Теория и практика современной науки

№7(133) июль 2026

ISSN 2412-9682

МЕЖДУНАРОДНЫЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

«Теория и практика современной науки»

http://www.modern-j.ru

ISSN 2412-9682

Свидетельство о регистрации средства массовой коммуникации
Эл № 61970 от 02.06.2015г.

Выпуск № 7(133) июль, 2026.

Журнал размещается на сайте Научной электронной библиотеки
на основании договора 435-06/2015 от 25.06.2015

Nguyen Thi Viet Ha, Ph.D.
Saigon University

ENHANCING THE ROLE OF YOUTH ORGANIZATIONS IN THE DIGITAL ERA AMID THE GROWING INFLUENCE OF SOCIAL MEDIA AND INFORMAL COMMUNITIES

Abstract: *This article examines the impact of social media and informal communities on the role of youth organizations in the context of digital transformation. Drawing on a review of domestic and international studies, it argues that the rapid expansion of digital platforms has fundamentally reshaped the ways young people connect, participate in society, and construct their identities, thereby creating a form of soft competition between traditional youth organizations and online communities. While these developments have expanded opportunities for youth engagement, they have also generated significant challenges, including the erosion of social capital, declining effectiveness of political and civic education, the proliferation of short-term forms of participation, and the fragmentation of shared values. In response, the article proposes several strategic directions to strengthen the adaptive capacity of youth organizations, including the development of hybrid digital–physical ecosystems, the renewal of communication strategies and organizational practices, the promotion of digital citizenship education, the expansion of collaboration with diverse social actors, and the improvement of governance through flexible, youth-centered approaches. These measures are expected to reinforce the role of youth organizations in the evolving digital society.*

Keywords: *youth organizations; social media; informal communities; digital transformation; Generation Z; digital citizenship.*

1. Introduction

Over the past two decades, the rapid development of the Internet, social media, artificial intelligence, and digital platforms has fundamentally transformed the ways young people communicate, learn, work, and participate in social life worldwide. Digital space is no longer merely a channel for information exchange; it has become a new social infrastructure where young people establish relationships, construct personal identities, share values, and engage in diverse community activities. In particular, the emergence of online communities organized around shared interests, professions, or common concerns has significantly expanded opportunities for social connection and participation while simultaneously reshaping the role of traditional social institutions (Anderson & Jiang, 2018; Bennett & Segerberg, 2012; Cortés-Ramos et al., 2021).

In Vietnam, the national digital transformation agenda, together with the widespread adoption of the Internet and smartphones, has enabled social media to become one of the primary spaces for youth interaction. Recent reports indicate that Vietnam ranks among the countries with the highest rates of Internet and social media usage in the region, with individuals aged 16–24 representing the most active user group (We Are Social & DataReportal, 2025). For Generation Z, online environments are not only spaces for entertainment but also platforms for learning, job seeking, building social networks, and participating in community activities (Hội Sinh viên Việt Nam, 2023; Lê Đình Hải & Đỗ Thị Nụ, 2025). The rapid growth of informal communities on Facebook, TikTok, Discord, LinkedIn, and other digital platforms has fostered new forms of social engagement characterized by flexibility, decentralization, and voluntary participation (Bennett & Segerberg, 2012; Barati, 2023).

Against this backdrop, traditional youth organizations—particularly the Ho Chi Minh Communist Youth Union and the Vietnam Youth Federation—are facing increasing demands for institutional innovation. While these organizations have historically played central roles in political education, youth mobilization, and community engagement, they now compete with a wide range of digitally mediated communities for the attention, participation, and commitment of young people. This competition is not one of direct confrontation but rather of attracting sustained engagement and responding effectively to the increasingly diverse needs and expectations of youth (Mạnh Cường, 2025; Anh Thơ, 2023). Consequently, there is a pressing need to reassess the roles, organizational models, and adaptive capacities of youth organizations in the digital era.

Recent scholarship has extensively examined the influence of social media on youth behavior, political participation, civic engagement, media literacy, and the emergence of online communities (Barati, 2023; Hassoun et al., 2023; Saxena, 2023; Ushanova et al., 2021). Other studies have explored the transformation of youth work in the context of digitalization (Alruthaya et al., 2021). Nevertheless, existing research has largely addressed these issues separately, with limited attention given to the interrelationship between the rise of social media, the expansion of informal communities, and the changing role of youth organizations from the perspectives of institutional adaptation and social capital. In the Vietnamese context, systematic analyses of the shift from traditional youth organizations toward digital communities, as well as its implications for youth work and mass organizations, remain relatively scarce.

Addressing this research gap, the present study analyzes changes in youth social participation under the influence of social media and informal communities, evaluates the challenges confronting traditional youth organizations, and proposes strategic directions to enhance their adaptive capacity and social role in the digital era. Drawing on the theoretical perspectives of social capital, connective action, and institutional adaptation, the article contributes to the literature on the transformation of youth organizations in digital societies while offering policy implications for the renewal of youth work in contemporary Vietnam.

2. Social Media, Informal Communities, and the Transformation of Youth Participation in the Digital Era

2.1. Changing Patterns of Youth Participation in the Digital Era

The rapid advancement of digital technologies has fundamentally transformed the social behavior of young people worldwide. Unlike previous generations, Generation Z has grown up with the Internet, smartphones, and social media, and is therefore widely regarded as a generation of "digital natives." For this generation, digital space is no longer merely a communication tool but an integral part of everyday social life, where learning, work, entertainment, identity formation, and community engagement occur simultaneously (Anderson & Jiang, 2018; Alruthaya et al., 2021). Consequently, the ways in which young people establish social relationships and participate in collective activities have undergone profound changes.

International studies indicate that young people increasingly prefer flexible forms of participation that emphasize autonomy and self-determination rather than hierarchical organizational structures. Anderson and Jiang (2018) found that the vast majority of American teenagers use social media as their primary communication environment, with nearly half reporting that they are "online almost constantly." As Internet access has become ubiquitous, digital platforms have evolved into the primary spaces through which young people access information, maintain social relationships, and express personal opinions. This trend has been consistently confirmed by more recent studies, which demonstrate that digital platforms now play a central role in shaping the identities, values, and social behaviors of younger generations (Hassoun et al., 2023; Deloitte, 2025).

