УДК 681.325.3

В.А. Пласковицкий

ЗАЩИТА ПРОГРАММНОГО КОДА С ПОМОЩЬЮ МЕТОДОВ ОБФУСКАЦИИ

Белорусский государственный технологический университет, Минск

Спецификой программных продуктов является сравнительно легкое создание аналогов на основе распространяемых программ, взлом, а также практически нулевая стоимость копирования. Это происходит из-за свободного доступа к программному коду и ведет к угрозе безопасности и нарушению авторских прав.

На сегодняшний день можно следующие наиболее активно развивающиеся подхода к защите программного кода:

– разработка безопасной архитектуры операционной системы, которая не позволит пользователю получать доступ к программному коду.

– использования технологий криптографии «на лету» (fly-description), при которой программа хранится в зашифрованном виде, а дешифрование производится только для выполняемых в текущий момент участков программы, с последующим обратным шифрованием [1].

– выполнение программ на удаленном сервере, когда пользователь получает только приложение-интерфейс, для взаимодействие с программой.

– обфускация – изменение кода таким образом, чтобы затруднить возможность его анализа, сохранив логику его работы.

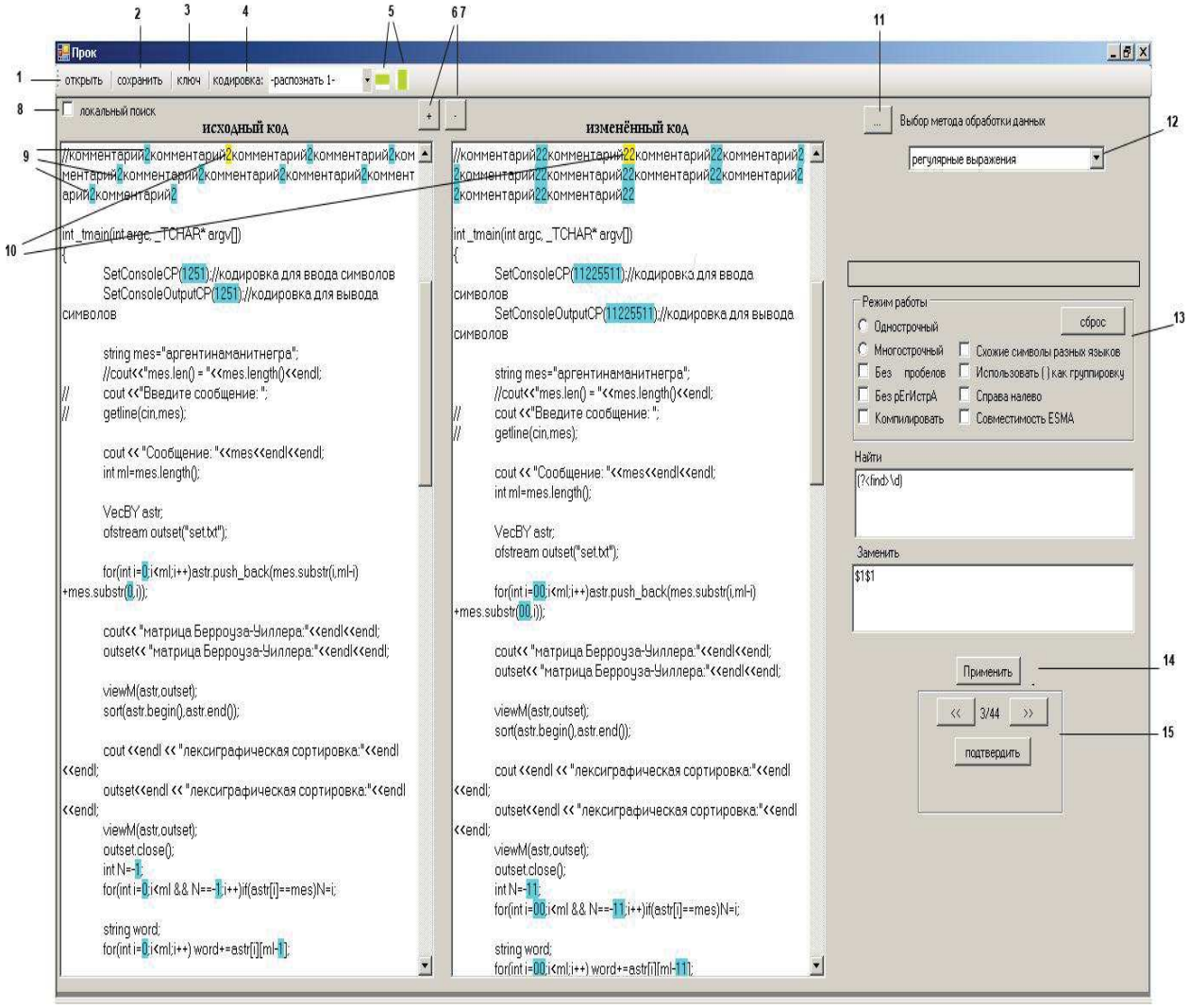
У каждого из этих подходов есть свои преимущества и недостатки. Так, перевод всех компьютеров на безопасную архитектуру вряд ли осуществим по экономическим причинам. Шифрование на лету становится бесполезным, при перехвати дешифрованных частей, или наличии ключа шифрования. Для выполнения программ на удаленном сервере нужны гораздо большие вычислительные мощности ЭВМ, чем существуют на сегодняшний день, а так же каналы связи между компьютерами. При использовании обфускации сохраняется логика программного кода, благодаря чем в нем всегда можно разобраться, вопрос только сколько на это уйдет времени.

