Сеидов М.С-А., Ясевич Б.О. Мониторинг аномальной активности в операционной системе ЗОСРВ «Нейтрино» // Международный журнал информационных технологий и энергоэффективности. – 2026. – Т. 11 № 1(63) с. 177–185

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

МОНИТОРИНГ АНОМАЛЬНОЙ АКТИВНОСТИ В ОПЕРАЦИОННОЙ СИСТЕМЕ ЗОСРВ «НЕЙТРИНО»

Сеидов М.С-А., [1]Ясевич Б.О.
ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М. ГУБКИНА" Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e -mail: boris.yasevich2005@gmail.com

В рамках исследования выполнено экспериментальное развертывание системы мониторинга аномальной активности процессов, проведено обучение модели на данных штатного функционирования системы и выполнено моделирование различных типов аномального поведения. Оценивалась способность системы выявлять отклонения в поведении процессов, а также накладные расходы, связанные с её работой.
Результаты исследования показали, что предложенный подход позволяет обнаруживать аномальную активность в режиме, максимально приближенному к реальному времени, при умеренных затратах вычислительных ресурсов. Полученные данные подтверждают возможность применения поведенческого анализа для мониторинга процессов в операционной системе «Нейтрино»..

Ключевые слова: операционная система «Нейтрино», аномальная активность процессов, поведенческий анализ, мониторинг процессов, машинное обучение, производительность системы.

MONITORING ANOMALOUS ACTIVITY IN THE NEUTRINO RESEARCH SYSTEM

Seidov M.S.-A., [1]Yasevich B.O.
GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail: 1 boris.yasevich2005@gmail.com

As part of the study, an experimental deployment of an anomalous process activity monitoring system was carried out, a model was trained on data representing normal system operation, and various types of anomalous behavior were simulated. The system's ability to detect deviations in process behavior, as well as the overhead associated with its operation, was evaluated.
The experimental results showed that the proposed approach makes it possible to detect anomalous process activity in near real-time while incurring moderate computational costs. The obtained data confirm the feasibility of applying behavioral analysis for process monitoring in the Neutrino operating system.

Keywords: Neutrino operating system, anomalous process activity, behavioral analysis, process monitoring, machine learning, system performance.

Современные операционные системы повсеместно используются в специализированных и интегрированных вычислительных комплексах. В этих комплексах выдвигаются высокие требования к надежности, отказоустойчивости и предсказуемости работы. В этих системах отклонения от привычного поведения процессов приводят к снижению производительности, отказам и, следовательно, нарушению требований безопасности. В связи с этим задача

своевременного обнаружения аномальной активности процессов является актуальной и практически значимой. [1]

В жизни состояние операционной системы отслеживается с помощью с двух подходов: сигнатурного и правил-ориентированного. Эти подходы позволяют невероятно эффективно выявлять известные нарушения, однако обладают ограниченной гибкостью и плохо адаптируются к постоянно обновляющимся условиям эксплуатации. Кроме того, они не позволяют обнаруживать новые типы аномалий, не описанные ранее.

Одно из направлений, имеющих большой потенциал – поведенческий анализ, основанный на формировании модели нормального поведения системы. При таком виде анализа за аномалию принимается считается отклонение поведения в данный момент времени от ранее наблюдавшегося состояния, которое принимается как нормальное. Использование машинного обучения позволяет автоматизировать процесс построения эксклюзивной модели нормального поведения и снизить зависимость от ручной настройки параметров. [2]

В этой работе рассматривается экспериментальное обнаружение аномальной активности процессов в операционной системе «Нейтрино» с использованием поведенческого анализа. Работа ориентирована на практическую проверку применимости данного подхода в условиях реальной системы.

В этой работе мы изучаем операционную систему «Нейтрино» и то, как в ней работают программы. Главная задача – найти способы замечать, когда программы ведут себя странно, анализируя то, что они делают в системе. Мы хотим проверить, можно ли находить такие отклонения с помощью анализа поведения и машинного обучения.

Для этого мы настроили систему, которая следит за активностью программ. Сначала мы обучили модель на данных, которые получили, когда система работала нормально. Далее создали ситуацию аномальной активности, проверили обнаруживает ли ее система. Произвели оценку количества ресурсов, требуемых для работы системы мониторинга.

Обнаружение аномальной активности происходит с помощью сигнатурного и правил-ориентированного методов. Сигнатурный подход – сопоставление состояния с известным шаблоном. Его преимущество – высокая точность определения известных нарушений. Его недостаток – необходимость частого обновления шаблонов.

