УДК 004.42

Н. П. Цыганенко, студ.; Н. А. Жиляк, доц., канд. техн. наук
(БГТУ, г. Минск)

ШИФРОВАНИЕ XML ДОКУМЕНТА СРЕДСТВАМИ .NET

В наши дни XML формат является передовым способом хранения и передачи данных в сети Интернет. На данном формате основывается работа RSS, SOAP, FB2 и прочего. Поэтому вопрос шифрования XML документа является актуальным.

В консорциуме W3C была создана рабочая группа, которая специально занималась вопросами шифрования XML данных. В 2001 г. выпущена первая спецификация – XML Encryption Syntax and Processing. Последние изменения сделаны 24 января 2013 г. Спецификация носит рекомендационный характер. Компания Microsoft создала пространство имён (System.Security.Cryptography.Xml) в рамках .NetFramework. Оно реализует спецификацию W3C, но не обеспечивает высокоуровневую поддержку работы с XML документами.

Для осуществления шифрования и дешифрования средствами System.Security.Cryptography.Xml платформы .Net требуется наличие сертификата соответствующего стандарту X.509. Это стандарт определяет форматы данных и процедуры распределения открытых ключей с помощью сертификатов с цифровыми подписями, которые предоставляются сертификационными органами. Процесс шифрования запутан, децентрализован и не стандартизирован. К тому же реализация алгоритмов шифрования и дешифрования является закрытой, что не даёт 100% гарантии надёжности их использования.

В связи с вышесказанным предлагается разработка пространства имён на языке C#, обеспечивающего высокоуровневое шифрование и дешифрование XML документа. Для обеспечения большей эффективности данных процессов требуется проанализировать стандарт W3C на наличие избыточности. Весь разработанный код предполагается сделать общедоступным, для возможности последующей кроссплатформенной реализации.

ЛИТЕРАТУРА

1 Кобайло А.С. Введение в XML: учеб.-метод. пособие для студентов специальности «Информационные системы и технологии» (издательско-полиграфический комплекс) / А.С. Кобайло, Н.А. Жиляк. – Минск: БГТУ, 2011. – С. 320.