На правах рукописи

ДЬЯКОНОВ Максим Юрьевич

НЕЙРОСЕТЕВАЯ СИСТЕМА ОБНАРУЖЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ ВЫЧИСЛИТЕЛЬНЫХ ПРОЦЕССОВ МИКРОЯДЕРНЫХ ОПЕРАЦИОННЫХ СИСТЕМ

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

АВТОРЕФЕРАТ
диссертации на соискание ученой степени кандидата технических наук

Уфа – 2010

Работа выполнена
на кафедре вычислительной техники и защиты информации
и кафедре информатики
ГОУ ВПО Уфимский государственный авиационный
технический университет

Научный руководитель	д-р техн. наук, проф. **Валеев Сагит Сабитович** каф. информатики Уфимский государственный авиационный технический университет
Официальные оппоненты	д-р техн. наук, проф. **Миронов Валерий Викторович** каф. автоматизированных систем управления Уфимский государственный авиационный технический университет
	канд. техн. наук **Саляхов Алмаз Фанилович** ООО «Лукойл-Информ» филиал в г. Уфа
Ведущая организация	**ГОУ ВПО «Челябинский государственный университет»**

Защита состоится 29 декабря 2010 г. в 10 часов
на заседании диссертационного совета Д-212.288.07
при Уфимском государственном авиационном техническом университете
по адресу: 450000, Уфа-центр, ул. К. Маркса, 12.

С диссертацией можно ознакомиться в библиотеке университета.
Автореферат разослан «24» ноября 2010 г.

Ученый секретарь
диссертационного совета
д-р техн. наук, проф. **С. С. Валеев**

Общая характеристика работы

Актуальность темы

Основной задачей исследований в области защиты информации является совершенствование известных и разработка новых методов, алгоритмов обеспечения безопасности информации в процессе ее сбора, хранения, обработки, передачи и распространения. В документе «Приоритетные проблемы научных исследований в области обеспечения информационной безопасности Российской Федерации» приведен список приоритетных направлений научных исследований, в числе которых под номером 63 указано следующее: «Исследование проблем обнаружения компьютерных атак на информационно-телекоммуникационные системы и противодействия компьютерному нападению». Статистика по числу инцидентов в области информационной безопасности, приводимая в различных Интернет-изданиях, показывает, что многие методы проведения атак на информационные системы (ИС) в некоторых случаях не удается распознать с использованием существующих средств защиты информации. Этот недостаток может привести к нарушению конфиденциальности, целостности или доступности информации. Возникают задачи, связанные с созданием методов и алгоритмов, способных достоверно распознавать новые типы атак и предупреждать их распространение в ИС.

Одним из уязвимых мест ИС является программное обеспечение. Большинство атак направлено на использование существующих известных уязвимостей прикладного и системного программного обеспечения. Существующие средства защиты информации достаточно эффективно справляются с обнаружением известных типов атак на основе их сигнатур. В то же время существует иной класс атак, для которых сигнатуры не известны. Обнаружение и предотвращение атак с неизвестными сигнатурами наиболее сложная и нетривиальная задача. К сложному по архитектуре и реализации системному программному обеспечению относятся операционные системы.

Существует множество классификаций типов операционных систем и областей их практического применения. Как показал анализ, выделяют три типа операционных систем: монолитные, микроядерные и гибридные. Монолитные и гибридные архитектуры в основном применяются в серверных многопользовательских системах и персональных компьютерах общего назначения. К основным особенностям указанных архитектур следует отнести высокую сложность реализации и подверженность к нестабильной работе в случае нарушения работоспособности отдельных программ, входящих в состав операционной системы (драйверы устройств, подгружаемые модули ядра и т.п.). К достоинствам относится их универсальность. Микроядерные операционные системы в большинстве случаев имеют практическую применимость в классе встраиваемых систем. Под встроенными системами понимаются механические или электронные устройства, управляемые вычислителем, встроенным в само устройство. Примеры встраиваемых систем: автоматизированные системы управления технологическими процессами, технические системы защиты информации, бортовые компьютеры летательных аппаратов,

SCADA-системы, телекоммуникационные устройства, платежные терминалы и т.п. Область применения встраиваемых систем расширяется с каждым годом. В некоторых случаях возможна интеграция их в сетевые приложения. С точки зрения информационной безопасности во встраиваемых системах применение распространенных средств защиты информации оказывается малоэффективным ввиду специфики встраиваемых систем, области их приложений и ограниченной номенклатуры используемых программных средств. В результате анализа выяснилось, что известные типы атак также могут нарушать безопасность микроядерных операционных систем встраиваемых устройств. В данной работе рассматривается задача обеспечения безопасности микроядерных операционных систем на примере встраиваемых систем, обладающими внешними интерфейсами взаимодействия.

Вопросам обнаружения атак на различные компоненты ИС посвящены исследования В. И. Васильева, Д. Денинг, А. В. Лукацкого, А. В. Мельникова, Ю. В. Романец, С. Форестер, В. Ф. Шаньгина, и др. Несмотря на это область исследования безопасности встраиваемых систем недостаточно проработана: к нерешенным задачам можно отнести анализ в реальном времени аномального поведения вычислительных процессов микроядерных операционных систем. В результате анализа выяснилось, также, что при разработке систем обнаружения атак в недостаточной мере используются потенциал нейросетевых классификаторов. Таким образом, задача разработки эффективных методов и алгоритмов обнаружения атак на ИС с микроядерными операционными системами является актуальной.

Цель и задачи исследования

Объектом исследования в работе является обеспечение основных свойств информационной безопасности вычислительных процессов в микроядерной операционной системе (МОС). В качестве **предмета** исследования рассматриваются методы и алгоритмы распознавания аномального поведения вычислительных процессов на основе технологий искусственных нейронных сетей.

Целью исследования является повышение защищенности микроядерных операционных систем на основе методов и алгоритмов распознавания аномального поведения процессов.

