Информации в файлах — надежную защиту!

Александр Кальфа

Зачем и чем?

Тогда пешеход остановился... и тихо сказал:
— Может быть, тебе дать еще ключ от квартиры, где деньги лежат?
Зарвавшийся беспризорный понял всю беспочвенность своих претензий и отстал.
И.Ильф, Е.Петров. «Двенадцать стульев»

На жестких дисках наших персоналок, как правило, хранится много конфиденциальной информации — договоры и счета, сведения о компаньонах и конкурентах, личные письма и адреса. Доступ посторонних лиц к этой информации всегда, мягко говоря, нежелателен.

У нас в России почему-то считается, что надежнее всего вообще не хранить такую информацию на компьютере. Наиболее ценное переписывается на дискеты и носится с собой или хранится в сейфе под замком. Некоторые идут еще дальше и просто регулярно снимают с компьютера жесткий диск. Все признают, что это неудобно, сложно, противоречит самому духу компьютерной обработки информации, но кажущаяся надежность перевешивает прочие резоны. При этом обычно забывают, что злоумышленники могут просто «попросить» показать им хранимые в кейсе или сейфе носители информации. И просьба прозвучит настолько «аргументированно», что отказать будет трудно. Постоянно перемещаемые дискеты владелец может потерять, да и выкрасть их не представляет особого труда.

Для защиты файлов непосредственно на дисках можно использовать одну из многочисленных программ, свободно распространяемых в сети Internet. Однако надежность защиты таких программ определить практически невозможно. Закрытая с их помощью информация зачастую может быть вскрыта специалистом средней квалификации. Да и доступность программ для всех желающих вызывает сомнение: ведь никто не установит в квартире замок, найденный вместе с ключами на улице. И, конечно, нельзя забывать о сыре, который бывает бесплатным только в мышеловке.

К счастью, существует несколько вполне надежных разработок специализированных отечественных фирм, давно и успешно работающих в области защиты информации. Одна из них — программа CryptoMania, созданная в ОАО «ИнфоТеКС» (www.infotecs.ru).

CryptoMania предназначена для защиты от несанкционированного доступа к файлам и каталогам любого формата (кроме системных) на жестких дисках, дискетах и других носителях информации. Она позволяет, во-первых, закрыть доступ к конфиденциальным материалам, хранимым на жестких дисках компьютеров. Во-вторых, с ее помощью можно разграничить доступ нескольких пользователей к информации, хранимой на одном компьютере. В-третьих, CryptoMania способна защитить информацию на переносных и карманных компьютерах, дискетах и иных накопителях. И, наконец, закрытые с помощью программы конфиденциальные материалы можно пересылать как по обычной открытой почте, так и по электронной, не опасаясь, что они будут прочитаны.

Секрет ее стойкости

— Как! — закричал Буратино радостно. — Ты знаешь тайну золотого ключика?
— Знаю, где ключик лежит, как его достать, знаю, что им нужно открыть одну дверцу...
А.Толстой. «Золотой ключик»

Высокая стойкость к попыткам взлома в программе CryptoMania достигается за счет особой конструкции механизма закрытия файлов. Параметры этого механизма находятся в сложной зависимости как от номера лицензии, выдаваемой пользователю, так и от вводимого пароля. Поскольку номер лицензии уникален и генерируется специальной программой, а пароль известен лишь пользователю, защищенные файлы оказываются недоступными даже для тех, кто программу CryptoMania разработал. Механизм настолько сложен, что перебор всех его возможных комбинаций на современных ЭВМ требует не одного десятка лет.

Пароль выполняет еще одну роль. Он позволяет организовать разграничение доступа к файлам нескольких сотрудников фирмы или членов семьи, использующих один компьютер. Каждый из пользователей может защищать свои файлы личным паролем, а несколько пользователей, объединенных общими интересами, — еще и общими паролями. Но не стоит неограниченно расширять круг лиц, пользующихся программой с одним и тем же номером лицензии. Ведь в этом случае они используют одинаковый механизм защиты, стойкость которой определяется лишь удачным выбором пароля. Поэтому пользователям CryptoMania не стоит передавать программу для копирования даже друзьям и знакомым — ведь при этом передается и часть защитного механизма. Окольным путем программа может попасть к лицам, которые попытаются получить доступ к информации законного пользователя. Поскольку имя последнего фиксируется в каждой лицензионной копии, сделать это будет нетрудно.

