Н.А. Байдакова, Н.Ю. Кульман

ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОТ НЕСАНКЦИОНИРОВАННОГО ИПОЛЬЗОВАНИЯ В СИСТЕМАХ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ С ПОМОЩЬЮ ЛИЦЕНЗИРОВАНИЯ

Филиал «Протвино» университета «Дубна»
Кафедра информационных технологий

Рассматривается проблема защиты от несанкционированного использования ПО в системах промышленной автоматизации с помощью лицензирования. Работа выполнена на базе предприятия ООО «Системы телемеханики и автоматизации» (г. Протвино), созданного в 1992 году с целью внедрения современных информационных технологий в различные отрасли промышленности.

За годы работы в энергетике специалисты ООО «Систел» приобрели опыт проектирования, разработки и внедрения систем телемеханики, автоматизированных систем диспетчерского и технологического управления и учёта энергоресурсов для энергетических объектов и систем, крупных промышленных предприятий [1]. Специалистами предприятия разработаны и реализованы проекты систем автоматизации для объектов энергетики различного уровня сложности.

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. Это обусловливает необходимость принятия мер по защите интересов разработчика программного обеспечения от несанкционированного их использования.

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", поскольку оно слишком широко трактуется, и подразумевает практически все аспекты информационной безопасности.

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[2]. Методы защиты можно разделить на программные и аппаратные. К первым относятся методы, реализуемые без затрагивания физических характеристик носителей информации, специального оборудования. К аппаратным относятся методы, использующие специальное оборудование (например, электронные ключи, подключаемые к портам компьютера) или физические особенности носителей информации (компакт-дисков, дискет), чтобы идентифицировать оригинальную версию программы и защитить продукт от нелегального использования.

Целью данной работы являлась разработка 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[3]. 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 любой из систем лицензирования заключается в том, что после установки программного обеспечения пользователю необходимо получить от производителя лицензионный файл, кото-

рый был бы тем или иным образом 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 используется множество способов:

- 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. 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 платформы Windows. WMI упрощает сбор информации о компьютере и делает его более последовательным.

Организации для получения лицензии необходимо взять в Сертификационном центре приложение «Запрос лицензии» (LicenseRequest.exe) и запустить на ПК, где установлено или будет установлено ПО, которое необходимо лицензировать.

