Министерство образования Республики Беларусь
учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

СБОРНИК МАТЕРИАЛОВ
61-ой научной конференции
аспирантов, магистрантов и студентов
21–25 апреля 2025 года

Минск, БГУИР

Министерство образования Республики Беларусь
учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

**61-я научная конференция
аспирантов, магистрантов и студентов**

Сборник материалов

21–25 апреля 2025 года
Минск, БГУИР

УДК 621.391

61-я научная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 21-25 апреля 2025 г., БГУИР, Минск, Беларусь: сборник материалов. – Мн. – 2025. – 159 с.; ил.

В сборнике опубликованы материалы докладов, представленных на 61-й научной конференции аспирантов, магистрантов и студентов БГУИР. Материалы одобрены оргкомитетом и публикуются в авторской редакции.

Для научных и инженерно-технических работников, преподавателей, аспирантов, магистрантов и студентов вузов.

СОДЕРЖАНИЕ

СЕКЦИЯ «ЗАЩИТА ИНФОРМАЦИИ»

СЕКЦИЯ «СИСТЕМЫ И СЕТИ ИНФОКОММУНИКАЦИЙ»

СЕКЦИЯ «ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ СИСТЕМЫ»

Статистика по 60-ой научной конференции аспирантов, магистрантов и студентов УО «Белорусский государственный университет информатики и радиоэлектроники»

НАПРАВЛЕНИЕ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Рисунок 1 – Диаграмма «Количество статей по секциям»

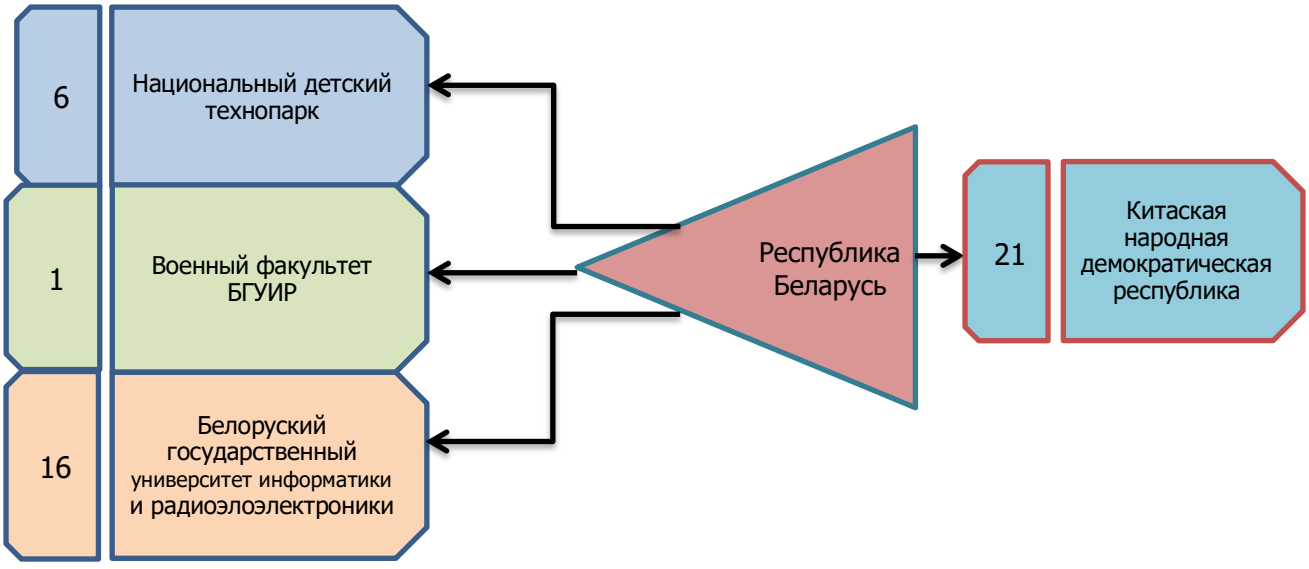


Рисунок 2 – Учреждения образования, принявшие участие в конференции (статьи)

Рисунок 3 – Участники конференции

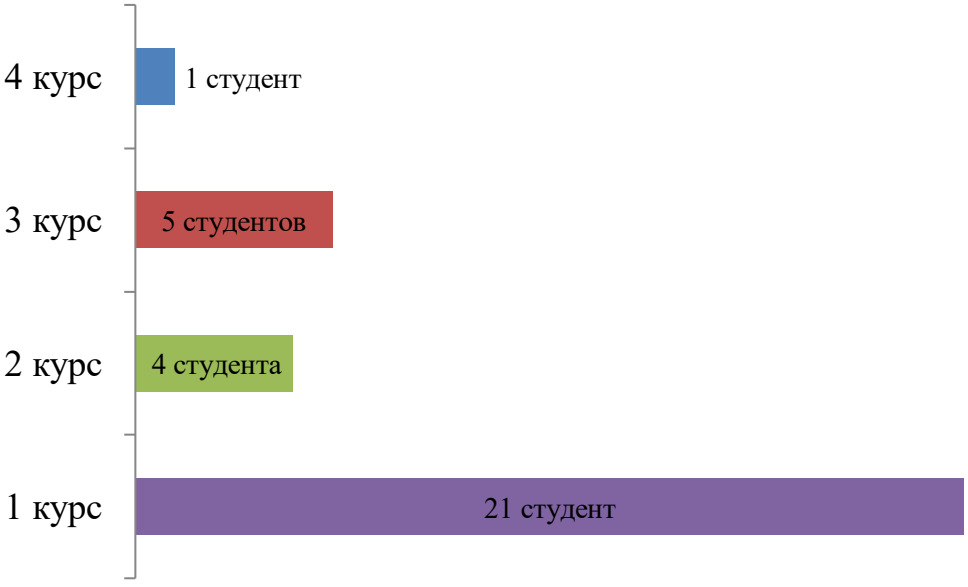


Рисунок 4 – Студенты-участники конференции

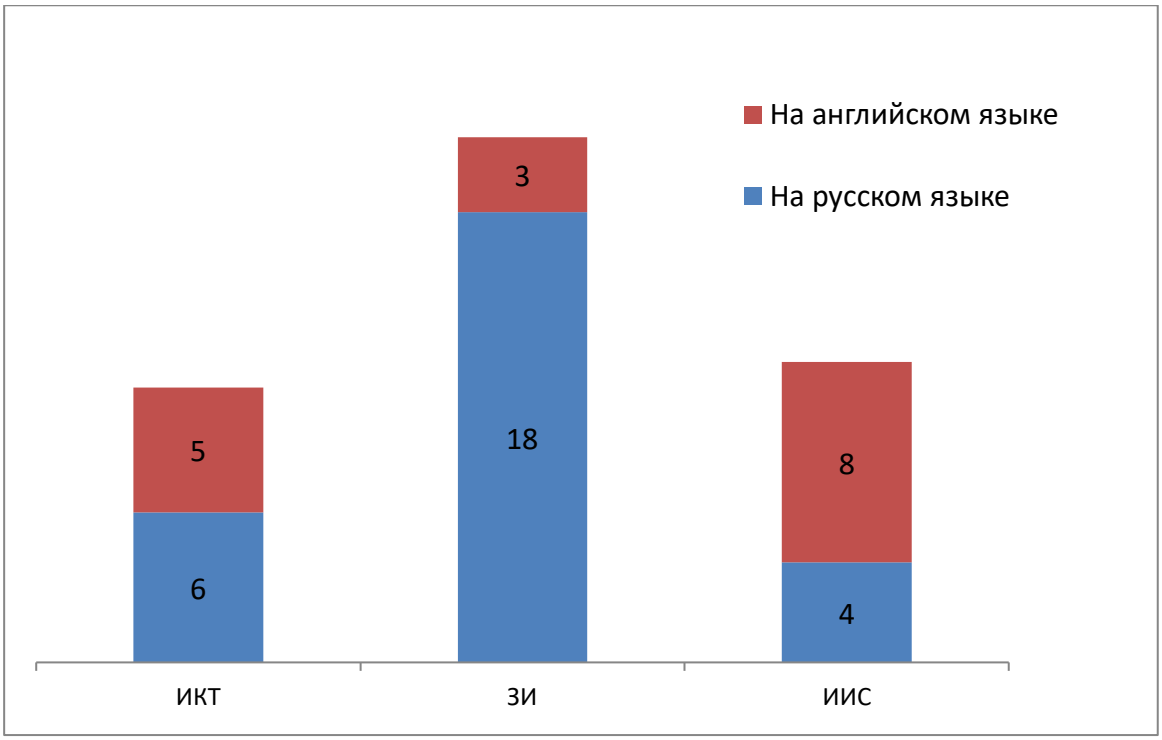


Рисунок 5 – Диаграмма «Материалы конференции на русском и английском языках»

СЕКЦИЯ «ЗАЩИТА ИНФОРМАЦИИ»

RESEARCH ON SOFTWARE MODULE FOR PROTECTION OF INFORMATION FROM A LEAKAGE VIA ACOUSTIC CHANNELS

Dai Junyi [1]

[1]*Belarusian State University of Informatics and Radio Electronics*
Minsk, Republic of Belarus

O.B. Zelmansky – PhD, associate professor

Annotation. Aiming at the problem of information leakage in acoustic channels, a software module is designed and studied. This module can effectively reduce the risk of leakage and ensure information security in multiple scenarios, which has important practical value.

Keywords. acoustic channels, sound leakage prevention, software module, information security.

Introduction

With the rapid development of information technology, smart devices are widely popularized, which brings convenience to people, but also increasingly serious information security issues 1. . Acoustic channels, as a potential channel for information leakage, have gradually attracted attention2. . The built-in microphones of smart devices are often in a "monitoring" state, making it very easy for voice information to be stolen through the acoustic channel, which in turn leads to the risk of privacy leakage. In places such as government, military, and scientific research institutions that have extremely high requirements for information confidentiality, information security is of great importance, and once leaked, it will cause serious consequences. Therefore, in order to effectively respond to these information security threats, it is crucial to design a software module to prevent information leakage in acoustic channels, which has extremely important practical significance for protecting personal privacy, corporate trade secrets, and national information security.

To achieve this goal, the following tasks were determined:

– Investigate existing technologies and risks: Study the current acoustic channel information leakage related technologies, analyze their principles and application scenarios, accurately identify information leakage risk points, and provide a basis for software design.

– Build software module architecture: Design the overall architecture of the software module, integrate voice cloning, acoustic interference control and user management functions, and ensure that the architecture is stable.

– Develop core functional modules: Implement audio management and voice cloning core modules, ensure audio security management and high-quality voice cloning, and improve information protection capabilities.

– Test and optimize software performance: Test the software in multiple scenarios, evaluate the anti-leakage effect and performance, optimize according to the test results, and enhance the practicality and stability

of the software.

Research on acoustic channel information leakage

1. Acoustic channels and monitoring technology

Acoustic channels use sound waves to transmit information and are widely used in underwater communications, medical, industrial, and consumer electronics 3. . With the development of technology, monitoring technology has been evolving from traditional microphone-based monitoring methods to advanced technologies such as laser microphones and vibration sensors, as well as non-invasive monitoring technologies such as gyro microphones and visual microphones, which pose a serious threat to privacy 4. .

Different monitoring technologies have their own characteristics. Laser microphones can collect sound from a long distance, but are greatly affected by the monitoring surface and environmental factors; vibration sensors can achieve non-line-of-sight monitoring, but the clarity of audio collected in noisy environments is limited; acoustic sensors are restricted by the environment and microphone quality. In addition, the reliability of existing countermeasures against monitoring technology needs to be improved.

2. Information leakage risk and protection strategy

Smart device microphones can easily obtain sensitive information of users when collecting environmental sounds, and malware may also secretly transmit this information through acoustic channels 5. . In the communication system, if there is a security vulnerability in the transmission of sound signals, attackers can capture and restore the signals and steal important information. Information leakage will cause serious harm to individuals, enterprises and national security 6. .

To deal with these risks, acoustic information protection strategies are divided into active protection and passive protection. Active protection technologies such as active noise interference, acoustic encryption, dynamic acoustic barriers, and real-time acoustic monitoring and alarm systems block the risk of information leakage by intervening in the propagation of acoustic signals in real time, but they have problems such as low energy efficiency, real-time bottlenecks, high-frequency attenuation, and sensor interference 7. .

Passive protection technologies include acoustic stealth technology, physical isolation, environmental noise protection, and acoustic signal confusion 8. . These technologies reduce risks by designing security measures, but they also face limitations such as poor low-frequency performance, large space occupation, environmental dependence, and signal distortion.

Software module design and implementation

1. System design goals and requirements analysis

1.1 Protection scenarios and problem definition

For open office environments, the software module mainly guards against two risks: one is voice feature leakage, that is, attackers use voice cloning technology to forge user voice features to interfere with the voice recognition system; the other is voice content leakage, that is, attackers use cloned voices to play meaningless texts, reducing the recognition accuracy of the voice-to-text system.

1.2 Core functional requirements

The software module has the function of user voice cloning, and voice training is realized through the Fineshare API. The input is a clear recording uploaded by the user with a sampling rate of more than 1 minute and 16kHz (supports MP3 format, no more than 50MB). The API automatically completes voice feature extraction and cloning model training (about 3 minutes), and outputs cloned audio files (MP3 format).

In terms of acoustic interference control, it provides basic environmental noise (such as rain, cafe background sound, white noise) and supports volume adjustment; preset meaningless text templates, and use

cloned timbre to play text randomly in real time.

The user management system covers basic functions such as registration/login, playing public and private audio library audio, managing private audio, and cloning personal voice.

2. Software module architecture design

2.1 Overall architecture design

The software module adopts a three-layer architecture, including the front-end interaction layer, the back-end service layer, and the third-party API layer. The front-end interaction layer is responsible for page structure display and dynamic content rendering, including page templates such as login and registration, which are implemented through the Jinja2 template engine. CSS is responsible for page style layout, and JavaScript implements client interaction logic, including modules such as audio playback control and voice cloning management.

The back-end service layer is based on the Flask application, processes front-end HTTP requests, and implements business logic and data access management. The routing layer is responsible for processing user authentication, audio files, user information, voice cloning and other related requests. The storage layer uses SQLite database to store user information and system configuration, and the file system stores audio files, which are divided into public audio library, private audio library and cloned voice library.

The third-party API layer provides voice cloning function, processes voice sample conversion and returns cloned voice files. Each layer interacts through a clear interface to realize functions such as user operation processing, data transmission and storage, and voice cloning.

2.2 Database Design

The system uses SQLite database and implements data persistence through SQLAlchemy ORM framework. Database design follows the principle of normalization to ensure data integrity and consistency. The user model defines the user data structure, including fields such as user ID, user name, password, email, administrator ID, password reset token and expiration time.

Database configuration is implemented by creating database engine, session and declaring base classes. The data access layer encapsulates database session management and CRUD operations, including functions such as obtaining database session, creating users, and querying users by username. The database security mechanism includes password encryption storage and transaction management to ensure user password security and atomicity of data operations.

3. Core module implementation

3.1 Audio management module

The audio management module is responsible for the storage, playback and management of audio files. It adopts a hierarchical design to isolate and manage public noise libraries and private voice libraries. Set the file storage directory and allowed file extensions, and limit the uploaded file size to 16MB. Get the list of audio files from the specified directory through the function implementation, and provide an interface for obtaining the public audio playlist in the web application.

Playback control is implemented through the PlaybackManager class of JavaScript, which supports loop playback and random playback modes. File upload processing is implemented in the routing of the Flask application, checking the user login status, whether the file exists, whether the file type is legal, and saving the file to the user-specific directory to ensure the security and standardization of file upload.

3.2 Voice cloning module

The voice cloning module provides users with voice cloning functions through recording and API integration. The recording interface is implemented using the VoiceCloneManager class of JavaScript to obtain the audio stream of the user's media device for recording. Manage sample text and provide multiple preset texts for user recording. Process voice file upload in the Flask application, create a user-specific directory to save

files, and handle file name conflicts

Conclusion

This study designed and implemented a software module based on Web application, which can effectively reduce the risk of information leakage in the acoustic channel, ensure information security in a variety of scenarios, and has good practicality and flexibility. In the future, the module will continue to be optimized to further improve its performance and security to better cope with the ever-changing information security challenges.

List of sources used:

1. Gaouzi, Z., & Chougdali, K. (2022). Impact of security and privacy risks on the adoption of IoT: A state of the art. Information Security Journal, 29(2), 115-130.

2. Oleynikov, A., Bilotserkivet, O., & Shirokyi, O. (2023). Modeling the Acoustic Channel of Voice Information Leakage. Cybersecurity & Privacy Journal, 18(3), 250-266.

3. Pan, C., Liu, S., Qing, X., & Qiao, G. (2023). Feature extraction and classification of deep-sea mobile underwater acoustic channels. Marine Science Journal, 14(2), 85-99.

4. Cunningham, C. F., Hopps, A. M., Losee, W., Sandberg, R., Allred, D., & Neilsen, T. (2023). Frequency Characterization of Laser Microphones. Journal of Acoustical Science, 45(3), 210-225.

5. Duan, L., Zhang, K., Cheng, B., & Ren, B. (2021). Privacy Threats of Acoustic Covert Communication among Smart Mobile Devices. Cybersecurity Journal, 12(4), 678-693.

6. Prytys, V., Krymchak, L., & Havlovska, N. (2020). Leakage of Information as a Key Problem of Economic Security. Cyber Risk Journal, 19(5), 421-438.

7. Lai, S. K. (2019). Real-time prediction of noise signals for active control based on Bayesian forecasting and time series analysis. Acoustics and Noise Control Research, 37(1), 55-72.

8. Feng, X., Yan, L., & Chun, W. (2021). Review on vibration isolation technology. Journal of Physics: Conference Series, 1820(1), 012009.

UDC 004.934

SOFTWARE FOR RECOGNIZING SPEAKER BY VOICE

Chen Zhengyu

Group 467311

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Zelmansky O.B. – Associate Professor of the Department of Information Security, PhD, Associate Professor.

Annotation. FBank (Filter Bank) is a front-end processing algorithm that processes audio in a way similar to the human ear and extracts features to improve the performance of speech recognition. The system uses an efficient context-aware masking-based network, CAM++, which uses a densely connected time-delay neural network (D-TDNN) as the backbone and adopts a novel multi-granularity pooling to capture different levels of context information.Based on the respective advantages of FBank and CAM++ models, this study designs a software for recognizing speaker by voice and implements the system through pytorch.

Keywords. speaker recognition, feature Extraction, neural networks, pytorch

Introduction. Speaker recognition (SR) is a biometric technology that identifies individuals based on unique vocal characteristics. In recent years, with the rapid development of deep learning technology, speaker recognition technology has become more and more widely used, for example call center operation, criminal investigation, smart speaker and robotics, security for phone and other fields.

This thesis focuses on the design and implementation of software for recognizing speaker by voice. This involves two main aspects: one is selecting and training the model, and the other is designing the front-end interface.This system is based on the CAM++ model.[1] It includes a convolutional module as the front end and a D-TDNN as the backbone. Each D-TDNN layer has an improved context-aware mechanism built in, including multi-granularity pooling to capture speaker characteristics. This reduces the amount of computation and increases the inference speed. PyQt5 is then used to design an interface that implements registration, recording, recognition, and other functions, connecting it to the model.

Before training the model, FBank is used to extract features from the training data to simulate the characteristics of the human ear to improve the accuracy of the model. Experiments were conducted on the CN-Celeb database of about 1,000 speakers. The preprocessing method used was FBank, and the loss function was Angular additive margin softmax (AAM-Softmax) loss. The EER of the CAM++ model was 14.73% and the MinDCF was 0.41999.

Main Part. In the SR (Speaker Recognition) system, the first step is to extract features. The most commonly used features in speech-related tasks are MFCC and FBank. This system chooses to use FBank to extract features from data. The general steps to obtain the FBank features of speech signals are: pre-emphasis, framing, windowing, short-time Fourier transform (STFT), Mel filtering, etc.

Pre-emphasis strengthens high frequencies because the human vocal tract radiates sound waves through air, which acts as a signal carrier that both transmits and dissipates energy. As the medium is the carrier of sound energy, when the size of the sound source is constant, the higher the frequency, the more serious the loss of sound energy by the medium. It is necessary to divide the audio of indefinite length into small segments of fixed length. This step is called framing. Generally, 10-30ms is taken as one frame. In order to avoid missing the signal at the window boundary, there should be frame overlap when offsetting the frame (frames need to overlap a part). This can avoid too much change in characteristics between frames. The usual choice is 25ms per frame, and the frame shift is 10ms. For example, our system uses 80-dimensional FBank features extracted over a 25 ms long window for every 10 ms as input. After framing, the signal is still in the time domain. In order to extract FBank features, we first need to convert the time domain signal into the frequency domain signal. Fourier transform can convert the signal from the time domain to the frequency domain. Fourier transform can be divided into continuous Fourier transform and discrete Fourier transform. Because this system uses digital audio (not analog audio), discrete Fourier transform is used. The discrete Fourier transform is calculated as follows:

$$S_i(k) = \sum_{n=1}^{N} x(n) e^{-j2\pi kn/N} \qquad 1 \le k \le K$$

Where $x(n)$ – audio sampling point, N – Number of sampling points.

The specific relationship between Mel frequency and actual frequency is as follows:

$$f_{mel}(f) = 2595 \cdot log(1 + \frac{f}{700Hz})$$

The hearing characteristics of the human ear are consistent with the growth of the Mel frequency. The actual frequency is linear below 1000Hz and logarithmic above 1000Hz.

Usually we set the upper and lower limits of the frequency to shield some unnecessary or noisy frequency ranges (the lower limit is usually set to around 20 Hz, and the upper limit is half of the audio sampling rate), and convert it to Mel frequency. Then configure a triangular filter bank of K channels on the Mel frequency axis, and K is generally 40. The triangular window function is:

$$H_m(k) = \begin{cases} \dfrac{k - f_{m-1}}{f_m - f_{m-1}} & f_{m-1} \le k < f_m \\ \dfrac{f_{m+1} - k}{f_{m+1} - f_m} & f_m \le k < f_{m+1} \\ 0 & otherwise \end{cases}$$

Where f_m – Center frequency of the m filter, k – Frequency index after FFT.

The system's input consisted of 80-bin FBank features computed with a 25 ms window size and 10 ms frame shift. In addition, two types of data augmentation are applied simultaneously during model training: synthesizing reverberation effects through room impulse response (RIR)[2], and adding environmental noise using the MUSAN corpus [3]. Speech, music, and noise from the MUSAN database and RIR are randomly added to the original training data. The training dataset is augmented twofold by synthesizing reverberation effects (RIR) and adding environmental noise (from MUSAN). This increases the amount and diversity of the existing training data, and achieves a significant improvement for the system[4].

The proposed CAM++ architecture adopts a dual-module design consisting of a front-end convolution module (FCM) and a D-TDNN backbone. The FCM employs multiple 2D convolutional blocks with residual connections to effectively capture high-resolution time-frequency representations from the acoustic features. These feature maps are then flattened along both channel and frequency dimensions before being fed into the subsequent D-TDNN backbone. The backbone comprises three sequential blocks, each containing stacked D-TDNN layers enhanced with improved CAM modules. These modules dynamically assign attention weights to the TDNN layer outputs, enabling network-wide context-aware feature refinement. This hierarchical architecture allows for comprehensive processing of spectro-temporal patterns while maintaining efficient feature abstraction.

AAM-Softmax (Additive Angular Margin Softmax) is a loss function widely used in speaker recognition and facial recognition[5]. It is an improved method of Large Margin Softmax series. Its core idea is to increase the difference between classes and improve the discriminability of features by introducing margin in the angular space.The formula of AAM-Softmax is as follows:

$$\mathcal{L} = -\frac{1}{N}\sum_{i=1}^{N} log \frac{e^{s\cdot(cos(\theta_{y_i}+m))}}{e^{s\cdot(cos(\theta_{y_i}+m))} + \sum_{j=1, j\neq y_i}^{n} e^{e\cdot cos\theta_j}}$$

Where θ_{y_i} – the angle between the sample x_i and the weight vector W_{y_i} of its true category y_i. s – a scaling factor used to control the effect of the modulus of the feature vector on the loss. m – the angle margin, which is used to increase the classification difficulty of samples near the decision boundary.

The model evaluation metrics are Equal Error Rate (EER) and Minimum Detection Cost (MinDCF). EER does not rely on manually set thresholds and directly reflects the inherent distinguishing ability of the model. EER is the error rate when the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) are equal, that is:

$$EER = FAR = FRR$$

MinDCF is the value that minimizes the detection cost function (DCF).MinDCF is the minimum value of DCF under all possible thresholds θ. By adjusting the $C_{Miss}/C_{FalseAlarm}$ ratio, it can adapt to different scene requirements. The formula is as follows:

$$C_{Det}(\theta) = C_{Miss} \times P_{Target} \times P_{Miss}(\theta) + C_{FalseAlarm} \times (1 - P_{Target}) \times P_{FalseAlarm}(\theta)$$

Where θ – decision threshold, C_{Miss} – Cost of missed judgment, $C_{FalseAlarm}$ – The cost of misjudgment, P_{Target} – a priori probability of the specified target speaker.

The prediction module can receive audio, resample the audio (16kHz), normalize, extract features. Using a pre-trained neural network model, a fixed-dimensional speaker recognition vector is extracted. That is, the feature data is put into the model for inference to obtain a 256-dimensional vector representing the speaker's voiceprint features, which is stored in the audio database together with the label. This system uses cosine similarity to calculate the score. The formula is as follows：

$$similarity = cos(\theta) = \frac{A \cdot B}{\|A\|\|B\|} = \frac{\sum_{i=1}^{n} A_i \times B_i}{\sqrt{\sum_{i=1}^{n}(A_i)^2} \times \sqrt{\sum_{i=1}^{n}(B_i)^2}}$$

If the similarity exceeds the set threshold, they are determined to be the same speaker. In speaker recognition, the system will select the speaker with the highest score and exceeding the threshold as the recognition result. If it does not exceed the threshold, it will be judged as not recognizing the registered user. In addition, this system is designed so that each user can register multiple voice samples, and the system will calculate the average features to improve recognition robustness.

The front-end interface is designed by pyqt5. Users can register speaker recognition information or perform speaker recognition by recording through the interface. At the same time, the recording length and judgment threshold can be set. The recognized registration name and confidence will be returned to the interface. Audio files can also be recognized. By passing the path of the audio file into the system, the system can recognize it and return the result.

Conclusion. This thesis introduces the design and implementation of a software for recognizing speaker by voice, which combines deep learning techniques with a PyQt5 front-end interface to achieve robust speaker recognition through FBank feature extraction, data augmentation, CAM++ model and an optimized AAM-Softmax loss function. The system shows competitive performance on the CN-Celeb dataset with an EER of 14.73% and a MinDCF of 0.41999, using a combination of convolutional front-end modules and context-aware D-TDNN layers of the CAM++ architecture to effectively capture speaker features while reducing computational overhead. By using FBank features to simulate human auditory perception and enhancing model generalization through data augmentation techniques such as RIR reverberation and MUSAN noise, the system supports practical applications such as speech registration, real-time recognition, and audio file analysis, and adopts a threshold-based speaker verification decision mechanism. The PyQt5 interface provides seamless interaction with configurable parameters for recording, registration, and recognition, thereby fulfilling all software functional requirements.

References:

1. CAM++: A fast and efficient network for speaker verification using context-aware masking / H. Wang, S. Zheng, Y. Chen [et al.] // arXiv preprint arXiv:2303.00332, 2023..

2. Musan: A music, speech, and noise corpus / D. Snyder, G. Chen, D. Povey [et al.] // arXiv preprint arXiv:1510.08484, 2015.

3. A study on data augmentation of reverberant speech for robust speech recognition / T. Ko, V. Peddinti, D. Povey [et al.] // 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). - P. 5220-5224.

4. X-vectors: Robust DNN embeddings for speaker recognition / D. Snyder, D. Garcia-Romero, G. Sell [et al.] // 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). - P. 5329-5333.

5. Deng J, Guo J, Xue N, et al. Arcface: Additive angular margin loss for deep face recognition[C]//Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2019: 4690-4699.

ЛИЦЕНЗИРОВАНИЕ ДЕЯТЕЛЬНОСТИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ: ТРЕБОВАНИЯ И ПРАКТИКА (ОСОБЕННОСТИ ЛИЦЕНЗИРОВАНИЯ В КОНТЕКСТЕ СОБЛЮДЕНИЯ ЗАКОНОДАТЕЛЬСТВА О ПЕРСОНАЛЬНЫХ ДАННЫХ)

Ахриева М.Р.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Пухир Г.А. – старший преподаватель кафедры защиты информации

Аннотация. В условиях стремительного развития технологий и возрастающей глобализации защита персональных данных принимает ключевое значение в жизни современного общества. В данной работе анализируется комплекс мероприятий, направленных на охрану конфиденциальности, целостности и доступности информации, связанной с индивидуумом. Актуальность темы обоснована тем фактом, что каждый гражданин оставляет цифровой след в различных сферах деятельности, который может быть использован как в целях обеспечения безопасности и удобства, так и для манипуляции или нарушения прав человека. Рассматриваются современные угрозы, связанные с обработкой персональных данных, такие как киберпреступность, утечки информации и неправомерное использование данных. Подчеркивается необходимость внедрения эффективных систем защиты, включая законодательные меры, технологии шифрования и практики управления данными, чтобы обеспечить не только защиту прав граждан, но и комплексную безопасность информационного пространства в целом. Работа имеет целью осветить важность защиты личной информации в условиях цифровой трансформации общества и предложить рекомендации по улучшению существующих подходов к её защите.

Ключевые слова: персональные данные, защита данных, конфиденциальность, целостность, доступность, цифровой след, информационная безопасность, глобализация, технический прогресс, киберпреступность, утечки информации, шифрование данных

. ***Введение.*** В условиях стремительного технического прогресса и глобализации информация о личных данных граждан становится все более уязвимой. Защита персональных данных — это комплекс мероприятий, направленных на обеспечение конфиденциальности, целостности и доступности информации, относящейся к индивидууму. В современных реалиях каждый из нас оставляет цифровой след, который может быть использован как в доброжелательных, так и в недоброкачественных целях. Поэтому эффективная защита персональных данных становится необходимостью не только для соблюдения прав граждан, но и для обеспечения безопасности информационного пространства в целом. Лицензирование деятельности в области защиты персональных данных играет ключевую роль в регулировании этой сферы. Наличие лицензии удостоверяет, что организация соответствует установленным законом требованиям и стандартам безопасности, и готова взять на себя ответственность за обработку и защиту персональных данных клиентов. Лицензирование не только повышает уровень доверия со стороны клиентов, но и создает здоровую конкурентную среду, способствуя улучшению общей практики защиты данных в стране. Цель данной статьи — рассмотреть требования и практику лицензирования в сфере защиты персональных данных, а также выявить особенности и сложности, с которыми сталкиваются организации в процессе получения лицензии. Мы проанализируем существующее законодательство, процедуры лицензирования и их влияние на

соблюдение прав граждан, поставив акцент на важности комплексного подхода к защите персональных данных в условиях современных вызовов.

Основная часть. В Республике Беларусь защиту персональных данных регулирует Закон от 7 мая 2021 года № 87-З «О защите персональных данных». Этот закон определяет основные принципы обработки данных, включая законность, добросовестность и прозрачность, а также права субъектов данных и обязанности операторов. Закон вводит меры, требующие от операторов четкого определения целей обработки, соблюдения принципов минимизации данных и уведомления субъектов о целях обработки. Также обозначены требования к организации и технической безопасности данных.

Государственный надзор осуществляют специализированные органы, такие как Министерство антимонопольного регулирования и торговли, которые проверяют соблюдение законодательства и лицензирования, а также применяют санкции за нарушения. Кроме того, закон предоставляет субъектам возможность обращаться в правоохранительные органы при нарушении их прав.

Лицензирование в области обработки и защиты персональных данных в Республике Беларусь — важный процесс, который обеспечивает соответствие организаций законодательным требованиям. Процедура лицензирования создает безопасную среду для обработки персональных данных и повышает доверие граждан к компаниям.

Организации, такие как банки, телекоммуникационные компании и медучреждения, проходят лицензионную процедуру из-за значительного объема обрабатываемых данных. Например, банки обязаны получать лицензии для работы с персональными данными клиентов, а медицинские учреждения делают это для соблюдения требований по защите данных о здоровье. При получении лицензии компании сталкиваются с рядом проблем.

Одной из главных трудностей является недостаточная осведомленность о требованиях законодательства и процессах лицензирования. Часто организации не знают, какие документы нужны и какие шаги следует предпринять. Также необходимый аудит внутренней документации и практик обработки данных может требовать значительных ресурсов и времени.

Для успешного получения лицензии компаниям рекомендуется изучить законодательство и подготовить необходимую документацию, включая внутренние инструкции и политику безопасности. Предварительный аудит текущих практик обработки данных также поможет выявить слабые места. Обучение сотрудников обеспечит их осведомленность о важности соблюдения норм законодательства. Консультация с экспертами или юридическими консультантами может значительно повысить шансы на успешное прохождение лицензирования.

Комплексный подход к подготовке обеспечит эффективную деятельность в области защиты персональных данных. Организации обязаны разрабатывать внутренние инструкции и положения, регулирующие порядок обработки и защиты персональных данных. Эти локальные акты должны определять процедуры получения согласия субъектов данных, методы обеспечения безопасности информации, а также правила доступа к персональным данным.

Документы также должны содержать инструкции по проведению оценок рисков и реагированию на инциденты, связанные с утечкой данных. Внедрение таких актов помогает обеспечить соблюдение законодательства, минимизирует риски и повышает уровень защиты персональных данных в организации. Лицензирование играет ключевую роль в соблюдении законодательства о персональных данных, так как оно требует от организаций выполнения строгих требований и стандартов в области обработки и защиты данных.

Процесс лицензирования помогает убедиться, что компании имеют необходимые меры безопасности, что, в свою очередь, снижает риски утечек и несанкционированного доступа. Взаимосвязь между лицензированием и качеством защиты данных заключается в том, что лицензированные

организации обычно представляют более высокий уровень соответствия требованиям законодательства. Они обязаны проводить регулярные аудиты, обновлять свои внутренние регламенты и улучшать технологии защиты данных, что способствует более надежной защите персональной информации.

Ответственность за нарушение законодательства о персональных данных может включать как административные, так и уголовные санкции. К ним относятся штрафы, приостановление или аннулирование лицензий, а также возможные судебные иски со стороны субъектов данных. Эти меры подчеркивают важность соблюдения норм защиты персональной информации и способствуют повышению общей ответственности в этой области.

Таким образом, лицензирование является ключевым элементом обеспечения соблюдения законодательства о защите персональных данных, поднимая уровень безопасности и ответственности организаций. В дальнейшем ожидается развитие законодательства с акцентом на современные технологии и соответствие международным стандартам. Рекомендуется бизнесу активно готовиться к лицензированию и внедрять внутренние регламенты, в то время как органам власти следует обновлять законодательство и повышать осведомленность населения о важности защиты персональных данных.

Список литературы

1. Нугманова, Г.З. Лицензирование в сфере защиты персональных данных: проблемы и перспективы // Вестник юридической науки. — 2020. — № 3. — С. 34-41.

2.Иванов, С.Е. Практика лицензирования в области защиты персональных данных // Журнал права и экономики. — 2021. — Т. 17. — № 2. — С. 76-85.

3.Петров, А.Ю., Кузнецова, О.В. Зависимость защиты персональных данных от уровня лицензирования: анализ и рекомендации // Информационное право. — 2022. — Т. 14. — № 1. — С. 20-28.

4.Ковалев, И.А., Сидорова, Е.А. Лицензирование в сфере обработки персональных данных: российский и международный опыт // Право и информационные технологии. — 2021. — Т. 9. — № 3. — С. 45-53.

5.Дьяконов, В.Л. Законодательство о защите персональных данных: особенности лицензирования // Российский юридический журнал. — 2019. — Т. 16. — № 6. — С. 12-18.

УДК 004.056.53

КОНФИГУРАЦИЯ SIEM-СИСТЕМЫ WAZUH

Багонский И.А., Жук К.Д., студенты гр. 261401, 261402

Белорусский государственный университет информатики и радиоэлектроники,

г. Минск, Республика Беларусь

Белоусова Е.С. – канд. тех. наук, доцент

Аннотация. В статье поясняется процесс установки SIEM Wazuh с открытым исходным кодом. Рассмотрены ключевые этапы установки системы: развертывание Wazuh Manager на сервере Ubuntu, смена пароля администратора, установка агентов на устройствах с операционной системой Windows и настройка мониторинга журналов. Платформа Wazuh обеспечивает сбор, анализ и визуализацию данных безопасности, что позволяет изучать методы обнаружения угроз, анализа событий и реагирования в реальных условиях. Внедрение SIEM Wazuh способствует формированию практических навыков работы с современными инструментами кибербезопасности.

Ключевые слова. SIEM, Wazuh, Windows 10, Wazuh Manager.

SIEM (Security Information and Event Management) – система, которая позволяет собирать данные о безопасности из компонентов информационной инфраструктуры и представлять эти

данные в виде полезной информации через единый интерфейс [1].

SIEM-платформы представляют собой комплексные решения, объединяющие три основных уровня: уровень сбора данных, уровень управления и хранения данных и уровень визуализации и реагирования.

На рынке представлено большое количество SIEM-систем, отличающиеся способами сбора данных, реализацией расположения и конфигурации самой системы. Одними из наиболее известными являются такие SIEM-решения как, MaxPotrol разработанная компанией Positive Technologies, KUMA (Kaspersky Unified Monitoring and Analysis Platform) разработанная компанией Лаборатория Касперского и Wazuh разработанная одноименной компанией Wazuh Inc.

Цель данной работы заключается в обосновании внедрения SIEM Wazuh в учебный процесс на кафедре защиты информации.

Wazuh – платформа безопасности с открытым исходным кодом для обнаружения угроз, мониторинга целостности файлов, анализа логов и соответствия стандартам [2]. SIEM Wazuh включает агенты на оконечных утсройстваъ и центральный сервер, интегрируемый с ELK для визуализации данных.

Процесс установки SIEM Wazuh может быть описан следующими этапами:

1 Установка Wazuh Manager. Для установки Wazuh Manager на сервер Ubuntu версии 24.02.2 [1] была использована команда загрузки и запуска помощника по установке Wazuh Manager `wget https://packages.wazuh.com/4.11/wazuh-install.sh && sudo bash ./wazuh-install.sh -a`. После завершения установки на выходе появляются учетные данные для доступа к веб-интерфейсу и информационное сообщение, что установка прошла успешно.

2 Смена пароля по умолчанию. Для смены пароля был использован инструмент смены паролей Wazuh. Для его использования, его необходимо загрузить скрипт с помощью команды `wget wazuh-passwords-tool.sh https://packages.wazuh.com/4.11/wazuh-passwords-tool.sh`. Скрипт запускался с помощью команды `bash wazuh-passwords-tool.sh -u admin -p E58#QHCkn@g423i`.

3 Установка агентов Wazuh. Агент работает на конечной точке и взаимодействует с сервером Wazuh, отправляя данные практически в режиме реального времени через зашифрованный и аутентифицированный канал. Для установки агента Wazuh на конечную точку с операционной системой Windows10 был скачан установщик с ресурса [3]. После установки в главном меню программы указывается Manager IP, как показано на рисунке 1.

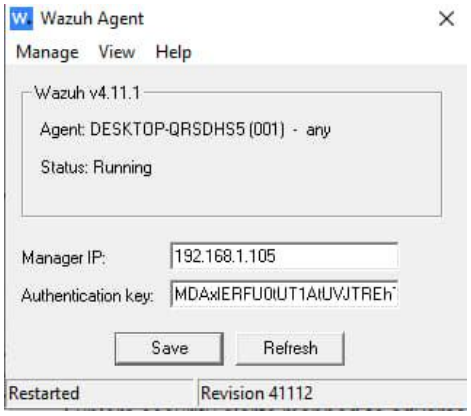


Рисунок 1 – Главное меню программы Wazuh Agent

4 Проверка регистрации агентов на SIEM Wazuh. На рисунке 2 показаны подключенные активные агенты.

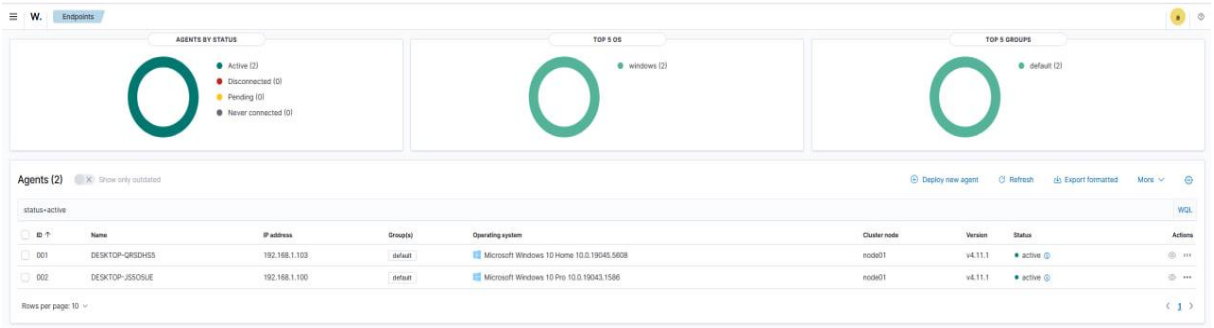


Рисунок 2 – Главная страница веб-интерфейса SIEM Wazuh

5 Настройка конфигурации для мониторинга файлов журнала. Файл ossec.conf является основным файлом конфигурации на сервере Wazuh и агенте Wazuh. Агент Wazuh собирает журналы с контролируемых конечных точек и пересылает эти журналы на сервер Wazuh для анализа. Файл ossec.conf в операционной системе Windows10 находится по пути C:\Program Files (x86)\ossec-agent\ossec.conf. После успешной настройки на SIEM Wazuh возможен просмотр журналов. Информацию об угрозах можно получить при помощи инструмента Theat Hunting. На рисунке 3 показан пример получения общей информации по виду, количеству и значимости угрозы в разделе Dashboard на SIEM Wazuh, которую более подробно можно изучить разделе Events, рисунок 4.

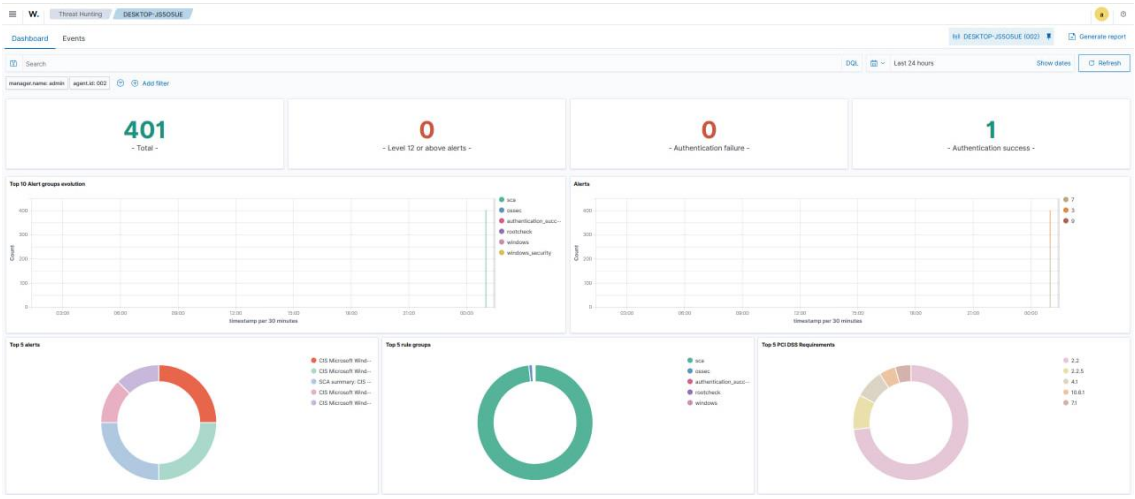


Рисунок 3 – Результат получения общей информации об угрозах на SIEM Wazuh

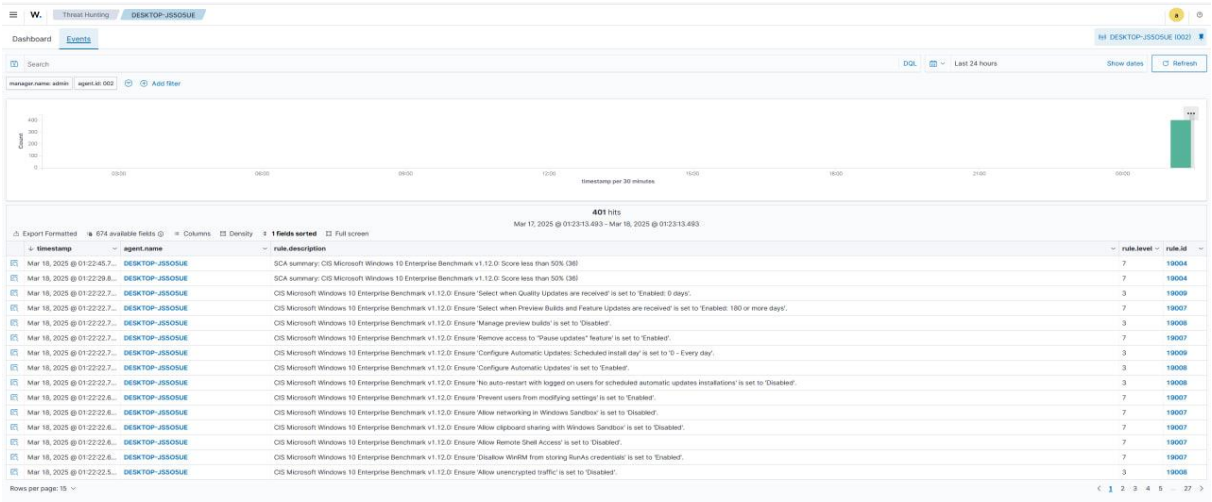


Рисунок 4 – Раздел Events SIEM Wazuh

Таким образом, были продемонстрированы простата и удобство установки и конфигурации SIEM Wazuh, что подтверждает его актуальность внедрения в учебный процесс на кафедре защиты информации для развития следующих навыков у студентов:

1 Определение уязвимостей информационной системы с помощью платформы Wazuh.

2 Работа с системами мониторинга и журналирования событий информационной системы.

3 Устранение выявленных уязвимостей в информационной системе.

Список использованных источников:

1 Computer security resource center [Электронный ресурс]. – Режим доступа: https://csrc.nist.gov/glossary/term/security_information_and_event_management_tool

2 Платформа Wazuh [Электронный ресурс]. – Режим доступа: https://documentation.wazuh.com/

3 Установщик Wazuh Агента [Электронный ресурс]. – https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html

UDC 004.056.53

WAZUH SIEM SYSTEM CONFIGURATION

Bahonski I.A., Zhuk K.D.

Belarusian State University of Informatics and Radioelectronics,

Minsk, Republic of Belarus

Belousova E.S. – PhD (Tech.), Ass. Prof. of Department of IP

Annotation. This article explains how to deploy the open-source Wazuh SIEM platform. It covers key installation steps: deploying Wazuh Manager on an Ubuntu server, changing the administrator password, installing agents on Windows devices, and configuring log monitoring. The Wazuh platform provides collection, analysis, and visualization of security data, allowing you to study threat detection, event analysis, and response methods in real-world conditions. Implementing the Wazuh SIEM helps you develop practical skills in working with modern cybersecurity tools.

Keywords. SIEM, Wazuh, open source, threat detection, file integrity monitoring, log analysis, ELK, agents, Ubuntu, Windows 10, Wazuh Manager, installation, ossec.conf configuration, Threat Hunting, Dashboard, Events, web interface, agent registration, security logs, cybersecurity, information infrastructure, data visualization, threat management, systems integration.

ФИШИНГ И АНТИФИШИНГ.КАК ЗАЩИТИТЬ ПОЛЬЗОВАТЕЛЕЙ В КОРПОРАТИВНОЙ СРЕДЕ

Безбородов Д.В.
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Латушко М.М.

Аннотация. В условиях стремительной цифровизации все сферы жизни, включая государственные и корпоративные структуры, сталкиваются с возрастающим числом киберугроз. Среди них фишинг — один из наиболее распространённых и эффективных методов социальной инженерии. В данной научной работе рассматриваются современные типы фишинга, методы его детектирования и предотвращения, особенности противодействия в корпоративной и государственной среде, а также перспективы развития антифишинговых технологий. Особое внимание уделено специфике угроз для силовых структур и методам их нейтрализации.

В условиях стремительной цифровизации все сферы жизни, включая государственные и корпоративные структуры, сталкиваются с возрастающим числом киберугроз. Среди них фишинг — один из наиболее распространённых и эффективных методов социальной инженерии. В данной научной работе рассматриваются современные типы фишинга, методы его детектирования и предотвращения, особенности противодействия в корпоративной и государственной среде, а также перспективы развития антифишинговых технологий. Особое внимание уделено специфике угроз для силовых структур и методам их нейтрализации.

Цифровая трансформация значительно повысила зависимость бизнеса, государства и общества от информационных технологий. Это сделало киберпространство приоритетной целью для злоумышленников. Одной из самых массовых и сложных к выявлению угроз остаётся фишинг. Его эффективность обусловлена тем, что он эксплуатирует человеческий фактор — доверие, недостаточную осведомлённость, усталость, повседневную рутину. В отличие от технических атак, фишинг требует минимальных ресурсов, но способен нанести колоссальный ущерб.

Для силовых структур, обладающих особым статусом и обрабатывающих чувствительную информацию, фишинговые атаки представляют особую опасность. Их успешное проведение может повлечь утечку государственной тайны, нарушение работы критически важных систем и компрометацию оперативных мероприятий.

Эволюция фишинга:

Исторически фишинг развивался от примитивных писем с орфографическими ошибками до сложных, персонализированных атак, которые используют данные из социальных сетей, корпоративных ресурсов и утечек. Сегодня злоумышленники применяют методы таргетирования, глубокого изучения поведения жертвы (behavioral profiling), а также технологии deepfake и искусственный интеллект.

Классификация фишинга и его признаки:

- Email-фишинг — массовая рассылка писем с вредоносными ссылками или вложениями;

- Spear phishing — атаки, ориентированные на конкретных лиц с персонализированным содержанием;

- Whaling — фишинг, нацеленный на руководителей и управленцев высокого уровня;

- Vishing — телефонные звонки, маскирующиеся под службы поддержки;

- Smishing — фишинг через SMS и мессенджеры;

- Фарминг — перенаправление пользователя на фальшивые сайты посредством DNS-отравления.

Основные признаки фишинга:

- Давление на пользователя: срочные просьбы, угрозы;

- Ошибки в орфографии, непривычная стилистика;

- Поддельные адреса отправителей и доменные имена;

- Запросы конфиденциальной информации.

Силовые ведомства являются приоритетной целью фишинговых кампаний из-за:

- наличия закрытой информации;

- использования устаревших каналов связи;

- ограниченного уровня цифровой грамотности у отдельных сотрудников;

- сложности многоуровневой структуры и распределённости систем управления.

Типовые сценарии атак включают:

- рассылку вредоносных писем с темами приказов и распоряжений;

- имитацию обращений от вышестоящих инстанций;

- фальсификацию писем из государственных структур.

Методы защиты и технологии антифишинга

- Аутентификация и шифрование: внедрение S/MIME, TLS, двухфакторной аутентификации;

- Проверка отправителей (SPF, DKIM, DMARC): предотвращение подделки доменов;

- SIEM-системы и поведенческий анализ: обнаружение аномалий на основе логов;

- Обновление антивирусов и прокси-фильтров: своевременная реакция на новые угрозы;

- Изоляция среды выполнения вложений (sandboxing).

Дополнительные предложения по усилению защиты:

- Внедрение автоматизированных систем обнаружения фишинга на основе нейросетей, способных адаптироваться к новым паттернам угроз;

- Использование honeypot-механизмов для анализа поведения атакующих и выявления источников фишинговых атак;

- Создание межведомственных центров быстрого реагирования на фишинговые инциденты с возможностью оперативного обмена информацией;

- Разработка специализированных решений для мобильных устройств, включая антифишинговые фильтры на уровне операционной системы;

- Внедрение киберучений с фокусом на имитацию фишинговых сценариев для формирования устойчивых поведенческих навыков у сотрудников.

Ключевым фактором устойчивости к фишингу является сознательное поведение сотрудников. Для этого необходимо:

- регулярное проведение тренингов и тестов с элементами геймификации;

- формирование каналов оперативного оповещения и отчётности о подозрительных письмах;

- развитие культуры кибербезопасности и обратной связи внутри подразделений.

По данным ENISA, в 2023 году фишинг стал причиной более 36% всех инцидентов информационной безопасности в ЕС. В России, по отчётам ФСТЭК, около 40% атак на госорганы связаны с фишинговыми письмами. Это подтверждает высокую актуальность темы.

Будущее антифишинга связано с:

- применением ИИ для анализа аномального поведения пользователей;

- интеграцией антифишинга в архитектуру Zero Trust;

- развитием поведенческой аналитики (UEBA);

- защитой от голосовых и видеофейков;
- международным обменом данными о фишинговых доменах и IP-адресах;
- внедрением интеллектуальных помощников и систем обучения.

Фишинг — это вызов, который требует междисциплинарного подхода. Только комплексные меры, сочетающие технологии, регламенты и обучение, могут гарантировать устойчивость к фишинговым угрозам. В условиях роста гибридных угроз и активизации внешнего вмешательства, особенно для силовых структур, тема антифишинга становится вопросом не только информационной, но и национальной безопасности.

Список использованных источников:

1. IBM Security Data Breach Report 2024.
2. ENISA Threat Landscape 2023.
3. Verizon Data Breach Investigations Report (DBIR) 2023.
4. Bruce Schneier, "Secrets and Lies: Digital Security in a Networked World."
5. Соловьёв А.В., "Информационная безопасность: Учебное пособие." — М.: Инфра-М, 2022.
6. Anti-Phishing Working Group Reports.
7. OWASP Phishing Awareness Guide.
8. NIST SP 800-61: Computer Security Incident Handling Guide.
9. ФСТЭК России. Методические рекомендации по обеспечению защиты информации.

УДК 621.376

АНАЛИЗ ПРОЦЕССОВ МОДУЛЯЦИИ И ДЕМОДУЛЯЦИИ В СИСТЕМЕ ТЕЛЕКОММУНИКАЦИЙ

Биюмен Е.А., Макареня Е.А., студенты гр. 361401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Фильченкова Т.М. – ст. преподаватель каф. ЗИ

Аннотация. Анализ процессов модуляции и демодуляции в системе телекоммуникаций представляет собой исследование, в ходе которого были рассмотрены методы формирования, модуляции и последующей демодуляции радиоимпульса с целью выделения исходной огибающей сигнала. В работе использовалась программная реализация на языке Python, позволяющая смоделировать как спектральное преобразование, так и воздействие различных фильтров, что критически важно для задач цифровой обработки сигналов в телекоммуникационных системах.

Ключевые слова. Амплитудная модуляция, демодуляция, Python, спектр сигнала, фильтр Чебышева, фильтр Баттерворта, быстрое преобразование Фурье.

Математическое моделирование позволяет провести исследование модуляции и демодуляции сигналов в системах телекоммуникаций. Этот метод относится к теоретическим и характеризуется следующими достоинствами: 1) не нужна практическая реализация устройств для их осуществления (это сокращает экономические затраты); 2) есть возможность имитировать разные условия работы исследуемых устройств систем телекоммуникаций (это позволяет произвести оценку качества и эффективность системы).

Цель данной научно-исследовательской работы: провести анализ процессов модуляции и

демодуляции в системе телекоммуникаций посредствам математического моделирования. Задачи данной работы: 1) провести теоретическое исследование процесса модуляции по схеме, представленной на рисунке 1; 2) выполнить математическое моделирование процесса демодуляции.

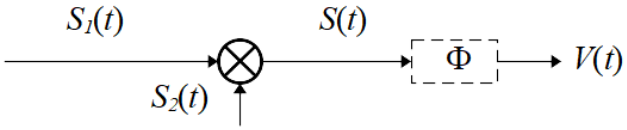


Рисунок 1 – Схема амплитудной модуляции

Исходные данные для моделирования:

– сигнал $S_1(t)$ – полезный информационный сигнал:

$$S_1(t) = \begin{cases} A, |t| \le \frac{T}{2} \\ 0, |t| > \frac{T}{2} \end{cases}, \quad 1)$$

где A – амплитуда радиоимпульса; T – период радиоимпульса.

– сигнал $S_2(t)$ – несущее колебание:

$$S_2(t) = cos(2\pi f_0 t) \quad 2)$$

где f_0 – частота несущего колебания.

– выполнение условия $2f_0 >> 1/T$,

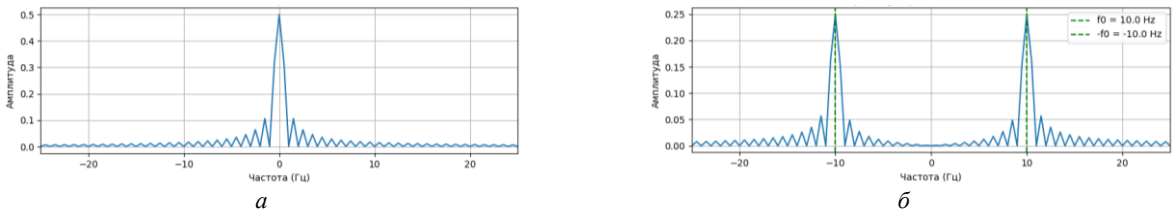
– f_0 = 10 Гц (частота несущего сигнала);

– A = 1 В (амплитуда радиоимпульса);

– T = 1 с (период радиоимпульса);

– f_s = 1000 Гц (частота дискретизации, для преобразований Фурье).

