Защита данных организации в Microsoft Office 2010

Дата публикации: январь 2011 г.

Оглавление

Краткое содержание

В этом документе рассматриваются новые средства безопасности и улучшения в Microsoft Office 2010, позволяющие защитить пользователей приложений Office в организации от атак с использованием известных уязвимостей. В начале документа описывается процесс эволюции угроз, для предотвращения которых группа технических специалистов Office разработала эти улучшения.
Также описывается развитие системы безопасности Office по мере выпуска новых версий этого набора. Далее рассматриваются три основные задачи обеспечения безопасности, которыми руководствовались разработчики набора Office: усовершенствование процессов проектирования системы безопасности, разработка эффективных и простых в использовании технологий защиты для пользователей приложений Office, а также усиление основных средств и технологий защиты Office. Затем приводится описание модели многоуровневой защиты Office, после чего подробно рассматриваются основные технологии обеспечения безопасности, такие как проверка файлов Office, защищенный просмотр и надежные документы. В заключение дается краткий обзор других улучшений системы безопасности Office 2010, таких как предотвращение выполнения данных, бит аннулирования ActiveX, требования к сложности паролей, а также улучшения технологий шифрования и цифровых подписей.

Система безопасности в предыдущих версиях набора Office

Прежде чем описывать улучшения системы безопасности в Office 2010 и возможности их применения для многоуровневой защиты, рассмотрим процесс эволюции угроз параллельно с непрерывным развитием системы безопасности Microsoft Office. [1]

Развитие системы безопасности Office по мере эволюции угроз

Начиная с середины 90-х годов, когда конкурентоспособность бизнеса на глобальном рынке стала все в большей степени зависеть от наличия подключения к Интернету, структура угроз для ИТ-систем организаций претерпела существенные изменения. Изначально атаки злоумышленников, пытавшихся вторгнуться в сети организаций, были направлены на обнаружение и использование уязвимостей в операционных системах. При этом главной целью чаще всего оказывались серверы, на которых хранились важные бизнес-данные. Поставщики операционных систем, в том числе и корпорация Майкрософт, реагировали соответствующим образом, усиливая защиту серверных операционных систем, включая в них встроенные брандмауэры и применяя более жесткие параметры безопасности в стандартной конфигурации. ИТ-отделы организаций также шли в ногу со временем, применяя дополнительные уровни безопасности, такие как брандмауэры сети периметра и технологии шифрования для более эффективной защиты своих сетей.

[1] В рамках этого документа не рассматривается система безопасности Outlook 2010, которая имеет свою специфику и требует отдельного рассмотрения. Дополнительные сведения о системе безопасности Outlook 2010 см. в разделе «Дополнительные ресурсы» в конце этого документа.

Тем не менее все эти улучшения не позволили полностью исключить атаки на сети организаций или хотя бы уменьшить их число. По мере развития технологий злоумышленники попросту переключили свое внимание с серверов на клиентские компьютеры, повысив интенсивность атак. Предвидя подобные изменения, корпорация Майкрософт с каждым новым выпуском ОС Windows для настольных компьютеров особое внимание уделяла усилению системы безопасности, внедряя новые компоненты защиты, модернизируя основные компоненты, а также предоставляя средства для автоматического управления исправлениями, что позволило максимально быстро устранять уязвимости по мере их обнаружения. Однако, поскольку злоумышленники обычно предпочитают идти по пути наименьшего сопротивления, все эти улучшения повлекли за собой лишь очередное смещение приоритетов, на этот раз в сторону приложений.

Последние несколько лет атаки на сети организаций идут преимущественно по двум направлениям. Во-первых, злоумышленники все чаще обращают внимание на приложения для настольных систем. Это вызвано тем, что в области защиты своих продуктов поставщики операционных систем обычно опережают коллег, специализирующихся на приложениях. Из числа наиболее популярных среди злоумышленников приложений можно выделить такие, как Adobe Flash Player, Adobe Acrobat, Apple QuickTime и Microsoft Office. Во-вторых, существенно возрос объем атак на веб-сайты и веб-приложения, целью которых преимущественно являются серверные базы данных. При этом используются атаки путем внедрения кода SQL и межсайтовые сценарии, позволяющие несанкционированно получать права и внедрять вредоносный код в веб-страницы. В представленном в сентябре 2009 года отчете института SANS исправление уязвимостей в приложениях для настольных систем и веб-приложениях было определено как наиболее приоритетное направление деятельности ИТ-отделов, обеспечивающих безопасность сетей организаций.[2]

---

[2] Институт SANS, отчет *Top Cyber Security Risks — Executive Summary* (Ключевые угрозы кибербезопасности — общие положения); см. веб-сайт http://www.sans.org/top-cyber-security-risks/summary.php.

Почти десять лет корпорация Майкрософт является лидером в области разработки систем безопасности приложений. С момента появления вируса Melissa в марте 1999 г. в каждой новой версии набора Microsoft Office были представлены новейшие технологии и функции обеспечения безопасности, благодаря которым ИТ-отделы организаций всегда находились на шаг впереди злоумышленников. Представив Центр обновления Майкрософт в июне 2005 года, корпорация Майкрософт стала первым из поставщиков, кто предложил услуги автоматического исправления клиентских и серверных приложений, включая Office 2003, Exchange Server 2003 и SQL Server 2000. В настоящее время сторонние поставщики предлагают возможности системы безопасности, которые были представлены еще в предыдущих версиях Office, благодаря чему Майкрософт уверенно сохраняет за собой позиции лидера в этой области. Например, компания Adobe объявила, что в предстоящем выпуске приложения Acrobat Reader будет представлен защищенный режим на базе технологии изолированной среды («песочницы»), который уже реализован в Office 2010.[3]

Прежде чем приступить к изучению новых средств безопасности Office 2010, рассмотрим систему безопасности предыдущих версий набора. Ниже приведен краткий обзор основных улучшений системы безопасности, представленных в предыдущих версиях Office, начиная с версии Office 2000. Большинство этих функций безопасности, начиная с версии Office XP, можно настраивать с помощью групповой политики.

Основные улучшения системы безопасности в Office 2000:

- **Подписи макросов**. Добавление цифровых подписей к макросам, что позволяет проверить подлинность создателя макроса и гарантировать, что макрос не подвергся незаконному изменению.

---

[3] Блог группы разработчиков Adobe Secure Software Engineering Team (ASSET), *Introducing Adobe Reader Protected Mode* (Общие сведения о защищенном режиме Adobe Reader); см. веб-страницу по следующему адресу: http://blogs.adobe.com/asset/2010/07/introducing-adobe-reader-protected-mode.html.

- **Надежные источники**. Определение надежных источников по цифровым подписям, добавляемым к макросам. Это позволяет пользователям настраивать приложение Word 2000 на автоматический запуск внедренных в документ макросов из надежных источников при его открытии.

Основные улучшения системы безопасности в Office XP:

- **Уровни безопасности макросов**. Расширение защиты макросов за счет внедрения трех уровней безопасности: высокого, среднего и низкого. При высоком уровне безопасности (настройка по умолчанию) неподписанные макросы отключаются; разрешается запуск только подписанных макросов, полученных из надежных источников. При среднем уровне безопасности необходимость запуска неподписанных макросов определяется пользователем. При низком уровне безопасности разрешен запуск любых макросов без предупреждения. В Office 2003 к этой системе был добавлен очень высокий уровень безопасности.

Основные улучшения системы безопасности в Office 2003:

- **Поддержка интерфейса CryptoAPI**. Поддержка новых типов шифрования, доступных в любом установленном в системе поставщике CryptoAPI. Кроме того, все приложения Office можно настроить на использование по умолчанию определенного типа шифрования. Это позволяет применять стандартный тип шифрования при защите любых файлов данных Office паролем.
- **Надежные издатели**. Функции управления надежными издателями, в том числе возможность удаления установленных сертификатов, которые являются неблагонадежными или более не используются. Кроме того, внедрение списка недопустимых издателей гарантирует отклонение отозванных или просроченных сертификатов при попытке открыть документ с цифровой подписью, запустить макрос или инициализировать элемент ActiveX в приложении Office.
- **Безопасность элемента ActiveX**. Расширенные возможности управления поведением элементов ActiveX, запускаемых на компьютерах пользователей, для администраторов. Например, в предыдущих версиях Office элементы ActiveX не разделялись на безопасные и небезопасные

для инициализации. В Office 2003 при работе с небезопасными для инициализации элементами управления отображается соответствующее оповещение. При этом пользователь самостоятельно определяет необходимость инициализации элемента управления (по умолчанию инициализация не выполняется).

- **Управление правами на доступ к данным**. Технологии управления правами на доступ к данным (IRM) позволяют организациям более эффективно контролировать пересылку, копирование и печать данных. Технологии IRM Office 2003 интегрированы со службой управления правами Windows (RMS), представленной в ОС Windows Server 2003, что позволяет организациям создавать подробные политики разрешений, определяющие действия, которые разные группы пользователей могут выполнять с документами Office.
- **Дополнительные улучшения системы безопасности**. Различные улучшения системы безопасности отдельных приложений из набора Office, в том числе улучшенные функции защиты документов в Word 2003, которые позволяют ограничить возможности форматирования документов предварительно определенным набором стилей, а также разрешать доступ к функциям редактирования строго определенным пользователям и группам. Аналогичные улучшения представлены в Excel 2003, PowerPoint 2003 и других приложениях Office.

Основные улучшения системы безопасности в Office 2007:

- **Изменения стандартных функциональных возможностей**. Параметры по умолчанию блокируют доступ к потенциально опасному внешнему контенту; разрешено выполнение только надежных макросов; разрешено выполнение установленных и зарегистрированных надстроек без участия пользователя; разрешено открытие документов даже в том случае, если они содержат ненадежное активное содержимое (например, контент, отключенный до его явного включения пользователем с помощью отображаемого уведомления); разрешено выполнение элементов ActiveX без участия пользователя при строго определенных обстоятельствах.
- **Сокращение числа решений и запросов, связанных с безопасностью**. Число решений, принимаемых пользователями в связи с обеспечением безопасности, сокращено до минимума; изменен способ предоставления

пользователям сведений, на основе которых принимаются решения, связанные с безопасностью; предупреждения системы безопасности стали менее навязчивыми и более информативными. В результате пользователи получают запросы только в тех случаях, когда их участие необходимо для обеспечения безопасности рабочей среды. Эти изменения также позволяют пользователям принимать более взвешенные решения, связанные с безопасностью, благодаря чему снижаются риски атак вредоносных программ на домашние компьютеры пользователей и сети организаций.

- **Формат файла Office Open XML**. В Office 2007 представлены новые форматы файлов на основе XML — Open XML для приложений Word, Excel и PowerPoint 2007. Благодаря этому удалось повысить эффективность управления файлами и восстановления данных, а также упростить взаимодействие, поскольку доступ к файлам данных Office могут получать любые бизнес-приложения, поддерживающие формат XML. Внедрение формата Open XML позволяет повысить безопасность набора Office 2007 за счет того, что данные в документе хранятся в формате XML. Таким образом, файлы данных Office в таких форматах, как DOCX, XLSX и PPTX, представляют собой обычные текстовые файлы в сжатом (архивном) виде, которые, в отличие от файлов, сохраненных в старых двоичных форматах файлов Office (DOC, XLS, PPT), не могут содержать исполняемый код. Это означает, что ИТ-отделы организаций могут беспрепятственно разрешать передачу DOCX-, XLSX- и PPTX-файлов через брандмауэры сети периметра. Файлы данных, содержащие внедренный код, сохраняются с другим расширением (DOCM, XLSM и PPTM), что позволяет ИТ-специалистам быстро определять и при необходимости блокировать такие файлы.
- **Центр управления безопасностью**. Большинство параметров безопасности и конфиденциальности, связанных с определенными приложениями, объединены в одном компоненте — центре управления безопасностью. Благодаря этому повышается эффективность управления соответствующими параметрами приложений Office и гарантируются конфиденциальность, целостность и высокий уровень доступности данных, хранящихся на компьютерах пользователей.
- **Панель сообщений**. Большинство предупреждений системы безопасности отображаются в новой области — на панели сообщений. С ее помощью

пользователи также могут открывать и просматривать документы, содержащие активное содержимое, в том числе макросы и элементы ActiveX, не запуская и не инициализируя их.

- **Надежные расположения**. Возможность указать надежное расположение, такое как локальная или сетевая папка (по умолчанию в качестве надежных расположений пользователи могут указывать только локальные папки). При открытии документа Office, сохраненного в надежном расположении, все активное содержимое, в том числе элементы ActiveX, макросы и ссылки на внешние ненадежные источники данных, автоматически включается и инициализируется без отображения предупреждений.
- **Безопасность активного содержимого**. Параметры безопасности макросов определены более четко, благодаря чему пользователи могут задавать условия, при которых отображаются уведомления и предупреждения относительно макросов. Кроме того, пользователи могут настраивать большинство параметров безопасности для отдельных приложений. Также добавлен новый глобальный параметр, позволяющий отключить VBA для всех приложений Office.
- **Параметры блокировки форматов файлов**. Определение администратором форматов файлов Office, которые могут использоваться в организации.
- **Инспектор документов**. Удаление скрытых конфиденциальных сведений из документов (задается пользователями).

Общие сведения о системе безопасности Office 2010

С момента выпуска Office 2007 продолжается непрерывная эволюция угроз, с которыми сталкиваются организации. Все чаще в качестве целей для своих атак создатели вредоносных программ выбирают пользовательские приложения, в результате чего продукты Office постоянно подвергаются атакам разнообразных видов. Наибольшую опасность для пользователей Office теперь представляют не только эксплойты, связанные с макросами. Все чаще используются уязвимости, связанные с форматами файлов, когда с помощью измененных файлов Word, Excel

или PowerPoint в старых двоичных форматах (DOC, XLS или PPT) предпринимаются попытки создать условия для переполнения буфера. Это позволяет злоумышленникам несанкционированно получать права и обходить защиту системы, что на данный момент является одной из основных опасностей для пользователей Microsoft Office.

Учитывая новые и сохраняющиеся проблемы, связанные с безопасностью в этой области, техническая группа Office выделила три основные цели процесса разработки Office 2010:

- Усовершенствование процессов проектирования системы безопасности Office.
- Разработка эффективных и простых в применении технологий защиты для пользователей приложений Office.
- Усиление основных средств и технологий защиты Office.

Улучшения в процессах проектирования системы безопасности Office 2010

Основная задача при проектировании системы безопасности заключается в разработке безопасного программного обеспечения за счет эффективного моделирования угроз, соблюдения рекомендаций по созданию безопасного кода, а также применения средств проверки и тестирования. Улучшения системы безопасности Office 2007 были реализованы преимущественно благодаря применению новых процессов проектирования, рекомендаций и средств, реализованных технической группой Office в рамках программы Trusted Computing[4]. К ним относятся, в том числе, жизненный цикл разработки

[4] Дополнительные сведения о программе Microsoft Trustworthy Computing см. в следующем документе: http://download.microsoft.com/download/a/f/2/af22fd56-7f19-47aa-8167-4b1d73cd3c57/twc_mundie.doc.