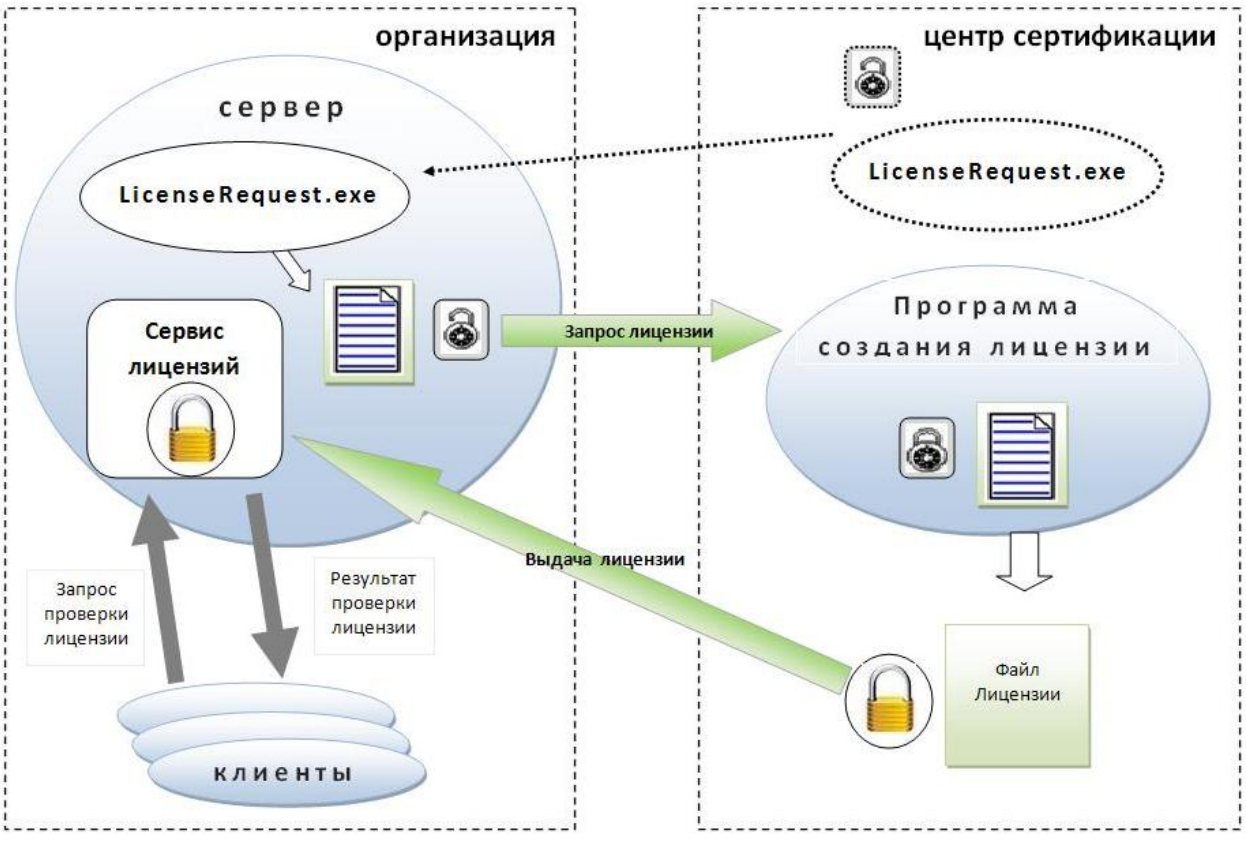

Рис. «Схема лицензирования программных продуктов»

Приложение «Запрос лицензии» сформирует файл запроса. Информация файла является конфиденциальной, поэтому её необходимо зашифровать. Эффективным методом для шифрования файла запроса лицензии является криптографический алгоритм с открытым ключом RSA [5]. Для криптосистемы с общим ключом требуется два взаимосвязанных, комплементарных ключа. Пара ключей генерируется в центре сертификации, один ключ является открытым и передаётся в

организацию с приложением LicenseRequest.exe. Этим ключом шифруется файл запроса лицензии и передаётся Сертификационному центру. Второй ключ является секретным, хранится в Сертификационном центре и необходим для расшифровки полученного от организации файла запроса лицензии.

Программа создания лицензий в сертификационном центре, получив файл запроса лицензии, формирует лицензию. Создавать файл лицензии может только Сертификационный центр, поэтому для шифрования используется симметричный алгоритм шифрования. Файл лицензии шифруется закрытым ключом центра сертификации и передаётся организации, пославшей запрос лицензии. Лицензия, как правило, хранится на сервере организации. При установке прикладного ПО на сервер устанавливается Сервис лицензий. При использовании программного обеспечения от клиентов посылается запрос в сервис лицензий для проверки наличия лицензии в организации. Сервис лицензии проверяет соответствие характеристик сервера, указанных в лицензии, тем которыми обладает сервер, на котором запущенно ПО. Если перенести ПО и лицензию на другой сервер, то такого соответствия не будет, и прикладные программы не будут нормально функционировать.

Работа выполнялась в среде разработки Visual Studio 2008 [6].

В результате выполнения данной работы, разработана система 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.

Библиографический список

1. Рыкованов С.Н. Оперативный информационный управляющий комплекс «Систел» / С.Н. Рыкованов, Н.Ю. Кульман, В.И. Ухов // Автоматизация от А до Я. – 2007, №1. – С. 9-11.
2. Побегайло А.П. Системное программирование в Windows / А. П. Побегайло. – СПб.: БХВ-Петербург, 2006. – 1056 с.
3. Агуров П.В. C#. Разработка компонентов в MS Visual Studio 2005/2008 / П. В. Агуров. – СПб.: БХВ – Петербурга, 2008. – 480с.
4. Соломон Д. Внутреннее устройство Microsoft Windows 2000. Мастер-класс / Д. Соломон, М. Руссинович; пер. с англ. – СПб.: Питер; М.: Русская Редакция, 2004. – 746 с.
5. Фридман А. C/C++. Архив программ / А. Фридман, Л. Кландер, М. Михаэлис. – М.: ЗАО «Издательство БИНОМ», 2001. – 640 с.
6. 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.