Международный журнал информационных технологий и энергоэффективности

Том 9 Номер 6 (44)

2024

Международный журнал информационных технологий и энергоэффективности
Т.9 №6(44) 2024 г.

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

СОДЕРЖАНИЕ / CONTENT

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Лозница С.Ю., Гундобин Г.В., Саляхетдинов А.М. Применение дифференциальных уравнений для моделирования и решения практических задач// Международный журнал информационных технологий и энергоэффективности.– 2024. –
Т. 9 № 6(44) ч.2 с. 5–10

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.942

ПРИМЕНЕНИЕ ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ ДЛЯ МОДЕЛИРОВАНИЯ И РЕШЕНИЯ ПРАКТИЧЕСКИХ ЗАДАЧ

Лозница С.Ю., [1]Гундобин Г.В., Саляхетдинов А.М.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ ИМЕНИ ГЛАВНОГО МАРШАЛА АВИАЦИИ А.А. НОВИКОВА", Санкт-Петербург, Россия (196210, город Санкт-Петербург, ул. Пилотов, д.38), e-mail: [1]grishagundobin@gmail.com

В статье рассмотрена тематика применения дифференциальных уравнений для моделирования и решения практических задач. Изучены аспекты применения дифференциальных уравнений для моделирования и решения конкретных практических задач в сфере медицины, физики, биологии. Показано, что использование дифференциальных уравнений в практических аспектах позволяет найти оптимальное решение многих проблем.

Ключевые слова: Дифференциальные уравнения, применение, моделирование, практические задачи.

APPLICATION OF DIFFERENTIAL EQUATIONS FOR MODELING AND SOLVING PRACTICAL PROBLEMS

Loznitsa S.Yu., [1]**Gundobin G.V.**, **Salakhetdinov A.M.**
ST. PETERSBURG STATE UNIVERSITY OF CIVIL AVIATION NAMED AFTER AIR CHIEF MARSHAL A.A. NOVIKOV", St. Petersburg, Russia (196210, St. Petersburg, Pilotov st., 38), e-mail: [1]grishagundobin@gmail.com

The article discusses the topic of using differential equations for modeling and solving practical problems. Aspects of the application of differential equations for modeling and solving specific practical problems in the field of medicine, physics, and biology have been studied. It is shown that the use of differential equations in practical aspects allows one to find the optimal solution to many problems.

Keywords: Differential equations, application, modeling, practical problems.

Введение.

Современная математика применяется при изучении экономических, гуманитарных, биологических, физических, технических и других явлений. Это происходит посредством построения математической модели, учитывающей все существенные связи внутри явления. Под математическим моделированием будем понимать метод исследования процессов или явлений путем построения их математических моделей и исследования этих процессов [1]. Математические модели реального процесса или объекта могут иметь вид формулы, уравнений, системы уравнений, графиков и т.п. Изучая разные задачи экономики, физики, техники, часто можно установить связь между величинами, описывающими тот или иной процесс, и скоростями их изменения относительно других независимых переменных величин.

При этом применяются уравнения, в которых неизвестные функции находятся под знаком производной, называемой дифференциальной. Характерным свойством дифференциальных уравнений является множество решений. Поэтому, решив дифференциальные уравнения, описывающие течение определенного процесса, невозможно однозначно найти зависимость между величинами, характеризующими этот процесс. Чтобы найти конкретное решение уравнения, которое соответствует конкретной задаче, нужно иметь дополнительную информацию, характеризующую исходные условия, то есть решить задачу Коши. Известнейшие практические примеры использования дифференциальных уравнений связаны с моделированием движения океанских течений, воздушных масс, турбулентных потоков в атмосфере, изучение поведения цен на фондовом рынке, анализ распространение эпидемий или динамики численности популяций.

Цель статьи – исследование применения дифференциальных уравнений для моделирования и решения практических задач.

Основная часть.

Упомянем, что дифференциальным уравнением называется нетождественное соотношение между независимой переменной, искомой функцией и ее производными по независимой переменной к определенному порядку включительно.

В общем виде дифференциальное уравнение первого порядка имеет вид $F(x, y, y') = 0$, а дифференциальное уравнение n-го порядка имеет вид:

$$F(x, y, y' \dots y^{(n)}) = 0$$

Решением дифференциального уравнения $F(x, y, y') = 0$ на некотором интервале $I = (a, b)$ называется непрерывно дифференцированная функция $y = \varphi(x)$, таковая, что $F(x,\varphi(x), \varphi'(x) = 0$.

Дифференциальное уравнение имеет бесконечное множество решений, необходимо указать начальное условие $y(x_0) = y_0$, чтобы решить задачу Коши.

Рассмотрим применение дифференциальных уравнений для моделирования и решения конкретных практических задач.

Первым из прикладных направленй использования дифференциальных уравнений для моделирования практических задач будет решение проблем распространения эпидемий на примере Covid-19. Мы живем в динамической среде, в которой протекают разные процессы, и факторы, влияющие на них, также часто изменяются. Атака коронавируса SARS-CoV-2 2019 сильно изменила весь мир и сделала стремительные изменения условий проживания людей в нем. Модификации этого вируса до сих пор атакуют все страны мира.

Смоделируем модель SIR, описывающая распространение инфекционной болезни среди населения и предусматривающая три ее состояния: инфицированное (S – от англ. susceptible), инфекционное (I – от англ. infected) и выздоровившее (R – от англ. recovered) [1 , с. 110–113]. При определенных условиях эти состояния могут превращаться одно в другое по схеме (Рисунок 1) [2].

Рисунок 1 – Модель SIR

Рисунок 2 – Модель SEIR

Описывается системой SIR дифференциальных уравнений:

$$\frac{dS}{dt} = -\frac{\beta \cdot S \cdot I}{N}, \frac{dI}{dt} = \frac{\beta \cdot S \cdot I}{N} - \gamma \cdot I, \frac{dR}{dt} = \gamma \cdot I$$

где S – количество здоровых людей;

I – количество инфицированных людей;

R – количество выздоровевших или умерших людей;

N=S+I+R – общее количество лиц в системе;

β – коэффициент переноса инфекции;

γ – коэффициент излечения.

Модель позволяет оценивать количество инфицированных и определять эффективность стратегий борьбы с болезнью. Существует много модификаций этой модели, которые учитывают разные факторы, влияющие на распространение инфекционной болезни среди избранного населения. Наиболее важные факторы: иммунитет населения, вакцинация и карантинные ограничения и самоизоляция.

У Оксфордской SIR модели для Covid-19 коэффициент переноса инфекции и коэффициент излечения выражаются через новые два параметра:

$$\beta = \frac{R_0}{T_{inf}}, \gamma = \frac{1}{T_{inf}}$$

где R_0 – коэффициент репродукции или среднее количество заражений, вызванных одним больным человеком (зависит от поведения людей и карантинных ограничений);

T_{inf} – активный период или время, которое больной является заразным (характеризует реакцию организма человека на вирус и не зависит от карантинных ограничений) [2].

Известный ученый и профессор прикладной математики Корнеллского университета Стивен Строгац для исследования динамики распространения болезней решает эти модели численно с помощью метода Эйлера или метода Рунге-Кутты [3].

Представим разработку модели класса SEIR, отличающиеся от SIR дополнительным компартментом E – это больные в инкубационном периоде, когда они еще не заразны. Эти модели оказались наиболее успешными в прогнозировании распространения COVID-19 в Китае 2019 [3, с. 13]. Состояния компартментов могут превращаться один в другой по схеме (рис. 2) [2]. Описуется SEIR системой дифференциальных уравнений:

$$\frac{dS}{dt} = -\frac{R_0}{T_{inf}} \cdot \frac{1}{N} \cdot S \cdot I, \frac{dE}{dt} = \frac{R_0}{T_{inf}} \cdot \frac{1}{N} \cdot S \cdot I - \frac{E}{T_{inc}},$$

$$\frac{dI}{dt} = \frac{E}{T_{inc}} - \frac{I}{T_{inf}}, \frac{dR}{dt} = \frac{I}{T_{inf}},$$

где дополнительный параметр T_{inc} – инкубационный период (E – от англ. exposed).

Достаточно гибкая к наполнению калиброванными для выбранного региона параметрами и факторами, актуальными в определенное время именно для него.

Была разработана модель SEIR_U, адаптированную к ситуации в РФ по состоянию на март-май 2020 года [2, с. 8-10]. Модели SEIR можно эффективно использовать для прогнозирования распространения эпидемий, вызванных новыми вирусами или модификациями старых вирусов. Могут использоваться и для количественной оценки эффективности выбранных контрмер, уменьшая с момента их внедрения коэффициенты, характеризующие снижение передаточных коэффициентов инфекции вследствие введения ограничений на контакты и выбранных контрмер.

Рассмотрим также несколько прикладных задач физики, химии, биологии и экономики, которые приводят к дифференциальным уравнениям. Исследуем первичные структуры материи и соответствующие им простейшие формы движения. Скорость охлаждения нагретого тела пропорциональна разности температур тела и окружающей среды. За 20 минут тело остыло от 100 до 50 ºС. до 20 ºС?

Пусть время t – независимая переменная, а x(t) – закон изменения температуры с течением времени, взятой с противоположным знаком, т.е. $-\frac{dx}{dt}$. По условию задачи $-\frac{dx}{dt} = k(x(t) - 15)$, где k – коэффициент пропорциональности.

Кроме того, из условия следует, что x(0) = 100, x(20) = 50.

Решая дифференциальное уравнение, получим:

$$\frac{dx}{x-15} = -kdt, \ln|x-15| = -kt + \ln(C), \text{откуда } x(t) = 15 + Ce^{-kt}$$

Из начальных условий x(0) = 100, x(20) = 50, найдем C и k.

$100 = 15+Ce^0$, C = 85.

$50=15+85e^{-20k}$, $e^{-20k} = \frac{35}{85} = \frac{7}{17}, -20k = \ln\frac{7}{17}$

Откуда $x(t) = 15 + 85e^{\frac{t}{20}\ln\frac{17}{7}} = 15 + 85\left(\frac{17}{7}\right)^{-\frac{t}{20}}$

Вычислим теперь значение времени t охлаждения тела до 20 ºС:

$$x(t) = 15 + 85\left(\frac{17}{7}\right)^{-\frac{t}{20}} = 20.$$

$$85 \cdot (2{,}4)^{\frac{t}{20}} = 5. (2{,}4)^{\frac{t}{20}} = 0.059. t = 65 \text{ минут}$$

Таким образом, будет определено, что тело остынет до 20ºС за 65 минут.

Целый ряд задач в природе, медицине, химии, биологии, экологии по своему прикладному содержанию, математической моделью имеют уравнение в виде $\acute{f}(x) = kf(x)$, где k − const, которое называют дифференциальным уравнением показательного роста.

Пусть скорость размножения микробов пропорциональна их количеству в исходный момент времени. Количество микробов утраивается в течение 4 часов. Найти зависимость количества бактерий от времени.

Пусть P(t) – количество бактерий популяции в момент времени t , скорость размножения является производной P′(t) от количества. Получим дифференциальное уравнение показательного роста. P′(t) = k · P(t), где k > 0 – математическая модель этой задачи.

$$\frac{\mathrm{P}'(\mathrm{t})}{\mathrm{P}(\mathrm{t})} = k \cdot \frac{\mathrm{P}(\mathrm{t})}{\mathrm{P}(\mathrm{t})}, \frac{\mathrm{P}'(\mathrm{t})}{\mathrm{P}(\mathrm{t})} = k,$$

что равносильно уравнению $(\ln(P(t))' = k$, откуда $\ln (P(t) = k\,t + C_1$, C − const.

Назначим $C_1 = \ln C$. Имеем $\ln(P(t)) = kt + C_1$, откуда: $\ln (P(t)) = k\,t + \ln C$. $P(t) = Ce^{kt}$.

Найдем частное решение при начальных условиях: $P(0) = P_0$, $P(4) = 3P_0$. Учитывая, $P(t) = Ce^{kt}$, имеем $P_0 = Ce^0 = C$

Из второго условия имеем $3P_0 = P_0(e^k)^4$, откуда $e^{4k} = 3$ в момент времени t, а $e^k = 3^{1/4}$. Следовательно, количество бактерий определяется законом $P(t) = P_0(3^{1/4}) = P_0 3^{1/4}$

Решение проблем в области медицины связано с законом уменьшения массы лечебного препарата в организме человека, если через 12 часов после введения 10 мг его масса уменьшилась вдвое. Считаем, что скорость растворения прямо пропорциональна времени. Пусть m(t) – масса лечебного препарата в организме человека в момент времени t , тогда m′(t) – скорость его растворения, математической моделью задачи является уравнение [4]:

m′(t)= –kt, где k>0

Общим решением этого дифференциального уравнения является функция

$$\mathrm{m}(\mathrm{t}) = \int (-\mathrm{kt})\mathrm{dt} = -\frac{\mathrm{kt}^2}{2} + \mathrm{C}$$

Используя начальные условия m (0)=10, m(12)=5, имеем:

$$10 = -\frac{k0}{2} + C, C = 10, m(12) = -\frac{k \cdot 12^2}{2} + 10 = 5$$

$$-72k + 10 = 5. -72k = -5. k = \frac{5}{72}$$

Отсюда $m(t) = -\frac{5t^2}{72 \cdot 2} + 10 = -\frac{5t^2}{144} + 10.$

Итак, уменьшение лечебного препарата в организме человека происходит по закону.

$$m(t) = -\frac{5t^2}{144} + 10$$

В этом случае математической моделью задачи является самое простое дифференциальное уравнение.

Заключение

Дифференциальные уравнения являются мощным инструментом для исследования различных динамических процессов в технических, экономических, социальных и природных системах. Использование математического моделирования на основе дифференциальных уравнений позволяет прогнозировать поведение системы с динамическими процессами в будущем и устанавливать оптимальные стратегии управления ими. В статье рассмотрены различные направления применения дифференциальных уравнений для моделирования и решения конкретных практических задач.

Список литературы

1. Keeling M., Rohani P. Modeling infectious diseases in humans and animals. – Princeton, USA : Princeton University Press, 2018. – p.464
2. Strogatz S. Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering. 2nd ed. – Boulder, USA : Westview Press, 2018. – p.528
3. Применение дифференциальных уравнений для решения прикладных задач [Электронный ресурс] : учеб. пособие / авт.-сост.: Л. И. Родина, А. В. Егорова ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2022. – 83 с.
4. Мальцев Н.М., Медведева Н.В. Применение дифференциальных уравнений для математического моделирования процессов природы//Материалы IX Международной студенческой научной конференции «Студенческий научный форум» URL: https://scienceforum.ru/2017/article/2017040262 (дата обращения: 11.04.2024).

References

1. Keeling M., Rohani P. Modeling infectious diseases in humans and animals. – Princeton, USA : Princeton University Press, 2018. – p.464
2. Strogatz S. Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering. 2nd ed. – Boulder, USA : Westview Press, 2018. – p.528
3. Application of differential equations for solving applied problems [Electronic resource] : textbook. the manual / author-comp.: L. I. Rodina, A.V. Egorova; Vladimir State University named after A. G. and N. G. Stoletov. – Vladimir : Publishing House of the All-Russian State University, 2022. – p.83
4. Maltsev N.M., Medvedeva N.V. Application of differential equations for mathematical modeling of natural processes // Proceedings of the IX International Student Scientific Conference "Student Scientific Forum" URL: https://scienceforum.ru/2017/article/2017040262 (date of application: 04/11/2024).

Удальцов К.Р. Искусство тестирования программного обеспечения: методы и подходы к созданию надежных тестов// Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 6(44) с. 11–15

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.052

ИСКУССТВО ТЕСТИРОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ: МЕТОДЫ И ПОДХОДЫ К СОЗДАНИЮ НАДЕЖНЫХ ТЕСТОВ

Удальцов К.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: 2003.06.10kr@gmail.com

В данной статье рассматривается важность и методы создания надежных тестов программного обеспечения. Описываются методы черного ящика, такие как тестирование эквивалентных классов и тестирование граничных значений, а также методы белого ящика, включая тестирование покрытия кода и тестирование путей выполнения. Автоматизированное тестирование рассматривается как эффективный способ повышения надежности и ускорения процесса тестирования. В заключение подчеркивается важность планирования и организации тестирования, анализа результатов и составления отчетов для обеспечения качества программного обеспечения.

Ключевые слова: Тестирование программного обеспечения, надежные тесты, черный ящик, белый ящик, тестирование эквивалентных классов, тестирование граничных значений, тестирование покрытия кода, тестирование путей выполнения, автоматизированное тестирование, планирование тестирования, анализ результатов, отчеты о тестировании.

THE ART OF SOFTWARE TESTING: METHODS AND APPROACHES TO CREATING RELIABLE TESTS

Udaltsov K.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: 2003.06.10kr@gmail.com

This article discusses the importance and methods of creating reliable software tests. Black box methods such as equivalent class testing and boundary value testing are described, as well as white box methods including code coverage testing and execution path testing. Automated testing is considered as an effective way to increase reliability and speed up the testing process. In conclusion, the importance of planning and organizing testing, analyzing results, and compiling reports to ensure software quality is emphasized.

Keywords: Software testing, reliable tests, black box, white box, equivalent class testing, boundary value testing, code coverage testing, execution path testing, automated testing, test planning, results analysis, test reports.

Введение

Тестирование программного обеспечения является неотъемлемой частью разработки программных продуктов. Это процесс, который позволяет выявить ошибки и дефекты в программе, а также убедиться в ее соответствии требованиям и ожиданиям пользователей. Качество тестирования напрямую влияет на качество и надежность программного

обеспечения. В данной статье рассматриваются различные методы и подходы к созданию надежных тестов, которые помогут повысить эффективность и эффективность тестирования.

1. Методы черного ящика

Методы черного ящика основаны на анализе программы без учета ее внутренней структуры. [1] Этот подход позволяет проверить функциональность программы, не зная о ее внутренней реализации. Вот некоторые методы черного ящика:

- Тестирование эквивалентных классов

Этот метод основан на разделении возможных входных данных на эквивалентные классы, которые должны вести себя одинаково. Затем выбираются представители каждого класса для тестирования. Это позволяет сократить количество тестов, сохраняя при этом покрытие различных сценариев.

- Тестирование граничных значений

Метод тестирования граничных значений заключается в проверке программы на предельных значениях входных данных. Это позволяет выявить ошибки, которые могут возникнуть при обработке крайних случаев. Например, если программа должна обрабатывать числа от 1 до 100, то тестирование граничных значений включает проверку для 1, 100 и значений рядом с ними.

2. Методы белого ящика

Методы белого ящика основаны на анализе внутренней структуры программы. Этот подход позволяет проверить правильность работы программы на основе ее кода и алгоритмов. [2] Вот некоторые методы белого ящика:

- Тестирование покрытия кода

Этот метод основан на измерении покрытия кода тестами. Цель состоит в том, чтобы проверить, насколько хорошо тесты охватывают код программы. Популярные метрики покрытия кода включают покрытие строк, покрытие ветвей и покрытие условий.

- Тестирование путей выполнения

Этот метод направлен на проверку всех возможных путей выполнения в программе. Пути выполнения представляют собой последовательности операций и условий, которые могут быть выполнены программой. Тестирование путей выполнения позволяет выявить ошибки, связанные с неправильной логикой программы или недостаточным покрытием различных сценариев.

3. Автоматизированное тестирование

Автоматизированное тестирование является методом, который использует программные инструменты и скрипты для выполнения тестов. Это позволяет повторно использовать тесты, ускоряет процесс тестирования и уменьшает вероятность человеческих ошибок. [3] Автоматизированное тестирование может быть применено как к методам черного ящика, так и к методам белого ящика.

Планирование и организация тестирования

Эффективное тестирование программного обеспечения требует хорошо спланированного и организованного подхода. Вот некоторые важные аспекты планирования и организации тестирования:

*Определение целей тестирования**:*** Первым шагом является определение целей тестирования. Что именно вы хотите проверить и какие аспекты программы требуют особого внимания? Цели тестирования могут включать проверку функциональности, производительности, безопасности и других аспектов программы.

Создание тестовых планов и сценариев: На основе целей тестирования необходимо разработать тестовые планы и сценарии. Тестовый план описывает общую стратегию тестирования, включая ресурсы, расписание и ожидаемые результаты. Сценарии тестирования представляют собой конкретные шаги и данные, которые будут использованы для тестирования программы.

Выбор подходящих методов тестирования: Исходя из целей тестирования и характеристик программы, выберите подходящие методы тестирования. Комбинируйте методы черного ящика и белого ящика, используйте тестирование граничных значений и тестирование покрытия кода в зависимости от требований проекта.

Использование автоматизированного тестирования: В случае, если это возможно, рекомендуется использовать автоматизированное тестирование. Это позволяет повторно использовать тесты, автоматизировать выполнение тестовых сценариев и ускорить процесс тестирования. Существуют различные инструменты и фреймворки для автоматизации тестирования, которые могут быть адаптированы под ваши потребности.

Управление тестовыми данными: Тестирование требует разнообразных тестовых данных, которые должны быть правильно управляемыми. Создайте наборы тестовых данных, которые покрывают различные сценарии и граничные случаи. Обратите внимание на конфиденциальность и безопасность данных, особенно если ваши тестовые данные содержат конфиденциальную информацию.

*Анализ и отчетность результатов**:*** После выполнения тестов необходимо проанализировать результаты и составить отчеты. Зафиксируйте найденные ошибки и дефекты, оцените покрытие кода и выполнение тестовых сценариев. Отчеты о тестировании помогут команде разработки понять текущее состояние программы и принять меры для устранения проблем.

Заключение:

Создание надежных тестов программного обеспечения - это сложный и ответственный процесс, который требует внимательного планирования и организации. Комбинация методов черного ящика и белого ящика, таких как тестирование эквивалентных классов, тестирование граничных значений, тестирование покрытия кода и тестирование путей выполнения, позволяет достичь более полного покрытия различных аспектов программы.

Список литературы

1. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO//Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
2. Красов А. В. и др. Программная реализация средств предотвращений вторжений и аномалий сетевой инфраструктуры.
3. Сахаров Д. В. и др. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IOT-сети//Научно-аналитический

журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». – 2020. – №. 2. – С. 86-94.
4. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных//Региональная информатика и информационная безопасность. – 2020. – С. 260-262.
5. Волкогонов В. Н. и др. Анализ безопасности wi-fi сетей//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 270-275.
6. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411.
7. Небаева К. А. Разработка необнаруживаемых стегосистем для каналов с шумом //СПб.: СПбГУТ. – 2014. – Т. 176.
8. Ахрамеева К. А. и др. Анализ средств обмена скрытыми данными злоумышленниками в сети интернет посредством методов стеганографии //Телекоммуникации. – 2020. – №. 8. – С. 14-20.
9. Березина Е. О., Виткова Л. А., Ахрамеева К. А. Классификация угроз информационной безопасности в сетях IOT//Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 2. – С. 11-18.
10. Бирих Э. В., Ферапонтова С. С. К вопросу об аудите персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 111-114.
11. Бирих Э. В. и др. Исследование вопросов повышения уровня защищенности органов исполнительной власти //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 107-110.

References

1. Krasov A. V. et al. Methods of Packet Switching in CISCO Networks // Proceedings of the All-Russian Scientific and Practical Conference "National Security of Russia: Actual Aspects" of the State Research Institute "National Development". July 2018. – 2018. p. 31-35.
2. Krasov, A. V., et al. Software Implementation of Intrusion and Anomaly Prevention Tools for Network Infrastructure.
3. Sakharov, D. V., et al. Ispol'zovanie matematicheskikh metody prognozirovanii dlya otsenki naload na vychuchutel'nuyu vozdushnosti IOT-neti [Use of mathematical methods of forecasting for assessing the load on the computing power of the IOT network]. – 2020. – №. 2. p. 86-94.
4. Gelfand A. M. Methods of Choosing Stegocontainers for Data Transfer//Regional Informatics and Information Security. – 2020. p. 260-262.
5. Volkogonov V. N. et al. Analysis of the security of wi-fi networks // Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. p. 270-275.
6. Budarny, G. S., et al. Varieties of Security Violations and Typical Attacks on the Operating System//Actual Problems of Infotelecommunications in Science and Education (APINO, 2022). – 2022. p. 406-411.
7. Nebaeva K. A. Development of undetectable stegosystems for channels with noise. – 2014. – T. 176.

8. Akhrameeva K. A. et al. Analysis of the means of exchanging hidden data by intruders on the Internet through steganography methods. – 2020. – №. 8. p. 14-20.
9. Berezina E. O., Vitkova L. A., Akhrameeva K. A. Classification of Information Security Threats in IOT Networks. Series 1: Natural and Technical Sciences. – 2020. – №. 2. p. 11-18.
10. Birikh E. V., Ferapontova S. S. On the Issue of Personal Data Audit//Actual Problems of Infotelecommunications in Science and Education (APINO 2018). – 2018. p. 111-114.
11. Birikh E. V. et al. Issledovanie voprosy povysheniya urovannosti zashchnosti organov executive vlasti [Study of issues of increasing the level of protection of executive authorities]//Aktual'nye problemy infotelekomtelekomatsii v nauke i obrazovaniya (APINO, 2018). – 2018. p. 107-110.

Гуреев В.А., Храмцов О.В., Тимофеев А.М. Исследование актуальности Data Loss Prevention системы в условиях дистанционной работы// Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 6(44) с. 16–25

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

ИССЛЕДОВАНИЕ АКТУАЛЬНОСТИ DATA LOSS PREVENTION СИСТЕМЫ В УСЛОВИЯХ ДИСТАНЦИОННОЙ РАБОТЫ

[1]Гуреев В.А., Храмцов О.В., Тимофеев А.М.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: [1]gureevvadim62@gmail.com

В данной статье рассмотрена актуальность такого средства обеспечения информационной безопасности данных, как Data Loss Prevention системы в непростое время пандемии, в условиях применения дистанционных технологий. Также было проведено небольшое описание и сравнение Data Loss Prevention систем, представленных на Российском и международном рынке.

Ключевые слова: DLP системы, безопасность данных, информационная безопасность, дистанционная работа, предотвращение потери данных.

THE STUDY OF THE RELEVANCE OF THE DATA LOSS PREVENTION SYSTEM IN THE CONTEXT OF REMOTE WORK

[1]Gureev V.A., Khramtsov O.V., Timofeev A.M.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: [1]gureevvadim62@gmail.com

This article examines the relevance of such a means of ensuring information security of data as the Data Loss Prevention system in a difficult time of the pandemic, in the context of the use of remote technologies. A short description and comparison of Data Loss Prevention systems presented on the Russian and international markets was also carried out.

Keywords: DLP systems, data security, information security, remote operation, data loss prevention.

С развитием технических систем, человек стремится создать максимально комфортные условия работы для себя. Применения дистанционных технологий позволяет сотруднику выполнять поставленные задачи, находясь не на рабочем месте. Так же причина дистанционного режима работы может быть связана с болезнью работника или не благоприятной ситуацией в стране, например с пандемией. Тут перед работодателем встает вопрос о защите конфиденциальных данных компании. Так как сотрудник работает из дома его часы, проведенные за работой, контролируются им же, вдобавок его персональный компьютер имеет доступ к данным организации. Работодатель заинтересован в защите данных от утечек и контроле своих сотрудников. Системы Data Loss Prevention способны подключаться на расстоянии к рабочим столам персональных компьютеров, что позволит в режиме реального времени проконтролировать работу работника. Система может

фиксировать распечатывание документов и их копирование, отправку сообщений на неизвестные или личные электронные адреса. Важно понимать, что утечка данных может нанести серьезный вред организации. Data Loss Prevention так же может использоваться в условиях очной работы сотрудников для защиты данных компании и контроля сотрудников. Применение этой системы сократит риски утечки данных по неосторожности или злому умыслу. Так же можно выделить неочевидные способы использование этой системы. Обеспечение юридической поддержки. Задача DLP состоит не только в том, чтобы предотвратить утечки, но еще и при наличии судебного разбирательства, предоставить доказательства злоумышленной деятельности. DLP как инструмент мотивации. Когда сотрудники осознают, что их трудовая деятельность находится под мониторингом, появляется большая ответственность за рабочий процесс. И это в свою очередь приводит к улучшению климата в коллективе. Как хранилище. DLP-технология гарантирует сохранность всей информации, поскольку содержит в своём архиве все коммуникации сотрудников, к которым в случае необходимости можно будет обратиться. Целью данной работы является исследование актуальности Data Loss Prevention систем в условиях применения дистанционных технологий [1].

Что же такое DLP система

DLP-система — специализированное программное обеспечение, предназначенное для защиты компании от утечек информации. Эта аббревиатура на английском расшифровывается как Data Loss Prevention (предотвращение потери данных) или Data Leakage Prevention (предотвращение утечки данных). [7]

Какие DLP системы уже есть на рынке

Falcongaze SecureTower

SecureTower — это DLP система 2 в 1 (Защита от утечек данных + контроль активности пользователей). Клиент получает полный контроль корпоративной информации за счет мониторинга максимального числа коммуникационных каналов и протоколов передачи данных. Все действия сотрудников автоматически анализируются и, в случае выявления нарушения, система мгновенно отправляет уведомление руководителю или службе безопасности. [8]

InfoWatch Traffic Monitor

DLP-система, основанная на методах полноценного анализа контента информационных потоков, эффективно предотвращает утечки конфиденциальной информации. InfoWatch Traffic Monitor демонстрирует высокую надежность в работе даже при значительных нагрузках на сотнях тысяч рабочих мест, способная не только мониторить, но и блокировать подозрительные действия. Система способна обнаруживать и распознавать сложные текстовые и графические объекты, даже если нарушитель попытается изменить их и скрыть свои действия. [9]

Zecurion

В комплекс Zecurion DLP входят средства для решения различных задач в рамках защиты информации, которые тесно интегрируются друг с другом в любой комбинации и составляют единую систему защиты от утечек. Все четыре системы могут использоваться самостоятельно для решения специальных задач и в то же время дополняют друг друга. Zgate, Zlock, Zdiscovery и Zserver управляются из единой консоли Zconsole с общим удобным интерфейсом. [10]

Symantec

Защита данных по всем каналам утечек: облака, электронная почта, веб-сайты, рабочие станции и серверы, системы хранения. Комплексные технологии детектирования с минимальным числом ложных срабатываний. Единая консоль для управления политиками, реагирования на инциденты, создания отчетов и администрирования. Поддержка множества продуктов для анализа поведения пользователей, шифрования, классификации данных и управления правами доступа. [11]

Solar Dozor

Высокопроизводительная DLP-система для блокирования утечек информации, контроля коммуникаций сотрудников и выявления признаков корпоративного мошенничества. Ее возможности обеспечивают контроль коммуникаций сотрудников, блокировку или изменение нежелательных сообщений, выявление и мониторинг групп риска, а также ретроспективный анализ архива коммуникаций для проведения расследований. Кроме этого, Solar Dozor может анализировать поведение пользователей (User Behavior Analytics). [12]

МФИ Софт – Гарда Предприятие

Аппаратно-программный комплекс для контроля и анализа информационных потоков компании, защиты и предотвращения утечек конфиденциальной информации. Решение совмещает в себе классические инструменты DLP и мощные аналитические возможности. «Гарда Предприятие» разработана для реализации ежедневных задач ИБ/ЭБ/HR-специалистов — она автоматизирует рутинную работу и позволяет видеть полную картину коммуникаций в любой момент времени. [13]

Сравнение DLP систем

Для сравнения систем была составлена таблица (Таблица 1).

Таблица 1 – Сравнение DLP систем

Название	**Falcongaze SecureTower**	**InfoWatch Traffic Monitor**	**Zecurion**	**Symantec**	**Solar Dozor**	**МФИ Софт – Гарда Предприятие**
Потребители	Крупные фирмы и небольшие предприятия	Компании как маленькие, так и крупные	Государственный сектор, компании могут быть как маленькие, так и крупные	Крупнейшие корпорации, насчитывающие до 100 тысяч работников	Государственные предприятия и крупные компании	Бизнес среднего и крупного уровня
Предоставление услуг	Техподдержка, помощь по внедрению, проведение обучения, а также оказание	Услуги консалтинга в системе информационной безопасности	Проведение аудита, оказание консалтинговых услуг, оказание техподдер	Обучение персонала при помощи партнеров, внедрение	Наличие технической поддержки, возможность пройти партнерское и клиентское обучение,	Возможность проведения удаленного обучения, оказание техническо

	помощи по формированию информационной защиты в организации		жки, проведение обучения		услуги консалтинга и аутсорсинга	й поддержки
Язык панели управления	Русский, английский, французский, испанский, итальянский, корейский, турецкий	Украинский, международный английский, русский, белорусский	Английский и русский	Английский, русский, японский, китайский, французский	Русский и английский	Только русский
Запись в журнал	+	+	+	+	+	+
Сохранение файлов (теневое копирование)	+	+	+ для Zlock и Zgate	+	+	+
Уведомление администратора	+ по электронной почте	+ по электронной почте	+ по электронной почте	+ по электронной почте регистрация событий через SMTP, Syslog сообщения	+ по электронной почте	+ по электронной почте
Блокировка соединения	Да, SMTP, HTTP, SMTPs, HTTP	Да, SMTP, HTTP(S)	все контролируемые каналы (около 150 штук)	Да, любой протокол распознанный системой	Да, SMTP, HTTP	НЕТ
Автоизменение сообщений	НЕТ	НЕТ	+	+	+	НЕТ

Актуальность внедрения DLP систем в организации

Большинство предпринимателей думает, что DLP-системы используются исключительно ради обеспечения информационной безопасности, но на самом деле DLP-системы уже давно используются не только для защиты от утечек данных. Рост объема технологий сменился их развитием по вертикали. DLP начали расти вглубь, качество анализа

и перехвата контента улучшилось. Данные из DLP теперь очень ценны для принятия любых решений по управлению бизнесом. Это позволяет не только обеспечить информационную безопасность, но и сервис для других подразделений компании — от HR до экономической безопасности.

Общие сведения о DLP-системе Falcongaze SecureTower 6.3.

Российская компания Falcongaze разработала SecureTower, DLP-систему, которая является программным продуктом, позволяющим предотвратить утечку корпоративных данных, и обладает средствами для анализа деятельности персонала. SecureTower способствует реализации комплексного подхода к обеспечению защиты конфиденциальной информации и является мощным инструментом управления репутационными, операционными и правовыми рисками. Это позволяет оптимизировать бизнес-процессы в компании и обеспечить ее информационную и экономическую безопасность. Система разделена на две части: серверную и клиентскую. В северную часть входят: центральный сервер, сервер индексирования, сервер пользователей, сервер контроля агентов, сервер обработки почты, сервер сетевого трафика, сервер ICAP, сервер распознавания, сервер безопасности и отчетности, сервер журналирования событий. Интерфейсная часть включает в себя консоль администратора и пользователя. [14]

Системные и технические требования для установки Falcongaze SecureTower.

Системные и технические требования приведены в виде таблицы (Таблица 2). [15]

Таблица 2 - Технические требования

Характеристика	Серверное оборудование	Клиентская часть (работа с консолью)	Конечные точки (для агентской схемы)
Процессор	2,2+ ГГц (4 ядра и более)	2 ГГц и выше	600 МГц и выше
Сетевые адаптеры	1 Гбит (2 адаптера при централизованном перехвате)	100 Мбит/1 Гбит	
Оперативная память	6 ГБ и более	не менее 4 ГБ	256 МБ и более
Жесткий диск	100 ГБ раздел для операционной системы и файлов SecureTower (RAID1 / RAID10); раздел для хранения перехваченных данных на RAID1 / RAID10	300 МБ свободного пространства	15-25 МБ свободного пространства
Видеокарта		поддержка DirectX 7.0 и выше (разрешение экрана 1024 x 768)	
Поддерживаемые ОС	Microsoft Windows Server 2008R2/2012/2016/2019 x64 Для сервера централизованного перехвата	Microsoft Windows Vista SP2 / 7 SP1 / 8 / 8.1 / 10 / Server 2008 R 1 / Server 2012 (x86 или x64)	Microsoft Windows XP SP3/Vista/7/8/10/Server 2003/2008/2012/2016/2019 (x86/x64)

	только Microsoft Windows Server 2008R2		
Предустановленные компоненты	Microsoft .Net Framework 4.7 Microsoft Visual C++ Redistributable 2008, 2010, 2013 и 2015 (x86 и x64)	Microsoft .Net Framework 4.7 Microsoft Visual C++ Redistributable 2008, 2010, 2013 и 2015 (x86 и x64)	

Функции Falcongaze SecureTower для предотвращения утечек информации.

В DLP-системе Falcongaze SecureTower выделяются следующие функции. Выявление утечек конфиденциальной информации и инсайдерской деятельности. Контроль каналов передачи данных и действий сотрудников на их рабочих компьютерах. Блокировка портов подключения, доступа веб-ресурсов и запуска приложений. Анализ контента пересылаемых файлов, в том числе текст, изображения и аудиофайлы. Расследование инцидентов информационной безопасности, причин нарушений правил безопасности. Так же можно выделить неявные функции системы. Например, Сотрудники, осознавая факт их контроля, будут более ответственно подходить к своей работе, стараясь не совершать ошибок. Более того компания сможет проанализировать рабочий день сотрудников, что поможет оптимизировать их работу. [16]

Преимущества и недостатки Falcongaze SecureTower 6.3.

Преимущества:

- Высокая скорость внедрения при наличии всех классических технологий контроля;
- Наличие широкого спектра возможностей для блокировки;
- Поддержка контроля различных мессенджеров;
- Широкое функциональное оснащение для перехвата и обработки траффика;
- Контроль многочисленных каналов обмена данными;
- Возможность наблюдения за деятельностью работников на рабочем месте;
- Удобная, наглядная отчетная система, в которой есть функция создания собственного отчета;
- Интерактивные графические анализаторы для мониторинга контактов сотрудника;
- Быстрый поиск по перехваченным данным;
- Ведение архива коммуникации сотрудников;
- Распознавание печатей и текста на изображениях;
- Низкие системные требования;
- Простой интерфейс и гибкие настройки системы.

Недостатки:

- Блокировка принтера невозможна;
- Отсутствие блокировки каналов сетевой связи;
- Отсутствует интерфейс для мобильных устройств;
- Отсутствие спецагента для мобильных ОС;
- Отсутствует подтверждение присутствия в реестре отечественного ПО.

Применение DLP-системы в условиях дистанционных технологий.

Актуальность применения дистанционных технологий на предприятиях выражается в повышении эффективности работника. Сотруднику не нужно тратить время на дорогу до места работы, так же находясь в служебной командировке, он может продолжить выполнять свои обязанности. Более того применение дистанционных технологий не всегда добровольное решение компании. В 2020г. из-за пандемии, на удаленную работы были отправлены большое количества предприятий. Компании, которые не имели возможность обеспечить достаточные условия работы для сотрудников удаленно, столкнулись с трудностями и понесли финансовые потери. По данным аудиторской компании FinExpertiza, за весну 2020 года более трети Российских организаций оказались в убытке на 1,65 трлн рублей, а остальные заработали 3,05 трлн рублей. В итоге прибыль российского бизнеса составила 1,4 трлн рублей, это на 67 % меньше, чем весной прошлого года. [17]

DLP-система в условиях дистанционных технологий.

В условиях применения дистанционных технологий подразумевается, что сотрудник будет работать на своем домашнем компьютере, следовательно, будет иметь доступ к данным предприятия. Поднимается проблема о безопасности компании и утечки персональной информации.

Для решения вышесказанных проблем предлагается рассмотреть DLP-систему Falcongaze SecureTower 6.3, как инструмент защиты компании в условиях дистанционных технологий.

Инструменты контроля Falcongaze SecureTower в условиях дистанционных технологий.

Из пяти основных функций DLP-системы Falcongaze SecureTower можно выделить четыре: выявление, контроль, анализ, расследование. Выявление утечек важная функция которая остается актуальной в условиях дистанционных технологий, так как DLP-система способна фиксировать нарушения со стороны сотрудника, он не сможет выкрасть сведения организации незаметно. Falcongaze SecureTower способен контролировать работников, проверяя их деятельность в период рабочего времени. DLP-система может подключаться к рабочему столу сотрудника, что позволит проверить добросовестное выполнение работы в режиме реального времени и при необходимости принять меры. Функция анализа позволит оптимизировать работу предприятия, выявить недостатки рабочего дня. Расследование включает в себя сохранения трафика всех рабочих, их электронные письма и действия. Это поможет предоставить доказательства в случаи необходимости. Функция блокировки портов считается не актуальной, так как предприятие не может пойти на ограничение доступа сотрудника к собственному компьютеру.

Так же остается актуальным неявное влияние DLP-системы, сотрудник будет качественнее выполнять свою работу, зная, что за ним видеться контроль. Работодатель же найдет проблемные места и сможет улучшить условия работы подчинённых в условиях дистанционных технологий. Например, удлинить или же укоротить рабочий день.

Заключение

С развитием технологий, появилась возможность выполнять работу, не находясь на рабочем месте. В связи с этим появились проблемы и вопросы связанные с безопасностью предприятия. Предложенная в данной статье DLP-система, рассматривается как инструмент защиты в условиях дистанционных технологий. Программа способна обеспечить высокую

информационную безопасность для компании, имея множества различных функций защиты и контроля, более того система способна решать широкий спектр бизнес-задач, не связанных с ее прямой целью. В условиях удаленной работы Falcongaze SecureTower 6.3 закрывает слабые места IT-безопасности и держит под контролем не только данные, но и каждого сотрудника, фиксируя нарушения. Используя рассмотренную в данной статье DLP-систему предприятия смогут, не только справиться с трудностями удаленной работы, но и оптимизировать свой график для максимального достижения целей.

Список литературы

1. В. В. Андрианов С. Л. Зефиров В. Б. Голованов Н. А. Голдуев Обеспечение информационной безопасности бизнеса//Информационная безопасность: науч.-техн. книга: электр. версия. 2010. С. 265. URL: https://pqm-online.com/assets/files/lib/books/andrianov.pdf. Дата публикации: 2010.
2. Боридько И. С., Забелиский А. А., Коваленко Ю. И. Применение DLP-систем для защиты персональных данных. // Безопасность информационных технологий: науч.-техн. журнал: электр. версия. 2012. С. 20-24. URL: https://bit.mephi.ru/index.php/bit/article/view/424. Дата публикации: 2012. Режим доступа: для зарегистрир. пользователей
3. Российская Федерация. Законы. Конституция РФ (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). послед. ред.//КонсультантПлюс: сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_28399/. (дата обращения: 22.03.2024). Режим доступа: для зарегистрир. пользователей
4. Каскинов И.И. Галимов Р.Р. Анализ эффективности DLP-систем//В сборнике: современные информационные технологии в науке. 13.11.2014. С. 128-130. URL: https://elibrary.ru/item.asp?id=22566563. Дата публикации: 13.11.2014.
5. Каширина Е.А. DLP-системы как средство защиты информации // конференция: роль и место информационных технологий в современной науке Саранск, 03.02.2016. С. 17-19. URL: https://elibrary.ru/item.asp?id=25358627. Дата публикации: 03.02.2016.
6. Российская Федерация. Законы. Приказ ФСТЭК России от 14 марта 2014 г. N 31. : послед. ред.//ФСТЭК России: сайт. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31. (дата обращения: 22.03.2024).
7. Solar Dozor: офиц. сайт. URL: https://rt-solar.ru/products/solar_dozor/blog/2080. (дата обращения: 22.03.2024).
8. Falcongaze. офиц. сайт. URL: https://falcongaze.com/ru/product/what-is-the-secure-tower-dlp-system/. (дата обращения: 22.03.2024).
9. Infowatch. офиц. сайт. URL: https://www.infowatch.ru/products/traffic-monitor. (дата обращения: 22.03.2024).
10. Zecurion. офиц. сайт. URL: https://www.zecurion.ru/products/zlock/description/dlp-solution/. (дата обращения: 22.03.2024).
11. Symbuy. офиц. сайт. URL: https://www.symbuy.ru/files/Symantec-DLP.pdf. (дата обращения: 22.03.2024).
12. Solar Dozor: офиц. сайт. URL: https://rt-solar.ru/products/solar_dozor/ (дата обращения: 22.03.2024).

13. Gardatech. офиц. сайт. URL: https://gardatech.ru/produkty/gp/. (дата обращения: 22.03.2024).
14. Falcongaze. офиц. сайт. URL: https://falcongaze.com/ru/support/documentation/quick-start/general-information/system-structure.html
15. Falcongaze. офиц. сайт. URL: https://falcongaze.com/ru/product/tech-info/. (дата обращения: 22.03.2024).
16. Falcongaze. офиц. сайт. URL: https://falcongaze.com/ru/. (дата обращения: 22.03.2024).
17. Sberbank. офиц. сайт. URL: https://www.sberbank.ru/ru/s_m_business/pro_ business/poteri-rossijskogo-biznesa-ot-koronavirusa (дата обращения: 22.03.2024).

References

1. V. V. Andrianov S. L. Zefirov V. B. Golovanov N. A. Golduev Ensuring business information security // Information security: scientific and technical. Book: elektr. version. 2010. Pp. 265. URL: https://pqm-online.com/assets/files/lib/books/andrianov.pdf . Date of publication: 2010.
2. Boridko I. S., Zabelisky A. A., Kovalenko Yu. I. Application of DLP systems for personal data protection. // Information technology security: scientific and technical Magazine: elektr. version. 2012. Pp. 20-24. URL: https://bit.mephi.ru/index.php/bit/article/view/424 . Date of publication: 2012. Access mode: for registration. users
3. The Russian Federation. Laws. The Constitution of the Russian Federation (adopted by popular vote on 12.12.1993 with amendments approved during the all-Russian vote on 07/01/2020). last ed.//ConsultantPlus: website. URL: https://www.consultant.ru/document/cons_doc_LAW_28399/. (date of application: 03/22/2024). Access mode: for registration. users
4. Kaskinov I.I. Galimov R.R. Efficiency analysis of DLP systems // In the collection: modern information technologies in science. 13.11.2014. Pp. 128-130. URL: https://elibrary.ru/item.asp?id=22566563 . Date of publication: 13.11.2014.
5. Kashirina E.A. DLP-systems as a means of information protection // conference: the role and place of information technologies in modern science Saransk, 02/03/2016. pp. 17-19. URL: https://elibrary.ru/item.asp?id=25358627 . Date of publication: 02/03/2016.
6. Russian Federation. Laws. Order of the FSTEC of Russia dated March 14, 2014 N 31.: last ed.//FSTEC of Russia: website. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31. (date of access: 03/22/2024).
7. Solar Dozor: official website. URL: https://rt-solar.ru/products/solar_dozor/blog/2080. (date of access: 03/22/2024).
8. Falcongaze. ofic. website. URL: https://falcongaze.com/ru/product/what-is-the-secure-tower-dlp-system/. (date of access: 03/22/2024).
9. Infowatch. ofic. website. URL: https://www.infowatch.ru/products/traffic-monitor. (date of access: 03/22/2024).
10. Zecurion. ofic. website. URL: https://www.zecurion.ru/products/zlock/description/dlp-solution/. (date of access: 03/22/2024).
11. Symbuy. ofic. website. URL: https://www.symbuy.ru/files/Symantec-DLP.pdf. (date of application: 03/22/2024).
12. Solar Dozor: official website. URL: https://rt-solar.ru/products/solar_dozor / (date of access: 03/22/2024).

13. Gardatech. ofic. website. URL: https://gardatech.ru/produkty/gp/. (date of access: 03/22/2024).
14. Falcongaze. ofic. website. URL: https://falcongaze.com/ru/support/documentation/quick-start/general-information/system-structure.html
15. Falcongaze. ofic. website. URL: https://falcongaze.com/ru/product/tech-info/. (date of access: 03/22/2024).
16. Falcongaze. ofic. website. URL: https://falcongaze.com/ru /. (date of access: 03/22/2024).
17. Sberbank. ofic. website. URL: https://www.sberbank.ru/ru/s_m_business/pro_ business/poteri-rossijskogo-biznesa-ot-koronavirusa (date of access: 03/22/2024).

Кравченко Д.А. Многозадачность в WINDOWS от NT до 11 // Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 6(44) с. 26–33

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.45

МНОГОЗАДАЧНОСТЬ В WINDOWS ОТ NT ДО 11

Кравченко Д.А.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: den.151.22839@gmail.com

В статье описывается понятие, функции и особенности многозадачности в операционной системе Windows. Анализируются следующие операционные системы: Windows NT, Windows XP, Windows 7, Windows 8, Windows 10, Windows 11. Также проводиться сравнительный анализ данных систем, делается вывод о них.

Ключевые слова: многозадачность, операционные системы, Windows NT, Windows XP, Windows 7, Windows 8, Windows 10, Windows 11, многозадачность в Windows NT, многозадачность в Windows XP, многозадачность в Windows 7, многозадачность в Windows 8, многозадачность в Windows 10, многозадачность в Windows 11.

MULTITASKING IN WINDOWS FROM NT TO WINDOWS 11

Kravchenko D.A.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: 2003.06.10kr@gmail.com

The article describes the concept, functions and features of multitasking in the Windows operating system. The following operating systems are analyzed: Windows NT, Windows XP, Windows 7, Windows 8, Windows 10, Windows 11. A comparative analysis of these systems is also carried out, and a conclusion is drawn about them..

Keywords: Multitasking, operating systems, Windows NT, Windows XP, Windows 7, Windows 8, Windows 10, Windows 11, multitasking in Windows NT, multitasking in Windows XP, multitasking in Windows 7, multitasking in Windows 8, multitasking in Windows 10, multitasking in Windows 11.

Актуальность.

Многозадачность в операционных системах актуальна в современные дни. На данный момент компьютеры используются для выполнения разных задач: работа с текстами, графикой, мультимедиа, сетевыми соединениями, приложениями. Имеется возможность одновременно выполнять несколько задач.

Главный плюс - эффективное использование ресурсов за счет того, что многозадачные ОС могут эффективно использовать ресурсы компьютера: процессорное время, оперативная память, дисковое пространство. Данный подход позволяет одновременно выполнять несколько задач без необходимости ожидания поочередного завершения.

Происходит также повышение производительности - путем распределения процессорного времени между различными задачами. Многозадачные ОС способствуют повышению производительности компьютерной системы. Данный подход позволяет

пользователям выполнять несколько задач параллельно, не снижая скорость работы.

Кроме того, в многозадачных ОС пользователи с легкостью переключаются между приложениями/задачами, что повышает удобство использования. Пользователь слушает музыку в одном приложении, работает в Word с текстом, одновременно просматривает веб-страницы в браузере.

С развитием технологий появились следующие аспекты: виртуализация, облачные вычисления, большие данные, многозадачные ОС - основа для реализации, использования данных технологий.