Правил-ориентированные методы используют пороговые значения параметров и заранее заданные условия. Недостатком данного подхода является сложность выбора универсальных порогов, а также высокая вероятность ложных срабатываний при изменении режима работы системы.

Поведенческий анализ представляет собой альтернативный подход, при котором система рассматривается с точки зрения характерных для неё паттернов активности. Отклонения от этих паттернов интерпретируются как потенциальные аномалии. Такой подход не требует явного описания всех возможных нарушений и может выявлять нетипичное поведение общего характера.

На практике поведенческий анализ часто реализуется с использованием методов машинного обучения, в том числе алгоритмов обучения без учителя. Для специализированных операционных систем важным требованием является низкая вычислительная сложность используемых моделей и возможность их работы в режиме реального времени. Поэтому при выборе конкретного решения необходимо учитывать не только точность обнаружения аномалий, но и накладные расходы, связанные с его использованием. [3]

Операционная система «Нейтрино» предназначена для применения в специализированных и встроенных вычислительных системах. Для данной ОС характерны модульная архитектура, чёткое разделение процессов и наличие стандартных средств получения информации о состоянии системы, что делает возможным проведение поведенческого анализа без существенного вмешательства в её работу. [4]

В качестве средства исследования используется программный комплекс мониторинга аномальной активности процессов. Комплекс включает сервис сбора и анализа данных, а также утилиту управления конфигурацией и режимами работы. Сбор информации о процессах осуществляется с использованием стандартных механизмов операционной системы, в частности данных, предоставляемых ядром и виртуальной файловой системой /proc. (Рисунок 1) [5]

В ходе эксперимента анализируются параметры, характеризующие поведение процессов: использование оперативной памяти, количество потоков, состав загруженных библиотек и параметры сетевой активности. Данные характеристики выбраны как наиболее информативные с точки зрения выявления отклонений от нормального функционирования и при этом доступные для мониторинга с минимальными накладными расходами.

Для анализа данных, собранных при использовании операционной системы, используется машинное обучение. С его помощью формируется образ нормального поведения процессов на основе наблюдений за работой системы в обычном, повседневном режиме. Полученная модель используется для выявления несоответствий нормальному поведению в режиме мониторинга без предварительного создания и указания конкретных сценариев нарушений.

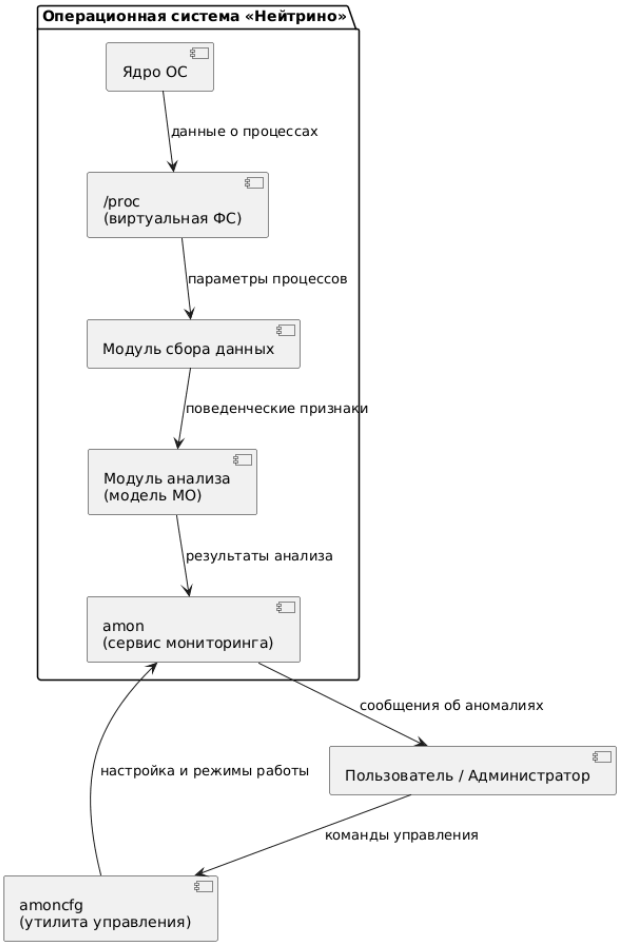

Рисунок 1 – Структурная схема программного комплекса мониторинга

Эксперимент проводился в специально созданном, изолированном программно-аппаратном окружении. На виртуальной машине была запущена операционная система «Нейтрино» и установлен программный комплекс мониторинга. Перед началом эксперимента была выполнена проверка успешности установки и работоспособности всех установленных компонентов.

Для запуска сервиса мониторинга использовалась стандартная команда запуска фонового процесса.

