УДК 004

# Анализ возможностей поиска неисправностей в информационных системах

**А.П. Преображенский**✉, **И.А. Тихонов, А.В. Котов, Ю.П. Преображенский**

*Воронежский институт высоких технологий, Воронеж, Россия*

*В данной работе рассматриваются некоторые особенности поиска неисправностей в информационных системах. Приведены методы, на основе которых такой поиск может проводиться. Показаны особенности распределения трафика во времени. Выделена совокупность требований, которые предъявляются к мониторингу. Представлен общий алгоритм поиска неисправностей в сетевых система, приведена статистика по итогам применения разработанных рекомендаций на предприятии.*

*Ключевые слова: информационная система, неисправность, контроль, мониторинг, сеть.*

# Analysis of troubleshooting capabilities in information systems

**A.P. Preobrazhenskiy**✉, **I.A. Tikhonov, A.V. Kotov, Yu.P. Preobrazhenskiy**

*Voronezh Institute of High Technologies, Voronezh, Russia*

*This paper discusses some features of troubleshooting in information systems. The methods on the basis of which such a search can be carried out are given. The features of traffic distribution over time are shown. A set of requirements for monitoring is highlighted. The general algorithm of troubleshooting in network systems is presented, statistics on the results of application of the developed recommendations at the enterprise is given.*

*Keywords: information system, malfunction, control, monitoring, network.*

Информационно-телекоммуникационные системы играют ключевую роль в современном обществе, оказывая огромное влияние на различные аспекты нашей жизни, поэтому крайне важно поддерживать работоспособность сетевых систем, как для отдельных пользователей, так и для крупных организаций [1]. Но, как и в любой системе, сетевая инфраструктура также может выходить из строя по целому ряду причин. Именно поэтому актуальность разработки методики по поиску неисправностей в сетевых системах сегодня высока, как никогда раньше.

Целью данной работы является исследование особенностей неисправностей в сетевых системах.

Один из основных способов повысить надежность и эффективность в сетях – применение систем для автоматического поиска неисправностей. Контролировать вручную сложные сети представляется практически невозможным, так как на поиск неисправности порой требуется довольно большой промежуток времени [2]. Автоматизация процесса контроля позволяет сильно сократить затраты времени на проверку и профилактику оборудования, что в свою очередь приводит к повышению полезного времени работы системы, кроме того, это дает возможность оптимизировать штат обслуживающего персонала и снизить требуемую для него квалификацию. Все это приводит к существенному сокращению эксплуатационных расходов, что в свою очередь приводит к значимой экономии.

В системах автоматического контроля при обнаружении неисправности обычно используется метод контроля прохождения сигнала. На вход проверяемого участка

 

логической схемы подаются данные, обычно совпадающие с реальными входными сигналами. В контрольных точках производится проверка параметров. Если данные, снимаемые в контрольных точках, не соответствуют «эталонным», то ошибку следует искать в этом участке логической схемы.

Среди методов поиска неисправностей можно отметить следующие:

**1. Анализ на основе аномалий.** Этот метод основан на установлении базового уровня нормального поведения сети и обнаружении отклонения от этого базового уровня. Он ориентирован на поиск необычных схем трафика, высокие объемы трафика из конкретных источников, необычные протоколы или порты или другое ненормальное поведение сети, которое гипотетически может указывать на угрозу безопасности [3].

**2. Анализ на основе сигнатур.** Этот проверенный метод обнаружения несанкционированных вторжений сравнивает данные сетевого трафика с уже заранее известными шаблонами (сигнатурами) угроз, обнаруженных ранее, вредоносных программ или способов атак. Такой анализ крайне эффективен против известных атак, но затрудняет обнаружение атак новых [4].

**3. Машинное обучение и поведенческий анализ.** Одним из основных преимуществ современных инструментов мониторинга сетевого трафика является использование алгоритмов машинного обучения для анализа сетевого трафика [5]. Модели МО обучаются на имеющихся записях о данных сетевого трафика для обнаружения закономерностей, подозрительных отклонений и потенциально вредоносных действий.

Польза машинного обучения для мониторинга сетевого трафика заключается в обнаружении и изучении сетевых атак, даже если они не были достаточно достоверно определены или описаны ранее. Машинное обучение позволяет распознавать шаблоны, которые могут не соответствовать известным сигнатурам или базовым методам [6], и идентифицировать любую подозрительную активность.

