: Tue, 18 Nov 1997 11: 38: 07 - 0600

From: masha@flash. net

X-Mailer: Mozilla 3.02 (Win95; U)

MIME-Version: 1.0

To: petya@geocities. com

Subject: I don't love you any more, you \*&$%#!!!!

Да, много всякого. Не вдаваясь в технические подробности, в общих чертах: заголовки Received сообщают о пути, который прошло сообщение в процессе пересылки по сети. Имена машин (geocities. com, endeavor. flash. net) указывают на то, что сообщение, скорее всего, пришло к вам в geocities. com из домена вашей жены flash. net. Если имена машин не имеют ничего общего с flash. net (например, mailrelay. tiac. net), это повод задуматься о подлинности сообщения. Но самая главная строка для нас - последняя из строк, начинающихся со слова Received:

Received: from masha. flash. net (really [209.30.69.99])

Она отражает имя машины (masha. flash. net) и уникальный IP адрес, с которого было отправлено сообщение. Мы видим, что домен (flash. net) соответствует адресу вашей жены. Впрочем, ваши умные друзья могли подделать и строку masha. flash. net (в Windows 95 это делается через Control Panel=>Network=>TCP/IP Properties=>DNS Configuration, указав masha и flash. net в полях Host и Domain соответственно), поэтому для нас важно определить имя, соответствующее данному IP адресу: 209.30.69.99.

Для определения имени, соответствующего цифровому адресу, можно воспользоваться одной из доступных программ, например WS Ping32 (http: // www. glasnet. ru/glasweb/rus/wsping32. zip), а лучше CyberKit (http: // www. chip. de/Software/cyber. zip). Набрав цифровой адрес, мы даем команду NS LookUp (Name Server Lookup) и смотрим на полученный результат. Если имя определилось, то дальше все просто: если вы получили что-нибудь вроде ppp303. flash. net или p28-dialup. flash. net, то сообщение отправлено вашей женой (или кем-то, имеющим счет в Flashnet, но тут вы уже бессильны что-либо выяснить). Если нечто весьма далекое от flash. net - она его скорее всего не посылала.

Бывают ситуации, когда адрес не определяется. Не отчаивайтесь: воспользуйтесь функцией TraceRoute из той же программы. Эта функция поможет проследить путь от вашей машины до указанного IP адреса. Этот адрес (он будет последним в списке узлов, через которые сигнал прошел от вашего компьютера до компьютера с указанным IP адресом) снова не определится, но последний из определившихся по имени узлов все-таки укажет на примерное географическое положение компьютера отправителя.

Еще более простым и изящным способом определения страны и даже названия провайдера или сети является использования этого адреса:

http: // www. tamos. com/bin/dns. cgi Итак, вы получили что-нибудь вроде Brasilian Global Network. Ваша жена не бывала последнее время в Бразилии? Нет??? Ну тогда она от вас и не уходила. Вас разыграли. Будьте бдительны!

2. ОТПРАВКА E-Mail

Заметим, что вполне добропорядочные граждане иногда хотят сохранить в тайне свою личность при высказывании своего мнения, скажем автору сайта, пропагандирующего фашизм, или президенту Лукашенко.

Вопросы приобретения второго (анонимного) электронного адреса вынесены в отдельную главу ВАШ ВТОРОЙ АДРЕС.

Remailer Римейлер - это компьютер, получающий сообщение, и переправляющий его по адресу, указанному отправителем. В процессе переадресовки все заголовки (headers), содержащие информацию об отправителе, уничтожаются, так что конечный получатель лишен всякой возможности выяснить, кто автор сообщения. Remailer'ов в сети много, некоторые из них позволяют указывать фиктивный адрес отправителя, большинство же прямо указывают в заголовке, что сообщение анонимно. Вы можете воспользоваться римейлером, послав сообщение по адресу remailer@replay. com, указав Subject: remailer-help. Вы получите файл с подробными инструкциями об отправке анонимных сообщений. Еще более простой способ - это отправиться по адресу: http: // www. replay. com/remailer/

Там расположен римейлер, позволяющий посылать сообщения прямо из WWW. На этом же сайте вы также можете воспользоваться цепочкой из ремейлеров, так что ваше сообщение пройдет через несколько компьютеров, каждый из которых старательно уничтожит все заголовки предыдущего, хотя автор и не рекомендует этого делать. Во-первых, одного римейлера вполне достаточно (если вы не параноик), во-вторых, сообщение может затеряться и не дойти до получателя, в-третьих, оно может идти очень долго. Пример полученного сообщения:

Date: Mon, 31 Mar 1997 12: 33: 23 +0200 (MET DST)

Subject: The rest is silence:

To: petya@glasnet. ru

From: nobody@REPLAY. COM (Anonymous)

Organization: Replay and Company UnLimited

X-URL: http: // www. replay. com/remailer/

X-001: Replay may or may not approve of the content of this posting

X-002: Report misuse of this automated service to abuse@replay. com

Выявить реального отправителя сообщения с использованием римейлера теоретически можно, но очень сложно. Практически невозможно.

На это способны лишь подлецы из разных там ФСБ, ФАПСИ, ЦРУ и им подобных, им придется запастись решением суда, чтобы римейлер открыл им требуемую информацию. А если вы использовали цепочку римейлеров, то им надо будет обойти всех римейлеров в цепочке. Но если вы к тому же при отправке через WWW интерфейс пользовались анонимным прокси-сервером и (или) анонимайзером, то шанс найти вас становиться еще намного меньше (да не забудьте еще отключить использование файлов Cookies).

Итак, первое апреля. Вы умираете от желания сообщить своему другу от имени его провайдера о том, что его счет закрыт за неуплату (сообщение с обратным адресом его провайдера). Описанные ниже способы хороши для розыгрышей, но мало пригодны, если вы хотите остаться действительно анонимны. Варианты таковы:

Использование вашей почтовой программы. Самый простой: поставьте в своей почтовой программе в поле Return Address любой адрес, и если получатель письма не станет изучать его header, то он останется в уверенности, что получил сообщение именного от того, чей адрес указан в поле From. Очень просто и очень мало надежно.

