УДК 004.056 (043.2)

В.В. Давыдов[1], А.В. Мовчан[1], И.И. Сидоренко[2]

[1] *Национальный технический университет «ХПИ», Харьков*
[2] *Национальная академия Национальной гвардии Украины, Харьков*

РАЗРАБОТКА СИСТЕМЫ ФОРМИРОВАНИЯ ЦИФРОВОГО ИДЕНТИФИКАТОРА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ЗАЩИТЫ АВТОРСКИХ ПРАВ

Отличительной особенностью разработанной структуры процесса формирования цифрового идентификатора является использование формальных данных о компьютерных системах, на которые устанавливается лицензионное программное обеспечение (ПО) в процессе формирования лицензионного цифрового идентификатора. Также авторами предложен алгоритм функционирования системы и генерации лицензионного ключа, адаптированный к входным данным и возможным условиям верификации ПО.

Ключевые слова: *авторское право, лицензионный ключ, цифровой идентификатор.*

Введение

Постановка задачи. В соответствии со статьями 433 Гражданского кодекса Украины и 18 Закона Украины "Об авторском праве и смежных правах" [2] – компьютерные программы (программное обеспечение) охраняются как литературные произведения. Такая охрана распространяется на компьютерные программы независимо от способа или формы их выражения. Основанием для отнесения программного обеспечения (ПО) к литературным произведениям служит некая общность отображения строк литературного произведения и компьютерной программы: и строки литературного произведения, и строки компьютерной программы автор наполняет символами-литерами или символами-операторами. Тождественность творческого процесса относительно создания форм авторских произведений литературы и компьютерных программ и стала определяющей для выбора формы защиты ПО [1].

Охраняется ПО как объект авторского права, т.е. без выполнения каких-то особенных формальностей относительно него и независимо от его завершенности, назначения, ценности и т.п., а также способа или формы их выражения.

Существуют определенные сложности охраны ПО. Первая сложность заложена уже в самом объекте: это и литературное произведение, и одновременно – набор инструкций. Т.е. это и некий набор символов (рассказ – тоже литературное произведение) и набор инструкций для неких действий (а это уже скорее алгоритм или способ действий).

Вторая сложность регистрации авторского права на ПО заложена также и в самом объеме программного кода, представляемого на регистрацию. Особенно учитывая то, что он представляется на регистрацию в печатном виде. Кроме того, к материалам заявки на регистрацию авторского права на компьютерную программу, кроме обычных документов, прилагается и наставление по использованию программы [1, 5].

Третья сложность заложена в том, что сама регистрация авторского права – это депонирование программы, т.е. попросту говоря – это сохранение компьютерной программы с четким определением срока ее сдачи на хранение и содержания сданного продукта. Авторское право на ПО не распространяется на заложенные в нем: идеи; процессы; методы деятельности или математические концепции как таковые, на которых основана компьютерная программа (в т.ч. и на сопряжение, то есть на ту часть программы, которая обеспечивает диалог с пользователем и совместимость ее с элементами аппаратуры); логику работы программы; алгоритмы работы программы; языки программирования. Таким образом, авторским правом защищается текст (код) программы, а не функции, которые она выполняет.

Анализ литературы [3, 4, 6] показал, что одним из механизмов защиты авторских прав на ПО является распространение лицензионного соглашения на использование программ. Обеспечение соответствия использования программных продуктов требованиям лицензионных соглашений является проблемой, с которой не так-то просто справиться. При этом существует множество различных рекомендаций технического, социального, психологического и других направлений по эффективному использованию указанного механизма защиты. Это и независимый аудит ПО, использование четко сформулированной политики с налаженной системой оповещения, а также инструментов для резервного копирования, и конечно автоматизация процесса с использованием инструментов активного обнаружения, которые бы находили как разрешенные, так и неразрешенные установленные программы.

В то же время в последнее время в научной литературе [3, 4] все больше внимания уделяется защите ПО с помощью внедренных цифровых водя-

ных знаков, цифровой подписи и других меток, подтверждающих авторство, и упрощающих процесс автоматической идентификации и верификации ПО.

Проведенные исследования показали, что одним из основных недостатков, разрабатываемых в настоящее время технических систем идентификации и лицензирования ПО является пренебрежение формальными данными о компьютерных системах, на которые лицензионной ПО устанавливается. Устранению данного недостатка посвящена статья.

Основная часть

На рис. 1 представлена структурная схема процесса формирования цифрового идентификатора ПО.