Для достижения поставленной цели в работе были сформулированы следующие задачи:

1. Разработка принципов построения системы обнаружения аномального поведения вычислительных процессов микроядерных операционных систем.

2. Разработка модели вычислительного процесса в микроядерной операционной системе на основе сбора статистики штатного поведения вычислительных процессов, необходимой для решения задачи распознавания аномального поведения вычислительных процессов и выявления новых типов атак с неизвестными сигнатурами.

3. Разработка метода и алгоритмов для нейросетевой системы обна-

ружения аномального поведения вычислительных процессов в микроядерной операционной системе.

4. Разработка исследовательского прототипа нейросетевой системы обнаружения аномального поведения вычислительных процессов в микроядерной операционной системе, реализующей функции сбора статистической информации о поведении вычислительных процессов и классификацию состояний на основе самообучаемой нейронной сети.

5. Оценка эффективности предложенного метода и алгоритмов на базе микроядерной операционной системы.

Методы исследования

При работе над диссертацией использовались: методология защиты информации, методы системного анализа, теория множеств, теория вероятности, теория моделирования дискретных систем, теория нейронных сетей. Для оценки эффективности предлагаемых решений использовались методы математического и имитационного моделирования.

Основные научные результаты, полученные автором и выносимые на защиту

1. Принципы построения системы обнаружения аномального поведения вычислительных процессов в микроядерной операционной системе, для осуществления сбора статистической информации о поведении системных процессов на уровне микроядра и распознавания класса поведения на основе нейросетевого классификатора.

2. Модель вычислительного процесса в микроядерной операционной системе на основе сбора статистики штатного поведения вычислительных процессов.

3. Метод и алгоритмы обнаружения аномального поведения вычислительных процессов на основе иерархической структуры микроядерной операционной системы, модели вычислительного процесса и нейронных сетей.

4. Методика обнаружения аномального поведения вычислительных процессов в микроядерной операционной системе на базе нейронной сети.

Обоснованность и достоверность результатов диссертации

Обоснованность результатов, полученных в диссертационной работе, базируется на использовании апробированных научных положений и методов исследования, корректным применением математического аппарата, согласованности новых результатов с известными теоретическим положениями.

Достоверность полученных теоретических положений и выводов подтверждается результатами имитационного моделирования, апробации и промышленного внедрения предложенных алгоритмов обнаружения аномального поведения процессов.

Практическая ценность работы

1. Обеспечивается повышение эффективности решения задач защиты информации в микроядерной операционной системе.

2. Разработан алгоритм обнаружения аномального поведения вычислительных процессов в микроядерной операционной системе на базе нейронной сети, позволяющий решать задачи обеспечения информационной безопасности.

3. Результаты исследования приняты к внедрению в виде программного прототипа для анализа поведения вычислительных процессов телекоммуникационного оборудования в Уфимский филиал ОАО «Вымпелком» (Билайн).

Связь исследований с научными программами

Исследования выполнялись с 2006 г. по 2010 г. на кафедре вычислительной техники и защиты информации Уфимского государственного авиационного технического университета, в том числе в рамках гранта РФФИ № 07-08-00386 «Методы и алгоритмы интеллектуального управления информационной безопасностью высшего учебного заведения» (2007-2009 гг.)

Апробация работы

Основные научные и практические результаты диссертационной работы докладывались и обсуждались на следующих конференциях:

- 2-я региональная зимняя школа-семинар аспирантов и молодых ученых. Интеллектуальные системы обработки информации и управления, Уфа, 2007;
- XXXIII Международная молодежная научная конференция «Гагаринские чтения». Научные труды в 8 томах, Москва, 2007 г.;
- Всероссийская молодежная научная конференция с международным участием «IX Королевские чтения», Самара, 2007 г.
- 10, 11, 12 Международные научные конференции «Компьютерные науки и информационные технологии» (CSIT), Красноусольск, 2007 г., Анталия, Турция 2008, Крит, Греция, 2009;
- Всероссийская молодежная научная конференция «Мавлютовские чтения», Уфа, 2007 г., 2008 г., 2009 г.;
- Всероссийская научно-техническая конференция с международным участием «Актуальные проблемы информационной безопасности. Теория и практика использования программно-аппаратных средств», Самара, 2008 г.;
- 4-я региональная зимняя школа-семинар аспирантов и молодых ученых. Интеллектуальные системы обработки информации и управления, Уфа, 2009 г.;
- Всероссийская научно-техническая конференция студентов, аспирантов и молодых ученых, г. Томск, 2009 г.;
- III Международная научно-практическая конференция «Актуальные проблемы безопасности информационных технологий», Красноярск, 2009 г.;
- Научно-техническая конференция «Свободный полет», Уфа, 2010 г.
- Зимняя школа-семинар молодых ученых и аспирантов, Уфа, 2010 г.

Публикации

Результаты диссертационной работы отражены в 16 публикациях: в 11 научных статьях, в том числе 1 статья в рецензируемом журнале из списка периодических изданий, рекомендованных ВАК, в 5 тезисах докладов в материалах международных и российских конференций.

Структура и объем работы

Диссертационная работа состоит из введения, четырех глав, заключения, приложений, библиографического списка и изложена на 154 страницах машинописного текста. Библиографический список включает 82 наименования литературы.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность темы исследований в области повышения защищенности микроядерных операционных систем. Формулируется цель работы и решаемые в ней задачи, обсуждается научная новизна и практическая ценность выносимых на защиту результатов.

В первой главе выполняется анализ основных признаков и источников информации об атаках, направленных на различные информационные системы. Также проанализированы различные технологии обнаружения атак, указаны достоинства и недостатки существующих методов. Делается вывод о целесообразности разработки новой архитектуры, методов и алгоритмов системы обнаружения аномального поведения процессов микроядерной операционной системы, позволяющей повысить эффективность защиты информации в совокупности с существующими технологиями.

