Библиографический список

1. Никулина О.В. Перспективы развития деятельности современных предприятий в условиях инновационной экономики // Финансы и кредит. 2009. № 37. С 37–44.

2. Федеральная служба государственной статистики [Электронный ресурс]. URL: http://www.gks.ru/wps/wcm/connect/rosstat/rosstatsite/main/16.11.11.

3. Информационный бизнес-портал [Электронный ресурс]. URL : http://www.ma-com.ru/osobennosti-finansov-malogo-biznesa.htm. 16.11.11.

4. Майоров А.А. К вопросу о совершенствовании регионального организационно-финансового механизма развития малого бизнеса // Финансы и кредит. 2011. № 15. С. 66–74.

УДК 004.056

Студ. О.В. Самарина
Рук. Т.С. Крайнова
УГЛТУ, Екатеринбург

МЕХАНИЗМЫ ЗАЩИТЫ ПРОГРАММНЫХ ПРОДУКТОВ

Программные продукты являются предметом интеллектуального труда специалистов высокой квалификации. Процесс проектирования и реализации 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 программ от несанкционированного их использования. Программные комплексы являются объектом защиты также и в связи со сложностью и трудоемкостью восстановления их работоспособности.

Программные продукты должны быть защищены по нескольким направлениям воздействия[*]:

- человека – хищение машинных носителей и документации программного обеспечения;
- аппаратуры – подключение к компьютеру аппаратных средств для считывания программ и данных или их физического разрушения;
- специализированных программ – приведение программного продукта в неработоспособное состояние (например, вирусное заражение) и т.д.

[*] Гагарина Л.Г., Кокорева Е.В., Виснадул Б.Д. Технология разработки программного обеспечения. М.: ФОРУМ, ИНФРА-М, 2010. 399 с.

Самый простой и доступный способ защиты программного продукта – ограничение доступа паролем. Но нельзя один и тот же механизм защиты с успехом применять как к программе, поставляемой на компакт-диске и выполняемой прямо с него, так и к программе, работающей с жесткого диска компьютера. В зависимости от характера защищаемого программного обеспечения используется свое решение защиты:

1) ограничение числа установок программы на компьютер: при каждой инсталляции «вычитается» значение допустимого количества установок программного продукта с компакт-диска;

2) ограничение числа запуска программы: применяется для создания демонстрационных версий программы;

3) контрольные вопросы: пользователю, купившему пиратскую копию программы, по истечении определенного срока со дня применения задается контрольный вопрос, требующий при ответе наличия лицензионной версии программного продукта и справочного руководства к нему;

4) версии, работающие с ограничениями: пользователь в одном сеансе запуска обладает ограниченными функциями или временем работы программы. Для перевода программы в полноценный режим работы необходим уникальный для данного компьютера ключ, который можно приобрести у компании-разработчика;

5) аппаратные ключи: для запуска программного обеспечения необходимо наличие аппаратного ключа, устанавливаемого на COM-, LPT- или USB-порт;

6) обфускация: трансформирование программного кода (удаление комментариев, включение произвольных наборов символов и т.д.) так, чтобы это не повлияло на работоспособность, но сделало алгоритм программы нечитабельным, трудным для изучения и, как следствие, модификации посторонними лицами.

Однако следует помнить, что абсолютной защиты не существует, любую защиту можно сломать. Купить «пиратский» продукт легко, гораздо труднее правильно настроить его и поддерживать. Для разработчика единственно верным способом надежной защиты программного продукта является перевод его из разряда программного обеспечения в разряд платформы, когда достаточно сложный программный комплекс требует при эксплуатации тесного сотрудничества с производителем.