Наибольшее внимание в последнее время уделяется методам обфускации. Их неоспоримыми преимуществами являются: техническая и экономическая возможность их реализации, а также возможность их применения практически для любого программного продукта вне зависимости от среды выполнения, что особенно актуально для интернет-приложений [2].

На момент написания данной статьи не было известно о каких-либо отечественных продуктов производящих обфускацию, в то время как за рубежом происходит довольно бурная разработка обфускаторов, стоимость отдельных из которых доходят до 6000-8000$ [3].

Целью работы стала разработка авторской защитной системы «Прок», производящей защиту программного кода с помощью методов обфускации [4]. Во время разработки данной системы ее возможности были значительно

расширены, благодаря чему в нее можно включать так же методы криптографии, а также использовать с целью поиска и изменения структурированных частей каких-либо данных (рисунок 1).



1 – выбор данных для изменения; 2 – сохранения результатов; 3 – применение ключа для восстановления результатов; 4 – настройка параметров кодировки; 5 – настройка позиции блоков приложения; 6, 7 – изменение размера шрифта; 8 – включение локального режима обработки; 9 – найденные участки текста, над которыми производится операция изменения; 10 – текущий изучаемый участок; 11 – выбор набора модулях; 12 – навигация по методам выбранного списка; 13 – интерфейс для работы с выбранным методом обработки данных; 14 – применение произведенных настроек; 15 – навигация по найденным для изменения участкам данных с подсветкой текущего участка.

Рисунок 1 - Интерфейс приложения Прок

Достигается это за счет реализации модульной технологии защиты, при которой сама программа является лишь интерфейсом, а само изменение данных происходит в отдельных модулях, подключаемых к ней определенным образом.

Помимо удобной навигации по используемым модулям, а так же интерфейса для обмена между ними данными в защитную систему входит несколько внутренних модулей для изменения данных с помощью регулярных выражений (рисунок 2) и методов вставок/замен (рисунок 3).

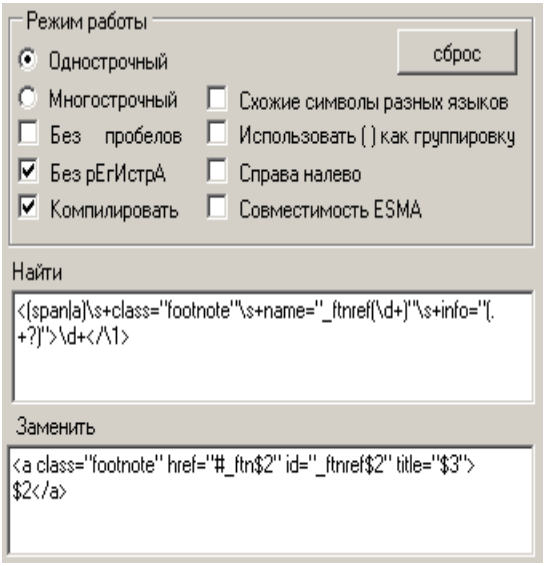


Рисунок 2 – Интерфейс для использования регулярных выражений

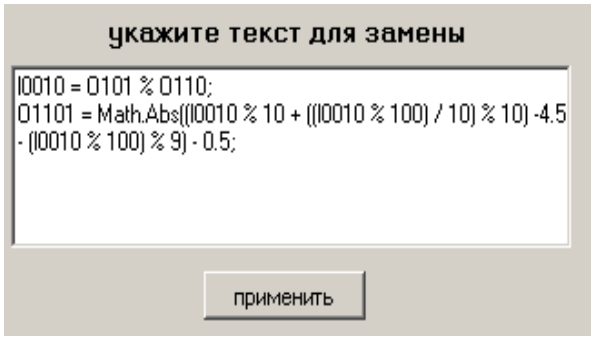


Рисунок 3 – Интерфейс для использования методов вставок/замен

Так же можно обрабатывать только отдельные участки данных, включив локальный режим работы и выбрав необходимый участок текста с помощью простого выделения (рисунок 4).