A defining characteristic of Generation Z is the increasing personalization of social participation. Rather than maintaining long-term commitment to a single organization, young people tend to engage selectively in activities that align with their personal interests, competencies, and immediate needs. Alruthaya, Nguyen, and Lokuge (2021) argue that digital environments facilitate more flexible models of learning, communication, and collaboration, allowing young people to independently determine the content, timing, and forms of their participation. This reflects a broader transition from obligation-based participation toward participation motivated by personal interests and individual values (Deloitte, 2025).

These developments have also reshaped young people's understanding of community. Whereas social belonging was traditionally established through formal institutions such as schools, youth organizations, and civic associations, social ties are increasingly formed around shared interests, professional aspirations, or common goals within digital environments. Young people can simultaneously participate in multiple online communities with varying degrees of commitment, free from the structural constraints of traditional organizations. The ability to establish connections rapidly, expand social networks, and adjust

participation flexibly has become a major source of attraction for digital communities (Bennett & Segerberg, 2012; Barati, 2023).

In Vietnam, these trends have accelerated alongside the country's national digital transformation. According to the Digital 2025: Vietnam report published by We Are Social and DataReportal, more than three-quarters of the Vietnamese population use the Internet and social media, with individuals aged 16–24 representing the most active user group. Digital platforms have become essential spaces where young people seek information, pursue education, build professional networks, develop personal brands, and engage in various forms of civic participation (We Are Social & DataReportal, 2025). Surveys conducted by the Vietnam Students' Association similarly indicate that social media has become an indispensable medium for learning, communication, and student activities (Hội Sinh viên Việt Nam, 2023).

These developments suggest that changing patterns of youth participation are not merely technological consequences but reflect a broader restructuring of social relationships in the digital era. Young people increasingly favor open, flexible, and voluntary forms of participation, while their attachment to traditional institutions has gradually weakened. This transformation has created favorable conditions for the emergence of new forms of digital communities and simultaneously poses significant challenges for youth organizations seeking to maintain their capacity to mobilize, guide, and empower younger generations (Bennett & Segerberg, 2012; Trần Quang Thái, 2023).

2.2. Social Media and the Emergence of Informal Communities

The widespread adoption of social media has accelerated the rapid emergence of informal communities within digital environments. Unlike traditional social organizations, which are established through formal structures, institutional regulations, and clearly defined membership, online communities are primarily formed through voluntary connections among individuals who share common interests, professions, values, or concerns. Characterized by openness, flexibility, and low participation costs, these communities have become increasingly attractive forms of social organization for young people (Bennett & Segerberg, 2012; Barati, 2023).

Research on digital communication suggests that social media functions not merely as a channel for information exchange but also as a new social infrastructure through which individuals establish networks, share knowledge, collaborate, and mobilize community resources (Cortés-Ramos et al., 2021; Barati, 2023). Through platforms such as Facebook, TikTok, Discord, LinkedIn, and Reddit, young people can easily participate in study groups, professional communities, content creation networks, volunteer initiatives, and entrepreneurial ecosystems without being constrained by geographical boundaries, fixed schedules, or rigid organizational structures. Consequently, digital communities have substantially expanded opportunities for youth participation beyond those offered by conventional organizations (Deloitte, 2025; Ushanova et al., 2021).

One defining feature of informal communities is their decentralized governance. Rather than operating through hierarchical administrative structures, most online communities rely on horizontal interactions among members. Leadership typically emerges through expertise, credibility, and active contribution rather than through formally appointed positions. Such decentralized structures foster open communication, encourage creativity, and promote greater individual initiative among participants (Bennett & Segerberg, 2012).

Many scholars argue that the proliferation of online communities has fundamentally transformed patterns of youth civic engagement. Bennett and Segerberg (2012) introduced the concept of connective action to explain digitally networked forms of collective action, in which individual participation depends less on intermediary organizations and more on direct connections facilitated by digital platforms. Under this model, individuals are able to determine their own level of involvement, disseminate information, or initiate collective activities without relying on centralized organizational coordination. This perspective helps explain why numerous social campaigns, volunteer initiatives, and environmental movements have spread rapidly through online networks without being organized by traditional institutions (Barati, 2023; Cortés-Ramos et al., 2021).

Despite their significant contribution to expanding opportunities for civic engagement, informal communities also present substantial challenges to conventional social institutions. The growing influence of digital networks has dispersed the mobilizing capacity of many youth organizations by providing young people with numerous alternative avenues for social interaction and personal development. Moreover, algorithm-driven content recommendations, information bubbles, and the rapid dissemination of unverified information may contribute to value fragmentation and reduce meaningful dialogue among different social groups (Hassoun et al., 2023; Lê Đình Hải & Đỗ Thị Nụ, 2025).

In Vietnam, online communities have expanded rapidly across various domains, including education, professional development, technology, entrepreneurship, content creation, volunteerism, and social activism. These communities have created new opportunities for learning, collaboration, and skills development while enabling young people to broaden their social networks and contribute to addressing societal challenges (Hội Sinh viên Việt Nam, 2023; We Are Social & DataReportal, 2025). At the same time, however, their growth has fundamentally altered the competitive environment among social institutions seeking to attract and sustain youth participation. Under these conditions, youth organizations are no longer the sole institutions responsible for community building but must instead adapt to an increasingly polycentric social ecosystem in which social media platforms and informal communities have become influential actors shaping youth behavior and civic participation (Mạnh Cường, 2025; Trần Quang Thái, 2023).

2.3. Fragmentation of Youth Identity, Values, and the Capacity for Youth Guidance in the Digital Space

Another important consequence of the growing influence of social media and informal communities is the fragmentation of youth identity formation and value systems. In the past, youth organizations played a central role in transmitting shared values, fostering civic ideals, and cultivating a sense of collective responsibility. Today, however, young people's socialization increasingly occurs through digital platforms, where algorithms, media trends, and diverse online communities exert significant influence. While this transformation broadens young people's exposure to multiple value systems, it also weakens the coherence of their beliefs, identities, and developmental orientations (Hassoun et al., 2023; Lê Đình Hải & Đỗ Thị Nụ, 2025).