Играет важную роль управление безопасностью. Многозадачные ОС предоставляют средства управления безопасностью: изоляция процессов, разделение ресурсов. Предотвращают распространение вредоносных программ, обеспечивают защиту данных пользователя.

Таким образом, многозадачность считается критически важным аспектом в современных операционных системах, так как обеспечивает эффективное использование ресурсов, повышает производительность [1].

Многозадачность в операционных системах.

Многозадачность в операционных системах (далее - ОС) - возможность системы выполнять несколько задач/процессов параллельно, таким образом, что пользователь может одновременно работать с несколькими приложениями, выполнять несколько операций.

Одним из важнейших ресурсов представляется процессорное время. Распределение процессорного времени между определенным количеством процессов определяет вид ОС. Существует 2 основных вида реализации многозадачности: не вытесняющая многозадачность, вытесняющая многозадачность. Главное различие - механизм планирования процессов может действовать разнообразно: в ОС с не вытесняющей многозадачностью механизм планирования распределен между ОС и прикладными программами, вытесняющий вид многозадачности полностью сосредоточен в ОС [2].

Компоненты многозадачности.

Итак, основные компоненты многозадачности в ОС включают:

Планирование процессов.

ОС должна имеет механизмы управления процессами, выделение ресурсов. Это включает в себя планирование времени процессора между различными процессами, определение приоритетов и распределение ресурсов (например, процессорного времени, памяти) в соответствии с этими приоритетами.

Механизмы синхронизации.

В многозадачных системах возникает необходимость в синхронизации доступа к общим ресурсам: файлы, устройства ввода-вывода. Операционная система предоставляет механизмы синхронизации: семафоры, мьютексы, блокировки с целью обеспечения правильного взаимодействия между процессами [3].

Управление памятью.

Вследствие того, что многозадачные системы выполняют много процессов - ОС должна эффективно управлять доступом к памяти, обеспечивать изоляцию между процессами, предотвратить взаимное воздействие процессов, обеспечить безопасность системы.

Переключение контекста.

Когда операционная система переключается между выполнением процессов, сохраняет/восстанавливает состояние каждого процесса. Данный процесс именуется переключением контекста, требует времени и ресурсов.

Многозадачность - один из основных принципов современных операционных систем, обеспечивает эффективность использования ресурсов компьютера, удовлетворения потребностей пользователей в выполнении нескольких задач одновременно.

Сравнительный анализ аспектов многозадачности в операционных системах Windows

Проанализирует от Windows NT до Windows 11 версии ОС с точки зрения их многозадачности.

Таблица 1. – Аспекты многозадачности от Windows NT до Windows 11.

Версия	Описание
Windows NT 3.1	Выпустилась в 1993 году, представляет архитектуру ядра, которое впервые позволило запускать несколько приложений одновременно. Указанная версия включала механизмы защиты памяти. Они изолировали процессы друг от друга, повышали стабильность системы.
Windows NT 4.0	Выпустилась в 1996 году, улучшила аспект многозадачности. Она ввела поддержку многопоточности, что позволило эффективнее использовать многопроцессорные системы и повысило производительность. Планирование процессов было улучшено для более эффективного распределения процессорного времени. Также были внедрены дополнительные средства для управления памятью и файловой системой.
Windows 2000	Выпустилась в 2000 году, продолжает совершенствоваться аспект многозадачности. Версия обновила механизмы синхронизации процессов, предоставила дополнительные возможности управления памятью, усилила обработку сетевых запросов. Введена поддержка современного аппаратного обеспечения - USB, Plug-and-Play.
Windows XP	Была выпущена в 2001 году, представила обновления в области многозадачности. Ввела поддержку гиперпотоковых

	процессоров, что позволило эффективнее использовать вычислительные ресурсы на многопроцессорных системах. Внедрены механизмы, стабилизирующие планирование процессов, управление памятью.
Windows Vista	Windows Vista выпустилась в 2006 году. Представила технологию SuperFetch, которая обновила и улучшила загрузку приложений: повысила общую производительность системы. Основывалась на анализе использования ресурсов/предварительной загрузке в память часто используемых данных. Данные аспекты существенно снизили время ожидания при запуске приложений. В Windows Vista внедрены механизмы обработки ошибок, повышающие стабильность системы.
Windows 7	Выпустилась в 2009 году. Версия сосредоточилась на улучшении производительности/стабильности. В указанной версии были внедрены: улучшенное планирование процессов (повысило отзывчивость системы, снизило время ожидания при запуске приложений), обновлены механизмы управления памятью/ввода-вывода. Данный ход повысил производительность работы с файлами, другими устройствами.
Windows 8	Windows 8 вышла в свет в 2012 году. Имеет поддержку новых типов устройств: сенсорные экраны, устройства с архитектурой ARM. Данный результат потребовал изменений в механизмах многозадачности, принес эффективность работы на разных устройствах. Центральное внимание уделялось оптимизации производительности на планшетах, гибридных устройствах.
Windows 10	Вышла в 2015 году, ввела функцию виртуальных рабочих столов. Данная функция позволяет пользователям организовывать приложения на разных рабочих столах, легко переключаться между ними. Указанная система дополнительно повысила удобство

	работы с приложениями/задачами. В Windows 10 улучшены механизмы безопасности/производительности.
Windows 11	Windows 11 вышла в 2021 году. Также произошли обновления в системе многозадачности, производительности системы. Внедряет систему обновлений в интерфейс виртуальных рабочих столов, в механизм управления памятью, процессами. Повышен уровень отзывчивости системы, имеется плавное переключения между приложениями/задачами.

Обобщенный результат исследования.

Развитие многозадачности в операционных системах от Windows NT до Windows 11 отражает следующие тенденции в области информационных технологий: улучшение производительности, повышение эффективности использования ресурсов, удовлетворение потребностей пользователей в мобильности/удобстве.

Первоначально многозадачность в ОС Windows NT - в форме возможности запуска нескольких приложений одновременно благодаря архитектуре ядра, обеспечивающей изоляцию процессов, защиту памяти. Windows NT 4.0 ввела поддержку многопоточности, сделала возможным использование многопроцессорных систем эффективнее, улучшила планирование процессов [4].

С появлением Windows 2000, а также последующих версий, многозадачность усовершенствовалась, стала комплексной. Механизмы управления памятью, механизмы синхронизации процессов, оптимизации производительности внедрены с целью обеспечения стабильной работы системы при одновременном выполнении множества задач.

Windows XP и последующие версии показывали усовершенствованную многозадачность, вводили новые технологии, поддержку гиперпотоковых процессоров, SuperFetch, налаженное планирование процессов. Данные схемы повышали производительность, системы [6].

Начиная от Windows 8, Windows 10 в операционной системе Windows многозадачность стала мобильной и адаптированной к следующим типам устройств: планшеты, гибридные устройства и т.д., что обозначило дальнейшие изменения в механизмах многозадачности в целях реализации безопасной работы на устройствах[7].

Windows 11 ведет тенденцию на улучшение многозадачности, обновляет интерфейс виртуальные рабочие столы, оптимизирует производительность системы. Пользователи ожидают кликабельную, плавную работу [5].

Преимущества и недостатки многозадачности в операционных системах Windows.

Рассмотрим преимущества и недостатки многозадачности в в операционных системах Windows.

Таблица 2. – Преимущества и недостатки многозадачности в каждой версии.

Версия	Преимущества	Недостатки
Windows NT 3.1	Возможность одновременного выполнения нескольких задач.	Ограниченные ресурсы процессора, памяти, снижение производительности.
Windows NT 4.0	Слаженнее происходит планирование процессов. Повышение производительности на многопроцессорных системах.	Увеличенное потребление ресурсов ОС вследствие дополнительных механизмов управления процессами.
Windows 2000	Дополнительные механизмы синхронизации процессов. Совершенствуется управление памятью.	Возможность конфликтов при совместном доступе к ресурсам.
Windows XP	Поддержка гиперпотоковых процессоров с целью распределения нагрузки между ядрами процессора. Совершенствуется планирование процессов, повышается производительность.	Возможность возникновения конфликтов при работе с устройствами/файлами из-за одновременного доступа.
Windows Vista	Технология SuperFetch стабилизирует загрузки приложений/быстрый доступ. Дополнительные механизмы управления ошибками.	Значительное потребление памяти, ресурсов для SuperFetch, замедление работы.
Windows 7	Оптимизация работы с файлами и устройствами.	Возможность перегрузки системы.
Windows 8	Поддержка новых типов устройств - планшеты и сенсорные экраны.	Адаптация к новым типам устройств могла привести к сложностям.
Windows 10	Функция виртуальных рабочих столов для организации приложений и задач. Механизмы безопасности.	Необходимость дополнительной настройки и обучения пользователей.

Windows 11	Улучшение интерфейса виртуальных рабочих столов.	Проблемы совместимости при переходе на новую версию ОС.

Выводы

Таким образом, развитие многозадачности в операционной системе Windows демонстрирует постоянное стремление к улучшению производительности, стабильности и удобства использования компьютерных систем, что делает их более эффективными инструментами для повседневной работы и развлечений.

Список литературы

1. Багдасаров Д.М. Архитектура Windows NT. Столыпинский вестник. 2022. №4(4). С. 1924-1934.
2. Дорогой Я.Ю., Мороз И.Д. Способ выполнения нескольких потоков команд на одном динамически реконфигурируемом процессорном ядре. Технические науки – от теории к практике. 2016. №7 (55). С.39-44.
3. Зонова Д.Ю. Исследование путей развития операционных систем. Colloquium-journal. 2022. №35(158). С.31-33.
4. Красов А.В., Борисов В.И. Исследование применимости известных методов внедрения цифровых водяных знаков к исполняемым файлам unix-подобных систем. 2022. №2. С. 38-42.
5. Манелис В. Б., Сладких В. А., Козьмин В. А., Бизюков П. Е.Адресное пеленгование базовых станций GSM, UMTS, LTE сетей сотовой связи. Системы управления, связи и безопасности. 2021. № 2. С. 142-158.
6. Прихожий А.А., Карасик О.Н. Кооперативная модель оптимизации выполнения потоков на многоядерной системе. Системный анализ и прикладная информатика. 2014. №4. С.13-20.
7. Штеренберг С.И., Бударный Г.С., Ахметов Р.Р. Обеспечение безопасности на высокоуровневой среде WINDOWS. 2022. С.585-586.

References

1. Bagdasarov D.M. Windows NT architecture. Stolypinsky Bulletin. 2022. No. 4(4). pp. 1924-1934. (In Rus.).
2. Dear Ya.Yu., Moroz I.D. A method for executing multiple instruction threads on a single dynamically reconfigurable processor core. Technical sciences - from theory to practice. 2016. No. 7 (55). pp.39-44. (In Rus.).
3. Zonova D.Yu. Research of ways of development of operating systems. Colloquium-journal. 2022. No. 35(158). pp.31-33. (In Rus.).
4. Krasov A.V., Borisov V.I. A study of the applicability of known methods for introducing digital watermarks to executable files of unix-like systems. 2022. No. 2. pp. 38-42. (In Rus.).
5. Manelis V. B., Sladkikh V. A., Kozmin V. A., Bizyukov P. E. Addressable direction finding of base stations of GSM, UMTS, LTE cellular networks. Control, communication and security systems. 2021. No. 2. pp. 142-158. (In Rus.).
6. Prikhozhy A.A., Karasik O.N. A cooperative model for optimizing thread execution on a multi-

core system. System analysis and applied informatics. 2014. No. 4. pp.13-20. (In Rus.).

7. Shterenberg S.I., Budarny G.S., Akhmetov R.R. Ensuring security in a high-level WINDOWS environment. 2022. pp 585-586. (In Rus.).

Некрасов Т.Д. и др. Использование математической модели атмосферных уравнений для численного прогнозирования погоды NWP в гражданской авиации/Некрасов Т.Д., Лозница С.Ю., Дроц Т.С., Боровикова Д.В.// Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 6(44) с. 34–39

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.942

ИСПОЛЬЗОВАНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ АТМОСФЕРНЫХ УРАВНЕНИЙ ДЛЯ ЧИСЛЕННОГО ПРОГНОЗИРОВАНИЯ ПОГОДЫ NWP В ГРАЖДАНСКОЙ АВИАЦИИ

[1]Некрасов Т.Д., Лозница С.Ю., [2]Дроц Т.С., [3]Боровикова Д.В.
ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ ИМЕНИ ГЛАВНОГО МАРШАЛА АВИАЦИИ А.А. НОВИКОВА", Санкт-Петербург, Россия (196210, город Санкт-Петербург, ул. Пилотов, д.38), e-mail: [1]Kvakolka885@gmail.com, [2]drots2005@mail.ru, [3]borovikovadasha05@mail.ru

В статье рассматриваются принципы и технические возможности численного прогнозирования погодных условий на территории аэродрома. Составление прогноза TAF и составление сводок GAMET.

Ключевые слова: ЭВМ, СЭВМ, Прогноз, Погодные явления, Атмосферные явления, дифференциальные уравнения, МКР.

USING A MATHEMATICAL MODEL OF ATMOSPHERIC EQUATIONS FOR NUMERICAL NWP WEATHER FORECASTING IN CIVIL AVIATION.

[1]Nekrasov T.D., Loznitsa S.Yu., [2]Drotz T.S., [3]Borovikova D.V.
"ST. PETERSBURG STATE UNIVERSITY OF CIVIL AVIATION NAMED AFTER AIR CHIEF MARSHAL A.A. NOVIKOV", St. Petersburg, Russia (196210, St. Petersburg, ул. Pilotov, д.38), e-mail: [1]Kvakolka885@gmail.com, [2]drots2005@mail.ru, [3]borovikovadasha05@mail.ru

The article examines the principles and technical possibilities of numerical forecasting of weather conditions on the territory of the airfield. Making a TAF forecast and compiling GAMET summaries.

Keywords: Computer, SuperComputer, Forecast, Weather phenomena, Atmospheric phenomena, differential equations, Finite difference method.

Проблема получения прогноза погоды никогда не теряла своей актуальности. На данный момент используется численное прогнозирование погоды NWP (Numerical weather prediction). Современное численное прогнозирование погоды основано на использовании компьютерных моделей, которые учитывают множество параметров, таких как температура воздуха, влажность, скорость и направление ветра, атмосферное давление и др. Эти модели позволяют делать прогнозы на различные временные промежутки, от нескольких часов до нескольких недель вперед.

Для численного прогнозирования метеорологических явлений используются каскады примитивных атмосферных уравнений. Примитивные атмосферные уравнения - это уравнения, описывающие основные процессы, происходящие в атмосфере Земли. С их помощью можно моделировать различные явления, такие как циркуляция воздуха,

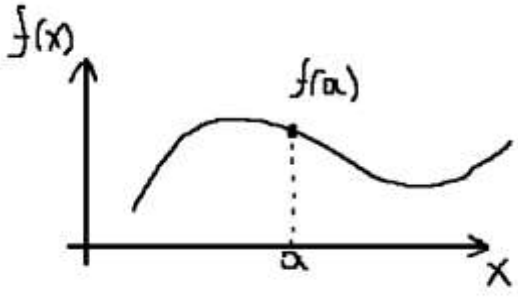
формирование облаков, погодные изменения. Эти уравнения показывают изменения плотности, давления и температуры в атмосфере с течением времени. Данные проходят через нелинейные уравнения частных производных. Используются разные модели решения математическо-метеорологических задач. Некоторые глобальные модели используют метод конечных разностей для пространственного счисления. Метод конечных разностей (МКР) является достаточно универсальным численным методом ориентированным на решение зада с граничными условиями как в одномерных, так и многомерных системах. Причем МКР является одним из немногих численных методов, который может быть использован для решения математических моделей процессов (объектов) с распределенными параметрами, описываемых дифференциальными уравнениями в частных производных. В этом случае переменные исследуемой модели могут зависеть как от времени t, так и от пространственных координат (x, y) в двумерном случае и (x, y, z) в трехмерном.

Общей идеей МКР является сведение исходной задачи с граничными условиями (краевой задачи) к более простой задаче решения системы линейных или нелинейных алгебраических уравнений. Вид получаемой системы алгебраических уравнений зависит от вида исходного дифференциального уравнения. Конечно-разностные уравнения в МКР получают путем замены производных в исходном дифференциальном уравнении соответствующими конечно-разностными выражениями. Конечно-разностные выражения для какой-либо частной производной можно получить из разложения функции в ряд Тейлора по соответствующей переменной. Многочлен Тейлора используется для решения задач аппроксимации. **Аппроксимация** (от лат. proxima — ближайшая) или **приближение** — научный метод, состоящий в замене одних объектов другими, в каком-то смысле близкими к исходным, но более простыми.

Аппроксимация позволяет исследовать числовые характеристики и качественные свойства объекта, сводя задачу к изучению более простых или более удобных объектов.

Ряд Тейлора – это разложение некторой функции в бесконечный ряд.

Пусть есть некоторая функция f(x), которая непрервына и дифференцируема, причем функция дифференцируема число K раз в некоторой точке a.



Изобразим график функции. Мы можем определить полином(многочлен) Тейлора. Он означает, что функция f(x) в точке a равна:

$$f(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2}(x-a)^2 + \cdots + \frac{f(a)^k}{k!}(x-a)^k$$

Выходит так, что ξ окрестность можно представит в виде вышенаписанного многочлена.

Рассмотрим случай, в котором функция дифференцируема в точке а неограниченное число раз. k=∞ (к примеру экспонента).

$$f(x) = f(a) + f'(a)(x-a) + \cdots + \frac{f(a)^k}{k!}(x-a)^k + \cdots \text{ до бесконечности}$$

Сама функция f(a) – это производная нулевого порядка. Тогда $f'(a)(x-a)$ производная первого порядка.

Приведем запись к следующему виду: (где n=k)

$$\sum_{n=0}^{\infty} \frac{f(a)^n}{n!}(x-a)^n$$

Например, разложение функции u(x, y) по координате x будет иметь вид:

$$u\left(x_i + h, y_j\right) = u\left(x_i, y_j\right) + h \cdot \frac{\partial u}{\partial x} + \text{члены более высоких порядков малости}$$

где h – приращение x в точке.

Отбросив члены более высоких порядков малости и выразив частную производную, получим:

$$u_{xx} \equiv \frac{\partial u}{\partial x} \approx \frac{u\left(x_i + h, y_j\right) - u\left(x_i, y_j\right)}{h} = \frac{u_{i+1,j} - u_{i,j}}{h}$$

Таким образом, решая атмосферные уравнения с помощью МКР, можно просчитывать прогноз погоды. Разеберем некоторые решения атмосферных уравнений. (Обратим внимание, что расчет используется для городской среды с пространственным разрешением 0,5-1км).

Разберем математическую модель TSUNM3, развиваемую в Томском университете и институте оптики атмосферы имени В.В.Зуева. СО РАН мезомасштабной негидростатической модели высокого разрешения TSUNM3 (Tomsk State University Nonhydrostatical Mesoscale Meteorological Model).

Математическая модель оперирует следующими уравнениями:

-Уравнение неразрывности

-Уравнения движения

-Уравнение баланса энергии

-Уравнение Параметризации микрофизики влаги

-Уравнения Процессов аккреции (захвата) облачной влаги дождевыми каплями, снежинками и частицами

-Уравнения Процессов испарения или конденсации с участием дождевых капель

-Таяние (плавление) снежинок или снежной крупы с образованием дождевых капель

-И другие уравнения состояния атмосферы.

Приведем к примеру уравнение неразрывности:

$$\frac{\partial(\rho u)}{\partial x}+\frac{\partial(\rho v)}{\partial y}+\frac{\partial(\rho w)}{\partial z}=0.$$

Уравнение движения:

$$\rho\left(\frac{\partial u}{\partial t}+u\frac{\partial u}{\partial x}+v\frac{\partial u}{\partial y}+w\frac{\partial u}{\partial z}\right)=-\frac{\partial p}{\partial x}+\rho fv+$$
$$+\frac{\partial}{\partial x}\left(K_H\frac{\partial u}{\partial x}\right)+\frac{\partial}{\partial y}\left(K_H\frac{\partial u}{\partial y}\right)+\frac{\partial}{\partial z}\left(K_Z^m\frac{\partial u}{\partial z}\right),$$

$$\rho\left(\frac{\partial v}{\partial t}+u\frac{\partial v}{\partial x}+v\frac{\partial v}{\partial y}+w\frac{\partial v}{\partial z}\right)=-\frac{\partial p}{\partial y}-\rho fu+$$
$$+\frac{\partial}{\partial x}\left(K_H\frac{\partial v}{\partial x}\right)+\frac{\partial}{\partial y}\left(K_H\frac{\partial v}{\partial y}\right)+\frac{\partial}{\partial z}\left(K_Z^m\frac{\partial v}{\partial z}\right),$$

$$\rho\left(\frac{\partial w}{\partial t}+u\frac{\partial w}{\partial x}+v\frac{\partial w}{\partial y}+w\frac{\partial w}{\partial z}\right)=-\frac{\partial p}{\partial z}-\rho g+$$
$$+\frac{\partial}{\partial x}\left(K_H\frac{\partial w}{\partial x}\right)+\frac{\partial}{\partial y}\left(K_H\frac{\partial w}{\partial y}\right)+\frac{\partial}{\partial z}\left(K_Z^m\frac{\partial w}{\partial z}\right).$$

Здесь t – время; u, v, w – продольная, поперечная и вертикальная компоненты вектора осредненной скорости ветра в направлении декартовых координат x, y, z соответственно; ρ – плотность; f – параметр Кориолиса; KH – коэффициент горизонтальной диффузии; m Kz – коэффициент вертикальной диффузии количества движения; g – ускорение свободного падения; p – давление.

После инициализации данных их обрабатывают супер – компьютеры. Инициализация данных производится с метеостанций, позже вся информация отправляется на ЭВМ. На которой с помощью математического аппарата TSUNM3 высчитывается прогноз погоды с разными вероятностями. Одним из таких является TAF (Terminal Aerodrome Forecast). В TAF есть группа PROB, в которой указывается вероятность того или иного атмосферного явления. Вероятность может указываться только в 30% и 40%. 50% В авиации вероятностью не считается. Данные по прогнозу TAF пилоты обязаны учитывать при полете. Так же существует прогноз GAMET и AIRMET с SIGMET сводкой. В отличие от TAF, который показывает прогноз погоды в районе аэродрома, вышеперечисленные прогнозы используются пилотами для определения условий на высоте. В прогнозах GAMET и AIRMET могут указываться передвижения воздушных масс, высчитанных с помощью математических уравнений, направление и скорость ветра, турбулентность, давление, циклоны, антициклоны, опасные погодные явления.

Пример GAMET:

YUCC GAMET VALID 220600/221200 YUDO –

YUCC AMSWELL FIR/2 BLW FL120

SECN I

SFC WIND: 10/12 310/16MPS

SFC VIS: 06/08 N OF N51 3000M BR

SIGWX: 11/12 ISOL TS MT OBSC: S OF N43 MT PASSES

SIG CLD: 06/09 N OF N51 OVC 800/1100FT AGL 10/12 ISOL TCU 1200/8000FT AGL

ICE: MOD FL050/080

TURB: MOD ABV FL090

MTW: 10/15 N OF N43 MOD ABV FL080

SIGMETS APPLICABLE: 3, 5

SECN II

PSYS: 06 N5130 E01000 1004HPA MOV NE 25 KT WKN

WIND/T: 2000FT N5500 W01000 270/18MPS PS03 5000FT N5500 W01000 250/20MPS MS02 10000FT N5500 W01000 240/22MPS MS11

CLD: BKN SC 2500/8000FT AGL

FZLVL: 3000FT AGL

MNM QNH: 1004HPA

SEA: T15 HGT 5M

VA: NIL

Прогнозы TAF GAMET AIRMET используются пилотами при выполнении полетов.

Прогнозы погоды играют важную роль в авиации. Пилоты нуждаются в точных и надежных прогнозах погоды, чтобы принимать решения о безопасности полета, маршруте и времени прибытия.

Воздействие погоды на авиацию может быть разнообразным, от турбулентности и гроз до сильного ветра и тумана. Некорректная оценка и прогноз погодных условий может привести к задержкам рейсов, отменам, авариям и даже катастрофам.

Данные о собранных погодных явлениях обрабатываются на ЭВМ. Зачастую мощностей ЭВМ не хватает для точного и долгосрочного прогноза. Предлагается воспользоваться системой SharePC. Данная система рассчета уже работает на БАК (Большой Адронный Коллайдер).

Рассчет БАКа происходит за счет распределения нагрузки между компьютерами пользователей. Это говорит о том, что каждый персональный компьютер может стать маленькой частичкой вычислителя в большой сети. Нагрузка на СЭВМ (Супер ЭВМ) спадает, тем самым вычисления становятся точнее и выходят из вычислителя быстрее.

Нельзя обходить и квантовые технологии. Квантовые компьютеры могут играть значительную роль в улучшении прогнозов погоды. Благодаря своей способности обрабатывать и анализировать огромные объемы данных за короткое время, они могут помочь ученым более точно моделировать погодные явления и предсказывать их развитие.

Квантовые компьютеры также способны решать сложные задачи оптимизации, что может быть полезно при создании более эффективных моделей прогноза погоды. Кроме того, они могут использоваться для анализа большого количества данных с различных источников, что поможет улучшить точность прогнозов и предотвратить серьезные последствия экстремальных погодных явлений.

Список литературы

1. Бенистон, Мартин (1998). От турбулентности к климату: численные исследования атмосферы с иерархией моделей.

2. Блюм, Эндрю (2019). Машина погоды: путешествие внутрь прогноза. Нью-Йорк: HarperCollins.
3. Роулстоун, Ян и Норбери, Джон (2013). Невидимый в шторме: роль математики в понимании погоды. Издательство Принстонского университета.
4. А.В. Старченко, Л.И. Кижнер, Е.А. Данилкин, Е.А. Шельмина, С.А. Проханов. (2022) Численное моделирование погоды и качества атмосферного воздуха в городах.

References

1. Beniston, Martin (1998). From turbulence to climate: numerical studies of the atmosphere with a hierarchy of models.
2. Bloom, Andrew (2019). The weather machine: a journey inside the forecast. New York: HarperCollins.
3. Rowlstone, Jan and Norbury, John (2013). Invisible in a Storm: The role of mathematics in understanding the weather. Princeton University Press.
4. A.V.Starchenko, L.I.Kizhner, E.A.Danilkin, E.A.Shelmina, S.A.Prokhanov. (2022) Numerical modeling of weather and atmospheric air quality in cities.

Пучков Г.Ю. Оптимизация корпоративных сетей передачи данных // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 6(44) с. 40–47

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.7

ОПТИМИЗАЦИЯ КОРПОРАТИВНЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Пучков Г.Ю.
ФКУ "НАУЧНО-ПРОИЗВОДСТВЕННОЕ ОБЪЕДИНЕНИЕ «СПЕЦМАЛЬНАЯ ТЕХНИКА И СВЯЗЬ»МВД РОССИИ, Москва, Россия, (111024, город Москва, ул. Пруд-Ключики, д.2), e-mail: pgu7@yandex.ru

В статье рассматриваются аспекты оптимизации компьютерных сетей с целью повышения эффективности передачи данных. Подробно рассмотрены основные механизмы оптимизации, включая улучшение физической инфраструктуры сети, оптимизацию сетевых протоколов и настроек, а также балансировку нагрузки. Описывается значимость обновления сетевой инфраструктуры на более высокие скорости Ethernet и применение различных алгоритмов балансировки нагрузки для равномерного распределения трафика в сети.

Ключевые слова: Оптимизация сетей, эффективность передачи данных, физическая инфраструктура, сетевые протоколы, балансировка нагрузки.

ON THE ISSUE OF OPTIMIZING CORPORATE DATA TRANSMISSION NETWORKS

Puchkov G.Yu.
RESEARCH AND PRODUCTION ASSOCIATION "SPECIAL EQUIPMENT AND COMMUNICATIONS" OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA, Moscow, Russia, (111024, Moscow, Prud-Klyuchiki str., 2), e-mail: pgu7@yandex.ru

The article discusses aspects of optimizing computer networks in order to increase the efficiency of data transmission. The main optimization mechanisms are discussed in detail, including improving the physical network infrastructure, optimizing network protocols and settings, as well as load balancing. The importance of upgrading the network infrastructure to higher Ethernet speeds and the use of various load balancing algorithms for uniform distribution of traffic in the network is described.

Keywords: Network optimization, data transfer efficiency, physical infrastructure, network protocols, load balancing.

В современном цифровом мире компьютерные сети играют ключевую роль в обеспечении связности и эффективности между различными устройствами и системами. Они стали незаменимым инструментом для бизнеса, образования, научных исследований, медицинских учреждений и повседневной жизни. Однако с ростом зависимости от сетевых технологий возникают и новые вызовы, связанные с производительностью, надежностью и безопасностью сетей.

С учетом динамичного развития информационных технологий и увеличения объема передаваемых данных сети сталкиваются с постоянным напряжением. Оптимизация компьютерных сетей становится необходимостью, чтобы обеспечить их готовность к современным требованиям. Правильная оптимизация позволяет сетям более эффективно

передавать данные, минимизировать временные задержки и обеспечивать безопасность передаваемой информации.

В данной статье рассматриваются ключевые стратегии и методы оптимизации компьютерных сетей, которые помогут организациям повысить производительность, улучшить надежность и обеспечить безопасность своих сетевых инфраструктур.

Существует множество способов оптимизации компьютерных систем, в данной статье мы остановимся на четырех основных направлениях:

- анализ и мониторинг производительности сети;
- оптимизация пропускной способности сети;
- оптимизация конфигурации сетевых устройств;
- балансировка нагрузки.

Путем анализа существующих проблем, оптимизации конфигурации устройств, балансировки нагрузки, увеличения пропускной способности мы сможем создать оптимальные условия для работы сети в современной информационной среде. Рассмотрим данные направления оптимизации компьютерных сетей подробнее.

Анализ и мониторинг производительности

Прежде чем приступить к оптимизации сети, необходимо провести тщательный анализ текущего состояния производительности. Использование специальных инструментов мониторинга позволяет выявить узкие места в сети, такие как узлы с низкой пропускной способностью или высокие задержки. Этот анализ позволяет определить приоритеты при оптимизации и обеспечивает основу для принятия обоснованных решений.

Мониторинг производительности представляет собой непрерывный процесс сбора данных о работе сети, включая использование ресурсов (таких как процессоры, память, сетевая пропускная способность), уровень загрузки и сетевой трафик. Средства мониторинга, такие как системы управления сетью (NMS) и программы мониторинга, позволяют администраторам отслеживать состояние сети в реальном времени и выявлять проблемы производительности до их возникновения.

Мониторинг может осуществляться с помощью различных метрик, включая уровень использования ресурсов, скорость передачи данных, задержки, потери пакетов и другие.

Существует множество инструментов и программных средств для мониторинга производительности сети, включая бесплатные и коммерческие решения. Некоторые популярные средства мониторинга включают в себя Nagios, Zabbix, PRTG Network Monitor, SolarWinds, Wireshark.

Эти инструменты обеспечивают возможности для мониторинга различных аспектов сети, визуализации данных, создания отчетов и оповещения администраторов о возникших проблемах.

Анализ производительности сети - это процесс оценки и изучения работы компьютерной сети с целью выявления узких мест, оптимизации ее работы и обеспечения высокого уровня производительности, который позволяет администраторам сети и инженерам выявлять причины проблем производительности, определять узкие места в сети и принимать меры по их устранению. Этот процесс включает в себя обработку собранных данных, выявление аномалий и трендов, а также прогнозирование будущих изменений в сетевой нагрузке.

Как правило, анализ производительности осуществляется поэтапно.

Сбор данных. Первый этап анализа производительности заключается в сборе данных о работе сети. Это включает в себя сбор информации о трафике, использовании ресурсов, пропускной способности, задержках и других параметрах сети. Для сбора данных могут использоваться различные инструменты и программы мониторинга, такие как Wireshark, SNMP-агенты или специализированные системы управления сетью (NMS).

Анализ данных. Полученные данные анализируются с целью выявления аномалий, узких мест и проблем производительности. В процессе анализа могут использоваться различные методы и техники, такие как статистический анализ, визуализация данных, построение графиков и диаграмм, а также корреляционный анализ.

Выявление проблем. На основе анализа данных выявляются потенциальные проблемы и узкие места в сети, которые могут влиять на ее производительность. Это могут быть, например, перегруженные сетевые узлы, неправильная конфигурация оборудования, узкие каналы передачи данных или нестабильные соединения.

Оптимизация и улучшение производительности. После выявления проблем и узких мест в сети принимаются меры по их устранению и оптимизации работы сети. Это может включать в себя перенастройку сетевого оборудования, увеличение пропускной способности каналов связи, улучшение качества обслуживания (QoS), улучшение конфигурации сетевых протоколов и другие меры.

Мониторинг и повторный анализ. После внесения изменений и оптимизации сети необходимо продолжить мониторинг ее производительности для оценки эффективности внесенных изменений. Повторный анализ данных позволяет убедиться в том, что проблемы были успешно устранены и производительность сети улучшена.

Оптимизация пропускной способности сети

В современном мире информационных технологий пропускная способность является одним из важных аспектов оптимизации компьютерных сетей. Этот параметр определяет максимальную скорость передачи данных между различными устройствами в сети и является основным показателем ее производительности.

С постоянным увеличением объема данных, которые требуется передавать в сетях, вопрос обеспечения достаточной пропускной способности становится все более актуальным. Недостаточная пропускная способность может привести к узким местам в сети, перегрузкам и задержкам в передаче данных, что негативно сказывается на производительности и эффективности работы предприятия.

Оптимизация пропускной способности сети включает в себя оптимизацию физической инфраструктуры сети, такой как использование более быстрых коммутаторов, маршрутизаторов, сетевых кабелей и оптимизацию сетевых протоколов и настроек, направленных на увеличение эффективности передачи данных [1].

Важным аспектом увеличения пропускной способности сети и улучшения ее производительности является переход на более высокие скорости Ethernet (0/100/1000/10G/40G/100G Ethernet). Эти стандарты Ethernet представляют собой эволюцию скорости передачи данных в компьютерных сетях и позволяют адаптировать сетевую инфраструктуру к растущим требованиям производительности и пропускной способности. Выбор конкретного стандарта зависит от требований конкретной сети и ее способности

обеспечить соответствующую скорость передачи данных. Это особенно важно в сетях с высоким трафиком, где требуется передача больших объемов данных.

Более мощные маршрутизаторы и коммутаторы обычно предлагают богатый набор функциональных возможностей, таких как поддержка расширенных протоколов маршрутизации, виртуальных частных сетей (VPN), качества обслуживания (QoS), сегментации сети и многое другое. Эти возможности позволяют настраивать сеть для соответствия конкретным требованиям и бизнес-процессам, а встроенные в них механизмы отказоустойчивости, такие как поддержка протоколов группового маршрутизирования (HSRP, VRRP) и технологии стекирования для создания резервных путей позволяют обеспечить бесперебойную работу сети даже в случае отказа отдельных узлов.

Оптимизация сетевых протоколов и настроек достигается за счет использования современных технологий сжатия данных и кэширования, грамотной настройки TCP/IP параметров, назначения приоритетов для различных видов трафика и использования протоколов маршрутизации, учитывающих особенности конкретной сети.

Технологии сжатия данных и кэширования могут также помочь увеличить пропускную способность сети, сокращая объем передаваемой информации. Такие протоколы сжатия данных как HTTP Compression для веб-серверов или TCP/IP Header Compression для сетей передачи данных, позволяют уменьшить объем данных, передаваемых по сети, что в свою очередь позволяет сократить время передачи и использовать доступную пропускную способность более эффективно.

Транспортный протокол TCP/IP является основным протоколом для передачи данных в современных компьютерных сетях. Оптимизация его параметров, таких как размер окна TCP, время ожидания и использование алгоритмов контроля потока, может значительно повысить эффективность передачи данных и снизить задержки.

Использование Quality of Service (QoS). QoS позволяет устанавливать приоритеты для различных видов трафика в сети. Это позволяет обеспечивать приоритет передачи данных с высокой важностью, таких как голосовая и видеосвязь, перед менее важными данными. Правильная настройка QoS может значительно снизить задержки и улучшить качество обслуживания в сети.

Протоколы маршрутизации, такие как OSPF (Open Shortest Path First) или BGP (Border Gateway Protocol), можно настроить для оптимизации маршрутов и уменьшения задержек в передаче данных. Это может быть достигнуто путем настройки метрик маршрутизации, использования альтернативных маршрутов и оптимизации обмена маршрутной информацией.

Важно отметить, что оптимизация пропускной способности должна быть комплексным процессом, включающим анализ текущего состояния сети, выявление узких мест и принятие мер для их устранения. Правильная настройка и поддержка пропускной способности сети позволяет обеспечивать быструю и надежную передачу данных.

Оптимизация пропускной способности

Увеличение пропускной способности сети может быть достигнуто путем оптимизации физической инфраструктуры, такой как замена устаревшего оборудования на более производительное, или использование технологий сжатия данных и кэширования. Кроме того, использование протоколов сетевого уровня, таких как Multipath TCP, может повысить пропускную способность за счет распределения данных по нескольким путям.

Увеличение пропускной способности сети является ключевым аспектом её оптимизации. Это может быть достигнуто путем улучшения физической инфраструктуры сети, такой как использование более быстрых коммутаторов и маршрутизаторов, а также оптимизации сетевых протоколов. Например, технологии сжатия данных, кэширования и мультиплексирования могут значительно увеличить пропускную способность сети.

и настроек является важным аспектом увеличения эффективности передачи данных в компьютерных сетях. Этот процесс направлен на улучшение пропускной способности, снижение задержек и повышение надежности передачи данных. Рассмотрим подробнее несколько ключевых методов оптимизации.

Использование кэширования. Кэширование данных на уровне сети позволяет временно хранить копии часто запрашиваемых данных ближе к конечным пользователям. Это уменьшает необходимость передачи данных через сеть и ускоряет доступ к ресурсам.

Оптимизация конфигурации сетевых устройств

Конфигурация сетевых устройств, таких как маршрутизаторы, коммутаторы и файерволы, играет ключевую роль в производительности сети. Оптимизация параметров конфигурации, таких как размеры буфера, таблицы маршрутизации и настройки безопасности, может значительно повысить эффективность сети. Кроме того, важно регулярно обновлять прошивки и программное обеспечение сетевых устройств для исправления уязвимостей и улучшения производительности [2].

Конфигурация сетевых устройств имеет огромное значение для производительности сети. Настройки, такие как размеры буфера, максимальный размер передаваемого пакета (MTU), таблицы маршрутизации и настройки безопасности, могут значительно влиять на производительность и надежность сети.

Эффективное управление буферами и очередями в сетевых устройствах позволяет избежать переполнения и потери пакетов данных. Правильная настройка размеров буферов и очередей уменьшает задержки и повышает пропускную способность сети.

Например, размер буфера определяет количество данных, которые сетевое устройство может временно хранить перед их обработкой или передачей. Слишком маленький размер буфера может привести к переполнению буфера и потере пакетов данных в случае временной перегрузки сети. С другой стороны, слишком большой размер буфера может привести к увеличению задержек и неэффективному использованию памяти устройства. Настройка оптимального размера буфера требует анализа характеристик сети и объема передаваемого трафика. Настройка размера очереди влияет на задержки в сети и способность устройства обрабатывать пакеты в условиях высокой загрузки. Слишком маленький размер очереди может привести к отбрасыванию пакетов из-за переполнения очереди, тогда как слишком большой размер очереди может привести к увеличению задержек и потере пакетов из-за долгого ожидания обработки.

Некоторые современные сетевые устройства поддерживают адаптивную настройку размеров буфера и очередей, которая позволяет устройству динамически изменять их в зависимости от текущей нагрузки и характеристик сети. Это позволяет устройству эффективно управлять ресурсами и минимизировать задержки при различных условиях сети.

После настройки размеров буфера и очередей важно провести мониторинг и тестирование сети для оценки их эффективности. Это позволяет выявить возможные

проблемы и необходимость корректировки настроек для достижения оптимальной производительности.

Настройка размеров буфера и очередей в сетевых устройствах требует тщательного анализа и опыта работы с сетевым оборудованием. Правильная настройка помогает предотвратить потерю данных, минимизировать задержки и обеспечить высокую производительность сети. Поэтому важно регулярно проводить аудит и оптимизацию конфигурации сетевых устройств.

Балансировка нагрузки.

Балансировка нагрузки позволяет равномерно распределять трафик между различными узлами сети, что помогает избежать перегрузок и увеличить пропускную способность. Применение правильной стратегии балансировки нагрузки позволяет оптимизировать использование ресурсов сети.

К ключевым аспектам балансировки нагрузки следует отнести:

- методы балансировки нагрузки;
- механизмы реализации;
- алгоритмы балансировки нагрузки;
- масштабирование и отказоустойчивость;
- мониторинг и управление**.**

Методы балансировки нагрузки. Существует несколько методов балансировки нагрузки:

- распределение нагрузки на основе IP-адресов - трафик распределяется между серверами на основе IP-адресов запросов клиентов;
- распределение нагрузки на основе сессий - трафик для каждой сессии клиента направляется к одному серверу для обеспечения целостности сеанса;
- распределение нагрузки на основе контента - трафик направляется на серверы на основе характеристик запроса, таких как URL, тип контента и другие.

Механизмы реализации. Механизмы реализации балансировки нагрузки определяют способы, с помощью которых осуществляется распределение трафика между серверами в компьютерной сети. Эти механизмы могут быть реализованы на различных уровнях сетевой инфраструктуры, включая уровни приложений, транспорта и сети. Вот несколько распространенных механизмов реализации [3, 4]:

- балансировка нагрузки на уровне сетевых устройств (Layer 4-7);
- аппаратные балансировщики нагрузки (Load Balancers) это специализированные устройства управляющие трафиком на уровне сетевого транспорта (Layer 4) или приложений (Layer 7). Они обеспечивают высокую пропускную способность и поддерживают различные методы балансировки нагрузки, такие как Round Robin, Least Connections и другие. Примерами таких балансировщиков нагрузки являются устройства от компаний F5 Networks, Citrix Systems и Barracuda Networks;
- программные решения для балансировки нагрузки обычно работают на серверах и предоставляют функциональность балансировщика нагрузки на уровне приложений (Layer 7). Они могут быть реализованы в виде приложений на основе операционных систем или как виртуальные машины. Примеры программных балансировщиков нагрузки включают HAProxy, NGIN

Алгоритмы балансировки нагрузки. Данные алгоритмы определяют способы распределения трафика между различными серверами или узлами в компьютерной сети. Целью применения этих алгоритмов является равномерное распределение нагрузки на все доступные ресурсы, с целью улучшения производительности сети, повышения уровня отказоустойчивости и эффективности использования сетевой инфраструктуры. Наиболее распространенными алгоритмами балансировки нагрузки являются:

- Round Robin (Круговой метод) - распределяет запросы последовательно между всеми доступными серверами в циклическом порядке.
- При каждом новом запросе выбирается следующий сервер из списка. Этот процесс повторяется до тех пор, пока все серверы не получат равное количество запросов. Round Robin прост в реализации и обеспечивает равномерное распределение нагрузки между серверами.
- Least Connections (Наименьшее количество соединений) - направляет новые запросы к серверу, у которого наименьшее количество активных соединений. Таким образом, запросы распределяются между серверами пропорционально их текущей загруженности. Least Connections особенно эффективен в сетях с неоднородной нагрузкой.
- Weighted Round Robin (Взвешенный круговой метод) - каждому серверу назначается вес, отражающий его пропускную способность или производительность. При выборе сервера для обработки запроса учитывается его вес. Серверы с более высоким весом получают больше запросов. Это позволяет более гибко управлять распределением нагрузки и адаптировать его к особенностям сети.
- IP Hash (Хеширование IP-адресов) - для каждого запроса вычисляется хеш-значение IP-адреса клиента или сервера. Затем запрос направляется к серверу, который соответствует полученному хеш-значению. IP Hash особенно полезен в случае, когда необходимо обеспечить сессионную привязку запросов клиентов к определенным серверам.
- Random (Случайный выбор) - случайным образом выбирает сервер для обработки каждого нового запроса. При использовании этого метода нельзя гарантировать равномерное распределение нагрузки, но он может быть полезен в некоторых сценариях, например, в случаях когда информация о состоянии серверов отсутствует

Каждый из этих алгоритмов имеет свои преимущества и недостатки, и выбор конкретного метода зависит от требований к нагрузке, характеристик сети и особенностей приложения. Оптимальный алгоритм балансировки нагрузки помогает обеспечить высокую производительность, отказоустойчивость и эффективное использование ресурсов сети.

Заключение

Оптимизация компьютерных сетей играет решающую роль в обеспечении эффективной работы сетевой инфраструктуры. Путем анализа производительности, оптимизации конфигурации устройств, балансировки нагрузки и увеличения пропускной способности можно добиться значительного повышения производительности и надежности сети. Регулярное обновление и мониторинг сетевой инфраструктуры являются ключевыми компонентами успешной стратегии оптимизации.

Список литературы

1. T. Ryder. Nagios Core Administration Cookbook.//Packt Publishing ltd, 2016, 386 с. //ISBN 178588135, 9781785883132.
2. Мартин Л. Эбботт, Майкл Т. Фишер Комплексный, проверенный подход к масштабируемости ИТ, дополненный новыми стратегиями, технологиями и тематическими исследованиями//Addison-Wesley Professional, 2015 г.//ISBN 9780134032801.
3. Диип Медхи, Картик Рамасами. Сетевая маршрутизация: алгоритмы, протоколы и архитектуры.//Morgan Kaufmann Publisers, 2017 г.// ISBN: 978-0120885886.
4. Г.Ю. Пучков. «Оптимизация крупномасштабных территориально распределенных информационных систем, построенных с использованием технологии «тонкий клиент»//В журнале: «Инновации и инвестиции», 2024, № 2, стр. 278-281//ISSN:2307-180К.

References

1. T. Ryder. Nagios Core Administration Cookbook. // Packt Publishing ltd, 2016, 386 p. // ISBN 178588135, 9781785883132.
2. Martin L. Abbott, Michael T. Fisher A comprehensive, proven approach to IT scalability, complemented by new strategies, technologies and case studies // Addison-Wesley Professional, 2015 //ISBN 9780134032801.
3. Diip Medhi, Kartik Ramaswamy. Network routing: algorithms, protocols and architectures.// Morgan Kaufmann Publishers, 2017. / ISBN: 978-0120885886.
4. G.Y. Puchkov. "Optimization of large-scale geographically distributed information systems built using thin client technology. Innovation Investments Magazine, 2024, No. 2. pp. 278-281// ISSN:2307-180К.

Журавлев Д.С., Забегайлов А.Д., Верещагин А.А. Технологии и инструменты разработки приложений для шлемов виртуальной реальности // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 6(44) с. 48–55

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.94

ТЕХНОЛОГИИ И ИНСТРУМЕНТЫ РАЗРАБОТКИ ПРИЛОЖЕНИЙ ДЛЯ ШЛЕМОВ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

[1]Журавлев Д.С., Забегайлов А.Д., Верещагин А.А.
ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия, (119454, г. Москва, просп. Вернадского, 78, стр. 4.), e-mail: [1] zhur125@yandex.ru

В данной научной статье рассматриваются основные технологии и инструменты разработки приложений для шлемов виртуальной реальности. Также были выявлены ключевые проблемы в разработке приложений для шлемов виртуальной реальности с точки зрения аппаратной части вопроса, в том числе путем сравнения лидеров разработки программного обеспечения на рынке в этой области. Были предложены теоретически возможные, а также современные варианты решения данных проблем.

Ключевые слова: Виртуальная Реальность, шлемы виртуальной реальности, разработка приложений VR, технологии разработки приложений для шлемов VR.

TECHNOLOGIES AND TOOLS FOR DEVELOPING APPLICATIONS FOR HELMETS VIRTUAL REALITY

[1]Zhuravlev D.S., Zabegailov A.D., Vereshchagin A.A.
MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: [1]zhur125@yandex.ru

This research paper discusses the main technologies and tools for developing applications for virtual reality helmets. Also key problems in the development of applications for virtual reality helmets from the point of view of the hardware part of the issue were identified, including by comparing the leaders of software development on the market in this area. Theoretically possible, as well as modern options for solving these problems were proposed.

Keywords: Virtual Reality, Virtual reality helmets, VR application development, Application development technologies for VR helmets.

1. Что такое VR шлемы

VR-шлем – это устройство для погружения в виртуальный мир. Оно включает в себя гарнитуру и два экрана для каждого глаза, создавая трехмерное пространство. Шлемы виртуальной реальности используется в различных сферах, обеспечивая полное погружение и взаимодействие с виртуальными объектами при помощи контроллеров или жестов.

Технология шлемов основана на сенсорах, отслеживающих движения головы, создавая ощущение полной свободы. Они имеют преимущества, такие как высокая реалистичность, широкий угол обзора и возможность создания персонализированного опыта. Кроме того, шлемы виртуальной реальности совместимы с различными устройствами и постоянно улучшаются, открывая новые возможности в виртуальной реальности.

VR-шлемы являются одной из самых инновационных технологий современности, представляющей огромный потенциал для будущего. Они открывают новые возможности в виртуальной реальности и с каждым годом становятся все более доступными и улучшенными, позволяя людям переживать неповторимые и захватывающие приключения, не выходя из дома [1-2].

2. Инструменты разработки приложений для шлемов виртуальной реальности

Теперь, закончив с краткой вводной частью, перейдём к анализу инструментов и технологий разработки приложений для шлемов виртуальной реальности.

Для начала рассмотрим такое понятие, как VR движки. Движок (англ. Software Engine) – в программировании – ядро компьютерной программы для реализации конкретной прикладной задачи, чтобы отличить ее от наполнения и внешнего вида конкретной программы. Наиболее часто используемые (Рисунок 1):

1. Unity
2. Unreal Engine

Рисунок 1 – Логотипы Unity и Unreal Engine [9]

Для начала проведем сравнительный анализ этих движков и углубимся в их историю.

Unity и Unreal Engine – основные движки для создания игр и приложений. Первоначально большинство серьезных движков были платными, но появление Unity, предлагающего полный спектр функций бесплатно, привлекло многих пользователей. Сейчас основным конкурентом Unity является также бесплатный Unreal Engine.

Оба предоставляют широкий набор инструментов, но в последнее время наблюдается предпочтение разработчиков в пользу Unreal Engine, который превосходит Unity в графическом моделировании и поддержке. Несмотря на это, Unity привлекает своей простотой в программировании на языке C# и имеет большое сообщество, обеспечивая доступность для начинающих разработчиков [3-4].