безопасности (SDL)[5], рекомендации по созданию безопасного кода, практические занятия по моделированию угроз и собственные средства проверки. Благодаря этим усилиям удалось повысить безопасность кода, лежащего в основе приложений Office. Кроме того, эти улучшения наряду с упомянутым выше форматом Open XML позволили сделать набор Office 2007 более защищенным по сравнению с предыдущими версиями.

Однако, несмотря на все улучшения процессов проектирования системы безопасности Office 2007, многие организации по-прежнему вынуждены работать с большим числом документов, электронных таблиц и презентаций, созданных в более ранних версиях Office. Даже в организациях, в которых введен стандарт Office 2007 и репозиторий двоичных файлов Office преобразован в формат Open XML, по-прежнему встречаются файлы старого формата при обмене бизнес-данными с партнерами и клиентами, еще не перешедшими на Office 2007.

Чтобы решить эту проблему и обеспечить безопасную работу с устаревшими двоичными файлами данных, группой разработчиков Office 2010 активно применялось нечеткое тестирование. Эта концепция проектирования системы безопасности подразумевает добавление, удаление или изменение произвольных фрагментов файлов данных в попытках обнаружить ранее неизвестные уязвимости форматов файлов. Как показывают исследования, злоумышленники зачастую обнаруживают уязвимости в двоичных файлах Office именно посредством нечеткого тестирования документов Word или электронных таблиц Excel. Например, злоумышленник может случайным образом изменять биты в файле в старом формате Word (например, DOC) и пытаться открыть такие файлы в приложении Word. В конечном итоге существует реальная возможность, что один из таких измененных файлов приведет к сбою приложения Word, например, в результате выхода введенных данных за пределы допустимого для какого-либо раздела файла диапазона. Затем с помощью отладчика злоумышленник может исследовать причины сбоя приложения в результате открытия измененного файла,

---

[5] Дополнительные сведения о концепции жизненного цикла разработки безопасности в рамках программы Microsoft Trustworthy Computing см. в разделе http://msdn.microsoft.com/en-us/library/ms995349.aspx веб-сайта MSDN.

что позволяет обнаружить уязвимости и использовать их для последующих атак на пользователей Word. Создав соответствующий измененный DOC-файл с активным содержимым, злоумышленник может разослать его по Интернету в виде вложения в сообщение электронной почты, используя тем самым обнаруженную уязвимость. Данные пользователей, которые получили и открыли такие вложения с включенным активным содержимым, подвергаются опасности, что влечет за собой дополнительные проблемы для администраторов сетей и общее снижение производительности.

Поскольку нечеткое тестирование зарекомендовало себя как достаточно простой и очень эффективный способ обнаружения уязвимостей в форматах файлов, техническая группа Office включила в процесс проектирования системы безопасности Office 2010 этап расширенного нечеткого тестирования. Из Интернета были загружены миллионы файлов, представляющие весь спектр из более чем 300 различных форматов файлов, поддерживаемых набором Office. Чтобы определить новые уязвимости в двоичных файлах Word, Excel и PowerPoint, с ними было проведено несколько десятков миллионов различных нечетких тестов. Результаты этих тестов были использованы по двум направлениям: для устранения сотен новых ошибок, обнаруженных в коде приложений Office, а также для создания спецификаций определения схемы XML (XSD) для двоичных форматов файлов Office, таких как DOC, XLS и PPT, для которых ранее отсутствовали спецификации XSD, позволяющие проверить эти файлы. В Office 2010 были реализованы новые технологии защиты на базе этих спецификаций XSD, позволяющие защитить пользователей от эксплойтов, основанных на изменении двоичных форматов файлов Office. Эти технологии защиты описываются в следующем разделе.

Новые технологии защиты в Office 2010

Помимо улучшений в процессе проектирования системы безопасности в наборе Office 2010 также были реализованы новые технологии защиты и новая модель надежности, которые позволяют сформировать многоуровневую систему безопасности для эффективного противостояния атакам. Например, в предыдущих версиях Office при попытке открыть документ Word сначала предпринимается попытка проверить правильность его формата. Если документ имеет формат DOCX и создан в Word 2007 на основе спецификации Office Open XML, его проверка выполняется посредством синтаксического анализа по спецификации XSD

соответствующего формата. Однако если документ имеет формат DOC и создан в версии Word 97–2003, файл просто загружается в память и отображается без каких-либо проверок, поскольку для таких файлов не была определена спецификация XML или другой стандарт проверки. Аналогичная ситуация наблюдается и в предыдущих версиях приложений Excel и PowerPoint.

Учитывая это, техническая группа Office разработала новые технологии защиты и снижения угроз для приложений Word 2010, Excel 2010 и PowerPoint 2010. Две из них, проверка файлов Office и защищенный просмотр, обеспечивают защиту ресурсов организации за счет снижения потенциального вреда, который может нанести использование эксплойтов, связанных с двоичными форматами файлов Office. Третья технология Office 2010, которая получила название «Надежные документы», может использоваться совместно с первыми двумя и позволяет усовершенствовать пользовательский интерфейс путем уменьшения числа решений, связанных с безопасностью, которые приходится принимать при работе с документами с активным содержимым, таким как макросы или элементы ActiveX.

Например, в приложении Word 2010 при попытке открыть DOC-файл он не загружается в само приложение Word и не отображается. Вместо этого файл передается в библиотеку DLL, в которой тщательно проверяется по спецификации XML для DOC-файлов. Эта спецификация была разработана по результатам интенсивного нечеткого тестирования в процессе проектирования системы безопасности Office 2010. Если такой DOC-файл проходит проверку, он передается из библиотеки DLL в приложение Winword.exe, в котором его содержимое открывается и выводится на экран с полной поддержкой возможностей редактирования. Файл, который не прошел проверку, может быть опасен для компьютера пользователя. В этом случае файл открывается в изолированной среде защищенного просмотра, в которой доступен просмотр содержимого документа, однако отключены возможности редактирования и все активное содержимое. При этом вместо хост-процесса Winword.exe запускается изолированный процесс Winword.exe с низким уровнем доступа, в котором обрабатывается документ.

После того как пользователь проверит содержимое документа и убедится в подлинности его источника, можно разрешить редактирование этого документа с помощью соответствующего запроса на панели сообщений. В этом случае

изолированный процесс защищенного просмотра завершается, а документ открывается в хост-процессе Winword.exe с полной поддержкой возможностей редактирования. Если в документе имеется активное содержимое, отображается второй запрос панели сообщений, в котором пользователю предлагается включить это содержимое. Если пользователь включает активное содержимое документа, этот выбор запоминается с помощью функции «Надежные документы» Office 2010. При следующем открытии надежного документа его активное содержимое автоматически включается без отображения запроса. В Word 2007 было реализовано другое поведение, при котором пользователю предлагается включить активное содержимое при каждой попытке открыть документ с макросами или элементами ActiveX.

Библиотеки DLL, аналогичные разработанным для Word 2010, тоже были созданы для приложений Excel 2010 и PowerPoint 2010. С помощью этих библиотек реализуется проверка XLS- и PPT-файлов, а также их отображение в соответствующих приложениях с помощью защищенного просмотра. Администраторы тоже могут настраивать Office 2010 для отправки сведений о файлах, которые не прошли проверку, по каналу отчетов об ошибках программы «Доктор Ватсон». В этом случае проводится их расширенный анализ специалистами центра Microsoft Security Response Center (MSRC). При обнаружении новых уязвимостей в двоичном формате файлов Office выпускаются обновления спецификации XML, которые автоматически загружаются в систему Office 2010 и могут использоваться компонентом проверки файлов Office. Основное преимущество такого подхода заключается в более оперативном реагировании на новые уязвимости формата файлов по сравнению с традиционным процессом установки исправлений для программного обеспечения.

Основные улучшения системы безопасности в Office 2010

Улучшения в процессе проектирования системы безопасности и новые технологии защиты не являются единственными нововведениями в Office 2010. Также были улучшены основные технологии, что позволило повысить эффективность защиты и реализовать новые сценарии совместной работы. В Office 2010 был представлен ряд улучшений в технологиях цифровых подписей и шифрования. Кроме того, были расширены возможности управления правами на доступ к данным (IRM),

что позволило реализовать поддержку совместной работы между разрозненными организациями. Была усовершенствована даже система паролей, которая использовалась для защиты документов Word от несанкционированного изменения — теперь стало возможно принудительное применение требований к сложности паролей в домене при защите файлов данных Office паролем. Подробное описание этих и других основных улучшений системы безопасности приведено далее в этом документе.

Система безопасности Office 2010: многоуровневая защита

В основе стратегии любого решения по защите данных лежит концепция многоуровневой защиты. Реализация нескольких резервных элементов управления безопасностью на разных уровнях информационной системы позволяет блокировать угрозы, которым все-таки удается преодолеть один из уровней защиты. В Office 2010 эта стратегия реализована в виде четырех уровней и обеспечивает защиту пользователей от содержащих вредоносные изменения документов Word, электронных таблиц Excel или презентаций PowerPoint. На каждом уровне системы безопасности Office 2010 реализуются уникальные меры защиты, которые активируются при попытке пользователя открыть файл в приложении Office 2010 и продолжают действовать до тех пор, пока файл не будет успешно открыт для редактирования. На рис. 1 показаны функции, реализуемые на каждом из уровней системы безопасности Office.

- Усиление защиты по направлениям вероятных атак за счет усовершенствования процессов проектирования системы безопасности и интеграции основных средств безопасности ОС Windows в систему Office 2010. Поддержка технологии предотвращения выполнения данных (DEP/NX), надежной и гибкой системы шифрования и других технологий позволяет сформировать первый уровень защиты от угроз, содержащихся во вредоносных файлах данных Office.
- Уменьшение возможностей для атак за счет ограничения типов файлов, которые можно открывать в приложении, а также посредством запрета на выполнение определенных типов внедренного кода. В основе этого уровня лежит технология проверки файлов Office (две другие технологии —

блокировки параметров файлов и бита аннулирования ActiveX для Office 2010 описываются в последующих разделах этого документа).
В совокупности эти технологии позволяют существенно сократить как число самих атак, преодолевших первый уровень защиты, так и количество их целей.

- Противодействие эксплойтам позволяет свести к минимуму последствия атак, преодолевших первые два уровня защиты. На этом уровне защиты Office 2010 основной является технология защищенного просмотра, которая обеспечивает предварительный просмотр опасных файлов Office без нанесения вреда компьютеру пользователя или всей сети.
- Улучшение взаимодействия с пользователями, выраженное в сокращении числа принимаемых ими решений в отношении безопасности и повышении эффективности таких решений. На этом уровне ведущую роль играет функция «Надежные документы», которая позволяет предотвратить невосприимчивость пользователей к запросам. Такое состояние может возникнуть при многократном отображении повторяющихся предупреждений системы безопасности и, в конечном итоге, ведет к тому, что пользователь попросту игнорирует последующие предупреждения.

Рис. 1. Многоуровневая система безопасности Office 2010.

Система безопасности Office 2010: управление потоком информации

В дополнение к технологиям, позволяющим противостоять эксплойтам, в Office 2010 также представлен ряд улучшенных технологий, обеспечивающих управление потоком информации в рамках организации. К ним относятся следующие:

- Расширенные параметры сложности паролей.
- Ряд улучшений системы шифрования.
- Улучшения цифровых подписей.
- Инспектор документов.
- Улучшения в области управления правами на доступ к данным.

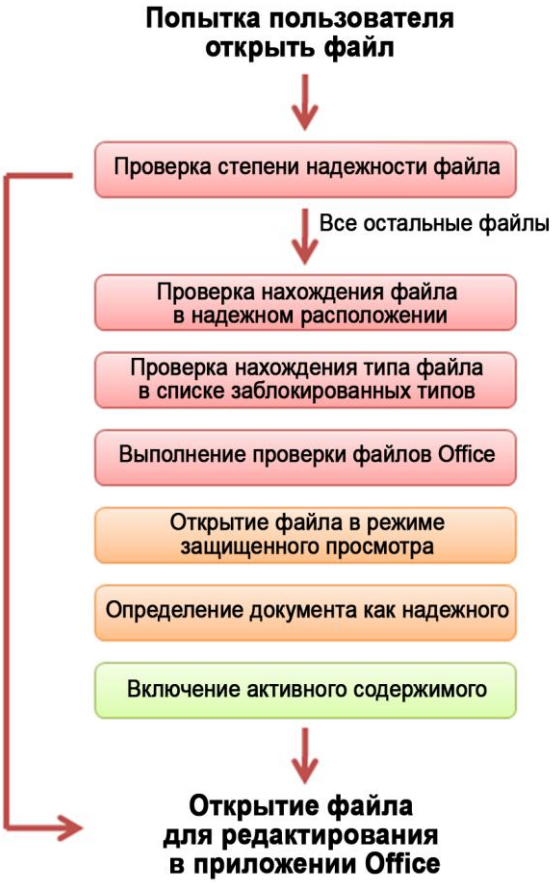
В следующих разделах описываются принципы противодействия потенциальным эксплойтам, реализованные в системе безопасности Office 2010. После этого рассматриваются возможности Office 2010 по управлению потоком информации в организации.

Противодействие эксплойтам в Office 2010

Чтобы лучше понять, каким образом многоуровневая система безопасности Office 2010 обеспечивает защиту компьютера, рассмотрим, что происходит при работе пользователя с приложением Office. На приведенном выше рис. 1 указаны основные технологии, с помощью которых обеспечивается защита пользователей Office 2010 от потенциальных эксплойтов. Тем не менее гораздо более эффективным будет практическое знакомство с тем, как эти технологии работают при открытии пользователем файла в приложении из набора Office 2010, например в Word 2010. С этой целью на рис. 2 показаны основные выполняемые проверки и операции, позволяющие противодействовать потенциальным эксплойтам при открытии документа в приложении Word 2010.[6] Аналогичная последовательность

[6] Представленные на этом рисунке проверки выполняются в приложении Word 2010 при открытии документа непосредственно пользователем, с помощью скрипта команд или любым другим способом. Обратите внимание, что на рисунке

действий реализована в приложениях Excel 2010 и PowerPoint 2010. Некоторые из этих действий выполняются также при открытии файлов с помощью других приложений Office 2010. В разделах ниже подробно описаны улучшения в области противодействия эксплойтам, реализованные в Office 2010, а также предоставлены ссылки на дополнительные ресурсы на веб-сайте Microsoft TechNet.



показаны не все проверки, выполняемые в приложениях Office 2010. Например, для противодействия потенциальным эксплойтам в системе Office 2010 также используется технология предотвращения выполнения данных (DEP), которая реализована в ОС Windows, а не в самой системе Office.

Рис. 2. Последовательность действий, выполняемых при попытке пользователя открыть файл с помощью Word 2010, Excel 2010 или PowerPoint 2010.

Предотвращение выполнения данных

На первой стадии противодействия эксплойтам в Office 2010 используется технология предотвращения выполнения данных (DEP), которая на аппаратном и программном уровнях встроена в операционную систему Windows. DEP позволяет предотвратить выполнение вредоносного кода путем укрепления защиты по направлениям вероятных атак вирусов и других видов угроз. Это достигается посредством определения файлов, которые пытаются выполнить код из фрагментов памяти, зарезервированных только для данных и недоступных для исполняемых программ. Технология предотвращения выполнения данных впервые была представлена в пакете обновления 2 (SP2) для Windows XP и в Windows Server 2003. С выпуском Office 2010 была реализована поддержка этой технологии во всех приложениях Office. Она лежит в основе первого уровня многоуровневой системы безопасности Office 2010 (см. рис. 1).