A defining characteristic of the digital environment is the emergence of echo chambers and filter bubbles, in which users are predominantly exposed to content that reinforces their existing interests and viewpoints. When information consumption is confined to like-minded communities, young people are more likely to develop selective perspectives, become less willing to engage with opposing viewpoints, and experience difficulties in cultivating critical thinking. Consequently, information fragmentation affects not only individual cognition but also undermines the development of shared values and collective responsibility within society (Hassoun et al., 2023).

Moreover, the rapid expansion of informal online communities has made youth identity formation increasingly individualized. Young people often participate simultaneously in multiple communities based on shared interests, professions, lifestyles, or social values without maintaining long-term commitment to any single organization. Although this model provides greater flexibility and broader opportunities for personal development, it also produces more fragmented and fluid social identities, making sustained attachment to collective values increasingly difficult. For many young people, identification with an online community has become more salient than affiliation with traditional social organizations (Bennett & Segerberg, 2012; Deloitte, 2025).

Against this backdrop, the capacity of youth organizations to provide value-based guidance faces unprecedented challenges. As social media has become the dominant source of information and digital influencers, content creators, and online communities increasingly shape youth behavior, youth organizations no longer possess an exclusive role in guiding younger generations. Without substantial innovation in organizational practices, communication strategies, and interaction mechanisms, these organizations will face increasing difficulties in maintaining their position as institutions responsible for value formation and youth mobilization (Trần Quang Thái, 2023; Anh Thơ, 2023; Mạnh Cường, 2025). This shift has implications not only for the effectiveness of youth work but also for the accumulation of social capital and the development of social cohesion necessary for national development (Bennett & Segerberg, 2012).

Nevertheless, such fragmentation should not be viewed solely as a risk to be mitigated. Rather, it reflects an inherent characteristic of digital societies, where young people seek to express individual identities while participating in multiple overlapping communities (Barati, 2023; Deloitte, 2025). Consequently, the primary challenge is not to replace or compete with informal communities but to reposition youth organizations as network hubs within the broader digital social ecosystem. In this capacity, youth organizations should facilitate dialogue among diverse communities, promote shared civic values, and support young people's development as responsible digital citizens (Hassoun et al., 2023; Trần Quang Thái, 2023). By fulfilling these functions, youth organizations can move beyond their traditional educational and mobilizing roles to become key actors in strengthening social cohesion within an increasingly digitalized society (Mạnh Cường, 2025).

3. Strategies for Strengthening the Role of Youth Organizations in the Digital Era

3.1. Transforming Organizational Models toward a Youth-Centered Digital Ecosystem

The preceding analysis suggests that the principal challenge confronting youth organizations does not arise from the emergence of social media or informal communities themselves, but rather from the inability of conventional organizational models to keep pace with changing patterns of youth participation and engagement (Mạnh Cường, 2025; Bennett & Segerberg, 2012). Accordingly, strengthening the role of youth organizations requires more than simply incorporating digital technologies into existing activities; it demands a comprehensive transformation toward a youth-centered digital ecosystem (Anh Thơ, 2023; Alruthaya et al., 2021).

Within this framework, digital space should be regarded as an integral component of organizational operations rather than merely a communication channel. Digital platforms should not only facilitate membership management but also provide environments where young people can learn, exchange knowledge, build networks around shared interests, develop professional competencies, and implement social initiatives (Alruthaya et al., 2021; Deloitte, 2025). Furthermore, online activities should be systematically integrated with face-to-face engagement through hybrid organizational models, ensuring continuous interaction between digital environments and real-world community life (Cortés-Ramos et al., 2021).

At the same time, youth organizations need to shift from standardized, program-based approaches toward more personalized forms of engagement. Developing specialized clubs, interest-based communities, entrepreneurship networks, research groups, digital innovation initiatives, and volunteer programs tailored to diverse needs would enable young people to participate according to their individual interests, competencies, and developmental aspirations (Deloitte, 2025; Alruthaya et al., 2021). Under such a model, youth organizations would no longer function merely as coordinators of collective campaigns but would become

comprehensive platforms that support the holistic development of each individual (Mạnh Cường, 2025; Bennett & Segerberg, 2012).

3.2. Innovating Educational Approaches, Communication Strategies, and the Development of Digital Citizenship

Within the contemporary digital media environment, the capacity of youth organizations to guide younger generations depends not only on the content of their educational messages but also on their communication approaches and the quality of interaction they establish with young people (Trần Quang Thái, 2023; Anh Thơ, 2023). Accordingly, youth education and communication should evolve from a one-way transmission model toward a more participatory approach characterized by dialogue, interaction, and the co-creation of content with young people themselves (Cortés-Ramos et al., 2021).

Social media platforms should be utilized as open educational spaces through which positive values are communicated in ways that resonate with the digital culture of younger generations. The use of short-form videos, podcasts, infographics, livestreams, and other interactive media formats can significantly enhance accessibility while fostering stronger emotional engagement among young audiences (Trần Quang Thái, 2023; Deloitte, 2025). At the same time, the participation of scholars, professionals, entrepreneurs, positive digital influencers, and young people themselves can enrich educational content, strengthen its credibility, and broaden the social reach of youth initiatives (Barati, 2023; Cortés-Ramos et al., 2021).

More importantly, youth education in the digital era should prioritize the development of digital citizenship competencies. Alongside political awareness and social responsibility, young people should be equipped with the ability to evaluate information critically, exercise analytical thinking, communicate effectively in digital environments, protect personal data, and behave responsibly online (Hassoun et al., 2023). These competencies constitute the essential foundations that enable young people not only to adapt successfully to digital society but also to contribute proactively to the creation of a safe, inclusive, and ethically responsible digital environment (Alruthaya et al., 2021; Hassoun et al., 2023).

3.3. Building Open Collaborative Networks to Expand the Social Influence of Youth Organizations

In an increasingly networked digital society, youth organizations cannot effectively fulfill their missions if they remain confined within traditional institutional boundaries. Consequently, organizational strategies should shift from a management-oriented mindset toward a network-oriented approach that promotes open collaboration among youth organizations, businesses, educational institutions, civil society organizations, professional communities, and diverse online communities (Bennett & Segerberg, 2012; Barati, 2023).

Such collaborative networks can diversify the financial, technological, intellectual, and human resources available for youth development activities. Furthermore, engagement with informal communities should not be regarded as a

form of institutional competition but rather as an opportunity to broaden outreach, harness grassroots social innovation, and encourage wider youth participation in community initiatives (Cortés-Ramos et al., 2021; Mạnh Cường, 2025).