**Характеристики визуализации и отчетности.** Данные, которые уже были проанализированы, отображаются в виде графиков, информационных панелей или отчетов, обеспечивающих полный обзор сетевой активности и событий сетевой безопасности. Инструменты мониторинга сетевого трафика также способны генерировать оповещения на основе заранее предопределенных правил.

Например, предупреждение будет отправлено, если трафик какого-либо приложения превышает определенный уровень использования полосы пропускания или если пользователь получает или пытается получить доступ к конфиденциальным данным в нерабочее время. Эти оповещения могут быть дополнены другими инструментами безопасности для повышения эффективности реагирования на инциденты.

Внедрение мониторинга сетевого трафика помогает системным администраторам повышать эффективность управления сетевыми ресурсами, оптимизировать производительность самой сети, максимально сократить количество атак и, самое главное, повысить безопасность. Мониторинг сетевого трафика, также может помочь в выявлении возможных неисправностей.

У мониторинга сетевого трафика есть следующие преимущества.

**1. Повышенная наглядность.** В настоящее время набирает обороты тенденция внедрения облачных технологий, а также переход к удаленной работе при покупке собственного устройства для выполнения рабочих задач (BYOD). Это создает пробелы для видимости в корпоративных сетях. Мониторинг сетевого трафика решает эту проблему путем сбора и изучения данных в режиме реального времени о внутреннем сетевом трафике (трафик восток-запад) и трафике, входящем в корпоративную сеть и

исходящем из нее (трафик север-юг). Инструменты мониторинга сетевого трафика отслеживают традиционные пакеты данных в сети, а также трафик виртуальной сети, облачные рабочие нагрузки, вызовы интерфейса прикладного программирования (API) к приложениям SaaS, экземпляры бессерверных вычислений и другие формы сетевых коммуникаций. Это обеспечивает ИТ-подразделениям большую наглядность и полную картину деятельности на уровнях со 2 по 7 модели сетевого подключения open system interconnection (OSI), устраняя любые слепые зоны. Следует отметить, что неисправности могут быть связаны с любым из уровней. Для устранения неисправностей специалистам придется планировать в таком случае разные действия.

**2. Повышение производительности сети.** Мониторинг сетевого трафика предоставляет хороший обзор доступности сети, времени ее безотказной работы и простоев. Это помогает ИТ-отделу адекватно оценивать качество обслуживания и быстро устранять проблемы с доступностью сети, такие как большое время отклика, потеря пакетов или перегрузка сети [7]. Мониторинг сетевого трафика также помогает организациям отслеживать использование полосы пропускания и выявлять пользователей, приложения, протоколы и группы IP-адресов, которые требуют большую полосу пропускания. Возникающие в сети неисправности могут оказывать разное влияние на перераспределение трафика. Кроме того, неисправности могут оказывать влияние на распределение полосы пропускания, что сказывается на производительности сети. Например, предприятия могут использовать приложения, которым требуется большая пропускная способность, и сетевые ресурсы, которые необходимо полностью отключить, чтобы избежать потерь при использовании NTA. Дополнительным преимуществом мониторинга сетевого трафика является прогнозирование будущих тенденций трафика на основе имеющихся данных. Это помогает при планировании распределения полосы пропускания и контроле перегрузки сетевого трафика в случае, если в сетевой структуре возникнут какие-либо неисправности.

Процесс мониторинга распределен во времени, что подразумевает охват:

1. Истории состояния объекта мониторинга (например, SIEM системы по журналам событий, сохраненным ранее, полученным из различных источников, например, сетевых устройств, программ, журналов ОС и др.).

2. Текущие параметры состояния объекта мониторинга (сбор и анализ информации о функционировании в настоящее время рассматриваемого объекта).

3. Прогноз состояний объекта (по записям прошлых и показаниям текущих состояний объекта мониторинга прогнозируется его вероятное дальнейшее состояние и уровень адаптации к новым условиям функционирования.

Можно выделить совокупность рекомендаций, предъявляемых к мониторингу:

1. Своевременность (отображение факта перехода объекта мониторинга в состояния с предельными отклонениями в реальном времени).

