ЗАЩИТИТЕ ВАШИ ДАННЫЕ!

А. ЛОМОВ, г. Москва

В наши дни, когда информация стала товаром, а компьютерные технологии общедоступны, приходится защищать данные от возможного несанкционированного доступа. На крупных предприятиях, содержащих для этого специальный персонал, проблемы эффективной защиты как на отдельных ПК, так и в локальных сетях, уже давно и надежно разрешены. Но на жестком диске компьютера, находящегося в офисе небольшой фирмы или дома, порой тоже могут содержаться очень важные или даже секретные (от конкурентов) данные. В предлагаемой статье рассказывается о некоторых простых и легко выполнимых приемах, позволяющих пользователям обычных IBM-совместимых компьютеров не допустить нежелательных утечек и потерь информации.

Прежде чем приступить к практической стороне дела, необходимо уяснить, от кого приходится защищать данные. В первую очередь, — от посторонних, случайно или преднамеренно оказавшихся рядом с вашим компьютером и проявляющих чрезмерное любопытство. Потенциально могут быть опасны и "свои" — по неосторожности, а иногда и умышленно (скажем, после ссоры) они могут повредить или удалить с жесткого диска два-три файла, возможно даже, не подозревая об их важности.

Но любая защита бесполезна, когда за дело берутся профессионалы. Так что, если хранящимися данными заинтересуются "компетентные органы", они прочитают и расшифруют их в любом случае. Правда, эта процедура может обойтись им дороже, чем все секреты вашей фирмы, вместе взятые.

ВХОД В СИСТЕМУ ПО ПАРОЛЮ

Работая в многолюдном офисе, где часто бывают посторонние, прежде всего необходимо установить пароль на запуск компьютера. Это предотвратит доступ к нему лиц, не знающих пароля. Естественно, его должны знать все, кто пользуется одним и тем же компьютером "на законных основаниях". Такая защита не очень надежна и охраняет данные лишь от тех, кто не знает ее тонкостей. Тем не менее в условиях квартиры или малого предприятия приемы, описанные в этом и следующих двух разделах, могут оказаться весьма полезными.

Пароль обычно устанавливают, пользуясь утилитой CMOS Setup либо всевозможными дополнительными программами, запускаемыми из файла автоконфигурации AUTOEXEC.BAT. Мы расскажем, как сделать это с помощью Setup фирмы Award Software — программы, хранящейся в ПЗУ большинства ПК.

Итак, включите компьютер и, нажав клавишу [Del], войдите в Setup. Выберите в появившемся меню пункт "BIOS Features Setup" ("Установка свойств BIOS"), а в нем — "Security Options" ("Режимы безопасности"). Убедитесь, что эта опция имеет значение "System" (пароль распространяется на всю систему). Если установлено значение "Setup" (защищена только программа конфигурации), измените его клавишей [PgDn].

После этого, нажав клавишу [Esc], вернитесь в главное меню. Выберите в нем пункт "Password Setting" ("Установка пароля"). В появившемся окне введите свой пароль и нажмите клавишу [Enter]. Программа предложит вам сделать это повторно, подтвердив тем самым свои намерения. Затем выйдите из Setup с сохранением внесенных изменений (пункт "Save & Exit Setup" главного меню). Компьютер будет перезагружен, и на экране появится просьба ввести пароль. Не сделав этого, продолжить работу невозможно. Эта просьба будет повторяться при каждом включении компьютера, а также после нажатия кнопки "RESET" или комбинации клавиш [Ctrl]+[Alt]+[Del].

Аналогичным образом можно изменить или вовсе отменить пароль. Но теперь запустить Setup удастся только с помощью уже установленного пароля. Войдя в знакомый режим "Password Setting", введите новое кодовое слово, а если хотите снять защиту, не набирая нового значения, нажмите клавишу [Enter].

Имейте в виду, что обойти пароль совсем не сложно — достаточно на короткое время выключить питание микросхемы CMOS-памяти на материнской плате компьютера. Правда, при этом будут уничтожены и другие хранящиеся в ней установки (например, параметры жесткого диска), и их придется вводить заново с помощью все той же программы Setup. На платах стандарта ATX питание отключают специальной съемной перемычкой. Если ее нет, приходится извлекать из гнезда батарею питания.

