На правах рукописи

Коркин Игорь Юрьевич

МЕТОДИКА ОБНАРУЖЕНИЯ НЕЛЕГИТИМНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИСПОЛЬЗУЮЩЕГО ТЕХНОЛОГИЮ АППАРАТНОЙ ВИРТУАЛИЗАЦИИ

Специальность: 05.13.19 – методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание учёной степени
кандидата технических наук

Автор: 

Москва – 2011

Работа выполнена в Национальном исследовательском ядерном университете «МИФИ» (НИЯУ МИФИ)

Научный руководитель: кандидат технических наук, доцент
Петрова Тамара Васильевна

Официальные оппоненты: доктор технических наук, профессор
Зегжда Пётр Дмитриевич

кандидат физико-математических наук
Жуков Алексей Евгеньевич

Ведущая организация: Учреждение Российской академии наук
Институт системного программирования РАН

Защита состоится "9" февраля 2012 г. в 15 часов 00 минут на заседании диссертационного совета ДМ 212.130.08 при Национальном исследовательском ядерном университете «МИФИ» по адресу: 115409, г. Москва, Каширское шоссе, дом 31. Тел. для справок: +7 (499) 323-95-26, +7 (499) 324-73-34.

С диссертацией можно ознакомиться в библиотеке Национального исследовательского ядерного университета «МИФИ».

Отзывы в двух экземплярах, заверенные печатью организации, просьба направлять по адресу: 115409, г. Москва, Каширское шоссе, дом 31, диссертационные советы НИЯУ МИФИ, тел.: +7 (499) 323-95-26.

Автореферат разослан "23" декабря 2011 г.

Ученый секретарь диссертационного совета,
кандидат технических наук, доцент Горбатов В.С.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. На современном этапе развития информационных технологий и массового внедрения средств вычислительной техники в различные области и сферы деятельности человека задача обнаружения вредоносного программного обеспечения в электронно-вычислительных машинах (ЭВМ) приобретает всё более актуальное значение.

С 2006 г. компании Intel и AMD начали выпускать процессоры для персональных и серверных ЭВМ с поддержкой технологии аппаратной виртуализации. Программное обеспечение, использующее технологию аппаратной виртуализации (ПОАВ) работает в новом, более привилегированном, чем ОС, режиме. Кроме того, технология аппаратной виртуализации позволяет запускать во вложенном виде несколько различных образцов ПОАВ.

С одной стороны, ПОАВ, выполняющее функции монитора виртуальных машин (МВМ), повышает сервисные возможности ЭВМ и снижает её эксплуатационные расходы. Благодаря МВМ на одной ЭВМ может быть одновременно запущено несколько ОС в разных виртуальных машинах. МВМ контролирует совместное использование системных ресурсов, изоляцию виртуальных машин и их ключевые функции, в результате чего создаётся иллюзия, что гостевые ОС взаимодействуют непосредственно с аппаратным обеспечением (рис. 1).

Но, с другой стороны, можно негласно внедрить образец ПОАВ – программную закладку, которая обладает бесконтрольными возможностями. В результате появляются угрозы информационной безопасности, поскольку такая программная закладка позволяет активно добывать информацию и оказывать деструктивное информационное воздействие на ЭВМ различного назначения, в том числе на информационно-телекоммуникационные системы критически важных объектов.

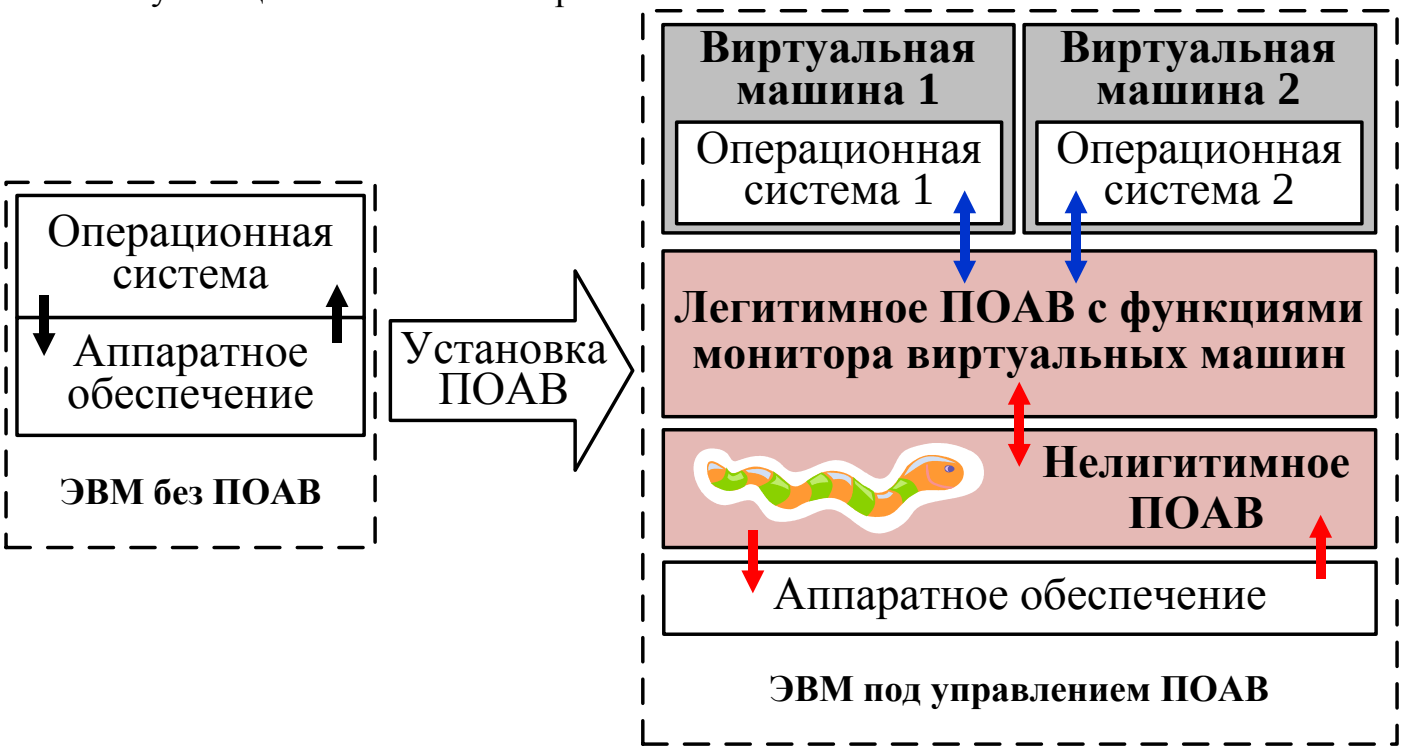


Рисунок 1 – Схема взаимодействия операционной системы с аппаратным обеспечением в случаях отсутствия (присутствия) двух образцов ПОАВ: легитимного с функциями МВМ и нелегитимного, находящихся во вложенном виде

Согласно статистике компании «Liliputing», в течение последних пяти лет наблюдается устойчивый рост продаж процессоров компании Intel для персональных ЭВМ с поддержкой технологии аппаратной виртуализации со 160 до 190 миллионов единиц в год, а общее число таких процессоров к 2012 году по прогнозу составит более миллиарда. Объём продаж процессоров компании AMD имеет схожую тенденцию.

В открытом доступе имеются два программных средства, «Blue Pill» и «Vitriol», реализованные в виде драйвера, которые устанавливают ПОАВ прозрачно для пользователя в ЭВМ, находящейся в эксплуатации.

Программное средство «Blue Pill» было разработано в 2006–2007 гг. исследователями Д. Рутковской (J. Rutkowska), А. Терешкиным (A. Tereshkin), Р. Войтчуком (R. Wojtczuk) и Р. Фаном (R. Fan) из компании Invisible Things Labs для демонстрации возможностей аппаратной виртуализации процессоров AMD.

Другим примером ПОАВ является программное средство «Vitriol», разработанное для процессоров Intel исследователем Дино А. Даи Зови (Dino A. Dai Zovi) из компании Matasano Security одновременно с Blue Pill в 2006 году. Однако, несмотря на широкую распространённость ПОАВ, штатные средства для их обнаружения отсутствуют, а опубликованные имеют существенные недостатки.

Обнаружением ПОАВ занимались как целые компании: Komoku, North Security Labs и др., так и отдельные специалисты: Ю. Булыгин, А. Луценко, К. Адамс (K. Adams), Э. Барбоса (E. Barbosa), Э. Филиол (E. Filiol), Х. Фритш (H. Fritsch), Н. Лоусон (N. Lawson), М. Майерс (M. Myers), Д. Медли (D. Medley), Т. Пташек (T. Ptacek), Р. Ридмюллер (R. Riedmuller), Д. Зу (D. Xu), З. Ванг (Z. Wang), и др. Анализ опубликованных подходов и реализованных продуктов по обнаружению ПОАВ выявил такие их недостатки, как отсутствие возможности выявить ПОАВ в случае его противодействия обнаружению, а также неудобство использования и тиражирования ряда средств.