Использование специальной программы - анонимизатора. Таких программ несколько, попробуйте, скажем, AnonyMail (ftp: // ftp. tordata. se/www/hokum/amail10. zip). Вы заполняете поля From, To, Subject (тут все ясно), и поле Host, в котором вы должны указать имя хоста, через который будет отправлена почта. Поскольку протокол отправки сообщений SMTP не требует в подавляющем большинстве случаев какой-либо авторизации отправителя, вы смело можете воспользоваться практически любым именем хоста, желательно тем же, что имеет получатель вашей почты. Это затруднит определение подлинности сообщения для непродвинутого пользователя. Например, если вы хотите отправить письмо по адресу kiska@frontier. net, укажите в поле Host адрес frontier. net. Попробуйте отправить сообщение сначала самому себе. Недостатки: IP адрес вашей машины все-таки будет отражен в header. Кроме того, поле To в полученном сообщении превратится, скорее всего, в Apparently-To. Правда, мало кто обратит на это внимание.

Так что выбирайте подходящий для вас способ! Все вышеперечисленные способы вполне корректно работают и с русскими кодировками. Поскольку de facto стандартом для пересылки сообщений между разными компьютерами является KOI8-R, рекомендую использовать эту кодировку при посылке сообщений. Тогда ваше сообщение, скорее всего, будет правильно перекодировано почтовым компьютером получателя.

3. ВАШ ВТОРОЙ АДРЕС

Проблема защиты вашей частной жизни в сети ставит перед нами вопрос об обладании вторым (третьим... десятым) электронным адресом.

Его хорошо иметь там, где вашу почту не будут читать, и в том домене, географическая принадлежность которого "нейтральна". В общем, все те же требования, что и ко второму паспорту и гражданству. Такой адрес защитит вас от попыток выяснения вашей личности, даст вам возможность предоставлять разные адреса разным корреспондентам в зависимости от их статуса, избавит от необходимости извещать всех ваших корреспондентов о вашем новом адресе, если вы сменили провайдера или переехали в другую страну.

Существует довольно много служб, позволяющих бесплатно получить второй электронный адрес. По способу отправки и получения почты эти службы подразделяются на 3 основных типа.

Тип 1. Пример: http: // www. europe. com. Службы этого типа дают пользователю возможность перенаправлять полученную на новый адрес корреспонденцию по адресу, указанному пользователем. Таким образом у вас уже должен быть какой-либо адрес, т. к. "напрямую" (с использованием протокола POP3) почту забрать нельзя. Отправка почты осуществляется напрямую через хост этой службы (протокол SMTP).

Существует, правда, 60-дневный период, в течение которого можно пользоваться и почтовым ящиком (POP3), после истечения периода - за деньги. Вы самостоятельно выбираете userid, а также домен из нескольких (бесплатно) или многих (платно) предложенных имен, например: iname. com, writeme. com, girls. com, boys. com etc. Выполнив несложные инструкции, вы становитесь обладателем нового адреса, скажем ohhhhhhh@girls. com. В процессе заполнения анкеты вы указываете свою страну (например, Албания), имя (ну тут вариантов мало, все пишут Иван Петров или Петр Иванов), и адрес, на который должна пересылаться вся приходящая корреспонденция. Этот адрес впоследствии легко изменить, это потребуется, когда вы смените провайдера или уедете жить в княжество Лихтенштейн. Вот и все! Недостаток: ваш настоящий адрес известен сотрудникам службы.

Тип 2. Службы этого типа дают пользователю возможность как отправлять почту напрямую, так и получать ее (POP3 и SMTP), так что вам не нужен первичный адрес, либо он потребуется всего лишь раз, при открытии счета. Для этих целей можно использовать адрес вашего приятеля или адрес в Hotmail (см. ниже). Пример:

http: // www. geocities. com или http: // www. netaddress. com (последняя имеет даже еще более широкие возможности, позволяя помимо POP3 и SMTP читать и отправлять почту из окна браузера, что позволяет отнести эту службу также и к Типу 3. Технология открытия счета примерно такая же.

Преимущество: ваш настоящий первичный адрес неизвестен, единственный "след", который вы оставляете, это ваш IP адрес, с которого происходит чтение и отправка почты. Службы также дают возможность перенаправлять почту на ваш первичный адрес, если есть такое желание. Кроме того, практически вашу почту смогут прочесть только администраторы службы, а не ваш московский провайдер или ФАПСИ с ФСБ, хотя теоретически и это возможно.

Тип 3. Принципиально другой тип службы. Чтение и отправка почты происходят не с использованием вашей любимой почтовой программы, а прямо в окне вашего браузера. Пример: http: // www. hotmail. com.

Переадресовка на ваш первичный адрес невозможна. Преимущества: можно читать почту из любого места, где есть доступ в WWW, будь то другая страна или Интернет-кафе в Южном Бутово, плюс опять же сложности слежки за вашей почтой. Недостаток: не очень удобно работать с Attachements, посылать можно не более одного за раз, и только с использованием Netscape Navigator 2.0 и выше или Internet Explorer 4.0 и выше. Совсем не сложно, зато как удобно! Стоит также отметить:

http: // www. mailcity. com - которая позволяет создавать неограниченное количество копий и слепых копий адресов, эта программа на основе Web - воплощенная мечта для тех, кто занимается массовой рассылкой писем. И в заключение еще одно важное соображение касательно privacy. При отправке почты через любую из этих служб заголовок сообщения содержит IP адрес, с которого отправлено сообщение. Даже Hotmail это делает. Но если при отправке сообщения с использованием почтовых служб первых двух типов скрыть свой реальный IP адрес нельзя (это связано с самим принципом работы протокола SMTP), то при использовании почтовой службы третьего типа, т.е. при отправке почты из окна браузера, лазейка все-таки есть, что позволят говорить о том, что почтовый адрес третьего типа можно сделать практически полностью анонимным, достаточно лишь воспользоваться одним из способов анонимизации своих путешествий по сети. Хотите знать как? Читайте раздел ПО WWW БЕЗ СЛЕДОВ. Другим способом отправить почту полностью анонимно остается использование римейлеров (см. выше).

4. ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ ПО E-MAIL

Да, действительно, а зачем устанавливать личность по известному адресу электронной почты? А зачем ставят автоматический определитель номера (АОН) на телефон? А зачем существует база данных, в которой по телефону можно определить имя и адрес человека? Много причин, начиная от чистого развлечения (кто не хочет поиграть в Пинкертона?) до желания выяснить, кто это с адресом someone@oxford. edu поздравляет вас каждый год с днем рожденья и признается в любви. Кроме того, описывая методики такого поиска информации, автор хотел бы показать читателю, как уязвима (или неуязвима) его privacy в сети.

Заметим сразу, что способы выяснения личности по известному адресу e-mail весьма разнообразны, причем ни один из них не гарантирует успеха. Обратная задача решается довольно тривиально: множество e-mail directories (Four11, WhoWhere etc) позволяют найти по имени человека его адрес (если, конечно, он сам того захотел). Мы же рассмотрим задачу нетривиальную.

Finger

Воспользовавшись программой WS Ping32

(http: // www. glasnet. ru/glasweb/rus/wsping32. zip), а лучше CyberKit

(http: // www. chip. de/Software/cyber. zip) вы получите возможность как бы направить ваш указательный палец на любой адрес электронной почты и спросить "А это кто? ". Иногда вам могут ответить. Итак, мы задаем адрес (выдуманный автором) someone@oxford. edu, получаем:

Login name: someone In real life: John McCartney

Directory: /usr/someone Shell: /usr/bin/csch

Last login Fri Aug18, 1995 on ttyv3 from dialup. oxford. edu

No mail

No plan

OK, someone@oxfrord. edu принадлежит John McCartney. Дело сделано, хотя очень часто вы не получите никакого результата, либо строку следующего содержания:

Forwarding service denied

или:

Seems like you won't get what you are looking for;)

Тоже самое можно сделать, не перекачивая указанные программы (хотя они и очень полезны и пригодятся не раз), а пойдя по этому адресу в WWW, где расположен Web интерфейс, позволяющий получить тот же самый результат (http: // web. lm. com/sfw. html).

Следует заметить, что выполнение Finger с использованием имени хоста (в данном случае oxford. edu) может не принести никакого результата, в то время как использование видоизмененного (альтернативного) имени хоста результат даст. Как узнать альтернативное имя хоста? Воспользуйтесь CyberKit, функция NS LookUp.

Введите имя www. oxford. edu и посмотрите на полученный результат. Он может содержать альтернативные имена хоста, называемые aliases, ну скажем panda. oxford. edu. Попробуйте someone@panda. oxford. edu, может сработать.

Иногда информация в ответ на finger-запрос может быть выдана только пользователю из того же домена, к которому принадлежит адрес, который вы хотите идентифицировать. Решение простое: найдите пользователя из искомого домена в Internet Relаy Chat (смотрите главу об IRC), и попросите его сделать finger запрос. Программа-клиент для IRC содержит функцию finger, так что никакой специальный софт человеку, к которому вы обратились, не потребуется.

Поиск в WWW.

Очень просто: наберите адрес в http: // www. altavista. digital. com и нажмите Find! Есть вероятность, что вы либо найдете домашнюю страницу искомого пользователя, либо упоминание о нем на других страницах. Там вполне может быть имя обладателя адреса, а может и фото, если повезет.

Поиск в Usenet.

Если человек с искомым адресом отправлял в какую-нибудь группу Usenet сообщение, то его можно разыскать по адресу. Для этого можно воспользоваться AltaVista (http: // www. altavista. digital. com), которая позволяет производить поиск во всех недавно отправленных в Usenet сообщениях. Заполните поле поиска искомым адресом прямо здесь (перед адресом необходимо написать from:. После нажатия кнопки Find откроется новое окно с результатами поиска.

Более предпочтительным вариантом является поиск в системе DejaNews (http: // www. dejanews. com), т. к. если искомый адрес не найден среди недавних сообщений, система предлагает поискать его среди старых. Поиск также можно произвести прямо с этой страницы (from: писать не нужно, просто адрес).

Поиск в E-mail Directories.

Службы, позволяющие разыскать электронный адрес человека по его имени, широко представлены в Интернете. Между тем эти же службы иногда можно использовать для выполнения обратной задачи. Зайдя на какую-либо из страниц:

http: // www. four11. com

http: // www. yahoo. com/search/people

http: // www. bigbook. com

http: // www. bigfoot. com

http: // www. bigyellow. com

http: // www. infospace. com

http: // www. abii. com/lookupusa/adp/peopsrch. htm

http: // www. looksmart. com

http: // www. switchboard. com

http: // www. whowhere. com

http: // www. dubna. ru/eros/ (поиск по русским ресурсам)

Можно не задавать имя человека, а задать лишь домен искомого адреса. Если пользователей, чьи адреса принадлежат к искомому домену, немного, то система в ответ на запрос выведет список всех таких людей, но, как правило, не более сотни и без указания части адреса, стоящей перед знаком @. Чтобы выяснить адрес целиком, придется следовать по ссылке для каждого имени, что займет много времени, если адресов много. Если же людей с таким доменом больше ста, то поиск таким способом теряет смысл. Другими словами человека из @aol. com или @netcom. com так не найдешь.

5. ЗАЩИТА ОТ SPAM

Для многих пользователей Интернет спам (рассылка всевозможно рекламы и мусора в ваш почтовый ящик) стал настоящим бедствием.

Основные рекомендации для защита от спама следующие:

- пишите письма в конференции Usenet исключительно с левых (бесплатных) адресов, потому что именно письма в конференции Usenet являются основной "засветкой" для спамеров. А если будет много спама, то такой адрес можно что называется выбросить и за пару минут сделать другой подобный;

- установите какую-либо программу фильтр для E-mail. Существует великое множество таких программ - все они доступны на таких бесплатных серверах как http: // www. shareware. com и http: // www. download. com.

6. ОПТИМАЛЬНЫ ВЫБОР ПОЧТОВОГО КЛИЕНТА

На наш взгляд оптимальным выбором является Microsoft Outlook Express 98 или The Bat 1.043 и выше.