From a long-term perspective, youth organizations should gradually transform from organizers of collective campaigns into architects of comprehensive youth development ecosystems. Under this model, they would continue to provide value-based guidance while simultaneously connecting social resources to support young people's education, entrepreneurship, innovation, and participation in addressing community challenges (Anh Thơ, 2023; Mạnh Cường, 2025). This transformation is consistent with contemporary governance approaches, in which organizational effectiveness is measured not only by membership size but also by the ability to cultivate collaborative networks and generate positive social impact (Bennett & Segerberg, 2012).

Conclusion

The rapid expansion of social media and informal communities has fundamentally reshaped the socialization processes, patterns of civic participation, and value systems of young people. While these developments provide unprecedented opportunities for young people to expand social networks, access knowledge, and pursue personal development, they also present significant challenges for the traditional roles of youth organizations. Declining social capital, increasing difficulties in value-based guidance, and the growing prevalence of fragmented and short-term forms of civic engagement indicate that conventional organizational models must adapt to the realities of an increasingly digital society.

Drawing upon an analysis of the transformation of youth participation in digital environments and its implications for youth work, this study argues that strengthening the role of youth organizations should not be understood as competing with social media or informal communities. Instead, youth organizations should seek to position themselves as coordinating and guiding institutions within the broader digital social ecosystem. Achieving this objective requires comprehensive transformation in organizational models, educational and communication strategies, and collaborative mechanisms with diverse social actors in order to respond more effectively to the evolving needs of younger generations.

In the long run, the effectiveness of youth organizations should be evaluated not merely by the number of members they recruit or the scale of the campaigns they organize, but by their capacity to create environments that enable young people to learn, innovate, contribute, and develop throughout their lives. By serving as hubs that connect social resources, support the holistic development of young people, and promote positive values across digital spaces, youth organizations can continue to play a pivotal role in developing future generations, strengthening social capital, and contributing to Vietnam's sustainable development in the digital era.

References

1. Mai An. (2024). 69% of Vietnamese Gen Z use social media as a tool for seeking travel ideas and inspiration. Sai Gon Giai Phong Newspaper. https://www.sggp.org.vn/69-gen-z-viet-nam-su-dung-mang-xa-hoi-nhu-mot-cong-cu-tim-kiem-y-tuong-va-cam-hung-du-lich-post755954.html
2. Manh Cuong. (2025). Building a strong and comprehensive Youth Union organization from the grassroots level. Thanh Nien Newspaper. https://thanhnien.vn/xay-dung-to-chuc-doan-vung-manh-toan-dien-tu-co-so-185251206114658986.htm
3. Le Dinh Hai, & Do Thi Nu. (2025). Characteristics of Generation Z's news consumption behavior on social media in Vietnam. Journal of Political Theory and Communication. https://lyluanchinhtrivatruyenthong.vn/dac-diem-hanh-vi-tieu-thu-tin-tuc-tren-mang-xa-hoi-cua-the-he-z-tai-viet-nam-p29211.html
4. Vietnam Students' Association. (2023). More than 85% of surveyed students use social media every day: What are their purposes? https://doanthanhnien.vn/tin-tuc/hoi-sinh-vien-viet-nam/hon-85_-sinh-vien-duoc-khao-sat-len-mang-xa-hoi-hang-ngay-voi-muc-dich-gi
5. Tran Quang Thai. (2023). The impact of social media on political communication methods for youth. Journal of State Management. https://www.quanlynhanuoc.vn/2023/10/24/tac-dong-cua-mang-xa-hoi-den-phuong-thuc-tuyen-truyen-chinh-tri-cho-thanh-nien/
6. Anh Tho. (2023). Rethinking and redesigning youth movements to meet the demands of a new era. Government News. https://baochinhphu.vn/can-suy-nghi-thiet-ke-phong-trao-thanh-nien-phu-hop-voi-giai-doan-moi-102230906124129871.htm
7. Alruthaya, A., Nguyen, T.-T., & Lokuge, S. (2021). The Application of Digital Technology and the Learning Characteristics of Generation Z in Higher Education. https://arxiv.org/abs/2111.05991
8. Anderson, M., & Jiang, J. (2018). Teens, Social Media & Technology 2018. Pew Research Center. https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018
9. Barati, M. (2023). Casual Social Media Use among the Youth: Effects on Online and Offline Political Participation. https://arxiv.org/abs/2312.10095
10. Bennett, W. L., & Segerberg, A. (2012). The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics. https://www.researchgate.net/publication/287393379_The_logic_of_connective_action_Digital_media_and_the_personalization_of_contentious_politics
11. Cortés-Ramos, A., Pavón-Rivera, D., & Águila-Urbano, C. (2021). Activism and Social Media: Youth Participation and Communication in the Malaga Student Environment. Sustainability, 13(18), 10485. https://www.mdpi.com/2071-1050/13/18/10485
12. Deloitte. (2025). 2025 Gen Z and Millennial Survey. https://www.deloitte.com/content/dam/assets-shared/docs/campaigns/2025/2025-genz-millennial-survey.pdf

13. Hassoun, A., Beacock, I., Consolvo, S., Goldberg, B., Kelley, P. G., & Russell, D. M. (2023). Practicing Information Sensibility: How Gen Z Engages with Online Information. https://arxiv.org/abs/2301.07184
14. ResearchGate. (2022). Barriers to Youth Civic Engagement on Social Media. https://www.researchgate.net/publication/360098123_Barriers_to_youth_civic_engagement_on_social_media

Vu Thi Lan Anh, doctor of philosophy (PhD)
Hanoi University of Mining and Geology
Nguyen Phuong Dong, PhD in geography
Hanoi University of Mining and Geology
Nguyen Thi Hong, master lecturer
Hanoi University of Mining and Geology
Vietnam

ASSESSMENT OF OIL SPILL IMPACTS AND DISPERSION ASSOCIATED WITH RIVER SAND MINING: A CASE STUDY IN THE LOWER RED RIVER, VIETNAM