В 64-разрядных выпусках Office 2010 технология предотвращения выполнения данных применяется автоматически и не может быть отключена. В 32-разрядных выпусках системы эту технологию можно включать и отключать для отдельных приложений с помощью центра управления безопасностью или групповой политики. В 32-разрядных версиях приложений Word, Excel и PowerPoint включить и отключить эту технологию можно на странице защищенного просмотра в центре управления безопасностью. В 32-разрядных версиях других приложений Office 2010 представлена отдельная страница для настройки параметров предотвращения выполнения данных.[7] Изменения параметров предотвращения выполнения данных в приложениях Office вступают в силу только после перезапуска самого приложения.

---

[7] Если флажок «Параметры предотвращения выполнения данных» недоступен (выделен серым цветом), это означает, что соответствующая политика на данном компьютере постоянно включена (AlwaysOn) или отключена (AlwaysOff).

Чтобы проверить, работает ли технология предотвращения выполнения данных в приложениях Office, воспользуйтесь диспетчером задач. Например, на следующем рисунке показана вкладка «Процессы» в диспетчере задач для приложения Word 2010, работающего в режиме защищенного просмотра.[8] На эту вкладку добавлен столбец «Предотвращение выполнения данных», свидетельствующий о том, что для этого приложения Office включена соответствующая технология.

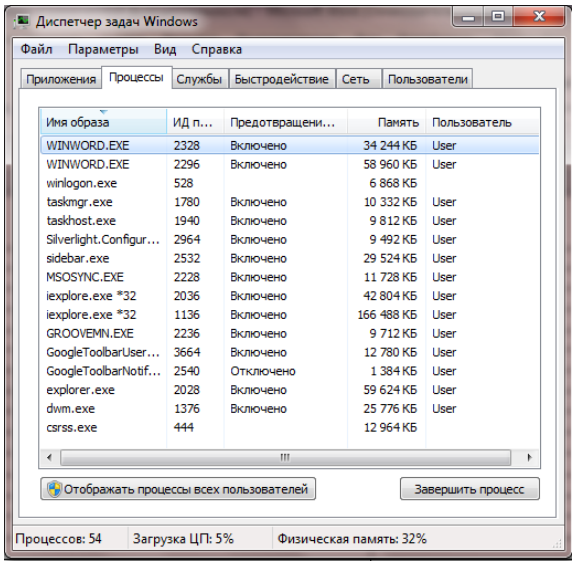


Рис. 3. С помощью диспетчера задач можно проверить, включена ли технология предотвращения выполнения данных.

Исключения предотвращения выполнения данных вызываются при каждой попытке программы выполнить код в страницах памяти, не помеченных как исполняемые. Приложения Office 2010 крайне редко вызывают исключения

---

[8] Первый процесс Winword.exe на этом рисунке представляет собой клиентский процесс защищенного просмотра (изолированная среда). Второй процесс Winword.exe — это хост-процесс Word 2010, вызванный этим клиентским процессом.

предотвращения выполнения данных; обычно причинами таких исключений становится вредоносный или неверно написанный код надстроек.
При возникновении такого исключения в надстройке для приложения Office его работа автоматически завершается, чтобы обеспечить защиту компьютера пользователя. При следующем запуске приложения Office отображается диалоговое окно с рекомендациями по отключению неисправной надстройки до тех пор, пока проблема не будет обнаружена и устранена.

Дополнительные сведения о поддержке предотвращения выполнения данных в Office 2010 см. в блоге группы разработчиков Office по следующему адресу: http://blogs.technet.com/b/office2010/archive/2010/02/04/data-excecution-prevention-in-office-2010.aspx.

Модель надежности

При попытке пользователя открыть файл приложение Office 2010 в первую очередь оценивает степень надежности файла. Например, документы Word с активным содержимым (таким как макросы или элементы ActiveX) могут рассматриваться в Office 2010 как надежные или ненадежные. Если файл и его содержимое являются *надежными*, все оставшиеся проверки безопасности при открытии документа, описываемые ниже, не выполняются. Например, если дважды щелкнуть надежный документ Word, он просто откроется в приложении Word. При этом будет включено все его активное содержимое, в том числе макросы, надстройки, элементы ActiveX, гиперссылки, а также ссылки на источники данных и файлы мультимедиа. Если файл или любая часть его содержимого считаются *ненадежными*, выполняется последовательность описываемых далее проверок безопасности (в зависимости от поддерживаемых приложением Office функций безопасности). Например, защищенный просмотр поддерживается только приложениями Word 2010, Excel 2010 и PowerPoint 2010, поэтому соответствующая проверка безопасности не выполняется, в частности, при открытии файла в приложении Publisher 2010.

Каким образом в Office определяется степень надежности определенного файла и его содержимого? В предыдущей версии системы Office 2007 файлы и их содержимое можно было определить как надежные двумя способами.

- Макросы, надстройки и элементы ActiveX с цифровой подписью надежных издателей считаются надежными и, соответственно, автоматически включаются при открытии содержащего их файла в приложении Office. *Надежный издатель* — это издатель, цифровой сертификат которого (файл с расширением CER, используемый для подписи контента) добавлен в список надежных издателей в приложении Office. Макросы и активное содержимое могут быть подписаны надежными издателями. Дополнительные сведения о функции надежных издателей в Office 2010 см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/ff428091.aspx.
- Файлы, сохраняемые в надежных расположениях, автоматически считаются надежными. При этом надежным признается все их содержимое, включая неподписанные макросы, надстройки или элементы ActiveX. Такие файлы не открываются в режиме защищенного просмотра. *Надежное расположение* может быть как локальным (папка на жестком диске компьютера пользователя), так и удаленным (общая папка на сетевом файловом сервере). Обратите внимание, что по умолчанию назначение удаленных надежных расположений не поддерживается. Надежные расположения могут указываться как глобально для всех приложений Office, так и для каждого приложения в отдельности. В стандартной конфигурации некоторые расположения, в том числе папка пользовательских шаблонов Word, являются надежными. Некоторые расположения, характеризующиеся высокой степенью риска, такие как кэш Outlook 2007 и папка временных файлов, нельзя определить как надежные. Дополнительные сведения о функции надежных расположений в Office 2010 см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/cc179039.aspx.

В Office 2007 файлы можно определить как надежные двумя способами: убедиться, что все активное содержимое имеет цифровые подписи, или переместить файл в надежное расположение. Оба эти способа можно настраивать для отдельных пользователей с помощью центра управления безопасностью, в котором доступны все параметры безопасности и конфиденциальности Office 2007. В средах Active Directory оба эти способа можно настраивать и блокировать с помощью групповой политики. В Office 2010 поддерживаются

обе описываемые выше модели надежности и оба способа их настройки. Кроме того, в этой системе представлена новая функция «Надежные документы», с помощью которой можно определять как надежные отдельные документы. Другими словами, с помощью этой функции пользователи могут самостоятельно определять степень надежности отдельных документов, электронных таблиц и файлов Office других видов. Если пользователь определяет как надежный документ Word, который был открыт в режиме защищенного просмотра из-за наличия в нем макросов или другого активного содержимого, этот выбор запоминается, и в следующий раз документ не открывается в режиме защищенного просмотра. Это означает, что при следующем открытии документа не будут отображаться запросы на включение макросов. Это позволяет значительно упростить взаимодействие с пользователем по сравнению с системой Office 2007, в которой запросы на включение макросов отображаются при каждой попытке открыть документ Word, содержащий макросы, или электронные таблицы Excel, содержащие ссылки на внешние источники данных. Более подробное описание функции надежных документов представлено в разделах ниже. Важно понимать, что при попытке открыть файл в Office в первую очередь проверяется степень его надежности.

Блокировка файлов

Если пользователь пытается открыть файл, который определен как ненадежный, на следующем этапе перед его открытием в приложении Office проверяется, не включен ли тип файла в список блокируемых типов. Функция блокировки файлов была представлена в Office 2007. Она позволяет разрешать или запрещать открытие пользователями определенных типов файлов Word, Excel или PowerPoint. С помощью этой функции администраторы могут запрещать открытие или сохранение пользователями файлов Office в форматах, которые могут использоваться при атаках нулевого дня. Например, злоумышленник может создать эксплойт, в котором используются вредоносные файлы в двоичном формате Word 97. Как только появятся сообщения о существовании такого эксплойта, администратор может настроить параметры блокировки файлов Word 2007, запретив пользователям открывать файлы в этом формате. После выпуска обновления программного обеспечения, которое позволяет устранить указанную

проблему, администратор может отменить ранее выполненные настройки, разрешив открытие файлов такого типа.

В Office 2007 параметры блокировки файлов обычно настраиваются администратором с помощью групповой политики. Опытные пользователи, которым требовалась настройка этих параметров, вынуждены были прибегать к изменению реестра. В системе Office 2010 для приложений Word, Excel и PowerPoint представлена новая страница «Параметры блокировки файлов». Эта страница доступна в центре управления безопасностью и позволяет пользователям самостоятельно настраивать параметры блокировки для отдельных приложений или просматривать параметры, применяемые к приложению с помощью групповой политики.

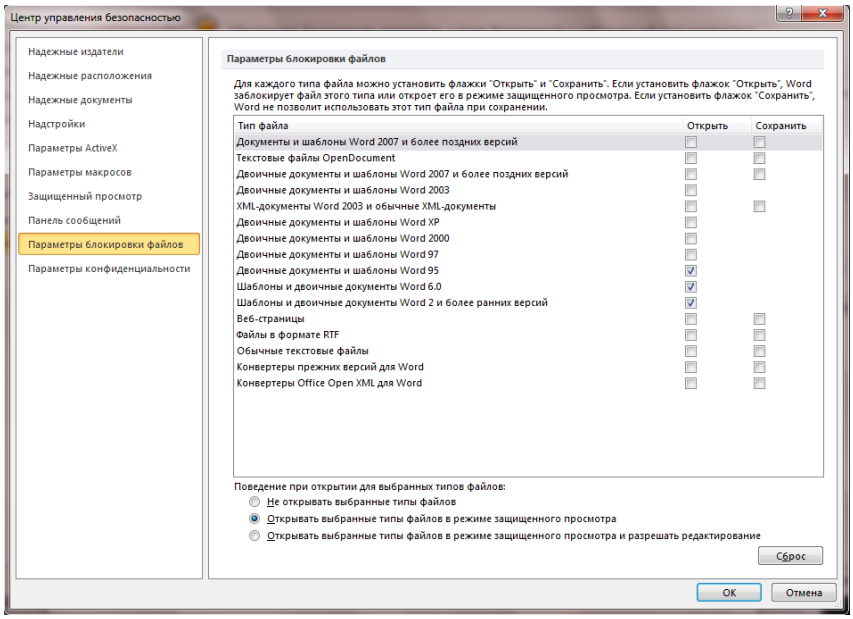


Рис. 4. Настройка параметров блокировки файлов с помощью центра управления безопасностью в Word 2010.

Как показано в нижней части предыдущего рисунка, по умолчанию файл, формат которого включен в список заблокированных форматов, открывается в режиме защищенного просмотра с отключенными возможностями редактирования. Пользователь получает соответствующее уведомление на панели сообщений.

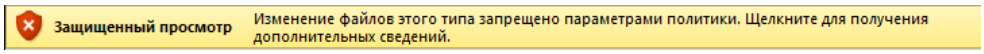


Рис. 5. По умолчанию файлы заблокированных форматов открываются в режиме защищенного просмотра с отключенными возможностями редактирования.

При попытке ввести любой текст в файл заблокированного формата, который отображается в приложении Word в режиме защищенного просмотра, в строке состояния в нижней части окна отображается сообщение «Такое изменение запрещено, так как документ открыт только для просмотра». Если щелкнуть текст на панели сообщений (см. рисунок выше), откроется обновленное меню «Файл». В этом представлении пользователь может щелкнуть ссылку (отмечена стрелкой на следующем рисунке), чтобы перейти на страницу «Параметры блокировки файлов» центра управления безопасностью.

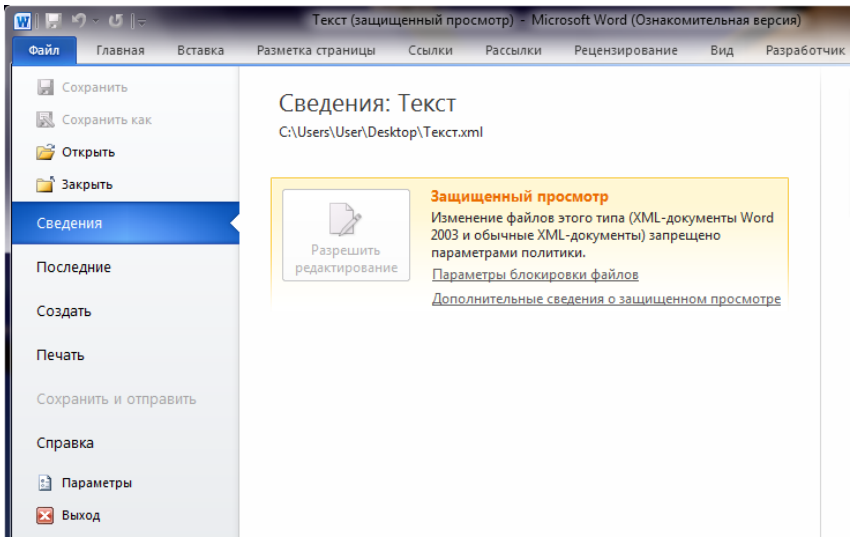


Рис. 6. Обновленное меню «Файл» со ссылкой на страницу «Параметры блокировки файлов» центра управления безопасностью.

Как показано на рис. 4, поведение функции блокировки файлов по умолчанию можно настроить двумя другими способами: полная блокировка открытия (или сохранения) файлов или открытие заблокированных файлов в режиме защищенного просмотра с возможностью включения функций редактирования. Если выбран последний способ, на панель сообщений добавляется кнопка,

с помощью которой пользователь при необходимости может включить возможности редактирования.

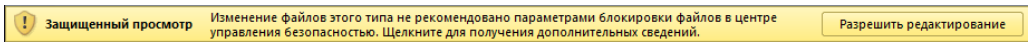


Рис. 7. С помощью параметров блокировки файлов можно настраивать отображение заблокированных файлов в режиме защищенного просмотра (при необходимости можно разрешать редактирование).

Ниже приведены дополнительные рекомендации по использованию функции блокировки файлов в Office 2010.

- Параметры блокировки не распространяются на файлы, сохраненные в надежном расположении или определенные как надежные документы.
- Параметры блокировки файлов настраиваются для каждого отдельного приложения и доступны только для Word, Excel и PowerPoint.
- Если в процессе развертывания Office 2010 администратор настроил параметры блокировки файлов с помощью центра развертывания Office, пользователи смогут изменить эти параметры позднее, при условии, что доступ к ним не заблокирован с помощью групповой политики.

Дополнительные сведения о функции блокировки файлов в Office 2010 см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/cc179230.aspx.

