УДК 004.0

ПРОВЕРКА ЛИЦЕНЗИИ ПРОГРАММНОГО ПРОДУКТА НА ОСНОВЕ АЛГОРИТМА RSA

Азаревич В. А., Ковалева И.Л.
Белорусский национальный технический университет, Минск

Вместе с распространением новых информационных технологий появляются новые методы взлома компьютеров и похищения информации. Наибольшей опасности взлома компьютер подвергается тогда, когда он подключен к интернету. Поэтому одним и способов обеспечения безопасности при работе с конфиденциальной информацией на компьютере является отключение компьютера от интернета. Однако отключение компьютера от интернета затрудняет проверку лицензионного ПО, установленного на этом компьютере. Для решения этой проблемы предлагается подход по проверке лицензии ПО, разработанный на основе алгоритма RSA.

Интернет для данного алгоритма проверки лицензии нужен только при установке ПО с целью отправки единичного сообщения на сервер.

На вход сервер получает 2 набора данных: данные, идентифицирующие пользователя, и подтверждение о возможности использования лицензии. В первый набор входят ID различного оборудования компьютера. Наиболее важными являются материнская плата и процессор. Общение между сервером и пользователем должно происходить по любому защищённому протоколу. Для этих целей лучше всего подходит протокол HTTPS.

После того, как сервер подтвердил право использования лицензии, он шифрует закрытым ключом всю полученную информацию, а так же важные элементы программного кода, изменение которых недопустимо. Так же в зашифрованном виде отправляется количество дней разрешенного использования. Полученная строка отправляется обратно пользователю, где она сохраняется в реестр компьютера и может проверяться при помощи публичного ключа. Таким образом, уведомлять пользователя об истечении срока использования программного продукта можно в дальнейшем без подключения компьютера к интернету.

Предлагаемый подход позволяет запретить использование вашего программного продукта неавторизованным пользователям, а так же пользователям, не имеющим прав использования. Более того, такой подход предотвращает возможность нарушения целостности программного кода и уведомляет пользователя об истечении срока использования лицензии без подключения к интернету. Реализация выполнена на языке C#.