Во второй главе рассматривается задача разработки принципов построения системы обнаружения аномального поведения вычислительных процессов (СОАПП). Рассматриваются особенности архитектуры микроядерной операционной системы MINIX 3, принципы организации взаимодействия процессов между различными компонентами МОС. Выполняется анализ основных поведенческих характеристик вредоносного ПО, построены модели типичного поведения при осуществлении атаки. Предлагается иерархическая модель МОС и проводится анализ данной модели на предмет выявления уровня, на котором задача обнаружения аномального поведения решается более эффективно. Анализируются структуры данных микроядра с целью выделения значимых для СОАПП атрибутов при классификации поведения процессов. Предлагается статистическая модель поведения вычислительного процесса в МОС, которая используется в качестве основы при формировании базы данных векторов поведения процессов. Предлагается модульная архитектура СОАПП, позволяющая эффективно решать задачи сбора статистики поведения процессов и их классификации. В качестве неделимой единицы выполнения задачи в микроядерной операционной системе является вычислительный процесс – изменяющийся набор системных структур данных, отражающих состояние программы в момент исполнения. Поведение

процесса может делиться на две составляющие: нормальное и аномальное, т.е. не удовлетворяющее установленным требованиям. Задача обнаружения аномального поведения процесса является комплексной, поскольку поведение любого процесса в МОС можно охарактеризовать некоторым набором состояний и признаков нахождения в соответствующем состоянии. Таким образом, задачу обнаружения аномального поведения процессов можно разбить на две подзадачи: выявление признаков или атрибутов, характеризующих состояние, а также поведение процесса; распознавание по ряду значащих характеристик аномального поведения на основе выявленных признаков. Первая подзадача связана с построением модели процесса в МОС, отражающей его состояние в любой момент времени функционирования. Сложность данной подзадачи заключается в том, что в большинстве случаев отсутствует исходная информация для определения возможных состояний процесса, например, такая как граф взаимодействия модулей процесса, исходные тексты процесса и т.п. Вторая подзадача связана непосредственно с методами и алгоритмами распознавания аномальных состояний, так как неполная модель процесса или недостаточность признаков приводит к уменьшению эффективности используемых подходов в существующих системах обнаружения аномального поведения.

В ходе анализа выделяются информационные потоки и модули, характерные для задачи распознавания аномального поведения (рис. 1).

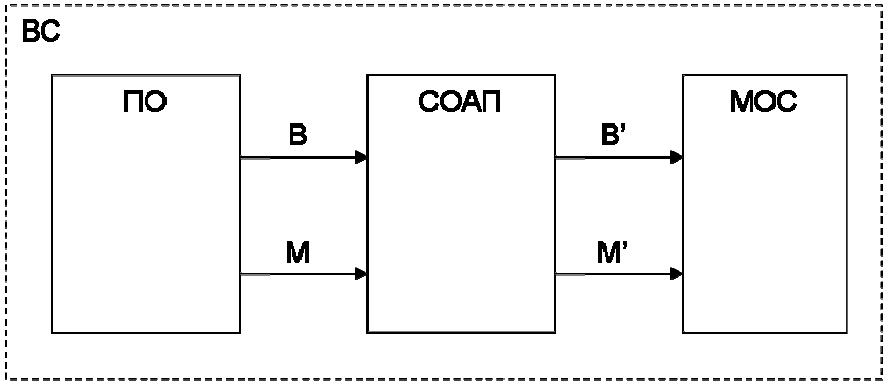

Рисунок 1 – Модель взаимодействия компонентов ВС

$$|B| - |B'| \to 0 \quad (1)$$

$$|M| - |M'| \to \max, \quad (2)$$

где B - множество системных вызовов, совершаемые ПО при нормальном функционировании ВС; B' - множество системных вызовов, которые классифицируются СОАП как допустимые для данного ПО; M - множество вредоносных системных вызовов, приводящих к нарушению нормального функционирования ВС и способных привести к возникновению уязвимостей или угроз; M' - множество вредоносных системных вызовов, неверно классифицированных СОАП.

Для обеспечения безопасности МОС необходимо выполнение условий (1) – надежная работа ПО, не проявляющего аномалий и (2) – увеличение числа обнаруживаемого вредоносного ПО, с неизвестными сигнатурами.

Анализ архитектуры и принципов взаимодействия модулей МОС показал, что в структуре МОС можно выделить три иерархических уровня:

- уровень исполнения (УИ);
- уровень координации (УК);
- уровень планирования (УП).

К исполнительному уровню отнесены устройства ПК и микроядро ОС (рис. 2), взаимодействующих на данном уровне посредством команд прерывания внешних устройств, команд ввода/вывода, команд обмена информацией между компонентами микроядра. Взаимодействие микроядра с вышестоящим уровнем координации обеспечивается посредством системных вызовов. К уровню координации отнесены системные библиотеки, драйверы устройств, менеджеры файловой системы и процессов, взаимодействующих с вышестоящим уровнем планирования с использованием интерфейса прикладного программирования и системных библиотек. На уровне планирования находится прикладное ПО пользователя (рис. 2), которое получает команды и данные для обработки от пользователя и других программных модулей.