Такой метод модуляции должен, согласно теории, приводить к расщеплению спектральной плотности импульса на две части, которые смещаются на частоты $\pm f_0$, что подтверждается полученной нами визуализацией спектров, построенных с помощи быстрого преобразования Фурье (FFT) (рисунок 2) [1].



а *б*

а – спектр радиоимпульса $S_1(t)$; б – спектр модулированного сигнала S(t);

Рисунок 2 – Схема амплитудной модуляции

Демодуляция осуществляется посредством повторного умножения модулированного сигнала на несущий сигнал, что приводит к появлению как полезной составляющей, так и паразитных компонент (рисунок 3), их можно увидеть на частотах $2f_0$ (в нашем случае ±20 Гц). Для восстановления исходного сигнала применяется фильтрация с помощью фильтров нижних

частот.

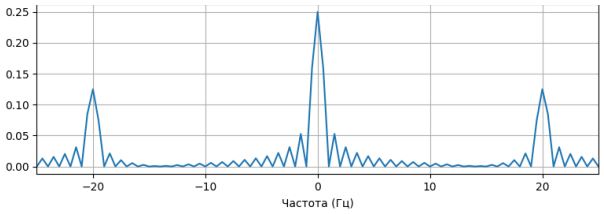


Рисунок 3 – Спектр сигнала после демодуляции

В работе были использованы два типа фильтров – фильтр Баттерворта и фильтр Чебышева первого рода – с порядком 4 и частотой среза, равной несущей f_0, АЧХ фильтров представлены на рисунке 4.

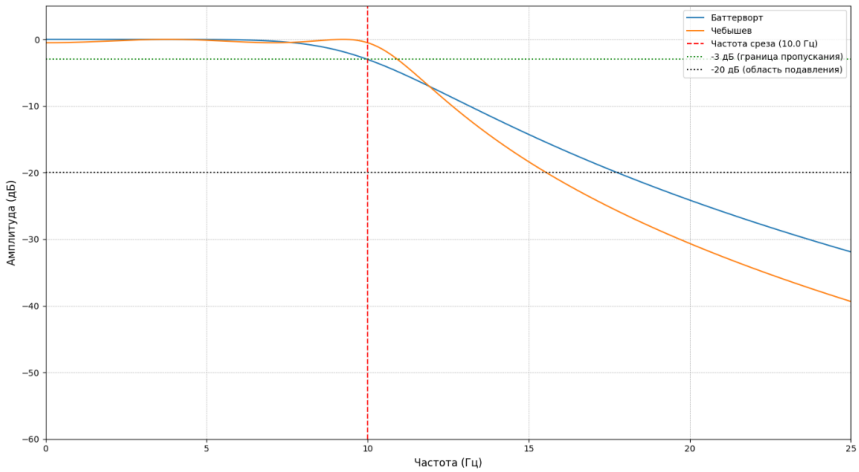
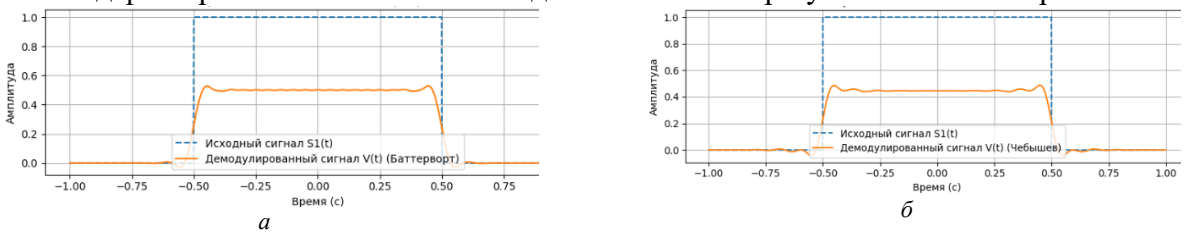


Рисунок 4 – АЧХ фильтров Баттерворта и Чебышева

Сигналы, полученные после демодуляции и фильтрации приведены на рисунке 5. Можно заметить, что восстановленный сигнал после фильтра Чебышева имеет большую рябь, по сравнению с фильтрацией Баттерворта. Это явление напрямую связано с АЧХ фильтров (рисунок 4). На графике АЧХ фильтра Чебышева есть незначительные колебания до частоты среза. Этот вид фильтра оказывает меньшее подавление частот сразу после частоты среза.



а *б*

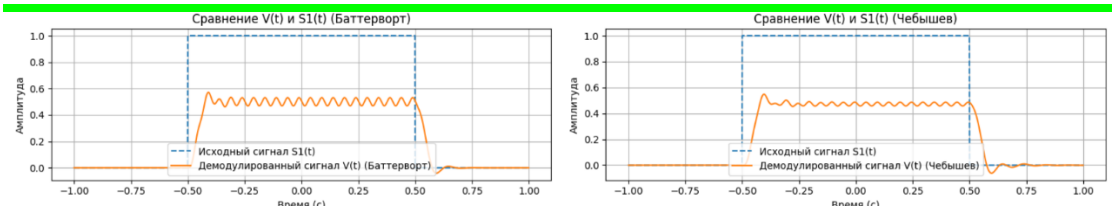
а – вид демодулированого сигнала с фильтром Баттерворта; б – вид демодулированого сигнала с фильтром Чебышева;

Рисунок 5 – Сигналы после демодуляции и фильтрации

В программной реализации все этапы – от формирования исходного прямоугольного импульса до вычисления спектральных плотностей и визуализации временных и частотных характеристик – были реализованы с использованием библиотеки NumPy и пакета matplotlib. Для анализа спектров использовалась быстрое преобразование Фурье (FFT), а вычисленные спектры корректно центрировались с помощью fftshift (построение спектра относительно нулевой частоты) [2].

Нами была установлена зависимость конечного результата демодуляции в случаях

использования функций lfilter и filtfilt. Первый вариант даёт фазовые искажения, но отражает реалистичную работу системы, второй – устраняет сдвиг фазы и даёт более гладкий результат, что позволяет лучше сравнивать сигналы (до и после демодуляции). В данной научно-исследовательской работе мы привели результаты для случая filtfilt на рисунке 5, а на рисунке 6 – для lfilter.



а *б*

а – вид демодулированого сигнала с фильтром Баттерворта; б – вид демодулированого сигнала с фильтром Чебышева;

Рисунок 6 – Сигналы после демодуляции и фильтрации с использованием функции lfilter

Сравнительный анализ фильтрации проводился посредством вычисления среднеквадратичной ошибки (MSE) и максимальной ошибки между восстановленным сигналом и исходным прямоугольным импульсом. Полученные результаты показали, что оба фильтра – как Баттерворта, так и Чебышева – способны в достаточной мере выделить огибающую, однако фильтр Баттерворта продемонстрировал более гладкую амплитудно-частотную характеристику, что обеспечивает менее выраженные искажения формы импульса (рисунок 5, 6). Полученные значения ошибок:

– среднеквадратичная ошибка (MSE) для Баттерворта равна 0,129629;

– максимальная ошибка для Баттерворта равна 0,750481;

– среднеквадратичная ошибка (MSE) для Чебышева равна 0,156025;

– максимальная ошибка для Чебышева равна 0,778497.

Таким образом, выполненное исследование подтверждает, что выбранная схема модуляции и демодуляции является эффективной для задач выделения огибающей. Реализованный на Python код продемонстрировал возможность проведения комплексного анализа как во временной, так и в частотной областях, а также позволил оценить качество фильтрации с учётом влияния параметров фильтра.

Список использованных источников

1. Смещение спектра сигнала [Электронный ресурс]. Режим доступа: https://studfile.net/preview/8761054/page:7/. Дата доступа: 10.03.2024.

2. filtfilt — SciPy v1.15.2 Manual [Электронный ресурс]. Режим доступа: https://docs.scipy.org/doc/scipy/reference/generated/scipy.signal.filtfilt.html. Дата доступа: 10.03.2024.

UDC 621.376

ANALYSIS OF MODULATION AND DEMODULATION PROCESSES IN TELECOMMUNICATION SYSTEM

Biyumen E.A., Makarenya E.A., students of gr.361401

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Filchenkova T.M. – Senior Lecturer

Annotation. The analysis of modulation and demodulation processes in a telecommunication system is a study that examined the methods of formation, modulation and subsequent demodulation of a radio pulse in order to extract the original envelope of the signal. The work used a software implementation in the Python language, which allows modelling both the spectral transformation and the effects of various filters, which is critical for digital signal processing tasks in telecommunication systems.

Keywords. *Amplitude modulation, demodulation, Python, signal spectrum, Chebyshev filter, Butterworth filter, fast Fourier transform.*

РАЗРАБОТКА СТРУКТУРНОЙ СХЕМЫ ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Восковцева К.Р., учащаяся по направлению «Информационная безопасность»,
Клиндухов Я.А., учащийся по направлению «Информационная безопасность»

Национальный детский технопарк
г. Минск, Республика Беларусь

Тимофеев А.М. – канд. техн. наук, доцент, доцент кафедры защиты информации БГУИР (научный руководитель)

Аннотация. С учетом требований законодательства Республики Беларусь в сфере защиты информации предложена структурная схема, посредством которой возможна реализация процедуры обезличивания персональных данных на базе метода изменения состава или семантики. Данная схема характеризуется достаточно высоким уровнем информационной безопасности, достигаемого посредством парирования частотного анализа обезличенных персональных данных.

В настоящее время одной из наиболее важных задач, решаемых при построении информационных систем, является обеспечение защиты информации [1 – 3]. Защита информации подразумевает применение комплекса правовых, организационных и технических мер, направленных на обеспечение целостности (неизменности), конфиденциальности, доступности и сохранности информации [4]. В соответствие с требованиями законодательства Республики Беларусь [5, 6] собственник (владелец) информационной системы, предназначенной для обработки персональных данных (информации ограниченного распространения/предоставления) обязан принимать меры по обеспечению информационной безопасности персональных данных в случае, если персональные данные не являются общедоступными, а относятся к биометрическим, генетическим, специальным или иным персональным данным. Для обеспечения информационной безопасности персональных данных целесообразно использовать методы их обезличивания [6]. К числу таких методов относят метод изменения состава или семантики, сущность реализации которого заключается в обобщении, изменении или удалении части сведений, позволяющих идентифицировать субъекта персональных данных. Обезличивание персональных данных указанным выше методом не требует наличия больших вычислительных мощностей, однако характеризуется следующими недостатками. Например, удаление части сведений, позволяющих идентифицировать субъекта персональных данных, без их сохранения в отдельной базе данных приводит к утрате такого свойства обезличенных персональных данных, как полнота. Также важно отметить, что простые замены исходных символов персональных данных обезличенными сохраняют вероятности появления соответствующих символов обезличенных персональных данных. В этом случае нарушитель информационной безопасности имеет возможность, получив доступ к обезличенным персональным данным, рассчитать вероятности появления отдельных

символов и различных их сочетаний, что позволит ему раскрыть содержимое доверительной вычислительной базы (ДВБ).

В связи с этим целью данной работы являлась разработка схемы обезличивания персональных данных, построенной на базе метода изменения состава или семантики, которая свободна от недостатков существующих схем обезличивания персональных данных и не требует больших вычислительных ресурсов от оборудования легитимных пользователей. В качестве объекта исследования использован метод изменения состава или семантики. Предметом исследования являлась разработка структурной схемы, реализующей обезличивание персональных данных на основе метода изменения состава или семантики с применением набора ДВБ.

В рамках выполненных исследований разработана структурная схема обезличивания персональных данных, построенная на базе метода изменения состава или семантики. Сущность функционирования данной схемы заключается в следующем. Персональные данные, подлежащие обезличиванию, загружают в ДВБ, которая содержит набор таблиц подстановки ДВБ 1, ДВБ 2, …, ДВБ *N*. Персональные данные разбивают на блоки, каждый из которых последовательно обезличивают с помощью ДВБ 1, ДВБ 2, …, ДВБ *N*, ДВБ 1, ДВБ 2, …, ДВБ *N* и т.д. Важно отметить, что содержимое ДВБ необходимо сохранять в секрете и обновлять в соответствии с требованиями, предъявляемыми в месте эксплуатации информационной системы.

Выполненная оценка показала, что предложенные принципы обезличивания персональных данных на основе метода изменения состава или семантики, заключающиеся в использовании наборов ДВБ, позволили повысить уровень информационной безопасности обезличенных персональных данных за счет изменения вероятности появления символов обезличенных персональных данных по отношению к соответствующим символам исходных персональных данных.

Список использованных источников:

1. Ворона, В. А. Биометрическая идентификация личности / В. А. Ворона. – Москва : Горячая линия-Телеком, 2023. – 228 с.

2. Коллинз, М. Защита сетей. Подход на основе анализа данных / М. Коллинз. – Москва : ДМК Пресс, 2020. – 308 с.

3. Остапенко, Г. А. Информационные операции и атаки в социотехнических системах : организационно-правовые аспекты противодействия : учебное пособие / Г. А. Остапенко, Е. А. Мешкова ; под ред. В. Г. Кулакова. – 2-е изд., стер. – Москва : Горячая линия-Телеком, 2020. – 208 с.

4. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=2012&oldDoc=2008-279/2008-279(014-027).pdf&oldDocPage=1. – Дата доступа: 28.02.2025 г.

5. Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=12551&p0=H12100099. – Дата доступа: 28.02.2025 г.

6. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 10 декабря 2024 г. № 259 «Об изменении приказов Оперативно-аналитического центра при Президенте Республики Беларусь от 28 марта 2014 г. № 26 и от 20 февраля 2020 г. № 66» [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2024%20-%20259.pdf. – Дата доступа: 28.02.2025 г.

УДК 004.056

СРАВНИТЕЛЬНЫЙ АНАЛИЗ SIEM ДЛЯ КИБЕРЦЕНТРОВ

Рубанова К.В., студент гр.261401,

Голуб А.А., студент гр.261401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук, доцент

Аннотация. Статья посвящена роли SIEM-систем в обеспечении кибербезопасности и их интеграции в SOC. Проведен сравнительный анализ популярных SIEM-систем, таких как IBM QRadar Security Intelligence, Splunk Enterprise Security, Kaspersky Unified Monitoring and Analysis Platform (KUMA) и PT MaxPatrol SIEM. Изучены нормативные акты Республики Беларусь, регулирующие использование SIEM в центрах кибербезопасности. Рассматривается актуальность создания SOC и интеграции SIEM-систем в образовательные учреждения для защиты важных информационных ресурсов.

Ключевые слова. Кибербезопасность, киберинциденты, расследование, SIEM, SOC, корреляция событий, мониторинг, реагирование, угрозы, PT MaxPatrol SIEM, Kaspersky KUMA.

Расследование киберинцидентов – одна из ключевых задач кибербезопасности, и в этом процессе главную роль играет взаимодействие SIEM (Security Information and Event Management) и SOC (Security Operations Center). Современные кибератаки становятся все более сложными и изощренными, поэтому организации вынуждены оперативно выявлять и нейтрализовать угрозы. SOC, будучи центром мониторинга и реагирования [1], полагается на SIEM-системы, которые собирают, анализируют и коррелируют огромные объемы логов, помогая быстро обнаруживать инциденты. SIEM отслеживает активность пользователей, серверов, сетевого оборудования, объединяя разрозненные события в единую картину [2]. Например, множественные неудачные попытки входа, затем успешная авторизация с нового IP-адреса и скачивание большого объема данных могут свидетельствовать о проникновении нарушителем, что позволит SOC немедленно реагировать.

Расследование инцидентов с SIEM проходит в несколько этапов: первичный анализ тревоги, корреляция событий для выявления истинных угроз, реагирование, изоляция зараженных систем и последующий анализ для предотвращения аналогичных кибератак в будущем. Основные преимущества SIEM – автоматизированный анализ данных, визуализация сложных атак и снижение нагрузки на аналитиков. Однако система требует грамотной настройки, иначе возможны ложные срабатывания и перегрузка тревогами. Например, SIEM фиксирует аномальное поведение фишинговой кибератаки, специалисты, работающие в SOC, анализируют угрозу, изолируют зараженные устройства и предотвращают дальнейшее распространение кибератаки. Интеграция SIEM в работу SOC значительно повышает скорость и точность расследования инцидентов, что делает его незаменимым инструментом для защиты организации от современных киберугроз.

В Республике Беларусь важную роль в развитии SOC играют нормативные акты, регулирующие кибербезопасность. 14 февраля 2023 года был издан Указ № 40 «О кибербезопасности» [3], который установил единые требования к защите информации и обязал государственные и критически важные объекты информатизации (КВОИ) создать центры кибербезопасности для мониторинга и реагирования на инциденты. Развитие таких центров предполагает активное использование SIEM для анализа угроз и корреляции событий. 25 июля 2023 года вышел Указ № 130 «О мерах по реализации Указа президента Республики Беларусь от 14 февраля 2023 г. № 40» [4], который уточнил требования к функционированию SOC. В частности, центры кибербезопасности обязаны использовать SIEM-системы

для сбора и хранения логов, выявления аномалий и автоматизированного анализа киберинцидентов. Также SOC должны обеспечивать постоянный мониторинг сетевого трафика, проводить аудит событий безопасности и разрабатывать сценарии реагирования на угрозы. Соблюдение этих требований критично для повышения киберустойчивости организаций и защиты от сложных кибератак.

В таблице 1 представлен сравнительный анализ следующих SIEM [5]: IBM QRadar Security Intelligence (США), Splunk Enterprise Security (США), Kaspersky Unified Monitoring and Analysis Platform (KUMA) [6] (РФ), PT MaxPatrol (РФ). Интеграция SIEM в процессы SOC является основой современной защиты информации, обеспечивая оперативное выявление и нейтрализацию киберугроз. Сравнительный анализ различных SIEM-систем, демонстрирует их возможности и ограничения. Например, системы IBM QRadar Security Intelligence [7] и Splunk Enterprise Security [8] выделяются своей высокой скоростью обработки данных и гибкостью настройки правил корреляции, что делает их эффективными для крупных организаций с сложной IT-инфраструктурой. Kaspersky Unified Monitoring and Analysis Platform (KUMA) и PT MaxPatrol SIEM также являются перспективными решениями, предлагающими централизованную архитектуру и корреляцию событий, что важно для защиты от современных кибератак.

Таблица 1 – Сравнительная таблица SIEM-систем

Характеристика	IBM QRadar Security Intelligence	Splunk Enterprise Security	Kaspersky Unified Monitoring and Analysis Platform (KUMA)	PT MaxPatrol SIEM
Разработчик	IBM	Splunk Inc.	Лаборатория Касперского	Positive Technologies
Год выпуска	2011	2011	2020	2013
Архитектура	Централизо-ванная	Децентрализо-ванная	Централизо-ванная	Централизованная
Лицензирование	Коммерческое	Коммерческое	Коммерческое	Коммерческое
Методы анализа	Корреляция событий, поведенческий анализ, машинное обучение	Корреляция событий, анализ логов, UEBA, машинное обучение	Корреляция событий, поведенческий анализ, ML	Корреляция событий, UEBA, машинное обучение
Интеграция с Threat Intelligence	IBM X-Force, STIX/TAXII	Splunk Security Essentials, STIX/TAXII	Kaspersky Threat Intelligence	PT ISIM, STIX/TAXII
Основной язык написания	Java, Python	Python, Go	C++, Python	Java, C++
Поддерживаемые форматы логов	Syslog, JSON, CEF, LEEF и др.	Syslog, JSON, CEF и др.	Syslog, JSON, CEF	Syslog, JSON, CEF
Отчетность и дашборды	Гибкие дашборды, отчеты	Расширенные дашборды, поиск, отчеты	Кастомизируе-мые дашборды	Расширенные отчеты и визуализация
Скорость обработки данных	Высокая (оптимизиро-ванные алгоритмы обработки)	Высокая, но зависит от конфигурации	Средняя	Высокая
Гибкость настройки правил корреляции	Средняя	Высокая	Средняя	Высокая
Легкость развертывания	Сложная настройка	Требует мощных ресурсов	Относительно простая	Средняя сложность
Страна происхождения	США	США	Россия	Россия

В Республике Беларусь выбор SIEM-систем для центров кибербезопасности осуществляется в соответствии с реестром оперативно-аналитического центра при Президенте Республики Беларусь [9]. В этот реестр включены PT MaxPatrol SIEM и Kaspersky Unified Monitoring and Analysis Platform (KUMA), которые соответствуют требованиям к сбору, корреляции и анализу событий информационной безопасности. Эти решения обеспечивают выполнение нормативных требований по мониторингу и расследованию инцидентов.

Учитывая важность защиты персональных данных, интеллектуальной собственности, научных исследований и других важных активов в различных организациях, включая образовательные учреждения, становится актуальным вопрос об интеграции эффективных SIEM-систем в их процессы безопасности. Однако, в отличие от многих организаций, у которых уже создан SOC, образовательные учреждения, такие как БГУИР, не имеют таких структур. В этом контексте целесообразно рассмотреть создание полноценного SOC для образовательных учреждений, что позволит обеспечить непрерывный мониторинг и реагирование на инциденты безопасности. Для интеграции в такой SOC актуально выбрать SIEM-систему Kaspersky Unified Monitoring and Analysis Platform (KUMA), поскольку она обеспечивает централизованную архитектуру, корреляцию событий и поведенческий анализ, что важно для защиты от современных кибератак. Кроме того, KUMA соответствует требованиям нормативных актов Республики Беларусь и включена в реестр ОАЦ. Таким образом, создание SOC с интеграцией KUMA в образовательных учреждениях может существенно повысить уровень кибербезопасности и защитить важные информационные ресурсы.

Список использованных источников:

[1] SOC - центр мониторинга и реагирования [Электронный ресурс]. – Режим доступа: https://softline.ru/solutions/security/soc

[2] Применение SIEM для расследования инцидентов [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/otus/articles/854440/

[3] О кибербезопасности Указ № 40 от 14 февраля 2023 г. [Электронный ресурс]. – Режим доступа: https://president.gov.by/ru/documents/ukaz-no-40-ot-14-fevralya-2023-g

[4] ПРИКАЗ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ 25 июля 2023 г. № 130 [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2023%20-%20130.pdf

[5] Сравнение SIEM-систем [Электронный ресурс]. – Режим доступа: https://searchinform.ru/products/siem/sravnenie-siem-sistem/

[6] Центральный элемент вашей системы безопасности [Электронный ресурс]. – Режим доступа: https://go.kaspersky.com/ru-kuma

[7] IBM QRadar Security Intelligence Platform [Электронный ресурс]. – Режим доступа: https://www.ibm.com/docs/ru/qsip/7.4?topic=quick-start-guide

[8] Зачем вам нужен Splunk? Аналитика событий безопасности [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/tssolution/articles/419493/

[9] Реестр средств защиты информации, прошедших сертификацию [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/information-security-tools/activity/technical-and-cryptographic-information-protection/registry-ism

Comparative Analysis of SIEM for Cyber Centers

Rubanova K.V., student of group 261401
Golub A.A., student of group 261401
Belarusian State University of Informatics and Radioelectronics,
Minsk, Republic of Belarus

Belousova E.S. – Candidate of Technical Sciences, Associate Professor

Annotation. The article focuses on the role of SIEM systems in ensuring cybersecurity and their integration into Security Operations Centers (SOC). It analyzes a comparative table of popular SIEM systems, such as IBM QRadar Security Intelligence, Splunk Enterprise Security, Kaspersky Unified Monitoring and Analysis Platform (KUMA), and PT MaxPatrol SIEM. Special attention is paid to the regulatory acts of the Republic of Belarus governing the use of SIEM in cybersecurity centers. The article discusses the relevance of creating SOC and integrating SIEM systems into educational institutions to protect important information resources.

Keywords. Cybersecurity, cyber incidents, investigation, SIEM, SOC, event correlation, monitoring, response, threats, PT MaxPatrol SIEM, Kaspersky KUMA.

УДК 004.934

ИЗВЛЕЧЕНИЕ ПРИЗНАКОВ - MFCC ДЛЯ ОБРАБОТКИ РЕЧИ

До А.Т., магистрант гр.467311

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Зельманский О.Б. – канд. тех. наук, доцент

Аннотация. Извлечение признаков играет ключевую роль в системах обработки речи, и коэффициенты мел-частотного цепстра (MFCC) становятся одним из самых эффективных представлений, которые близко приближают человеческое слуховое восприятие. MFCC эффективно имитируют нелинейное восприятие человеческой слуховой системы, преобразуя звуковые сигналы в компактный набор дискриминативных признаков. Процесс извлечения включает несколько ключевых этапов: предварительная усиление для повышения высокочастотных компонент, фреймирование и окно для захвата краткосрочных признаков, преобразование Фурье для получения спектральной информации, обработка фильтров Мел для приближения чувствительности человеческого слуха, логарифмическое сжатие для акцентирования перцептивно важных компонент и, наконец, дискретное косинусное преобразование (DCT) для декорреляции признаков и получения цепстральных коэффициентов.

Ключевые слова. Речевые сигналы, распознавание речи, MFCC, извлечение признаков, преобразование Фурье, DCT.

Чтобы преобразовать человеческую речь в информацию, которую компьютер может понять и обработать, система распознавания речи должна пройти через процесс цифровой обработки сигналов, состоящий из нескольких важных этапов. Каждый этап играет ключевую роль в обеспечении точности и эффективности системы. Данная статья сосредоточена на методе извлечения признаков MFCC (мел-частотные кепстральные коэффициенты) – популярной технике в обработке речи, особенно в задачах распознавания речи (ASR) и обработки звуковых сигналов. Процесс начинается с деления входного звукового сигнала на короткие фреймы по 25 мс с перекрытием в 10 мс для обеспечения непрерывности. Затем каждый фрейм преобразуется в вектор размерности 39 с помощью обработки, включающей преобразование Фурье, применение фильтра шкалы Мел и вычисление кепстральных коэффициентов. Это создает признаки с низким уровнем шума, высокой независимостью и эффективной акустической репрезентацией, отвечающими требованиям алгоритмов машинного обучения, при этом обеспечивая разумные вычислительные затраты. Весь процесс, начиная от сырого звукового сигнала до окончательных признаков MFCC, подробно иллюстрирован на рисунке ниже.

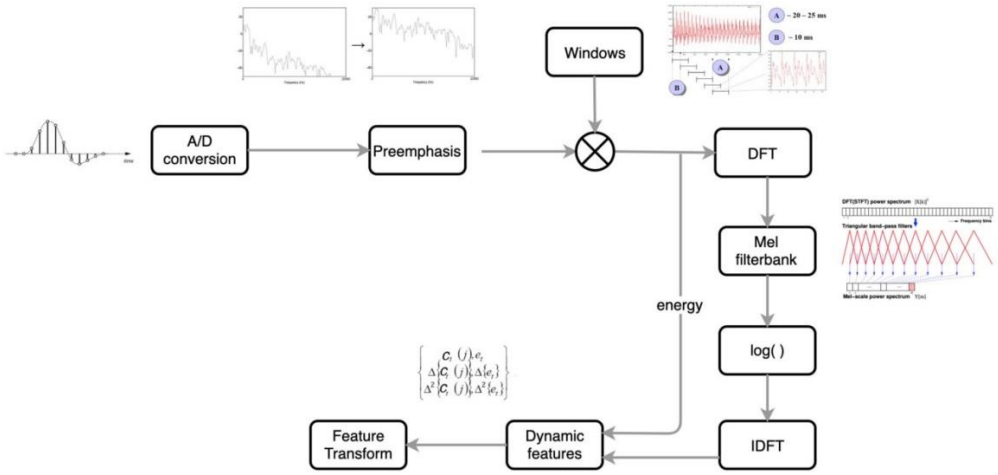


Рисунок 1 – Процесс извлечения признаков MFCC из речевого сигнала

Поскольку звук является непрерывным (аналоговым) сигналом, в то время как компьютеры обрабатывают данные в дискретной (цифровой) форме, процесс преобразования требует выборки сигнала в равномерно распределенные моменты времени с определенной частотой, называемой частотой дискретизации (sample rate). Например, при sample_rate = 8000 Hz система будет получать 8000 значений амплитуды звука каждую секунду, создавая точное цифровое представление оригинального сигнала.

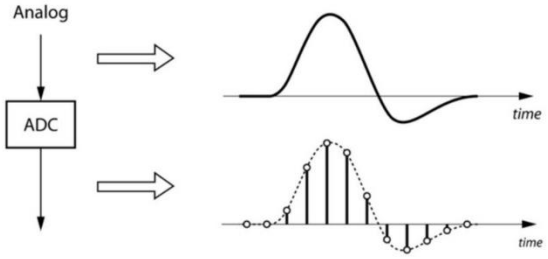


Рисунок 2 – Процесс преобразования аналогового сигнала в цифровой (АЦП)

Человеческое ухо может воспринимать звук в диапазоне от 20 Гц до 20 000 Гц. Согласно теореме дискретизации Найквиста-Шеннона: для сигнала с компонентами частоты ≤ f_m, чтобы гарантировать, что дискретизация не приведет к потере информации (aliasing), частота дискретизации f_s должна удовлетворять условию $f_s \geq 2\, f_m$.

Таким образом, чтобы обеспечить отсутствие потерь информации при дискретизации, частота дискретизации должна составлять $f_s = 44100$ Гц. Однако во многих случаях достаточно использовать $f_s = 8000$ Гц или $f_s = 16000$ Гц.

Из-за особенностей строения гортани и органов артикуляции наша речь имеет следующие характеристики: звуки низкой частоты обладают высокой энергией, тогда как звуки высоких частот имеют довольно низкий уровень энергии. В то же время высокие частоты содержат много информации о фонемах. Поэтому нам нужен этап предварительного усиления (pre-emphasis), чтобы повысить уровень этих высокочастотных сигналов.

$$x'[t_d] = x'[t_d] - \alpha x[t_d\text{-}1] \qquad 0{,}95 < \alpha < 0{,}99$$

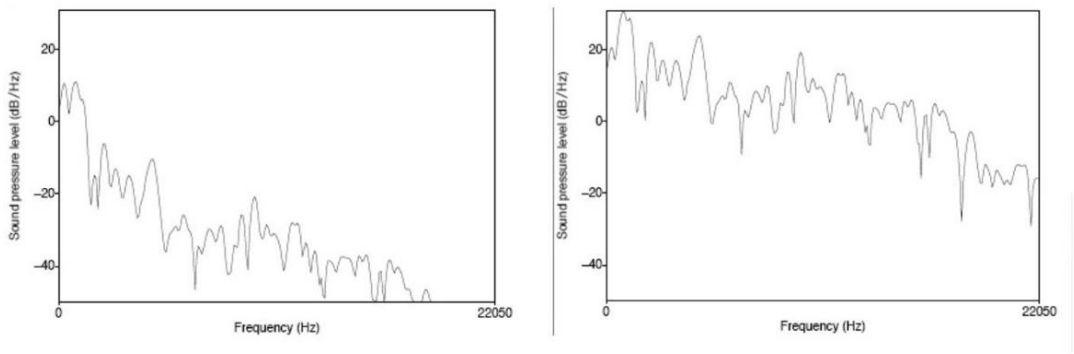


Рисунок 3 – Предварительное усиление высоких частот (Pre-emphasis) в обработке речи

Вместо того чтобы применять преобразование Фурье к длинному участку звука, мы скользим по сигналу с помощью окна, чтобы извлечь фреймы, а затем применяем ДПФ (дискретное преобразование Фурье) к каждому из этих фреймов. Средняя скорость речи человека составляет около 3-4 слов в секунду, каждое слово состоит из 3-4 звуков, а каждый звук делится на 3-4 части. Таким образом, 1 секунда звука делится на 36-40 частей. Мы выбираем ширину каждого фрейма около 20-25 мс, что достаточно для охвата одной части звука. Фреймы перекрываются друг с другом на 10 мс, чтобы можно было захватить изменения контекста.

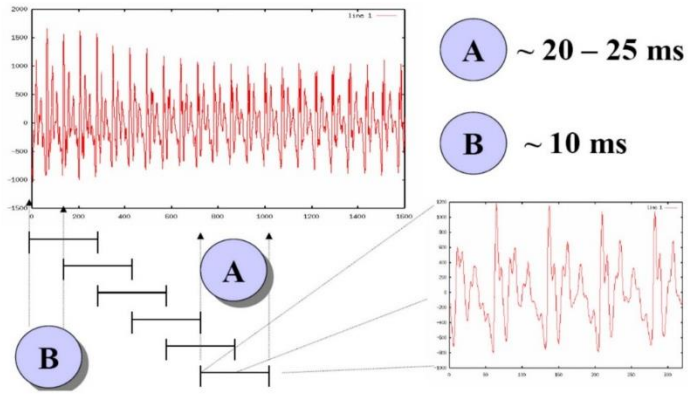


Рисунок 4 – Анализ речи методом скользящего окна (Framing) с ДПФ

Однако обрезка фрейма приводит к резкому снижению значений на обоих краях фрейма (до нуля), что приводит к тому, что при применении ДПФ в частотной области возникает много шумов на высоких частотах. Чтобы исправить это, необходимо сгладить фрейм, умножив его на несколько типов окон. Существуют несколько распространенных окон, таких как окно Хэмминга, окно Ханнинга и другие, которые помогают постепенно снижать значения на краях фрейма.

На каждом фрейме мы применяем ДПФ (дискретное преобразование Фурье) по формуле:

$$X[k] = \sum_{n=0}^{N-1} \mathrm{x[n]} \exp\left(-j\frac{2\pi}{N}kn\right)$$

На каждом фрейме мы получаем список значений амплитуды (magnitude) для каждой частоты от 0 до N. Применяя это ко всем фреймам, мы получаем спектрограмму, как показано ниже. Ось x – это ось времени (соответствующая порядку фреймов), ось y представляет диапазон частот от 0 до 10000 Гц, а значение амплитуды на каждой частоте отображается цветом. Наблюдая за этой

спектрограммой, мы замечаем, что на низких частотах обычно высокая амплитуда, а на высоких частотах – низкая амплитуда.

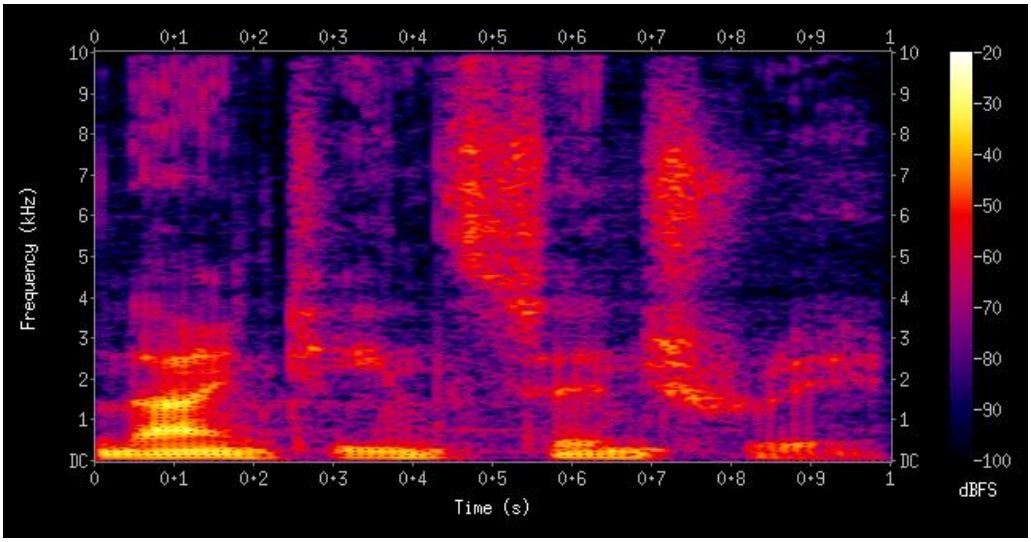


Рисунок 5 – Распределение звуковой энергии по времени и частоте

Человеческое слуховое восприятие имеет особенности нелинейной обработки звука, которые полностью отличаются от обычных измерительных устройств. В частности, человеческое ухо имеет высокую чувствительность в низкочастотном диапазоне (около 20 Гц - 2 кГц), но значительно снижает чувствительность в высокочастотном диапазоне (выше 5 кГц). Чтобы точно смоделировать, как человек воспринимает звук, нам необходимо создать механизм частотного отображения (frequency mapping), который имитирует эту нелинейную характеристику слуховой системы.

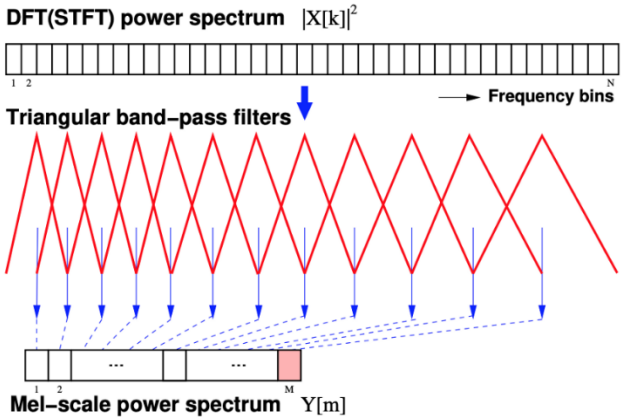


Рисунок 6 – Процесс извлечения мел-спектральных признаков из кратковременного преобразования Фурье (КПФ)

Сначала мы возводим в квадрат значения в спектрограмме, получая спектр мощности ДПФ (DFT power spectrum). Затем мы применяем набор полосовых фильтров Mel-scale на каждом диапазоне частот (каждый фильтр применяется к определенному диапазону частот). Значение на выходе каждого фильтра – это энергия диапазона частот, который этот фильтр покрывает. В результате мы получаем спектр мощности в масштабе Мел (Mel-scale power spectrum). Кроме того, фильтры, используемые для низких частот, обычно уже, чем фильтры для высоких частот.

Этот процесс также можно описать с помощью иллюстрации ниже:

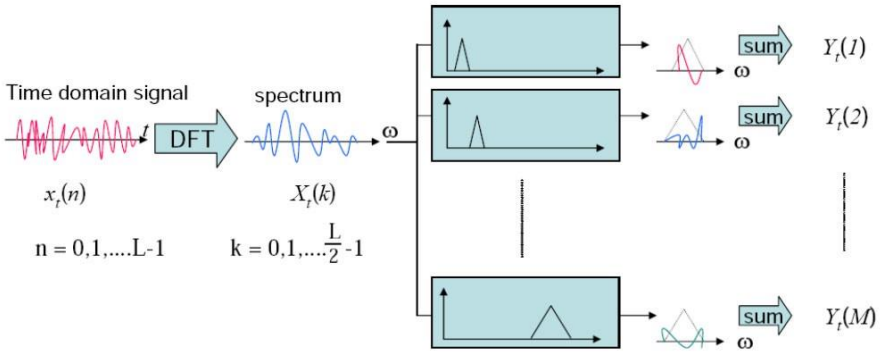


Рисунок 7 – Преобразование временного сигнала в мел-спектр с использованием полосовых фильтров

Фильтровая банка Мел возвращает спектр мощности звука, также известный как спектр энергии. На самом деле, человек менее чувствителен к изменениям энергии на высоких частотах и более чувствителен на низких частотах. Поэтому мы будем вычислять логарифм спектра мощности в масштабе Мел (Mel-scale power spectrum). Это также помогает уменьшить незначительные вариации звука для распознавания речи.

В обработке речи информация о основной частоте F0 (около 125 Гц у мужчин и 210 Гц у женщин) обычно не полезна для распознавания речи. Чтобы исключить F0 и оставить только важные форманты (F1, F2, F3 и так далее), мы используем обратное преобразование Фурье (IDFT) для перехода сигнала в область цепстрюма (Cepstrum) – техника, название которой образовано путем обращения слова "спектр" (spectrum). В области цепстрюма информация о F0 и формантах четко разделяется, что позволяет легко удалить компонент F0, просто взяв 12 первых цепстральных коэффициентов (соответствующих формантам). Это преобразование также можно выполнить с помощью дискретного косинусного преобразования (DCT), которое создает меньше коррелирующие признаки, что идеально подходит для алгоритмов машинного обучения. В конечном итоге мы получаем 12 цепстральных признаков, сосредоточенных на фонетических характеристиках, не зависимых от высоты голоса каждого человека.

Таким образом, из каждого кадра мы извлекли 12 цепстральных признаков, которые стали первыми 12 признаками MFCC. 13-й признак – это энергия этого кадра, вычисляемая по формуле:

$$Energy = \sum_{t=t_1}^{t_2} x^2[t]$$

В распознавании речи информация о временных изменениях играет важную роль в определении фонем, особенно на переходных позициях между фонемами (таких как начало или конец согласного). Эти изменения очень явные, и фонемы могут быть распознаны на основе этих изменений. Следующие 13 коэффициентов – это первая производная (по времени) первых 13 признаков. Она содержит информацию о изменении от кадра t до кадра t+1. Формула:

$$d(t) = \frac{c(t+1) - c(t-1)}{2}$$

Аналогично, последние 13 значений MFCC представляют собой изменение d(t) во времени – производную d(t), а также вторую производную c(t). Формула:

$$b(t) = \frac{d(t+1) - d(t-1)}{2}$$

Таким образом, из 12 цепстральных признаков и 13-го признака мощности, проведя две производные, мы получаем 39 признаков. Это и есть признаки MFCC.

Метод извлечения признаков MFCC зарекомендовал себя как эффективный в обработке речи благодаря способности точно моделировать характеристики слуха человека через фильтр шкалы Мел, одновременно предоставляя компактный набор признаков благодаря цепстральному преобразованию. Несмотря на некоторые ограничения в чувствительности к шуму и фиксированной структуре фильтра, MFCC сохраняет важную позицию благодаря своим выдающимся преимуществам в вычислительной эффективности и надежности. Будущие направления развития сосредоточены на улучшении адаптивных фильтров, комбинировании с современными методами извлечения признаков и повышении устойчивости к шуму, что продолжает подтверждать ценность MFCC как в традиционных системах, так и в современных архитектурах глубокого обучения.

Список использованных источников:

1. Li, T.LH. Genre classification and the invariance of MFCC features to Key and Tempo / T.LH. Li, A.B. Chan // International Conference on MultiMedia Modeling, Taipei, 2011.

2. Mel-frequency cepstrum. [Электронный ресурс]. – Режим доступа: https://en.wikipedia.org/wiki/Mel-frequency_cepstrum – Дата доступа: 04.03.2025.

3. Распознавание речи. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Распознавание_речи – Дата доступа: 04.03.2025.

4. Мел-кепстральные коэффициенты (MFCC) и распознавание речи. [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/140828/– Дата доступа: 04.03.2025.

UDC 004.934

SOFTWARE FOR SPEECH DETECTION IN SIGNAL

Do A. T.

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Zelmansky O.B. – Candidate of Technical Sciences, Associate Professor

Annotation. Automatic detection of speech segments in audio signals is an important task in the field of natural language processing and human-computer interaction. This article proposes software based on the extraction of MFCC features (Mel-Frequency Cepstral Coefficients) combined with deep learning for accurately distinguishing speech from other components (noise, silence, music). The methodology includes signal preprocessing (noise filtering, normalization), extraction of mel-frequency features, and training of a CNN-LSTM model capable of analyzing both frequency characteristics and temporal sequences. Testing on the LibriSpeech and TIMIT datasets demonstrated an accuracy of 93.5% with an F1 score of 95.2%, surpassing traditional methods (SVM, HMM). The developed software also demonstrates the capability to operate in real-time on embedded devices, opening up prospects for applications in virtual assistants, medical dialogue analysis, and intelligent audio monitoring systems.

Keywords. Speech signals, speech recognition, MFCC, Feature extraction, Fourier transform, DCT.

УДК 621.317

ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК ИЗМЕРИТЕЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИГНАЛОВ

Змачинская У.А.[1], студент гр.361403, Маршалова К.Ц.[2], студент гр.361401

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Фильченкова Т.М. – ст. преподаватель каф. ЗИ

Аннотация. В данной работе проведен анализ двух сигналов с целью нахождения их спектральной плотности. Были построены графики спектров, с помощью языка программирования Python, что позволило наглядно оценить распределение энергии по частотам. Оценено различие сигналов по энергии, установлена зависимость между амплитудой и длительностью сигналов. Изучены практические применения сигналов в цифровой обработке и телекоммуникационных системах, что подчеркивает их важность в современных технологиях передачи информации.

Ключевые слова. Амплитуда, векторная диаграмма, временной интервал, комплексная экспоненциальная функция, косинусоидальная волна, метод Уэлча, модуляция, окно данных, периодограмма, ряд Фурье, сигнал, спектральная плотность, фаза, частота, шум, энергия.

В современном мире, охваченном потоками информации и данных, анализ сигналов становится важнейшей областью исследовательской и прикладной деятельности. Спектральный анализ сигналов, представляющий собой изучение распределения сигналов по частотам, занял центральное место в таких дисциплинах, как обработка аудио, радиосвязь, биомедицинская инженерия и многих других. Одним из ключевых аспектов в этой области является понимание того, как различные сигналы ведут себя в частотной области, что непосредственно связано с их временными характеристиками и свойствами.

Спектральная плотность мощности сигнала служит важным инструментом для оценки распределения энергии сигналов по частотам. Она позволяет исследователям и инженерам выявлять присутствие различных частот, их амплитуду и, следовательно, дает возможность проводить различные виды анализа, включая фильтрацию, распознавание и классификацию сигналов.

В этой работе мы сосредоточим внимание на анализе двух сигналов:

$$S_1(t) = a \cdot cos2\pi f_0 t, \quad (1)$$

$$S_2(t) = a \cdot e^{j2\pi f_0 t}. \quad (2)$$

Сигнал $S_1(t)$ представляет собой косинусоидальную волну, а сигнал $S_2(t)$ — комплексную экспоненциальную функцию. Оба сигнала имеют одинаковую частоту и амплитуду, соответственно равные 50 Гц и 1 В, что предоставляет уникальную возможность для сравнительного анализа. Основной задачей данной работы является оценка спектральных плотностей данных сигналов.

Существует множество методов для решения задач спектрального анализа временных рядов, однако, одним из эффективных способов оценивания спектра является метод Уэлча. Он позволяет получить оценку спектральной плотности прямо на основе исходного набора данных. А именно, этот метод включает усреднение оценок спектральной плотности для

нескольких сегментов сигнала, что помогает уменьшить шум и улучшить оценку.

Мы имеем в виду вычислительный алгоритм, включающий в себя разбиение всего интервала наблюдения длины N на конечное число неперекрывающихся или частично перекрывающихся сегментов длины $M < N$, вычисление по каждому из них периодограммы и ее последующее осреднение по числу сегментов длины M. При этом, говоря о периодограмме, вычисляемой по каждому из сегментов длины M, мы имеем в виду ее модифицированную версию, определяемую данным соотношением:

$$I_M^{\{B\}}(\omega) = \left|\sum_{k=1}^{M} b(k)X(k)e^{ik\omega}\right|^2 \left[2\pi \sum_{k=1}^{M} b^2(k)\right]^{-1} \quad (3)$$

Здесь $B = \{b(k), k = \overline{1,M}\}$ – так называемое окно данных, используемое для домножения (неравномерного взвешивания) отрезка реализации $\{X(k), k = \overline{1,M}\}$. Последовательность $b(k)$ чаще всего плавно убывает от середины отрезка реализации к его краям, чем достигается сглаживание краев реализации и в конечном счете уменьшение смещения (систематической ошибки смещения) периодограммы. Большое число разнообразных окон можно найти в [1–3]. В настоящей работе в качестве сглаживающих окон данных B при построении оценки Уэлча используем разложение в ряд Фурье при полиномиальных тригонометрических ядрах типа Джексона [4].

Следующим этапом вычисления спектральной плотности сигналов станет разработка кода, продемонстрированного на рисунке 1, где мы детально рассмотрим и подчеркнем, как этапы генерации сигналов, их спектрального анализа и визуализации взаимосвязаны и дополняют друг друга, обеспечивая полное понимание спектральных характеристик двух сигналов.

```
import numpy as np
import matplotlib.pyplot as plt
from scipy.signal import welch

# Параметры сигналов
fs = 1000  # Частота дискретизации (Гц)
t = np.arange(0, 1.0, 1/fs)  # Время от 0 до 1 секунды

# Параметры сигналов
a = 1       # Амплитуда
f0_1 = 50   # Частота для S1 (Гц)
f0_2 = 50   # Частота для S2 (Гц)

# Сигналы
S1 = a * np.cos(2 * np.pi * f0_1 * t)  # Сигнал 1
S2 = a * np.exp(1j * 2 * np.pi * f0_2 * t)  # Сигнал 2

# Нахождение спектральных плотностей с улучшенными параметрами
nperseg = 512  # Увеличение длины сегмента для более детального анализа
f1, Pxx1 = welch(S1, fs, nperseg=nperseg)
f2, Pxx2 = welch(np.real(S2), fs, nperseg=nperseg)

# Построение графиков
plt.figure(figsize=(12, 8))

# График для сигнала 1
plt.subplot(2, 1, 1)
plt.semilogy(f1, Pxx1, color='blue', linewidth=2)
plt.title('Спектральная плотность сигнала S1', fontsize=14)
plt.xlabel('Частота (Гц)', fontsize=12)
plt.ylabel('Спектральная плотность (V^2/Гц)', fontsize=12)
plt.xlim(0, 200)  # Ограничение по оси X для лучшего отображения
plt.grid(True)
plt.axvline(x=f0_1, color='red', linestyle='--', label='f0 = 50 Гц')
plt.legend()

# График для сигнала 2
plt.subplot(2, 1, 2)
plt.semilogy(f2, Pxx2, color='green', linewidth=2)
plt.title('Спектральная плотность сигнала S2', fontsize=14)
plt.xlabel('Частота (Гц)', fontsize=12)
plt.ylabel('Спектральная плотность (V^2/Гц)', fontsize=12)
plt.xlim(0, 200)  # Ограничение по оси X для лучшего отображения
plt.grid(True)

plt.tight_layout()
plt.show()
```

Рисунок 1 – Код для оценки спектральной плотности сигналов $S_1(t)$ и $S_2(t)$

После этого результаты визуализируются с помощью графиков, что поможет наглядно проиллюстрировать на рисунке 2 характеристики сигналов в частотной области.

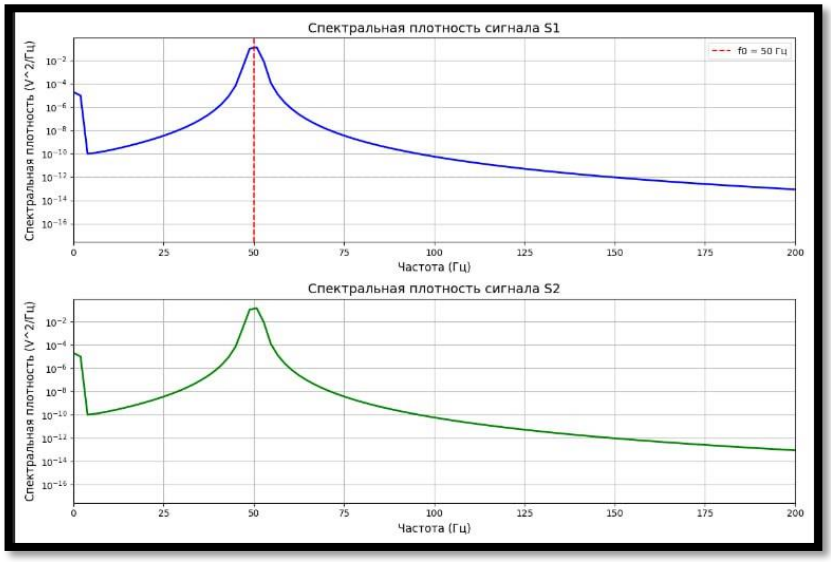


Рисунок 2 – Графики спектральных плотностей сигналов S1 и S2

Проанализировав рисунок 2, можно сделать вывод. Графики визуально совпадают, это ожидаемо из-за схожести частоты и амплитуды, но важно учитывать, что они могут иметь разные фазы и другие характеристики. На первом графике видно значительное пикирование на частоте 50 Гц, что соответствует частоте сигнала, полагаясь на формулу 1. Это подтверждает, что сигнал имеет ярко выраженную частотную составляющую. Убывание происходит на частотах отличных от 50 Гц, что свидетельствует о том, что сигнал в основном сосредоточен вокруг этой частоты. На втором графике видно более равномерное распределение спектральной плотности, без ярко выраженных пиков. Это связано с тем, что, глядя на формулу 2, можно сказать, что сигнал является комплексным экспоненциальным, который не имеет реальной амплитуды в классическом смысле. Спектральная плотность также убывает, но не так резко, как у сигнала $S_1(t)$.

При сравнении сигналов $S_1(t)$ и $S_2(t)$ по энергии мы можем выявить, что энергия сигнала является важным индикатором его мощности и, как следствие, его воздействия на систему. Сигнал $S_1(t)$ имеет четко определенную частоту равную 50 Гц и высокую энергию в этой области, что делает его более подходящим для приложений, требующих детального анализа частоты (например, в радиосвязи), а также будет полезен в задачах, где важно конкретное выделение частоты.

В нашем случае различия в энергетических характеристиках $S_1(t)$ и $S_2(t)$ могут быть проанализированы через их спектральные плотности. Сигнал $S_1(t)$ имеет конечную и фиксированную энергию в пределах одного периода, а сигнал $S_2(t)$ может иметь бесконечную энергию, если его рассматривать на бесконечном временном интервале, что делает его менее подходящим для анализа в классическом понимании энергии, но полезным в теоретических расчетах и приложениях, связанных с фазовой информацией.

Исследуемые сигналы могут быть применены в различных задачах цифровой обработки сигналов, включая компрессию, фильтрацию, детекцию и распознавание сигналов. Сигналы $S_1(t)$ и $S_1(t)$ могут быть полезны в телекоммуникационных системах, где важны точки сходства

и различия в обработке сигналов. Например, косинусоидальные волны могут использоваться в модуляции для передачи информации, а комплексные экспоненциальные функции – в задачах, связанных с фазовой манипуляцией или векторной диаграммой.

Список использованных источников

1. Журбенко, И.Г. Анализ стационарных и однородных случайных систем / И.Г. Журбенко. – М. : Изд-во Моск. ун-та, 1987. – 240 с.

2. Бриллинджер, Д. Временные ряды. Обработка данных и теория / Д. Бриллинджер. – М.:Мир, 1980. – 536 с

3. Kay, S.M. Modern Spectral Estimation: Theory and Application / S.M. Kay. – Englewood Cliffs (NJ):Prentice-Hall, 1988. – 543 p.

4. Алексеев, В. Г. Оценка спектральной плотности типа Уэлча. Случай дискретного аргумента / В. Г. Алексеев // Автометрия. – 2001. – № 6. – С. 92.

UDC 621.317

INVESTIGATION OF THE CHARACTERISTICS OF MEASURING TELECOMMUNICATION SIGNALS

Zmachynskaya U.A.[1], student of the gr..361403, Marshalova K.Z.[2], student of the gr.361401

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Filchenkova T.M. – Senior Lecturer

Annotation. In this paper, two signals are analyzed in order to find their spectral density. Graphs of the spectra were constructed using the python programming language, which made it possible to visually assess the distribution of energy across frequencies. The difference in energy between the signals is estimated, and the relationship between the amplitude and duration of the signals is established. Practical applications of signals in digital processing and telecommunication systems have been studied, which underlines their importance in modern information transmission technologies.

Keywords. *Amplitude, vector diagram, time interval, complex exponential function, cosine wave, Welch method, modulation, data window, periodogram, Fourier series, signal, spectral density, phase, frequency, noise, energy.*

УДК 004.93'1

СИСТЕМА УПРАВЛЕНИЯ АУТЕНТИФИКАЦИЕЙ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ РЕСУРСОВ С ИСПОЛЬЗОВАНИЕМ СКУД

Иванов А.П., Кисель А.В.

гр.161402

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Научный руководитель: Белоусова Е.С. – доцент кафедры ЗИ, кандидат технических наук, доцент.

Аннотация. В материалах доклада представлены результаты разработки и тестирования системы контроля и управления доступом на основе RFID-карты и

биометрической аутентификации, интегрированной с Keycloak. Данная система может использоваться для обучения студентов различных специальностей, включая 6-05-0611-02 «Информационная безопасность», для повышения их навыков в области информационной безопасности.

Ключевые слова: СКУД, RFID-карта, биометрическая аутентификация, Keycloak.

Введение. С развитием информационных технологий и ростом количества цифровых ресурсов обеспечение надежной аутентификации пользователей становится критически важной задачей. Традиционные методы, основанные только на парольной защите, не всегда обеспечивают достаточный уровень безопасности, особенно в крупных организациях. В связи с этим активно развивается многофакторной аутентификации, которая сочетает несколько уровней проверки пользователя.

Одним из эффективных решений является интеграция систем контроля и управления доступом с централизованными механизмами аутентификации. В такой системе пользователь сначала проходит проверку по RFID-карте, затем подтверждает личность с помощью биометрии, после чего данные передаются в систему управления доступом и аутентификацией, такую как Keycloak. На основании полученной информации происходит автоматическая разблокировка учетной записи и предоставление доступа к информационным ресурсам.

Актуальность данного подхода обусловлена ростом числа киберугроз, связанных с компрометацией учетных данных и несанкционированным доступом. Использование такой системы позволяет значительно повысить уровень безопасности, минимизировать риски несанкционированного доступа и обеспечить надежный контроль как за физическим объектам, так и за информационными ресурсами.

Цель данной научной работы заключается в разработке и реализации СКУД с интеграцией механизмов многофакторной аутентификации и управления учетными записями. Полученные результаты могут стать основой для создания безопасных и эффективных решений по защите корпоративных и государственных информационных ресурсов.

Основная часть. Для обеспечения надежной аутентификации пользователей и защиты информационных ресурсов была разработана система контроля и управления доступом с многофакторной аутентификацией. Основной задачей системы является повышение уровня безопасности и исключение несанкционированного доступа за счет использования RFID-карт и биометрической аутентификации, а также интеграции с системой управления учетными записями для централизованного контроля доступа.