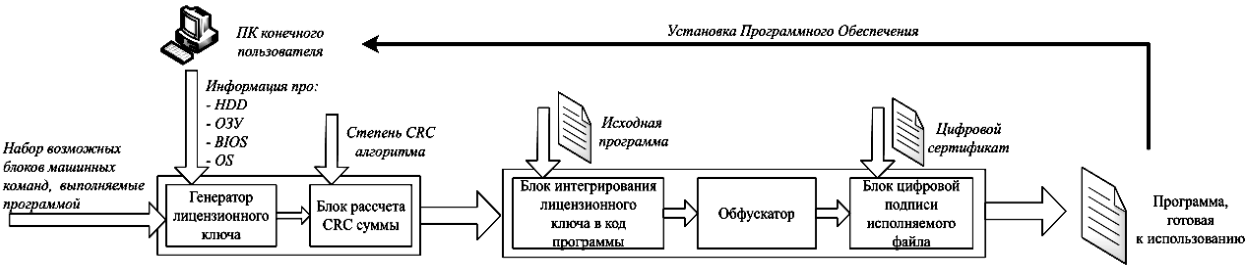

Рис. 1. Структурная схема процесса формирования цифрового идентификатора ПО

Как видно из рисунка основными составляющими разрабатываемой системы являются: генератор лицензионного ключа; блок расчета CRC суммы; блок интегрирования лицензионного ключа в код программы, обфускатор; блок формирования цифровой подписи исполняемого файла.

В соответствии с предполагаемыми процедурами формирования лицензионного цифрового идентификатора необходимо выполнить такие шаги:

1. *Формирование шаблона программного кода, на основе которого генерируется лицензионный ключ*: запись в глобальную переменную MODE значения необходимого режима работы приложения, от которого зависит функционал (FULL – весь функционал доступен; DEMO – доступен только «базовый» функционал); сравнение типа продукта, версии, сопоставимости текущего программного продукта с установленным типом операционной системы. В случае расхождения программы – вывод соответствующего сообщения пользователю, и завершение программы.

2. *Получение информации о компонентах системы конечного пользователя*. Данная функция выполняется путем создания программы-утилиты, которая запускается на системе конечного пользователя и отправляет по защищенному каналу необходимую информацию во избежание перехвата трафика и его анализа/изменения на сервер. Полученная информация будет храниться для дальнейших действий. Программа-утилита находится на защищенном носителе, доступ к которому есть только у авторизованного сотрудника (данный вариант не исключает вероятность проникновения злоумышленников, но в контексте предлагаемой реализации, действия данного фактора игнорируется). Информация, поступающая на сервер о компонентах системы конечного пользователя, имеет такую структуру: **накопители,** например: «WDC WD5000AAKX-001CA0; PCI\VEN_8086; DEV_1C02; SUBSYS_844D1043; REV_05\3»; **процессоры**, например: «Intel(R) Pentium(R) CPU G620 @ 2.60GHz; ACPI_HAL\PNP0C08\0»; **ОС**, например: «6.3.9600 N/A Build 9600; 00261-80443-28329-AA407»; **BIOS**, например: «American Megatrends Inc. 0409, 8/26/2011».

3. *Формирование результирующего лицензионного ключа*. Для выполнения данной функции в качестве входных данных используются: информация о системе конечного пользователя; шаблон программного кода, который будет выполняться; размер CRC суммы для валидации лицензионного ключа.

Представим обобщенный алгоритм процесса формирования цифрового идентификатора ПО:

1. Формирование программного кода (на ассемблере), который будет выполняться на системе конечного пользователя с учетом полученной информации и предоставленного шаблона

2. Полученный код трансформируется в соответствующие машинные коды.

3. Для каждого байта полученного машинного коды выполняются следующие действия:

- поиск данного байта в текстовом представлении полученной информации;
- поиск данного байта в бинарном представлении полученной информации;
- если найден соответствующий код в текстовом представлении, то в конец формирующегося лицензионного ключа дописывается 2 байта: «0» и «код устройства», если в бинарном представлении – то 2 байта: «1» и «код устройства», затем 2 байта, отражающие позицию найденного символа. В случае, если код не был найден – 2 байта «00», а затем 2 байта, отражающие hex представление указанного байта (напр., символ «A» имеет код «65», что в hex представлении – 41 – будет записано два байта «4» и «1»).

В конец полученного лицензионного ключа добавляется 2 байта, характеризующие степень CRC суммы, например «32». Далее идет CRC сумма в текстовом hex представлении (для CRC32 количество – 8 символов). В процессе формирования цифрового идентификатора ПО можно использовать следующие

коды устройств: 1 – накопители; 2 – процессоры; 3 – ОС; 4 – BIOS. В этом случае на выходе получаем сгенерированный лицензионный ключ, который будет встраиваться в программный продукт. Исходный программный продукт проходит 3 фазы перед поступлением к конечному пользователю:

1. Полученный лицензионный ключ встраивается в сегмент данных программы. При этом сегмент данных должен быть сформирован таким образом, чтобы лицензионный ключ поместился в выделенном для этого блоке.