Abstract: *River sand mining relies on dredging vessels, pumps, generators, and waterborne transport, creating a potential risk of oil leakage and spills directly into the aquatic environment. This study assesses potential spill sources, hydrodynamic conditions, oil dispersion, and environmental impacts associated with an oil-spill scenario at a sand mine in the lower Red River. Flow conditions were surveyed using an Acoustic Doppler Current Profiler (ADCP) at seven cross-sections. The hydrodynamic model employed an unstructured mesh with element sizes of approximately 10–30 m, refined to about 10 m within the mining area. Cross-sectional mean velocities ranged from approximately 0.20 to 0.26 m/s, with discharges of 621.65–1,056.46 m³/s. Simulations of the existing and post-mining conditions indicated only minor changes in water level, whereas localized changes occurred in flow velocity and direction. The worst-case scenario assumed that the entire daily diesel oil (DO) demand of 1,036.5 L was continuously released over 24 h, equivalent to approximately 922.5 kg/day and 38.44 kg/h, with particle trajectories updated at 5-min intervals. The oil slick was initially concentrated around the source and subsequently elongated along the prevailing flow direction over 30–120 min. The results highlight the importance of the flow field, surface wind, oil properties, and release rate in predicting oil trajectories and planning spill-response measures.*

Keywords: *sand mining; oil spill; dispersion modeling; environmental risk.*

1. INTRODUCTION

River sand mining supplies essential construction materials but may alter bed morphology, velocity distribution, flow direction, and bank stability. In addition to morphological and hydraulic impacts, dredging vessels and mechanical equipment pose risks of oil contamination through fuel-system leakage, refueling, maintenance activities, tank damage, or vessel accidents. Previous studies on in-channel aggregate extraction have shown that bed lowering can induce hydraulic and morphological changes ranging from local effects to river-reach-scale responses (Kondolf, 1997; Rinaldi et al., 2005; Koehnken & Rintoul, 2018).

Once released into the aquatic environment, oil is simultaneously affected by spreading, advection, diffusion, evaporation, dissolution, dispersion, oxidation, oil–particle interactions, and biodegradation (National Research Council, 2003; Spaulding, 2017; Reed et al., 1999; Fingas, 2017; Lee et al., 2015; Gong et al., 2014). For diesel oil, aromatic hydrocarbons and oil associated with suspended particulate matter may be toxic to aquatic organisms and can ultimately be transferred to sediments (Fingas, 2017; Incardona et al., 2004; Carls et al., 1999; Barron et al., 2004; Peterson et al., 2003). Oil-trajectory modeling is therefore an important tool for predicting affected areas, estimating arrival times at sensitive receptors, and allocating spill-response resources (Spaulding, 2017; Reed et al., 1999; ITOPF, 2014).

Although research on river sand mining has largely focused on channel morphology, hydrodynamics, bank erosion, and water quality, the risk of oil spills from vessels and mining equipment operating directly on rivers has received comparatively limited attention from a dispersion-modeling perspective. In particular, mining-induced changes in the flow field may modify the direction and spatial extent of oil transport during an accidental release. Integrating hydrodynamic modeling with oil-spill simulation is therefore useful for delineating potentially affected areas and supporting environmental emergency-response planning.

2. RESEARCH METHODOLOGY

2.1. Study area

The sand mine covers approximately 3.92 ha and is located in the lower Red River in the Nam Tien Hai area.

2.2. ADCP flow survey

Flow was measured at seven cross-sections: MC1–MC2 upstream, MC3–MC5 within the mining area, and MC6–MC7 downstream (Figure 1). Measurements were obtained using an Acoustic Doppler Current Profiler (ADCP), which provides velocity distributions over depth and across a cross-section and is well suited to large rivers and tidally influenced environments (Simpson & Oltmann, 1993; Mueller et al., 2013).

Figure 1. Locations of the surveyed cross-sections

Table 1.

Summary of hydrological survey data for the mining area

Cross-section	Cross-section width B (m)	Wetted cross-sectional area F (m²)	Mean cross-sectional velocity Vmean (m/s)	Discharge Q (m³/s)	Maximum depth Hmax (m)
MC1	358.91	4,136.56	0.26	621.65	16.12
MC2	269.40	3,195.54	0.20	634.99	14.62
MC3	343.44	3,621.11	0.20	708.12	13.12
MC4	348.28	3,726.06	0.20	755.98	12.12
MC5	387.91	4,020.81	0.22	883.33	11.62
MC6	400.08	3,978.48	0.26	1.046.95	11.62
MC7	358.91	4,136.56	0.26	1.056.46	14.12

The velocity distributions across selected cross-sections are shown below:

