«Информационные технологии» № 10,2014.

В. Ю. Михайлов, д-р техн.наук, проф.,
В.Н. Гридин, д-р техн.наук, проф.
Московский авиационный институт (Национальный исследовательский университет)

План статьи журнал «Безопасное информационное взаимодействие. Проблемы и решения»:

1) Введение
2) Проблемы безопасности СИВ и их категории.
3)Уязвимости среды исполнения
4) Методы обнаружения ВПО.
5) Заключение

Тезисы статьи журнал «Безопасное информационное взаимодействие. Проблемы и решения»:

Способы проникновения в систему вредоносного программного обеспечения позволяет повысить эффективность решения задачи по сравнению с традиционным утилитарным стилем, использующим отдельные, слабосвязанные приемы, методы и средства обеспечения информационной безопасности.

В распоряжении разработчиков СИВ находится множество разнообразных методов, технологий и приемов противодействия возникающим угрозам. Однако в силу разных причин , они не в состоянии эффективно и своевременно парировать возникающие угрозы. Главной проблемой в категориях является недостаточное качество проекта со слабой адаптацией к изменяющимся условиям функционирования и потенциальным угрозам.

Функциональные особенности среды исполнения выражаются в виде широкого набора различного набора различного уровня услуг, предоставляемых ОС программам и реализованных на различных языках программирования. Основой компонентного проектирования является богатый выбор готовых компонентов и массовое их использование в разработках ПО.

Методы обнаружения ВПО разделяют на три типа в зависимости от используемой ими технологии обнаружения: обнаружение на этапе загрузки, обнаружение в процессе работы ОС и обнаружение при работе ОС под управлением гипервизора.

Одним из главных результатов проведенного анализа является вывод о целесообразности разработки единой методики и соответствующего набора инструментальных средств борьбы с ВПО.