УДК 004.056.5

Криптографические методы обеспечения информационной безопасности

Ковалькова И. А.
Белорусский национальный технический университет

Широкое применение компьютерных технологий и постоянное увеличение объёма информационных потоков вызывает постоянный рост интереса к криптографии. *Криптография* – это наука, которая изучает и описывает модель информационной безопасности данных. Криптографические методы защиты информации – это специальные методы шифрования, кодирования или иного преобразования информации, в результате которого её содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования. Криптографический метод защиты реализуется в виде программ или пакетов программ.

Современная криптография включает в себя четыре крупных раздела:

1. *Симметричные криптосистемы*. В симметричных криптосистемах для шифрования и для дешифрования используется один и тот же ключ (шифрование – преобразование исходного или открытого текста в шифрованный текст, а дешифрование – обратный шифрованию процесс, когда на основе ключа шифрованный текст преобразуется в исходный; ключ – информация, необходимая для беспрепятственного шифрования и дешифрования текстов); 2. *Криптосистемы с открытым ключом*. В системах с открытым ключом используются два ключа – открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения; 3. *Электронная подпись*. Системой электронной подписи называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения; 4. *Управление ключами*. Это процесс системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

Основные направления использования криптографических методов передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.