Но, надо сказать, у Outlook Express есть и одна неприятная особенность (видимо так же один из "черных ходов" сделанных для спецслужб) - он хранит (даже когда письма уже стерты) все письма, какие только вы получали, удаляли или отправляли (хотя естественно вы это не замечаете). Поэтому периодически рекомендуем удалять (лучше невосстановимыми методами, например с помощью программы Kremlin 2.1) эти файлы. Они расположены в директориях:

\Windows\Aplication\Microsoft\Outlook Express\Mail\ - почта - здесь необходимо удалить все файлы с расширениями IDX и MBX.

\Windows\Aplication\Microsoft\Outlook Express\News\ - новости - здесь необходимо удалить все файлы с расширениями NCH.

### 11.5. Анонимность на IRC

Ну кто не знает про IRC, это гениальное изобретение, позволяющее с помощью программы-клиента mIRC (а еще лучше pIRCH), установленной на вашем компьютере, общаться в реальном времени и обмениваться файлами с любым человеком в Интернете! IRC настолько популярна, что многие люди проводят в IRC больше времени, чем бродя по WWW. И коль скоро для многих людей это часть жизни, следует подумать и о вашей безопасности в этой виртуальной жизни.

Вы - дичь Вас могут подстерегать разные опасности при работе в IRC по следующим причинам:

1. Возможность прослушивания того, что вы говорите другому человеку при общении один на один. Здесь все довольно просто: если вы считаете, что обсуждаемый вопрос конфиденциален, не пользуйтесь общением на канале, даже если кроме вас и вашего собеседника на нем никого нет. Не пользуйтесь командой /msg или окном query, что одно и то же. Вся информация проходит через IRC сервер и технически может быть записана. Вместо этого воспользуйтесь DCC (Direct Client to Client). При этом информация будет передаваться вашему собеседнику напрямую, минуя сервер, от которого можно даже отключиться после установления связи по DCC. В принципе, и эту информацию можно расшифровать на любом из узлов, через который установлена связь между вами и вашим собеседником, но это сложно. Если вы хотите быть уверены в полной приватности вашей беседы, воспользуйтесь методами, описанными в главе Защищенный разговор.

2. Сбор информации о том, на каких каналах вы находитесь, с последующей идентификацией вашей личности.

Итак, первое. Если вы хотите быть анонимны, не указывайте свой настоящий адрес e-mail в соответствующем поле в Setup. Во-вторых, станьте "невидимы". Это свойство позволяет вам оставаться необнаруженным при попытке любого пользователя, не знающего точное написание вашего nick, найти вас в IRC по имени вашего домена или userid (часть вашего e-mail, стоящая перед знаком @), используя команду /who или /names. (см. ниже). Это делается командой /mode $me +i, которая может быть для удобства включена в список команд, автоматически выполняемых при подключении (mIRC Options=>Perform). В последних версиях mIRC 5. \*\* надо просто поставить галочку напротив Invisible Mode в диалоговом окне Setup. В-третьих, не давайте свой адрес людям в IRC, в добропорядочности которых вы не уверены. Или, по крайней мере, давайте свой альтернативный адрес. Вот, пожалуй, и все, что можно сделать. В-четвертых отключите всевозможные ident в ваших IRC клиентах. А теперь рассмотрим, что и как другие люди в IRC могут о вас узнать (или вы о них).

Вы - охотник Оговорюсь, что мы будем исходить из предположения, что имя домена или IP адрес пользователя в IRC подделать очень сложно, и подавляющее большинство людей этим не занимаются, хотя такие методы и есть.

На ум приходят два метода: IP spoofing и использование специального прокси сервера, способного поддерживать IRC протокол.

Техника, называемая IP spoofing (обман IP), весьма сложна в применении. Хакерские сайты предлагают пользователям Windows 95 с версией Winsock 2.0 и выше несколько программ для подобных проделок.

1. Поиск пользователей по домену, имени, и userid. Довольно мощным средством поиска по какой-либо известной части информации о пользователе (или группе пользователей) является команда /who, о которой почему-то нет ни слова в mIRC'овском Help файле. Странно, правда. Делая запрос о пользователе командой /whois, мы обычно получаем примерно такой текст:

ShowTime ~mouse@ml1\_12. linknet. net \* May flower

ShowTime on #ircbar #newbies

ShowTime using Oslo-R. NO. EU. Undernet. org [194.143.8.106] Scandinavia Online AS End of /WHOIS list.

Команда /who позволяет задать маску для поиска пользователей по любой части их доменного имени, userid или имени (то, что в поле Real Name). Допустим, мы ищем людей из домена global. de. Синтаксис таков:

/who \*global. de\*

Или ищем всех пользователей из Сингапура:

/who \*. sg\*

Или мы уже общались с господином ShowTime, и хотим найти его опять:

/who \*mouse\*, или /who \*flower\*

Так же могут найти и вас, если вы не воспользуйтесь командой /mode $me +i, как было описано выше.

2. Определение адреса электронной почты. Задача довольно сложная, но иногда выполнимая. Начнем с "лобовой" атаки. Команда /ctcp ShowTime userinfo (или, проще, через меню) покажет нам e-mail address, указанный самим пользователем. Поскольку мало кто сообщает свой настоящий адрес, надежды на правдивый ответ мало. Если домен полученного адреса совпадает с тем, что следует за знаком @ в ответе, полученном на запрос /whois, то вероятность того, что адрес указан правдивый, повышается.

Следующая возможность - использовать информацию, содержащуюся в ответе на запрос /whois. Имя домена подделать крайне сложно, поэтому мы наверняка знаем, что пользователь ShowTime из домена linknet. net.

Это первый шаг. Часто вместо буквенной строки после знака @ следует цифровой IP адрес, который по той или иной причине не определился при подключении пользователя к серверу. Его можно попытаться определить командой /DNS ShowTime. Если результат получен, то переходим к следующему абзацу. Если нет, то попробуем еще один способ.

Воспользовавшись программой WS Ping32

(http: // www. glasnet. ru/glasweb/rus/wsping32. zip), или CyberKit

(http: // www. chip. de/Software/cyber. zip), сделаем TraceRoute с указанием цифрового адреса. Программа проследит путь от вашего IP адреса до искомого IP, принадлежащего ShowTime. Последний из определившихся по имени адресов укажет, скорее всего, на имя домена пользователя.

