ЗАЩИТА ИНФОРМАЦИИ МОБИЛЬНЫХ МАШИН

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Павловский А. В.

Савченко В.В. – кандидат техн. наук

Целью работы является разработка системы защиты информации мобильных машин, с использованием привязки программного обеспечения бортового компьютера к индивидуальным характеристикам исполняемой среды мобильного объекта и аппаратных ключей.

Разработана система осуществляющая противодействие несанкционированному выполнению скопированных программ путем использования блока контроля среды размещения программы.

Блок контроля среды размещения является дополнительной частью защищаемой программы. Он создается при инсталляции программы. В него включаются контрольные характеристики среды, в которой размещается защищаемая программа, а также средства получения и сравнения характеристик. В качестве характеристик среды могут использоваться особенности архитектуры бортового компьютера, тип и частота процессора, состав и характеристики внешних устройств, особенности их подключения, режимы работы блоков и устройств.

Система защиты требует повторной инсталляции защищаемого программного обеспечения после проведения модернизации, изменения структуры или ремонта с заменой устройств. Общий алгоритм использования защиты от несанкционированного использования программ в «чужой» среде размещения показан на рисунке 1.

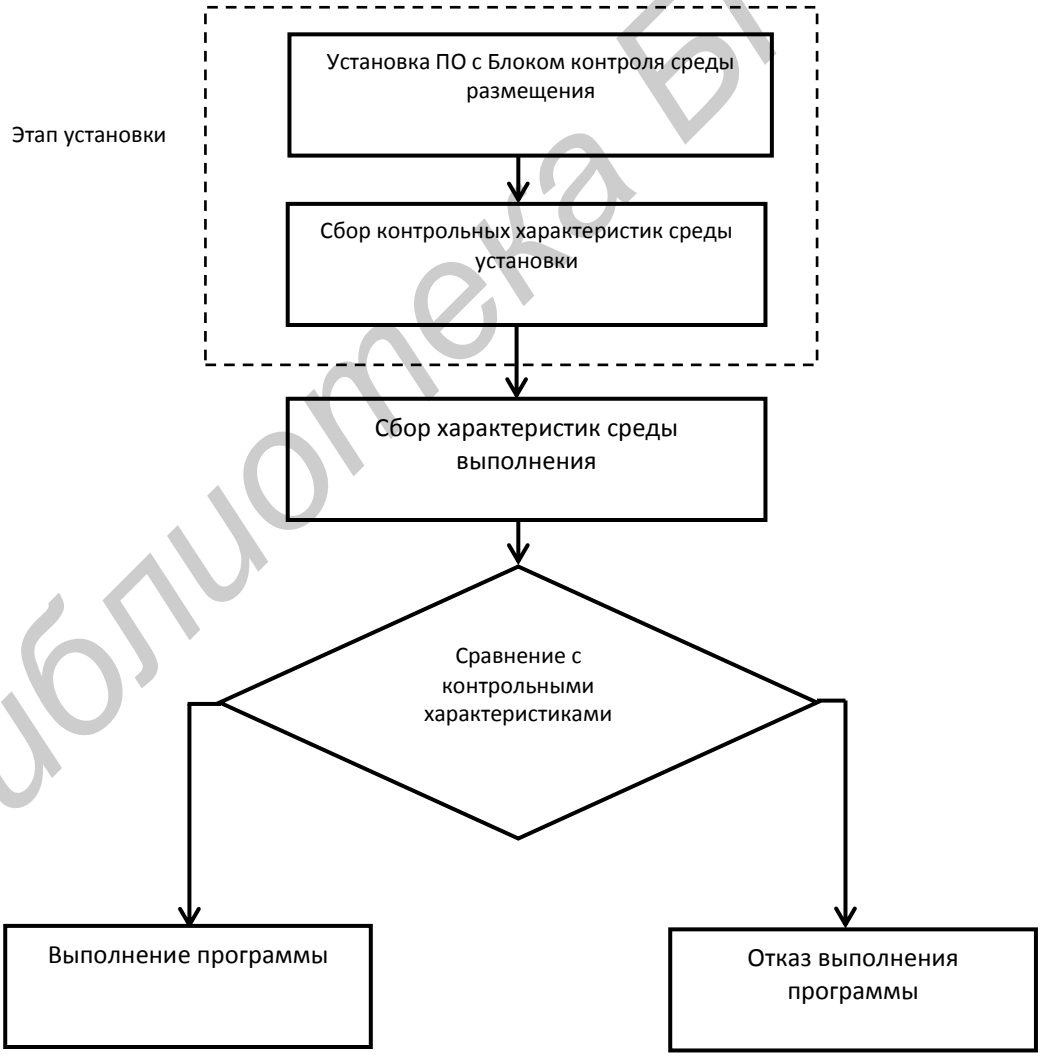

Рис. 1 – Блок-схема работы метода защиты от несанкционированного копирования с использованием привязки к индивидуальным параметрам среды выполнения

Инсталлированная программа при каждом запуске выполняет следующие действия:

− анализ аппаратно-программной среды мобильной машины, на котором она запущена, формирование на основе этого анализа текущих характеристик своей среды выполнения;

− проверка подлинности среды выполнения путем сравнения ее текущих характеристик с эталонными;

− блокирование дальнейшей работы программы при несовпадении текущих характеристик с эталонными.