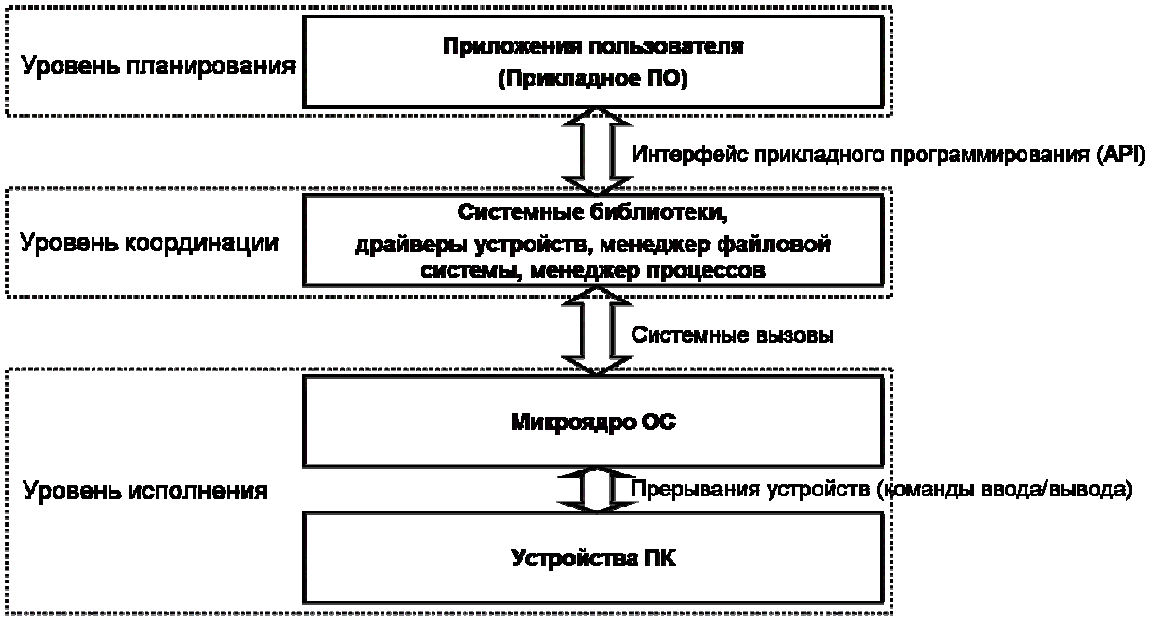

Рисунок 2 – Иерархические уровни МОС

В ходе анализа иерархических уровней МОС показано, что уровень исполнения является ключевым для МОС, так как через него проходят любые информационные потоки, связанные с системными вызовами.

Управляющая часть процесса для микроядра на уровне исполнения представлена некоторым определенным подмножеством системных вызовов, которые передают запросы более верхних уровней микроядру ОС. Независи-

мо от сложности, любой запрос верхнего уровня в итоге будет отображен в множество системных вызовов, которые предоставляет микроядро для работы процессов. Как было указано выше, мощность данного множества может варьироваться в зависимости от типа и назначения операционной системы.

Как известно, каждый процесс характеризуется в МОС несколькими структурами данных, чаще всего, это таблицы, содержащие атрибуты процесса и определяющие его состояние в рамках МОС (рис. 3). Информация о текущем состоянии процессов сохраняется в таблицах, используемые МОС для планирования запуска процессов и управления ВС.

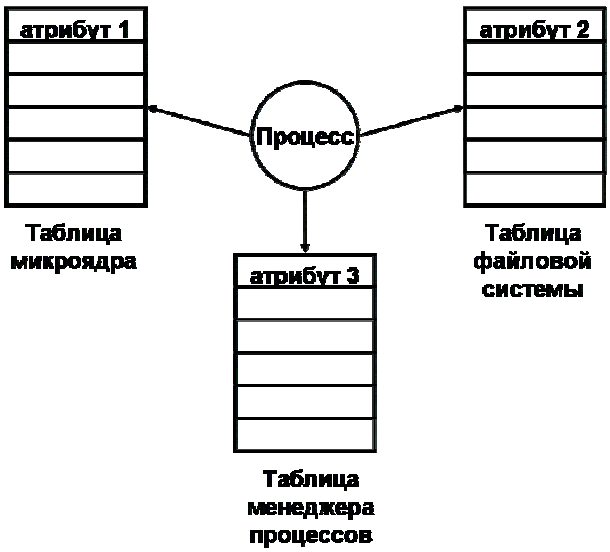

Рисунок 3 – Пример таблиц процессов, содержащих различные атрибуты процессов

При функционировании процесса и выполнении им определенных разработчиком функций, связанных с управлением ВС, значения атрибутов в таблицах МОС изменяются.

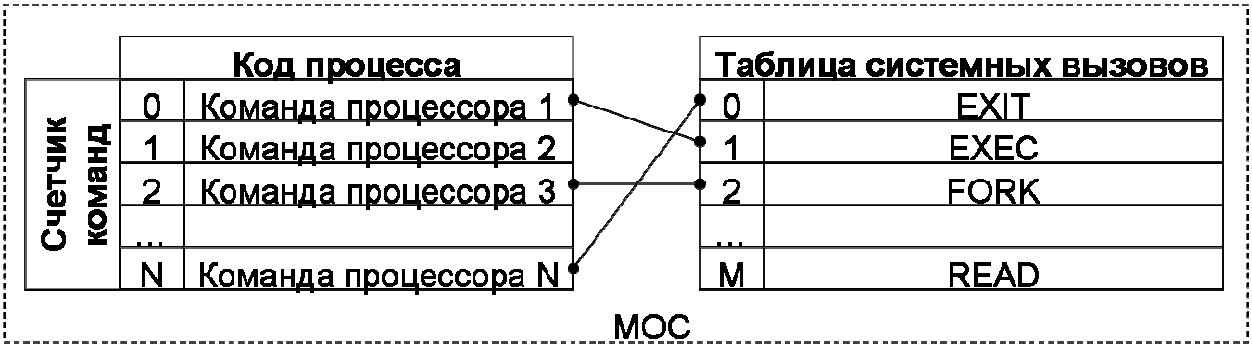

Рисунок 4 – Процесс совершает системные вызовы при определенных значениях счетчика команд

Следует отметить, что, во-первых, системные вызовы совершаются процессом в определенных точках кода процесса, т.е. в момент вызова счетчик команд имеет определенное значение (рис. 4), а, во-вторых, при исполнении процесс совершает системные вызовы с частотой, необходимой для выполнения алгоритма, который он реализует. Как известно, код ПО, в большинстве случаев, можно представить в виде графа потока управления, где в узлах графа находятся участки кода, не содержащие команд условного и безусловного перехода, а направленные дуги – команды перехода от одного участка кода к другому (рис. 5). При совершении любого системного вызовы происходит переключение процесса из режима пользователя в привилегированный режим ядра операционной системы и, таким образом, изменяется граф потока управления процесса.