Бит аннулирования ActiveX

Следующая технология противодействия эксплойтам в системе Office 2010 — бит аннулирования ActiveX. Это параметр реестра, с помощью которого можно запретить загрузку заданного элемента ActiveX при определенных обстоятельствах (в том числе после полной загрузки этого элемента управления). Это позволяет добиться того, что даже изначально или повторно установленные в системе уязвимые элементы управления остаются неактивными и неопасными. Технология битов аннулирования ActiveX впервые была представлена в пакете обновления 2 (SP2) для Internet Explorer 5.01. Эта технология позволяет предотвратить загрузку вредоносных элементов ActiveX в механизм визуализации HTML браузера Internet Explorer. Эти биты иногда устанавливаются при загрузке и установке определенных

обновлений из центра обновления Windows, чтобы обеспечить защиту пользователей от критических эксплойтов, обнаруживаемых специалистами центра MSRC.

Технология битов аннулирования ActiveX впервые представлена в Office 2010 и позволяет запретить выполнение определенных элементов ActiveX в приложениях Office 2010 (Word, Excel, PowerPoint, Access или Visio), не затрагивая поведение этих элементов в браузере Internet Explorer. Бит аннулирования ActiveX по умолчанию не настроен и может включаться для каждого элемента управления отдельно (требуется изменение реестра). В Office 2007 аналогичные возможности реализовывались с помощью битов аннулирования ActiveX браузера Internet Explorer; тем не менее в Office 2010 используются разные разделы реестра для битов аннулирования для приложений Office и браузера Internet Explorer, что дает администраторам более гибкие возможности для блокировки вредоносных элементов ActiveX.[9]

Например, если для определенного элемента ActiveX установлен бит аннулирования, этот элемент не загружается и не инициализируется при открытии содержащего такой элемент документа в Word 2010. При этом на панели сообщений не отображается запрос на включение элемента управления пользователем. Это поведение не изменяется независимо от того, был ли документ сохранен в надежном расположении или определен как надежный документ. Пользователи также не могут добавлять такой элемент управления в создаваемые документы Word.

В Office 2010 также используется бит аннулирования COM, с помощью которого администраторы могут запрещать выполнение определенных COM-объектов (в том числе и элементов ActiveX) в приложениях Office 2010. Как и биты

---

[9] Если бит аннулирования для определенного элемента управления установлен одновременно в Office и Internet Explorer, по умолчанию значение бита в Office имеет приоритет (при необходимости это поведение можно настроить с помощью групповой политики).

аннулирования ActiveX, биты COM также задаются в реестре с использованием идентификатора класса (CLSID) COM-объекта.

Дополнительные сведения о поддержке битов аннулирования ActiveX в Office 2010 см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/cc179076.aspx.

Проверка файлов Office

Если открываемый файл определен как ненадежный, но его тип не входит в число заблокированных, на следующем этапе в системе Office 2010 выполняется проверка файлов Office, в ходе которой проверяется внутренняя структура файла. Как уже упоминалось выше, функция проверки файлов Office является одной из новых технологий защиты, представленных в приложениях набора Office 2010 (Word, Excel и PowerPoint). Эта технология позволяет предотвратить атаки, связанные с использованием форматов файлов Office, за счет сканирования файлов Office перед их открытием. При этом проверяется полное соответствие структуры файлов спецификациям форматов файлов Office. Проверяются только файлы в двоичном формате Office (Office 97–2003) с расширениями DOC, DOT, XLS, XLT, PPT, PPS и POT.

Если открываемый файл находится в надежном расположении и проходит эту проверку, то защищенный просмотр не применяется, а необходимость следующей проверки безопасности определяется наличием в файле активного содержимого, которое требуется включить. Однако если файл не проходит эту проверку, он открывается в режиме защищенного просмотра, а на панели сообщений отображается предупреждение о проблеме с файлом.

Рис. 8. Открываемый файл не прошел проверку.

Конструктивно функция проверки файлов Office не требует настройки, однако при необходимости можно изменить ряд доступных для нее параметров. Например, администратор может отключить проверку для отдельных приложений, однако корпорация Майкрософт не рекомендует делать это. Также администраторы могут настраивать поведение для файлов, не прошедших проверку. По умолчанию такие

файлы открываются в режиме защищенного просмотра. Кроме того, функция проверки файлов Office поддерживает постоянное накопление данных о новых файлах: для каждого не прошедшего проверку файла в системе Office собираются сведения о причинах этого. Затем, в течение около двух недель с того момента, как файл не прошел проверку, отображается диалоговое окно программы «Доктор Ватсон» с запросом на отправку собранных данных в корпорацию Майкрософт посредством системы отчетов об ошибках Windows.

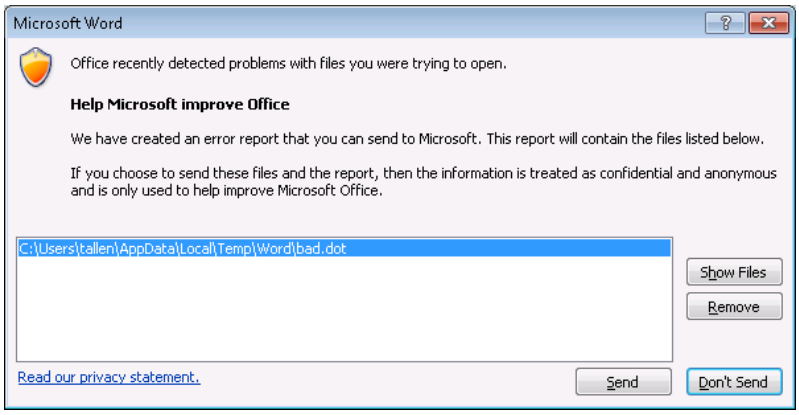


Рис. 9. Диалоговое окно программы «Доктор Ватсон», которое отображается для файла Word, не прошедшего проверку.

Для каждого такого файла передаются сведения о его типе, размере, времени, затрачиваемом на его открытие и проверку, а также копия самого файла. Благодаря этим сведениям корпорация Майкрософт продолжает совершенствовать функцию проверки файлов Office. Организации, работающие с конфиденциальными данными, могут отключить отправку отчетов о проверке файлов Office.

В отличие от большинства других функций безопасности Office 2010 параметры проверки файлов Office не удастся настроить с помощью центра управления безопасностью. Эти параметры можно настраивать только с помощью групповой

политики или центра развертывания Office.[10] Например, параметры политики для отключения проверки файлов располагаются по следующему пути:

> Конфигурация пользователя\Политики\Административные шаблоны\Microsoft Word 2010\Параметры Word\Безопасность.

На рисунке ниже показано положение политики в редакторе групповой политики при импорте файлов административных шаблонов Office 2010 (с расширением ADMX) в папку SYSVOL\<домен>\PolicyDefinitions на контроллере домена.

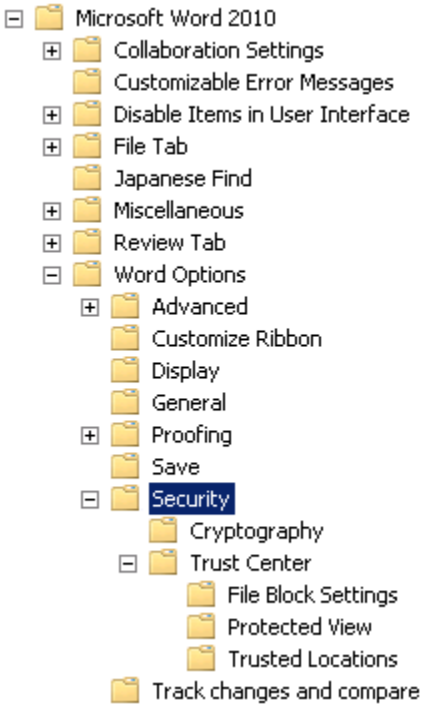


Рис. 10. Расположение политики для отключения проверки файлов Office в Word 2010.

---

[10] Опытные пользователи могут настраивать параметры проверки файлов Office путем изменения реестра.

Политика «Отключить проверку файлов», располагающаяся по этому пути, определяет поведение проверки файлов Office для приложения Word 2010.

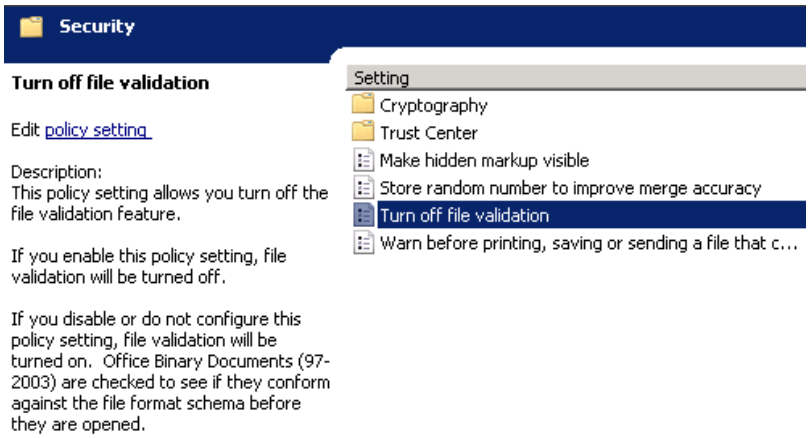


Рис. 11. Параметр политики, позволяющий отключить проверку файлов Office для приложения Word 2010.

Параметр политики, с помощью которого настраивается поведение для не прошедших проверку файлов, располагается по следующему пути:

> Конфигурация пользователя\Политики\Административные шаблоны\Microsoft Word 2010\Параметры Word\Безопасность\Центр управления безопасностью\Защищенный просмотр.

С помощь этого параметра администратор может задавать открытие файлов, не прошедших проверку, в режиме защищенного просмотра с отключенными возможностями редактирования (по умолчанию); открытие в режиме защищенного просмотра с возможностью включения функций редактирования пользователем, а также полную блокировку открытия файла.

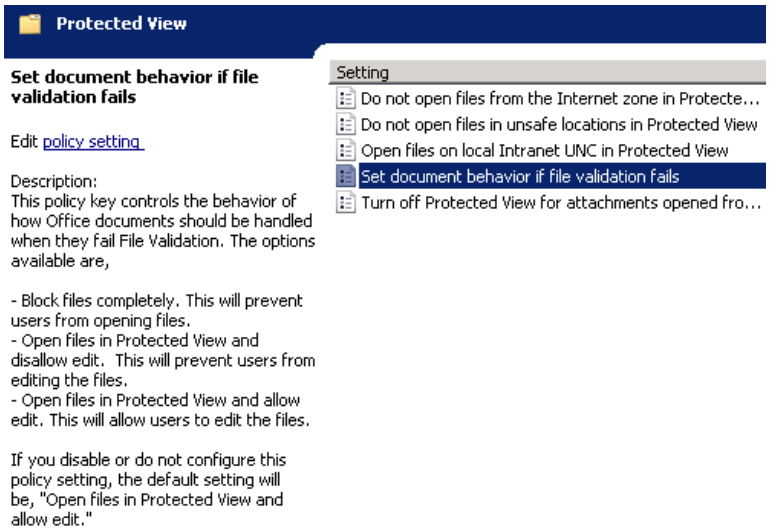


Рис. 12. Параметр политики, определяющий поведение для файлов, не прошедших проверку.

Наконец, администраторы при необходимости могут отключить отображение для пользователей запросов на отправку в корпорацию Майкрософт сведений о файлах, не прошедших проверку. Отключить соответствующие диалоговые окна можно с помощью параметра политики «Отключить отчеты об ошибках для файлов, не прошедших проверку файлов», который применяется ко всем приложениям Office и находится по следующему пути:

> Конфигурация пользователя\Политики\Административные шаблоны\Microsoft Office 2010\Безопасность.

Ниже приведены дополнительные рекомендации по использованию функции проверки файлов Office в Office 2010.

- Функция проверки файлов Office настраивается отдельно для каждого приложения (помимо отчетов об ошибках) и доступна только для приложений Word, Excel и PowerPoint.
- Проверка не выполняется, если файл сохранен в надежном расположении или определен как надежный документ.

- В некоторых случаях файл, не прошедший проверку, на самом деле может оказаться допустимым. Поэтому в Office 2010 по умолчанию настроена отправка файлов, не прошедших проверку, в корпорацию Майкрософт с помощью системы отчетов об ошибках Windows. Это позволяет постоянно совершенствовать функцию проверки файлов Office.

Дополнительные сведения о функции проверки файлов Office см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/ee857084.aspx, а также в блоге группы разработчиков Office по следующему адресу: http://blogs.technet.com/b/office2010/archive/2009/12/16/office-2010-file-validation.aspx. Дополнительные сведения о параметрах групповой политики Office 2010 см. в файле *Office2010GroupPolicyAndOCTSettings_Reference.xls*, который доступен на странице, посвященной файлам административных шаблонов Office 2010 (ADM, ADMX/ADML) и центру развертывания Office, веб-сайта Центра загрузки Майкрософт. Дополнительные сведения о центре развертывания Office для Office 2010 см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/cc179097.aspx.

Защищенный просмотр

Если открываемый файл не является надежным или не проходит проверки безопасности Office, на панели сообщений отображается запрос, свидетельствующий о том, что файл был открыт в изолированной среде или, другими словами, в режиме защищенного просмотра. Это одна из новых технологий защиты, представленных в Office 2010 для приложений Word, Excel и PowerPoint. Функция защищенного просмотра позволяет предварительно просматривать подозрительные файлы с использованием ограниченной среды с низким уровнем доступа. По умолчанию в этом режиме пользователь может прокручивать содержимое подозрительных документов, электронных таблиц или презентаций, чтобы ознакомиться с ним. При этом отключаются все функции редактирования, сохранения и печати, а также любое активное содержимое файла.

В определенных случаях файл автоматически открывается в режиме защищенного просмотра. Например, если в среде не настроена политика блокировки файлов, ненадежный файл, загруженный из Интернета, будет открыт в режиме

защищенного просмотра. При этом панель сообщений будет выделена желтым цветом, на ней появится значок щита синего цвета, а также кнопка, с помощью которой можно будет включить функции редактирования.

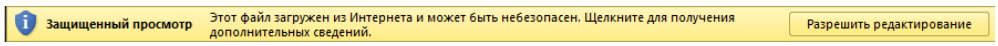


Рис. 13. Внешний вид панели сообщений (настройки по умолчанию) при открытии файла, загруженного из Интернета, в режиме защищенного просмотра.

При открытии файла из ненадежного расположения, например, из кэша вложений Outlook, панель сообщений будет выглядеть аналогично.

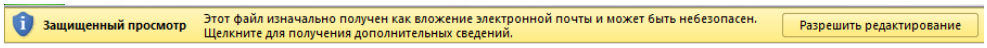


Рис. 14. Внешний вид панели сообщений (настройки по умолчанию) при открытии вложения Outlook в режиме защищенного просмотра.

Если файл имеет заблокированный формат, строка сообщений также выделяется желтым, однако значок щита будет красного цвета, а кнопка «Разрешить редактирование» будет отсутствовать.

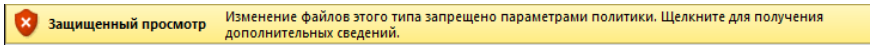


Рис. 15. Внешний вид панели сообщений (настройки по умолчанию) при открытии файла, имеющего заблокированный формат, в режиме защищенного просмотра.