Unreal Engine хорош для создания крупных игр и прототипирования, но требует знания C++. Оба движка предоставляют примерно одинаковое качество графики, зависящее от опыта пользователей.

3. Технологии шлемов виртуальной реальности

А теперь рассмотрим устройство VR шлема на примере работы каждой его составляющей детали:

Автоматический стерео-дисплей

Для стереоскопических дисплеев (Рисунок 2) не требуется иметь две камеры. Любая камера, которая не имеет текстуры рендеринга, автоматически отображается в стерео на вашем устройстве. Матрицы вида и проекции настраиваются для учета поля зрения и отслеживания головы.

Оптимизация происходит автоматически, чтобы сделать менее дорогостоящим рисование кадров дважды (по одному для каждого глаза).

Рисунок 2 – Пример работы со стерео-дисплеем [5]

Автоматический ввод с отслеживанием головы

Отслеживание головы (Рисунок 3) и соответствующий FOV автоматически применяются к вашей камере (если ваше устройство установлено на голове).

Это происходит по умолчанию, потому что отслеживание головы с низкой задержкой является неотъемлемой частью хорошего опыта VR [5-6].

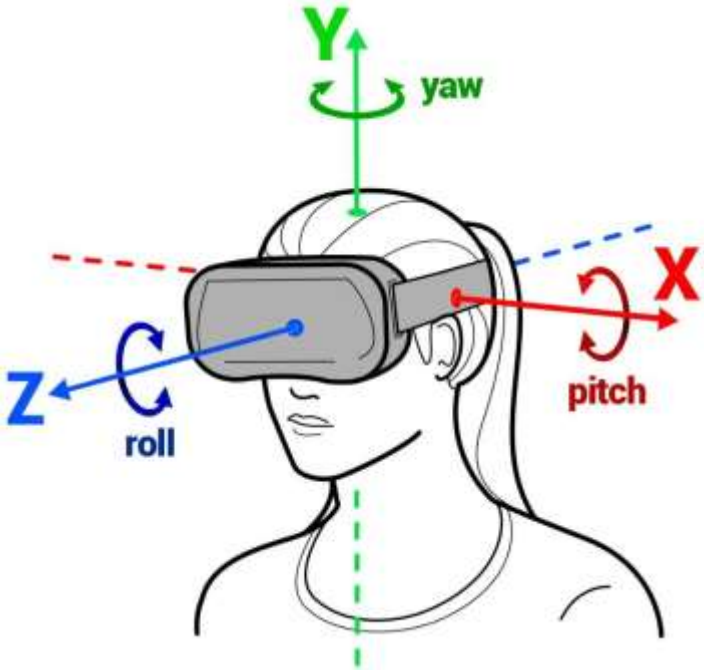


Рисунок 3 – Координатные оси при отслеживании положения головы [6]

4. Основные направления разработки приложений для шлемов виртуальной реальности

Если отойти от темы сред и глубже погрузиться в технологии и инструменты разработки приложений виртуальной реальности, то можно выделить основные направления, на которые опираются разработчики при создании приложений:

*Трекинг.*Трекинг – это набор технологий, который применяется в шлемахвиртуальной реальности.

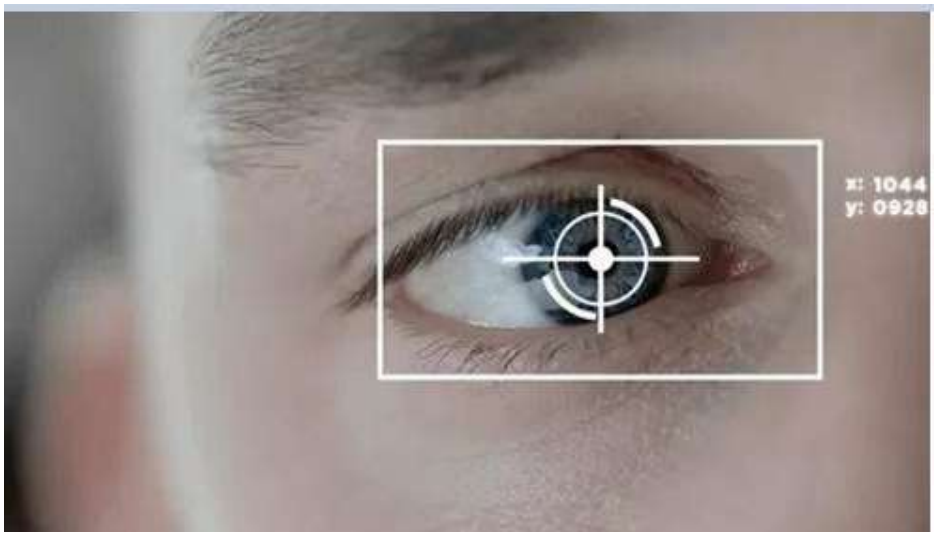


Рисунок 4 – Трекинг глаза [7]

Когда дело доходит до трекинга в современных VR шлемах, существует два основных подхода. Первый подход, известный как внутренний трекинг (Рисунок 4) или inside-out трекинг, использует камеры с широким углом обзора, размещенные на самом шлеме. Эти

камеры отслеживают положение ваших контроллеров и шлема относительно окружающих объектов. Чтобы контроллеры были видны, они подсвечиваются. Одним из преимуществ такого подхода является его относительная дешевизна и простота использования и настройки.

Однако этот подход имеет свои недостатки. Например, он не всегда точен, и камеры не могут отслеживать части вашего тела, находящиеся за пределами обзора камеры. В VR-играх это может быть проблемой, поскольку некоторые части тела могут оказаться "вне зоны видимости" камеры, например, за спиной. Эта система трекинга используется в шлемах Quest, Oculus Rift S и младшей модели HTC Vive Cosmos.

Вторая система трекинга, называемая Lighthouse (маяк), использует базовые станции или маяки, расположенные напротив друг друга и охватывающие игровую зону. Система работает следующим образом: первая базовая станция мигает инфракрасным светом, а затем излучает широкий падающий лазерный луч. Каждое мигание – это начало отсчета, и это происходит 60 раз в секунду. Шлем и контроллеры начинают отсчет с момента получения первого мигания и продолжают считать 1, 2, 3 и так далее. Затем датчики на шлеме и контроллерах улавливают лазерный луч. Используя задержку в отсчете сигналов от разных датчиков, определяется положение шлема и контроллеров в пространстве.

Внешний трекинг (Рисунок 5) куда более точный и надежный. Но в начале немного времени придется потратить на установку так называемых маяков (Рисунок 6).

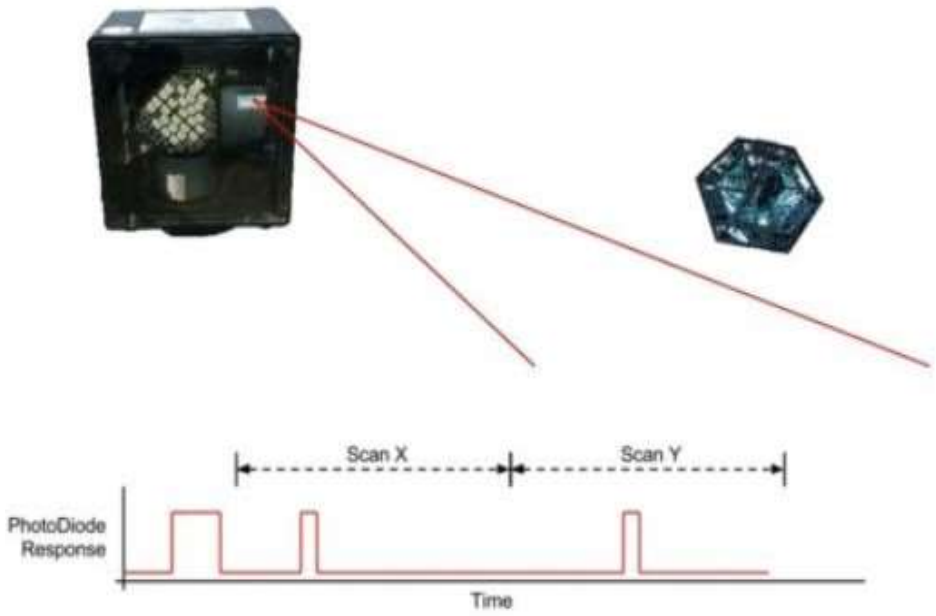


Рисунок 5 – Схема работы внешнего трекинга [8]

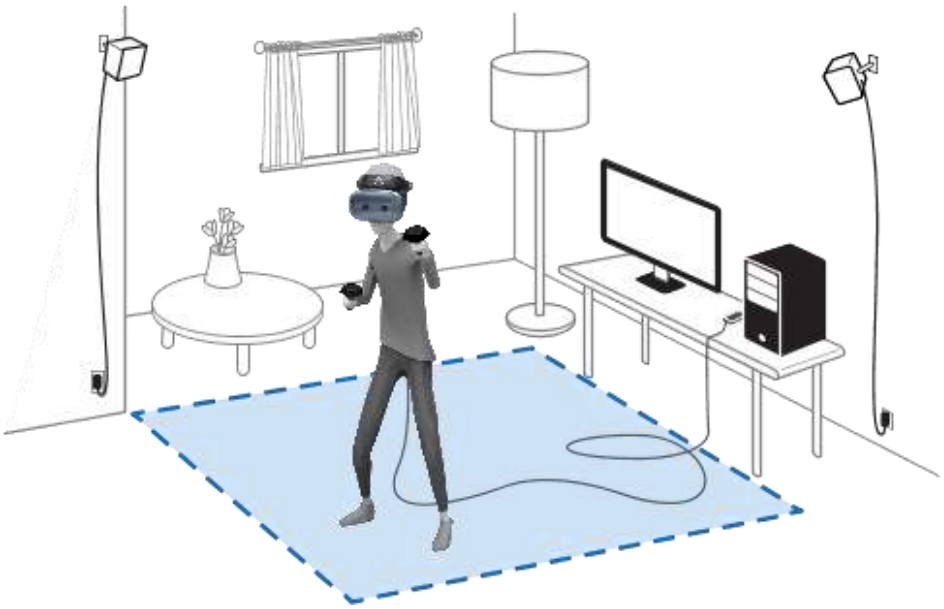


Рисунок 6 – Графическое представление работы внешнего трекинга в пространстве [8]

Экраны.Следующей важной технологией являются экраны (Рисунок 7). Критичным для экрана в VR является время задержки отображения. OLED-экраны самые быстрые, поэтому с них и началось освоение. Но с ними возникла проблема иного толка.

Рисунок 7 – Пример работы экранов шлема виртуальной реальности[7]

При использовании VR шлемов особенно важно иметь высокое разрешение и плотность пикселей, так как глаза пользователя находятся очень близко к дисплеям. В настоящее время OLED-дисплеи не являются наилучшим выбором для VR из-за PenTile-раскладки и

зернистости изображения, вызванной расстоянием между OLED-диодами. Однако в будущем эту проблему, скорее всего, решит технология microLED.

На данный момент лучшим выбором для VR является Super-Fast LCD, который по сути является усовершенствованным IPS с высокой скоростью обновления изображения.

Еще одним важным параметром является частота обновления, которая должна быть не менее 80 Гц, предпочтительно 90 Гц или выше. Шлем Valve Index в настоящее время обладает самой высокой частотой обновления в 144 Гц, однако на практике найти компьютер, который сможет обеспечить такую скорость кадров в VR, довольно сложно. В VR для каждого глаза необходимо рендерить две разные картинки одновременно [9].

Также необходимо учитывать угол обзора. В настоящее время система трекинга глаз, такая как Vive Pro Eye, предлагает лучшую технологию для определения направления взгляда и реализации технологии фовеального рендеринга (Рисунок 8). Фовеальный рендеринг позволяет отображать область, на которую фокусируется глаз пользователя, с максимальным качеством, тогда как остальную область можно рендерить с меньшим качеством. Такая технология существенно улучшает визуальный интерфейс пользователя [8].

Итак, чтобы достичь наилучшего качества изображения в VR, важно обратить внимание на разрешение и плотность пикселей, выбрать дисплей с высокой скоростью обновления и углом обзора, а также рассмотреть возможность использования системы трекинга глаз для реализации фовеального рендеринга.

Рисунок 8 – Пример работы технологии фовеального рендеринга [8]

Вывод

В заключение хочется отметить, что в настоящей статье были рассмотрены технологии и инструменты разработки приложений для шлемов виртуальной реальности. Также можно заключить, что безусловными лидерами среди приложений для разработки VR движков стали Unreal Engine и Unity, которые, имея свои плюсы и минусы, примерно равны по качеству. По результатам анализа технологий можно прийти к выводу о том, что в настоящий момент по качеству лидируют в своих сферах следующие технологии: Vive Pro Eye, Valve Index, внешний трекинг и фовеальный рендеринг.

Список литературы

1. ГОСТ 7.32–2017 СИБИД. Отчет о научно–исследовательской работе. Структура и правила оформления (с Поправками). – М., 2018.
2. Augmented Reality and Virtual Reality: New Trends in ImmersiveTechnology (2021) – 1

издание, 2021
3. Unity 2020 By Example: A project–based guide to building 2D, 3D,augmented reality, and virtual reality games from scratch – 3 издание, 2020
4. Unreal Engine VR Cookbook: Developing Virtual Reality with UE4(2017) – 2 издание, 2017
5. Control Oculus Rift [Электронный ресурс] – URL: https://laptrinhx.com/control–oculus–rift–drones–and–google–glass–with–these– gloves–2013492622/ (дата обращения: 14.04.2024)
6. Head tracking in VR [Электронный ресурс] – URL: https://www.pinterest.ru/pin/774900679632785385/ (дата обращения: 14.04.2024)
7. Oculus Rift Technology [Электронный ресурс]–URL: http://rifting.ru/oculus–rift–c–tehnologiey–otslezhivaniya–dvizheniya– glaz/maxresdefault/(дата обращения: 14.04.2024)
8. HTC Technology [Электронный ресурс]–URL: https://droider.ru/tag/5294–5614/ (дата обращения: 14.04.2024)
9. Unity vs Unreal Engine [Электронный ресурс]–URL: https://ixbt.games/articles/2021/04/23/unity–protiv–unreal–kakoi–dvizok–vybrat– nacinayushhemu–razrabotciku.html (дата обращения: 14.04.2024)

References

1. GOST 7.32-2017 SIBID. Report on research work. Structure and rules of execution (with Amendments). - M., 2018.
2. Augmented Reality and Virtual Reality: New Trends in Immersive Technology (2021) - 1st edition, 2021
3. Unity 2020 By Example: A project-based guide to building 2D, 3D, augmented reality, and virtual reality games from scratch - 3rd edition, 2020
4. Unreal Engine VR Cookbook: Developing Virtual Reality with UE4 (2017) - 2nd edition, 2017
5. Control Oculus Rift [Electronic Resource] - URL: https://laptrinhx.com/control-oculus-rift-drones-and-google-glass-with-these- gloves-2013492622/ (Date accessed: 14.04.2024)
6. Head tracking in VR [Electronic resource] - URL: https: //www.pinterest.ru/pin/774900679632785385/ (date of reference: 14.04.2024)
7. Oculus Rift Technology [Electronic resource] - URL: http://rifting.ru/oculus-rift-c-tehnologiey-otslezhivaniya-dvizheniya- glaz/maxresdefault/(date of reference: 14.04.2024)
8. HTC Technology [Electronic resource] - URL: https: //droider.ru/tag/5294-5614/ (date of reference: 14.04.2024)
9. Unity vs Unreal Engine [Electronic resource] - URL: https://ixbt.games/articles/2021/04/23/unity-protiv-unreal-kakoi-dvizok-vybrat-nacinayushhemu-razrabotciku.html (date of address: 14.04.2024).

Мироненко А.В. Исследование проблем безопасности контейнеризованных сред при выполнении учебных практических работ в университете на примере Kubernetes: угрозы и меры защиты // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 6(44) с. 56–62

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

ИССЛЕДОВАНИЕ ПРОБЛЕМ БЕЗОПАСНОСТИ КОНТЕЙНЕРИЗОВАННЫХ СРЕД ПРИ ВЫПОЛНЕНИИ УЧЕБНЫХ ПРАКТИЧЕСКИХ РАБОТ В УНИВЕРСИТЕТЕ НА ПРИМЕРЕ KUBERNETES: УГРОЗЫ И МЕРЫ ЗАЩИТЫ

Мироненко А.В.
ФГБОУ ВО "МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)", Москва, Россия, (125993, Москва, Волоколамское ш., д. 4), e-mail: qwerty.mironenko@gmail.com

С увеличением популярности контейнерных технологий, возникают новые угрозы безопасности, особенно в образовательных учреждениях. В статье рассматриваются проблемы безопасности контейнеризованных сред, на примере Kubernetes в учебной среде, показываются различные потенциальные угрозы, а также предлагаются меры защиты для минимизации рисков и обеспечения безопасного использования контейнеров для учебных работ.

Ключевые слова: Информационные технологии, контейнеризация, развертывание, безопасность кластера, Kubernetes, обучение.

INVESTIGATION OF THE SECURITY PROBLEMS OF CONTAINERIZED ENVIRONMENTS WHEN PERFORMING EDUCATIONAL PRACTICAL WORK AT THE UNIVERSITY USING THE EXAMPLE OF KUBERNETES: THREATS AND PROTECTION MEASURES

Mironenko A.V.
MOSCOW AVIATION INSTITUTE (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (125993, Moscow, Volokolamskoye shosse, 4), e-mail: qwerty.mironenko@gmail.com

With the increasing popularity of container technologies, new security threats are emerging, especially in educational institutions. The article discusses the security problems of containerized environments, using Kubernetes as an example in an educational environment, shows various potential threats, and also suggests protective measures to minimize risks and ensure the safe use of containers for educational work.

Keywords: Information technology, containerization, deployment, cluster security, Kubernetes, training.

Введение

В современном мире информационных технологий контейнеризация стала неотъемлемой частью разработки и внедрения программных продуктов. Она обеспечивает удобство развертывания, масштабируемость и изоляцию приложений, что делает ее востребованной как в корпоративной, так и в академической среде. Однако вместе с ростом популярности контейнерных технологий возникают новые угрозы безопасности, особенно в образовательных учреждениях, где студенты используют контейнеры для выполнения учебных заданий. В данной статье рассматривается проблема безопасности

контейнеризованных сред на примере Kubernetes в университетской среде, выявляются потенциальные угрозы и предлагаются меры защиты для минимизации рисков и обеспечения безопасного использования контейнеров в учебных практических работах.

Краткая информация о Kubernetes

Kubernetes, первоначально разработанный Google и теперь поддерживаемый Cloud Native Computing Foundation, произвел революцию в способах развертывания, управления и масштабирования контейнерных приложений в организациях. По своей сути Kubernetes — это платформа с открытым исходным кодом, предназначенная для автоматизации развертывания, масштабирования и работы контейнеров приложений в кластерах хостов.

Его архитектура состоит из нескольких ключевых компонентов: главного узла (control plane, master node), который управляет кластером, рабочих узлов (worker nodes), на которых выполняются контейнерные приложения, etcd key-value базы данных для управления состоянием кластера и набора процессов вроде kubelet, который управляет узлами и взаимодействует с мастером, и kube-proxy, который управляет сетевым взаимодействием. Также для понимания терминологии необходимо пояснить что такое под.

Под — это наименьшая развертываемая вычислительная единица, которая может быть создана в Kubernetes. Под (от англ. pod (pea pod) - стручок гороха) — это группа из одного или нескольких контейнеров с общим хранилищем и сетевыми ресурсами, а также спецификацией запуска контейнеров. Содержимое пода всегда размещается и планируется совместно и запускается в общем контексте. Под моделирует «логический хост» для конкретного приложения: он содержит один или несколько контейнеров приложений, которые относительно тесно связаны. В необлачных контекстах приложения, выполняемые на одной и той же физической или виртуальной машине, аналогичны облачным приложениям, выполняемым на том же логическом хосте. [1]

Почему нужно защищать учебный кластер?

Можно подумать, что серьезно защищать кластер, использующийся студентами в учебных целях, не имеет смысла, поскольку он не содержит в себе чувствительных для бизнеса данных и критических приложений, которые требуют бесперебойного доступа.

Однако вот несколько ключевых причин, по которым следует серьезно относиться к его безопасности:

Обучение лучшим практикам: Учебные кластеры предоставляют студентам возможность изучать и применять best practice в сфере безопасности. Эти знания студенты могут перенести в будущую профессиональную деятельность.

Предотвращение злоупотреблений: Незащищенные кластеры могут быть использованы для незаконной деятельности, такой как распространение вредоносного ПО, атаки на другие сети или майнинг криптовалюты, что может привести как к повышенным расходам, так и к юридической ответственности.

Сохранение репутации учебного заведения: Инциденты безопасности могут негативно сказаться на репутации учебного заведения и подорвать доверие к его разработкам, выпускникам и программам обучения.

Создание безопасной учебной среды: Защита кластеров помогает создать безопасную и стабильную среду для обучения, где студенты могут сосредоточиться на учебе, не беспокоясь о потере работы из-за атак или сбоев.

Защита интеллектуальной собственности: Студенты могут работать над инновационными проектами, которые могут иметь коммерческую ценность. Незащищенные кластеры могут стать целью для кражи данных.

Угрозы безопасности

1. Небезопасные образы контейнеров

Одним из основных источников угроз безопасности в Kubernetes являются небезопасные образы контейнеров. Образы контейнеров, используемые в учебных целях, часто скачиваются из общедоступных источников и могут содержать уязвимости, которые могут быть использованы злоумышленниками для получения доступа к контейнеризованной среде.

2. Компрометация учетных данных

Еще одна распространенная угроза безопасности - это компрометация учетных данных. Злоумышленники могут использовать атаки фишинга или социальной инженерии для получения доступа к учетным данным администраторов Kubernetes. Как только злоумышленник получает доступ к учетным данным администратора, он может получить полный контроль над кластером Kubernetes, что позволяет ему развертывать вредоносные контейнеры, красть данные или нарушать работу приложений.

3. Внедрение вредоносного кода

Студенты могут случайно или намеренно внедрить вредоносный код в свои контейнеры. Это может привести к заражению всего Kubernetes-кластера, что может привести к серьезным последствиям, таким как кража данных, потеря работоспособности и финансовые убытки.

4. DoS-атаки

Kubernetes-кластеры могут быть подвержены атакам типа "отказ в обслуживании" (DoS). Эти атаки могут быть вызваны как неправильным использованием ресурсов студентами, так и целенаправленными атаками злоумышленников. DoS-атаки могут сделать кластер Kubernetes недоступным для пользователей, что может привести к перебоям в работе и финансовым потерям.

5. Несанкционированный доступ к API

API Kubernetes предоставляет мощный интерфейс для управления кластером. Однако уязвимости в API Kubernetes могут быть использованы злоумышленниками для получения несанкционированного доступа к кластеру. Это может позволить злоумышленникам развертывать вредоносные контейнеры, красть данные или нарушать работу приложений. [2]

Общие рекомендации по защите кластера.

Управление настройкой кластера. Защита control plane и worker nodes Kubernetes имеет основополагающее значение для защиты всего кластера. Крайне важно укрепить control plane, сердце Kubernetes, путем ограничения доступа, обеспечения связи по безопасным каналам, а также регулярного обновления и исправления его компонентов. Worker nodes, на которых фактически запускаются приложения, требуют не меньшего внимания. Их следует настроить по принципу наименьших привилегией и минимальных разрешений, необходимых для

работы. Сетевые политики имеют решающее значение для определения того, как модули взаимодействуют друг с другом и с внешним миром. Реализация жесткой сетевой политики помогает создать глубокую защиту, снижая риск перемещения вредоносной нагрузки по сети в случае взлома.

Аутентификация и авторизация. Надежное управление доступом пользователей является ключом к поддержанию целостности безопасности кластера Kubernetes. Внедрение контроля доступа на основе ролей (RBAC) имеет решающее значение для обеспечения того, чтобы пользователи (как студенты, так и преподаватели) и службы имели только тот доступ, который им необходим. Политики RBAC позволяют администраторам указывать, кто и к каким ресурсам имеет доступ в кластере. Интеграция с внешними поставщиками удостоверений через такие протоколы, как OpenID Connect, может централизовать управление пользователями и упростить процесс аутентификации. Регулярные проверки этих разрешений имеют жизненно важное значение для обеспечения того, чтобы они продолжали отражать необходимые уровни доступа.

Безопасность сети. Безопасность сети Kubernetes заключается в контроле потока входящего и исходящего трафика кластера. Сетевые политики и сегментация имеют основополагающее значение для изоляции и защиты конфиденциальных рабочих нагрузок. Сетевые политики позволяют администраторам контролировать поток трафика между модулями и между модулями и внешними сетями, тем самым определяя, как группы модулей могут взаимодействовать друг с другом и с другими конечными точками сети. При отсутствии сетевых политик модули в кластере Kubernetes могут иметь неограниченный доступ к сети, что потенциально позволяет беспрепятственному распространению вредоносного трафика или нарушений. Реализация сегментации сети в кластере Kubernetes может предотвратить несанкционированный доступ и ограничить радиус атаки в случае компрометации. Кроме того, шифрование трафика как внутри кластера (внутрикластерная связь), так и при выходе из кластера или входе в него (например, входящий и исходящий) имеет важное значение для защиты данных от перехвата и подделки. Рассмотрите возможность использования Kubernetes — собственных или сторонних инструментов, которые улучшают управление и визуализацию сетевых политик. Такие инструменты, как Calico, Cilium или Weave Net, могут предоставлять расширенные возможности сетевой политики, упрощая управление сложными сетевыми конфигурациями и визуализируя взаимодействие между различными сетевыми политиками. [3]

Безопасность подов. Pod Security Admission имеют решающее значение для определения условий безопасности, которым должны соответствовать поды для работы в кластере. Они помогают применять лучшие практики, такие как предотвращение привилегированного доступа, ограничение доступа к ресурсам хоста и контроль использования томов и файловых систем. Включает в себя также определение лимитов ресурсов для подов как по памяти, так и по использованию процессора. Это предотвращает перегрузку узлов кластера и обеспечивает бесперебойную работу других приложений. Использование запросов ресурсов (requests) для определения минимального количества ресурсов, необходимых для работы пода гарантирует, что под будет запланирован на узел с достаточными ресурсами и не прекратит работу в связи с их исчерпанием. Помимо этого, регулярное сканирование образов контейнеров и сред

выполнения на уязвимости помогает выявлять и устранять потенциальные проблемы безопасности до того, как их можно будет использовать.

Безопасность данных. Защита данных, как при хранении, так и при передаче, является важнейшим аспектом безопасности Kubernetes даже для тестового студенческого кластера. Применение всех доступных средств защиты данных позволит студентам разрабатывать любые приложения. Шифрование хранящихся данных, использование серверов хранения, поддерживающих шифрование, и безопасное управление ключами шифрования являются фундаментальными практиками. Что касается передаваемых данных, использование Transport Layer Security (TLS) для всех внутренних и внешних коммуникаций гарантирует, что данные шифруются во время передачи, защищая их от утечки и атак типа «man-in-the-middle».

Ведение журнала и мониторинг. Эффективное ведение журнала и мониторинг необходимы для поддержания безопасности кластера Kubernetes. Это предполагает сбор и анализ журналов различных компонентов кластера Kubernetes для обнаружения, оповещения и реагирования на аномальные действия, которые могут указывать на нарушение безопасности. Такие инструменты, как Prometheus для мониторинга и Elasticsearch, Fluentd и Kibana (стек EFK) для ведения журналов, могут показаться избыточными, но стать полезными в учебных целях. Обнаружение аномалий можно дополнительно улучшить за счет интеграции передовых инструментов безопасности, которые используют машинное обучение для обнаружения необычных закономерностей в работе системы. [4]

Применение политики с помощью Open Policy Agent (OPA). Open Policy Agent (OPA) — это механизм политики общего назначения с открытым исходным кодом, который унифицирует применение политики во всем стеке. В Kubernetes OPA можно использовать для применения пользовательских политик в кластерах, помимо того, что предлагается политиками безопасности подов. OPA интегрируется с процессом контроля доступа Kubernetes, позволяя администраторам определять детальные, контекстно-зависимые политики, контролирующие, какие ресурсы можно создавать и изменять. Используя OPA, организации могут применять широкий спектр политик, включая лучшие практики безопасности, требования соответствия и даже сложные организационные политики. Этот уровень контроля имеет решающее значение для поддержания целостности и безопасности кластеров Kubernetes, особенно в средах со строгими нормативными требованиями и требованиями соответствия. [5]

Сканирование образов в Kubernetes. Сканирование образов включает в себя анализ образов контейнеров на наличие известных уязвимостей, таких как устаревшие пакеты программного обеспечения, небезопасные конфигурации или открытые секреты. Этот процесс имеет решающее значение, поскольку образы контейнеров составляют основу рабочих нагрузок приложений, работающих в кластерах Kubernetes. Инструменты автоматического сканирования могут выявлять уязвимости на самой ранней стадии, позволяя студентам решать проблемы безопасности до того, как они достигнут производственной среды. Для сканирования образов контейнеров доступно несколько инструментов и платформ. Эти инструменты обычно поддерживают базы данных известных уязвимостей, которые они используют для оценки уровня риска образа контейнера. Некоторые популярные варианты: Twistlock и grype. Эти инструменты могут сканировать изображения на наличие широкого

спектра уязвимостей, в том числе перечисленных в базе данных Common Vulnerabilities and Exposures (CVE), и предоставлять подробные отчеты о результатах.

Обучение и осведомленность. Создание кластера со всеми мерами безопасности малополезно без обучения студентов основам безопасности контейнеров и Kubernetes. Кроме того, важной частью является предоставление студентам ресурсов для изучения лучших практик безопасности и создание культуры безопасности, в которой студенты могут без опасений сообщать о проблемах безопасности, которые возникли или были ими обнаружены.

Заключение.

В заключение хочется отметить, что безопасность сред Kubernetes — это постоянный путь, а не пункт назначения. Лучшие практики, изложенные в этой статье, могут служить основой, но их необходимо постоянно пересматривать и совершенствовать в ответ на новые идеи, технологии и угрозы. Поскольку Kubernetes укрепляет свою роль краеугольного камня облачных вычислений, приверженность безопасности как со стороны сообщества, так и отдельных пользователей будет играть решающую роль в долгосрочном успехе и надежности платформы.

Список литературы

1. Kubernetes Documentation: Securing a Cluster [Электронный ресурс] URL: https://kubernetes.io/docs/tasks/administer-cluster/securing-a-cluster/ (дата обращения: 05.04.2024)
2. Containers’ Security: Issues, Challenges, and Road Ahead [Электронный ресурс] URL: https://www.researchgate.net/publication/332482728_Containers'_Security_Issues_Challenges_and_Road_Ahead (дата обращения: 05.04.2024)
3. Ida, Or. Kubernetes Pentest Methodology [Электронный ресурс] URL: https://www.cyberark.com/resources/threat-research-blog/kubernetes-pentest-methodology-part-3 (дата обращения: 05.04.2024)
4. Shamim M. S. I., Bhuiyan F. A., Rahman A. Xi commandments of kubernetes security: A systematization of knowledge related to kubernetes security practices //2020 IEEE Secure Development (SecDev). – 2020. – С. 58-64.
5. Open Policy Agent Documentation [Электронный ресурс] URL: https://www.openpolicyagent.org/docs/latest/ (дата обращения: 05.04.2024)

References

1. Kybernetes Documentation: Securing a Cluster [Electronic resource] URL: https://kubernetes.io/docs/tasks/administer-cluster/securing-a-cluster / (date of request: 04/05/2024)
2. Containers’ Security: Issues, Challenges, and Road Ahead [Electronic resource] URL: https://www.researchgate.net/publication/332482728_Containers'_Security_Issues_Challenges_and_Road_Ahead (accessed 05.04.2024)
3. Ida Or. Kybernetes Pentest Methodology [Electronic resource] URL: https://www.cyberark.com/resources/threat-research-blog/kubernetes-pentest-methodology-part-3 (date of application: 04/05/2024)

4. Shami m M. S. I., Bhuiyan F. A., Rahman A. Xi commands of kubernetes security: A systematization of knowledge related to kubernetes security practices //2020 IEEE Secure Development (SecDev). – 2020. – pp. 58-64.
5. Open Policy Agent Documentation [Electronic resource] URL: https://www.openpolicyagent.org/docs/latest / (date of application: 04/05/2024)

Варнавский А.В. Методы автоматизации однотипных операций на примере заполнения основной надписи в программном комплексе Autodesk Revit // Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 6(44) с. 63–69

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.4

МЕТОДЫ АВТОМАТИЗАЦИИ ОДНОТИПНЫХ ОПЕРАЦИЙ НА ПРИМЕРЕ ЗАПОЛНЕНИЯ ОСНОВНОЙ НАДПИСИ В ПРОГРАММНОМ КОМПЛЕКСЕ AUTODESK REVIT

Варнавский А.В.
ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АРХИТЕКТУРНО-СТРОИТЕЛЬНЫЙ УНИВЕРСИТЕТ", Санкт-Петербург, Россия (190005, г. Санкт-Петербург, 2-я Красноармейская ул., д.4), e-mail: a.v-var@mail.ru

В работе представлены методы автоматического заполнения основной надписи при оформлении чертежей в программном комплексе Autodesk Revit. Для реализации данных методов были применены такие программные комплексы как Dynamo, встроенная платформа для визуального программирования Autodesk Revit, а также Revit API, для которого был разработан плагин на объектно-ориентированном языке программирования C#, с помощью интегрированной среды разработки Microsoft Visual Studio. Для заполнения основной надписи с помощью расширения созданном в Dynamo был использован метод импортирования данных из электронной таблицы Microsoft Excel, во втором случае данные вводятся через интерфейс. Таким образом созданы расширения, позволяющие сократить время заполнения основной надписи.

Ключевые слова: BIM; визуальное программирование; Dynamo; Revit API; C#; объектно-ориентированное программирование.

METHODS FOR AUTOMATING SIMILAR OPERATIONS USING THE EXAMPLE OF FILLING IN THE MAIN LABEL IN THE AUTODESK REVIT SOFTWARE PACKAGE

Varnavsky A.V.
ST. PETERSBURG STATE UNIVERSITY OF ARCHITECTURE AND CIVIL ENGINEERING, St. Petersburg, Russia (190005, St. Petersburg, 2nd Krasnoarmeyskaya st., 4), e-mail: a.v-var@mail.ru

The paper presents methods for automatically filling in the main label when making drawings in the Autodesk Revit software package. To implement these methods, software packages such as Dynamo, the built-in visual programming platform Autodesk Revit, as well as the Revit API, for which a plugin was developed in the object-oriented programming language C#, using the integrated development environment Microsoft Visual Studio. To fill in the main label using the extension created in Dynamo, the method of importing data from a Microsoft Excel spreadsheet was used, in the second case, the data is entered through the interface. Thus, extensions have been created to reduce the time required to fill in the main label.

Keywords: BIM; visual programming; Dynamo; Revit API; C#; object-oriented programming.

В наше время быстрыми темпами развиваются технологии информационного моделирования. Данный факт затрагивает не только сферу строительства и проектирования, но и так или иначе отражается на экономике, так как внедрение и апробация новых технологий требуют времени и материальных вложений компаний [1].

Наиболее тяжело переход к новым технологиям даётся малому и среднему бизнесу. Это связано с дороговизной программного обеспечения, временем, которое необходимо затратить

на обучение сотрудников, актуализацию текущих проектов под новые стандарты и методы проектирования. Однако необходимо учитывать тот факт, что в перспективе такой переход поможет наладить более качественное производство [2].

Основным преимуществом, которое отмечают инженеры и проектировщики при использовании технологий информационного моделирования, является возможность находить и устранять коллизии на этапе проектирования. При этом можно отметить большую экономию сил и времени [3].

Современные программные комплексы BIM позволяют детально настроить работу путём создания дополнительных расширений. Это позволяет автоматизировать процессы, ещё больше ускоряя сроки проектирования.

Существуют различные инструменты автоматизации проектирования в Autodesk Revit, из основных можно выделить Dynamo и Revit API. Эти два расширения наиболее широко используются при создании плагинов.

Основная надпись является неотъемлемой частью любого чертежа. Заполнение и оформление её в графической части проектной документации может занимать значительное время, поэтому автоматизация данного процесса поможет освободить время проектировщикам.

Самым простым решением является создание расширения на базе встроенной в Autodesk Revit платформы визуального проектирования Dynamo, которая позволяет без стороннего программного обеспечения, внутри Autodesk Revit, запустить данную платформу.

Структура данного расширения (Рисунок 1) следующая:

- Импорт данных для заполнения основной надписи из таблицы Microsoft Excel.
- Выбор необходимых параметров проекта для заполнения.
- Присвоение выбранным параметрам проекта экспортированных данных.

Рисунок 1 – Упрощённая структура расширения (Dynamo)

Источник: анализ автора

Основные ноды, которые используются при реализации данного расширения:

1. Для экспорта данных из таблицы Microsoft Excel используется нод «Data.ImportExcel» (Рисунок 2).

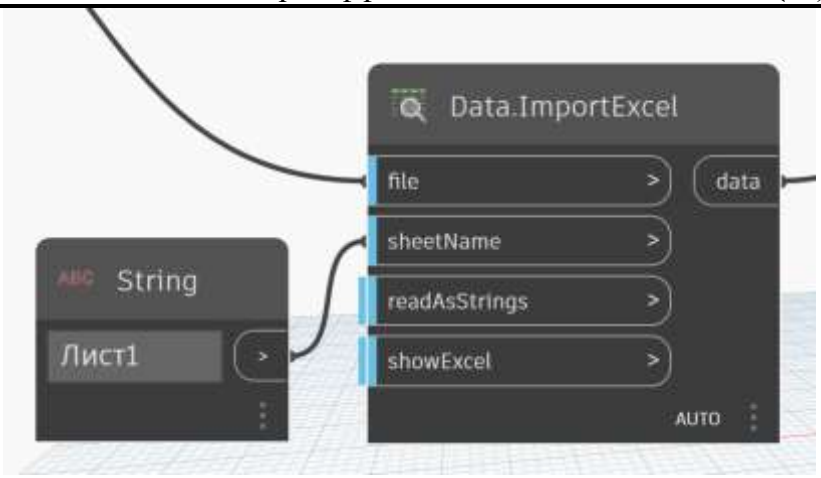


Рисунок 2 – Структура нода «Data.ImportExel»

Источник: Платформа визуального программирования Dynamo

Структура данного нода выглядит следующим образом:

a. В узел входных данных «file» подключается объект, преобрази-ванный в ноде «File From Path», из этого файла будет идти импорт данных.
b. В узле «sheetName» определяется из какого листа электронной таблицы должен производиться импорт данных. Тип вводных данных «String».
c. В узле «readAsString» переключается чтение ячеек по строкам. Тип вводных данных «bool» (значение по умолчанию «false»).
d. В узле «showExcel» переключается отображение главного окна Microsoft Excel. Тип вводных данных «bool» (значение по умолчанию «false»).
e. В узел выходных данных выводятся строки с данными из листа электронной таблицы Microsoft Excel.

2. Для того, чтобы в проекте экспортированные данные встали на свои места, требуется выделить из внутреннего списка элементов проекта необходимые (Рисунок 3).

a. Нод «Categories» позволяет выделить из всех категорий, заложенных в программе не обходимую для решения задачи, в данном случае это категория «Листы», так как в них и будут заполняться параметры основной надписи.
b. Нод «All Elements of Category» возвращает значение всех элементов категории, которая была подключена в вводном узле нода.
c. Для простоты вводятся дополнительные ноды, в которых указываются наименования необходимых для заполнения элементов.

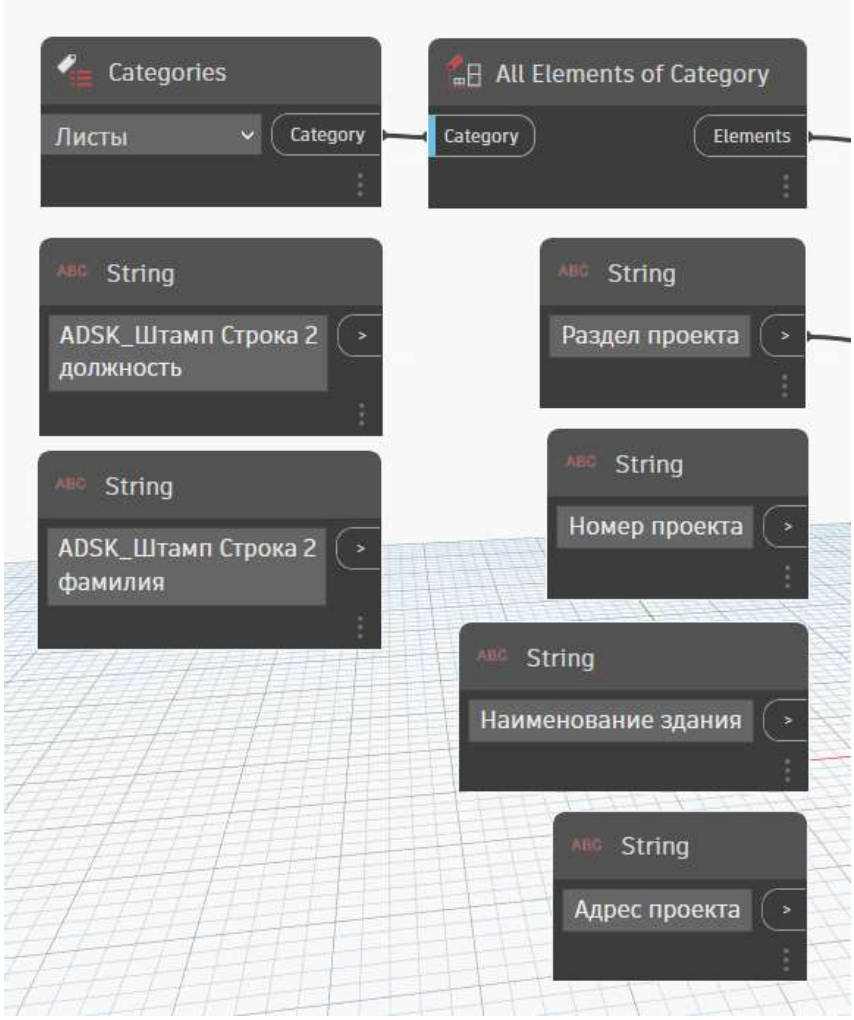


Рисунок 3 – Структура нода «Data.ImportExel»

Источник: Платформа объектно-ориентированное программирование Dynamo

3. Для присвоения параметров элементу используем нод Element.SetParameterByName (Рисунок 4), имеющий следующую структуру:

a. В вводной узел «element» подаётся информация о том какой, элемент будет вводиться изменение;
b. В вводной узел «parameterName» подаётся информация о том, какой параметр элемента будет изменён (в данном случае это «Раздел проект-та»);
c. В вводной узел «value» подаётся информация о том, какое значение будет присвоено параметру элемента.

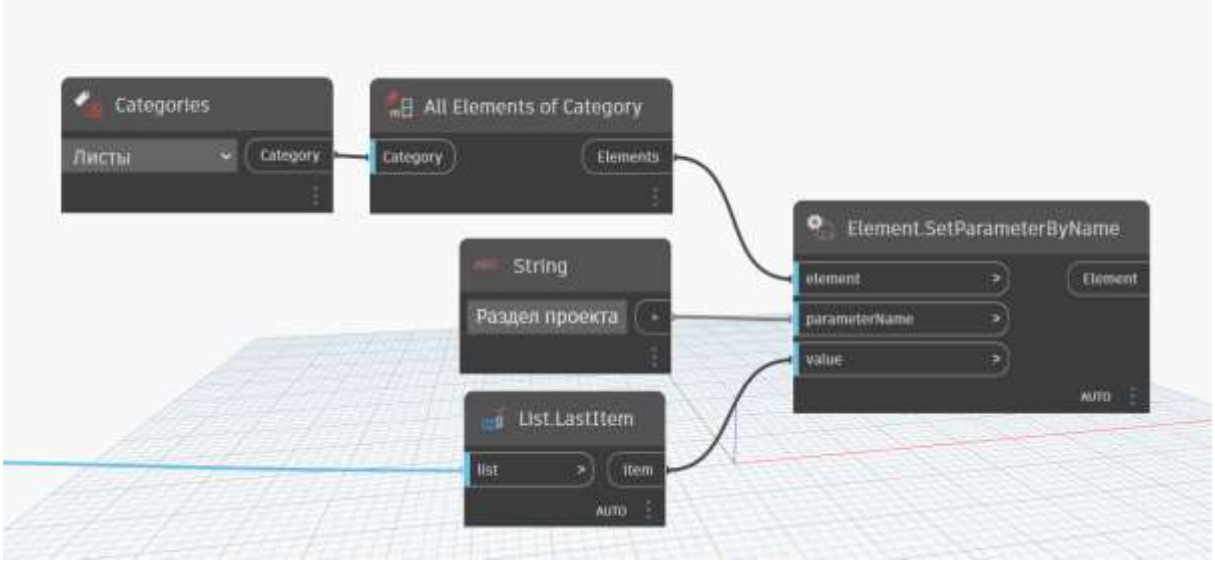


Рисунок 4 – Структура нода «Element.SetParameterByName»

Источник: Платформа визуального программирования Dynamo

После компиляции данного расширения и сохранения файла, его можно загрузить в «Проигрыватель Dynamo» непосредственно в Revit во вкладке «Управление» для более быстрого доступа к расширению, без необходимости запускать Dynamo.

Другой способ, более сложный в плане реализации, но более простой с точки зрения пользователя, использует в своей основе Revit API.

Структура расширения, созданного на языке программирования C#, представлена на Рисунке 5.

Рисунок 5 – Упрощённая структура расширения (C#)

При запуске расширения открывается окно ввода данных (Рисунок 6), в котором задаются необходимые данные для заполнения основной надписи. После заполнения программа, используя метод «get_Parameter» находит необходимый параметр для заполнения и присваивает ему, с помощью метода «Set», вводимые данные.

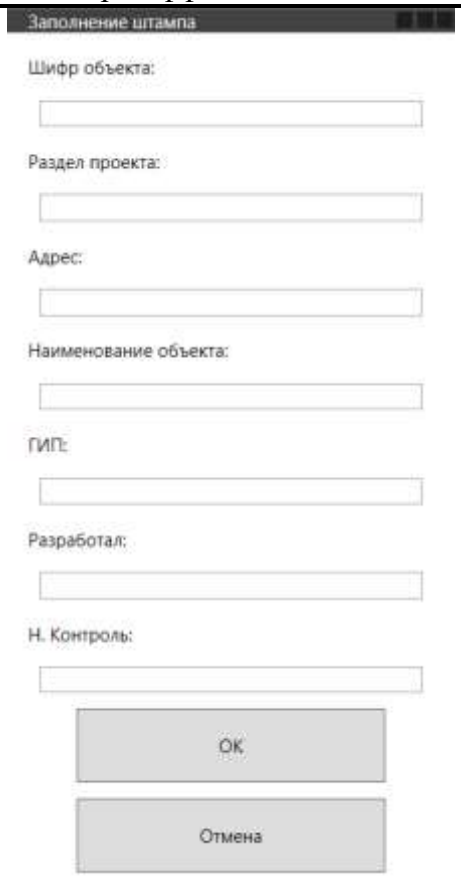


Рисунок 6 – Окно ввода данных (C#)
Источник: Платформа визуального программирования Microsoft Visual Studio

На основании проведенного анализа и разработанных скриптов представлены результаты, которые позволят упростить процесс разработки документации при проектировании зданий и сооружений.

Время, сэкономленное за счет повышения оперативности решения рутинных задач, позволит проектировщикам сконцентрировать усилия на более значимых проблемах [4].

Внедрение информационного моделирования в строительство направлено на оптимизацию проектирования объектов капитального строительства. В дальнейшем есть возможность ещё больше упростить процессы проектирования, например, инженерных сетей. Уже сейчас есть расширения для программного комплекса Autodesk Revit, которые автоматически прокладывает трубопроводы, воздуховоды и электрические сети по заданным ключевым точкам [5], а также создавать конструкции сложной конфигурации, проектирование которых занимает значительную часть рабочего времени проектировщиков, архитекторов и конструкторов что положительно скажется на экономической стороне проекта [6]. Не все проектные решения, принятые машинным интеллектом, реализуемы и корректны. Человеку так или иначе приходится корректировать трассировки тех же инженерных сетей. Но в то же время исключение из работы рутинных и монотонных процессов и операций существенно облегчает проектирование, оставляя больше времени для более творческих задач.

Список литературы

1. Воропаев Л.Ю., В.П. Мамугина В.П. Проблемы проектирования в BIM-среде // Жилищное строительство. 2018. № 7. С. 27–31. EDN REWTRM.

2. Попов А.Р., Попов Р.А., Савенко А.А. Перспективы моделирования экономико-технологических процессов в строительном комплексе на основе BIM-технологий // Экономика устойчивого развития. 2019. № 3(39). С. 239–243. EDN CGWFUZ.
3. Данилина Н.В. Применение BIM-технологий на стадии градостроительного проектирования//Промышленное и гражданское строительство. 2018. № 9. С. 48–54. EDN MFSOPZ.
4. Карасёв И.С., Опарина Л.А. Сокращение сроков проектирования за счет автоматизации типовых задач с использованием BIM//Молодые ученые - развитию Национальной технологической инициативы. 2022. № 1. С. 430–432. EDN AYWHRA.
5. Чернецова А.А., Марченко А.Е., Лясковская Е.А. Автоматизация BIM-технологий в проектировании инженерных систем//Управление развитием социально-экономических систем: Материалы V Всероссийской научно-практической конференции, Ульяновск, 27 мая 2022 года. Ульяновск: Ульяновский государственный технический университет. 2022. С. 241–443. EDN BJHQGH.
6. Перцева А. Е., Хижняк Н. С., Радаев А. Е. Алгоритм проектирования конструкций сложной конфигурации с использованием средств автоматизации (на примере Autodesk Revit, Autodesk AutoCAD и Dynamo)//Транспортные сооружения. 2018. Т. 5, № 4. С. 4. DOI 10.15862/04SATS418. EDN YURQWD.