Но, между прочим, во многих версиях CMOS Setup предусмотрен "универсальный" пароль, введя который можно получить доступ к защищенному компьютеру. В частности, в рассмотренной программе Setup фирмы Award Software это — "AWARD_SW" (все буквы в верхнем регистре). По замыслу разработчиков он должен быть известен только обслуживающему персоналу фирмы. Но не секрет, что все тайное становится явным...*

* Зная, что универсальный пароль быстро перестает быть секретом, изготовители компьютеров периодически меняют его. Так, для BIOS фирмы Award известно не менее девяти вариантов **(Прим. ред.)**.

ПОЛЬЗОВАТЕЛЬСКИЕ КОНФИГУРАЦИИ

Операционная система Windows 95 предоставляет каждому из работающих на одном и том же компьютере возможность создать свою собственную конфигурацию системы. В меню "Завершение работы", появляющемся на экране перед выключением компьютера, среди других пунктов имеется и такой — "Войти в систему под другим именем". Выбрав его, можно ввести свое имя (или псевдоним), пароль и зарегистрироваться в Windows 95 как новый пользователь. Теперь, сообщая эти данные при каждой загрузке операционной системы, можете работать в конфигурации, которую без вашего ведома не изменит никто. Это предотвращает и доступ к Windows незарегистрированных пользователей, даже прошедших первую преграду — пароль CMOS Setup.

Перед тем, как создавать рабочие конфигурации для каждого пользователя, необходимо открыть "Панель управления" и выбрать там значок "Пароли". Сделав это, перейдите к закладке "Конфигурации", где установите в активное состояние кнопку с надписью "Каждый пользователь может иметь свою систему настроек, выбираемую при входе в Windows". В нижней рамке закладки установите все флаги (там их два). После этого перезагрузите Windows. На экране появится уже упоминавшееся предложение ввести имя и пароль. Теперь можно приступать к созданию своей собственной конфигурации рабочего стола, меню и прочих элементов Windows.

К сожалению, организовать несколько пользовательских конфигураций, работая с MS DOS или Windows 3.x, значительно труднее, но все же можно. Существует, например, несложный способ, основанный на копировании разных версий инициализационных файлов Windows в рабочий каталог среды перед ее запуском.

Основной недостаток MS DOS и Windows 3.x, с точки зрения рассматриваемой проблемы, заключается в невозможности установки паролей стандартными средствами этих систем. Поэтому, работая в названных средах, уделите серьезное внимание установке пароля CMOS Setup.

ПАРОЛЬ ПОСЛЕ ПЕРЕРЫВОВ

Во время коротких перерывов в работе, которые случаются довольно часто, компьютер обычно не отключают: время, которое он затратит на "пробуждение" и, например, загрузку Windows и открытие всех документов, может оказаться больше продолжительности собственно перерыва. Да и вообще, частые включения и выключения пагубно сказываются на "здоровье" любой электронной аппаратуры. Как же защитить компьютер, не отключая питания? Ведь в этом случае пароль на вход в систему бесполезен — она уже запущена. Задачу решают программы-хранители экрана (screen savers), запрашивающие пароль, при попытке выхода из них.

Для установки хранителя экрана в Windows 3.x откройте окно "Панель управления" и щелкните по пиктограмме "Оформление". В рамке "Хранитель экрана" выберите из списка любой графический эффект от "Blank Screen" ("Чистый экран") до "Starfield Simulation" ("Имитация звездного неба"). Можно предварительно оценить его, нажимая кнопку "Тест". Затем в нижней части рамки установите время задержки запуска хранителя экрана, после чего нажмите кнопку "Параметры". В рамке "Опции пароля" установите флаг "Защита паролем" и нажмите кнопку "Назначить пароль". В появившемся окне дважды (в среднем и нижнем полях) введите свой секретный код, после чего нажмите кнопку "OK".

Отныне вы можете смело уходить с рабочего места — через заданное время после последнего нажатия клавиши или манипуляции с "мышью" запустится хранитель экрана. Некоторые программы, расширяющие возможности Windows, например, IconHear-It, позволяют активизировать screen saver без обязательного ожидания: достаточно переместить указатель "мыши" в правый верхний угол экрана (при желании и в любой другой) — и появится заставка хранителя экрана. Кстати, подобные программы снабжены собственными графическими эффектами, часто более привлекательными, чем стандартные заставки Windows.