Если файл не проходит проверку файлов Office, и значок щита, и панель сообщений будут красного цвета. Кнопка включения редактирования будет отсутствовать.

Рис. 16. Внешний вид панели сообщений (настройки по умолчанию) при открытии файла, не прошедшего проверку файлов, в режиме защищенного просмотра.

Если в последнем из описываемых выше сценариев пользователь, просмотрев файл, определяет, что его содержимое является надежным, можно щелкнуть текст

в выделенной красным цветом панели сообщений, чтобы открыть обновленное меню «Файл» (см. ниже). Если пользователь выбирает элемент «Все равно редактировать», файл определяется как надежный и открывается в соответствующем приложении Office. Режим защищенного просмотра закрывается.

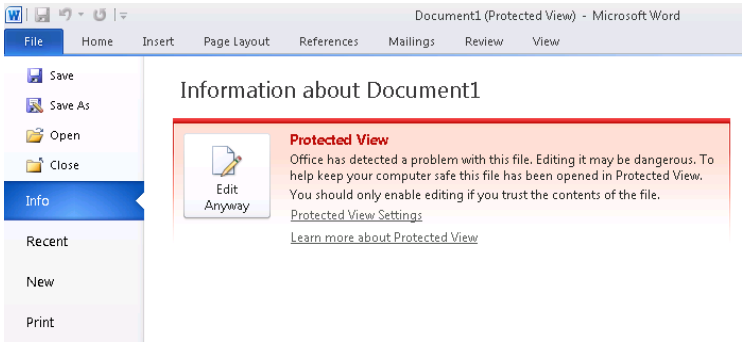


Рис. 17. При выборе элемента «Все равно редактировать» файл открывается в соответствующем приложении Office; режим защищенного просмотра при этом закрывается.

Если щелкнуть ссылку «Параметры защищенного просмотра», показанную на приведенном выше рисунке, откроется страница режима защищенного просмотра в центре управления безопасностью. На этой странице представлены параметры, с помощью которых можно настроить защищенный просмотр (см. рисунок ниже). С помощью этих параметров можно включить и отключить режим защищенного просмотра для файлов, загруженных из Интернета, полученных в виде вложений Outlook 2010 или хранящихся в ненадежных расположениях.[11]

[11] Параметр, позволяющий включить режим предотвращения выполнения данных, рассматривается далее в этом документе.

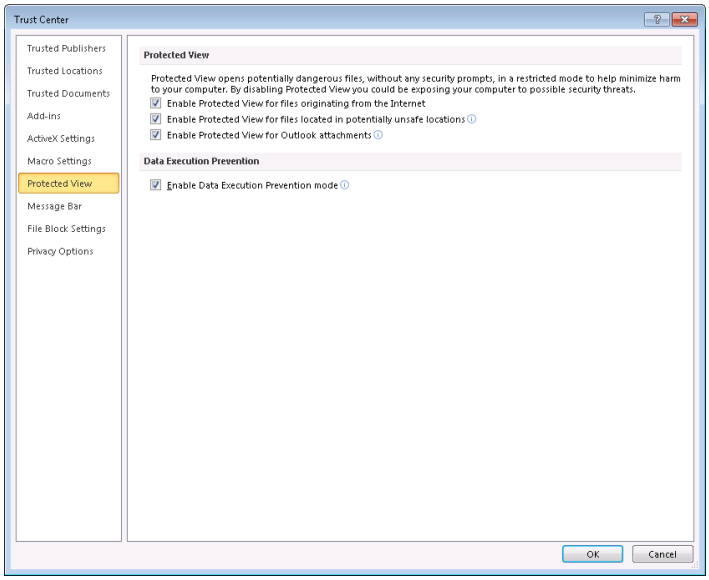


Рис. 18. Настройка режима защищенного просмотра с помощью центра управления безопасностью.

В процессе развертывания Office 2010 администратор может заблокировать описываемые выше параметры с помощью групповой политики или предварительно настроить их с помощью центра развертывания Office. Параметры групповой политики, предназначенные для настройки поведения режима защищенного просмотра, находятся по следующему пути:

> Конфигурация пользователя\Политики\Административные шаблоны\ Microsoft Word 2010\Параметры Word\Безопасность\Центр управления безопасностью\Защищенный просмотр.

В групповой политике также представлен дополнительный параметр режима защищенного просмотра, который недоступен в центре управления безопасностью. Этот параметр задает принудительное открытие в режиме защищенного просмотра файлов, расположенных в общих папках в локальной интрасети, если их UNC-пути определяются как принадлежащие к зоне Интернета.

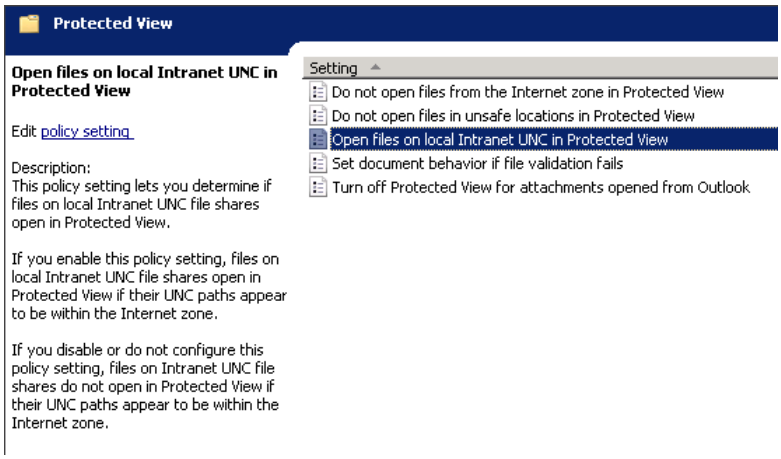


Рис. 19. Параметр политики режима защищенного просмотра, недоступный в пользовательском интерфейсе центра управления безопасностью.

Ниже приведены дополнительные рекомендации по использованию защищенного просмотра в Office 2010.

- Режим защищенного просмотра настраивается для каждого отдельного приложения и доступен только для приложений Word, Excel и PowerPoint.
- Режим защищенного просмотра не используется, если файл сохранен в надежном расположении или определен как надежный документ.
- Защищенный просмотр включается автоматически при попытке пользователя открыть подозрительный файл. При необходимости можно принудительно открыть любой файл в этом режиме. Для этого, удерживая нажатой клавишу SHIFT, щелкните правой кнопкой мыши название файла в проводнике и выберите команду «Открыть в режиме защищенного просмотра».
- В режиме защищенного просмотра отключены все функции редактирования, сохранения и печати. Тем не менее при необходимости пользователи могут скопировать содержимое файла и вставить его в другой документ.
- Чтобы определить, отключены ли функции редактирования в режиме защищенного просмотра в приложениях Word, Excel или PowerPoint, проверьте состояние различных вкладок — элементы ленты должны быть недоступны (выделены серым цветом).

- При попытке сохранить файл в режиме защищенного просмотра отображается диалоговое окно с сообщением «Сохранение недоступно в режиме защищенного просмотра. При наличии доверия к источнику этого файла нажмите кнопку "Разрешить сохранение", чтобы включить эту команду». При нажатии кнопки «Разрешить сохранение» режим защищенного просмотра закрывается, после чего открывается диалоговое окно «Сохранить как», в котором можно указать расположение для сохранения файла. Аналогичные действия выполняются при попытке напечатать файл в режиме защищенного просмотра. В обоих случаях при выходе из этого режима файл определяется как надежный документ. Это поведение более подробно описано в следующем разделе.

Дополнительные сведения о режиме защищенного просмотра см. в разделе библиотеки TechNet по следующему адресу:
http://technet.microsoft.com/en-us/library/ee857087.aspx,
а также в блоге группы разработчиков Office по следующему адресу:
http://blogs.technet.com/b/office2010/archive/2009/08/13/protected-view-in-office-2010.aspx.

Надежные документы

Как было указано в начале этого руководства, в приложениях Word, Excel и PowerPoint набора Office 2010 представлена новая функция «Надежные документы», с помощью которой можно определять степень надежности отдельных файлов. В частности, с помощью этой функции пользователи могут самостоятельно определять степень надежности отдельных документов, электронных таблиц или презентаций, которые не прошли одну или несколько проверок безопасности при попытке их открыть. Например, если пользователь включает функции редактирования или активное содержимое для файла, не прошедшего проверку, степень надежности этого файла изменяется. Такие изменения отслеживаются функцией надежных документов и записываются в куст реестра HKCU на компьютере пользователя.

Например, пользователь загружает из Интернета документ Word, содержащий макросы. Поскольку в Windows XP с пакетом обновления 2 (SP2) служба выполнения вложений (AES) добавляет к файлам, загруженным из Интернета,

сведения о зоне, в свойствах такого файла указано, что он был загружен из Интернета. В результате при двойном щелчке документа загруженный файл открывается в режиме защищенного просмотра. При этом на панели сообщений всегда отображается приведенный ниже запрос.

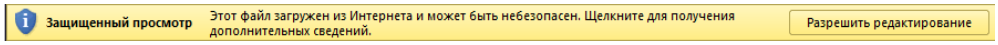


Рис. 20. Запрос на панели сообщений со сведениями о том, что файл получен из зоны Интернета.

Если нажать кнопку «Разрешить редактирование» на показанной выше панели сообщений, функция надежных документов сохранит выбранную пользователем степень надежности файла в реестре как запись доверия.[12] Это означает, что после закрытия этого документа при его повторном открытии на панели сообщений не появится соответствующий запрос. Тем не менее на этом этапе файл не получает полного доверия, поскольку содержит макросы. При нажатии кнопки «Разрешить редактирование» на панели сообщений отображается второй запрос следующего вида:

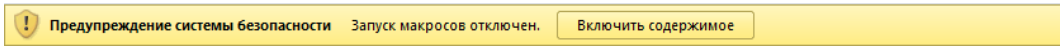


Рис. 21. Второй запрос на панели сообщений со сведениями о наличии макросов в документе.

Если на изображенной выше панели сообщений нажать кнопку «Разрешить редактирование», документ получает полное доверие, в связи с чем его состояние надежности в реестре обновляется соответствующим образом. Это означает, что при закрытии и повторном открытии этого документа на панели сообщений не будут отображаться соответствующие запросы, и документ будет открываться в приложении Word с включенной поддержкой макросов. Аналогичного результата можно добиться, переместив файл в надежное расположение.

---

[12] Аналогичный результат можно получить, если щелкнуть правой кнопкой мыши название файла в проводнике, выбрать пункт «Свойства», а затем на вкладке «Общие» выбрать команду «Разблокировать».

Функцию надежных документов Word 2010 можно настраивать с помощью центра управления безопасностью, групповой политики или центра развертывания Office. На рисунке ниже показаны параметры, доступные при настройке функции надежных документов с помощью центра управления безопасностью. В этом случае пользователи могут определять документы в общих сетевых папках как надежные (по умолчанию включено), отключать функцию надежных документов (запросы на панели сообщений будут отображаться каждый раз при открытии файлов с активным содержимым), а также очищать кэш реестра надежных документов (после этого все документы, за исключением хранящихся в надежном расположении или подписанных надежными издателями, будут определены как ненадежные).

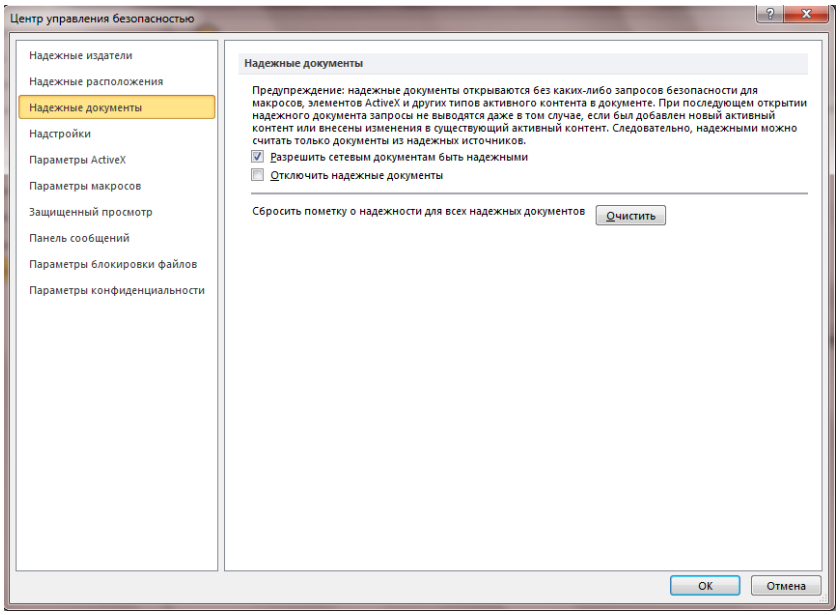


Рис. 22. Настройка функции надежных документов с помощью центра управления безопасностью.

Помимо настройки этих параметров с помощью групповой политики можно задать максимальное число записей доверия, сохраняемых в реестре этой функцией. По умолчанию максимальное число надежных документов составляет 500. При необходимости это ограничение можно увеличить вплоть до 20 000, однако

это может отрицательно сказаться на производительности. Параметры политики для настройки надежных документов находятся по следующему пути:

Конфигурация пользователя\Политики\Административные шаблоны\Microsoft Word 2010\Параметры Word\Безопасность\Центр управления безопасностью.

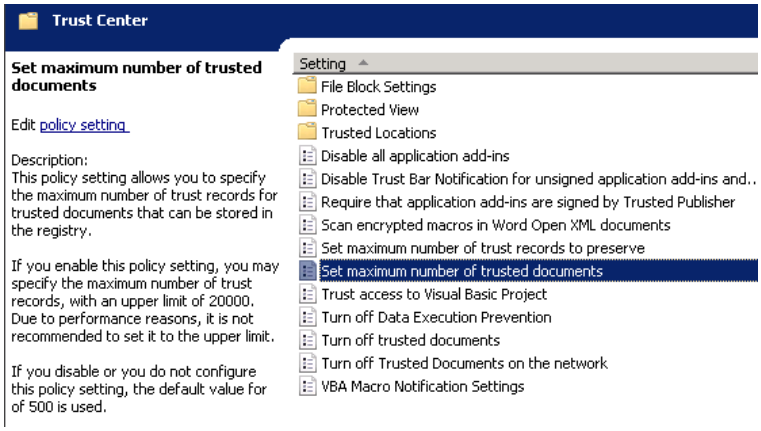


Рис. 23. Параметр групповой политики, позволяющий задать максимальное число записей доверия для надежных документов.

Ниже приведены дополнительные рекомендации по использованию функции надежных документов в Office 2010.

- Функция надежных документов настраивается для каждого отдельного приложения и доступна только для приложений Word, Excel, PowerPoint, Access и Visio.
- Надежные документы проходят только две проверки безопасности из всех (проверка на вирусы и проверка бита аннулирования ActiveX).

Дополнительные сведения о надежных документах см. в блоге группы разработчиков Office по следующему адресу: http://blogs.technet.com/b/office2010/archive/2009/09/28/trusted-documents.aspx.