References

1. Voropaev L.Yu., V.P. Mamugina V.P. Problems of design in a BIM environment // Housing construction. 2018. No. 7. pp. 27-31. EDN REWTRM.
2. Popov A.R., Popov R.A., Savenko A.A. Prospects for modeling economic and technological processes in the construction complex based on BIM technologies // The economics of sustainable development. 2019. No. 3(39). pp. 239-243. EDN CGWFUZ.
3. Danilina N.V. Application of BIM technologies at the stage of urban planning design // Industrial and civil engineering. 2018. No. 9. pp. 48-54. EDN MFSOPZ.
4. Karasev I.S., Oparina L.A. Shortening the design time by automating typical tasks using BIM // Young scientists - development of the National Technological Initiative. 2022. No. 1. pp. 430-432. EDN AYWHRA.
5. Chernetsova A.A., Marchenko A.E., Lyaskovskaya E.A. Automation of BIM technologies in engineering systems design // Management of socio-economic systems development: Materials of the V All-Russian Scientific and Practical Conference, Ulyanovsk, May 27, 2022. Ulyanovsk: Ulyanovsk State Technical University. 2022. pp. 241-443. EDN BJHQGH.
6. Pertseva A. E., Khizhnyak N. S., Radaev A. E. Algorithm for designing structures of complex configuration using automation tools (using the example of Autodesk Revit, Autodesk AutoCAD and Dynamo) // Transport structures. 2018. Vol. 5, No. 4. p. 4. DOI 10.15862/04SATS418. EDN YURQWD.

Нижлукченко И.Д. VPN: как это работает и почему это важно для вашей приватности. объяснение принципов работы виртуальных частных сетей и их роли в обеспечении конфиденциальности данных // Международный журнал информационных технологий и энергоэффективности.– 2024. –Т. 9 № 6(44) с. 70–74

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.7

VPN: КАК ЭТО РАБОТАЕТ И ПОЧЕМУ ЭТО ВАЖНО ДЛЯ ВАШЕЙ ПРИВАТНОСТИ. ОБЪЯСНЕНИЕ ПРИНЦИПОВ РАБОТЫ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ И ИХ РОЛИ В ОБЕСПЕЧЕНИИ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ

Нижлукченко И.Д.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: nizhluchenk@gmail.com

В эпоху, когда цифровая безопасность и конфиденциальность данных стали важнейшими аспектами нашего онлайн-присутствия, использование виртуальных частных сетей (VPN) выходит на передний план как эффективное средство защиты. Настоящая статья представляет собой всесторонний анализ принципов работы VPN, подчеркивая их критическую роль в обеспечении анонимности и безопасности пользовательских данных в интернете. Мы исследуем, как зашифрованный канал, создаваемый VPN, защищает информацию от внешних угроз, включая злоумышленников и наблюдение со стороны интернет-провайдеров. Освещается важность изменения IP-адреса пользователя на адрес сервера VPN для обеспечения анонимности и обхода географических ограничений.

Ключевые слова: Виртуальные частные сети, VPN, цифровая безопасность, конфиденциальность данных, шифрование, анонимность в интернете, защита персональных данных, политика конфиденциальности VPN, протоколы шифрования, выбор VPN-провайдера, обход географических ограничений, безопасное подключение, интернет-приватность, безопасность Wi-Fi, кибербезопасность, защита от слежки, сохранение анонимности.

VPN: HOW IT WORKS AND WHY IT'S IMPORTANT FOR YOUR PRIVACY. EXPLANATION OF THE PRINCIPLES OF VIRTUAL PRIVATE NETWORKS AND THEIR ROLE IN ENSURING DATA PRIVACY

Nizhlukchenko I.D.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: nizhluchenk@gmail.com

In an era when digital security and data privacy have become the most important aspects of our online presence, the use of virtual private networks (VPNs) is coming to the fore as an effective means of protection. This article provides a comprehensive analysis of the principles of VPN operation, emphasizing their critical role in ensuring the anonymity and security of user data on the Internet. We are investigating how the encrypted channel created by a VPN protects information from external threats, including intruders and surveillance by Internet service providers. The importance of changing the user's IP address to the address of the VPN server to ensure anonymity and circumvent geographical restrictions is highlighted.

Keywords: Virtual private networks, VPN, digital security, data privacy, encryption, anonymity on the Internet, personal data protection, VPN privacy policy, encryption protocols, choosing a VPN provider, circumventing geographical

restrictions, secure connection, Internet privacy, Wi-Fi security, cybersecurity, protection from surveillance, preservation anonymity.

VPN создает зашифрованный туннель между вашим устройством и сервером VPN, через который проходит весь ваш интернет-трафик. Это означает, что вся информация, отправляемая и получаемая через VPN, зашифрована и скрыта от любых внешних наблюдателей, включая вашего интернет-провайдера (ISP), правительственные органы и злоумышленников.

Ключевым элементом технологии VPN является использование протоколов шифрования, таких как OpenVPN, IKEv2/IPSec и WireGuard. Эти протоколы обеспечивают высокий уровень безопасности данных, передаваемых через интернет, благодаря сложным алгоритмам шифрования.

Кроме того, VPN позволяет пользователям скрыть свой истинный IP-адрес, заменив его IP-адресом сервера VPN. Это не только повышает анонимность в сети, но и позволяет обойти географические ограничения, предоставляя доступ к контенту, который может быть заблокирован в их стране.

Принцип работы виртуальных частных сетей (VPN) укоренен в создании безопасного и зашифрованного канала между устройством пользователя и интернетом. Этот процесс начинается, когда пользователь подключается к VPN-серверу, выбранному из списка доступных географических локаций. После установления соединения между устройством пользователя и VPN-сервером, все интернет-трафик пользователя начинает перенаправляться через этот сервер.

Суть работы VPN заключается в том, что перед отправкой данных из устройства пользователя в интернет, эти данные зашифровываются. Зашифрование обеспечивается благодаря использованию сложных алгоритмов, которые преобразуют передаваемую информацию в форму, недоступную для чтения любым сторонним наблюдателям без соответствующего ключа для расшифровки. Таким образом, даже если данные перехватываются в процессе передачи, они остаются защищенными и конфиденциальными.

После того как данные достигают VPN-сервера, они расшифровываются и отправляются в интернет от имени сервера. Это означает, что внешние наблюдатели, такие как интернет-провайдеры или веб-сайты, видят IP-адрес VPN-сервера, а не истинный IP-адрес пользователя. Такой подход не только способствует анонимности пользователя в сети, но и позволяет обходить географические ограничения контента, поскольку пользователь может казаться подключенным к интернету из любой точки мира, где расположен VPN-сервер.

Данный механизм работы VPN обеспечивает критический уровень безопасности и приватности в современном цифровом мире, где угрозы персональным данным и конфиденциальности постоянно растут. Путем зашифровки данных и скрытия истинного IP-адреса пользователя, VPN помогает защитить личную информацию от несанкционированного доступа, снижает риск кибератак и способствует сохранению конфиденциальности в сети.

Использование VPN важно по нескольким причинам. Во-первых, оно защищает вашу онлайн-активность от внешнего наблюдения, что критически важно в условиях современного цифрового мира, где данные пользователя часто собираются и анализируются без его согласия. Во-вторых, VPN обеспечивает защиту данных при использовании публичных Wi-Fi сетей, которые часто являются уязвимыми для атак злоумышленников.

Важность использования виртуальных частных сетей (VPN) для защиты приватности в современном мире трудно переоценить, учитывая масштабы и разнообразие угроз в интернете. Приватность в интернете не просто о защите личных данных от посторонних глаз; это также вопрос сохранения контроля над информацией, которую мы делимся в сети, и предотвращения ее использования без нашего согласия.[3] В этом контексте VPN выступает как мощный инструмент, обеспечивающий защиту и анонимность пользователям.

Во-первых, зашифрованный канал, создаваемый VPN, обеспечивает безопасность данных пользователя во время их передачи в интернет. Это особенно важно при использовании незащищенных сетей Wi-Fi, таких как общественные точки доступа в кафе или аэропортах, где риск перехвата данных злоумышленниками особенно высок. Благодаря VPN пользователи могут быть уверены, что их персональная информация, включая пароли, финансовые данные и личные сообщения, защищена от подобных атак.

Во-вторых, изменение IP-адреса пользователя на адрес сервера VPN помогает сохранить анонимность в интернете. Это не только усложняет задачу для сайтов и рекламодателей, пытающихся отслеживать онлайн-активность и создавать детализированные профили пользователей для таргетирования рекламы, но и предоставляет возможность обхода цензуры и доступа к информации без ограничений, которые могут быть наложены правительствами или интернет-провайдерами.

Кроме того, в условиях постоянно растущего объема сбора данных и наблюдения со стороны государственных органов и частных компаний, использование VPN становится важным инструментом для защиты права на частную жизнь.[4] Оно позволяет пользователям в некоторой степени восстановить контроль над своей личной информацией, сократить количество собираемых о них данных и снизить вероятность их неправомерного использования.

Таким образом, в контексте непрерывно расширяющегося цифрового пространства, где личная информация становится все более уязвимой, VPN выступает не просто как средство для улучшения сетевой безопасности, но и как фундаментальный элемент в стремлении к сохранению приватности в интернете. Он предоставляет пользователям возможность защитить свои данные и сохранить анонимность, что является ключевым аспектом в обеспечении свободы и конфиденциальности в цифровую эпоху.

Выбор надежного VPN-провайдера является критически важным аспектом в обеспечении онлайн-безопасности и приватности. В мире, где цифровая безопасность играет все более значительную роль, качество и надежность VPN-сервиса напрямую влияют на степень защиты, которую пользователь получает при его использовании.[5] Надежный VPN-провайдер обеспечивает не только высокий уровень шифрования и безопасности данных, но и строгую политику конфиденциальности, гарантирующую, что пользовательские данные не собираются, не хранятся и не передаются третьим лицам без согласия пользователя.

Одним из ключевых аспектов надежности VPN-сервиса является использование передовых технологий шифрования. Это обеспечивает, что даже в случае перехвата данных злоумышленниками, они останутся недоступными для чтения без соответствующего ключа расшифровки. Но технологии шифрования — это лишь один из элементов. Важно также обратить внимание на протоколы безопасности, которые использует провайдер, поскольку они определяют уровень защиты и скорость соединения.

Другой критически важный аспект — политика конфиденциальности провайдера. Надежные VPN-сервисы придерживаются политики «без журналов», что означает отсутствие сохранения записей о действиях пользователя в интернете. Это предотвращает возможность доступа к пользовательским данным даже при получении официального запроса от правоохранительных органов, тем самым обеспечивая анонимность пользователя.

Кроме того, репутация и прозрачность деятельности VPN-провайдера играют значительную роль в выборе надежного сервиса. Провайдеры, которые открыто делятся информацией о своих операционных процедурах, политиках безопасности и конфиденциальности, а также регулярно проходят независимые аудиты безопасности, заслуживают большего доверия. Отзывы пользователей и экспертные обзоры также могут служить хорошим ориентиром при выборе сервиса, так как они отражают реальный опыт использования.

В заключение, выбор надежного VPN-провайдера не только увеличивает эффективность защиты пользовательских данных в интернете, но и обеспечивает спокойствие пользователя, зная, что его приватность находится в надежных руках.[1] Учитывая широкий спектр предложений на рынке VPN-сервисов, важно провести тщательный анализ и выбрать провайдера, который соответствует высоким стандартам безопасности, приватности и пользовательского опыта.

Роль виртуальных частных сетей (VPN) в современном цифровом пространстве не может быть недооценена. Как мощный инструмент для обеспечения анонимности и безопасности в интернете, VPN предоставляет пользователям необходимые средства для защиты их персональных данных от внешних угроз. Через создание зашифрованного туннеля и скрытие IP-адреса, VPN способствует сохранению конфиденциальности и предотвращению несанкционированного доступа к информации.

Однако выбор надежного VPN-провайдера является ключевым аспектом, определяющим эффективность защиты. Пользователям следует уделять внимание таким факторам, как политика конфиденциальности, качество шифрования, репутация и отзывы о сервисе.[2] Важно помнить, что VPN является лишь одним из элементов комплексной стратегии кибербезопасности, и его использование должно дополняться другими методами защиты, включая соблюдение мер безопасности при онлайн-активности и использование надежных антивирусных программ.

В контексте постоянно растущих угроз в интернете, VPN остается незаменимым инструментом для тех, кто стремится к максимальной защите своей приватности и безопасности данных. Внедрение и активное использование VPN становится важным шагом на пути к обеспечению цифровой свободы и защиты в глобальной сети, подчеркивая важность информационной безопасности в нашей повседневной жизни.

Список литературы

1. Гельфанд А. М. и др. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе//Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2018. – №. 8. – С. 91-97.

2. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO//Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
3. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения–Информационные технологии и телекоммуникации, 2021 //Т. – 2021. – Т. 9. –С. 1-2
4. Катасонов А. И., Штеренберг С. И., Цветков А. Ю. Оценка стойкости механизма, реализующего Мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства gnu linux//Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 2. – С. 50-56.
5. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411

References

1. Gelfand A.M. et al. Development of a model for the distribution of self-modifying code in a protected information system //Modern science: actual problems of theory and practice. Series: Natural and Technical Sciences. – 2018. – No. 8. – pp. 91-97.
2. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: current aspects of the "GNII" National Development". July 2018. – 2018. – pp. 31-35.
3. Shterenberg S. I., Moskalchuk A. I., Krasov A.V. Development of security scenarios for creating vulnerable virtual machines and studying penetration testing methods–Information technologies and Telecommunications, 2021 //Vol. – 2021. – vol. 9. –pp. 1-2
4. Katasonov A. I., Shterenberg S. I., Tsvetkov A. Yu. Assessment of the stability of the mechanism implementing... The mandatory essential role model of access rights differentiation in gnu linux operating systems //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – No. 2. – pp. 50-56.
5. Budarny G. S. et al. Types of security breaches and typical attacks on the operating system //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 406-411.

Борисенко Д.С. сравнение алгоритмов обработки естественной речи: Longformer-Encoder-Decoder и Big Bird // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 6(44) с. 75–79

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.932.2

СРАВНЕНИЕ АЛГОРИТМОВ ОБРАБОТКИ ЕСТЕСТВЕННОЙ РЕЧИ: LONGFORMER-ENCODER-DECODER И BIG BIRD

Борисенко Д.С.
ФГАОУ ВО «МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия, (107023, Москва, Большая Семёновская ул., д. 38), e-mail: 12325477@yandex.ru

В данной статье проведено сравнение алгоритмов обработки естественной речи (NLP), на моделях Longformer-Encoder-Decoder (LED) и Big Bird, с фокусом на выбор между точностью и эффективностью на долгих текстах. Исследование основано на четырёх наборах данных из SCROLLS бенчмарка и покрывает два основных направления задач NLP: суммаризацию и ответы на вопросы. Особое внимание уделено влиянию размера модели и длины входных последовательностей на общую эффективность и точность.

Ключевые слова: Обработка естественного языка, сравнение алгоритмов NLP, Longformer-Encoder-Decoder, Big Bird, SCROLLS бенчмарк, суммаризация текста, энергоэффективность в NLP.

COMPARISON OF NATURAL SPEECH PROCESSING ALGORITHMS: LONGFORMER-ENCODER-DECODER AND BIG BIRD

Borisenko D.S.
MOSCOW POLYTECHNIC UNIVERSITY, Moscow, Russia, (107023, Moscow, Bolshaya Semyonovskaya str., 38), e-mail: 12325477@yandex.ru

This article compares natural speech processing (NLP) algorithms based on Longformer-Encoder-Decoder (LED) and Big Bird models, with a focus on choosing between accuracy and efficiency on long texts. The study is based on four datasets from the SCROLLS benchmark and covers two main areas of NLP tasks: summarization and answering questions. Special attention is paid to the effect of the model size and the length of the input sequences on overall efficiency and accuracy.

Keywords: Natural language processing, comparison of NLP algorithms, Longformer-Encoder-Decoder, Big Bird, SCROLLS benchmark, text summarization, energy efficiency in NLP.

Введение

В последние годы область обработки естественного языка (NLP) испытала значительный прогресс, благодаря развитию алгоритмов машинного обучения и, в частности, архитектур на основе Transformer [1]. Эти модели демонстрируют выдающиеся результаты в широком спектре задач NLP, включая перевод текста, генерацию ответов на вопросы и суммаризацию. Тем не менее, улучшение качества моделей часто требует увеличения их размера и, как следствие, роста вычислительных затрат и энергопотребления. Это особенно актуально при работе с длинными текстами, где требуется обработка больших объемов данных и поддержка длительных зависимостей в тексте [2].

С развитием инициативы Green AI возникла необходимость в разработке более эффективных моделей, которые могут достигать высокой точности при сниженных затратах ресурсов. В этом контексте особый интерес представляют модели Longformer-Encoder-Decoder (LED) и Big Bird, разработанные для эффективной работы с длинными текстами. Настоящее исследование направлено на сравнение этих алгоритмов с точки зрения баланса между точностью и эффективностью, что является ключевым аспектом при выборе подхода к решению задач NLP в условиях ограниченных ресурсов.

Методология

В основу нашего исследования положен анализ производительности моделей LED и Big Bird на данных из бенчмарка SCROLLS, включающего четыре датасета, охватывающих задачи суммаризации и ответов на вопросы. Эти задачи были выбраны в силу их актуальности и сложности, а также для оценки способности алгоритмов эффективно обрабатывать длинные тексты[3].

Основной фокус исследования направлен на изучение влияния двух ключевых факторов на производительность моделей: размера модели и длины входных последовательностей. Было проведено сравнение по нескольким параметрам, включая точность (основываясь на метриках, специфичных для каждой задачи), скорость обработки данных, потребление энергии и общую эффективность использования ресурсов.

Для обеспечения объективности результатов, все модели обучались и тестировались в единых условиях на одинаковом оборудовании. Был проведен детальный анализ результатов, который включал в себя не только сравнение точности, но и оценку затрат энергии и времени на обучение и инференс моделей. Такой подход позволил выявить наиболее эффективные стратегии работы с длинными текстами в рамках задач NLP, учитывая текущие ограничения по ресурсам и необходимость минимизации энергопотребления.

Результаты и Анализ

Исследование продемонстрировало значительные различия в производительности между моделями LED и Big Bird на задачах суммаризации и ответов на вопросы. В обеих категориях задач модель LED показала лучшую точность при меньшем энергопотреблении по сравнению с моделью Big Bird.

Для задач суммаризации точность моделей оценивалась с использованием метрики Rouge, которая определяется следующим образом:

$$Rouge = \frac{\text{Количество совпадающих слов в референсном и генерированном суммариях}}{\text{Общее количество слов в референсном суммарии}}$$

Модель LED показала лучшие результаты по метрике Rouge на всех длинах входных последовательностей, что указывает на её превосходную способность к суммаризации длинных текстов.

В задачах на ответы на вопросы точность оценивалась с использованием F1-меры, которая рассчитывается как гармоническое среднее точности и полноты [4]

$$F_1 = 2 \times \frac{\text{Точность} \times \text{Полнота}}{\text{Точность} + \text{Полнота}}$$

На этом фронте меньшие модели LED показали себя особенно хорошо, обеспечивая высокую точность при сравнительно низком энергопотреблении, благодаря возможности

использования большего размера обучающих пакетов в рамках фиксированного ресурсного бюджета.

Энергоэффективность моделей была изучена через измерение общего энергопотребления во время обучения и инференса, а также скорости обработки данных. Энергопотребление было рассчитано с использованием следующей формулы:

$$\text{Энергопотребление} = \text{Мощность} \times \text{Время}$$

где мощность измерялась в ваттах (Вт), а время – в секундах (с). Результаты показали, что увеличение размера модели LED ведёт к улучшению точности с меньшим увеличением энергопотребления по сравнению с увеличением длины входных последовательностей. Это подчеркивает важность выбора оптимального размера модели для баланса между эффективностью и точностью в приложениях NLP.

Таблица 1 – Сравнение производительности моделей на задачах суммаризации

Модель	Длина Последовательности	Rouge Score	Энергопотребление (кВт·ч)
LED-base	1024	45.2	0.5
LED-base	2048	46.7	0.7
LED-large	1024	48.3	0.8
LED-large	2048	49.5	1.1
Big Bird-large	1024	44.8	0.6
Big Bird-large	2048	45.4	0.9

Таблица 2 – Сравнение производительности моделей на задачах ответов на вопросы

Модель	Длина Последовательности	F1 Score	Энергопотребление (кВт·ч)
LED-base	1024	67.4	0.4
LED-base	2048	69.1	0.6
LED-large	1024	70.5	0.9
LED-large	2048	72.0	1.2
Big Bird-large	1024	66.8	0.5
Big Bird-large	2048	67.5	0.8

Эти таблицы демонстрируют, как увеличение размера модели и длины входных последовательностей влияет на производительность и энергопотребление. В обоих случаях, LED-large показывает лучшие результаты по сравнению с LED-base и Big Bird в плане точности (Rouge Score и F1 Score), но это сопровождается увеличением энергопотребления. Однако, повышение точности может оправдать дополнительные затраты энергии, особенно в приложениях, где высокая точность является критически важным фактором [5].

Выводы

Исследование подтвердило, что модели Longformer-Encoder-Decoder обеспечивают лучшую балансировку между точностью и энергоэффективностью по сравнению с моделью Big Bird, особенно при работе с длинными текстами. Выбор между увеличением размера модели и длины входных последовательностей оказывает значительное влияние на общую производительность и потребление ресурсов, что делает наше сравнение ценным руководством для оптимизации ресурсов в приложениях NLP.

Список литературы

1. Beltagy, I., Peters, M. E., & Cohan, A. (2020). Longformer: The Long-Document Transformer. [Электронный ресурс]. Режим доступа: https://arxiv.org/abs/2004.05150.
2. Chen M., Chu Z., Wiseman S., & Gimpel, K. (2021). SummScreen: A Dataset for Abstractive Screenplay Summarization. [Электронный ресурс]. Режим доступа: https://arxiv.org/abs/2104.07091.
3. Devlin J., Chang M.-W., Lee K., & Toutanova K. (2019). BERT: Pre-training of deep bidirectional transformers for language understanding. В: Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, С. 4171–4186. [Электронный ресурс]. Режим доступа: https://doi.org/10.18653/v1/N19-1423.
4. Dasigi, P., Lo, K., Beltagy, I., Cohan, A., Smith, N. A., & Gardner, M. (2021). A dataset of information-seeking questions and answers anchored in research papers. В: Proceedings of the 2021 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, С. 4599–4610. [Электронный ресурс]. Режим доступа: https://doi.org/10.18653/v1/2021.naacl-main.365.
5. Huang, L., Cao, S., Parulian, N., Ji, H., & Wang, L. (2021). Efficient attentions for long document summarization. В: Proceedings of the 2021 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, С. 1419–1436. [Электронный ресурс]. Режим доступа: https://doi.org/10.18653/v1/2021.naacl-main.112.

References

1. Beltagy, I., Peters, M. E., & Cohan, A. (2020). Longformer: The Long-Document Transformer. [electronic resource]. Access mode: https://arxiv.org/abs/2004.05150
2. Chen, M., Chu, Z., Wiseman, S., & Gimpel, K. (2021). SummScreen: A Dataset for Abstractive Screenplay Summarization. [electronic resource]. Access mode: https://arxiv.org/abs/2104.07091 .
3. Devlin, J., Chang, M.-W., Lee, K., & Toutanova, K. (2019). BERT: Pre-training of deep bidirectional transformers for language understanding. In: Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, pp. 4171-4186. [electronic resource]. Access mode: https://doi.org/10.18653/v1/N19-1423 .
4. Dasigi, P., Lo, K., Beltagy, I., Cohan, A., Smith, N. A., & Gardner, M. (2021). A dataset of information-seeking questions and answers anchored in research papers. In: Proceedings of the 2021 Conference of the North American Chapter of the Association for Computational

Linguistics: Human Language Technologies, pp. 4599-4610. [electronic resource]. Access mode: https://doi.org/10.18653/v1/2021.naacl-main .365.

5. Huang, L., Cao, S., Parulian, N., Ji, H., & Wang, L. (2021). Efficient attentions for long document summarization. In: Proceedings of the 2021 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, pp. 1419-1436. [electronic resource]. Access mode: https://doi.org/10.18653/v1/2021.naacl-main.112 .

Петропавлов Д.М. Повышение безопасности и эффективности: комплексный обзор корпоративных систем контроля и управления доступом // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 6(44) с. 80–87

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.09

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ И ЭФФЕКТИВНОСТИ: КОМПЛЕКСНЫЙ ОБЗОР КОРПОРАТИВНЫХ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Петропавлов Д.М.
ФГБОУ ВО "МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Н.Э. БАУМАНА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)", Москва, Россия, (105005, город Москва, 2-Я Бауманская ул, д. 5 стр. 1), e-mail: petropavlov.deniz@yandex.ru

В статье исследуется пересечение корпоративных систем контроля и управления доступом (СКУД) и систем учета рабочего времени (СУРВ) в современных организациях. Начиная с подробного введения, рассматриваются приложения, состав и требования СКУД, подчеркивая ее роль в защите цифровых активов и регулировании доступа, дополнительно разъясняются сложные технологические аспекты и преимущества интеграции СУРВ, обеспечивая детальное понимание того, как эти системы взаимодействуют друг с другом для оптимизации управления персоналом и усиления мер безопасности. Подчеркивается динамичный характер этой интеграции, учитывая будущие соображения, и поощряет организации оставаться адаптивными в постоянно меняющемся технологическом ландшафте. Эта статья послужит руководством, предлагающим информацию для предприятий, стремящихся повысить уровень безопасности, оптимизировать управление персоналом и использовать перспективный подход к цифровой инфраструктуре.

Ключевые слова: Контроль доступа предприятия, системы управления, учет рабочего времени, аудит пользователей, биометрическая аутентификация, облачные решения, уровень безопасности, управление персоналом.

IMPROVING SECURITY AND EFFICIENCY: A COMPREHENSIVE REVIEW OF CORPORATE ACCESS CONTROL AND MANAGEMENT SYSTEMS

Petropavlov D.M.
BAUMAN MOSCOW STATE TECHNICAL UNIVERSITY (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (105005, Moscow, 2nd Baumanskaya str., 5, bldg. 1), e-mail: petropavlov.deniz@yandex.ru

This article explores the intersection of Enterprise Access Control and Management Systems (EACMS) and Time Tracking Systems (TTS) within the modern organizations. Beginning with an insightful introduction, the article navigates through the applications, composition, and requirements of EACMS, emphasizing its role in securing digital assets and regulating access, it further elucidates on the intricate technological aspects and benefits of integrating a TTS, providing a nuanced understanding of how these systems synergize to streamline workforce management and bolster security measures. It emphasizes the dynamic nature of this integration, addressing future considerations and encouraging organizations to remain adaptive in the ever-evolving technological landscape. This article serves as a guide, offering valuable insights for organizations seeking to fortify their security postures, streamline workforce management, and embrace a future-ready approach to digital infrastructure.

Keywords: Enterprise access control, management systems, time tracking, user auditing, biometric authentication, cloud-based solutions, security posture, workforce management.

Введение

В динамичной и цифровой среде современных предприятий первостепенную важность защиты конфиденциальной информации и управления доступом невозможно переоценить. По мере того, как организации преодолевают сложности взаимосвязанного мира, необходимость в надежном и комплексном решении для контроля и управления доступом становится насущной.

Наступление цифровой эпохи привело к беспрецедентному удобству и эффективности, но одновременно подвергло бизнес множеству киберугроз и проблем безопасности. Растущая зависимость от цифровых платформ для хранения данных, связи и совместной работы требует стратегического и комплексного подхода к контролю доступа. СКУД выступает в качестве стержня этой стратегии, являясь привратником в цифровую сферу организации, одновременно обеспечивая плавное и безопасное взаимодействие.[9]

Цель данной работы — предоставить дорожную карту для организаций, стремящихся улучшить свои меры безопасности и оптимизировать операционную эффективность за счет синергетического объединения систем управления персоналом.

1. Применение и структура системы контроля управления доступом

В сложной системе современного предприятия применение и структура корпоративных систем контроля и управления доступом образуют основу, на которой строится безопасная и эффективная организационная структура. Углубимся в многогранное применение СКУД, выходящее за традиционные границы контроля доступа, и раскроем сложную структуру, определяющую ее функциональность в корпоративной экосистеме.

1.1. Применение

Роль СКУД выходит далеко за рамки простого регулирования физического доступа к зданиям или цифровым системам. В современной динамичной бизнес-среде СКУД служит комплексным решением для управления идентификацией, обеспечивает детальный подход к безопасности: от управления доступом сотрудников к цифровым платформам, базам данных и конфиденциальным файлам до регулирования доступа в безопасные физические места.

Более того, СКУД облегчает управление механизмами аутентификации пользователей, включая биометрические идентификаторы, смарт-карты и многофакторную аутентификацию для укрепления системы безопасности. Это не только предотвращает несанкционированный доступ, но и защищает организацию от кражи личных данных и мошеннических действий.

В сфере контроля цифрового доступа СКУД играет ключевую роль в регулировании разрешений и авторизаций, что позволяет организациям определять детализированную политику доступа. Это не только защищает важную информацию, но и оптимизирует рабочие процессы, обеспечивая доступ к необходимым ресурсам.[2]

Кроме того, СКУД находит применение в управлении посетителями. Предприятия могут улучшить протоколы безопасности, гарантируя, что временный доступ предоставляется только определенным областям и персоналу.

1.2. Структура

Эффективность СКУД заключается в ее сложной структуре, состоящей из нескольких фундаментальных компонентов, которые работают согласованно, укрепляя инфраструктуру безопасности организации:

- *Политики контроля доступа*: определяют правила и положения, регулирующие доступ пользователей. Эти политики адаптированы к конкретным потребностям организации и определяют, кто, к каким ресурсам и при каких условиях может получить доступ.
- *Механизмы аутентификации*: процесс проверки системой личности пользователя, запрашивающего доступ. Могут быть нескольких видов: от комбинаций имен пользователя и пароля, заканчивая усовершенствованными биометрическими идентификаторами. Многофакторная аутентификация добавляет уровень безопасности за счет объединения двух или более механизмов, укрепляя структуру контроля доступа.
- *Протоколы авторизации*: определят уровень доступа, предоставленный аутентифицированным пользователям. Управление доступом на основе ролей (RBAC) назначает разрешения на основе предопределенной роли, в то время как управление доступом на основе атрибутов (ABAC) учитывает характеристики пользователей, время и местоположение, для определения уровней доступа.
- *Мониторинг и аудит*: предоставляют организациям информацию в режиме реального времени о действиях пользователей и потенциальных угрозах безопасности. Регистрация попыток доступа, изменения в разрешениях и аномальное поведение позволят заранее выявить и снизить риски безопасности.

По сути, СКУД представляет собой сложное сочетание политик, технологий и протоколов, сложно переплетенных вместе для создания надежной и адаптируемой структуры контроля доступа внутри предприятия.

2. Требования к системе контроля и управления доступом на предприятие

Развертывание корпоративной системы контроля и управления доступом (СКУД) — это стратегическое мероприятие, требующее тщательного рассмотрения множества требований. Поскольку организации стремятся укрепить свою безопасность и оптимизировать операционную эффективность, понимание и выполнение этих требований становится ключевым. Рассмотрим их:

- *Масштабируемость*: по мере развития и роста организаций инфраструктура контроля доступа должна плавно расширяться. Масштабируемость гарантирует, что СКУД может умело адаптироваться к динамичному характеру предприятий, предотвращая узкие места и неэффективность, которые могут возникнуть в жесткой и нерасширяемой системе. Независимо от того, происходит ли органический рост или стратегическое расширение, масштабируемая СКУД гарантирует, что система контроля доступа остается гибкой и реагирует на меняющиеся требования.[3]
- *Возможности интеграции*: фундаментальным требованием СКУД является его способность интегрироваться с существующей инфраструктурой, приложениями и базами данных, что устраняет разрозненность и повышает общую эффективность системы контроля доступа. Совместимость с протоколами отраслевых стандартов обеспечивает процесс внедрения.
- *Соответствие отраслевым стандартам*: Соблюдение отраслевых стандартов и нормативной базы не подлежит обсуждению для СКУД. Организации действуют в

рамках сложной сети законодательных и нормативных требований, требующих защиты конфиденциальной информации и обеспечения безопасного доступа. Будь то здравоохранение, финансы или любая другая отрасль, СКУД должна соответствовать таким стандартам, как ISO 27001[6], HIPAA или GDPR. Соблюдение требований не только обеспечивает соблюдение правовых норм, но и создает основу для надежных методов обеспечения безопасности. СКУД, соответствующая отраслевым стандартам, предоставляет организациям основу, признанную и уважаемую в глобальном масштабе, укрепляя доверие между заинтересованными сторонами и регулирующими органами.

- *Удобный интерфейс*: удобный интерфейс является обязательным условием, поскольку от него напрямую зависит эффективность взаимодействия сотрудников с системой контроля доступа. Дизайн должен быть интуитивно понятным, сводить к минимуму время обучения для пользователей и обеспечивать удобство работы. С точки зрения администраторов, управляющих разрешениями доступа для конечных пользователей, осуществляющих процессы аутентификации, интерфейс должен быть эргономичным, обеспечивающим положительный опыт без ущерба для безопасности.
- *Адаптация к новым технологиям*: эффективная СКУД должна демонстрировать способность адаптироваться к новым технологиям, гарантируя, что она останется в авангарде достижений в области безопасности. Будь то интеграция методов биометрической аутентификации, внедрение искусственного интеллекта для обнаружения угроз или внедрение блокчейна для повышения целостности данных, адаптируемая СКУД защищает организацию от развивающихся проблем безопасности.
- *Непрерывный мониторинг*: надежная СКУД должна осуществлять бдительный контроль за действиями пользователей. Функции непрерывного мониторинга предоставляют в режиме реального времени информацию о поведении пользователей и потенциальных угрозах безопасности. Регистрация попыток доступа, изменений в разрешениях и аномальных действий позволяет организациям активно выявлять и снижать риски.[8]
- *Мобильный доступ и вопросы удаленной работы*: система должна обеспечивать безопасный доступ с различных устройств, гарантируя, что сотрудники смогут беспрепятственно работать из разных мест без ущерба для безопасности. Это включает в себя внедрение безопасных методов мобильной аутентификации, протоколов шифрования и безопасных соединений для обеспечения гибкости, необходимой современной рабочей силе.

3. Система учета рабочего времени на предприятии

По мере развития современного корпоративного ландшафта интеграция системы учета рабочего времени (СУРВ) с более широкой системой контроля и управления доступом предприятия (СКУД) становится все более необходимой. Комплексные функциональные возможности СУРВ выходят за рамки простого включения и выключения синхронизации; они воплощают в себе сложный подход к управлению персоналом, мониторингу посещаемости и

повышению производительности. В этом разделе рассматриваются тонкости интеграции СУРВ в рамках предприятия, изучаются технологические аспекты, преимущества и соображения, которые делают его синергетическим дополнением к СКУД.

3.1. Технологические аспекты систем учета рабочего времени

Биометрическая аутентификация: современные СУРВ часто используют передовые методы биометрической аутентификации для обеспечения точного и безопасного отслеживания времени. Биометрические идентификаторы[5], такие как отпечатки пальцев, распознавание лиц или сканирование сетчатки глаза, добавляют дополнительный уровень проверки личности, исключая возможность мошенничества со временем.[4]

Мобильные приложения: в эпоху растущей мобильности СУРВ включает в себя мобильные приложения, которые позволяют сотрудникам отслеживать свое время независимо от их физического местонахождения. Мобильные приложения обеспечивают удаленный доступ к функциям учета рабочего времени, обеспечивая гибкую рабочую среду и отвечая потребностям современной рабочей силы.

Облачные решения: облачная СУРВ обеспечивает масштабируемость, доступность и синхронизацию данных в режиме реального времени. При интеграции с СКУД облачные решения обеспечивают беспрепятственный обмен информацией и аналитическими данными между системами контроля доступа и учета рабочего времени.[7]

3.2. Управление посещаемостью и мониторинг производительности

Оптимизация управления посещаемостью: СУРВ при интеграции с СКУД упрощает управление посещаемостью за счет автоматизации процесса регистрации посещаемости сотрудников. СУРВ обеспечивает точное отслеживание данных о посещаемости в режиме реального времени. Эти данные затем легко интегрируются с СКУД, что способствует представлению о деятельности сотрудников и соблюдению политик контроля доступа.

Улучшение мониторинга производительности: СУРВ способствует мониторингу производительности, предоставляя информацию о том, как сотрудники распределяют свое рабочее время. Классифицируя задачи, отслеживая сроки реализации проекта, организации получают данные для оптимизации распределения ресурсов, улучшая управление проектами. Интеграция с СКУД гарантирует, что данные о производительности совпадают с данными контроля доступа, обеспечивая полное понимание вовлеченности сотрудников.[1]

3.3. Синергетическая интеграция с СКУД

Единые профили пользователей: интеграция между СУРВ и СКУД приводит к созданию унифицированных профилей пользователей и созданию централизованного хранилища данных о сотрудниках. Этот подход обеспечивает согласованность аутентификации пользователей, политик контроля доступа и действий, связанных со временем. Полная интеграция гарантирует, что любые изменения в ролях пользователей, разрешениях или уровнях доступа единообразно отражаются в обеих системах, что снижает административные издержки и повышает точность.

Политика скоординированного контроля доступа и учета рабочего времени: сплоченная интеграция СКУД и СУРВ позволяет организациям координировать политику контроля доступа и учета рабочего времени, при которой права доступа динамически корректируются на основе показателей, связанных со временем, что способствует как безопасности, так и эффективности. Например, определенные права доступа могут зависеть

от определенных критериев, связанных со временем, таких как регулярное посещение или выполнение назначенных задач.

Отчетность и аналитика: интеграция облегчает создание комплексных отчетов и аналитики. Эти данные позволяют организациям оценивать производительность сотрудников, выявлять тенденции и принимать обоснованные решения относительно распределения ресурсов, сроков реализации проекта и протоколов безопасности.

3.4. Соображения и преимущества

Соответствие требованиям и точность расчета заработной платы: интеграция СУРВ и СКУД обеспечивает соблюдение трудового законодательства путем предоставления точного и поддающегося проверке учета рабочего времени. Это не только защищает организацию от юридических проблем, но и повышает точность расчета заработной платы, поскольку данные, связанные со временем, легко интегрируются с профилями сотрудников и записями контроля доступа.

Расширение возможностей и вовлеченность сотрудников: СУРВ способствует расширению прав и возможностей сотрудников, предоставляя им возможность просмотра своих данных, связанных со временем. Сотрудники могут активно участвовать в управлении своим рабочим временем, задачами и производительностью. Это расширение прав и возможностей способствует развитию вовлеченности, что соответствует современным тенденциям на рабочем месте, которые ставят во главу угла благополучие и удовлетворенность сотрудников.

Вывод

В быстро развивающемся ландшафте современных предприятий интеграция надежных корпоративных систем контроля и управления доступом (СКУД) и систем учета рабочего времени (СУРВ) становится стратегическим императивом. Это исследование позволило углубиться в сложные области применения, состав, требования и синергетическую интеграцию этих систем, подчеркнув их симбиотическую роль в укреплении безопасности и оптимизации операционной эффективности.

Взаимосвязанное значение СКУД и СУРВ: СКУД с ее приложениями для контроля доступа, управления идентификацией и авторизации обеспечивает базовый уровень защиты цифровых активов. В то же время интеграция СУРВ привносит динамичный элемент за счет оптимизации управления посещаемостью, улучшения мониторинга производительности и развития культуры подотчетности. Объединение систем приводит к созданию единой цифровой экосистемы, в которой органично сочетаются контроль доступа, учет рабочего времени и управление пользователями.

Повышение безопасности и операционной эффективности: меры контроля доступа подкреплены методами биометрической аутентификации СУРВ, которые предотвращают мошенничество и обеспечивают точность личности пользователя. Операционная эффективность оптимизируется за счет оптимизации управления посещаемостью и аналитики, полученной с помощью СУРВ. Организации получают представление о вовлеченности сотрудников, сроках реализации проекта и распределении ресурсов, что позволяет принимать обоснованные решения.

Расширение прав и возможностей пользователей и соблюдение требований: интегрированный подход расширяет возможности сотрудников, предоставляя им видимость и

контроль над их данными. Преимущества соблюдения требований, получаемые за счет точного учета рабочего времени и контроля доступа, способствуют укреплению правовой и нормативной базы, снижая риски, связанные с несоблюдением требований.

Будущие соображения: поскольку технологии продолжают развиваться, будущие соображения по интеграции СКУД и СУРВ могут включать в себя интеграцию искусственного интеллекта для прогнозной аналитики, усовершенствованные методы биометрической аутентификации и исследование технологии блокчейн для обеспечения большей целостности данных. Постоянное развитие технологий кибербезопасности и управления персоналом, несомненно, будет определять траекторию развития этих систем, требуя от организаций сохранять бдительность и адаптивность.

Список литературы

1. Шварц М. и Мачулак М. (2018). «Защита периметра: развертывание управления идентификацией и доступом с помощью бесплатного программного обеспечения с открытым исходным кодом».
2. Рави С. Сандху. (2008). «Управление доступом на основе ролей».
3. Ангелос Д. Керомит, Джонатан М. Смит (2007). «Требования к масштабируемым архитектурам контроля доступа и управления безопасностью».
4. Крахмалев А. Нормативная база для СКУД // Алгоритм безопасности. № 4. (2008).
5. Лиакат Али, Джон В. Монако, Чарльз К. Тапперт, Мэйкан Цю (2016). «Биометрические системы для аутентификации пользовалей».
6. Международная организация по стандартизации. (ISO/IEC 27001:2022). «Системы менеджмента информационной безопасности – Требования».
7. Цзяньтин Нин, Синьи Хуан, Вилли Сусило, Кайтай Лян, Симэн Лю, Инхуэй Чжан (2020). «Двойной контроль доступа для облачного хранения данных и их совместного использования».
8. РД 78.36.003-2002 Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств / НИЦ «Охрана» ГУВО МВД России; сост. Н.Н. Котов, Л.И. Савчук, Е.П. Тюрин. (2002).
9. Бадиков А.В., Бондарев П.В. Системы контроля и управления доступом. Лабораторный практикум. М.: НИЯУ МИФИ. (2010).
10. Рекомендации Р 78.36.005-99 / НИЦ «Охрана» ГУВО МВД России; сост. Н.Н. Котов, Л.И. Савчук, Е.П. Тюрин, В.Г. Синилов. (1998).

References

1. Schwartz M. and Machulak M. (2018). "Perimeter Protection: Deploying identity and access management using free and open source software."
2. Ravi S. Sandhu. (2008). "Role-based access control".
3. Angelos D. Keromit, Jonathan M. Smith (2007). "Requirements for scalable access control and security management architectures."
4. Krakhmalev A. Regulatory framework for ACS // Security algorithm. № 4. (2008).
5. Liaqat Ali, John V. Monaco, Charles K. Tappert, Meikan Qiu (2016). "Biometric systems for user authentication".

6. International Organization for Standardization. (ISO/IEC 27001:2022). "Information Security Management Systems – Requirements".
7. Jiantin Ning, Xinyi Huang, Willy Susilo, Kaitai Liang, Ximeng Liu, Yinhui Zhang (2020). "Dual access control for cloud storage and data sharing."
8. RD 78.36.003-2002 Engineering and technical fortification. Technical means of protection. Requirements and design standards for the protection of objects from criminal encroachments / SIC "Protection" GUVO of the Ministry of Internal Affairs of Russia; comp. N.N. Kotov, L.I. Savchuk, E.P. Tyurin. (2002).
9. Badikov A.V., Bondarev P.V. Access control and management systems. Laboratory workshop. Moscow: NRU MEPhI. (2010).
10. Recommendations P 78.36.005-99 / SIC "Protection" GUVO of the Ministry of Internal Affairs of Russia; comp. N.N. Kotov, L.I. Savchuk, E.P. Tyurin, V.G. Sinilov. (1998).

Чаплыгина В.А., Котовенко В.В., Терехова А.Е. Искусственный интеллект и BI системы: интеграция, автоматизация и перспективы развития // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 6(44) с. 88–94

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.8

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И BI СИСТЕМЫ: ИНТЕГРАЦИЯ, АВТОМАТИЗАЦИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

[1]Чаплыгина В.А., [2]Котовенко В.В., [3]Терехова А.Е.
ФГБОУ ВО "ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ УПРАВЛЕНИЯ", Москва, Россия, (109542, город Москва, Рязанский пр-кт, д.99), e-mail: [1]chaplygina.lera.2018@mail.ru, [2]kotolera00@mail.ru, [3]anterehova@guu.ru

Интеграция технологий искусственного интеллекта (ИИ) в системы бизнес-аналитики (BI) открывает новые возможности для автоматизации задач, углубленного анализа данных и повышения эффективности принятия решений. В статье исследуется роль ИИ в совершенствовании BI-систем российских компаний.

Анализируется текущее состояние внедрения ИИ в отечественные BI-решения, основные области применения, достоинства и ограничения. Рассматриваются перспективы автоматизации процессов за счет машинного обучения, интеллектуальной аналитики, визуализации на основе ИИ.

Выявляются ключевые технические, организационные и правовые барьеры при интеграции передовых ИИ-технологий в BI. Анализируются тренды и инновации в сфере ИИ для BI, включая предиктивную и предписывающую аналитику, конверсационные интерфейсы.

На основе исследования сформулированы рекомендации по разработке комплексной стратегии успешного внедрения ИИ в BI российских организаций с акцентом на выбор технологий, управление изменениями и обучение персонала. Подчеркивается необходимость консолидации усилий бизнеса, ИТ и науки для эффективной реализации потенциала ИИ.

Ключевые слова: Искусственный интеллект, бизнес-аналитика, системы BI, интеграция ИИ, машинное обучение, автоматизация процессов.

ARTIFICIAL INTELLIGENCE AND BI SYSTEMS: INTEGRATION, AUTOMATION AND DEVELOPMENT PROSPECTS

[1]Chaplygina V.A., [2]Kotovenko V.V., [3]Terekhova A.E.
STATE UNIVERSITY OF MANAGEMENT, Moscow, Russia, (109542, Moscow, Ryazanskiy prospekt, 99), e-mail: [1]chaplygina.lera.2018@mail.ru, [2]kotolera00@mail.ru, [3]anterehova@guu.ru

The integration of artificial intelligence (AI) technologies into business intelligence (BI) systems opens up new opportunities for automating tasks, in-depth data analysis and improving decision-making efficiency. The article examines the role of AI in improving the BI systems of Russian companies.

The current state of AI implementation in domestic BI solutions, the main areas of application, advantages and limitations are analyzed. The prospects of automating processes through machine learning, intelligent analytics, and AI-based visualization are considered.

The key technical, organizational and legal barriers to integrating advanced AI technologies into BI are identified. Trends and innovations in the field of AI for BI are analyzed, including predictive and prescriptive analytics, conversational interfaces.

Based on the research, recommendations are formulated for the development of a comprehensive strategy for the successful implementation of AI in the BI of Russian organizations with an emphasis on technology selection, change management and staff training. The need to consolidate the efforts of business, IT and science to effectively realize the potential of AI is emphasized.

Keywords: Artificial intelligence, business analytics, BI systems, AI integration, machine learning, process automation.

Системы бизнес-аналитики (BI) играют ключевую роль в современном российском бизнесе, обеспечивая компании инструментами для всестороннего анализа данных и принятия обоснованных решений [1]. BI системы позволяют извлекать ценные знания из накопленной информации, выявлять бизнес-тренды, оптимизировать процессы и стратегически управлять ресурсами.

Искусственный интеллект (ИИ) с его способностями к машинному обучению, обработке естественного языка и распознаванию сложных моделей в данных открывает новые возможности для усовершенствования BI решений [2]. Интеграция передовых технологий ИИ позволяет автоматизировать многие задачи, повысить точность аналитики и упростить взаимодействие пользователей с системами.

Необходимость внедрения ИИ в российские BI системы продиктована растущими требованиями к эффективности бизнес-анализа в условиях больших объёмов разнородных данных и возрастающей конкуренции [3]. Способность ИИ дополнить человеческий интеллект открывает новые горизонты для извлечения знаний и превращения их в конкурентные преимущества.

На российском рынке наблюдается стремительный рост применения технологий ИИ в системах бизнес-аналитики. Основные области использования включают:

- Интеллектуальную обработку структурированных и неструктурированных данных с помощью машинного обучения.
- Предиктивную аналитику на базе алгоритмов прогнозирования для предсказания бизнес-трендов.
- Автоматическую генерацию аналитических отчётов и дашбордов с использованием обработки естественного языка [4].

Лидирующие российские ИТ-компании активно внедряют ИИ в свои продуктовые линейки BI-решений. Например, Яндекс интегрировал технологии машинного обучения в Yandex DataLens, а Россети применяют компоненты ИИ для анализа энергосетей в своей платформе Ситуационно-аналитический центр [5].

Крупнейшие заказчики BI, такие как Сбербанк, Газпром нефть, РЖД, активно используют собственные ИИ-системы для интеллектуального анализа больших данных, оптимизации процессов и повышения эффективности [6]. Достоинствами текущих подходов является автоматизация рутинных задач, повышение скорости и качества аналитики. Однако сохраняются ограничения по сложности задач, масштабируемости, требованиям к данным и ресурсам.

Таблица 1 – Примеры успешного внедрения ИИ в BI-системы российскими компаниями

Компания	Область применения ИИ в BI
Сбербанк	Выявление мошеннических операций, анализ поведения клиентов
Яндекс	Автоматическая генерация отчетов, предиктивная аналитика
Газпром нефть	Интерпретация сейсмических данных, геологическое моделирование
X5 Retail Group	Компьютерное зрение для анализа видеоданных из магазинов
РЖД	Оптимизация логистики, предиктивное обслуживание техники
КАМАЗ	Прогнозная аналитика производственных затрат

Применение технологий искусственного интеллекта позволяет автоматизировать множество аналитических процессов в BI системах:

- Алгоритмы машинного обучения способны самостоятельно выполнять задачи ETL (извлечение, преобразование и загрузка данных) из разнородных источников [7].
- Методы кластеризации и распознавания образцов повышают качество бизнес-аналитики за счёт выявления скрытых паттернов в данных [7].
- Интеллектуальные системы могут автоматически генерировать отчёты и визуализации, адаптируя их под конкретные пользовательские потребности [7].

Рисунок 1 – Распространенность ИИ по областям применения

Широкое внедрение технологий ИИ, особенно глубокого обучения, раскрывает новые горизонты для бизнеса в сфере предиктивной и предписывающей аналитики. Интеллектуальная обработка больших массивов разнородных данных позволяет строить высокоточные прогнозные модели и формировать рекомендации по оптимальным решениям.