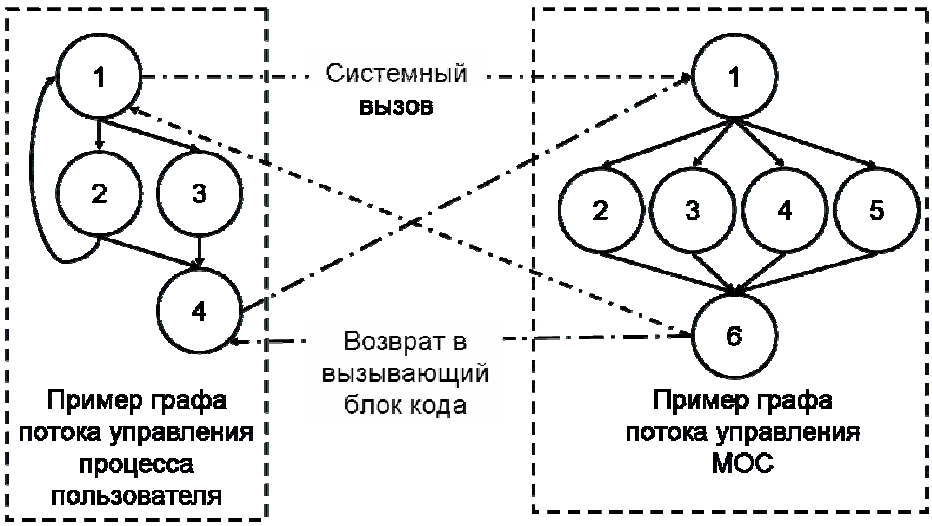

Рисунок 5 – Изменение графа потока управления при совершении системного вызова

После обработки системного вызова микроядро возвращает управление процессу, совершившему системный вызов. Таким образом, для разных процессов статистически можно выделить в графе потока управления узлы, в которых совершаются системные вызовы, а также построить статистическую модель системных вызовов, характеризующих поведение процесса. Рассмотрим обобщенную модель вычислительного процесса микродерной операционной системы, представленную в виде множества вычислительных процессов P.

Основные характеристики модели процесса приведены в табл. 1. Для реализации определенной функциональности системы каждый вычислительный процесс использует системные вызовы МОС из S.

Предполагается, что в зависимости от типа вычислительного процесса системные вызовы совершаются с характерной для них частотой, образуя множество V.

Таблица 1 – Основные характеристики модели вычислительного процесса МОС

Характеристика модели	Описание
$P = \{p_k \mid k = 1 \div j\}$	Множество пользовательских процессов, где j - число процессов
$S = \{s_i \mid i = 1 \div n\}$	Множество системных вызовов, где n - число системных вызовов
$V = \{v_m\}$	Множество частот системных вызовов пользовательских процессов, где $m \in N$
$G : P \times S \times S \to V$	Функция формирования матрицы смежности системных вызовов
$H : P \times S \times S \to V$	Функция формирования матрицы частот последовательных системных вызовов
$I = \{v_{ml} \mid v_{ml} \in V; m,l = 1 \div n\}$	Квадратная матрица смежности системных вызовов пользовательского процесса p_k, где v_{mm} - частота совершения вызова s_m
$J = \{v'_{ml} \mid v'_{ml} \in V; m,l = 1 \div n\}$	Квадратная матрица частот системных вызовов пользовательского процесса p_k, где v'_{ml} - частота совершения вызова s_l после s_m
$D = \{d_r \mid d_r \in Z; r = 1 \div n\}$	Содержимое стека процесса при системном вызове

Предполагается, что множество системных вызовов *S*, а также соответствующее множество частот системных вызовов *V* вычислительного процесса остаются постоянными при многократном запуске системного процесса.

$$|G(p,s,s)| \to const \text{ при } t \to \infty \quad (3)$$

$$|H(p,s,s)| \to const \text{ при } t \to \infty \quad (4)$$

Поставим задачу сбора статистики совершения системных вызовов вычислительного процесса *S* и соответствующих частот системных вызовов *V*, а также последующего анализа состояния процессов ОСРВ на базе данной статистики.

Пусть *P*, *S*, *V*, *I*, *J*, *D* – множества, характеризующие нормальное состояние МОС, полученные при многократном запуске вычислительных процессов в системе до момента времени *t*. А множества P', S', V', I', J', D' отражают новое состояние системы в момент времени $t_1 > t$. Таким образом, предполагается, что для анализа состояния процессов МОС может оказаться достаточным сравнение множеств I', J', D' с множествами *I, J, D*.

$$I' \cap I = I' \quad (5)$$

$$J' \cap J = J' \quad (6)$$

$$D' \cap D = D' \quad (7)$$

$$S' \cap S = S' \quad (8)$$

В итоге, задача анализа состояний процессов МОС по совокупности системных вызовов и их частотных характеристик сводится к задаче распознавания образов. Задача может быть эффективно решена на базе нейросетевого классификатора.

В третьей главе рассматриваются задачи разработки алгоритма сбора статистики поведения процессов в МОС, алгоритма анализа состояний процесса, а также классификации на основе применения искусственных нейронных сетей. В качестве классификатора предлагается использовать самоорганизующиеся карты Кохонена. При построении векторов поведения процессов используется статистическая модель процесса, позволяющая выделить значимые для задачи классификации признаки. Модульная архитектура СОАПП позволяет реализовать способность к самообучению.

Обобщенную модель процесса на уровне системных вызовов можно представить следующим образом (рис. 6).