Едем дальше. У нас есть либо полное имя, соответствующее IP адресу пользователя под кличкой ShowTime (ml1\_12. linknet. net), либо, в худшем случае, только имя домена (linknet. net). В первом случае мы можем попытаться, воспользовавшись командой finger (либо в одной из двух вышеупомянутых программ, либо прямо в mIRC, где есть кнопка Finger прямо на Tool Bar'е), определить всех текущих пользователей из домена linknet. net. Для этого мы делаем finger адреса @linknet. Net (userid не указываем). При удачном стечении обстоятельств мы получим что-нибудь в этом роде:

Trying linknet. net

Attempting to finger @linknet. net

[linknet. net]

Login Name TTY When Where

root 0000-Admin console Fri 16: 27

henroam John Brown pts/1 Tue 10: 57 pckh68. linknet. net

pailead Jack White pts/2 Tue 11: 03 ml4\_17. linknet. net

oneguy Michael Lee pts/3 Tue 11: 08 ml1\_12. linknet. net

sirlead6 Joan Jackson pts/4 Tue 11: 05 ml4\_16. linknet. net

End of finger session

Вот он наш ml1\_12, принадлежит oneguy@linknet. net. Отметим, что иногда информация в ответ на finger-запрос может быть выдана только пользователю из того же домена, к которому принадлежит адрес, который вы хотите идентифицировать. Решение простое: найдите пользователя из искомого домена (/who \*linknet. net\*), и попросите его сделать finger запрос.

И в первом, и во втором случае есть еще одна возможность. Если "охотнику" известно реальное имя или фамилия искомого пользователя, можно послать figer-запрос в виде имя@домен или фамилия@домен.

Например, finger на John@some. net может нам дать список всех пользователей по имени John с их login'ами.

Вот, пожалуй, и все известные автору средства, которые есть у "охотника". А выяснив ваш e-mail адрес, "охотник" может выяснить и ваше реальное имя. Как? Читайте в разделе ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ

ПО E-MAIL.

### 11.6. Безопасность ICQ

ICQ - иначе Интернет-пейджер - стал для многих незаменимым средством оперативного общения с друзьями, коллегами и просто интересными людьми. Но технология ICQ такова (если не принять соответствующих мер) что вас легко могут идентифицировать (узнать ваш IP адрес). Существует несколько рекомендаций по защите от этого:

- при регистрации в системе ICQ ни в коме случае не указывайте вашего настоящего E-Mail, адреса, имени и т.д. (все данные должны быть вымышленными);

- не забудьте установить режим обязательной авторизации (вашего согласия) при попытках других пользователей сети добавить ваш UIN (персональный номер в сети ICQ) в свою записную книжку;

- отключите в настройках ICQ отображение вашего IP адреса и других идентификаторов. В противном случае - в сети довольно много шутников которые могут например напустить на вас Nuke Attack;

- никогда не используйте какие-либо дополнительные утилиты и русфикаторы для ICQ, все они, как правило, содержат в себе "троянцев";

- по возможности (если у вас получится) настройте ICQ для роботы через анонимный прокси-сервер.

### 11.7. Защита от NUKE ATTACK

В Интернете можно найти множество программ для т. н. Nuke Attack, Winnuke, Land Attack и пр. - большинство из этих программ осуществляют атаку по указанному IP адресу (чаще всего используя порт 139) что как правило вызывает зависание атакуемого компьютера. Сущность и сама возможность этих атак связана с особенностями протокола TCP/IP - мы не будем углубляться в эти дебри, а лишь кратко остановимся на способах защиты:

- Если Вы используете операционную систему Windows (95, 98 или NT) то все что Вам нужно так это периодически заглядывать в:

http: // www. microsoft. com

и скачивать свежие апдейты для своих операционных систем устраняющих подобные проблемы;

- также существует много бесплатных программ защищающих от подобных атак. Их можно поискать на бесплатных серверах программного обеспечения. Мы рекомендуем NukeNabber 2.9, его можно скачать на:

http: // www. download. com

Эта программа, позволит вам защититься от распространенных атак на 95 и NT через Интернет. Она прослушивает до 50 портов, которые чаще всего атакуются и дает вам достаточно информации, чтобы выследить нападающего. В том числе есть методы, позволяющие вычислить псевдоним, используемый нападающим в IRC.

### 11.8. Мошенничество в интернет

Для защиты от мошенничества в Интернет мы можем дать следующие рекомендации:

- никогда не осуществляйте покупок через Интернет, особенно с использованием кредитных карточек (это излюбленное лакомство для многих хакеров);

- никогда и ни где не вводите каких либо настоящих данных о себе (ФИО, адрес, E-Mail и т.д.) - все данные должны быть вымышленными!

### 11.9. Защищенный разговор

В то время как существуют десятки программных продуктов, позволяющих шифровать файлы и сообщения, передаваемые по электронной почте, средств для защиты разговоров в режиме on-line все еще очень мало. Какой бы из известных программ для разговора в текстовом режиме (chat) мы ни пользовались, наш разговор может стать объектом для любопытных ушей. Я не хочу сказать, что провайдеру или любой другой заинтересованной организации так уж легко прочесть то, что мы печатаем на клавиатуре в процессе общения на IRC или ICQ, но если им будет очень интересно послушать наши разговоры, они это сделают. Простой текст (а любой стандартный chat - это простой текст) может быть выделен из IP пакетов с помощью специального оборудования и/или программного обеспечения (sniffers).

Способ 1: Разговор в текстовом режиме Авторы попытались найти в сети программы для защищенных разговоров on-line, и нашел всего один продукт. Называется он Secure Communicator (http: // www. idirect. com/secure/).

Secure Communicator позволяет шифровать онлайновые разговоры и файлы, передаваемый одним пользователем другому. Для начала разговора нужно знать IP адрес собеседника или воспользоваться on-line directory service, аналогичным тому, что есть в Netscape CoolTalk, MS NetMeeting или IPhone, только вот он не работает никогда. Но это проблема небольшая для умелых рук (мозгов), всегда можно сначала встретиться на IRC или ICQ, узнать IP адрес и договориться о пароле, а затем перейти на Secure Communicator, который позволяет вести беседу как в mIRC.

Плохая новость состоит в том, что evaluation copy, а это именно то, что вы можете скачать в сети, разговаривать позволяет, а вот шифровать разговор не дает. Но вот здесь первый и последний раз я приведу серийный номер: 5aaDa7aa6a для регистрации программы.

