## [Урок 9. Защита жесткого диска.](file:///C:\Users\Пользователь\Desktop\учебник%20архив\public_html\page9.html)

Любую часть компьютерной системы можно заменить на новую, но утратив данные, записанные на жестком диске, вы будете вынуждены воссоздать их заново. На это могут уйти месяцы, а то и годы. Гораздо проще заранее организовать защиту содержимого жесткого диска.

Начинать следует с создания аварийной загрузочной дискеты. Она очень пригодится, если по какой-то причине не удастся загрузить операционную систему с жесткого диска.

Владельцам Windows-систем придется cоздать дискету аварийной загрузки самостоятельно.

**Создание аварийного загрузочного диска**

Приготовив чистую дискету, выполните в среде Windows следующие действия:

• в меню Пуск выберите Настройка/Панель управления;

• выберите позицию Установка и удаление программ

• щелкните по закладке Системный диск в Windows-95 или Загрузочный диск в Windows-98;

• щелкните на кнопке Создать диск;

• по требованию вставьте дискету в дисковод и щелкните по кнопке ОХ;

• по завершении процедуры выньте дискету из дисковода, наклейте на нее этикетку с маркировкой «Аварийная загрузочная дискета» и положите в безопасное место.

**Резервное копирование данных**

Другой враг нашей информации — сбои самого компьютера. Даже при самом строгом соблюдении мер профилактики нельзя быть абсолютно застрахованным от потери данных, хранящихся на жестком диске. Рано или поздно что-нибудь случается, и вос становить все в прежнем виде можно будет только в том случае, если у вас имеется копия содержимого жесткого диска.

Логика здесь очень простая: если одни и те же данные хранятся в двух разных местах, вероятность лишиться их значительно уменьшается. Поэтому всегда следует хранить данные в двух экземплярах: один на жестком диске, другой на сменных носителях, используемых для резервного копирования. Чтобы определиться со стратегией создания резервных копий, необходимо решить, каким носителем вы будете пользоваться и какие данные нужно продублировать.

Информацию можно хранить на различных съемных носителях: флешках, облаках и дисках [CD-ROM](file:///C:\Users\Пользователь\Desktop\учебник%20архив\public_html\page37.html). Чаше всего для хранения резервных копий используют флешки.

**Коварство мусорной корзины**

При удалении информации она не исчезает бесследно, а попадает сначала в Корзину, если только документ не находился на дискете. Это ежедневно спасает многих небрежных пользователей, случайно удаливших документ неосторожным нажатием клавиши [Delete], поскольку документы из Корзины можно восстанавливать.

Для полного удаления информации из Корзины, т.е. ее очистки, сделайте щелчок правой кнопкой мыши по значку Корзины на рабочем столе и в открывшемся контекстном меню выберите команду Очистить корзину или выберите в окне Корзина команду очистки корзины

Считается, что после принудительной очистки Корзины документы теряются безвозвратно, но это не совсем так. Физические данные с жесткого диска никуда не исчезают и могут быть легко восстановлены специальными программами вплоть до того момента, пока на то же место винчестера не будет записана другая информация. А ведь это может произойти через неделю или месяц.

Чтобы быть точно уверенным, что ваши данные уничтожены навсегда, систематически проводите [дефрагментацию](file:///C:\Users\Пользователь\Desktop\учебник%20архив\public_html\page37.html) [жесткого диска](file:///C:\Users\Пользователь\Desktop\учебник%20архив\public_html\page37.html). Программа дефрагментации Defrag входит в состав служебных программ(Пуск/Программы/Стандартные/Служебные) и перемещает данные на диске таким образом, чтобы файлы и свободное пространство размещались оптимально.

Эта процедура может занять от нескольких минут до получаса и более в зависимости от степени фрагментации диска. Желательно проводить дефрагментацию не реже одного раза в месяц, а при большом количестве операций по удалению файлов — еженедельно.

**Установка паролей на документ**

Известно, что любое приложение [MS Office](file:///C:\Users\Пользователь\Desktop\учебник%20архив\public_html\page37.html) позволяет закрыть любой документ паролем, и многие успешно пользуются этим проверенным средством. Для установки пароля на текстовый документ необходимо его открыть, далее в меню Сервис выберите команду Параметры. В открывшемся окне на вкладке Сохранение наберите пароль для открытия файла вашего документа, сделайте подтверждение его повторным набором и нажмите на кнопку ОК.