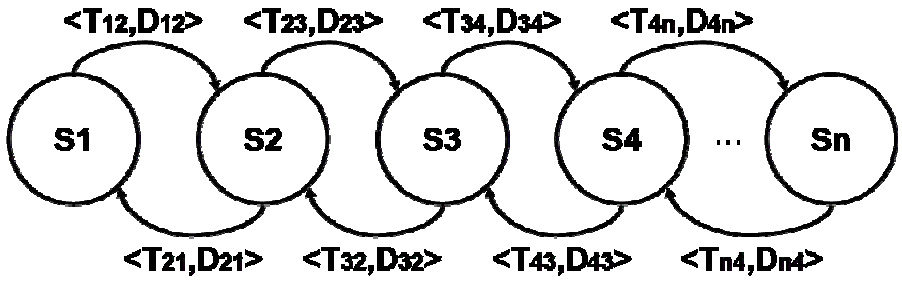

Рисунок 6 – Обобщенная модель процесса на уровне системных вызовов

где: T_{ij} – путь перехода от i-го системного вызова к j-му в графе потока управления процесса; D_{ij} – поток данных, передаваемых при переходе от i-го системного вызова к j-му в графе потока управления процесса; $i, j = 1 \div n$ – общее число системных вызовов, совершаемых процессом.

В алгоритме сбора статистики и извлечения признаков аномального поведения используется информация о пути перехода.

Предложена архитектура СОАПП, которая отличается от известных тем, что встраивается непосредственно в микроядро ОС для повышения эффективности функционирования. Для реализации принципа модульности вся структура СОАПП разделена на отдельные модули: модуль сбора статистики (МСС); модуль анализа состояний процесса (МАСП); нейросетевой модуль классификации (НСМК).

В результате проведенных исследований с СОАПП образовалась БД векторов поведения процессов. Для каждого из выбранных процессов был выполнен анализ частоты используемых системных вызовов при обращении к ним. Результаты численного эксперимента в графическом виде представлены на рис. 7.

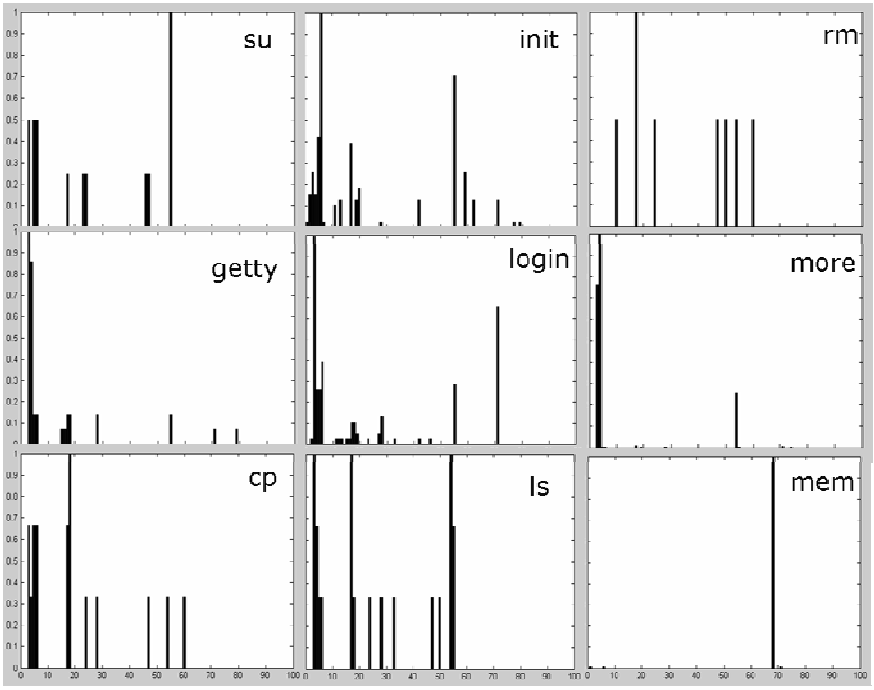

Рисунок 7 – Гистограммы частот совершения системных вызовов процессами МОС

В графическом виде матрицы смежности некоторых системных вызовов можно представить следующим образом (рис. 8).

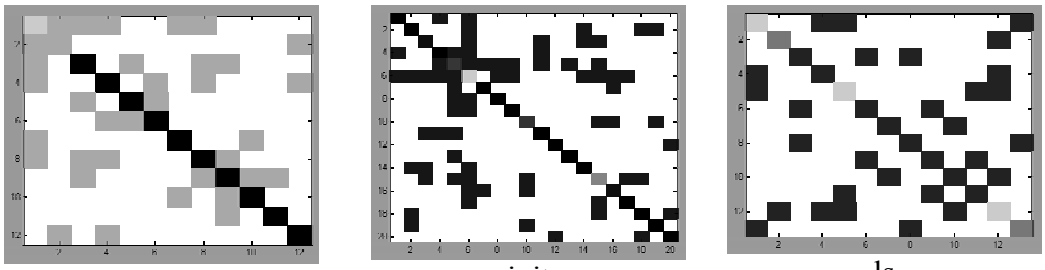

Рисунок 8 – Графическое представление матриц смежности системных вызовов процессов МОС

Как показано, каждый системный процесс может отличаться от другого частотами совершения системных вызовов, а также подмножеством совершаемых системных вызовов. Также в качестве признака аномального поведения процесса в МОС использовались данные из программного стека процесса. Эти характеристики использовались для повышения качества распознавания аномальных событий. Как показали результаты эксперимента, программные стеки процессов МОС отличаются друг от друга, а также отличны во многих случаях и между собой внутри одного процесса. Этот факт подтверждает целесообразность применения данных программного стека об адресах возврата процесса в качестве признака поведения процесса.

Для решения задачи сбора статистической информации о поведении процесса оказывается достаточным использование указанных признаков аномального поведения процесса. Задача классификации состояний эффективно решается с использованием самоорганизующейся нейронной сети.