Несмотря на колоссальный потенциал ИИ для BI, российские компании сталкиваются с рядом технических, организационных и правовых вызовов:

- сложности интеграции разнородных ИИ-компонентов с существующими BI-системами и инфраструктурой [3].
- проблемы производительности, масштабируемости и высокие аппаратные требования для работы ИИ-решений с большими данными.
- нехватка квалифицированных кадров и экспертизы в сфере машинного обучения и разработки ИИ [5].
- организационная культура, инертность и сопротивление трансформационным изменениям.
- необходимость обработки персональных данных и соблюдения требований законодательства о защите данных [1].

Для эффективного внедрения ИИ-технологий требуется комплексный подход, консолидация ресурсов и тесная кооперация ИТ-компаний, ВУЗов и предприятий реального сектора.

Передовые достижения в сфере ИИ формируют новые тренды и инновации для дальнейшего развития и повышения эффективности BI-систем [4]:

- рост применения обучения без учителя для автоматического извлечения знаний из больших массивов данных.
- более широкое распространение гибридных ИИ-систем на базе нейросетей и символьных методов.
- усовершенствование предиктивной аналитики с использованием глубоких нейросетей и ансамблей моделей.
- развитие предписывающей аналитики для автоматизации поддержки принятия управленческих решений.
- внедрение конверсационных интерфейсов с возможностью поддержки естественно-языкового диалога с ИИ.
- рост спроса на объяснимые системы ИИ, обеспечивающие необходимую транспарентность моделей.

Рисунок 2 – Цикл внедрения ИИ в организации

По мере дальнейшей интеграции передовых ИИ-технологий в BI, принцип "аналитика везде" станет стандартом для организаций, стремящихся к повышению конкурентоспособности за счет данных.

Для успешной интеграции ИИ в BI организациям необходимо разработать комплексную стратегию и учесть следующие ключевые аспекты:

- оценка существующего состояния - инфраструктура, данные, человеческие ресурсы, цели бизнеса.
- выбор приоритетных областей и кейсов применения ИИ с учетом их ценности и достижимости.
- выбор зрелых и стабильных технологий ИИ от надежных российских и зарубежных вендоров с акцентом на интероперабельность [5].
- разработка детализированной дорожной карты поэтапного внедрения ИИ-решений.
- создание центров компетенций по ИИ, обучение ключевых ИТ и бизнес-специалистов.
- выстраивание эффективной системы управления изменениями для внедрения новых процессов.
- разработка KPI для отслеживания эффективности внедренных ИИ-систем в масштабе предприятия.

Тесное взаимодействие между ИТ и бизнес-подразделениями на всех этапах внедрения является залогом успеха [2].

Интеграция передовых технологий искусственного интеллекта в российские системы бизнес-аналитики — это не просто тренд, а веление времени. ИИ способен автоматизировать многие трудоемкие процессы, открыть новые возможности для предиктивной аналитики, упростить взаимодействие с аналитическими системами и извлечение знаний.

Несмотря на существующие технические, организационные и правовые барьеры, российские компании все активнее внедряют подходы на основе ИИ в свои BI-решения. Тренды указывают на ускорение данной тенденции благодаря прогрессу в машинном обучении, обработке естественного языка и других областях ИИ [6].

Для обеспечения конкурентоспособности в долгосрочной перспективе компаниям необходима проработанная стратегия интеграции ИИ. Достижение успеха требует консолидации усилий, квалифицированных кадров, системного подхода и постоянного обучения. Симбиоз передовых ИИ-технологий и человеческого интеллекта в BI позволит отечественному бизнесу максимально реализовать потенциал, заложенный в данных.

Список литературы

1. Волперт, Э. (2022). Потенциал искусственного интеллекта в области бизнес-аналитики. VC.ru. URL: https://vc.ru/u/2830724-andrew-volpert/1009007-potencial-iskusstvennogo-intellekta-v-oblasti-biznes-analitiki (дата обращения: 27.02.2024)
2. Тузова, Р. (2021). Искусственный интеллект и аналитика: создаем умную организацию. IT-World. URL: https://www.it-world.ru/cionews/business/195056.html (дата обращения: 28.02.2024)
3. Сидоров, М. (2020). BI-системы и искусственный интеллект: автоматизация процессов. WebSoft. URL: https://www.websoftshop.ru/information/articles/automation/bi_and_ai/ (дата обращения: 04.03.2024)
4. Корус Консалтинг (2022). BI-системы: технологические тренды и перспективы развития. URL: https://data.korusconsulting.ru/press-center/blog/bi-sistemy-tekhnologicheskie-trendy-i-perspektivy-razvitiya/ (дата обращения: 07.03.2024)
5. "Обзор российских BI-систем" (2023). Отзыв Маркетинг. URL: https://otzyvmarketing.ru/articles/rossijskie-bi-sistemy/ (дата обращения: 11.03.2024)
6. Чумак, Д. (2023). AI/ML в облачной аналитической платформе Beeline Cloud. Хабр. URL: https://habr.com/ru/companies/beeline_cloud/articles/734952/ (дата обращения: 14.03.2024)
7. "Каталог BI систем" (2023). TAdviser. URL: https://www.tadviser.ru/index.php/ (дата обращения: 14.03.2024)

References

1. Volpert, E. (2022). Potential of Artificial Intelligence in Business Analytics. VC.ru. URL: https://vc.ru/u/2830724-andrew-volpert/1009007-potencial-iskusstvennogo-intellekta-v-oblasti-biznes-analitiki (accessed: 27.02.2024)
2. Tuzova, R. (2021). Artificial Intelligence and Analytics: Building a Smart Organization. IT-World. URL: https://www.it-world.ru/cionews/business/195056.html (accessed: 28.02.2024)

3. Sidorov, M. (2020). BI Systems and Artificial Intelligence: Process Automation. WebSoft. URL: https://www.websoftshop.ru/information/articles/automation/bi_and_ai/ (accessed: 04.03.2024)
4. Korus Consulting (2022). BI Systems: Technological Trends and Development Perspectives. URL: https://data.korusconsulting.ru/press-center/blog/bi-sistemy-tekhnologicheskie-trendy-i-perspektivy-razvitiya/ (accessed: 07.03.2024)
5. "Overview of Russian BI Systems" (2023). Otzyv Marketing. URL: https://otzyvmarketing.ru/articles/rossijskie-bi-sistemy/ (accessed: 11.03.2024)
6. Chumak, D. (2023). AI/ML in Beeline Cloud's Cloud Analytics Platform. Habr. URL: https://habr.com/ru/companies/beeline_cloud/articles/734952/ (accessed: 14.03.2024)
7. "BI Systems Catalog" (2023). TAdviser. URL: https://www.tadviser.ru/index.php/ (accessed: 14.03.2024)

Нижлукченко И.Д. Безопасность в облаке: как защитить свои данные в облачных сервисах. советы по выбору облачных провайдеров и настройке облачных сервисов для обеспечения безопасности данных // Международный журнал информационных технологий и энергоэффективности.– 2024. –Т. 9 № 6(44) с. 95–100

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

БЕЗОПАСНОСТЬ В ОБЛАКЕ: КАК ЗАЩИТИТЬ СВОИ ДАННЫЕ В ОБЛАЧНЫХ СЕРВИСАХ. СОВЕТЫ ПО ВЫБОРУ ОБЛАЧНЫХ ПРОВАЙДЕРОВ И НАСТРОЙКЕ ОБЛАЧНЫХ СЕРВИСОВ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ

Нижлукченко И.Д.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: nizhluchenk@gmail.com

В статье "Безопасность в облаке: как защитить свои данные в облачных сервисах" освещаются ключевые аспекты и стратегии обеспечения безопасности цифровой информации в условиях широкого использования облачных технологий. В условиях быстрого роста объемов генерируемых данных и их ценности, вопросы конфиденциальности, целостности и доступности информации становятся всё более актуальными. Статья представляет собой комплексный обзор методов защиты данных, начиная с выбора надежных облачных провайдеров, настройки облачных сервисов, до проведения регулярных аудитов и мониторинга системы безопасности. Особое внимание уделяется не только техническим, но и организационным аспектам защиты данных, подчеркивая важность комплексного подхода, который включает в себя обучение персонала, разработку и внедрение политик безопасности. Статья подчеркивает, что в современных условиях обеспечение безопасности данных в облаке является непрерывным процессом, требующим от организаций гибкости, постоянного обучения и адаптации к изменяющемуся ландшафту угроз.

Ключевые слова: Безопасность данных, облачные сервисы, облачные провайдеры, шифрование данных, аудит безопасности, мониторинг безопасности, настройка облачных сервисов, многофакторная аутентификация, резервное копирование, непрерывность бизнеса, кибербезопасность, защита конфиденциальности, целостность данных, доступность данных, управление угрозами, стандарты безопасности данных, GDPR, HIPAA, обучение персонала, культура безопасности.

SECURITY IN THE CLOUD: HOW TO PROTECT YOUR DATA IN CLOUD SERVICES. TIPS ON CHOOSING CLOUD PROVIDERS AND CONFIGURING CLOUD SERVICES TO ENSURE DATA SECURITY

Nizhlukchenko I.D.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: nizhluchenk@gmail.com

The article "Security in the cloud: how to protect your data in cloud services" highlights key aspects and strategies for ensuring the security of digital information in the context of widespread use of cloud technologies. With the rapid growth of the volume of data generated and its value, issues of confidentiality, integrity and accessibility of information are becoming increasingly relevant. The article provides a comprehensive overview of data protection methods, from choosing reliable cloud providers, configuring cloud services, to conducting regular audits and

monitoring the security system. Special attention is paid not only to the technical, but also to the organizational aspects of data protection, emphasizing the importance of an integrated approach that includes staff training, development and implementation of security policies. The article emphasizes that in modern conditions, ensuring data security in the cloud is an ongoing process that requires organizations to be flexible, constantly learning and adapting to the changing threat landscape.

Keywords: Data security, cloud services, cloud providers, data encryption, security audit, security monitoring, configuring cloud services, multi-factor authentication, backup, business continuity, cybersecurity, privacy protection, data integrity, data availability, threat management, data security standards, GDPR, HIPAA, staff training, culture security.

В эпоху цифровизации, облако стало ключевым элементом в хранении и обработке данных для организаций и индивидуальных пользователей. Однако с ростом его популярности возрастает и количество угроз безопасности данных. Поэтому понимание методов защиты информации в облаке и правильный выбор облачных провайдеров становится критически важным для обеспечения конфиденциальности, целостности и доступности данных.

Защита данных в облаке представляет собой многоаспектный процесс, основанный на глубоком понимании как технологических, так и человеческих факторов, способных повлиять на безопасность информации. В рамках комплексного подхода к безопасности данных ключевым является осознание того, что угрозы могут исходить как извне, так и изнутри организации, а также понимание того, как технические и организационные меры могут работать вместе для минимизации рисков.

На начальном этапе аудит существующих систем безопасности позволяет выявить слабые места и уязвимости в текущей архитектуре безопасности. Это исследование охватывает как физические, так и цифровые аспекты защиты данных, включая анализ методов аутентификации, шифрования, а также процедур восстановления после сбоев. Основываясь на результатах аудита, разрабатывается стратегия безопасности, предусматривающая внедрение современных технологий защиты данных и обновление устаревших систем.[1]

Следующим шагом является определение критериев выбора облачного провайдера, что включает в себя анализ его политики безопасности, возможностей по шифрованию данных и предложений по резервному копированию. Ключевым моментом здесь является выбор провайдера, способного обеспечить не только высокий уровень защиты данных, но и соответствие международным стандартам и нормативным требованиям в области защиты данных.

Организационные меры включают в себя разработку политик и процедур, регулирующих доступ к данным, их использование и распределение. Важно обучать сотрудников основам кибергигиены, правилам работы с чувствительной информацией и способам распознавания фишинговых атак. Также критически важным является введение политики регулярного обновления программного обеспечения и использования современных антивирусных решений для защиты от вредоносного программного обеспечения и других угроз.

Интеграция технических и организационных мер требует не только первоначальных инвестиций в инфраструктуру безопасности, но и постоянного мониторинга ситуации в области кибербезопасности, адаптации к новым угрозам и уязвимостям. Таким образом, комплексный подход к безопасности данных в облаке предполагает непрерывное взаимодействие между технологиями, процессами и людьми, направленное на защиту самого ценного актива любой организации — ее данных.

Выбор облачного провайдера является одним из наиболее значимых решений, влияющих на безопасность данных. Этот процесс начинается с тщательного анализа потребностей организации в области хранения, обработки и управления данными. Важно оценить, какие виды данных будут храниться в облаке, и какие требования к безопасности эти данные предъявляют.[4] Это помогает определить, какие функции безопасности должен предлагать провайдер, чтобы соответствовать как операционным, так и нормативным требованиям.

Ключевым аспектом является изучение политик безопасности и практик облачного провайдера, включая методы шифрования, которые он использует для защиты данных в покое и во время передачи. Шифрование становится критически важной защитой, поскольку оно обеспечивает, что даже в случае несанкционированного доступа данные останутся недоступными для злоумышленников.

Далее, оценка механизмов аутентификации и контроля доступа, предлагаемых провайдером, позволяет убедиться, что только авторизованные пользователи смогут получить доступ к данным. Это включает в себя поддержку многофакторной аутентификации, ролевого доступа и других современных методов управления идентификацией и доступом.

Важно также учитывать политику и механизмы резервного копирования и восстановления данных, предлагаемые провайдером. В случае кибератак, технических сбоев или других чрезвычайных ситуаций, возможность быстро восстановить данные является ключевым аспектом поддержания непрерывности бизнеса.

Помимо технических аспектов, в процессе выбора провайдера важно учитывать его репутацию, опыт работы на рынке и отзывы других клиентов. Не менее важным является и его способность соответствовать местным и международным нормативным требованиям в области защиты данных, таким как GDPR или HIPAA, что особенно актуально для организаций, работающих в регулируемых отраслях.

В итоге, выбор облачного провайдера должен основываться на глубоком понимании как технических возможностей провайдера в области обеспечения безопасности данных, так и его способности соответствовать требованиям бизнеса и законодательства. Это стратегическое решение требует комплексного подхода и должно включать в себя как тщательную оценку текущих и будущих потребностей в облачных услугах, так и глубокий анализ предлагаемых провайдером решений по обеспечению безопасности.

Настройка облачных сервисов для обеспечения безопасности данных требует внимательного подхода и глубокого понимания как функционала облачных платформ, так и потенциальных угроз. Этот процесс начинается с анализа предоставляемых облачной платформой инструментов и возможностей по управлению доступом, шифрованию, аудиту и мониторингу. Важно настроить эти инструменты таким образом, чтобы максимально усилить защиту данных, при этом сохраняя баланс между безопасностью и удобством использования для конечных пользователей.

Применение принципа наименьших привилегий при настройке учетных записей пользователей является фундаментальным аспектом защиты данных в облаке. Это означает предоставление пользователям таких прав доступа, которые строго соответствуют их ролям и задачам, минимизируя тем самым возможность несанкционированного доступа к чувствительной информации. В дополнение к этому, регулярное обновление паролей и

использование многофакторной аутентификации значительно увеличивают уровень защиты учетных записей от взлома.

Шифрование данных, как в состоянии покоя, так и в процессе их передачи, становится неотъемлемой частью стратегии безопасности. Настройка шифрования должна проводиться с учетом специфики данных и требований к их защите. Облачные платформы обычно предлагают различные опции шифрования, позволяя выбрать наиболее подходящие в зависимости от уровня требуемой безопасности и производительности.

Кроме того, важным аспектом настройки является настройка процессов резервного копирования и восстановления данных. Это не только способ защиты от потери данных в случае технических сбоев или кибератак, но и ключевой элемент стратегии обеспечения непрерывности бизнеса. Настройка резервного копирования должна включать определение частоты создания резервных копий, а также выбор надежных и безопасных мест их хранения.

Настройка систем мониторинга и аудита играет важную роль в своевременном выявлении и реагировании на инциденты безопасности.[2] Эти системы должны быть сконфигурированы таким образом, чтобы обеспечить непрерывный анализ активности в облачной инфраструктуре, выявляя подозрительные действия и аномалии, которые могут указывать на попытки несанкционированного доступа или другие угрозы безопасности.

В целом, настройка облачных сервисов для обеспечения безопасности данных - это процесс, требующий не только технических знаний, но и понимания текущего ландшафта угроз и лучших практик в области кибербезопасности.

В контексте обеспечения безопасности данных в облаке, регулярный аудит и мониторинг становятся неотъемлемой частью стратегии защиты. Эти процессы позволяют не только выявлять и устранять уязвимости в системе безопасности, но и адаптироваться к постоянно меняющемуся ландшафту угроз.

Регулярный аудит системы безопасности облачных сервисов предполагает всестороннюю проверку всех аспектов защиты данных, включая анализ эффективности применяемых методов шифрования, политик доступа, механизмов аутентификации и инструментов мониторинга. В рамках аудита осуществляется также проверка соответствия действующим стандартам и регуляторным требованиям в области защиты данных. Этот процесс позволяет идентифицировать потенциальные уязвимости и разработать план их устранения, повышая тем самым общий уровень безопасности облачной инфраструктуры.

Мониторинг активности в облачных сервисах является постоянным процессом, который позволяет в реальном времени отслеживать события безопасности, анализировать трафик данных и выявлять подозрительные действия, которые могут указывать на попытки несанкционированного доступа, вредоносные атаки или внутренние угрозы. Современные системы мониторинга обладают возможностью автоматического распознавания аномалий в поведении пользователей и приложений, что позволяет своевременно реагировать на потенциальные угрозы и предотвращать инциденты безопасности.

Ключевым моментом является то, что регулярный аудит и мониторинг не являются разовыми мероприятиями, а представляют собой непрерывный процесс. Это требует от организаций не только наличия квалифицированных специалистов в области кибербезопасности, но и использование передовых инструментов и технологий для анализа и управления безопасностью.[3] Регулярное обновление политик безопасности, а также

адаптация к новым угрозам и изменениям в регуляторной среде, позволяет поддерживать высокий уровень защиты данных в облаке.

Таким образом, регулярный аудит и мониторинг служат важным звеном в цепочке обеспечения безопасности данных в облаке, позволяя организациям не только обнаруживать и устранять уязвимости, но и прогнозировать потенциальные угрозы, обеспечивая тем самым надежную защиту своих цифровых активов.

В заключение, безопасность данных в облачных сервисах остается важнейшей задачей для организаций всех размеров и сфер деятельности. В современном мире, где цифровизация проникает во все аспекты нашей жизни, и где объемы данных растут с каждым днем, вопросы защиты информации становятся критически важными.[5] Принятие комплексного подхода к безопасности, который включает в себя тщательный выбор облачных провайдеров, настройку облачных сервисов, регулярный аудит и мониторинг, позволяет создать надежную систему защиты данных. Это не только обеспечивает сохранность и конфиденциальность важной информации, но и способствует поддержанию доверия клиентов и партнеров, что является неотъемлемым аспектом успешного ведения бизнеса.

С другой стороны, необходимо осознавать, что процесс обеспечения безопасности данных в облаке – это непрерывная активность, требующая постоянного внимания, обучения и адаптации к изменяющемуся ландшафту угроз. В этом контексте важна не только технологическая составляющая, но и человеческий фактор, включая обучение сотрудников и формирование культуры безопасности внутри организации. В конечном итоге, безопасность облачных данных становится совместной ответственностью провайдеров облачных услуг и их клиентов, требующей скоординированных усилий, передовых технологий и стратегического планирования для обеспечения защиты цифровых активов в долгосрочной перспективе.

Список литературы

1. Гельфанд А. М. и др. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе//Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2018. – №. 8. – С. 91-97.
2. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO//Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
3. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения–Информационные технологии и телекоммуникации, 2021 //Т. – 2021. – Т. 9. –С. 1-2
4. Катасонов А. И., Штеренберг С. И., Цветков А. Ю. Оценка стойкости механизма, реализующего Мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства gnu linux//Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 2. – С. 50-56.
5. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411

References

1. Gelfand A.M. et al. Development of a model for the distribution of self-modifying code in a protected information system //Modern science: actual problems of theory and practice. Series: Natural and Technical Sciences. – 2018. – No. 8. – pp. 91-97.
2. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: current aspects of the "GNII" National Development". July 2018. – 2018. – pp. 31-35.
3. Shterenberg S. I., Moskalchuk A. I., Krasov A.V. Development of security scenarios for creating vulnerable virtual machines and studying penetration testing methods–Information technologies and Telecommunications, 2021 //Vol. – 2021. – vol. 9. –pp. 1-2
4. Katasonov A. I., Shterenberg S. I., Tsvetkov A. Yu. Assessment of the stability of the mechanism implementing... The mandatory essential role model of access rights differentiation in gnu linux operating systems //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – No. 2. – pp. 50-56.
5. Budarny G. S. et al. Types of security breaches and typical attacks on the operating system //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 406-411.

Петров А.С. Комбинированный метод структурной оптимизации локальной вычислительной сети // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 6(44) с. 101–112

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.7

КОМБИНИРОВАННЫЙ МЕТОД СТРУКТУРНОЙ ОПТИМИЗАЦИИ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Петров А.С.

ФГБОУ ВО " "МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Н.Э. БАУМАНА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)", Москва, Россия, (105005, город Москва, 2-Я Бауманская ул, д. 5 стр. 1), e-mail: bauman@bmstu.ru

В статье рассматривается комбинированный генетический алгоритм применительно к структурной оптимизации сегмента локальной сети посредством максимизации пропускной способности и достоверности передаваемой информации (минимизации BER) при минимизации количества узлов сети с использованием различных методов многокритериальной оптимизации по Парето. Представлены результаты сравнения методов NSGA-II, VEGA, FFGA (MOGA), NPGA И SPEA-II при одних и тех же параметрах сети.

Ключевые слова: Многокритериальная оптимизация, комбинированный метод, генетический алгоритм с адаптивной мутацией, локальная сеть, NSGA-II, VEGA, FFGA (MOGA), NPGA, SPEA-II.

COMBINED METHOD OF STRUCTURAL OPTIMIZATION OF A LOCAL COMPUTER NETWORK

Petrov A.S.

BAUMAN MOSCOW STATE TECHNICAL UNIVERSITY (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (105005, Moscow, 2nd Baumanskaya ul, 5 bld. 1), e-mail: bauman@bmstu.ru

The article discusses a combined genetic algorithm in relation to the structural optimization of a local network segment by maximizing the throughput and reliability of transmitted information (minimizing BER) while minimizing the number of network nodes using various methods of multicriteria Pareto optimization. The results of comparison of NSGA-II, VEGA, FFGA (MOGA), NPGA AND SPEA-II methods with the same network parameters are presented

Keywords: Multicriteria optimization, combined method, genetic algorithm with adaptive mutation, local network, NSGA-II, VEGA, FFGA (MOGA), NPGA, SPEA-II.

Введение

В настоящее время компьютерные сети применяются в множестве областей человеческой жизни: научной, технической, социальной, медицинской, коммерческой и т.д. [1]. Исходя из этого, вычислительные сети являются одним из наиболее перспективных направлений развития информационных технологий. Структурная оптимизация компьютерной сети, в свою очередь, позволит снизить затраты на ее управление, а также улучшить производительность и надежность. Оптимизацию столь сложной системы необходимо производить одновременно по нескольким критериям, поэтому традиционные методы оптимизации зачастую не справляются с этой задачей. Для нахождения Парето-оптимального

решения, удовлетворяющего сразу нескольким критериям, хорошо подходят так называемые эволюционные алгоритмы (ЭА). Одним из наиболее популярных ЭА, применяемых для решения сложных задач комбинаторики и оптимизации, является генетический алгоритм (ГА), впервые описанный Дж. Голландом [2]. Суть данного алгоритма состоит в том, что оптимизация основана на принципах естественного отбора, в которых из начальной популяции выделяют наиболее подходящих по функции приспособленности потомков. Поиск решений происходит с использованием таких генетических операторов, как: скрещивание (кроссинговер), мутация и селекция.

Пусть есть n переменных $x_1, x_2, \dots, x_n$ и их k независимых целевых функций $f_1(x_1, x_2, \dots, x_n), f_2(x_1, x_2, \dots, x_n), \dots, f_k(x_1, x_2, \dots, x_n)$ [3]. Тогда задачу многокритериальной оптимизации в общем случае можно сформулировать следующим образом [4]:

$$y = f(x) = \big(f(x_1, x_2, \dots, x_n)\big) \to optimal, \begin{cases} g_i(x) \le 0, j = \overline{1, r}, \\ h_i(x) = 0, j = \overline{r+1, M}, \end{cases} \quad (1)$$

где x $= (x_1, x_2, \dots, x_n) \in X$ - вектор решений, y $= \big(f_1(x), f_2(x), \dots, f_k(x)\big) \in Y_f$ - вектор целевых функций. При этом X - пространство решений, Y_f - критериальное пространство (область значений критериев).

Стоит отметить, что приведенная постановка задачи не дает никаких указаний в случае, если невозможно добиться оптимальных значений для всех целевых функций одновременно. Также из данной формулировки многокритериальной оптимизации нельзя сделать вывод о том, как именно сравнивать различные полученные во время оптимизации результаты.

Существует несколько наиболее популярных методов решения этой проблемы [4-5].

- Метод линейной свертки.

$$F(x) = \sum_{i=1}^{k} w_i f_i(x), \quad (2)$$

где F(x) - общий критерий оптимизации, w_i - весовые коэффициенты, отражающие относительную "важность" каждого критерия, а $f_i(x)$ - критерии оптимизации.

- Принцип доминирования по Парето.

Согласно принципу доминирования по Парето параметр x1 *доминирует* над параметром x2, если он по всем критериям не хуже, чем x2, и хотя бы по одному --- лучше. В таком случае параметр x1 называется *доминирующим*, а x2 --- *доминируемым*. Если ни один из параметров x1, x2 не доминирует над другим, то они называются *недоминируемыми*. Множество Парето --- это множество, состоящее из недоминируемых объектов.

Формальное определение множества Парето в критериальном пространстве Y_f можно записать в следующем виде:

$$P(x) = x^* \in X \mid x \in X : y(x) \ge y(x^*), \quad (3)$$

для задачи максимизации.

$$P(x) = x^* \in X \mid x \in X : y(x) \le y(x^*), \quad (4)$$

для задачи минимизации.

Структурная оптимизация будет реализована с помощью методов, использующих принцип Парето-доминирования.

При наличии нескольких целевых функций в стандартном ГА используются различные методы многокритериальной оптимизации, направленные на модификацию этапов назначения пригодности и селекции. Наиболее популярные из них перечислены далее: NSGA-II (модифицированный Non-dominated Sorting Genetic Algorithm), VEGA (Vector Evaluated Genetic Algorithm), FFGA (MOGA, Fonseca and Fleming's Multiobjective Genetic Algorithm), NPGA (Niched Pareto Genetic Algorithm) и SPEA2 (модифицированный Strength Pareto Evolutionary Algorithm).

Критерии сравнения многокритериальных методов

В задаче структурной оптимизации сегмента локальной вычислительной сети при выборе многокритериального алгоритма необходимо учитывать следующие критерии (при одинаковых параметрах ГА и одинаковой конфигурации сети).

1. Средние значения функции приспособленности индивидов на каждом поколении в процессе работы алгоритма. Для каждого поколения k, $k = 1, 2, \ldots, K$.

$$AvgThroughput_k = \frac{1}{N_k}\sum_{i=1}^{N_k}\left(\frac{\sum_{j=1}^{M_{i,k}} C_{j,i,k}}{M_{i,k}}\right), \quad (5)$$

$$AvgBER_k = \frac{1}{N_k}\sum_{i=1}^{N_k}\left(\frac{\sum_{j=1}^{M_{i,k}} BER_{j,i,k}}{M_{i,k}}\right), \quad (6)$$

где:

- $\mathrm{AvgThroughput}_k$ - средняя пропускная способность индивидов в k-м поколении;
- $\mathrm{AvgBE}R_k$ - средняя надежность (BER) индивидов в k-м поколении;
- $\mathrm{AvgVertices}_k$ - среднее количество вершин индивидов в k-м поколении;
- K - суммарное количество поколений;
- N_k - количество индивидов в k-м поколении;
- $M_{i,k}$ - количество ребер i-го индивида в k-м поколении;
- $C_{i,j,k}$ - значение пропускной способности j-го ребра i-го индивида в k-м поколении;
- $V_{i,k}$ - количество вершин i-го индивида в k-м поколении.

2. Максимальные и минимальные значения функции приспособленности на каждом поколении в процессе работы алгоритма. Для каждого поколения k, $k = 1, 2, \ldots, K$.

$$maxThroughput_k = \max_{i=1}^{N_k}\left(\frac{\sum_{j=1}^{M_{i,k}} C_{j,i,k}}{M_{i,k}}\right), \quad (8)$$

$$minThroughput_k = \min_{i=1}^{N_k}\left(\frac{\sum_{j=1}^{M_{i,k}} C_{j,i,k}}{M_{i,k}}\right), \quad (9)$$

$$maxBER_k = \max_{i=1}^{N_k}\left(\frac{\sum_{j=1}^{M_{i,k}} BER_{j,i,k}}{M_{i,k}}\right), \quad (10)$$

$$minBER_k = \min_{i=1}^{N_k}\left(\frac{\sum_{j=1}^{M_{i,k}} BER_{j,i,k}}{M_{i,k}}\right), \quad (11)$$

$$maxVertices_k = \max(V_{1,k}, V_{2,k}, \dots, V_{N_k,k}), \quad (12)$$

$$minVertices_k = \min(V_{1,k}, V_{2,k}, \dots, V_{N_k,k}), \quad (13)$$

где:

- maxThroughput_k и minThroughput_k - максимальная и минимальная пропускные способности индивидов в k-м поколении соответственно;
- maxBER_k и minBER_k - максимальная и минимальная надежности (BER) индивидов в k-м поколении соответственно;
- maxVertices_k и minVertices_k - максимальное и минимальное количество вершин индивидов в k-м поколении соответственно;
- K - суммарное количество поколений;
- N_k - количество индивидов в k-м поколении;
- $M_{i,k}$ - количество ребер i-го индивида в k-м поколении.
- $C_{i,j,k}$ - значение пропускной способности j-го ребра i-го индивида в k-м поколении;
- $V_{i,k}$ - количество вершин i-го индивида в k-м поколении.

3. Номер поколения, на котором получено конечное решение.

$$k_{target} = \min\{ k \mid \exists i \in N_k : (C_{i,k} = C_{goal}) \wedge (BER_{i,k} = BER_{goal}) \wedge (V_{i,k} = V_{goal})\}, \quad (14)$$

где:

- k_{target} - номер поколения, на котором получено конечное решение;
- $C_{i,k}, BER_{i,k}, V_{i,k}$ - значения пропускной способности, надежности и количества вершин i-го индивида в k-м поколении соответственно;
- $C_{goal}, BER_{goal}, V_{goal}$ - значения пропускной способности, надежности и количества вершин конечного решения соответственно.

4. Качество полученного решения - значения функции приспособленности полученного в результате работы алгоритма решения.
5. Наличие застреваний в локальном оптимуме.
6. Способность поддержания разнообразия решений.

Выбор критерия 1 обусловлен следующими факторами:

- помогает отслеживать изменения популяции от поколения к поколению;
- позволяет оценить эффективность алгоритма в целом и его способность к улучшению решений;
- помогает идентифицировать моменты застревания в локальных оптимумах (минимальные изменения лучших и худших значений функции приспособленности индивидов в каждом поколении при постоянном среднем значении фитнесс-функции может указывать на то, что индивиды начинают сходиться к одному и тому же решению [6]).

С помощью критерия 2 можно оценить пространство поиска решений по конкретному критерию в каждом из поколений, а с помощью критерия 3 можно сравнить скорости сходимости алгоритмов. Критерии 4-6 помогают проанализировать, насколько корректно отрабатывают операторы кроссовера и мутации в процессе работы генетических алгоритмов.

Классический вероятностный генетический алгоритм

Сложность генетического алгоритма состоит в использовании множества необходимых параметров, неправильная настройка которых может повлиять на его эффективность. Поскольку подбор корректных значений параметров является нетривиальной задачей, было создано множество модификаций алгоритма, упрощающих настройку ГА. Одна из таких модификаций - вероятностный генетический алгоритм (ВГА).

ВГА - это традиционный ГА, сформулированный в терминах теории псевдобулевой оптимизации [7]. Модификация заключается в явном вычислении компонентов вектора вероятностей и замены оператора скрещивания на оператор случайного выбора в соответствии с построенным распределением. Такие изменения в работе ГА помогают упростить настройку параметра, отвечающего за вероятность кроссовера.

Работу базового ВГА можно описать следующими шагами.

1) Генерация случайным образом начальной популяции решений.
2) Выбор r наиболее пригодных индивидов текущей популяции (родителей). Вычисление вектора вероятностей по формуле 15.

$$\overline{P} = (p_1, \dots, p_n), p_j = P\{x_j = 1\} = \frac{1}{r}\sum_{i=1}^{r} x_j^i, j = \overline{1,n}, \tag{15}$$

где n - длина хромосомы, x_j^i - j-й бит i-го индивида.

3) Формирование популяции потомков в соответствии с распределением $\overline{P}$.
4) Формирование новой рабочей популяции из популяции родителей и потомков.
5) Применение мутации к новой популяции.
6) Повторение пунктов 2-6 до выполнения условий остановки.

Ниже приведены основные преимущества вероятностного генетического алгоритма по сравнению с стандартным ГА:

- многокритериальная оптимизация;
- меньшее число настраиваемых параметров;
- в общем случае является более надежным и эффективным по трудоемкости;
- множество вариаций многокритериальных методов.

Однако ВГА также имеет несколько недостатков:

- более сложные реализация и вычисления из-за использования вероятностных операторов и стохастического выбора родителей;
- возможность получения менее точных решений.

Вероятностный генетический алгоритм с адаптивной мутацией

Данный алгоритм является модификацией ВГА посредством автоматического расчета вероятности мутации на каждом шаге, вследствие чего у пользователя отсутствует необходимость настраивать этот оператор вручную [4].

Вероятность мутации рассчитывается по формуле 16.

$$P_m = \frac{S}{n}, S = \begin{cases} \frac{n}{2}, (X_k = 0) \cup \left(\frac{X_{k-1}}{2X_k} \geq \frac{n}{2}\right) \\ \left(\frac{X_{k-1}}{2X_k}\right), \text{ иначе,} \end{cases} \tag{16}$$

где n - длина хромосомы, X_{k-i} - разброс точек в пространстве решений на $(k-i)$-ом поколении, X_k - разброс точек в пространстве решений на k-ом поколении. Функция S определяет силу мутации.

Разброс точек в пространстве решений вычисляется по формуле 17.

$$X = \frac{1}{N}\sum_{n=1}^{\overline{N}} \frac{\Delta d^n}{M_n - m_n},$$

где:

- $\Delta d^{\square} = \frac{1}{N'}\sum_{i,j}^{N'} |d_{ij}^n - d^n|$ --- среднее отклонение расстояний между индивидами i и j от среднего расстояния d^n в пространстве решений по каждой из n переменных;
- $d_{ij}^n = |d_i^n - d_j^n|$ --- расстояние между индивидами i и j по каждой из n переменных в пространстве решений;
- i, j - номера индивидов в популяции;
- N' - число всех возможных пар индивидов;
- $\overline{N}$ - количество переменных (альтернатив) в решаемой задаче;
- M_n и m_n - максимально и минимально возможные значения n-й переменной во всей допустимой области соответственно.

Одной из особенностей такой мутации является то, что ее вероятность пропорционально зависит от плотности группировки решений-индивидов около какого-либо локального оптимума.

Главным преимуществом данного алгоритма является адаптивная мутация, а главным минусом, в свою очередь, - сложность реализации.

Структурная оптимизация сегмента локальной вычислительной сети

Для структурной оптимизации сегмента ЛВС в данной статье будет использоваться ВГА с адаптивной мутацией, поскольку в процессе работы именно этого алгоритма параметр мутации настраивается автоматически. Локальная сеть в условиях поставленной задачи может быть формализована взвешенным неориентированным графом, каждая вершина которого соответствует узлу сети, а каждое ребро - каналу связи. Поскольку оптимизация проводится на основании пропускной способности (в МБ/с) и надежности (BER) каналов связи, эти две характеристики следует хранить на каждом из ребер графа.

Так как в вершинах графа не хранится никаких характеристик, в процессе мутации можно случайным образом удалять одну из вершин индивида (или удалять ребра). На первый взгляд может показаться, что следует заведомо удалять ребра с самым большим значением пропускной способности и самым маленьким значением BER, однако такая мутация приведет к преждевременному схождению алгоритма к локальным оптимумам, что противоречит основной идее использования ГА. Особой разницы между случайным удалением вершин или ребер нет, так как независимо от этого во время вычисления фитнесс-функции необходимо дополнительно проверять связность подграфа и штрафовать решения, ведущие к несвязным графам. Это позволит обеспечить связность итогового решения. В сегменте сети могут находиться как сетевые устройства (коммутаторы, маршрутизаторы и т. д), так и конечные устройства (компьютеры, принтеры, сканеры, серверы и т. д.). Определенные типы узлов сети соединяются конкретными типами каналов связей, поэтому при оптимизации сети важно не переставлять каналы связи местами (возможно, что конкретное ребро не подходит для соединения других вершин графа). Алгоритм является стохастическим, поэтому во избежание получения различных результирующих графов сети следует закрепить случайное зерно генератора случайных чисел ($random.seed(42)$).

Для оптимизации сети и сравнения многокритериальных алгоритмов были использованы следующие параметры:

- размер начальной популяции - 100;
- количество поколений - 15;
- вероятность кроссовера (для каждого гена в хромосоме) - 0.5;
- начальная и конечная вероятности мутации (для каждого гена в хромосоме) - 0.01 и 0.3 соответственно.

Использование более высоких значений параметров может привести к тому, что в результате оптимизации граф (при заданной начальной конфигурации) будет иметь слишком маленькое количество узлов или каналов связи.

На Рисунках 1,2 представлены сегмент сети до структурной оптимизации и после.

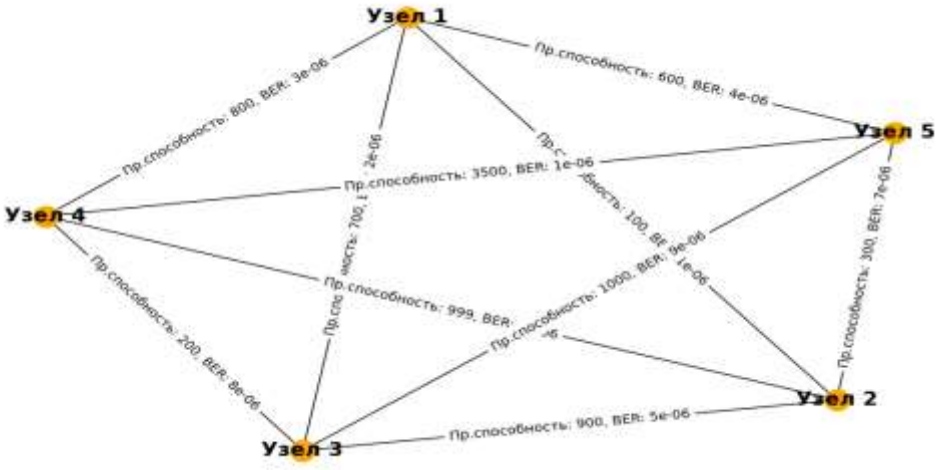


Рисунок 1 – Сегмент ЛВС до оптимизации

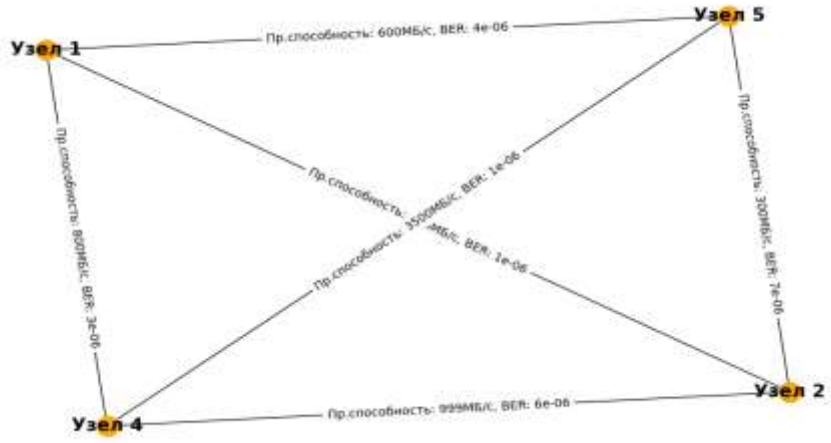


Рисунок 2 – Сегмент ЛВС после оптимизации

На Рисунках 3-8 приведены графики зависимости максимальных, средних и минимальных значений пропускной способности, BER и количества вершин популяции в зависимости от номера поколения. По этим графикам можно сделать выводы о критериях 2--6 для каждого из алгоритма.

Рисунок 3 – Зависимость функции приспособленности от поколения в NSGA-II

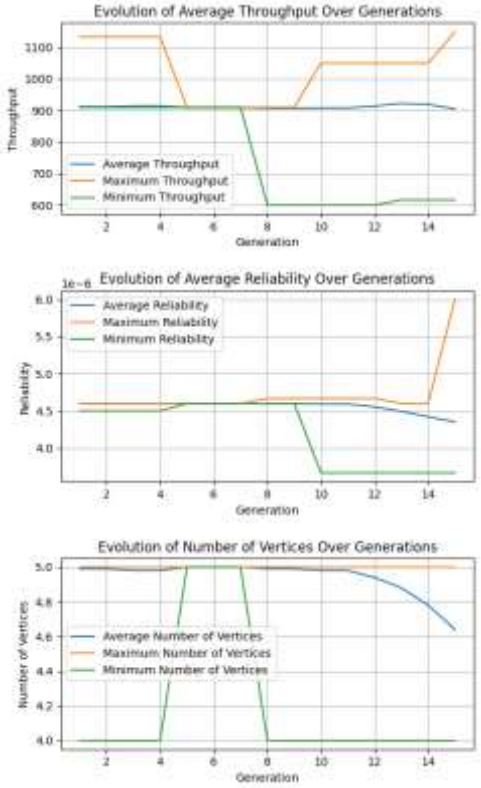


Рисунок 4 – Зависимость функции приспособленности от поколения в VEGA

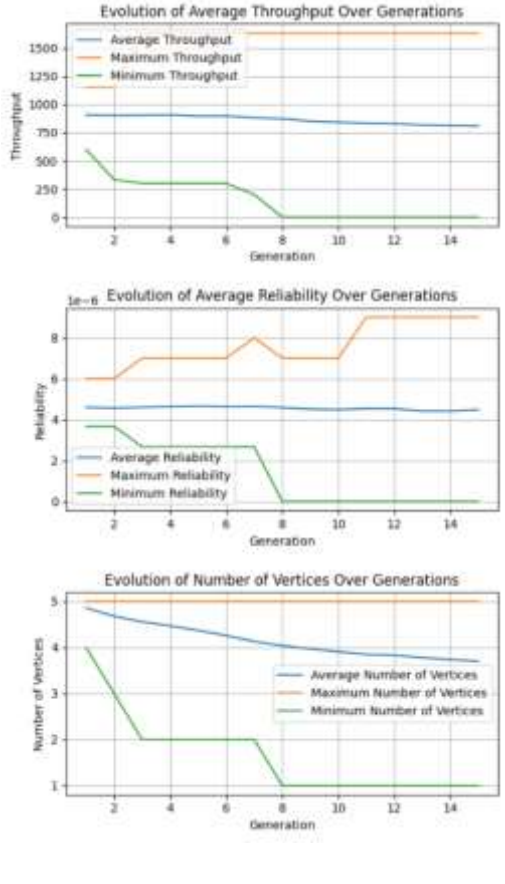


Рисунок 5 – Зависимость функции приспособленности от поколения в MOGA

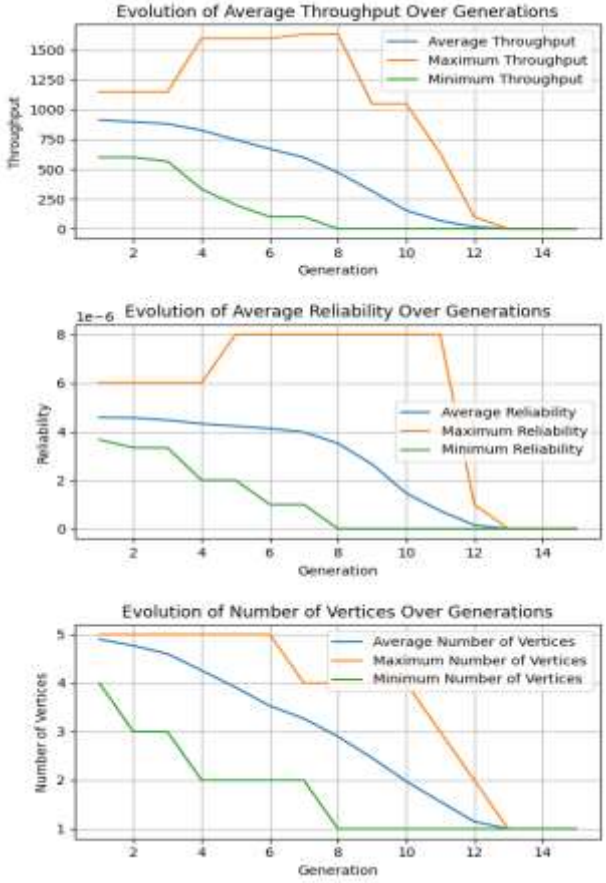


Рисунок 6 – Зависимость функции приспособленности от поколения в NPGA

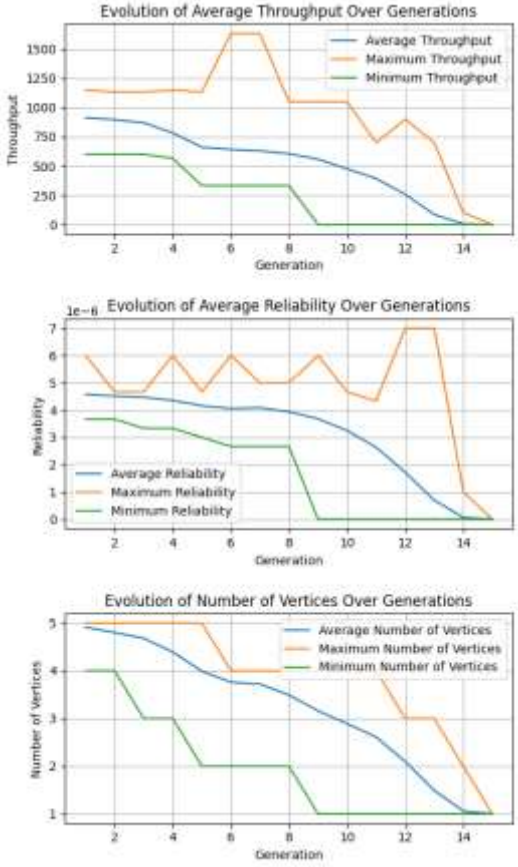


Рисунок 7 – Зависимость функции приспособленности от поколения в SPEA-II

По графикам видно, что наименее склонными к наличию застреваний в локальном оптимуме (критерии 1, 2, 5) при заданных параметрах являются MOGA и SPEA-II, однако учитывая малое разнообразие значений пропускной способности и надежности исходного графа можно сделать вывод о том, что алгоритм NSGA-II также не склонен к данной проблеме.

Разнообразие индивидов (критерий 6) присутствует в каждом из алгоритмов, поскольку ни в одной схеме нет ни единого критерия, среднее значение функции приспособленности которого оставалось бы постоянным. Стоит отметить, что даже малое изменение значений фитнесс-функции при данных параметрах и конфигурации сети считаются значительными. В алгоритмах NPGA и SPEA-II индивиды более разнообразны, но это приводит к слишком большому уменьшению количества вершин при заданных параметрах.

Сравнить многокритериальные методы по критерию 4 исходя из полученных графиков не получится. Для этого требуется провести дополнительные замеры. Так как алгоритм обладает стохастической природой, для анализа эффективности многокритериальных схем каждый алгоритм независимо запускался по 100 раз. Затем, исходя из ста полученных исходов, рассчитывалась средняя величина функции приспособленности итоговых решений оптимизации. Во время работы различных алгоритмов значения функции приспособленности лучшего индивида на каждой итерации улучшались или оставались примерно постоянными с течением времени, что может свидетельствовать о сходимости алгоритма и, как следствие, его правильной работе [8]. Результаты замеров приведены в Таблице 1.

Таблица 1 – Значения функции приспособленности полученного в результате работы алгоритма решения

	Многокритериальная схема				
	NSGA-II	VEGA	FFGA (MOGA)	NPGA	SPEA-II
Пропускная способность	1098.563075 9453447	904.170029 7999148	975.825194 3072648	1010.825194 3072648	1088.688319 4139193
BER	4.0985065141 40451e-06	4.2561089825 45764e-06	4.0476251830 96482e-06	4.47391826 54093e-06	4.29384908424 90845e-06
Количество вершин	3.790943755 9580554	4.17624521 0727969	2.5829478 1639427	3.812357246 3582749	3.629450549 4505493
Поколение, на котором получено конечное решение	12	13	14	13	14

Из таблицы видно, что при выбранных значениях параметров и конфигурации сети схема NSGA-II показывает лучший результат по пропускной способности среди рассмотренных алгоритмов, в то время как VEGA показывает наименьшую пропускную способность. По критерию минимизации BER схема NSGA-II находится на втором месте, при этом количество вершин не сильно отличается от других методов. Несмотря на то, что алгоритмы находят оптимальные решения почти с одинаковой скоростью, NSGA-II опережает остальных на 1-2 поколения.

Исходя из вышеперечисленного, можно сделать следующий вывод: при структурной оптимизации сегмента локальной вычислительной сети вероятностным генетическим алгоритмом с адаптивной мутацией наиболее эффективным многокритериальным алгоритмом является вероятностный генетический алгоритм с адаптивной мутацией, использующий NSGA-II.

Заключение

В статье была проведена структурная оптимизация сегмента локальной вычислительной. Также было проведено сравнение многокритериальных методов на основании выделенных критериев. при структурной оптимизации сегмента локальной вычислительной сети вероятностным генетическим алгоритмом с адаптивной мутацией наиболее эффективным многокритериальным алгоритмом является вероятностный генетический алгоритм с адаптивной мутацией, использующий NSGA-II.

