

У техники есть душа, и она нуждается в защите

В наш цифровой век любая техника – ничто без программного обеспечения. ПО – это душа машины, без которой сегодня она является грудой железа, годящегося разве что на продажу по частям.



Основа работы любого механизма – ПО, которое руководит действиями устройства, контролирует параметры и т.д. ПО бывает разное, но у всех типов программ есть одна общая черта – их создал человек. Потратил время и нервы на разработку, тестирование, продвижение на рынок и техническую поддержку программного продукта. Разумно было бы предположить, что за свою работу человек хочет получить достойное вознаграждение. Однако существуют и другие люди, не желающие заниматься разработкой самостоятельно, а ворующие часть дохода программиста, продавая нелегальные копии ПО. Таких людей называют пиратами, а программы, продаваемые ими, – пиратскими. Граждане с удовольствием покупают такие программы, тем самым лишая честного дохода правообладателей ПО.

С развитием Интернета распространение пиратской продукции стало ещё легче. Достаточно выложить дистрибутив программы на какой-нибудь сервер в районной сети – и продажи её упадут в разы. Здесь преследуются уже не столько коммерческие интересы пиратов, сколько их желание самоутвердиться среди себе подобных: «Наша группа первая достала программу и выложила её в сеть!».

Естественно, программисты и издатели ПО не хотят мириться с существующим положением вещей. Им, как минимум, надо окупить затраты на разработку продукта. А в идеале – получить прибыль, которая частично пойдёт на зарплату сотрудников и будет инвести-

рована в новые программы. Именно поэтому в мире существуют компании, занимающиеся разработкой средств борьбы с пиратами и хакерами, чтобы дать возможность отрасли развиваться.

Наиболее уязвимыми считаются компьютерные игры. Именно в этой отрасли от пиратства страдают больше всего. В 1998 г. российская компания Protection Technology первой в мире предложила использовать технологию под названием «виртуальная машина» для защиты компьютерных игр. В то время в России из десяти продаваемых игровых дисков девять были пиратски-



ми, а потому проблема стояла очень остро. Идея предложенной технологии заключалась в том, чтобы не просто защитить носитель от копирования, а внедрить защиту в программный код игры, максимально осложнив тем самым анализ и взлом игры и, как следствие, – выпуск пиратской партии дисков. Отечественному потребителю эта защита известна как StarForce. Сегодня технология, предложенная отечественными разработчиками, является индустриальным стандартом во всем мире. Виртуальная машина для защиты не только игр, но и остального ПО применяется очень широко.

В чём же суть технологии? Исполняемые файлы игры разбираются на модули. Часть функций переносится в библиотеку защиты, оставшаяся часть шифруется. Библиотека защиты представляет собой виртуальный процессор внутри системы. Все команды, выполняемые этим процессором, написаны на особом языке программирования и

скомпилированы особым компилятором. При запуске защищённая программа запрашивает функции из библиотеки защиты. Библиотека выполняет внутри себя эти функции и возвращает программе результат. Хакеру чрезвычайно сложно проанализировать работу такого виртуального процессора и понять всё, что там происходит, а следовательно, и перехватить выполнение защищённых функций. Кроме того, библиотека защиты может проверять подлинность носителя, электронной лицензии, целостность защиты, контрольные суммы файлов и многое другое.

Помимо виртуальной машины, StarForce использует уникальный запатентованный метод проверки оптического диска на соответствие параметрам лицензии. При запуске программа защиты считывает дисковый ключ из области данных диска, сверяет параметры, в нём зашифрованные, с физическими параметрами диска и в зависимости от результата запускает программу или нет. Сочетание такой проверки диска и виртуальной машины дают очень надёжную защиту программы в целом.