Запуск сервиса мониторинга amon:

```
#amon -v &

Config file loaded
Running kernl operator...
Loading analizer...
Using structure without learning data...
Modl name: amon neiral network
Modl desc: neiral net structure for amon
Modl ver: 1.1
Neuron count: 7

Kernel operator init done
```

Далее производилась настройка параметров мониторинга. В файле конфигурации задали список процессов, подлежащих анализу, набор контролируемых параметров и периодичность сбора данных. Конфигурация писалась таким образом, чтобы захватить процессы, привычные для штатного режима работы системы.

Фрагмент конфигурационного файла мониторинга:

```
{
 "name": "simple_user",
 "buffer_size": 1024,
 "providers": [
  {
   "name": "kernl_provider",
   "processes": [
    "io-usb",
    "io-hid",
    "netmgr"
   ],
   "data": [
    "memory",
    "threads",
    "libraries",
    "network"
   ],
```

"polling_time": 3000,
"structure": "structure/kernl/structure.json",
"anomaly_action": "scrips/anomaly.sh"
}
]
}

После загрузки конфигурации произошла очередная проверка правильности настроек с использованием специализированных команд. Отсутствие ошибок и предупреждений подтвердило готовность системы к переходу на следующий этап эксперимента. Следующий этап – обучение модели нормального поведения.

Для перехода в режим обучения использовалась базовая команда управления системой мониторинга. После её выполнения сервис начал сбор и аккумуляцию данных о поведении процессов без выполнения анализа на наличие непонятных аномалий в поведении системы.

Перевод системы в режим обучения:

amonctl -L

Обучение проводилось в условиях штатной работы системы, без подключения дополнительных устройств и без проведения нагрузочного тестирования. За отведённое время система записала, чем занимались процессы: сколько памяти использовали, сколько потоков создавали, какие библиотеки загружали и как работали в сети. Обучали систему достаточно долго, чтобы охватить все обычные варианты её работы.

Сколько времени займет обучение, зависит от того, как трудно повторить действие и насколько разные ситуации мы хотим считать надежными. Это может занять от пары секунд до гораздо большего времени.

После завершения обучения система мониторинга переводилась в режим анализа, в котором выполнялось сравнение текущего поведения процессов с ранее сформированной моделью нормального поведения. На данном этапе система начинала выявлять отклонения и фиксировать потенциальные аномалии.

Переход в режим мониторинга осуществлялся с помощью команды управления, после чего система начинала работать в режиме реального времени.

Перевод системы в режим анализа активности:

amonctl -R

Корректность завершения этапа обучения подтверждалась отсутствием ошибок в диагностическом выводе системы мониторинга.

Вывод состояния системы:

amonctl -S

Trust value: 99.9893%
Objects captured: 34
Alerts captured: 0
Time: 7 ms

Для проверки работы системы выполнялось моделирование аномальной активности. При обнаружении отклонений система мониторинга формировала диагностические сообщения, содержащие идентификатор процесса и параметр, по которому было зафиксировано несоответствие модели нормального поведения.

Для создания аномальной активности был выбран процесс запуска калькулятора (/phcalc), так как во время обучения системы мониторинга такого процесса не было, и система, вероятно, посчитает его аномальным и сообщит нам об этом. Просмотр аномалий проводился с помощью Amon GUI. [6]

Просмотр обнаруженных аномалий (рисунок 2)