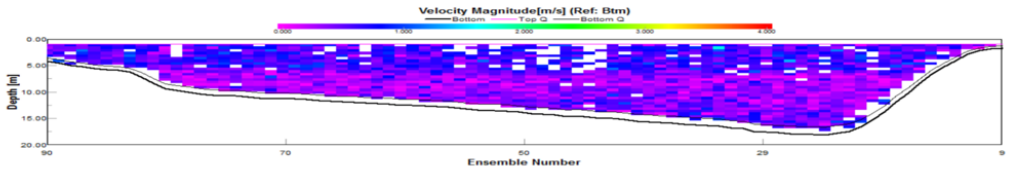

Figure 2. Flow velocity distribution across cross-section MC1

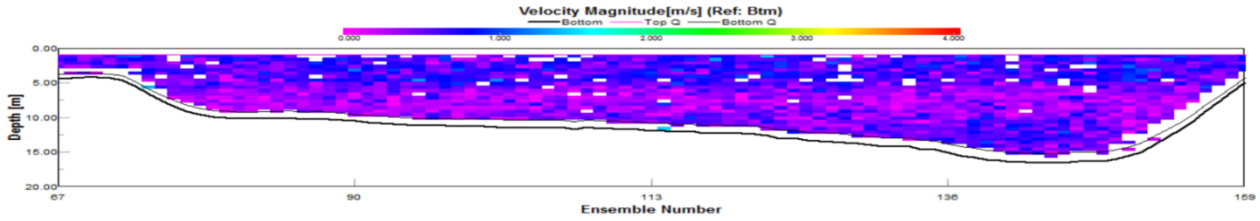

Figure 3. Flow velocity distribution across cross-section MC2

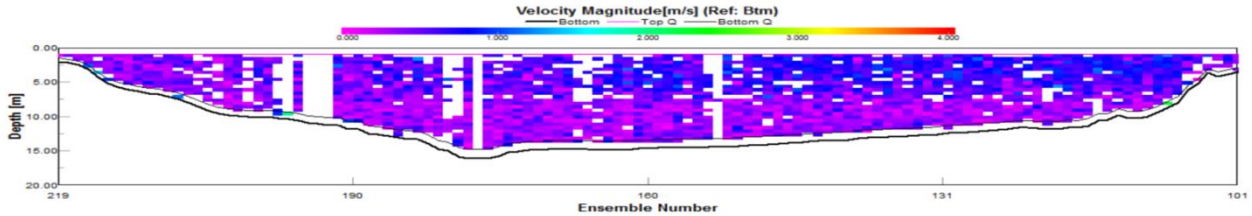

Figure 4. Flow velocity distribution across cross-section MC7

2.3. Hydrodynamic model

The model is based on the Reynolds-averaged Navier–Stokes equations for an incompressible fluid, together with the Boussinesq approximation and hydrostatic-pressure assumption. The horizontal domain was discretized using an unstructured mesh with element sizes of approximately 10–30 m and refined to about 10 m within the mining area. Two scenarios were compared: the existing bathymetry and the post-mining bathymetry with a lowered bed elevation, both subjected to representative flood conditions associated with Typhoon Yagi in September 2024. Flexible-mesh hydrodynamic modeling is well suited to river–estuary systems with complex geometries (DHI, 2017; Hervouet, 2007).

2.4. Oil-spill scenario

The total diesel oil demand of the mining operation is 1,036.5 l/day. Assuming a density of 0.89 kg/L, this corresponds to approximately 922.5 kg/day. The adverse scenario assumes that the entire amount is released continuously over 24 h from a source located near the center of the mining area, corresponding to a release rate of approximately 38.44 kg/h. Trajectories were updated at 5-min intervals and analyzed at 0, 30, 60, and 120 min. Key oil-model inputs include oil type and quantity, release rate, currents, tides, wind, and temperature (Spaulding, 2017; Reed et al., 1999; French-McCay, 2004).

3. RESULTS AND DISCUSSION

3.1. Hydrodynamic characteristics

The surveyed cross-sections were approximately 269–400 m wide. Cross-sectional mean velocities ranged from 0.20 to 0.26 m/s, while measured discharges ranged from 621.65 to 1,056.46 m³/s. Velocity distributions varied over both depth and channel width, reflecting the influence of channel morphology, tidal forcing, and local flow structures.

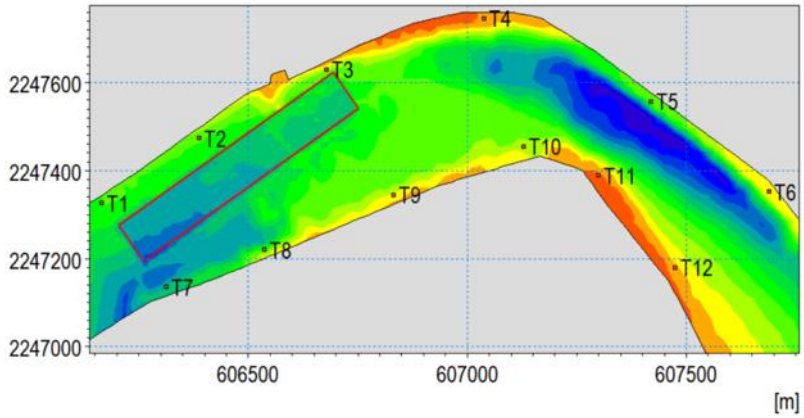

Figure 5. Locations of model-output extraction points

Water level:

Within the study area, including both the left and right banks, the simulations indicate that water levels remain virtually unchanged relative to the existing condition. Water-level variations at the monitoring points are very small, generally ranging from −0.002 to 0.006 m. Along the left bank, most monitoring points from T1 to T6 show mean water-level differences of zero or near zero, indicating no localized water-level rise along the bank. At T3, a slight increase is observed, with a mean value of approximately 0.004 m. This is mainly attributable to the change in bed morphology after lowering the bed elevation, which modifies the local flow distribution and produces slight water accumulation near the mining area. However, this increase is negligible. Similarly, along the right bank, water levels at T7–T12 after mining are nearly identical to those under existing conditions, with mean differences of approximately ±0.001 m. T9 and T10 also show very small, localized, and intermittent increases.

Flow velocity:

- Reach 1 (T1–T3): This bank segment runs parallel to the longitudinal boundary of the mining area. The simulations show a slight decrease in flow

velocity after bed lowering compared with the existing condition. Mean velocity decreases by approximately 0.026 m/s at T1, 0.060 m/s at T2, and 0.081 m/s at T3. The time series indicate that these reductions are most pronounced during strong flood- and ebb-tidal phases. The principal reason is that bed lowering locally enlarges the flow cross-section, disperses flow energy, and reduces near-bank current intensity.

- Reach 2 (T4–T6): This bank segment is located downstream of the mining area. At these points, flow velocity increases slightly after mining during some periods of strong tidal flow, with mean increases of approximately 0.005 m/s at T4, 0.003 m/s at T5, and 0.002 m/s at T6.

- The overall pattern of velocity variation is similar to that along the left bank, but the magnitude of change is smaller. At T7–T10, post-mining velocities are only slightly lower, with mean reductions ranging from 0.013 to 0.041 m/s. The decrease is stable and no abrupt periods of velocity increase are observed.

- At T11 and T12, the velocity time series for the two scenarios are nearly coincident, with only very small increases (below 0.004 m/s).

Flow direction:

Changes exceeding 1° are observed at several locations, notably T1, T3, and T11. At T3, the mean flow direction decreases by approximately 1.64°, indicating that the current becomes more oblique toward the bank than under existing conditions. This location warrants attention because such a directional change may increase the risk of localized bank erosion. At T11, the mean flow direction increases by approximately 2.28°; however, this point is farther from the mining area and the directional change is not accompanied by an increase in velocity, so the potential adverse impact is limited. The remaining locations show no substantial change in flow direction.

