Система лицензирования программного обеспечения в электроэнергетике*

Н. Ю. Кульман, Н. А. Байдакова
Kulman.nik@gmail.com|Baydakova.natalia@gmail.com
ООО «Прикладные программы», Протвино

В докладе рассмотрена проблема защиты от несанкционированного использования ПО в системах промышленной автоматизации с помощью лицензирования. Особое внимание уделено архитектуре системы лицензирования. Рассмотрены различные варианты схем лицензирования. Разработан пример системы лицензирования приложений.

Ключевые слова: *лицензирование программ, защита программного обеспечения.*

Software Licesing System in Electronic Power Industry*

N. Yu. Kuhlman, N A. Baidakova
Ltd. “Applications program”, Protvino

The report deals with the problem of protection against unauthorized software applying in Industrial Automation Systems by using the licensing. Particular attention is paid to architecture of the licensing system. The different variants of licensing system’s schemes are considered. An example of software licensing system is developed.

Keywords: *licensing programs, software protection.*

Программные продукты являются предметом интеллектуального труда специалистов высокой квалификации. Процесс проектирования и реализации программных продуктов характеризуется значительными материальными и трудовыми затратами, основан на использовании наукоемких технологий и инструментария, требует применения и соответствующего уровня дорогостоящей вычислительной техники. Поэтому результаты разработки и производства программного обеспечения (ПО) необходимо защитить от несанкционированного использования. Это особенно актуально в связи с необходимостью импортозамещения зарубежных программных продуктов, распространённых в настоящее время на российском рынке.

О важности этого говорит приказ №96 от 01.04.2015 «Об утверждении плана импортозамещения программного обеспечения», изданный министром связи и массовых коммуникаций Российской Федерации. В государственных корпорациях и крупнейших промышленных и производственных компаниях России, прошли бурные обсуждения возможности полного перехода на отечественное программное обеспечение. Тем самым начато формирование благоприятных условий для развития разработки отечественного конкурентоспособного ПО.

Для развития отрасли производства программного обеспечения в РФ необходимо решить много вопросов, в частности, о защите интеллектуальной собственности.

Работа опубликована при финансовой поддержке РФФИ, грант 15-07-20370.

По данным исследования IDC (аналитическая фирма, специализирующаяся на исследованиях рынка информационных технологий), уровень использования контрафактного софта в России снизился на 24 пункта за 9 лет с 2003 по 2011 год (последние данные) и составил 63% [1, 2]. Несмотря на то, что эта цифра каждый год снижается, для производителей коммерческого программного обеспечения это означает огромную недополученную прибыль. Многие крупные производители софта предпочитают бороться с пиратством техническими и юридическими мерами. В большинстве случаев надежными и эффективными остаются программные способы защиты, а для более успешного противостояния всем угрозам разработчики коммерческого программного обеспечения должны озаботиться вопросами защиты своих продуктов еще на начальной стадии разработки нового ПО.

В данной работе мы не касаемся юридических и организационных аспектов данной проблемы, а рассмотрим тему с точки зрения создания программных средств для защиты ПО.

Программное обеспечение является объектом защиты также и в связи со сложностью и трудоемкостью восстановления его работоспособности, значимостью программного обеспечения для работы систем промышленной автоматизации. Достаточно трудно дать точную характеристику понятию «защита», Защита программного обеспечения преследует цели:

- ограничение несанкционированного доступа к программам или их преднамеренное разрушение и хищение;

- исключение несанкционированного копирования (тиражирования) программ. Основная идея организационных мер защиты заключается в том, что полноценное использование продукта невозможно без соответствующей поддержки со стороны производителя.

Целью всех современных средств защиты от несанкционированных действий является ограничение использования программных продуктов. Для достижения этой цели используются самые различные методы [3]. Методы защиты можно разделить на аппаратные и программные. К первым относятся методы, использующие специальное оборудование (например, электронные ключи, подключаемые к портам компьютера) или физические особенности носителей информации (компакт-дисков, флеш-накопителей и др.), чтобы идентифицировать оригинальную версию программы и защитить продукт от нелегального использования. К программным методам относятся те, что реализуются без затрагивания физических характеристик носителей информации и специального оборудования. В данной работе мы рассмотрим программные методы защиты ПО.

Целью данной работы является разработка архитектуры системы лицензирования приложений для защиты от несанкционированного использования ПО в системах промышленной автоматизации.

