Правила хранения персональных данных

Владимир Безмалый

Сегодня мы все чаще храним и свои, и чужие персональные данные на компьютерах. Безусловно, хранить адреса, номера телефонов, адреса электронной почты и блогов, а также такую информацию, как номер паспорта, водительского удостоверения, а то и номер банковской карты, гораздо удобнее в электронном виде. Но вот безопасно ли? Если этому не уделять внимания, то, конечно, нет. А ведь у каждого из нас есть подобная информация о наших друзьях и знакомых. Причем с каждым днем ее все больше и больше.

Ежедневно в Интернете появляются новые сообщения о преступлениях, связанных с хищением персональных данных. Но тем не менее люди не становятся менее доверчивыми и все так же продолжают хранить персональные данные, как свои, так и чужие, не уделяя должного внимания их безопасности.

А когда вы в последний раз пытались разобрать ворох визиток, лежащий на столе? Наверное, когда искали нужный телефон. Да и то при этом неоднократно пожалели, что не ведете такую базу в электронном виде, верно?

И хотя по закону персональные данные — совокупность ведомостей о физическом лице, которое идентифицировано или может быть идентифицировано, всегда ведь можно сослаться на то, что мы, как физические лица, не попадаем под действие закона о защите персональных данных и не отвечаем за нарушение данного закона, но кому из нас понравится обвинение в том, что именно с нашего компьютера ушли данные о друзьях и партнерах? А то и наши собственные данные? Думаю, никому.

Как же правильно хранить подобные данные на своем компьютере? В данной статье мы рассмотрим несколько возможных технологий и соответственно примеров программного обеспечения. На самом деле их намного больше.

Шифрование всего компьютера

На мой взгляд, это кардинальный подход. Вариантов программного обеспечения, осуществляющих полное шифрование всех жестких дисков, масса. Я остановлюсь лишь на тех, которыми пользуюсь сам.

Шифрование BitLocker

Я считаю, что шифрование BitLocker — оптимальное решение. Особенно если ваш компьютер оснащен TrustedPlatformModule (TPM). Правда, в этом случае вам придется задействовать Windows 7 Ultimate (поскольку речь идет о малых предприятиях или вообще физических лицах, я думаю, что вряд ли кто-то из этой группы использует Windows 7 Enterprise).

Итак, если на вашем ноутбуке (или стационарном компьютере) установлена версия Windows 7 Ultimate, то шифровать с помощью BitLocker — идеальный вариант. Единственный совет: если ваш компьютер оснащен TPM, вы можете применять данный модуль для хранения ключа. Выбирайте шифрование TPM+PIN, то есть фактически используйте для расшифровывания двухфакторную аутентификацию.

Если же ваш компьютер не оснащен TPM, вам придется использовать в качестве места для хранения ключа флэш-накопитель USB. Не забудьте, естественно, в том и другом случае сделать резервную копию ключа (конечно же, не на тот USB-ключ, который будет использоваться в качестве основного) и распечатайте ключи. Потом положите распечатанные ключи в какое-то закрытое хранилище. И не забудьте, что не следует носить USB-флэш с записанным ключом в той же сумке, что и ноутбук!

SecretDisk 4.0 от компании «Аладдин Р. Д.»

SecretDisk 4 — система защиты конфиденциальной информации и персональных данных, хранящихся и обрабатываемых на персональном компьютере, от несанкционированного доступа плюс двухфакторная аутентификация для доступа к зашифрованным данным и защита системного раздела, прозрачная работа для пользователя, соответствие закону по защите персональных данных (ФЗ-152) и наличие сертифицированной версии продукта.

Перечислим случаи, когда бывает необходим SecretDisk 4.

- При работе на ноутбуке. Утеря или кража ноутбука, несанкционированное использование посторонними лицами (во время деловых поездок или на отдыхе).
- При работе на персональном компьютере в офисе. Несанкционированный доступ к данным по локальной сети или неправомерное использование посторонними лицами во время отсутствия пользователя на рабочем месте.
- Если компьютер передается на сервисное обслуживание. Несанкционированный доступ к данным во время проведения ремонтных и сервисных работ внутренней ИТ-службой или внешней сервисной компанией.
- Если информация конфиденциального характера переносится или пересылается на съемных носителях (утеря или кража носителей).

Необходимо обеспечить выполнение требований федерального закона «О персональных данных» от 27 июля 2006 года. Нарушение конфиденциальности персональных данных, которые хранятся и обрабатываются на персональных компьютерах в организации.

Для чего предназначен SecretDisk?

