С.А. Иливицкий[1], П.В. Трешников[2], Л.С. Зеленко[1]

ПРОЕКТИРОВАНИЕ ПОДСИСТЕМЫ ЛИЦЕНЗИРОВАНИЯ ПРОГРАММНОГО КОМПЛЕКСА «ТЕХНОДОК»

([1] Самарский национальный исследовательский университет
имени академика С.П. Королёва
[2] ООО Научно-внедренческая фирма «Сенсоры. Модули. Системы»)

В настоящее время проблема защиты интеллектуальной собственности является актуальной для любой области творческой деятельности и не имеет гражданства. В сфере программного обеспечения она стоит не менее остро. По результатам исследования, произведенного в 2017 году ассоциацией BSA (Business Software Alliance), на персональных компьютерах пользователей в России 62% программного обеспечения (ПО) является нелицензионным. В соседних странах доля нелицензионных приложений составляет: в Белоруссии – 82%, в Молдавии – 83%, на Украине – 80% [1]. В связи с этим компании теряют существенную долю прибыли. Из-за этого проблема защиты программного обеспечения от незаконного использования стала одной из актуальнейших на сегодняшний момент.

Большинство разработчиков программного обеспечения используют различные программные модули, контролирующие доступ пользователей к нему с помощью ключей активации, серийных номеров и т. д. Однако такая защита легко подвержена взлому и не является достаточно надежной.

В начале 1980 годов в качестве усовершенствования защиты программного обеспечения стали применятся электронные ключи. Они предоставили более надежный способ лицензирования программного обеспечения. Так же их использование позволило не привязываться к определенному аппаратному обеспечению, тем самым обеспечивая переносимость лицензионной информации с одного сервера на другой.

В связи с перечисленными выше преимуществами возникла задача разработки подсистемы лицензирования, базирующейся на электронных ключах Guardant Sign, которая войдет в состав программного комплекса производственной отчетности и аналитики для промышленных предприятий «ТехноДок» [2].

Основными функциями подсистемы являются:

1) авторизация и аутентификация пользователя в системе, настройка интерфейса пользователя на заданную роль;
2) предоставление лицензии пользователю;
3) проверка корректности лицензии;
4) обновление лицензии пользователя;
5) запрос на предоставление лицензии;
6) запрос на обновление лицензии.

Подсистема лицензирования поможет предотвратить незаконное распространение программного обеспечения и будет способствовать оперативному переносу лицензионной информации с одного сервера на другой.

Литература

1 Стоимость нелицензионного программного [Электронный ресурс]. URL: http://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf (дата обращения : 20.05.2019).

2 Программный комплекс «ТехноДок» [Электронный ресурс]. URL: http://www.sms-automation.ru/solutions/technodoc/ (дата обращения: 20.05.2019).

Р.И. Канафеев, М.А. Кудрина

ИСПОЛЬЗОВАНИЕ ОБФУСКАЦИОННЫХ ПРЕОБРАЗОВАНИЙ ДЛЯ ЗАЩИТЫ ПРОГРАММНОГО КОДА

(Самарский университет)

Несмотря на наличие всего комплекса законодательных и правовых мер по защите авторских и смежных прав на интеллектуальную собственность, ситуация с пиратским рынком программного обеспечения (ПО) остается весьма плачевной. Согласно исследованиям международной ассоциации производителей программного обеспечения BSA, доля использования пиратского ПО в России в 2017 г. составила 62% [1]. Для производителей коммерческого ПО это означает огромную недополученную прибыль. Подобная проблема существует не только на отечественном рынке, но и во всем мире. Для ее устранения используются различные методы защиты программного обеспечения, которые получили широкое распространение и находятся в процессе постоянного развития, благодаря глубокой интеграции информационных технологий в общество.

Упаковка исполняемого файла и техники защиты ПО, основанные на недокументированных возможностях среды программирования, не защищают должным образом от анализа и модификации программ, поскольку в первом случае код доступен в момент передачи на него управления, а во втором – злоумышленнику достаточно знать какой именно прием используется, чтобы в дальнейшем создать механизмы, способные преодолеть такого рода защиту [2-4]. Более того, приемы, основанные на недокументированных возможностях, могут дестабилизировать работу приложения. Очевидно, что защитить код приложения от доступа к нему невозможно. А значит в обоих случаях возможно создать автоматические средства деактивации защиты. Следовательно, первоочередная задача защиты ПО от анализа – максимально затруднить понимание внутренней логики работы ПО злоумышленником и обеспечить невозможность создания им автоматической утилиты модификации этого кода. Тогда даже обладая доступом к коду приложения, его анализ будет крайне затруднен. В связи с этим наиболее актуальными в настоящий момент являются методы