Список литературы

1. Букатов А.А., Гуда С.А.. Компьютерные сети: расширенный начальный курс. Учебник для вузов. -- СПБ, 2020г.
2. Коваленко Н.Н., Семенкина О.Е. "Метод самоконфигурирования для настройки генетического алгоритма комбинаторной оптимизации". Актуальные проблемы авиации и космонавтики, vol. 2, no. 14, 2018, С. 49-51
3. Вычислительные технологии Том 23, № 5, 2018 Сравнение генетических алгоритмов MOGA и NSGA-II на задаче оптимизации формы рабочего колеса гидротурбины А. К. Гарагулова*, Д. О. Горбачева, Д. В. Чирков.
4. Сопов Е. А., Сопов, С. А. (2011). Вероятностный генетический алгоритм решения сложных задач многокритериальной оптимизации с адаптивной мутацией и прогнозом множества Парето. Вестник Самарского государственного аэрокосмического

университета им. академика С.П. Королёва (национального исследовательского университета), (6), С.273-282.
5. Зинченко А. С., Болквадзе И. Р., Внучков Ю. А. Применение метода линейной свертки критериев при оптимизации финансового обеспечения деятельности организации. Вестник университета, no. 1, 2017, С. 113-117.
6. Городилов А.Ю., Данилова Е.Ю. "". Вестник Пермского университета. Серия: Математика. Механика. Информатика, no. 4 (31), 2015, С. 84-90.
7. P.V. Galushin, and E.S. Semenkin. «The asymptotic probabilistic genetic algorithm». Сибирский аэрокосмический журнал, no. 5, 2009, С. 45-49.
8. Alcaraz, M. Landete, J. F. Monge and J. L. Sainz-Pardo. Multi-objective evolutionary algorithms for a reliability location problem. Eur. J. Oper. Res., vol. 283, no. 1, pp. 83-93, May 2020.

References

1. Bukatov A.A., Guda S.A. Computer Networks: An Extended Introductory Course. Textbook for universities. -- St. Petersburg, 2020.
2. Kovalenko N.N., Semenkina O.E. "SELF-CONFIGURATION METHOD FOR SETTING UP A GENETIC ALGORITHM OF COMBINATORIAL OPTIMIZATION". Current Problems in Aviation and Cosmonautics, vol. 2, no. 14, 2018, pp. 49-51.
3. Garagulova A.K., Gorbacheva D.O., Chirkov D.V. "Comparison of MOGA and NSGA-II Genetic Algorithms in the Optimization Task of the Shape of a Hydraulic Turbine Runner Blade." Computational Technologies Volume 23, No. 5, 2018.
4. Sopov E.A., Sopov S.A. (2011). "A Probabilistic Genetic Algorithm for Solving Complex Multi-Criteria Optimization Problems with Adaptive Mutation and Prediction of the Pareto Set". Bulletin of the Samara State Aerospace University named after academician S.P. Korolev (National Research University), (6), 273-282.
5. Zinchenko A.S., Bolkvadze I.R., Vnuchkov Y.A. "Application of the Method of Linear Convolution of Criteria in the Optimization of Financial Support for the Activities of an Organization". University Bulletin, no. 1, 2017, pp. 113-117.
6. Gorodilov A.Y., Danilova E.Y. " ". Bulletin of Perm University. Series: Mathematics. Mechanics. Informatics, no. 4 (31), 2015, pp. 84-90.
7. Galushin P.V., Semenkin E.S. "The Asymptotic Probabilistic Genetic Algorithm". Siberian Aerospace Journal, no. 5, 2009, pp. 45-49.
8. Alcaraz, M., Landete, J. F., Monge, J. L., Sainz-Pardo, J. L. "Multi-objective Evolutionary Algorithms for a Reliability Location Problem". European Journal of Operational Research, vol. 283, no. 1, pp. 83-93, May 2020.

Бондаренко О.С., Смирнов А.А., Вдовин В.С. Сравнительный анализ современных методов рендеринга ВЕБ-приложений и их влияния на производительность //Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 6(44) с. 113–121

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.4'2

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СОВРЕМЕННЫХ МЕТОДОВ РЕНДЕРИНГА ВЕБ-ПРИЛОЖЕНИЙ И ИХ ВЛИЯНИЯ НА ПРОИЗВОДИТЕЛЬНОСТЬ

[1]Бондаренко О.С., [2]Смирнов А.А., [3]Вдовин В.С.
ФГАОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ (ИТМО)», Санкт-Петербург, Россия (197101, город Санкт-Петербург, Кронверкский пр-кт, д. 49 литер а), e-mail: [1]rancerenly@gmail.com, [2]smirnov.andrew.1999@yandex.ru, [3]me@vladislavvdovin.ru

Постоянное развитие современных технологий сопровождается увеличением потребляемых ресурсов для их использования. Рост связан с непрерывным созданием нового контента и способов взаимодействия с ним, а также развитием используемых технологий и подходов к разработке продукта. Множество систем переходят на новый формат использования – в веб-среду, предпочитая повышать простоту взаимодействия с программой, так как сайт не требует установки дополнительного программного обеспечения и постоянных обновлений со стороны клиента, однако реализация подобной системы включает в себя большие наборы данных, их постоянную обработку, тем самым утяжеляя и усложняя веб-приложение.

Наращивание функционала в приложении приводит к необходимости оптимизировать внутренние процессы работы приложения путем анализа и адаптации техник рендеринга и отслеживания событий в веб-приложении.

С учетом развития современных технологий и способов размещения контента, стоимость ресурса, как и его вес, увеличиваются, в связи с чем появляется запрос на оптимизацию существующих подходов к разработке веб-приложений с целью получить тот же ресурс, но работающий быстрее и эффективнее в процессе взаимодействия с системой.

Актуальность работы обусловлена существованием проблемы оптимизации рендеринга веб-приложений является, так как эффективность работоспособности системы определяет уровень вовлеченности пользователей, что поднимает показатели конверсии сайтов.

Ключевые слова: Рендеринг, веб-приложение, фронтенд, производительность, JavaScript.

COMPARATIVE ANALYSIS OF MODERN WEB APPLICATION RENDERING METHODS AND THEIR IMPACT ON PERFORMANCE

[1] Bondarenko O.S., [2] **Smirnov A.A.**, [3] **Vdovin V.S.**
NATIONAL RESEARCH UNIVERSITY OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS (ITMO), St. Petersburg, Russia (197101, St. Petersburg, Kronverkskiy pr-kt, 49), e-mail: [1]rancerenly@gmail.com, [2]smirnov.andrew.1999@yandex.ru, [3]me@vladislavvdovin.ru

The constant development of modern technologies is accompanied by an increase in the resources consumed for their use. Growth is associated with the continuous creation of new content and ways to interact with it, as well as the development of technologies used and approaches to product development. Many systems are switching to a new format of use – to the web environment, preferring to increase the ease of interaction with the program, since the site does not require the installation of additional software and constant updates from the client, however, the

implementation of such a system includes large datasets, their constant processing, thereby weighing down and complicating the web application.
Increasing the functionality in the application leads to the need to optimize the internal processes of the application by analyzing and adapting rendering techniques and tracking events in the web application.
Taking into account the development of modern technologies and methods of content placement, the cost of the resource, as well as its weight, are increasing, and therefore there is a request to optimize existing approaches to developing web applications in order to get the same resource, but working faster and more efficiently in the process of interacting with the system.
The relevance of the work is due to the existence of the problem of optimizing the rendering of web applications, since the efficiency of the system determines the level of user engagement, which raises the conversion rates of sites.

Keywords: Rendering, web application, frontend, performance, JavaScript.

В работе «Сравнительный анализ популярных JavaScript фронтенд решений» Еремин М. В. анализирует современные фронтенд-фреймворки.[2] Начиная с Vue, автор определяет его как подходящий для одностраничных приложений и рендеринга на стороне сервера. Он отмечает высокую производительность и гибкость решения, однако риск чрезмерной гибкости относит к недостаткам, так как такое качество является негативным в рамках разработки большого и сложного проекта. Гибкость как негативное качество автор определяет в связи с большим количеством вариантов построения решения с использованием данного инструмента, это объясняется отсутствием строгой архитектуры проекта.

Касательно фреймворка Angular, стоит отметить, что есть две версии данного фреймворка: Angular и AngularJS. Первый представляет из себе переписанную версию старого AngularJS, включающую в себя множество улучшений и применение TypeScript как основного языка при разработке. В отличие от AngularJS, который полностью базируется на JavaScript.

К достоинствам фреймворка Angular Еремин М.В. относит производительность сервера и связывание данных. Механизм связывания данных в Angular позволяет отслеживать изменения в реальном времени, которые автоматически отображаются в модели, а производительность сервера улучшает производительность приложения в целом. К недостаткам использования этого фреймворка относит сложность архитектуры и большое количество файлов, связанных друг с другом, что объясняется множеством зависимостей в одном компоненте. Однако Толстых М.А. в статье отмечает, что строгая архитектура и высокая масштабируемость фреймворка Angular относится к достоинствам использования данного решения для реализации крупных и сложных систем в сегменте корпоративной разработки.

Толстых М.А. в своей работе определяет ReactJS как инструмент для быстрой разработки, в связи с низким порогом входа. Библиотека используется для создания динамических пользовательских интерфейсов, отличительным механизмом при изменении данных является виртуальный DOM, позволяющий эффективно управлять элементами на странице.

Последний, рассмотренный Ереминым М.В., популярный фреймворк – Svelte – обладает высокой производительностью у пользователя, так как работает на этапе сборки приложения, преобразуя код в стандартный JavaScript код, а также отличается отсутствием необходимости использовать виртуальный DOM.

Так, можно сравнить проанализированные решения по следующим критериям в Таблице 1.

Таблица 1 – Сравнение фронтенд-фреймворков по основным критериям

Критерий	VueJS	Angular	React	Svelte
Взаимодействие с DOM	Построение vDOM и сравнение с DOM	Incremental DOM	Построение vDOM и сравнение с DOM	Точечное обновление DOM
Архитектура	MVVM (officially)	MVVM-based	MVVM-based	MVVM-based
Масштаб проекта	Средний, небольшой	Крупный, средний	Средний, небольшой	Средний, небольшой

Авторы статьи «Рендеринг и его влияние на архитектуру веб-приложений» Заманов Е.А., Дутова Е.А. и Селецкая Н.Г., выделяют три основных подхода к рендерингу веб-приложений [3]:

1. Рендеринг на стороне клиента (Client-site rendering, CSR).
2. Рендеринг на стороне сервера (Server-side rendering, SSR).
3. Регидрация.

Суть первого подхода (CSR) заключается в отправлении сервером клиенту пустой HTML-страницы с некоторым набором скриптов, контент которой отображается в браузере при помощи JavaScript с использованием ресурсов сервера в дальнейшем за получением исходных данных.

К недостаткам можно отнести проблемы с SEO, высокая нагрузка на клиент, а также снижение производительности при масштабировании приложения.

Преимуществами такого подхода можно считать распределение нагрузки на веб-приложение между всеми клиентами и упрощение серверной части веб-приложение, как следствие, снижение затрат на поддержку ресурса.

Для решения проблемы с оптимальным отображением сайтов для поисковых систем является регидрация. Эта технология совмещает в себе подход к рендерингу как серверный, так и клиентский: с использованием веб-фреймворка на стороне клиента происходит преобразование статического DOM, полученного с сервера, в динамический, дополняя его функциональными элементами для корректной работы веб-приложения.

Фреймворками, которые относятся к подходу CSR, являются Vue, React, Angular и Svelte. Приложение в перечисленных фреймворках строится в виде дерева компонентов, каждый из компонентов описывает подмножество DOM, однако процесс взаимодействия с DOM отличается. В связи с ветвлением структуры компонентов, каждый компонент-родитель может разделять свое состояние с компонентами-потомками. Привязка данных реализована в одностороннем порядке из состояния приложения в пользовательский интерфейс, что гарантирует стабильность состояния приложения во время цикла рендеринга при манипуляции с DOM.

В статье «Современные фреймворки для разработки web-приложений» Байдыбеков А.А., Гильванов Р.Г., Молодкин И.А. отмечают различия в подходе к перерисовке DOM между React и Vue [4]. В ReactJS изменение состояния компонента приводит к изменению всего поддерева этого компонента, представление этого процесса отображено на Рисунке 1.

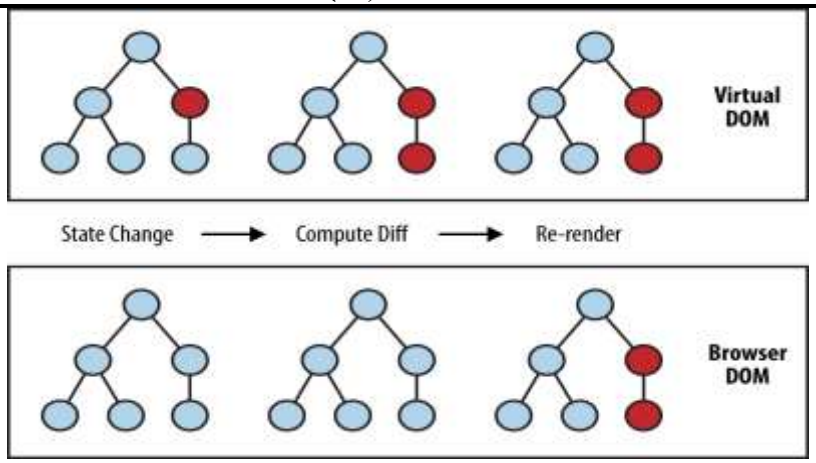


Рисунок 1 – Схема перерисовки DOM ReactJS

Vue реализует изменения точечно, автоматически отслеживая зависимости компонентов, что положительно сказывается на производительности приложения. Схема работы обновления DOM у VueJS представлена на Рисунке 2.

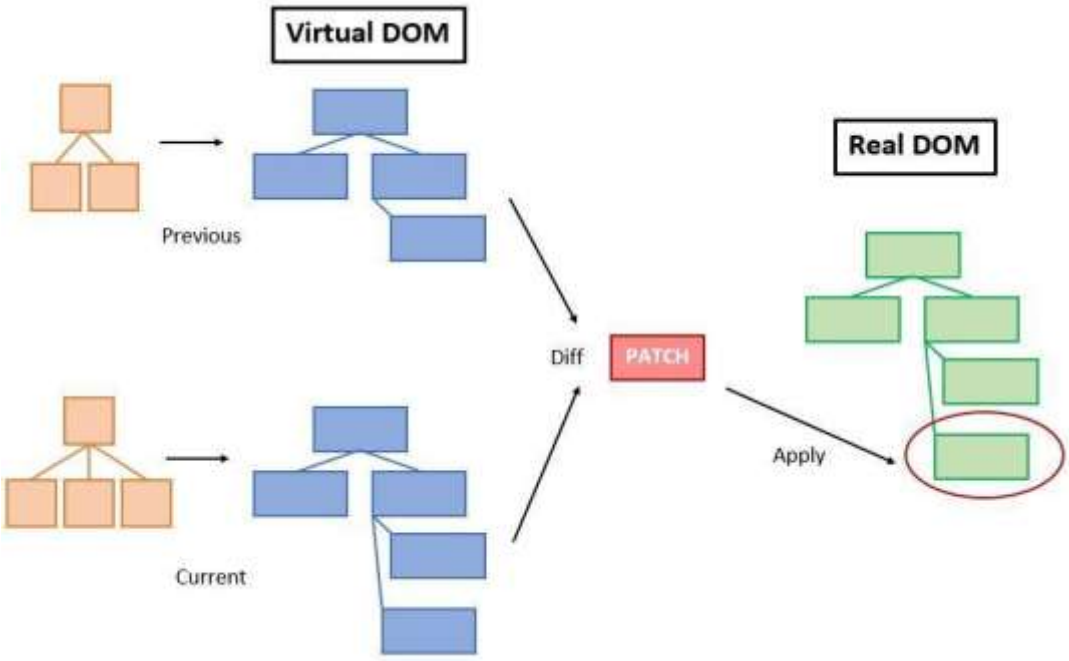


Рисунок 2 – Схема перерисовки DOM VueJS

К.Ю. Бетеев и Г.В. Муратова для определения механизмов эффективной перерисовки DOM ссылаются на книги Томаса Марка «React в действии» и Чиннатамби К. «Изучаем React», выделив следующие механизмы:

1. Использование паттерна проектирования «Наблюдатель».
2. Пакетное (batch) обновление DOM.
3. Алгоритм поиска различий с линейной сложностью O(n).

Паттерн Observer в React.js реализован при помощи распределения элементов в интерфейсе в виде компонентов, имеющих состояние (родительское или собственное). В

момент изменения состояния, запускается цепочка сравнения и перерисовки интерфейса в DOM.

Пакетное обновление представляет из себя сбор изменений, перерисовку которых можно отложить до завершения манипуляции с состоянием, позволяя снизив потерю эффективности в случае постоянных обновлений состояния компонента, таким образом, произведя процесс перерисовки единожды.

Поиск различий с линейной сложностью позволяет сравнивать деревья в vDOM перед отрисовкой в браузере в моменте согласования элементов.

Авторы статьи подмечают, что эффективная работа с DOM возможна с использованием различных практик, не требующих внедрения vDOM. Такие фреймворки как Angular и Svelte не используют данную концепцию, ориентируясь на точечных изменениях в DOM для эффективного обновления.

Как и в vDOM, каждый компонент определяет набор узлов DOM, которые должны быть отображены экземпляром компонента. В отличие от vDOM, здесь нет отдельного шага, на котором вычисляются все необходимые изменения пользовательского интерфейса.

Рендеринг заключается в прохождении по дереву компонентов, выполнении проверок привязок данных, чтобы увидеть, какие из них изменились и применении изменений к DOM для каждой найденной привязки.

Статья «Исследование методологии оптимизации рендеринга компонентов на примере Svelte», написанная Летоном Г., Глазько П.Е., описывает механизмы оптимизации рендеринга, выделяя одним из ключевых – уменьшение конечного размера веб-приложения.[5] Авторы статьи отмечают, что операции с DOM сильно влияют на производительность веб-приложений, соответственно, оптимальным решением для улучшения производительности является уменьшение взаимодействия с DOM.

Авторы статьи оценили производительность такой реализации решения и взаимодействия с DOM путем сравнения метрики FID с выполнением аналогичного функционала в React-приложении. Проанализировав и оценив работу двух приложений на основании выбранных метрик, Летон Г. и Глазько П.Е. пришли к следующему выводу: показатели приложения на Svelte выше примерно в полтора раза, компактность приложения. 24 Кб против 340 Кб в React отличается преимуществом использования Svelte вместо ReactJS, в случае отсутствия механизмов оптимизации в React-приложении разрыв в производительности будет только расти.

Данная статья позволяет сделать вывод, что использование механизмов компиляции кода в JavaScript при помощи компилятора-Svelte относит этот фреймворк к разряду более производительных на основании оценки метрик исследования.

Помимо рендеринга на клиентской стороне необходимо исследовать процесс серверного рендеринга веб-приложений, что позволит сравнить эффективность и производительность двух противоположных инструментов к реализации веб-сайтов.

SSR представляет возможность рендеринга двумя способами:

1. Статический – возвращение подготовленной HTML-страницы, которая была сгенерирована на этапе сборки сайта.

2. Контент по запросу – после запроса происходит обращение к базе данных, вследствие чего с помощью шаблонизатора происходит генерация страницы и отправка разметки в браузер.

Стоит отметить, что такой подход ведет к удорожанию стоимости разработки в связи с усложнением архитектуры приложения и высокой нагрузки на сервер, однако улучшает производительность веб-приложения на устройствах пользователей за счет отсутствия JavaScript кода.

В различных реализациях «server-side rendering» ключевой концепцией является способность запускать JavaScript на сервере с целью создания веб-разметки. Далее эта сгенерированная разметка передается в браузер пользователю, и там начинается процесс построения DOM-дерева. Это позволяет отображать веб-страницы согласно типичному для веб-браузера сценарию. Таким образом, можно выделить три основных этапа в использовании подхода серверного рендеринга для одностраничных веб-приложений. Первый этап - запуск JavaScript-кода на сервере и создание статических HTML-страниц. Второй этап - оптимальная передача сгенерированной разметки клиенту. Третий этап - выполнение полученного кода в веб-браузере и построение DOM-дерева.

Для реализации этого подхода необходимо наличие платформы Node.js вне зависимости от выбранного фронтенд-фреймворка, соответственно, нужен сервер для осуществления рендеринга, а также необходимо предусмотреть способы по сериализации и десериализации разметки на клиенте и сервере.

Отмечая преимущества такого решения в виде увеличения производительности клиентской части приложения и улучшении SEO-оптимизации сайта за счет сгенерированных HTML-страниц, а не JavaScript кода, возникают и недостатки с точки зрения повышения расходов на поддержу приложения относительно расходов сервера, разработка более сложной архитектуры, что приводит к бóльшим затратам на поддержку такого решения.

В работе «Optimize along the way: An industrial case study on web performance» авторы отмечают, что повышение производительности веб-приложений является комплексной задачей, поскольку требует глубокого понимания как механизма браузера, так и конкретных сценариев использования рассматриваемого веб-приложения. [7] За счет улучшения времени загрузки, производительность, воспринимаемая пользователем, увеличивается.

Различия в процессе рендеринга с использованием vDOM объясняются архитектурой фреймворков. Nian Li и Bo Zhang в статье «The Research on Single Page Application Front-end development Based on Vue» исследуют одностраничные приложения в рамках реализации на основе фреймворка Vue, отмечая следующий паттерн проектирования как ведущий в данном инструменте – MVVM [8].

Vue придерживается идее управления данными и компонентами, используя дизайн инкрементальной разработки. С паттерном MVVM данные (model) и представления (view) разделены таким образом, чтобы исключить прямое взаимодействие.

Для декомпозиции взаимодействия между двумя слоями приложения используется view-model, при помощи которого возможно отслеживание действий с обеих сторон и своевременное выполнение соответствующей операции реагирования на изменения, обновления данных и связывания элементов.

Схема архитектуры MVVM в приложении, реализованном с использованием фреймворка Vue, представлена на Рисунке 3.

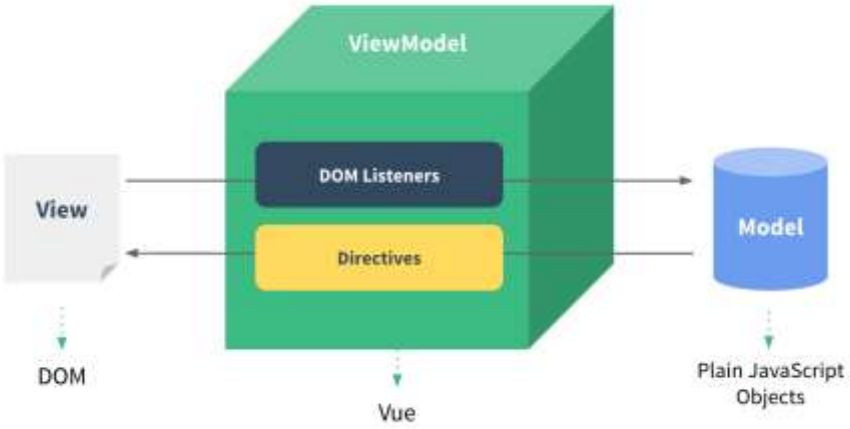


Рисунок 3 – Архитектура MVVM в приложении Vue

Принцип работы представляет собой двунаправленное связывание, после создания привязки, происходит синхронизация DOM с данными. В момент обновления данных, узлы DOM также будут синхронизироваться с данными. Если представление обновится в DOM, то view-model, в свою очередь, вызовет определенную логику приложения для запуска механизма обновления данных в модели (model), чтобы реализовать двунаправленное связывание.

В статье «Modern Web Frameworks: A Comparison of Rendering Performance» Risto Ollila, Niko Makitalo и Tommi Mikkonen рассмотрели, как работают стратегии рендеринга современных фронтенд-фреймворков и представили способ их относительной производительности. [10]

Таблица 2 – Описание факторов, влияющих на производительность исследуемых фреймворков

Фреймворк / Библиотека	**Обрабатываемые компоненты**	**Обработанные элементы**	**Наличие vDOM**
Vue	Только «грязные» компоненты	Только привязанные	Есть
Angular	Все	Только привязанные	Нет
React	Поддерево обновляемого компонента	Все	Есть
Svelte	Только «грязные» компоненты	Только привязанные	Нет

Таким образом, Vue и Svelte имеют преимущество, когда обновляются только небольшие части интерфейса, так как они ограничиваются обновлением только необходимых элементов.

В то время как Angular и React могут потреблять больше ресурсов на обновление элементов, даже если они не привязаны к изменяющимся данным.

Заключение

В процессе анализа было выявлено, что темы, связанные с процессами пререндеринга и регидратации (изоморфного рендеринга), остаются недостаточно исследованными и подробно освещены как в отечественных, так и в зарубежных исследованиях.

Анализ источников показал, что актуальность проблемы оптимизации рендеринга веб-приложений обусловлена динамичным развитием современных веб-приложений. По мере того, как приложения становятся все более сложными и функциональными, нагрузка на клиентскую сторону с использованием CSR (client-side rendering) значительно увеличивается, что отмечается в исследованиях и зарубежных, и отечественных авторов.

Таким образом, изучение процесса рендеринга и поиски оптимизационных решений в этой области являются крайне важными задачами для современных разработчиков и исследователей. Необходимо стремиться к нахождению баланса между богатством функциональности веб-приложений и их производительностью, чтобы обеспечить плавное и комфортное взаимодействие пользователей с приложениями в любых условиях.

Список литературы

1. Толстых, М. А. Оценка перспективности фреймворков для создания современных web-приложений//Научные исследования XXI века. – 2020. – №1(3). – С. 79–82.
2. Еремин М.В. Сравнительный анализ популярных JavaScript фронтенд решений//Тенденции развития науки и образования. – 2022. – №87– 1. – С. 64–68.
3. Заманов Е.А., Дутова Е.А., Селецкая Н.Г. Рендеринг и его влияние на архитектуру веб-приложений//Российский университет транспорта (Москва). – 2021. – С. 297–301.
4. Байдыбеков А.А., Гильванов Р.Г., Молодкин И.А. Современные фреймворки для разработки web-приложений//Интеллектуальные технологии на транспорте. – 2020. – №4 (24). – С. 23–29.
5. Летон Г., Глазько П.Е. Исследование методологии оптимизации рендеринга компонентов на примере svelte//XI Конгресс Молодых Учёных Сборник научных трудов. Санкт-Петербург, 2022. – 2022. – С. 231– 234.
6. Ростов Д.С., Готская И.Б., Государев И.Б. Исследование методов имплементации рендеринга клиентского интерфейса на стороне сервера//XLVIII Научная и Учебно-Методическая Конференция Университета ИТМО Санкт-Петербург, 29 января – 01 февраля 2019 года. – 2019. – С. 244– 246.
7. Jasper van Riet, Ivano Malavolta, Taher A. Ghaleb Optimize along the way: An industrial case study on web performance//Journal of Systems and Software. – 2023. Volume 198
8. Nian Li, Bo Zhang The Research on Single Page Application Front-end development Based on Vue//Journal of Physics: Conference Series. – 2021. Volume 1883
9. Ollila R., Mäkitalo N, Mikkonen T. Modern Web Frameworks: A Comparison of Rendering Performance//Journal of Web Engineering. – 2022. – №21(03). – С. 789–814.

References

1. Tolstykh, M. A. Evaluation of the prospects of frameworks for creating modern web applications // Scientific research of the XXI century. – 2020. – №1(3). – Pp. 79-82.
2. Eremin M.V. Comparative analysis of popular JavaScript frontend solutions // Trends in the development of science and education. – 2022. – №87– 1. – Pp. 64-68.
3. Zamanov E.A., Dutova E.A., Seletskaya N.G. Rendering and its influence on the architecture of web applications // Russian University of Transport (Moscow). - 2021. – pp. 297-301.
4. Baidybekov A.A., Gilvanov R.G., Molodkin I.A. Modern frameworks for web application development // Intelligent technologies in transport. – 2020. – №4 (24). – Pp. 23-29.
5. Leton G., Glazko P.E. A study of the methodology for optimizing component rendering on the example of svelte // XI Congress of Young Scientists Collection of scientific papers. St. Petersburg, 2022. – 2022. – pp. 231-234.
6. Rostov D.S., Gotskaya I.B., Gosudarev I.B. Research of methods of implementation of rendering of the client interface on the server side // XLVIII Scientific and Educational-Methodical Conference of ITMO University St. Petersburg, January 29 – February 01, 2019. - 2019. – pp. 244-246.
7. Jasper van Riet, Ivano Malavolta, Taher A. Ghaleb Optimize along the way: An industrial case study on web performance // Journal of Systems and Software. – 2023. Volume 198
8. Nian Li, Bo Zhang The Research on Single Page Application Front-end development Based on Vue // Journal of Physics: Conference Series. – 2021. Volume 1883
9. Ollila R., Mäkitalo N, Mikkonen T. Modern Web Frameworks: A Comparison of Rendering Performance // Journal of Web Engineering. – 2022. – №21(03). – pp. 789-814

Сафонова Т.В. и др. Обзор использования технологии интернета вещей в современном мире / Сафонова Т.В., Мокряк А.В., Муленко М.Д., Лескова Д.О., Осина Д.А // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 6(44) с. 122–128

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.9

ОБЗОР ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ ИНТЕРНЕТА ВЕЩЕЙ В СОВРЕМЕННОМ МИРЕ

Сафонова Т.В., [1]Мокряк А.В., Муленко М.Д., Лескова Д.О., Осина Д.А.,
ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ" Санкт-Петербург, Россия (192007, город Санкт-Петербург, Воронежская ул., д. 79)
[1]ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ ГОСУДАРСТВЕННОЙ ПРОТИВОПОЖАРНОЙ СЛУЖБЫ МИНИСТЕРСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ ИМЕНИ ГЕРОЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ГЕНЕРАЛА АРМИИ Е.Н.ЗИНИЧЕВА", Санкт-Петербург, Россия (196105, г.Санкт-Петербург, Московский проспект, д.149), e-mail: mokryakanna@mail.ru

Использование технологии интернета вещей в современном мире становится все более распространенным и влиятельным. Данная технология позволяет устройствам быть связанными и обмениваться данными через интернет, что открывает множество возможностей для автоматизации, мониторинга и улучшения эффективности. Цель данной статьи – исследование технологии иинтернета вещей. В процессе анализа были раскрыты базовые компоненты изучаемой технологии. Посредством их взаимодействия происходит формирование единой сети устройств интернета вещей, которая дает возможность управлять объектами, находящимися вокруг нас. В статье представлены преимущества использования интернета вещей, а также обзор технологий, расширяющих возможности данной технологии.

Ключевые слова: Технология интернета вещей, искусственный интеллект, аналитика данных.

OVERVIEW OF THE USE OF INTERNET OF THINGS TECHNOLOGY IN THE MODERN WORLD

Safonova T.V., [1]Mokryak A.V., Mulenko M.D., Leskova D.O., Osina D.A.
RUSSIAN STATE HYDROMETEOROLOGICAL UNIVERSITY, St. Petersburg, Russia (192007, St. Petersburg, Voronezhskaya str., 79)
[1]ST. PETERSBURG UNIVERSITY OF THE STATE FIRE SERVICE OF THE MINISTRY OF THE RUSSIAN FEDERATION FOR CIVIL DEFENSE, EMERGENCIES AND ELIMINATION OF CONSEQUENCES OF NATURAL DISASTERS NAMED AFTER THE HERO OF THE RUSSIAN FEDERATION, GENERAL OF THE ARMY E.N. ZINICHEV, St. Petersburg, Russia (196105, St. Petersburg, Moskovsky prospekt,149), e-mail: [1]mokryakanna@mail.ru

The use of Internet of Things technology in the modern world is becoming more widespread and influential. This technology allows devices to be connected and share data over the Internet, which opens up many possibilities for automation, monitoring and efficiency improvement. The purpose of this article is to study the technology and Internet of things. During the analysis, the basic components of the technology under study were revealed. Through their interaction, a unified network of Internet of Things devices is being formed, which makes it possible

to control objects around us. The article presents the advantages of using the Internet of Things, as well as an overview of technologies that expand the capabilities of this technology.

Keywords: Internet of Things technology, artificial intelligence, data analytics.

Введение

Технология интернета вещей представляет собой кардинальную технологическую модификационную разработку, которая распространяется по всем отраслям производства. Текущая тенденция развития технологий цифровой трансформации содержит взаимосвязанные устройства и данные, где реальные объекты преобразуются в интеллектуальные, которые обмениваются данными между собой и принимают управленческие решения. Технология интернета вещей открывает уникальные возможности для развития разных индустрий и улучшения качества жизни [1].

Каждый день растет число устройств интернета вещей во всех странах. Объекты интернета вещей собирают данные с помощью миллионов сенсоров и отправляют их для анализа. Эта технология стала важной частью нашей жизни, меняя привычные бизнес-процессы посредством улучшения качества услуг и безопасности деятельности.

Тенденция по использованию технологии интернета вещей

Интернет вещей базируется на ряде ключевых технологических компонентах (рис.1):

Рисунок 1 – Основные компоненты технологии интернета вещей

- сенсорах и датчиках, позволяющих собирать данные о внешнем мире;
- технологиях связи, обеспечивающих передачу данных между разными ресурсами;
- облачных технологиях для хранения и обработки данных;
- средствах автоматизации, позволяющих управлять устройствами на основе исследования данных;

- методах машинного обучения и искусственного интеллекта, используемых для анализа данных и принятия решений на основе алгоритмов [2, 3].

Технология интернета вещей находит свое применение в различных отраслях индустрии, к примеру:

- умный дом: устройства технологии интернета вещей дают возможность автоматизировать управление светом, отоплением, системами безопасности и другими функциями;
- умный город: технологии интернета вещей применяются для оптимизации транспортных систем для улучшения качества коммунальных услуг и повышения безопасности;
- промышленность: технологии интернета вещей помогают контролировать функциональное состояние оборудования и оптимизировать производственные процессы, что приводит к повышению эффективности и снижению затрат;
- агропромышленный комплекс: технологии интернета вещей улучшают мониторинг посевов и позволяют управлять уровнем продовольственной безопасности страны [4];
- здравоохранение: технологии интернета вещей используются в медицине для диагностики заболеваний, мониторинга здоровья пациентов и контроля за работой медицинского оборудования;
- торговля и логистика: технологии интернета вещей обеспечивают мониторинг и контроль за движением товаров, оптимизацию логистических функций и улучшение коммуникации в цепи поставок;
- энергетика: технологии интернета вещей используются для мониторинга и управления энергосистемами, оптимизации потребления энергии и развития возобновляемых источников энергии;
- образование: технологии интернета вещей используются для реализации интерактивных обучающих систем, анализа данных об успеваемости студентов и оптимизации учебного процесса;
- финансы: технологии интернета вещей дают возможность формировать интеллектуальные системы учета, анализа и контроля финансовых операций, а также оптимизировать управление рисками и инвестициями [5, 6].

Развитие технологии интернета вещей

По прогнозам, количество устройств интернета вещей будет продолжать увеличиваться в ближайшие годы. Подключенные устройства могут значительно увеличиться из-за роста числа устройств в таких областях, как умный дом, промышленность, агропромышленный комплекс и здравоохранение.

Предварительные прогнозы указывают на то, что к 2025 году число подсоединенных к интернету вещей устройств превысит 75 миллиардов по всему миру. Этот значительный рост вызван расширением масштабов внедрения технологии интернета вещей в различных сферах деятельности [7].

Развитие 5G сети сыграет важную задачу в масштабировании возможностей интернета вещей. 5G предоставляет высокую скорость передачи данных, низкую задержку и увеличенную пропускную способность, что делает ее идеальным выбором для подключения

устройств интернета вещей. Это дает возможность аккумулировать большое количество устройств в одной локации и обеспечивает эффективную работу всей системы [8].

Взаимодействие технологии интернета вещей с искусственным интеллектом и аналитикой данных

Искусственный интеллект (ИИ) и аналитика данных играют немаловажную роль в модификации данных интернета вещей в формат полезной информации.

Искусственный интеллект изменяет метод обработки данных в интернете вещей. Алгоритмы машинного обучения анализируют обширные наборы данных, выявляют скрытые закономерности и тенденции, которые могут оставаться незамеченными при первом взгляде. К примеру, в медицине ИИ анализирует данные о пациентах и предсказывает возможные заболевания. В производстве ИИ помогает предсказывать сбои оборудования и планировать его обслуживание.

Безопасность интернета вещей

Безопасность является одним из главных вызовов для технологии интернета вещей ввиду того, что рост количества устройств масштабно увеличивает угрозы и риски.

Одной из главных угроз, связанных с технологией интернета вещей, являются уязвимости в оборудовании. Неавторизованный доступ, утечка данных и даже возможность кибератак на критическую инфраструктуру — все это риски, связанные с уязвимостями в устройствах интернета вещей. Поэтому очень важно обеспечивать безопасность устройств и данных, которые они собирают и передают.

Для обеспечения безопасности в сфере интернета вещей используются разнообразные меры защиты, включая шифрование информации, проверку подлинности пользователей и использование сетевых брандмауэров.

С появлением новых технологий интернета вещей возрастает важность обеспечения безопасности, что подчеркивает необходимость постоянного совершенствования методов защиты и внедрения инновационных технологий для обеспечения безопасности сети интернета вещей [9].

Все эти аспекты — рост числа устройств, влияние ИИ и безопасность — играют важную роль в будущем развитии технологии интернета вещей и определяют ее перспективы в мире современных инновационных разработок.

Достоинства использования технологии интернета вещей в геоэкологии

Интернет вещей проявляет значительное влияние на энергопотребление. Устройства интернета вещей могут потреблять значительное количество энергии, особенно если они подключены к Интернету. Однако, существуют способы снижения энергопотребления устройств интернета вещей, например, использование энергоэффективных технологий и алгоритмов [10]. Кроме того, устройства интернета вещей могут помочь в оптимизации использования энергии, например, путем мониторинга энергопотребления и предоставления информации для принятия решений о том, как использовать энергию наиболее эффективно.

Технология интернета вещей благоприятствует стабильному использованию ресурсов и спаду потребления энергии, что приводит к снижению выбросов парниковых газов и улучшению экологической ситуации, посредством эффективного управления ресурсами. Следует отметить, что технология интернета вещей благополучно используется для

корректной и адекватной подкормки растений, что позволит сократить применение удобрений и снизить воздействие на окружающую среду.

Экологические аспекты технологии интернета вещей приобретают все большее значение. Разработка и внедрение данной технологии должны принимать во внимание вопросы энергопотребления и устойчивого развития, чтобы способствовать формированию более экологичного будущего и снижению отрицательного влияния на окружающую среду [11].

Выводы

Технология интернета вещей трансформировалась из идеи в мощную силу, которая изменила мир и улучшила повседневную жизнь. Данная статья была ориентирована на ключевые аспекты и перспективы развития технологии интернета вещей, на основании чего формируются следующие тезисы:

1. Активный рост технологии интернета вещей: прогнозы показывают, что количество устройств интернета вещей будет быстро расти в ближайшие годы. 5G сети будут играть ключевую роль в этом процессе, обеспечивая более высокую скорость передачи данных и увеличивающиеся возможности для интернета вещей.
2. Возможности искусственного интеллекта: ИИ и анализ данных меняют способ работы с информацией в интернете вещей, позволяя обнаруживать скрытые закономерности и создавать прогнозы, что используется в медицине, промышленности и многих других сферах.
3. Безопасность: увеличение количества устройств интернета вещей сопровождается угрозами и рисками безопасности. Однако новейшие методы защиты и непрерывное развитие технологий безопасности способствуют защите сетей интернета вещей.
4. Экологический аспект технологии интернета вещей: эффективное управление энергией и устойчивое использование ресурсов делают технологию интернета вещей более экологичной и способствуют сохранению окружающей среды.

Интернет вещей продолжает активно развиваться и оказывает значительное влияние на общество и экономику. С учетом упомянутых аспектов можно с уверенностью утверждать, что технология интернета вещей продолжит трансформировать наш мир, связывая его, делая более умным и экологичным.

Список литературы

1. Сафонова Т.В. Обзор технологий создания интеллектуальных геоинформационных систем//Информационные технологии и системы: управление, экономика, транспорт, право. 2020. №3(39). С.18-27.
2. Сафонова Т.В. Мультиагентные системы//Информационные технологии и системы: управление, экономика, транспорт, право. 2020. №4(40). С.12-29.
3. Сафонова Т.В. Взаимодействие глобальной многофункциональной инфокоммуникационной спутниковой системы связи с объектами IoT в сельскохозяйственном производстве. Международный научно-исследовательский журнал/ Истомин Е.П., Яготинцева Н.В., Колбина О.Н., Мокряк А.В. 2023. №11 (137)

4. Сафонова Т.В, Колбина О.Н., Яготинцева Н.В, Мокряк А.В. Использование мультиагентных систем в лесном хозяйстве IOP Conference Series: Наука о Земле и окружающей среде. № 806 (2021) 012028
5. Колбина О.Н., Истомин Е.П., Яготинцева Н.В. Каламбет М.В. Особенности создания базы данных для IoT-системы городского лесоуправления в городе Санкт-Петербурге. IOP Conference Series: Наука о Земле и окружающей сред, 2021, № 876(1), 012039
6. Интернет вещей в сельском хозяйстве (Agriculture IoT / AIoT): мировой опыт, кейсы применения и экономический эффект от внедрения в РФ // Аналитический отчет. – J'son &Partners Consulting, 2017 [Электронный ресурс]. – URL: http://json.tv/ict_telecom_analytics_view/internet-veschey-v-selskom-hozyaystve-agriculture-iot-aiot-mirovoy-opyt-keysy-primeneniya-i-ekonomicheskiy-effekt-ot-vnedreniya-v-rf-20170621045316.
7. Сафонова Т.В., Яготинцева Н.В., Колбина О.Н., Мокряк А.В. Концепция развития интернета вещей информационные технологии: управление, экономика Транспортное право. 2022. №2(42). С.4
8. Сафонова Т.В., Колбина О.Н., Яготинцева Н.В., Мокряк А.В. Контроль и мониторинг экологической безопасности окружающей среды Международный научно-исследовательский журнал 54-1 (119). 2022. С. 115-119.
9. Вершинин А.К., Сафонова Т.В., Русскин В.Д., Логинов И.С., Ясников А.И. Интернет вещей в сельском хозяйстве Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 1 (45). С. 28-34.
10. Тикки Д.А., Никольский В.Е., Авакян Е.В., Самошкин Н.С., Сафонова Т.В. Обзор применения сенсорных датчиков в промышленности Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 2 (46). С. 29-36.
11. Тикки Д.А., Сафонова Т.В., Русскин В.Д. Цифровые двойники в сельском хозяйстве Информационные технологии и системы: управление, экономика, транспорт, право. 2022. № 4 (44). С. 49-53.

References

1. Safonova T.V. Review of technologies for creating intelligent geoinformation systems // Information technologies and systems: management, economics, transport, law. 2020. No.3(39). pp.18-27.
2. Safonova T.V. Multi-agent systems // Information technologies and systems: management, economics, transport, law. 2020. No.4(40). pp.12-29.
3. Safonova T.V. Interaction of the global multifunctional infocommunication satellite communication system with IoT objects in agricultural production. International Scientific Research Journal/ Istomin E.P., Yagotintseva N.V., Kolbina O.N., Mokryak A.V. 2023. No.11 (137)
4. Safonova T.V., Kolbina O.N., Yagotintseva N.V., Mokryak A.V. The use of multi-agent systems in forestry IOP Conference Series: Earth and Environmental Science. № 806 (2021) 012028

5. Kolbina O.N., Istomin E.P., Yagotintseva N.V. Kalambet M.V. Features of creating a database for the IoT system of urban forest management in St. Petersburg. IOP Conference Series: Earth and Environmental Science, 2021, № 876(1), 012039
6. The Internet of Things in agriculture (Agriculture IoT / AIoT): world experience, application cases and the economic effect of implementation in the Russian Federation // Analytical report. – J'son & Partners Consulting, 2017 [Electronic resource]. – URL: http://json.tv/ict_telecom_analytics_view/internet-veschey-v-selskom-hozyaystve-agriculture-iot-aiot-mirovoy-opyt-keysy-primeneniya-i-ekonomicheskiy-effekt-ot-vnedreniya-v-rf-20170621045316.
7. Safonova T.V., Yagotintseva N.V., Kolbina O.N., Mokryak A.V. The concept of the development of the Internet of Things information technologies: management, economics and transport law. 2022. No.2(42). p.4
8. Safonova T.V., Kolbina O.N., Yagotintseva N.V., Mokryak A.V. Control and monitoring of environmental safety International Scientific Research Journal 54-1 (119). 2022. pp. 115-119.
9. Vershinin A.K., Safonova T.V., Russkin V.D., Loginov I.S., Yasnikov A.I. Internet of Things in agriculture Information technologies and systems: management, economics, transport, law. 2023. No. 1 (45). pp. 28-34.
10. Tikki D.A., Nikolsky V.E., Avakian E.V., Samoshkin N.S., Safonova T.V. Overview of the application of sensor sensors in industry Information technologies and systems: management, economics, transport, law. 2023. No. 2 (46). pp. 29-36.
11. Tikki D.A., Safonova T.V., Ruskin V.D. Digital twins in agriculture Information technologies and systems: management, economics, transport, law. 2022. No. 4 (44). pp. 49-53.

Мерзлякова Е.Ю. Стеганографический метод BCES встраивания информации в растровые файлы// Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 6(44) с. 129–136

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056.55

СТЕГАНОГРАФИЧЕСКИЙ МЕТОД BCES ВСТРАИВАНИЯ ИНФОРМАЦИИ В РАСТРОВЫЕ ФАЙЛЫ

Мерзлякова Е.Ю.
ФГБОУ ВО "СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ", Новосибирск, Россия, (630102, Новосибирская область, город Новосибирск, ул. Кирова, д. 86), e-mail: katerina.artist@yandex.ru

Представлен стеганографический метод встраивания информации в файлы формата bmp на основе алгоритма интерполяции изображений. Выполнен анализ разработанного метода BCES по разностным показателям искажения и проведено сравнение с похожими методами. Рассмотренный стегометод BCES имеет ёмкость 0.5 bpp и может применяться в области защиты пользовательских данных.

Ключевые слова: Стеганография, цифровые изображения, встраивание информации, интерполяция, искажения.

THE BCES STEGANOGRAPHIC METHOD OF EMBEDDING INFORMATION IN RASTER FILES

Merzlyakova E.Yu.
SIBERIAN STATE UNIVERSITY OF TELECOMMUNICATIONS AND INFORMATICS, Novosibirsk, Russia, (630102, Novosibirsk region, Novosibirsk, Kirova street, 86), e-mail: katerina.artist@yandex.ru

Steganographic method for embedding information into bmp files based on an image interpolation algorithm is presented. The developed BCES method was analyzed using difference distortion indicators and compared with similar methods. The considered BCES stegomethod has capacity of 0.5 bpp and can be used in the field of protecting user data.

Keywords: Steganography, digital images, information embedding, interpolation, distortion.

Введение

Стеганография цифровых изображений является отдельной актуальной областью исследований в компьютерной стеганографии. Роль контейнера, в который встраивается информация, часто выполняют растровые файлы. Особенность таких файлов том, что можно легко заменить младшие биты без видимых искажений изображения. На данной особенности основано большинство стеганографических алгоритмов [1]. С целью улучшения безопасности в таких стегосистемах применяют также криптографические алгоритмы защиты информации [2], а для повышения качества контейнера часто используются методы интерполяции [3-8], что позволяет затем восстановить исходный (cover) контейнер. Для оценки качества стегосистем, в том числе основанных на интерполяции, используют два основных показателя: объем встроенной информации (BPP) и мера искажения изображения, выраженная в максимальном

(пиковом) соотношении сигнала к шуму (PSNR). Также иногда применяются показатель искажений (AD) и качества (IF). Цель представленной работы состоит в том, чтобы разработать метод встраивания информации в контейнеры формата bmp, применяя алгоритм интерполяции, а также исследовать полученную стегосистему в отношении возникающих искажений при встраивании.

Разработка и реализация метода BCES

Рассмотрим исходный контейнер *C*, представляющий собой 8-битный файл формата bmp размером 225 точек по высоте и 225 по ширине. Каждой точке соответствуют значения яркостей RGB — красного (R), зелёного (G) и синего (B) цвета. Для экспериментов при разработке стеганографических методов встраивания информации в изображения обычно используют изображения в градациях серого, когда каждый пиксель имеет равные значения яркостей для всех составляющих. Также полученные результаты действительны и для других схожих форматов с неискажающими методами сжатия, например png.

Применение метода интерполяции позволяет увеличить исходный контейнер *C*, добавив в него дополнительные пиксели, которые удобно использовать для встраивания данных. В методе BCES изображение увеличивается по строкам и столбцам посредством интерполяции Лагранжа, как наиболее оптимального метода получения контейнера для встраивания с использованием алгоритмов интерполяции [9]. Таким образом, размер интерполированного контейнера в данном случае составит 450 на 450 пикселей, то есть увеличится в 2 раза по сравнению с исходным. Информация будет записываться только в интерполированные значения, поэтому мы всегда можем восстановить исходное изображение *C*. Контейнер, полученный в результате работы стегометода называется стегоконтейнером *S*.

В качестве сообщения для встраивания используется двоичная псевдослучайная последовательность. Предполагается, что для повышения защиты встраиваемой информации будет использован секретный ключ, полученный, например, с помощью шифра Вернама.

Итак, возьмем интерполированный контейнер и рассмотрим значения пикселей как точки некоторой кривой. Воспользуемся формулой кривой Безье [10], чтобы построить более гладкую кривую по заданным точкам изображения. Оптимально использовать 5 точек для построения кривой по формуле (1):

$$P(t) = \sum_{i=0}^{n} P_i \cdot \frac{n!}{i!(n-1)!} \cdot (1-t)^{n-i} \cdot t^i, \quad (1)$$

n=4 для пяти точек, i – номер опорной точки;

$P(t)$ – ордината опорной точки кривой Безье;

P_i – значение цвета пикселя изображения,

$t \in [0,1]$ – заданный шаг.

Таким образом, будем рассматривать значения точек контейнера блоками по 5 пикселей, соответственно формуле (1). В каждом таком блоке три пикселя являются оригинальными опорными точками интерполяции и составляют исходную матрицу изображения до ее увеличения. Остальные точки каждого блока вычислены по алгоритму интерполяции и могут быть заменены на другие значения точек построенной кривой. Количество всевозможных точек регулируется параметром *t*, который может принимать значения 0,1 или меньше. Если мы хотим получить больше точек, то соответственно, нужно задать меньшее значение *t*. В итоге значения точек кривой в каждом блоке из пяти точек вычисляются по формуле (2):

$$P = (1-t)^4 \cdot P_0 + 4 \cdot (1-t)^3 \cdot t \cdot P_1 + 6 \cdot (1-t)^2 \cdot t^2 \cdot P_2 + 4 \cdot (1-t) \cdot t^3 \cdot P_3 + t^4 \cdot P_4. \quad (2)$$

Так как точки изображения рассматриваются подобно непрерывному сигналу, то каждая последняя точка P_4 в блоке должна являться первой точкой P_0 следующего блока.