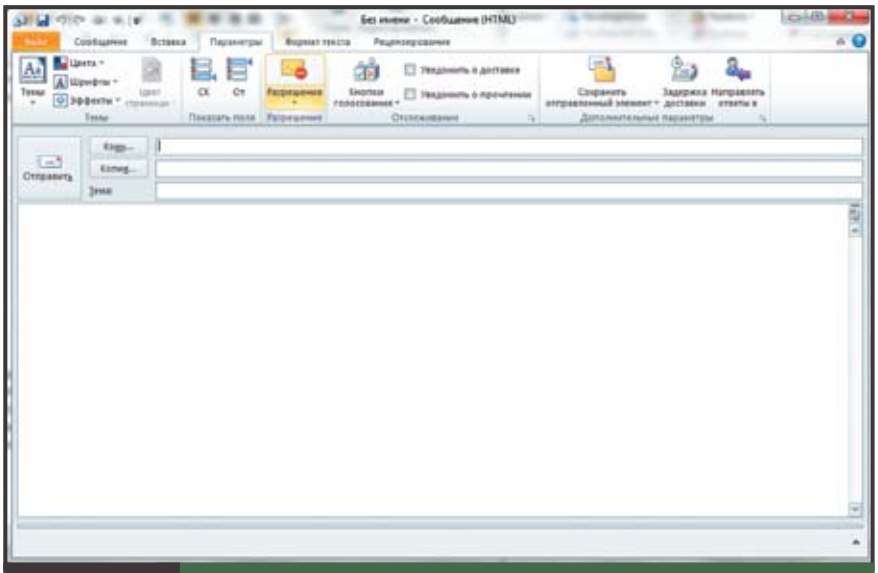
- Защита от несанкционированного доступа и раскрытия конфиденци-

альности информации, хранящейся и обрабатываемой на персональном компьютере или ноутбуке.
- Защита информации при переносе и хранении на съемных носителях.
- Разграничение прав пользователей на доступ к защищенной информации с использованием надежной двухфакторной аутентификации (владение электронным ключом e-Token и знание PIN-кода).

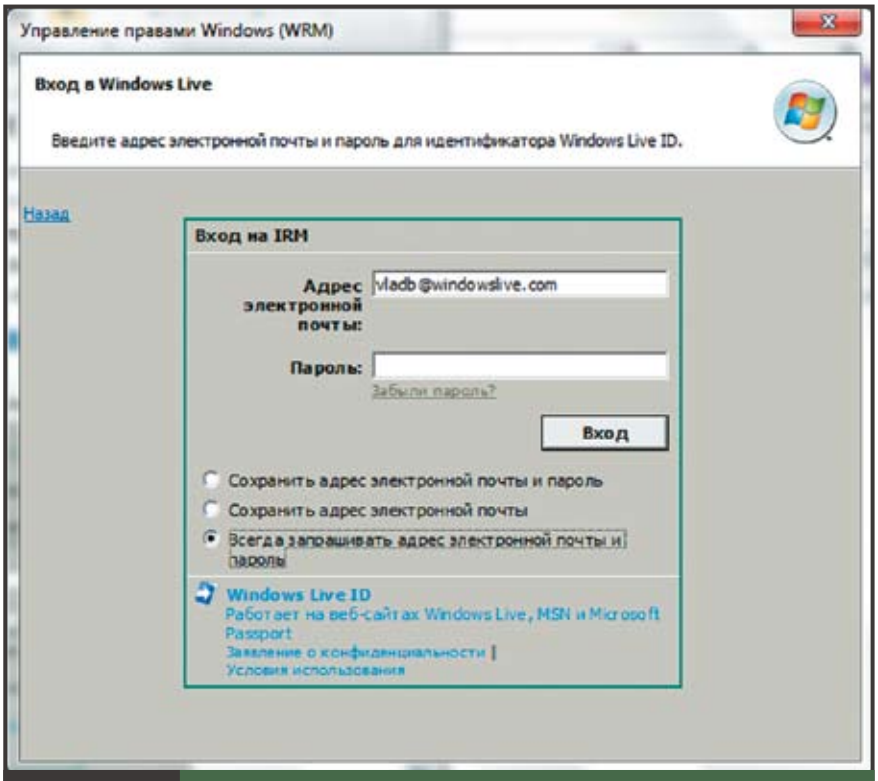
В данном случае вы сможете шифровать весь жесткий диск, если ваш компьютер работает под управлением любых версий операционных систем Microsoft Windows XP, Microsoft WindowsVista, Microsoft Windows 7.