Способ 2: Интернет-телефония Телефонные разговоры и обмен электронной почтой во всевозрастающей степени подвержены подслушиванию. Практически любая незашифрованная электронная коммуникация может быть перехвачена.

PGPfone защищает телефонные разговоры по каналам Интернет и телефонным линиям, используя самые стойкие из существующих криптографических технологий. Помимо этого, используя Интернет в качестве среды голосового общения, вы можете значительно снизить свои расходы по сравнению с использованием обычной телефонной связи.

Характеристики PGPfone

PGPfone позволяет "говорить на ухо" по телефону, даже если это ухо расположено в тысячах миль от вас.

PGPfone (Pretty Good Privacy Phone) - это программный продукт, который превращает ваш персональный компьютер или ноутбук в защищенный телефон. Для того, чтобы предоставить возможность вести защищенные телефонные разговоры в реальном времени (по телефонным линиям и каналам Интернет) в нем используется технология сжатия звука и стойкие криптографические протоколы. Звук вашего голоса, принимаемый через микрофон, PGPfone последовательно: оцифровывает, сжимает, шифрует и отправляет тому, кто находится на другом конце провода и также использует PGPfone. Все криптографические протоколы и протокол сжатия выбираются динамически и незаметно для пользователя, предоставляя ему естественный интерфейс, подобный обычному телефону. Для выбора ключа шифрования используются протоколы криптографии с открытым ключом, так что предварительного наличия защищенного канала для обмена ключами не требуется.

Все, что нужно для запуска PGPfone, это:

по-настоящему надежный модем, поддерживающий скорость передачи как минимум 14.4. Kbps по протоколу V.32bis (рекомендуется 28.8 Kbps по протоколу V.34); IBM PC-совместимый компьютер с процессором как минимум 66 MHz 486 (рекомендуется Pentium), звуковой картой и динамиками или наушниками, работающий под управлением Windows 95 или NT, или Apple(r) Macintosh(tm) с процессором 25MHz 68LC040 или старше (рекомендуется PowerPC) под управлением System 7.1 или старше с установленными Thread Manager 2.0.1, ThreadsLib 2.1.2, и Sound Manager 3.0 (все эти программы доступны с FTP-сервера Apple) - работа PGPfone на 68030 Mac не гарантируется, но в некоторых ситуациях она возможна; также, он запустится не на всех 68040, в зависимости от того, установлено ли соответствующее звуковое оборудование.

Для интересующихся технологией: PGPfone не требует предварительного наличия защищенного канала для обмена криптографическими ключами. Стороны обмениваются ключами с использованием протокола обмена ключами Диффи-Хеллмана, который не дает тому, кто перехватывает разговор, получить какую-либо полезную информацию, и в то же время позволяет сторонам обменяться информацией для формирования общего ключа, который используется для шифрования и расшифровки речевого потока.

В PGPfone версии 1.0 для аутентификации обмена ключами используется биометрическая подпись (ваш голос), для шифрования речевого потока - алгоритмы тройной DES, CAST или Blowfish, а для сжатия речи - алгоритм GSM. (из: Philip R. Zimmermann. PGPfone Owner's Manual Version 1.0, 1996, pp.6-7) PGPfone 1.0 для Macintosh и Windows 95/NT распространяется бесплатно. Существует также коммерческая версия PGPfone 2.0 (только для Macintosh и доступная "легально" лишь американским и канадским покупателям).

Новые характеристики PGPfone 2.0

Выбор технологии сжатия речевого потока (GSM, GSM Lite and ADPCM) с возможностью динамической ее смены без разрыва связи. Это позволяет достичь оптимального качества звука.

Возможность защищенного обмена файлами.

Телефонная записная книжка.

Требования к системе:

MacOs 7.5 или старше, PowerPC Macintosh; или 68040 Macintosh с тактовой частотой не менее 33Mhz (для повышения качества звука рекомендуется более быстрый процессор); микрофон и наушники вместо колонок - в полнодуплексном режиме это позволяет избежать наводок от акустического короткого замыкания;

Примечание для русских пользователей PGPfone 1.0

1. PGPfone изначально настроен на тоновый набор; переключение на импульсный набор, используемый большинством российских телефонных станций, опциями не предусмотрено и в документации не описано. Чтобы переключится на импульсный набор, просто введите латинскую букву "p" перед номером в поле набора, как показано на рисунке.

2. При полнодуплексном соединении, во избежание автовозбуждения усилителя звуковой частоты, в документации рекомендуется использовать наушники, а не динамики. Неплохие результаты можно получить также, подключив к звуковым разъемам платы телефонную трубку. Некоторые новейшие звуковые платы, разработанные с учетом требований компьютерной телефонии, реализуют функцию гашения самовозбуждения.

3. Поскольку PGPfone для работы с потоком данных в реальном времени отключает аппаратную коррекцию ошибок модема, программа очень требовательна к качеству модема. Для некоторых клонов качество и даже сама возможность установления связи с помощью PGPfone зависят не только от чипсета, но и от партии, и даже от конкретного экземпляра.

Где взять PGPfone?

Версия 1.0 для Windows 95/NT (необходимы mfc40. dll и msvcrt40. dll)

ftp. ifi. uio. no (Норвегия)

web. mit. edu (США - не для экспорта!)

Версия 1.0 для Mac OS

ftp. ifi. uio. no (Норвегия)

web. mit. edu (США - не для экспорта!)

http: // www. pgpi. com/pgpfone/ (Для международных пользователей).

Версия 2.0 для Mac OS

http: // www. pgp. com (США - не для экспорта!)

### 11.10. Анонимность в USENET

Большинство людей, использующих Usenet, знают, как важно бывает скрыть свою личность. Во-первых, как только вы послали любое сообщение в любую группу новостей, ваш почтовый ящик с необычайной скоростью начинает наполняться junk mail, т.е. всяким мусором, рассказывающим, как разбогатеть за месяц, остановить выпадение волос и другой подобной дрянью. Во-вторых, ваши публично высказанные взгляды могут вызвать волну откликов, причем не только в рамках группы новостей, но и направленных напрямую автору сообщения, что не всегда желательно.

