АЛГОРИТМ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПОЛЬЗОВАТЕЛЯ ПРИВЯЗКОЙ К РЕСУРСАМ ПК

И. А. Шалатонин, П. П. Коваленко

Белорусский государственный университет
Минск, Беларусь
E-mail:Shalat@bsu.by

Рассматриваются вопросы защиты ПО пользователя при его тиражировании. Предложен устойчивый ко взлому алгоритм защиты пользовательских приложений путем привязки к характеристикам ПК.

Ключевые слова: защита программного обеспечения, API, криптозащита.

Защита авторских прав разработчиков программных средств в настоящее время является одной из важнейших задач. Развитие рынка пиратской продукции побуждает владельцев интеллектуальной собственности учиться эффективно применять имеющиеся методы и изыскивать новые средства защиты информации.

Среди решений, предлагаемых для защиты тиражируемого программного обеспечения (ПО), можно выделить несколько основных групп.

Использование защищенных компакт-дисков, паролей и регистрационных номеров.

Эти методы защиты не требуют больших финансовых издержек при внедрении, однако обладают низкой стойкостью к взлому. Вследствие чего, применение такой защиты оправдано только для ПО нижней ценовой категории.

Привязка к уникальным характеристикам компьютера.

Стойкость к взлому у этого метода защиты гораздо выше, чем у предыдущих, при небольших затратах на внедрение. Применение такой защиты целесообразно в случаях, когда производитель уверен, что не отпугнет клиентов недостатками данного метода: трудностями при модернизации ПК. Пример использования этого метода – встроенная защита от копирования новых программных продуктов Microsoft.

Программно-аппаратная защита с использованием электронных ключей

На сегодняшний день это наиболее надежный и удобный метод защиты тиражируемого ПО средней и высшей ценовой категории. Он обладает высокой стойкостью ко взлому и не ограничивает использование легальной копии программы. Применение этого метода экономически оправдано для программ стоимостью свыше $100, так как использование даже самых дешевых электронных ключей увеличивает стоимость ПО на $15–20.

Выбирая средство защиты, разработчик должен исходить из принципа экономической целесообразности. Защита должна выполнить свое основное предназначение – существенно сократить, а в идеале – прекратить, потери от пиратства, не сильно при этом увеличивая стоимость программы. В идеале защита не должна причинять неудобства пользователям.

В докладе рассматривается защита ПО пользователя привязкой к ресурсам ПК.

Характеристиками компьютера, на которые обычно выполняется настройка устанавливаемого программного обеспечения [1]: имя компьютера, имя пользователя, версия операционной системы, параметры центрального процессора, параметры оперативной памяти, тип используемой клавиатуры, параметры используемой мыши, ширина и высота экрана монитора, информация о дисковых устройствах компьютера, параметры диска, на котором выполняется установка программного продукта (емкость, тип файловой системы, метка тома, путь к папкам с файлами операционной системы и др.).

Для получения значений указанных характеристик могут использоваться следующие функции из набора Windows API: GetUserName(…), GetComputerName(…), GetWindowsDirectory(…), GetSystemDirectory(…), GetKeyboardType(…),

GetSystemMetrics(…), GetLogicalDriveStrings(…), GlobalMemoryStatus(…), GetDiskFreeSpace(…), GetVolumeInformation(…), SystemParametresInfo(…), GetSystemInfo(…).

Однако из-за особенностей реализации механизма защиты рассматриваемый метод часто является неудобным для конечных пользователей и вызывает нарекания. Возникают трудности с модернизацией. Увеличение числа используемых параметров позволяет повысить надежность системы защиты, однако приводит к увеличению числа ложных срабатываний, что увеличивает неудобства пользователя защищаемого приложения. Мы не рекомендуем использовать при настройке ПО часть рассмотренных в [1] параметров ПК: имя компьютера, имя пользователя, версия операционной системы, тип используемой клавиатуры, параметры используемой мыши, параметры монитора, путь к папкам с файлами операционной системы, параметры оперативной памяти. Данные параметры часто меняются в процессе эксплуатации ПК.