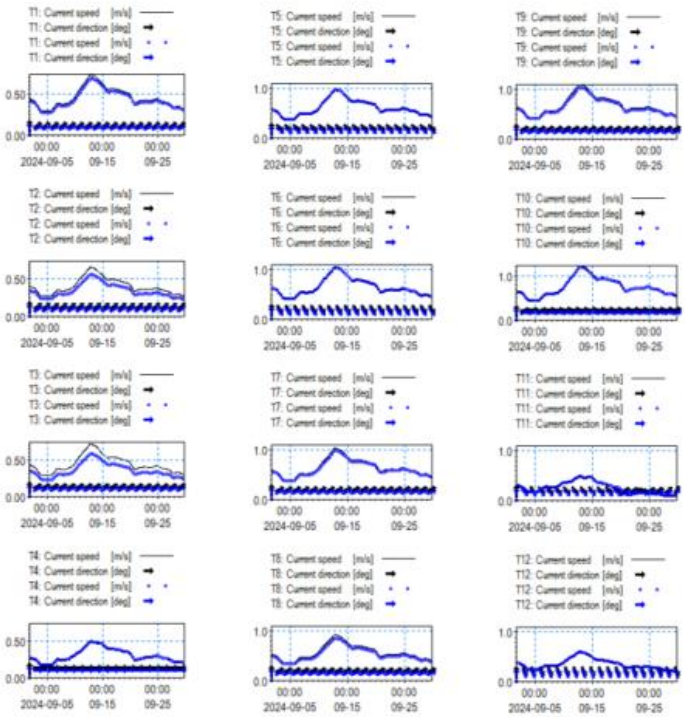

Figure 6. Time series of flow velocity at 12 bank-side points

3.2. Mining-induced changes in the flow field

Water-level differences between the two scenarios were generally between −0.002 and 0.006 m. Along the left bank, mean velocity at T1–T3 decreased by approximately 0.026–0.081 m/s, whereas T4–T6 showed slight increases of about 0.002–0.005 m/s. Along the right bank, velocities at T7–T10 decreased by approximately 0.013–0.041 m/s, while changes at T11–T12 were very small. Changes in flow direction were below 1° at most locations; however, the mean direction at T3 decreased by approximately 1.64°, while that at T11 increased by about 2.28°. Thus, bed lowering did not substantially alter the overall water-level regime but could locally redistribute flow velocity and direction.

3.3. Oil-spill dispersion

At the onset of the release, oil was concentrated around the source. After 30 min, the slick elongated along the principal flow direction but remained largely within the mining area and adjacent waters. After 60 min, its spatial extent increased. By 120 min, the slick formed a relatively continuous band along the near-bank current, while oil density near the source decreased as the oil was advected and dispersed. This evolution is consistent with oil-trajectory behavior that is initially controlled by currents and wind while simultaneously undergoing weathering processes (National Research Council, 2003; Spaulding, 2017; Reed et al., 1999).

The simulation indicates that under a continuous release at a relatively low rate (38.44 kg/h), the slick does not develop abruptly at high density; rather, it forms and spreads progressively over time, directly controlled by the prevailing current regime and surface wind at the time of the incident.

At the onset of the incident (Figure 7), the amount of newly released oil is small relative to the transport capacity of the flow; consequently, the oil remains concentrated mainly around the spill source. The affected area is still limited, and the oil has not yet spread widely into surrounding waters.

After 60 min (Figure 9), as oil continues to enter the environment, the spatial extent of the slick increases more clearly. The slick is transported along the prevailing flow direction. Although the affected area expands, oil density within individual areas tends to decrease because the oil is advected and dispersed over a larger area.

After 120 min (Figure 10), the slick forms a relatively continuous band along the near-bank flow direction. Oil density near the source gradually decreases as the oil is transported and dispersed spatially.

Figure 7. Oil slick location at the onset of the spill

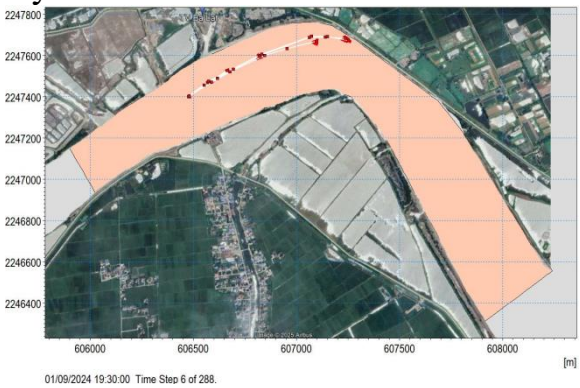

Figure 8. Oil spill trajectory 30 minutes after the onset of the spill

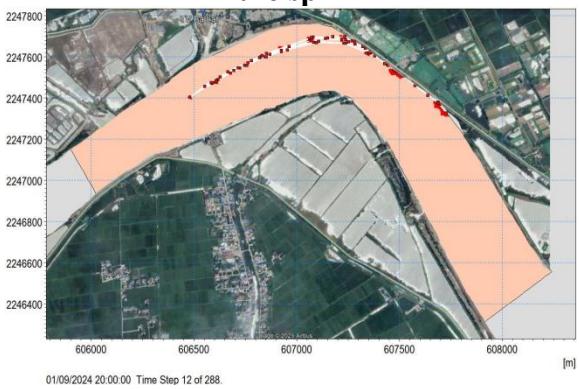

Figure 9. Oil spill trajectory 60 minutes after the onset of the spill

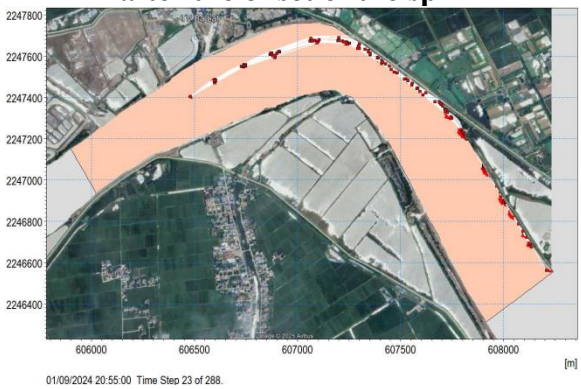

Figure 10. Oil spill trajectory 120 minutes after the onset of the spill

3.4. Discussion

During dispersion, a decrease in oil density at the water surface does not imply that the oil has been completely removed from the environment. A fraction may evaporate, dissolve, or disperse into the water column, while the remainder may undergo oxidation and biodegradation or become associated with suspended particles and settle to the bed (National Research Council, 2003; Fingas, 2017; Lee et al., 2015; Gong et al., 2014). In sand-mining areas, dredging and sand unloading disturb sediments and may increase suspended-solid concentrations. Consequently, oil may adhere to these particles and accumulate in bottom sediments (Lee et al., 2015; Gong et al., 2014).