В связи с широким распространением различного ПО, использующего технологию аппаратной виртуализации, особую опасность представляет нелегитимное ПОАВ, которое для своего сокрытия использует легитимное ПОАВ с помощью вложенной виртуализации (рис. 1). В открытых источниках отсутствуют сведения о наличии способов обнаружения нескольких вложенных образцов ПОАВ.

Таким образом, обнаружение нелегитимного программного обеспечения, использующего технологию аппаратной виртуализации, является актуальной задачей для обеспечения информационной безопасности новейших ЭВМ.

Существуют инструкции, при выполнении которых в ОС управление всегда передаётся ПОАВ. По результатам измерения длительности выполнения таких инструкций, например, с помощью процессорного счётчика тактов, можно принять решение о наличии ПОАВ, поскольку под управлением ПОАВ эта длительность на порядок превышает длительность в случае отсутствия ПОАВ. Однако нарушитель может использовать функциональные возможности ПОАВ по компрометации процессорного счётчика, в результате чего средняя длительность выполнения набора процессорных инструкций (трассы), безусловно перехватываемых ПОАВ, в случаях отсутствия и присутствия ПОАВ совпадёт. В таких ситуациях обнаружить ПОАВ не представляется возможным.

Автором предлагается методика обнаружения нелегитимного ПОАВ для ситуаций, когда противодействие выявлению со стороны ПОАВ осуществляется указанным

выше способом, а также путём временной выгрузки ПОАВ из памяти. Методика основана на измерении длительности выполнения набора процессорных инструкций (трассы), безусловно перехватываемых ПОАВ.

Тема работы удовлетворяет пунктам 3, 6, 13 и 14 паспорта специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Объект исследования. Операционная среда ЭВМ в случаях отсутствия (присутствия) одного образца (нескольких образцов) ПОАВ.

Предмет исследования. Статистические характеристики длительности выполнения инструкций процессора, измеряемой в операционной среде с использованием процессорного счётчика тактов.

Цель диссертационной работы. Разработка методики обнаружения нелегитимного программного обеспечения, использующего технологию аппаратной виртуализации в классе процессоров Intel и AMD.

Научная задача заключается в анализе статистических характеристик длительности выполнения трассы в случаях отсутствия (присутствия) ПОАВ и в синтезе критерия присутствия ПОАВ в условиях близости моментов первого порядка длительности выполнения трассы.

В рамках решения научной задачи необходимо:

- провести сравнительный анализ и классификацию существующих способов и средств обнаружения ПОАВ;
- построить модель нарушителя, провести анализ угроз и возможных способов противодействия обнаружению ПОАВ;
- исследовать длительность выполнения трассы в случаях отсутствия (присутствия) одного образца (нескольких образцов) ПОАВ, построить модели выполнения трассы и провести их анализ;
- разработать критерий присутствия образца ПОАВ;
- разработать методику обнаружения нелегитимного ПОАВ;
- разработать архитектуру и реализовать программное средство обнаружения ПОАВ.

Методы исследований. В работе используются методы теории графов, теории вероятностей и математической статистики.

Научная новизна работы состоит в следующем:

- представлены модели выполнения трассы в терминах теории графов, которые позволили выявить особенности статистических характеристик длительности выполнения трассы в случаях отсутствия (присутствия) одного образца (нескольких образцов) ПОАВ;
- синтезирован критерий присутствия образца ПОАВ на основе моментов 2-го и 4-го порядков, а также длины вариационного ряда длительности выполнения трассы;
- предложена методика обнаружения нелегитимного ПОАВ, позволяющая выявлять как один, так и несколько вложенных образцов ПОАВ.

Практическая значимость результатов работы заключается в следующем:

- разработанная методика позволяет обнаружить как один, так и несколько вложенных образцов ПОАВ, которые могут быть загружены из BIOS или из ОС в персональных или серверных ЭВМ;
- реализованное программное средство обнаружения ПОАВ позволяет принять

решение о наличии ПОАВ в условиях его противодействия выявлению.

Результаты работы представляют практическую ценность для реализации систем защиты от вредоносного программного обеспечения.

Достоверность результатов. Достоверность теоретических результатов обеспечивается корректным применением математического аппарата. Теоретические результаты согласуются с экспериментальными данными. Достоверность экспериментальных данных подкрепляется проведением опытов в полном соответствии с методическими рекомендациями. Допущения и ограничения, принятые в доказательствах утверждений, достаточно обоснованы.

Внедрение результатов исследований. Программное средство обнаружения ПОАВ использовано в составе системы обеспечения информационной безопасности в Государственном научном центре Российской Федерации федеральном государственном унитарном предприятии «Центральный научно-исследовательский институт химии и механики им. Д.И. Менделеева» (ГНЦ РФ ФГУП «ЦНИИХМ»).

Программное средство обнаружения было использовано как самостоятельная программа для контроля отсутствия нелегитимного ПОАВ при подготовке к вводу в эксплуатацию части парка ЭВМ федерального государственного унитарного предприятия «Научно-исследовательского института стандартизации и унификации» (ФГУП «НИИСУ»).

Теоретические и практические результаты, полученные в ходе выполнения диссертационной работы, использованы в учебном курсе «Безопасность операционных систем» кафедры «Криптология и дискретная математика» НИЯУ МИФИ для подготовки материалов лабораторных работ.

Публикации и апробация работы. Результаты диссертации изложены в 10 публикациях, 4 из которых опубликованы в рецензируемых журналах ВАК РФ. Результаты работы докладывались на конференциях и семинарах различного уровня:

- XVI, XVII, XVIII Всероссийская научно-практическая конференция «Проблемы информационной безопасности в системе высшей школы», г. Москва, 2009-2011 гг. (Инфофорум);
- XIV Международная телекоммуникационная конференция молодых ученых и студентов «Молодежь и наука», г. Москва, 2011 г.;
- XIX и XX Общероссийская научно-техническая конференция «Методы и технические средства обеспечения безопасности информации», г. Санкт-Петербург, 2010-2011 гг.;
- XV конференция «Телекоммуникации и новые информационные технологии в образовании», г. Москва, 2011 г.;
- семинары в Институте системного программирования Российской академии наук, г. Москва, 2011 (21 февраля 2011 года, 19 сентября 2011 года);
- семинар в Московском Государственном Техническом Университете им. Н.Э. Баумана, 2011 (1 марта 2011 года);
- XIII Международная конференция «РусКрипто» в 2011 году; представленная работа вышла в финал конкурса докладов.

Основные положения, выносимые на защиту:

- модели выполнения трассы в терминах теории графов для случаев отсутствия (присутствия) одного образца (нескольких образцов) ПОАВ;
- критерий присутствия образца ПОАВ на основе моментов 2-го и 4-го поряд-

ков, а также длины вариационного ряда длительности выполнения трассы;
- методика обнаружения нелегитимного ПОАВ;
- архитектура и программное средство обнаружения ПОАВ.

Структура работы. Работа состоит из введения, пяти глав, заключения, списка литературы, включающего 173 наименования, и 2 приложений. Текст диссертации изложен на 140 страницах, включая 42 рисунка и 10 таблиц.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы диссертации, представляется общий обзор предметной области, формулируются цель и задачи, предмет и объект исследования, описывается структура и логика диссертационной работы.

В **первой главе** описывается применение технологии аппаратной виртуализации для сокрытия ПО, приводится систематизированный обзор и даётся классификация описанных в литературе способов обнаружения ПОАВ, анализируются существующие средства обнаружения ПОАВ, уточняются методы и пути решения поставленной научной задачи.

На основе анализа способов обнаружения ПОАВ предложена их классификация (рис. 2), согласно которой все способы делятся на проактивные и сигнатурные.