В четвертой главе рассматриваются особенности реализация системы обнаружения аномального поведения процессов в МОС. Предлагаемая система обнаружения аномального поведения процессов встраивается в микроядро ОС, что повышает уровень защищенности МОС. Модульность и открытость архитектуры позволяют адаптировать систему при использовании на различных аппаратных и программных платформах, а также, при необходимости, производить замену отдельных модулей при необходимости. Разработанная система обнаружения аномального поведения процессов размещается на исполнительном уровне предложенной иерархической структуры МОС, что позволяет осуществлять перехват всех возможных обращений с запросами на предоставление служб микроядра – системных вызовов. Таким образом, обеспечивается контроль поведения процессов в МОС с учетом статистики совершения системных вызовов и частотных характеристик поведения процессов СОАПП.

В качестве основной цели модуля сбора статистики является сбор первичной информации из различных системных структур данных. Для реализации поставленной цели необходимо выполнение следующих задач: перехват сообщений с запросами на выполнение системных вызовов, пересылаемых микроядру; сбор исходных данных о поведении процесса из системных структур МОС и секции стека процесса; ведение БД поведенческих характеристик процессов; установка режима работы СОАПП.

Главной задачей модуля анализа состояний процессов является координация действий компонентов СОАПП и МОС. В связи с этим выделен следующий ряд подзадач:

1. Поддержка актуального состояния таблицы текущего поведения процессов.

2. Оценка отклонения поведения процессов по различным статистическим характеристикам.

3. Блокирование выполнения системного вызова и уведомление пользователя системы, либо занесение соответствующей записи в журнал работы СОАПП.

Целью НСМК является оценка наличия аномальности в поведении исполняющихся процессов в МОС. Исходя из поставленной цели, модуль решает следующий набор задач:

1. Предварительная обработка исходных данных для формирования вектора поведения процесса.

2. Классификация состояния вектора поведения процесса на предмет наличия аномальности с использованием аппарата самообучаемой нейронной сети.

Таблица 2 – Сравнение различных классификаторов

Классификатор	**Верно классифицировано, %**	**Ошибочно классифицировано, %**
Байесса	92,07	7,93
Многослойный персептрон	95,25	4,75
Самоорганизующиеся карты Кохонена	98,25	1,75

Сравнительный анализ классификаторов показал (см. табл. 2, рис. 9), что самоорганизующиеся карты Кохонена имеют достаточно высокую способность к распознаванию аномальностей в процессах МОС.

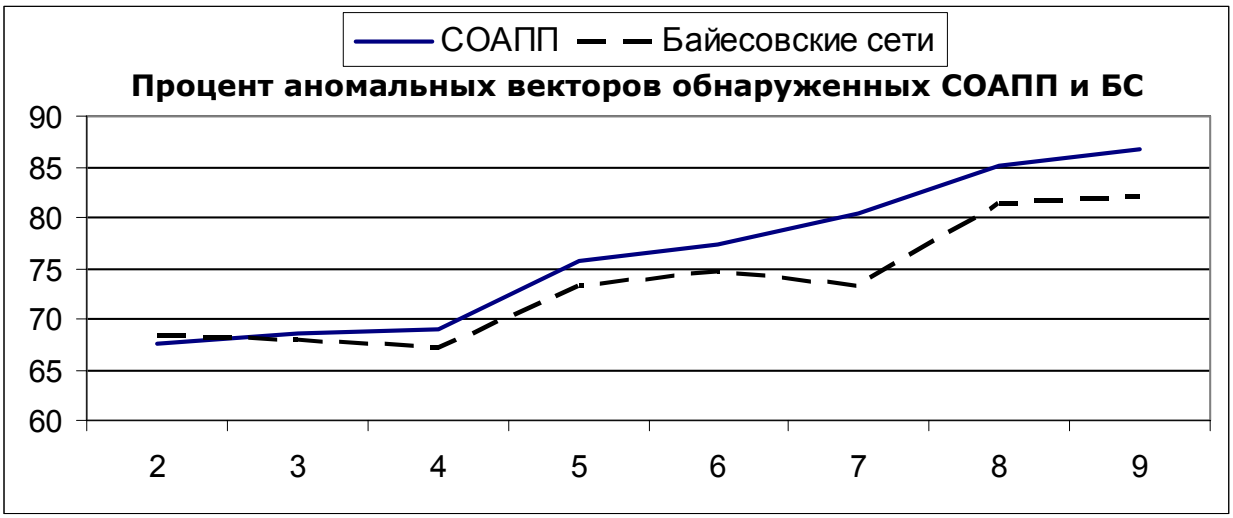

Рисунок 9 – Относительная точность распознавания

В заключении приводятся основные научные результаты, полученные в ходе выполненных исследований, а также представлены выводы по работе.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

1. Предложены принципы построения системы обнаружения аномального поведения вычислительных процессов в микроядерной операционной системе, позволяющие осуществлять сбор статистической информации о поведении системных процессов на уровне микроядра и проводить распознавание класса поведения на основе нейросетевого классификатора, что в отличие от существующих подходов позволяет повысить эффективность обнаружения неизвестных типов атак за счет модификации микроядра операционной системы.

2. Предложена модель вычислительного процесса в микроядерной

операционной системе, основанная на собранной статистической информации о штатном поведении вычислительных процессов, отличающуюся тем, что она может быть использована для решения задачи распознавания аномального поведения вычислительных процессов и выявления новых типов атак с неизвестными сигнатурами.

3. Предложен эффективный метод и алгоритмы классификации поведения вычислительных процессов на основе нейросетевого классификатора, отличающиеся от существующих тем, что позволяют на базе собранной статистики нормального поведения процессов эффективно решать задачу выявления аномальностей, влияющих на информационную безопасность микроядерной операционной системы.

