ЗАЩИТА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ШТАТНЫМИ СРЕДСТВАМИ ПАКЕТА MICROSOFT OFFICE

Студент гр. 113018 Попыванов С.Н.
Кандидат физ.-мат. наук, доцент Кривицкий П.Г.
Белорусский национальный технический университет
научный сотрудник Кузьмицкая С.М.
ГНУ «НИЭИ Минэкономики РБ»

Для многочисленных пользователей одного из самых популярных приложений для персональных компьютеров – Microsoft (MS) Office актуальным вопросом является выбор из имеющихся в нем алгоритмов шифрования документов для обеспечения конфиденциальности информации при передаче по открытым каналам связи.

Вместе с тем, представляет интерес надежность парольной защиты в смысле ее устойчивости к попыткам взлома. В известном программном пакете MS Office 2003 при записи файла на диск можно задать следующие алгоритмы шифрования: 1) без ключа: Слабое шифрование (XOR); Совместимое с Office 97/2000; 2) с длиной ключа от 40 до 56 бит: MS Base Cryptographic Provider; MS Base DSS and Diffie-Hellman Cryptographic Provider; 3) с длиной ключа до 128 бит: MS DH SChannel Cryptographic Provider; MS Enhanced Cryptographic Provider; MS Enhanced DSS and Diffie-Hellman Cryptographic Provider; MS Enhanced RSA and AES Cryptographic Provider; MS RSA SChannel Cryptographic Provider; MS Strong Cryptographic Provider.

Проведенный анализ и экспериментальная проверка стойкости шифрования показали, что парольная защита алгоритмами группы 1 не обеспечивает никакой защиты. Они классифицируются термином «запутывание» («obfuscation»), и любые пароли восстанавливались мгновенно. Алгоритмы группы 2 разработаны с учетом экспортных ограничений, которые предписывали не иметь в программах, использующихся за пределами США, криптоалгоритмы с ключом более 40 бит. Используя современные ПК и ПО, взлом зашифрованного 40-битовым ключом документа производится за время порядка 10 мин.

Таким образом, для обеспечения конфиденциальности информации в документах MS Office следует использовать шифрование группы 3 (например, алгоритм AES) с длиной ключа 128 бит. Данные алгоритмы были разработаны фирмой Microsoft в новой версии Office после отмены экспортных ограничений с на базе технологии CryptoAPI. В этом случае криптоатака фактически сводится к перебору паролей «в лоб».

При выборе версии пакета MS Office следует обязательно учитывать, что задача снижения скорости перебора паролей была решена путем многократного хэширования пароля только в алгоритмах шифрования, начиная с версии MS Office 2007 с пакетом обновления 2 (SP2).