В Windows 95 пароль хранителя экрана устанавливают несколько иначе. Щелкните правой кнопкой "мыши" и выберите в появившемся меню пункт "Свойства". На закладке "Заставка" в рамке "Энергосберегающие функции монитора" уберите все флаги, а в рамке "Заставка" выберите из списка графический эффект (он отображается в стилизованном изображении монитора компьютера, но можно увидеть его во весь экран, воспользовавшись кнопкой "Просмотр"). В правой части рамки активизируйте флаг "Пароль" и нажмите кнопку "Сменить". Введите пароль дважды (в верхнем и нижнем полях) и нажмите кнопку "OK". На экране появится сообщение: "Пароль был успешно изменен".

Как и в Windows 3.x, через заданное время бездействия клавиатуры и "мыши" заработает программа-хранитель экрана. Такие пакеты, как Microsoft PLUS! и Microsoft Power Toys, позволяют аналогично IconHear-It задать угол экрана, при перемещении в который курсора "мыши" заставка появляется немедленно. Они располагают, разумеется, и своими графическими эффектами.

К сожалению, все описанные выше средства работают только под управлением Windows. А как быть пользователям MS DOS? В популярной оболочке Norton Commander версии 5.0 имеется достаточно много экранных заставок, но возможность защиты выхода из них паролем не предусмотрена. Не устанавливать же Windows специально для того, чтобы пользоваться хранителем экрана с паролем!

Полноценные хранители экрана для DOS все же существуют, но найти их, как и другие полезные программы для этой операционной системы, очень сложно: рынок заполнен ПО только для Windows 95/98. Не мудрствуя лукаво, лучше написать свою программу, выполняющую нужную операцию. Это легко сделать, например, с помощью системы программирования QuickBASIC. Текст программы одного из возможных вариантов защищенного паролем хранителя экрана приведен в таблице. Нетрудно заметить, что это слегка измененная версия программы из статьи автора "Типовой шаблон программного модуля на языке высокого уровня" ("Радио", 1998, №1, с.22, 23). Поэтому не будем останавливаться на ней подробно, отметим лишь некоторые важные моменты.

В ответ на предложение задать пароль необходимо ввести любой набор букв и цифр и нажать клавишу [Enter]. Делайте это внимательно, поскольку возможность исправить ошибку не предусмотрена (впрочем, задача автора — подсказать идею, а читатели могут усовершенствовать программу). Затем можно спокойно отлучиться. Для выхода из хранителя необходимо еще раз ввести тот же пароль. Если он не совпадет с заданным, то после второй попытки его ввода раздастся звуковой сигнал (наподобие сирены) и компьютер "зависнет".

Если при компиляции программы не была предусмотрена возможность прекратить ее работу нажатием [Ctrl]+[Break], возвратить компьютер в рабочее состояние можно будет только трехклавишной комбинацией [Ctrl]+[Alt]+[Del] либо кнопкой "RESET". В результате на экране появится другое приглашение ввести пароль — это сделает программа CMOS Setup.

Исполняемому файлу хранителя экрана лучше всего дать короткое имя, например S.EXE. Для его запуска (если в AUTOEXEC.BAT установлен соответствующий путь) достаточно нажать всего две клавиши: [S] и [Enter]. Красивый вариант — подключить свой хранитель к оболочке Norton Commander 5.0, в меню которого "Команды" — "Конфигурация" — "Гашение экрана" нужно выбрать произвольный графический эффект (какой именно — не имеет значения, хранитель все равно использует собственный) и задать время задержки. Файл программы следует назвать SAVER.EXE и заменить им одноименный в рабочем каталоге оболочки (как правило, NC).

```
DEFINT A-Z: SCREEN 0,0: WIDTH 40,25:
RANDOMIZE TIMER
COLOR RND*6+9,0:CLS
PRINT"Хранитель экрана с защитой паролем"
PRINT"Copyright (C) А. Ломов, 1997";
IF SCREEN(1,1)<>149 GOTO Quit
Time0!=TIMER
WHILE TIMER-Time0!<2:WEND

COLOR 14:CLS:LOCATE 12,13
PRINT"ВВЕДИТЕ ПАРОЛЬ"
DO
 PassSym$=INPUT$(1):
 IF PassSym$=CHR$(13) THEN EXIT DO
 InPassword$=InPassword$+PassSym$
LOOP

SCREEN 12:WHILE INKEY$=""
 DrParam=RND*100
 IF DrParam=0 THEN COLOR RND*6+9
 ELSE COLOR 0
 CIRCLE(RND*599+20,RND*439+20),RND*18+2
WEND

SCREEN 0,0:WIDTH 40:COLOR 14:CLS
LOCATE 12,13:PRINT"ВВЕДИТЕ ПАРОЛЬ"
OutCtrl:DO
 PassSym$=INPUT$(1)
 IF PassSym$=CHR$(13) THEN EXIT DO
 OutPassword$=OutPassword$+PassSym$
LOOP

IF InPassword$=OutPassword$ THEN
  GOTO Quit
ELSE
 ErrTime=ErrTime+1
 IF ErrTime<2 THEN
  BEEP:GOTO OutCtrl
 ELSE
  LOCATE 12,6:COLOR 28
  PRINT"!!! ЗА КОМПЬЮТЕРОМ ХАКЕР !!!"
  DO
   FOR Snd=200 TO 800 STEP 5
    SOUND Snd, .1
   NEXT
   FOR Snd=800 TO 200 STEP -5
    SOUND Snd, .1
   NEXT
  LOOP
 END IF
END IF

Quit:
WIDTH 80:COLOR 7:CLS:END
```