2. Полнота (достаточность данных необходимых для определения необходимых характеристик объекта мониторинга) [8].

3. Достоверность (мониторинг подразумевает отображение истинного состояния объекта).

4. Целенаправленность (следование к конкретному конечному результату, выбор типа мониторинга, наиболее подходящего для корректного и точного выполнения возложенных на него задач).

5. Объективность (данные о параметрах состояния объекта мониторинга не должны зависеть от пользователя).

6. Гибкость (способность к адаптации при изменении каких-либо внешних или внутренних параметров) [9].

Процесс поиска неисправностей в сетевых системах можно представить как последовательность действий [10]. На рисунке представлен общий алгоритм поиска неисправностей в сетевых системах.

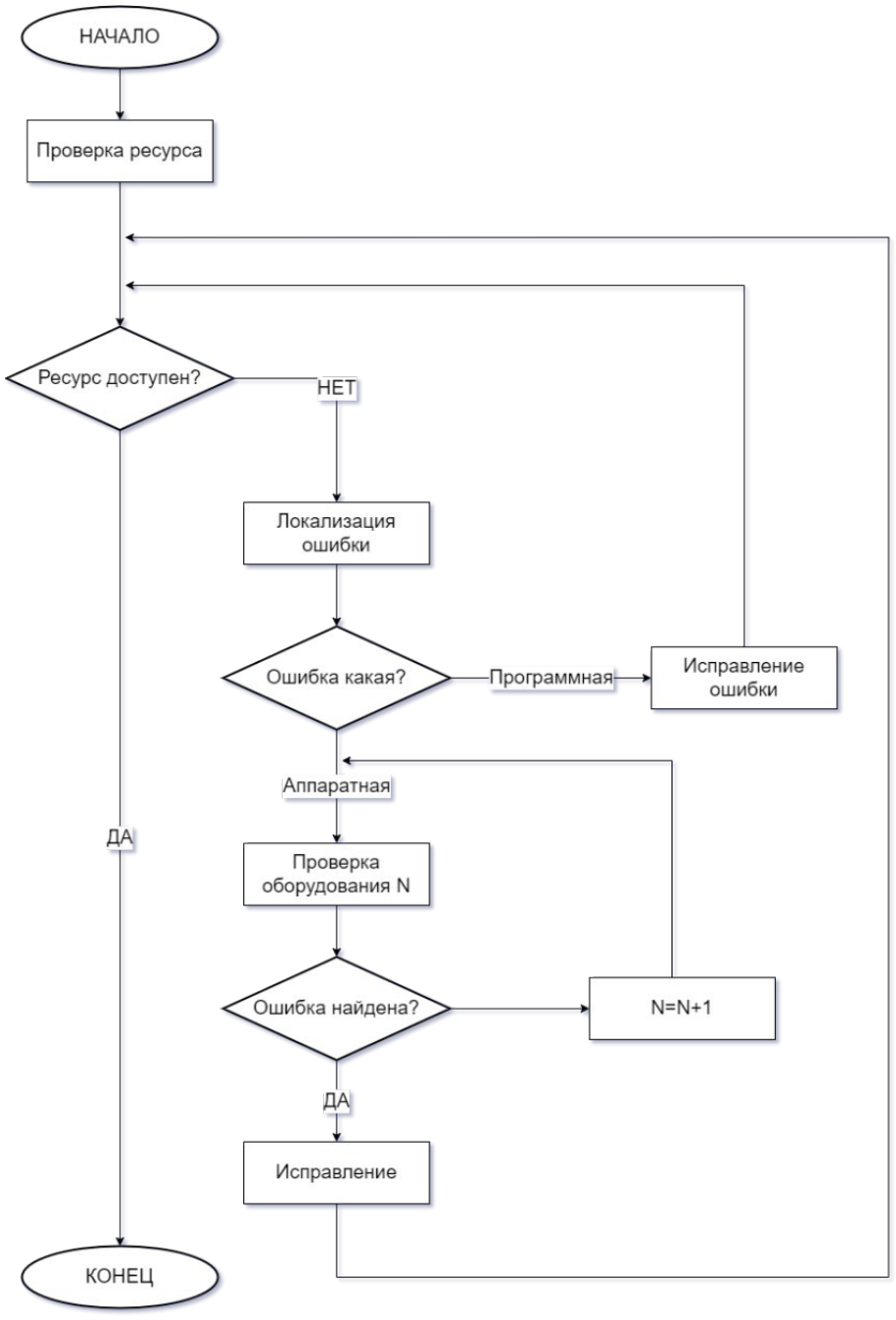


Рисунок. Общий алгоритм поиска неисправностей в сетевых системах

Согласно алгоритму, при возникновении ошибки, некий общий ресурс становится недоступным, что влечет за собой следующие действия:

