

The points of interest detection is a key step in such application as: object recognition, path tracking, computer vision, robot navigation etc. The requirements which desirable for a corner detectors are: high repeatability rate (good stability), robustness to noise, efficiency of using computing resources.

УДК 681.3.06

*Доц. А.П. Матковский, канд. техн. наук;
доц. О.А. Немкова, канд. физ.-мат. наук –
Львовский ГИИТУ им. Вячеслава Чорновола*

ЗАЩИТА ДАННЫХ В ОФИСНОМ ПАКЕТЕ MICROSOFT OFFICE 2007 ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS XP

Рассмотрен вопрос программной защиты компьютерной информации, в том числе документов офисного пакета Windows XP. Приведены как общие методы защиты данных ОС Windows XP, так и специфические, которые отвечают различным офисным приложениям. Обращается внимание на возможность "взлома" защиты.

Ключевые слова: защита данных, параметры безопасности, технологии безопасности, пароль, Microsoft Office 2007.

В настоящее время бурного развития информационных систем, технологий и коммуникаций особо острой является необходимость защиты информации. Очевидна актуальность вопросов с повышения уровня информационной безопасности документов офисных приложений на сегодня и в ближайшем будущем. В литературе (в большинстве англо- и русскоязычной) изучаются проблемы информационной безопасности компьютерных сетей, баз данных, разных типов электронных документов. В работе [1] рассматривалась защита данных офисного пакета Windows XP 2003.

Данная работа посвящена вопросам защиты и взлома информации в наиболее популярном на сегодняшний день офисном пакете Microsoft Office 2007 операционной системы Windows XP. Приведены некоторые рекомендации по защите документов.

Параметры безопасности Office. При настройке параметров безопасности Office 2007 с помощью программы Office Customization Tool есть возможности:

1. добавить цифровые сертификаты к списку надежных издателей;
2. задать пути к папкам – надежным источникам;
3. определить параметры надежных источников при запуске приложений Visual Basic;
4. установить параметры инициализации небезопасных элементов управления ActiveX.

Технологии обеспечения безопасности. Существует большое количество технологий для обеспечения безопасности документов Microsoft Office 2007, коротко охарактеризуем основные из них [2, с. 1].

1. Internet Protocol Security (IPSec) – протокол защиты сетевого трафика на IP-уровне.

IPSec – это метод шифрования, который используется во время передачи данных по сети. Защита IPSec заканчивается в тот момент, когда информация достигает места назначения.

2. Rights Management Services (RMS) – служба управління правами.

Information Rights Management (IRM) – служба управління правами на доступ к данным.

Служба Windows RMS обеспечивает защиту документов путем шифрования с применением ограничений доступа, позволяющая сохранять эти ограничения даже после загрузки и открытия файла.

Служба IRM управления правами на доступ к данным предназначена для приложений Microsoft Office 2007, она позволяет пользователям задавать разрешения на доступ к документам для предотвращения копирования и печати данных пользователями, которые не имеют соответствующих прав. После ограничения разрешений на доступ к файлу с помощью службы IRM эти ограничения будут применяться независимо от того, где находятся данные, поскольку разрешения на доступ к документу хранятся в самом файле. С помощью службы управления правами на доступ к данным в Microsoft Word 2007 можно защитить файлы с расширениями.doc,.docx,.docm, dot,.dotx,.dotm.

3. Encrypting File System (EFS) – шифрованная файловая система.

Эта система позволяет пользователям шифровать файлы и папки при хранении их на томах NTFS, ограничивая доступ к файлам для ненужных пользователей. Шифрование защищает документы от других пользователей компьютера. Однако, если файл, хранящийся с помощью EFS, посылается по сети, то сначала он дешифруется, и лишь затем отсылается. EFS использует симметричное шифрование для защиты файлов, а также шифрование, основанное на паре открытый/закрытый ключ для защиты случайно сгенерированного ключа шифрования для каждого файла. Система отсутствует в версиях для домашних пользователей.

4. Файловая система NTFS (New Technology File System).

Файловая система NTFS позволяет пользователям установить разрешение на доступ к документам, хранящимся на диске. Пользователь, у которого нет разрешения на открытие файла, не сможет увидеть этот документ.

5. Подписи документа в Microsoft Office 2007.