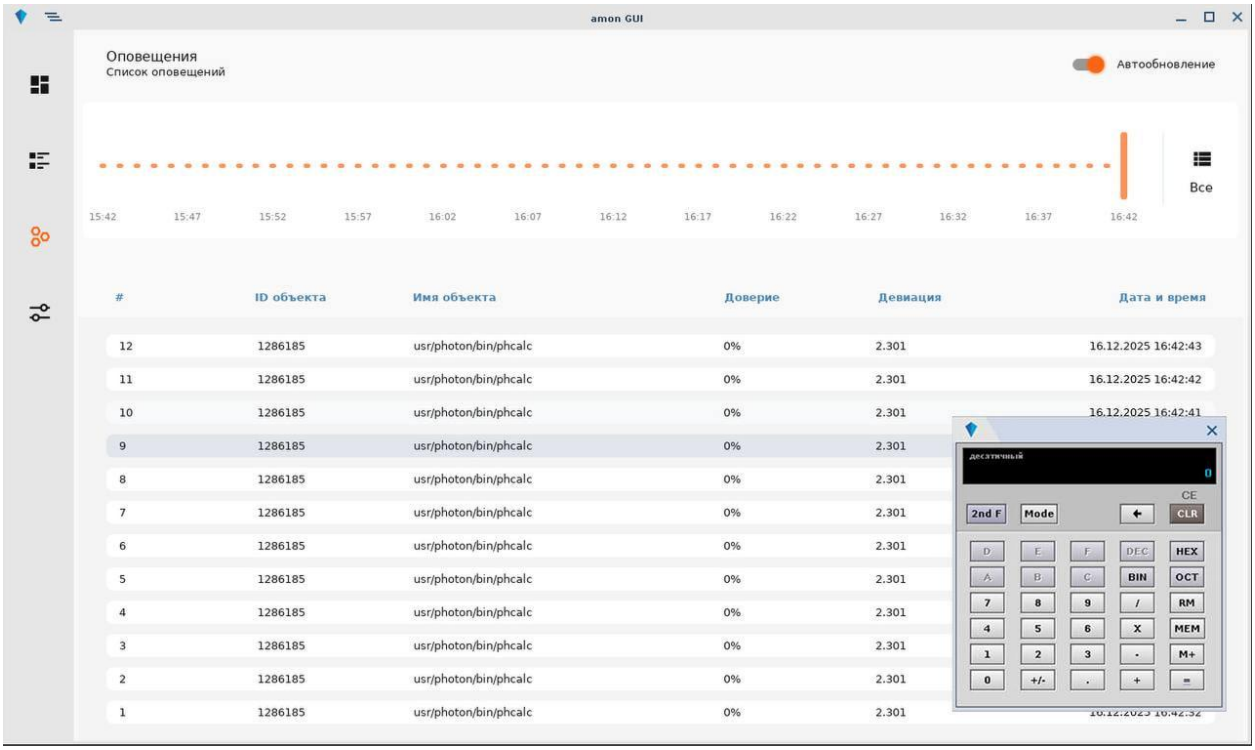

Рисунок 2 – Отслеживание аномальной активности через Amon GUI

На Рисунке 2 представлены имя объекта, вызвавшего аномальную активность, процент уверенности в его идентификации, а также точное время фиксации аномалии.

В рамках данного исследования рассматривалось влияние работы системы мониторинга на использование вычислительных ресурсов операционной системы «Нейтрино». Основное внимание уделялось загрузке процессора и потреблению оперативной памяти.

Измерения проводились в нескольких режимах работы системы: до начала мониторинга, в режиме обучения модели нормального поведения и после перехода в режим анализа. Для контроля состояния системы использовались стандартные средства операционной системы, а также графический интерфейс amon gui, обеспечивающий наглядную визуализацию работы сервиса мониторинга. [7]

Для анализа загрузки процессора использовался интерфейс amon gui, позволяющий отслеживать изменение нагрузки при переходе между режимами работы системы мониторинга. На начальном этапе, до запуска мониторинга, система находилась в стабильном состоянии без дополнительной вычислительной нагрузки. (Рисунок 3)

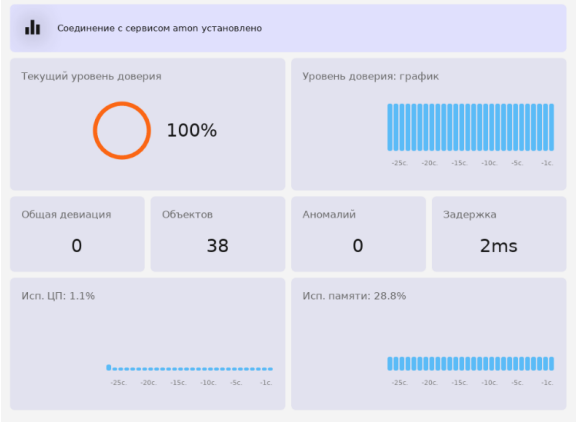

Рисунок 3 – Интерфейс amon gui до начала мониторинга

После запуска мониторинга и перехода системы в режим анализа наблюдалось умеренное увеличение загрузки процессора, связанное с выполнением операций сбора и обработки данных. При этом рост нагрузки не носил скачкообразного характера и оставался стабильным в течение всего времени наблюдения. (Рисунок 4)

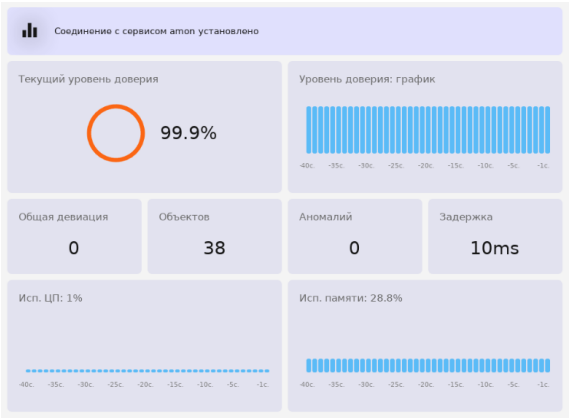

Рисунок 4 – Интерфейс amon gui после начала мониторинга

Анализ системы до и после запуска мониторинга показал, что этот процесс почти не влияет на производительность и может работать в фоновом режиме. Несмотря на то, что задержка выросла в 5 раз, она всё равно остаётся очень маленькой.