Для эффективной работы системы была разработана четкая последовательность действий, которая начинается с идентификации пользователя через RFID-карту, затем выполняется биометрическая аутентификация, и только после этого осуществляется проверка учетной записи через систему Keycloak. Эта последовательность обеспечивает надежную защиту на каждом этапе процесса. На рисунке 1 представлена блок-схема, описывающая функционирование СКУД, а на рисунке 2 – блок-схема, описывающая функционирование система управления доступом и аутентификацией – Keycloak.

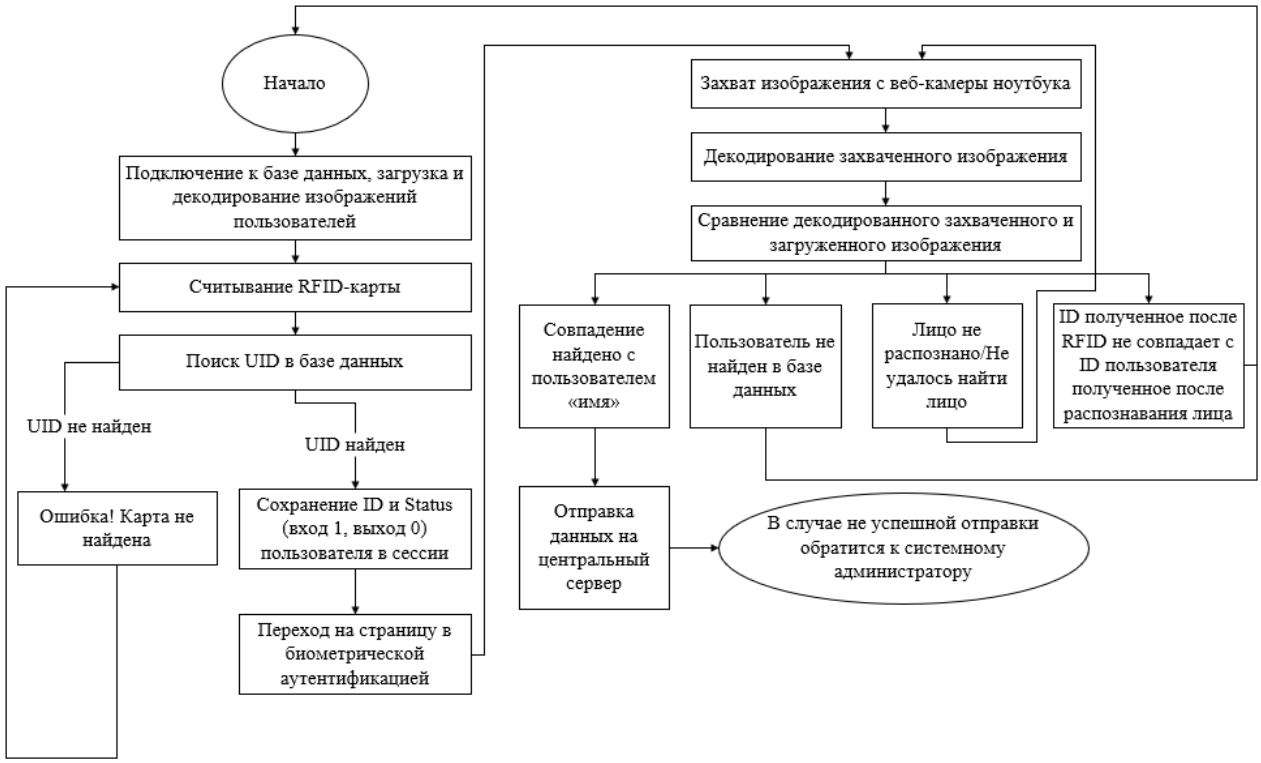


Рисунок 1 – Блок-схема функционирования СКУД

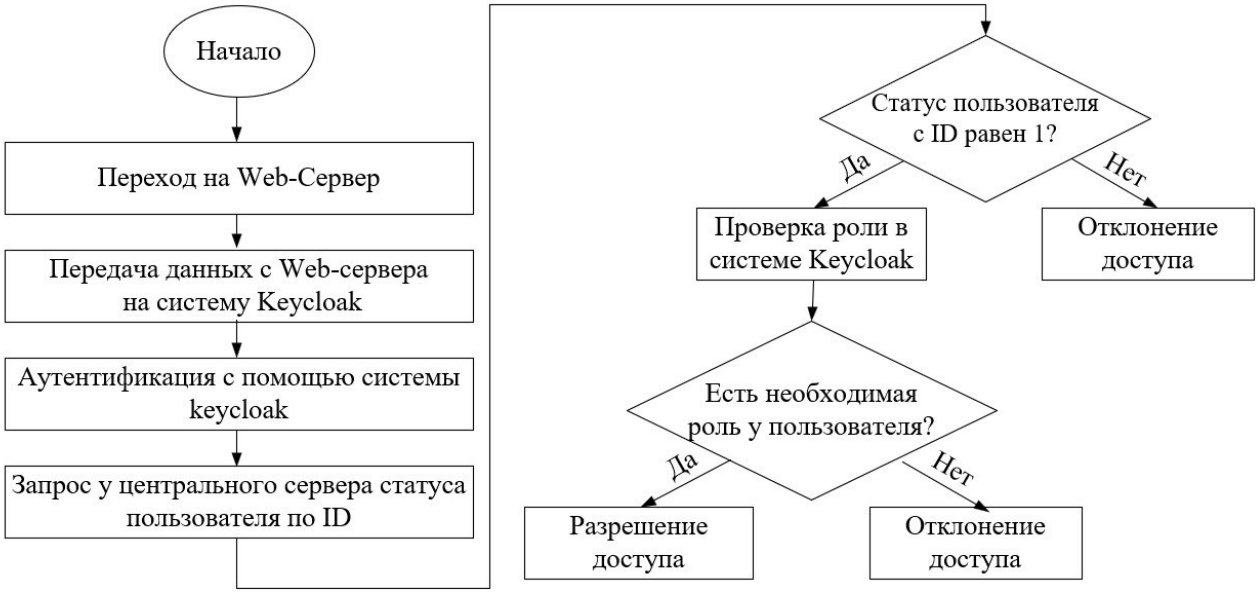


Рисунок 2 – Блок-схема функционирования Keycloak

В процессе тестирования системы были проведены различные сценарии, включая успешный вход с RFID-картой и биометрическими данными, а также отказ в доступе при несоответствии биометрических данных или использовании незарегистрированной карты. Все этапы аутентификации были проверены на корректность работы, и система показала высокую степень надежности. Результаты тестирования подтверждают, что система эффективно предотвращает несанкционированный доступ и минимизирует риски компрометации учетных

данных.

Разработанная система может быть дополнительно усилена следующими мерами:

1 Журналирование событий – ведение логов всех попыток входа, что позволяет своевременно выявлять подозрительную активность.

2 Мониторинг в реальном времени – отображение информации о пользователях, которые зашли в здании или вышли из него.

3 Интеграция с системой управления инцидентами – для повышения уровня безопасности можно внедрить систему, которая будет автоматически реагировать на подозрительные события, отправляя уведомления систему администратору.

Заключение. В ходе разработки была создана эффективная система контроля и управления доступом, сочетающая RFID, биометрическую аутентификацию и интеграцию с Keycloak для управления учетными записями. Тестирование подтвердило ее высокую надежность и защиту от несанкционированного доступа. Перспективы дальнейшего развития включают интеграцию дополнительных методов защиты, таких как журналирование событий, мониторинг в реальном времени и расширение функциональности. Такая система может быть внедрена в учебные процессы для студентов различных специальностей, включая 1-98 01 02 «Защита информации в телекоммуникациях».

Список литературы

1. MFRC522 [Электронный ресурс]. Режим доступа: https://github.com/miguelbalboa/rfid?ysclid=m82qd1ku2p160266956. – Дата доступа: 11.02.2025.

2. Server Administration Guide [Электронный ресурс]. Режим доступа: https://www.keycloak.org/docs/latest/server_admin/index.html. – Дата доступа: 24.02.2025.

3. Flask's documentation [Электронный ресурс]. Режим доступа: https://flask.palletsprojects.com/en/stable/. – Дата доступа: 01.03.2025.

UDC 004.93'1

USER AUTHENTICATION MANAGEMENT SYSTEM FOR INFORMATION RESOURCES USING ACCESS CONTROL SYSTEMS

Ivanov A.P., Kisel A.V.

gr.161402

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Belousova E.S. – PhD (Tech.), associate professor at the information security department

Annotation. The report presents the results of the development and testing of an access control system based on RFID cards and biometric authentication, integrated with Keycloak. This system can be used for training students of various specialties, including 6-05-0611-02 "Information Security," to enhance their skills in information security.

Keywords: ACS, RFID card, biometric authentication, Keycloak.

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ КИБЕРЗАЩИТЫ ВОЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Каравай М.А., Пинголь Е.И.
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Гусаков П.Б.

Аннотация. Современные вооружённые конфликты всё чаще включают киберкомпонент. Информационные системы армии и объектов критической инфраструктуры становятся приоритетными целями для кибератак. Использование искусственного интеллекта (ИИ) в военной сфере позволяет создать адаптивные и автоматизированные системы защиты, способные в реальном времени обнаруживать, анализировать и устранять угрозы. В работе рассматриваются особенности применения ИИ в кибербезопасности военных систем, примеры существующих решений и перспективы развития.

С расширением спектра киберугроз и переходом вооружённых конфликтов в цифровую плоскость защита военных информационных систем выходит на первый план. Традиционные методы кибербезопасности не всегда эффективны при атаках на сетевые структуры армейских подразделений, системы управления, радиосвязи, навигации и вооружения. Искусственный интеллект предлагает новые подходы, основанные на непрерывном анализе поведения систем, обнаружении аномалий и оперативном реагировании на потенциальные инциденты.

Одним из ключевых направлений является применение ИИ для защиты военных сетей в условиях ограниченного времени и ресурсов. Используются методы машинного обучения, включая глубокие нейросети, обучение без учителя и методы самообучения, позволяющие выявлять признаки атак даже без заранее заданных сигнатур. Это особенно актуально при противодействии APT-группировкам, использующим сложные и многоэтапные сценарии вторжения. ИИ способен анализировать сетевой трафик, лог-файлы, данные телеметрии с узлов связи и управления, создавая модель нормального поведения системы и оперативно определяя отклонения.

Важной особенностью военных ИИ-систем является требование к их автономности. В условиях радиоэлектронного противодействия, блокировки каналов связи и физической изоляции подразделений системы киберзащиты должны функционировать без внешней поддержки. Такие решения проектируются с учётом устойчивости к атакам на сами алгоритмы — в том числе попыткам внедрения вредоносных данных, способных изменить поведение модели. Кроме того, особое внимание уделяется интерпретируемости решений, чтобы командный состав мог оперативно принимать обоснованные действия на основе отчётов системы.

Дополнительным направлением развития ИИ-средств в военной информационной безопасности становится их интеграция с платформами класса SOAR (Security Orchestration, Automation and Response). Это позволяет не только выявлять инциденты, но и в автоматическом режиме запускать защитные сценарии: блокировать сетевые подключения, изолировать атакованные узлы, создавать маршруты обхода и передавать оперативные отчёты ответственным офицерам. В условиях ограниченного времени реагирования и высокой динамики боевой обстановки такая автоматизация становится критически важной.

Особое значение приобретает разработка систем объяснимого искусственного интеллекта (XAI), способных не только выносить решения, но и предоставлять их интерпретацию. Это необходимо при функционировании в связке с человеком-оператором в

центрах боевого управления. Такие системы позволяют повысить доверие к автоматизированным решениям, минимизируя риски ошибочных действий и повышая оперативность принятия решений в условиях неопределённости.

В перспективе искусственный интеллект может быть глубоко интегрирован в единые автоматизированные системы управления войсками (АСУ), обеспечивая защиту от информационного воздействия на всех уровнях – от индивидуального бойца до командных пунктов оперативного звена. Возможно создание «умных» кибербарьеров, динамически адаптирующихся к боевой обстановке, обладающих способностью к самообучению и самостоятельному восстановлению после атак. Применение таких технологий укрепляет цифровую безопасность армии и становится одним из ключевых направлений обеспечения военного превосходства в XXI веке.

Таким образом, искусственный интеллект открывает новые горизонты для повышения устойчивости военных информационных систем. Он обеспечивает проактивную защиту, сокращает время реагирования, снижает нагрузку на операционный персонал и позволяет эффективно противостоять киберугрозам в условиях реального и гибридного конфликта. Комплексная интеграция ИИ в системы кибероборонs позволит вооружённым силам сохранить технологическое преимущество и обеспечить цифровой суверенитет в информационном противостоянии.

Список использованных источников:

1. Злотин А.И., Мацкевич В.М. Кибероборона: современные подходы и технологии. Военная мысль, 2020.

2. Чеботарёв А.А. Интеллектуальные системы в кибероборонe. Вестник ВА РБ, 2022.

3. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020.

4. Мельников И.С. Искусственный интеллект в военном деле: перспективы и вызовы. Информационная безопасность, 2021.

УДК 0004.056.53

МЕТОДИКА ИСПОЛЬЗОВАНИЯ МАТРИЦЫ MITRE ATTACK ДЛЯ ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ СЕТЕЙ

Кравченко Е.Д., Буцкевич Е.М. студенты гр.261402

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. технических наук, доцент

Аннотация. В статье изучается применение матрицы MITRE ATT&CK в тестировании безопасности корпоративных сетей, с фокусом на технику T1190. Рассматриваются методы компрометации веб-приложений, включая сканирование сети, перебор учетных данных и эксплуатацию уязвимостей. Описаны сценарии атак и их влияние на инфраструктуру, а также предложены меры защиты: ограничение доступа, многофакторная аутентификация и мониторинг активности. Работа предназначена для специалистов в сфере кибербезопасности и исследователей атак по модели MITRE ATT&CK..

Ключевые слова MITRE ATT&CK, T1190, Exploit Public-Facing Application, безопасность корпоративных сетей, тестирование безопасности, моделирование атак, уязвимости веб-приложений.

Структура MITRE ATT&CK охватывает весь жизненный цикл кибератак, начиная с

получения нарушителем первоначального доступа к системе и заканчивая эксфильтрацией данных или разрушением инфраструктуры. Понимание этих техник позволяет специалистам по кибербезопасности выявлять потенциальные угрозы и предпринимать проактивные меры защиты.

Модель MITRE ATT&CK – это база знаний, в которой содержится информацию о тактиках, техниках и процедурах, применяемых нарушителями на различных этапах кибератаки. Тактики определяют цель, которой атакующие хотят достичь путём использования определённых техник и процедур, называемых также подтехниками. Всё это вместе обозначается аббревиатурой TTP (Tactics, Techniques and Procedures). Каждая тактика или техника имеет свой уникальный идентификатор, используемый для простоты работы с матрицей.

Цель данной работы заключается в анализе применения модели MITRE ATT&CK для тестирования безопасности корпоративных сетей, выявлении уязвимостей, возникающих в ходе эксплуатации техники T1190, и предложении эффективных методов защиты от возможных атак.

Одним из ключевых этапов тестирования безопасности является анализ наиболее распространенных способов получения нарушителями первоначального доступа к системе. Для получения доступа в инфраструктуру чаще всего используется техника Exploit Public-Facing Application (T1190) – эксплуатация уязвимостей в публично доступных приложениях. Рассмотрим, каким образом атака может быть реализована и какие меры.

В качестве эксплуатируемых приложений чаще всего выступают веб-сайты/веб-серверы, но также могут использоваться базы данных (например, SQL), стандартные службы (например, SMB или SSH), протоколы администрирования и управления сетевыми устройствами (например, SNMP и Smart Install), а также любые другие системы с открытыми сокетами, доступными через Интернет Смоделируем ситуацию, когда обнаруживается уязвимость в веб-приложении, связанная с недостаточной защитой публично доступных директорий и слабой системой аутентификации.

Перед началом кибератаки авторами была развернута среда с Kali Linux в VirtualBox для проведения тестов. В процессе проведения кибератаки, основанной на технике T1190 (Exploit Public-Facing Application), была смоделирована ситуация эксплуатации уязвимого веб-приложения с целью проникновения в корпоративную сеть.

Первоначально с помощью сканирования портов с помощью команды nmap и перебора директорий с помощью команды dirb были обнаружены потенциально уязвимые точки входа, включая /admin, /login, /dashboard, /images и /includes.

В ходе кибератаки была проведена проверка защищенности веб-приложения от Brute-force атак на учетные записи. Для этого использовался инструмент Hydra (рисунок 1), который позволил успешно подобрать пароли администратора и нескольких других учетных записей. Полученный доступ к административной панели /admin открыл возможность выполнения дальнейших кибератак, включая загрузку веб-оболочки (web shell). С ее помощью установили обратное соединение с сервером, что позволило выполнить команды в системе с правами веб-пользователя www-data.

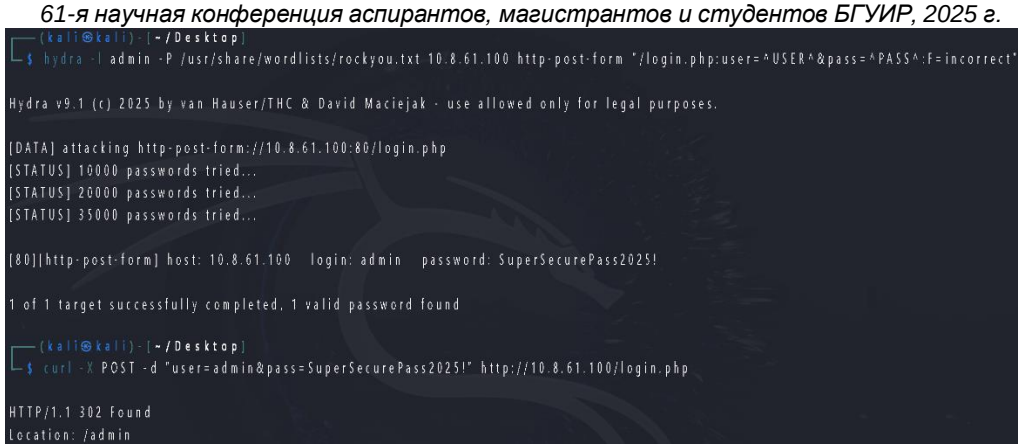


Рисунок 1 – Использование инструмента hydra

После получения доступа к командной оболочке сервера удалось загрузить вредоносный скрипт с использованием команды curl, а затем установить соединение через обратный шелл с помощью команды nc. Действуя от имени пользователя www-data, было произведено изучение файловой системы сервера. В процессе анализа директории /var/www/html/ были обнаружены следующие значимые файлы и папки: config.php, вероятно, содержавший конфигурационные данные; директория /includes, где могли бы находиться дополнительные важные файлы; директория /backup, возможно, содержавшая резервные копии данных. Эта информация позволила продолжить дальнейший анализ системы и потенциально раскрыть дополнительные векторы атаки.

На следующем этапе, исследовав содержимое конфигурационного файла config.php, были обнаружены учётные данные для подключения к базе данных. Используя эту информацию, удалось получить доступ к серверу базы данных MySQL и выполнить авторизацию. Проведение запросов позволило извлечь конфиденциальные данные, включая зашифрованные пароли пользователей и информацию о структуре базы данных, представленных на рисунке 2. Анализ этих данных стал ключевым шагом в изучении системы, предоставив дополнительные возможности для дальнейшего проведения кибератаки.

Рисунок 2 – Извлечение конфиденциальных данных

Следующим этапом стало сканирование внутренней сети для выявления дополнительных узлов. С помощью Nmap были обнаружены активные системы в той же

подсети. Используя найденные ранее учетные данные, попробовали выполнить подключение к другим серверам по SSH. В результате удалось получить доступ к одному из узлов, используя ту же учетную запись администратора, что указывало на повторное использование паролей внутри корпоративной сети. Это расширило возможности кибератаки, открыв доступ к еще большему количеству системных ресурсов.

На заключительном этапе была проведена эскалация привилегий для получения полного контроля над системой, представленная на рисунке 3. Проверка конфигурации sudo выявила возможность выполнения команд с привилегиями root без запроса пароля. С помощью этого механизма смогли запустить командную оболочку от имени «суперпользователя» и получить полный контроль над сервером. Доступ на уровне root позволит изменять файлы конфигурации, манипулировать учетными записями пользователей и устанавливать постоянные точки доступа для сохранения контроля над системой.

Рисунок 3 – Эскалация привилегий

Для сокрытия следов кибератаки были удалены журналы событий, временные файлы и история выполненных команд, что затруднит последующий анализ инцидента администраторами системы. Проведенная атака продемонстрировала, как эксплуатация уязвимости веб-приложения, связанная с недостаточной защитой публично доступных ресурсов, может привести к компрометации не только отдельного сервера, но и всей корпоративной сети.

Таким образом доказывается, что эксплуатация уязвимостей веб-приложений может привести к компрометации серверов, утечке данных и развитию кибератаки внутри сети, подчеркивая необходимость их своевременного устранения.

Использование модели MITRE ATT&CK для тестирования безопасности корпоративных сетей, в частности с применением техники T1190, показало высокую эффективность в выявлении уязвимостей в веб-приложениях. Проводя анализ уязвимых точек входа, было продемонстрировано, как нарушители могут воспользоваться уязвимостями для компрометации систем и дальнейшего распространения кибератаки по сети. Результаты работы подтверждают необходимость применения комплексных подходов к защите. Организациям следует активно использовать методы тестирования безопасности, основанные на MITRE ATT&CK, для более эффективного выявления угроз и своевременного реагирования на них.

В заключение, развитие и совершенствование систем защиты необходимо для того, чтобы адаптироваться к быстро меняющимся угрозам в сфере кибербезопасности. Использование моделей, таких как MITRE ATT&CK, позволяет не только тестировать существующие

механизмы защиты, но и создавать эффективные стратегии для противодействия новыми атакам, что в итоге способствует повышению общей безопасности корпоративных сетей.

Список использованных источников:

1. Techique T1190 [Электронный ресурс] – 2024. Режим доступа : https://attack.mitre.org/versions/v9/techniques/T1190/

UDC 0004.056.53

METHODOLOGY OF USING THE MITRE ATTACK MATRIX FOR TESTING THE SECURITY OF CORPORATE NETWORKS

Krauchanka E.D., Butskevich E.M

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Belousova E.S. – PhD (Tech.), Associate Professor

Annotation. The article examines the application of the MITRE ATT&CK matrix in testing the security of corporate networks, with a focus on the T1190 technique. It considers methods for compromising web applications, including network scanning, brute-force attacks, and exploitation of vulnerabilities. It describes attack scenarios and their impact on the infrastructure, and proposes protective measures: access restrictions, multifactor authentication, and activity monitoring. The work is intended for cybersecurity specialists and researchers of attacks based on the MITRE ATT&CK model.

Keywords. MITRE ATT&CK, T1190, Exploit Public-Facing Application, enterprise network security, security testing, attack modeling, web application vulnerabilities.

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Орлов К. И., Шклянко А. А., Полоско Е. И.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ефремов А.А. – заведующий кафедрой ЭИ, к.э.н., доцент

Аннотация. Данная работа посвящена исследованию на тему использования технологий искусственного интеллекта в информационной безопасности и их влиянию на повышение уровня защиты данных. Также будет рассмотрены такие аспекты, как преимущества использования искусственного интеллекта в информационной безопасности, как он помогает при защите от новых видов кибератак и предотвращении использования вредоносных программ.

Искусственный интеллект (ИИ) – это мощная технология, которая помогает специалистам сферы информационной безопасности автоматизировать рутинные задачи, идентифицировать и реагировать на угрозы в наименьшие сроки, а также повышать точность своих действий для укрепления уровня безопасности от различных проблем и кибератак.

Искусственный интеллект доказал свою важность в борьбе с проблемами информационной безопасности, предлагая разработку «Интеллектуальных Агентов» для эффективного решения

конкретных задач безопасности. «Интеллектуальный Агент», в виде аппаратного или программного обеспечения, разработан для повышения вероятности достижения определенной цели из-за его способности наблюдать, учиться и принимать проанализированные решения. Эти «Интеллектуальные Агенты» могут обнаруживать недостатки в сложных структурах кода, выявлять необычные образцы входа пользователей и даже распознавать новые типы вредоносных программ, отличающихся от традиционных методов обнаружения.

Внутри «Интеллектуальные Агенты» обрабатывают огромные объемы данных для изучения и понимания паттернов (шаблонов). Когда они открываются в системах защиты, агенты применяют свои знания, анализируя входящие данные, включая ранее неизвестную информацию.

Применение ИИ в кибербезопасности может быть ценным и эффективным подходом, но, как и любая технология, она имеет свои достоинства и недостатки. Хотя автоматизация и приносит значительные преимущества, важно найти баланс и сочетать её с человеческой экспертизой. Синергия между автоматизированными инструментами и опытными специалистами по кибербезопасности необходима для создания надежной защиты от разнообразных и постоянно меняющихся киберугроз. Использование искусственного интеллекта в кибербезопасности позволяет эффективно преодолевать сложности, с которыми сталкиваются организации, и значительно улучшать их уровень безопасности. Вот ряд преимуществ, которые автоматизация может предложить:

– Эффективность и скорость. Автоматизация может значительно увеличить скорость и эффективность кибербезопасности. Автоматизированные системы могут быстро анализировать огромные объемы данных, обнаруживать угрозы и реагировать на проблемы гораздо быстрее, чем при ручных методах. Эта скорость крайне важна в столь быстро меняющейся обстановке;

– Снижение человеческого фактора. Автоматизация помогает уменьшить риск человеческой ошибки, часто являющейся причиной киберинцидентов. Автоматизированные системы могут следовать заранее определенным протоколам безопасности, минимизируя вероятность ошибок, которые могут привести к уязвимостям систем безопасности;

– Круглосуточный мониторинг и реагирование. Автоматизированные меры кибербезопасности обеспечивают постоянный мониторинг сетей и систем, обеспечивая активную защиту от потенциальных угроз. Это бдительное наблюдение сложно поддерживать вручную, особенно в больших и сложных информационных технологиях;

– Масштабируемость. Автоматизированные системы могут легко масштабироваться для обработки большого объема данных и различных задач безопасности. Эта масштабируемость крайне важна для организаций с сложной инфраструктурой и большим объемом сетевого трафика;

– Рутинные и повторяющиеся задачи. Автоматизация хорошо подходит для выполнения рутинных и повторяющихся задач, позволяя человеческим специалистам по кибербезопасности сосредоточиться на более сложных и стратегических аспектах безопасности. Это повышает удовлетворенность работой и использует человеческую экспертизу там, где она наиболее необходима.

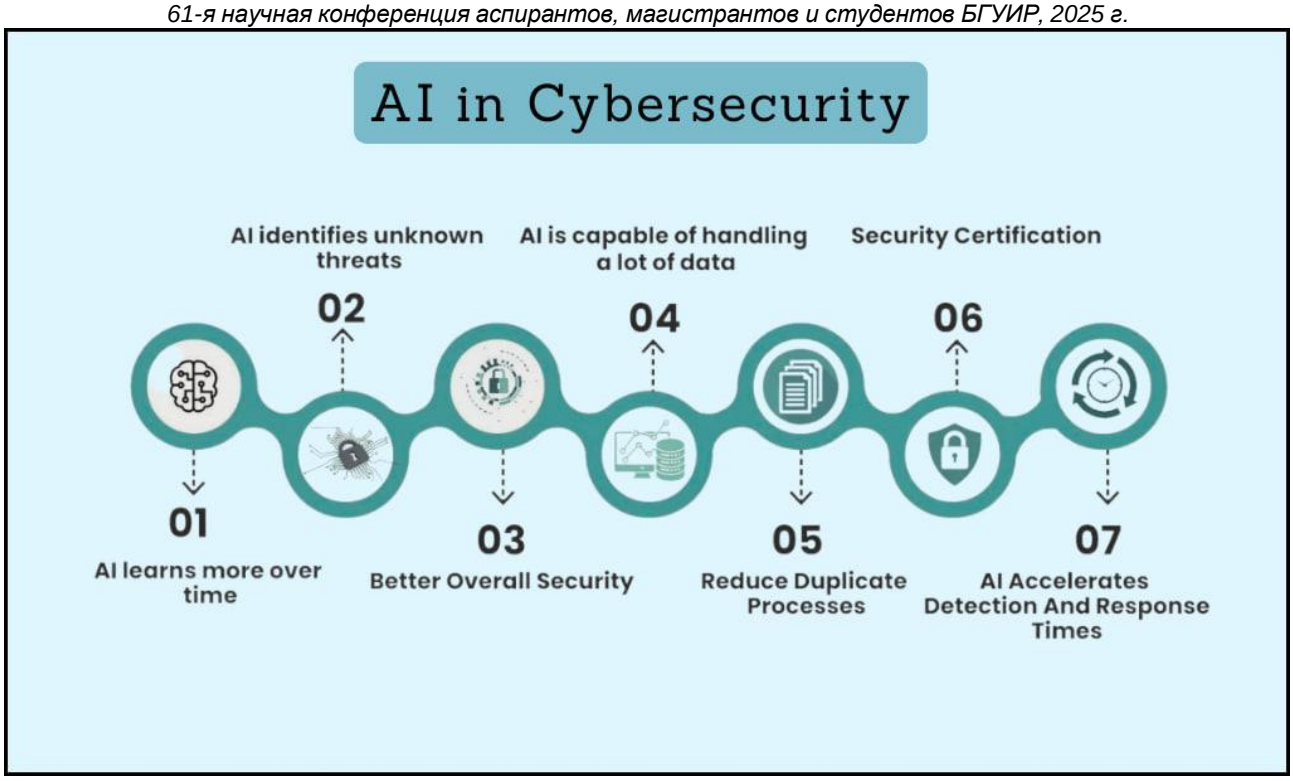


Рисунок 1.Преимущества использования ИИ в кибербезопасности

Как и было упомянуто выше, в использовании искусственного интеллекта, как и в любой другой технологии присутствуют свои недостатки:

– Снижение порога входа для злоумышленников. Искусственный интеллект представляет опасность для информационной безопасности тем, что снижает порог знаний, необходимых для создания злоумышленниками вредоносного программного обеспечения. Таким образом он не только помогает справляться с угрозами, но и сам стимулирует увеличение их количества.

– Зависимость от данных и алгоритмов. Использование искусственного интеллекта в информационной безопасности требует постоянного обновления баз данных и алгоритмов, что может быть затруднительно и в случае атаки злоумышленников на эти ресурсы, может привести к большим угрозам для безопасности.

– Повышенная опасность для неподготовленных пользователей.

– Усиление сложности киберугроз. С использованием ии увеличилась важность наличия квалифицированных специалистов по кибербезопасности. Однако глобальный спрос на этих экспертов значительно превышает предложение. Согласно исследованию 2022 года о кибербезопасности от (ISC)², в мире наблюдается дефицит в 3,4 миллиона специалистов по кибербезопасности.

– Более серьезные угрозы. По мере увеличения сложности искусственного интеллекта возрастает и сложность киберугроз. Может возникнуть ситуация, когда опытный киберпреступник использует инструмент искусственного интеллекта для создания высоко персонализированного сообщения спирфишинга. Это сообщение, идеально вписываясь во внутренний стиль коммуникации организации, может обмануть даже самых бдительных сотрудников, не говоря уже о рядовых пользователях.

Список использованных источников:

1. The Role of AI in Cybersecurity – A Comprehensive Guide on AI in Cybersecurity [Электронный ресурс] – Режим доступа: https://www.eccu.edu/blog/technology/the-role-of-ai-in-cyber-security/ – Дата доступа: 06.04.2025

2. The Role of Artificial Intelligence (AI) in Modern Cybersecurity [Электронный ресурс] – Режим доступа: https://www.encryptionconsulting.com/the-role-of-artificial-intelligence-ai-in-modern-cybersecurity/ – Дата доступа: 06.04.2025

3. Artificial intelligence for cybersecurity: Literature review and future research directions [Электронный ресурс] – Режим доступа: https://www.sciencedirect.com/science/article/pii/S1566253523001136 – Дата доступа: 06.04.2025

4. Cybersecurity and AI: The challenges and opportunities [Электронный ресурс] – Режим доступа: https://www.weforum.org/agenda/2023/06/cybersecurity-and-ai-challenges-opportunities/ – Дата доступа: 06.04.2025

5. The Power and Limitations of AI in Cybersecurity [Электронный ресурс] – Режим доступа: https://www.fortinet.com/blog/ciso-collective/power-and-limitations-of-ai-in-cybersecurity – Дата доступа: 06.04.2025

УДК 004.422.833

СИСТЕМА БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ KIRTapp

Романов Д. А., Колбанов Г.П.,

Учащиеся УО «Национальный детский технопарк»
г. Минск, Республика Беларусь

Научный руководитель: Белоусова Е.С. – канд. техн. наук, доцент кафедры защиты информации

Аннотация. В данной работе рассматривается система биометрической аутентификации KIRTapp, предназначенная для регистрации и контроля доступа с использованием распознавания лиц. Проведён анализ различных алгоритмов, на основе которого был выбран оптимальный метод идентификации Face Recognition. Система KIRTapp обеспечивает постоянный мониторинг пользователя и автоматическое реагирование на изменения в процессе аутентификации, снижая риск несанкционированного доступа. В перспективе планируется интеграция нейросетей и анти-спуфинг технологий для повышения безопасности.

Ключевые слова. Face Recognition; OpenCV; биометрическая аутентификация; машинное обучение, нейронные сети; распознавание лиц.

В современном мире аутентификация играет ключевую роль в обеспечении безопасности данных и ограничении доступа к системам [1]. Традиционно для идентификации пользователей применялись пароли и PIN-коды, но эти методы имеют ряд недостатков: они могут быть забыты, украдены или скомпрометированы.

Биометрическая аутентификация предлагает более надёжную альтернативу, используя уникальные физиологические характеристики человека, такие как отпечатки пальцев, радужка глаза и лицо. Одним из наиболее популярных и удобных методов является распознавание лиц [2].

В статье проведен сравнительный анализ распространенных моделей распознавания лиц, на основе которого обоснован выбор, внедрение и тестирование модели Face Recognition в операционной системе Secux Linux для контроля пользователей корпоративных сетей.

Для выбора модели для системы биометрической аутентификации изучено исследование разных моделей распознавания лиц [3]:

1 RetinaFace – это высокоточный детектор лиц, представленный в 2019 году. Он использует одностадийный метод обнаружения лиц с дополнительными возможностями предсказания ключевых точек (глаз, носа, рта).

2 DBFace – это компактная, одностадийная нейросеть для детекции лиц, разработанная для высокой скорости работы.

3 Facenet-pytorch – это высокоуровневый интерфейс для FaceNet**,** модели, представленной Google в 2015 году.
4 Face Recognition – это популярная библиотека для Python, основанная на dlib. Она предоставляет удобный API для детекции, кодирования и сравнения лиц.
5 Ultra-Light-Fast-Generic-Face-Detector-1MB – это ультралегковесная модель для детекции лиц, предназначенная для мобильных устройств и встроенных систем.
Автором исследования [3] был создан собственный датасет, проведен процесс его разметки и осуществлено тестирование ранее перечисленных моделей.
Для проведения анализа результатов тестирования и определения наиболее подходящей модели использовались следующие метрики: Precision**,** Recall и Intersection over Union (IoU)**.** Эти метрики позволят нам оценить производительность моделей в контексте точности распознавания лиц, полноты детекции и качества локализации объектов.
Precision (Точность) – метрика измеряет долю правильно предсказанных положительных примеров (истинных положительных) среди всех предсказанных положительных примеров и вычисляется по формуле:

$$Precision = \frac{TP}{TP + FP} \quad (1)$$

где TP – количество истинных положительных предсказаний (правильно распознанных лиц); FP –количество ложных положительных предсказаний (ошибочно распознанных лиц).
Precision важен, когда необходимо минимизировать количество ложных срабатываний (когда модель ошибочно распознает лицо, где его нет).
Recall (Полнота) – метрика для измерения способности модели обнаружить все реальные положительные примеры среди всех истинных положительных. Она отражает, сколько из всех объектов были корректно обнаружены моделью. Формула для расчета Recall:

$$Recall = \frac{TP}{TP + FN} \quad (2)$$

где TP – количество истинных положительных предсказаний; FN – количество ложных отрицательных предсказаний (когда модель не распознает лицо, которое есть на изображении).
Recall критичен в задачах, где важно н пропустить ни одного лица, даже если это приводит к большему числу ложных срабатываний.
Intersection over Union (IoU) – метрика IoU измеряет степень совпадения между предсказанной областью (например, bounding box) и реальной областью, охватывающей объект. Эта метрика особенно важна для задач детекции объектов, так как она позволяет оценить точность локализации. Формула для расчета IoU:

$$IoU = \frac{\text{Area of Intersection}}{Area\,of\,Union}$$

$$IoU = \frac{Area\ of\ Intersection}{Area\ of\ Union} \quad (3)$$

где Area of Intersection – площадь пересечения предсказанного прямоугольника и истинного прямоугольника, ограничивающего лицо; Area of Union – площадь объединения этих двух прямоугольников.

Таблица 1 – Сравнительный анализ моделей биометрической аутентификации

Метрика	RetinaFace	DBFace	Facenet-pytorch	Face Recognition	Ultra-Light-Fast-Generic-Face-Detector-1MB
Precision	0,99	1	0,95	1	0,74
Recall	0,8	0,8	0,71	0,38	0,75
IoU	0,75	0,74	0,72	0,67	0,59
Время обработки, с	91	13	14	11	3

Анализ результатов показал, что модель RetinaFace продемонстрировала наилучшие показатели точности, однако её время выполнения составило 91 секунду, что является неприемлемым для системы биометрической аутентификации. DBFace также показала хорошие результаты, но не предоставляет встроенного механизма сравнения лиц, что потребовало бы дополнительной реализации, например, с использованием евклидова расстояния. В связи с этим Face Recognition является наиболее подходящим выбором: несмотря на не самое высокое значение Recall, полное распознавание всех лиц не является приоритетом для разрабатываемой системы биометрической аутентификации, так как она анализирует только единственного пользователя, работающего за устройством.

Таким образом, для разработки системы биометрической аутентификации KIRTapp была выбрана модель Face Recognition. Принцип работы KIRTapp основан на регистрации пользователей администратором, и в последующем автоматическим сканированием пользователей каждые N минут, где N – число, настраиваемое администратором.

Алгоритм работы фоновой службы автоматического сканирования пользователей представлен на рисунке 1.

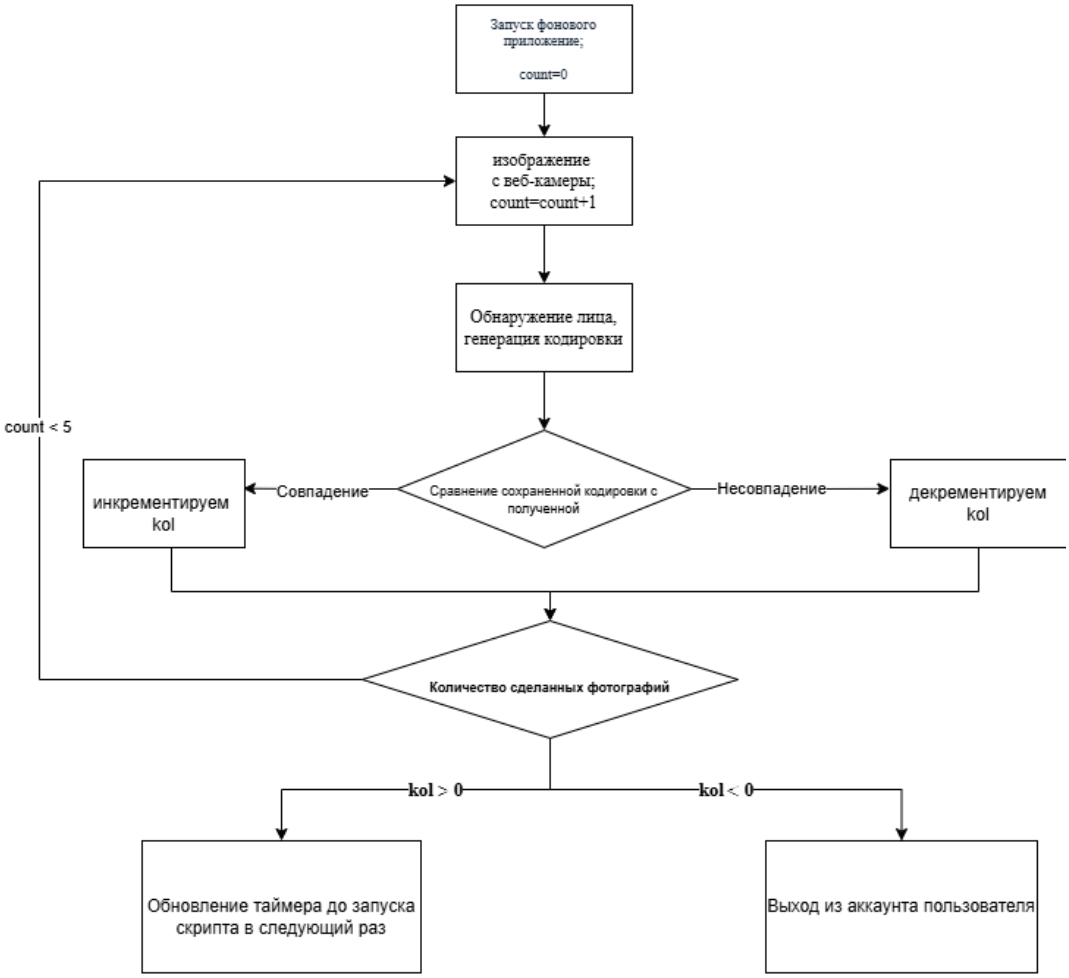


Рисунок 1. Алгоритм работы фоновой службы автоматического сканирования пользователей

На следующем этапе алгоритм, основанный на библиотеке face_recognition, выполняет детекцию лица на полученном изображении. Обнаруженное лицо преобразуется в вектор признаков, называемый кодировкой (face_encoding). Этот вектор представляет собой компактное числовое описание уникальных характеристик лица пользователя, вычисленное с помощью сверточной нейронной сети.

Процесс повторяется 5 раз с интервалом в 2 секунды между итерациями. На каждом этапе фиксируется результат: идентифицирован ли пользователь как владелец устройства или нет. Если по итогам пяти попыток количество положительных идентификаций превышает количество отрицательных, система подтверждает присутствие владельца и продолжает работу. В противном случае система выполняет блокировку: текущий сеанс завершает свою работу, предотвращая несанкционированный доступ.

Такой подход, основанный на многократной проверке, позволяет повысить надёжность алгоритма, минимизируя вероятность ошибок распознавания, вызванных внешними факторами, такими как изменения освещения или случайные искажения изображения.

Система биометрической аутентификации KIRTapp была внедрена в операционную систему Secux Linux. На рисунке 2 показан процесс работы KIRTapp. При успешном распознавании пользователя выводится "good", а при несовпадении или отсутствии распознавания – "bad" в журнале сервиса. Вся информация также сохраняется в файл logs в папке с программой (рисунок 3).

```
мар 14 20:46:16 kirttest systemd[1]: Starting Run KIRTapp...
мар 14 20:46:18 kirttest python3[3698]: [ WARN:0@1.321] global cap_gstreamer.cpp:1777 open OpenCV
мар 14 20:46:30 kirttest python3[3698]: good
мар 14 20:46:30 kirttest python3[3698]: kol - 1
мар 14 20:46:30 kirttest python3[3698]: count - 1
мар 14 20:46:30 kirttest python3[3698]: good
мар 14 20:46:30 kirttest python3[3698]: kol - 2
мар 14 20:46:30 kirttest python3[3698]: count - 2
мар 14 20:46:30 kirttest python3[3698]: good
мар 14 20:46:30 kirttest python3[3698]: kol - 3
мар 14 20:46:30 kirttest python3[3698]: count - 3
мар 14 20:46:30 kirttest python3[3698]: good
мар 14 20:46:30 kirttest python3[3698]: kol - 4
мар 14 20:46:30 kirttest python3[3698]: count - 4
мар 14 20:46:30 kirttest python3[3698]: good
мар 14 20:46:30 kirttest python3[3698]: kol - 5
мар 14 20:46:30 kirttest python3[3698]: count - 5
```

Рисунок 2 – Журнал сервиса KIRTapp

```
  GNU nano 8.3
2025-03-14 20:46:30 - INFO - The checking was successful
2025-03-14 20:51:43 - INFO - The checking was successful
2025-03-14 20:57:03 - INFO - The checking was failed
2025-03-14 21:02:33 - INFO - The checking was failed
2025-03-14 21:07:40 - INFO - The checking was failed
2025-03-14 21:13:03 - INFO - The checking was failed
2025-03-17 19:09:46 - INFO - The checking was successful
```

Рисунок 3 – Файл с логами

Таким образом, на основе проведенного тестирования показано, что система KIRTapp обеспечивает надёжный контроль доступа и мониторинга пользователей, минимизируя риск несанкционированного входа. В будущем планируется внедрение нейросетей и анти-спуфинг технологий для повышения точности распознавания и защиты от попыток обхода системы.

Список использованных источников:

1. Вержбицкий, С. В. Биометрические системы и технологии: основы, методы, средства. – М.: Горячая линия – Телеком, 2019 г. – 304 с.
2. Исследование эффективности библиотек распознавания лиц [Электронный ресурс]. – Режим доступа: https://libeldoc.bsuir.by/bitstream/123456789/51893/1/Petrov_Issledovanie.pdf.
3. Сравнение алгоритмов детекции лиц [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/661671/.

UDC 004.422.833

KIRTAPP BIOMETRIC AUTHENTICATION SYSTEM

Romanov D.A., Kolbanov G. P.
students of the educational institution "National Children's Technopark",
Minsk, Republic of Belarus
Belousova E.S. – PhD (Tech.), Ass. Prof. of Department of IP

Annotation. In this paper, we consider the KIRTapp system, designed for registration and access control using facial recognition. The analysis of various algorithms was carried out, on the basis of which the optimal identification method of Face Recognition was chosen. The KIRTapp system provides continuous monitoring of the user and automatic response to changes in the authentication process, reducing the risk of unauthorized access. In the future, it is planned to integrate neural networks and anti-spoofing technologies to increase security.

Keywords. Face Recognition; OpenCV; biometric authentication; machine learning, neural networks; face recognition.

УДК 004.056

УЯЗВИМОСТИ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ

Романова М.П.

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Научный руководитель: Насонова Н.В. – доктор техн. наук, доцент

Аннотация. В статье рассматриваются вопросы реализации и уязвимости одно- и многофакторной аутентификации. Проведён практический анализ возможностей эксплуатации механизмов многофакторной аутентификации на веб-сайтах с использованием специализированного ПО Burpsuite. В заключении автор предлагает несколько рекомендаций по внедрению многофакторной аутентификации на веб-сайтах для предотвращения возникновения описанных уязвимостей.

Ключевые слова: Аутентификация, уязвимости, эксплуатация.

Многофакторная аутентификация (multi-factor authentication, MFA) — расширенная аутентификация, метод контроля доступа, в котором пользователю для получения доступа к

информации необходимо предъявить более одного «доказательства механизма аутентификации». Среди всех рекомендаций по обеспечению безопасности доступа, многофакторная аутентификация, безусловно является одной из наиболее часто встречающихся [1].

Уязвимости аутентификации оказывают серьёзное влияние на безопасность информационного ресурса. Если злоумышленник обходит аутентификацию и получает доступ к учётной записи другого пользователя, он получает доступ ко всем данным и функциям, которыми обладает скомпрометированная учётная запись. Если удаётся скомпрометировать учётную запись с высоким уровнем привилегий, например, учётную запись системного администратора, они могут получить полный контроль над всем приложением и потенциально получить доступ к внутренней инфраструктуре.

Многие веб-сайты полагаются исключительно на однофакторную аутентификацию с использованием пароля для аутентификации пользователей. Однако она является небезопасной, поскольку пароли могут быть скомпрометированы различными способами. Например, согласно исследованию Verizon Data Breach Investigations Report за 2023 год, 82% утечек данных были связаны с человеческим фактором, включая использование слабых или украденных паролей [2]. Эффективным способом повысить защищенность процесса аутентификации является внедрение многофакторной аутентификации. Хотя проверка биометрических факторов может быть нецелесообразна для большинства веб-сайтов, все чаще встречается как обязательная, так и необязательная двухфакторная аутентификация (2FA), основанная на комбинации факторов «что вы знаете» (пароль) и «что у вас есть». Обычно это включает ввод традиционного пароля и временного кода проверки, полученного с физического устройства, находящегося во владении пользователя.

Большинство уязвимостей в механизмах аутентификации проявляются в одном из двух способов: механизмы аутентификации слабы, потому что они не могут адекватно защитить от атак методом перебора или же есть логические недостатки или ошибки реализации, которые позволяют злоумышленнику полностью обойти механизмы аутентификации. Иногда это называется «нарушенной аутентификацией».

Несмотря на то, что иногда злоумышленник может получить один фактор, основанный на знаниях, например, пароль, возможность одновременного получения другого фактора из внешнего источника значительно менее вероятна [3]. По этой причине двухфакторная аутентификация более безопасна, чем однофакторная аутентификация. Однако, как и любая мера безопасности, она безопасна настолько, насколько безопасна её реализация. Плохо реализованную двухфакторную аутентификацию можно обойти или даже полностью обойти, так же как и однофакторную аутентификацию.

Иногда реализация двухфакторной аутентификации несовершенна до такой степени, что её можно полностью обойти. Если пользователю сначала предлагается ввести пароль, а затем ввести код подтверждения на отдельной странице, пользователь фактически находится в состоянии «вошёл в систему» до того, как он ввёл код подтверждения. В этом случае стоит проверить, сможете ли вы напрямую перейти к страницам «только для входа в систему» после завершения первого шага аутентификации. Иногда вы можете обнаружить, что веб-сайт на самом деле не проверяет, выполнили ли вы второй шаг перед загрузкой страницы.

Уязвимости многофакторной аутентификации, связанные с ошибочной логикой процесса.

Например, если после того, как пользователь завершил первый этап входа в систему, веб-сайт не проверяет должным образом, что тот же пользователь завершает второй этап аутентификации.

Например, пользователь входит в систему со своими обычными учетными данными на

первом шаге следующим образом:

```
POST /login-steps/first HTTP/1.1
Host: vulnerable-website.com
...
username=carlos&password=qwerty
```

Затем им присваивается файл cookie, относящийся к их учетной записи, прежде чем они переходят ко второму этапу процесса входа в систему:

```
HTTP/1.1 200 OK
Set-Cookie: account=carlos

GET /login-steps/second HTTP/1.1
Cookie: account=carlos
```

При отправке кода подтверждения запрос использует этот файл cookie, чтобы определить, к какой учетной записи пользователь пытается получить доступ:

```
POST /login-steps/second HTTP/1.1
Host: vulnerable-website.com
Cookie: account=carlos
...
verification-code=123456
```

В этом случае злоумышленник может войти в систему, используя свои учетные данные, но затем изменить значение файла cookie на любое произвольное имя пользователя при отправке кода подтверждения. account

```
POST /login-steps/second HTTP/1.1
Host: vulnerable-website.com
Cookie: account=victim-user
...
verification-code=123456
```

Это чрезвычайно опасно, если злоумышленник затем сможет подобрать код верификации, поскольку это позволит ему входить в учетные записи произвольных пользователей, основываясь исключительно на их имени пользователя. Им даже не нужно будет знать пароль пользователя.

Уязвимости многофакторной аутентификации, связанные со слабыми механизмами.

Как и в случае с паролями, веб-сайты должны принимать меры для предотвращения подбора кода проверки 2FA. Это особенно важно, потому что код часто представляет собой простое 4 или 6-значное число. Без надёжной защиты от перебора взломать такой код несложно.

Некоторые веб-сайты пытаются предотвратить это, автоматически выходя из системы, если пользователь вводит определённое количество неправильных кодов подтверждения. На практике это неэффективно, потому что продвинутый злоумышленник может даже автоматизировать этот многоступенчатый процесс, создав макросы для Burp Intruder. Для этой цели также можно использовать удлинитель Turbo Intruder.

Подводя итоги, дадим некоторые рекомендации по внедрению многофакторной

аутентификации на веб-сайтах для предотвращения описанных уязвимостей. Итак, они включают выбор надёжных методов MFA, таких как FIDO2, приложения-аутентификаторы и push-уведомления с подтверждением номера, избегая менее предпочтительных вариантов вроде SMS-кодов и email-кодов, реализацию MFA с плавной интеграцией, простым процессом настройки, предложением нескольких вариантов и безопасных резервных методов, а также безопасное хранение секретных ключей и защиту от обхода MFA, обеспечение удобства использования через возможность запоминания устройств и адаптивную MFA, обучение и поддержку пользователей с информированием о важности MFA и предоставлением инструкций, а также постоянное совершенствование через мониторинг, регулярное обновление и аудит безопасности. Внедрение MFA помогает предотвратить атаки с использованием украденных учётных данных, фишинг, атаки типа "человек посередине", атаки на сеансы и внутренние угрозы, значительно повышая безопасность веб-сайта.

Список литературы

1. *За пределами MFA: почему пароли все еще играют ключевую роль в безопасности? [Electronic resource] / SecurityLab. – Mode of access :https://www.securitylab.ru/analytics/546198.php?ysclid=m8hadlgxes727904854&utm_referrer=https%3A%2F%2Fyandex.by%2F – Date of access : 21.02.2023.*

2. *Verizon Data Breach Investigations Report [Электронный ресурс] / Verizon. – Режим доступа : https://www.verizon.com/business/en-nl/resources/reports/dbir/2023/summary-of-findings/. – Дата доступа : 15.02.2024*

3. *Виды многофакторной аутентификации [Electronic resource] / Keeper. – Mode of access : https://www.keepersecurity.com/blog/ru/2023/06/27/types-of-multi-factor-authentication-mfa/. – Date of access : 27.06.2023.*

UDC 004.056

Multifactor Authentication vulnerabilities

Romanova M.P.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Nasonova N.V. – Doctor of Technical Sciences, Associate Professor

Annotation. The article discusses the implementation and vulnerability of single- and multi-factor authentication. A practical analysis of the possibilities of using multifactor authentication mechanisms on websites using specialized Burpsuite software has been carried out. In conclusion, the author offers several recommendations for implementing multi-factor authentication on websites to prevent the occurrence of the described vulnerabilities.

Keywords: Authentication, vulnerabilities, exploitation.

УДК 004.056.53

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ОТ УГРОЗ IP SPOOFING С ИСПОЛЬЗОВАНИЕМ GNS3

Русецкая Т.Б.[1], студент гр.261401

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Научный руководитель: Бойправ О.В. – кандидат технических наук, заведующий кафедрой защиты информации, доцент

Аннотация. В материалах доклада представлены результаты анализа угроз IP Spoofing, проведенного с использованием симулятора GNS3. Для проведения указанного анализа был разработан виртуальный макет, состоящий из устройств нарушителя, целевого устройства и маршрутизатора. Исследование состояло из описания проведения IP Spoofing, а также последствия кибератаки для безопасности сети. В результате анализа были предложены рекомендации для повышения уровня защищенности информационных систем. Полученные результаты могут быть полезны для специалистов в области защиты информации и разработки эффективных мер по предотвращению подобных угроз, а также для улучшения безопасности сетевых коммуникаций.

Ключевые слова. Сетевые кибератаки, IP Spoofing, GNS3, VMware, iptables, Wireshark.

Введение. Протокол IP предназначен для обеспечения соединения хостов. Протокол обеспечивает передачу блоков данных, называемых дейтаграммами между отправителем и получателем, узлы которых идентифицируются адресами фиксированной длины. На рисунке 1 показан формат заголовка пакета IP.

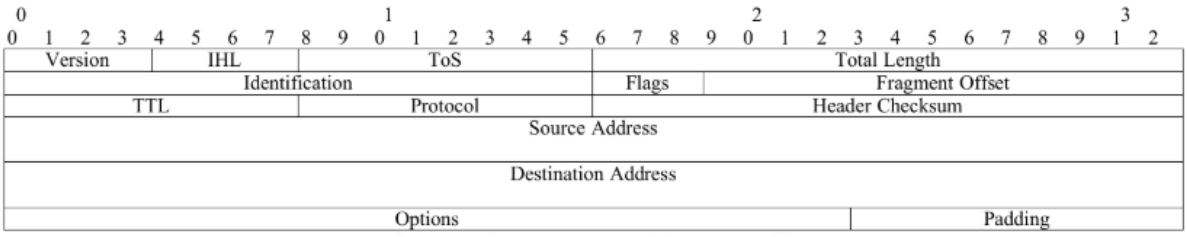


Рисунок 1 – Формат заголовка пакета IP

В полях Source Address и Destination Address указываются адреса источника и назначения.

Актуальность проблемы сетевой атаки IP Spoofing остается высокой из-за использования нарушителями для онлайн-мошенничества, кражи личных данных и нарушения работы корпоративных веб-сайтов и серверов. Также такая атака является основой других атак (DDoS, MITM и маскировка ботнет-устройств). В ходе проведения IP Spoofing адрес источника нарушителя меняется на поддельный, чтобы скрыть реальный IP-адрес и создать видимость легитимного подключения к сети.

Цель данной научной работы состояла в анализе эффективности методов защиты от угроз IP Spoofing. Практическая значимость результатов данного исследования состоит в возможности их применения в целях повышения эффективности алгоритмов фильтрации пакетов и создания современных систем предотвращения атак.

Основная часть. Для изучения принципов передачи IP-пакетов была создана локальная сеть в виртуальной лаборатории, построенной с использованием симулятора GNS3.