1. Локализация ошибки. Применяя сетевое программное обеспечение, оператор получает информацию о состоянии сети [11] и делает вывод о том программная это ошибка или аппаратная.

2. Если ошибка программная, она исправляется и работоспособность ресурса проверяется повторно, если же ошибка носит аппаратный характер, выполняется проверка оборудования N.

3. В случае, если ошибка найдена в оборудовании N, она исправляется ремонтом или заменой оборудования, и ресурс снова проверяется на работоспособность.

4. Если оборудование N работает штатно, индексу N присваивается значение N+1 и проводится проверка следующего элемента оборудования.

5. Как только обнаруживается оборудование, ставшее причиной ошибки, оно ремонтируется или заменяется, а затем снова проводится проверка доступности ресурса.

Разрабатываемый список рекомендаций нацелен на решение целого ряда задач, связанных с повышением отказоустойчивости оборудования на предприятиях и поиском неисправностей в сетях. Чтобы убедиться в эффективности разработанных рекомендаций, была подсчитана статистика по нескольким показателям:

1. Статистика по количеству отказов в сети на предприятии, в случае применения рекомендаций по выбору оборудования.

2. Статистика по времени поиска ошибок в сети предприятия, в случае применения рекомендаций по проверке оборудования.

3. Статистика по времени реагирования на отказ какого-либо элемента сети, в случае применения рекомендаций по выбору сетевого программного обеспечения.

4. Статистика по количеству вышедшего из строя оборудования по причине внешнего воздействия, в случае применения рекомендаций по защите сетевого оборудования от внешнего воздействия.

Статистика по итогам применения разработанных рекомендаций на предприятии, на котором работает один из авторов данной работы, дает представление о том, как менялись различные параметры надежности сетевой системы предприятия после применения на практике рекомендаций и приведена в таблицах 1–4.

Таблица 1

Статистика по количеству отказов в сети на предприятии

| **Вид отказа** | **Количество до применения рекомендаций, год** | **Количество после применения рекомендаций, год** |
|---|---|---|
| Полная недоступность сети | 7 | 3 |
| Частичная недоступность сети | 20 | 8 |

Таблица 2

Статистика по времени поиска ошибок в сети предприятия

| **Вид ошибки** | **Время на поиск ошибки до применения рекомендаций, ч** | **Время на поиск ошибки после применения рекомендаций, ч** |
|---|---|---|
| «Узел недоступен» | 2 | 0,5 |
| «Коллизия» | 2,5 | 0,3 |
| «Фрагментированный пакет» | 1 | 0,25 |

Таблица 3

Статистика по времени реагирования на отказ какого-либо элемента сети

| Отказавший элемент | Время реагирования до применения рекомендаций, мин | Время реагирования после применения рекомендаций, мин |
|---|---|---|
| Коммутатор | 60 | 10 |
| Принтер | 180 | 10 |
| Рабочее место | 45 | 10 |

Таблица 4

Статистика по количеству вышедшего из строя оборудования по причине внешних воздействий

| Вышедшее из строя оборудование | Количество до применения рекомендаций, шт/год | Количество после применения рекомендаций, шт/год |
|---|---|---|
| Коммутатор | 2 | 0 |
| Принтер | 4 | 1 |
| Маршрутизатор | 1 | 0 |
| Кабель | 25 | 10 |

Заключение. Были предложены рекомендации для поиска неисправностей в сетевых системах. Данные рекомендации могут быть внедрены практически в любой организации с большой, разветвленной сетевой системой. Важным преимуществом разработанного списка рекомендаций является его универсальность. При необходимости можно список дополнить с учетом развития сетевых структур.

