обчислювальних системах. К. НТУУ "КПІ" //Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні. Випуск 8// 2004, с. 20-26. ***5****. Матов О. Я., Василенко В. С., Будько М. М. Визначення залишкового ризику при оцінці захищеності інформації в інформаційно – телекомунікаційних системах. // К.: Реєстрація, зберігання і обробка даних, 2004, Т. 6, № 2, с. 62 – 74.* ***6.*** *Василенко В. С., Будько М. М. Методики визначення вихідних даних для оцінки залишкових ризиків у ЛОМ. НТУУ "КПІ" //Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні. Випуск 9// 2004, с. 110-120.*

УДК 004.056.5(045)

БЕЗОПАСНОСТЬ ПРИ ПЕРЕНОСЕ ДАННЫХ НА ДРУГУЮ ОПЕРАЦИОННУЮ СИСТЕМУ

Сергей Егоров
Национальный авиационный университет

Анотація: **Розроблено рекомендації щодо безпечного зберігання даних при електронному документообігу і безпечного переносу даних при переході на молодші операційні системи або на інший комп'ютер.**
Summary: **The recommendations for the safe storage of data in electronic document and safely moving the data in the transition to lower operating system or to another computer.**
Ключові слова: **Електронний документообіг, резервне копіювання, безпека даних, захист даних, бекап.**

Постановка проблемы

В связи с резким ростом в повседневной жизни электронного документооборота и влиянием информационных войн на электронную документацию вопрос о безопасном переходе на другую операционную систему (ОС) и безопасном резервном копировании становится актуальным. Постановка задачи: целью данной статьи является разработка рекомендаций для осуществления безопасного перехода с версии ОС Windows на другую, младшую версию.

Анализ последних научных исследований и публикаций

Большой спектр проблем защиты пользовательских ОС и рекомендации для их решения были изложены в [1 – 2]. Однако в этих источниках была обойдена стороной проблема безопасного резервного копирования, которые необходимо решить при апгрейде ОС или переходе на младшую версию. Нет чётких рекомендаций по этому вопросу и в [3 – 5], а затронуты лишь основные процедуры резервного копирования с помощью своих программных продуктов. Также следует отметить, что многие функции, которые предлагаются программными продуктами, предложенными в [3 – 5] с успехом могут быть заменены штатными средствами ОС. Пользуясь, например, штатными средствами ОС Windows Vista, которые она предлагает для резервного копирования, можно существенно сэкономить время, деньги и место на жестком диске, которое будет занимать соответствующее программное обеспечение от стороннего производителя.

Стратегия планирования резервного копирования

Резервное копирование – создание копии файла, хранящейся в другом месте отдельно от оригинала. Резервное копирование файла можно создавать многократно для отслеживания его изменений.

Резервное копирование позволяет защитить файлы в случае их потери в результате случайного удаления, атаки червя или вируса, аппаратного сбоя. Во всех этих случаях можно без проблем извлечь из архива нужную копию файла.

Следует выполнять резервное копирование тех файлов, которые трудно или невозможно заменить или если файл часто изменяется. Кандидатами на резервное копирование могут быть следующие файлы: рисунки, цифровые фотографии, видео, финансовые документы, проекты.

Не следует выполнять резервное копирование тех программ, которые обычно занимают много дискового пространства, так как их можно восстановить, воспользовавшись дисками оригинальных продуктов для повторной установки.

Частота резервного копирования зависит от количества создаваемых файлов и от того как часто они создаются или изменяются. Создавая файлы каждый день, возможно, имеет смысл делать резервные копии

еженедельно или даже ежедневно. Если создано сразу слишком много файлов, например, цифровых фотографий и видео с вашего юбилея, необходимо сразу сделать резервную копию. Лучше всего запланировать резервное копирование для его автоматического выполнения, чтобы о нём не думать. Резервное копирование можно выполнять вручную между автоматическими резервными копированиями.

Количество места, необходимого для резервного копирования зависит от размера файлов, резервная копия которых делается. Если используются штатные средства резервного копирования Windows (начиная с Windows Vista) то ОС следит за резервными копиями. Если такая существует, то для экономии места эта копия просто обновляется, а не создаётся новая.