Схема виртуальной лаборатории, построенной в GNS3, приведена на рисунке 2. В ее состав входит следующее оборудование:

– маршрутизатор Cisco c7200;

– коммутатор (Swith1);

– компьютер нарушителя с ОС Alpine Linux (AlpineLinux);

– компьютер жертвы с ОС Alpine Linux (AlpineLinux-victim);

– компьютер с ограниченной ОС (VPCS).

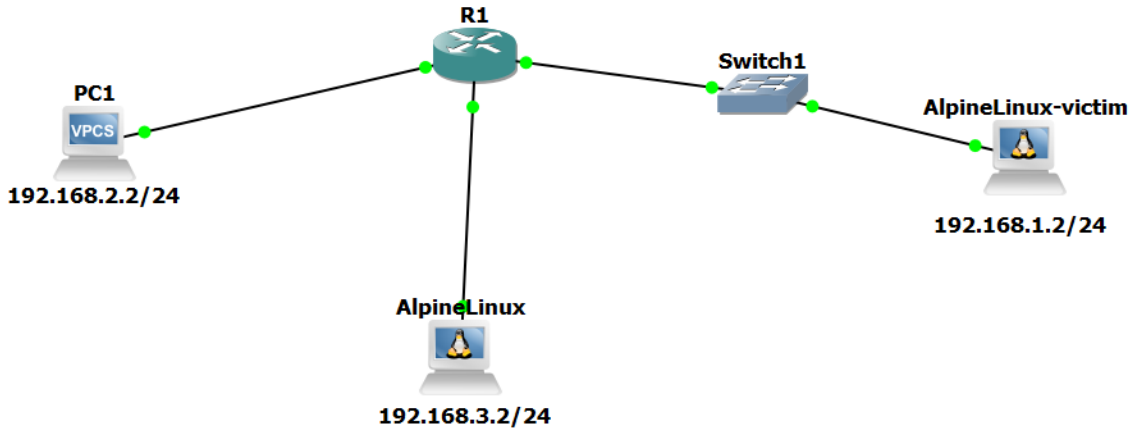


Рисунок 2 – Схема виртуальной лаборатории, построенной
с использованием симулятора GNS3

В рамках исследования был рассмотрен сценарий с подменой IP-адреса и проведением DDoS-атаки на устройство с ограниченной ОС. Для проведения кибератаки необходимо изменить IP-адрес через изменение значения поля Source Address в заголовке IP-пакета. В топологии локальной сети в GNS3 определены следующие IP-адреса:

1) 192.168.1.2 – устройство жертвы (AlpineLinux-victim);
2) 192.168.3.2 – устройство нарушителя (AlpineLinux);
3) 192.168.2.2 – устройство с ограниченной ОС (VPCS).

На устройствах нарушителя и целевой машины был установлен инструмент iptables. На устройстве AlpineLinux с помощью команды, представленной на рисунке 3, был изменен IP-адрес источника в IP-пакетах.

```
/ # iptables -t nat -A POSTROUTING -p icmp -j SNAT --to-source 192.168.5.2
```

Рисунок 3 – Команда для изменения адреса источника в IP-пакете

На рисунке 4 приведены полученные с помощью анализатора трафика Wireshark сведения о пакетах, отправленных в ходе реализации успешной DDoS-атаки, при которой была осуществлена замена адреса источника при отправке пакетов с устройства нарушителя.

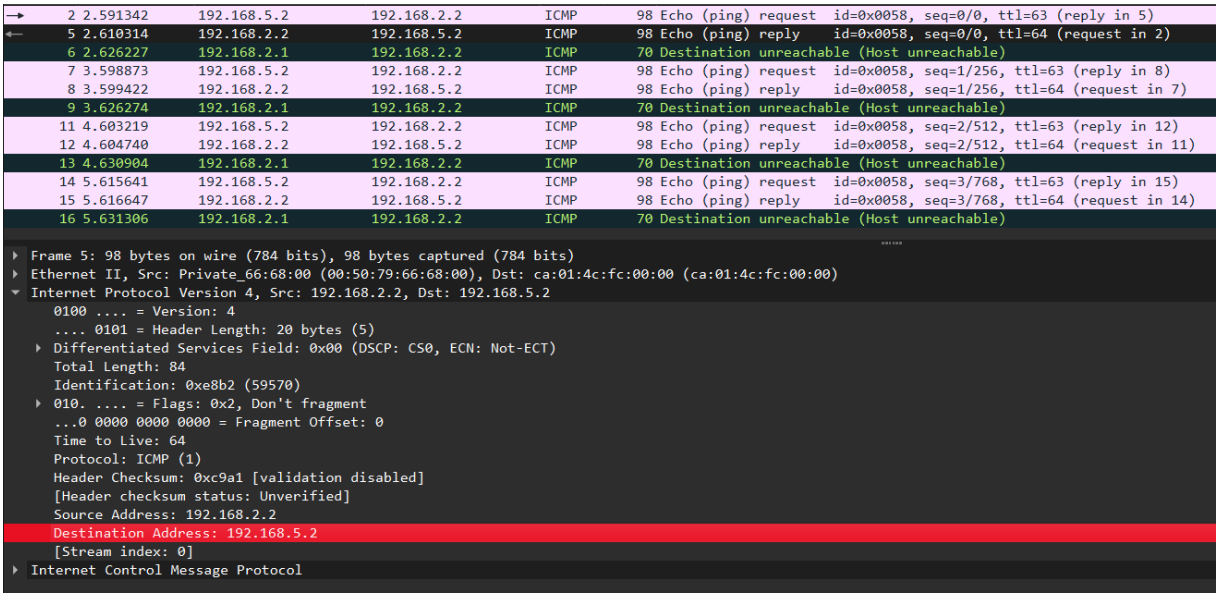


Рисунок 4 – Сведения о пакетах, отправленных в ходе реализации успешной DDoS-атаки

Методы защиты от угроз IP Spoofing включают:

– мониторинг сетей на предмет подозрительной активности;

– использование аутентификации;

– использование межсетевого экрана;

– включение Unicast Reverse Path Forwarding (uRPF) на маршрутизаторах для поиска обратного маршрута пакетов;

– ограничение доступа к сетевым ресурсам (настройка access-list).

Подход к защите от угроз IP Spoofing, основанный на использовании access-list и uRPF на маршрутизаторах для фильтрации трафика, приведен на рисунке 5.

```
R1#sh access-list
Extended IP access list FILTER_TRAFFIC
    10 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 (4 matches)
    20 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 (12 matches)
    30 deny ip any any (19 matches)
```

```
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 ip access-group FILTER_TRAFFIC in
 ip verify unicast reverse-path
 duplex half
!
interface FastEthernet1/0
 ip address 192.168.1.1 255.255.255.0
 ip access-group FILTER_TRAFFIC in
 ip verify unicast reverse-path
 duplex half
!
interface FastEthernet2/0
 ip address 192.168.3.1 255.255.255.0
 ip verify unicast reverse-path
 duplex half
```

Рисунок 5 – Настройка access-list и проверка маршрута пакета

Механизм работы Unicast Reverse Path Forwarding включает в себя проверку маршрута пакета в таблице маршрутизации, если адрес источника входящего пакета существует, то осуществляется поиск обратных маршрутов к адресу источника, если найден интерфейс, который соответствует интерфейсу получения, то пакет пропускается, в ином случае отбрасывается.

Результаты анализа трафика при включенной фильтрации пакетов приведен на рисунке 6.

2 3.896275	192.168.5.2	192.168.2.2	ICMP	98	Echo (ping) request id=0x0089, seq=0/0, ttl=63 (reply in 5)
5 3.927704	192.168.2.2	192.168.5.2	ICMP	98	Echo (ping) reply id=0x0089, seq=0/0, ttl=64 (request in 2)
6 3.974412	192.168.2.1	192.168.2.2	ICMP	70	Destination unreachable (Communication administratively filtered)
7 4.915986	192.168.5.2	192.168.2.2	ICMP	98	Echo (ping) request id=0x0089, seq=1/256, ttl=63 (reply in 8)
8 4.915986	192.168.2.2	192.168.5.2	ICMP	98	Echo (ping) reply id=0x0089, seq=1/256, ttl=64 (request in 7)
9 4.959386	192.168.2.1	192.168.2.2	ICMP	70	Destination unreachable (Communication administratively filtered)
10 5.916578	192.168.5.2	192.168.2.2	ICMP	98	Echo (ping) request id=0x0089, seq=2/512, ttl=63 (reply in 11)
11 5.916578	192.168.2.2	192.168.5.2	ICMP	98	Echo (ping) reply id=0x0089, seq=2/512, ttl=64 (request in 10)
12 5.932204	192.168.2.1	192.168.2.2	ICMP	70	Destination unreachable (Communication administratively filtered)
14 11.128433	192.168.5.2	192.168.2.2	ICMP	98	Echo (ping) request id=0x008a, seq=0/0, ttl=63 (reply in 15)
15 11.128433	192.168.2.2	192.168.5.2	ICMP	98	Echo (ping) reply id=0x008a, seq=0/0, ttl=64 (request in 14)
16 11.156775	192.168.2.1	192.168.2.2	ICMP	70	Destination unreachable (Communication administratively filtered)
17 12.151722	192.168.5.2	192.168.2.2	ICMP	98	Echo (ping) request id=0x008a, seq=1/256, ttl=63 (reply in 18)
18 12.152712	192.168.2.2	192.168.5.2	ICMP	98	Echo (ping) reply id=0x008a, seq=1/256, ttl=64 (request in 17)
19 12.166758	192.168.2.1	192.168.2.2	ICMP	70	Destination unreachable (Communication administratively filtered)

Рисунок 6 – Результаты анализа трафика при фильтрации пакетов

Заключение. На основе проведенных исследований можно сделать следующие выводы.

1. Регулярное проведение анализа эффективности методов защиты от угроз информационной безопасности является важным мероприятием, направленным на повышение защищенности информационных систем.

2. Применение таких технологий, как фильтрация трафика, Unicast Reverse Path Forwarding, а также списков контроля доступа обеспечивает эффективное выявление и блокировку поддельных пакетов, что способствует защите данных. Настройка этих инструментов предоставляет возможность анализировать сетевую активность и разрабатывать эффективные меры защиты от угроз кибератаки IP Spoofing.

Список использованных источников:

1. IP Spoofing: что это и как работает [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/resource-center/threats/ip-spoofing – Дата доступа: 07.04.2025.

2. Черкасов Д. Ю., Иванов В. В. IP-spoofing // Евразийский научный журнал. – 2017. – №. 6. – С. 197-200.

3. Предотвращение подделки адресов через Unicast Reverse Path Forwarding [Электронный ресурс] – Режим доступа: https://www.opennet.ru/base/cisco/unicast_reverse_path_forwarding.txt.html – Дата доступа: 07.04.2025.

4. Бобов М. Н., Мохаммед Ф. О. Методы использования механизма поиска обратного маршрута для защиты локальных сетей от атаки спуфинга //Доклады БГУИР. – 2010. – №. 5 (51). – С. 72-75.

UDC 004.056.53

ANALYSIS OF PROTECTION METHODS AGAINST IP SPOOFING THREATS USING GNS3

Rusetskaya T.B.[1], gr.261401

Belarusian State University of Informatics and Radioelectronics[1],
Minsk, Republic of Belarus

Boiprav O.V. – PhD in Technical Sciences, Head of the Department of Information Security, Associate Professor

Annotation. The article presents the results of an IP Spoofing threat analysis performed using GNS3 simulator. For this analysis, a virtual mockup consisting of the intruder's devices, target device and router was developed. The study consisted of a description of IP Spoofing as well as the effects of the cyber-attack on network security. The study's findings yielded recommendations to enhance the security level of information systems. The results obtained may be of use to information protection specialists, in order that they might develop effective measures to prevent such threats, as well as for improving the security of network communications.

Keywords. Network cyber-attack, IP Spoofing, GNS3, VMware, iptables, Wireshark.

КИБЕРКУЛЬТУРА: МЕМЫ И ТРЕНДЫ, ВЛИЯЮЩИЕ НА БЕЗОПАСНОСТЬ В СЕТИ

Рута А.М.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Канаш А.В. – старший преподаватель, кафедра экономической информатики

Данная научная работа исследует влияние мемов и трендов на киберкультуру, подчеркивая их роль в формировании общественного мнения о безопасности в сети. Однако также обсуждаются вызовы и проблемы, связанные с искажением информации и возможной дезинформацией. В этой работе рассмотрены преимущества использования мемов для распространения информации и повышения осведомленности о киберугрозах.

Киберкультура представляет собой совокупность ценностей, практик и сообществ, формирующихся в виртуальном пространстве интернета. Мемы, как единицы культурной информации, быстро распространяются в сети, достигая вирусной популярности. Они передаются через ремиксы, адаптации, изменения и модификации оригинального контента, что способствует их трансформации и эволюции. Мемы оказывают значительное влияние на общественное мнение, способствуют формированию трендов и могут быть интегрированы в маркетинговые стратегии, а также использоваться в политических контекстах для мобилизации и воздействия на аудиторию.

Мемы и тренды могут представлять собой угрозу безопасности в цифровом пространстве. Фишинговые атаки нередко используют мемы для маскировки своих намерений и обмана пользователей, что затрудняет распознавание вредоносных действий. Вредоносные программы также распространяются через популярные тренды и вирусные видеоматериалы, что увеличивает вероятность их распространения среди пользователей. Кроме того, мемы могут быть использованы в целях манипуляции, позволяя злоумышленникам получать доступ к конфиденциальным данным и личной информации пользователей, что подчеркивает необходимость повышения осведомленности о рисках, связанных с потреблением контента в интернете [1].

В целом, мемы оказывают значительное влияние на подсознание, формируя мнения и установки пользователей. Их способность к быстрому распространению и визуальной привлекательности делает их мощным инструментом манипуляции вниманием. Эффект FOMO (Fear of Missing Out), или боязнь упустить важную информацию, способствует повышенной восприимчивости пользователей к манипуляциям, заставляя их реагировать на контент без должной проверки источников и фактов.

Кроме того, автоматическое восприятие информации, характерное для потребления мемов, может снижать уровень критического мышления. Это приводит к недостаточной аналитической оценке представленных данных и, как следствие, увеличивает риск обмана и дезинформации. Пользователи, не подвергающие сомнению увиденное, становятся более уязвимыми к манипуляциям, что подчеркивает необходимость развития навыков критического мышления и осознанного потребления контента в киберкультуре.

Мемы оказывают значительное воздействие на аспекты безопасности в цифровом пространстве, как положительное, так и отрицательное. Они также служат инструментом социальной инженерии, позволяя злоумышленникам манипулировать пользователями и создавать ложное чувство доверия. Например, мемы могут быть разработаны с использованием знакомых тем или персонажей, что повышает их привлекательность и

снижает настороженность пользователей. Злоумышленники активно используют для привлечения внимания пользователей к фишинговым ссылкам и вредоносным файлам. С другой стороны, мемы могут быть использованы в рамках образовательных кампаний для повышения осведомленности о кибербезопасности. Они способны сделать сложные темы более доступными и понятными для широкой аудитории [2].

Одним из примеров мемов является «Это не баг, это фича». Мем помогает упрощать обсуждение технических проблем, делая их более доступными для широкой аудитории. Это может повысить интерес к вопросам IT и безопасности. Поскольку мем акцентирует внимание на недостатках и ошибках, это может вызвать у пользователей недоверие к продуктам и системам. Понимание, что некоторые баги могут быть фичами, заставляет пользователей быть более внимательными и критичными.

Другим примером мемов являются реалистичные видео, созданные с использованием технологий искусственного интеллекта, которые иллюстрируют жизнь в исторических контекстах, таких как Древний Египет, Древняя Греция, на борту «Титаника» или в Помпеях. Эти видеоматериалы демонстрируют события и повседневную жизнь в указанные эпохи, создавая иллюзию, что они происходят в настоящее время. Мем подчеркивает, как легко можно создать фальшивый контент, что вызывает опасения по поводу подделки исторических фактов и манипуляций с информацией. Это может привести к недоверию к источникам информации. С другой стороны, такие мемы могут быть использованы для образовательных целей, привлекая внимание к истории и культуре. Они могут способствовать интересу к древним цивилизациям и их наследию.

Также примером искусственных мемов являются ии-коты, что приведено на рисунке 1. Он может влиять на восприятие угроз. Люди могут воспринимать киберугрозы менее серьезно, если они представлены в игривом формате, что может снизить бдительность. Картинки, вызывающие смех, могут быть использованы для привлечения внимания к важным вопросам безопасности в интернете. Например, аналогия с акулой может символизировать киберугрозы, а котёнок - уязвимость пользователей [3].

Рисунок 1 – Мем созданный искусственным интеллектом

В условиях всеобъемлющего влияния мемов и вирусного контента в интернете, пользователям необходимо развивать навыки защиты от манипулятивных и дезинформационных эффектов. Пользователи должны обучаться критическому анализу информации, прежде чем принимать её за правду, что включает в себя проверку источников и сравнения с другими. Ключевыми аспектами здесь являются идентификация эмоционального

воздействия и распознавание трюков социальной инженерии. Пользователи должны устанавливать личные границы в отношении того, какой контент они потребляют и как реагируют на него.

Таким образом, мемы и тренды в киберкультуре представляют собой двусторонний инструмент, обладающий потенциалом как для повышения осведомленности о кибербезопасности, так и для манипуляции и распространения дезинформации. Это подчеркивает необходимость критического подхода к контенту и развития навыков медиаграмотности среди пользователей. Образовательные инициативы, основанные на мемах, могут сыграть важную роль в формировании более безопасного цифрового пространства, если будут направлены на осознание потенциальных угроз и развитие аналитического мышления.

В заключение, исследование влияния мемов и трендов на киберкультуру подчеркивает их двойственную природу как инструмента формирования общественного мнения и потенциальной угрозы безопасности в сети. Мемы, обладая способностью быстро распространяться и привлекать внимание, могут как повышать осведомленность о киберугрозах, так и служить средством манипуляции и дезинформации [4].

Однако с этими возможностями приходят и значительные риски. Злоумышленники могут использовать мемы для социальной инженерии, подрывая доверие пользователей и увеличивая уязвимость к киберугрозам. Это подчеркивает настоятельную необходимость развития критического мышления, медиаграмотности и навыков анализа информации у пользователей.

Важным шагом к созданию более безопасного цифрового пространства является обучение пользователей методам распознавания манипуляций и дезинформации, а также развитие личных границ в потреблении контента. Таким образом, мемы и тренды могут стать не только инструментом развлечения, но и важным ресурсом для повышения уровня осведомленности и безопасности в интернете.

Список использованных источников:

1. Смирнов, И. (2020). Роль мемов в цифровой культуре: Понимание их влияния на общественное мнение. *Журнал киберкультуры, 12(3), 45-60.*

2. Петрова, А. (2021). Осведомленность о кибербезопасности через мемы: Образовательные стратегии для современной аудитории. *Международный журнал информационной безопасности, 15(2), 123-135.*

3. Иванов, Р. & Чен, Ю. (2022). Вирусный контент и его последствия для цифровой безопасности: Исследование меметического влияния. *Киберпсихология, поведение и социальные сети, 25(1), 67-75.*

4. Давыдова, М. (2023). Навигация по мемной среде: Риски и возможности в киберосведомленности. *Журнал цифровой этики, 8(4), 201-215.*

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОСНОВЕ МЕТОДА ВВЕДЕНИЯ ИДЕНТИФИКАТОРОВ

Тавгень М.А., учащийся по направлению «Информационная безопасность»,
Янковец А.С., учащийся по направлению «Информационная безопасность»

Национальный детский технопарк
г. Минск, Республика Беларусь

Тимофеев А.М. – канд. техн. наук, доцент, доцент кафедры защиты информации БГУИР (научный руководитель)

Аннотация. Разработаны структурные схемы обезличивания и деобезличивания персональных данных, построенные на базе симметричного блочного стандарта ГОСТ 28147-89. В предложенных схемах секретными параметрами являются ключи шифрования данных длиной 256 бит и 8 узлов замены, содержащихся в блоке подстановки. Шифротексты, полученные с помощью ГОСТ 28147-89, использованы в качестве псевдослучайной величины, посредством которой реализованы процедуры обезличивания и деобезличивания персональных данных.

В настоящее время одной из важнейших задач, решаемых при проектировании современных информационных систем, является обеспечение информационной безопасности персональных данных, что реализуется посредством обезличивания персональных данных [1 – 3]. В соответствии с требованиями законодательства Республики Беларусь одним из методов обезличивания персональных данных является метод введения идентификаторов. Известные способы реализации обезличивания персональных данных на основе метода введения идентификаторов [6 – 9] подразумевают использование в качестве идентификаторов хэшированных значений персональных данных. Это не позволяет деобезличить персональные данные без знания таблиц соответствия, что является недостатком способов [6 – 9]. В связи с этим целью данной работы являлось разработать структурные схемы обезличивания и деобезличивания персональных данных на основе метода введения идентификаторов, свободных от этого недостатка.

В качестве объекта исследования использован стандарт шифрования данных ГОСТ 28147-89. Предметом исследования являлось установить криптографические операции, позволяющие выполнить обезличивание и деобезличивание персональных данных на основе метода введения идентификаторов, которые не требуют обязательного использования таблиц соответствия.

В рамках выполненных исследований разработана структурная схема генерации идентификаторов, построенная на базе симметричного блочного стандарта ГОСТ 28147-89. Применение этого стандарта является обязательным для всех организаций и предприятий Республики Беларусь, осуществляющих криптографическую защиту информации. В предложенной схеме секретными параметрами являются ключ шифрования данных длиной 256 бит и 8 узлов замены, содержащихся в блоке подстановки. Шифротексты использованы в качестве псевдослучайной величины.

Разработана структурная схема деобезличивания персональных данных, которая, как и схема обезличивания персональных данных, построена на базе ГОСТ 28147-89. Это позволило выполнить процедуру деобезличивания аналогичным образом, как и процедуру обезличивания. Таким образом, реализовав программное обеспечение для обезличивания персональных данных, появляется возможность использовать это же программное обеспечение для деобезличивания персональных данных, что упрощает практическую реализацию схем обезличивания и деобезличивания персональных данных.

Список использованных источников:

1. Ворона, В. А. Биометрическая идентификация личности / В. А. Ворона. – Москва : Горячая линия-Телеком, 2023. – 228 с.

2. Коллинз, М. Защита сетей. Подход на основе анализа данных / М. Коллинз. – Москва : ДМК Пресс, 2020. – 308 с.

3. Остапенко, Г. А. Информационные операции и атаки в социотехнических системах : организационно-правовые аспекты противодействия : учебное пособие / Г. А. Остапенко, Е. А. Мешкова ; под ред. В. Г. Кулакова. – 2-е изд., стер. – Москва : Горячая линия-Телеком, 2020. – 208 с.

4. Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=12551&p0=H12100099. – Дата доступа: 28.02.2025 г.

5. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 10 декабря 2024 г. № 259 «Об изменении приказов Оперативно-аналитического центра при Президенте Республики Беларусь от 28 марта 2014 г. № 26 и от 20 февраля 2020 г. № 66» [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2024%20-%20259.pdf. – Дата доступа: 28.02.2025 г.

6. Raghunathan, S. The Complete Book of Data Anonymization: From Planning to Implementation. – Boca Raton: CRC Press, 2013. – 500 с.

7. Ali, J., Dyo, V. Practical Hash-based Anonymity for MAC Addresses [Электронный ресурс]. – Режим доступа: https://arxiv.org/abs/2005.06580. – Дата доступа: 28.02.2025 г.

8. Determe, J.-F., Azzagnuni, S., Horlin, F., De Doncker, P. MAC Address Anonymization for Crowd Counting [Электронный ресурс]. – Режим доступа: https://arxiv.org/abs/2009.09876. – Дата доступа: 28.02.2025 г.

9. European Data Protection Supervisor. Introduction to the Hash Function as a Personal Data Pseudonymisation Technique [Электронный ресурс]. – Режим доступа: https://www.edps.europa.eu/sites/default/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf, свободный. – Дата доступа: 28.02.2025 г.

ПРОГРАММНЫЙ МОДУЛЬ ПО ПОИСКУ ФИШИНГОВЫХ ДОМЕННЫХ ИМЕН В НАЦИОНАЛЬНОМ СЕГМЕНТЕ СЕТИ ИНТЕРНЕТ

Феденко Р.Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Игнатенко А.А.

Аннотация. Фишинг, как вид интернет-мошенничества, целью которого является получение персональных данных пользователей Интернет. Угроза данной кибератаки, способы защиты от неё. Тайпсквоттинг и киберсквоттинг, как вид фишинговой атаки, использование программного модуля для защиты от данной атаки.

Фишинг – подмножество социальной инженерии, цель которого – получить персональные данные пользователя или другую ценную информацию. Существует два вида фишинговых атак:

– массовый фишинг – это тип атаки на нескольких людей сразу,

– целевой фишинг – это атаки на конкретных пользователей.

Фишинг представляет собой сообщение в мессенджере, почтовые письма со ссылкой на веб-ресурс или рекомендациями для дальнейших действий, поддельные страницы служб поддержки компаний, создание фишинговых сайтов, идентичных с легитимными.

Опасность фишинга в том, что не увидеть угрозу может любой человек, если он недостаточно внимателен к мелким деталям. Злоумышленники имитируют действующие публичные сети Wi-Fi в общественных местах, защищают свои фишинговые сайты с помощью классического изображения HTTPS в начальной адресной строки. В случае отсутствия активности, веб-страница перезагружается на странице ввода пароля, имитирующую легитимный сайт. Используют уязвимости сайтов для встраивания скрытых ловушек, для перехвата персональных данных, ловят пользователей на неправильном вводе веб-адреса, перенаправляют трафик с безопасного веб-сайта на фишинговую страницу. В случае получения доступа к электронной почте пользователя, злоумышленник может рассылать фишинговые письма от имени пользователя, что делает атаку еще более скрытой.

Для защиты от фишинга необходимо:

– не сообщать кому-либо конфиденциальную информацию,

– не открывать вложения, содержащие в письмах от неизвестного адресата,

– не переходить по ссылкам в письмах,

– своевременно обновлять программное обеспечение и операционную систему.

Фишинг наносит большой вред легитимным компаниям, понижая репутацию того или иного продукта. Поэтому выявлять и ликвидировать фишинг, необходимо до того, как он причинит значительный ущерб.

Тайпсквоттинг – это один из видов фишинговых атак, нацеленный на пользователей интернета, допустивших опечатку при вводе веб-адреса в браузере, начальный этап такой фишинговый атаки заключается в кибersквоттинге – вид киберпреступления, представляющий собой покупку или регистрацию доменного имени, полностью схожим с существующим [1]. Злоумышленники регистрируют домены с именами, являющимися намеренно ошибочными названиями известных веб-сайтов и пользователи могут попасть на такие альтернативные веб-сайты при случайном ошибочном вводе названия популярных веб-сайтов, или в результате перенаправления на вредоносный веб-сайт в рамках широкой фишинговой атаки [2].

Один из первых и самых известных примеров атак с тайпсквоттингом, связан с Google. В 2006 году был зарегистрирован сайт Goggle.com, который функционировал, как фишинговый. За прошедшие годы были зарегистрированы различные варианты названия Google: foogle, hoogle, boogle, yoogle (все они были выбраны из-за близости их первых букв к букве g на qwerty-клавиатурах). В преддверии президентских выборов 2020 года в США сообщалось [3], что злоумышленниками были созданы тайпсквоттинговые домены на имена нескольких кандидатов с различными злонамеренными мотивами.

С целью защиты от тайпсквоттинга, был разработан модуль по поиску фишинговых доменных имен в национальном сегменте сети Интернет, который поможет сохранять репутацию популярных компаний, а также известных личностей.

Список использованных источников:

1. Kaspersky [Электронный ресурс]. – Режим доступа : https://www.kaspersky.ru/resource-center/preemptive-safety/cybersquatting

2. Kaspersky [Электронный ресурс]. – Режим доступа : https://www.kaspersky.ru/resource-center/definitions/what-is-typosquatting

3. CPOmagazine [Электронный ресурс]. – Режим доступа : https://www.cpomagazine.com/cyber-security/will-typosquatting-influence-the-2020-presidential-election/

УДК 519.6

СИНТЕЗ РЕЧЕОБРАЗНОГО ШУМА НА БАЗЕ МОДЕЛИ НЕЙРОННОЙ СЕТИ

Шуневич А.И., студент гр.362201, Макареня Е.А., студент гр.361401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Зельманский О.Б. – канд. техн. наук, доцент

Проект «Синтез речеобразного шума на базе модели нейронной сети» посвящен разработке методов защиты речевой информации от утечек в условиях современного информационного общества. Основное внимание уделяется созданию акустических помеховых сигналов, адаптированных к конкретной речи с использованием машинного обучения. Исследуются существующие методы и устройства, а также разрабатываются алгоритмы для формирования речеподобных помех на русском языке. Работа направлена на повышение уровня безопасности конфиденциальных переговоров и может найти применение в бизнесе и государственных структурах.

Речевая информация, защита, помеховые сигналы, акустическая маскировка, нейронные сети, машинное обучение, конфиденциальность, алгоритмы, речеподобные помехи, информационная безопасность, анализ, синтез речи, технологии, сегментация, классификация, аудиосигнал, русский язык, фреймы, динамическое создание, системы защиты.

Речь является наиболее естественной формой человеческого взаимодействия и носителем множества конфиденциальной информации, включая личные данные, финансовые сведения и коммерческие тайны. Эта особенность делает речевую информацию уязвимой в контексте информационной безопасности, так как утечка таких данных может иметь серьезные последствия. В условиях стремительного развития технологий и нарастающей цифровизации угроза утечек данных становится все более актуальной, и защита речевой информации приобретает критическое значение. С каждым днем увеличивается количество устройств и платформ, на которых происходит обмен речевой информацией, что только усиливает необходимость в надежной защите.

Существующие методы защиты, такие как активная маскировка информации с помощью помехового сигнала, включают различные типы помех. К числу таких методов относятся белый шум, окрашенный шум и некоррелированная речеподобная помеха. Каждый из этих методов имеет свои преимущества и недостатки. Однако у всех них есть общая проблема: доступное в интернете программное обеспечение может эффективно компенсировать эти помехи, что ставит под угрозу безопасность речевой информации. Это создает необходимость в разработке более сложных алгоритмов и устройств, которые будут генерировать помеховой шум непосредственно из скрываемого речевого сигнала. Такой подход позволит создать уровень маскировки, при котором отделение информационного сигнала от помехового станет практически невозможным.

В частности, применение методов машинного обучения и искусственного интеллекта для динамического создания помехового сигнала, адаптированного к конкретной речи, может значительно повысить эффективность маскировки. Использование алгоритмов, которые учитывают интонации, паузы и другие особенности речи, может усложнить задачу для программного обеспечения, пытающегося распознать исходный сигнал. Это, в свою очередь, откроет новые горизонты в области защиты информации, так как позволит создать более совершенные системы, способные эффективно справляться с современными угрозами.

Таким образом, разработка новых методов защиты речевой информации становится не только желательной, но и необходимой в условиях постоянно меняющегося технологического ландшафта. Создание более надежных и адаптивных систем защиты позволит не только обеспечить безопасность конфиденциальных данных, но и повысить уровень доверия пользователей к технологиям, используемым для общения. Повышение уровня защиты речевой информации также может способствовать развитию новых стандартов и практик в области информационной безопасности, что в конечном итоге принесет пользу обществу в целом.

Цель данной работы заключается в разработке метода формирования акустического помехового сигнала на основе речи дикторов, участвующих в конфиденциальных переговорах. Этот метод будет предназначен для использования в активных системах защиты информации и будет реализован в виде программно-аппаратного модуля, что позволит обеспечить высокую степень защиты.

Для достижения указанной цели сформулированы следующие задачи:

1. **Анализ существующих методов защиты речевой информации.** Необходимо изучить и оценить текущие технологии и подходы, используемые для защиты речевых данных, чтобы выявить их сильные и слабые стороны. Это позволит понять, какие элементы защиты работают эффективно, а какие требуют доработки.
2. **Обзор устройств формирования речеподобных помех.** Потребуется исследовать существующие устройства и технологии, которые могут генерировать помехи, имитирующие человеческую речь, и оценить их эффективность в контексте защиты информации. Это

включает анализ того, как различные устройства справляются с задачами маскировки и какой уровень защиты они могут обеспечить.

3. **Создание речеподобных помех на русском языке.** Будет разработан алгоритм для формирования речеподобных помех с использованием компиляции фрагментов записи речи дикторов. При этом будет учитываться псевдотекст, который основывается на статистических особенностях русского языка. Это обеспечит более естественное звучание генерируемых помех, что важно для повышения их эффективности.
4. **Разработка программно-аппаратного средства.** На завершающем этапе работы будет создано программно-аппаратное средство, способное генерировать речеподобные помехи в реальном времени. Это устройство должно быть достаточно гибким, чтобы адаптироваться к различным условиям использования и обеспечивать высокий уровень защиты речевой информации.

Объектом исследования являются системы активной защиты информации, предназначенные для защиты речевых данных в различных сферах, включая бизнес и личные коммуникации. Это подчеркивает важность разработки универсальных решений, которые могут быть адаптированы к различным условиям и требованиям пользователей.

Предметом исследования являются алгоритмы анализа и синтеза речи, которые обеспечивают формирование речеподобных помех, способствующих повышению уровня безопасности информации. Эти алгоритмы должны быть достаточно мощными и гибкими, чтобы справляться с разнообразными задачами, возникающими в процессе защиты речевой информации.

Гипотеза: Современные системы активной защиты речевой информации используют помеховые сигналы, которые не обеспечивают необходимого уровня защиты. Эти сигналы могут быть эффективно компенсированы с помощью доступного программного обеспечения, что ставит под угрозу конфиденциальность передаваемой информации. В связи с этим предлагается новый подход, заключающийся в формировании маскирующего акустического сигнала непосредственно из скрываемого речевого сигнала. Этот метод позволит создать помехи, которые будут значительно сложнее для идентификации и компенсации, что повысит уровень защиты конфиденциальных переговоров.

В процессе исследования применялись различные методы и подходы, включая теоретические (анализ), эмпирические (эксперимент), общенаучные (синтез) и количественные (сбор и классификация данных). Эти методы обеспечили углубленное понимание проблематики защиты речевой информации и способствовали разработке эффективных стратегий.

Блоки установки:

1. **Блок загрузки сигнала.** В ходе цифровой обработки речевой сигнал представляется как последовательность отдельных стационарных фрагментов, известных как фреймы. На вход блока поступают отсчёты аудиосигнала, которые могут быть получены из файла или с микрофона. Затем сигнал разбивается на несколько фреймов (анализируемых окон) продолжительностью 0,07 секунды. Фреймы накладываются с частичным перекрытием, что позволяет избежать потерь информации на границах.

   Далее полученная последовательность в каждом фрейме умножается на весовую функцию окна Хемминга. Эта функция акцентирует внимание на центральных данных и минимизирует затухание на краях. Формула для расчёта функции Хемминга представлена ниже.
2. **Блок детектирования речи.** Принцип функционирования блока обнаружения речи основывается на сравнении параметров сигнала с заранее установленными порогами. В качестве таких параметров используются среднеквадратичное значение сигнала, количество нулевых переходов и спектральная характеристика.

Среднеквадратичное значение (Root Mean Square) позволяет вычислить среднюю мощность сигнала в анализируемом окне и затем сравнить её с установленным пороговым значением. Формула для расчета среднеквадратичного значения сигнала:

$$RMS = \sqrt{\frac{1}{N}\sum_{i=1}^{N} x_i^2}$$

Среднее количество нулевых переходов сигнала может быть вычислено по формуле:

$$Z = \frac{1}{T}\sum_{t=1}^{T} |s(t)| \cdot \delta(s(t))$$

где δ — функция, указывающая на переход через ноль.

3. **Блок сегментации речи.** На вход блок сегментации получает массив речевых фрагментов, представляющих собой последовательность временных фреймов. Сегментация осуществляется путём вычисления расстояний между значениями классификационных параметров соседних фреймов. Для этой задачи было выбрано расстояние Минковского, так как оно обеспечивает наилучшее соотношение между количеством неверно определённых и пропущенных границ.
4. **Блок классификации речи.** Блок классификации речи принимает на вход сегментированный речевой сигнал и создает массив фонетических единиц, организованных по классам и дикторам. Эти данные затем сохраняются в базе аллофонов для каждого диктора. В основе процесса классификации лежит модель нейронной сети Salute Speech, которая обеспечивает высокую точность классификации фонетических единиц.
5. **База аллофонов дикторов.** База данных аллофонов предназначена для хранения и быстрого извлечения аллофонов, принадлежащих различным дикторам. Данные каждого диктора организованы отдельно, что позволяет эффективно управлять информацией. Это обеспечивает возможность предварительно загрузить уже сформированную базу данных для конкретного диктора или сохранить новосозданную базу для последующего использования.
6. **Блок формирования фонемного псевдотекста.** Для создания фонемного псевдотекста были проанализированы статистические характеристики русского языка с испоыльзованием специального программного инструмента. В исследовании рассматривались тексты различных стилей с объемом более 80 тысяч символов каждый. Это обеспечило репрезентативность данных и позволило получить надежные статистические результаты преимуществ и недостатков представленных в таблице 1.

Таблица 1 – Преимущества и недостатки методов защиты

Метод	Преимущества	Недостатки
Белый шум	Простота реализации	Легко компенсируется
Окрашенный шум	Более естественное звучание	Уязвимость к специальным алгоритмам
Некоррелированная помеха	Сложнее для распознавания	Ограниченная эффективность
Речеподобные помехи	Высокая степень маскировки	Сложная реализация

В ходе выполнения работы была обоснована необходимость защиты речевой информации от утечек

через акустические и вибрационные каналы. Современное общество сталкивается с множеством угроз, связанных с конфиденциальностью данных, особенно в условиях цифровой трансформации. Увеличение объема передаваемой информации, включая личные данные и коммерческие тайны, делает защиту речевой информации актуальной. Эта ситуация обостряется ростом числа кибератак и утечек данных, что подчеркивает важность разработки эффективных методов защиты.

Показано, что активные средства акустической маскировки представляют собой более эффективное решение для защиты речевой информации. Эти методы позволяют снижать отношение сигнал/шум в контролируемой зоне путем увеличения уровня шума, что делает распознавание и анализ речевого сигнала значительно более сложными. Использование новых технологий и алгоритмов, основанных на искусственном интеллекте и машинном обучении, позволяет динамически адаптировать помеховые сигналы к особенностям передаваемой информации и окружающей акустической среды. Разработанный модуль синтеза речеподобных сигналов включает в себя ключевые этапы, такие как обнаружение речи, её сегментацию, классификацию на аллофоны, формирование фонемного псевдотекста и компиляцию аллофонов. Каждый из этих этапов играет важную роль в создании эффективной системы защиты. Например, сегментация речи позволяет выделить ключевые моменты, которые должны быть замаскированы, а классификация на аллофоны обеспечивает более высокую точность и качество синтезируемых сигналов.

Актуальность данного проекта обусловлена растущей угрозой утечки конфиденциальной информации в условиях современного информационного общества. Технологический прогресс, связанный с развитием систем обработки речи и анализа данных, открывает новые возможности для злоумышленников, что делает защиту речевой информации необходимой. В условиях, когда утечки конфиденциальной информации могут привести к значительным финансовым и репутационным потерям, использование активных средств акустической маскировки становится важным. Современные системы защиты должны быть способны адаптироваться к меняющимся условиям и угрозам, что подразумевает не только использование статических методов, но и внедрение динамических алгоритмов, которые могут эффективно реагировать на новые вызовы.

Разработанные технологии и методы могут значительно повысить уровень защиты речевой информации, что делает проект вкладом в область информационной безопасности. Эта работа продвигает научные исследования в области обработки речи и имеет практическое значение для защиты конфиденциальной информации в различных сферах, таких как бизнес, государственные структуры и личные коммуникации. Применение полученных результатов может привести к созданию более безопасных систем передачи данных. В бизнесе это может обеспечить защиту переговоров, в государственных структурах — конфиденциальность государственных тайных данных, а в личной жизни — защиту от утечек личной информации. Использование новых технологий и методов может способствовать повышению доверия пользователей к современным средствам связи и улучшению общей ситуации в области информационной безопасности.

Работа по разработке методов защиты речевой информации является шагом к созданию более безопасной среды для коммуникаций. Учитывая текущие тенденции в области информационных технологий, реализация предложенных решений может снизить риск утечек и повысить уровень защиты данных. Это позволит обеспечить безопасность не только личных, но и коммерческих интересов в условиях глобализированного мира. Успешная реализация данного проекта может стать основой для дальнейших исследований и разработок в области защиты информации, открывая новые горизонты для применения активных средств акустической маскировки и других инновационных технологий.

Список использованных источников:

1. Зайцев, А. П., Шелупанов, А. А., Мещеряков, Р. В., Голубятников, И. В., Солдатов, А. А., Скрыль, С. В. Технические средства и методы защиты информации - *горячая линия-Телеком, 2012.Россия.*

2. Калинин, С. В., Кондратьев, А. В..Защита информации: Учебное пособие - *инфра-М, 2015. Россия - М.: Книжный дом "ЛИБРОКОМ", 2014.*

3. Кузнецов, А. В..Методы защиты информации в компьютерных системах - *БХВ-Петербург, 2014.*

4. Смирнов, И. А. Информационная безопасность: Теория и практика - *Юрайт, 2016.*

UDC 519.6

SYNTHESIS OF SPEECH-LIKE NOISE BASED ON NEURAL NETWORK MODEL

Shunevich A.I., student of group 362201, Makarenya E.A., student of group 361401

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Zelmanovsky O.B. – Candidate of Technical Sciences, Associate Professor

The project "Synthesis of Speech-Like Noise Based on Neural Network Model" is dedicated to developing methods for protecting speech information from leaks in the context of modern information society. The main focus is on creating acoustic noise signals adapted to specific speech using machine learning. Existing methods and devices are studied, and algorithms for generating speech-like noise in the Russian language are developed. The work aims to enhance the security of confidential negotiations and can be applied in business and government structures.

Keywords: speech information, protection, noise signals, acoustic masking, neural networks, machine learning, confidentiality, algorithms, speech-like noise, information security, analysis, speech synthesis, technologies, segmentation, classification, audio signal, Russian language, frames, dynamic creation, protection systems.

СЕКЦИЯ «СИСТЕМЫ И СЕТИ ИНФОКОММУНИКАЦИЙ»

UDC 004.931

STATIC NETWORK SIMULATION BASED ON NS-3: PACKET NODE COMMUNICATION EXPERIMENT

DANG Z.F. (group 263111)

Belarusian State University of Informatics and Radioelectronics,Minsk, Republic of Belarus

MA J. – Assistant, Department of Information and Communications Technology

Annotation. In this paper, the method of packet node communication experiment using NS-3 network simulator is discussed. By building a static network with nine nodes, and using the CSMA protocol and UDP echo application, packet switching and data transmission between nodes are realized. Experimental results show that the NS-3 simulator can effectively simulate the communication process of packet nodes, and provides a powerful tool for network performance analysis and optimization.

Keywords: NS-3, packet node communication, CSMA protocol, UDP echo.

Introduction. With the continuous development of network technology, packet switching technology has become the core of modern networks. In packet-switched networks, data is split into small packets and transmitted through network devices. Node grouping is an important concept in packet-switched networks, which can divide nodes in a network into different groups for easy management and optimization of network performance. NS-3 is an open-source network simulator that provides a rich set of network models and tools that can be used to simulate various network scenarios and protocols.

The main part. Network topology construction: NS-3 [1] was utilized to establish a static network comprising nine nodes, which were then partitioned into three groups, each consisting of three nodes. The nodes within each group were interconnected through CSMA network devices, while the groups themselves were linked via point-to-point connections.

Protocol configuration: Inside each group, the nodes were connected using the CSMA protocol [2], with IP addresses assigned accordingly. The CSMA protocol [2], a form of media access control, facilitates the sharing of a communication medium among multiple nodes. It operates by requiring each node to sense the medium's availability before transmitting data, thereby reducing the likelihood of data collisions and enhancing network efficiency.

Application Configuration: A UDP echo [3] server was installed on the master node of each group, with UDP echo clients set up on the remaining nodes to facilitate packet exchange and data transfer between nodes. The UDP echo [3] application is a straightforward network application where a client sends a packet to a server, and the server echoes the packet back to the client.

Analysis of experimental results: The performance of packet node communication was evaluated by monitoring network traffic and packet loss rates. The experimental outcomes indicated that the CSMA protocol [2] effectively prevents data collisions and improves network efficiency. Packet node communication was found to be a reliable method for data transmission between nodes, and the network's performance was analyzed and optimized based on these experimental results.

Packet node communication experiment. In the experiment, as shown in Figure 1, in the packet node communication experiment, the master node of each group acts as a UDP echo server [3], while the other nodes act as clients, sending UDP packets to the server. After receiving the packet, the server performs an echo operation to send the packet back to the client. By monitoring key performance indicators such as network traffic and packet loss rate, the communication performance between packet nodes is analyzed in detail.

```
Flow 1 (10.1.1.2 -> 10.1.1.1)
  Tx Packets: 1
  Tx Bytes:   1052
  Rx Packets: 1
  Rx Bytes:   1052
  Lost Packets:   0
  Throughput: 0.988741 Mbps
  Delay: 0 - 0.001, Count: 0
  Delay: 0.001 - 0.002, Count: 0
  Delay: 0.002 - 0.003, Count: 0
  Delay: 0.003 - 0.004, Count: 0
  Delay: 0.004 - 0.005, Count: 0
  Delay: 0.005 - 0.006, Count: 0
  Delay: 0.006 - 0.007, Count: 0
  Delay: 0.007 - 0.008, Count: 0
  Delay: 0.008 - 0.009, Count: 1
```

Figure 1. Schematic diagram of a UDP packet node communication experiment

Performance comparison and experimental analysis. Experimental results show that the NS-3 simulator [1] can effectively simulate the communication process of packet nodes, and provides a powerful tool for network performance analysis and optimization. By adjusting the parameters of the CSMA protocol [2] and

the network topology, the network performance can be optimized, and the data transmission efficiency and reliability can be improved.

Conclusion. In this paper, the method of using NS-3 network simulator for packet node communication experiments is introduced, and the effectiveness of NS-3 simulator [1] is verified by experiments. Experimental results show that the NS-3 simulator can effectively simulate the communication process of packet nodes and provides a powerful tool for network performance analysis and optimization. In the future, the influence of packet node communication protocol and network topology on network performance can be further studied, and the application of NS-3 simulators in other network scenarios can be explored.

List of references:

1. ns-3 documentation: https://www.nsnam.org/docs/release/latest/

2. CSMA protocol: https://en.wikipedia.org/wiki/Carrier_sense_multiple_access

3. UDP echo protocol: https://en.wikipedia.org/wiki/Echo_protocol

УДК 004.732-021.131:004.056.5

РОЛЬ VPN-ТЕХНОЛОГИЙ В ПОВЫШЕНИИ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ ПРЕДПРИЯТИЯ

Ковалько О.А., Кулешов И.С.

гр. 367041

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Научный руководитель: Хацкевич О.А. – кандидат технических наук, доцент кафедры ИКТ

Аннотация. В статье рассматривается вопрос использования виртуальных частных сетей (VPN) в корпоративных структурах компаний. Анализируются наиболее значимые преимущества внедрения VPN для обеспечения целостности и конфиденциальности информации. Раскрывается процесс подключения к VPN. Исследуются тенденции развития технологий реализации VPN-каналов.

Ключевые слова: VPN, GRE, защита данных, виртуальная частная сеть, сетевой трафик.

Введение. В современном мире информация является одной из наиболее ценных составляющих, и, как любую другую ценность, человек стремится защитить её от несанкционированного доступа и вмешательства. С развитием компьютерных технологий вопрос сохранения и защиты информации приобретает всё большее значение, и проблема информационной безопасности становится чрезвычайно актуальной.

Среди методов, направленных на обеспечение доступности информации, исследователи отмечают использование сочетания различных подходов к контролю, дублированию и резервированию данных. Для обеспечения целостности и конфиденциальности информации в сетях применяются методы построения виртуальных каналов, основанные на использовании криптографических технологий.

В этом контексте, VPN (виртуальная частная сеть или туннелирование) представляет собой технологию, позволяющую установить постоянное защищенное соединение между

компьютером и сервером, основанное на передаче данных в виде зашифрованных пакетов GRE. Для шифрования используется современный алгоритм MPPE с 128-битным состоянием, который обеспечивает высокий уровень безопасности.

Основная часть. Актуальность исследования потенциала внедрения виртуальных частных сетей (VPN) в корпоративные структуры компаний обусловлена несколькими ключевыми аспектами:

– VPN-сети обеспечивают высокий уровень безопасности передаваемой информации посредством шифрования, что особенно актуально для защиты конфиденциальных корпоративных данных;

– использование VPN позволяет существенно снизить риски утечки данных, предотвращая несанкционированный доступ к внутренней информации компании;

– с помощью VPN сотрудники получают возможность подключаться к корпоративной сети независимо от своего местоположения, что крайне важно в условиях растущей популярности гибридных и удаленных режимов работы;

– удаленные работники благодаря VPN имеют беспрепятственный доступ ко всем необходимым ресурсам компании, включая внутренние базы данных и приложения;

– при наличии у организации нескольких офисов, VPN обеспечивает безопасное и надежное соединение между ними;

– VPN способствует управлению трафиком и распределению нагрузки между различными узлами сети;

– внедрение VPN-сетей позволяет создать защищённую сеть без необходимости прокладывания физических линий связи, что существенно снижает затраты на развитие инфраструктуры;

– VPN предоставляет возможность централизованного управления доступом и правами пользователей, что упрощает процессы администрирования безопасности и позволяет оперативно реагировать на потенциальные угрозы;

– использование VPN позволяет скрыть реальный IP-адрес пользователей, затрудняя проведение атак на корпоративную сеть и повышая общую безопасность компании.

Процесс подключения к виртуальной частной сети VPN выглядит следующим образом: на компьютере формируется пакет GRE, который затем шифруется с использованием одного из доступных алгоритмов шифрования. После этого зашифрованный пакет отправляется на VPN-сервер, где происходит его расшифровка. Сервер обрабатывает запрос и пересылает его к нужному ресурсу для получения или передачи информации. Ресурс, получив запрос от VPN-сервера, обрабатывает его и отправляет обратно необходимую информацию. Затем сервер VPN вновь формирует зашифрованный пакет GRE и передает его на компьютер пользователя, где происходит расшифровка и отображение запрашиваемого результата.

Такой процесс обеспечивает постоянный защищенный поток зашифрованной информации от компьютера к ресурсам Интернета, что гарантирует безопасность и конфиденциальность передаваемых данных.

Хотя использование данной технологии приводит к некоторой задержке в передаче данных из-за многоэтапного процесса шифрования и расшифровки, это замедление обычно несущественно и не влияет на комфортную работу пользователя [1].

Технология VPN (Virtual Private Network – виртуальная частная сеть) представляет собой один из эффективных способов защиты сетей и данных, которые передаются через них.

Основная концепция технологии VPN заключается в следующем:

– на всех устройствах (в частности, ПК), имеющих доступ к сети Интернет, устанавливается программное обеспечение, реализующее функционал VPN, например, VPN-

агент. Это гарантирует, что ни одно устройство конечного пользователя не останется незащищенным;

– VPN-агенты автоматически шифруют всю исходящую информацию и, соответственно, расшифровывают входящие данные. Они также обеспечивают проверку целостности данных, используя электронную цифровую подпись (ЭЦП) или хэш (криптографическая контрольная сумма, рассчитанная на основе ключа шифрования);

– поскольку данные, передаваемые по Интернету, представляют собой совокупность пакетов, сформированных протоколом IP, VPN-агенты работают именно с такими пакетами;

– перед отправкой IP-пакета VPN-агент выполняет следующие действия:

1) по IP-адресу получателя из имеющихся алгоритмов шифрования и ЭЦП выбирается соответствующий алгоритм для защиты пакета, и формируются ключи. Если информация о получателе отсутствует в настройках, передача данных не осуществляется;

2) добавляется ЭЦП отправителя или соответствующий хэш в пакет;

3) происходит полное шифрование пакета, включая его заголовок;

4) выполняется процесс инкапсуляции, при котором создается новый заголовок, указывающий не на конечного получателя, а на его VPN-агент. Эта функция обеспечивает дополнительную защиту, представляя обмен данными между двумя сетями как взаимодействие между двумя компьютерами, оснащенными VPN-агентами, и скрывает внутренние IP-адреса от злоумышленников.

– при получении IP-пакета выполняются следующие обратные операции:

1) если заголовок содержит информацию о VPN-агенте отправителя, который отсутствует в списке разрешенных адресов, пакет просто игнорируется. Аналогичная процедура применяется к пакетам с поврежденными заголовками.

2) в соответствии с настройками выбираются соответствующие алгоритмы шифрования и ЭЦП, а также необходимые ключи;

3) пакет расшифровывается, и проверяется его целостность. В случае неверной ЭЦП, пакет отклоняется;

4) затем пакет в исходном формате передается конечному получателю по внутренней сети.

Все данные операции выполняются в автоматическом режиме. Основная сложность технологии VPN заключается в настройке VPN-агентов, однако опытный пользователь вполне способен справиться с этой задачей.

VPN-агент устанавливается непосредственно на защищенном компьютере, что особенно эффективно для мобильных пользователей, подключающихся к сети Интернет. В этом случае обеспечивается безопасность обмена данными только для устройства, на котором установлен VPN-агент.

Существует возможность объединения функций VPN-агента с маршрутизатором, в этом случае он приобретает название криптографического маршрутизатора IP-пакетов [2].

Основной задачей VPN-агента является создание безопасного канала между защищаемыми сетями, часто называемого «туннелем». Кроме этого, все пакеты данных проходят через процесс «фильтрации» в соответствии с установленными настройками агента. Таким образом, работа VPN-агента сводится к выполнению двух ключевых функций: созданию туннелей и фильтрации передаваемых пакетов.

Набор правил, регулирующих создание туннелей, называется «политикой безопасности» и задается в настройках VPN-агента. После проверки пакетов они либо направляются в определенные туннели, либо отбрасываются на основании следующих критериев: IP-адреса источника (для исходящих пакетов это адрес конкретного компьютера, входящего в

защищаемую сеть); IP-адреса назначения; протоколы более высокого уровня, к которым относятся данные пакеты (например, TCP или UDP); номера портов, через которые осуществляется отправка информации (например, 1080).

Таким образом, выделенные механизмы позволяют VPN-агенту эффективно обеспечивать безопасность и контроль передачи данных в корпоративной или частной сети.

В последние годы наблюдается значительное развитие технологий, связанных с внедрением виртуальных частных сетей (VPN). Это обусловлено не только растущей потребностью в защите данных в условиях повсеместной цифровизации, но и стремлением пользователей к более свободному и безопасному доступу к информации.

Одной из основных тенденций является совершенствование криптографических методов, применяемых для шифрования сетевого трафика. Традиционные протоколы, такие как PPTP и L2TP, постепенно уступают место более современным и надежным решениям, таким как OpenVPN и WireGuard. Эти новые протоколы обеспечивают более высокий уровень защиты данных, применяя улучшенные алгоритмы шифрования и аутентификации, что значительно усложняет перехват и расшифровку данных для потенциальных злоумышленников.

Еще одной важной тенденцией является интеграция VPN-технологий с облачными сервисами. Современные VPN-решения позволяют не только создавать защищенные каналы на локальных серверах, но и использовать возможности облачных инфраструктур. Это обеспечивает бизнесу новые возможности в плане гибкости, масштабируемости и доступности VPN-сетей посредством децентрализованных архитектур.

Также, в связи с глобализацией и увеличением количества удаленно работающих сотрудников, наблюдается повышенный интерес к мобильным VPN-решениям. Разработчики активно создают приложения, позволяющие пользователям подключаться к корпоративным сетям из любой точки мира через мобильные устройства. Это требует тщательной оптимизации, как в плане производительности, так и обеспечения безопасности, что способствует разработке новых протоколов и алгоритмов, адаптированных для мобильных платформ.

Особое внимание уделяется также вопросу конфиденциальности данных. В условиях усиления требований, таких как Общий регламент по защите данных (GDPR) в Европе, компании все чаще внедряют VPN не только для защиты собственной информации, но и для обеспечения конфиденциальности данных клиентов. Прозрачность работы VPN-провайдеров и возможность аудита их политики безопасности становятся ключевыми факторами в этом процессе.

Нельзя не отметить также растущую роль искусственного интеллекта и машинного обучения в развитии VPN-технологий. Эти инструменты все чаще используются для мониторинга сетевого трафика, автоматизации выявления нежелательных действий и оптимизации использования ресурсов. Внедрение ИИ в VPN-системы позволяет создавать более адаптивные и интеллектуальные решения, которые способны прогнозировать и предотвращать потенциальные угрозы [3].

Таким образом, развитие технологий VPN-каналов характеризуется комплексным подходом к вопросам безопасности, приватности и доступности. Эти изменения, происходящие на фоне быстрого развития информационных технологий, формируют новые стандарты и определяют дальнейшее направление развития виртуальных частных сетей.

Заключение. Организация защищенного канала передачи данных является одной из ключевых задач, поскольку информация представляет собой ценный ресурс для любой компании. Корпоративные сети должны обеспечивать высокий уровень безопасности и надежности, что нередко требует использования сложных технологий, таких как VPN.

Виртуальные частные сети позволяют создавать зашифрованные каналы для передачи данных, обеспечивая защиту информации от несанкционированного доступа.

В ходе исследования и анализа современных технологий создания сетей VPN было выявлено, что за последние годы технологии виртуальных частных сетей (VPN) значительно эволюционировали. Этот прогресс обусловлен растущей потребностью пользователей в обеспечении безопасности данных и свободном доступе к информации.