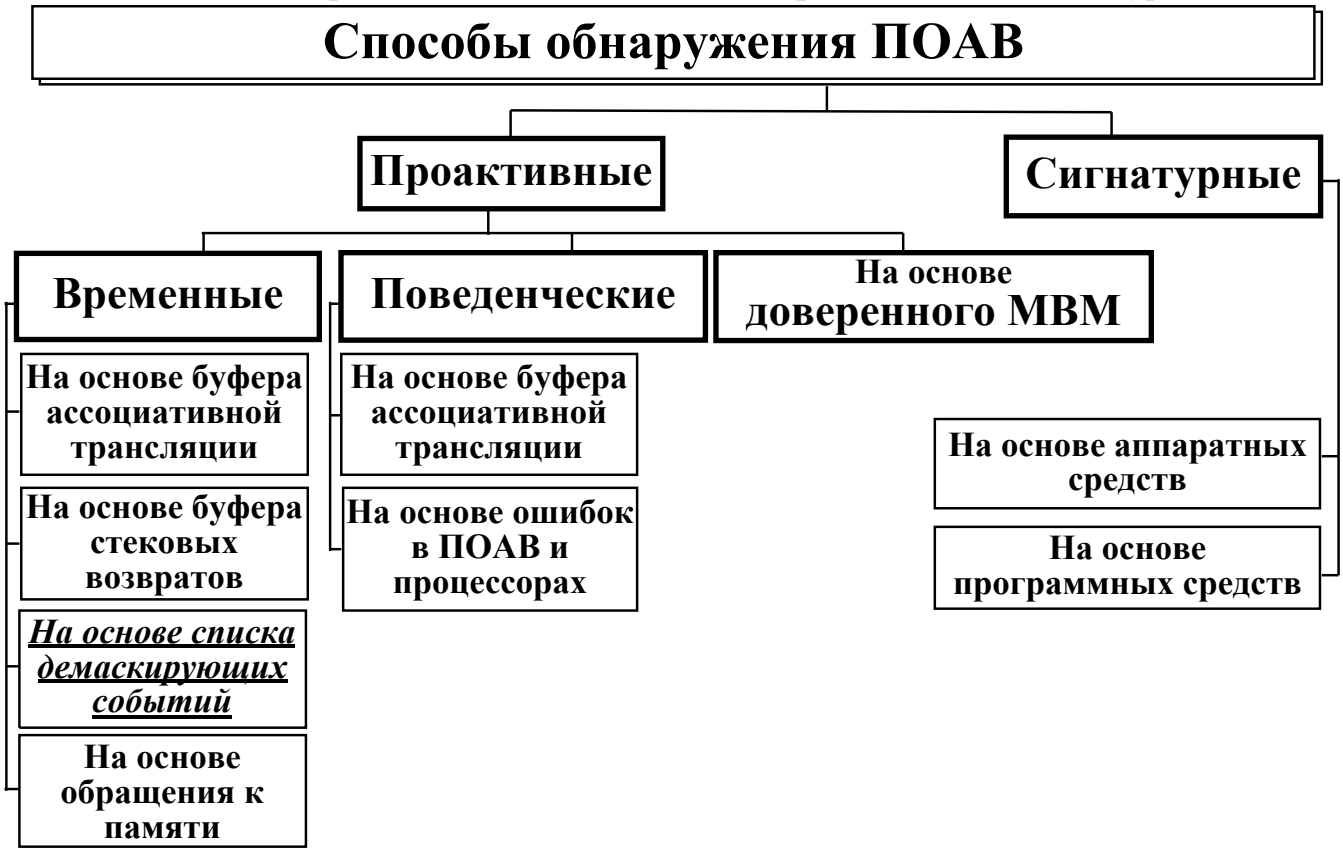


Рисунок 2 – Классификация способов обнаружения ПОАВ

Сигнатурные способы основаны на поиске в дампе памяти сигнатур ПОАВ и связанных с ним структур. Эти способы можно разделить по принципу получения дампа памяти: на основе аппаратных и программных средств. Способы на основе аппаратных средств неудобны в использовании и тиражировании, а на основе программных – уязвимы к противодействию ПОАВ.

В группу проактивных способов обнаружения входят такие, как временны́е, поведенческие способы и способ на основе доверенного МВМ.

Временны́е способы обнаружения основаны на том, что статистики времени об-

работки заданных событий гостевой ОС существенно зависят от того, имеется или нет ПОАВ: в присутствии ПОАВ длительность обработки событий значительно больше. Использование этой особенности позволяет сравнительно просто выявлять ПОАВ, однако только в тех случаях, если нарушителем не предприняты меры по сокрытию ПОАВ. В ситуациях, когда осуществляется целенаправленная компрометация процессорного счётчика тактов, либо временная выгрузка ПОАВ из памяти, известные временны́е способы не позволяют обнаружить ПОАВ.

Поведенческие способы обнаружения основаны на том, что результат выполнения определённых инструкций зависит от наличия ПОАВ. Эти способы используют особенности определённых моделей процессоров и версий ПОАВ. Адаптация поведенческих способов обнаружения на новые версии затруднительна, поскольку связана с проведением исследований и поиском уязвимостей.

Способ на основе доверенного МВМ заключается в использовании возможностей специально установленного легитимного МВМ, контролирующего работу операционной среды ЭВМ и препятствующего установке нелегитимного ПОАВ. Однако данный способ уязвим для атаки «человек-посередине» («Man-In-The-Middle»), поскольку нелегитимное ПОАВ может получить управление на более раннем этапе загрузки ЭВМ и скомпрометировать доверенный МВМ, загруженный позже.

Были проанализированы существующие средства обнаружения ПОАВ, результаты их сравнения представлены в табл. 1. Под не скрытым образцом ПОАВ подразумевается отсутствие в этом образце компонента, обеспечивающего противодействие обнаружению. Под скрытым образцом ПОАВ подразумевается наличие в этом образце такого компонента. В табл. 1 знаки «+» и «—» показывают наличие (отсутствие) указанной характеристики соответственно. Под удобством тиражирования понимается отсутствие в средстве обнаружения внешнего аппаратного компонента, необходимого на протяжении всего времени работы.

Таблица 1 – Сравнение существующих средств обнаружения ПОАВ

Наименование средства	**Способ обнаружения ПОАВ**	**Возможность обнаружения образца ПОАВ**		**Удобство использования и тиражирования**	**Обнаружение нескольких образцов ПОАВ**
		не скрытого	**скрытого**		
Hypersight Rootkit Detector (North Security Labs, 2007–2011)	На основе доверенного МВМ	+	—	+	—
«Красная пилюля» (Луценко А. 2010 г.)		+	—	+	—
DeepWatch (Булыгин Ю. 2008 г.)	Сигнатурный на основе аппаратных средств	+	+	—	—
Copilot (Komoku, 2008 г.)		+	+	—	—
Экспериментальные образцы ПО	Временные и поведенческие способы на основе буфера ассоциативной трансляции и др.	+	—	+	—

В отдельную группу отнесены различные экспериментальные образцы про-

граммного обеспечения, которые позволяют обнаруживать ПОАВ, но отсутствуют в открытом доступе. Сведения о них содержатся, например, в работах Т. Гарфинкеля (T. Garfinkel), К. Адамса (K. Adams), Э. Барбосы (E. Barbosa) и М. Майерса (M. Myers).

По результатам проведенного анализа было установлено, что существующие способы обнаружения ПОАВ обладают рядом недостатков:

- временны́е способы не позволяют выявить ПОАВ в случае использования компрометации счётчика тактов либо временной выгрузки из памяти;
- поведенческие способы не могут обнаруживать новые образцы ПОАВ и не работоспособны на новых моделях процессоров;
- способы на основе доверенного МВМ уязвимы к атаке «человек-посередине» («Man-In-The-Middle»);
- сигнатурные аппаратные средства неудобны в использовании и тиражировании, а программные средства – нестойки к противодействию ПОАВ;
- все опубликованные способы и средства обнаружения не позволяют обнаружить несколько вложенных образцов ПОАВ.

Предлагаемая в работе методика обнаружения нелегитимного ПОАВ лишена указанных недостатков.

Представляется перспективным для обнаружения ПОАВ использовать различия статистических характеристик длительности выполнения трассы в случаях отсутствия (присутствия) одного образца (нескольких образцов) ПОАВ. В качестве инструкций трассы предлагается использовать безусловно перехватываемые ПОАВ инструкции, выполнение которых всегда приводит к передаче управления образцу ПОАВ. Для измерения длительности выполнения трассы был выбран процессорный счётчик тактов. Этот подход относится к временны́м способам на основе списка демаскирующих событий (на рис. 2 он выделен курсивом и подчёркнут).

Во **второй главе** описаны теоретические предпосылки обнаружения ПОАВ. Проводится построение модели нарушителя и анализ угроз, описываются возможные способы сокрытия ПОАВ. Анализируется длительность выполнения трассы, и представляются модели выполнения трассы в терминах теории графов. Осуществляется проверка их адекватности экспериментально полученным данным и анализ построенных моделей. Предлагается критерий присутствия образца ПОАВ.

В данной работе рассматривается нарушитель, обладающий возможностью несанкционированно внедрять ПОАВ с помощью:

- установки драйвера операционной системы;
- модификации главной загрузочной записи жёсткого диска;
- внесения изменений в микропрограмму BIOS аппаратного обеспечения.

При этом учитывается, что реализованный нарушителем образец ПОАВ может противодействовать обнаружению посредством компрометации процессорного счётчика тактов, вре́менной деинсталляции из памяти, а также предотвращать получение копии дампа памяти, содержащей ПОАВ.

Нарушителями могут являться производители программного и аппаратного обеспечения, соответствующие 3 и 4 уровню предоставляемых возможностей, согласно РД ФСТЭК «Концепция защиты средств вычислительной техники и автоматизированных систем».