Цифровая подпись, также называемая цифровым идентификатором, представляет собой электронный идентификатор, аутентифицирующий документ и подтверждающий достоверность его источника. Цифровые подписи помогают удостовериться подлинность и целостность документа, а также доказать любой из сторон авторство подписанного содержимого. Цифровую подпись можно добавить в документ как видимую, так и не видимую. Цифровая подпись выдается специальной организацией – Центром сертификации.

6. DeviceLock – ограничение доступа.

Программа позволяет ограничивать доступ к USB-портам, сменным носителям и любым другим устройствам. С помощью DeviceLock можно настроить права доступа, как для отдельных пользователей, так и групп пользователей. Поддерживаются все виды файловых систем – FAT, NTFS 4/5, CDFS, UDF и т.п. Имеется возможность удаленного управления, что позволяет обеспечивать доступ ко всем функциям программы по локальной сети.

Защита файлов. В Office Word 2007, Office Excel 2007 и Office PowerPoint 2007 меню File (Файл) содержит новую команду Finish (Подготовить) [3, с. 55], предоставляющую набор возможностей по защите завершаемых документов, рабочих листов и презентаций. Приведем некоторые из этих возможностей.

1. Опция **Properties** (Свойства) служит для ввода идентификационной информации об открытом файле.
2. Опция **Inspect Document** (Инспектор документов) позволяет осуществлять поиск и удаление любой личной или конфиденциальной информации в документе.
3. Опция **Restrict Permission** (Ограничить разрешения) дает возможность настроить и осуществлять контроль доступа к вашим файлам других пользователей.
4. Для присоединения к документу скрытой подписи следует воспользоваться опцией **Add A Digital Signature** (Добавить цифровую подпись),
5. Опция **Mark As Final** (Пометить как окончательная) позволяет сохранить доступную только для чтения версию файла.

Замечание. 1. Настройка и управление файловыми разрешениями, в отличие от Microsoft Office 2003, может осуществляться непосредственно из меню File (Файл): Finish (Подготовить) и затем Restrict Permissions (Ограничить разрешения).

Замечание 2. Из приложений: Microsoft Word 2007, Office Excel 2007, Office PowerPoint 2007 и Office Access 2007 можно обратиться к Trust Center (Центр управления безопасностью), открыв меню File (Файл) и выбрав команду Options (Параметры), чтобы установить соответствующие параметры безопасности и конфиденциальности.

Защита документов Microsoft Office посредством пароля. В Microsoft Office 2007 значительно улучшена защита документов. Если файл защищен паролем "на открытие", документ представляет собой OLE-контейнер, в котором находится информация о шифровании и сам зашифрованный документ. Для шифрования применяется криптостойкий алгоритм AES с длиной ключа 128 бит и хеширование SHA-1. Шифрование и хеширование обеспечивает криптопровайдер Microsoft Enhanced RSA and AES Cryptographic Provider. При формировании ключа происходит 50 тыс. преобразований по алгоритму SHA-1. При открытии документа эти операции выполняются почти мгновенно. Однако при последовательном переборе паролей скорость перебора резко падает. Поэтому если использовать вычислительную мощность только одного компьютера, реально возможно найти пароль длиной лишь до 4-5 символов. Следовательно, стойкий пароль к документу Office 2007 восстановить практически невозможно.

Значительно изменился алгоритм проверки паролей read only, защиты объектов **Excel**. Раньше в документе хранился двухбайтовый хеш пароля, сейчас же алгоритм хеширования определен записью в XML-файле, где определено количество итераций хеша.

Улучшилась система защиты и в **Microsoft Access**. Если раньше пароль на открытие файла хранился в заголовке почти открытым текстом, то теперь на

его нахождение путем прямого перебора потребуетсь весьма много времени. В Access 2007 убрана защита на уровне пользователей и групп пользователей.

Защита PST-файлов **Microsoft Outlook** не изменилась. Как и прежде, в файле хранится 32-битный хеш (CRC-32) от пароля, который может быть легко реверсирован.