Таким образом, учитывая современные тенденции в реализации VPN-технологий, можно заключить, что их грамотное и эффективное применение представляет собой важнейший этап на пути к созданию безопасной и высокодоступной вычислительной среды, способной удовлетворить текущие требования и вызовы времени.

Список литературы

1. *Прокопов, В. VPN. Теория и реальность / В. Прокопов [Электронный ресурс]. – Режим доступа: https://www.solidex.by/wp-content/uploads/2017/07/vpn_-_teoriya_i_realnost.pdf. – Дата доступа: 20.09.2024.*

2. *Олифер, В.Г. Компьютерные сети: Принципы протоколы технологии / В.Г. Олифер, Н.А. Олифер. – 3-е издание. – СПб: Пирер, 2006. – 367 с.*

3. *The Future of VPN Technology: Trends and Innovations to Watch in 2024 [Electronic resource]. – Mode of access: https://neg.by/novosti/otkrytj/risk-slit-dannye-est-li-smysl-ispolzovat-opensorsnye-resheniya-pri-zashchite-kanalov-svyazi/. – Date of access: 20.09.2024.*

UDC 004.732-021.131:004.056.5

THE ROLE OF VPN TECHNOLOGIES IN INCREASING THE SECURITY OF THE ENTERPRISE'S CORPORATE NETWORK

Kovalko O.A, Kuleshov I.S.

gr.367041

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Khatskevich O.A. – Candidate of Technical Sciences, Associate Professor of the Department of ICT

Annotation. The article examines the issue of using virtual private networks (VPN) in corporate structures of companies. The most significant advantages of implementing VPN to ensure the integrity and confidentiality of information are analyzed. The process of connecting to VPN is disclosed. Trends in the development of technologies for implementing VPN channels are studied.

Keywords: VPN, GRE, data protection, virtual private network, network traffic.

UDC 621.391

DEEP LEARNING BASED RUSSIAN HANDWRITEN RECOGNITION

LIU J.H., XIONG S., DANG Z.F. (Group 263111)

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

MA J. – Assistant, Department of Information and Communications Technology

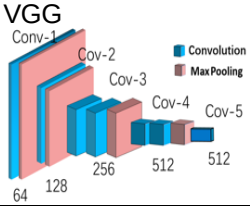
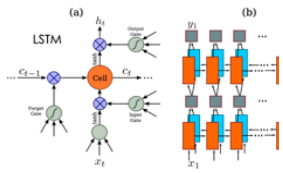
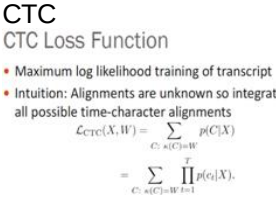
Annotation. This paper presents a Russian handwriting recognition algorithm based on deep learning. The algorithm combines improved VGG network feature extraction capabilities with LSTM time modeling capabilities and introduces data enhancement and optimizer tuning strategies. Experimental results show that the proposed algorithm is significantly superior to the existing methods in recognition accuracy and training efficiency.

Keywords: Russian Handwriting recognition, Deep learning, VGG network, LSTM network, Data enhancement.

Introduction. Russian handwriting recognition is of great value in the field of information processing. With the increase in communication between China and Russia, the demand for automated Russian handwriting recognition systems is growing. However, due to the complexity of the Russian Cyrillic alphabet and the diversity of writing styles, the existing recognition systems are still lacking in accuracy and speed. In recent years, deep learning techniques have made significant progress in the field of text recognition, but there has been relatively little specialized research on Russian handwriting.

The main part. The model used in this paper is based on EasyOCR framework, which combines LSTM, VGG convolutional neural network and CTC loss function. EasyOCR is an open source OCR framework that supports multiple languages. The EasyOCR framework is shown in Table Through data enhancement, optimizer adjustment and parameter filtering, the original model is improved, and the recognition accuracy is increased. In this paper, VGG is used to extract feqatures from handwritten images to provide high-quality input for recognition. LSTM is a recursive neural network, which can effectively deal with long-term dependency in sequence data and capture the context information of character sequences, so as to improve the recognition accuracy. The CTC loss function is suitable for the character sequence annotation in handwriting recognition, allowing the model to predict the character sequence directly without pre-segmentation of the input image.

Table 1- The EasyOCR Framework Table

CRNN		
VGG	LSTM	CTC
		

Model Structure and Parameter Tuning. In order to optimize the performance of the model, we adjusted the parameters, including: data enhancement, optimizer Settings, parameter filtering. Through the experiment, we got the following improvement. The experimental results show that the improved algorithm shows significant improvement in both training and validation loss. The training loss of the original algorithm decreases rapidly in the initial stage, but the verification loss fluctuates after reaching a certain degree, which indicates that there may be overfitting phenomenon. However, the training and verification losses of the new algorithm show a steady decline trend, and the final loss value is lower than that of the original algorithm, showing better generalization ability. In terms of accuracy, the performance of the improved algorithm continued to improve, eventually reaching an accuracy of about 42%. In contrast, the accuracy of the original algorithm increased rapidly in the early stage of training and then stabilized at about 30%. This result shows that the improved algorithm has obvious advantages in learning ability and adaptability. In the comparison of training time, the total training time of the improved algorithm is about 5000 seconds, which is reduced from 6000 seconds of the original algorithm. This result shows that the improved algorithm has a significant improvement in training efficiency, especially when dealing with large-scale data sets, and can save more computing resources and time. Overall, the improved algorithm is superior to the original algorithm in terms of loss, accuracy and

training time, demonstrating better model optimization and training efficiency. These results provide strong support for the practical application of Russian handwriting recognition.

Performance Comparison and Experimental Analysis. Comparison of training and validation losses is shown in Table . Training accuracy comparison is shown in Table Comparison of total training time is shown in Table .

The original algorithm drops rapidly in training loss, but the validation loss stabilizes or even rises slightly after an initial drop, indicating possible overfitting.

The new algorithm shows a steadier decline in both training and validation losses, and the final loss values are lower than those of the original algorithm, showing better generalization. The comparison of training and validation losses is shown in Table .

Table 2- Comparison of training and validation losses Table

Iterations	Original Method		Proposed Method	
	Train Loss	Valid Loss	Train Loss	Valid Loss
10000	0,1	1,5	0,25	0,9
20000	0,05	1,8	0,1	1
30000	0,05	2,1	0,05	1,2
40000	0,05	2,2	0,05	1,3
50000	0,05	2,2	0,05	1,4

The accuracy of the original algorithm rose rapidly in the early stages but then grew slowly and eventually stabilized at about 30 %.

The accuracy of the new algorithm continues to rise throughout the training process, eventually reaching about 42 %, showing better learning ability and higher accuracy. A comparison of the training accuracies is shown in **Error! Reference source not found.**

Table 3- Training accuracy comparison

Iterations	Accuracy	
	Original Method	Proposed Method
10000	25%	32%
20000	25%	35%
30000	27%	36%
40000	27%	36%
50000	30%	42%

The total training time of the original algorithm grows linearly with the number of iterations, eventually reaching about 6000 seconds.

The total training time of the new algorithm grows at a slower rate, eventually totaling about 5000 seconds, showing greater time efficiency throughout the training process. Comparison of total training time is shown in **Error! Reference source not found.**

Table 4- Comparison of total training time

Iterations number	Time Comsuption for trainning	
	Original method	Proposed method
50000	6000	5000

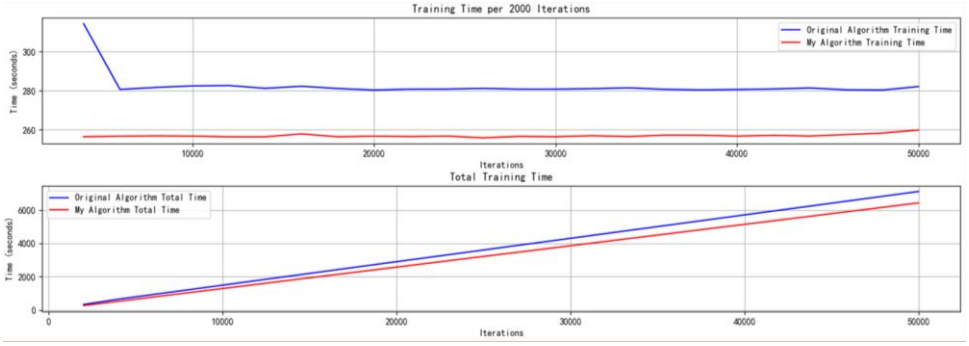


Figure 1. Comparison of total training time

Conclusion. By optimizing the model structure and adjusting the parameters, the accuracy and speed of Russian handwriting recognition are significantly improved. The experimental results show that the improved model is superior to the original algorithm in terms of training time and total training time, showing higher efficiency and better performance. Future research will explore deeper network structures to further improve performance and investigate more efficient feature extraction methods for handwriting recognition in other languages and for deployment and optimization on mobile devices.

List of references:

1. The Generation of Human Handwriting in Russian / A. B. Ivanov. Pattern Recognition and Image Analysis. 2023.

2. Russian and Kazakh Handwriting Database for Text Recognition / E. V. Petrova., D. A. Smirnov. Journal of Pattern Recognition. 2022.

3. Handwritten Character Recognition: Feature Extraction and Classifier Research. / M. I. Kuznetsov. Journal of Computer Science. 2021.

4. Multi-Language Online Handwriting Recognition / R. A. Johnson., J. B. Smith. International Conference on Pattern Recognition. 2020. P. 456–478.

5. Deep Learning-Based Handwritten Text Recognition / L. N. Petrov. Journal of Artificial Intelligence. 2023. P. 789–812.

6. MetaHTR: Style-Adaptive Handwritten Text Recognition / K. L. Brown. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2022. P. 901–923.

UDC 535.81: 519.25

IMPROVING LASER METHANE EMISSION MONITORING WITH FREQUENCY–AMPLITUDE FEATURE OF ABSORPTION PULSE

Bach N.V.[1]

Belarusian State University of Informatics and Radioelectronics[1]*, Minsk, Republic of Belarus*

Tsviatkou V.Yu. – Doctor of Technical Sciences, Professor

Annotation. Accurate monitoring of methane emissions is vital for environmental management and safety in oil and natural gas operations. This paper introduces a methodology leveraging advanced analytics and experimental data to build a linear regression model for methane concentration estimation. The approach utilizes a time–frequency analysis and incorporates proposed frequency–amplitude features of the absorption pulse, which have shown a strong correlation with methane concentration. Experimental results validate that the proposed feature achieves a higher correlation (R^2=0.981) with methane concentration.

Keywords. Laser absorption spectroscopy, time–frequency, methane emission, absorption pulse, frequency–amplitude.

Introduction. Methane is a colorless, odorless and flammable gas that can be found in a variety of environments, including natural gas production and distribution facilities, landfills, agricultural operations and industrial plants. Detecting methane leaks is important for safety, environmental and regulatory reasons. Optical methods for determining methane gas concentration employ spectroscopic techniques, providing accurate and reliable measurements. Infrared absorption spectroscopy is a prominent approach within this category, where methane molecules absorb specific wavelengths of infrared light. The concentration of methane is based on the level of light absorption, offering a highly sensitive and selective detection method. There exist three major approaches based on tunable diode laser absorption spectroscopy: direct absorption spectroscopy (DAS), wavelength modulation spectroscopy (WMS) and wavelength modulation–direct absorption spectroscopy (WM–DAS).

DAS is the most straightforward version of laser absorption spectroscopy due to limited equipment required for its implementation, quick alignment and interpretation of raw data. [1, 2]. However, this method has lower sensitivity due to uncertainty in the laser output signal measurement. In contrast to DAS, WMS using the harmonic detection technology can effectively eliminate the influence of baseline uncertainty and work with a much higher modulation frequency (as high as several hundred kHz) [3, 4] . Therefore, WMS is resistant to low–frequency noise and has a higher sensitivity. As it is known, WMS technology has been widely studied and used for gas properties measurement [5, 6, 7, 8]. While WMS can achieve higher accuracy and sensitivity in gas absorption measurements compared to DAS, the complexity of signal modulation and the use of a lock–in amplifier make WMS more challenging to implement than the DAS method. WM–DAS combines the simplicity and calibration–free nature with the enhanced noise rejection and high sensitivity offered by the harmonic detections, establishing it as an efficient and reliable method for methane gas concentration estimation.

This paper implements advanced analytics techniques on experimental datasets to build a linear regression model for estimating methane concentration. A larger experimental dataset improves model accuracy by capturing complex relationships between independent variables and the dependent variable. Additionally, larger sample sizes are more representative of the overall population, thereby reducing variance–related errors.

In our paper, we focus on analyzing the raw absorption signal features related to methane gas concentration obtained by laser absorption spectroscopy in time–frequency domain. The main contributions of our research are summarized as follows:

– The proposed frequency–amplitude feature of absorption pulse is proposed to improve methane concentration estimation accuracy;

– The proposed linear regression model for estimating methane concentration;

– A detailed step–by–step methodology for estimating the features of the absorption pulse is presented, enhancing the precision and reliability of the estimation process.

The method for methane absorption pulse features estimation. The transmitted light intensity $I_t(t)$ of the radiation can be related to the absorbing gas concentration and presented by the Beer–Lambert law, is given by:

$$I_t(t) = I_0(t) \cdot exp[-\sigma(\lambda)cl] \tag{1}$$

where $I_0(t)$ is the laser output signal; λ is the wavelength of laser emitter; $\sigma(\lambda)$ is the absorption coefficient, which is a function of wavelength λ; c is the gas concentration; l is the optical path length.

When performing the harmonic analysis [9], the detected signal $I_t(t)$ in Eq. (1) can be divided as:

$$I_t(t) = \left\{(V_{DC} \propto \bar{I}) + \left(V_{indep_{1f}} \propto i\right) + \left[\left(V_{dep_{2f}} + V_{dep_{3f}} + V_{dep_{4f}} + \cdots\right) \propto (\sigma cl)\right]\right\} \tag{2}$$

where V_{DC} represents the DC signal depending on the average intensity $\bar{I}$; $V_{indep_{1f}}$ is the absorption independent $1f$ component which is related to the intensity scanning depth i; $V_{dep_{2f}}, V_{dep_{3f}}, V_{dep_{4f}}, \ldots$ are amplitudes of harmonics.

As follow from Eq. (1) and (2) transmitted intensity signal $I_t(t)$ consists two main components: laser output and absorption signals. Based on the literature review, it can be confirmed that the method for methane absorption pulse features estimation (**Figure 1**) is based on procedures including signal decomposition [9], signal calibration [5], segmentation and fusion of pulse in absorption signal (as show in Absorption pulse extraction session).

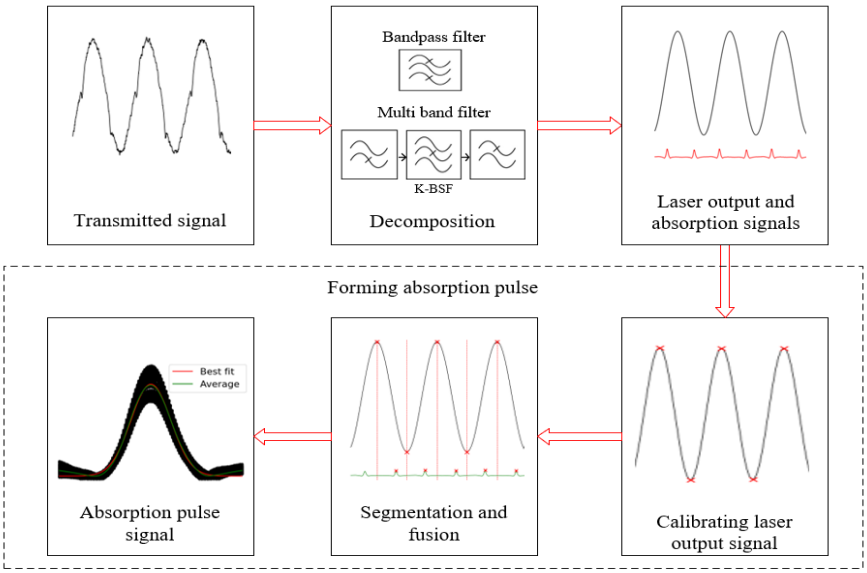


Figure 1 – The method for methane absorption pulse features estimation

In the final step, the absorption pulse signal $AP_{I_{ATSMA}}$ is defined in the time domain. For estimating the absorption pulse features related to gas concentration, it is proposed the following two frequency–amplitude features of absorption pulse.

1.The amplitude spectrum of absorption pulse.

$$A_{F_{AP}} = \max_{1 \le k \le N_F} |F_{AP}(k)| \tag{3}$$

where $|F_{AP}(k)|$ is the *k*–th spectral sample value of the spectrum of absorption pulse $AP_{I_{ATSMA}}$; N_F is the number of spectral samples of the spectrum of absorption pulse.

2.The integrated spectrum of absorption pulse.

$$F_{APint} = \sum_{k=1}^{N_F} F_{AP}(k) \tag{4}$$

Laser output and absorption signals extraction. The aim of this process is to extract the laser output and absorption signals. **Figure 2** shows the transmitted signal.

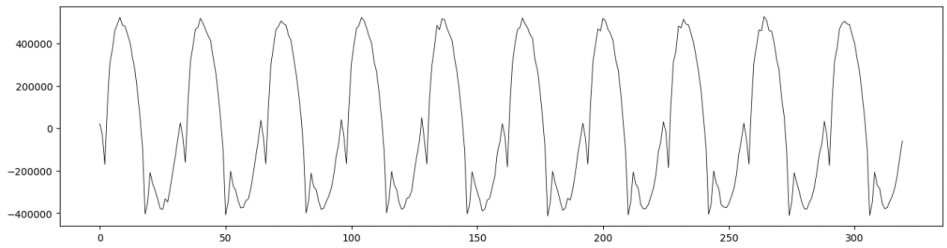


Figure 2 – Transmitted signal

After analyzing the transmitted signal, the laser output signal is extracted by applying bandpass filter with center frequency 10 kHz and bandwidth 100Hz, as shown in **Figure 3**. This signal represents the initial laser light and serves as a reference for calibrating absorption signal.

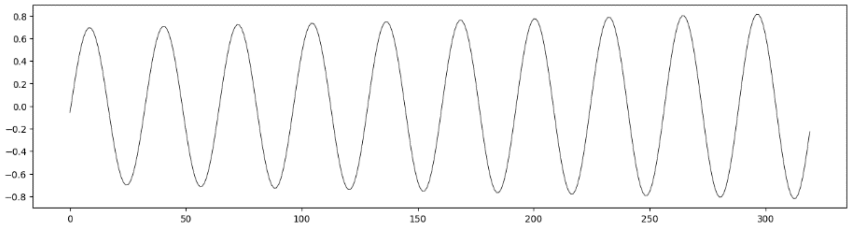


Figure 3 – Laser output signal

The absorption signal is extracted by Fourier–domain–based line shape recovery method [9. and represented in **Figure 4**. This signal is critical for determining the concentration of methane, as it represents the amount of laser light absorbed by the methane molecules.

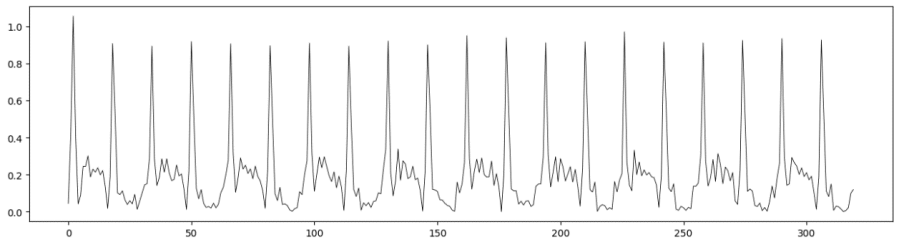


Figure 4 – Absorption signal

Absorption pulse extraction. In this section, the focus is on the extraction of the absorption pulse from the laser output and absorption signals. To begin the extraction process, the absorption signal is segmented (red dot line) based on peak and valley of the laser output, as depicted in **Figure 5**. This segmentation helps in isolating the pulse interval of the absorption signal that correspond to each half cycle of the laser output signal.

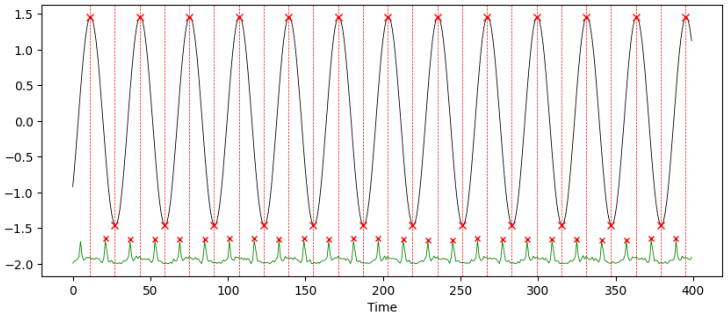


Figure 5 – Illustration of the segmentation of the absorption signal

As the laser intensity transitions from a local maximum to a local minimum, the laser's wavelength sweeps across the methane absorption line. The absorption line in spectroscopy refers to a specific wavelength where a target gas molecule absorbs laser light and it is less affected by other gases. When the laser wavelength coincides with the methane absorption line, the absorption intensity reaches its peak.

Once the segmentation is completed, the next step involves averaging all the segmented absorption pulses. **Figure 6** shows the averaged absorption pulse and its best fit curve.

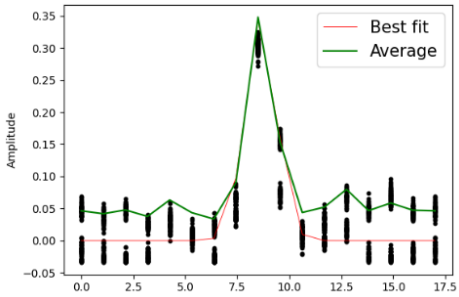


Figure 6 – The averaged absorption pulse signal

These steps are essential for accurately extracting and analyzing the absorption pulse, which is a key factor in absorption pulse features estimation.

Absorption pulse features estimation in frequency domain. Analyzing the absorption pulse in the frequency domain allows for the extraction of key features that characterize the methane absorption process, which can be more effective than time–domain analysis. The process begins by applying a Fourier transform to the averaged absorption pulse, converting the signal from the time domain to the frequency domain. **Figure 7** presents the frequency spectrum of the absorption pulse.

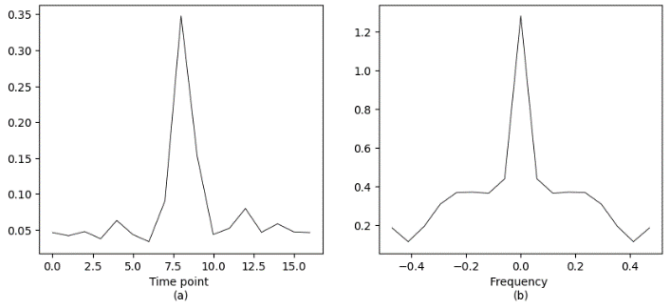


Figure 7 – Absorption pulse in time (a) and frequency domain (b)

The features of absorption pulse in frequency domain provide valuable insights into the methane concentration and can be used to enhance the accuracy of concentration measurements.

Estimation of the relationship between CH_4 concentration and absorption pulse features. The experiment was performed with laser output power of 166nW passing through a methane volume with different concentrations:100 ppm, 250 ppm, 540 ppm, 1000 ppm and 2000 ppm. For each of five concentration value, 5 measured signals will be used.

Relationship between methane concentration and well–known absorption pulse features, such as absorption pulse amplitude [10] and integrated absorption pulse [11] in time domain, was compared with proposed frequency–amplitude features of absorption pulse (amplitude spectrum and integrated spectrum of absorption pulse) as shown in **Figure 8**. The coefficient of determination R^2 is used as a measure of goodness of fit.

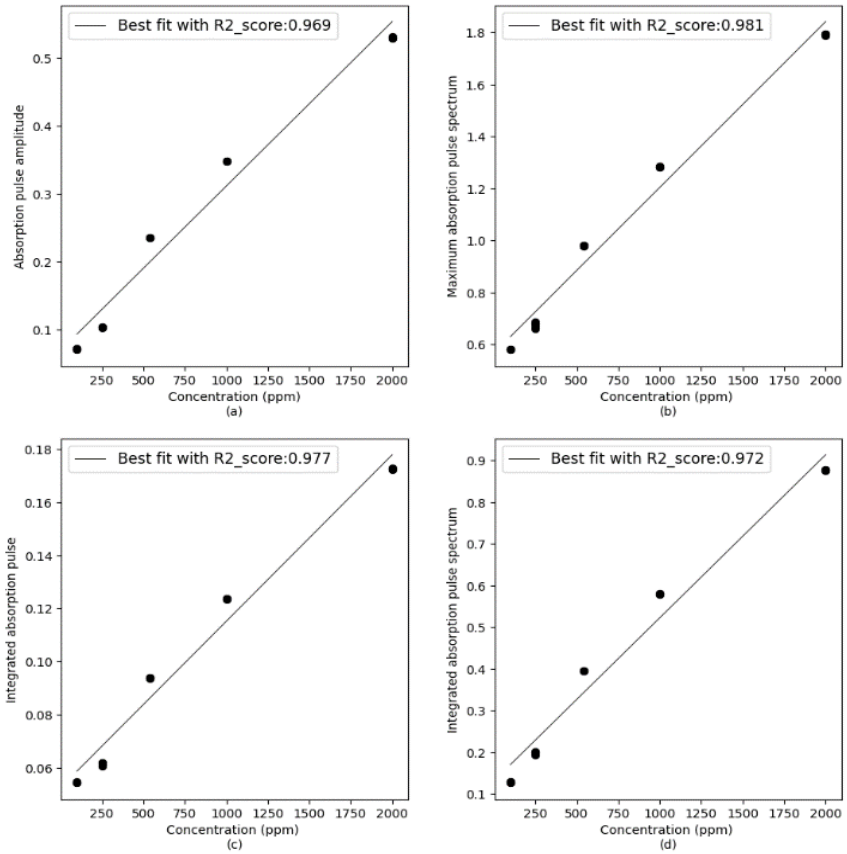


Figure 8 – Relationship between the absorption pulse features and methane concentration: (a) absorption pulse amplitude (R2=0.969), (b) amplitude spectrum of absorption pulse (R2=0.981), (c) integrated absorption pulse (R2=0.977), (d) integrated spectrum of absorption pulse (R2=0.972)

It follows from **Figure 8** that the linear regression model $y = 0.00064x + 0.566$ with $R^2 = 0.981$ (**Figure 8 (b)**), where x is CH_4 concentration value and y is amplitude spectrum of absorption pulse, is more robust. It is mentioned that with a large amount of experimental data, the linear regression model can achieve higher accuracy.

Conclusion. The two frequency absorption pulse features (amplitude spectrum and integrated spectrum **of absorption** pulse) related to gas concentration have been proposed. These features were derived from a time–frequency analysis of the absorption signal, and they significantly enhance the correlation of methane concentration and absorption signal feature. These features show a strong correlation with methane concentration, with an $R^2 = 0.981$, indicating their effectiveness in accurately estimating methane concentrations.

References:

1. Wojtas, J. Aspect of the applications of cavity enhanced spectroscopy to nitrogen oxides detection / J. Wojtas, J. Mikolajczyk, Z. Bielecki // Sensors (Basel), 2013 Jun. –Vol. 13, iss. 6. – P. 7570–98.

2. Goldenstein, C.S. Diode laser measurements of linestrength and temperature–dependent lineshape parameters of H_2O–, CO_2–, and N_2–perturbed H_2O transitions near 2474 and 2482 nm / C. S. Goldenstein, J. B. Jeffries, R. K. Hanson // Journal of Quantitative Spectroscopy and Radiative Transfer, 2013. –Vol. 130. – P. 100–111.

3. Marc–Simon, B. Determining the most suitable spectral range for TDLS–A quantitative approach / B. Marc–Simon, B. Bernd, W. Marcus // Journal of Quantitative Spectroscopy and Radiative Transfer, 2022. –Vol. 286. – P. 108–216.

4. Pyun, S.H. Interference–free mid–IR laser absorption detection of methane / S. H. Pyun, J. Cho, D. F. Davidson, R. K. Hanson // Meas. Sci. Technol, 2011. –Vol. 22. – P. 100–111.

5. Yihong, W. Calibration–free wavelength modulation spectroscopy based on even–order harmonics / W. Yihong, Z. Bin, L. Chang // Opt. Express, 2021. –Vol. 29. – P. 26618–26633.

6. Avetisov, V. Geiser. Hydrogen Sensor Based on Tunable Diode Laser Absorption Spectroscopy / V. Avetisov, O. Bjoroey, J. Wang. –P. Geiser // Sensors, 2019. –Vol. 19, iss. 23. – P. 5313–5319.

7. Peng, Z. Highly Sensitive, Calibration–Free WM–DAS Method for Recovering Absorbance–Part I / Z. Peng, Y. Du, Y. Ding // Sensors, 2020. –Vol. 20, iss. 3. – P. 681–695.

8. Peng, Z. Highly Sensitive, Calibration–Free WM–DAS Method for Recovering Absorbance–Part II: Experimental Analysis / Z. Peng, Y. Du, Y. Ding // Sensors, 2020. –Vol. 20, iss. 3. – P. 616–624.

9. Liang, R. A Fourier–domain–based line shape recovery method used in direct absorption spectroscopy / R. Liang [et al.] // Spectrochimica Acta Part A: Molecular and Biomolecular Spectroscopy, 2022. –Vol. 275. – P. 117–123

10. He, H. In–Situ Testing of Methane Emissions from Landfills Using Laser Absorption Spectroscopy / H. He [et al.] // Applied Sciences, 2021. –Vol. 11, iss. 5. – P. 2117–23.

11. Mayerhöfer, T.G. Beer's law-why integrated absorbance depends linearly on concentration / T.G. Mayerhöfer, A.V. Pipa, and J. Popp // ChemPhysChem, 2019. –Vol. 20, iss. 21. – P. 2748–2753.

УДК 004.658:656.82-048.35

МОДЕРНИЗАЦИЯ СЕТИ СБОРА И ПЕРЕДАЧИ ДАННЫХ ПРЕДПРИЯТИЯ СВЯЗИ

Ножников Е.А., магистрант гр.367041; Ножников Р.А., магистрант гр.367041

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Научный руководитель: Хацкевич О.А. – кандидат технических наук, доцент

Аннотация. В материалах доклада рассматриваются способы повышения эффективности работы центров обработки данных связи на базе современных технологий. Разработка системы виртуализации ресурсов сети и динамического распределения нагрузки, позволит оптимизировать ресурсы сети и осуществить эффективное управление нагрузкой и защитой информации на сети.

Ключевые слова: модернизация, центр сбора и обработки информации, виртуализация

Введение. Объем генерируемой человечеством информации постоянно растет. По прогнозам специалистов, к 2025 году объем всех данных в мире составит 175 зетабайтов (ЗБ). Это в 10 раз больше, чем в 2016 году [1].

Актуальность темы связана с тем, что, в связи с увеличением спроса на услуги, предоставляемые сетью сбора и обработки данных предприятия связи, а также изменением структуры трафика сети, возникает острая необходимость в проектирование отказоустойчивой комплексной централизованной системы с более высоким уровнем производительности.

Для обработки и хранения информации существуют центры обработки данных (ЦОД).

Центр обработки данных представляет собой централизованную вычислительную систему с достаточно высоким уровнем производительности и высокой готовностью для решения задач предприятия.

Задача ЦОД состоит в обеспечении бесперебойного функционирования сервисов информационной системы предприятия.

В общем случае, понятие ЦОД включает в себя следующие элементы:

– серверы с высокой надежностью и кластеризацией;

– сетевое оборудование;

– системы хранения данных с возможностью локальной репликации;

– систему резервного копирования;

– программное обеспечение конфигурирования, управления и контроля;

– системы обеспечения бесперебойного питания;

– систему обеспечения микроклимата;

– систему контроля доступа;

– систему пожаротушения.

Исходя из опыта эксплуатации ЦОД столкнулись с рядом проблем, решением которых является модернизация ЦОД.

Основная часть.

Проблемы которые привели к необходимости модернизации ЦОД – это, во-первых, недостаточная востребованность мощностей серверного "железа" программными продуктами и, следовательно, возврат инвестиций в сервера (ROI). На данный момент в среднем на наших серверах и на серверах наших клиентов утилизация серверной инфраструктуры составляет порядка 15-20%, при экономически оправданной 70-75%.

Во-вторых, нехватка площадей серверных залов, места в стойках, кабельных каналов, высокие требования к энергопотреблению при нехватки мощностей линий.

В-третьих, низкие сроки внедрения и модернизации серверных мощностей и связанных с ними сервисов, сложности резервного копирования и восстановления.

Технология виртуализации представляет собой комплексное решение возникших проблем, позволяя существенно снизить расходы на расширение ИТ-инфраструктуры и на ее обслуживание.

В самом общем виде под виртуализацией понимается возможность использования физических ресурсов (памяти, процессора, дисков, сетевых адаптеров и так далее) компьютера для работы с несколькими параллельно функционирующими операционными системами. Иными словами, речь идет о том, что на одном и том же компьютере или сервере могут быть одновременно запущены, например, Windows и Linux и при этом обе системы будут использовать реальные ресурсы машины. Это актуально в том случае, если какое-либо ПО или веб-сервер существует или имеет полный набор функций только под одной версией ОС, отличной от той, на которой работает основной парк компьютеров в фирме. Кроме того, виртуализация помогает сэкономить на покупке нового оборудования: вместо приобретения второго, третьего и так далее сервера или ПК достаточно докупить нужный объем ОЗУ и дисковых накопителей. Также заметна экономия других ресурсов: электричества (работает один компьютер или сервер, а не несколько), пространства (площади дата-центра не потребуют расширения под новые серверные стойки) и усилий технического специалиста, который поддерживает, скажем, два сервера вместо двадцати.

Существует несколько вариантов создания виртуальных сред. Одним из них является использование гипервизора. Гипервизор - это специальное программное решение, позволяющее запустить на физическом сервере несколько операционных систем изолированно. В этом случае каждая операционная система имеет собственную файловую систему, процессы, пользователей, установленные приложения, настройки сетевых интерфейсов и так далее.

Второй вариант – контейнерная виртуализация или хост-виртуализация, где каждая виртуальная среда использует файлы и библиотеки одной операционной системы. Это позволяет в любой момент управлять тем, какие ресурсы использует тот или иной контейнер.

Так, например, при выполнении тяжелых задач одна виртуальная среда может задействовать все процессоры сервера, а не ограничиваться одним, выделяемым на виртуальную машину. Соответственно, эти системы можно обслуживать по отдельности (например, проводить перенос или копирование данных) без остановки самого сервера, на котором они запущены[2].

Двумя крупнейшими игроками, предоставляющими решения по виртуализации инфраструктуры, являются компании VMware и Microsoft. Обе компании предлагают различные подходы к организации виртуальной инфраструктуры и предоставляют собственный набор фирменных технологий и решений в области виртуализации.

В результате выполнения работы в тестовых целях на оборудовании ЦОД была развёрнута система ESX серверов, объединённая одним vCenter Server.

Благодаря использованию технологий VMware vMotion и Microsoft Live Migration была осуществлена миграция ряда служебных серверов с работающих машин с одного физического узла на другой в реальном времени без остановки и простоя служб. Это позволило добиться высвобождения ряда серверов, уплотнив нагрузку на других, а также добиться большей надёжности за счёт создания резервных копий и шаблонов виртуальных машин.

При этом, использование ESX сервера позволяет упростить изменение квот как на параметры CPU и оперативной памяти, так и на использование дискового пространства.

ESX позволяет контролировать и динамически перераспределять вычислительные ресурсы серверов виртуализации (процессоры, память, диски) при помощи пулов ресурсов (Resource Pool).

Современная архитектура сети организаций предоставляет множество сервисов и масштабируема до сотен узлов и тысяч пользователей. Администраторам необходимо сегментировать сеть из соображений безопасности и управления трафиком, что не всегда может быть достижимо традиционными решениями. ESX позволяет производить настройку виртуального коммутатора и управлять логическими ресурсами сети, вместо физических. Используя виртуализацию, появляются дополнительные возможности по сегментированию сети относительно нужд пользователей и групп, с применениями отдельных регламентов и политик безопасности.

Для тестовых целей, при построении системы виртуализации отдельных сервисов ЦОД были использованы разные дисковые накопители – от внутренних SATA дисков, до систем хранения данных, работающих по интерфейсам SAS, iSCSI и Fibre Channel. При модернизации ЦОД рационально использовать уже имеющиеся дисковые массивы. Таковым является HP EVA 8000.

Совместное использование HP EVA 8000 и VMware позволяет добиться гибкости подключения серверов по интерфейсам SAS, iSCSI и Fibre Channel, а также их сочетаниям; доступ к высокопроизводительному хранилищу (работающее на блоковом уровне), масштабируемому с файловой системой VMware для поддержки запросов от виртуальных машин и многочисленных приложений; получить сбалансированную производительность как для транзакционных, так и для последовательных приложений, включая Exchange, SQLServer, Oracle, Sharepoint, бэкап- и файл-серверы.

Таким образом, использование виртуализации на базе технологии VMware и кластеризации данных на дисковых массивах HP EVA 8000, обеспечивает существенную экономию на аппаратном обеспечении, обслуживании, повышается гибкость инфраструктуры, упрощает процедуру резервного копирования и восстановления после сбоев.

Заключение. Модернизация построения сети сбора и обработки данных ЦОД предприятия связи заключается в том, что она позволяет оптимизировать ресурсы сети, реализовать её масштабируемость, добиться эффективного управления нагрузкой и защитой

информации на сети. Использование системы виртуализации позволяет существенно сократить временные издержки на развёртывание новых серверов, упростить процесс миграции и резервного копирования данных.

Список литературы

1. Data Age 2025: The Evolution of Data to Life-Critical [Электронный ресурс]. – Режим доступа : https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/workforce/ey-seagate-wp-data-age-2025-march-2017.pdf. – Дата доступа : 12.02.2024.

2. Воронцов Ю.А. Технико-экономическое обоснование эффективности проектов информационных систем. —М.: Инсвязьиздат, 2008. —367 с.

UDC 004.658:656.82-048.35

MODERNIZATION OF THE COMMUNICATIONS COMPANY'S DATA COLLECTION AND TRANSMISSION NETWORK

Nozhnikov E.A., gr.367041; Nozhnikov R.A., gr.367041

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Khatskevich O.A. – PhD in technical sciences, associate professor

Annotation. The materials of the report consider ways to improve the efficiency of communication data centers based on modern technologies. The development of a network resource virtualization and dynamic load balancing system will optimize network resources and implement effective load management and information protection on the network.

Keywords: modernization, information collection and processing center, virtualization

UDC 621.391

COMPARISON OF YOLOV12 AND YOLOV11 IN SAR IMAGE SHIP DETECTION

WANG W.Q., ZHANG X. (group 263111)

Belarusian State University of Informatics and Radioelectronics, Republic of Belarus

MA J. – Assistant in Department of Infocommunication Technologies.

Annotation: This study evaluates the performance of YOLOv12 in SAR image target detection compared to YOLOv11. Experimental results demonstrate that YOLOv12 outperforms YOLOv11 in detection accuracy (mAP50 and mAP50-95), small target detection, and complex background processing, exhibiting faster training convergence and stronger generalization ability. The study validates the advantages of YOLOv12 in SAR image target detection.

Keywords: SAR image; target detection, YOLOv12, performance comparison.

Introduction. Synthetic Aperture Radar (SAR) images play a crucial role in target detection tasks due to their all-weather and all-day imaging capabilities. However, SAR image characteristics such as speckle noise, complex textures, and small target distribution pose challenges to detection models. As the latest version of the YOLO series, YOLOv12 introduces the Area Attention module and Residual Efficient Layer Aggregation Network (R-ELAN), further enhancing global modeling capability and feature aggregation efficiency. This study aims to evaluate YOLOv12's performance in SAR image target detection and compare it with YOLOv11 [1]. The key improvements in YOLOv12 over YOLOv11 include the introduction of Area Attention module for enhanced global dependency capture in complex scenes, implementation of R-ELAN for optimized multi-scale feature fusion, enhanced Anchor-Free mechanism for simplified target box generation, and improved small target detection capabilities.

Experimental Methods and Results. The evaluation of model performance was conducted using several key metrics, including mAP50 (mean Average Precision at IoU threshold 0.5), mAP50-95 (mean Average Precision across IoU thresholds from 0.5 to 0.95), and various training losses including box regression loss, classification loss, and distribution focal loss. The experimental results revealed significant performance improvements in YOLOv12 compared to YOLOv11. Training metrics showed that YOLOv12 achieved lower box loss values, indicating more accurate target localization and faster convergence during training [2]. The classification loss was also notably reduced, demonstrating improved accuracy in target classification. Validation results further confirmed YOLOv12's superior performance, with lower validation box loss indicating stronger generalization ability in Figure 1.

Performance comparison between the two models showed that YOLOv12 consistently outperformed YOLOv11 across all evaluation metrics. The improved mAP50 and mAP50-95 scores demonstrated enhanced detection accuracy, particularly under strict IoU thresholds. YOLOv12 exhibited superior capabilities in handling complex backgrounds and detecting small targets, which are crucial challenges in SAR image processing [3]. The model showed faster convergence during training and demonstrated more robust performance across various testing scenarios.

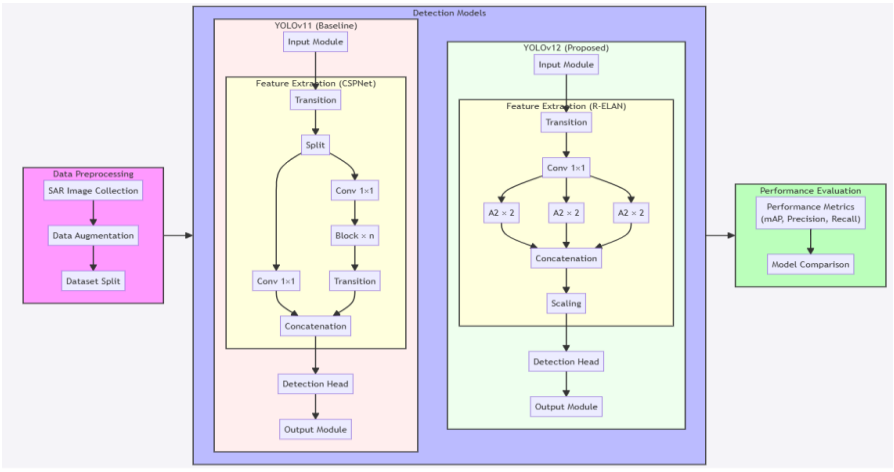


Figure 1 – Comparison Workflow Diagram of YOLOv11 and YOLOv12 for SAR Image Target Detection

YOLOv12 outperforms YOLOv11 across all evaluation metrics. During both training and validation phases, YOLOv12 demonstrates significantly lower loss values (Box Loss, Cls Loss, and DFL Loss), indicating faster convergence and stronger generalization capability. Additionally, YOLOv12 achieves substantial improvements in precision, recall, as well as core metrics such as

mAP50 and mAP50-95, which comprehensively validates its enhanced detection performance in Table 1.

Table 1. Comparison of YOLOv11 and YOLOv12 Performance Metrics

Metric	YOLOv11	YOLOv12	Improvement
Train Box Loss	Higher	Lower	Faster convergence, more accurate localization
Train Cls Loss	Higher	Lower	More accurate classification
Train DFL Loss	Higher	Lower	Better distribution predictions
Val Box Loss	Higher	Lower	Stronger generalization ability
Val Cls Loss	Higher	Lower	More stable classification performance
Val DFL Loss	Higher	Lower	Stronger generalization ability
Precision	Lower	Higher	Lower false positive rate
Recall	Lower	Higher	Lower false negative rate
mAP50	Lower	Higher	Higher detection accuracy
mAP50-95	Lower	Higher	Better performance under strict IoU

Conclusion. Through comprehensive experimental validation, YOLOv12 has demonstrated significant advantages in SAR image target detection tasks. Compared to YOLOv11, it shows notable improvements in detection accuracy and robustness, particularly excelling in small target detection and complex background processing. Although its inference speed is slightly lower than YOLOv11, it still meets real-time detection requirements. The research findings provide important references for the development of SAR image target detection technology, suggesting that YOLOv12's architectural improvements effectively address the unique challenges posed by SAR image processing. Future research can further explore the application of YOLOv12 in more SAR image tasks (such as semantic segmentation and change detection) and combine multimodal data (such as optical images and SAR images) to further improve the detection performance.

List of references:

[1]. YOLO: You Only Look Once / J. Redmon., A. Farhadi. // ARXiv preprint arXiv:1506.02640. 2016.

[2.] Efficient Real-Time Object Detection with Attention Mechanisms / Z. Ge., S. Liu., F. Wang., et al. // arXiv preprint arXiv:2308.12345. 2023.

[3]. SAR Image Target Detection Using Deep Learning Methods / Z. Zhang., H. Sun. // IEEE Transactions on Geoscience and Remote Sensing. 2021.

UDC 004.931

A REVIEW OF YOLOV11 BASED ON SAR SHIP DETECTION

ZHAO S.Y., ZHANG C. (Group 263111)

Belarusian State University of Informatics and Radioelectronics, Republic of Belarus

MA J. – Assistant in Department of Infocommunication Technologies.

Annotation. Synthetic Aperture Radar (SAR) imaging technology holds significant value in military reconnaissance and maritime monitoring due to its all-weather and all-time imaging capabilities. Ship detection, as a core task of maritime monitoring, plays a crucial role in ensuring maritime safety, combating illegal fishing, protecting the marine environment, and military target reconnaissance. However, SAR images inherently suffer from noise, difficulties in detecting small targets, and interference from complex sea conditions, which pose challenges to the design of ship detection algorithms. In recent years, the YOLO series of algorithms has continuously evolved in SAR ship detection, with the latest version, YOLOv11, significantly improving detection accuracy and efficiency through innovations such as lightweight design, multi-scale feature modeling,

and improved attention mechanisms. This paper analyzes the key technological features of YOLOv11 and its performance advantages in SAR ship detection while exploring its application prospects in complex scenarios and future optimization directions.

Keywords: SAR ship detection, YOLOv11, object detection algorithm**.**

Introduction. With the growing global demand for ocean resource development, maritime traffic management, and military reconnaissance, ship detection has become increasingly important. SAR, with its active microwave imaging technology, overcomes the limitations of traditional optical sensors affected by weather and lighting conditions, making it an essential tool for maritime monitoring. However, the inherent speckle noise, low resolution, and target occlusion in SAR images under complex sea conditions increase the difficulty of detection. Therefore, leveraging advanced algorithms to improve the accuracy and efficiency of SAR ship detection has become a key research focus. As the latest version of the YOLO series, YOLOv11 achieves breakthroughs in both accuracy and efficiency through a series of technical improvements, demonstrating stronger adaptability in complex scenarios.

Main Content. YOLOv11 excels in object detection tasks, with its technical enhancements primarily reflected in three aspects. First, the C3k2 module adopts a lightweight design to replace the traditional C2f module, reducing the number of parameters while maintaining multi-scale feature fusion capabilities. Second, the Fast Spatial Pyramid Pooling (SPPF) enhances the model's robustness to various target sizes through multi-scale pooling. Lastly, the Parallel Spatial Attention Convolution Block (C2PSA) combines self-attention mechanisms with parallel processing paths to strengthen global feature modeling. These improvements enable YOLOv11 to perform exceptionally well in tasks such as instance segmentation, pose estimation, and oriented object detection, particularly in complex scenarios like ship detection.

YOLOv11 performs excellently in SAR ship detection, mainly due to its multiple technical improvements. First, it can simultaneously capture global features of large targets and detailed information of small targets through a multi-scale feature pyramid and a dynamic anchor point allocation mechanism, effectively addressing the issue of significant size differences in ships 0. Second, in response to the complex sea waves and clutter backgrounds in SAR images, YOLOv11 introduces an improved attention mechanism and context information modeling, significantly enhancing its ability to suppress background noise and reducing both false detection and missed detection rates 0. Additionally, YOLOv11 adopts a lightweight design, with only 2.4M parameters, fast inference speed, and high computational efficiency, meeting real-time requirements **Error! Reference source not found.**. This makes it highly applicable and reliable in practical applications such as maritime safety monitoring. Overall, YOLOv11 provides strong technical support for SAR ship detection with high precision, adaptability, and efficient performance.

Performance Comparison and Experimental Analysis. In the SAR-Ship-Dataset, the performance comparison between YOLOv11 and YOLOv10 is shown in Table .

Table 2.YOLO Model Performance Evaluation Table

Model	P	R	mAP50	mAP50-95
YOLOv10	0.906	0.869	0.947	0.613
YOLOv11	0.927	0.898	0.967	0.613

YOLOv11 improved by 2.32%, 3.34%, and 2.11% in precision, recall, and mAP50, respectively, but showed no improvement in the overall metric mAP50-95. Additionally, the training and validation loss curves of YOLOv11 decline more quickly and smoothly, indicating faster convergence and stronger generalization ability.

Conclusion. YOLOv11 demonstrates outstanding technical advantages in SAR ship detection tasks. Experimental results indicate that it significantly outperforms YOLOv10 in key metrics such as precision, recall, and mAP50, while also achieving faster convergence and stronger adaptability. However, its performance on

the comprehensive metric mAP50-95 still requires improvement. Future research should focus on further optimizing the algorithm's adaptability to complex physical environments and enhancing the physical characteristic modeling of SAR images to improve detection robustness and overall performance.

List of references:

1. Detection Method of Key Ship Parts Based on YOLOv11. / Wang, Y., Jiang, Y., Xu, H., Xiao, C., Zhao, K. // Processes. 2025.

2. SAR Small Ship Detection Based on Enhanced YOLO Network. / Guan, T., Chang, S., Wang, C., Jia, X. // Remote Sensing. 2025.

3. LW-YOLO11: A Lightweight Arbitrary-Oriented Ship Detection Method Based on Improved YOLO11. / Huang, J., Wang, K., Hou, Y., Wang, J. // Sensors.

УДК 004.75

ВЛИЯНИЕ АЛГОРИТМОВ СЖАТИЯ ДАННЫХ НА ПРОИЗВОДИТЕЛЬНОСТЬ ВЕБ-ПРИЛОЖЕНИЙ

Анциферова Е.И.

гр.467041

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Научный руководитель: Шевчук О.Г. – кандидат технических наук, доцент кафедры ИКТ

Аннотация. В материалах доклада рассматривается влияние алгоритмов сжатия данных на производительность веб-приложений. Происходит сравнение основных методов сжатия, таких как Gzip, Brotli и Zstandard их эффективность в снижении объема передаваемых данных и влияние на скорость загрузки страниц. Рассматриваются экспериментальные результаты и рекомендации по выбору оптимального алгоритма в зависимости от особенностей веб-приложения.

Ключевые слова: сжатие данных, производительность, Gzip, Brotli, Zstandard, скорость загрузки, lossless алгоритмы, lossy алгоритмы

Введение. В настоящее время улучшение клиентского опыта имеет первостепенное значение для повышения вовлеченности и достижения успеха в бизнесе. Одним из важнейших аспектов, который существенно влияет на удовлетворенность клиентов, является скорость загрузки веб-сайта [1].

В условиях растущей конкуренции и стремления к удержанию пользователей, улучшение клиентского опыта становится одной из ключевых задач бизнеса. Пользователи ожидают мгновенного отклика и плавной работы веб-сайтов. Несомненно, скорость загрузки контента играет решающую роль в восприятии веб-ресурса и влияет на его успех.

Веб-приложения передают огромное количество данных, включая текстовые файлы, изображения, видео и другие ресурсы. Высокая нагрузка на сеть может замедлить загрузку страниц, особенно на устройствах с низкой пропускной способностью соединения. Для преодоления этих ограничений разработчики все чаще прибегают к использованию алгоритмов сжатия данных.

Использование алгоритмов сжатия позволяет уменьшить объем передаваемых файлов, что сокращает время загрузки страниц и снижает потребление сетевого трафика. Это особенно важно при

передаче текстовых данных, таких как HTML, CSS, JavaScript и JSON.

Сжатие данных позволяет существенно сократить объем передаваемых файлов, что приводит к уменьшению времени загрузки, оптимизации потребления сетевого трафика и повышению общей производительности приложения. Эта технология особенно актуальна для мобильных подключений, где скорость интернета может быть ограничена.

На сегодняшний день наиболее популярными алгоритмами сжатия для веб-приложений являются Gzip, Brotli и Zstandard. Каждый из них имеет свои особенности, такие как уровень сжатия, скорость декомпрессии и нагрузка на вычислительные ресурсы. Выбор подходящего алгоритма зависит от множества факторов, включая характеристики сервера, требования к скорости обработки данных и поддержку браузерами.

Правильный выбор алгоритма сжатия зависит от многих факторов, включая характеристики оборудования сервера, требования к скорости обработки данных и поддержку алгоритмов браузерами. Кроме того, важным аспектом является нахождение баланса между степенью компрессии и возможной нагрузкой на серверное и клиентское оборудование.

Основная часть. Сжатие данных представляет собой процесс уменьшения их объема без потери информации с целью оптимизации передачи и хранения. В контексте веб-приложений это позволяет снизить нагрузку на сеть, уменьшить время загрузки страниц и, как следствие, повысить удобство взаимодействия пользователя с системой.

Существуют два типа сжатия: без потерь (lossless), с потерями (lossy).

Lossless алгоритмы сокращают размер данных без изменения их структуры (Gzip, Brotli, Zstandard). Lossy алгоритмы используют частичное удаление информации для значительного снижения объема (JPEG, WebP, MP3).

Рассмотрим алгоритм сжатия веб-контента Gzip. Он является одним из самых популярных и давно используемых алгоритмов сжатия в веб-разработке. Он был разработан в 1990-х годах и с тех пор зарекомендовал себя как надежный и эффективный инструмент для уменьшения объема текстовых данных в интернет-приложениях.

Gzip обеспечивает значительное сокращение объема данных, особенно для текстовых файлов, таких как HTML, где происходит уменьшение избыточности за счет удаления повторяющихся символов и структур; CSS, где сжатию поддаются стили, содержащие часто повторяющиеся ключи и значения; JavaScript, где упаковываются длинные цепочки символов, комментарии и пробелы. В результате, использование Gzip может сократить размер файлов на 60–80% в зависимости от структуры данных.

Рассмотрим разработанный Google алгоритм Brotli. Его преимуществами является поддержка большинством современных браузеров, оптимизация для веб-ресурсов, улучшенное сжатие по сравнению с Gzip, особенно для текстовых файлов.

Одной из ключевых особенностей Brotli является его способность использовать кодирование Huffman — метод, который основывается на вероятностном анализе. Часто встречающиеся символы и фразы получают короткие коды, а редкие — более длинные, что позволяет минимизировать общий объем данных.

Также Brotli использует заранее заданный словарь, содержащий часто встречающиеся фразы и выражения, которые особенно актуальны для веб-контента. Например, фразы из HTML-разметки или JavaScript-кода могут быть упакованы в более компактный формат. Эта особенность позволяет алгоритму работать быстрее и эффективнее, чем Gzip, особенно с текстовыми файлами.

Zstandard — сравнительно новый алгоритм, разработанный Facebook. Он ориентирован на быструю компрессию и декомпрессию, что делает его удобным для серверных приложений.

Этот алгоритм сочетает гибкость и высокую производительность, что делает его универсальным инструментом для различных сценариев. Одной из ключевых особенностей алгоритма является возможность регулировать уровни компрессии в диапазоне от 1 до 22, позволяя разработчикам

адаптировать процесс под задачи. Низкие уровни обеспечивают максимальную скорость обработки данных, что важно для приложений, работающих в реальном времени.

Высокие уровни компрессии позволяют достичь значительного уменьшения объема файлов, что особенно полезно при передаче больших объемов данных. Благодаря высокой скорости компрессии и декомпрессии, Zstandard демонстрирует одну из лучших производительностей среди современных алгоритмов, успешно справляясь с обработкой информации в реальном времени.

Использование сжатия данных позволяет достичь значительного уменьшения объема передаваемой информации, что приводит к следующим улучшениям: сокращение времени загрузки — уменьшение размера файлов на 30–80% снижает задержки при передаче данных по сети; снижение нагрузки на сервер — передача сжатых данных уменьшает объем передаваемого трафика, снижая использование пропускной способности; оптимизация мобильных подключений — компрессия особенно важна для пользователей с медленными или нестабильными соединениями. Однако чрезмерное сжатие может привести к увеличению нагрузки на процессор сервера и клиента, что особенно критично для ресурсоемких приложений. Поэтому важно находить баланс между степенью сжатия и скоростью обработки данных.

Gzip обеспечивает средний уровень сжатия при высокой скорости компрессии и декомпрессии. Он широко поддерживается браузерами и серверами и подходит для динамических данных.

Brotli демонстрирует более высокий уровень сжатия, чем Gzip, особенно для текстовых данных. Он менее быстрый, но оптимален для статического контента, такого как CSS и JavaScript, и поддерживается современными браузерами.

Zstandard сочетает высокий уровень сжатия с самой высокой скоростью обработки данных. Он идеален для серверных приложений и обработки больших массивов данных, но имеет ограниченную поддержку браузерами.

При выборе алгоритма компрессии следует учитывать специфику веб-приложения и его пользователей. Для большинства случаев рекомендуется Brotli из-за его высокой эффективности при передаче статических файлов [2]. Gzip остается актуальным для обратной совместимости и быстрого сжатия в реальном времени. Zstandard подходит для серверных приложений и обработки больших объемов данных.

Для оценки влияния алгоритмов сжатия данных на производительность веб-приложений были проведены тестирования с различными типами контента и в разных сценариях. Основная цель экспериментов заключалась в определении эффективности алгоритмов Gzip, Brotli и Zstandard в снижении объема передаваемых данных, ускорении загрузки страниц и минимизации нагрузки на серверы.