Производитель ПО может разрабатывать приложения, после инсталляции которых в операционную среду происходит установка ПОАВ. Производитель аппаратного

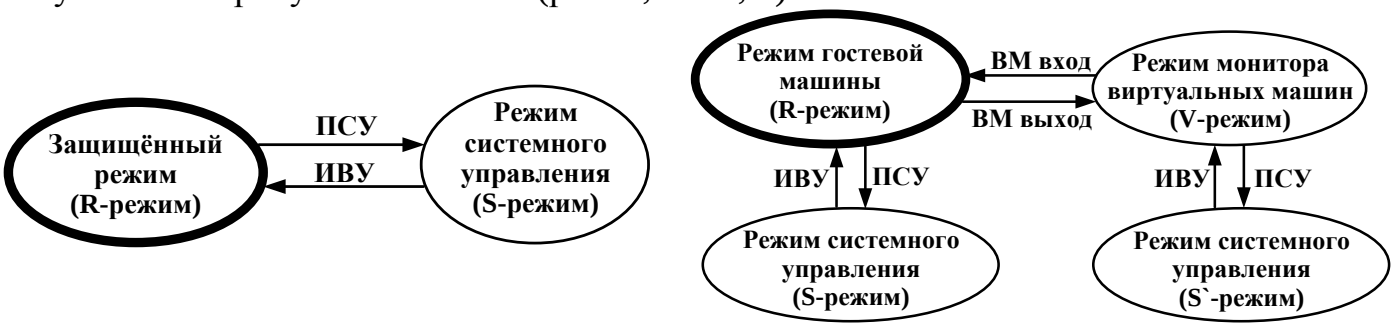
обеспечения (АО) может внедрять ПОАВ путём модификации микропрограммы BIOS.

Важно отметить, что образец ПОАВ может быть нелегально внедрён в ЭВМ через сеть Интернет, например, как вирус Duqu, при помощи специально сконструированного doc-файла, использующего уязвимость Microsoft Office Word.

В результате от нарушителей исходит целый ряд угроз информационной безопасности: нарушения конфиденциальности, целостности и доступности. Угроза нарушения конфиденциальности может быть снята, если ЭВМ находится в контуре, не связанном какими-либо телекоммуникационными соединениями с сетью Интернет. При этом утечка информации возможна посредством внешних носителей. Угрозы нарушения целостности и доступности заключаются в том, что ПОАВ может осуществлять деструктивное информационное воздействие как на данные, обрабатываемые ЭВМ, так и на ПО и АО, в том числе и на АО, подключаемое к ЭВМ, а также нарушать работу информационно-телекоммуникационных сетей и технологических процессов.

Для предотвращения описанных выше угроз необходимо периодически проверять ЭВМ на отсутствие образцов нелегитимного ПОАВ.

Для разработки методов обнаружения ПОАВ были построены схемы переключения между режимами работы процессора с поддержкой аппаратной виртуализации при выполнении набора безусловно перехватываемых ПОАВ инструкций для случаев отсутствия и присутствия ПОАВ (рис. 3, *а* и 3, *б*).



а *б*

Рисунок 3 – Схемы переключения между режимами работы процессора при выполнении набора безусловно перехватываемых ПОАВ инструкций в случаях отсутствия ПОАВ (*а*) и присутствия ПОАВ (*б*)

В случае отсутствия ПОАВ (рис. 3, *а*) процессор может находиться либо в защищённом режиме (R-режим), либо в режиме системного управления (S-режим).

В случае присутствия ПОАВ процессор может находиться не двух, а в трёх режимах (рис. 3, *б*). При этом R- и S-режим сохраняются, и добавляется режим монитора виртуальных машин (V-режим). На рис. 3, *б* S-режим разнесён для наглядности как S и S`. В этом случае R-режим называется режимом гостевой машины.

На основе схем переключения между режимами процессора построены соответствующие модели выполнения трассы в терминах теории графов для случаев отсутствия (присутствия) одного образца ПОАВ. В обоих случаях выполнение трассы осуществляется из ОС, находящейся в R-режиме. При этом были приняты допущения, что все рассматриваемые инструкции выполняются последовательно на одном вычислительном устройстве, длительность выполнения каждой инструкции одинакова и составляет k тактов, а ПОАВ для своего сокрытия компрометирует показания процессорного счётчика тактов на постоянную величину.

На рис. 4 приведена разработанная автором модель выполнения трассы в случае

отсутствия ПОАВ в виде ориентированного помеченного мультиграфа. Вершинами графа являются инструкции трассы, дуги соответствуют возможным переключениям между режимами процессора при выполнении инструкций. При выполнении каждой инструкции трассы процессор может перейти с некоторой вероятностью из R- в S-режим, на схеме это показано нижней дугой. В противном случае произойдёт переход по верхней дуге. Вероятность перехода в S-режим обозначим p, тогда вероятность прохода по верхней дуге – q, $q = 1 - p$.

На рис. 4 инструкции трассы обозначены символами U_i, $i = 1,..,n_0$, где n_0 – число инструкций в трассе, n_S – число инструкций в обработчике S-режима.

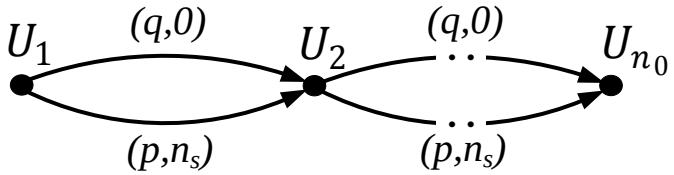


Рисунок 4 – Модель выполнения трассы в случае отсутствия ПОАВ

Длительность выполнения трассы t_{OT} из n_0 инструкций в случае отсутствия ПОАВ выражается формулой (1), где случайная величина m_{OT}, соответствующая числу переключений в S-режим, подчиняется закону биномиального распределения с параметрами n_0 и p

$$t_{OT} = (n_0 + m_{OT} * n_S) * k. \quad (1)$$

На рис. 5 приведена построенная автором модель выполнения трассы в случае присутствия ПОАВ, которая также представляет собой ориентированный помеченный мультиграф. При выполнении каждой инструкции трассы U_i управление передаётся в ПОАВ.

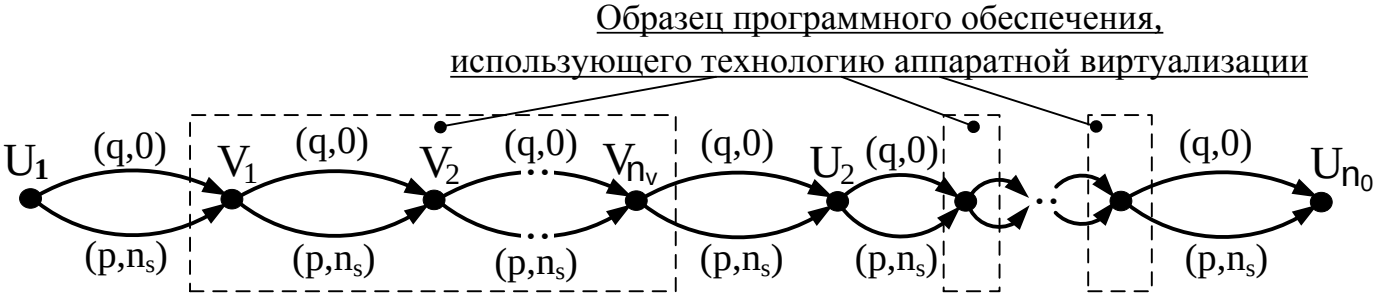


Рисунок 5 – Модель выполнения трассы в случае присутствия ПОАВ

На рис. 5 инструкции образца ПОАВ обозначены символами V_i, $i = 1,..,n_V$, где n_V число инструкций в этом образце. При выполнении любых инструкций, как трассы, так и ПОАВ, возможен переход в S-режим, что условно обозначено нижними дугами. В противном случае произойдёт переход по верхним дугам.

Длительность выполнения трассы $t_{ПР}$ из n_0 инструкций в случае присутствия ПОАВ с компрометацией счётчика тактов выражается формулой (2), где случайная величина $m_{ПР}$, соответствующая числу переключений в S-режим, подчиняется закону биномиального распределения с параметрами $(n_0 + n_0 * n_V)$ и p

$$t_{ПР} = (n_0 + n_0 * n_V + m_{ПР} * n_S + n_0 * \delta) * k, \quad (2)$$

где слагаемое $n_0 * n_V$ соответствует тому, что при выполнении каждой из n_0 инструкций трассы происходит переключение в V-режим (передача управления образцу ПОАВ), на что тратится дополнительное время. Слагаемое $n_0 * \delta$ соответствует тому, что при обработке каждой из n_0 инструкций трассы образец ПОАВ компрометирует

счётчик тактов путём прибавления к его значению величины δ, $\delta < 0$. В результате при многократных измерениях средняя длительность выполнения трассы в случаях отсутствия и присутствия ПОАВ может совпасть, и тогда по средней длительности выполнения трассы станет невозможным обнаружить присутствие образца ПОАВ.