Источники угроз

Согласно [1] в качестве источника угроз информационной безопасности может выступать человек либо группа людей, а также некие, независящие от деятельности человека, проявления. Исходя из этого, все источники угроз можно разделить на три группы.

- Человеческий фактор. Данная группа угроз связана с действиями человека, имеющего санкционированный или несанкционированный доступ к информации. Угрозы этой группы можно разделить на:
  - внешние (к ним относятся действия кибер-преступников, хакеров, интернет-мошенников, недобросовестных партнеров, криминальных структур);
  - внутренние (к ним относятся действия персонала компаний, а также пользователей домашних компьютеров); действия данных людей могут быть как умышленными, так и случайными.
- Технический фактор. Эта группа угроз связана с техническими проблемами: физическое и моральное устаревание использующегося оборудования, некачественные программные и аппаратные средства обработки информации. Все это приводит к отказу оборудования и зачастую к потере информации.
- Стихийный фактор. Эта группа угроз включает в себя природные катаклизмы, стихийные бедствия и прочие форс-мажорные обстоятельства, независящие от деятельности людей.

При проектировании Комплексной системы безопасности необходимо учитывать все вышеперечисленные источники угроз.

Согласно [1] виды угроз бывают такими:

- черви (worms), вирусы (viruses)
- троянские программы (Trojans)
- программы-рекламы (adware)
- программы-шпионы (spyware)
- программы-шутки (jokes)
- программы-маскировщики (rootkit)
- хакерские атаки, фишинг (phishing)
- дозвон на платные Интернет-ресурсы
- навязчивая реклама
- спам (spam), прочие опасные программы.

Переменные среды

Для конфигурирования, поиска, выделения памяти определённым программам и управления приложениями операционная система Windows и прикладные программы требуют определённой информации, называемой переменной среди системы и пользователей. В Windows Vista их можно посмотреть на вкладке «Дополнительно» окна «Система» нажав на кнопку «Переменные среды».

Системные переменные среды определяются в Windows независимо от того, кто зарегистрировался на компьютере. Если вы зарегистрировались как член группы Администраторы, то можете добавить новые переменные или изменить их значения.

Переменные среды пользователя устанавливаются индивидуально для каждого пользователя одного и того же компьютера. Сюда включаются любые переменные среды, которые вы хотите определить, или переменные, определённые вашим приложением, например путь к файлам приложения.

В зависимости от версии Windows папки, в которых хранятся одни и те же данные, расположены в разных местах. Например, в Windows XP профиль пользователя расположен в папке C:\Document and Settings\Имя Пользователя\. А в Vista и Seven C:\Users\ Имя Пользователя\. Путь к папкам, в которых приложения хранят данные пользователя, выглядит соответственно так: C:\Document and Settings\Имя Пользователя\Application Data и C:\Users\Имя Пользователя\AppData\Roaming.

Все эти пути записаны в системных переменных, которые называются одинаково для всех версий Windows, начиная с Windows 95. Путь к профилю пользователя хранится в переменной %USERPROFILE%, а путь к папкам, в которых приложения хранят данные пользователя, – %APPDATA%. Посмотреть значения всех системных переменных можно, если ввести в окне консоли «set» (без параметров), а использовать как в консоли, так и в командной строке Проводника. Используя имена системных переменных легко попасть в папку с профилем, например, Mozilla Firefox, чтобы сохранить закладки.

Системные переменные также применяются для облегчения написания сценариев, которые выполняются при входе пользователя в систему и служат для настройки рабочей среды пользователя. В нашем случае системные переменные служат просто для облегчения доступа к папкам с данными пользователя. Без использования системной переменной, для того, чтобы получить доступ к папке с профилем Mozilla Firefox, в консоли нужно набрать следующую команду (для ОС Windows Vista): cd "C:\Users\Имя Пользователя\AppData\Local\Mozilla\Firefox\Profiles". Кавычки нужны, если путь содержит пробелы. С использованием системной переменной этот же путь выглядит так: cd %APPDATA%\Mozilla\Firefox\Profiles. Использование системных переменных в командной строке Проводника позволяет быстро переходить к нужным папкам, не включая отображение скрытых системных папок и файлов. Всё, что от вас требуется для этого, – ввести в адресной строке Проводника имя соответствующей системной переменной, заключённой между знаками процента, и нажать клавишу «Enter». Если вы знакомы с технологией программирования .NET, то вам не составит труда написать соответствующую программу для доступа к нужным папкам, пути которых хранятся в переменных среды, используя пространство имён System.Environment.

