граммных средств или сочетания аппаратных устройств, функционирующих в режиме plug-and-play, и программных решений. Этот вид мониторинга позволяет отслеживать практически любую сеть, будь то проводная или беспроводная, локальная сеть предприятия, виртуальная частная сеть или инфраструктура, предоставляемая провайдером. Мониторинг способен охватывать устройства с различными операционными системами и множеством функций – от КПК и сотовых телефонов до серверов, маршрутизаторов и коммутаторов. Это означает, что вы можете контролировать работу и состояние различных устройств в вашей сети. Интеллектуальный сетевой мониторинг позволяет обнаруживать и устранять проблемы в сети, такие как сбои в работе устройств, перегрузки сети или нарушения безопасности. Он также может предоставлять информацию о производительности сети, использовании ресурсов и других параметрах, которые могут быть полезны при планировании и оптимизации сетевой инфраструктуры.

Системы NMS помогают выявить любую специфическую активность в сети, определить параметры производительности и предоставить результаты, которые позволяют решать множество разнообразных задач, включая выполнение технических требований, предупреждение о внутренних угрозах безопасности и обеспечение прозрачности сетевых операций [5].

Решение о том, за чем конкретно нужно следить в сети, столь же важно, как и решение об использовании интеллектуального мониторинга как такового. Чтобы убедиться, что карта топологии корпоративной сети отражает реальное положение дел, необходимо учесть следующие аспекты:

– Карта должна точно описывать типы сетевых сегментов, мониторинг которых будет выполняться. Это поможет определить, какие участки сети требуют особого внимания и контроля.

– Карта должна предоставлять данные о серверах, а также работающих на них приложениях и операционных системах. Это позволит отслеживать работу серверов и обнаруживать возможные проблемы или уязвимости.

– Карта должна содержать информацию о количестве настольных систем, которые необходимо учитывать. Это поможет оценить нагрузку на сеть и обеспечить ее эффективное функционирование.

– Карта должна также указывать типы удаленных устройств, имеющих доступ к каждой сети. Это позволит контролировать и обеспечивать безопасность удаленного доступа.

Чем больше ясности будет в самом начале, тем проще будет потом выбрать инструменты мониторинга, которые следует приобрести.

Можно возразить, что, если сеть работает, то нечего с ней заниматься. Зачем добавлять еще одну проблему сетевым администраторам, если количество их задач уже едва умещается в списках, занимающих всю стену от пола до потолка? Причины настаивать на внедрении сетевого мониторинга в общих словах можно выразить так: поддержка текущего состояния сети, гарантия готовности, увеличение производительности. Кроме того, NMS позволит накопить бесценную информацию, которая пригодится при планирования дальнейшего развития сетевой инфраструктуры.

Для того чтобы предсказать перспективы роста сети, необходимы сведения об истории развития инфраструктуры. Решения, принятые на основе слишком скудных данных, могут стать источником очень глубоких проблем. Сеть с момента ее создания серьезно изменилась. Изменения конфигурации, добавление сетевых устройств, серверов и настольных систем привели к дисбалансу трафика на Web-серверах и серверах электронной почты, перегрузке коммуникаций и каналов связи, которые не увеличили своего быстродействия.

Интеллектуальный мониторинг сети будет бессмысленным, если он не обеспечивает определение наиболее важных параметров. Анализируют, как правило, использование пропускной способности сети, производительность приложений и серверов.

Список литературы

1. Андрюшкевич С.К., Ковалёв С.П. Интеллектуальный мониторинг распределенных технологических объектов с использованием информационных моделей состояния // Известия ТПУ. 2010. № 5. С. 35-39.

2. Будко Н.П. Концептуальная модель подсистемы интеллектуального мониторинга состояния информационно-телекоммуникационной сети общего пользования // Системы управления, связи и безопасности. 2021. № 5. С. 65-119.

3. Аветисян Т.В., Львович Я.Е., Преображенский А.П. Анализ возможностей построения рациональной структуры киберфизической системы // Моделирование, оптимизация и информационные технологии. 2023. № 11. URL: https://moitvivt.ru/ru/journal/pdf?id=1235 (дата обращения: 15.09.2023).

4. Клименко Ю.А., Преображенский А.П. Мониторинг распределительной электрической сети на базе когнитивных измерений // Международный научно-исследовательский журнал. 2020. № 8-1 (98). С. 76-80.

5. Артюшевский Р.В. О возможностях интеллектуализации в системах связи // Интеллектуальные информационные системы: тенденции, проблемы, перспективы: сборник научных статей 8-й Международной научно-практической конференции «ИИС-2020», Курск, 18 декабря 2020 года. Курск: Юго-Западный государственный университет, 2020. С. 17-19.

ОБ АНАЛИЗЕ СЕТЕЙ НА БАЗЕ ИНТЕЛЛЕКТУАЛЬНОГО МОНИТОРИНГА

Пендурова Е.А., Модина Ю.С.