Недостаток обоих предложенных выше способов состоит в том, что контейнер с вашими персональными данными привязан к компьютеру, следовательно, вы не можете носить его с собой. Разве что сделаете шифрованный сменный носитель. Опять же учтите, что, для того чтобы сменный носитель, зашифрованный на компьютере под управлением Windows 7 Ultimate, вы смогли прочесть на компьютерах под управлением более младших операционных систем, параметр групповой политики Allow access to BitLocker-protected removable data drives from earlier versions of Windows должен быть установлен в значение «Да» или не настроен!

В случае использования SecretDisk вы можете создать криптоконтейнер, но тогда на том компьютере, на котором вы хотите прочесть из него информацию, также должно быть установлено соответствующее программное обеспечение, что, согласитесь, далеко не всегда удобно.



Экран 1 Параметры



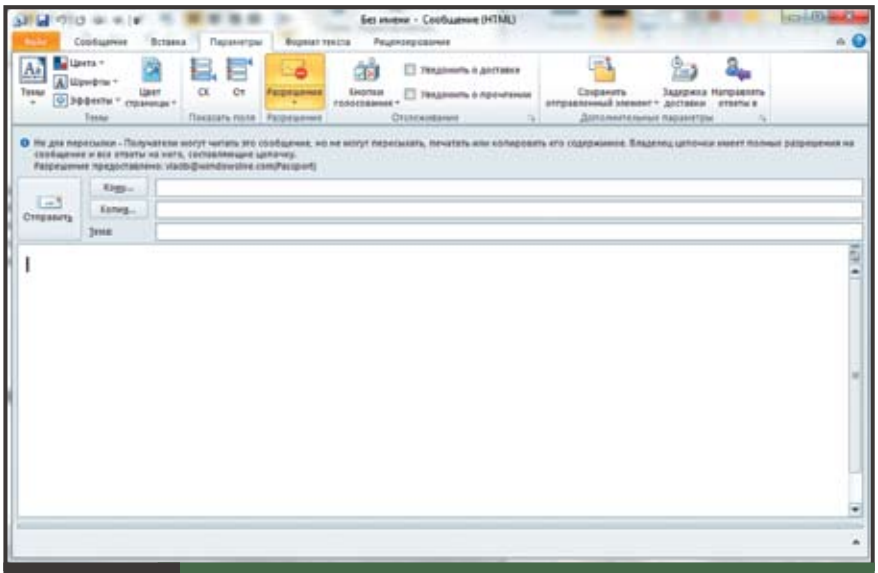
Экран 2 Регистрация в Windows Live

IRM

Несмотря на то что технология Information Rights Management (IRM) применяется в Microsoft Office начиная с версии Office 2003, ее использование и сегодня вызывает у ИТ-специалистов много вопросов. Технология управления правами на доступ к данным IRM позволяет ограничивать действия, которые может произвести пользователь с файлами, загруженными из библиотек, списков SharePoint или сообщений электронной почты. Это дает возможность ограничить круг пользователей, которым разрешено открывать или расшифровывать названные файлы (письма). Вместе с тем администратор может ограничить права пользователей, имеющих разрешение на чтение этих файлов, запретить им копировать файлы, копировать текст из файла, пересылать письма по электронной почте или открывать их после определенной даты.

IRM + Windows Live

Что же делать в подобных случаях? Запускать службу управления правами? Конечно, это выход. Но как



Экран 3 Задание нужных разрешений

быть в небольшой компании, где всего-то 5–10 сотрудников? Или как поступить при пересылке сугубо личного письма, если необходимо, чтобы адресат не мог переслать его дальше или распечатать? Здесь на помощь придет технология, применяемая Microsoft Outlook 2010.

Для маленькой компании или для частного пользователя подойдет вариант применения IRM на основе Windows Live ID. Как защитить ваше сообщение? Для того чтобы выставить разрешения своему письму, необходимо сделать следующее. Во вкладке «Параметры» письма выберите пункт меню «Разрешения» (экран 1).

Если вы впервые настраиваете IRM, вам придется выполнить еще несколько действий. Вначале потребуется оформить подписку на службу управления правами на доступ к данным. После этого, в случае отсутствия идентификатора Windows Live ID, вам будет предложено его создать. После создания идентификатора Windows Live ID (или если у вас уже есть этот идентификатор) потребуется ввести его (электронный адрес), а также пароль (экран 2).