Документы

По умолчанию, все документы пользователя сохраняются в переменной %USERPROFILE%. Это место не самое удачное для сохранения ценной информации. Это связано с тем, что при крахе системы у вас могут появиться проблемы с доступом к данным или даже их восстановлением. Чтобы максимально уменьшить возникновение такой ситуации, необходимо переместить папку с документами на другой диск. В идеальном случае даже на другой винчестер, а не просто на логический диск. Делается это довольно просто. В контекстном меню значка «Документы» (для ОС Windows Vista или Windows 7) или «Мои документы» (для ОС Windows XP) выберите «Свойства» и на вкладке «Папка» (для ОС Windows Vista) или «Папка назначения» (для ОС Windows XP) нажмите кнопку «Переместить» и укажите новую папку для документов.

Для повышения отказоустойчивости и эффективности систем компьютерных запоминающих устройств можно использовать систему RAID (Redundant Array of Independent/Inexpensive Disks) [6]. Однако через дороговизну (наличие контроллера RAID, нескольких жестких дисков) используется, в основном, в серверах.

Почта

Почтовые клиенты содержат базу данных писем и контактов. По умолчанию эти базы хранятся на системном диске. Поэтому с ними надо поступить также, как и с документами: переместить с системного диска на другой диск (логический, а лучше физический). Почтовые клиенты Microsoft Outlook Express, Windows Mail, The Bat! позволяют указать расположение папки с сообщениями.

Если вы зарегистрировали свой почтовый ящик в браузере Opera, то все письма тот клиент сохраняет в %APPDATA%\Opera\Opera\mail. Для изменения расположения писем этого клиента в «Редакторе настроек» программы укажите (opera:config#Mail|Mail Root Directory) и задайте новую папку.

Закладки

В системном браузере ОС Windows резервное сохранение «Избранного» и файлов cookie делается очень просто: нужно вызвать окно «Параметры импорта-экспорта», с помощью меню «Файл», в котором надо выбрать пункт «Импорт и экспорт», и выбрать в этом окне команду «Экспортировать в файл».

В Mozilla Firefox 6 эта операция делается следующим образом: с помощью меню «Закладки», в котором надо выбрать пункт «Показать все закладки», вызвать окно «Библиотека». В этом окне, на панели инструментов выбрать выпадающий список «Импорт и резервное копирование», в нём выбрать «Экспорт в HTML…» и после чего указать расположение резервной копии.

Резервную копию всего профиля таких программ, как Mozilla Suite, SeaMonkey, Firefox, Thunderbird и Netscape можно сохранить при помощи программы MozBackup 1.5.1.

Драйвера

Перед тем, как перейти на младшую ОС необходимо выяснить у производителей аппаратной части или у производителя ОС, поддерживается ли данное устройство новой ОС.

Если у вас имеется резервная копия системы и задействована функция теневого копирования, а также имеются дистрибутивы драйверов, то резервное копирование драйверов не имеет никакого смысла. Тем более, что производители аппаратного обеспечения регулярно выпускают обновления к своим продуктам до тех пор, пока данный продукт выпускается. А в случае неудачной установки драйверов ОС (только Windows Vista и Windows 7) способны сделать откат установки (если задействована функция теневого копирования системного диска).

Резервная копия драйвера имеет смысл только в одном случае: вы потеряли дистрибутив драйвера и найти его, в том числе и в Интернете, невозможно. В этом случае для извлечения драйверов из ОС Windows можно воспользоваться программой DriverMax 5.9 или Double Driver.