Некоторые рекомендации по защите документов Microsoft Office. При задании пароля на открытие документа **Word, Excel** и **PowerPoint**:

- Не выбирайте алгоритм защиты, установленный по умолчанию.
- Выбирайте криптопровайдера Microsoft Strong Cryptographic Provider и длину ключа 128 бит [4].
- Задавайте пароль длиной не менее 8 символов и включайте в него разные виды символов – заглавные и строчные буквы, цифры, спецсимволы.
- Не используйте в качестве пароля слова из словаря, свои личные данные.
- При разработке приложений с использованием **VBA** макросы компилируйте и сохраняйте только откомпилированный код.
- При работе в **Microsoft Access** создавайте файлы MDE, что сделает недоступными исходные тексты.
- В **Microsoft Outlook** для хранения персональных данных используйте сервер Microsoft Exchange.

Восстановление забытых паролей. Охарактеризуем некоторые популярные программные продукты для восстановления паролей и данных.

Password Recovery Bundle – полный пакет программ для восстановления потерянных паролей и аудита безопасности системы.

Elcomsoft Distributed Password Recovery – программа для распределенного нахождения забытых паролей к различным типам документов.

Advanced Office Password Recovery (AOPR) – программа для восстановления потерянных паролей к документам, созданным в Microsoft Office 95/97/2000/XP/2003/2007/2010. Поддерживаются все типы документов Office. Для документов Microsoft Office 2007/2010 поддерживается аппаратное ускорение при помощи графических ускорителей и одновременное использование для перебора паролей всех имеющихся в системе центральных и графических процессоров.

Advanced Archive Password Recovery (ARCHPR) – программа для восстановления потерянных паролей к архивам, созданным ARJ/WinARJ, ZIP/WinZIP, ACE/WinACE, RAR/WinRAR.

Advanced Mailbox Password Recovery (AMBPR) – программа для восстановления забытых паролей к аккаунтам электронной почты, сохраненных в E-Mail клиентах. Поддерживаются почти все современные E-Mail клиенты.

Advanced VBA Password Recovery (AVPR) – программа для восстановления потерянных паролей к VBA-макросам в документах MS Office 97/2000/XP/2003.

Elcomsoft System Recovery (ESR) – это загрузочный диск (CD или USB flash drive) – восстановление паролей и данных в операционных системах, который подходит к любому компьютеру с установленной операционной системой Windows.

Elcomsoft Internet Password Breaker находит пароли для веб-сайтов, учетных записей, а также почтовых ящиков, хранимые в различных приложе-

ниях. Поддерживает все версии Internet Explorer до IE8 включительно, а также все версии Outlook Express, Microsoft Outlook, Windows Mail и Windows Live Mail, Elcomsoft Internet.

Proactive System Password Recovery (PSPR) – программа для восстановления паролей в ОС Microsoft Windows.

Ознакомьтесь с другими программами для восстановления паролей можно на <http://www.passwords.ru>.

Дополнительные возможности повышения безопасности.

I. Использование Office Excel 2007 с Excel Services. В Office Excel 2007 существует новая функция, позволяющая сохранять рабочую книгу на сервере с Microsoft Office SharePoint Server 2007 [3, с. 100]. Использование этой функции обеспечивает конфиденциальность электронных таблиц в Office SharePoint Server 2007. При этом задаются разрешения, определяющие, какие объекты (рабочие листы, таблицы, диаграммы и т.д.) будут доступны другим пользователям.

Настройка разрешений для рабочего листа осуществляется через меню **File**, далее **Save As** и **Excel Services**. В открывшемся диалоговом окне использование кнопки **Excel Services Options** (Параметры Excel Services) позволяет выбрать необходимые параметры отображения листов в браузере пользователя. После выбора опций и нажатия **ОК** необходимо ввести имя общей папки в поле **Save In** и нажать на кнопку **Save**. Файл сохранится в Office SharePoint Server 2007, и ваши сотрудники будут иметь доступ к рабочим листам через Интернет.

II. Список "Надежные издатели" в Office Access 2007. При открытии приложения базы данных Access 2007 программа автоматически сверяет его со списком Trusted Publishers (Надежные издатели), чтобы определить, представляет ли файл угрозу безопасности данных [3, с. 186]. Если файл содержит объекты, установленные отсутствующим в списке лицом, программа выдает предупреждение об угрозе безопасности. Чтобы добавить кого-либо в список Trusted Publishers, следует выбрать Trust Center (Центр доверия) на панели Document Action (Действия документа) и в открывшемся окне просмотреть список Trusted Publishers (Надежные издатели).

