А. Н. Мазурок
(*БелГУТ, Гомель*)

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТАМОЖЕННОЙ ДЕЯТЕЛЬНОСТИ ПОСРЕДСТВОМ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ

Таможенные органы являются одной из государственных структур. От их эффективности деятельности в информационной сфере

существенно зависит эффективность обеспечения экономической безопасности Республики Беларусь.

В настоящее время криптоатаки стали серьезной проблемой, потому что они становятся все технологичнее. Для противостояния атакам и угрозам атак применяются процедуры шифрования и расшифрования, совокупность которых представляет собой криптосистему.

Различают два основных типа криптосистем: симметричные (с секретным ключом) и асимметричные (с открытым ключом) [1].

При использовании симметричных криптосистем используются открытый алгоритм шифрования и секретный ключ, причем один и тот же для шифрования и расшифрования. Это порождает необходимость наличия надежного канала, по которому ключ должен попасть к получателю зашифрованного текста. Так как алгоритм шифрования не содержится в секрете, то стойкость шифра определяется только секретностью ключа.

В ассиметричной криптосистеме у каждого пользователя есть своя пара ключей – открытый и личный. Открытый ключ используется адресантом для шифрования сообщения, которое сможет прочитать только тот пользователь, у которого есть второй ключ из пары. Это избавляет от необходимости создания секретного канала для передачи ключей и самих зашифрованных сообщений.

Таким образом, средствами криптографической защиты информации решается множество задач, непосредственно связанных с обеспечением информационной безопасности любой системы, базы данных или сети передачи информации.

Литература

1 Основы криптографии : учебное пособие для высших учебных заведений по группе специальностей в области информационной безопасности / А. П. Алферов [и др.]. – М. : Гелиос АРВ, 2005. – 479 с.