Для исследования использовались различные типы контента, которые часто встречаются в веб-приложениях. Среди них текстовые файлы, такие как HTML, CSS, JavaScript, а также JSON и XML, которые широко применяются для структурированных данных. HTML позволяет уменьшить объем за счет оптимизации повторяющихся элементов структуры, CSS выигрывает благодаря сокращению ключей и значений, а в JavaScript эффективно сжимаются длинные цепочки, пробелы и комментарии.

Изображения в формате SVG, содержащие текстовые элементы и метаданные, также поддаются сжатию, тогда как форматы JPEG и PNG имеют встроенные методы компрессии, из-за чего дополнительные алгоритмы почти не улучшают их размер.

Веб-шрифты, такие как WOFF и TTF, успешно сжимаются при использовании Brotli, что особенно полезно для ускорения загрузки страниц. Видео и аудиофайлы, например, MP4, MP3 и WebM, уже используют сжатие с потерями, поэтому дополнительная компрессия для них не дала значительных результатов.

Также были протестированы API-ответы в форматах JSON и XML, которые играют важную роль в обмене данными между клиентами и серверами. Эти форматы продемонстрировали высокий уровень

уменьшения объема из-за предсказуемой структуры. Отдельное внимание было уделено текстовым лог-файлам серверов, так как они имеют значительные размеры, и Zstandard показал лучшие результаты по скорости сжатия и минимальным задержкам при их обработке.

Каждый тип контента дал различные результаты. Brotli оказался оптимальным для CSS и JavaScript благодаря высокой степени сжатия, Zstandard продемонстрировал исключительную производительность при работе с большими данными, такими как логи или API-ответы, а Gzip эффективно справился с динамическими текстовыми файлами, минимизируя нагрузку на процессор. Такой подход показал, что выбор алгоритма зависит от структуры и особенностей обрабатываемого контента.

По влиянию на скорость загрузки Brotli обеспечил сокращение времени загрузки статического контента, такого как CSS и JavaScript, на 25–35% по сравнению с Gzip. Благодаря этому он становится оптимальным выбором для заранее сжатых файлов. Zstandard продемонстрировал высокую производительность при компрессии динамических данных, минимизируя задержки в высоконагруженных серверных приложениях. Gzip сохранил свою эффективность для обработки мелких текстовых файлов, обеспечивая минимальную нагрузку на сервер.

По коэффициенту сжатия Gzip уменьшил размер текстовых данных на 60–70%, что обеспечивает значительное сокращение объема. Brotli превзошел Gzip, сократив размер на 70–80%, особенно для больших текстовых массивов. Zstandard достиг аналогичных результатов, сравнимых с Brotli, но обеспечил значительно более высокую скорость компрессии, что делает его предпочтительным для серверных задач.

Приведем сравнение алгоритмов сжатия по коэффициенту сжатия (рис. 1).

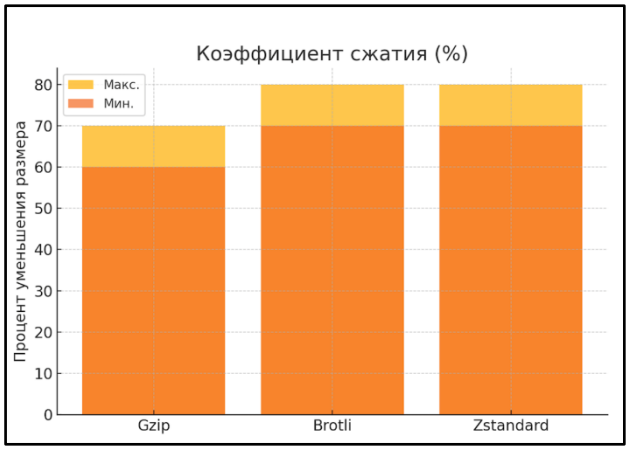


Рисунок 1 – Сравнение алгоритмов сжатия по коэффициенту сжатия

Еще одним важным показателем является скорость загрузки (рис.2).

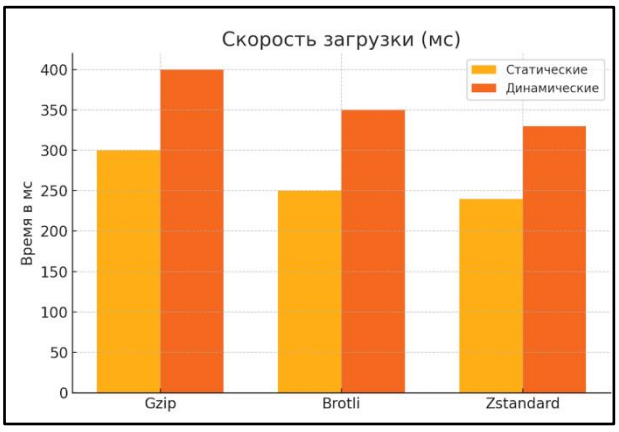


Рисунок 2 – Сравнение алгоритмов сжатия по скорости загрузки

Для того, чтобы сравнить скорость обработки при компрессии и декомпрессии обратимся к диаграмме

на рисунке 3.

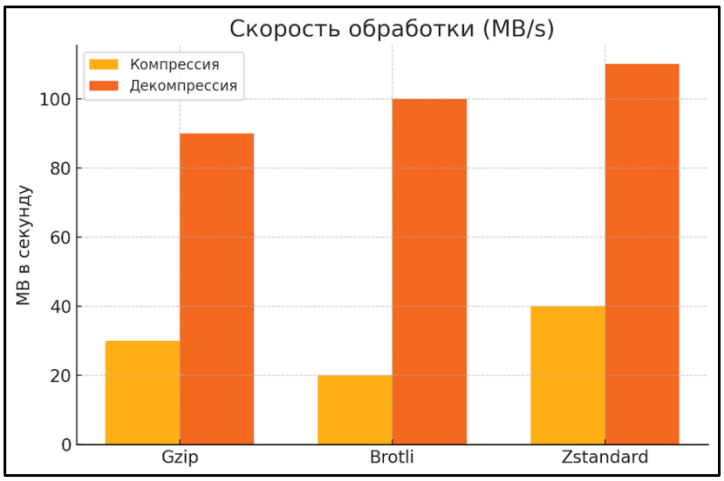


Рисунок 3 – Сравнение алгоритмов сжатия по скорости обработки при компрессии и декомпрессии

Заключение. Алгоритмы сжатия данных играют важную роль в оптимизации веб-приложений, позволяя уменьшить объем передаваемых файлов и улучшить производительность системы. Gzip, Brotli и Zstandard обладают разными характеристиками, и выбор метода сжатия должен учитывать баланс между степенью компрессии, скоростью обработки и нагрузкой на сервер. Грамотное применение компрессии способствует улучшению пользовательского опыта, снижению нагрузки на сеть и более эффективному использованию ресурсов.

Список литературы

1. *Brotli vs. GZIP: A Comprehensive Comparison of Compression Algorithms. / Abdul Rehman 2023. – 17 Min Read.*
2. *How Image Compression Affects Your Website's Loading Times – John Hughes 2023.*

UDC 004.75

THE IMPACT OF DATA COMPRESSION ALGORITHMS ON WEB APPLICATION PERFORMANCE

Antsiferova E.I.

gr.467041

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Shevchuk O.G. – Ph. D

Annotation. The report examines the impact of data compression algorithms on the performance of web applications. It compares key compression methods such as Gzip, Brotli, and Zstandard, analyzing their effectiveness in reducing the volume of transmitted data and their influence on page load speed. Experimental results and recommendations for selecting the optimal algorithm based on the characteristics of the web application are discussed.

Keywords: Data compression, performance, Gzip, Brotli, Zstandard, load speed, lossless algorithms, lossy algorithms

УДК 621.397.13:654.9-049.7

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫВИДЕОНАБЛЮДЕНИЯ И КОНТРОЛЯ

Воронович Д.Ю.

гр.467041

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Научный руководитель: Вишняков В.А. – доктор технических наук, профессор кафедры ИКТ

Аннотация. В статье рассматриваются современные системы видеонаблюдения, их преимущества и отличия от стандартных систем видеонаблюдения

Ключевые слова: интеллектуальные системы видеонаблюдения, видеоконтроль, видеоаналитика

Введение. Актуальность проекта определяется тем фактом, что на сегодняшний день традиционные камеры видеонаблюдения не удовлетворяют в полной мере потребностям в оперативном реагировании на внештатные ситуации на крупных производственных и иных объектах. Для решения современных задач требуются комплексные интеллектуальные системы, в основе которых лежат сложные алгоритмы видеоаналитики.

Интеллектуальные системы видеонаблюдения и контроля обладают рядом ключевых факторов, которые повышают безопасность и эффективность видеонаблюдения. Главным аспектом является повышение безопасности, что позволит предотвратить кражи и акты вандализма, а также снизить ошибки, связанные с человеческим фактором. Неотъемлемой частью системы является оптимизация операционных процессов, это позволит нам производить мониторинг за производством (например, остановка конвейера) для минимизации простоев. Система позволит анализировать перемещение сотрудников и транспорта, что позволит оптимизировать маршруты и распределение задач [1].

Непосредственным преимуществом также является интеграция с другими системами и экономическая выгода системы видеонаблюдения. Совмещение с системами контроля доступа, IoT-датчиками и пожарной сигнализацией позволит повысить безопасность на предприятии. Также имеется возможность мониторинга объектов из любой точки мира, что критично для сетевых предприятий.

Основная часть. Интеллектуальные системы видеонаблюдения — это аппаратно-программный комплекс, который используется для автоматизированного сбора информации с потокового видео. В своей работе эти системы опираются на различные алгоритмы распознания изображений, систематизации и обработки полученных данных. Оказываем полный комплекс услуг по созданию систем видеонаблюдения.

Интеллектуальное видеонаблюдение, как любая высокотехнологичная система, имеет свои плюсы и минусы. К главным преимуществам оборудования с аналитическими алгоритмами можно отнести:

– практически неограниченный функционал;

– высокую точность и надежность;

– широкий спектр реальных сценариев применения оборудования;

– дружественный интерфейс;

– широкий выбор аналитических алгоритмов;

– постоянная разработка новых программно-аппаратных комплексов.

Главный недостаток интеллектуального видеонаблюдения – высокая стоимость оборудования и программных модулей. Расходы на внедрение системы на крупном заводе или производственном объекте могут достигать очень больших сумм.

К менее значимым минусам можно отнести:

– высокую нагрузку на каналы связи из-за передачи большого объема данных;

– размещение в архиве «пустой, мусорной» информации;

– недостаточный уровень защищенности базы данных.

Перед внедрением интеллектуальной системы видеонаблюдения следует тщательно проанализировать целесообразность мероприятия. Если аналитические алгоритмы помогают повышать производительность труда, снижают вероятность человеческих ошибок, способствуют развитию бизнеса и повышению продаж, то расходы на покупку, установку и обслуживание оборудования быстро окупятся [3].

Системы видеонаблюдения, в которых реализованы интеллектуальные функции, позволяют более эффективно решать поставленные задачи. Исходя из многочисленных опытов, утомляемость, неспособность к длительной концентрации сказываются на человеке уже через полчаса работы с несколькими камерами, что приводит к резкому падению эффективности наблюдения. В то же время интеллектуальные системы видеонаблюдения дают стабильное и высокое качество, а решение таких задач, как распознавание большого количества людей, проходящих на предприятие в режиме реального времени, практически не представляется возможным для человека.

Большинство современных систем видеонаблюдения имеют простейшие средства анализа видеоизображения – например, детектор движения. Однако этого недостаточно для решения очень многих актуальных на сегодняшний день задач. Именно для их решения была разработана видеоаналитика.

Видеоаналитика — технология, использующая методы компьютерного анализа для автоматизированного получения данных на основании анализа последовательности изображений, поступающих с видеокамер в режиме реального времени или из архивных записей. Видеоаналитика представляет собой программное обеспечение для работы с видеоконтентом. В основе программного обеспечения лежит комплекс алгоритмов машинного зрения, позволяющих вести видеомониторинг и производить анализ данных без прямого участия человека.

Видеоаналитика имеет множество полезных функций: распознавание лиц бесцельного поведения, слежение за объектами и закрытыми зонами, детектирование проникновения, анализ видеонаблюдения ограниченной зоны и периметра, распознавание номеров автотранспорта. Основной комплекс услуг, предоставляемый системой видеоаналитики для охраны закрытых зон, следующий:

– Выявление и определение вероятностей возникновения предполагаемых угроз объекту в закрытой зоне.

– Определение зон объекта, подверженных уязвимостям.

– Обнаружение факта пересечения периметра закрытой зоны.

– Информирование соответствующих служб о наличии потенциальных угроз или фактов проникновения.

– Посылка извещений и изображений нештатного случая дежурному персоналу безопасности объекта, включая носимые устройства.

Результатами работы видеоаналитики являются события в виде сообщений, которые

должны быть переданы оператору системы видеонаблюдения или записаны в видеоархив для последующего использования [2].

Заключение. Интеллектуальные системы видеонаблюдения трансформируют пассивный сбор данных в инструмент активного управления, обеспечивая не только безопасность, но и рост эффективности предприятия. Система позволяет повысить эффективность работы оператора наблюдения, оптимизировать хранение и использование данных, сконцентрировать работу оператора на потенциальных угрозах и обеспечить безопасность сотрудников.

Список литературы

1. Пескин А.Е. Обслуживание и ремонт систем видеонаблюдения: учебное пособие. М.: Горячая линия-Телеком, 2013. 256 с.

2. Ярышев С.Н. Цифровые методы обработки видеоинформации видеоаналитика: учеб. пособие. СПб.: СПбГУ ИТМО, 2011. 83 с

3. ГОСТ Р 51558-2008. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний. М.: ФГУП СТАНДАРТИНФОРМ, 2009.

UDC 621.397.13:654.9-049.7

INTELLIGENT VIDEO SURVEILLANCE AND CONTROL SYSTEMS

Voronovich D.Y.

gr.467041

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Vishnyakov V.A.– Dr. of Sci. (Tech.), professor of the ICT department

Annotation. The article discusses modern video surveillance systems, their advantages and differences from standard video surveillance systems.

Keywords: intelligent video surveillance systems, video monitoring, video analytics

УДК 004.75:[61+004.42]

СИСТЕМЫ БЛОКЧЕЙН В IT-МЕДИЦИНЕ

Кацко М.О.

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Научный руководитель: Вишняков В.А. – доктор технических наук, профессор кафедры ИКТ

Аннотация. В материалах доклада рассматривается возможности и перспективы применения технологии блокчейн в IT-медицине. Рассмотрены математические модели и схемы передачи медицинских данных при использовании блокчейн. Обобщены проблемы и недостатки применения блокчейн-технологии в IT-медицине.

Ключевые слова: блокчейн, IT-медицина, электронных медицинские карты, потенциал применения блокчейн, конфиденциальность данных

Введение. Блокчейн – это распределенный реестр, который обеспечивает способ записи информации и совместного использования сообществом, в котором каждый участник ведет свою собственную копию информации, все участники должны проверять любые обновления коллективно. С помощью блокчейна криптология заменяет сторонних посредников в качестве хранителя доверия, при этом все участники блокчейна запускают сложные алгоритмы для подтверждения целостности информации.

Современная электронная медицина (e-health) сталкивается с проблемами безопасности данных, отсутствием доверия между участниками системы и сложностью обмена медицинской информацией. Блокчейн-технология, благодаря своей децентрализованной природе, криптографической защите и неизменяемости данных, предлагает решения этих проблем [1].

Цель данной статьи – дать краткое описание работы блокчейн, проанализировать текущее состояние и перспективы применения блокчейна в IT-медицине, а также обозначить проблемы внедрения технологии.

Основная часть. Блокчейн опирается на: хеш-функции (SHA-256, Keccak) – обеспечивают целостность данных; алгоритмы консенсуса (Proof of Work, Proof of Stake, PBFT) – гарантируют согласованность данных в сети. В медицинских блокчейн-системах применяются алгоритмы консенсуса: Proof of Authority (PoA) – для быстрой валидации транзакций (подходит для EHR – Electronic Health Records); Delegated Proof of Stake (DPoS) – баланс между скоростью и децентрализацией [9]. Блокчейн позволяет хранить хэши записей в цепочке, а сами данные – в IPFS (InterPlanetary File System); контролировать доступ через смарт-контракты.

Данные и трафик в блокчейне шифруются с использованием протоколов высочайших стандартов безопасности (ECC, AEC). API играют важную роль в конфиденциальности и безопасности данных здравоохранения, обеспечивая безопасную передачу информации о пациентах между системами [2].

В сфере здравоохранения используется большое число умных медицинских устройств, которые постоянно собирают и отслеживают различную информацию. Блокчейн обеспечивает постоянный контроль за такими устройствами, который сводит к минимуму какие-либо несанкционированные манипуляции с ними [3].

Для кодировки и защиты данных медицинского характера при организации медицинского обслуживания на базе блокчейн-платформы в наибольшей степени подходит технология умных контрактов (смарт-контракты). Эффективность данной технологии с точки зрения обеспечения защиты данных пациента заключается в том, что доступ к ним обеспечивается только после его согласия. Технология умных контрактов обеспечивает достоверность и защиту передаваемых данных, а также разделяет информационные потоки на общедоступные (в обезличенной форме) и требующие разрешения на их передачу третьим лицам (персонализированные) [4].

Преимущества использования блокчейн в здравоохранении [1]:

1. Децентрализация – отсутствие центрального узла, хранящего и управляющей информацией (у всех участников равные права, поэтому совершение операций проводится между ними напрямую);

2. Конфиденциальность данных – блокчейн неизменяемая структура, обязательно применяются криптографические алгоритмы шифрования, хеширования и аутификации;

3. Ограничение доступа – только владелиц информации может управлять доступом к свои данным;

4. Надежность – записи блоки блокчейна хранятся на всех узлах сети, что минимизирует их утрату;

5. Проверка данных – без доступа к информации, хранящейся внутри блока, можно проверить ее целостность и неизменность.

Обобщенную модель управления медицинскими данными можно представить в виде [1]:

$$M_{mic} = \{M_{cehr}, M_{cct}, M_{dma}, M_{cbi}, M_{rpm}\},$$

где M_{cehr} – управление электронными медицинскими картами; M_{cct} – управление цепочками поставок лекарств и борьба с контрафактом; M_{dma} – анализ медицинских данных; M_{cbi} – проведение клинических и биомедицинских исследований; M_{rpm} – удаленный мониторинг пациентов.

В таблице 1 приведены самые актуальные направления для интеграции блокчейн-технологии в сфере IT-медицине на сегодняшний день [1,3 – 4].

Таблица 1 – Направление применения блокчейн в ИТ-медицине

№	Направление	Проблема	Оптимизация	Примеры
1	Управление электронными медицинскими картами (ЭМК)	Целостность данных, контроль доступа	Обеспечивает безопасное хранение и передачу данных между субъектами	MedRec, платформа Panacea, Платформа Akiri
2	Контроль цепочки поставок лекарств	Контроль подлинности товаров	Прозрачное документирование, отслеживание товара	ADLTTM, TraceRX, Компания MediLedger
3	Телемедицина	Целостность и конфиденциальность данных	Защищает данные пациентов при удаленных консультациях	Solve.Care MyClinic
4	Исследования и клинические испытания	Целостность и конфиденциальность данных	Гарантирует достоверность данных, сбор данных с медицинских устройств, автоматизация процессов	Платформа CTRR, компания Chronicled
5	Подтверждение квалификации медицинского персонала	Фальсификация документов	Гарантирует достоверность документов	Протокол блокчейна R3 Corda
6	Регулирование страховых споров	Большие временные затраты, фальсификация документов	Повышение прозрачности, снижению случаев мошенничества, автоматизация обработки обращений	Компания MetLife

Пользователи занимают различные позиции в системе и могут просматривать только те записи, к которым они получили доступ. Пациенты могут добавлять записи с помощью клиентской программы, которая вызывает код цепочки для фиксации транзакции в сети. После фиксации транзакции в сети блокчейна обновленные транзакции распространяются по сети и гарантируют, что каждая транзакция по сети распространяется среди всех участников системы. Ни одна транзакция не может быть изменена или удалена неавторизованными пользователями. Транзакции применяются только к предыдущему хэшу с временной меткой, поэтому сеть полностью безопасна. Записи изменяются и доступны любому пользователю блокчейн-сети. Поставщики услуг, включая медиков и сотрудников лабораторий, могут запрашивать необходимые данные через сеть.

На примере использования электронных медицинских карт можно рассмотреть схему передачи медицинских данных. Первоначально данные генерируются из носимого или медицинского устройства пациента, передаются в блокчейн через API и в конечном итоге в EHR очень прозрачным способом. Таким же образом данные будут возвращены пациенту или медицинскому работнику. Любые действия с данными должны быть согласованы с другие заинтересованные стороны.

На рисунке 1 показан поток данных от их источника (пациента) до электронной медицинской карты (EHR) [5].

Рисунок 1 – Схема передачи медицинских данных

Схема состоит из 6 компонентов:

1 Сбор данных пациента. Этот компонент отвечает за сбор данных от пациента из различных источников, включая медицинские приборы, носимые устройства и поставщиков медицинских услуг и т. д.

2 Шифрование и хранение данных. Этот компонент получает, записывает и хранит зашифрованные медицинские данные пациента в блокчейн-сети.

3 Предоставления медицинских услуг. Этот компонент предоставляет медицинские услуги поставщикам медицинских услуг, пациентам и другим на основе данных о здоровье пациента хранящихся в блокчейне. Эти услуги могут включают телемедицину, удаленный мониторинг и т. д.

4 Приложений для здравоохранения. Этот компонент, которые позволяют медицинским работникам поставщикам медицинских услуг получить доступ к медицинским данным пациентов, хранящимися в блокчейне. Эти приложения выступают в виде мобильных приложений, веб-порталов и электронных медицинских карт (EHR).

5 Управление и регулирование. Данный компонент обеспечивает надзор и управление системы, обеспечивая доступ к медицинским данным с соблюдением нормативных требований, конфиденциальности и стандартов безопасности.

6 Получение вознаграждений. Этот компонент стимулирует заинтересованные стороны, поощряя обмен медицинскими данными и использование предоставляемых услуг. Эти стимулы могут быть в виде собственной криптовалюты либо в виде скидок.

Такая схема призвана обеспечить безопасную и прозрачную платформу для сбора, хранения и обмена медицинскими данными пациентов, а также предоставить поставщикам медицинских услуг и пациентам возможность доступа к этим данным и их использования для улучшения результатов медицинского обслуживания.

Несмотря на существующие препятствия, блокчейн открывает значительные перспективы для оптимизации процессов в сфере наук о жизни. Ключевым вызовом на пути к широкому внедрению является необходимость трансформации взглядов руководителей в частном и государственном секторах, а также политиков, наряду с адаптацией управленческих подходов. По мере развития технологии и появления успешных кейсов, демонстрирующих снижение рисков, ожидается увеличение темпов ее освоения в ближайшие пять лет. Это, в свою очередь, позволит блокчейну в полной мере реализовать свой потенциал в рамках экосистемы наук о жизни [6].

Барьерами для широкого применения блокчейна в здравоохранении являются также проблемы масштабируемости, задержки передачи данных, взаимодействия между различными системами, безопасности данных и конфиденциальности. Эти препятствия требуют комплексного решения для успешного внедрения блокчейн-технологий в здравоохранении. В качестве первостепенного решения могут выступить вопросы правового регулирования.

В России уже несколько лет используются медицинские электронные карты пациентов, активно развивается сегмент телемедицины. При этом на государственном уровне технология блокчейн не используется, но рассматривается как один из возможных вариантов [7].

Заключение. Блокчейн обладает значительным потенциалом для трансформации электронной медицины, обеспечивая безопасность, прозрачность и автоматизацию. Но остаются вызовы, связанные с масштабируемостью и регуляцией. Дальнейшие исследования должны быть направлены на оптимизацию алгоритмов и интеграцию с существующими медицинскими системами. Приведены математические модели и схема передачи медицинских данных.

Список использованных источников:

1. Вишняков В. А. Технология блокчейн в образовании и ИТ-медицине: модели, алгоритмы, программные средства : [монография] / В. А. Вишняков, Д. А. Качан. – Минск : РИВШ, 2023. – 184 с.

2. Blockchain for Healthcare: How to Enhance Data Privacy and Security in Patient Information Transfers [Электронный ресурс]. – Режим доступа: https://mpost.io/blockchain-for-healthcare-how-to-enhance-data-privacy-and-security-in-patient-information-transfers/. Дата доступа: 01.04.2025

3. Вишняков В.А. Использование технологии блокчейн в ИТ-медицине // Вишняков В.А. / Системный анализ и прикладная информатика. 2024, № 3. – С. 48-53.

4. Борисов, И. В. Блокчейн-платформа как инструмент цифровизации процессов управленческой деятельности в здравоохранении / И. В. Борисов // Вестник евразийской науки. – 2023, Т.15, № 1.

5. Mehak Maqbool Memon , Manzoor Ahmed Hashmani, Filmann Taput Simpao, Anthony Cinco Sales, Neil Quinones Santillan, Dodo Khan. Blockchain in Healthcare: A Comprehensive Survey of Implementations and a Secure Model Proposal //Proceedings of the Pakistan Academy of Sciences: A // Pakistan Academy of Sciences Physical and Computational Sciences 60(3). 2023. – С. 1-13.

6. Райт Ч., Джоши Р. Блокчейн в здравоохранении и науки о жизни // PreScouter, 2020.

7. Берсенева Е.А., Умнов С.В., Умнов М.С., Агамов З.Х. Технология блокчейн как компонент цифровизации здравоохранения // Профилактическая медицина. 2023;26(4):95-99.

UDC 004.75:[61+004.42]

BLOCKCHAIN SYSTEMS IN IT-MEDICINE

Katsko M.A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Scientific supervisor: Vishnyakov V.A. – Doctor of Technical Sciences, professor at the department of ICT

Annotation. The report considers the possibilities and prospects of blockchain technology application for IT-medicine. Mathematical models and schemes of medical data transmission when using blockchain are considered. Problems and disadvantages of blockchain technology application in IT-medicine are summarized.

Keywords: blockchain, IT-medicine, electronic health records, potential applications of blockchain, data privacy.

УДК 004.75

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ГЕТЕРОГЕННОГО РАДИОПОКРЫТИЯ

Родионов М.А.

гр.467041

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Научный руководитель:Астровский И.И. – кандидат технических наук, доцент кафедры ИКТ

Аннотация. В статье рассматриваются вопросы организации совместного радиопокрытия гетерогенных радиосетей, когда на территории относительно большой городской соты культивируются малые пикосоты outdoor типа. С помощью компьютерного моделирования получены зависимости размеров малых сот от ряда параметров. Полученные результаты позволяют дать рекомендации по оптимизации гетерогенных сетевых решений.

Ключевые слова: гетерогенные сети, микросоты, пикосоты, гарантированное подключение, модели распространения волн, компьютерное моделирование, Matlab

Введение. Под гетерогенной сотовой сетью – HetNet – обычно понимают такой вариант радиопокрытия, когда на территории относительно большой городской микросоты (радиус от нескольких сотен метров до 1 км) организуются маленькие пикосоты (радиус от нескольких десятков метров до 150 метров) для обслуживания большого трафика в определённых локальных «горячих точках», или hot-spots (см. рисунок 1). По этой причине синонимом понятия HetNet часто является термин Small Cells – маленькие соты. При этом речь идёт как о пикосотах outdoor на улицах, так и о пикосотах indoor внутри помещений [1]. Кроме пико-BS локальное радиопокрытие могут создавать выносные радиомодули RRU, играющие роль репитеров сигналов центральной микро-BS. Такой сценарий характерен для покрытия «тёмных точек» – dark-spots.

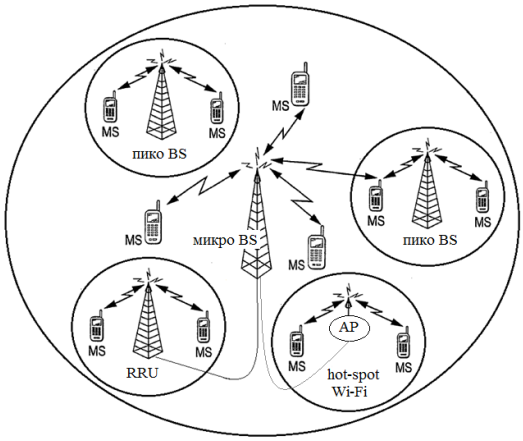


Рисунок 1 – Схема гетерогенной сети

(RRU – Remote Radio Unit, выносной приёмопередатчик; AP – Access Point, точка доступа Wi-Fi) [2]

Во всех перечисленных случаях возникает ситуация, когда мобильные станции MS оказываются под воздействием сигналов от центральной микробазы и ближайшей пикобазы. Мобильная станция обычно выбирает для дальнейшей работы ту базовую станцию, от которой она принимает более мощный специальный сигнал для выполнения процедуры Cell Select. Поэтому от характера распределения и взаимного соотношения уровней этих сигналов будет сильно зависеть, какие абоненты будут обслуживаться в пикосоте, а какие останутся в микросоте [3].

Основная часть. Для оценки размера формируемой пикосоты внутри микросоты была написана программа моделирования в среде MATLAB, результаты работы которой показаны на рисунке 2. Моделировалась ситуация, когда внутри городской относительно низкочастотной микросоты размещается высокочастотная пикосота типа PoleStation диапазона FR2. Программа вычисляла изменение уровня сигнала при удалении от микробазовой станции на основе модели COST 231-Hata [4] для частоты 1800 МГц, высоты установки антенны этой базы в 30 м и излучаемой мощности 46 дБм (40 Вт). Моделирование распределения уровня сигнала пикобазы выполнялось симметрично от точки установки этой пикобазы D на основе модели из [5] для сценария UMI-Street Canyon-LOS для частоты 27500 МГц, мощности 23 дБм (на рисунке 2) и высоты установки антенны 10 м. Следует особо отметить, что входящие в модели из [4, 5] логарифмы имеют точки разрыва при нулевом расстоянии. По этой причине пиковые мощности 46 дБм и 23 дБм для базовых станций на графиках рисунка 2 не отображаются.

Продольный размер пикосоты измерялся по координатам X1 и X2 точек пересечения графиков распределения сигналов от двух базовых станций. Далее отдельно вычислялся размер dX1 от точки D до координаты X1. Аналогично вычислялся размер dX2 и сумма R=dX1+dX2, имеющая смысл продольной длинны пикосоты.

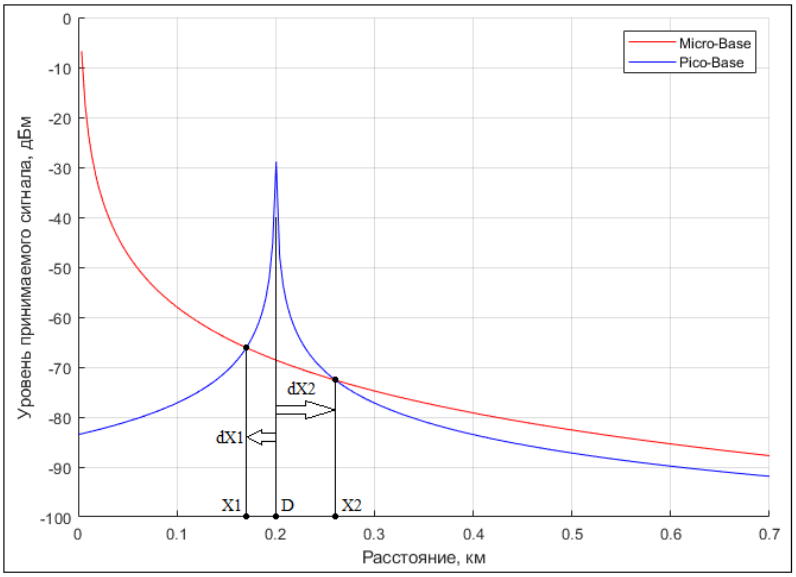


Рисунок 2 – Распределение уровней принимаемого сигнала от микробазы и пикобазы.

По результатам моделирования на рисунках 3 и 4 показан характер изменения размеров пикосоты R, dX1 и dX2 при изменении, соответственно, места установки пикобазы D (при её мощности 23 дБм) и изменении мощности пикобазы (D=250 м).

При росте излучаемой пикобазой мощности, так и её передвижении на границу микросоты, где ниже уровень сигнала микробазы, наблюдается рост линейного размера пикосоты. Причём изменение размера dX1 не очень значительное, а рост R достигается исключительно увеличением размера dX2.

Другими словами, происходит смещение вправо точки X2 на графике рисунка 2. Можно предположить, что при этом происходит изменение формы пятна пикосоты, как это показано на рисунке 5. В случае превышения сигнала пикобазы над сигналом микробазы в ограниченной области, эта область имеет некоторую овальную форму, соответствующую кривой 1. По мере роста уровня сигнала пикобазы, правая граница пикосоты смещается вправо, а сама пикосота, очевидно, увеличивается в размерах, как кривые 2 и 3. При некотором уровне сигнал пикобазы будет превышать сигнал микробазы всегда, т.е. до границы микросоты. Эту ситуацию иллюстрирует кривая 4.

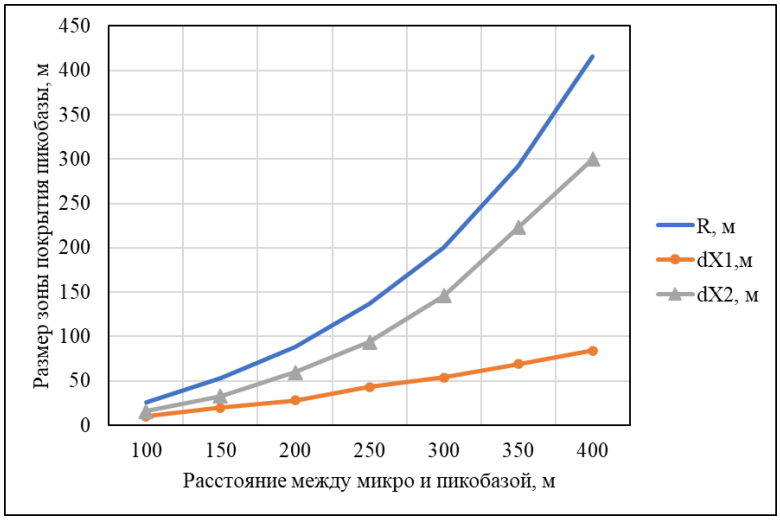


Рисунок 3 – Изменение продольного размера пикосоты при изменении расстояния между микро- и пикобазой.

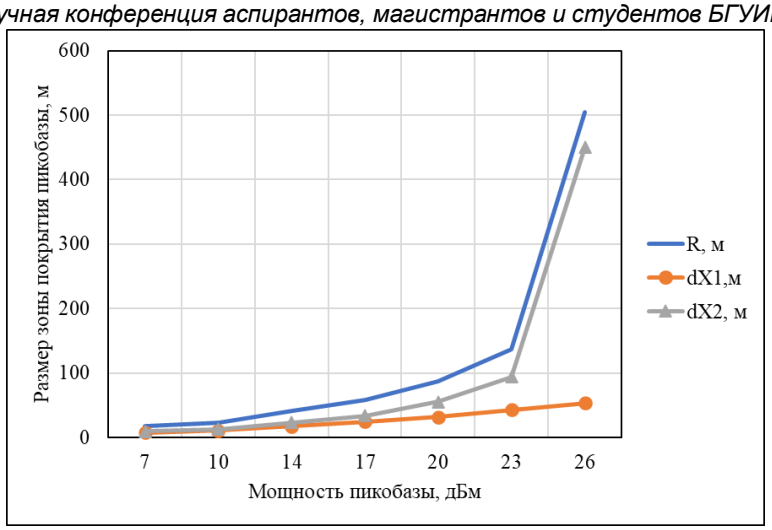


Рисунок 4 – Изменение продольного размера пикосоты при изменении мощности пикобазы.

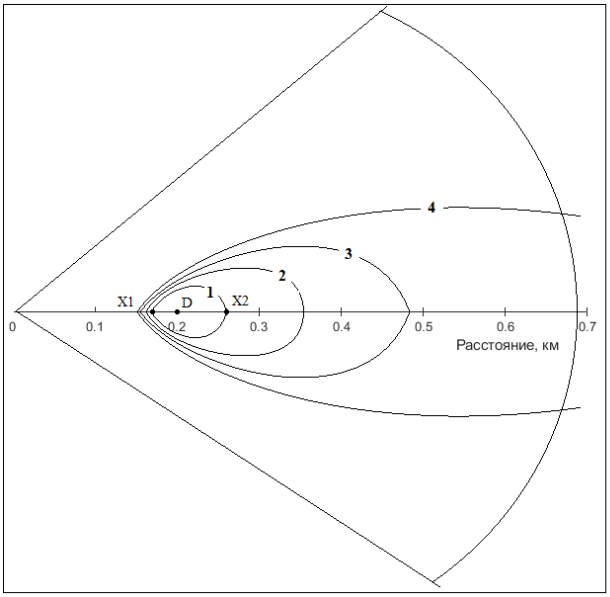


Рисунок 5 – Изменение формы пикосоты при увеличении уровня сигнала пикобазы.

Разумеется, сделанное предположение не полностью корректно. Для оценки уровня сигнала пикобазы применялось математическое выражение сценария UMI-Street Canyon-LOS, соответствующее распространению по прямой видимости вдоль улицы или проспекта. При условии расположения антенны пикобазы ниже крыш прилегающих зданий (10 метров против 15–30 метров) и очень высокой рабочей частоты 27500 МГц, радиоволны пикобазы не смогут преодолеть здания, расположенные вдоль улицы. Кроме того, диаграмма направленности антенны базовых станций обычно наклоняется максимумом в низ, что также ограничит дальность распространения волн даже вдоль улицы.

Тем не менее результаты моделирования однозначно предостерегают, что пикосота, вопреки своему названию, может вырваться из габаритов небольшого округлого пятна и своими «щупальцами» распространится на сотни метров вдоль городских улиц. Подобная ситуация наиболее вероятна при расположении пикобазовых станций вблизи границы микросоты.

Заключение. Результаты компьютерного моделирования позволяют сделать несколько выводов.

Во-первых, размеры покрытия пикосот могут сильно меняться даже при незначительных изменения места расположения и уровня излучаемой мощности пикобазы.

Во-вторых, использование для пикосот достаточно высоких радиочастот не гарантирует

локализацию радиопокрытия на небольшой площади.

В-третьих, ключевую роль в гармонизации гетерогенного радиопокрытия играет форма и угол наклона диаграммы направленности всех задействованных антенн, в том числе и антенных массивов с Beamforming.

Полученные результаты имеют практическое значение при проектировании сотовых радиосетей гетерогенного типа.

Список литературы

1. *Small cell networks: Deployment, Management, and Optimization. Holger Claussen, David Lopez-Perez, Lester Ho, Rouzbeh Razavi, Stepan Kucera. The Institute of Electrical and Electronic Engineers, Inc. – John Wiley & Sons, Inc. – 2017. – 555 p.*
2. *Jeanette Wannstrom, Keith Mallinson. Heterogeneous Networks in LTE. /WiseHarbor [Электронный ресурс] – URL: https://www.3gpp.org/technologies/keywords-acronyms/1576-hetnet.*
3. *Аксёнов, В. А. Гетерогенные радиосети мобильного и фиксированного доступа. Белорусский государственный университет информатики и радиоэлектроники, 2023, № 1, с. 60–75.*
4. *ETSI TR 101 362 V7.0.0 (1999-07). Digital cellular telecommunications system (Phase 2+); Radio network planning aspects. Annex B: Propagation loss formulas for mobile radiocommunications. P. 20-21. [Электронный ресурс] – URL: https://www.etsi.org/deliver/etsi_tr/101300_101399/101362/07.00.00_60/tr_101362v070000p.pdf*
5. *3GPP TR 38.901 version 16.1.0 Release 16. 5G. Study on channel model for frequencies from 0.5 to 100 GHz. [Электронный ресурс] – URL:https://www.etsi.org/deliver/etsi_tr/138900_138999/138901/16.01.00_60/tr_138901v160100p.pdf*

UDC 004.75

MATHEMATICAL MODEL OF HETEROGENEOUS RADIO COVERAGE

RODIONOV *M.A.*

gr.467041

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Astrovskiy I.I. – Ph. D

Annotation. The article considers the issues of organizing joint radio coverage of heterogeneous radio networks, when small outdoor picocells are cultivated on the territory of a relatively large urban cell. Using computer modeling, the dependences of the sizes of small cells on a number of parameters are obtained. The results obtained allow us to give recommendations on optimizing heterogeneous network solutions.

Keywords: heterogeneous networks, network architecture, guaranteed connection, mathematical modeling, simulation, coverage optimization

УДК 004.75

ПОСТРОЕНИЕ ЭФФЕКТИВНОГО CI/CD КОНВЕЙЕРА

Яцеивч К.В.

гр.367041

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Научный руководитель: Кореневский С.А. – кандидат технических наук, доцент кафедры ИКТ

Аннотация. Доклад посвящен построению эффективного ci/cd конвейера, который является неотъемлемой частью современного процесса разработки программного обеспечения. В нем рассматриваются ключевые этапы автоматизации: от интеграции изменений в код до развертывания в рабочем окружении, включая тестирование, управление артефактами и мониторинг.

Ключевые слова: Continuous integration, continuous deployment

Введение. Современная разработка программного обеспечения требует не только высокой скорости внедрения изменений, но и стабильности, предсказуемости и надежности процессов. В условиях динамично развивающихся проектов ручное управление тестированием, сборкой и развертыванием становится сложной и ресурсоемкой задачей[1].

Continuous integration и continuous deployment позволяет автоматизировать эти процессы, обеспечивая постоянную интеграцию изменений, их тестирование и доставку в рабочее окружение. Это снижает вероятность ошибок, ускоряет выпуск новых версий и упрощает совместную работу команд.

Эффективный ci/cd-конвейер включает в себя несколько ключевых этапов, таких как автоматическая сборка, тестирование, управление артефактами, развертывание и мониторинг. Для его реализации существует множество инструментов, каждый из которых подходит для различных масштабов проектов и инфраструктурных решений.

Основная часть. Continuous integration и continuous deployment — это набор практик, направленных на автоматизацию процессов разработки, тестирования и развертывания приложений.

Continuous integration — это процесс интеграции изменений в основной код проекта как можно чаще. Цель continuous integration — обеспечить, чтобы код, написанный различными разработчиками, не конфликтовал между собой. Он включает автоматическую сборку и тестирование, чтобы оперативно выявлять ошибки на ранних стадиях. Continuous deployment — это процесс автоматической доставки проверенного кода в рабочее окружение. Continuous deployment подразумевает автоматическое развертывание изменений в среду, которая предназначена для конечного пользователя, сразу после успешного тестирования.

Все начинается с разработки кода. При использовании ci/cd подхода коммиты, сделанные разработчиками, автоматически проверяются системой, что позволяет предотвратить проблемы в кодовой базе на ранних этапах.

После того как код попадает в репозиторий, система ci/cd инициирует процесс сборки, который включает компиляцию исходного кода, зависимостей и создание артефактов, таких как исполнимые файлы или контейнеры docker. Это критический момент, так как любые

ошибки на этом этапе могут повлиять на стабильность и функциональность приложения.

Одним из ключевых преимуществ ci/cd является автоматическое тестирование, которое проводится сразу после сборки[2].

Во время процесса сборки и тестирования важно проверять качество кода с помощью таких инструментов, как sonarqube для статического анализа, которые помогут выявить потенциальные проблемы до того, как код попадет в продакшн.

После успешной сборки и тестирования приложение должно быть готово к развертыванию. Артефакты хранятся в репозиториях артефактов, таких как nexus или artifactory, которые позволяют эффективно управлять версиями и зависимостями[2].

После успешного прохождения всех тестов система ci/cd автоматизирует развертывание в тестовом или продакшн окружении. Этот процесс может быть настроен для безостановочного развертывания или через стратегию канареечных релизов, при которой новая версия приложения доступна лишь небольшой части пользователей, чтобы минимизировать риски.

После развертывания приложения важно отслеживать его состояние с помощью инструментов мониторинга, таких как prometheus, grafana или elk stack. Эти инструменты позволяют своевременно обнаруживать проблемы и отправлять уведомления. В случае необходимости система должна поддерживать возможность быстрого отката на предыдущую стабильную версию.

Не все приложения одинаковы, и ci/cd конвейеры должны быть адаптированы под особенности конкретных типов приложений. Для мобильных приложений можно настроить автоматическое тестирование на разных устройствах и платформах с использованием инструментов fastlane и firebase test lab. Также важно автоматизировать сборку и деплой на платформы app store и google play.

К популярным ci/cd инструментам можно отнести jenkins, gitlab ci, github actions, circle ci, travis ci.

Jenkins — это один из самых популярных инструментов для автоматизации ci/cd. Он поддерживает множество плагинов, что позволяет интегрировать его с различными системами и инструментами для тестирования, сборки, развертывания и мониторинга. Jenkins хорош для проектов любого масштаба и легко масштабируется.

Gitlab ci/cd встроен непосредственно в Gitlab, что делает его удобным для команд, использующих Gitlab как основную систему контроля версий. Gitlab ci/cd поддерживает автоматическую сборку, тестирование, деплой и мониторинг. Он также позволяет интегрировать дополнительные инструменты для обеспечения качества кода и безопасности.

Github Actions предоставляет удобную платформу для continuous integration и continuous deployment непосредственно в Github. Это мощный инструмент, позволяющий автоматизировать сборку, тестирование и развертывание приложений на различных облаках и сервисах.

Circle ci — это облачное решение для ci/cd, которое отличается высокой скоростью и простотой интеграции с github и bitbucket. Оно поддерживает масштабируемость и быструю настройку конвейеров.

Travis CI — облачный continuous integration инструмент, который интегрируется с github и обеспечивает автоматическую сборку и тестирование. Он особенно популярен среди проектов с открытым исходным кодом.

Для построения действительно эффективного ci/cd конвейера недостаточно просто автоматизировать процесс интеграции и развертывания. Важно учитывать такие аспекты, как безопасность, масштабируемость, отказоустойчивость и удобство сопровождения.

Автоматизация процессов развертывания не должна приводить к компрометации безопасности. Безопасность должна быть не дополнительным этапом, а неотъемлемой частью ci/cd. Для этого стоит внедрить практики devsecops, которые интегрируют безопасность на всех этапах разработки и развертывания. Для безопасного хранения токенов, паролей и ключей используются инструментов типа hashicorp vault или aws secrets manager. Также применяется принцип минимально необходимого доступа в настройках прав разработчиков, devops-инженеров и автоматических процессов. Для проверки целостности создаваемых бинарных файлов используется цифровые подписи на этапах сборки. Важным аспектом является автоматический анализ безопасности на этапе программирования. Для этого используются checkmarx или snyk для выявления уязвимостей в коде и зависимостях. На регулярной основе необходимо производить сканирование docker образов для поиска известных уязвимостей.

При увеличении нагрузки ci/cd должен масштабироваться без потери скорости развертывания. Для этого применяется горизонтальное масштабирование исполняющих узлов: добавление дополнительных исполняющих узлов позволяет выполнять тесты и сборки параллельно. Важным фактором является кэширование зависимостей. Использование кеша для хранения ранее загруженных пакетов ускоряет сборку.

Документация играет важную роль в успешной настройке и поддержке ci/cd конвейера. Без четкой документации команды могут столкнуться с проблемами при развертывании, тестировании и мониторинге. Важно описать каждый этап конвейера, используемые инструменты, а также процедуры для откатов, восстановления и реагирования на ошибки. Это поможет новым сотрудникам быстрее разобраться в процессе и минимизировать ошибки. Регулярные тренинги и семинары по ci/cd, внедрению новых инструментов и поддержке уже существующих пайплайнов обеспечат команду необходимыми знаниями для эффективной работы с ci/cd.

Заключение. Построение эффективного ci/cd конвейера является ключевым элементом в современной разработке программного обеспечения. Он позволяет автоматизировать многие рутинные процессы, такие как сборка, тестирование и развертывание, тем самым снижая риски ошибок и ускоряя выпуск новых версий приложений. Этапы ci/cd, включая автоматизацию тестирования, управление артефактами и деплоймент, требуют тщательной настройки и использования правильных инструментов.

Чтобы ci/cd действительно принесло пользу, важно учитывать несколько факторов. Это грамотный выбор инструментов, настройка подходящих процессов, а также наличие культуры devops в команде. Только слаженная работа всех участников процесса — разработчиков, тестировщиков, devops-инженеров и других — может обеспечить полную автоматизацию и эффективную работу ci/cd конвейера.

Таким образом, continuous integration и continuous deployment — это не просто набор инструментов, а целая философия, которая помогает ускорить процесс разработки, повысить качество приложений и снизить затраты на поддержку. Понимание и грамотное применение этих практик позволит командам быстрее реагировать на изменения и эффективно управлять жизненным циклом разработки.

Список литературы

1. Eberhard Wolf. Continuous delivery. The practice of continuous updates – Person Education, Inc 2018. – 320 c.

2. Continuous Integration: Improving Software Quality and Reducing Risk. – O'Reilly Media, Inc., 2007. – 336 c.

UDC 004.75

BUILDING AN EFFICIENT CI/CD PIPELINE

Yatsevich K.V.

gr.367041

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Korenevksy S.A. – Ph. D

Annotation. The report is devoted to building an effective ci/cd pipeline, which is an integral part of the modern software development process. It covers key stages of automation: from integrating changes into the code to deploying to the production environment, including testing, artifact management and monitoring.

Keywords: Continuous integration, continuous deployment

СЕКЦИЯ «ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ СИСТЕМ»

D-S EVIDENCE THEORY-DRIVEN FPGA ARCHITECTURE FOR RADAR AND VISUAL FUSION ALGORITHM

Hao Ni, Hongfei Lian, Qiuyu Liu, Hongqi Fan

College of Electronic Science and Technology, National University of Defense Technology, Changsha 410073, China

Abstract: To address the issue of low real-time fusion efficiency in multi-source sensor data, this paper proposes an FPGA-based radar-vision fusion method using D-S evidence theory. By implementing a parallel architecture and pipeline optimization, the fusion latency is reduced to the microsecond level while improving resource utilization. Simulation experiments demonstrate that the proposed method offers high reliability and low latency in autonomous driving scenarios, with potential scalability to intelligent transportation systems.

Keywords: D-S evidence theory, radar-vision fusion, FPGA, autonomous driving

In autonomous driving multimodal perception systems, the fusion of millimeter-wave radar and visual sensors encounters challenges in real-time processing of heterogeneous data. While Dempster-Shafer (D-S) evidence theory enhances target detection robustness through confidence fusion, its high computational complexity impedes real-time applications. This study proposes a hardware acceleration module based on FPGA parallel architecture and pipeline optimization, achieving high-speed synthesis of dynamically conflicting evidence via the D-S algorithm. The solution delivers low-latency, highly reliable multisource perception for autonomous vehicles, addressing microsecond-level response demands in complex scenarios.

The D-S evidence theory-based radar-visual fusion algorithm is implemented in two stages. First, Basic Probability Assignment (BPA) functions are constructed for millimeter-wave radar and visual sensors respectively, tailored to their heterogeneous data characteristics. An unknown event category is incorporated to model target classification uncertainty, ensuring normalization constraints in probability allocation. Second, the D-S combination rule dynamically fuses BPA data from both

modalities, with fusion weights adaptively adjusted based on quantified sensor uncertainty levels to resolve evidence conflicts. As illustrated in Figure 1, this framework enhances multi-source perception confidence and robustness through heterogeneous data modeling and probabilistic fusion mechanisms. Detailed implementation procedures are provided in Reference [2].

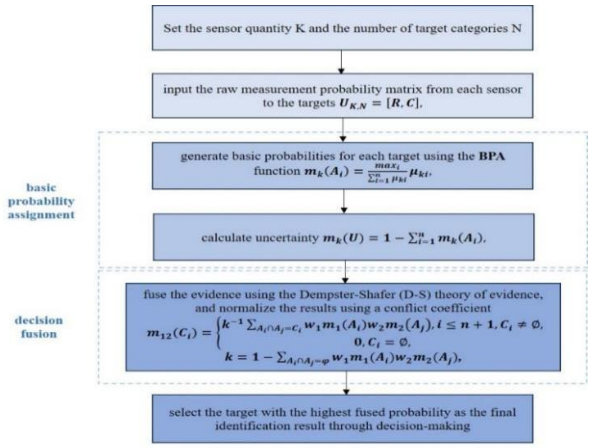


Figure 1,Algorithm Flowchart

The FPGA implementation comprises two phases: first validating the D-S algorithm logic in MATLAB, followed by hardware migration via Vitis HLS. To address real-time requirements for radar-visual fusion, a collaborative optimization strategy integrating loop unrolling and pipeline techniques is adopted. This approach establishes a parallel architecture for BPA computation across millimeter-wave radar and visual sensors, enhancing data throughput while optimizing hardware resource utilization. System validation is conducted through a three-stage process encompassing C simulation, synthesis, and co-simulation to ensure compliance with stringent latency and reliability constraints in multimodal perception scenarios.

To validate the functional correctness of the algorithm, C simulation is employed. In this case, data from relevant literature [3] is used as input. Specifically, visual sensor data originates from ImVoxelNet (WACV 2022) [4], and millimeter-wave radar data comes from PointPillars (CVPR 2019) [5], as shown in Table 1.

Table 1 - Credibility of Possible Targets for Vision Sensors and Radar Sensors（%）

Sensor	Car	Pedestrian	Cyclist	Truck
Vision Sensor	22.55	13.73	9.67	13.87
Radar Sensor	21.26	28.33	52.47	11.18

The results obtained after applying the Basic Probability Assignment (BPA) are shown in Table 2.

Table 2 - Basic Probability Assignments of Possible Targets for Vision Sensors and Radar Sensors(%)

Sensor	Car	Pedestrian	Cyclist	Truck	Uncertainty
Vision Sensor	8.50	5.18	3.65	5.23	77.45
Radar Sensor	9.85	13.13	24.31	5.18	47.53

The results after fusion are shown in Table 3.

Table 3 - Fusion Results of Vision Sensors and Radar Sensors(%)

Car	Pedestrian	Cyclist	Truck	Uncertainty	Fusion Result
13.77	14.65	23.61	7.45	40.52	Cyclist

By comparing Table 1 and Table 3, it can be observed that neither a single vision sensor nor a radar sensor can achieve a unified identification of the target based solely on its own detection results. However, by applying D-S evidence theory for fusion, the final detection result identifies the target as a cyclist, which is consistent with the original results provided in reference [2]. Furthermore, by comparing Table 2 and Table 3, it is evident that the fusion process reduces the uncertainty of the detector. Lower uncertainty indicates higher reliability of the identification.

The FPGA hardware architecture mapping was implemented through C synthesis, generating critical performance metrics. The acceleration factor of the code was calculated by comparing its execution efficiency with MATLAB simulation results, as summarized in Table 4.

Table 4 - Results of C Synthesis for Vitis HLS Code and Speedup Factor Benchmarking

Key Metrics	Target	Estimated	Uncertainty	Latency(ns)	Latency in Matlab(ms)
Synthesis Results	20.00ns	13.42ns	5.40ns	1680.00	5.301
Key Metrics	**Interval**	**BRAM**	**DSP**	**FF**	**LUT**
Synthesis Results	85	0	32	3059	5466

The analysis of Table 4 reveals that the actual clock period of 14.60 ns meets the requirement of exceeding the estimated 13.42 ns. The total fusion latency is measured at 1,680 ns, achieving a 3100× speedup factor compared to the 5.3 ms latency observed in MATLAB simulations for identical datasets. Furthermore, resource utilization metrics—including DSP slices, flip-flops (FFs), and look-up tables (LUTs)—remain significantly below the maximum thresholds of FPGA platforms typically deployed for radar-visual fusion tasks. These results validate the algorithm's capability to support high-throughput processing of large-scale inputs in autonomous driving systems while maintaining hardware efficiency.

Functional correctness and timing violations were validated through co-simulation, with the timing diagram generated during this process illustrated in Figure 2.

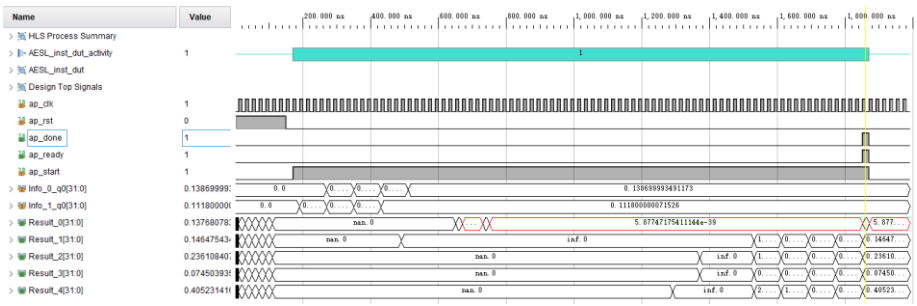


Figure 2, Timing diagram generated after co-simulation using Vitis HLS software

Figure 2 shows that the simulation results are consistent with the C simulation results, indicating that the functionality of the hardware implementation is correct. The sensor inputs are sampled accurately on the rising clock edges, and the fusion results are output within the expected cycles. Key signals (such as start, done) are stable at the clock edges, presenting no risk of metastability. This confirms the successful realization of the FPGA design implementation.

To address the challenges of low multi-sensor fusion efficiency and insufficient reliability of single-sensor environmental perception in autonomous driving, this paper proposes an FPGA-based hardware acceleration method for radar-visual fusion utilizing Dempster-Shafer (D-S) evidence theory. A hierarchical parallel pipeline architecture combined with dynamic resource scheduling strategies achieves efficient fusion of millimeter-wave radar and vision heterogeneous data, leveraging FPGA's

parallel computing capabilities to compress fusion latency to microsecond levels. This solution provides all-weather reliable perception for autonomous vehicles while demonstrating extensibility to smart transportation systems and agricultural robotics domains. The proposed methodology exhibits significant industrial application prospects for multi-modal perception technologies in dynamic complex scenarios

Reference

1. Yao S., Guan R., Huang X. [et al.] Radar-Camera Fusion for Object Detection and Semantic Segmentation in Autonomous Driving: A Comprehensive Review // IEEE Transactions on Intelligent Vehicles. – 2023. – T. 9, № 1. – C. 1-40.