III. Фильтрация почты и защита от фишинга в Office Outlook 2007. В Outlook 2007 усовершенствован фильтр почты, выявляющий, перехватывающий и уничтожающий входящие сообщения, которые могут представлять собой нежелательную почту [3, с. 214]. Фильтр сканирует входящие сообщения, отслеживает подозрительные из них и отключает ссылки, которые могут привести на опасный сайт. При этом выводится предупреждение, ссылки в сообщении отключаются до тех пор, пока не будут разрешены пользователем.

В Office Outlook 2007 присутствуют функции защиты от фишинга, автоматически активирующиеся при начале работы с приложением. Параметры настройки защиты от фишинга находятся на вкладке Options диалогового окна Junk E-Mail Options (Параметры нежелательной почты).

Выводы. Существует много видов защиты и взлома информации, причем их количество и качество увеличивается из года в год. Исходя из конкрет-

ных условий (технические, программные, организационные возможности, важность данных) необходимо планировать систему защиты, используя имеющиеся возможности и помня, что абсолютных способов защиты не существует.

Литература

1. **Матковський А.П.** Захист даних в офісному пакеті Windows XP / А.П. Матковський // Збірник наукових праць ЛДІНТУ ім. В'ячеслава Чорновола. – Сер.: Фізико-математичні та технічні науки, 2009. – № 1. – С. 65-72.
2. **Microsoft Corporation.** Семь степеней защиты документов Office 2007. – Русские документы. [Електронний ресурс]. – Доступний з http://www.rusdoc.ru/articles/sem_stepenej_zaschity_dokumentov_office_2007/18285/.
3. **Мюррей К.** Новые возможности системы Microsoft® Office 2007 / К. Мюррей. – СПб.: Изд-во "ЭКОМ", 2007. – 248 с.
4. **Андрей Малышев.** Парольная защита документов Microsoft Office. – Компьютер Пресс 7'2007. [Електронний ресурс]. – Доступний з <http://www.compress.ru/article.aspx?id=17853&iid=827>.

Матковський А.П., Немкова О.А. Захист даних в офісному пакеті Microsoft office 2007 операційної системи Windows XP

Розглянуто питання програмного захисту комп'ютерної інформації, зокрема документів офісного пакету Windows XP. Наведено як загальні методи захисту даних ОС Windows XP, так і специфічні, що відповідають різним офісним додаткам. Зосереджено увагу на можливості "злому" захисту.

Ключові слова: захист даних, параметри безпеки, технології безпеки, пароль, Microsoft Office 2007.

Matkovsky A.P., Nemkova Ye.A. Data protection in office suite Microsoft Office 2007 of operating system Windows XP

Work is devoted the question of program defense computer's information, in particular, documents of office packet of Windows XP. Listed as common methods for data protection in OS Windows XP and specific one that correspond different applications of offices. Attention applies on possibility to "break" defense.

Keywords: data protection, security settings, technology security, password, Microsoft Office 2007.

УДК 621.438

*Асист. О.Ю. Жулай; асист. М.М. Труш;
доц. О.Б. Чайковський, канд. техн. наук – Кіровоградський НТУ;
доц. І.Б. Назар, канд. техн. наук – НУ "Львівська політехніка"*

ОБҐРУНТУВАННЯ ТА АЛГОРИТМ ВИБОРУ МЕТОДІВ ОТРИМАННЯ ДІАГНОСТИЧНОЇ ІНФОРМАЦІЇ

Обґрунтовано та отримано алгоритм вибору методів дослідження зміни технічного стану дизелів за діагностичною інформацією. Наведено основні характерні особливості вибору способів інформаційного забезпечення складних технічних об'єктів.

Ключові слова: засоби транспорту, дизелі, технічне обслуговування, ремонт, планово-попереджувальна стратегія, адаптивна стратегія, ресурс, надійність.

Вступ. Відомо [1], що будь-який із методів діагностики може дати лише часткову інформацію про технічний стан того чи іншого спряження, вузла чи агрегату. До того ж достовірність отриманої інформації відрізняється не лише для певного діагностичного методу, а й за діапазонами вимірювання. Саме