Проведённый компьютерный эксперимент *наглядно показывает практическую значимость* выполненной работы.

Полностью ознакомиться с работой можно на сайте https://www.rae.ru/ в рамках проведения XVIII Международного конкурса научно-исследовательских и творческих работ учащихся “Старт в науке” в секции “Информатика”.

РАЗРАБОТКА ТЕСТОВЫХ МАТЕРИАЛОВ СРЕДСТВАМИ ИКТ

Машталова М.С., Наумова А.И.

Санкт-Петербургский государственный университет телекоммуникаций, Санкт-Петербург, e-mail: mashtalovamasha@gmail.com

Средства информационных и коммуникационных технологий все чаще применяют в ОУ для *автоматизации процессов контроля и измерения результативности обучения*. Педагоги используют как специально разработанные средства, нацеленные на педагогические измерения с использованием компьютерной техники, так и контрольно-измерительные подсистемы образовательных электронных изданий и ресурсов, применяемых в ОУ.

Основными преимуществами заданий, представляемых в *компьютерной тестовой форме*, по сравнению с традиционными задачами и вопросами, являются *краткость, логическая структурированность, стандартизованность и единая относительно простая процедура проведения тестирования и оценки его результатов*. Именно эти преимущества делают тесты *наиболее пригодными* для оценки результатов обучения и проверки соответствия этих результатов требованиям государственных стандартов образования.

В 2022-2023 году в Тверском лицее под руководством преподавателя информатики высшей категории А.И. Наумовой ученица 11 физико-математического класса Машталова Мария написала научную работу на тему: “Особенности организации проверки и оценивания знаний с использованием компьютерной техники”.

Цель данной работы заключается в том, чтобы получить *дополнительные знания и навыки* по этой теме.

Задача состоят в том, чтобы подобрать соответствующий материал с последующей систематизацией, обобщением и иллюстрацией текста, а также *практического* решения задачи по разработке и проведению компьютерного эксперимента *программы компьютерного тестирования* на современном языке программирования *Python* с использованием *двух текстовых файлов* (Вопросы и Правильные ответы).

Полностью ознакомиться с работой можно на сайте https://www.rae.ru/ в рамках проведения XVIII Международного конкурса научно-исследовательских и творческих работ учащихся “Старт в науке” в секции “Информатика”.

ОБ АНАЛИЗЕ СЕТЕЙ НА БАЗЕ ИНТЕЛЛЕКТУАЛЬНОГО МОНИТОРИНГА

Меняйленко М.Д., Фоменко М.И.

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

Любая компьютерная сеть, независимо от ее типа, состоит из следующих компонентов:

1) сетевое оборудование;
2) кабельная система;
3) средства коммутации;
4) программное обеспечение;
5) сетевые протоколы;
6) сетевые службы.

Стоит отметить, что этот принцип устройства компьютерных сетей является обобщенным, поскольку каждый компонент обладает очень сложной структурой и состоит из множества подуровней. Тем не менее, все устройства находятся в тесном взаимодействии и работают по единому алгоритму. В свою очередь администрирование сетей Windows направлено на поддержание стабильной работы всех этих компонентов [1, 2].

Интеллектуальный мониторинг корпоративных сетей – критически важная функция ИТ, которая позволяет добиться экономии при повышении производительности инфраструктуры, высокой эффективности деятельности сотрудников, а также предоставляет возможность уменьшить затраты [3, 4].

Этот вид мониторинга позволяет отслеживать и анализировать различные аспекты работы корпоративных сетей, включая использование ресурсов, производительность, безопасность и доступность. Интеллектуальные системы мониторинга могут автоматически обнаруживать и предотвращать проблемы, а также предоставлять рекомендации по оптимизации сетевой инфраструктуры.

Системы сетевого мониторинга (Network Monitoring System, NMS) обычно используется для мониторинга производительности сети, отслеживания трафика, анализа использования ресурсов и выявления сбоев в работе сети. Он предоставляет информацию о состоянии сети, ее компонентов и устройств, а также помогает в обнаружении и устранении проблем, связанных с производительностью.

В отличие от NMS, IDS (система обнаружения вторжений (Intrusion Detection System)) и IPS (система предотвращения вторжений (Intrusion Prevention System)) фокусируются на обнаружении и предотвращении вторжений в сеть. Они могут анализировать сетевой трафик, обнаруживать аномальное поведение и блокировать подозрительные активности, чтобы защитить сеть от несанкционированного доступа или вредоносных действий.

Интеллектуальный сетевой мониторинг может выполняться с помощью различных про-

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