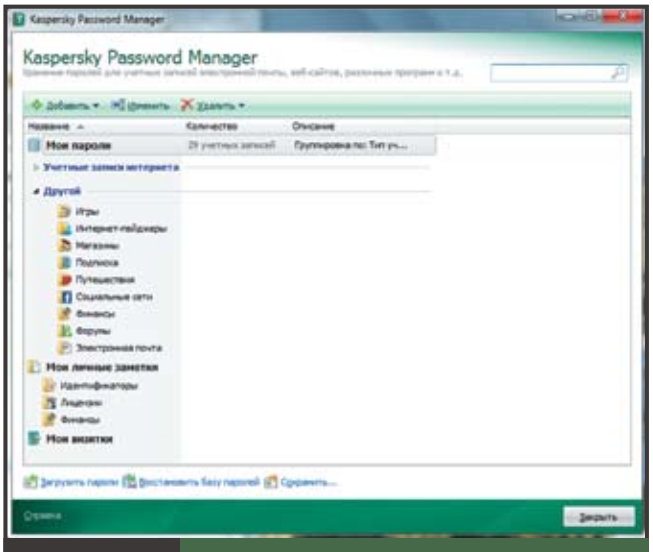
Далее вам нужно будет указать, используете вы частный компьютер или общедоступный. На этом настройка механизма управления правами WRM завершается. Если вы обладаете несколькими учетными записями Windows Live ID, вы всегда сможете выбрать, какую из них использовать в данный момент. После этого вы можете приступать к отправке письма, задав нужные разрешения (экран 3).

Если получатель использует веб-интерфейс, а не клиентскую программу для работы с почтой, ему придется установить у себя дополнительную надстройку для Internet Explorer. После перехода по ссылке, указанной в теле письма, нужно будет загрузить надстройку RightsManagementAdd-on для Internet Explorer.

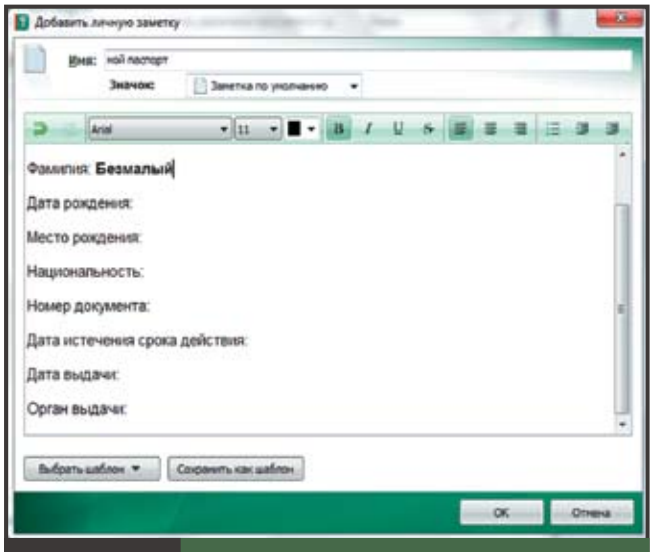
Как осуществляется защита содержимого?

При использовании функции управления правами на доступ к данным вы получаете следующие возможности защиты:

- запрет копирования файла, изменения и печати его содержимого, отправки по факсу, копирования, вырезания, вставки содержимого файла пользователями, которым предоставлен доступ только на просмотр;
- запрет копирования с помощью клавиш PrintScreen в Microsoft Windows пользователями, имеющими разрешение на просмотр данных;
- предотвращение просмотра содержимого пользователями, которые не имеют на это разрешения, при отправке содержимого в электронном сообщении после загрузки с сервера;



Экран 4 Основное окно Kaspersky Password Manager



Экран 5 Паспорт

- ограничение доступа к сообщению по истечении заданного времени.

Вместе с тем нужно учесть, что вы не сможете защитить данные с помощью указанной технологии в следующих случаях:

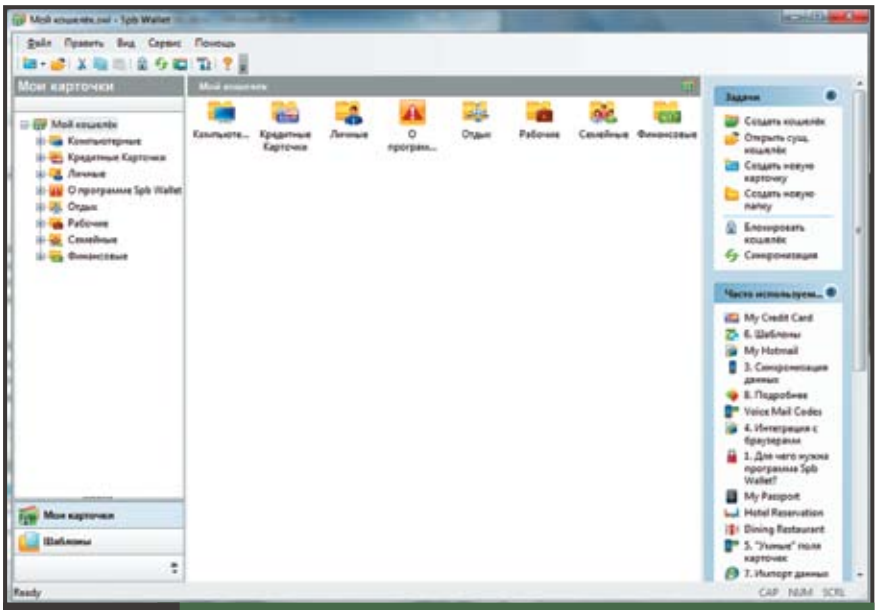
- при удалении, краже, записи или передаче данных с помощью шпионского программного обеспечения, троянских программ, программ записи нажатий клавиатуры и т. д.;
- при утере или повреждении содержимого в результате воздействия вредоносного программного обеспечения;
- если пользователь захочет вручную переписать сообщение или сфотографировать его;
- при копировании содержимого экрана с помощью программ сторонних разработчиков, делающих с него снимки.

Kaspersky Password Manager

Данное программное обеспечение, как следует из названия, в первую очередь является менеджером паролей. Однако на самом деле область его применения намного шире, так как фактически вы можете хранить не только свои пароли, но и персональные данные (данные о паспорте, водительском удостоверении, банковских карточках и счетах и т. д.). Причем, естественно, не только свои персональные данные, но данные ваших близких, сотрудников или партнеров.

Рассмотрим подробнее, как работает эта программа. Установка ее не вызывает никаких сложностей, поэтому здесь я не буду ее описывать. Сразу же после установки вам будет предложено на выбор несколько вариантов авторизации.

- Мастер-пароль (по умолчанию). При этом автоматически будет отслеживаться сложность вашего мастер-пароля.
- Аутентификация с помощью USB-flash. Естественно, в этом случае вы должны носить флэшку не в той же сумке, что и ноутбук ☺.
- Bluetooth-устройство.
- Без аутентификации. Данный способ, несомненно, самый удобный, однако не рекомендуется ввиду отсутствия безопасности как таковой.



Экран 6 Главное окно SPB Wallet

После того как вы введете свой мастер-пароль, на экране появится основное окно программы (экран 4). После этого вы можете вручную ввести пароли к необходимому программному обеспечению (например, ICQ). Однако наиболее интересным, на мой взгляд, является создание личных заметок. В диалоговом окне вам будут предложены шаблоны личных заметок (хотя вы можете создавать их сами). В частности, с помощью данного модуля можно хранить такую информацию, как:

- лицензии на использование программного обеспечения;
- кредитная карта;
- банковский счет;
- удостоверение личности;
- водительские права;
- паспорт;
- виза;
- удостоверение избирателя;
- студенческий билет;
- параметры подключения к Интернету.

Для себя я бы еще добавил налоговый код (весьма актуально на Украине). Пример ввода паспортных данных показан на экране 5.

Таким образом вы можете хранить не только свои личные данные. А теперь, на мой взгляд, самое интересное. Если перейти на вкладку «Настройка», то вы сможете изменить алгоритм шифрования своих данных. Для этого нужно выбрать разработчика (по умолчанию — Microsoft Strong Cryptographic Provider) и алгоритм (по умолчанию RC4 с длиной ключа 128 разрядов). Вместе с тем необходимо отметить, что вы можете создать переносную версию на основе USB-накопителя, что позволит воспользоваться вашими данными на другом компьютере.

SPB Wallet

Данная программа реализована как для компьютеров под управлением Windows, так и для смартфонов под управлением Android, Symbian, Windows Mobile, iPhone, а также для iPad. Главное окно программы показано на экране 6.

В данном окне вы можете создать огромное количество карточек, на которых записать как свои, так и чужие компьютерные и персональные данные. От пароля для доступа к любимому сайту или почте до паспортных и иных персональных данных. Всего существует более 60 шаблонов для создания карточек. Кроме того, в данной программе вы можете создавать новые шаблоны и изменять существующие. Пользователи могут обмениваться шаблонами на форуме SpbClub.com/forum.

Владимир Безмалый (vladb@windowslive.com) — специалист по обеспечению безопасности, имеет звания MVP Consumer Security, Microsoft Security Trusted Advisor