Пароли

Пароль предоставляет пользователю доступ к очень ценной и важной информации пользователя. Потеря пароля может привести и к потере информации, которая была защищена этим паролем, или эта информация может попасть в руки злоумышленника. Поэтому к проблеме хранения паролей следует отнестись ответственно. Проблему запоминания паролей каждый решает по своему: можно завести один пароль для всего и подвергать себя огромному риску, а можно для каждого сайта завести отдельный пароль, которые можно хранить в специальных менеджерах паролей, в зашифрованном виде; база паролей в них защищена ключом. В качестве таких программ можно порекомендовать, например, Password Safe 3.25, KeePass.

Профиль пользователя

Резервным копированием профиля пользователя почти всегда пренебрегают. Хотя этим ни в коем случае пренебрегать нельзя по той простой причине, что в профиле пользователя хранятся данные о настройках рабочего стола, вида папок в проводнике, текущие настройки всех профилей приложений, которыми пользуется данный пользователь.

В ОС Windows XP резервное копирование профиля пользователя делается так: на вкладке «Дополнительно» окна «Свойства системы», которое можно вызвать, нажав пиктограмму «Система» на «Панели управления», нажать кнопку «Параметры» в группе «Профили пользователей». В появившемся окне «Профили пользователей» выбрать нужного пользователя, а затем нажать кнопку «Копировать» и в появившемся окне указать место, куда копировать. Делается всё это под учётной записью с правами администратора (но не из-под записи, с которой делается копия).

Для ОС Windows Vista резервное копирование профиля пользователя делается следующим образом: в адресной строке Проводника введите команду SystemPropertiesAdvanced и нажмите клавишу «Enter».

В появившемся окне на вкладке «Дополнительно» нажать кнопку «Параметры» в группе «Профили пользователей». В появившемся окне «Профили пользователей» выбрать нужного пользователя, а затем нажать кнопку «Копировать» и в появившемся окне указать место, куда копировать. Делается всё это под встроенной учётной записью «Администратор».

Перенос данных со старшей ОС на младшую

Для перехода на Windows Vista или Windows 7 вам понадобится бесплатная утилита от Microsoft – Windows Easy Transfer (средство переноса данных Windows). Её можно найти на сайте компании Microsoft.

С помощью средства переноса данных Windows можно перенести большую часть файлов и параметров программ. А именно:

- файлы и папки; все, что находится в папках «Документы», «Изображения» и «Общие документы»; с помощью дополнительных параметров можно выбрать дополнительные файлы и папки для переноса;
- параметры, контакты и сообщения электронной почты; сообщения, параметры учетных записей и адресные книги из Microsoft Outlook Express, Outlook, Почты Windows и других программ электронной почты;
- параметры программ; параметры, которые позволят сохранить такие же настройки программ, как и на старом компьютере; сначала необходимо установить программы на новый компьютер, так как Windows Easy Transfer не переносит сами программы; возможно, некоторые программы не будут работать с этой версией Windows, например программы обеспечения безопасности (которые часто несовместимы со всеми версиями Windows), антивирусные программы, брандмауэры (на новом компьютере уже должен быть запущен брандмауэр для обеспечения безопасности при переносе данных), а также программы драйверов (часть которых может быть несовместима со всеми версиями Windows);

- учетные записи пользователей и параметры; цветовые схемы, фоновые рисунки рабочего стола, сетевые соединения, экранные заставки, шрифты, параметры меню «Пуск», параметры панели задач, папки, определенные файлы, сетевые принтеры и диски и параметры специальных возможностей;
- параметры подключения к Интернету и избранное; параметры подключения к Интернету, избранное и файлы cookie;
- музыка; электронные музыкальные файлы, списки воспроизведения и обложки альбомов;
- изображения и видео; изображения — во всех файлах визуального типа (например JPG, BMP, GIF) и личные видеозаписи.