2. Xie H., Pu J. Research on Information Fusion Algorithm of Multi-mode Composite Detector Based on D-S Evidence Theory // Photoelectric Technology Application. – 2017. – T. 32, № 2. – C. 41-43.

3. Bai X., Yu Z., Zheng L. [et al.] SGDet3D: Semantics and Geometry Fusion for 3D Object Detection Using 4D Radar and Camera // IEEE Robotics and Automation Letters. – 2025. – T. 10, № 1. – C. 828-835.

4. Rukhovich D., Vorontsova A., Konushin A. ImVoxelNet: Image to voxels projection for monocular and multi-view general-purpose 3D object detection // Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision. – 2022. – C. 1265-1274.

5. Lang A.H., Vora S., Caesar H. [et al.] PointPillars: Fast encoders for object detection from point clouds // Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. – 2019. – C. 12689-12697.

FPGA ACCELERATION MODULE DESIGN FOR SYSTEMATIC RESAMPLING IN PARTICLE FILTERS

Xinran Zhang, Hongfei Lian, Qiuyu Liu, Hongqi Fan

College of Electronic Science and Technology, National University of Defense Technology, Changsha 410073, China

Abstract: The resampling algorithm addresses the degeneracy problem in particle filters, but its high computational load limits real-time applications. This paper proposes an FPGA-accelerated implementation of the systematic resampling algorithm, significantly improving the processing speed of particle filters.

Keywords: systematic resampling algorithm, FPGA, particle filter

As a powerful nonlinear state estimation method, particle filtering demonstrates unique advantages in target tracking, autonomous driving, sound source localization, and other fields[1-3]. However, the high computational complexity of its resampling process severely restricts the real-time performance of particle filters, limiting their application in embedded real-time scenarios such as intelligent unmanned aerial vehicles and guidance radars[4]. To address this issue, this paper proposes an FPGA acceleration scheme based on systematic resampling. By parallelizing computations, the scheme improves computational efficiency while ensuring algorithmic accuracy, significantly enhancing the processing speed of particle filters to meet real-time requirements. This advancement expands the application of particle filters in edge devices with stringent real-time demands, such as intelligent unmanned aerial vehicles and guidance radars.

The implementation of the resampling algorithm on FPGA is divided into two main stages. First, the code is developed according to the algorithmic principles and validated for correctness using MATLAB. Subsequently, the algorithm is ported into the Vitis HLS environment, where test benches are developed for simulation. This chapter focuses on the simulation of the resampling algorithm within Vitis HLS and provides a comparative performance analysis with MATLAB simulations.

Taking 100 particles as an example, first input the particle weights and random numbers. After processing in Vitis HLS, a new set of particle weights is generated. Then, in MATLAB, plot both the original particle weights before resampling and the new weights produced by the simulation.

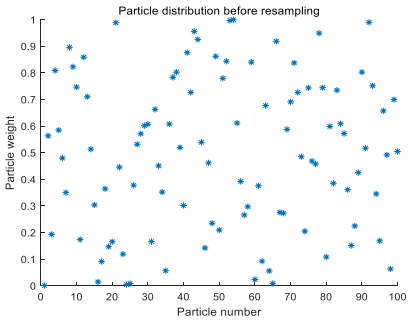


Fig.1. Particle distribution before resampling

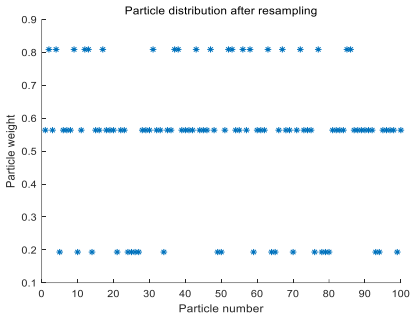


Fig.2. Particle distribution after resampling

By comparing Figure 1 and Figure 2, it can be observed that after resampling, particles with larger weights are duplicated multiple times, while those with smaller weights are replicated less frequently, t hereby verifying the correctness of the algorithm's functionality.

The timing diagram generated by the simulation is shown in figure 3:

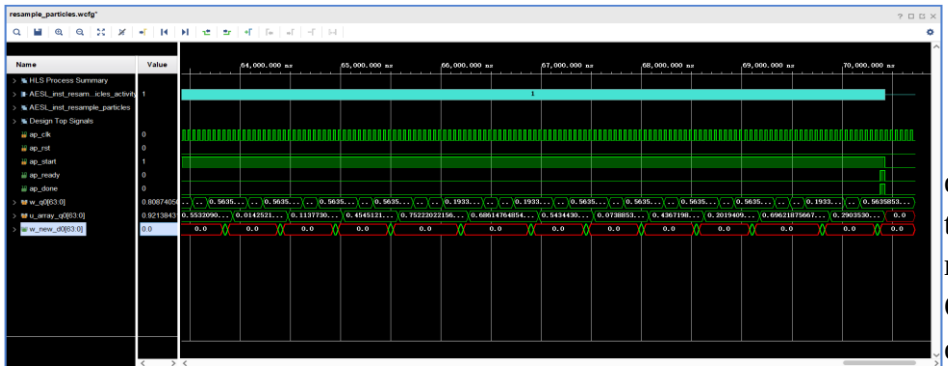


Fig.3. Timing diagram for the resampling algorithm

Figure 3 demonstrates that the simulation results match the C simulation outputs, confirming the functional correctness of the hardware implementation. The input weights and random numbers are properly sampled at clock rising edges, while resampling results are generated within the expected cycle count. Critical control signals (e.g., start, done) remain stable at clock edges with no metastability risks, verifying the successful FPGA implementation of the resampling algorithm.

The resource utilization report for the resampling implementation on FPGA is presented in Table I:

TABLE Ⅰ. The result of C synthesis

Indicators	Target	Tarated	Estimainty	Uncertes)	Latency(cycly(ns)	Latency
Result	50.00ns	33.917ns	13.50ns	406	2.03E4	
Indicators	Interval	BRAM	DSP	FF	LUT	
Result	406	0	0	217	111	

According to Table I, the clock cycle is 50.00 ns. Subtracting the uncertainty of 13.50 ns yields an actual cycle of 33.917 ns. The total cycle time for completing the resampling algorithm is 105 clock cycles (2.03E4 ns), while the MATLAB implementation requires 2.81E4 ns. This demonstrates that the algorithm meets the low-latency requirements of the resampling algorithm while occupying minimal DSP resources. Therefore, the algorithm can achieve high throughput in particle filters when processing large-scale inputs.

When the number of particles is 100, the algorithm's speedup ratio $\frac{t_{Matlab}}{t_{FPGA}}$=1.4. As the particle count NN varies, the speedup ratio also changes, as shown in Figure 4.

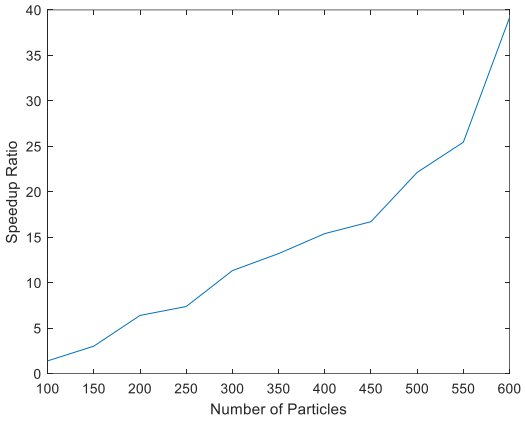


Fig.4. Speedup Ratio versus Number of Particles Diagram

As shown in the figure, the speedup ratio increases progressively with the number of particles, demonstrating more pronounced acceleration effects at higher particle counts. While the weight distribution also influences the relationship between speedup ratio and particle number, this aspect is not explored in the present study.

To address the challenges of high computational complexity and insufficient real-time performance in resampling algorithms, this paper proposes an FPGA-based hardware acceleration scheme utilizing systematic resampling. By implementing a parallel computing architecture, the solution significantly enhances processing efficiency while maintaining algorithmic accuracy, thereby dramatically improving the particle filter's execution speed. Experimental results demonstrate that the proposed approach achieves high energy efficiency and superior real-time performance, effectively enabling the deployment of particle filters in latency-critical edge computing applications such as intelligent UAVs and guidance radar systems.

Reference

[1]*Wang Ning, Duan Rui, Zhou Xiaoyi. A Box Particle Filtering Approach for Target Tracking Under Measurement Uncertainty[J]. Journal of Electronics & Information Technology, 2024, 46(9): 3654-3661.*

[2]*Gao Yan, Fu Chunyun, Yang Zhong, Yang Guanlong. Vehicle Speed Estimation Based on Improved Particle Filter Algorithm[J]. Journal of Chongqing University, 2024, 47(3): 44-52.*

[3]*Liu Wangsheng, Pan Haipeng, Wang Minghuan. Composite Model Particle Filter for Indoor Sound Source Localization Using Multi-Feature Fusion [J]. Acta Armamentarii, 2024, 45(3): 975-985.*

[4]*A. KRISHNA, A. VAN SCHAIK, C. S. THAKUR. FPGA Implementation of Particle Filters for Robotic Source Localization[J]. IEEE Access, 2021, 9: 98185–98203*

[5]*Su Zhibao, Lu Jilian. Research Methods for Formation Control of Multiple Mobile Robots [J]. Robot, 2003, 25(1): 88-91.*

HARDWARE-DEPENDENCY-REDUCED VISUAL SLAM

Lian YU, Dongsheng LI, GuoYan WANG*, Fei ZHAO, Hongqi FAN

National Key Laboratory of Automatic Target Recognition, College of Electronic Science and Technology, National University of Defense Technology, Changsha 410073, China

Annotation: To address the poor real-time performance and hardware dependency of traditional visual Simultaneous Localization and Mapping on embedded platforms, this paper proposes a cloud-native collaborative framework enabling low-latency data transmission and cloud-based pose estimation. Experimental results demonstrate stable frame rates without map fragmentation or tracking failures in scenario testing. The architecture enhances environmental adaptability and computational robustness

for visual Simultaneous Localization and Mapping on compact unmanned platforms, providing a high-precision solution for resource-constrained scenarios.

Keywords: Cloud-Native Architecture; Visual Simultaneous Localization and Mapping; Unmanned Systems; Real-Time Streaming Protocol;

1. Introduction

In modern unmanned combat systems, autonomous environmental perception and real-time localization capabilities constitute the critical operational advantages of unmanned platforms. As the core enabling technology for environmental awareness and navigation positioning, Simultaneous Localization and Mapping (SLAM) establishes spatial cognition for unmanned systems by simultaneously computing platform motion trajectories and constructing environmental topological models in real-time. Notably, visual SLAM has emerged as the preferred solution for autonomous localization in structured environments at low velocities, owing to its low sensor cost and strong environmental adaptability.

However, visual SLAM faces dual performance constraints: (1) algorithmic complexity arising from feature extraction (e.g., ORB feature detection) and nonlinear optimization processes (e.g., pose graph optimization), and (2) real-time performance degradation caused by resource contention between pose estimation and mapping threads. For small-scale unmanned systems with stringent size-, weight-, and power-constrained (SWaP-constrained) configurations, these limitations result in positioning accuracy and computational efficiency that fail to meet real-time requirements for battlefield reconnaissance tasks.

To address these technical bottlenecks, this paper proposes a cloud-native architecture-based collaborative computing framework for visual SLAM, effectively mitigating onboard hardware constraints.

2 Background and Related Work

2.1 Visual SLAM

Simultaneous Localization and Mapping (SLAM) is a foundational technology that enables autonomous device positioning and concurrent environmental mapping in unknown environments through multi-sensor data fusion. Its technical evolution can be delineated through the following developmental stages:

Early research predominantly utilized filtering frameworks, where state estimation and map

MODELING OF SEISMIC WAVE ATTENUATION FOR HELICOPTER DETECTION

Liu Xiaojun, Wang Zhuang

College of Electronic Science and Technology, National University of Defense Technology, Changsha, 410073, China

Annotation. Seismic wave detection technology provides a viable solution for monitoring low-altitude helicopters in border airspace. This paper proposes a seismic wave attenuation model and validates it through numerical simulations.

Keywords. Border defense, low-altitude helicopter, seismic wave detection, seismic wave attenuation

Introduction. Modern aerial vehicles, particularly helicopters, threaten low-altitude border defense. Therefore, developing effective low-altitude helicopter detection technological approaches is essential. The seismic sensor system provides a viable passive detection technology—seismic wave detection—for low-altitude border defense, offering advantages over radar (environmental covertness and anti-electromagnetism interference) and electro-optical systems (non-line-of-sight capability), with additional benefits of low cost, compact size, and flexible deployment. This paper focuses on effectively detect low-altitude helicopters via seismic waves. First, the propagation process from helicopter radiated acoustic waves to seismic wave signals received by sensors is characterized, and a model for Rayleigh wave attenuation is established. Then, the time-domain and frequency-domain models of the received signals are derived. Finally, numerical simulation results and conclusion are presented.

Propagation Process of Helicopter Radiated Acoustic Pressure Signals. Helicopter external noise includes aerodynamic noise (dominant far-field) and mechanical noise (near-field attenuation, negligible). Given the directional radiation pattern of the acoustic field[1], this study focuses on main rotor aerodynamic pressure signals (excluding tail rotor effects). As illustrated in Figure 9, the energy conversion process involves three sequential phases: 1) acoustic propagation in the air, 2) acoustic-seismic coupling at the air-ground interface, and 3) seismic waves propagation to sensors in the ground.

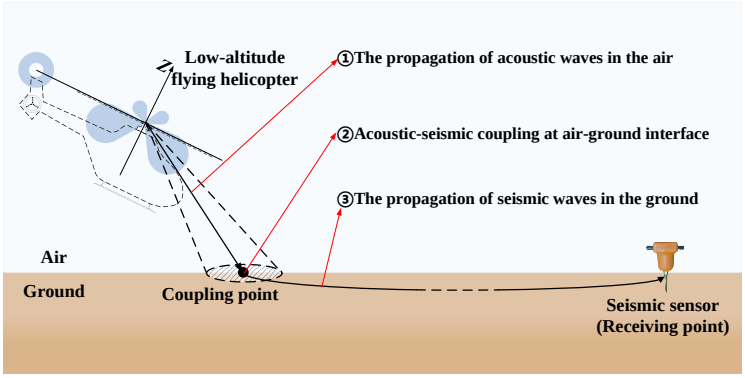


Figure 9 - The propagation process

Seismic Wave Attenuation Model in Propagation Media. Based on Huygens principle, the coupling point can be modeled as new ground vibration source. Previous researches about ground vibration sources have revealed that the energy of Rayleigh waves dominate at long distances (≈67%) due to the much lower attenuation rate. It can be concluded that sensors primarily detect Rayleigh wave energy. Combining absorption and geometric divergence, Rayleigh wave attenuation follows the Bornitz equation:

$$A(r) = A_0 \cdot r^{-0.5} \cdot \exp(-\alpha r) \tag{1}$$

where A_0 is the initial amplitude at the coupling point, $A(r)$ is the amplitude received by sensor at distance r .The term $r^{-0.5}$ refers to the geometric divergence of Rayleigh waves. The parameter α is the absorption attenuation coefficient:

$$\alpha = \frac{\pi f}{V_R Q} \tag{2}$$

where f is the vibration frequency, V_R is the phase velocity of Rayleigh waves, and Q is the quality factor that depends on soil type. However, the in-situ quality factor Q cannot be accurately obtained, restricting the estimation of α using Eq.(2). For this reason, a “frequency-independent” attenuation

coefficient α_0 has been proposed[2], defined as follows:

$$\alpha_0 = \frac{\alpha}{f} = \frac{\pi}{V_R Q} \tag{3}$$

Based on Eq.(3), the coefficient α_0 can be approximated as a constant, making it effectively applicable in estimating absorption attenuation. Consequently, the amplitude attenuation for Rayleigh waves can be further written as given by:

$$A(r) = A_0 \cdot r^{-0.5} \cdot \exp(-\alpha_0 fr) \tag{4}$$

Models of Acoustic Pressure Signal Propagation. *Equivalent Vibration Source Signals at Coupling Point.* The coupling point between the acoustic wave and the ground can be regarded as an acoustic signal receiving point (virtual microphone), then the acoustic pressure signal at the coupling point is given by the following equation (the absolute time delay of acoustic wave propagation from the rotor to the coupling point, being irrelevant to passive detection, is thus omitted for simplicity)[3]:

$$U_{p_L}(t) = \begin{cases} \sum_{j=1}^{J}\sum_{l=1}^{N_L} U_{p_{L1}}\left[t-(l-1)\frac{T_V}{N_L}-(j-1)T_V\right], \ 0 \le t \le \tau \\ 0, \ \tau < t \le T \end{cases} \tag{5}$$

where N_L is the number of main rotor blades, T_V is the rotation period, J is the number of rotation cycles, $\tau = JT_V$ is the pulse width of radiated acoustic signal, T is the total signal duration, and $U_{p_{L1}}(t)$ is the acoustic pressure signal generated by a single blade during one cycle:

$$U_{p_{L1}}(t) = \begin{cases} U_{p_{L1-pr}}(t) + U_{p_{L1-ud}}(t), \ 0 \le t \le T_V \\ 0, \ t > T_V \end{cases} \tag{6}$$

where $U_{p_{L1-pr}}(t)$ and $U_{p_{L1-ud}}(t)$ are respectively the high-pressure and low-pressure signals generated by the rotor blade. The expressions are expressed as following:

$$U_{p_{L1-pr}}(t) = \begin{cases} 0, \ 0 \le t < t_{f.s-N} \\ k_{rt} k_{p0-\alpha} \dfrac{\rho 2\pi^2 r_{sL}^2}{T_V^2}\left(1+\dfrac{k_{N-\alpha}}{R_L} r_{sL}\right), \ t_{f.s-N} \le t \le t_{f.s-K} \\ 0, \ t > t_{f.s-K} \end{cases} \tag{7}$$

$$U_{p_{L1-ud}}(t) = \begin{cases} 0, \ 0 \le t < t_{f.s-NU} \\ -k_{rt} k_{u0-\alpha} \dfrac{\rho 2\pi^2 r_{sL}^2}{T_V^2}\left(1+\dfrac{k_{N-\alpha}}{R_L} r_{sL}\right), \ t_{f.s-NU} \le t \le t_{f.s-KU} \\ 0, \ t > t_{f.s-KU} \end{cases} \tag{8}$$

where k_{rt} is the acoustic attenuation coefficient from the rotor to the coupling point, k_{p0_α} is the angle of attack coefficient at the blade root, and $k_{N-\alpha}$ is the pressure variation coefficient induced by angle of attack variations along the radial blade. The parameter ρ is the undisturbed flow density, r_{sL} is the radial distance from an arbitrary point on the blade to the rotor center, and R_L is the radial distance from blade tip to rotor center (rotor disk radius). The parameters $t_{f.s-N}$ and $t_{f.s-K}$ are the initial time and the final time of the high-pressure signal respectively, and their calculation is correspondingly related with the radial distance from the blade root to the rotor center r_{sN} and the rotor disk radius R_L. The parameters of the low-pressure signal follow analogous definitions to the above, hence their descriptions are not reiterated for brevity.

The acoustic-seismic coupling accomplishes the conversion of acoustic pressure into seismic vibration source at the coupling point, it can be quantified by the coupling coefficient ε. Then the

vibration amplitude at the coupling point can be expressed as:

$$U_t(t)=\varepsilon U_{p_L}(t)=\begin{cases}\sum_{j=1}^{J}\sum_{l=1}^{N_L}\varepsilon U_{p_{L1}}\left[t-(l-1)\frac{T_V}{N_L}-(j-1)T_V\right], & 0\le t\le\tau\\ 0, & \tau<t\le T\end{cases} \tag{9}$$

where $U_t(t)$ corresponds to A_0 defined in Eq.(4). The frequency spectrum of the vibration signal obtained after discrete Fourier transform (DFT) is as follows:

$$G_t(k)=DFT\left[U_t(n)\right]=\sum_{n=0}^{N-1}U_t(n)\exp\left(-j\frac{2\pi}{N}kn\right),\ k=0,\ldots,N-1 \tag{10}$$

Frequency Response of Rayleigh Wave Attenuation. The frequency-dependent attenuation characteristics of Rayleigh waves can be formulated by frequency response as[4]:

$$G_{SR}(k,r)=\left|G_{SR}(k,r)\right|\exp\left(-j2\pi f_k\frac{r}{V_R}\right) \tag{11}$$

where the phase factor $\exp\left(-j2\pi f_k\frac{r}{V_R}\right)$ denotes the phase shift due to time delay, in which f_k represents the discrete frequency. Following Eq.(4), the amplitude-frequency response of attenuation can be explicitly expressed as:

$$\left|G_{SR}(k,r)\right|=K_P(r)D_{SR}(k,r) \tag{12}$$

In the above equation, the factors $K_P(r)=r^{-0.5}$ and $D_{SR}(k,r)=\exp(-\alpha_0 f_k r)$ correspond to geometric divergence and absorption attenuation, respectively.

Models of Signal Received by Sensor. The frequency spectrum of the signal received by the seismic sensor is:

$$G_r(k,r)=G_t(k)G_{SR}(k,r) \tag{13}$$

The seismic wave's discrete time-domain signal at the receiving point is obtained via the inverse discrete Fourier transform (IDFT) of its spectrum:

$$U_r(n,r)=IDFT\left[G_r(k,r)\right]=\frac{1}{N}\sum_{k=0}^{N-1}G_r(k,r)\exp\left(j\frac{2\pi}{N}kn\right),\ n=0,\ldots,N-1 \tag{14}$$

Numerical Simulation Experiment. The simulation parameters listed in Table 3 are established based on helicopter design specifications and aerodynamic acoustic theories, combined with research on seismic wave attenuation characteristics. Figure 10 shows the acoustic pressure signals generated by a single blade at the coupling point during one cycle: high-pressure in blue, low-pressure in black, and superimposed signal $U_{p_{L1}}(t)$ in red.

Table 3 - Simulation parameters of the helicopter main rotor

Parameter	Symbol	Value	Unit	Parameter	Symbol	Value	Unit
Number of blades	N_L	5	-	Rayleigh wave phase velocity	V_R	350	m/s
Rotational speed	N_{rpm}	192	rpm	Frequency-independent attenuation coefficient	α_0	0.50×10^{-3}	s/m
Rotation period	T_V	0.3125	s	Undisturbed flow density	ρ	1.225	kg/m^3

Distance from blade root to rotor center	r_{sN}	0.87	m	Acoustic pressure attenuation coefficient	k_{rt}	0.005	-
Distance from blade tip to rotor center	R_L	10.647	m	Acoustic-seismic coupling coefficient	ε	5×10^{-6}	(m/s)/Pa
High-pressure coefficient at blade root	k_{p0_α}	0.02	-	Number of rotation cycles	J	2	-
Low-pressure coefficient at blade root	k_{u0_α}	0.02	-	Pulse width of radiated acoustic signal	τ	0.625	s
Radial pressure variation coefficient	$k_{N-\alpha}$	0.1		Signal total duration	T	4.096	s

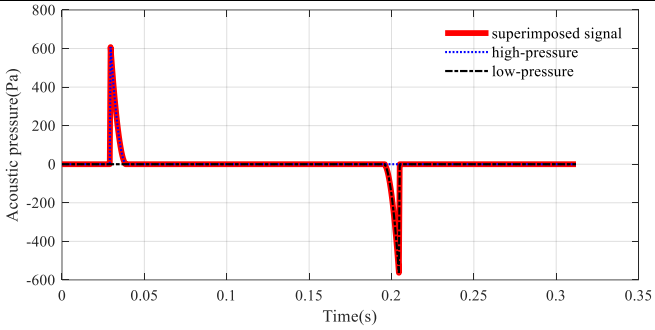
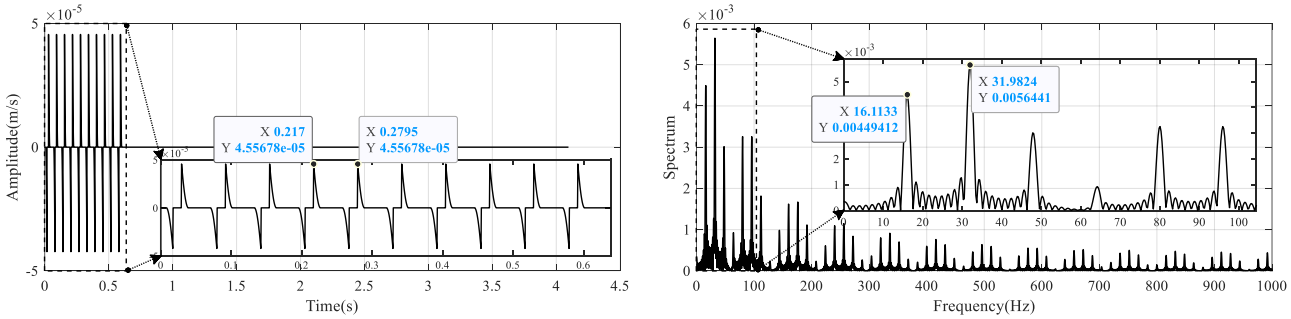


Figure 10 - The acoustic pressure signal of a single blade in a single cycle

Due to the periodic rotor motion, Figure 11(a) shows vibration waveforms with a period of approximately $T_0 = 0.0625\text{s}$. And Figure 11(b) shows discrete harmonics on the broadband noise, matching the spectrum characteristics of aerodynamic noise. The fundamental frequency $f_0 = 1/T_0 = 16\text{Hz}$ aligns with theoretical blade passing frequency (BPF) calculated as $f_{BPF} = N_L N_{rpm}/60 = 16\text{Hz}$.



(a) (b)

Figure 11 - The vibration signal and its spectrum at the coupling point

The frequency-dependent attenuation coefficient α is presented in Figure 12. Different distances r are set to analyze the attenuation effects in Eq.(11). Then the time and frequency characteristics of the vibration signal received by the sensor at different distances r are presented in Figure 13.

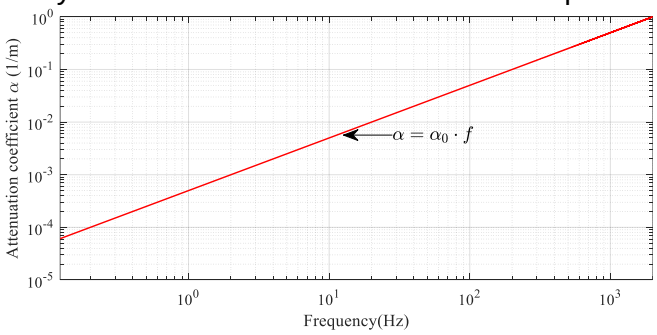
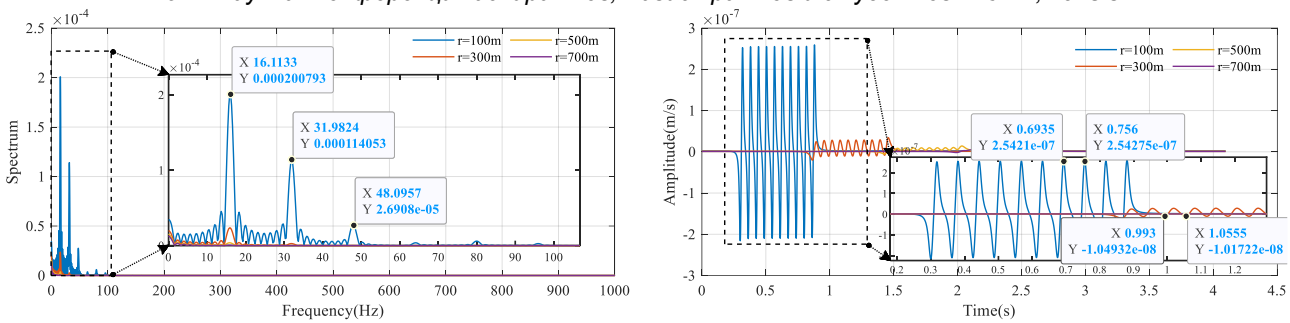


Figure 12 - The attenuation coefficient of Rayleigh waves



(a) (b)

Figure 13 - The vibration signal and its spectrum received by the sensor

Figure 13(a) demonstrates that the received signal spectrum exhibits discrete harmonic and bandwidth reduction. The latter results from the non-uniform frequency absorption attenuation of Rayleigh waves—weaker low-frequency attenuation and rapid high-frequency attenuation. With increasing propagation distance, the fundamental frequency f_0 and low-order harmonics gradually diminish. The spectrum further reveals an attenuation mechanism transition from dominant exponential absorption at short distances to prevailing power-law geometric divergence at long distances. Figure 13(b) displays periodic waveform with a fundamental period matching the acoustic signals in Figure 11, where progressive high-frequency suppression due to distance increase leads to bandwidth reduction, waveform smoothing, and prolonged signal duration.

Conclusion. The frequency-dependent attenuation in the ground of the helicopter main rotor acoustic pressure signals after coupling, constitutes a complex physical phenomenon, whose attenuation magnitude is predominantly governed by vibration frequency and medium properties, exerting direct effects on the signals received by sensors. This integrated modeling framework establishes theoretical foundations for helicopter detection, localization, and identification algorithms.

Reference

[1] *M. E. Goldstein,* Aeroacoustics. *New York: McGraw-Hill International Book Company, 1976.*

[2] *G. A. Athanasopoulos, P. C. Pelekis, and G. A. Anagnostopoulos, "Effect of soil stiffness in the attenuation of Rayleigh-wave motions from field measurements,"* Soil Dynamics and Earthquake Engineering, *vol. 19, no. 4, pp. 277–288, 2000,*

[3] *A. M. Jackie and A. S. Heister, "Basic physics of acoustic wave forming performed by the aircraft propeller and mathematical model of acoustic signal time structure of the ideal blade,"* Doklady BSUIR, *vol. 3, no. 33, pp. 20–26, 2008.*

[4] *S. R. Heister, R. V. Bykov, and A. M. Jackie, "The Evolution of the Temporal and Spectral Structures of the Acoustic Signal of a Shot (Explosion) as it Propagates through the Air,"* Bulletin of the Military Academy of the Republic of Belarus, *vol. 17, no. 4, pp. 67–75, 2007.*

МОДЕЛИРОВАНИЕ АТТЕНЮАЦИИ СЕЙСМИЧЕСКИХ ВОЛН ДЛЯ ОБНАРУЖЕНИЯ ВЕРТОЛЁТОВ

Лю Сяоцзюнь, Ван Чжуан

Национальный университет оборонных технологий, Чанша, Китай

Аннотация. Технология обнаружения сейсмических волн предоставляет жизнеспособное решение для мониторинга вертолётов на малых высотах в пограничном воздушном пространстве. В данной статье предлагается модель аттенюации сейсмических волн, которая проверяется с помощью численных симуляций.

Ключевые слова. Пограничная оборона, вертолёт на малой высоте, обнаружение сейсмических волн, аттенюация сейсмических волн

DOMAIN ADAPTIVE DEHAING BASED ON PHYSICAL PROPERTIES

Feng Ling, Yan Zhang

National University of Defense Technology

Annotation. Deep learning-based single image dehazing has advanced significantly, yet models trained on synthetic data struggle in real-world scenarios. To address this cross-domain gap, we propose a Synthetic-to-Real Dehazing framework comprising two key components: 1) A domain adaptation network that generates Synthetic-to-Real hazy images by learning real haze characteristics through depth-transmission map correlations, and 2) A physics-guided dehazing network based on the atmospheric scattering model. Crucially, our framework requires no real hazy data during dehazing training. Experiments demonstrate our framework's superior cross-domain dehazing generalization.

Keywords. *Image hazing/dehazing, Deep learning, Image enhancement, Domain adaptation, Image restoration.*

Haze, caused by atmospheric water droplets, degrades computer vision tasks (e.g., object detection, image segmentation) through light attenuation and scattering. This drives the importance of single image dehazing research. The atmospheric scattering model [1] formalizes this phenomenon as:

$$I(x) = J(x)t(x) + A(1-t(x)), \quad (1)$$

where *I* is observed hazy image, *J* is scene radiance, *t* is transmission map, and *A* is atmospheric light.

Deep learning has advanced single image dehazing, yet most methods rely on paired hazy/clear images that are impractical to acquire in real settings. While synthetic datasets circumvent this need, their simplified haze simulations lack real-world complexity, resulting in domain gaps that degrade performance on natural hazy images. Based on this problem, we propose the cross-domain dehazing framework. The framework is divided into two parts: data synthesis more in line with real haze characteristics and haze removal.

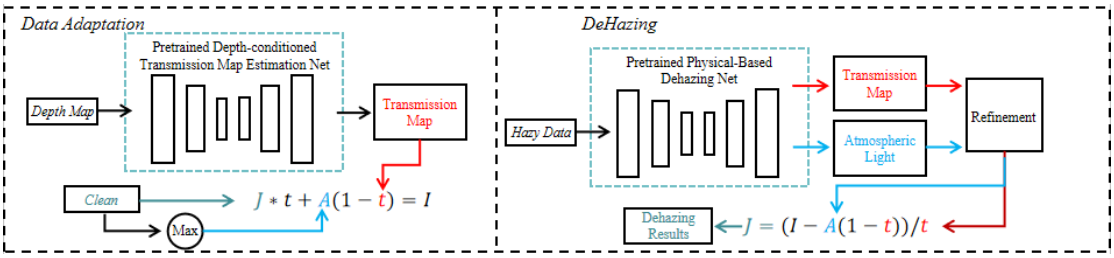
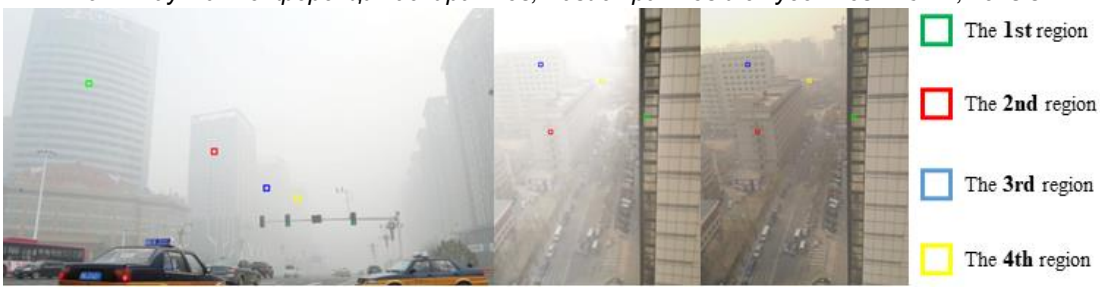


Figure 1 – Framework flow chart. The framework consists of two parts: 1. cross-domain data synthesis and single image dehazing.

The proposed dehazing framework, as illustrated in Figure 1, comprises two core components: a domain-adaptive data synthesis module and a dual-stage dehazing network. In the data synthesis phase, we establish a novel physical correlation model among the scattering coefficient β, transmission map *t*, and scene depth map *d*, where $t=e^{-\beta d}$. A pretrained depth-conditioned transmission map estimation network dynamically adjusts the scattering coefficient β through adaptive optimization algorithms. This process integrates scene depth information *d* [2] to generate physically accurate transmission maps that faithfully replicate real-world haze dispersion characteristics. By substituting the synthesized transmission map *t* and haze-free images *J* into the atmospheric scattering model (Equation 1), we efficiently construct the cross-domain datasets, providing robust training data for subsequent network optimization.



(a) Real Hazy Data (b) Ours (c) Baseline [5] (d) Region

Figure 2 – The 4 regions demonstrate the superiority of our synthetic data through comparative analysis (across four depth regions) against real haze data and baseline methods [5], validating that our results naturally reflect haze concentration attenuation with scene depth.

The dehazing network architecture adopts a two-stage progressive processing pipeline. Initially, hazy images are processed through a physical based dehazing network to obtain initial transmission estimates *t* and atmospheric light estimates *A*. Subsequently, a refinement module optimizes these parameters, yielding precise transmission map *t* and atmospheric light *A*. The optimized physical parameters are then incorporated into the equation (inverse form of Equation 1) to reconstruct high-quality haze-free images.

(a) Hazy (b) C2P Net [3] (c) DCP [4] (d) Ours

Figure 3 – Visual comparison of dehazing results of different methods.

Extensive experimental validation confirms the effectiveness of our proposed dehazing framework (detailed presentation is omitted here due to space constraints). The cross-domain synthesis method efficiently constructs domain-adaptive training data to enhance model robustness, while the dual-stage network accurately estimates transmission map *t* and atmospheric light *A*, achieving high-quality restoration.

Reference:

1. N. Narasimhan and S. Nayar, "Vision and the atmosphere," International Journal of Computer Vision, vol. 48, no. 3, pp. 233–254, 2002.

2. L. Yang, B. Kang, Z. Huang, X. Xu, J. Feng, and H. Zhao, "Depth Anything: Unleashing the Power of Large-Scale Unlabeled Data," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR) 2024.

3. K.M. He, J. Sun, and X.O. Tang, "Single image haze removal using dark channel prior," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 33, no. 12, pp. 2341–2353, 2011.

4. Y. Zheng, J. Zhan, S. He, J. Dong, and Y. Du, "Curricular Contrastive Regularization for Physics-aware Single Image Dehazing," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), 2023.

5. B. Li, W. Ren, D. Fu, D. Tao, D. Feng, W. Zeng, and Z. Wang, "Benchmarking single-image dehazing and beyond," IEEE Transactions on Image Processing, vol. 28, no. 1, pp. 492–505, 2018.

UDC: 621.3

REAL-TIME DETECTION OF MULTI-SCALE MINIATURE UNMANNED AERIAL VEHICLES BASED ON YOLOV9

*Shijie Chen,Xinpeng Lu,Jiashuo Sun, Zhichao Yin, Moufa Hu**

*Ph.D., Associate Researcher

National Key Laboratory of Science and Technology on ATR, College of Electronic Science and Technology, National University of Defense Technology, Changsha ,China

Abstract:

Aiming at the security risks of unregulated and unmanned aerial vehicles (UAVs), this paper proposes a new real-time detection method based on YOLOv9, which integrates reversible functions, programmable gradient information, and a generalized high-efficiency layer aggregation network, and combined with downsampling and local feature training method. Experiments show that the detection accuracy of the method is more than 90% and the processing frame rate is more than 20Hz @640*640.

Keywords: YOLOv9; unmanned aerial vehicle(UAV); real-time detection; Confidence optimization

1.Introduction

With the rapid development of unmanned aerial vehicles (UAVs), UAVs have been widely used in many fields, such as logistics and transportation, agricultural monitoring, and disaster rescue [1]. Miniature UAVs are characterized by compact size, light weight, and high flexibility. They can easily enter narrow spaces for reconnaissance or rescue, and are suitable for performing tasks in complex environments[2]. However, the emergence of unregulated and indiscriminate drones has also emerged, causing many problems for society[3].

Real-time UAV monitoring faces many challenges[4]. Traditional monitoring methods often rely on devices such as radar and optical cameras, but these devices have problems such as limited monitoring range, insufficient real-time performance, and difficulty in target identification when facing a large number of UAVs.YOLOV9, as an advanced target detection algorithm, provides a new solution for real-time UAV monitoring[5].It improves the detection speed while maintaining high detection accuracy, and is able to process large amounts of image data in real time. In this paper, a YOLO-based UAV detection algorithm is proposed to achieve efficient recognition by a single-stage end-to-end deep learning framework for the UAV detection task. The model can efficiently differentiate UAVs from similar objects like birds and kites by fine-tuning it through migration learning on a dataset containing multi-scene and multi-angle UAV images.

2. Real-time detection of multi-scale miniature UAVs based on YOLOv9

In this paper, a new detection method based on YOLOv9 is proposed. The flowchart is depicted in Figure 1.

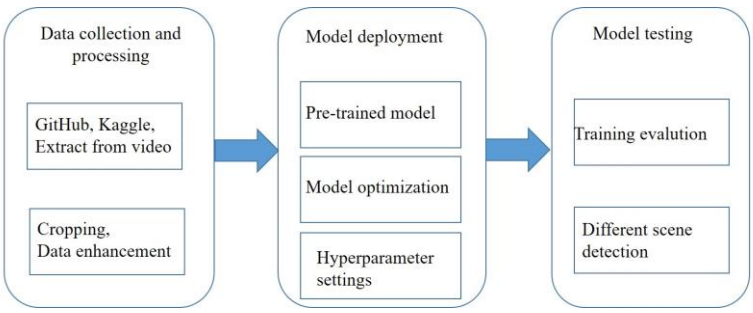


Figure 1 the flowchart of detection method based on YOLOv9

2.1 Data collection and processing

In this paper, LabelMe tool is used for image annotation work. The dataset images in this study

are mainly derived from GitHub, Kaggle and other database sites ,as well as extracted from the video at the rate of one frame per second. In addition, this study also adopts the method of highlighting and cropping parts of the images, which makes enhances the data, and can better distinguish the recognized target features as well as the details.

2.2 Model deployment and training

YOLOv9 addresses key challenges in object detection by integrating reversible functions for data integrity, programmable gradient information for accurate gradient updates, and generalized High-efficiency Layer Aggregation networks to simplify feature extraction and speed [6].

After the core network extracts features, the model merges the features, and the head network utilizes these fused features for target recognition [7], achieving high accuracy. However, when the data is transmitted through the multi-layer neural network and changes in space, part of the feature vector will be lost, resulting in incomplete feature information of the target object, thus reducing the recognition efficiency and accuracy. HWD downsampling can effectively solve the problem of local feature pooling, which uses Haar wavelet transform to retain most of the feature information, but also reduces the amount of computation, and improves the accuracy and speed.

In this paper, ImageData from different environments are selected to form the training set, test set and verification sets with a ratio of 8:1:1. The input image size is unified as 640*640, Batch-size is set to 4, and Epoch is set to 200. The works value is set to 0, SGD is selected by the optimizer, and the random number seed is set to 0.

The prediction accuracy of the UAS category reaches 0.85, indicating that it can effectively distinguish the target category from the background.

2.3 Model testing

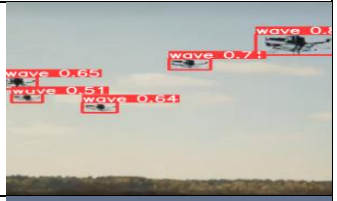
The test work is divided into online and offline sections. The speed and accuracy of the detection are evaluated. In this paper, Intel(R)Core (TM)i7-13650HX CPU and NVIDIA GeForce GTX 4060 GPU is used as the test platform.

3.Results and analysis

Experimental results demonstrate that the YOLOv9-based UAV detection algorithm exhibits robust detection performance in diverse environments, with varying flight altitudes, and heterogeneous external environments. Some results are shown in Table 1 and Tabel2.

The results of four sets of experiments show that the method of this paper enables the detection of micro UAVs. Table 1 shows the recognized UAV position frame and confidence level. Table 2 shows the statistical results. Among them, Daytime, Low Altitude and High Altitude detected all the UAVs, while Wilderness missed only one UAV, and the detection rates are all above 90%. This paper's method handles frames at frame rates of 24 Hz and 28 Hz, which are all over 20 Hz for 640*640 images.

Table 1 - Comparison of detection results in typical scenarios

Scenarios	Original image	Detection result
Daytime		
Low Altitude		

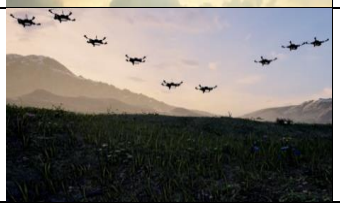
High Altitude		
Wilderness		

Table 2 - Statistical result of detection in typical scenarios

Scenario	Actual Targets (Units)	Detected Targets (Units)	Precision (%)	Frame Rate (Hz)
Daytime	5	5	100	26
Low Altitude	3	3	100	28
High Altitude	6	6	100	26
Wilderness	11	10	91	24

4 Conclusion

The phenomenon of 'black flights' and 'overflights' occurs frequently. To solve this problem, a real-time detection method based on YOLOv9 was given. The combination of adaptive hierarchical downsampling technology and local feature enhancement training framework resulted in the innovation of a reversible feature reconstruction mechanism, dynamic gradient optimization strategy, and lightweight hierarchical aggregation network. The experimental results show that the method can adapt to complex lighting, dynamic backgrounds, and dense occlusion scenes, which provides a solution for the construction of low altitude safety protection.

List of references:

[1]C. Koulouris, P. Dimitrios, I. Al-Darraji, G. Tsaramirsis and H. Tamimi. A Comparative Study of Unauthorized Drone Detection Techniques[C]. 2023 9th International Conference on Information Technology Trends (ITT), Dubai, United Arab Emirates, 2023, pp. 32-37.

[2]Kangunde V, et al.. A review on drones controlled in real-time[J]. International journal of dynamics and control, 2021, 9(4): 1832-1846.

[3]Seidaliyeva U, Akhmetov D, et al. Real-time and accurate drone detection in a video with a static background[J]. Sensors, 2020, 20(14): 3856.

[4]Cetin E, Barrado C, et al.Improving real-time drone detection for counter-drone systems[J]. The Aeronautical Journal, 2021, 125(1292): 1871-1896.

[5]Yaseen M. What is yolov9: An in-depth exploration of the internal features of the next-generation object detector[J]. arXiv preprint arXiv:2409.07813.

[6]Zhou S ,Yang L ,Liu H , et al.A Lightweight Drone Detection Method Integrated into a Linear Attention Mechanism Based on Improved YOLOv11[J].Remote Sensing,2025,17(4):705-705.

[7]Wang C Y, Yeh I H, Mark Liao H Y. Yolov9: Learning what you want to learn using programmable gradient information[C]//European conference on computer vision. Cham: Springer Nature Switzerland, 2024: 1-21.

UDC 004.056

PROTECTION AGAINST VARIOUS CLASSES OF DDOS ATTACKS

Pan Huiqin, Master's degree student

Nasonova N.V., Dr.Sc., Assoc.Prof.

Belarusian State University of Informatics and Radioelectronics

Minsk, Republic of Belarus

Annotation. This paper introduces a DDoS attacks defense technique, which includes the measures for the four stages, such as pre-configuration, detection, blockage and mitigation. The DDoS defense technique is suggested for development of algorithms for defenses against various types of DDoS attacks applying the analysis of their OSI-level characteristics.

Keywords. DDoS-attacks, Defense Technique, OSI levels.

1.Analysis of DDoS attacks

A Distributed Denial of Service attack (DDoS) is a malicious attempt to flood a targeted server, service, or network with massive amounts of Internet traffic, disrupting its normal traffic and rendering it inaccessible to legitimate users. Unlike traditional denial-of-service (DoS) attacks, DDoS attacks utilize multiple infected computer systems as the source of the attack traffic, making defense more difficult. The general DDoS attack model is shown in Figure 1.

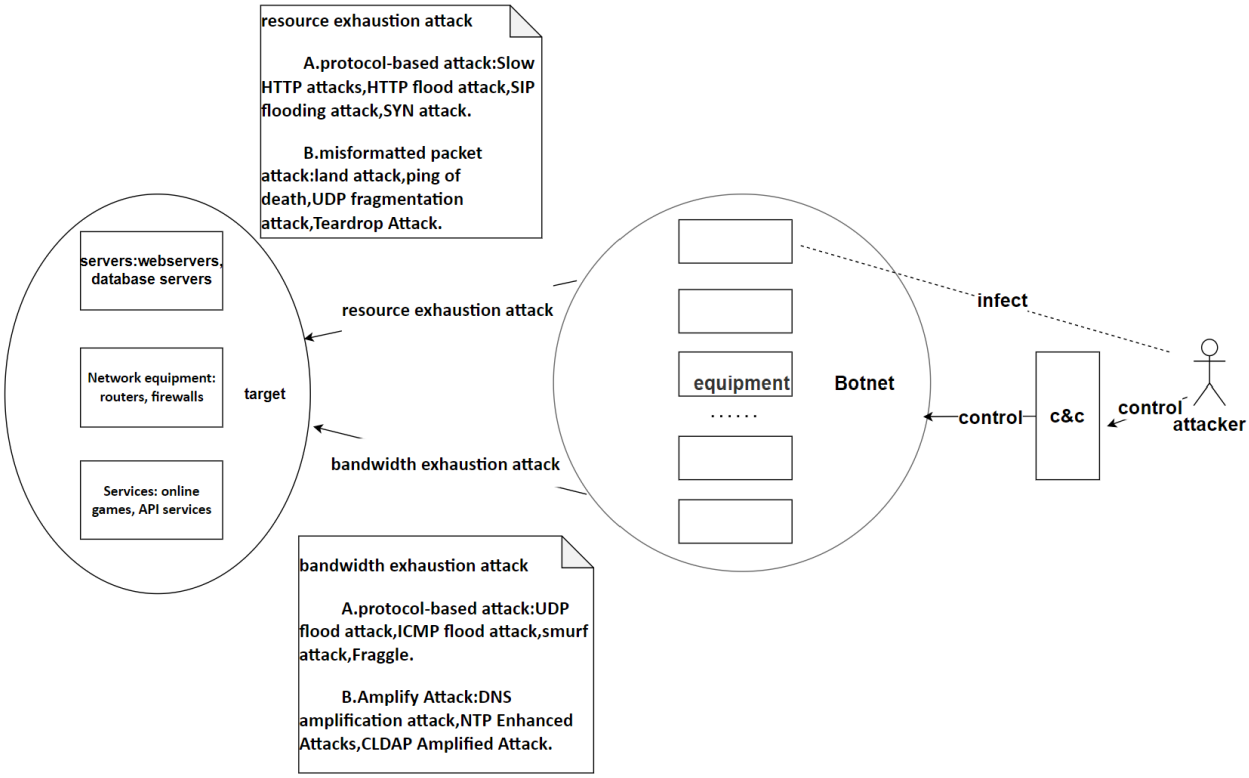


Figure 1 – General DDoS Attack Model

The DDoS attack model includes the parts of attacker, botnet, connection between attacker and botnet, attack channel, attack target, connection between attacker and target, and attack result.

Attackers include controllers as well as command and control servers, and controllers are usually the initiators of attacks, using a variety of tools and techniques to control large numbers of botnets. The attacker uses the command and control server to send commands to the controlled devices. Attackers infect a large number of devices with malware, turning them into botnets, which are often distributed across the globe, helping attackers hide their true origins.

Connection between attacker and botnet: Attackers infect a large number of devices in various ways. Incorporating them into a botnet. These devices may include personal computers, servers, IoT devices, etc. After infecting the devices, the attacker needs to install malware on the devices and create a control channel through which the attacker can remotely control these devices. The attacker manages and controls the botnet through a command and control server (C&C server). Communication between the attacker and the botnet typically uses encrypted or obfuscated protocols to avoid detection and

interception. Common communication protocols include IRC (Internet Relay Chat), HTTP, HTTPS, DNS, and others.

The attack channels include resource exhaustion attacks and bandwidth exhaustion attacks. Attack targets include servers (web servers, database servers, etc.), network devices (routers, firewalls, etc.), and services (online games, API services, etc.).

Connection between attacker and target: When an attacker initiates a DDoS attack, the C&C server sends commands to each device in the botnet in order to send a large number of requests to the target server. These requests may be HTTP requests, TCP connection requests, UDP packets, etc., depending on the type of attack. There are two results of the attack, either exhausting system resources or exhausting system bandwidth.

2.Classification of DDoS attacks

The OSI (Open Systems Interconnection) model categorizes network communications into seven layers, each with its own specific functions and protocols. DDoS attacks can be categorized based on the OSI layer they target. The classification of DDoS attacks with reference to the seven-layer network architecture is shown in Table 1.

Table 1 – Classification table for DDoS attacks

OSI level	Classification of attacks	Characteristics of the attack
data link layer	MAC Flood	ARP Spoofing Attackers launch DDoS attacks mainly by manipulating MAC addresses, ARP protocols, or switch forwarding logic, with the core objective of disrupting normal frame forwarding or exhausting link resources.
network layer	ICMP Flood IP Fragmentation Attack	Magnification effect Fake source IP Attackers mainly use IP protocol flaws and routing mechanisms to launch DDoS attacks and achieve damage by forging, amplifying, or exhausting target resources.
transport layer	SYN Flood attack UDP Flood attack ACK Flood attack	Halfway connection High flow rate and low power consumption Attackers primarily exploit TCP/UDP protocol flaws to launch DDoS attacks by exhausting connection resources or bandwidth.
session layer	Session Exhaustion Attack	Encryption overhead Session fixation attack Attackers mainly exploit vulnerabilities in the session management mechanism to launch DDoS attacks by exhausting encrypted resources, spoofing sessions, or maintaining malicious long connections.
presentation layer	SSL/TLS Flood attack	data malformation Attackers mainly use vulnerabilities in data format parsing, encryption/decryption process or encoding conversion to launch DDoS attacks and consume target system resources by constructing malformed data.
	DNS Flood Attack	low-flow, high-kill Protocol Abuse Precise targeting

application layer	DNS Reflex Attack HTTP Flood attack Slowloris attack CC attack	Attackers usually spoof the source IP, mimic legitimate traffic, and take advantage of protocol design flaws to exhaust the resources of the attack target with low traffic and high kills.

3. DDOS attack defense technique

DDoS attack is a complex network security threat that requires a comprehensive defense from multiple perspectives [1]. The principle mechanism of defense against various attacks generally includes the four steps, such as pre-configuration of the system to be protected, detection of attacks [2], blockage of attacks and mitigation the consequences of the attacks. In relation to DDoS attacks this mechanism was transformed into a defense technique against DDoS attack, which includes the following measures, shown in Figure 2.

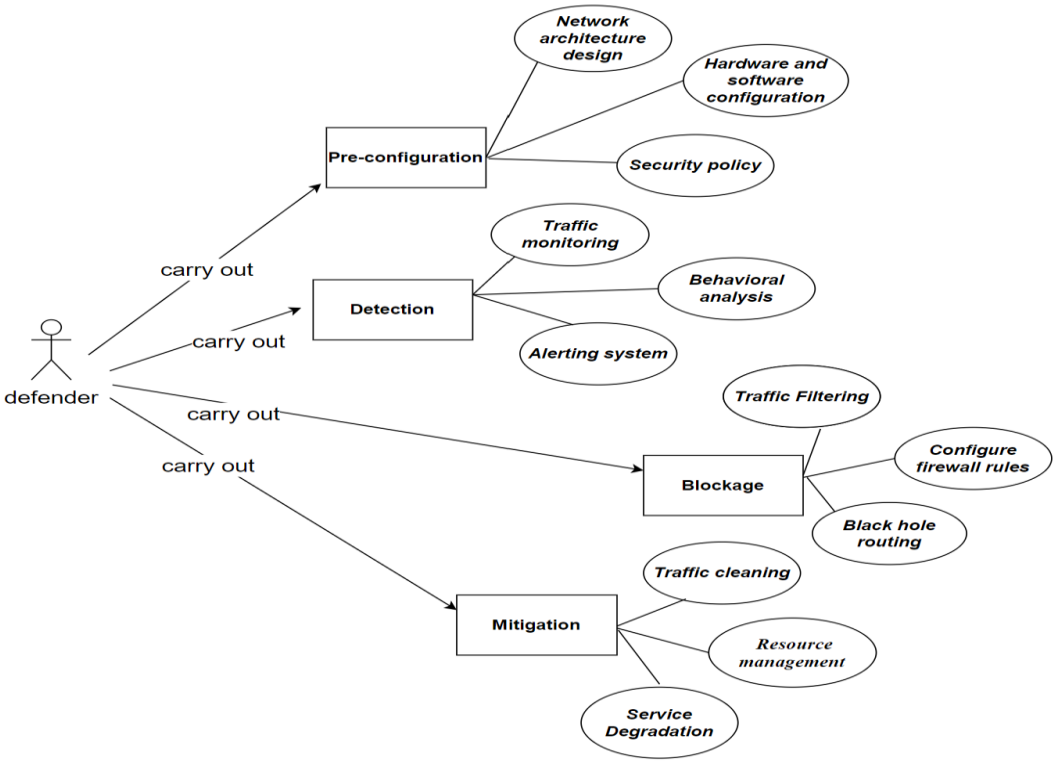


Figure 2 – Step-by-step diagram for DDoS defense technique implementation

1. Pre-configuration.

Network architecture design: deploy multiple servers and multiple data centers to disperse traffic pressure; use load balancers to evenly distribute traffic to multiple servers to avoid a single point of failure; distribute content via CDN to reduce direct access to the source server.

Hardware and software configuration: Enable firewall rules to filter abnormal traffic; configure routers to limit the traffic rate of protocols such as ICMP, UDP, etc.; optimize server configurations to improve processing power (e.g., increase connection limits, enable SYN cookies).

Security policy: Limit access to critical services and allow access only to trusted IP addresses; disable unnecessary protocols (e.g., ICMP, UDP) to reduce the attack surface; and update operating systems and applications in a timely manner to patch known vulnerabilities.

2. Detection.

Detecting DDoS attacks in real time is the first step in defense, and through early detection action can be taken quickly[3].

Traffic monitoring: establish a baseline of normal traffic and monitor traffic changes in real time; use tools (e.g., NetFlow, sFlow) to detect traffic anomalies (e.g., traffic spikes, abnormal protocol ratios).

Behavioral analysis: Identify abnormal behavior (e.g., a large number of requests coming from the same IP address) by analyzing user behavioral patterns; detect complex attack patterns using machine learning algorithms.

Alerting system: Setting traffic thresholds and triggering alerts when the traffic exceeds the thresholds; analyzing server logs regularly to find signs of potential attacks.