Поскольку переменные m_{OT} и $m_{ПР}$ в формулах (1) и (2) являются случайными величинами, которые подчиняются биномиальному закону, то длительности трасс t_{OT} и $t_{ПР}$ являются целочисленными случайными величинами, значения которых будут распределяться случайным образом по некоторым уровням. По этой причине график длительности выполнения трассы t_{OT} и $t_{ПР}$ при повторных измерениях будет иметь слоистый характер. Из сравнения выражений для m_{OT} и $m_{ПР}$ можно заключить следующее. Поскольку в случаях отсутствия и присутствия ПОАВ значения вероятностей успеха (переключений в S-режим) p совпадают, а число испытаний в случае присутствия ПОАВ больше, чем в случае его отсутствия в $(n_V + 1)$ раз, то и количество уровней (слоёв) на графике длительности трассы в случае присутствия ПОАВ будет больше, чем в случае его отсутствия. По этой причине значения моментов 2-го и 4-го порядков, а также длин вариационных рядов длительности трассы в случае присутствия ПОАВ будут больше, чем в случае его отсутствия.

Выявленные особенности статистических характеристик длительности выполнения трассы в случаях отсутствия (присутствия) одного образца (нескольких образцов) ПОАВ после экспериментальной проверки использованы при разработке критерия присутствия ПОАВ.

Модели выполнения трассы могут быть также представлены в терминах теории марковских процессов. Однако предложенные модели в терминах теории графов более наглядны.

Экспериментальная проверка построенных моделей с использованием Критерия Колмогорова показала, что на 5 % уровне значимости модельные данные согласуются с экспериментальными данными. Было установлено также, что критерии согласия Хи-квадрат и Колмогорова-Смирнова не позволяют с достаточной вероятностью принимать решение о наличии ПОАВ, в связи с чем были предприняты меры по созданию критерия, лишённого этого недостатка.

Предлагается критерий присутствия образца ПОАВ, позволяющий различать массивы (выборки) длительности выполнения трассы в случаях отсутствия и присутствия ПОАВ.

Пусть параметры $n_0, n_S, n_V, \delta, k \in \mathbb{Z}$; $p \in \mathbb{R}$ – некоторые фиксированные значения. Пусть X_{OT} – множество значений, полученных при реализации t_{OT}, $X_{ПР}$ – множество значений, полученных при реализации $t_{ПР}$. Пусть генеральная совокупность X: $X = X_{OT} \cup X_{ПР}$. Пусть $\vec{x}_n = (x_1, .., x_n)$ – выборка объёма n из генеральной совокупности X.

Критерий присутствия образца ПОАВ на основе дисперсии.

Критическое множество (образец ПОАВ присутствует): $W = \{\vec{x}_n : \hat{\sigma}^2(\vec{x}_n) \geq d\}$, где $\hat{\sigma}^2$ – выборочная дисперсия, $d \in \mathbb{Z}$ – определяется экспериментально.

Принятие решения: если $\vec{x}_n \in W$, то образец ПОАВ присутствует, если $\vec{x}_n \notin W$, то образец ПОАВ отсутствует.

Критерий присутствия образца ПОАВ на основе момента 4–го порядка.

Критическое множество (образец ПОАВ присутствует): $W = \{\vec{x}_n : \hat{v}_2(\vec{x}_n) \geq \mu\}$, где $\hat{v}_2$ – выборочный центральный момент 4–го порядка, $\mu \in \mathbb{Z}$ – определяется экспе-

риментально.

Принятие решения: если $\vec{x}_n \in W$, то образец ПОАВ присутствует, если $\vec{x}_n \notin W$, то образец ПОАВ отсутствует.

Критерий присутствия образца ПОАВ на основе длины вариационного ряда.

Критическое множество (образец ПОАВ присутствует): $W = \{\vec{x}_n : \hat{l}(\vec{x}_n) \geq e\}$, где $\hat{l}$ – длина вариационного ряда, построенного по выборке, $e \in \mathbb{Z}$ – определяется экспериментально.

Принятие решения: если $\vec{x}_n \in W$, то образец ПОАВ присутствует, если $\vec{x}_n \notin W$, то образец ПОАВ отсутствует.

Пороговые значения d, μ, e, значения вероятностей ошибок первого и второго рода α и β, а также объём выборки n определяются экспериментально.

Предложенные критерии присутствия образца ПОАВ проверяются и уточняются в главе 3.

Третья глава посвящена экспериментальным исследованиям статистических характеристик длительности выполнения трассы на различных ЭВМ с целью проверки выдвинутых в главе 2 критериев и разработке на их основе методики обнаружения нелегитимного ПОАВ.

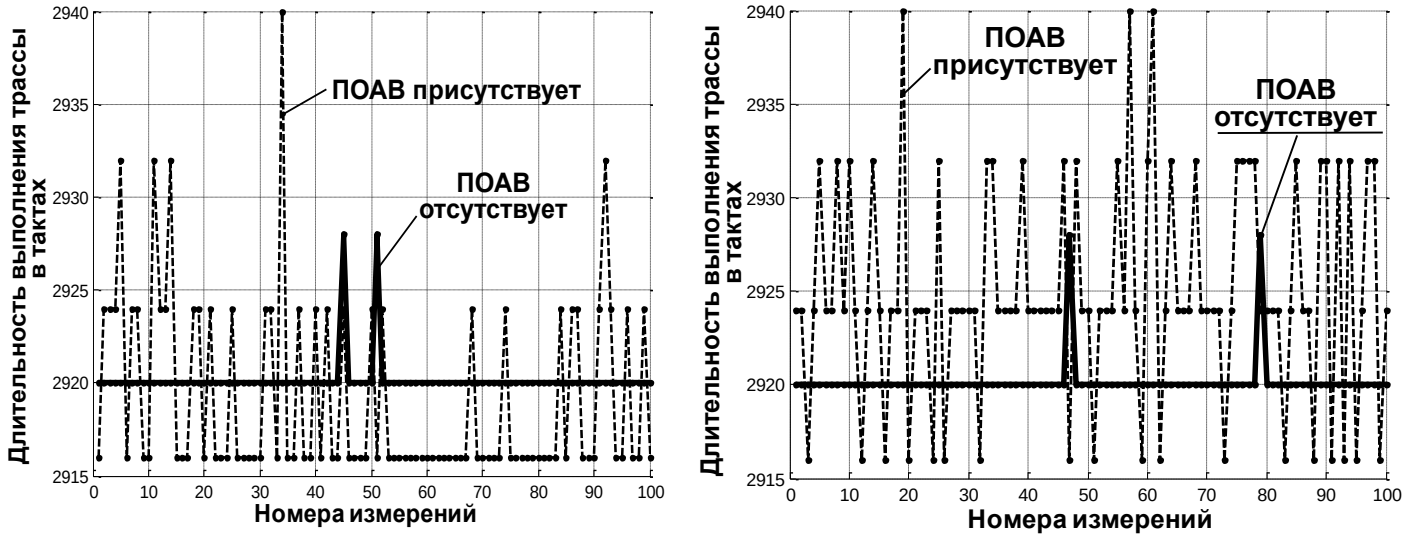
Излагается методика статистических измерений длительности выполнения трассы и организация проведения опытов с учётом недостаточной сходимости и воспроизводимости результатов испытаний.

Эксперименты осуществлялись по схеме однофакторных опытов. Варьируемым фактором была операционная среда ЭВМ с двумя качественными уровнями: в случаях отсутствия и присутствия ПОАВ. Результирующими признаками были различные статистики длительности выполнения трассы. Результатами опытов являлись матрицы размером 1000x10, содержащие данные измерений длительности выполнения трассы.

Экспериментально подтверждён вывод из анализа предложенных моделей выполнения трассы о том, что длительность выполнения трассы – это случайная величина, зависящая от наличия ПОАВ: в случае его присутствия значение и вариабельность длительности выполнения трассы в целом больше, чем без ПОАВ (рис. 6).

Подтверждено также, что образец ПОАВ путём искажения показаний процессорного счётчика тактов может уменьшать среднюю величину длительности трассы до значений, неотличимых от тех, что в случае отсутствия ПОАВ. Из этого следует, что по величине длительности выполнения трассы можно выявлять наличие образца ПОАВ только в тех случаях, когда компрометация показаний счётчика выполняется недостаточно тщательно.

Отсюда следует, что принимать решение о наличии ПОАВ на основе анализа только моментов 1-го порядка длительности трассы в условиях искажения счётчика тактов представляется не всегда возможным. В то время как использование моментов 2-го и 4-го порядков в сочетании с дополнительными критериями и предварительной обработкой данных позволяет обнаружить ПОАВ. Установлено также, что искажение показаний счётчика образца ПОАВ не уменьшает вариабельность длительности трассы, поэтому соответствующие показатели вариации длительности трассы могут быть использованы для обнаружения ПОАВ.



