УДК 681.142.2

ВЫЯВЛЕНИЕ АНОМАЛЬНЫХ СОСТОЯНИЙ В ОПЕРАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ НЕЙРОСЕТЕВОГО КЛАССИФИКАТОРА ПРОЦЕССОВ

М.Ю. Дьяконов
Научный руководитель – д.т.н., профессор С.С. Валеев
Уфимский государственный авиационный технический университет

Основная особенность современных встраиваемых систем (бортовые компьютеры летательных аппаратов, станки с ЧПУ, банкоматы и т.д.) - использование сложного по своей функциональности и, как следствие, содержащего немалое количество ошибок программного обеспечения (ПО), которым может воспользоваться злоумышленник. Таким образом, возникает вопрос о защищенности операционных систем (ОС) от ошибок в ПО, которые могут привести к краху системы, а в худшем случае – может произойти передача управления на программный код злоумышленника. Ситуация может еще более усложниться тем, что многие встраиваемые системы имеют средства сетевого мониторинга и управления.

Целью исследования является выбор архитектуры защищенной ОС, а также обзор методов анализа вредоносного программного кода. Использование сигнатурных методов анализа исполняемого кода программ не обеспечивает необходимого уровня защищенности от разрушающих программных средств с еще не известной сигнатурой, эвристические методы анализа часто оказываются малоэффективны. Наиболее эффективным представляется анализ поведения процессов во встроенных системах на основе «истории» поведения. Так как состав программного обеспечения подобных систем определен и ограничен, то статистические данные, полученные в результате наблюдения за конкретным процессом, можно считать обучающей выборкой для нейронной сети (НС). В качестве архитектуры ОС для замкнутых систем является целесообразным использование микроядерной ОС. Микроядро выполняет строго определенный минимальный набор функций, обеспечивающих согласованную работу остальных частей ОС. При этом программный код микроядра может быть верифицирован как «вручную» с использованием формальных методов, так и автоматизированным способом. Несколько меньшая производительность (на 7-10% ниже, чем монолитные ОС, такие как *UNIX*, *Linux*, *Windows XP*) компенсируется высокой степенью надежности и отказоустойчивости.

Результатом исследования является постановка задачи построения модуля, обеспечивающего классификацию состояний процессов в текущий момент времени по признаку аномальности последовательности их действий в системе (вызов системных функций, не характерных для данного процесса, нарушение последовательности создания процессов-потомков, выполнение процесса дольше обычного и т.п.). Модуль при этом должен быть внедрен в микроядро ОС. В качестве ОС с микроядерной архитектурой предлагается использовать ОС *Minix 3* (некоммерческая ОС с открытыми исходными кодами). В качестве классификатора состояний процессов предлагается использовать НС, обученную на примерах поведения процессов. НС может представлять многослойный персептрон или самоорганизующуюся сеть Кохонена.

Проект представляется на рассмотрение экспертному совету по отбору инновационных научных разработок в рамках программы У.М.Н.И.К. (участник молодёжного научно-инновационного конкурса) в связи с возможностью дальнейшей коммерциализации.