Лицензирование программ – это процедура, позволяющая организации или частному лицу использовать программное обеспечение на отдельном компьютере или в сети, соответственно лицензионному соглашению с производителем этого программного обеспечения.

Использование лицензионного программного обеспечения помогает повысить эффективность и результативность работы компаний за счет снижения угроз безопасности и рисков потерь данных, в том числе конфиденциальных. Это позволяет сократить количество сбоев и неполадок, уменьшить время простоя и снизить издержки, связанные с восстановлением нормальной работы ИТ-инфраструктуры. Кроме того, только при работе с лицензионным ПО пользователи получают полную техническую поддержку и гарантию безопасности от производителя. Таким образом, лицензирование позволяет защитить как инвестиции компании-разработчика, так и инвестиции предприятия-заказчика, исключив некорректную работу пиратского ПО и риск наказания за использование пиратского программного обеспечения.

Как правило, разработчик реализует лицензионное соглашение путем встраивания в программный продукт специальных механизмов, не позволяющих использовать программу в случае нарушения пользователем каких-либо пунктов этого соглашения.

Суть системы лицензирования заключается в том, что после установки программного обеспечения пользователь получает от производителя лицензионный файл, который привязан к компьютеру. В этом файле, в зашифрованном виде содержится информация о пользователе, продукте и другие данные.

Как правило, используются модули лицензирования, которые встраиваются в программный продукт после его окончательной разработки. Лицензия запрашивается в различные моменты времени желательно при выполнении важных функциональных операций.

Для идентификации ПК используются различные компоненты оборудования:

- серийный заводской номер жесткого диска;
- серийный номер сетевой карты;
- MAC-адрес сетевой карты;
- сведения, которые содержаться в BIOS компьютера;
- различные характеристики ОС и др.

Способы привязок можно комбинировать. Более строгие схемы привязок усиливают безопасность, но при этом также увеличивается число звонков в службу технической поддержки от тех клиентов, которые могли, например, просто заменить жесткий диск. Если схема менее строгая, то снижается уровень безопасности. Возможна схема с сочетанием четырех свойств, где разрешено изменять только один элемент. В таком случае, активированная лицензия остается действительной до тех пор, пока три элемента остаются неизменными.

Многие параметры компьютера можно получить через WMI [4]. Это одна из базовых технологий для централизованного управления и слежения за работой различных частей компьютерной инфраструктуры под управлением ОС Windows. WMI упрощает сбор информации о компьютере и делает его более последовательным.

Заказчику для получения лицензии у производителя ПО необходимо отправить файл запроса лицензии. Есть разные варианты: заказчику поставляется программа для создания запроса лицензии или запрос лицензии может быть встроен в программу производителя. Отправить запрос лицензии можно по почте.

Информация в файле запроса лицензии является конфиденциальной, поэтому она находится там в

шифрованном виде. Эффективным методом для шифрования является криптографический алгоритм с открытым ключом RSA.

Для криптосистемы с общим ключом требуется два взаимосвязанных, комплементарных ключа. Пара ключей генерируется на стороне производителя ПО. Один ключ является открытым и зашивается в ПО, передаваемое заказчику. Этот ключ используется для шифрования файла запроса лицензии. Второй ключ является закрытым и зашивается в специальную программу, находящуюся у производителя ПО. Он необходим для расшифровки полученного от заказчика файла запроса лицензии.

Создавать файл лицензии может только производитель ПО, поэтому для шифрования лицензии используется другая (2-я) пара ключей. Файл лицензии шифруется открытым ключом на стороне производителя ПО и передаётся организации, пославшей запрос лицензии.

Далее рассматриваются две схемы лицензирования. В первом варианте (Рис.1), обе пары ключей создаются на стороне производителя ПО. Ключи зашиваются в программы и не привязываются к компьютеру.

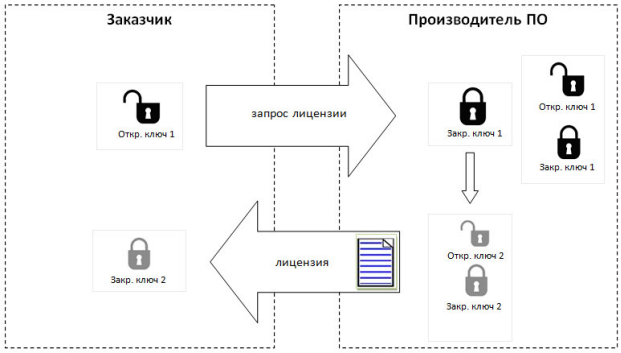

Рис. 1: Схема лицензирования программных продуктов I.