Активное содержимое

Файл, прошедший все проверки безопасности Office 2010, открывается с помощью соответствующего приложения Office. При этом включается все имеющееся в нем

активное содержимое. Выполнение всех проверок обычно занимает десятые доли секунды (за исключением файлов очень большого размера). В предыдущем разделе, посвященном надежным документам, указано, что в Office 2010 по умолчанию отключается все активное содержимое файлов, не определенных как надежные. Как и в Office 2007, поведение системы по умолчанию при работе с активным содержимым можно настроить разными способами — с помощью центра управления безопасностью, групповой политики или центра развертывания Office. Фактически доступные параметры для настройки поведения макросов VBA, элементов ActiveX и надстроек в Office 2010 во многом схожи с параметрами в предыдущей версии системы Office 2007. Например, на рисунке ниже показана страница «Параметры макросов» центра управления безопасностью в Office 2007.

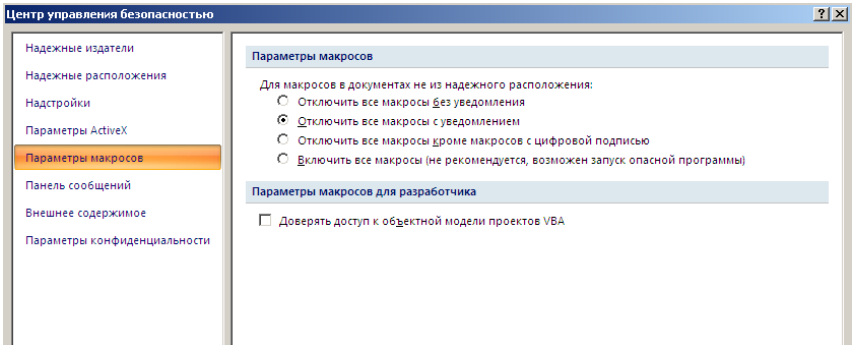


Рис. 24. Страница «Параметры макросов» центра управления безопасностью в Office 2007.

Для сравнения на следующем рисунке показана та же страница в центре управления безопасностью Office 2010:

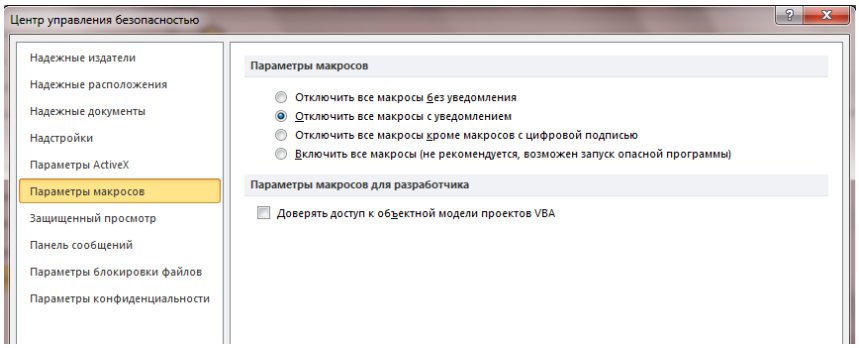


Рис. 25. Страница «Параметры макросов» центра управления безопасностью в Office 2010.

Помимо незначительных различий, существенных изменений в способе обработки макросов между версиями Office 2007 и Office 2010 не произошло. То же можно сказать и о страницах «Параметры ActiveX» и «Надстройки». Единственное исключение — поддержка бита аннулирования ActiveX, которая впервые реализована в Office 2010 и подробнее описана в разделе «Бит аннулирования ActiveX» настоящего документа. Поэтому в этом документе не описывается настройка параметров безопасности для макросов, элементов ActiveX или надстроек. Дополнительные сведения о работе с активным содержимым в Office 2010 см. в указанных ниже разделах библиотеки TechNet.

- Дополнительные сведения о настройке параметров для макросов VBA см. в разделе http://technet.microsoft.com/en-us/library/ee857085.aspx.
- Дополнительные сведения о настройке параметров для элементов ActiveX см. в разделе http://technet.microsoft.com/en-us/library/cc179076.aspx.
- Дополнительные сведения о настройке параметров для надстроек см. в разделе http://technet.microsoft.com/en-us/library/ee857086.aspx.

Панель сообщений

После того как открываемый файл проходит все проверки безопасности Office, пользователь может приступить к его редактированию в соответствующем приложении Office. Прежде чем закончить изучение этого раздела, кратко рассмотрим возможности панели сообщений, на которой отображаются уведомления об обнаруженных проблемах безопасности, а также предлагаются способы их устранения. В Office 2010 число уведомлений системы безопасности значительно меньше по сравнению с Office 2007. Кроме того, они стали более понятными для пользователей, не обладающих специализированной технической подготовкой. Техническая группа Office проделала огромный объем работы, в результате которой уведомления системы безопасности стали носить менее угрожающий и более информативный характер, что позволяет пользователям принимать более взвешенные решения относительно безопасности. Например, при попытке открыть в Word 2007 документ, который был загружен из Интернета и содержит макросы, панель сообщений приобретала следующий вид:

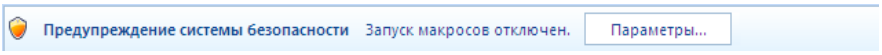


Рис. 26. Вид панели сообщений Word 2007 при открытии документа, содержащего макросы.

Вместо рекомендаций на панели сообщений представлен минимальный объем сведений, а также кнопка «Параметры», с помощью которой пользователь может получить дополнительные сведения о действиях, которые необходимо предпринять. Не имея полного представления о том, что следует сделать, а также о причинах отображения запроса, пользователь нажимает кнопку «Параметры», после чего видит следующее диалоговое окно устрашающего вида:

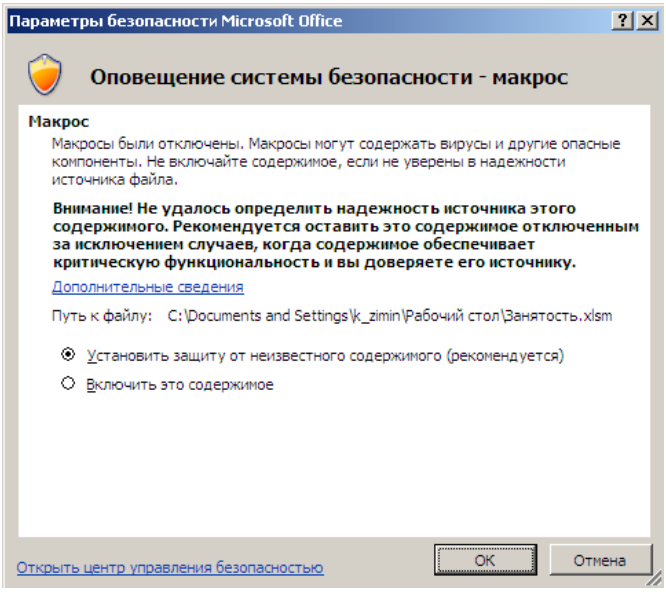


Рис. 27. Параметры, отображаемые в Word 2007 при работе с документом, содержащим макросы.

Внешний вид показанного выше диалогового окна может привести в замешательство по следующим причинам:

- очень крупный значок щита оранжевого цвета;
- надпись «Оповещение системы безопасности» крупными буквами;
- выделенное полужирным шрифтом предупреждение;

- объемное сообщение, содержащее более 80 слов;
- наличие сведений технического характера (путь к файлу).

Кроме того, в этом диалоговом окне приводятся рекомендации по отключению активного содержимого (макросов), однако фактически не называются причины этого, за исключением того, что не удается определить степень надежности файла. Вместе с тем у пользователя определенно есть свои причины для загрузки файла, а отключение макросов может повлечь за собой утрату функциональных возможностей документа.

Для сравнения: при открытии того же файла в Word 2010 панель сообщений будет иметь следующий вид:

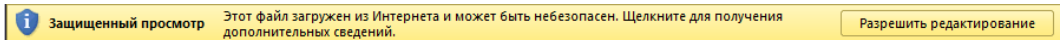


Рис. 28. Вид панели сообщений Word 2010 при открытии того же документа.

По сравнению с приложением Word 2007 вид панели сообщений существенно переработан:

- Панель выделена цветом и четко различима на фоне окна приложений, чего нет в Word 2007.
- Значок щита синего цвета с буквой «i» предполагает наличие на панели сведений, которые могут быть полезны пользователю.
- Желтый цвет панели предполагает привлечение внимания со стороны пользователя, но никак не опасность (сведения на панели красного цвета требуют более внимательного рассмотрения, чем на желтой панели).
- Четко описана причина, по которой требуется внимание пользователя: файл загружен из Интернета и может быть небезопасным.
- Поскольку файл может быть небезопасным, система информирует пользователя, что документ был открыт в режиме защищенного просмотра.
- Поскольку пользователь явно загружал файл из Интернета с определенной целью, в приложении Word 2010 предполагается, что пользователь будет работать с ним. Для этого имеется кнопка, позволяющая включить возможности редактирования документа всего одним щелчком мыши.

В тексте также содержится ссылка «Щелкните для получения дополнительных сведений», с помощью которой пользователи могут более подробно узнать о причинах появления сообщения. В этом случае открывается представление следующего вида:

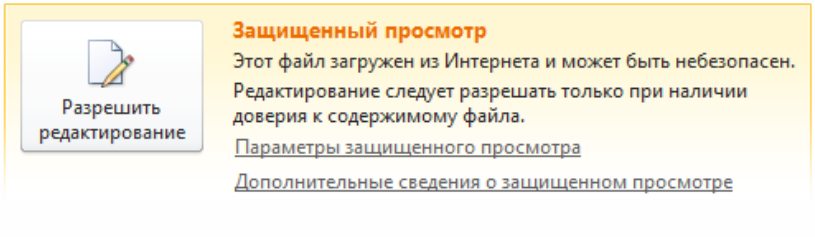


Рис. 29. Представление в приложении Word 2010, которое отображается при щелчке ссылки «Щелкните для получения дополнительных сведений».

Такой вид уведомлений гораздо более информативен и понятен пользователю, чем описанное выше предупреждение системы безопасности в приложении Word 2007. Вместо рекомендаций по выбору различных действий пользователю задается конкретный вопрос: «Можете ли вы доверять содержимому этого файла?». Таким образом, пользователю предлагается принять решение о надежности файла, которое само по себе является общим и не носит технический характер, как решение о безопасности. Если пользователь считает документ надежным, можно нажать кнопку «Разрешить редактирование», чтобы выйти из режима защищенного просмотра и открыть документ в приложении Word. Если точно определить степень надежности документа сложно, можно просто закрыть его и перейти к работе с другими документами.

Еще несколько слов о панели сообщений Word 2010. При нажатии кнопки «Разрешить редактирование» режим защищенного просмотра закрывается, документ открывается в приложении Word, после чего отображается вторая панель сообщений:

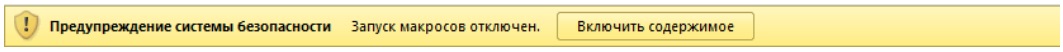


Рис. 30. Панель сообщений Word 2010 с уведомлением об отключении макросов.

По сравнению с показанной выше панелью сообщений Word 2007 в этой панели то же уведомление представлено совсем по-другому. В приложении Word 2007 цвет панели совпадает с цветом ленты, из-за чего ее достаточно сложно обнаружить, за исключением небольшого значка оранжевого цвета. Напротив, в приложении Word 2010 панель выделена желтым цветом и содержит желтый значок щита с восклицательным знаком, что свидетельствует о необходимости уделить внимание. Повторимся, в Word 2010 предполагается, что пользователь планирует продолжить работу с файлом, для чего на панели отображается кнопка, позволяющая одним щелчком мыши включить активное содержимое документа (макросы). Если в документе отсутствует активное содержимое, вторая панель сообщений не отображается.

После нажатия кнопки «Включить содержимое» включаются все находящиеся в документе макросы, и в дальнейшем уведомления системы безопасности не отображаются. Для сравнения: в приложении Word 2007 диалоговое окно предупреждения системы безопасности отображается каждый раз. Очевидно, что пользовательский интерфейс Office 2010 является более дружественным. В Office 2010 уведомление отображается только дважды при первом открытии документа. В Office 2007 уведомления отображаются каждый раз при открытии документа.

Управление потоком информации с помощью Office 2010

Как уже было отмечено выше, в системе Office 2010 не только обеспечивается противодействие потенциальным эксплойтам, но также представлены усовершенствованные технологии, позволяющие управлять потоком информации на уровне организации. В следующем разделе описываются некоторые улучшения системы безопасности Office 2010 в этой области.

Параметры сложности паролей

В предыдущих версиях приложений Word, Excel и PowerPoint поддерживается защита документов, электронных таблиц и презентаций паролем, что позволяет исключить несанкционированный доступ к их содержимому. При защите паролем документ шифруется с применением поддерживаемых в системе Office и в используемой ОС Windows технологий шифрования. Например, для защиты паролем документа в Word 2007 необходимо нажать кнопку Office, навести указатель мыши на элемент «Подготовить», выбрать команду «Зашифровать документ» и дважды ввести пароль для его подтверждения (обратите внимание, что пароли следует вводить с учетом регистра). После этого на основе пароля формируется ключ шифрования. Поэтому чем длиннее и сложнее пароль, тем надежнее будет зашифрован документ. В системе Office 2010, в которой реализован новый пользовательский интерфейс на основе обновленного меню «Файл», для защиты документа Word паролем необходимо последовательно выбрать элементы «Файл» > «Сведения» > «Защитить документ» > «Зашифровать паролем».

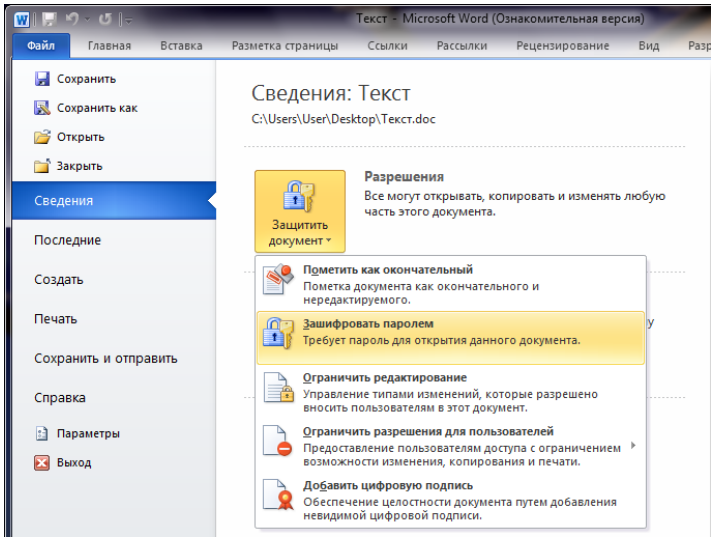


Рис. 31. Защита документа Word 2010 посредством шифрования на основе заданного пароля.

В системе безопасности Office 2010 для приложений Word, Excel и PowerPoint представлена новая возможность, позволяющая принудительно задавать требования к длине и сложности пароля, что гарантирует создание пользователями достаточно надежных паролей для шифрования документов. Эти требования могут настраиваться администраторами с помощью групповой политики или центра развертывания Office. Можно задать требования к минимальной длине, минимальной длине и сложности паролей, а также обязательное соответствие минимальной длины и сложности пароля требованиям, установленным политикой паролей домена. Параметры групповой политики, используемые для настройки требований к длине и сложности пароля в системе Office, находятся по следующему пути:

> Конфигурация пользователя\Политики\Административные шаблоны\Microsoft Office 2010\Безопасность.