а *б*

Рисунок 6 – Фрагменты графиков длительности выполнения трассы в случаях отсутствия (присутствия) ПОАВ, полученные с использованием *а* – построенных моделей выполнения трассы и *б* – экспериментальных измерений

Проанализированы возможности различных подходов к обработке получаемого из опытов статистического материала. Установлено, что процесс измерения длительности выполнения трассы есть случайный процесс, отличающийся некоторой упорядоченностью: регистрируемая длительность выполнения трассы в цикле распределяется по фиксированным уровням случайным образом. Другая отличительная черта наблюдаемого процесса – его нестабильность: структура процесса изменяется не только от опыта к опыту, но и по ходу одного опыта (наблюдается скачкообразное изменение среднего значения). По этим причинам использовать методы теории случайных процессов для выявления идентификационных показателей для обнаружения ПОАВ оказалось невозможным.

По сравнению с рассмотренным выборочные методы математической статистики оказались приемлемыми для обработки получаемых данных, но при условии, что будут обеспечены достаточная сходимость и воспроизводимость результатов испытаний, а также будет преодолена проблема, связанная с перекрытием интервалов варьирования статистических характеристик длительности выполнения трассы в случаях отсутствия и присутствия ПОАВ. Достичь этого можно, если опыты выполнять сериями в течение нескольких дней, из получаемых данных удалять низкочастотные значения и учитывать разрывы, а показатели вариации использовать в последовательной комбинации.

В случаях отсутствия разрывов для каждого столбца опытных матриц определяли выборочные средние, длины статистических (вариационных) рядов длительности трассы отфильтрованных столбцов, моменты 2-го и 4-го порядков. При обнаружении разрывов эти статистики определялись для участков между точками разрывов, которые затем усреднялись с учётом весов, равных длине этих участков.

Указанные статистики рассчитывались как по столбцам матрицы с последующим усреднением, так и по всей матрице в целом путём переформатирования её в вектор. Благодаря таким мерам, участки перекрытия интервалов варьирования определяемых статистик в случаях отсутствия и присутствия ПОАВ стабилизировались и сужались настолько, что эти статистики становились пригодными для практического

использования.

На их основе разработаны различные показатели и методы для обнаружения ПОАВ. Главные из них – это комбинация выборочных методов с использованием таких показателей варьирования длительности выполнения трассы, как моменты 2-го и 4-го порядков, длина вариационных рядов, координаты центра тяжести полигона относительных частот. Методики определения пороговых значений этих показателей в основном схожи. Определение доверительного интервала используемых статистик осуществлялось методом Корнфельда.

Для иллюстрации в табл. 2 приведены пороговые значения последовательной комбинации таких показателей, как дисперсии и длина их вариационных рядов, полученных на различных ЭВМ.

Таблица 2 – Пороговые значения тест-статистик длительности трассы и их доверительная вероятность, полученные на различных ЭВМ

ЭВМ	Тест-статистика	Уровень фильтрации f	Пороговое значение		Вероятности ошибок	
			ОТ	ПР	I рода, α	II рода, β
1	$\bar{L}_f$	0	≤ 7	≥ 8	0.04	0
	$\bar{D}_f$	0	≤ 14	≥ 18	0.02	0
	$\bar{M}_f$	0.1	≤ 679	≥ 947	0.02	0
2	$\bar{L}_f$	0	≤ 11	≥ 12	0.1	0.06
	$\bar{D}_f$	0.2	≤ 100	≥ 101	0.08	0.1
	$\bar{M}_f$	0.2	≤ 168	≥ 13030	0.14	0.02
3	$\bar{L}_f$	0	≤ 34	≥ 241	0	0
	$\bar{D}_f$	0	≤ 216	≥ 5478	0	0
	$\bar{M}_f$	0.02	≤ 54	≥ 956	0	0

При этом были приняты следующие обозначения: $\bar{L}_f$ – выборочная средняя от средней длины вариационных рядов, $\bar{D}_f$ – выборочная средняя от выборочной дисперсии и $\bar{M}_f$ – выборочная средняя от выборочного момента 4–го порядка. Индекс f означает уровень фильтрации получаемых из опыта выборок длительности трассы. В первом столбце табл. 2 номерами обозначены модели процессоров обследованных ЭВМ: 1 – Intel Core 2 Duo E8200 с ОС Windows 7, 2 – Intel Core 2 Duo E6300 с ОС Windows 7, 3 – AMD Phenom X4 945 с ОС Windows Live CD XP (DDD). В первых двух ЭВМ использовался разработанный автором образец ПОАВ, реализованный в виде драйвера ОС, в 3-ем случае – специализированный ПОАВ, получающий управление при загрузке ЭВМ из BIOS. Для упомянутых и других ЭВМ получены аналогичные результаты для различных тест-статистик, разработанных на базе вариационных рядов выборочных медиан и координат центра тяжести полигонов частот, определяемых по столбцам опытных матриц длительности трассы.

Предложенные тест-статистики и их пороговые значения можно использовать в качестве индикационных показателей для обнаружения образцов ПОАВ.

Анализ показал, что выявить пороговые значения статистик длительности выполнения трассы в случаях вложенных образцов ПОАВ можно с помощью поэтапного адаптивного подхода: сначала следует определить пороговые значения статистик длительности трассы S_1 в случае отсутствия ПОАВ, затем в ЭВМ установить ПО со встроенным ПОАВ или иной легитимный ПОАВ, после чего по аналогичной методике

определить пороговые значения статистик этого режима S_2. Для наглядности на рис. 7 на оси пороговых значений идентификационных статистик указаны пороговые значения S_1,S_2,..,S_n совместно с разделяемыми ими режимами работы ЭВМ.

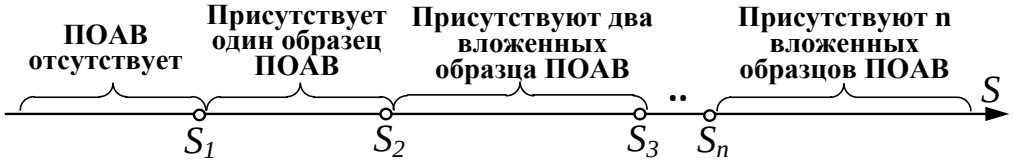


Рисунок 7 – Пороговые значения показателей в случае отсутствия (присутствия) одного образца (нескольких образцов) ПОАВ

Если при обнаружении ПОАВ окажется, что тестовые статистики $S_{тест} \leq S_1$, то ПОАВ отсутствует. При $S_1 < S_{тест} \leq S_2$ в ЭВМ только один, ранее легитимно установленный образец ПОАВ. Если $S_{тест} > S_2$, то принимается решение о присутствии двух вложенных образцов ПОАВ, один из которых нелегитимный.

Указанный порядок обнаружения ПОАВ сохраняется и при $S_{тест} > S_i$, где $i = 3,..,n$, при условии, что нелегальные образцы ПОАВ устанавливаются вне промежутков времени, когда определяются пороговые значения статистик для легитимных образцов ПОАВ. Альтернативным подходом к выявлению вложенных образцов ПОАВ может быть использование двух методов обнаружения одного ПОАВ: на основе длины вариационных рядов и механизмов кэширования.

Предлагается методика обнаружения нелегитимного ПОАВ, состоящая из двух этапов: предварительного и оперативного этапов, представленная в табл. 3.

Таблица 3 – Пошаговая методика обнаружения нелегитимного ПОАВ

Название этапа	**Содержание шагов**
Предварительный	1. Аппаратным образом записать доверенную микропрограмму в BIOS. 2. Установить операционную систему. 3. Получить пороговые значения для обнаружения ПОАВ с помощью соответствующего алгоритма.
Оперативный, на стадии эксплуатации ЭВМ	4. Начать проверку ЭВМ на отсутствие ПОАВ с помощью алгоритма обнаружения. 5. Последовательно установить дополнительное ПО (MS Office и др.). 6. Следить за сообщениями об обнаружении ПОАВ. 7. Для адаптации средства обнаружения к легитимному образцу ПОАВ выполнить шаг 3.

Программно реализованы 3-й и 4-й шаги методики.

В **четвертой главе** предлагается архитектура и описывается реализация программного средства обнаружения ПОАВ и его подсистем. Излагается порядок настройки и эксплуатации разработанного средства.

Сформулированы требования к программному средству обнаружения ПОАВ. Средство обнаружения должно:

- обеспечивать получение пороговых значений для обнаружения ПОАВ;
- обнаруживать как один, так и несколько вложенных образцов ПОАВ;
- обеспечивать возможность ручной обработки регистрируемых данных.

Для удовлетворения указанным требованиям программное средство обнаружения должно состоять из подсистем выработки пороговых значений, имитации дейст-

вий нарушителя и выявления образцов ПОАВ.

Архитектура программного средства обнаружения ПОАВ представлена на рис. 8.