Мы посмотрели, сколько памяти требует мониторинг. В ход анализа мы смотрели за потребляемой памятью. Объем используемой памяти почти не менялся. Даже когда система находила новый процесс потребление памяти не увеличивалось.

Еще мы проверили влияние системы мониторинга на производительность компьютера. Увидели, что это не замедляет работу операционной системы.

Тестирование системы, следящей за аномальной активности провели с помощью запуска приложения, которого не было при обучении.

Результаты эксперимента показали, что поведенческий подход позволяет выявлять аномалии в работе системы в режиме реального времени. Система не показала ложных срабатываний и не оказала сильного влияния на производительность машины.

В будущем можно анализировать больше параметров, автоматически подстраивать модель под меняющиеся условия и объединить систему мониторинга с другими инструментами для надёжности и безопасности..

Литература

1. QNX Software Systems. QNX Neutrino RTOS Architecture: официальная документация. [Электронный ресурс]. URL: https://www.qnx.com/developers/docs/ (дата обращения: 04.12.2025).
2. Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey // ACM Computing Surveys. – 2009. – Vol. 41, No. 3, Art. 15. – 58 p. – DOI: 10.1145/1541880.1541882.
3. Уймин А. Г., Цифровые двойники сетевых инфраструктур: точность, методы и практические решения // Радиотехнические и телекоммуникационные системы. – 2023. – № 3 (51). – С. 44–52.
4. QNX Software Systems. Process Manager and Resource Managers in QNX Neutrino: техническая документация. [Электронный ресурс]. URL: https://www.qnx.com/developers/docs/7.0.0/#com.qnx.doc.neutrino.sys_arch/topic/about.html (дата обращения: 04.12.2025).
5. QNX Software Systems. QNX OS (Neutrino) User’s Guide: руководство пользователя. [Электронный ресурс]. URL: https://www.qnx.com/developers/docs/8.0/com.qnx.doc.neutrino.user_guide/topic/about.html (дата обращения: 04.12.2025).
6. Мониторинг аномальной активности в операционной системе «Нейтрино»: форум Habr. [Электронный ресурс]. URL: https://habr.com/ru/companies/swd_es/articles/713690/ (дата обращения: 04.12.2025).
7. QNX Software Systems. System Analysis Toolkit (SAT) for QNX Neutrino: официальная документация. [Электронный ресурс]. URL: https://www.qnx.com/developers/docs/7.0.0/#com.qnx.doc.sat.userguide/topic/about.html (дата обращения: 04.12.2025).

References

1. QNX Software Systems. QNX Neutrino RTOS Architecture: Official Documentation. [Electronic resource]. URL: https://www.qnx.com/developers/docs/ (accessed: 04.12.2025).
2. Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey // ACM Computing Surveys. - 2009. - Vol. 41, No. 3, Art. 15. - 58 p. - DOI: 10.1145/1541880.1541882.
3. Uimin A. G., Digital twins of network infrastructures: Accuracy, methods, and practical solutions // Radiotechnical and telecommunication systems. - 2023. - No. 3 (51). - Pp. 44–52.
4. QNX Software Systems. Process Manager and Resource Managers in QNX Neutrino: technical documentation. [Electronic resource]. URL: https://www.qnx.com/developers/docs/7.0.0/#com.qnx.doc.neutrino.sys_arch/topic/about.html (accessed: 04.12.2025).
5. QNX Software Systems. QNX OS (Neutrino) User’s Guide: user’s guide. [Electronic resource]. URL: https://www.qnx.com/developers/docs/8.0/com.qnx.doc.neutrino.user_guide/topic/about.html (accessed: 04.12.2025).

6. Monitoring anomalous activity in the Neutrino operating system: Habr forum. [Electronic resource]. URL: https://habr.com/ru/companies/swd_es/articles/713690/ (accessed: 04.12.2025).
7. QNX Software Systems. System Analysis Toolkit (SAT) for QNX Neutrino: official documentation. [Electronic resource]. URL: https://www.qnx.com/developers/docs/7.0.0/#com.qnx.doc.sat.userguide/topic/about.html (accessed: 04.12.2025).