Важнейшую роль среди этих политик играет параметр «Задать уровень правил для паролей», изображенный на рисунке ниже.

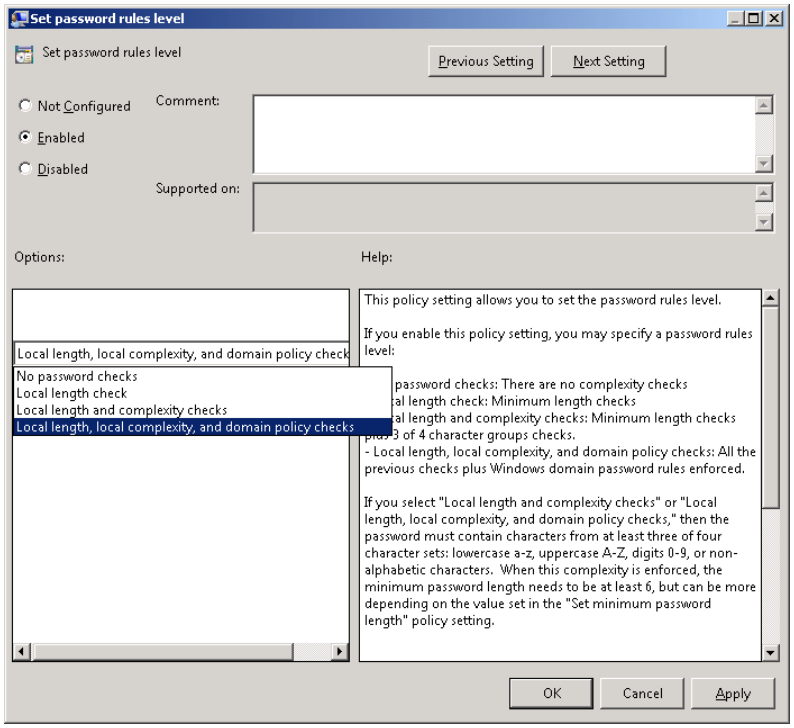


Рис. 32. Параметр политики «Задать уровень правил для паролей».

По умолчанию принудительная проверка паролей не выполняется, и пользователи могут устанавливать пароли произвольной длины или сложности. Если включена локальная проверка длины, число знаков в пароле не должно быть меньше значения, заданного с помощью параметра политики «Задать минимальную длину пароля», который также располагается в разделе «Административные шаблоны\Microsoft Office 2010\Безопасность». Если включена локальная проверка сложности, пароли должны содержать знаки как минимум трех из следующих четырех видов: a-z, A-Z, 0-9 и не буквенно-цифровые знаки. Если включена проверка с использованием политики домена, приложение Office сначала пытается подключиться к контроллеру домена и получить политику паролей домена.
Если в течение заданного в групповой политике временного интервала не удается подключиться к контроллеру домена, в приложении Office по умолчанию используются параметры политики для проверки длины и сложности паролей, заданные локально.

Корпорация Майкрософт рекомендует организациям, применяющим политики паролей домена, использовать эти политики для защиты документов Office. Для этого следует включить параметр политики «Задать уровень правил для паролей», как показано на приведенном выше рисунке, и соответствующим образом настроить другие политики паролей Office.

Дополнительные сведения о защите документов Office 2010 паролем см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/ff657853.aspx, а также в блоге группы разработчиков Office по следующему адресу: http://blogs.technet.com/b/office2010/archive/2009/10/16/enabling-password-rules-for-office-2010.aspx.

Улучшения системы шифрования

В системе Office 2010 также представлен ряд улучшений технологий шифрования и цифровой подписи, которые позволяют противостоять эксплойтам, связанным с нарушением целостности и конфиденциальности документов Office. В этой области введены два основных улучшения: гибкая система шифрования и проверка целостности зашифрованных файлов. Эти функции можно настраивать с помощью групповой политики; они не представлены в центре управления безопасностью.

Гибкая система шифрования поддерживает технологию криптографии следующего поколения (CNG), с помощью которой администраторы могут задавать собственные алгоритмы шифрования, которые будут использоваться для шифрования и подписывания документов Office. Технология CNG позволяет использовать любые алгоритмы шифрования и хэширования, поддерживаемые операционной системой. Кроме того, интерфейс CNG поддерживает расширение с использованием сторонних модулей шифрования. Интерфейс CNG поддерживается приложениями Word, Excel, PowerPoint, Access, OneNote и InfoPath из набора Office 2010. По умолчанию при защите паролем файла в формате Office 2010 OpenXML (например, DOCX) для шифрования документа

используется 128-битовый алгоритм AES.[13] В системах Office 2007 с пакетом обновления 2 (SP2) и Office 2010 по умолчанию поддерживается одинаковый набор алгоритмов шифрования (AES, DES, DESX, 3DES, 3DES_112 и RC2) и хэширования (MD2, MD4, MD5, RIPEMD-128, RIPEMD-160, SHA-1, SHA256, SHA384 и SHA512). Это означает, что зашифрованные документы Word 2010 также можно просматривать в приложении Word 2007 с пакетом обновления (SP2). Кроме того, приложения Office 2010 поддерживают шифрование по стандарту Suite B.

Проверка целостности зашифрованных файлов позволяет администраторам внедрять код HMAC при шифровании документа Office. Это гарантирует, что зашифрованный документ не подвергся незаконному изменению. С помощью групповой политики администраторы могут настраивать поставщик служб шифрования, хэш и контекст, используемый для создания кода HMAC. Поддержка целостности зашифрованных файлов поддерживается в приложениях Word, Excel и PowerPoint из набора Office 2010.

Дополнительные сведения об улучшениях системы шифрования в Office 2010 см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/cc179125.aspx.

Улучшения цифровых подписей

В системе Office 2010 представлен ряд улучшений в области цифровых подписей. Цифровые подписи все более активно используются в бизнес-сообществе и позволяют гарантировать подлинность, целостность и неподдельность данных, содержащихся в подписанных документах. Если документ подписан с использованием сертификата, полученного в надежном центре сертификации, получатель такого документа может проверить личность пользователя,

---

[13] В Office 2010 для шифрования старых двоичных форматов файлов Office (например, DOC) по-прежнему используется менее безопасный алгоритм RC4. Это позволяет обеспечить обратную совместимость с приложениями из набора Office 2003 и более ранних версий. Тем не менее, поскольку алгоритм RC4 легко поддается взлому, его не рекомендуется применять.

подписавшего документ. Это позволяет гарантировать, что документ не был незаконно изменен с момента подписания.

Основная проблема при работе с цифровыми подписями заключается в том, что по истечении срока действия соответствующего сертификата подпись становится недействительной и не может быть проверена. В Office 2010 эта проблема решена благодаря поддержке надежных отметок времени, которые позволяют проверить подлинность подписи и надежность защиты документа даже после того, как срок действия сертификата истек. Надежные отметки времени формируются на базе стандарта XAdES консорциума W3C и поддерживаются приложениями Word, Excel, PowerPoint и Infopath из набора Office 2010. Стандарт XAdES представляет собой набор многоуровневых расширений открытого стандарта XML-DSig, который использовался для добавления цифровых подписей в системе Office 2007.

В таблице 1 представлены разные уровни подписей XAdES, которые могут реализоваться в Office 2010 поверх подписей XML-DSig для более надежной защиты цифровых подписей. Поскольку в Office 2007 по умолчанию используется тип подписи, отличный от установленного в Office 2010, цифровые подписи, созданные в приложениях Office 2010, будут совместимы с приложениями Office 2007 только в том случае, если стандарт XAdES для системы Office 2010 был отключен с помощью групповой политики.[14]

Таблица 1. Расширения XAdES для стандарта XML-DSig в системе Office 2010.

Уровень подписи	Описание
XML-DSig	Базовая цифровая подпись, которая перестает считаться надежной в момент истечения срока действия сертификата (используется по умолчанию в Office 2007)

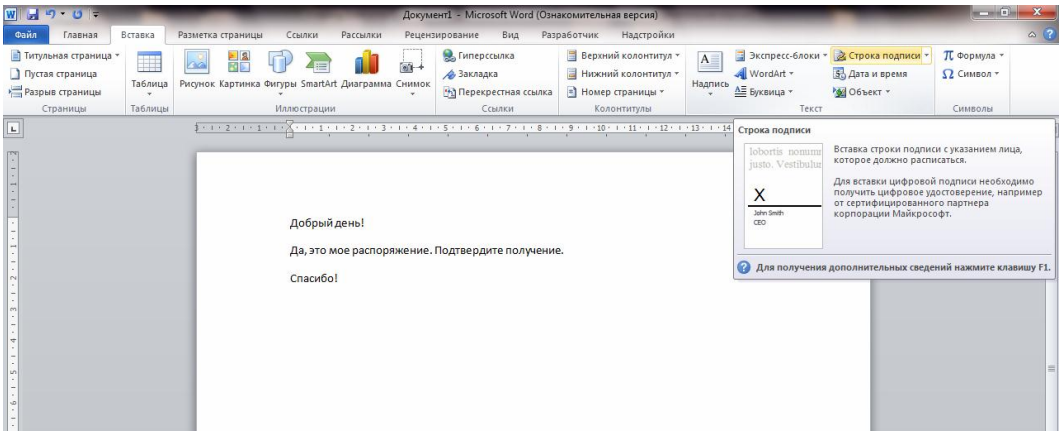
[14] Из-за различий в реализации цифровых подписей в разных версиях Office подписи документов, добавленные в приложениях Office 2010 или Office 2007, не подлежат проверке в приложениях Office 2003 или более ранних версий.

XAdES-EPES (базовый)	К подписи XML-DSig добавлены сведения о сертификате (используется по умолчанию в Office 2010)
XAdES-T (отметка времени)	К разделам подписи XML-DSig и XAdES-EPES добавлена отметка времени, что позволяет устранить проблему, связанную с истечением срока действия сертификата)
XAdES-C (полный)	Добавлены ссылки на сведения о цепочке сертификатов и состоянии отзыва
XAdES-X (расширенный)	К элементу XML-DSig SignatureValue, а также разделам –T и –C добавлена отметка времени, что позволяет защитить дополнительные данные от подделки
XAdES-X-L (расширенный долгосрочный)	Сведения о действительном сертификате и его отзыве сохранены вместе с подписью, что позволяет проверить сертификат даже в случае недоступности серверов сертификатов

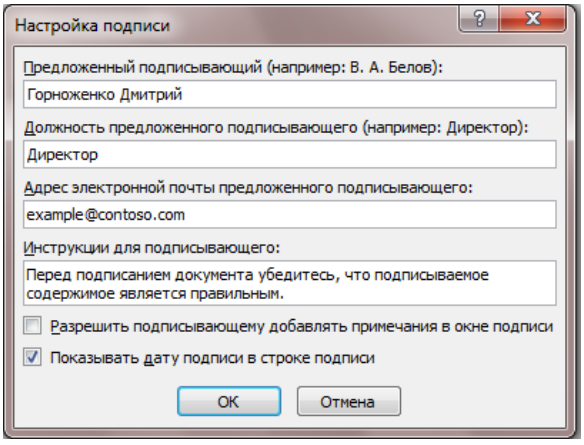
В Office 2010 также усовершенствован механизм применения цифровых подписей к документам. Например, при добавлении подписи к документу в приложении Word 2007 подпись невидима. Для ее отображения необходимо открыть область задач «Подпись». В Office 2010 скрытые подписи по-прежнему поддерживаются, однако пользователи могут вставлять строку подписи[15], благодаря которой можно визуально удостовериться, что документ имеет цифровую подпись. Например, чтобы вставить строку подписи в документ Word 2010, выполните указанные ниже действия.

[15]В Office 2010 также поддерживаются штампы подписей, которые часто используются вместо строк подписи в некоторых странах Юго-Восточной Азии.

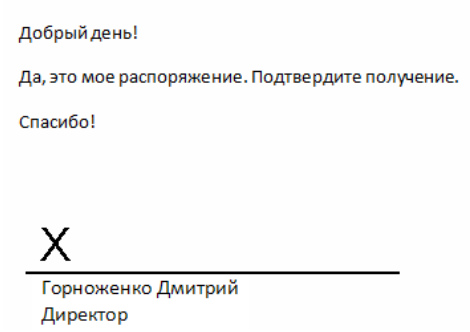
1. Сначала проверьте наличие цифрового удостоверения, с помощью которого можно подписывать документы. Сохраните документ в формате OpenXML (DOCX).
2. На вкладке «Вставка» ленты в группе «Текст» щелкните элемент «Строка подписи».



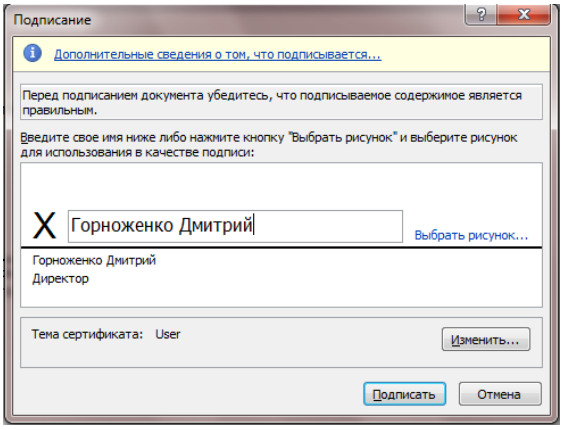
3. В диалоговом окне «Настройка подписи» введите свои имя, должность и адрес электронной почты.



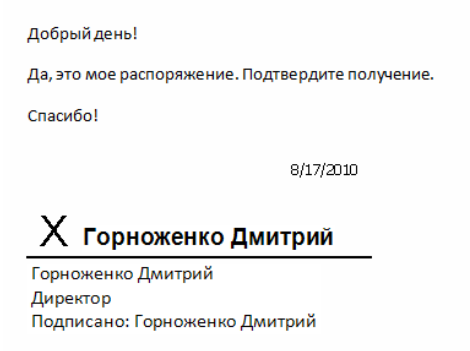
4. Нажмите кнопку «ОК». В документ будет добавлена пустая подпись.



5. Дважды щелкните строку подписи, чтобы открыть диалоговое окно «Подписание». Введите свое имя еще раз.



6. Нажмите кнопку «Подписать». Внешний вид строки подписи изменится, свидетельствуя о добавлении цифровой подписи к документу.



Дополнительные сведения об улучшениях в области цифровых подписей в Office 2010 см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/cc545900.aspx, а также в блоге группы разработчиков Office по следующему адресу: http://blogs.technet.com/b/office2010/archive/2009/12/08/digital-signitures-in-office-2010.aspx.

Инспектор документов

Инспектор документов — это средство обеспечения конфиденциальности, с помощью которого пользователи могут удалять из документов личные и скрытые сведения перед их отправкой другим лицам. Компонент «Инспектор документов» впервые был представлен в системе Office 2007. В Office 2010 пользовательский интерфейс этого компонента был улучшен.