Мы рекомендуем использовать следующие параметры ПК: параметры центрального процессора; информация о дисковых устройствах компьютера; параметры диска, на котором выполняется установка. Однако применяемые для получения данных параметров API-функции не позволяют получить уникальной информации о ПК (например, функция GetVolumeInformation (…) позволяет получить серийный номер тома, а не физического диска, и данный номер не связан с серийным номером диска).

В качестве уникальных параметров ПК предлагаем использовать серийный номер видеоадаптера, жесткого диска, материнской платы, MAC-адрес сетевой платы. Данные параметры присваиваются устройствам на этапе их изготовления и не меняются в процессе их функционирования. Для извлечения этих параметров требуется создать специальный драйвер, которым должны комплектоваться программный продукт и программа-регистратор. Однако существует более простой способ получения уникальных характеристик ПК – механизм WMI (Windows management instrumentation). В качестве примера рассмотрим получение информации о видеоадаптере. Данные о видеоадаптере можно получить, используя класс WMI *Win32_VideoController*. Важным является его поле *PNPDeviceID* (именно оно содержит всю необходимую информацию о видеоадаптере). Если на вашем компьютере установлен PowerShell, то вы можете получить информацию о видеоадаптере, набрав команду *get-WMIObject Win32_VideoController*.

Используемый нами метод привязки ПО пользователя к характеристикам ПК работает следующим образом:

Программный продукт

1. Анализирует параметры оборудования.
2. Анализирует лицензионную информацию.
3. При несоответствии принимает меры ограничения (программа запускается в демо – режиме).

Программа-регистратор

1. Анализирует параметры оборудования.

2. Генерирует регистрационный ключ.
3. Передает ключ пользователю продукта.

Для отключения защитной реакции взломщик может:

- нейтрализовать защитный механизм;
- дублировать регистрационный ключ.

Простая реализация метода защиты ПО привязкой к параметрам ПК [1] сводит анализ лицензионной информации, сгенерированной программой-регистратором к ее сравнению с необходимой, полученной в результате анализа параметров реального оборудования программным продуктом. Нейтрализация защиты в данном случае сводится к поиску и замене инструкции сравнения на безусловный переход.

Надежность защиты может быть увеличена путем использования криптозащиты. Шифрование должно применяться совместно с защитой от статического и динамического анализа кода программы и «изощренным программированием», т. е. стилем, позволяющим получить сложный и запутанный исполняемый модуль [2].

В предлагаемом нами варианте защиты в качестве параметров, к которым привязывается ПО пользователя, используются: параметры центрального процессора, информация о дисковых устройствах компьютера, данные о видеоадаптере. На основании собранной информации программный продукт и программа-регистратор генерируют ключи как MD6-хеш длиной 128 бит от суммарной информации.

В дальнейшем ключ программы-регистратора используется для шифрования изъятого фрагмента кода приложения пользователя.