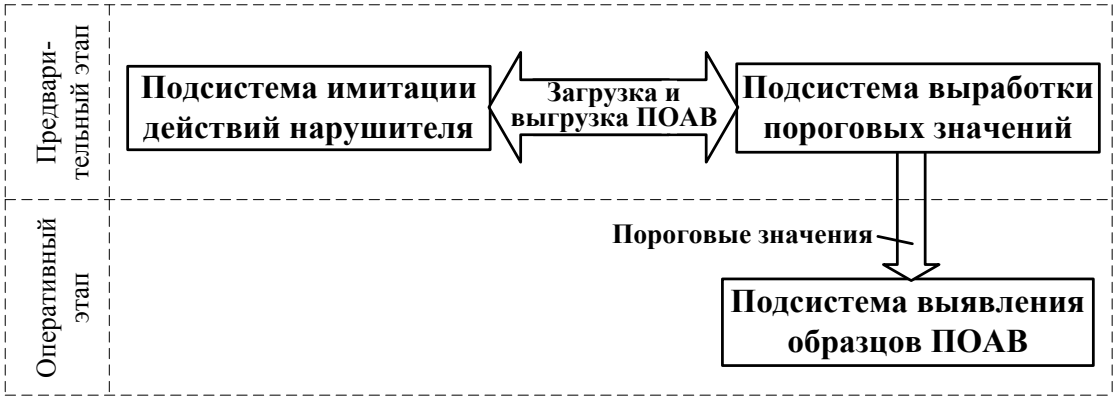


Рисунок 8 – Архитектура программного средства обнаружения ПОАВ

Для обнаружения ПОАВ необходимо выполнить два этапа: предварительный и оперативный. На предварительном этапе осуществляется совместная работа подсистем выработки пороговых значений и имитации действий нарушителя. Этот этап проводится при подготовке к вводу ЭВМ в эксплуатацию. В результате предварительного этапа вырабатываются пороговые значения статистик для обнаружения ПОАВ. Предварительный этап повторяется после установки каждого ПО, содержащего ПОАВ. Для обнаружения нескольких вложенных образцов ПОАВ используется поэтапный адаптивный подход, посредством которого создаются пороговые значения для каждого из вложенных образцов ПОАВ. После ввода ЭВМ в эксплуатацию реализуется оперативный этап, для чего используется подсистема выявления образцов ПОАВ.

Подсистема выработки пороговых значений обеспечивает регистрацию опытных данных для случаев отсутствия и присутствия ПОАВ, их обработку и получение пороговых значений. Архитектура подсистемы представлена на рис. 9.

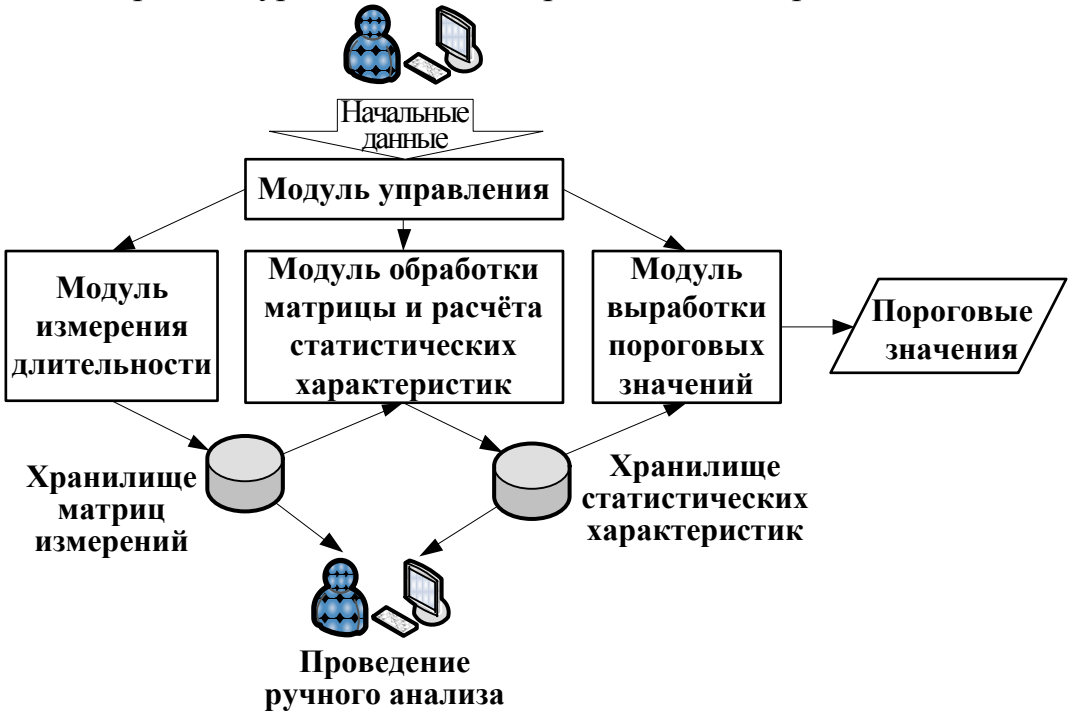


Рисунок 9 – Архитектура подсистемы выработки пороговых значений

После запуска подсистемы модуль управления создаёт для каждого из трёх мо-

дулей отдельные задания. Составленное задание передаётся в модуль измерения длительности, который осуществляет получение и сохранение матрицы измерений длительности выполнения трассы в хранилище. Модуль обработки матрицы и расчёта статистических характеристик извлекает матрицу и рассчитывает статистические характеристики для различных уровней фильтрации, которые сохраняются в соответствующем хранилище. Модуль выработки пороговых значений в соответствии с полученным заданием извлекает из хранилища статистические характеристики, осуществляет их анализ и выбор подходящих пороговых значений, которые являются результатом работы подсистемы. Модули подсистемы выработки пороговых значений реализованы с использованием двух языков программирования C++ и Matlab. Подсистема имитации действий нарушителя состоит из модулей управления и образца ПОАВ, позволяя воспроизводить поведение образца ПОАВ в условиях его противодействия обнаружению, компрометируя процессорный счётчик тактов. Подсистема имитации действий нарушителя реализована на языке программирования C++.

Подсистема выявления образцов ПОАВ (рис. 10) с учётом наработок предыдущих подсистем обеспечивает обнаружение ПОАВ в непрерывном режиме. Работа данной подсистемы осуществляется аналогично подсистеме выработки пороговых значений за исключением того, что модуль обработки матрицы и расчёта статистических характеристик рассчитывает лишь указанные в задании статистические характеристики и только для определённых уровней фильтрации. Модуль принятия решения в соответствии с заданием и полученными статистическими характеристиками принимает решение о наличии образцов ПОАВ и об их числе. Вывод отчёта пользователю осуществляется с использованием графической формы приложения. Подсистема выявления образцов ПОАВ реализована на языке программирования C++.

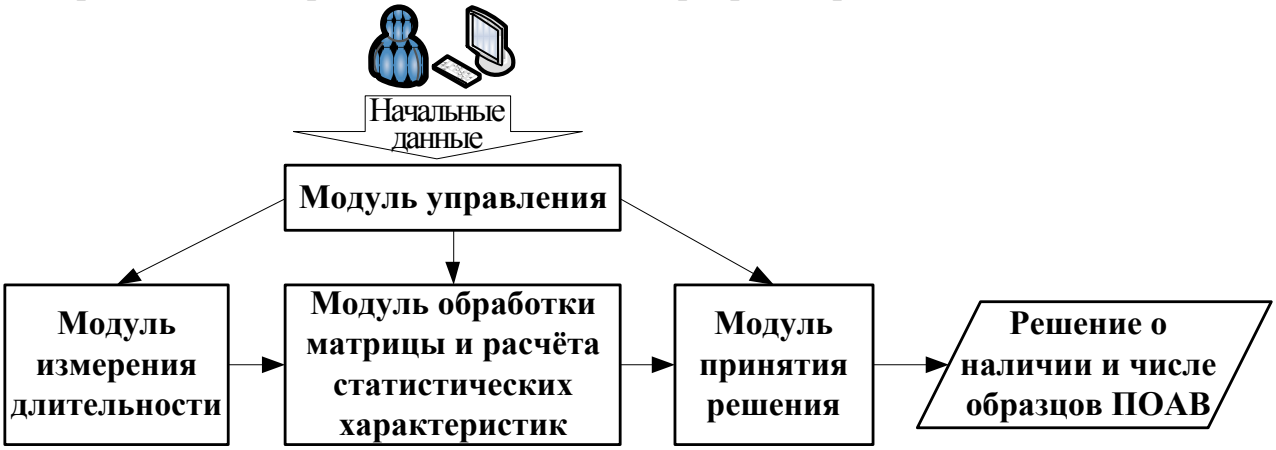


Рисунок 10 – Архитектура подсистемы выявления образцов ПОАВ

Разработанное программное средство позволяет вырабатывать пороговые значения для различных ЭВМ и осуществлять обнаружение ПОАВ в непрерывном режиме.

В **пятой главе** приводятся примеры практического применения результатов работы для решения конкретных прикладных задач в трёх проектах.