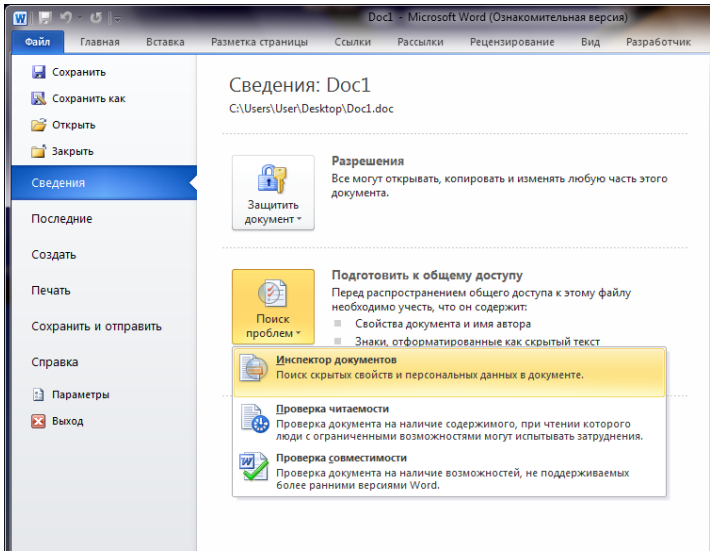


Рис. 33. Использование инспектора документов в Word 2010.

Инспектор документов — это новая возможность Office 2010, позволяющая проверять документы на наличие невидимого содержимого (объекты, которые имеют формат невидимых и не отображаются). Обратите внимание, что не проверяются объекты, которые скрыты под другими объектами. Также в Office 2010 представлена новая возможность «Проверка читаемости»,

с помощью которой пользователи могут проверять, насколько создаваемые ими документы будут удобны для восприятия пользователями с ограниченными возможностями. В Office 2010 также представлены различные параметры конфиденциальности, которые можно настраивать с помощью групповой политики.

Дополнительные сведения о параметрах конфиденциальности в Office 2010 см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/cc179123.aspx; сведения о новом средстве проверки читаемости см. по следующему адресу: http://technet.microsoft.com/en-us/library/ff602182.aspx.

Управление правами на доступ к данным

Управление правами на доступ к данным — это набор технологий, с помощью которых организации могут управлять потоком цифровых данных, устанавливая разрешения на доступ пользователей к документам и сообщениям. Технологии управления правами на доступ к данным построены на основе служб управления правами, которые были представлены в ОС Windows Server 2003. В ОС Windows Server 2008 R2 эти службы доступны в качестве роли сервера служб управления правами Active Directory (AD RMS). Внедрение этих технологий Майкрософт позволяет организациям предотвратить пересылку, копирование или печать конфиденциальных сведений пользователями, не имеющими соответствующих полномочий.

Для внедрения технологии управления правами на доступ к данным Office 2010 требуется инфраструктура служб управления правами. Настройку параметров для этой технологии можно выполнять с помощью групповой политики или центра развертывания Office. Дополнительные сведения о развертывании технологии управления правами на доступ к данным в Office 2010 см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/cc179103.aspx.

Сравнение систем безопасности Office 2010 и Office 2007

Если в организации планируется переход с Office 2007 на Office 2010, следует внимательно ознакомиться с новыми улучшениями средств обеспечения безопасности и конфиденциальности в Office 2010, с теми функциями, которые были представлены в Office 2007 и были улучшены в системе Office 2010, а также с возможностями новой версии Office, которые не претерпели существенных изменений. Эти сведения в удобной форме представлены в таблице 2.

Таблица 2. Сравнение функций обеспечения безопасности и конфиденциальности в Office 2010 и Office 2007.

Функция обеспечения безопасности	Описание	Office 2007	Office 2010
Параметры надстроек для приложений Office	Позволяет отключать надстройки, требовать подписи надстроек надежным издателем и настраивать предупреждения надстроек.	Новинка	Не изменено
Гибкие возможности шифрования	Позволяют задавать параметры для шифрования документов.	н/д	Новинка
Предотвращение выполнения данных (DEP)	Программная и аппаратная технология, которая позволяет усилить защиту по направлениям вероятных атак вирусов и вирусов-червей, которые используют уязвимости, связанные с переполнением буфера.	н/д	Новинка

Инспектор документов	Средство обеспечения конфиденциальности, которое позволяет пользователям удалять личные и скрытые сведения из документов.	Новинка	Улучшен пользовательский интерфейс
Улучшенные глобальные параметры и параметры, относящиеся к приложениям, для макросов VBA	Позволяют отключать VBA и настраивать параметры предупреждений о макросах.	Новинка	Не изменено
Параметры блокировки файлов	Набор параметров безопасности, которые позволяют предотвратить открытие и сохранение определенных типов файлов.	Новинка	Улучшены и расширены параметры
Глобальные параметры и параметры, относящиеся к приложениям, для элементов ActiveX	Позволяют отключать все элементы ActiveX, настраивать их инициализацию и запросы.	Новинка	Не изменено
Проверка целостности зашифрованных файлов	Позволяет реализовать код HMAC при шифровании файла.	н/д	Новинка
Панель сообщений	Элемент интерфейса пользователя, который служит для отображения уведомлений и предупреждений при открытии документа с потенциально опасным содержимым.	Новинка	Улучшен пользовательский интерфейс панели сообщений

Бит аннулирования ActiveX для Office	Возможность Office, с помощью которой администраторы могут запретить выполнение определенных элементов ActiveX в приложениях Office.	Реализовано как бит аннулирования ActiveX для браузера Internet Explorer	Реализовано как бит аннулирования ActiveX для Office
Проверка файлов Office	Компонент, который проверяет файлы на наличие отличий в формате и может запретить открытие файла, если формат недопустим.	н/д	Новинка
Проверка сложности паролей и ее принудительное применение	Позволяет проверять длину и сложность паролей, а также принудительно применять такую проверку с помощью политик паролей домена.	н/д	Новинка
Защищенный просмотр	Возможность, помогающая снизить риск атак и позволяющая пользователям просматривать ненадежные и потенциально опасные файлы в изолированной среде.	н/д	Новинка
Центр управления безопасностью	Центральная консоль в интерфейсе пользователя, которая позволяет просматривать и изменять параметры безопасности и конфиденциальности.	Новинка	Улучшены и расширены параметры

Надежные документы	Средство безопасности, которое позволяет пользователям обозначать безопасные документы.	н/д	Новинка
Надежные расположения	Возможность, которая позволяет отличать безопасные и небезопасные документы.	Новинка	Не изменено
Отметки времени для цифровых подписей	Отметки времени позволяют убедиться, что цифровые подписи действительны и защищены, даже если срок действия сертификата, который использовался для подписи документа, истек.	н/д	Новинка

Office 2010 и Windows 7

Система безопасности Office 2010 претерпела значительные изменения по сравнению с предыдущей версией этого набора. При этом нередко требуется знать, существуют ли какие-либо зависимости между этими улучшениями и версией ОС Microsoft Windows, в которой установлена система Office 2010. Это важный момент для организаций, которые по-прежнему используют ОС Windows XP и планируют развернуть систему Office 2010 в существующих средах.

Если коротко, то можно сказать, что Windows 7 является оптимальной операционной системой для работы с Office 2010. Ниже перечислены основные причины этого выбора.

- В Windows 7 благодаря системе криптографии следующего поколения (CNG) поддерживаются дополнительные алгоритмы шифрования. Этот набор программных интерфейсов, впервые представленный в ОС Windows Vista и Windows Server 2008, используется для установки дополнительных поставщиков служб шифрования, управления ключами шифрования, создания хэшей, а также шифрования и расшифровки данных. В отличие от интерфейса CryptoAPI 1.0 в ОС Windows XP, в системе CNG поддерживаются алгоритмы шифрования по стандарту Suite B, разработанному правительством США. Это означает, например, что в приложениях Office 2010, работающих в системе Windows 7, можно использовать алгоритмы шифрования на основе эллиптических кривых (ECC) и другие современные технологии, которые недоступны при использовании приложений Office 2010 в ОС Windows XP.
- В Windows 7 поддерживается технология ограничения привилегий пользовательского интерфейса (UIPI). Эта расширенная модель безопасности впервые была представлена в ОС Windows Vista и позволяет блокировать доступ процессов с низкой степенью целостности к процессам с высоким уровнем целостности. Такая модель обеспечивает защиту от так называемых «подрывных» атак, при которых процесс с низкой степенью целостности пытается получить повышенные права, внедряя код в процесс с высокой степенью целостности с помощью сообщений Windows. Например, в ОС Windows XP поверх подлинного диалогового окна Office

2010 с помощью вредоносного фрагмента кода может отрисовываться поддельное окно. Пользователь, считая отображаемое окно подлинным, выполняет в нем определенные действия, которые влекут за собой выполнение вредоносного кода. В Windows XP невозможно полностью предотвратить «подрывные» атаки такого рода, что может являться одним из оснований для модернизации инфраструктуры настольных компьютеров до Windows 7. Применение модели UIPI позволяет предотвратить атаки подобного рода в ОС Windows Vista и более поздних версий. Это означает, например, что, если в ОС Windows 7 появляется запрос Office 2010 на включение функций редактирования для документа, загруженного из Интернета, пользователь может быть уверен, что кнопка «Разрешить редактирование» панели сообщений действительно является кнопкой Office 2010 и не содержит вредоносный код.

- Улучшения пользовательского интерфейса в Windows 7, такие как усовершенствованная панель задач, списки переходов и унифицированная поддержка ленты в приложениях Windows, позволяют повысить производительность пользователей приложений Office 2010 по сравнению с тем, когда эти же приложения используются в ОС Windows XP. Новая функция библиотек в Windows 7 также позволяет более эффективно выполнять поиск документов Office и упорядочивать их.

В целом при работе с Office 2010 в ОС Windows 7 обеспечивается более высокий уровень безопасности и оптимизированное взаимодействие с пользователем по сравнению с использованием приложений Office 2010 в ОС Windows XP. Более подробный обзор новых функций системы безопасности Office, доступных в различных версиях Windows, см. в приложении к этому документу.

Заключение

Office 2010 — это наиболее защищенная на данный момент версия системы Microsoft Office. Благодаря усовершенствованной модели надежности, в которой можно определять надежность отдельных файлов, а также таким новым технологиям, как проверка файлов Office и защищенный просмотр, обеспечивается максимально эффективная защита пользователей от эксплойтов, использующих уязвимости документов Office. Кроме того, в рамках общего улучшения технологий шифрования реализованы новые возможности цифровых подписей и поддержка требований к сложности пароля на основе домена. Это позволяет более эффективно защищать документы Office пользователей от несанкционированного изменения. Поддержка технологии предотвращения выполнения данных обеспечивает дополнительную защиту, что в сочетании с другими технологиями безопасности Office позволяет сформировать многоуровневую систему безопасности для пользователей приложений Office. Дополнительные сведения о функциях и технологиях, описываемых в этом документе, см. в разделе «Дополнительные ресурсы» ниже.

Дополнительные ресурсы

В данном документе приводятся ссылки на некоторые дополнительные ресурсы, в том числе разделы библиотеки TechNet и публикации в блоге группы разработчиков Office. В этом разделе обобщены все приведенные в документе ссылки для более быстрого доступа к ресурсам, посвященным системе безопасности Office 2010.

- **Надежные издатели.** Дополнительные сведения о функции надежных издателей Office 2010 см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/ff428091.aspx.
- **Надежные расположения.** Дополнительные сведения о функции надежных расположений в Office 2010 см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/cc179039.aspx.
- **Блокировка файлов.** Дополнительные сведения о функции блокировки файлов в Office 2010 см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/cc179230.aspx.
- **Проверка файлов Office.** Дополнительные сведения о функции проверки файлов Office см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/ee857084.aspx, а также в блоге группы разработчиков Office по следующему адресу: http://blogs.technet.com/b/office2010/archive/2009/12/16/office-2010-file-validation.aspx.
- **Режим защищенного просмотра.** Дополнительные сведения о режиме защищенного просмотра см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/ee857087.aspx, а также в блоге группы разработчиков Office по следующему адресу: http://blogs.technet.com/b/office2010/archive/2009/08/13/protected-view-in-office-2010.aspx.
- **Надежные документы.** Дополнительные сведения о надежных документах см. в блоге группы разработчиков Office по следующему адресу: http://blogs.technet.com/b/office2010/archive/2009/09/28/trusted-documents.aspx.

- **Параметры макросов VBA.** Дополнительные сведения о настройке параметров для макросов VBA см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/ee857085.aspx.
- **Параметры элементов ActiveX.** Дополнительные сведения о настройке параметров элементов ActiveX см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/cc179076.aspx.
- **Параметры надстроек.** Дополнительные сведения о настройке параметров надстроек см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/ee857086.aspx.
- **Предотвращение выполнения данных.** Дополнительные сведения о поддержке предотвращения выполнения данных в Office 2010 см. в блоге группы разработчиков Office по следующему адресу: http://blogs.technet.com/b/office2010/archive/2010/02/04/data-excecution-prevention-in-office-2010.aspx.
- **Бит аннулирования ActiveX.** Дополнительные сведения о поддержке битов аннулирования ActiveX в Office 2010 см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/cc179076.aspx.
- **Параметры сложности пароля.** Дополнительные сведения о защите документов Office 2010 паролем см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/ff657853.aspx, а также в блоге группы разработчиков Office по следующему адресу: http://technet.microsoft.com/en-us/library/ff657853.aspx.
- **Улучшения системы шифрования.** Дополнительные сведения об улучшениях системы шифрования в Office 2010 см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/cc179125.aspx.
- **Улучшения цифровых подписей.** Дополнительные сведения об улучшениях в области цифровых подписей в Office 2010 см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/cc545900.aspx, а также в блоге группы разработчиков Office по следующему адресу:

http://blogs.technet.com/b/office2010/archive/2009/12/08/digital-signitures-in-office-2010.aspx.

- **Параметры конфиденциальности.** Дополнительные сведения о параметрах конфиденциальности в Office 2010 см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/cc179123.aspx.
- **Проверка читаемости.** Дополнительные сведения о компоненте «Проверка читаемости» см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/ff602182.aspx.
- **Управление правами на доступ к данным.** Дополнительные сведения о развертывании технологии управления правами на доступ к данным в Office 2010 см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/cc179103.aspx.
- **Система безопасности Outlook 2010.** Дополнительные сведения о системе безопасности Outlook 2010 см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/cc179213.aspx. См. также раздел, посвященный изменениям в Outlook 2010, по следующему адресу: http://technet.microsoft.com/en-us/library/cc179110.aspx.
- **Параметры групповой политики Office 2010.** Дополнительные сведения о параметрах групповой политики Office 2010 см. в файле *Office2010GroupPolicyAndOCTSettings_Reference.xls*, который доступен на странице, посвященной файлам административных шаблонов Office 2010 (ADM, ADMX/ADML) и центру развертывания Office, веб-сайта Центра загрузки Майкрософт.
- **Центр развертывания Office.** Дополнительные сведения о центре развертывания Office для системы Office 2010 см. в разделе библиотеки TechNet по следующему адресу: http://technet.microsoft.com/en-us/library/cc179097.aspx.
- **Стандарт Office Open XML.** Дополнительные сведения о стандарте Office Open XML, используемом в системах Office 2007 и более поздних версий, см. на веб-странице по следующему адресу: http://www.microsoft.com/standards/openxml/standard/.