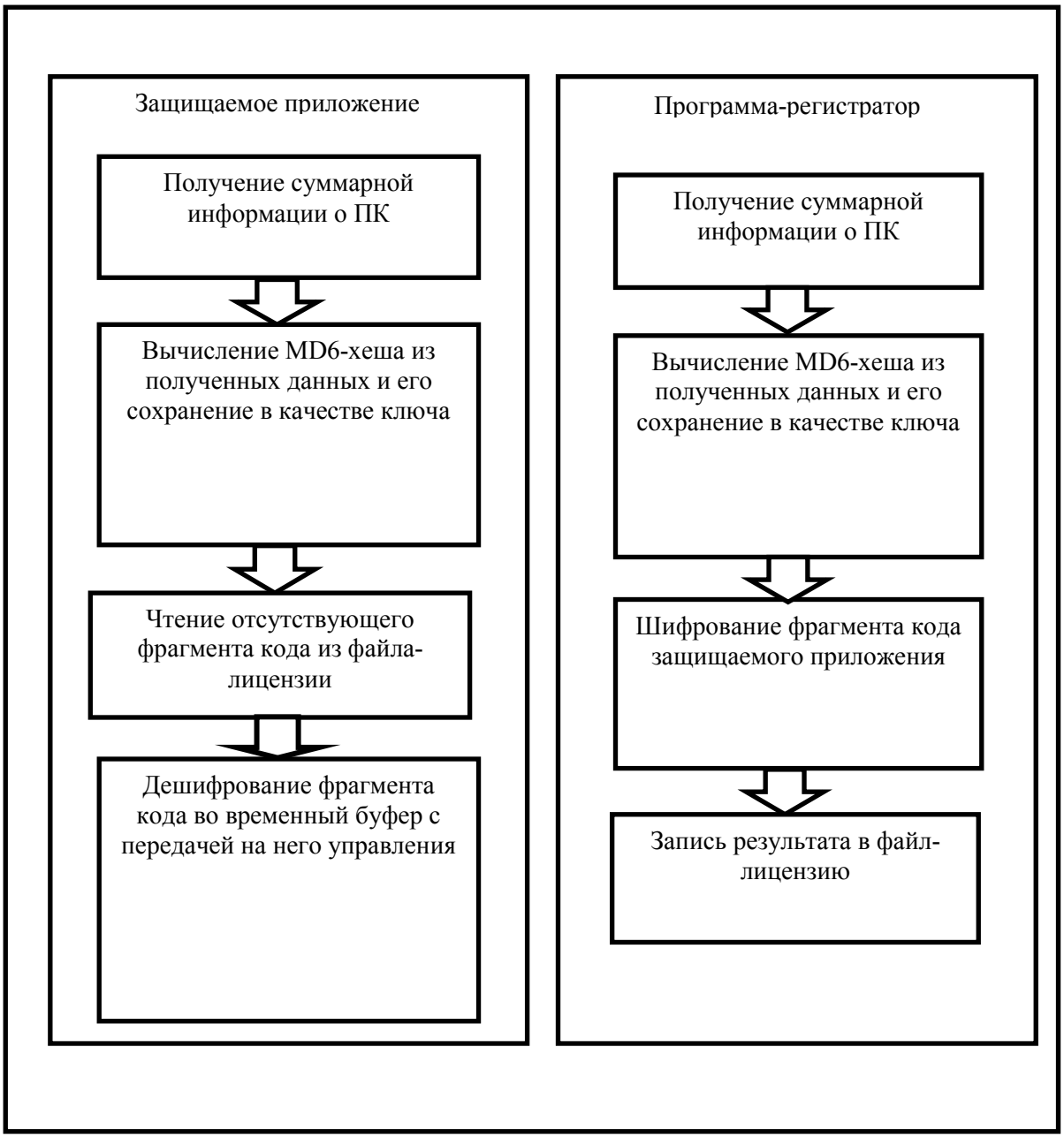
При запуске приложение пользователя генерирует свой ключ, читает недостающий зашифрованный фрагмент кода из файла лицензии, расшифровывает его во временный буфер при помощи полученного ключа. В случае правильной расшифровки программа запускается в полнофункциональном режиме.

Взломщик, имея исполняемый модуль программы, не может его корректно анализировать, так как в нем, как отмечалось выше, отсутствует фрагмент кода.

Для борьбы со снятием дампа и дизассемблерами было использовано динамическое изменение кода программы.

Для борьбы с отладчиками написан специфический обработчик прерывания int 3 (намеренно вызываемый программой), который выполняет коррекцию «ложных» ошибок, заранее включенных в текст программы. В случае если приложение запущено под отладчиком, то отладчик сам обработает int 3, и программа окажется нескорректированной. Используется также реализация защитного механизма на базе двух взаимодействующих потоков, что затрудняет динамическое исследование кода.

Разработанный нами алгоритм приведен на рисунке.



Алгоритм защиты ПО пользователя привязкой к ресурсам ПК

Таким образом, предложенный нами алгоритм защиты ПО пользователя привязкой к ресурсам ПК может быть использован для защиты реальных приложений в среднем ценовом диапазоне, а также в процессе подготовки специалистов в области компьютерной безопасности.

ЛИТЕРАТУРА

1. *Хорев, П. Б.* Методы и средства защиты информации в компьютерных системах/ П. Б. Хорев. М.: Академия, 2005.
2. *Абашев, А. А.* Ассемблер в задачах защиты информации / А. А. Абашев, И. Ю. Жуков, М. А. Иванов, Ю. В. Метлицкий, И. И. Тетерин. М.: Кудиз-Образ, 2004.