Система защиты требует повторной инсталляции защищаемого программного обеспечения после проведения модернизации, изменения структуры или ремонта, с заменой устройств. Эта обеспечивает невозможность установки сторонних обновлений или подключения дополнительных устройств.

Инсталлированная программа при каждом запуске выполняет следующие действия:

− анализ аппаратно-программной среды мобильной машины, на котором она запущена, формирование на основе этого анализа текущих характеристик своей среды выполнения;

− проверка подлинности среды выполнения путем сравнения ее текущих характеристик с эталонными;

− блокирование дальнейшей работы программы при несовпадении текущих характеристик с эталонными.

Таким образом, защищаемый мобильный объект будет устойчив не только к внедрению потенциально опасных программ, но и подключению любого рода устройств, не задействованных в момент установки базового программного обеспечения.

Для устранения уязвимости связанной с возможностью внесение в процесс сравнения контрольных характеристик с характеристиками среды изменений, применяются аппаратные ключи типа HASP или Sentinel.

Аппаратные ключи представляет собой программно-аппаратный комплекс содержащий код, процедуры или любые другие уникальные данные, по которым защита может идентифицировать легальность запуска.

Основой аппаратных ключей являются специализированные заказные микросхемы, имеющие уникальный для каждого ключа алгоритм работы.

В процессе выполнения защищённая программа опрашивает подключённый к бортовому компьютеру ключ. Если аппаратный ключ возвращает правильный ответ и работает по требуемому алгоритму, программа выполняется нормально. В противном случае, она может завершаться, переключаться в демонстрационный режим или блокировать доступ к каким-либо функциям программы.

Наличие энергонезависимой памяти дает возможность программировать такие ключи, размещая внутри модуля различные процедуры, либо хранить дополнительные ключи, а также:

− управлять доступом к различным программным модулям и пакетам программ;

− назначать каждой серии защищенных программ уникальный номер;

− хранить в ключе уникальную информацию идентификации мобильного объекта.

В памяти аппаратного ключа храниться уникальный опознавательный номер, или идентификатор, доступный для считывания защищёнными программами. Идентификаторы позволяют различать пользователей программы. Проверяя в системе идентификатор аппаратного ключа, пользователь имеет возможность предпринимать те или иные действия в зависимости от наличия конкретного ключа. Идентификатор присваивается электронному ключу в процессе изготовления, что делает невозможным его замену, но гарантирует надежную защиту от повтора.

Сочетание использования блока контроля среды исполнения и электронного ключа, реализованного на отдельном носителе и имеющего уникальные идентификационные признаки, обеспечивает реализацию достаточно надежной защиты.

Список использованных источников:

1. Аппаратно-программные средстваи методы защиты информации/ С.К. Варлатая, М.В. Шаханова – Изд-во: ДВГТУ.: Владивосток, 2007. – 318 с.
2. Ярочкин В.И. Информационная безопасность. Учебной пособие для студентов непрофильных вузов / Ярочкин В.И. – М.: Междунар. отношения, 2000. – 400 с.
3. Основы информационной безопасности: Учебн. Пособие / Белов Е.Б., Лось В.П, Мещеряков Р.В, Шелупанов А.А. – М.: Горячая линия Телеком, 2006. - 544 с.
4. Защита от утечки информации по техническим каналам Учебн. пособие / Бузов Г.А, Калинин СВ., Кондратьев А.В. – М.: Горячая линия - Теле- ком, 2005. - 416 с.
5. Информационная безопасность открытых систем. Часть 1: Учебник для вузов / Запечников СВ., Милославская Н.Г Толстой А.И, Ушаков Д.В. – М.: Горячая линия - Телеком, 2006. - 686 с.
6. Comprehensive Experimental Analyses of Automotive Attack Surfaces / Stephen Checkoway, Damon McCoy, Brian Kantor // Proceeding SEC'11. Proceedings of the 20th USENIX conference on Security. Pages 6-6.
7. Emerging Trends in Vehicular Communications [Электронный ресурс http://www.ieee.org/index.html]