ШИФРОВАНИЕ ДАННЫХ

Никакие рекомендации предыдущих разделов не помогут, если компьютер "взламывает" профессионал, которого всевозможные пароли только раззадорят. Когда данные необходимо уберечь надежно, защищайте и шифруйте файлы, в которых они содержатся, а не весь компьютер. В этой статье намеренно не затрагиваются такие возможности, как установка паролей на открытие документов текстового редактора Word или распаковку архивов с помощью программы ARJ, самодельные алгоритмы зашифровки и прочие методы, защищающие данные лишь от зауряд-

ного любопытства. Для надежной защиты, не поддающейся профессиональным взломщикам, необходимо применять только профессиональные средства.

Одно из них — шифрование информации по алгоритму DES, положенному в основу одного из федеральных стандартов США и отечественного ГОСТ 28147—89. Он реализован многими довольно популярными программами, в том числе PCSecure из пакета PC Tools, PGP, широко известной в Internet, и утилитой Diskreet из Norton Utilites.

На Diskreet для MS DOS — средстве, наиболее известном и доступном отечественным пользователям, остановимся более подробно. Эта утилита предлагает два способа засекречивания. С ее помощью можно зашифровать отдельные файлы или организовать на винчестере секретный логический диск (NDisk), где все данные будут храниться в зашифрованном виде. Широкие возможности этой программы невозможно описать в короткой журнальной статье, так что расскажем только об основных, требуемых для надежной зашифровки важных данных.

Запустив файл DISKREET.EXE, вы, возможно, увидите сообщение о том, что драйвер DISKREET.SYS не установлен. Если нет необходимости создавать секретный диск, то он и не понадобится и в окне сообщения можно установить флаг "Disable This Message" ("Не показывать это сообщение"). Аналогичного результата можно достичь, убрав флаг "Warn if Driver Not Loaded" ("Предупреждать, что драйвер не загружен") в меню "Options" — "Global".

Теперь зададим параметры зашифровки. В меню "Options" — "File" Diskreet предлагает два алгоритма: упрощенный ("Fast Proprietary Method") и по стандарту DES ("Government Standard"). Последний работает медленнее, но более надежен (если нужна высокая степень защиты, пользуйтесь именно DES-шифрованием). В этом же окне сделайте активными опции "Delete original files after encryption" ("Уничтожать исходные файлы после зашифровки"), "Use same password for entire session" ("Использовать один и тот же пароль во всем сеансе работы") и нажмите кнопку "Save".

Перейдя в меню "Options" — "Global", задайте метод удаления исходных файлов ("Data Clearing Method"). Чтобы никто не смог их восстановить, лучше всего использовать "Government Wipe (DOD Spec)" ("Стирание по стандарту Министерства обороны").

Для зашифровки файла или группы файлов воспользуйтесь меню "File" — "Encrypt". В появившемся окне выберите подлежащие шифрованию файлы (текстовые документы, базы данных, исполняемые коды программ и т. п.). При этом можно переходить на другой диск, листать каталоги, пользоваться масками (символами * и ?).