3. Blockage.

After a DDoS attack is detected, rapid measures are taken to block the attack traffic and reduce the impact on the target system.

Traffic Filtering: Add the source IP address of the attack to the blacklist and block its access; filter abnormal protocol traffic (e.g. ICMP Flood, UDP Flood); block traffic from a specific region based on the geographic location of the IP address[4].

Configure firewall rules to filter malicious traffic; utilize Intrusion Detection Systems (IDS) to detect and report attack traffic in real time; utilize Intrusion Prevention Systems (IPS) to automatically block detected attack traffic.

Black hole routing: direct attack traffic to the "black hole" to avoid affecting the target server; dynamically adjust black hole routing rules according to traffic conditions.

4. Mitigation.

While blocking attack traffic, take steps to mitigate the impact of the attack on the system and ensure service availability.

Traffic cleaning: Use professional DDoS protection services (e.g. Cloudflare, Akamai) to filter malicious traffic; deploy local traffic cleaning equipment to filter attack traffic in real time[5].

Resource management: Dynamically adjust resource allocation and prioritize the operation of critical services; in a cloud environment, resources are automatically expanded based on traffic.

Service Degradation: Temporarily shut down non-critical services during an attack and focus resources on securing core services.

The **algorithm for defenses against SYN Flood-type attacks** was developed according to the general technique described above and the OSI-level characteristics for this type of attacks. The algorithm is shown below:

For the Pre-configuration stage:

1.Enable SYN Cookie: Instead of allocating resources immediately upon receiving a SYN request, the server generates a SYN cookie (a hash containing connection information) as a SYN-ACK response. Only after receiving a legitimate ACK response does the server allocate resources.

Firewall Configuration: Configure rules on the firewall to limit the rate of SYN requests per IP address.

For the Detection stage:

2.Analyze the source IP address of SYN requests to identify abnormal behavior (e.g., a large number of SYN requests coming from the same IP address); monitor the status of the server's half-connection queue to find out when the half-connection queue is full.

Sets the threshold for SYN requests and triggers an alert when a SYN request exceeds the threshold.

For the Blockage stage:

3.Using a SYN proxy device, the proxy server handles SYN requests and filters malicious traffic. Utilizes Intrusion Detection System (IDS) to detect and report SYN Flood attack traffic in real-

time. Using Intrusion Prevention System (IPS), automatically blocking detected SYN Flood attack traffic.

For the Mitigation stage:

4.Switch dynamic websites to static pages to reduce server load; during an attack, temporarily shut down non-critical services and focus resources on safeguarding core services.

The DDoS defense technique is suggested for development of algorithms for defenses against various types of DDoS attacks applying the analysis of their OSI-level characteristics. The proposed defense algorithm against SYN flooding attack is tested in the lab environment, and it is found that the half-connection queue occupancy rate decreases by more than 80% and there is no queue overflow record in the kernel logs, the success rate of TCP connection establishment for normal users increases, and the attacking traffic is significantly reduced, which proves that the algorithm is effective.

List of references

1. Li Xiaoyong,Liu Dongxi,Gu Dawu,et al.Research on DDoS Defense and Response Technology[J]. Computer Engineering and Application, 2003, 39(12):4. DOI:10.3321/j.issn:1002-8331.2003.12.018.

2. Han Zhu,Fan Lei,Li Jianhua. DDoS defense mechanism based on source detection[J]. Computer Engineering, 2007, 33(19):150-151. DOI:10.3969/j.issn.1000-3428.2007.19.052.

3. Shang Zhanfeng,Zhang Dengyi.Research on DDoS defense mechanism[J]. Computer Technology and Development, 2008, 18(1):7-10.DOI:10.3969/j.issn.1673-629X.2008.01.002.

4. Wang Hui. A method and device for detecting forged source IPs in a DDOS defense system.2017[2025-03-27].

5. Wang, Xiaoling. Design and implementation of a DDoS defense system using source address information[J]. Journal of Southwest University for Nationalities:Natural Science Edition, 2015(41):467.

VALIDATION OF ORB-SLAM2'S APPLICABILITY ACROSS SCENARIOS

Fang Yixuan[1], Wang Guoyan[1], Fan Hongqi[1]

National Key Laboratory of Automatic Target Recognition, College of Electronic Science and Technology, National University of Defense Technology, Changsha 410073, China

Fang Yixuan – Master in Information and Communication Engineering

Wang Guoyan – PHD in Technical Sciences, Lecturer

Fan Hongqi – PHD in Technical Sciences, Research Professor

Annotation. This paper investigates the applicability of the ORB-SLAM2 across diverse scenarios based on 51 sequences from three public datasets: TUM RGB-D, EuRoC, and KITTI. Experimental results reveal that while ORB-SLAM2 demonstrates strong robustness in dynamic environments, its performance significantly deteriorates when encountering textureless regions, intense camera rotation, or extensive planar areas. In most cases within the same scenario, the stereo configuration achieves higher localization accuracy than the monocular mode. This study provides practical references for scene-specific adaptability considerations in SLAM technology applications.

Keywords. *ORB-SLAM2, dynamic environments, monocular, stereo, localization accuracy*

I. Introduction

Simultaneous Localization and Mapping (SLAM), proposed by Smith R.C. and Cheeseman P. in 1986 [1], is a technology that enables an agent equipped with specific sensors to construct environmental models and estimate its own motion in real time without prior environmental knowledge [2]. Based on sensor types, SLAM can be categorized into Visual SLAM (VSLAM) [3]

using cameras and LiDAR-based SLAM [4] using light detection and ranging sensors. This study focuses on monocular and stereo camera-based VSLAM systems.

The evolution of VSLAM has witnessed significant algorithmic advancements. Early monocular SLAM systems primarily relied on filter-based methods [5],[6],[7],[8], which faced challenges such as high computational complexity and error accumulation. A milestone was the Parallel Tracking and Mapping (PTAM) [9] algorithm, which pioneered a keyframe-based architecture by decoupling feature tracking and map construction into parallel threads. Subsequent improvements to PTAM included the integration of edge features and enhanced relocalization techniques [10]. Among feature-based SLAM systems [5], ORB-SLAM2 [11] emerged as a representative solution due to its rapid ORB [12] feature extraction and rotation invariance, achieving high operational efficiency and stability.

However, existing research lacks systematic validation of ORB-SLAM2's applicability in complex scenarios, such as dynamic environments, weakly textured regions, and large-scale planar surfaces. This study aims to address these gaps through multi-scenario experiments, specifically:

1) Robustness analysis in dynamic environments;

2) Comparative evaluation of localization accuracy between monocular and stereo modes across diverse environments;

3) Identification of limitations in textureless areas, rapid rotational motion, and expansive planar scenes.

II. System Overview

The ORB-SLAM2 system comprises three parallel threads: Tracking, Local Mapping, and Loop Closing, as illustrated in Figure 1.

The Tracking thread is responsible for searching feature correspondences between each frame and the local map to compute the corresponding camera pose. Based on this computation, it determines whether to appropriately insert a new keyframe into the keyframe buffer queue of the Local Mapping thread. In monocular mode, the system initializes the map through parallel computation of both the homography matrix suitable for planar scenes and the fundamental matrix applicable to non-planar scenes [13], selecting the optimal solution via RANSAC [14].Within the tracking thread, preliminary feature matching is first performed between the received current frame and its preceding frame. Subsequently, a motion-only Bundle Adjustment (BA) [15] algorithm is employed to optimize and refine the pose estimation of the current frame.

The Local Mapping thread manages the construction process of the local map and executes all BA optimizations related to the local map. This thread processes newly inserted keyframes from the Tracking Thread. Its core task is to perform local BA optimization to achieve optimal reconstruction of the surrounding environment under the current camera pose constraints.

The Loop Closing Thread detects large-scale loops and corrects accumulated drift through pose graph optimization. For each newly inserted keyframe from the Local Mapping Thread, this thread performs loop detection to verify loop formation. It constructs a place recognition database based on the DBoW2 [16] vocabulary model, while enhancing loop detection accuracy through covisibility graph-optimized candidate keyframe selection strategy. When a loop closure is detected, the system computes the relative geometric transformation (similarity transformation [17]) between the current keyframe and the identified loop-closing keyframe.

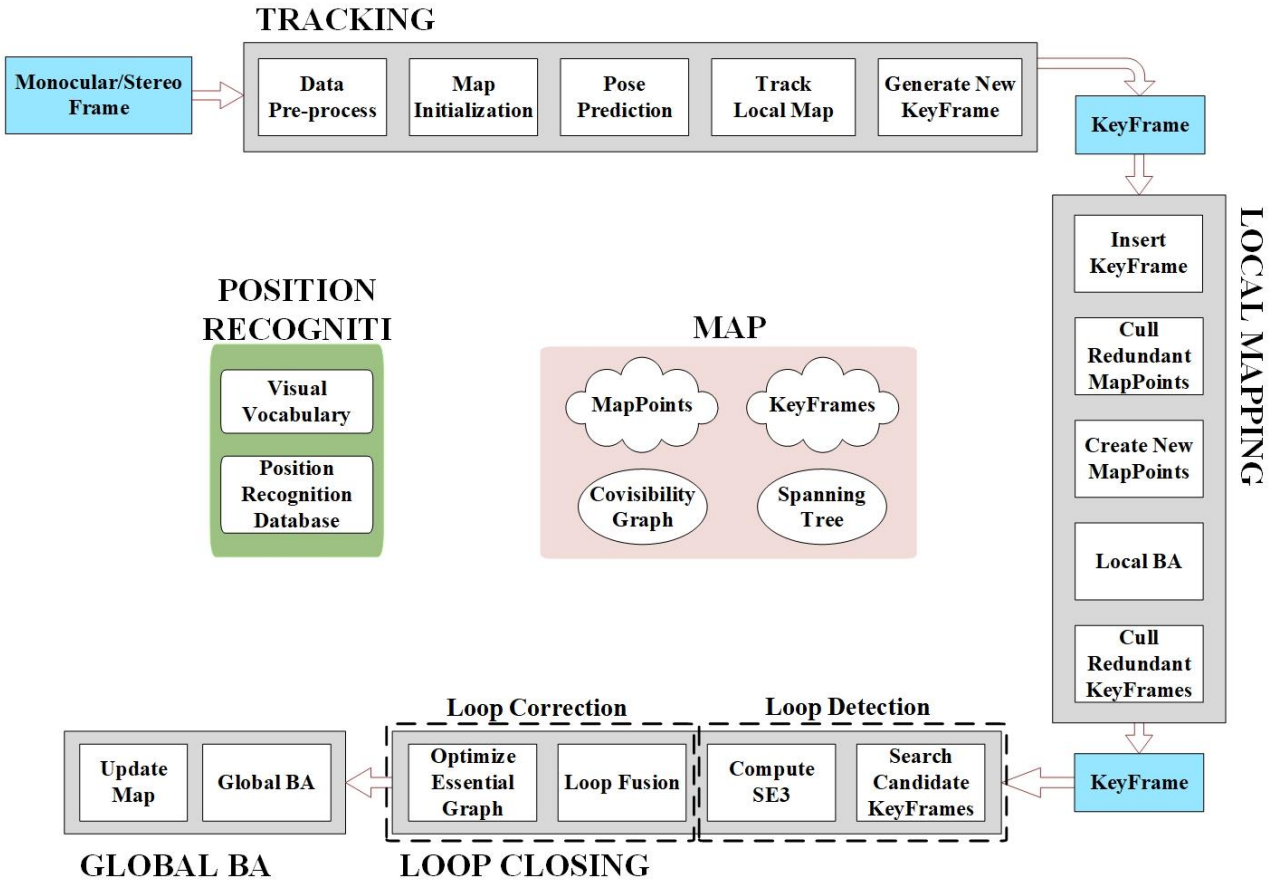


Figure 1 – ORB-SLAM2 system overview

III. Experimental Design and Analysis

The experiments were conducted on an Intel(R) Core(TM) i9-14900HX processor (2.20 GHz, x64-based) within an Ubuntu 18.04 virtual environment hosted by VMware Workstation Pro 17 on Windows 11.

Three public datasets – TUM RGB-D [18], EuRoC [19], and KITTI **Error! Reference source not found.** – were utilized to evaluate system performance. Key evaluation metrics include:

Absolute Trajectory Error (ATE), as shown in Equation (1).

$$ATE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\|trans(F_i)\|^2} \quad (1)$$

where N is the total number of trajectory points, F_i is the absolute error at i-th trajectory point, expressed as $F_i = \mathrm{Q}_i^{-1} S \mathrm{P}_i$ (with Q_i being the ground-truth pose at the i-th point, P_i being the estimated pose at the i-th point, and S being the rigid transformation aligning estimated and ground-truth trajectories), $trans(F_i)$ denotes the translational component of F_i.

Relative Pose Error (RPE), as shown in Equation (2).

$$RPE = \sqrt{\frac{1}{m}\sum_{i=1}^{m}\|trans(E_i)\|^2} \quad (2)$$

where $m = N - \Delta$ is the number of available relative pose error samples, E_i is the relative pose error at the i-th point, expressed as $E_i = (\mathrm{Q}_i^{-1}Q_{i+\Delta})^{-1}(\mathrm{P}_i^{-1}P_{i+\Delta})$ (with Q_i and $Q_{i+\Delta}$ being the ground-truth poses at points i and $i+\Delta$, and P_i and $P_{i+\Delta}$ being the estimated poses at points i and $i+\Delta$), $trans(E_i)$ denotes the translational component of E_i.

To ensure the reliability of the results, each sequence in all datasets was run five times, and the median of the five results was taken as the error value.

A. TUM RGB-D Dataset

This paper uses 29 sequences from the TUM RGB-D dataset, including Handheld SLAM, Dynamic Objects, Structure vs. Texture, and Robot SLAM sequences, to conduct a detailed analysis of the monocular mode of ORB-SLAM2. The evaluation metric is the ATE.

The validation results for the Handheld SLAM sequences are presented in Table 1.

Table 1 – Handheld SLAM Sequences of the TUM RGB-D Dataset

Sequence	Description			RMSE(cm)
	Avg. translational velocity (m/s)	Avg. angular velocity (deg/s)	with loop	
fr1_floor	0.258	15.071	No	1.737
fr1_desk	0.413	23.327	No	1.360
fr1_room	0.334	29.882	Yes	6.085
fr2_360_kidnap	0.304	13.425	No	4.154
fr2_desk	0.193	6.338	Yes	0.860
fr3_long_office	0.249	10.188	Yes	1.098
fr1_360	0.210	41.600	No	5.791
fr2_360_hemisphere	0.163	20.569	No	9.335

As shown in Table 1, the monocular mode of ORB-SLAM2 achieved an absolute trajectory error of approximately 1 cm in most Handheld SLAM sequences, except in scenarios with strong camera rotation (fr1_room, fr2_360_kidnap, fr1_360, and fr2_360_hemisphere).

The results for the Dynamic Objects sequence (an office scenario) are shown in Table 2.

Table 2 – Dynamic Objects Sequences of the TUM RGB-D Dataset

Sequence	Description	RMSE(cm)
fr2_desk_person	Interaction	0.743
fr3_sit_static	Two people sitting at a desk interacting, Asus Xtion fixed	\
fr3_sit_xyz	Two people sitting at a desk interacting, Asus Xtion moving along xyz	0.932
fr3_sit_halfsph	Two people sitting at a desk interacting, Asus Xtion moving along a half-sphere trajectory	1.693
fr3_sit_rpy	Two people sitting at a desk interacting, Asus Xtion moving along rpy with strong rotation	\
fr3_walk_static	Two people walking, Asus Xtion fixed	\
fr3_walk_xyz	Two people walking, Asus Xtion moving along xyz	\
fr3_walk_halfsph	Two people walking, Asus Xtion moving along a half-sphere trajectory	1.675
fr3_walk_rpy	Two people walking, Asus Xtion moving along rpy with strong rotation	7.300

From the results in Table 2, the monocular mode of ORB-SLAM2 achieved an absolute trajectory error of less than 2 cm in most Dynamic Object sequences, except in scenarios with strong camera rotation (fr3_sit_rpy and fr3_walk_rpy) and camera stationary (fr3_sit_static and

fr3_walk_static). This indicates that the system is robust to dynamic objects in monocular mode, except when the camera undergoes strong rotation and stationary.

The validation results for the Structure vs. Texture sequences are presented in Table 3.

Table 3 – Structure vs. Texture Sequences of the TUM RGB-D Dataset

Sequence	Description	RMSE(cm)
fr3_nstr_tex_far	planar, texture	9.249
fr3_nstr_tex_near	planar, texture, with loop	1.363
fr3_str_tex_far	non-planar, texture	0.922
fr3_str_tex_near	non-planar, texture	1.358
fr3_nstr_ntex_far	planar, textureless	\
fr3_nstr_ntex_near	planar, textureless, with loop	\
fr3_str_ntex_far	non-planar, textureless	\
fr3_str_ntex_near	non-planar, textureless, with loop	\

From the results in Table 3, the monocular mode of ORB-SLAM2 failed to complete initialization in textureless scenes (fr3_nstr_ntex_far, fr3_nstr_ntex_near, fr3_str_ntex_far and fr3_str_ntex_near).

However, in the Robot SLAM sequences, although the camera was not in a state of strong rotation, most sequences failed to initialize. The validation results are shown in Table 4.

Table 4 – Robot SLAM Sequences of the TUM RGB-D Dataset

Sequence	Description	RMSE(cm)
fr2_pioneer_360	warehouse, large-scale planar	\
fr2_pioneer_slam	warehouse, large-scale planar, with loop	5.038
fr2_pioneer_slam2	warehouse, large-scale planar	\
fr2_pioneer_slam3	warehouse, large-scale planar	\

By analyzing the commonalities of the Robot SLAM sequences, it is evident that such sequences often involve large-scale planar environments. Additionally, in sequences with loops (fr1_room, fr2_desk, fr3_long_office, and fr3_nstr_tex_near), the system achieved a trajectory error of approximately 1 cm, indicating strong loop closure handling capabilities.

ORB-SLAM2 demonstrated a trajectory error of less than 10 cm across all 29 sequences of the TUM RGB-D dataset. The validation results from the TUM RGB-D dataset confirm that ORB-SLAM2 is robust in dynamic scenes and effective in handling loop closures. However, it is not suitable for textureless scenes, scenarios with significant camera rotation, or scenes containing extensive planar structures.

B. EuRoC Dataset

This paper analyzed 11 sequences of the EuRoC dataset, categorized into easy, medium, and difficult levels. The ATE of the trajectory for each sequence is presented in Table 5.

Table 5 – Results of the EuRoC Dataset

Sequence	RMSE(cm)	
	Monocular	Stereo
MH_01_easy	4.510	3.759
MH_02_easy	3.423	3.754
MH_03_medium	3.958	3.733
MH_04_difficult	7.228	12.496
MH_05_difficult	6.986	5.730
V1_01_easy	9.551	8.638
V1_02_medium	5.094	6.040
V1_03_difficult	9.787	9.753
V2_01_easy	6.080	7.097
V2_02_medium	6.048	5.920

V2_03_difficult	22.309	19.299

As shown in Table 5, in the indoor EuRoC dataset, ORB-SLAM2 showed comparable performance in both monocular and stereo modes, with most sequences achieving a trajectory error of less than 10 cm, except for the V2_03_difficult sequence. This level of positioning accuracy is sufficient for small drones used in environmental exploration.

C. KITTI Dataset

This paper analyzed 11 sequences (00 to 10) of the KITTI dataset. In addition to calculating the ATE (t_{abs}) and RPE (t_{rel}), the relative rotational error (r_{rel}) was also computed. Table 6 presents the specific results for the 11 sequences of the KITTI dataset.

Table 6 – Results of the KITTI Dataset

Sequence	$m \times m$	Monocular			Stereo		
		$t_{rel}(\%)$	$r_{rel}(deg/100m)$	$t_{abs}(m)$	$t_{rel}(\%)$	$r_{rel}(deg/100m)$	$t_{abs}(m)$
00	564×496	5.230	0.946	**7.542**	1.094	0.689	**1.288**
01	1157×1827	153.859	0.929	**533.562**	1.698	0.359	**9.623**
02	599×946	14.228	0.647	**33.502**	1.116	0.495	**5.841**
03	471×199	1.277	0.302	**0.967**	0.950	0.365	**0.755**
04	0.5×394	0.588	0.308	**0.989**	0.445	0.310	**0.187**
05	479×426	5.165	0.506	**5.367**	0.632	0.352	**0.720**
06	23×457	9.799	0.418	**13.413**	0.699	0.300	**0.784**
07	191×209	3.809	0.603	**2.127**	0.567	0.392	**0.526**
08	808×391	32.224	0.674	**52.889**	1.301	0.659	**3.721**
09	465×568	4.949	0.719	**4.858**	0.916	0.484	**3.291**
10	671×177	7.446	0.509	**8.444**	0.881	0.474	**0.100**

As shown in Table 6, in monocular mode, the trajectory error of ORB-SLAM2 is typically around 1% of the map size (sequences 00, 05, 07, 09, and 10), sometimes lower—such as 0.21% for sequence 03 and 0.25% for sequence 04—or higher, like 3.54% for sequence 02, 2.94% for sequence 06, and 6.55% for sequence 08. In stereo mode, the trajectory error is consistently less than 1% of the map size. This indicates that, in most cases, stereo mode provides higher localization accuracy than monocular mode in the same scenario.

IV. Conclusion

This paper provides an extensive experimental evaluation of the ORB-SLAM2 algorithm to determine its applicability across different environments. The results show that the ORB-SLAM2 system operates effectively in both indoor and outdoor settings, demonstrates robustness in dynamic scenes, and handles loop closures well. However, it performs poorly in textureless environments, scenarios with strong camera rotation, and scenes featuring large-scale planar surfaces. In most cases, the stereo mode achieves higher localization accuracy than the monocular mode in the same scenario. This study offers practical insights into the environmental adaptability of SLAM technology.

References

[1] On the representation and estimation of spatial uncertainty / R. C. Smith [et al.] // The International Journal of Robotics Research, 1986. – P.56-68.

[2] A State of the Art in Simultaneous Localization and Mapping (SLAM) for Unmanned Ariel Vehicle (UAV): A Review / A. Rauf [et al.] // Electrical, Control and Communication Engineering, 2022. – P.50-56.

[3] Visual SLAM: What are the Current Trends and What to Expect? / A. Tourani [et al.] // Sensors, 2022. – P.9297.

[4] A Comparison of Modern General-Purpose Visual SLAM Approaches / A. Merzlyakov [et al.] // Proceedings of the 2021 IEEE/RSJ International Conference on Intelligent Robots and Systems, 2021. – P.9190-9197.

[5] MonoSLAM: real-time single camera SLAM / A. J. Davison [et al.] // IEEE Transactions on Pattern Analysis and Machine Intelligence, 2007. – P.1052-1067.

[6] Inverse Depth Parametrization for Monocular SLAM / J. Civera [et al.] // IEEE Transactions on Robotics, 2008. – P.932-945.

[7] Structure from motion causally integrated over time / A. Chiuso [et al.] // IEEE Transactions on Pattern Analysis and Machine Intelligence, 2002. – P.523-535.

[8] Scalable Monocular SLAM / E. Eade [et al.] // Proceedings of the 2006 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2006. – P.469-476.

[9] Parallel Tracking and Mapping for Small AR Workspaces / G. Klein [et al.] // Proceedings of the 2007 IEEE and ACM International Symposium on Mixed and Augmented Reality, 2007. – P.225-234.

[10] Improving the Agility of Keyframe-Based SLAM / G. Klein [et al.] // Proceedings of the 2008 European Conference on Computer Vision, 2008. – P.802-815.

[11] ORB-SLAM2: an Open-Source SLAM System for Monocular,Stereo and RGB-D Cameras / R. Mur-Artal[et al.] // IEEE Transactions on Robotics, 2017. – P. 1255-1262.

[12] ORB: an efficient alternative to SIFT or SURF / E. Rublee [et al.] // IEEE International Conference on Computer Vision, 2011. – P.2564–2571.

[13] ORB-SLAM: A Versatile and Accurate Monocular SLAM System / R. Mur-Artal [et al.] // IEEE Transactions on Robotics, 2015. – P. 1147-1163.

[14] Random Sample Consensus: A Paradigm for Model Fitting with Applications to Image Analysis and Automated Cartography / M. A. Fischler [et al.] // Communications of the Association for Computing Machinery, 1987. – P.726-740.

[15] Bundle adjustment a modern synthesis / B. Triggs [et al.] // Vision algorithms: theory and practice, 2000. – P.298–372.

[16] Bags of Binary Words for Fast Place Recognition inImage Sequences / D. Galvez-Lpez [et al.] // IEEE Transactions on Robotics, 2012, . – P.1188-1197.

[17] Scale drift-aware large scale monocular SLAM / H. Strasdat [et al.] // Robotics: Science and Systems, 2010. – P.73-80.

[18] A benchmark for the evaluation of RGB-D SLAM systems / J. Sturm [et al.] // Proceedings of the 2012 IEEE/RSJ International Conference on Intelligent Robots and Systems, 2012. – P.573-580.

[19] The EuRoC micro aerial vehicle datasets / M. Burri [et al.] // International Journal of Robotics Research, 2016. – P.1157-1163.

Vision meets robotics: The KITTI dataset / A. Geiger [et al.] // International Journal of Robotics Researc, 2013. – P.1231-1237.

УДК 621.317.08

МЕТОДИКИ ДИСТАНЦИОННОЙ КАЛИБРОВКИ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНОЙ СИСТЕМЫ СВЧ ДИАПАЗОНА

Зокиров Д.Т. гр.426401

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь
Научный руководитель: д-р тех. наук, профессор Гусинский А.В.

Аннотация. В материалах доклада рассматривается разработанная методика дистанционной калибровки информационно-измерительной системы СВЧ диапазона

Ключевые слова: дистанционная калибровка, информационно-измерительная система, сверхвысокая частота, метрологические характеристики

Введение. Одним из основных инструментов для измерений частотных характеристик комплексных параметров отражения и передачи сверхвысокочастотных (СВЧ) и крайне высокочастотных (КВЧ) устройств являются информационно-измерительные системы (ИИС) [1].

На сегодняшний день эти ИИС широко применяются при проведении измерений параметров

антенн, полупроводниковых устройств, активных устройств (усилители, смесители, умножители и делители частоты) и пассивных устройств (кабели, соединители, линии передачи).

Использование современных информационных технологий для передачи измерительной информации позволяет осуществлять дистанционные исследования метрологических характеристик (МХ) ИИС. Исключается необходимость периодически посылать ИИС в метрологическую службу для проведения поверки, калибровки, т.к. измерительная информация будет доступна метрологической службе с любого стационарного компьютера, подключенного к сети Internet.

В докладе рассматривается разработанная методика дистанционной калибровки ИИС СВЧ диапазона.

Основная часть. Для рассматриваемой информационно-измерительной системы характерно не только автоматизация таких процедур как регистрация, сбор и передача результатов измерений на обработку, но и возможности дистанционного проведения измерительного эксперимента при активном воздействии на объект исследования, оперативной передачи данных исследований и измерений по локальным и глобальным компьютерным сетям (Internet). Следовательно, имеется техническая возможность проведения дистанционной калибровки системы путем реализации технологии «клиент - сервер».

Система дистанционной калибровки предназначена для управления процессом измерений, подачи эталонных сигналов на калибруемое СИ, наблюдения за его реакцией и обработки результатов. Она требует соединения между персональным компьютером (ПК) калибровочной лаборатории (КЛ) и ПК с калибруемым средством измерении (СИ), воспроизведения физических величин с помощью эталонных СИ и возможности дистанционного управления. Также предполагается передача измерительной информации, оценка калибровочных характеристик и гибкость в соответствии с новыми задачами.

Технической основой метода являются транспортабельные эталонные меры (ТЭМ), которые должны обеспечивать необходимую точность. Система включает три главные компонента: специализированное программное обеспечение (ПО), калибруемое СИ и ТЭМ.

На рисунке 1. представлена обобщенная структурная схема системы дистанционной калибровки ИИС.

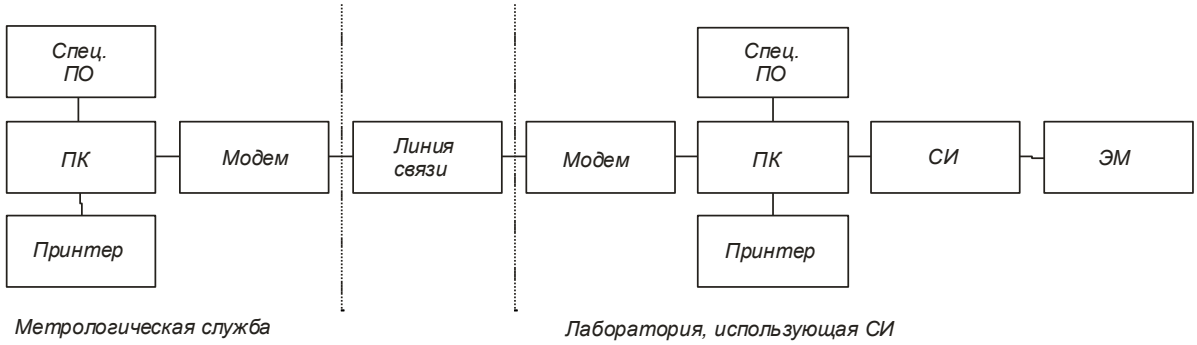


Рисунок 1 - Обобщенная структурная схема системы дистанционной калибровки

ПО калибровочной лаборатории управляет СИ, устанавливает диапазоны и режимы измерения, а также сохраняет результаты в базе данных, доступной для клиента. Клиент может просматривать данные и использовать их для проведения измерений. Функции ПО позволяют отображать данные, приостанавливать и перезапускать измерения, а информация сохраняется на сервере лаборатории.

Алгоритм дистанционной калибровки основывается на технологии "клиент-сервер". Лаборатория оформляет заявку на калибровку, после чего в КЛ доставляются необходимые эталонные меры. Устанавливается специализированное ПО на ПК КЛ и ПК, подключенной к исследуемому СИ.

Сервер переводится в режим ожидания, устанавливается соединение между ПК КЛ и лабораторным ПК. Проводится опробование системы дистанционной калибровки, с проверкой работоспособности калибруемого СИ. После самодиагностики, информация о состоянии СИ передается на ПК КЛ.

Выбираются исследуемый параметр, метод измерений, математическая обработка и эталонные меры. Лаборатория подключает эталонные и вспомогательные СИ согласно схеме измерений. Устанавливается частота калибровки, затем подготавливается калибруемое СИ.

На лабораторном ПК отправляется команда подключения исследуемого СИ, проводятся измерения и расчеты параметров с учетом характеристик СИ, оценивается неопределенность измерений. На основе полученных данных составляется свидетельство о поверке и протокол, который содержит информацию о СИ, условиях калибровки и результаты измерений.

На рисунке 2. представлен разработанный алгоритм дистанционной калибровки ИИС.

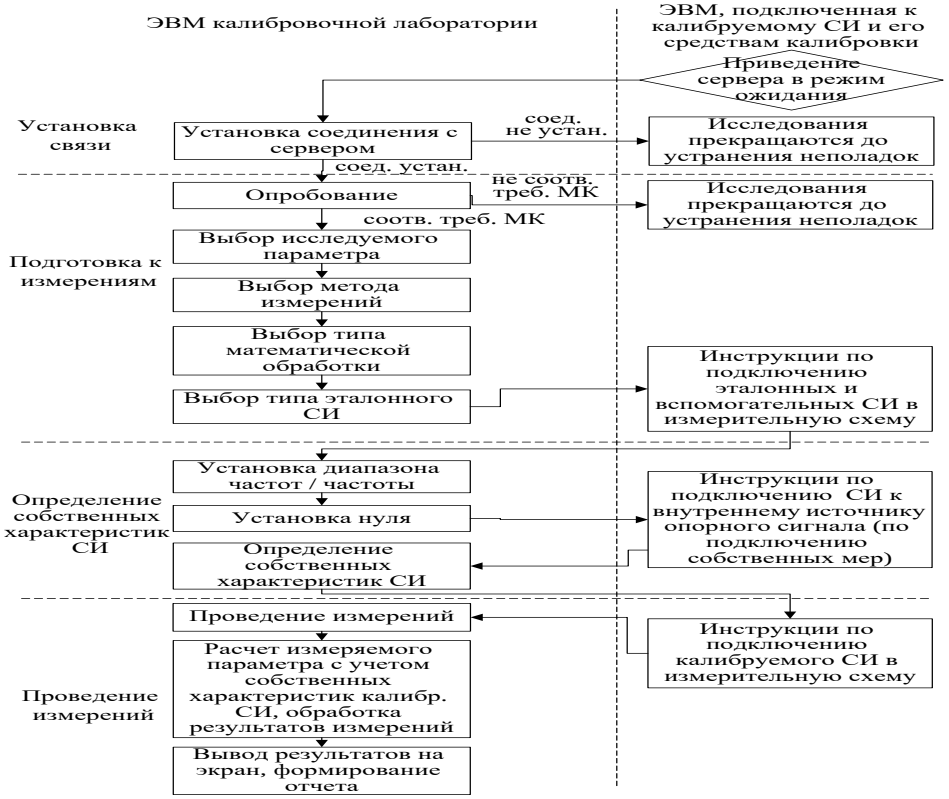


Рисунок 2 - Алгоритм проведения дистанционной калибровки

Структура ПО дистанционной калибровки ИИС включает блоки для управления измерительными средствами, функциональности КОП, вычислений, вывода информации и выполнения вспомогательных операций. Механизм "клиент-сервер" работает на протоколе TCP/IP, поддерживаемом локальными сетями, модемами и Интернетом.

Для дистанционных измерений ПО обеспечивает соединение между ПК КЛ и ПК, подключенным к калибруемому СИ. Сначала инициализируется серверная часть ПО (*Server.exe*), выполняется проверка всех подключенных измерительных устройств. Если приборы работают некорректно, выводится соответствующее сообщение. Затем сервер ждёт запросов клиента. Сотрудник лаборатории может остановить сервер и перевести его в режим ожидания.

Клиентская часть ПО (*Client.exe*) инициализируется сотрудником КЛ. Она проверяет соединение с сервером и, если его нет, переходит в режим ожидания. Параметры соединения настраиваются вручную. После установления связи сервер сохраняет информацию о новом клиенте и обслуживает запросы по очереди. После установки постоянного соединения между сервером и клиентом осуществляется обмен данными, включая запрос на начало измерений.

Алгоритм установки соединения реализован в СВЧ-измерительных приборах, разработанных БГУИР. Для разработки ПО используется LabVIEW, позволяющий визуально конструировать алгоритмы и обеспечивающий поддержку различных интерфейсов и протоколов. LabVIEW интегрируется с модулями, разработанными на традиционных языках программирования, что обеспечивает гибкость в разработке автоматизированных систем.

Заключение. Система дистанционной калибровки ИИС представляет собой современное решение, обеспечивающее эффективное управление процессом измерений и калибровки. Использование механизма "клиент-сервер" на базе протоколов TCP/IP позволяет осуществлять надежное соединение между лабораторными ПК и калибруемыми средствами измерений, что способствует более гибкому и быстрому обмену данными.

Разработка специализированного программного обеспечения на платформе LabVIEW обеспечивает не только высокую функциональность, но и возможность интеграции с различными аппаратными средствами и интерфейсами. Эта система калибровки значительно упрощает процесс, повышает точность измерений и позволяет оперативно вести учет результатов, доступных для клиентов.

Список литературы

1. *Богуш, В.А. Векторные анализаторы цепей сантиметрового и миллиметрового диапазонов длин волн / В.А. Богуш [и др.]. – Москва: Горячая линия–Телеком, 2019. – 328 с..*

UDC 621.317.08

METHODOLOGIES FOR DISTANCE CALIBRATION OF MICROWAVE RANGE INFORMATION AND MEASUREMENT SYSTEMS

Zokirov D.T.. gr.426401

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Doctor of Technical Sciences, Professor Gusinsky A.V.

Annotation. The report materials discuss the developed methodology for distance calibration of the microwave range information and measurement system.

Keywords: distance calibration, information and measurement system, superhigh frequency, metrological characteristics.

УДК 621.317.08

МЕТОДИКА ОПРЕДЕЛЕНИЯ ПАРАМЕТРОВ ИСТОЧНИКА СИГНАЛА ИЗ СОСТАВА НАЦИОНАЛЬНОГО ЭТАЛОНА ЕДИНИЦЫ МОЩНОСТИ

Доронина А.В. гр. 467241
Белорусский государственный университет информатики и радиоэлектроники,
г.Минск, Республика Беларусь

Научный руководитель: Белошицкий А.П., кандидат технических наук, доцент

Аннотация. *В материалах доклада рассматривается разработанная методика определения параметров источников сигнала из состава эталона единицы мощности электромагнитных колебаний в диапазоне частот от 37,5 до 178,4 ГГц.*
Ключевые слова: *методика исследования, источник сигнала, параметры, сверхвысокая частота, эталон, мощность*

Введение. Современные достижения в области метрологии стимулируют развитие и совершенствование эталонов, обеспечивающих единство измерений в миллиметровом диапазоне частот. Одним из ключевых направлений становится обеспечение высокой точности измерений мощности электромагнитных волн, что связано с растущими требованиями к метрологическим характеристикам приборов, предназначенных для измерения данной величины. В Центре 1.9 НИЧ БГУИР был разработан и изготовлен национальный эталон единицы мощности в диапазоне частот от 37,5 до 178,4 ГГц [1].

В докладе приведено описание и принцип работы эталонного оборудования, а также методика исследования параметров источников сигнала из состава эталона в диапазоне частот от 37,5 до 178,4 ГГц.

Основная часть.

Обобщенная структурная схема эталона единицы мощности электромагнитных колебаний в диапазоне частот от 37,5 до 178,4 ГГц представлена на рисунке 1.

Источники сигналов обеспечивают формирование сигналов электромагнитных колебаний сверхвысоких частот в режиме непрерывной генерации. Устройства сличения представляют собой комбинацию направленного ответвителя и согласующих устройств. Измеритель поглощаемой мощности включает четыре волноводных калориметрических преобразователя поглощаемой мощности и блок управления и индикации.

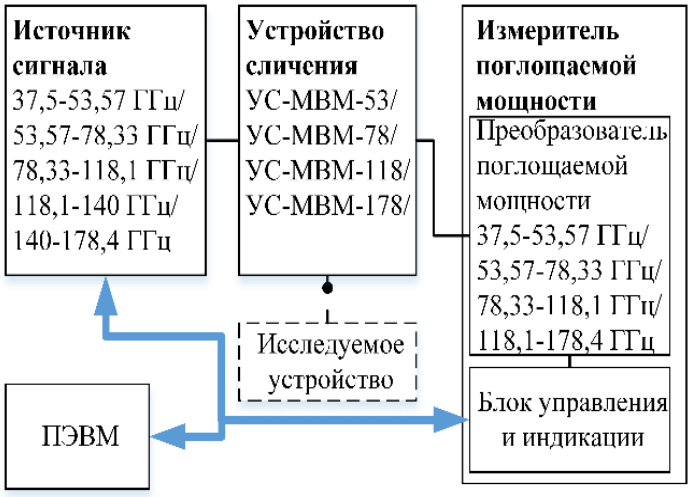


Рисунок 1 – Обобщенная структурная схема эталона

Программное обеспечение позволяет управлять работой измерительного оборудования с ПЭВМ, устанавливать поддиапазон, частотные точки, уровни измерительных сигналов, режимы измерений (определение коэффициента эффективности, коэффициента передачи или погрешности измерения мощности исследуемого устройства), считывать измерительную информацию с блока управления и индикации, обеспечивает корректировку измеренных значений с учетом коэффициентов калибровки и представление измерительной информации в форме, удобной для дальнейшей математической обработки в соответствии с методиками поверки/калибровки.

Важными составными частями эталона являются источники СВЧ сигнала. Одними из наиболее важных их характеристик, влияющих на точность и воспроизводимость результатов измерений являются нестабильность выходной мощности и коэффициент стоячей волны (КСВН) выходов источника сигнала.

В докладе рассматривается разработанная методика исследования нестабильности уровня выходной мощности и КСВН выхода источников сигнала эталона. Приведены также результаты экспериментальных исследований этих параметров для трех источников сигнала, работающих в диапазонах частот 78,33 – 118,1 ГГц; 118,10 ГГц – 140,0 ГГц и 140,0 ГГц – 178,4 ГГц.

Исследования нестабильности уровня выхода мощности источников сигнала в диапазоне частот от 78,33 ГГц до 178,4 ГГц проводятся методом прямых измерений с помощью ваттметра поглощаемой мощности М3-75 по схеме, приведенной на рисунке 2. Процесс измерений включает в себя следующие операции.

Источники сигналов в диапазонах частот 78,33 ГГц – 118,1 ГГц; 118,10 ГГц – 140 ГГц и 140 ГГц – 178,4 ГГц поочередно подключают к ваттметру М3-75.

При исследовании источника сигнала 78,33 ГГц –118,1 ГГц на его выходе устанавливают частоту, равную 95 ГГц. При исследовании источника сигнала 118,10 ГГц – 140 ГГц устанавливают частоту, равную 130 ГГц. При исследовании источника сигнала 140 ГГц – 178,4 ГГц устанавливают частоту 160 ГГц.

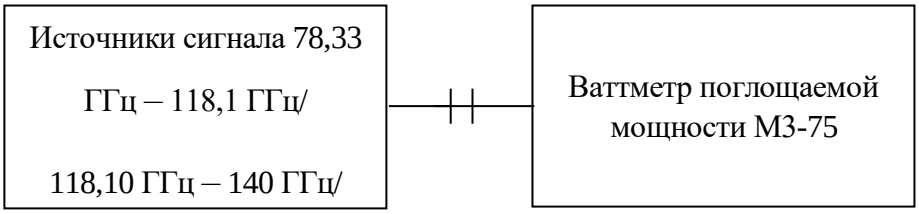


Рисунок 2 – Структурная схема измерений уровня мощности источников сигнала

Уровень мощности для всех источников устанавливается равным 1 мВт и в течении 15 минут снимаются показания значения мощности с ваттметра с фиксацией результата каждую минуту.

Из полученных результатов выбирается максимальная Pmax, мВт, и минимальная Pmin, мВт, мощность и вычисляется нестабильность уровня мощности δнР за промежуток времени t = 15 мин по формуле

$$\delta_{нР} = \frac{P_{max} - P_{min}}{P}.$$

где P_{max} – максимальное значение мощности, мВт;

P_{min} – минимальное значение мощности, мВт.

Определение КСВН выхода источников сигнала осуществляется методом прямых измерений с помощью измерителей КСВН панорамных по схеме, приведенной на рисунке 3.

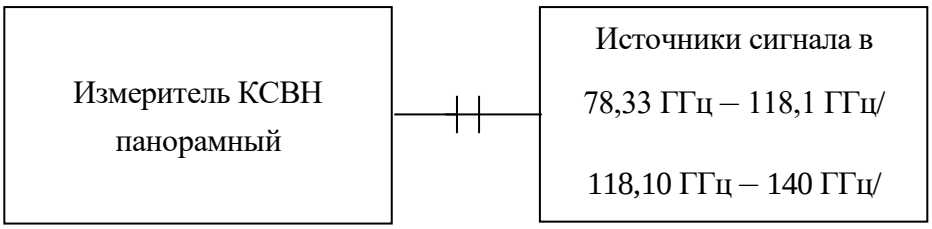


Рисунок 3 – Структурная схема измерений КСВН выхода источников сигнала

При исследовании источника сигнала 78,33 ГГц –118,1 ГГц используется измеритель РР2-01. При исследовании источников сигнала 118,10 ГГц – 140 ГГц и 140 ГГц – 178,4 ГГц используется измеритель Р2-123.

При исследовании источника 78,33 ГГц – 118,1 ГГц КСВН определяется для значений частот 78,33, 80, 85, 90, 95, 100, 105, 110, 115, 118,1 ГГц. При исследовании источника 118,10 ГГц – 140 ГГц КСВН определяется для значений частот 118,10; 120; 125; 130; 135; 140; 145; 150 ГГц. При исследовании источника в частотном диапазоне 140 ГГц –178,4 ГГц КСВН определяется для значений частот 140; 145; 150; 155; 160; 165; 170; 175; 178,4 ГГц.

При экспериментальных исследованиях источников сигнала эталона по описанной выше методике были получены следующие результаты.

Нестабильность уровня выходной мощности источника сигнала 78,33 ГГц –118,1 ГГц составила 0,001 мВт, а КСВН выхода находился в пределах от 1,15 до 1,18.

Нестабильность уровня выходной мощности источника сигнала 118,10 ГГц – 140 ГГц составила 0,002 мВт, при этом КСВН выхода находился в пределах от 1,15 до 1,20.

Нестабильность уровня выходной мощности источника сигнала 140 ГГц – 178,4 ГГц составила 0,003 мВт, при этом КСВН выхода находился в пределах от 1,17 до 1,35.

Заключение. Разработанная методика определения параметров источника сигнала дает возможность экспериментально определить их количественные значения и оценить их влияние на общую неопределенность результатов измерений, проводимых с использованием эталона единицы мощности в частотном диапазоне от 78,33 до 178,4 ГГц.

Список литературы

[1] Разработка эталона единицы мощности электромагнитных колебаний в диапазоне частот от 37,5 до 178,4 ГГц: Междунар. науч.-метод. конф. «Инженерное образование в цифровом обществе» В 2 ч. 4.1 / А. В. Гусинский [и др.] – Минск: БГУИР, 2024. – 298-301с.

UDC 621.317.08

METHOD OF DETERMINING THE PARAMETERS OF THE SIGNAL SOURCE FROM THE NATIONAL STANDARD OF THE UNIT OF POWER

Doronina A.V. gr. 467241

Belarusian State University of Informatics and Radioelectronics,
Minsk, Republic of Belarus

Beloshitsky A.P. – Cand. Sc. (Tech.), associate professor

Annotation. The materials of the report consider the developed methodology for determining the parameters of the signal sources from the standard of the unit of power in the frequency range from 37.5 to 178.4 GHz.

Keywords: methodology, signal source, parameters, standard, power

УДК 621.317.08:621.373

МЕТОДИКА ИССЛЕДОВАНИЙ МЕТРОЛОГИЧЕСКИХ ХАРАКТЕРИСТИК ГЕТЕРОДИНА ИЗ СОСТАВА НАЦИОНАЛЬНОГО ЭТАЛОНА ЕДИНИЦЫ ОСЛАБЛЕНИЯ

Маскей М. Ш. гр.367041

Белорусский государственный университет информатики и радиоэлектроники,

Научный руководитель: Белошицкий А. П. – кандидат технических наук, доцент

Аннотация. В материалах доклада рассматривается разработанная методика исследований технических и метрологических характеристик гетеродина, из состава эталона единицы ослабления электромагнитных колебаний в диапазоне частот от 37,5 до 178,4 ГГц.

Ключевые слова: методика, исследования, метрологические характеристики, гетеродин, сверхвысокая частота, эталон, ослабление

Введение. В последние годы наблюдается активное развитие в области создания и совершенствования эталонной базы для обеспечения единства измерений в миллиметровом диапазоне частот. Особое внимание уделяется метрологическому обеспечению измерений ослабления электромагнитных колебаний, что обусловлено ростом потребности в высокоточных средствах измерений данной физической величины. В рамках этих работ в Центре НИИ 1.9 БГУИР реализуется проект по созданию национального эталона единицы ослабления в диапазоне частот от 37,5 до 178,4 ГГц.

Важной составной частью эталонного комплекса является гетеродин, от метрологических характеристик которого существенно зависит точность и воспроизводимость результатов измерений. Исследования, направленные на оценку стабильности частоты, уровня выходного сигнала, фазового шума и других параметров гетеродина, позволяют обоснованно определить его вклад в общую неопределенность измерений.

В докладе рассматривается структурная схема эталона, принцип его работы и методика экспериментальных исследований метрологических характеристик гетеродина входящего в состав эталона.

Основная часть. Обобщенная структурная схема эталона единицы ослабления электромагнитных колебаний в диапазоне частот от 37,5 до 178,4 ГГц представлена на рисунке 1 [1].

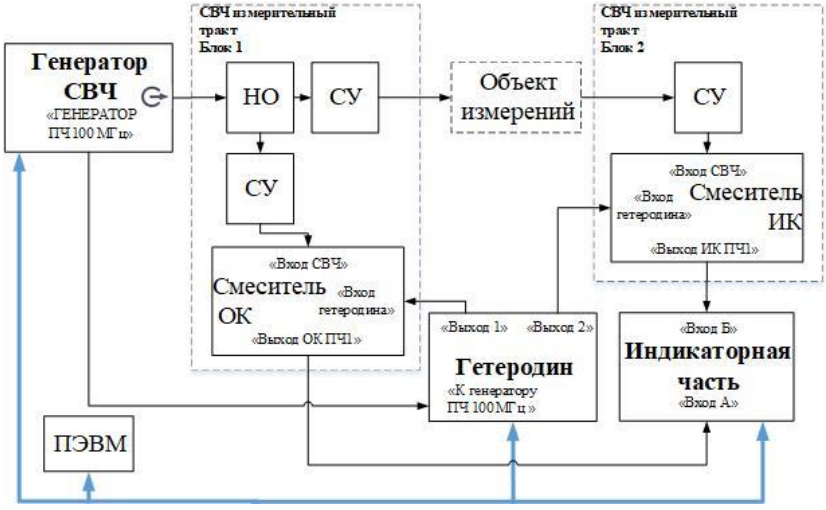


Рисунок 1 – Обобщенная структурная схема эталона

Принцип действия эталона основан на преобразовании частоты в опорном (ОК) и измерительном каналах (ИК) на постоянную промежуточную частоту 20 кГц. Преобразование частоты осуществляется в три этапа.

Гармонический сигнал от СВЧ-генератора с помощью направленного ответвителя (НО) делится на измерительный (ИК) и опорный (ОК) каналы. В ИК сигнал проходит через объект измерений (ОИ), затем поступает на смеситель ИК. В ОК сигнал поступает на смеситель ОК. На оба смесителя подаются сигналы от гетеродина. В них выполняется первое преобразование частоты и формируется сигнал первой промежуточной частоты:

$$f_{\text{пч1}} = f_{\text{свч}} \pm N \cdot f_{\text{гет}}, \quad (1)$$

где $f_{\text{свч}}$ – частота сигнала, поступающего на вход смесителя;

N – номер рабочей гармоники смесителя;

$f_{\text{гет}}$ – частота сигнала гетеродина.

В измерительной части, в качестве которой используется прибор для измерения ослабления ДК1-28, осуществляются второй и третий этапы преобразования частоты, (на частоты 20 МГц и 20 кГц соответственно) и измерение отношений уровней сигналов в каналах А и Б.

Сигналы генератора СВЧ соответствующего поддиапазона и гетеродина синхронизированы с помощью генератора ПЧ, конструктивно входящего в состав генератора СВЧ.

Согласующие устройства (СУ) элементов СВЧ измерительного тракта предназначены для обеспечения согласования, а также обеспечивают развязку между ИК и ОК.

Управление работой эталона и измерительным оборудованием из состава эталона, вывод, обработка и документирование результатов измерений осуществляется с помощью ПЭВМ через интерфейсы USB или RS-232.

Гетеродин, методика исследования характеристик которого приведена ниже, построен по схеме измерительного генератора и обеспечивает формирование электрического синусоидального сигнала частотой от 0,01 до 18,0 ГГц. Принцип действия гетеродина основан на формировании синусоидального СВЧ сигнала требуемой частоты в частотном диапазоне от 0,01 до 18,00 ГГц путем синтеза из опорного сигнала частотой 100 МГц.

Методика предусматривает определение следующих метрологических характеристик гетеродина: определение рабочего диапазона частот, погрешности установки и нестабильности частоты; определение динамического диапазона, погрешности установки и нестабильности уровня мощности; КСВН выходов гетеродина.

Определение рабочего диапазона частот, погрешности установки и нестабильности частоты приводится по схеме, приведенной на рисунке 2.

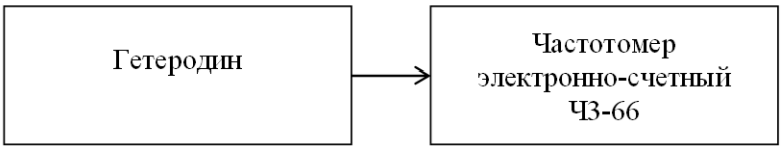


Рисунок 2 – Схема измерения частоты

Перед началом измерений частотомер прогревается в течение 2 часов. Гетеродин переводится в режим непрерывной генерации, после чего через 15 минут измеряется частота выходного сигнала на точках: 0,01; 5,00; 10,00; 15,00; 18,00 ГГц.

Основная относительная погрешность установки частоты рассчитывается по формуле:

$$\delta_f = \frac{f_у - f_и}{f_и}, \quad (2)$$

где $f_у$ – значение частоты, установленное на источнике, Гц;

$f_и$ – значение частоты, измеренное частотомером, Гц.

Нестабильность частоты $\delta_{нf}$ за промежуток времени t = 15 минут определяется следующим образом. Устанавливается частота, равная 10,0 ГГц. В течение 15 минут снимаются показания значений частоты с фиксацией результата каждую минуту.

Измерения проводятся для выхода 1 и выхода 2 гетеродина. Из полученных результатов выбрать максимальную f_{max}, Гц, и минимальную f_{min}, Гц, частоту сигнала и вычислить нестабильность частоты $\delta_{нf}$ за промежуток времени t = 15 мин по формуле

$$\delta_{нf} = \frac{f_{max} - f_{min}}{f_y}, \quad (3)$$

где f_{max} – максимальное значение частоты, Гц;

f_{min} – минимальное значение частоты, Гц.

Определение динамического диапазона, погрешности установки и нестабильности уровня мощности приводится по схеме, приведенной на рисунке 3.

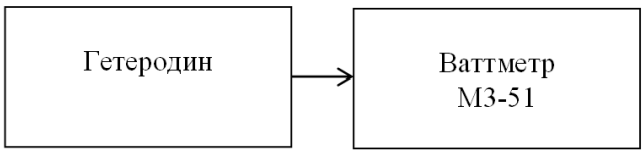


Рисунок 3 – Схема измерения мощности

Измерения проводятся на следующих значениях частоты выходного сигнала: 0,01; 5,00; 10,00; 15,00; 18,00 ГГц и значениях уровня мощности: 0,1; 0,3; 1 мВт.

Абсолютную погрешность установки уровня мощности Δ_P, мВт, вычислить для каждого установленного значения уровня мощности и частоты по формуле

$$\Delta_P = P_u - P_y, \quad (4)$$

где $P_и$ – измеренное значение мощности, мВт;

$P_у$ – установленное значение мощности, мВт;

Нестабильность уровня мощности определяется следующим образом. Устанавливается частота, равная 10,0 ГГц и уровень мощности равный 1 мВт. В течение 15 минут снимаются показания значений уровня мощности с фиксацией результата каждую минуту. Измерения проводятся для выхода 1 и выхода 2 гетеродина.

Из полученных результатов выбрать максимальную P_{max}, мВт, и минимальную P_{min}, мВт, мощность и вычислить нестабильность уровня мощности $\delta_{нP}$ за промежуток времени t = 15 минут по формуле

$$\delta_{нP} = \frac{P_{max} - P_{min}}{P_y}, \quad (5)$$

где P_{max} – максимальное значение мощности, мВт;

P_{min} – минимальное значение мощности, мВт.

Определение КСВН первого и второго выходов гетеродина K_{CTU} осуществляется методом прямых измерений с помощью анализатора цепей векторного MS4644A по схеме, приведенной на рисунке 4.

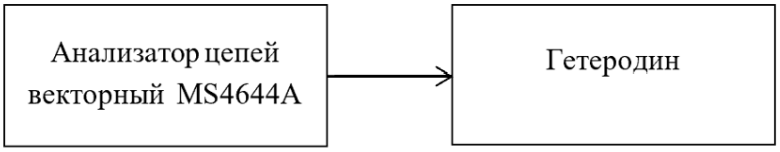


Рисунок 4 – Схема измерения КСВН

Измеряется коэффициент стоячей волны по напряжению (КСВН) на выходах гетеродина на частотах: 0,01; 5,00; 10,00; 15,00 и 18,00 ГГц. Полученные значения позволяют оценить согласование выходов гетеродина с измерительным трактом и его пригодность для работы в составе эталона.

Заключение. Разработанная методика исследований метрологических характеристик гетеродина позволяет экспериментально определить их значения количественно и оценить их вклад в общую неопределенность результатов измерений, выполняемых с использованием эталона единицы ослабления электромагнитных колебаний в диапазоне частот от 37,5 до 178,4 ГГц.

Список литературы

1. Разработка эталона единицы ослабления электромагнитных колебаний в диапазоне частот от 37,5 до 178,4 ГГц: Междунар. науч.-метод. конф. «Инженерное образование в цифровом обществе». В 2 ч. Ч.1 / А. В. Гусинский [и др.] – Минск: БГУИР, 2024. С. 302 – 303.

UDC 621.317.08:621.373

METHODOLOGY OF RESEARCH OF METROLOGICAL CHARACTERISTICS OF HETERODYNE FROM THE NATIONAL STANDARD OF ATTENUATION UNIT

Maskey M.S. gr.367041

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Beloshitsky A. P. – Cand. Sc. (Tech.), associate professor

Annotation. In the materials of the report the developed research methodology of technical and metrological characteristics of the heterodyne, from the composition of the standard of the unit of attenuation of electromagnetic oscillations in the frequency range from 37.5 to 178.4 GHz is considered.

Keywords: methodology, research, metrological characteristics, heterodyne, ultrahigh frequency, standard, attenuation

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Сборник материалов 61-ой научной конференции аспирантов, магистрантов и студентов

Ответственный за выпуск *В.И. Брилевский*

Компьютерная верстка *Михальцова Ю.В.*

Дизайн обложки *Кайдак Д.Н.*