Рассмотрим более подробно реализацию алгоритма встраивания BCES (Bezier Curves Embedding Strategy). Интерполированный контейнер рассматривается блоками из пяти значений яркости пикселей: $(P_0, P_1, P_2, P_3, P_4)$, где точки P_0, P_2, P_4 являются значениями точек исходного изображения *C*, а значения P_1 и P_3 являются добавленными точками соответственно выбранному алгоритму интерполяции. Обозначим значения точек кривой Безье, вычисленных между P_0 и P_2 множеством $R_1 = \{r_1, \dots, r_k\}$, а между P_2 и P_4 – множеством $R_3 = \{r_1, \dots, r_k\}$, где k – это количество значений при данном шаге t. Если рассматривать график кривой, проходящей от точки P_0 до точки P_4, то количество отрезков на ней и является значением k, исключая первый и последний отрезок, а также два отрезка, которые окружают значение кривой, соответствующей P_2. Таким образом, k вычисляется по следующей формуле:

$$k = \frac{1}{2 \cdot t} - 1, \quad (3)$$

Множество значений из R_1 будут использованы для замены значения точки P_1, а множество значений из R_3 соответственно для замены P_3. Значения точек кривой, соответствующие P_0, P_2 и P_4 не используются для замены значений P_1 и P_3, так как они являются пикселями изображения *C*. Если встраивать один бит информации в каждую подходящую точку изображения, то в данном алгоритме количество встроенных бит составит половину от общего числа точек всего изображения *S*, так как рассматриваемые блоки точек пересекаются в крайнем их значении.

Рассмотрим график кривой Безье, построенной по усредненным значениям яркостей пикселей с шагом t=0.1 (Рисунок 1):

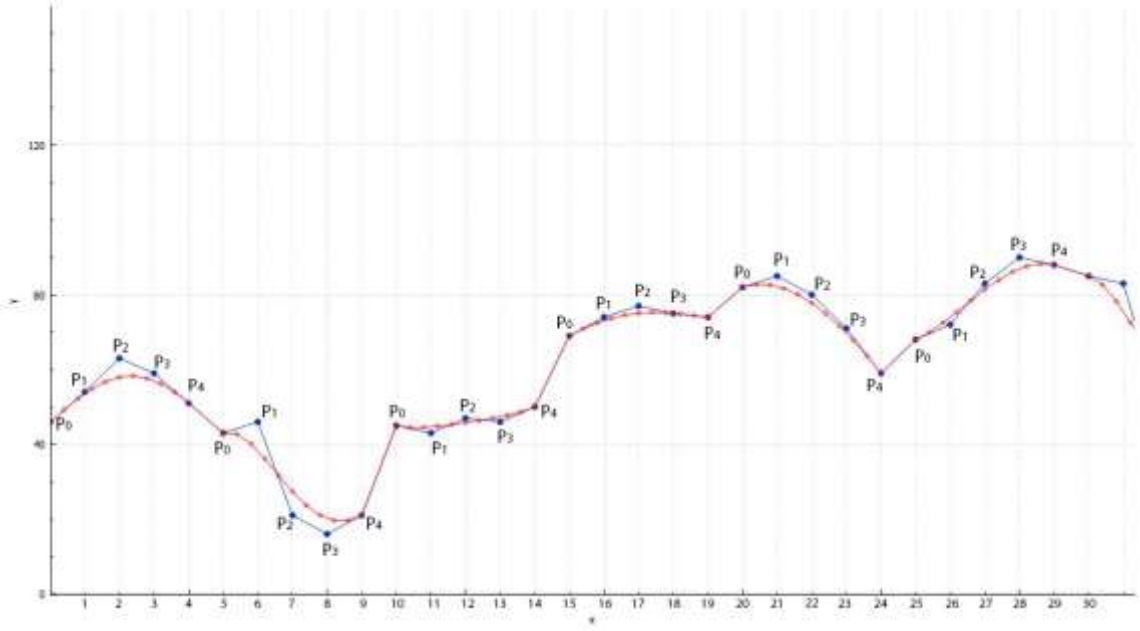


Рисунок 1 – Построение кривой Безье растрового файла с шагом t=0.1

По оси Y находятся значения яркостей точек одной из строк изображения *S*. По Оси X показан порядковый номер точек. Для наглядности в данном примере был взят шаг t=0.1. По

графику видно, что на каждые 5 точек яркостей интерполированной картинки (синяя линия), мы имеем 11 точек кривой Безье (красная линия).

Биты информации записываются в P_1 и в P_3 путем взятия такого значения с кривой Безье, у которого младший бит будет равен встраиваемому биту сообщения. При этом, нужно обратить внимание на шаг *t*, обеспечив достаточный выбор значений R_1 и R_3 для замены P_1 и P_3. Например, при *t*=0.05 для точки P_1 имеется выбор уже из 9 значений точек кривой Безье, которые можно использовать, округлив их до целого значения, и для точки P_3 аналогично.

В связи с необходимостью округлять полученные значения точек на кривой, возникает проблема возникновения ситуации, когда значения оказываются равными, что сокращает выбор для замены P_1 и P_3, а также есть вероятность того, что из всех возможных значений множества R_1 или R_3 не окажется ни одного подходящего. Очевидно, проблема будет возникать в изображениях, имеющих однотонные области. Поэтому рекомендуется выбирать более шумные фотографии в качестве контейнера, применяя дополнительно предварительные тесты на пригодность изображения *C*, а также устанавливать шаг *t* =0.01.

Для того чтобы извлечь встроенное сообщение из контейнера S, необходимо выделить интерполированные значения и получить их младшие биты. Предполагается, что применяемый алгоритм интерполяции заранее известен, так же как и метод встраивания.

Интерполированное изображение размером 450 точек по ширине и 450 точек по высоте позволяет использовать по 112 пересекающихся блоков в каждой строке матрицы пикселей. Таким образом, общее количество блоков для тестовых 8-битных изображений заданного размера составит 50400. Изменяя в каждом блоке по 2 пикселя, мы модифицируем около 50% младших бит изображения. Максимальное количество встроенных бит в изображение размером *W* по ширине и *H* по высоте равно:

$$N = 2 \cdot \lfloor {}^{W}/_{4} \rfloor \cdot H \qquad (4)$$

Таким образом, при правильно подобранных контейнерах с шагом *t* =0.01 максимальная ёмкость встраивания информации методом BCES составит 0.5 бит/пиксель.

Анализ метода BCES

Проанализируем разработанный стеганографический протокол. Для экспериментов возьмем набор из растровых 8-битных изображений размером 225 на 225 в градациях серого, с отсутствием однотонных областей пикселей. После применения интерполяции Лагранжа получим соответствующий набор изображений размером 450 на 450 и встроим случайную последовательность бит методом BCES при *t*=0.01 с заполнением 0.5 бит/пиксель.

Пусть E – это пустой интерполированный контейнер, S – соответствующий заполненный контейнер. Количество встроенных бит 100800. Определим значения разностных показателей визуального искажения [11] для пяти пар контейнеров:

Таблица 1 – Значения разностных показателей искажения

E	S	PSNR	IF	AD
		48.74	0.99	2.04
		48.91	1	1.37
		48.67	1	2.03
		48,99	1	2,79
		48,9	1	2,55

Показатели визуального искажения, использованные в Таблице 1, основаны на анализе пиксельной структуры контейнера и являются наиболее применяемыми в стеганографии изображений. Далее рассмотрим, как вычисляют и интерпретируют данные показатели.

Максимальное соотношение сигнал/шум (PSNR):

$\mathrm{PSNR} = 10 * \log\frac{255^2}{\varepsilon}$, где $\varepsilon = \frac{1}{MN}\sum_{i=0}^{M}\sum_{j=0}^{N}(S(i,j) - I(i,j))^2$, M, N – высота и ширина изображения соответственно.

Показатель PSNR часто используется в стеганографии для оценки качества полученных контейнеров [3, 7, 9, 12] и измеряется в зрительных децибелах (Вдб). Здесь Ɛ – это искажение. Чем больше значение PSNR, тем меньше расхождений между сравниваемыми изображениями. Качество обработки изображений считается высоким, если PSNR≥40 дБ для 8-битных изображений [13]. Так, в работе [7] рассмотрен метод встраивания на основе интерполяции, имеющий в среднем BPP=1,8 при PSNR=35,67, который является лучшим среди предложенных в работах подобных методов [3-5, 14-16].

Индекс качества изображения (IF):

$$\mathrm{IF} = 1 - \sum_{x,y}(C_{x,y} - S_{x,y})^2 / \sum_{x,y}(C_{x,y})^2.$$

Чем ближе данный индекс к 1, тем лучше качество модифицированного изображения по отношению к оригиналу.

Средняя абсолютная разность (AD):

$$\mathrm{AD} = \frac{1}{XY} \cdot \sum_{x,y} \left| C_{x,y} - S_{x,y} \right|$$

Низкое значение AD свидетельствует о низком уровне искажений в стегоизображении. Так, предложенный в работе [2] LSB-метод позволил снизить значение AD с 3.45 до 1.85.

Исходя из результатов экспериментов, приведенных в Таблице 1, можно утверждать, что искажения, вносимые стегопреобразованиями по методу BCES являются незначительными и сравнимы с показателями существующих подобных актуальных методов. Существующие стеганографические подходы, основанные на интерполяции, позволяют достигнуть приемлемого уровня PSNR при достаточно высоких показателях BPP. Предложенный в данной статье алгоритм имеет лучшие показатели качества, но уступает в ёмкости встраивания информации в контейнер. Дальнейшее увеличение показателя BPP метода BCES может быть легко достигнуто при использовании методов сжатия сообщений [17]. Таким образом, стегосистема BCES может успешно применяться в области защиты конфиденциальных данных и авторских прав.

Список литературы

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. Москва : СОЛОН-ПРЕСС, 2017. – 262 с.
2. Tutuncu, Kemal & çataltaş, Özcan. (2021). Compensation of degradation, security, and capacity of LSB substitution methods by a new proposed hybrid n-LSB approach. Computer Science and Information Systems. 18. 1311-1332. 10.2298/CSIS210227048T.
3. Jung K. H., Yoo K. Y. Data hiding method using image interpolation//Comput Stand Interfaces, 2009. V. 31, iss.2. pp. 465-470.

4. Lee C-F, Huang Y-L. An efficient image interpolation increasing payload in reversible data hiding//Expert Syst Appl. 2012. V. 39, iss.8. pp. 6712-6719.
5. Ahmad A. M., Ali A. H., Mahmoud F. An improved capacity data hiding technique based on image interpolation//Multimed Tools Appl. 2019. V.78, iss.6. pp. 7181-7205.
6. Нагиева А. Ф., Вердиев С. Г. Реверсивный стеганографический метод сокрытия информации, основанный на интерполяции изображений//Компьютерная оптика. 2022. – Т. 46, № 3. С. 465-472.
7. Mahasree M. Improved Reversible Data Hiding in Medical images using Interpolation and Threshold based Embedding Strategy//International Journal of Emerging Trends in Engineering Research. V. 8, 2020. pp. 3495-3501
8. Lu Tzu-Chuen, Huang Shi-Ru, Huang Shu-Wen Reversible hiding method for interpolation images featuring a multilayer center folding strategy//Soft Computing. V. 25, iss.7. 2021. pp.161-180.
9. Евсютин О. О., Кокурина А. С., Мещеряков Р. В. Алгоритмы встраивания информации в цифровые изображения с применением интерполяции//Доклады Томского государственного университета систем управления и радиоэлектроники. 2015. № 4(38). С. 108-112.
10. Bézier, P.E. Numerical Control-Mathematics and applications. London: John Wiley and Sons, 1972. p.240
11. Коханович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006, 288 с.
12. Kumar, Neeraj & Kumar, Rajeev & Malik, Aruna & Singh, Samayveer & Jung, Ki-Hyun. (2023). Reversible data hiding with high visual quality using pairwise PVO and PEE. Multimedia Tools and Applications. 82. 1-26. 10.1007/s11042-023-14867-3.
13. Kumari, Lalitha & Ramanathan, Pandian & Rani, J. & Vinothkumar, D. & Sneha, Adeline & Amalarani, V. & S, Bestley. (2017). Selection of optimum compression algorithms based on the characterization on feasibility for medical image. Biomedical Research (India). 28. . pp. 5633-5637.
14. Tang, Mingwei & Hu, Jie & Song, Wen. (2014). A high capacity image steganography using multi-layer embedding. Optik - International Journal for Light and Electron Optics. 125. 3972–3976. 10.1016/j.ijleo.2014.01.149
15. Hu, Jie and Tianrui Li. “Reversible steganography using extended image interpolation technique.” *Comput. Electr. Eng.* 46 (2015): pp.447-455
16. T. Lu. An interpolation-based lossless hiding scheme based on message recoding mechanism, Optik, Elsevier, Vol. 130, pp. 1377-1396, 2017
17. Shanmugasundaram S., Lourdusamy R.: A Comparative Study Of Text Compression Algorithms. International Journal of Wisdom Based Computing. 1 (2011) pp.68-76.

References

1. Gribunin V. G., Okov I. N., Turintsev I. V. Digital steganography. Moscow : SOLON-PRESS, 2017. – p.262
2. Tutuncu, Kemal & çataltaş, Özcan. (2021). Compensation of degradation, security, and capacity of LSB substitution methods by a new proposed hybrid n-LSB approach. Computer Science and Information Systems. 18. 1311-1332. 10.2298/CSIS210227048T.

3. Jung K. H., Yoo K. Y. Data hiding method using image interpolation // Comput Stand Interfaces, 2009. V. 31, iss.2. pp. 465-470.
4. Lee C-F, Huang Y-L. An efficient image interpolation increasing payload in reversible data hiding // Expert Syst Appl. 2012. V. 39, iss.8. pp. 6712-6719.
5. Ahmad A. M., Ali A. H., Mahmoud F. An improved capacity data hiding technique based on image interpolation // Multimed Tools Appl. 2019. V.78, iss.6. pp. 7181-7205.
6. Nagieva A. F., Verdiev S. G. A reversible steganographic method of information concealment based on image interpolation // Computer Optics. 2022. – vol. 46, No. 3. pp. 465-472.
7. Mahasree M. Improved Reversible Data Hiding in Medical images using Interpolation and Threshold based Embedding Strategy // International Journal of Emerging Trends in Engineering Research. V. 8, 2020. pp. 3495-3501
8. Lu Tzu-Chuen, Huang Shi-Ru, Huang Shu-Wen Reversible hiding method for interpolation images featuring a multilayer center folding strategy // Soft Computing. V. 25, iss.7. 2021. pp. 161-180.
9. Evsyutin O. O., Kokurina A. S., Meshcheryakov R. V. Algorithms for embedding information into digital images using interpolation // Reports of the Tomsk State University of Control Systems and Radioelectronics. 2015. No. 4(38). pp. 108-112.
10. Bézier, P.E. Numerical Control-Mathematics and applications. London: John Wiley and Sons, pp.1972. 240
11. Kokhanovich G.F., Puzyrenko A.Yu. Computer steganography. Theory and practice. K.: MK-Press, 2006, pp.288
12. Kumar, Neeraj & Kumar, Rajeev & Malik, Aruna & Singh, Samayveer & Jung, Ki-Hyun. (2023). Reversible data hiding with high visual quality using pairwise PVO and PEE. Multimedia Tools and Applications. 82. 1-26. 10.1007/s11042-023-14867-3.
13. Kumari, Lalitha & Ramanathan, Pandian & Rani, J. & Vinothkumar, D. & Sneha, Adeline & Amalarani, V. & S, Bestley. (2017). Selection of optimum compression algorithms based on the characterization on feasibility for medical image. Biomedical Research (India). 28. pp.5633-5637.
14. Tang, Mingwei & Hu, Jie & Song, Wen. (2014). A high capacity image steganography using multi-layer embedding. Optik - International Journal for Light and Electron Optics. 125. 3972–3976. 10.1016/j.ijleo.2014.01.149
15. Hu, Jie and Tianrui Li. “Reversible steganography using extended image interpolation technique.” Comput. Electr. Eng. 46 (2015): pp. 447-455
16. T. Lu. An interpolation-based lossless hiding scheme based on message recoding mechanism, Optik, Elsevier, Vol. 130, pp. 1377-1396, 2017
17. Shanmugasundaram S., Lourdusamy R.: A Comparative Study Of Text Compression Algorithms. International Journal of Wisdom Based Computing. 1 (2011) pp.68-76.

Сафонова Т.В. и др. Тенденции развития умного сельского хозяйства/Сафонова Т.В., Мокряк А.В., Муленко М.Д., Лескова Д.О., Осина Д.А // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 6(44) с. 137–144

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.9

ТЕНДЕНЦИИ РАЗВИТИЯ УМНОГО СЕЛЬСКОГО ХОЗЯЙСТВА

Сафонова Т.В., [1]Мокряк А.В., Муленко М.Д., Лескова Д.О., Осина Д.А.,
ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ" Санкт-Петербург, Россия (192007, город Санкт-Петербург, Воронежская ул., д. 79)
[1]ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ ГОСУДАРСТВЕННОЙ ПРОТИВОПОЖАРНОЙ СЛУЖБЫ МИНИСТЕРСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ ИМЕНИ ГЕРОЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ГЕНЕРАЛА АРМИИ Е.Н.ЗИНИЧЕВА", Санкт-Петербург, Россия (196105, г.Санкт-Петербург, Московский проспект, д.149), e-mail: mokryakanna@mail.ru

Тенденции развития умного сельского хозяйства включают в себя автоматизацию процессов, использование датчиков для мониторинга почвы и растений, внедрение технологий Интернета вещей для управления ресурсами, а также применение аналитики данных и искусственного интеллекта для оптимизации производства. Также важными являются развитие технологий дронов и робототехники для выполнения различных задач на поле. Эти тенденции направлены на увеличение эффективности, уменьшение затрат и повышение устойчивости сельского хозяйства. В данной статье изучается использование инновационных технологий интернета вещей в агропромышленном комплексе на основе приведенных примеров из разных стран. Рассматриваются передовые средства автоматизации исследуемой области. Технологии интернета вещей уже применяются фермерами в различных сферах, таких как профилактика заболеваний культур и животных, повышение урожайности и управление поливом.

Ключевые слова: Технология интернета вещей, сенсорные датчики, гидрометеорологические параметры

TRENDS IN THE DEVELOPMENT OF SMART AGRICULTURE

Safonova T.V., [1]Mokryak A.V., Mulenko M.D., Leskova D.O., Osina D.A.
RUSSIAN STATE HYDROMETEOROLOGICAL UNIVERSITY, St. Petersburg, Russia (192007, St. Petersburg, Voronezhskaya str., 79)
[1]ST. PETERSBURG UNIVERSITY OF THE STATE FIRE SERVICE OF THE MINISTRY OF THE RUSSIAN FEDERATION FOR CIVIL DEFENSE, EMERGENCIES AND ELIMINATION OF CONSEQUENCES OF NATURAL DISASTERS NAMED AFTER THE HERO OF THE RUSSIAN FEDERATION, GENERAL OF THE ARMY E.N. ZINICHEV, St. Petersburg, Russia (196105, St. Petersburg, Moskovsky prospekt,149), e-mail: [1]mokryakanna@mail.ru

Trends in smart agriculture include process automation, the use of sensors to monitor soil and plants, the introduction of IoT technologies for resource management, and the use of data analytics and artificial intelligence to optimise production. Also important are the development of drone technology and robotics to perform various tasks in the field. These trends aim to increase efficiency, reduce costs, and improve the sustainability of

agriculture. This paper explores the use of innovative Internet of Things technologies in agribusiness through case studies from different countries. The advanced automation tools of the study area are reviewed. IoT technologies are already being used by farmers in various areas such as crop and animal disease prevention, crop yield improvement and irrigation management.

Keywords: Internet of things technology, touch sensors, hydrometeorological parameters.

Введение

Агропромышленный комплекс играет ключевую роль в экономике страны, предоставляя продовольствие для населения и сырье для различных отраслей, тем самым поддерживая уровень продовольственной безопасности страны на высоком уровне. По всему миру более миллиарда специалистов заняты в данной отрасли. Начавшееся приблизительно 10 000 лет назад, сельское хозяйство стало одним из важнейших толчков для последующей эволюции цивилизации.

На сегодняшний день агропромышленный сектор является наиболее важной отраслью, так как обеспечивает продовольствием население всего мира. Стоит отметить, что через 30 лет потребуется на 70% больше объема продовольствия, чем в настоящее время [1]. Уменьшение плодородных земель, преобразование климатических показателей и высокие цены на энергоносители представляют серьезные препятствия для увеличения производительности и обеспечения населения сельскохозяйственной продукцией. Поэтому важными задачами являются повышение урожайности сельскохозяйственных культур и снижение издержек в современных условиях функционирования предприятий.

Для достижения данной цели требуется внедрить новый подход к сельскому хозяйству, который подразумевает использование интеллектуальных инструментов для развития аграрного сектора [2]. Эта концепция основана на использовании автоматизированных систем принятия решений, комплексной автоматизации и роботизации производственных процессов, а также использовании передовых технологий для моделирования экосистем.

В статье приведены примеры применения передовых технологий интеллектуального сельского хозяйства, которые демонстрируют возможность эффективной и экологически безопасной борьбы с вредителями, восстановления и сохранения плодородия почв и грунтовых вод, а также дистанционного контроля соблюдения сертификационных требований органического сельского хозяйства.

Предотвращение заболеваний

Сегодня информационные системы в сельском хозяйстве, применение которых казалось невозможным несколько поколений назад, активно применяются для управления растениеводством. Например, в области интеллектуального сельского хозяйства потенциал сенсорных датчиков открывают новые возможности для решения наболевших проблем.

Болезни и вредители негативно влияют на производство зерновых культур, причиняя значительный экономический ущерб. Традиционные методы лечения, к сожалению, требуют дополнительных затрат и часто оказываются неэффективными [3]. Однако использование сенсорных датчиков помогает улучшить сложившуюся ситуацию. Анализ данных, полученных с датчиков, позволяет расширить возможности систем прогнозирования заболеваний (Рисунок 1).

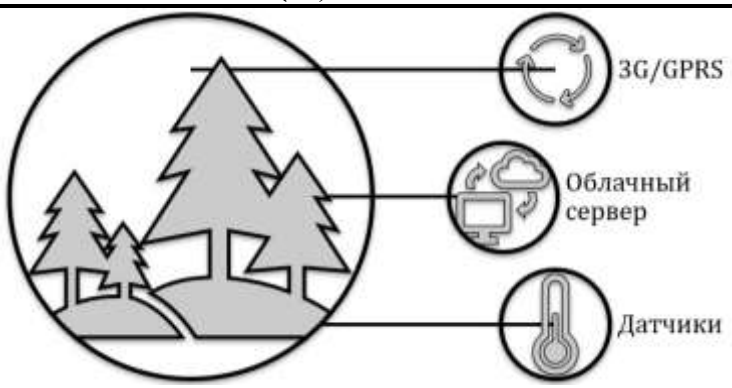


Рисунок 1 – Схема контроля параметров растительности для предотвращения заболеваний

Контроль параметров растительности позволяет эффективно бороться с вредителями и обеспечивать оптимальное орошение в нужное время, что способствует улучшению регулированием, росту качества аграрной продукции и уменьшению расходов. Путем мониторинга и анализа гидрометеорологических показателей, таких как температура, влажность воздуха, показатель эвапотранспирации и количество осадков, можно спрогнозировать появление опасных заболеваний [4, 5]. Также можно предложить своевременные целевые процедуры для поддержания здоровья сельскохозяйственных культур.

Специалисты и производители аграрного сектора могут адаптировать свои действия в соответствии с текущей обстановкой на местности благодаря системам контроля и анализа гидрометеорологических показателей. Эти системы генерируют уведомления с прогнозами фенологических событий, что позволяет производителям подготовиться к проведению инсектицидных мероприятий в нужное время. Использование таких инновационных платформ приносит ряд достоинств для фермеров, включая минимизацию времени, денег и ресурсов, а также снижение воздействия на окружающую среду за счет минимизации токсичных распылений [6]. Кроме того, они могут предупреждать фермеров о засухе на сельскохозяйственных территориях и других условиях, требующих внимания. Пользователи могут формировать отчетную документацию о техническом обслуживании оборудования и погоде, а также получать доступ к системе непосредственно с сельскохозяйственных полей.

Умная платформа по контролю сельскохозяйственных полей

Для таких систем часто используется инновационная платформа с сенсорными датчиками Waspmote Plug & Sense! от компании Libelium из Испании. Выбор данной платформы обусловлен ее доступностью по цене по сравнению с обычными метеостанциями, универсальностью программного кода и гибкостью в эксплуатации.

Платформа Waspmote Plug &Sense! предлагает клиентам решение для отслеживания погодных условий на конкретном участке сельскохозяйственного поля, что дает возможность в онлайн режиме отслеживать текущую ситуацию. Датчики собирают корректную информацию о таких ключевых показателях, как температура окружающей среды, влажность, количество осадков, атмосферное давление, направление и скорость ветра, влажность почвы и листьев.

Проанализированные параметры имеют большое значение для определения климатических особенностей региона и контроля текущего состояния окружающей среды.

Платформы с сенсорными датчиками размещаются в точках, где гидрометеорологическая информация недоступна из-за отсутствия метеостанций. В комплект платформы входит солнечная панель, обеспечивающая более длительное автономное питание метео-устройств [7].

Платформы Waspmote Plug & Sense! могут быть подключены к шлюзам Meshlium, которые получают данные от всех беспроводных устройств и отправляют их в облачную систему, или напрямую к облачным сервисам с использованием 4G или LoRaWAN. В облачной среде информация обрабатывается, и на основе предоставленных данных формируются управленческие решения по реализации сельскохозяйственных работ.

Удобное развёртывание узлов с датчиками способствует снижению стоимости интеллектуального решения, подходящего для маленьких хозяйств и масштабного производства [8]. Данная система окажется полезной для специалистов, борющихся с вредителями и болезнями и стремящихся оптимизировать график опрыскивания сельскохозяйственных культур. В отдельных случаях экономия на опрыскивании может достигать 20–30%.

Рост урожайности сельскохозяйственной продукции

Растения в теплице чрезвычайно восприимчивы к двум главным параметрам: температура воздуха (от посева до сбора урожая) и объема воды для полива (это особенно значимо в первые месяцы после посадки и перед сбором урожая). Оба фактора должны быть в оптимальных пределах, чтобы предотвратить потерю урожая, которая может доходить до 80% из-за появления деформированных, повреждённых растений и небольших плодов. Специалистам требуется знать, как меняются температура в теплице и уровень влажности почвы в течение суток, чтобы регулировать температуру и обеспечивать достаточное количество воды.

Решение этой задачи упрощается благодаря платформе Libelium Waspmote, в особенности стоит отметить модуль Waspmote Plug & Sense! Smart Agriculture. Используя специализированные датчики измерения температуры и влажности почвенного покрова, которые располагаются рядом с растениями, можно непрерывно отслеживать урожайность сельскохозяйственных культур. Фермер может быстро проверить текущее состояние растений через смартфон и принимать оповещения при достижении критических значений [9, 10]. Несмотря на то, что система окупается в течение нескольких лет, фермеры сразу получают ряд преимуществ:

- экономия времени: им не требуется ежедневно (или даже еженедельно) посещать поле для мониторинга состояния урожайности культур.
- уверенность в результатах: решения основаны на актуальных данных, которые извлекаются и предоставляются в режиме реального времени.
- экономия средств: минимизация ежедневного предоставления воды на 30% после посадки и на 15% во время сбора урожая зерновых культур и т.д.
- уменьшение потерь сельскохозяйственной продукции: предотвращение деформации, повреждений растений и т.д.

- высокие стандарты качества: рост лояльности потребителей и возможность продажи продукции по одной цене на протяжении всего периода уборки.

Анализ гидрометеорологических параметров имеет главное значение для сельскохозяйственных культур, выращиваемых на открытых пространствах. Избыточная влажность почвы, дефицит кислорода в земле, повышенная влажность воздуха, отрицательные температуры и недостаточное освещение негативно влияют на развитие и увеличивает риск заболеваний и атак вредителей [11]. В зимний период опасность возникновения болезней возрастает, поэтому необходимо применять подходящие минеральные удобрения и внимательно следить за этим процессом. Благодаря современным технологиям можно точнее определять моменты, когда действительно требуется применение минеральных удобрений.

Один из вариантов решения – это отслеживание состояния деревьев и растений с помощью специализированных датчиков, подсоединенных к Waspmote Plug & Sense! Smart Environment (Рисунок 1).

Рисунок 2 – Размещение сенсорных датчиков по сбору гидрометеорологических данных

Набор Waspmote Plug & Sense! Smart Environment представляет возможность контролировать такие параметры как (Рисунок 3):

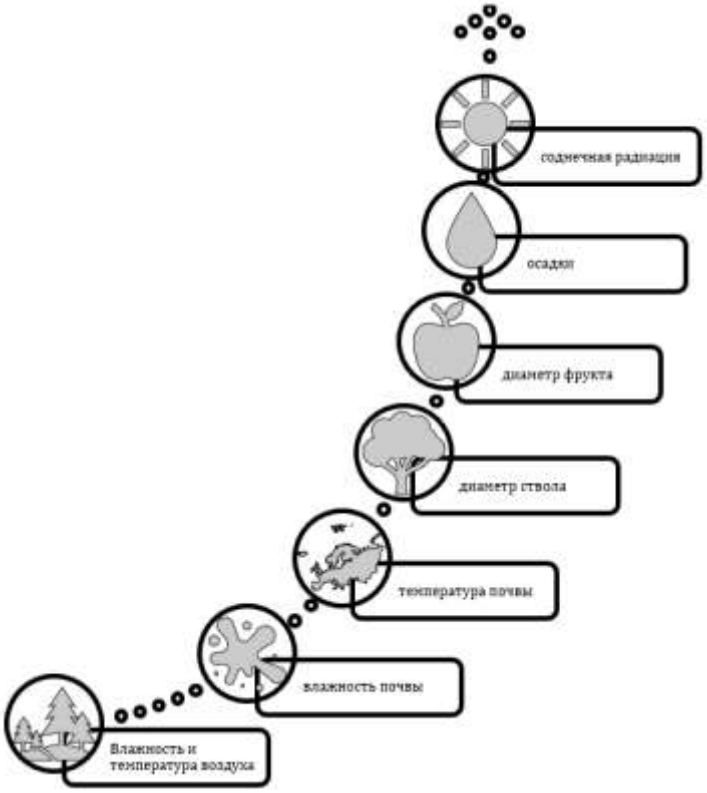


Рисунок 3 – Гидрометеорологические параметры, отслеживаемые системой Waspmote Plug & Sense! Smart Agriculture

Стоит отметить, что комплект Waspmote Plug & Sense! Smart Environment дает возможность контролировать уровень аммиака.

Отслеживание данных гидрометеорологических показателей позволяет удаленно контролировать окружающую среду и агрономические изменения. Это также помогает прогнозировать урожай, рационально расходовать водные ресурсы, предотвращать заболевания, сокращать количество применяемых удобрений и классифицировать типы почв в зависимости от климатических условий и выращиваемых культур [10, 11].

Ниже представлены достоинства, которые могут быть получены от внедрения исследуемой системы, а именно:

- повышение экологической и сельскохозяйственной устойчивости;
- поддержка стабильности урожайности сельскохозяйственных культу;
- контроль органических отходов;
- отслеживание сельскохозяйственных культур;
- обеспечение безопасности продукции.

Выводы

Современные технологии всё глубже проникают в агропромышленный сектор. Благодаря применению интеллектуальных сенсоров, беспроводных коммуникационных технологий и облачных сервисов улучшается качество мониторинга основных параметров, анализа данных и предоставления рекомендаций для снижения потерь и увеличения урожайности.

Новые технологии характеризуются относительно низкой стоимостью, небольшими затратами на установку и развертывание оборудования, легкостью внедрения и возможностью масштабирования проектов.

Контроль текущего состояния зерновых культур посредством использования сенсорных датчиков необходим для своевременного выявления проблем и принятия управленческих решений для их устранения. Это помогает повысить урожайность культур, снизить затраты на удобрения и средства защиты растений, что повысит качество зерна.

Список литературы

1. Precision Agriculture: Predicting Vineyard Conditions, Preventing Disease [Электронный ресурс] // Режим доступа : http://www.libelium.com/precision-agriculture-predicting-vineyard-conditions-preventing-disease/ (Дата обращения: 15.04.2024)
2. Smart Strawberries Crop Increases the Quality and Reduces the Time from Farm to Market [Электронный ресурс] // Режим доступа : http://www.libelium.com/smart-strawberries-crop-increases-the-quality-and-reduces-the-time-from-farm... http://www.libelium.com/precision-agriculture-predicting-vineyard-conditions-preventing-disease/ (Дата обращения: 15.04.2024)
3. Precision Farming to control irrigation and improve fertilization strategies on corn crops [Электронный ресурс] // Режим доступа: http://www.libelium.com/precision-farming-to-control-irrigation-and-improve-fertilization-strategies.... http://www.libelium.com/precision-agriculture-predicting-vineyard-conditions-preventing-disease/ (Дата обращения: 16.04.2024)
4. Smart Agriculture project for Organic Farms in UK [Электронный ресурс] // Режим доступа : http://www.libelium.com/smart-agriculture-project-for-organic-farms-in-uk/ (Дата обращения: 16.04.2024)
5. Reading Beehives: Smart Sensor Technology Monitors Bee Health and Global Pollination [Электронный ресурс] // Режим доступа: http://www.libelium.com/temperature-humidity-and-gases-monitoring-in-beehives/.http://www.libelium.com/precision-agriculture-predicting-vineyard-conditions-preventing-disease/ (Дата обращения: 17.04.2024)
6. Сафонова Т.В. Взаимодействие глобальной многофункциональной инфокоммуникационной спутниковой системы связи с объектами IoT в сельскохозяйственном производстве. Международный научно-исследовательский журнал/ Истомин Е.П., Яготинцева Н.В., Колбина О.Н., Мокряк А.В. 2023. №11 (137)
7. Сафонова Т.В., Яготинцева Н.В., Колбина О.Н., Мокряк А.В. Концепция развития интернета вещей информационные технологии: управление, экономика Транспортное право. 2022. №2 (42). С.4
8. Сафонова Т.В., Колбина О.Н., Яготинцева Н.В., Мокряк А.В. Контроль и мониторинг экологической безопасности окружающей среды Международный научно-исследовательский журнал 54-1 (119). 2022. С. 115-119.
9. Вершинин А.К., Сафонова Т.В., Русскин В.Д., Логинов И.С., Ясников А.И. Интернет вещей в сельском хозяйстве Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 1 (45). С. 28-34.
10. Тикки Д.А., Никольский В.Е., Авакян Е.В., Самошкин Н.С., Сафонова Т.В. Обзор

применения сенсорных датчиков в промышленности Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 2 (46). С. 29-36.

11. Тикки Д.А., Сафонова Т.В., Русскин В.Д. Цифровые двойники в сельском хозяйстве Информационные технологии и системы: управление, экономика, транспорт, право. 2022. № 4 (44). С. 49-53.

References

1. Precision Agriculture: Predicting Vineyard Conditions, Preventing Disease [Electronic resource] // Access mode : http://www.libelium.com/precision-agriculture-predicting-vineyard-conditions-preventing-disease / (Date of request: 04/15/2024)
2. Smart Strawberries Crop Increases the Quality and Reduces the Time from Farm to Market [Electronic resource] // Access mode : http://www.libelium.com/smart-strawberries-crop-increases-the-quality-and-reduces-the-time-from-farm... http://www.libelium.com/precision-agriculture-predicting-vineyard-conditions-preventing-disease / (Date of request: 04/15/2024)
3. Precision Farming to control irrigation and improve fertilization strategies on corn crops [Electronic resource] // Access mode: http://www.libelium.com/precision-farming-to-control-irrigation-and-improve-fertilization-strategies... . http://www.libelium.com/precision-agriculture-predicting-vineyard-conditions-preventing-disease / (Date of access: 04/16/2024)
4. Smart Agriculture project for Organic Farms in UK [Electronic resource] // Access mode : http://www.libelium.com/smart-agriculture-project-for-organic-farms-in-uk / (Date of access: 04/16/2024)
5. Reading Beehives: Smart Sensor Technology Monitors Bee Health and Global Pollination [Electronic resource] // Access mode: http://www.libelium.com/temperature-humidity-and-gases-monitoring-in-beehives /.http://www.libelium.com/precision-agriculture-predicting-vineyard-conditions-preventing-disease / (Date of access: 04/17/2024)
6. Safonova T.V. Interaction of the global multifunctional infocommunication satellite communication system with IoT objects in agricultural production. International Scientific Research Journal/ Istomin E.P., Yagotintseva N.V., Kolbina O.N., Mokryak A.V. 2023. No.11 (137)
7. Safonova T.V., Yagotintseva N.V., Kolbina O.N., Mokryak A.V. The concept of the development of the Internet of Things information technology: management, economics Transport law. 2022. No.2 (42). p.4
8. Safonova T.V., Kolbina O.N., Yagotintseva N.V., Mokryak A.V. Control and monitoring of environmental safety International Scientific Research Journal 54-1 (119). 2022. pp. 115-119.
9. Vershinin A.K., Safonova T.V., Russkin V.D., Loginov I.S., Yasnikov A.I. Internet of Things in agriculture Information technologies and systems: management, economics, transport, law. 2023. No. 1 (45). pp. 28-34.
10. Tikki D.A., Nikolsky V.E., Avakian E.V., Samoshkin N.S., Safonova T.V. Overview of the application of touch sensors in industry Information technologies and systems: management, economics, transport, law. 2023. No. 2 (46). pp. 29-36.
11. Tikki D.A., Safonova T.V., Ruskin V.D. Digital twins in agriculture Information technologies and systems: management, economics, transport, law. 2022. No. 4 (44). pp. 49-53.

Аклаева Я.Т., Коллеров В.И. Методика внедрения роботизированных процессов в нефтегазовых компаниях // Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 6(44) с. 145–148

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.9

МЕТОДИКА ВНЕДРЕНИЯ РОБОТИЗИРОВАННЫХ ПРОЦЕССОВ В НЕФТЕГАЗОВЫХ КОМПАНИЯХ

[1]Аклаева Я.Т., [2]Коллеров В.И.
ФГБОУ ВО "УФИМСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ (УГНТУ), Уфа, Россия (450064, Республика Башкортостан, город Уфа, ул. Космонавтов, д. 1), e-mail: [1]yana.aklaeva@mail.ru, [2]v.kollerov@icloud.com

В данной статье рассматриваются ключевые аспекты, а также выгоды и сложности внедрения роботизированных процессов в нефтегазовых компаниях.

Ключевые слова: Нефтегазовая компания, автоматизация, бизнес-процессы, роботизация процессов (RPA), автоматизированные решения, внедрение роботизированных процессов, преимущества роботизации, недостатки роботизации.

IMPLEMENTATION METHODOLOGY OF ROBOTIC PROCESSES IN OIL AND GAS COMPANIES

Aklaeva Ya.T., Kollerov V.I.
UFA STATE PETROLEUM TECHNOLOGICAL UNIVERSITY, Ufa, Russia (450064, Republic of Bashkortostan, Ufa, Kosmonavtov str., 1), e-mail: [1]yana.aklaeva@mail.ru, [2]v.kollerov@icloud.com

This article examines the key aspects, benefits, and challenges of implementing robotic processes in oil and gas companies

Keywords: Oil and gas company, automation, business processes, robotic process automation (RPA), automated solutions, implementation of robotic processes, advantages of robotics, disadvantages of robotics.

Нефтегазовая промышленность является одной из важнейших и наиболее технологически развитых отраслей мировой экономики. В современном мире она сталкивается с рядом вызовов, таких как волатильность цен на энергоносители, строгие требования к экологической безопасности, а также постоянное стремление к оптимизации операций и сокращению затрат.

В условиях таких вызовов внедрение роботизированных процессов представляется не только возможностью оптимизации бизнес-процессов, но и необходимым шагом для сохранения конкурентоспособности и эффективности компаний в данной отрасли.

Нефтегазовые компании оперируют сложными и масштабными бизнес-процессами, включающими в себя разведку, добычу, транспортировку и переработку углеводородов. Традиционно многие из этих процессов выполняются вручную или с минимальным участием автоматизации. Однако, с появлением новых технологий, таких как искусственный интеллект (ИИ), машинное обучение (МО), появляется возможность автоматизировать множество операций и задач [4].

Роботизированные процессы могут значительно повысить эффективность и точность выполнения операций, сократить временные и финансовые затраты, а также снизить риск возникновения человеческих ошибок. Кроме того, роботизация позволяет освободить человеческие ресурсы от рутинных и монотонных задач, что позволяет сотрудникам фокусироваться на более стратегически важных аспектах работы компании [2].

Ключевыми аспектами внедрения роботизированных процессов являются:

1. Анализ процессов. Первоначальный этап внедрения роботизированных процессов включает в себя детальный анализ текущих бизнес-процессов компании. Это позволяет выявить наиболее подходящие задачи и операции для автоматизации, а также определить потенциальные выгоды от внедрения роботизации;
2. Выбор технологий. После анализа процессов необходимо выбрать подходящие технологические решения для автоматизации. Это может включать в себя использование роботов-процессов (RPA), систем искусственного интеллекта для автоматического анализа данных и принятия решений, а также систем управления процессами (BPM) для координации и оптимизации бизнес-процессов;
3. Пилотные проекты. Рекомендуется начинать внедрение роботизированных процессов с пилотных проектов, которые позволяют оценить эффективность выбранных технологий и методов. Проведение пилотных проектов также позволяет выявить и устранить возможные проблемы и ограничения до масштабирования решения на всю компанию;
4. Обучение персонала. Внедрение роботизированных процессов требует не только технических знаний, но и изменения в культуре и методах работы компании. Поэтому важно обеспечить обучение сотрудников, которые будут работать с новыми системами, а также обучение технических специалистов, которые будут поддерживать и развивать автоматизированные процессы;
5. Масштабирование и оптимизация. После успешного завершения пилотных проектов и внедрения роботизированных процессов на определенных участках компании, необходимо масштабировать решения на всю организацию. При этом важно продолжать мониторинг и оптимизацию процессов, чтобы обеспечить их эффективную работу и соответствие стратегическим целям компании [5, 6].

Рассмотрим выгоды от внедрения роботизированных процессов:

- Повышение эффективности. Автоматизация повторяющихся задач позволяет сократить время и ресурсы, затрачиваемые на их выполнение, что ведет к увеличению общей производительности компании;
- Снижение затрат. Роботизированные процессы могут значительно снизить операционные затраты за счет уменьшения необходимости человеческого труда, сокращения ошибок и улучшения управления ресурсами;
- Улучшение качества. Автоматизация процессов позволяет снизить вероятность человеческих ошибок и повысить точность выполнения задач, что приводит к улучшению качества продукции и услуг [7];
- Ускорение принятия решений. Системы искусственного интеллекта могут анализировать большие объемы данных и предоставлять ценные инсайты для принятия стратегических решений быстрее и эффективнее, чем человеческие аналитики;

- Повышение гибкости. Роботизированные процессы позволяют легко масштабировать операции в зависимости от изменяющихся потребностей и условий рынка, что повышает гибкость и адаптивность компании к изменениям;
- Улучшение безопасности. Автоматизация опасных и рискованных операций может снизить риск производственных несчастных случаев и повысить общий уровень безопасности на предприятии [3].

Однако внедрение роботизированных процессов в нефтегазовых компаниях может столкнуться с рядом препятствий, включая:

- Некоторые сотрудники могут опасаться потерять свои рабочие места из-за автоматизации процессов. Важно провести адекватную коммуникацию и обучение персонала, чтобы преодолеть это препятствие;
- Нефтегазовые компании часто имеют сложные и уникальные процессы, что может затруднить внедрение роботизации. Важно тщательно анализировать и адаптировать технологические решения под специфику компании;
- Учитывая чувствительность данных в нефтегазовой отрасли, необходимо обеспечить высокий уровень безопасности информации при использовании роботизированных систем [1].

Таким образом, внедрение роботизированных процессов представляет собой важный шаг для современных нефтегазовых компаний, стремящихся повысить эффективность, снизить затраты и оставаться конкурентоспособными на рынке. Несмотря на определенные трудности и препятствия, правильно спланированное и реализованное внедрение роботизации может принести значительные выгоды как в краткосрочной, так и в долгосрочной перспективе.

Список литературы

1. Балашов П. Тенденции развития роботизации в РФ /П. Балашов//«Deloitte» conference of management. – 2022. – Т. 12, № 2. – С. 6–22.
2. Беломытцев И.О. Роботизированная автоматизация процессов (RPA)/И.О. Беломытцев//Инновационная наука. – 2021. – Вып. 1. – С. 17–19.
3. Левина А.И. Решения в области роботизации процессов для повышения эффективности процессного управления/А.И.Левина//Вестник Южного института менеджмента. – 2020. – Вып. 4. – С. 95–99.
4. Линник Ю.Н., Кирюхин М.А. Цифровые технологии в нефтегазовом комплексе//Вестник государственного университета управления. 2019. № 7. С. 37-40.
5. Одинцов Б.Е. Информационные системы управления эффективностью бизнеса: учебник и практикум для бакалавриата и магистратуры. - М.: Издательство Юрайт, 2015. - 206с.
6. Репин В. «Бизнес-процессы. Моделирование, внедрение, управление». - М.: МИФ, 2012. - 477 с.
7. Сайт центра роботизации и искусственного интеллекта. [Электронный ресурс]. – Режим доступа: https://rparussia.ru/rpa-solutions/ (Дата обращения: 01.04.2024).

References

1. Balashov, P. Trends in the Development of Robotics in the Russian Federation. «Deloitte» conference of management. 2022; 12(2): pp.6–22.

2. Belomytsev, I.O. Robotic Process Automation (RPA). Innovative Science. 2021; (1): pp.17–19.
3. Levina, A.I. Process Robotics Solutions to Enhance Process Management Efficiency. Bulletin of the Southern Institute of Management. 2020; 4: pp. 95–99.
4. Linnik, Yu.N., Kiryukhin, M.A. Digital Technologies in the Oil and Gas Industry // Bulletin of the State University of Management. 2019. No. 7. pp. 37-40.
5. Odintsov, B.E. Information Systems for Business Efficiency Management: Textbook and Workbook for Bachelor's and Master's Degrees. Moscow: Yurayt Publishing, 2015. p. 206
6. Repin, V. "Business Processes. Modeling, Implementation, Management". Moscow: MIF, 2012. p.477
7. Robotization and Artificial Intelligence Center Website. [Online]. Available: https://rparussia.ru/rpa-solutions/ (Accessed: April 1, 2024).

Канарейкин А.И. Математическая аналогия между уравнениями теплопроводности и диффузии // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 6(44) с. 149–156

Международный журнал информационных технологий и энергоэффективности

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

УДК 536.2

МАТЕМАТИЧЕСКАЯ АНАЛОГИЯ МЕЖДУ УРАВНЕНИЯМИ ТЕПЛОПРОВОДНОСТИ И ДИФФУЗИИ

Канарейкин А.И.
ФГБОУ ВО «РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГЕОЛОГОРАЗВЕДОЧНЫЙ УНИВЕРСИТЕТ ИМЕНИ СЕРГО ОРДЖОНИКИДЗЕ (МГРИ)», Москва, Россия, (МГРИ), г. Москва, Российская Федерация, (117485, г. Москва, ул. Миклухо-Маклая, 23), e-mail: kanareykins@mail.ru

Работа посвящена явлениям переноса за счёт теплопроводности и диффузии. В ней раскрывается сущность математической аналогии между уравнениями теплопроводности и диффузии. Под математической аналогией в приведённой работе понимается эквивалентность математических формулировок разных физических задач с точностью до постоянных. Привлекательность математических аналогий заключается как раз в том, что при известном решении одной задачи легко записать соответствующее решение математически идентичных задач другой физической сущности. Эти решения можно использовать при описании диффузионных процессов, а также других явлений при одинаковой математической постановке.

Ключевые слова: Теплопроводность, диффузия, математическая аналогия, оператор Лапласа, параболическое уравнение, гиперболическое уравнение.

MATHEMATICAL ANALOGY BETWEEN THE EQUATIONS OF THERMAL CONDUCTIVITY AND DIFFUSION

Kanareykin A.I.
SERGO ORDZHONIKIDZE RUSSIAN STATE UNIVERSITY FOR GEOLOGICAL PROSPECTING, Moscow, Russia, (117485, Moscow, st. Miklukho-Maklaya 23), e-mail: kanareykins@mail.ru

The work is devoted to the phenomena of transfer due to thermal conductivity and diffusion. It reveals the essence of the mathematical analogy between the equations of thermal conductivity and diffusion. The mathematical analogy in this paper refers to the equivalence of mathematical formulations of various physical problems up to constants. The attractiveness of mathematical analogies lies precisely in the fact that, with a known solution to one problem, it is easy to write down the corresponding solution to mathematically identical problems of another physical entity. These solutions can be used to describe diffusion processes, as well as other phenomena with the same mathematical formulation.

Keywords: Thermal conductivity, diffusion, mathematical analogy, Laplace operator, parabolic equation, hyperbolic equation.

Сущность математической аналогии между уравнениями теплопроводности и диффузии считается наиболее наглядной [1]. Нестационарные процессы перераспределения температуры и вещества описываются уравнениями параболического типа при соответствующих начальном и граничных условиях [2]. Эти уравнения отличаются друг от друга физическим смыслом постоянных. После перенормировки последних из решения задачи

теплопроводности легко записывается решение соответствующей задачи диффузии. Если в системе отсутствуют источники (стоки) тепла, то нестационарное уравнение теплопроводности для трехмерного случая имеет вид (декартовы координаты) [3-9]:

$$\frac{1}{a^2}\frac{\partial T}{\partial t} = \frac{\partial^2 T}{\partial x^2} + \frac{\partial^2 T}{\partial y^2} + \frac{\partial^2 T}{\partial z^2} \quad (1)$$

где $a^2 = \frac{\lambda}{C\rho}$ – коэффициент температуропроводности,

λ – коэффициент теплопроводности,

C – теплоемкость твердого тела при постоянном объеме,

ρ – плотность материала.