В документации к MS Office ничего не говорится о криптостой кости используемыхсхем парольной защиты, есть только фраза: «Внимание! Забытый пароль восстановить невозможно». В версии MS Office-2000 на открытие файлов MS Word предусмотрена сравнительно надежная защита. Защита электронных таблиц [MS Excel](file:///C:\Users\Пользователь\Desktop\учебник%20архив\public_html\page37.html) и пользовательской информации MS Outlook более слабая, чем у текстовых документов.

Обычному пользователю, не имеющему конкретной цели узнать вашу информацию, вскрыть пароль практически невозможно. Однако и специалисту-взломщику при использовании современного компьютера на взлом пароля методом прямого перебора вариантов понадобится примерно один месяц.

Парольная защита, входящая в комплект многих архиваторов, вполне может уберечь документ от посторонних глаз. В сети [Интернет](file:///C:\Users\Пользователь\Desktop\учебник%20архив\public_html\page37.html) можно найти ряд специальных программ «шифрования» отдельных документов и целых разделов винчестера, однако сто процентной гарантии от взлома паролей они не дают. Осложнить процесс взлома защиты вы можете, используя достаточно длинные и сложные пароли, исключающие ваше имя, фамилию и телефон. Лучше всего в качестве пароля выбирать фразу, в которой отсутствует осмысленная информация об авторе пароля. Скажем, фразу типа «Остались от козлика ножки да рожки» можно считать почти идеальным паролем — достаточно длинным и бессмысленным относительно автора.

Напоследок дадим несколько коротких практических советов по защите и резервному копированию ваших данных.

**Как защитить данные?**

• Установите пароли на [BIOS](file:///C:\Users\Пользователь\Desktop\учебник%20архив\public_html\page37.html) и на экранную заставку.

• Исключите доступ посторонних лиц к вашему компьютеру,

• Создайте аварийную загрузочную дискету.

• Систематически делайте резервное копирование данных.

• Регулярно очищайте Корзину с удаленными файлами.

• Устанавливайте пароли на файлы с важной информацией.

• При установке пароля не используйте ваше имя, фамилию, телефон.

• Проводите архивацию файлов.

• После удаления большого количества файлов, но не реже одного раза в месяц, производите дефрагментацию жесткого диска.

Говоря о безопасности информации, мы сознательно глубоко не затрагивали проблему компьютерных вирусов, и могло сложиться мнение, что такая проблема не актуальна.

Ничего подобного! Борьба с вирусами — это несомненно часть информационной безопасности, просто мимоходом говорить о такой важной проблеме неправильно. Борьба с вирусами — это тема отдельного разговора.

**Рассмотрим лишь общую схему без текстов программ.**

1. Защиту жесткого диска осуществляет программа, заменяющая главную загрузочную запись. Сама же загрузочная запись, а также ВООТ-сектор разделов хранятся на жестком диске в зашифрованном виде. Запуск операционной системы с дискеты не помогает, так как в данном случае жесткий диск для операционной системы перестает существовать. Стандартные методы восстановления загрузочных секторов не работают в данном случае, т.к. неизвестно, где начинаются

разделы.

2. Вход на жесткий диск осуществляется по паролю. Пароль определяет, какие разделы, каталоги, файлы, а также операции будут доступны пользователю. Если пароль введен правильно, то защищающая программа обеспечивает запуск операционной системы с жесткого диска. При этом в памяти остается некоторый резидентный модуль, который и осуществляет разграничение доступа.

3. Резидентный модуль должен обеспечить правильность работы операционной системы и других программ. В частности, должно быть сымитировано правильное содержимое всех загрузочных секторов, однако заблокирована возможность снятия с них копии обычными способами (через прерывание 1ЗН).

4. Резидентный модуль осуществляет разграничение доступа к разделам жесткого диска, каталогам и отдельным файлам, а также блокирование отдельных операций с гибкими дисками (например, запуск и копирование программы с них) посредством контроля над прерываниями 13Н, 21Н, 25Н, 26Н. Блокирование операций с гибкими дисками не позволяет запускать какие-либо программы, которые могли бы помочь снять защиту.

5. Резидентный модуль осуществляет свою собственную защиту в памяти.

6. Для полноты в данную схему можно было бы добавить также регистрацию попыток несанкционированных операций пользователя, который идентифицируется своим паролем. Это дало бы возможность оперативно реагировать на все попытки "взлома" системы сменой паролей, перераспределением доступа, применением к взломщику административных мер и т.д.

Данная схема в принципе проста и должна быть усилена средствами административного воздействия.