Если у вас отсутствует подключение к Интернету, то эту утилиту можно вытащить из самой ОС Windows Vista или Windows 7. Откройте меню «Пуск\Стандартные\Служебные\ Средство переноса данных Windows» и укажите «Внешний диск или USB-устройство флеш памяти». После этого выберите строку «Это мой новый компьютер». На вопрос о готовности переноса данных ответьте «Нет». Далее, чтобы программа скопировала исполняемый модуль на внешний диск, нажмите кнопку «Необходимо установить его сейчас» и выберите нужный тип носителя. После этих шагов Windows Vista или Windows 7 запишет на указанный вами диск утилиту, необходимую для переноса данных. Далее, подсоедините съёмный диск к старому компьютеру, запустите на нём Windows Easy Transfer и на втором шаге выберите необходимый тип носителя. Обратите внимание на то, что можно переносить данные не только посредством съёмных USB-накопителей, но ещё и по сети, посредством оптических приводов, USB-кабелей для переноса данных с одного компьютера на другой (обычные USB-кабели не подойдут). На следующем шаге нажмите кнопку «Это мой исходный компьютер», после чего программа совершит поиск всех персоональных данных пользователя и запишет их на диск в виде архивов. С помощью кнопки «Настройка», которая располагается под каждой из учётных записей, можно указать какие данные и параметры должны быть переданы, защитить файлы с данными паролями. Далее нажмите кнопку «Сохранить», укажите место сохранения и имя файла. Кликните опять по кнопке «Сохранить». После того, как данные будут скопированы на внешний диск, подключите его к новому компьютеру, запустите Windows Easy Transfer. Выберите нужный носитель и выберите файлы с расширением MIG и нажмите кнопку далее для начала переноса настроек в новую ОС

Выводы

Единственный способ максимально обезопасить себя от потери данных – это резервное копирование, с использованием рекомендаций, которые приведены в данной статье, и соблюдение рекомендаций, приведенных в [2].

Резервное копирование актуально не только в процессе эксплуатации ОС, но и при переходе на новую ОС. При первой установке новой ОС целесообразно создать резервную копию ОС сразу после того, как вы установите на неё всё программное обеспечение, которое вы используете, вместе с драйверами. Для создания резервной копии (если у вас ОС Windows Vista) зайдите в «Панель управления», нажмите в ней пиктограмму «Центр архивации и восстановления», в группе «Архивация файлов или всего содержимого компьютера» нажать кнопку «Архивировать компьютер» и далее следуйте подсказкам мастера архивации. По завершении и вас будет резервная копия системного диска (по умолчанию он всегда выбран) вместе с копией диска, который вы указали мастеру архивации. Центр архивации и восстановления Windows Vista позволяет делать копии и отдельных папок, которые вы укажете мастеру архивации. Для этого нажмите кнопку «Архивировать файлы». Последняя функция доступна только на дисках, которые отформатированы под файловую систему NTFS (New Technology File System).

Альтернативно, можно воспользоваться средствами, предлагаемыми в [3 – 5].

Литература: ***1.*** *Kaspersky Internrt Security 6.0. [электронный ресурс]: © ЗАО «Лаборатория Касперского» - Электорон. дан. (1 файл) – М., 2007. -319 с. – Режим доступа: http://docs.kaspersky-labs.com/ russian/kav6.0ru.pdf. – Назва з екрана.* ***2.*** *С. В. Єгоров Захист операційних систем від можливих загроз / С. В. Єгоров // Вісник НАУ. – 2011. – №4. – С. 80 – 82.* ***3.*** *Acronis® Backup & Recovery™ [электронный ресурс]: © Acronis Inc. – Режим доступа: http://www.acronis.ru/backup-recovery/. – Название с экрана.* ***4.*** *Comodo Backup [Electronic resource]: © Comodo Group, Inc. – Mode of access: http://www.comodo.com/home/data-storage-encryption/comodo-backup.php. – Title from the screen.* ***5.*** *Program Documentation & Help Files [Electronic resource]: © 2011 Runtime Software – Mode of access: http://www.runtime.org/data-recovery-documentation.htm. – Title from the screen.* ***6.*** *С. Мюллер. Модернизация и ремонт ПК. – М.: Издательский дом «Вильямс», 2006. – 1318 с.*