Бартошевич Д.А.
БГЭУ, ВШУБ, группа 10 ВВБ-5, 3 курс

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ КОММЕРЧЕСКОЙ ИНФОРМАЦИИ

Быстрый темп развития информационных технологий сопровождается столько же быстрым темпом развития киберпреступности. По данным МВД РБ количество преступлений в сфере высоких технологий выросло с 4, зарегистрированных в 1998г., до 2514 — в 2010г. [1] Среди основных объектов компьютерных атак отмечают базы данных государственных и коммерческих предприятий. Конфиденциальная информация может быть раскрыта и непреднамеренно, например, в случае утраты/кражи ноутбука или внешнего винчестера с данными. Все это дает основания считать, что угроза несанкционированного доступа к информации является реальной, а вопрос защиты информации — актуальным.

Криптографические методы все шире используются как при обработке, так и при хранении информации. А при ее передаче по каналам связи большой протяженности криптографию признают одним из самых надежных способов защиты информации.

Наиболее перспективными системами криптографической защиты данных сегодня считаются асимметричные, а также гибридные криптосистемы. Суть асимметричного алгоритма шифрования состоит в наличии двух видов ключей: для зашифровывания и для расшифровывания. Ключ для зашифровывания (открытый) не является секретным и может свободно распространяться. Однако расшифровать сообщение с помощью открытого ключа невозможно. Для расшифровывания используется другой, секретный ключ. И только человек, у которого он есть, сможет расшифровать сообщение. Гибридный алгоритм использует комбинацию стандартного шифрования с помощью симметричных ключей и шифрования с открытым ключом для безопасного обмена ключами. Открытый ключ необходим для шифрования ключа сессии, используемого единожды.

В качестве практического примера реализации гибридного алгоритма шифрования можно привести консольное приложение GnuPG. [2,3] Часто другие программы применяют GnuPG как криптографическое ядро,

например почтовый плагин Enigmail (в почтовом клиенте Thunderbird). Благодаря GnuPG+Enigmail+Thunderbird сотрудник получает возможность автоматического и быстрого шифрования при отправке и получении электронной почты. Преимущества использования такой связки заключаются не только в том, что деловая переписка не будет доступна посторонним лицам (даже при взломе почтового аккаунта), но и в том, что переписка будет сопровождаться цифровыми подписями, что гарантирует подлинность документов и сообщений. [4] Есть реализация GnuPG для Outlook [5], а в некоторые почтовые клиенты GnuPG включен по умолчанию (Evolution, Kmail).

С помощью GnuPG можно шифровать не только коммуникацию, но и файлы на дисках компьютера. Причем выбор открытого ключа(-ей) определяет уровень доступа к документу, а именно: тех лиц, которые смогут прочесть документ.

В качестве резюме можно отметить, что в ситуациях, когда необходимо быть уверенным, что никто несанкционировано не сможет ни подсмотреть, ни изменить важную коммерческую информацию (напр., при передаче ее по Internet или при получении физического доступа к носителю информации), следует использовать криптографические методы защиты данных, в частности GnuPG.

Литература

1. Министерство внутренних дел Республики Беларусь: статистика [Электронный ресурс]. – Режим доступа: http://mvd.gov.by/ru/main.aspx?guid=3311. – Дата доступа: 14.04.2011.

2. GnuPG: материал из Википедии [Электронный ресурс]. Режим доступа: http://ru.wikipedia.org/wiki/GnuPG. – Дата доступа: 14.04.2011.

3. GnuPG [Электронный ресурс]. Режим доступа: http://www.pgpru.com/soft/gnupg. – Дата доступа: 14.04.2011.

4. Thunderbird, Enigmail, GnuPG. Шифруем почту на лету [Электронный ресурс]. Режим доступа: https://security.ngoinabox.org/ru/thunderbird_main. – Дата доступа: 14.04.2011

5. Gpg4win - a secure solution [Электронный ресурс]. Режим доступа: http://www.gpg4win.org/ . – Дата доступа: 14.04.2011

БДЭУ Беларускі дзяржаўны эканамічны ўніверсітэт. Бібліятэка.
БГЭУ Белорусский государственный экономический университет. Библиотека.
BSEU Belarus State Economic University. Library.
http://www.bseu.by elib@bseu.by