Программа CryptoMania может использоваться и для защиты пересылаемой или перевозимой инфор-

мации. В этом случае программа с одним и тем же лицензионным номером устанавливается на двух или нескольких компьютерах, находящихся в разных офисах, в том числе в разных городах. Информация, закрытая на одном из компьютеров и записанная на дискеты, может быть раскрыта на другом, если в этот офис предварительно сообщен пароль. При утере или хищении пересылаемых по открытой почте дискет (перехвате сообщений, пересылаемых по электронной почте) файлы останутся недоступными для посторонних лиц и будут восприниматься ими как испорченные. Наивысшая степень защиты информации достигается в том случае, когда программа вообще не устанавливается на жестком диске, а запускается с дискеты или CD. Тот же эффект достигается, если уже инсталлированная программа стирается при угрозе прочтения файлов нежелательными лицами. Злоумышленник, получивший доступ к компьютеру, не найдет на нем программы защиты, а попытавшись открыть защищенные файлы в любой кодировке, обнаружит в них полную абракадабру.

Для запуска программы требуется компьютер IBM PC 486 и выше с ОС Windows 95/98/NT и свободным местом на жестком диске не менее 2 Мбайт.

Адреса, явки, пароли...

— У вас продается славянский шкаф?
— Шкаф продан. Есть никелированная кровать.
— С тумбочкой?

Из кинофильма «Подвиг разведчика»

Пароли — наиболее уязвимая часть любой системы защиты информации. Как бы ни была «крепка броня», создаваемая программой CryptoMania, она не устоит перед злоумышленником, получившим доступ к программному обеспечению и паролю законного пользователя. Мы уже говорили, что программу CryptoMania, как и любое другое программное средство защиты информации, ни в коем случае нельзя передавать для копирования даже самым надежным друзьям. А по поводу паролей можно дать несколько общих рекомендаций.

Регулярно меняйте пароли. Даже если злоумышленник случайно узнает или подберет ваш пароль, он не сможет долго им пользоваться и, в конце концов, потеряет доступ к вашей информации. Не используйте придуманные посторонними пароли, даже если они кажутся вам очень оригинальными. Ни в коем случае не применяйте в качестве паролей ассоциированную с вами информацию, то есть производные от своего имени, отчества или фамилии, имени супруги (супруга) или детей, даты своего и их рождения, номера телефона или автомобиля, домашнего адреса и т.п. И все-таки выбирайте достаточно простые и легко запоминающиеся пароли. Ведь их ни в коем случае нельзя записывать на бумаге.

В этом и кроется противоречие, делающее выбор пароля совсем непростой задачей. Выработка собственной парольной политики открывает большой простор для фантазии. И эта политика может оказаться наилучшей хотя бы потому, что о ней знаете только вы сами. Один из примеров выбора пароля приведен ниже.

Используйте фразу из 3-4 слов, содержащую сведения о хорошо знакомом лично вам событии. Желательно, чтобы об этом событии не знали окружающие, а фраза содержала имена собственные. Например, вряд ли кому-то из ваших нынешних коллег известно, что ваш школьный друг *Олег любил переплывать Волгу*. Возьмите из каждого слова, набранного курсивом, 2, 3 или 4 буквы. Если вы возьмете четыре буквы, то получите: «*ОлеглюбипереВолг*». Теперь можно перейти на английский шрифт клавиатуры, нажать клавишу «Caps Lock» и набрать полученный текст русскими буквами. Вы получите: «jKTUK><BGTHTdJKU». Согласитесь, что такой пароль выглядит беспорядочным набором символов, который практически невозможно запомнить обычным способом, но легко воспроизвести лично вам. Впрочем, изменение шрифта и замена строчных букв на заглавные, и наоборот — не очень оригинальная идея. Более принципиально то, что при вводе четырех букв от каждого из четырех слов задуманной вами фразы, вероятность угадать пароль простым перебором вариантов становится меньше 10^{-12}.