УДК 004.056.5

ЗАЩИТА ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

М.Ю. Летягин, М.С. Зуев

Данная статья посвящена разработке учебного пособия, посвященного криптографической защите информации, предназначенного для студентов и слушателей курсов повышения квалификации. Разрабатываемое пособие отличается простотой изложения и ориентировано на практическое изучение.

Ключевые слова: криптография, защита информации.

Тенденции нескольких лет ознаменовались постепенной заменой бумажной технологии обработки информации ее электронным аналогом. Со временем можно ожидать полного вытеснения бумажного документооборота электронным [1, 6, 8, 9]. В связи с этим одной из важнейших задач в электронном документообороте является обеспечение целостности и конфиденциальности электронных документов.

В связи с этим необходимо периодически проводить анализ основных способов защиты электронных документов и реализацию учебно-методического пособия, отражающего последние технологии защиты документов.

Под электронным документом понимают сведения, представленные в форме набора состояний элементов электронной вычислительной техники, иных электронных средств обработки, хранения и передачи информации, способной быть преобразованной в форму, пригодную для однозначного восприятия человеком, и имеющей атрибуты для идентификации документа [2, 7].

Надежным средством обеспечения конфиденциальности информации является шифрование. Шифрование – это процесс преобразования открытых данных в закрытые по определенному криптографическому алгоритму с использованием секретного ключевого элемента – ключа шифрования. Следующим средством, позволяющим на основе криптографических методов установить авторство и целостность электронного документа, является электронная цифровая подпись. Она формируется на основе секретного ключа и вычисленного с помощью хэш-функции значения хэша документа. Для обеспечения и конфиденциальности, и целостности информации следует использовать в комплексе шифрование и электронную цифровую подпись, что также можно совместить с каким-либо дополнительным сервисом, например, сжатием информации (архивацией). В качестве примера таких систем можно привести специализированный архиватор электронных документов Crypton ArcMail, предлагаемый фирмой «АНКАД». Также следует учесть, что использование любых систем защиты документооборота будет недостаточным без введения организационных мер [3].

Основные принципы парольной защиты документов можно разделить на три типа:

– хранение пароля в документе в виде обычного текста;

– хранение в документе контрольного значения, тем или иным образом получаемого из пароля;

– шифрование документа при помощи ключа, получаемого из пароля.

В разрабатываемом учебном пособии также рассматриваются технологии защиты документов в Microsoft Office и этапы их развития. Были выявлены угрозы, возникающие при работе с электронными документами. Более подробно была рассмотрена электронная цифровая подпись, ее виды, функции, технические особенности, программно-аппаратные комплексы для подписи документов и шифрование.

Рассмотрено программное обеспечение, позволяющее обеспечить защиту электронных документов. PGP Desktop является криптографической (шифровальной) программой с высокой степенью надежности, которая позволяет пользователям обмениваться информацией в электронном виде в режиме полной конфиденциальности. Эта программа построена на новом принципе работы – публичной криптографии или обмене открытыми (публичными) ключами, где пользователи могут открыто посылать друг другу свои публичные ключи с помощью сети «Интернет» и при этом не беспокоиться о возможности несанкционированного доступа каких-либо третьих лиц к их конфиденциальным сообщениям. PGP Desktop шифрует сообще-

ние таким образом, что никто, кроме получателя сообщения, не может ее расшифровать [4]. PGP Desktop предоставляет следующие возможности:

– хранение открытых ключей на удаленном сервере;

– использование 3 симметричных алгоритмов шифрования и 2 несимметричных;

– 4 способа запуска: E-mail plugins, PGP tray, PGP tools, контекстное меню;

– разделение ключей;

– установка уровня валидности ключа и доверия владельцу ключа.

TrueCrypt – компьютерная программа, которая позволяет создавать виртуальный зашифрованный логический диск, хранящийся в виде файла. С помощью TrueCrypt также можно полностью шифровать раздел жесткого диска или иного носителя информации, такой как флоппи-диск или USB флеш-память. Все сохраненные данные в томе TrueCrypt полностью шифруются, включая имена файлов и каталогов. Смонтированный том TrueCrypt подобен обычному логическому диску, поэтому с ним можно работать с помощью обычных утилит проверки и дефрагментации файловой системы [5]. TrueCrypt создавая зашифрованный виртуальный диск может создать его:

– в файловом контейнере, что позволяет легко работать с ним – переносить, копировать (в том числе на внешние устройства в виде файла), переименовывать или удалять;

– в виде зашифрованного раздела диска, что делает работу более производительной и удобной, в версии 5.0 добавилась возможность шифровать системный раздел;

– путем полного шифрования содержимого устройства, такого как USB флеш-память (устройства флоппи-диск не поддерживаются с версии 7.0).

Литература

1. Как обеспечить подлинность электронных документов [Электронный ресурс]. URL: http://ftp.forsys.ru

2. Традиционное понятие электронного документа [Электронный ресурс]. URL: http://www.okbsapr.ru

3. Электронная документация и ее защита [Электронный ресурс]. URL: http://www.coolreferat.com

4. Установка и применение программы PGP [Электронный ресурс]. URL: http://www.anwiza.com

5. TrueCrypt [Электронный ресурс]. URL: http://ru.wikipedia.org

6. Зуев М.С., Баранов П.А. Шифрование данных. Алгоритм ГОСТ 28147-89: учебное пособие // Федеральный депозитарий электронных изданий. Регистрационное свидетельство № 19565 от 14 июля 2010 г. № гос. регистрации 0321001202

7. Медведева О.Н., Зуев М.С. Электронное учебное пособие «Информатика для англоязычных студентов» // Гаудеамус. Тамбов, 2011. № 2(18). Материалы XV международной научно-практической конференции АПИИТ. С. 67-69.

8. Зуев М.С., Пелихосов А.А. Электронное учебное пособие «Разработка защищенного web-приложения на основе технологии AJAX» // Гаудеамус. Тамбов, 2011. № 2(18). Материалы XV международной научно-практической конференции АПИИТ. С. 37-38.

9. Хребтов Р.И., Зуев М.С. Разработка web-приложения, использующего защищенные базы данных // Гаудеамус. Тамбов, 2011. № 2(18). Материалы XV международной научно-практической конференции АПИИТ. С. 148-149.

УДК 004.6

БАЗА ДАННЫХ ПО СТАНДАРТАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

Д.В. Лопатин, В.А. Титова

Риски информационной безопасности представляют собой серьезную угрозу. Управление рисками является одним из ключевых элементов, позволяющих предотвращать интернет-мошенничество, перехват идентификаторов, повреждение веб-сайтов, кражу персональных данных и другие компьютерные инциденты.

Ключевые слова: стандарт, информационная безопасность, информационные угрозы, база данных.

Специалистам в области информационной безопасности (ИБ) сегодня почти невозможно обойтись без знаний соответствующих стандартов и спецификаций. Главной причиной систематизации является большое количество разработанных между-

* Работа выполнена при поддержке гранта РГНФ № 12-16-68005.