УДК 681.3

ПРИМЕНЕНИЕ ШИФРОВАННОГО ЛОГИЧЕСКОГО ДИСКА ДЛЯ ЗАЩИТЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Студент гр. 113017 Зеленкевич Н.Н.
Кандидат физ.-мат. наук, доцент Кривицкий П.Г.
Белорусский национальный технический университет,
научный сотрудник Кузьмицкая С.М.
ГНУ «НИЭИ Минэкономики РБ»

Проблема защиты данных на жестких дисках ПК является одной из самых актуальных в области защиты информации предприятий и учреждений. В операционной системе Windows имеется шифрованная файловая система (EFS), которая обеспечивает ядро технологии шифрования файлов, используемой для хранения шифрованных файлов на томах файловой системы NTFS. При этом, помощью криптографии открытого ключа шифруется содержимое файлов. Используются ключи, полученные от сертификата пользователя и дополнительных пользователей, а также от назначенных агентов восстановления шифрованных данных. После того как файл или папка зашифрованы, с ними работают так же, как и с другими файлами или папками. Шифрование является прозрачным для пользователя, зашифровавшего файл. Однако зашифрованные файлы могут стать расшифрованными, если файл копируется или перемещается на том, не являющийся томом NTFS. При перемещении незашифрованных файлов в зашифрованную папку они автоматически шифруются в новой папке. Для отдельного пользователя ПК решение о применении EFS связано со следующими вопросами. Во-первых, кто конкретно является агентами восстановления и дополнительными пользователями, имеющими доступ к зашифрованным файла пользователя. Во-вторых, как быть при утере сертификата (например, из-за вируса или ошибки ОС).

Привлекательным альтернативным решением является применение программных продуктов сторонних производителей, позволяющих создавать и поддерживать шифрованные логические диски. На таких дисках целесообразно хранить не только всю секретную информацию, но и другие программы шифрования (в т.ч. со всеми секретными ключами). Например, программа BestCrypt фирмы Jetico, программа TrueCrypt. Последняя из них является бесплатной программной с открытым кодом.

Экспериментальные оценки скорости доступа к информации на шифрованных логических дисках, созданных вышеуказанными программами, показали, что для современных ПК практически отсутствует задержки, т.е. скорость шифрования значительно больше скорости выполнения дисковых операций чтения/записи.