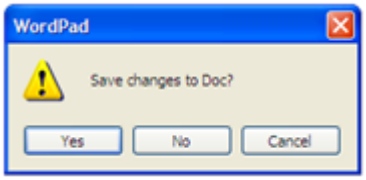

В настоящей статье я хотел бы осветить тему не столько безопасности, сколько именно сохранности данных.

Почему это важно? Большая часть данных, хранящихся на персональном компьютере пользователя, в большинстве своем, не является конфиденциальной информацией. Зачастую потеря или повреждение данных может нанести урон значительно больший, чем утечка этих данных в сеть (Интернет).

В данном случае речь пойдет о мерах, которые необходимо предпринять для обеспечения сохранности документов пользователя, например семейных фотографиях, записях лекций, офисных документов и т.д., и предотвращения их возможной потери.

Начнем с того, что борьба за сохранность данных предполагает дополнительные финансовые вложения и размер этих вложений зависит от степени важности сохраняемой информации.

Сначала я опишу ряд подходов к которым можно будет прибегнуть впоследствии для обеспечения сохранности данных. У каждого подхода есть свои преимущества и недостатки. Я постараюсь все их учесть, чтобы выбор каждого подхода был достаточно ясен и очевиден.

Затем, я укажу ряд последовательных шагов, необходимых для оперативного обеспечения сохранности данных. Таким образом пользователь сразу сможет предпринять какие-то конкретные шаги и получит пищу для размышлений.

Итак опишем варианты использования дополнительного устройства хранения информации т.е. жесткого диска (альтернативой может послужит флэш накопитель (флэшка) большого объема).

1. При наличии стационарного системного блока (как правило не подходит для владельцев ноутбуков) возможно установить дополнительный жесткий диск.

1.1. Если есть возможность установить аналог имеющегося (установленного) жесткого диска, т.е. диска той же фирмы и того же объема, то появляется возможность создания программного RAID массива типа "зеркало".

Плюсы этого подхода:

- Все данные на основном жестком диске будут автоматически скопированы на резервный диск.
- В случае выхода из строя одного из дисков, все данные будут доступны на резервном диске.

Минусы:

- В случае программной порчи данных, например в результате заражения вирусом, будут повреждены все данные, как на основном, так и на резервном диске.
- Также в случае случайного или умышленного удаления данных, данные будут автоматически удалены на обоих дисках.

1.2. Если есть возможность установить диск большего объема, то появляется возможность резервного копирования (архивирования) всех имеющихся данных и даже нескольких версий одних и тех же данных.

Плюсы этого подхода:

- Обеспечивается дополнительный уровень защиты, который заключается в том, что вирусы в первую очередь заражают системный диск и активные пользовательские файлы., второй диск иногда не подвергается заражению.
- При активной работе в первую очередь изнашивается рабочий диск, а уже потом резервный.
- Также обеспечивается дополнительная защита от случайного удаления файлов.

Минусы:

- Как и в предыдущем подходе, в случае серьезного заражения, могут быть повреждены данные как на основном, так и на резервном диске.
- Не защиты от умышленного удаления данных.
- В случае проблем с блоком питания может сгореть не только основной, но и резервный жесткий диск.

2. Использование внешнего жесткого диска с USB интерфейсом (подходит для всех

владельцев компьютеров, включая ноутбуки).

Данный подход заключается в кратковременном подключении жесткого диска (или флешки большого объема) с помощью кабеля USB (желательно версии 3.0 для более быстрого переноса данных) к стационарному компьютеру (ноутбуку).

Вся необходимая информация копируется на подключенный диск (флешку) либо в исходном виде, либо в виде подготовленных архивов. Программу для автоматизации этого процесса, например FreeFileSync, я рассмотрю позднее и возможно в отдельной статье.

Плюсы этого подхода:

- высокая степень сохранности данных и защита от повреждения вирусами
- в случае порчи оборудования, резервная копия всегда остается не тронутой на внешнем диске
- высокая степень мобильности

Минусы:

- данные не всегда актуальны (зависит от частоты резервного копирования)
- дополнительные трудозатраты: требуется периодически доставать из сейфа (тумбочки) диск и подключать его для синхронизации, проверять актуальность данных (информации)
- чем реже проводиться резервное копирование, тем оно, как правило, выполняется дольше.

3. Использование сетевой системы хранения данных (также называют сетевое хранилище или NAS)

Это наиболее дорогой вариант, т.к. требует затрат на покупку как самого жесткого диска, так и непосредственно системы хранения данных. Безусловно, можно приобрести устройство на основе жесткого диска, оснащенного сетевым контроллером, но такие устройства требую более бережного обращения и не предназначены для постоянной работы в режиме 24x7, т.е. круглосуточно.

Плюсы этого подхода:

- умеренно высокая степень сохранности данных
- при правильном разграничении доступа - высокая степень защиты от

повреждения вирусами
- высокая степень доступности по сети с разных устройств (компьютер , телевизор, телефон, IPTV приставка, планшет)

Минусы:

- при использовании пользователем с зараженного компьютера - высокая вероятность потери данных (заражения)
- высокая стоимость оборудования
- чувствительно к перепаду электроэнергии (может быть повреждён) и требует подключение через источник бесперебойного питания (ИБП)
- при неправильном подключении и настройке оборудовании - вероятность утечки данных в интернет

4. Использование облачной системы хранения данных

Если вас не смущает тот факт, что в документах (файлах), хранящихся на вашем компьютере могут копаться специалисты различных технических служб, например облачной системы хранения данных или их будут анализировать сотрудники спецслужб, например ФСБ или АНБ, то рекомендации, описанные ниже, вполне возможно, обеспечат вам спокойный сон.

Стоит отметить, что при наличии дополнительного шифрования данных, можно обеспечить и более высокую скрытность и безопасность данных. Все таки не стоит недооценивать такой фактор как случайные обстоятельства или чей-то злой умысел. Всегда есть вероятность развития наиболее худшего сценария событий.

Но и в этом случае есть хорошее решение, например с использованием шифрованных логических томов при помощи TrueCrypt или VeraCrypt.

5. Сохранение данных по старинке

Этот вариант уже мало где используется, но я думаю, он не потерял своей актуальности. Заключается он в копирование всех данных на оптические диски, например DVD-диски. Степень сохранности дисков при их высоком качестве, отсутствии попадания прямого солнечного света и умеренной комнатной температуре может достигать 25 - 30 лет. Даже обычные дешевые китайские диски вполне могут сохраняться в течение 5-10 лет.

Альтернативой записи дисков может послужить использование старых жестких

дисков. При отсутствии перепадов температуры и магнитного излучения, такой диск способен достаточно долго сохранять записанные данные (информацию).

Ну и исключительно для справки стоит упомянуть о старенькиx магнитных дискетах, 5.25 дюйма и 1.44 дюйма. Информация на них доступна спустя без малого 25 лет. Другое дело, что прочитать их затруднительно, но вместе с тем, информация сохранена отлично.

На теоретической части пока остановимся.

Об этом и некотором другом будет написано в продолжение статьи "Как сохранить свои личные данные".