В-третьих, ваши друзья, коллеги или работодатель могут натолкнуться на ваше сообщение, причем оно может им не понравиться. Короче говоря, причин может быть много, а вывод один: совсем не плохо знать, как сохранить анонимность в Usenet. Ниже следует краткое описание методов, которыми можно воспользоваться для этой цели. Первые два метода дают вам возможность пользоваться альтернативным электронным адресом, при этом ответы на ваше сообщение в Usenet (а также junk mail) вы получать все равно будете, а вот ваша реальная личность останется скрытой.

Третий метод дает полную анонимность: никакой почты вообще. Так что выбирайте тот, который больше подходит.

Метод ј1

Использование коммерческой службы для отправки сообщений в группы новостей. Стоит денег, но прост в использовании. Адреса:

http: // www. nymserver. com и http: // www. mailanon. com (последняя служба предоставляет семидневный бесплатный пробный период).

Метод ј2

Получение бесплатного электронного адреса (например в Hotmail или NetAddress) что, по сути, равнозначно получению "фиктивного" адреса, поскольку ваше настоящее имя давать совсем не обязательно, и использование DejaNews free posting service (http: // postnews. dejanews. com/post. xp). Метод чуть более сложен, чем первый. Никому не известно кто вы, но чтобы скрыть еще и где вы, следует воспользоваться прокси-сервером, иначе ваш IP адрес будет обнаруживать ваше географическое положение. Об использовании прокси серверов можно прочесть в главе ПО WWW БЕЗ СЛЕДОВ. Другим недостатком метода является поле FROM в отправленном сообщении, поскольку в нем какое-то, пусть и фиктивное, имя фигурировать будет, например "John Johnson".

Метод ј3

Использование mail-to-news gateway в сочетании с анонимным римейлером. Mail-to-news gateway позволяет пользователям отправлять сообщения в группы новостей с использованием электронной почты, а не местного сервера новостей. Но если пользоваться этим сервисом "в лоб", то ваше имя и обратный адрес будут фигурировать в сообщении, т. к. mail-to-news gateways их не анонимизируют.д.ля того, чтобы достичь полной анонимности, следует использовать комбинацию анонимного римейлера и mail-to-news gateway, т.е. отправить сообщение в mail-to-news gateway с сайта такого римейлера. Это просто: отправляйтесь на такой сайт (http: // www. replay. com/remailer/), затем к странице, позволяющей отправлять сообщения (можно воспользоваться SSL-защищенной формой), наберите ваше сообщение, а поле TO: заполните в соответствии со следующей схемой:

Для отправки сообщения, например, в группу alt. test, адрес должен быть таким:

m2n-YYYYMMDD-alt. test@alpha. jpunix. com

где YYYYMMDD - это текущая дата (год, месяц, день).

Для отправки сообщения в несколько групп их названия следует разделить знаком "+". Например, для отправки сообщения в alt. test и misc. test 11 сентября 1997, адрес таков:

m2n-19970911-alt. test+misc. test@alpha. jpunix. com

Вот и все. Ваше сообщение будет выглядеть так:

Date: Thu, 11 Sep 1997 11: 09: 02 +0200 (MET DST)

Message-ID: <199709111009. MAA29412@basement. replay. com>

Subject: Just testing

From: nobody@REPLAY. COM (Anonymous)

Organization: Replay and Company UnLimited

X-001: Replay may or may not approve of the content of this posting

X-002: Report misuse of this automated service to

X-URL: http: // www. replay. com/remailer/

Mail-To-News-Contact: postmaster@alpha. jpunix. com

Newsgroups: alt. test, misc. test

This is only a test

Как легко заметить, не малейшего следа отправителя! Следует не забывать о еще одном важном моменте. Mail-to-news gateways появляются и исчезают. Alpha. jpunix. com работает сегодня, но может исчезнуть завтра. Но не печальтесь, свежую информацию о таких службах можно всегда найти здесь: http: // www. sabotage. org/~don/mail2news. html. И не забывайте попробовать, как все работает, прежде чем отправить что-либо важное!

Метод ј4

Хвала создателям DDT. DEMOS. SU, www. fido7. ru, шлюзов и т.д.!

Теперь уже давно можно постить в ФИДО любой смотрелкой ньюзов, а не e-mail-ом, через шлюзы, прописывая команды вручную!

Вы постите в fido7. testing (лучше на ньюс сервер ddt. demos. su), далее получаете ответ с правилами и регистрируетесь. Все - да не все!

Есть такая штука, МоРдератор называется, которая сводит на нет все старания вышехваленых.

В ФИДО правил - как в школе времен застоя!!! Про свободу слова они не слышали (трафик большой - не дошло еще). Вы сидите в он-лайне, вам некогда рыскать в поисках всяких там полиси, счетчик онлайн$/секунда крутится, или Вы деловой человек, некогда Вам разбираться в оффтопиках и прочих придуманных глупостях. Фидошники-же могут - они денег за ФИДО не платят.

Кроме того, многие эхи (ru. hacker) вообще напрочь закрыты для интернета. Отпостить то, что предназначено для них в другую (открытую) группу - нарваться на отключение!

Итак, Вы ошиблись и отправили сообщение для fido7. mo. job в fido7. mo. job. talk, Вас отключили, Вы исчерпали запас почтовых ящиков, или надоело регистрироваться после каждой мессаги (тоже $/сек стоит), с тупыми упертыми МоРдераторами спорить бесполезно. Что же делать?

Все просто до банальности: На ddt. demos. su читаете любую группу (эху по ФИДОшному), смотрите обратные Интернет-адреса в хедерах. Они уж точно зарегистрировались. Дальше настраиваем параметры ньюс сервера ddt. demos. su, для MS OExpress:

Имя: Comoderator. of. Ru. Internet\*

Организация: "FIDO Destroy Ltd. "

Почта: отловленный@интернет. адрес Обратный адрес: ваш. реальный@адрес. для. ответа Все!!! Постите пока его не отключат! Затем ищите другой адрес, и никакой регистрации!

Hесправедливо? А отключать "не зашто - не прошто" справедливо?

Надо попробовать постить под адресами Комодераторов (Должно сработать, или нет?) - пусть их отключают! - Это справедливее, и уж полезнее, чем заваливать МайлБомбами. А с юридической точки зрения, ФИДО сеть не коммерческая... .