## СПИСОК ИСТОЧНИКОВ

1. Ахмедьянова Г.Ф. Оптимальное управление организационно-технической системой с учетом интенсивности приложения управляющих воздействий / Г.Ф. Ахмедьянова // Моделирование, оптимизация и информационные технологии. – 2024. – Т. 12. – № 1 (44). – URL: https://moitvivt.ru/ru/journal/pdf?id=1497 (дата обращения: 02.11.2024).

2. Даньшина К.А. Некоторые особенности обеспечения надежности компьютерных сетей / К.А. Даньшина, А.С. Стельмахов, В.Н. Кострова // Инновационный потенциал развития общества: взгляд молодых ученых: Сборник научных статей 4-й Всероссийской научной конференции перспективных разработок. – Курск: ЗАО «Университетская книга», 2023. – С. 131-134.

3. Модификация методики вейвлет-анализа для выявления аномалий в трафике компьютерной сети / В.В. Литвинов, И.С. Скитер, Е.В. Трунова [и др.] // Технические науки и технологии. – 2017. – № 2 (8). – С. 99-109.

4. Кудрявцев М.Е. Сигнатуры систем обнаружения вторжений: основы IDS сигнатур / М.Е. Кудрявцев, О.Б. Калугина // Актуальные проблемы современной науки, техники и образования. – 2019. – Т. 10. – № 1. – С. 80-83.

5. Машинное обучение для анализа и классификации шифрованного сетевого трафика / В.А. Мулюха, Л.Ю. Лабошин, А.А. Лукашин [и др.] // Международная конференция по мягким вычислениям и измерениям. – 2020. – Т. 1. – С. 238-241.

6. Преображенский Ю.П. Проблемы управления процессами в компьютерных системах / Ю.П. Преображенский, Ю.Л. Чупринская, Е. Ружицкий // Вестник Воронежского института высоких технологий. – 2022. – Т. 16. – № 1 (40). – С. 92-94.

7. Подходы к прогнозированию изменения состояния обеспечивающих компонентов информационно-управляющей системы / Ю.С. Шевнина, П.Е. Рябов, С.В. Прокопчина [и др.] // Моделирование, оптимизация и информационные технологии. – 2024. – Т. 12. – № 2 (45). – URL: https://moitvivt.ru/ru/journal/pdf?id=1549 (дата обращения: 02.11.2024).

8. Использование информационных систем на предприятиях / Д.П. Комаристый, А.М. Агафонов, А.П. Степанчук [и др.] // Вестник Воронежского института высоких технологий. – 2017. – Т. 11. – № 2 (21). – С. 104-106.

9. Обеспечение функциональной надежности телекоммуникационных систем на основе топологического ресурса / В.Е. Гвоздев, М.Б. Гузаиров, А.С. Ракипова [и др.] // Моделирование, оптимизация и информационные технологии. – 2024. – Т. 12. – № 3 (46). – URL: https://moitvivt.ru/ru/journal/pdf?id=1647 (дата обращения: 02.11.2024).

10. Львович А.И. Компьютерные системы управления предприятием / А.И. Львович // Юность и Знания – Гарантия Успеха – 2024: Сборник научных статей 11-й Международной молодежной научной конференции. – Курск: ЗАО «Университетская книга», 2024. – Т. 1. – С. 143-146.

11. Соломатин Д.А. О формировании моделей информационных сетей / Д.А. Соломатин, А.А. Плотников // Перспективы развития технологий обработки и оборудования в машиностроении: Сборник научных статей Всероссийской научно-технической конференции. – Воронеж: Воронежский государственный технический университет, 2023. – С. 363-366.

## ИНФОРМАЦИЯ ОБ АВТОРАХ

**Преображенский Андрей Петрович**, доктор технических наук, профессор, Воронежский институт высоких технологий, Воронеж, Россия.
*e-mail:* app@vivt.ru

**Тихонов Иван Александрович,** студент, Воронежский институт высоких технологий, Воронеж, Россия.
*e-mail:* Tihhon_Ivvan754@yandex.ru

**Котов Александр Владимирович,** студент, Воронежский институт высоких технологий, Воронеж, Россия.
*e-mail:* Kotov__Alex97@yandex.ru

**Преображенский Юрий Петрович**, кандидат технических наук, доцент, Воронежский институт высоких технологий, Воронеж, Россия.
*e-mail:* petrovich@vivt.ru