Воронежский институт высоких технологий, Воронеж, e-mail: bbosly@yandex.ru

Интеллектуальный мониторинг позволяет анализировать данные, полученные из сети, и выявлять аномалии, подозрительную активность

и потенциальные уязвимости. Это позволяет оперативно реагировать на возможные угрозы и принимать меры по их предотвращению.

Основные методы и технологии интеллектуального мониторинга [1]:

– С помощью алгоритмов машинного обучения можно анализировать данные сети и выявлять аномальную активность, подозрительные паттерны и потенциальные уязвимости. Это позволяет оперативно реагировать на возможные угрозы и принимать меры по их предотвращению Машинное обучение может быть применено для обнаружения аномалий в реальном времени, анализа потоков данных и анализа журналов событий.

– Глубокие нейронные сети могут быть использованы для анализа больших объемов данных и выявления сложных зависимостей. Эти сети обучаются на больших наборах данных и способны автоматически извлекать иерархические признаки из этих данных, что позволяет им обнаруживать сложные зависимости и паттерны. Глубокие нейронные сети широко применяются в различных областях, таких как компьютерное зрение, обработка естественного языка и распознавание речи. Они позволяют анализировать и обрабатывать большие объемы данных, что делает их эффективным инструментом для решения сложных задач анализа данных.

– Анализ потоков данных позволяет выявлять аномалии и подозрительную активность в реальном времени. Этот метод анализирует данные, проходящие через сеть, и выявляет необычные или подозрительные паттерны, которые могут указывать на наличие сетевых атак или других угроз. Анализ потоков данных осуществляется в режиме реального времени, что позволяет оперативно реагировать на возможные угрозы и принимать меры по их предотвращению. Этот подход особенно полезен для обнаружения и предотвращения DDoS-атак Анализ потоков данных может быть реализован с помощью специальных инструментов, таких как системы мониторинга сетевого трафика или системы безопасности информации.

– Анализ журналов событий позволяет выявлять аномалии и подозрительную активность на основе записей о событиях в сети. Этот метод анализирует журналы событий, которые содержат информацию о действиях и событиях, происходящих в сети. Анализируя эти записи, можно выявить необычные или подозрительные паттерны, которые могут указывать на наличие сетевых атак или других угроз. Анализ журналов событий позволяет оперативно реагировать на возможные угрозы и принимать меры по их предотвращению. Этот подход особенно полезен для обнаружения и предотвращения кибератак.

Интеллектуальный мониторинг успешно применяется в различных сферах, включая информационную безопасность, телекоммуникации и интернет вещей. В информационной безопасности он помогает обнаруживать и предотвращать кибератаки, в телекоммуникациях – оптимизировать сетевую инфраструктуру и обеспечивать качество обслуживания, а в интернете вещей – обнаруживать аномалии в работе устройств и предотвращать возможные сбои.

Интеллектуальный мониторинг в информационной безопасности помогает обнаруживать и предотвращать кибератаки. Он позволяет анализировать сетевой трафик и идентифицировать потенциально вредоносную активность. Такой мониторинг может использоваться для обнаружения атак на сетевую инфраструктуру, включая DDoS-атаки, вредоносные программы и другие угрозы.

Интеллектуальный мониторинг в информационной безопасности может включать использование различных инструментов и технологий, таких как системы обнаружения вторжений (IDS), системы обнаружения вредоносного программного обеспечения (MDS), системы управления инцидентами безопасности (ISIM) и другие [2].

Примеры специализированных решений, которые предлагают интеллектуальный мониторинг и защиту от киберугроз: RedCheck и Palo Alto Unit 42, Cisco Cyberthreat Defense.

В сфере телекоммуникаций интеллектуальный мониторинг помогает оптимизировать сетевую инфраструктуру и обеспечивать качество обслуживания. Он позволяет отслеживать и анализировать данные о производительности сети, чтобы выявлять узкие места и проблемы, которые могут влиять на качество связи. Такой мониторинг может помочь операторам связи улучшить производительность сети и обеспечить более стабильное и надежное соединение для пользователей.

Примеры возможностей интеллектуального мониторинга в сфере телекоммуникаций [3]:

– Отслеживание производительности сети и выявление узких мест.

– Анализ данных о трафике и использовании ресурсов.

– Мониторинг качества обслуживания и выявление проблем с соединением.

Преимущества интеллектуального мониторинга в сфере телекоммуникаций:

– Оптимизация сетевой инфраструктуры для повышения производительности и эффективности.

– Улучшение качества обслуживания и удовлетворенности пользователей.

– Более быстрое выявление и устранение проблем сети.

– Повышение надежности и стабильности соединения.

В области интернета вещей интеллектуальный мониторинг помогает обнаруживать аномалии в работе устройств и предотвращать возможные сбои. Он позволяет отслеживать и анализировать данные, поступающие от устройств, чтобы выявлять необычное поведение или отклонения от нормы. Такой мониторинг может быть полезен для предотвращения сбоев в работе устройств и обеспечения более надежной работы интернета вещей.