Бесплатные News сервера В некоторых (например если у вашего провайдера "слабый" или сильно загруженный news сервер) случаях целесообразно использовать т. н. бесплатные (не требующие пароля для входа) news сервера, список которых мы приводим ниже:

news. infotecs. ru (разрешен постинг в Фидо)

ddt. demos. su

ddt. dol. ru

news. corvis. ru

news. enet. ru

news. portal. ru

news. caravan. ru

news. com2com. ru

news. maxnet. ru

news. comtel. ru

news. solaris. ru

news. leivo. ru

news. info. tsu. ru

К вопросу о дате Маленькое, но важное замечание - если вы посылаете письма в какую-либо конференцию Usenet - проверьте чтобы системное время и дата на вашем компьютере были правильными. Иначе оно будет уничтожатся по пути как письмо из прошлого либо из будущего.

### 11.11. Интересные ресурсы интернет

1. ИНФОРМАЦИОННО-СПРАВОЧНЫЕ РЕСУРСЫ

http: // www. xland. ru: 8088/tel\_win/owa/tel. form

База по телефонам и адресам частных лиц г. Москвы, аналогичная известной базе KOTIK.

http: // www. fox. tt. ee/cheese. htm

Сервер, посвященный различным бесплатным ресурсам сети Интернет, таким как: бесплатной место на WWW, бесплатный E-MAIL, бесплатное ПО и многое другое.

http: // www. fox. tt. ee/

Списки средств массовой информации СНГ (Газеты, журналы, радио, телевидение), приводятся адреса Интернет и EMail.

2. ПОИСКОВЫЕ СЕРВЕРА

http: // www. medialingua. ru/www/wwwsearc. htm

Поисковый сервер Следопыт, позволяет производить поиск с учетом русской морфологии (а также с возможностью перевода слова на английский язык) используя ведущие поисковые системы: AltaVista, Yahho, Infoseek, Lycos и т.д.

http: // tela. dux. ru/win/index. html

Поисковая система по русским ресурсам Интернет.

http: // search. interrussia. com/index. win. html

Поисковая система по русским ресурсам Интернет.

http: // www. search. ru/

Поисковая система по русским ресурсам Интернет.

http: // www. comptek. ru/alta. html

Русская морфологическая надстройка к поисковой системе AltaVista.

http: // www. rambler. ru

Русская поисковая система RAMBLER

http: // www. medialingua. ru/www/wwwsearc. htm

Русская поисковая система Следопыт http: // www. comptek. ru/alta. html

Русская морфологическая надстройка к AltaVista

http: // www. altavista. digital. com

Поисковая система AltaVista

http: // www. dubna. ru/eros/

Поиск людей в Интернет по E-MAIL

http: // www. dejanews. com/

Поиск в телеконференциях 3.1. ПОИСКОВЫЕ СЕРВЕРА (по Программному обеспечению) Поисковые сервера, позволяющие отыскать в Интернете любую программу.

http: // www. softseek. com/

http: // www. cooltool. com/

http: // www. slaughterhouse. com/

http: // www. mediabuilder. com/

http: // www. davecentral. com/

http: // ftpsearch. ntnu. no/

Если вы знаете название файла (или хотя бы часть названия) то можете использовать этот поисковый сервер (поиск производиться в FTP

ресурсах Интернет).

3. КРЭКИ И КРИПТОГРАФИЯ

Сервера, посвященные поиску крэков, программ для взлома, криптографии и т.д.

http: // astalavista. box. sk/

http: // www. t50. com/

http: // www.2600. com/

http: // www. filefactory. com/

http: // www. avault. com/

http: // www. ssl. stu. neva. ru/psw/crack. html

http: // security. lgg. ru/

http: // www. ted. org/~hmaster

http: // www. chat. ru/~bonez/

http: // neworder. box. sk

http: // www. l0pht. com/index. html

http: // www. leader. ru/cgi-bin/go? secure

http: // www. tamos. com/privacy/ru/index. html

http: // www. werwolf. de/

http: // www. ntshop. net/

http: // www. geocities. com/SoHo/Studios/1059/pgp-ru. html

http: // www. halyava. ru/aaalexey/CryptFAQ. html

http: // wwwwin. wplus. net/~kvn/index. htm

http: // www. spymarket. com/

http: // www. halyava. ru/aaalexey/CryptLinks. html

Q: Какие есть интеpесные хакеpские WWW?

A: Вот несколько:

www. ilf. net (Information Liberation League)

www. hackerscatalog. com (no comments)

www. hackzone. ru (no comments)

radiophone. dhp. com (взлом сотовых телефонов, пейджеpов, итд).

www. eurosat. com (все пpо хак спyтниковых телепpогpамм).

www. l0pht. com (многое)

Q: Какие фpикеpские WWW можно поpекомендовать?

A:

radiophone. dhp. com - сотовые телефоны, пейджеpы www. semionoff. com - немного про A-Key

4. ЭЛЕКТРОННЫЕ БИБЛИОТЕКИ

На перечисленных серверах можно найти огромное кол-во литературы в электронном виде. Тематика самая разнообразная от произведений классиков и научной фантастики до кулинарных рецептов http: // kulichki. rambler. ru/moshkow/

Библиотека Максима Мошкова (самая крупная на сегодняшний день)

http: // dali. orgland. ru/tcd/

Библиотека Игоря Загуменова http: // nmsf. sscc. ru/authors. asp

Библиотека Дмитрия Трибиса http: // www. geocities. com/Athens/Academy/9997/

Советская электронная библиотека им.В.И. Ленина http: // kulichki. rambler. ru/sf/

Библиотека фантастики http: // www. delfin. ru/biblio/bibliot. htm

Библиотека Дельфин http: // www. spmu. runnet. ru/camelot/

Библиотека Камелота http: // www. fantasy. ru/

Библиотека фантастики http: // www. referats. corbina. ru/

Московская коллекция рефератов 5. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

На этих серверах периодически появляется новое, доступное для скачивание ПО:

http: // fosi. da. ru

http: // webtownd. da. ru

http: // www. freesoft. ru

http: // www. download. ru

http: // www. download. com

http: // www. shareware. com