Реализованное программное средство обнаружения ПОАВ применяется в составе системы обеспечения информационной безопасности для проверки отсутствия ПОАВ в части парка ЭВМ ГНЦ РФ ФГУП «ЦНИИХМ» (ФСТЭК России).

Компьютерная сеть ФГУП «ЦНИИХМ» состоит из двух контуров – непосредственно подключённого к сети Интернет с помощью сетевых коммуникаций и контура, не имеющего такого доступа, онлайн и оффлайн соответственно. Информационное

взаимодействие между контурами осуществляется с помощью внешних носителей. Специфика данных, обрабатываемых на компьютерах оффлайн контура, не позволяет подключать их к сети Интернет и с помощью штатных средств осуществлять установку обновлений ПО, поэтому компьютеры этого контура не защищены от угроз, использующие даже известные уязвимости. Разработанная сотрудниками института система обеспечения информационной безопасности (СОИБ) позволяет повышать защищённость компьютеров, находящихся в оффлайн контуре, путём инсталляции актуальных обновлений для прикладного и системного ПО. Внедрение разработанного программного средства осуществлялось путём включения его подсистемы выявления ПОАВ в состав СОИБ. Была проведена адаптация программного средства для работы в ЭВМ с процессорами Intel Xeon X5600 и ОС Windows 7 Professional, заключающаяся в получении пороговых значений для случая присутствия (отсутствия) авторского образца ПОАВ. Была проведена успешная проверка части ЭВМ, продемонстрировавшая работоспособность программного средства обнаружения. В результате проверки не было выявлено нелегальных образцов ПОАВ.

Задачей второго проекта было выявление новейших программных средств негласного съёма информации, использующих технологию аппаратной виртуализации, на компьютерах ФГУП «НИИСУ» (Минпромторг России). При этом реализованное программное средство обнаружения ПОАВ использовалось как самостоятельная программа для проверки ряда компьютеров института, вводимых в эксплуатацию. Процесс внедрения можно условно разделить на три этапа. На первом этапе осуществлялась запись новой микропрограммы в BIOS с использованием аппаратного программатора «ТРИТОН», что гарантировало отсутствие ПОАВ в BIOS. На втором этапе осуществлялась установка ОС Windows XP, после чего с использованием подсистем выработки пороговых значений и имитации действий нарушителя были получены значения статистик для обнаружения ПОАВ. На третьем этапе производилась установка дополнительного ПО, включающего в себя пакет программ Microsoft Office и интегрированную среду разработки программного обеспечения Microsoft Visual Studio, при этом в непрерывном режиме осуществлялась проверка ЭВМ на отсутствие ПОАВ. В результате была проведена успешная подготовка к эксплуатации ряда компьютеров, продемонстрировавшая работоспособность программного средства обнаружения.

В третьем проекте результаты диссертационной работы были внедрены в учебный курс «Безопасность операционных систем» кафедры «Криптология и дискретная математика» НИЯУ МИФИ. Существующий курс был расширен теоретическим описанием технологии аппаратной виртуализации и демонстрацией технических возможностей разработанной подсистемы имитации действий нарушителя. Расширенный курс в отличие от существующих иностранных курсов Г. Хоглунда «Offensive Aspects of Rootkit Technology» и Д. Рутковской «Understanding Stealth Malware Training» содержит анализ способов обнаружения ПОАВ, анализ статистических характеристик длительности выполнения трассы для случаев отсутствия и присутствия ПОАВ и методику обнаружения нелегитимного программного обеспечения, использующего технологию аппаратной виртуализации.

В **заключении** приведены основные результаты диссертационной работы и рассмотрены пути дальнейшего развития темы исследования.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ РАБОТЫ

1. Проведен анализ существующих способов обнаружения программного обеспечения, использующего технологию аппаратной виртуализации. Обоснована необходимость создания нового подхода к обнаружению ПОАВ, в том числе вложенных образцов.
2. Построена модель нарушителя, позволившая проанализировать возможные угрозы обрабатываемой в ЭВМ информации.
3. Представлены модели выполнения трассы для процессоров с поддержкой аппаратной виртуализации в случаях отсутствия (присутствия) одного образца (нескольких образцов) ПОАВ в терминах теории графов. Предложенные модели позволили выявить закономерности длительности выполнения трассы в этих условиях.
4. Предложен критерий присутствия образца ПОАВ. Получен теоретически и подтверждён экспериментально вывод о том, что статистические характеристики длительности выполнения трассы зависят от наличия ПОАВ. В случае присутствия ПОАВ значение и вариабельность длительности выполнения трассы существенно больше, чем в случае его отсутствия.
5. Разработана методика обнаружения нелегитимного ПОАВ, состоящая из двух этапов – предварительного и оперативного. На предварительном этапе осуществляется получение пороговых значений статистик. На оперативном этапе на основе полученных статистик осуществляется обнаружение ПОАВ в непрерывном режиме.
6. Построена архитектура и разработано программное средство обнаружения программного обеспечения, использующего технологию аппаратной виртуализации.
7. Разработанное программное средство обнаружения ПОАВ применено в составе системы обеспечения информационной безопасности для контроля отсутствия ПОАВ в ряде ЭВМ парка ГНЦ РФ ФГУП «ЦНИИХМ», что позволило проконтролировать отсутствие нелегальных образцов ПОАВ.
8. Реализованное программное средство обнаружения ПОАВ было использовано при подготовке к вводу в эксплуатацию ряда ЭВМ парка ФГУП «НИИСУ», что позволило проконтролировать отсутствие нелегальных образцов ПОАВ.
9. Проведенный анализ способов обнаружения ПОАВ и статистических характеристик длительности выполнения трассы для случаев отсутствия и присутствия ПОАВ был использован при создании лабораторных работ учебного курса «Безопасность операционных систем» кафедры «Криптология и дискретная математика» НИЯУ МИФИ.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. **Коркин И.Ю. Технологии сокрытия вредоносных программ и новые способы противодействия им // Безопасность Информационных Технологий. 2009, №4, – с. 43-46**
2. Коркин И.Ю. Способ обнаружения скрытых процессов в ОС Windows. В сб. научных трудов 16-й Всероссийской конференции «Проблемы информационной безопасности в системе высшей школы». – М.:, 2009, – с. 111-112
3. Коркин И.Ю., Петрова Т.В., Тихонов А.Ю. Метод обнаружения аппаратной виртуализации в компьютерных системах. В сб. научных трудов 17-й Всероссийской конференции «Проблемы информационной безопасности в системе высшей школы». М.:, 2010, – с. 114-115
4. Коркин И.Ю. Критерий обнаружения монитора виртуальных машин в ком-

пьютерных системах. В сб. материалов XIX Общероссийской научно-технической конференции «Методы и Технические Средства Обеспечения Безопасности Информации». СПб.:, 2010, – с. 113-114
5. Коркин И.Ю., Петрова Т.В., Тихонов А.Ю. Новый подход к выявлению аппаратной виртуализации в компьютерных системах. XIV Международная телекоммуникационная конференция студентов и молодых учёных «Молодёжь и наука». Тезисы докладов. Ч. 3. М.:,НИЯУ МИФИ, 2010. – с. 241-242
6. **Коркин И.Ю. Метод выявления аппаратной виртуализации в компьютерных системах на основе механизма кэширования // Безопасность Информационных Технологий. 2011, №1. – с. 101-103**
7. Коркин И.Ю. Статистическая идентификация режимов работы компьютерных систем. Сб. науч. тр.. XV конференция «Телекоммуникации и новые информационные технологии в образовании». М.:,НИЯУ МИФИ, 2011. – с. 163-165
8. **Коркин И.Ю. Выявление вложенных мониторов виртуальных машин // Системы высокой доступности. 2011, №2, т.6 – с. 76-77**
9. Коркин И.Ю. Обнаружение вложенных мониторов виртуальных машин методами математической статистики. В сб. материалов XX Общероссийской научно-технической конференции «Методы и Технические Средства Обеспечения Безопасности Информации». СПб.:, 2011, – с. 146-147
10. **Коркин И.Ю. Новые статистические показатели и методы для обнаружения мониторов виртуальных машин в компьютерных системах // Естественные и технические науки. 2011, № 4. – с. 498-502**

Личный вклад автора в работах, написанных в соавторстве, состоит в следующем: [3] – проведение сравнительного анализа способов обнаружения ПОАВ; [5] – разработка программного средства обнаружения ПОАВ на основе механизма кэширования.

КОРКИН ИГОРЬ ЮРЬЕВИЧ

МЕТОДИКА ОБНАРУЖЕНИЯ НЕЛЕГИТИМНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИСПОЛЬЗУЮЩЕГО ТЕХНОЛОГИЮ АППАРАТНОЙ ВИРТУАЛИЗАЦИИ

Подписано в печать 19.12.2011. Формат 60 × 84 $^{1}/_{16}$.
Усл. печ. л. 1,0. Уч.-изд. л. 1,0. Тираж 100 экз. Заказ № 37

Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ)

115409, Москва, Каширское шоссе, 31