В ответ на появляющиеся на экране просьбы введите ключ шифра, а затем подтвердите его и обязательно запишите где-нибудь (на бумаге), поскольку, в отличие от паролей CMOS Setup или хранителя экрана, которые можно обойти, расшифровать данные, не зная правильного ключа, не удастся. Выбирайте его не короче восьми символов, иначе код будет легко подобрать. Не используйте в составе ключа номера своего телефона, автомобиля, паспорта, инициалы и аналогичные данные родственников, друзей и знакомых. Специалисты по расшифровке начинают подбор ключей именно с этих вариантов. Чем бессмысленнее набор символов — тем лучше, однако, как говорится, не перестарайтесь: код вроде "D_0:a1^03kq" забудется через минуту после ввода!

Всем зашифрованным файлам программа Diskreet присваивает по умолчанию расширение SEC (от слов "secret" или "security"), а оригиналы стирает. Расшифровывают данные с помощью меню "File — Decrypt" той же программы. Файлы выбирают аналогично тому, как это делалось при зашифровке. После нажатия кнопки "OK" необходимо ввести ключ шифра.

Конечно, ключ к любому шифру, даже самому сложному, можно найти старым, как мир, методом перебора всех комбинаций — ведь компьютер использует всего 256 символов, из которых для формирования ключа доступны максимум 240. В соответствующих организациях для расшифровки применяют мощнейшие компьютеры, проверяющие сотни вариантов в секунду. Тем не менее описанный метод вполне надежно защищает данные от конкурентов, не располагающих неограниченными возможностями.

ХРАНЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Если вы не хотите, чтобы в ваших, пусть даже засекреченных всеми возможными способами данных копались посторонние, не давайте им такой возможности — не храните ничего, кроме программ, на жестком диске!

Существует достаточно много сменных носителей информации, пригодных для хранения больших объемов данных: это обычные дискеты и более емкие Zip-драйвы, дорогие, но надежные Jaz, разнообразные магнитооптические диски, стримеры, перезаписываемые компакт-диски и многое другое — выбирайте в зависимости от своих целей и финансовых возможностей.

Однако даже такое простое дело, как хранение данных на сменных носителях, применительно к конфиденциальной информации следует выполнять с особой ответственностью. Каждый файл необходимо записывать как минимум на два разных носителя (иными словами, каждый диск должен иметь копию) и хранить их в разных, в меру удаленных друг от друга местах. Если что-нибудь произойдет с одним из них (пожар или заурядная кража), можно рассчитывать на то, что вся информация осталась в целости и сохранности в другом месте. Разумеется, данные на съемных носителях должны быть зашифрованы.

Теперь — о специфике работы на компьютере с конфиденциальной информацией. Если сменные носители, которыми вы пользуетесь, достаточно быстродействующие, старайтесь вообще не копировать файлы с секретными данными на жесткий диск.**

Если обойтись без винчестера не удалось, по окончании работы обязательно уничтожьте на нем все файлы данных. Делать это с помощью стандартных средств MS DOS не имеет смысла, так как команда DEL на самом деле не стирает данные, а лишь дает возможность записывать на их место новые. Если записи не делались, удаленный файл легко восстановить — для этого предусмотрена специальная команда UNDELETE. Но даже после записи новых данных на диске нередко остаются большие куски "удаленной" информации, прочитать которую не представляет большого труда.

Работая с DOS, применяйте для удаления конфиденциальных данных программу Wipeinfo из пакета Norton Utilities. Она полностью стирает удаляемую информацию с диска и делает невозможным ее восстановление. Вместо нее можно пользоваться утилитами SpeeDisk или DEFRAG. Любая из них в режимах "Unfragment Files Only" ("Только дефрагментировать файлы") и "Full Optimization" ("Полная оптимизация"), кроме выполнения своей основной задачи — оптимизации размещения данных на диске, полностью стирает все, относящееся к удаленным обычным способом файлам.***

В Windows 95 никаких мер для стирания удаленных файлов принимать не нужно. Не забывайте только в конце работы "вынести мусор" — выбрав на рабочем столе значок "Корзина" (в англоязычной версии — "Recycled", что означает "вторсырье"), уничтожить ее содержимое.

** Многие программы, например, текстовые процессоры, во время работы создают на жестком диске временные файлы. Более того, сама операционная система Windows периодически записывает данные, не помещающиеся в ОЗУ, в так называемый "файл подкачки". Хотя все эти файлы автоматически уничтожаются, следы секретных данных все же могут остаться на "винчестере" **(Прим. ред.).**

*** Это не совсем так. Если были удалены файлы большого объема, находившиеся в конце занятого дискового пространства (т. е. записанные недавно), то и после дефрагментации часть имевшихся в них данных с большой вероятностью на диске все же останется **(Прим. ред.).**