4. Предложен программный прототип системы обнаружения аномального поведения вычислительных процессов, позволяющий оценить эффективность предложенного метода и алгоритмов и повысить число обнаруживаемых новых типов атак на 5-8%.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемом журнале из списка ВАК:

1. Нейросетевая система анализа аномального поведения вычислительных процессов в микроядерной операционной системе / Валеев С.С., Дьяконов М.Ю. // Вестник УГАТУ. 2010. Т. 14. № 5 (40). С. 198–204.

Другие публикации:

2. Обзор способов обеспечения надежности и безопасности в операционных системах / Дьяконов М.Ю. // Интеллектуальные системы обработки информации и управления: 2-я рег. зимн. шк.-сем. аспирантов и молодых ученых: Уфа : УГАТУ, 2007. Т. 2. С. 167–171.

3. Мониторинг процессов в операционных системах с использованием нейросетевых технологий / Дьяконов М.Ю. // Гагаринские чтения: XXXIII междунар. конф. Москва. 2007. Т. 4. С. 81–82.

4. Выявление аномальных состояний в операционных системах на основе нейросетевого классификатора процессов / Дьяконов М.Ю. // IX Королевские чтения: сб. тр. Всерос. молод. науч. конф. Самара. 2007. С. 286.

5. О применении нейронной сети для повышения защищенности микроядерной операционной системы / Дьяконов М.Ю., Валеев С.С. // Компьютерные науки и информационные технологии: тр. 9-й Междунар. конф. (CSIT’2007). Уфа : Виртуал, 2007. Т. 2. С. 156–159. (Статья на англ. яз.).

6. Интеллектуальная система обеспечения защищенности на уровне микроядра ОС / Дьяконов М.Ю. // Мавлютовские чтения: сб. тр. Всерос. молод. науч. конф. Уфа : УГАТУ, 2007. С. 87–89.

7. Обнаружение вредоносного кода на основе анализа процессов операционной системы с использованием нейронной сети / Дьяконов М.Ю. // Интеллектуальные системы обработки информации и управления: 3-я рег. зимн. школа-сем. асп. и молод. ученых: Уфа : УГАТУ, 2008. Т.2 С. 117–122.

8. Об использовании цепочки системных вызовов для обнаружения аномального поведения / Дьяконов М.Ю., Валеев С.С. // Компьютерные науки и информационные технологии: тр. 10-й Междунар. конф. (CSIT'2008). Анталия : УГАТУ, 2008. Т. 1. С. 109–111. (Статья на англ. яз.).

9. Динамический анализ безопасности программного обеспечения с использованием шаблонов поведения / Дьяконов М.Ю. // Актуальные проблемы безопасности информационных технологий. Теория и практика использования программно-аппаратных средств: сб. тр. Всерос. научн.-техн. конф. (АПроБИТ-2008). Самара. 2008. С. 50–54.

10.Повышения защищенности ОС на основе анализа последовательностей системных вызовов процессов / Дьяконов М.Ю. // Мавлютовские чтения: сб. тр. Всерос. науч. конф. Уфа : УГАТУ, 2008. С. 35–37.

11.Формирование контекста и обнаружение аномального поведения путем анализа последовательности системных вызовов / Дьяконов М.Ю. // Актуальные проблемы безопасности информационных технологий. Теория и практика использования программно-аппаратных средств: сб. тр. Всерос. научн.-техн. конф. (АПроБИТ-2008). Самара. 2008. С. 73–77.

12.Интеллектуальная система защиты операционной системы / Дьяконов М.Ю. // Интеллектуальные системы обработки информации и управления: 4-я рег. зимн. шк.-сем. аспирантов и молодых ученых. Уфа : УГАТУ, 2009. Т. 2. С. 131–134.

13.Повышение защищенности микроядерной операционной системы с использованием методов искусственного интеллекта / Дьяконов М.Ю., Валеев С.С. // Актуальные проблемы безопасности информационных технологий: матер. III Междунар. научн.-практ. конф. Красноярск : Сиб. ГАУ, 2009. С. 49–53.

14. Использование методов искусственного интеллекта для классификации состояний операционной системы / Дьяконов М.Ю. // Мавлютовские чтения: Сборник трудов Всероссийской молодежной научной конференции. Уфа. 2009. Т. 3 С. 18–20.

15.Интеллектуальная система защиты операционной системы на основе анализа процессов / Дьяконов М.Ю. // Всерос. научн.-техн. конф. студентов, аспирантов и молодых ученых: матер. докладов. Томск. 2009. Ч.3 С. 303–309.

16.Система обнаружения аномального поведения процессов в микроядерной ос Minix 3 на основе классификации процессов / Дьяконов М.Ю., Валеев С.С. // Свободный полет: сб. тр. конф. Уфа : Гилем, 2010. С. 27–35.

17.Система защиты процессов микроядерной операционной системы с использованием методов искусственного интеллекта / Дьяконов М.Ю. // Интеллектуальные системы обработки информации и управления: тр. 5-й рег. зимн. шк.-сем. аспирантов и молодых ученых. Уфа : УГАТУ, 2010. Т. 2. С. 147–151.

Диссертант М. Ю. Дьяконов

ДЬЯКОНОВ Максим Юрьевич

НЕЙРОСЕТЕВАЯ СИСТЕМА ОБНАРУЖЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ ВЫЧИСЛИТЕЛЬНЫХ ПРОЦЕССОВ МИКРОЯДЕРНЫХ ОПЕРАЦИОННЫХ СИСТЕМ

Специальность: 05.13.19 — Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Подписано к печати 22.11.2010 Формат 60x84 1/16.
Бумага офсетная. Печать плоская. Гарнитура Times New Roman Cyr.
Усл. печ. л. 1,0. Усл. кр. отт. 1,0. Уч. -изд. л. 0,9.
Тираж 100 экз. Заказ № 474
ГОУ ВПО Уфимский государственный авиационный
технический университет
Центр оперативной полиграфии
450000, Уфа-центр, ул. К.Маркса, 12.