Примеры использования интеллектуального мониторинга в интернете вещей [4,5]:

– Отслеживание и анализ данных, поступающих от устройств, чтобы выявлять аномалии и предотвращать возможные сбои.

– Обнаружение необычного поведения устройств, которое может указывать на проблемы или угрозы безопасности.

– Предупреждение о потенциальных проблемах или отклонениях от нормы, чтобы принять меры по их устранению до возникновения серьезных проблем.

– Оптимизация работы устройств и повышение их эффективности на основе анализа данных.

– Улучшение надежности и безопасности системы интернета вещей путем раннего обнаружения и предотвращения возможных сбоев.

В данной статье были рассмотрены основные аспекты интеллектуального мониторинга для анализа сетей. Интеллектуальный мониторинг является эффективным инструментом для обнаружения и предотвращения сетевых угроз, а также для оптимизации работы сети. Он позволяет проводить анализ данных в режиме реального времени, а также прогнозировать и предотвращать возможные проблемы. Примеры успешной реализации интеллектуального мониторинга в различных сферах подтверждают его важность и актуальность. В заключении делается вывод о необходимости использования интеллектуального мониторинга для обеспечения безопасности и эффективности работы сетей.

Список литературы

1. Артюшевский Р.В. О возможностях интеллектуализации в системах связи // Интеллектуальные информационные системы: тенденции, проблемы, перспективы: сборник научных статей 8-й Международной научно-практической конференции «ИИС-2020», Курск, 18 декабря 2020 г. Курск: Юго-Западный государственный университет, 2020. С. 17-19.

2. Двуреченская Е.О. Проблемы обработки информации в распределенных интеллектуальных системах // Интеллектуальные информационные системы: тенденции, проблемы, перспективы: сборник научных статей 8-й Международной научно-практической конференции «ИИС-2020», Курск, 18 декабря 2020 г. Курск: Юго-Западный государственный университет, 2020. С. 51-53.

3. Львович Я.Е. Проблемы интеллектуализации сетей нового поколения // Интеллектуальные информационные системы: тенденции, проблемы, перспективы: сборник научных статей 8-й Международной научно-практической конференции «ИИС-2020», Курск, 18 декабря 2020 г. Курск: Юго-Западный государственный университет, 2020. С. 136-139.

4. Белых В.С., Ткаченко А.В. Современные методы тестирования программных продуктов на основе искусственного интеллекта // Интеллектуальные информационные системы: тенденции, проблемы, перспективы: сборник научных статей 8-й Международной научно-практической конференции «ИИС-2020», Курск, 18 декабря 2020 г. Курск: Юго-Западный государственный университет, 2020. С. 25-26.

5. Загоруйко Д.А., Ткаченко А.В. Искусственный интеллект // Интеллектуальные информационные системы: тенденции, проблемы, перспективы : сборник научных статей 8-й Международной научно-практической конференции «ИИС-2020», Курск, 18 декабря 2020 г. – Курск: Юго-Западный государственный университет, 2020. С. 67-68.

ВЛИЯНИЕ ТИПОГРАФИКИ НА ВОСПРИЯТИЕ ИНФОРМАЦИИ В ЦИФРОВОЙ СРЕДЕ

Попов Т.И.

Мелитопольский государственный университет, Мелитополь, e-mail: mr4bread263@gmail.com

В современном мире, самым распространённым способом восприятия информации всё ещё является чтение текста. По этой причине, важно уметь правильно оформлять текст для удобства навигации в массивах информации. Это также жизненно необходимо для сайтов и рекламы в интернете, если пользователю будет некомфортно читать текст на сайте, то повышается вероятность, что он уйдёт с него.

Целью данной работы является исследование влияния типографики на восприятие информации в цифровой среде. Была поставлена задача – узнать, как сильно влияет соблюдение правил типографики на комфорт чтения и желание остаться на сайте у пользователей.

Актуальность темы обусловлена тем, что понимание влияния типографики может помочь создателям контента, дизайнерам и другим специалистам в области цифровых технологий улучшить качество и доступность информационных продуктов, а также удержать внимание читателей.

Методология

Исследование будет базироваться на базовых типографических правилах и их влияний на самом тексте. Для исследования будет составлен текст, что изменяется в ходе эксперимента, а контрольная группа будет оценивать его по нескольким критерием:

1) Скорость чтения;
2) Оценка комфорта чтения;
3) Понимание содержание текста.

Для обеспечения достоверности результатов, каждый участник контрольной группы будет оценивать один и тот же текст с различными типографическими параметрами. Это позволит нам увидеть, как изменения в типографике влияют на восприятие информации каждым конкретным участником.

В исследовании будут использоваться правила близости и схожести, принципы иерархии, шрифтовой пары и понятие ритма.