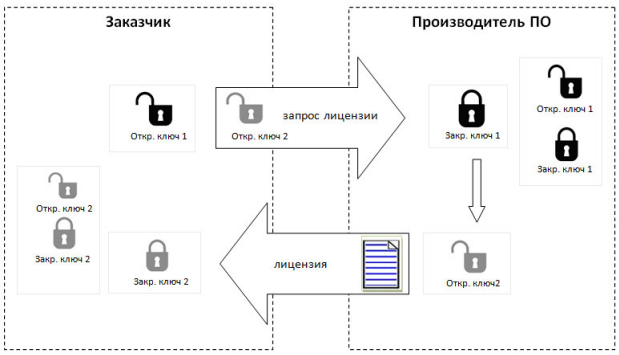

Рис. 2: Схема лицензирования программных продуктов II.

Вторая схема имеет более сильную защиту (Рис.2). Это обеспечивается тем, что 2-я пара ключей создается на компьютере заказчика и закрытый ключ привязывается к компьютеру, на котором он создан. Таким образом, 2-й закрытый ключ – это индивидуальный ключ, который привязан к компьютеру с помощью сервисов Microsoft CryptoAPI. Причем, способ привязки ключа к компьютеру не опубликован, а поэтому известен только Microsoft. При переносе этого ключа на другой компьютер он перестает работать.

ПО, поставляемое заказчику, может быть как отдельной программой, так и большой системой в архитектуре клиент-сервер. Во втором случае лицензия может выдаваться для сервера или индивидуально для конкретной программы. Если лицензия выдана для сервера, то от клиентского ПО посылается запрос на сервер для проверки наличия лицензии. В случае индивидуальной лицензии для ПО, программа сама проверяет наличие лицензии. Проверка лицензии осуществляется в процессе работы ПО через модули лицензирования. В модулях лицензирования осуществляется проверка данных указанных в лицензии к характеристикам ресурса, где запущено ПО. Если перенести ПО и лицензию на другой сервер, то такого соответствия не будет, и прикладные программы не будут нормально функционировать.

Учёт разработчиком выданных лицензий обеспечивается с помощью базы данных (БД), находящейся у производителя ПО. Эта же БД позволяет хранить информацию о заказчиках и вести учет выданных лицензий.

Используя сведения из БД можно узнать, кому выдана лицензия и на какой срок, существуют ли у заказчика ранее выданные лицензии и в каком количестве, когда дата окончания лицензии и т.п. Также в БД хранится информация о заказчике: название организации или частного лица, адрес, контактные данные.

В результате выполнения данной работы, разработана архитектура системы лицензирования приложений для защиты от несанкционированного использования программного обеспечения в системах промышленной автоматизации. Созданы приложения для формирования запроса лицензии, модуль для сбора информации о ПК, приложение для создания лицензии и модуль для проверки лицензии.

Литература

[1] Исследования по проблеме компьютерного пиратства [Электронный ресурс]. – UNITED STATES: Официальный сайт Microsoft. – Режим доступа: http://www.microsoft.com/rus/antipiracy/about/investigations.aspx - Загл. с экрана

[2] Статистика и вред пиратства [Электронный ресурс].
– UNITED STATES: Официальный сайт Microsoft.
– Режим доступа: https://www.microsoft.com/ru-ru/antipiracy/copyright-statisticsandharmpiracy.aspx - Загл. с экрана

[3] Побегайло А.П. Системное программирование в Windows / А. П. Побегайло. – СПб.: БХВ-Петербург, 2006. – 1056 с.

[4] Соломон Д. Внутреннее устройство Microsoft Windows 2000. Мастер-класс / Д. Соломон, М.Руссинович; пер. с англ. – СПб.: Питер; М.: Русская Редакция, 2004. – 746с.

[5] Джефри Рихтер. Windows via C/C++. Программирование на языке Visual C++ / Рихтер Джефри, Назар Кристоф; пер. с англ. – М.: Русская Редакция; СПб.: Питер, 2008. – 896 с.