2. Обфускация, для уменьшения вероятности взлома алгоритма обработки лицензионного ключа.

3. Подпись программного продукта сертификатом, для избежания возможности редактирования файла с целью обойти алгоритм верификации.

Далее полученный программный комплекс поставляется конечному пользователю. При каждом запуске, программа выполняет следующие действия:

1. Получает информацию о компонентах текущей системы.

2. Верификация лицензионного ключа на основе CRC суммы.

3. Формирования машинных кодов для выполнения на основе текущего лицензионного ключа и параметрах системы.

4. Выполнение сформированных машинных команд. В случае если лицензионный ключ оказался невалидным или программа была запущенна на другом компьютере, то текущий программный продукт аварийно завершит работу.

Структура исполняемого exe-файла представлена на рис. 2.

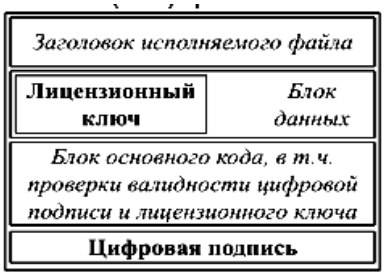

Рис. 2. Структура исполняемого exe-файла

Выводы

В статье предложен механизм и разработана обобщенная структура процесса формирования цифрового идентификатора ПО. Отличительной особенностью предложенной структуры является использование формальных данными о компьютерных системах, на которые лицензионной ПО устанавливается в процессе формирования лицензионного цифрового идентификатора. Предложен алгоритм функционирования системы и генерации лицензионного ключа, адаптированный к входным данным и возможным условиям верификации ПО.

Дальнейшей целью исследования является разработка имитационной модели и проведение практического эксперимента.

Список литературы

1. Авторское право на компьютерную программу [Электронный ресурс]. – Режим доступа к ресурсу: http://copyright.ua/komp.php.

2. Законодавство України про інтелектуальну власність. Темат. збірка: у 3-х т. Т. 1: Законодавчі акти України про інтелектуальну власність. – К.: Ін-т. інтел. власн. і права, – 2005. – 168 с.

3. Семенов С.Г. Исследование методов идентификации програмного обеспечения и их характеристик / С.Г. Семенов // Системи обробки інформації. – Х.: ХУ ПС, 2015. – Вип. 12 (137). – С. 148-150.

4. Семенов С.Г. Исследования технологий динамического анализа бинарного кода программного обеспечения / С.Г.Семенов, С.Ю. Гавриленко, А.В. Мовчан // НПК «Комп'ютерні системи і проект. технол. процесів та обладнання». – Чернівці: ЧФ НТУ «ХПІ», 2016. – С.152.

5. Соблюдение лицензионного соглашения программного обеспечения / [Электронный ресурс]. – Режим доступа: http://www.pcwork.ru/soblyudenie_litsenzionnogo_soglasheniya_programmnogo_obespecheniya_chast_2_.htm

6. Цифровые подписи в исполняемых файлах и обход этой защиты во вредоносных программах / [Электронный ресурс]. – Режим доступа к ресурсу: https://habrahabr.ru/post/112289/

Поступила в редколлегию 23.02.2016

Рецензент: д-р техн. наук, ст. научн. сотр. С.Г. Семенов, Национальный технический университет «ХПИ», Харьков.

РОЗРОБКА СИСТЕМИ ФОРМУВАННЯ ЦИФРОВОГО ІДЕНТИФІКАТОРА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАХИСТУ АВТОРСЬКИХ ПРАВ

В.В. Давидов, О.В. Мовчан, І.І. Сидоренко

Відмінною особливістю розробленої структури процесу формування цифрового ідентифікатора є використання формальних даних про комп'ютерних системах, на які встановлюється ліцензійне програмне забезпечення (ПЗ) в процесі формування ліцензійного цифрового ідентифікатора. Також авторами запропонований алгоритм функціонування системи і генерації ліцензійного ключа, адаптований до вхідних даних і можливих умов верифікації ПЗ.

Ключові слова: *авторське право, ліцензійний ключ, цифровий ідентифікатор.*

DEVELOPMENT OF FORMATION DIGITAL ID SOFTWARE FOR COPYRIGHT PROTECTION

V.V. Davydov, A.V. Movchan, I.I. Sidorenko

A distinctive feature of the developed structure of the formation of a digital ID is to use formal data on computer systems that are installed licensed software (software) in the process of licensing the digital ID. Also, the authors propose an algorithm of the system and generate a license key is adapted to the input data and verification of the conditions of possible software.

Keywords: *copyright, license key, numeric identifier.*