Третий аспект – затраты на обучение и осведомленность сотрудников. Помимо IT-специалистов, все сотрудники организации должны быть осведомлены о принципах и практиках информационной безопасности. Бездействие или неосторожное отношение к безопасности может привести к серьезным угрозам, включая утрату данных, взлом системы или нарушение конфиденциальности. Обучение сотрудников включает проведение семинаров, разработку политик и процедур, а также постоянное напоминание о безопасности информации. Эти затраты на обучение и повышение осведомленности персонала также включаются в общую стоимость информационной безопасности.

Четвертый аспект стоимости информационной безопасности связан с рисками и потенциальными угрозами. Информационные атаки, вирусы и другие угрозы могут причинить серьезный ущерб компании. Поддержание высокого уровня защиты может предотвратить такие атаки и снизить риски финансовых потерь. Ведение пассивной политики безопасности и недостаточные меры защиты могут привести к серьезным последствиям, таким как потеря репутации, судебные иски и прочие потери, как для компании, так и для ее клиентов.

Формула стоимостных аспектов информационной безопасности может включать в себя следующие составляющие:

1. Затраты на приобретение и внедрение средств защиты информации, такие как аппаратное и программное обеспечение, обучение персонала и т.д.

2. Затраты на поддержание и обновление систем информационной безопасности, включая расходы на обслуживание, лицензионные платежи, анализ уязвимостей и т.д.

3. Потери от возможных инцидентов информационной безопасности, такие как утечки данных, кражи конфиденциальной информации, вредоносные программы и др. Оценка таких потерь может включать в себя не только прямые финансовые убытки, но и репутационный ущерб, потерю клиентов и бизнеса, судебные издержки и т.д.

4. Экономический эффект от защиты информации, включая уменьшение рисков и потерь, повышение доверия клиентов и партнеров, усиление конкурентных преимуществ и т.д.

Список литературы

1. Преображенский Ю.П. Информационная безопасность – вызовы современного мира // Вестник Воронежского института высоких технологий. 2017. № 2(21). С. 60-63.

2. Смыкова В.Н., Нечволода В.Э., Орел Д.В. Экономические аспекты информационной безопасности // Студенческая наука для развития информационного общества: сборник материалов X Всероссийской научно-технической конференции с международным участием, Ставрополь, 07–08 ноября 2019 года. Том Часть 1. Ставрополь: Северо-Кавказский федеральный университет, 2019. С. 162-169.

3. Балашова А.В., Преображенский Ю.П. Проблемы обеспечения безопасности в информационных системах // Молодежь и XXI век. 2022. С. 15-19.

4. Компанейцева Г.А. и др. Стоимостные аспекты в концепции экономической безопасности компании // Вестник Московского финансово-юридического университета. 2017. № 3. С. 95-103.

5. Мандрица И.В., Мандрица О.В., Соловьева И.В., Петренко В.И. Метод обоснования затрат на информационную безопасность бюджетных организаций // Вестник Северо-Кавказского федерального университета. 2017. № 1(58). С. 67-71.

КОМПЬЮТЕРНАЯ ГРАФИКА НА ЯЗЫКЕ ПРОГРАММИРОВАНИЯ PYTHON

Макаров П.В., Наумова А.И.

МОУ "Тверской лицей", Тверь, e-mail: a_naumova_46@mail.ru

В процессе исследования формальных моделей часто производится их *визуализация*. Для визуализации алгоритмов используются *блок-схемы*, пространственных соотношений параметров объектов – *чертежи*, моделей электрических цепей – *электрические схемы*. При визуализации формальных моделей с помощью анимации может *отображаться динамика процесса*, *производится построение графиков изменения величин* и т. д.

В настоящее время широкое распространение получили *компьютерные интерактивные визуальные модели*. В таких моделях исследователь может менять начальные условия и параметры протекания процессов и наблюдать изменения в поведении модели.

Используя *компьютерную визуализацию*, в 2022-2023 году в Тверском лицее под руководством преподавателя информатики высшей категории А.И. Наумовой ученик 10 физико-математического класса Макаров Пётр написал научную работу на тему: "Исследование информационных моделей из курса математики на языке программирования Python ".

Цель данной работы заключается в том, чтобы получить *дополнительные знания* по этой теме и *научиться проводить исследования решений математических задач с помощью построения графиков.*

Работа состоит из двух частей: *описательной* (дана характеристика основных этапов разработки информационных моделей) и *практической* (приведён пример разработки алгоритма и программы (скрипта) *полного исследования квадратного уравнения* с использованием вложенных сложных условий, подключения модулей для работы с графикой и созданием функций пользователя с последующей обработкой данных на компьютере). Показаны примеры выполнения программы (скрипта) как в среде программирования, так и выполнение созданного файла .exe.

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-