Уравнение можно записать в компактной форме использую символическое обозначение оператора Лапласа в декартовой системе координат:

$$\nabla = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2} \quad (2)$$

С учетом (2) получим:

$$\frac{1}{a^2}\frac{\partial T}{\partial t} = \Delta T \quad (3)$$

Легко убедиться, что правая и левая части уравнения (3) имеют одинаковые размерности. Так, например, в системе СИ имеем:

$$[a^2] = \frac{m^2}{c}, \left[\frac{1}{a^2}\frac{\partial T}{\partial t}\right] = \frac{K}{m^2}; [\Delta T] = \frac{K}{m^2}$$

При этом используется абсолютная шкала температуры Правильность тех или иных соотношений очень часто проверяется с привлечением размерностей соответствующих величин. Если в системе имеются источники(стоки) тепла, то уравнение теплопроводности изменяется

$$\frac{1}{a^2}\frac{\partial T}{\partial t} = \Delta T \pm \frac{f(x,y,z,t)}{\lambda} \quad (4)$$

где f(x,y,z,t) –объемная плотность внутренних источников (стоков) тепла размерностью $\frac{Bm}{м^3}$. В качестве источников тепла рассматривают объемное тепловыделение за счёт ядерных реакций. Поглощение тепла может быть обусловлено химическими реакциями в твердом теле. В уравнении (4) знак плюс соответствует выделению тепла, а знак минус его поглощению. Остальные обозначения соответствуют принятым ранее.

Физическая интерпретация уравнения теплопроводности заключается в следующем. Для ясности понимания рассмотрим одномерный случай при отсутствии объемных источников тепла:

$$\frac{1}{\omega_2}\frac{\partial^2 T}{\partial t^2} + \frac{1}{a^2}\frac{\partial T}{\partial t} = \frac{\partial^2 T}{\partial x^2} \quad (5)$$

Это уравнение связывает между собой скорость изменения температуры во времени $\frac{\partial T}{\partial t}$ и вогнутость (выпуклость) температурного профиля (вторая производная температуры по координате $\frac{\partial^2 T}{\partial x^2}$). Если $\frac{\partial^2 T}{\partial x^2} > 0$ (вогнутый профиль), то $\frac{\partial T}{\partial t} > 0$. Физически это означает

повышение температуры. Для $\frac{\partial T}{\partial t} < 0$, что соответствует понижению температуры. В точке перегиба ($\frac{\partial^2 T}{\partial x^2} = 0$) температура остаётся постоянной.

Уравнение теплопроводности принадлежит к параболическому (нестационарное уравнение) или эллиптическому (стационарное уравнение) типам [10]. Решение нестационарного уравнения теплопроводности дает бесконечную скорость распространения теплового возмущения. Физически это означает, что температура во всех точках тела меняется одновременно.

Между тем любые возмущения распространяются в твердых телах с конечными скоростями, не превышающими скорости звука. Тепловое возмущение также должно иметь конечную скорость распространения. Такую скорость называют скоростью тепловых волн или вторым звуком. Свое название «второй звук» получил по аналогии между фононами в твёрдом теле и молекулами газа. Волновое колебательное возмущение плотности молекул раздаёт звук в газе, колебание локальной плотности фононов вызывает второй звук (тепловую волну) в твердом теле. Для определения температуры в этом случае используют гиперболическое уравнение теплопроводности:

$$\frac{1}{a^2}\frac{\partial T}{\partial t} = \Delta T \tag{6}$$

где ω_2 – скорость распространения теплового возмущения(тепловых волн). При $\omega_2 \to \infty$ уравнение (1) становится параболическим, то есть его решение даёт одновременное изменение температуры во всех точках твёрдого тела. Гиперболическое уравнение теплопроводности применяют, как правило, при тепловых импульсах малой длительности, когда путь теплового возмущения соизмерим с длиной диффузии тепла.

Далее рассмотрим некоторые конкретные примеры использования уравнений параболического типа. Эти примеры подтверждают сущность математических аналогий в механике сплошной среды. В первую очередь остановимся на математическом описании диффузионных процессов [11-19]. Под этим названием понимают перераспределение легирующих элементов сплава под действием градиентов концентрации, температуры и напряжений. Процессы диффузии в континуальном приближении, то есть распределение концентрации атомов примеси является непрерывной функцией. С позиции математического формализма уравнение диффузии идентично уравнению теплопроводности (1) (трехмерный случай):

$$\frac{1}{D}\frac{\partial C}{\partial t} = \frac{\partial^2 C}{\partial x^2} + \frac{\partial^2 C}{\partial y^2} + \frac{\partial^2 C}{\partial z^2} = \Delta C \tag{7}$$

где D - коэффициент диффузии атомов примеси, C - количество атомов примеси в единице объема (размерное значение) или отношение числа атомов примеси к числу мест для их размещения (безразмерная концентрация). Континуальное описание процесса диффузии предполагает, что в единице объема находится большое число атомов примеси Расстояние между соседними примесными атомами сопоставимо с параметром кристаллической решетки твердого тела. Интересно отметить, что коэффициенты температуропроводности a^2 и диффузии D имеют одинаковую размерность $\left[\frac{м^2}{с}\right]$. Это свидетельствует о математической аналогии двух уравнений с

разным физическим смыслом. Поэтому решение одной из задач может использоваться для описания другого физического процесса. Если в системе имеются источники или стоки доя атомов примеси, то соответствующее уравнение диффузии аналогично уравнению (4) теплопроводности:

$$\frac{1}{D}\frac{\partial C}{\partial t} = \Delta C \pm f_1(x, y, z, t) \tag{8}$$

где функция $f_1(x,y,z,t)$ в зависимости от знака определяет источники или стоки примесных атомов. При этом размерность этой функции должна соответствовать размерности соответствующих членов уравнения (8), то есть:

$$\left[\frac{1}{D}\frac{\partial C}{\partial t}\right] = \left[\Delta C\right] = \left[f_1(x, y, z, t)\right] \tag{9}$$

Источники и стоки атомов примеси возникают не только при химических реакциях, но и при облучении материала. Так, например, при нейтронном облучении возникают радиационные точечные дефекты, вакансии и межузельные атомы. Координатная зависимость появления последних описывается функцией $f_1(x,y,z,t)$ правой части уравнений (8). И в данном случае прослеживается математическая аналгия с задачей теплопроводности с источниками или стоками тепла.

Уравнение параболического типа используют при описании движения жидкости через пористую среду [20-27]. В континуальном приближении распределение давления жидкости в пористой среде подчиняется уравнению (трехмерный случай):

$$\frac{1}{D}\frac{\partial C}{\partial t} = \Delta C \pm f_1(x, y, z, t) \tag{10}$$

где α_p - коэффициент пропорциональности между градиентом давления жидкости и ее потоком, p - давление жидкости. Соотношения (3), (7) и (10) с точностью до постоянных математически эквивалентны, хотя и описывают различные физические явления: температура, концентрация примесей, давление жидкости.

Таким образом, математическая аналогия между уравнениями теплопроводности и диффузии позволяет охватить достаточно широкий спектр подобных задач. Привлекательность математических аналогий заключается как раз в том, что при известном решении одной задачи легко записать соответствующее решение математически идентичных задач другой физической сущности. Известно, что наиболее тщательно и подробно проанализированы задачи теплопроводности. Эти решения можно использовать при описании диффузионных процессов, а также других явлений при одинаковой математической постановке. При этом начальное и граничные условия рассматриваемых задач с точностью до постоянных также математически идентичны. Это обеспечивает единственность решения математической задачи и гарантирует достоверность полученных результатов.

Список литературы

1. Канарейкин, А. И. Математическая аналогия между температурными и концентрационными напряжениями//Международный журнал информационных технологий и энергоэффективности, 2024. - Т. 9. - № 3 (41). - С. 109-114.
2. Канарейкин, А. И. Уравнения параболического типа: учебное пособие. - Саратов: Издательство «Саратовский источник», 2024. - 31 с.
3. Канарейкин, А.И. Применение уравнения Пуассона в теплофизике//Научные труды Калужского государственного университета имени К.Э. Циолковского. - Калужский государственный университет им. К.Э. Циолковского, 2016. - С. 199-200.
4. Канарейкин, А. И. Основы термодинамики: учебное пособие. - Саратов: Издательство «Саратовский источник», 2023. - 63 с.
5. Канарейкин, А. И. Уравнения математической физики: учебное пособие. - Саратов: Издательство «Саратовский источник», 2024. - 35 с.
6. Канарейкин, А.И. О частном решении дифференциального уравнения в частных производных без перехода к эллиптической системе координат//Научные труды Калужского государственного университета имени К.Э. Циолковского. Региональная университетская научно-практическая конференция. Сер. "Естественные науки" Калужский государственный университет имени К.Э. Циолковского, 2015. - С. 140-141.
7. Канарейкин, А. Уравнения математической физики: учебное пособие. – Саратов: Издательство «Саратовский источник», 2024. — 35 с.
8. Петухов, Б.С., Генин, А.Г., Ковалев, С.А. Теплообмен в ядерных энергетических установках. - М.: Атомиздат, 1974. - 408 с.
9. Власов, Н.М. Тепловыделяющие элементы ядерных ракетных двигателей/Н.М.Власов, И.И. Федик. - М.: ЦНИИ атоминформ, 2001. - 208с.
10. Канарейкин, А. И. Уравнения эллиптического типа: учебное посо-бие. - Саратов: Издательство «Саратовский источник», 2024. - 31 с.
11. Ганюков А.А., Кадырова И.А., Кадыров А.С., Маратов Д.Д. Математическое моделирование процесса диффузии и кинетики массопереноса веществ в различных средах//Международный журнал прикладных и фундаментальных исследований. – 2021. – № 4. – С. 86-91
12. Кафаров В.В., Глебов М.Б. Математическое моделирование основных процессов химических производств: Учеб. пособие для вузов. – М.: Высш. шк., 1991. – 400 с.
13. Рапопорт Э.Я. Структурное моделирование объектов и систем управления с распределенными параметрами. – М.: Высш. шк., 2003. – 299 с.
14. Полянин А.Д. Справочник по линейным уравнениям математической физики. – М.: ФИЗМАТЛИТ, 2001. – 576 с.
15. Воробьев А.Х. Диффузионные задачи в химической кинетике. Учебное пособие − М.: Изд-во Моск. ун-та, 2003. − 98с.
16. Губарев С.В., Берг Д.Б., Добряк П.В. Математическая модель и численный метод для решения задач диффузии и теплопроводности // Современные проблемы науки и образования, 2013. – № 6.
17. Мартинсон, Л.К., Малов, Ю.И. Дифференциальные уравнения математической физики. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2002 – 368 с.

18. Труфанова, Т.В., Масловская, А.Г., Веселова, Е.М. Методы решения уравнений математической физики. Учебное пособие – Благовещенск: Амурский гос. ун-т, 2015. – 196 с.
19. Peacman, D.W. The numerical solution of parabolic and elliptic differential equations / D.W. Peacman, H.H.Jr. Rachford//J.Soc. Indust. Appl. Math, 1995. – V. 3. – p. 28-41.
20. Douglas, Jr.J. Alternating direction iteration for mildly nonlinear elliptic difference equations//II. Num. Math., 1962. – V. 4. – p. 301-302.
21. Вабищевич, П.Н. Разностные схемы для нестационарных задач конвекции-диффузии /П.Н.Вабищевич, А.А.Самарский//Журнал вычислительной математики и математической физики, 1998. – Т. 38, № 2. – С. 207-219.
22. Rosenberg, D.U. An explicit finite difference solution to the convection-dispersion equations // Num. Meth. Partial. Diff. Eqn., 1986. –V. 2. – p. 229-237.
23. Krukier, L.A. Numerical Solution of the Steady Convection-Diffusion Equation with Dominant Convection//International Conference on Computational Science, ICCS. – 2013. – V.18. – p. 2095-2100.
24. Buckova, Z. Alternating direction explicit methods for convection diffusion equations/Z. Buckova, M. Ehrhardt, M. Gunther//Bergische Universitat Wuppertal Fachbereich Mathematik und Naturwissenschaften, IMACM, 2015. – p. 309-325.
25. Maslovskaya, A.G., Sivunov, A.V. Simulation of electron injection and charging processes in ferroelectrics modified with the SEM-techniques // Solid State Phenomena, 2014. – V. 213. – p. 119-124.
26. Pavelchuk, A.V., Maslovskaya, A.G. Numerical simulation of electron beam-induced dielectric charging using advanced computational scheme for solving semilinear reaction-diffusion equation // World Journal of Modelling and Simulation, 2018. – V. 14, № 2. – p. 83-89.
27. Leonard, B.P. A stable and accurate convective modelling procedure based on quadratic upstream interpolation // Comput. Methods Appl. Mech. Engrg, 1979. – V. 19. – p. 59-98.

References

1. Kanarekin A. I. Mathematical analogy between temperature and concentration stresses // International Journal of Information Technology and Energy Efficiency, 2024. - Vol. 9. - № 3 (41). - pp. 109-114.
2. Kanarekin A. I. Equations of the parabolic type: a textbook. - Saratov: Publishing house "Saratov source", 2024. - p.31
3. Kanarekin A.I. Application of the Poisson equation in thermophysics // Scientific works of Kaluga State University named after K.E. Tsiolkovsky. - Kaluga State University named after K.E. Tsiolkovsky, 2016. - pp. 199-200.
4. Kanarekin A. I. Fundamentals of thermodynamics: a textbook. - Saratov: Publishing house "Saratov source", 2023. - p.63
5. Kanarekin A. I. Equations of mathematical physics: a textbook. - Saratov: Publishing house "Saratov source", 2024. - p.35
6. Kanarekin A.I. On the partial solution of a partial differential equation without transition to an elliptic coordinate system // Scientific works of Kaluga State University named after K.E. Tsiolkovsky. Regional University Scientific and Practical Conference. Ser. "Natural Sciences" Kaluga State University named after K.E. Tsiolkovsky, 2015. - pp. 140-141.

7. Kanarekin A. Equations of mathematical physics: a textbook. – Saratov: Publishing house "Saratov source", 2024. - p.35
8. Petukhov B.S., Genin, A.G., Kovalev, S.A. Heat transfer in nuclear power plants. - M.: Atomizdat, 1974. - p.408
9. Vlasov N.M. Fuel elements of nuclear rocket engines / N.M. Vlasov, I.I. Fedik. - - M.: Tsniiatominform, 2001. - p 208
10. Kanarekin A. I. Elliptic type equations: a textbook. - Saratov: Publishing house "Saratov source", 2024. – p. 31
11. Konyukov A.A., Kadyrova I.A., Kadyrov A.S., Muratov D.D. Mathematical modeling of the diffusion process and kinetics of mass transfer of substances in various media // International Journal of Applied and Fundamental Research. – 2021. – No. 4. – pp. 86-91
12. Kafarov V.V., Glebov M.B. Mathematical modeling of the main processes of chemical production: Textbook for universities. – M.: Higher School, 1991. – p.400
13. Rapoport E.Ya. Structural modeling of objects and control systems with distributed parameters. – M.: Higher School, 2003. – p.299
14. Polyanin A.D. Handbook of linear equations of mathematical physics. – M.: FIZMATLIT, 2001. – p.576
15. Vorobyov A.H. Diffusion problems in chemical kinetics. Textbook − Moscow: Publishing House of Moscow. Unita, 2003. − p.98
16. Gubarev S.V., Berg D.B., Dobryak P.V. Mathematical model and numerical method for solving problems of diffusion and thermal conductivity // Modern problems of science and education, 2013. – No. 6.
17. Martinson L.K., Malov Yu.I. Differential equations of mathematical physics. – M.: Publishing House of Bauman Moscow State Technical University, 2002 - p.368
18. Trufanova T.V., Maslovskaya A.G., Veselova E.M. Methods for solving equations of mathematical physics. Textbook – Blagoveshchensk: Amur State University, 2015. – p.196
19. Peacman D.W. The numerical solution of parabolic and elliptic differential equations / D.W. Peacman, H.H.Jr. Rachford//J. Soc. Indust. Appl. Math, 1995. – V. 3. – pp. 28-41.
20. Douglas Jr.J. Alternating direction iteration for mildly nonlinear elliptic difference equations //II. Num. Math., 1962. – V. 4. – . pp. 301-302.
21. Vabishevich P.N. Difference schemes for nonstationary convection-diffusion problems/P.N. Vabishevich, A.A. Samarsky//Journal of Computational Mathematics and Mathematical Physics, 1998. – Vol. 38, No. 2. – pp. 207-219.
22. Rosenberg D.U. An explicit finite difference solution to the convection-dispersion equations//Num. Meth. Partial. Diff. Eqn., 1986. –V. 2. – pp. 229-237.
23. Krukier L.A. Numerical Solution of the Steady Convection-Diffusion Equation with Dominant Convection//International Conference on Computational Science, ICCS. – 2013. – V.18. – pp. 2095-2100.
24. Buckova Z. Alternating direction explicit methods for convection diffusion equations/Z. Buckova, M. Ehrhardt, M. Gunther//Bergische Universitat Wuppertal Fachbereich Mathematik und Naturwissenschaften, IMACM, 2015. – pp. 309-325.
25. Maslovskaya A.G., Sivunov A.V. Simulation of electron injection and charging processes in ferroelectrics modified with the SEM-techniques//Solid State Phenomena, 2014. – V. 213. – pp. 119-124.

26. Pavelchuk A.V., Maslovskaya A.G. Numerical simulation of electron beam-induced dielectric charging using advanced computational scheme for solving semilinear reaction-diffusion equation//World Journal of Modelling and Simulation, 2018. – V. 14, № 2. – pp. 83-89.
27. Leonard, B.P. A stable and accurate convective modelling procedure based on quadratic upstream interpolation//Comput. Methods Appl. Mech. Engrg, 1979. – V. 19. – pp. 59-98.

Климачева А.А. Инновационные подходы при проектировании распределительных электрических сетей на территории Дальнего Востока // Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 6(44) с. 157–161

Международный журнал информационных технологий и энергоэффективности

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

УДК 621.316.1

ИННОВАЦИОННЫЕ ПОДХОДЫ ПРИ ПРОЕКТИРОВАНИИ РАСПРЕДЕЛИТЕЛЬНЫХ ЭЛЕКТРИЧЕСКИХ СЕТЕЙ НА ТЕРРИТОРИИ ДАЛЬНЕГО ВОСТОКА

Климачева А.А.
ФГБОУ ВО "АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ", Благовещенск, Россия (675028, Амурская область, город Благовещенск, Игнатьевское ш., д.21), e-mail: klimacheva_nastya21@mail.ru

В статье рассматривается новая технология цифровой двойник и эффект от ее применения в распределительных электрических сетях, а также показан пилотный проект данной технологии в распределительных сетях на основе интеграции геоинформационной системы.

Ключевые слова: Потребители электрической энергии; электрооборудование; цифровой двойник; линии электропередачи; подстанция.

INNOVATIVE APPROACHES IN THE DESIGN OF ELECTRIC DISTRIBUTION NETWORKS IN THE FAR EAST

Klimacheva A.A.
AMUR STATE UNIVERSITY, Blagoveshchensk, Russia (675028, Amur Region, Blagoveshchensk city, Ignatyevskoye sh., 21), e-mail: klimacheva_nastya21@mail.ru

The article discusses the new digital twin technology and the effect of its application in electrical distribution networks, and also shows a pilot project of this technology in distribution networks based on the integration of a geoinformation system.

Keywords: Consumers of electric energy; electrical equipment; digital twin; power transmission lines; substation.

Введение

С появлением цифровых счетчиков электроэнергии и развитием телекоммуникаций, а также элементов интеллектуальных электрических сетей, энергосистемы во всем мире обязаны осуществить "цифровой переход" или цифровизацию - значительное изменение внутренней структуры и управления. По определению, цифровизация представляет собой широкий спектр технологий и решений, которые в конечном итоге приведут к созданию цифровых электрических сетей. Все эти решения объединены через автоматизированный поток и бизнес-процессы, что исключает вмешательство человека в принятие рутинных решений. Цель цифровизации заключается не только в переходе на новую программно-аппаратную базу, но также в объединении технологических и бизнес-процессов, что позволяет снижать количество ошибок и значительно повышать скорость и точность принятия решений [1].

В современных условиях цифровизации, автоматизации и интеллектуализации, традиционная энергетика претерпевает изменения, которые сопровождаются появлением новых технологий, таких как "цифровой двойник". Эти технологии основаны на анализе больших объемов данных об объекте, системе или процессе и способны не только обнаруживать скрытые закономерности в данных, но и выявлять отклонения в параметрах функционирования с высокой чувствительностью еще на ранних стадиях, когда эти отклонения еще не оказывают влияния на состояние системы и не могут быть обнаружены с помощью традиционных систем управления и мониторинга [2].

Цифровой двойник для электрических сетей

Цифровая модель электрической сети, известная как ЦД, объединяет в себе базу данных с информацией об электрической сети и интегрируется с другими системами компании. Данные из различных источников автоматически согласовываются, чтобы точно отразить физическую структуру сети в цифровой форме.

Интеграция цифровых двойников в систему управления для электроэнергетических объектов считается ключевым моментом, необходимым для проверки эффективности предложенных решений.

Технологии цифровых двойников все более широко используются в различных технических областях, включая электроэнергетику, как в России, так и за рубежом. Однако следует отметить, что применение цифровых двойников в электроэнергетике находится на ранней стадии развития, в отличие от области автоматизированного проектирования и конструирования [3].

Цифровые двойники становятся всё более актуальными для современных энергокомпаний, поскольку в таких компаниях обычно существует только одна физическая электрическая сеть, но у неё имеется множество представлений в различных подразделениях. Каждая модель используется для разных целей и обладает разным программным обеспечением (например, для проведения сетевых расчётов, диспетчеризации, управления активами, в системе учёта и т. д.). Несоответствие данных в различных моделях может приводить к неточностям в представлении сети, неоптимальной производительности системы и проблемам, связанным с ручным обновлением данных в моделях.

Существуют три разновидности ЦД [4]:

- Двойник-прототип (Digital Twin Prototype). Элемент на всех этапах своего существования описывается в виртуальной форме, содержащей информацию о требованиях к производству, технологическим процессам и утилизации. Основные решения в этой области — это 3D-модели изделий, созданные в высокотехнологичных системах автоматизированного проектирования и полностью задокументированные.
- Двойник-экземпляр (Digital Twin Instance). Содержит в себе информацию по описанию элемента (оборудования), то есть данные о материалах, комплектующих, информацию от системы мониторинга оборудования. Этот тип чаще всего основан на математической модели системы.
- Агрегированный двойник (Digital Twin Aggregate). За собой тянет устройство или систему, объединяя прототип и экземпляр, а также собирая всю информацию, доступную об оборудовании.

Для распределительных сетей Дальнего Востока, наиболее актуален двойник-экземпляр. Он основывается на математической модели сети.

Цифровой двойник электрической сети содержит информацию о технических параметрах такого оборудования, как кабели, трансформаторы, выключатели и прочее. Он также включает данные о дате ввода в эксплуатацию, географические координаты и информацию, полученную от измерительных устройств. Эти данные используются для различных расчетов, включая расчеты при подключении новых потребителей и анализ параметров электрических сетей, включая режимы работы, токи короткого замыкания, и настройку релейной защиты. Обычно каждое подразделение в компании использует свою собственную математическую модель одной и той же физической сети, что влечет за собой возможные ошибки и снижение точности. Использование единого цифрового двойника всеми подразделениями позволяет преодолеть эту проблему.

Основными преимуществами цифрового двойника являются [1]:

1. Улучшение точности и согласованности модели (единого источника информации) для проведения расчетов и управления, включая:
   - Снижение вероятности серьезных ошибок в эксплуатации или планировании, вызванных некорректными данными в модели.
   - Отслеживание изменений в модели с возможностью восстановления состояний после изменений («контрольный журнал»).
   - Взаимодействие с ключевыми источниками данных и функциями, такими как система управления активами или геоинформационная система (ГИС).
2. Повышение эффективности и оптимизация процессов в планировании и эксплуатации, включая:
   - Устранение дублирующих процессов путем совместного использования модели сети в планировании и эксплуатации.
   - Автоматизация процессов, например, с использованием автоматического построения модели распределительной сети.
   - Сокращение сроков технологического присоединения к электрической сети.
   - Внедрение унифицированного процесса моделирования и управления данными для различных функций.
3. Обеспечение более простой интеграции подсистем в будущем и увеличение общей цифровизации компании, включая:
   - Более эффективное использование ресурсов сети, позволяющее эксплуатировать ее ближе к возможным предельным значениям.
   - Внедрение адаптивных установок релейной защиты, которые автоматически реагируют на изменения в сети и обеспечивают более точную и надежную защиту.
   - Предотвращение или отсрочка необходимости проведения работ по усилению сети путем использования моделирования и оптимизации в реальном времени.
   - Возможность проведения моделирования в режиме реального времени, как например, динамическая оценка и оценка безопасности защиты, а также прогнозирование на день вперед, что позволяет предотвратить отключения электроэнергии и обеспечить безопасную работу сети.

Важно отметить, что операторы магистральных сетей и операторы распределительных сетей имеют свою специфику, хотя их основные функции - передача электроэнергии и

обслуживание активов - схожи. В случае магистральных сетей, цифровой двойник может представлять собой базу данных, в которой модель сети хранится в формате CIM с использованием программного обеспечения. Для распределительных сетей, база данных, основанная на программном обеспечении для расчета электрических сетей и геоинформационной системы (ГИС), может выступать в качестве единого источника информации. Различие обусловлено тем, что распределительные сети имеют гораздо большее количество элементов, и в сочетании с частыми изменениями создают огромные объемы данных, обработка которых достаточно сложна.

Пример реализации технологии цифрового двойника для распределительных сетей

Пример создания цифрового двойника для распределительных сетей можно найти в проекте интеграции геоинформационной системы (ГИС) и программного обеспечения PSS SINCAL, реализованном компанией VSE Group в Словакии, которая является частью European RWE Group. Распределительная сеть компании передает ежегодно 3800 ГВтч электроэнергии в географическом районе, эквивалентном одной трети восточной Словакии, занимающем примерно 16 200 кв. км. Для обслуживания более чем 610 000 домашних хозяйств в сети используются 34 подстанции 110/22 кВ и 6000 подстанций 22/0,4 кВ. Общая длина воздушных и кабельных линий электропередачи составляет 21 тыс. км. К 2009 году компания установила большое количество информационных технологий (SCADA, ГИС, SAP), для оптимальной работы которых требовалась актуальная модель электрической сети. Создание цифрового двойника электрической сети успешно завершилось с внедрением расчетного комплекса для электрических сетей. Автоматическое преобразование данных позволило пользователям создавать точную модель распределительной сети в кратчайшие сроки. Внедрение данного решения в VSE Group существенно улучшило качество анализа распределительной сети и используется в качестве одного из критериев приоритизации обслуживания оборудования.

Заключение

Использование цифровых двойников для распределительных сетей имеет ряд преимуществ и позволяет:

1. Создавать единый источник информации о состоянии сети, объединяя данные из различных подсистем и создавая модель, которая отражает поведение реальной системы.
2. Снижать издержки на создание модели и использовать их для анализа сети, что позволяет более эффективно использовать ресурсы и сократить расходы.
3. Улучшать качество информации о состоянии электрической сети, обеспечивая более точные данные для принятия решений и управления сетью.
4. Упрощать процесс заявок на технологическое присоединение, ускоряя процесс и сокращая бюрократические процедуры.
5. Более точно рассчитывать технические потери в сети, что позволяет оптимизировать эффективность работы сети и снизить потери электроэнергии.

Применение технологий цифровых двойников также способствует улучшению работы дежурных электромонтеров, позволяя им более эффективно выполнять свои задачи и получать более достоверную информацию о текущем состоянии и остаточном ресурсе оборудования. Использование технологии цифрового двойника в составе Интеллектуальной системы

диагностики и технического обслуживания приносит значительные выгоды, такие как снижение эксплуатационных расходов за счет сокращения времени простоя оборудования из-за непредвиденных ремонтов и оптимизации планирования и выполнения ремонтных работ. Отображение электрооборудования, такого как генераторы, в виде цифрового двойника предоставляет возможности для анализа и прогнозирования. Технология позволяет моделировать различные ситуации, которые могут возникать в процессе эксплуатации оборудования и помогает в предотвращении проблем и принятии информированных решений.

Список литературы

1. Никитина Е.В., Полуэктов А.Н., Кох С. Цифровой двойник для электрических сетей//Энергия единой сети. – 2019. – № 4 (46). – С. 32-36.
2. С. А. Ерошенко, А. И. Хальясмаа//Электроэнергетика глазами молодежи-2019 : материалы юбилейной X Международной научно-технической конференции, Иркутск, 16–20 сентября 2019 года. – Иркутск: Иркутский национальный исследовательский технический университет, 2019. – С. 55-58. – EDN IECAJH.
3. Гвозде Д.Б., Болонов В.О., Окнин Е.П. [и др.]. О возможности применения цифровых двойников в управлении объектами электроэнергетики//Электроэнергия. Передача и распределение. – 2019. – № 6(57). – С. 30-35. – EDN BUZZXR.
4. Салов И.В., Щербатов И.А., Салова Ю.А. Применение цифровых двойников и киберфизических систем на объектах генерации тепловой и электрической энергии / И. В. Салов, И. А. Щербатов, Ю. А. Салова//International Journal of Open Information Technologies. – 2022. – Т. 10. – № 3. – С. 57-62. – EDN FHNYUS.

References

1. Nikitina E.V., Poluektov A.N., Koch S. Digital double for electric networks // The energy of a single network. – 2019. – № 4 (46). – pp. 32-36.
2. S. A. Eroshenko, A. I. Khalyasmaa//Electric power industry through the eyes of youth-2019 : materials of the jubilee X International Scientific and Technical Conference, Irkutsk, September 16-20, 2019. – Irkutsk: Irkutsk National Research Technical University, 2019. – pp. 55-58. – EDN IECAJH.
3. Gvozdi D.B., Bolonov V.O., Agnin E.P. [et al.]. About the possibility of using digital twins in the management of electric power facilities//Electricity. Transmission and distribution. – 2019. – № 6(57). – pp. 30-35. – EDN BUZZXR.
4. Salov I.V., Shcherbatov I.A., Salova Yu.A. Application of digital twins and cyberphysical systems at thermal and electric energy generation facilities / I. V. Salov, I. A. Shcherbatov, Yu.A. Salova//International Journal of Open Information Technologies. – 2022. – Vol. 10. – No. 3. – pp. 57-62. – EDN FHNYUS.

Борисов И.С., Королевская А.С., Нацубидзе С.В. Интеграция CES с атомной электростанцией (АЭС) // Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 6(44) с. 162–168

Международный журнал информационных технологий и энергоэффективности

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

УДК 621.039

ИНТЕГРАЦИЯ CES С АТОМНОЙ ЭЛЕКТРОСТАНЦИЕЙ (АЭС)

[1] Борисов И.С., [2] Королевская А.С., [3]Нацубидзе С.В.
ФГБОУ ВО «ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ» УНИВЕРСИТЕТ, Иркутск, Россия (664074, Иркутская область, город Иркутск, ул. Лермонтова, д. 83), e-mail: [1]myp3una@gmail.com, [2]anelok_03@mail.ru, [3]natsubidze00@bk.ru

Было предпринято значительное количество усилий, чтобы справиться со смещением нагрузки на АЭС, а общепринятым методом является использование гидроаккумулирующих накопителей энергии. В последние десятилетия были разработаны новые подходы к использованию избыточной электроэнергии для поддержания АЭС почти на полной нагрузке. Когда АЭС работают с частичной нагрузкой, стоимость производства электроэнергии становится высокой. Кроме того, частые изменения нагрузки могут привести к быстрому старению оборудования и повлиять на производительность установки, что приводит как к экономическим проблемам, так и к проблемам, связанным с безопасностью. Интеграция CES с АЭС может решить проблемы, связанные с регулированием нагрузки АЭС более экономичным и эффективным способом.

Ключевые слова: Возобновляемая энергия, криогенная энергетики, накопители энергии, электроэнергетика, атомная электростанция.

INTEGRATION OF CES WITH NUCLEAR POWER PLANTS (NPP)

[1]Borisov I.S., [2]Korolevskaya A. S., [3]Natsubidze S.V.
IRKUTSK NATIONAL RESEARCH TECHNICAL UNIVERSITY, Irkutsk, Russia (83 Lermontova st., Irkutsk, Irkutsk 664074, Irkutsk region), e-mail: [1]myp3una@gmail.com, [2]anelok_03@mail.ru, [3]natsubidze00@bk.ru

A significant amount of effort has been made to cope with the shift in load at nuclear power plants, and the generally accepted method is the use of pumped storage energy storage. In recent decades, new approaches have been developed to use excess electricity to maintain nuclear power plants at almost full load. When nuclear power plants operate with partial load, the cost of electricity production becomes high. In addition, frequent load changes can lead to rapid aging of the equipment and affect the performance of the installation, which leads to both economic and safety problems. The integration of CES with nuclear power plants can solve the problems associated with regulating the load of nuclear power plants in a more economical and efficient way.

Keywords: Renewable energy, cryogenic energy, energy storage, electric power industry, nuclear power plant.

Введение

В настоящее время на АЭС с водо-водяным ядерным реактором приходится значительная часть мировых АЭС [1-3]. Помимо проблем безопасности и сокращения срока службы, этот режим работы также сталкивается с двумя проблемами при отслеживании нагрузки. Во-первых, это ограниченный градиент изменения мощности, который обычно занимает несколько часов для достижения примерно половины нагрузки. Во-вторых,

снижение регулирования АЭС только уравновешивает выработку и спрос в течение нескольких часов, в то время как другие установки, такие как газовые электростанции, должны быть задействованы для удовлетворения пиковых потребностей.

1. Оценка производительности

На Рисунке 1 показана технологическая схема типичной установки CES, которая состоит из трех отличительных, но взаимосвязанных и интегрированных подсистем: установки сжижения воздуха, блока хранения и блока рекуперации энергии. Во время зарядки воздух из окружающей среды сжижается посредством серии процессов сжатия и расширения, основанных на модифицированном цикле Клода.

Процесс сжатия (потоки 1-5) оснащен двумя промежуточными охладителями, через которые накапливается тепло при сжатии. Здесь, в качестве примера рассматривается накопление тепла при сжатии в диатермическом масле. Такое мало действует как теплоноситель в промежуточных охладителях, так и как накопительная среда в резервуарах для хранения горячей воды (потоки 1-5). Воздух высокого давления поле последней стадии сжатия, охлажденный соответствующим промежуточным охладителем, дополнительно охлаждается в холодильной камере (потоки 5-6) холодным воздухом (потоки 14-15) из газожидкостного сепаратора и холодным воздухом (потоки 3C-4C) из холодильной камеры высокой степени (HGSC). Два воздушных потока 10 и 12 в холодильной камере расширяются в двух турбодетандерах для повышения эффективности процесса охлаждения. Наконец, охлажденный воздух в холодильной камере расширяется в криодетандере, образуя смесь газообразного и жидкого воздуха. Смесь разделяется в сепараторе с жидким воздухом, хранящимся в криогенном баке при температуре около -193°C и давлении, близком к давлению окружающей среды.

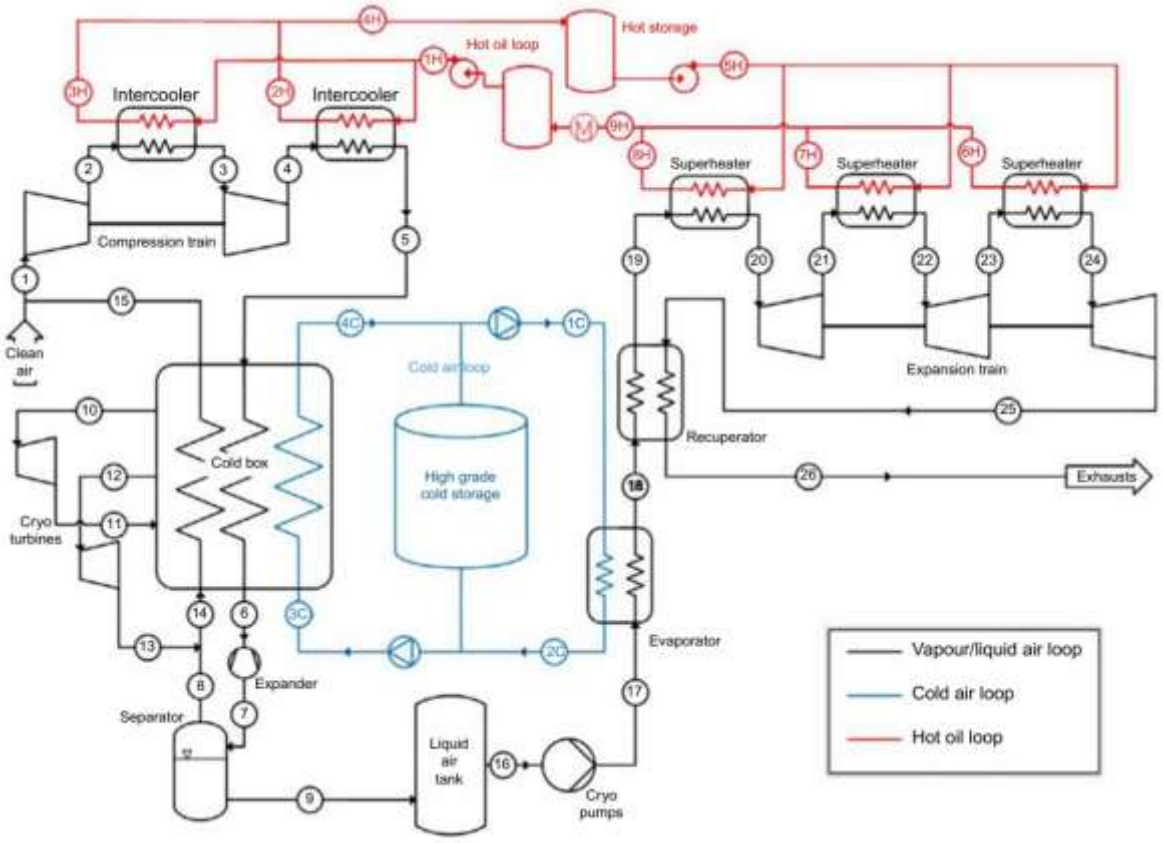


Рисунок 1 – Принципиальная схема предлагаемого криогенного накопителя энергии, основанная на сжижении природного газа

Во время разрядки, накопленный жидкий воздух сначала нагнетается криогенными насосами, а затем повторно нагревается с использованием тепла окружающей среды и тепла сжатия. Воздух нагревается в секции теплообменников, включающих: испаритель, рекуператор и пароперегреватель. Холодная энергия, выделяющаяся при испарении жидкого воздуха (потоки 17-18), улавливается встречным потоком теплоносителя (потоки 1C-2C) и накапливается в HGSC [6, 7]. HGSC могут быть реализованы с использованием таких технологий как уплотненные слои горных пород, как рассматривается здесь, и эксплуатироваться при давлении, близком к атмосферному, для снижения затрат и повышения безопасности HGSC. Наконец, нагретый воздух высокого давления расширяется в многоступенчатых турбинах для выработки электроэнергии (потоки 20-25).

Ключевым термодинамическим показателем эффективности для оценки установки CES является так называемый коэффициент эффектив6ности полезного действия в обе стороны, который определяет как отношение производительности в процессе выделения энергии к потребляемой мощности в процессе накопления энергии.

CES – это комбинированная технология накопления энергии на основе термодинамики, которая, вероятно, подойдет для применений с мощностью от десятков до сотен МВт и производительностью от десятков МВт·ч до нескольких ГВт·ч.

Основные преимущества этой технологии — легкость масштабирования и возможность более длительного, чем в традиционных аккумуляторах, хранения электроэнергии. Благодаря этим особенностям установки могут сыграть важную роль в эффективном использовании энергии, получаемой из возобновляемых источников.

2. Стремление к интеграции CES с АЭС

АЭС отличаются высокими капитальными и низкими эксплуатационными расходами. Это означает, что затраты на электроэнергию от такой капиталоемкой технологии могут быть низкими при эксплуатации на полную мощность, и в результате АЭС в основном использовались для выработки электроэнергии с базовой нагрузкой. Однако с увеличением числа установок АЭС мощность выработки электроэнергии может превышать базовую нагрузку электросетей. Например, на долю атомной энергетики приходится 53% от общей установленной мощности Франции, при этом вырабатывается 79% электроэнергии в стране. Избыток электроэнергии в непиковое время приходится либо экспортировать в другие страны, либо хранить для последующего использования (временной сдвиг). Если эти две меры не смогут сбалансировать выработку и спрос, АЭС должны быть сокращены.

Когда АЭС работают с частичной нагрузкой, стоимость производства электроэнергии становится высокой. Кроме того, частые изменения нагрузки могут привести к быстрому старению оборудования и повлиять на производительность установки, что приводит как к экономическим проблемам, так и к проблемам, связанным с безопасностью.

В настоящее время на АЭС с водо-водяным ядерным реактором приходится значительная часть мировых АЭС. Помимо проблем безопасности и сокращения срока службы, этот режим работы также сталкивается с двумя проблемами при отслеживании нагрузки. Во-первых, это ограниченный градиент изменения мощности, который обычно занимает несколько часов для достижения примерно половины нагрузки. Во-вторых, снижение регулирования АЭС только уравновешивает выработку и спрос в течение нескольких часов, в то время как другие установки, такие как газовые электростанции, должны быть задействованы для удовлетворения пиковых потребностей.

3. Интеграция CES с АЭС

Было предпринято значительное количество усилий, чтобы справиться со смещением нагрузки на АЭС, а общепринятым методом является использование гидроаккумулирующих накопителей энергии. В последние десятилетия были разработаны новые подходы к использованию избыточной электроэнергии для поддержания АЭС почти на полной нагрузке.

К ним относятся паровые аккумуляторы, крупномасштабное производство и хранение водорода и геотермальные накопители тепла.

Недавно была предложена интеграция CES с АЭС, которая потенциально может решить проблемы, связанные с регулированием нагрузки АЭС, более экономичным и эффективным способом. На рис. 6 показан принцип работы интегрированной системы, которая состоит из подсистемы АЭС и подсистемы CES [4, 5]. Подсистема АЭС в интегрированной системе аналогична обычной АЭС с водо-водяным ядерным реактором. Единственная разница заключается в том, что во вторичном контуре имеются два трехходовых клапана, которые позволяют рабочей жидкости подаваться либо в паровую турбину для выработки электроэнергии, либо в теплообменник 4 для перегрева воздуха высокого давления в подсистеме CES (Рисунок 2).

Подсистема CES состоит из блока сжижения воздуха в левой части и блока рекуперации энергии в правой нижней части Рисунка 2. Подсистема сжижения воздуха работает

аналогично простейшему сжижителю Linde-Hampson, за исключением использования внешней холодной энергии через теплообменник 6.

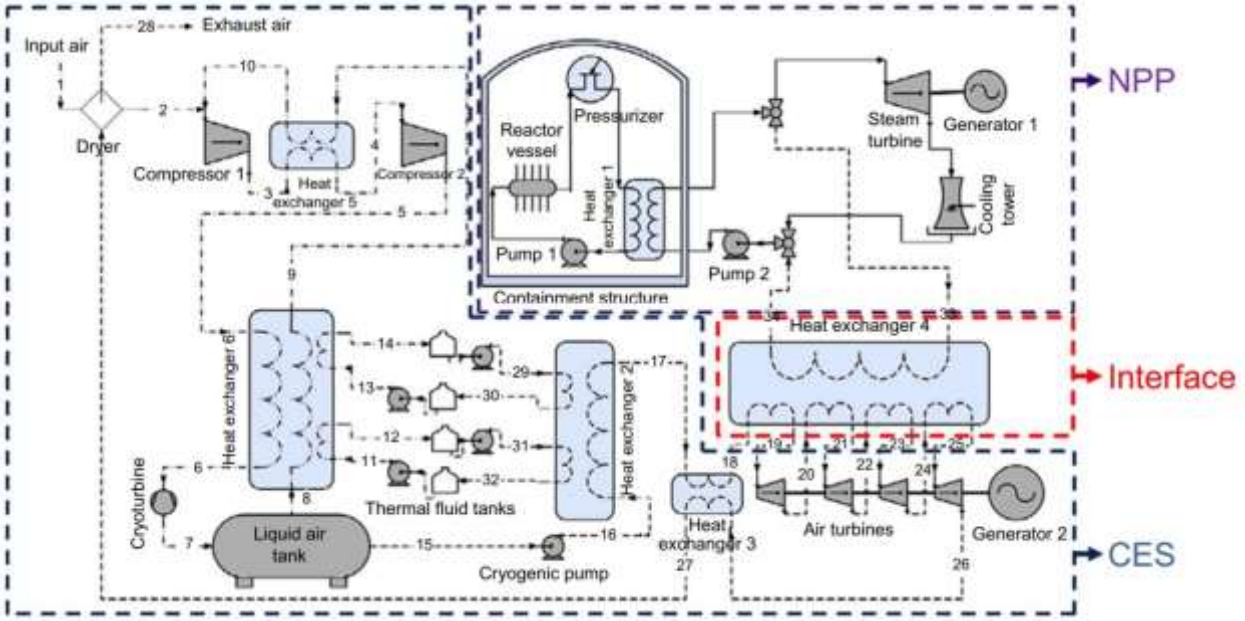


Рисунок 2 – Интегрированная технология АЭС-CES

Подсистема CES состоит из блока сжижения воздуха в левой части и блока рекуперации энергии в правой нижней части рис. 6. Подсистема сжижения воздуха работает аналогично простейшему сжижителю Linde-Hampson, за исключением использования внешней холодной энергии через теплообменник 6.

Холодильное хранилище и связанная с ним функция рекуперации действуют как связующее звено между блоком сжижения воздуха и блоком рекуперации энергии.

В качестве хладоносителей при оценке используются пропан и метанол, которые также действуют как рабочие жидкости для теплопередачи. Обоснованием для рассмотрения этих двух сред хранения холода является то, что они хорошо соответствуют требуемому температурному диапазону и обладают высокой удельной теплоемкостью. Предложена конфигурация с двумя резервуарами для хранения и рекуперации энергии холода для каждой из двух жидкостей: на этапе холодного хранения две жидкости перекачиваются соответственно из теплых резервуаров в холодные резервуары (энергия холода сохраняется, в то время как мощность восстанавливается); на этапе восстановления холода две жидкости перекачиваются соответственно из теплых резервуаров в холодные резервуары, жидкости вытекают соответственно из холодных резервуаров в теплые резервуары (высвобождается холодная энергия, в то время как энергия накапливается). Дополнительные преимущества использования охлаждающих жидкостей, как для передачи, так и для хранения холодной энергии включают в себя большее упрощение конструкции системы без дополнительных теплообменников и более простую эксплуатацию, при которой количество холодной энергии и заданная температура легко регулируются путем регулирования расхода жидкостей.

Блок рекуперации энергии соединен с АЭС посредством нагрева теплообменника 4, в котором утилизируется низкосортное тепло от АЭС. Использование такого подхода позволяет преобразовывать тепловую энергию, обычно расходуемую в процессе охлаждения, в

электрическую энергию с высокой эффективностью, которая не может быть достигнута никакими другими технологиями хранения.

Теплообменник 4 обеспечивает связь между подсистемой CES и подсистемой АЭС. Такая интеграция позволяет активной зоне реактора и первичному контуру АЭС стабильно работать при полной нагрузке в любое время, в то время как чистая выходная мощность регулируется только подсистемой CES. Восстановление мощности в подсистеме CES аналогично процессу выработки электроэнергии с использованием газовой турбины, при этом может быть достигнута гораздо более высокая скорость изменения мощности по сравнению с обычным регулированием АЭС.

Заключение

Технология CES, интегрированная с АЭС, обеспечивает эффективное и действенное решение для переключения нагрузки станций. Термодинамический анализ интегрированной системы CES-АЭС при довольно общих исходных допущениях показывает, что эффективность накопления электроэнергии в обе стороны составляет около 71%, в то время как чистая выходная мощность в режиме выделения электроэнергии может в 2,7 раза превышать номинальную мощность АЭС. Эта особенность делает интеграцию технологии CES с АЭС высококонкурентным вариантом, который не может быть достигнута никакими другими технологиями хранения.

Список литературы

1. Р.Б. Скотт. Техника низких температур. Перевод под ред. проф. М.П. Малкова. М.: Изд. иностр. литер. , 1962, С. 21-22.
2. C. Bruynooghe, A. Eriksson, G. Fulli, Load-following operating mode at nuclear power plants (NPPs) and incidence on operatio and maintenance (O&M) costs. Compatibility with wind power variability, European Commission, Joint Research Centre, Institute of Energy, 2010.
3. E.E. Michaelides, Nuclear Power Plants: Alternative Energy Sources, Springer, Berlin, Heidelberg, 2012, pp. 131–172.
4. M.V. Kothare, B. Mettler, M. Morari, P. Bendotti, C.M. Falinower, Level control in the steam generator of a nuclear power plant, IEEE Trans. Control Syst. Technol.
5. Быстрицкий Г. Ф. Основы энергетики. — М.: Инфра-М, 2007. — 276 с.
6. C. Coombs, French nuclear power: a model for the world? Hinckley J. Polit. 11 (2010) 7–13.
7. C.W. Forsberg, Y. Lee, M. Kulhanek, M.J. Driscoll, in: Gigawatt-year nucleargeothermal energy storage for light-water and high-temperature reactors, International Congress on the Advances in Nuclear Power Plants, Chicago, IL, 2012.

References

1. R.B. Scott. Low temperature technique. Translated by prof. M.P. Malkov. M.: Foreign Publishing House. lit., 1962, p. 21-22.
2. C. Bruynooghe, A. Eriksson, G. Fulli, Load-following operating mode at nuclear power plants (NPPs) and incidence on operatio and maintenance (O&M) costs. Compatibility with wind power variability, European Commission, Joint Research Centre, Institute of Energy, 2010.
3. E.E. Michaelides, Nuclear Power Plants: Alternative Energy Sources, Springer, Berlin, Heidelberg, 2012, pp. 131–172.

4. M.V. Kothare, B. Mettler, M. Morari, P. Bendotti, C.M. Falinower, Level control in the steam generator of a nuclear power plant, IEEE Trans. Control Syst. Technol.
5. Bystritsky G. F. Fundamentals of energy. — M.: Infra-M, 2007. — p.276
6. C. Coombs, French nuclear power: a model for the world? Hinckley J. Polit. 11 (2010) 7–13.
7. C.W. Forsberg, Y. Lee, M. Kulhanek, M.J. Driscoll, in: Gigawatt-year nucleargeothermal energy storage for light-water and high-temperature reactors, International Congress on the Advances in Nuclear Power Plants, Chicago, IL, 2012.