В. Ф. Иконников, *д-р техн. наук, профессор*
А. А. Гордич, *канд. техн. наук, доцент*
БГЭУ (Минск)

ОСВОЕНИЕ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ В УЧЕБНОМ ПРОЦЕССЕ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ЭКОНОМИЧЕСКОГО ПРОФИЛЯ

Необходимость успешного освоения методов криптографического преобразования информации в учебном процессе подготовки специалистов экономического профиля обусловлена несколькими причинами. Первая причина связана с вопросами сохранения коммерческой тайны в процессе производственно-хозяйственной деятельности. Во многих случаях деловую переписку осуществляют с помощью электронной почты по открытым каналам связи. При этом конфиденциальная информация может быть доступна конкурентам. В итоге предприятие или предприниматель могут понести большие убытки. Вторая причина обусловлена тем, что в настоящее время на практике широко применяется электронная цифровая подпись (далее — ЭЦП), которая является реквизитом электронного документа. В соответствии с Законом Республики Беларусь «Об электронном документе и электронной цифровой подписи» электронный документ имеет точно такую же юридическую силу, как и документ на бумажном носителе с печатью. Специалист с высшим образованием должен знать, как создается ЭЦП. И, наконец, третья причина связана с тем, что выпускник вуза должен знать, что ЭЦП применяется для проверки целостности и подлинности электронного документа. Студент экономического профиля должен на занятиях получить первичные навыки создания и применения ЭЦП.

Задачи криптографического преобразования информации, создания и применения ЭЦП решаются с помощью симметричных и асимметричных алгоритмов. К числу симметричных алгоритмов относятся DES, AES, IDEA, FEAL, BESTA. Для формирования ЭЦП можно использовать односторонние функции шифрования, называемые также хэш-функциями. В обоих случаях для формирования и проверки ЭЦП надо иметь секретный ключ. Надежная передача секретного ключа достигается только в процессе физического общения пользователей, что часто невозможно или нецелесообразно.

На практике в основном используются асимметричные алгоритмы с закрытыми и открытыми ключами. При этом ключи применяются парами. С помощью только одного ключа (открытого или закрытого) зашифровать и расшифровать нельзя. Наиболее известными асимметричными алгоритмами являются RSA, Elgamal, Diffie-Hellman и DSA. В алгоритме RSA ключи (открытый или закрытый) можно использовать как для шифрования, так и для расшифровывания. Шифрование с помощью закрытого ключа отправителя позволяет сфор-

мировать ЭЦП. Зашифрованное сообщение формируется с помощью открытого ключа абонента, которому передается сообщение. Абонент расшифровывает сообщение с помощью своего закрытого ключа.

Асимметричные алгоритмы реализуются с помощью тех или иных программных средств. Приобретение вузом программ, применяемых на практике (например, в Министерстве по налогам и сборам) и реализующих процедуры шифрования, создания и применения ЭЦП, является весьма проблематичным.

Таким образом, для учебных целей надо использовать те программы, которые имеются в свободном доступе. К числу таких программ относятся, например, TechGuard Crypto, Antar Crypto Deluxe Edition, PGP, SafeKuvert, IMCrypto Free. При выборе одной из них надо учитывать следующие характеристики: возможность реализации известных алгоритмов шифрования, размер ключа, возможность создания и проверки ЭЦП. Наиболее подходящей для использования в учебном процессе будет программа PGP, которая позволяет освоить методику симметричного и асимметричного шифрования. Эта программа позволяет не только создавать ЭЦП, но и проверять подлинность и достоверность электронного документа. Кроме того, с ее помощью можно создавать зашифрованные сообщения электронной почты.

***А. В. Марков**, канд. физ.-мат. наук, доцент*
БГЭУ (Минск)
***В. И. Яшкин**, канд. физ.-мат. наук, доцент*
БГУ (Минск)

ПРИМЕР МАТРИЧНОЙ МОДЕЛИ В МЕЖДУНАРОДНОМ ТУРИЗМЕ

Деятельность реальных экономических объектов связана с исследованием и решением ряда сложных задач математического моделирования. Приведем учебную модель, которая изучается будущими менеджерами в сфере международного туризма на лекционных и практических занятиях в разделе «Линейная алгебра» (аналогичные задачи см., например, [1, с. 51–54]).

Постановка задачи. Пусть имеется n стран с общими объемами продаж услуг в сфере туризма x_1, x_2, ..., x_n. Весь объем продаж в каждой стране складывается из продажи туристических услуг внутри страны (внутренний туризм) и продажи туристических продуктов других стран (гостеприимство и гостиничное дело). Пусть $x_{ij}(i, j = 1, 2, ..., n)$ — часть объема продаж туристических услуг j-й страны, которая приходится на покупку туристических услуг в i-й стране. Требуется найти вектор объемов продаж туристических услуг при условии бездефицитной торговли между странами.