**Некоторые особенности реализации алгоритма защиты программного обеспечения от нелегального использования**

**(На примере программы “генератор тестов 2.0”)**

Асп. Волошин С. Б.[[1]](#footnote-1)

Кафедра теории и автоматизации металлургических процессов и печей.

Северо-Кавказский горно-металлургический институт (государственный технологический университет)

Рассмотрены некоторые особенности реализации алгоритма защиты программного обеспечения от нелегального использования. Приведена принципиальная схема алгоритма и часть исходных кодов на языке программирования Microsoft Visual Basic 2005.

При проектировании современного программного продукта разработчики все чаще уделяют внимание той части программы, которая отвечает за защиту от нелегального использования.

Применение для написания программного продукта платформы Microsoft .NET Framework [1] позволяет достаточно просто реализовать в программе различные криптографические алгоритмы: как симметричные (DES, Triple-DES, RC2, Rijndael) и ассиметричные (DSA/DSS, RSA) алгоритмы шифрования, так и алгоритмы хеширования (HMACSHA-1, MACTripleDES, MD5, SHA-1, SHA-256, SHA-384, SHA-512) [2, 3].

В .NET Framework за криптографию отвечает пространство имен

System.Security.Cryptography

В это пространство входят три класса высокого уровня:

System.Security.Cryptography.SymmetricAlgorithm

System.Security.Cryptography.AsymmetricAlgorithm

System.Security.Cryptography.HashAlgorithm

Наиболее перспективной для организации защиты представляется комбинация асимметричного алгоритма RSA, разработанного Р. Ривестом, А. Шамиром и Л. Адлеманом, и алгоритма дайджеста сообщения MD5 [3].

Реализация алгоритма RSA и алгоритма MD5 на языке высокого уровня Microsoft Visual Basic 2005 выглядит следующим образом:

'подключаем пространство имен

Imports System.Security.Cryptography

Imports System.Text

Imports System.Xml

Public Class myCrypt

'I. Генерируем ключи RSA.

Dim rsaProvider0 As New RSACryptoServiceProvider()

Dim EK As String = rsaProvider0.ToXmlString(False)

Dim DK As String = rsaProvider0.ToXmlString(True)

'II. Создаем и настраиваем экземпляр класса

'RSACryptoServiceProvider перед шифрованием.

Dim cspParam As New CspParameters()

3 Труды молодых ученых № 4, 2007

cspParam.KeyContainerName = "SecretKey"

Dim rsaProvider1 As New RSACryptoServiceProvider(cspParam)

'III. Шифруем данные.

rsaProvider1.FromXmlString(EK)

Dim cipheredText As Byte() = rsaProvider1.Encrypt \_

(UTF8Encoding.UTF8.GetBytes("Данные пользователя"), True)

Dim EncodingText As String = Convert.ToBase64String(cipheredText)

'IV. Дешифруем данные.

Dim rsaProvider2 As New RSACryptoServiceProvider()

rsaProvider2.FromXmlString(DK)

Dim DecodingText As String = UTF8Encoding.UTF8.GetString \_ (rsaProvider2.Decrypt(Convert.FromBase64String(EncodingText), True))

'V. Получаем хеш-функцию расшифровывающего ключа.

Dim md5Provider As New MD5CryptoServiceProvider

Dim MD5Hash As String = Convert.ToBase64String \_

(md5Provider.ComputeHash(UTF8Encoding.UTF8.GetBytes(DK)))

End Class.

Используя асимметричный алгоритм RSA и алгоритм вычисления хеш-функции MD5, автор статьи разработал принципиальную схему алгоритма защиты программного обеспечения от нелегального использования. Данная схема была успешно применена при разработке программного комплекса “Генератор тестов 2.0”.

Каждый легальный дистрибутив программы “Генератор тестов 2.0” снабжается ключевым файлом. Ключевой файл подтверждает легальность установленного программного продукта и может служить для идентификации пользователя, ограничения времени работы программного продукта и т.д.

Ключевой файл состоит из трех блоков данных: информации о пользователе в открытом виде, информации о пользователе в зашифрованном виде и расшифровывающего ключа ассиметричного алгоритма шифрования RSA.

Принципиальная схема работы алгоритма защиты показана на рисунке.

Информация о пользователе

Зашифровывающий ключ

Ключевой файл

Расшифровывающий ключ

Алгоритм шифрования RSA

Алгоритм хеширования MD5

Защищаемый бинарный файл

Алгоритм хеширования MD5

**1**

**2**

**3**

**4**

**5**

**6**

**8**

**7**

**9**

Принципиальная схема работы алгоритма защиты.

Порядок работы алгоритма:

В процессе создания программного обеспечения:

Информация о пользователе в открытом виде записывается в ключевой файл (она служит для быстрого получения сведений о пользователе).

Информация о пользователе передается асимметричному алгоритму шифрования.

Зашифровывающий ключ передается алгоритму шифрования.

Зашифрованная с помощью зашифровывающего ключа информация о пользователе добавляется в ключевой файл.

Расшифровывающий ключ асимметричного алгоритма шифрования добавляется в ключевой файл.

Расшифровывающий ключ асимметричного алгоритма шифрования передается в алгоритм хеширования.

Хеш-функция расшифровывающего ключа помещается перед компиляцией в защищаемый бинарный файл (\*.exe, \*.dll и т.д.).

В процессе эксплуатации программного обеспечения:

Расшифровывающий ключ асимметричного алгоритма шифрования, записанный в ключевой файл, передается в алгоритм хеширования.

Значение хеш-функции расшифровывающего ключа из ключевого файла сравнивается со значением хеш-функции расшифровывающего ключа помещенной в защищаемый файл. В случае равенства значений двух хеш-функций зашифрованные данные пользователя, записанные в ключевом файле считаются достоверными. В случае несовпадения, данные из ключевого файла считаются недостоверными, сам ключевой файл блокируется, а защищаемый файл отказывается работать с ключевым файлом.

Выводы

Разработана принципиальная схема алгоритма защиты программного обеспечения от нелегального использования.

Реализован алгоритм защиты на языке высокого уровня Microsoft Visual Basic 2005. Данный алгоритм вошел в программный продукт “Генератор тестов 2.0”, разработанный в 2007 г. для Министерства образования и науки Республики Северная Осетия-Алания.

**Список литературы**

Кларк Д. Объектно-ориентированное программирование в Visual Basic .NET. СПб.: Питер, 2003.

Блэк У. Интернет: протоколы безопасности. СПб.: Питер, 2001.

Кровчек Э., Кумар В. и др. .NET. Сетевое программирование для профессионалов. М.: Лори, 2005.

1. Научный руководитель к.т.н., доц. Мамонтов Д. В. [↑](#footnote-ref-1)