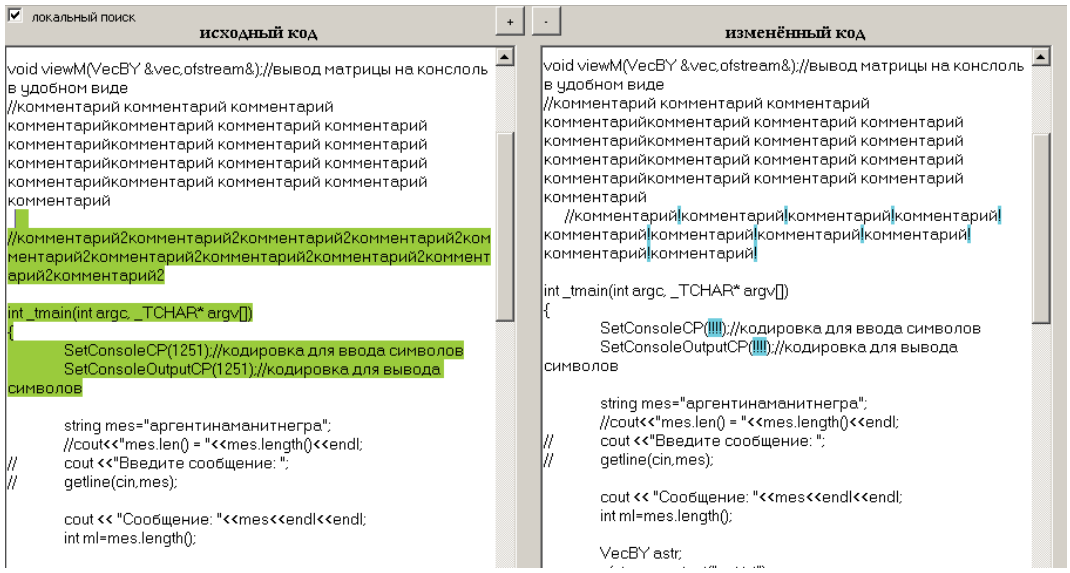


Рисунок 4 – Интерфейс для использования локального режима обработки данных

Еще одной особенностью разработанного приложения является возможность ведения журнала производимых изменений, для последующего восстановления первоначального вида данных. Для этого была разработана специальная XML-структура, в формате которой и происходит сохранение информации о производимых изменениях.

Кроме защитных методов в программе реализован генератор случайных чисел, с помощью которого можно автоматизировать составление ключей для отдельных защитных методов.

Генерирование случайных значений происходит за счет использования специального класса *RNGCryptoServiceProvider* входящего в состав библиотеки System.Security.Cryptography Framework.

Выводы: результаты работы внедрены в НИР ГБ 11-165 и учебный процесс при выполнении лабораторных работ студентами 4-го и 5-го курсов специальности «Информационные системы и технологии» в компьютерном классе 301-1 УО «Белорусский государственный технологический университет».

Литературные источники

1. Ярмолик В.М. Криптография, стеганография и охрана авторского права. Монография / В.Н. Ярмолик, С.С. Портянко, С.В. Ярмолик. – Минск, 2007. – 240с.

2. Пласковицкий В.А. Особенности реализации методов обфускации в интернет-приложениях / П.П. Урбанович; БГТУ, кафедра информационных систем и технологий // 62-ая научно-техническая конференция студентов и магистрантов: сборник научных работ. – Минск, 2010. – С. 156-168

3. Интернет-портал [Электронный ресурс] / Традиционные симметричные криптосистемы. – Режим доступа: http://store.vmware.com/store?Action=DisplayPage&Env=BASE&Locale=en_US&SiteID=vmware&id=ProductDetailsPage&productID=105855000&resid=TpKtiQoHAtYAABlIhF8AAAAj&rests=1318235529278. – Дата доступа: 10.10.2011.

4. Пласковицкий В.А., Урбанович П.П. Защита программного обеспечения от несанкционированного использования и модификации методами обфускации / Пласковицкий В.А., Урбанович П.П. // Труды БГТУ. Сер. VI. Физ.-мат. наук и информ. – 2011. вып. 19. – С. 173-176.

V.A. Plaskovitsky

PROTECTION OF SOFTWARE CODE THE METHOD OF OBFUSCATION

Belarusian State University of Technology, Minsk

Summary

Article on research and implementation methods of obfuscation for software protection code against unauthorized use. Were analyzed sovermennye trends in this area, identified their strengths and weaknesses. As a result of the program was created to implement these methods of obfuscation at the source and intermediate code. Describes its interface and functionality. The analysis of the possible areas of application.