Diesel oil contains numerous hydrocarbon constituents that can adversely affect aquatic organisms. In particular, some polycyclic aromatic hydrocarbons (PAHs) may cause toxicity and impair fish development, physiological function, and reproduction (Incardona et al., 2004; Carls et al., 1999; Barron et al., 2004; Peterson et al., 2003). Eggs and larvae are generally more sensitive to oil contamination than adult fish. For benthic organisms, effects may persist when oil associates with suspended matter, settles, and accumulates in sediments.

The simulation shows that the slick was transported predominantly by the flow field during the first 120 min, consistent with Reed et al. (Reed et al., 1999) and Spaulding (Spaulding, 2017), who emphasized the dominant role of the velocity field in controlling oil trajectories during the early stage of a spill. However, because post-mining changes in flow velocity and direction in the study area were relatively small, the influence of bed lowering on the oil trajectory was primarily local.

CONCLUSIONS

This study integrated ADCP observations, hydrodynamic modeling, and an oil-spill scenario to assess spill risk at a river sand mine. Surveys at seven cross-sections showed mean velocities of 0.20–0.26 m/s and discharges of 621.65–1,056.46 m^3/s. Bed lowering had little effect on the overall water level but produced localized changes in flow velocity and direction. Under the scenario in which 1,036.5 L of diesel oil per day was released continuously over 24 h, the modeled source rate was approximately 38.44 kg/h, and the slick was clearly transported by the flow field during the first 30–120 min. The results indicate that mining-induced changes in velocity and flow direction are primarily local, whereas water levels remain nearly unchanged. Under the hypothetical spill scenario, the flow field controls the direction of oil transport during the first 120 min, causing the slick to extend downstream along the riverbank. Oil-spill risk assessment for river sand mining should therefore integrate hydrodynamic conditions, spill-source location, and sensitive downstream receptors. These results can support the delineation of priority response zones and the strategic placement of oil-spill containment and control equipment at river sand-mining sites.

Acknowledgements

The authors thank the HUMG project “Research on the impact of sand mining activities in the Tra Ly River area, Hung Yen Province using the MIKE21SW – HD – MT model” under Project Code: T26-38.

REFERENCES

1. Kondolf, G.M. (1997). Hungry water: Effects of dams and gravel mining on river channels. Environmental Management, 21, 533–551.
2. Rinaldi, M., Wyzga, B., & Surian, N. (2005). Sediment mining in alluvial channels: Physical effects and management perspectives. River Research and Applications, 21, 805–828.
3. Koehnken, L., & Rintoul, M.S. (2018). Impacts of Sand Mining on Ecosystem Structure, Process and Biodiversity in Rivers. WWF.

4. National Research Council. (2003). Oil in the Sea III: Inputs, Fates, and Effects. National Academies Press..
5. Spaulding, M.L. (2017). State of the art review and future directions in oil spill modeling. Marine Pollution Bulletin, 115, 7–19.
6. Reed, M., Johansen, Ø., Brandvik, P.J., Daling, P., Lewis, A., Fiocco, R., Mackay, D., & Prentki, R. (1999). Oil spill modeling towards the close of the 20th century: Overview of the state of the art. Spill Science & Technology Bulletin, 5, 3–16.
7. Fingas, M. (Ed.). (2017). Oil Spill Science and Technology. Elsevier.
8. Lee, K., Boufadel, M., Chen, B., Foght, J., Hodson, P., Swanson, S., & Venosa, A. (2015). Expert Panel Report on the Behaviour and Environmental Impacts of Crude Oil Released into Aqueous Environments. Royal Society of Canada.
9. Gong, Y., Zhao, X., Cai, Z., O'Reilly, S.E., Hao, X., & Zhao, D. (2014). A review of oil, dispersed oil and sediment interactions in the aquatic environment. Marine Pollution Bulletin, 79, 16–33.
10. Incardona, J.P., Collier, T.K., & Scholz, N.L. (2004). Defects in cardiac function precede morphological abnormalities in fish embryos exposed to polycyclic aromatic hydrocarbons. Toxicology and Applied Pharmacology, 196, 191–205.
11. Carls, M.G., Rice, S.D., & Hose, J.E. (1999). Sensitivity of fish embryos to weathered crude oil: Part I. Environmental Toxicology and Chemistry, 18, 481–493.
12. Barron, M.G., Carls, M.G., Heintz, R., & Rice, S.D. (2004). Evaluation of fish early life-stage toxicity models of chronic embryonic exposures to complex PAH mixtures. Toxicological Sciences, 78, 60–67.
13. Peterson, C.H., Rice, S.D., Short, J.W., Esler, D., Bodkin, J.L., Ballachey, B.E., & Irons, D.B. (2003). Long-term ecosystem response to the Exxon Valdez oil spill. Science, 302, 2082–2086.
14. ITOPF. (2014). Fate of Marine Oil Spills. Technical Information Paper 2.
15. Simpson, M.R., & Oltmann, R.N. (1993). Discharge-Measurement System Using an Acoustic Doppler Current Profiler with Applications to Large Rivers and Estuaries. USGS Water-Supply Paper 2395.
16. Mueller, D.S., Wagner, C.R., Rehmel, M.S., Oberg, K.A., & Rainville, F. (2013). Measuring Discharge with Acoustic Doppler Current Profilers from a Moving Boat. USGS Techniques and Methods 3-A22.
17. DHI. (2017). MIKE 21 & MIKE 3 Flow Model FM: Hydrodynamic and Transport Module, Scientific Documentation.
18. Hervouet, J.-M. (2007). Hydrodynamics of Free Surface Flows: Modelling with the Finite Element Method. Wiley.
19. French-McCay, D.P. (2004). Oil spill impact modeling: Development and validation. Environmental Toxicology and Chemistry, 23, 2441–2456.
20. National Academies of Sciences, Engineering, and Medicine. (2022). Oil in the Sea IV: Inputs, Fates, and Effects. The National Academies Press.

УДК: 615.825

Андреева В. Л.
студент
Уральский государственный медицинский университет
Белослудцева А. Д.
студент
Кочугова Г. А.
старший преподаватель
кафедра физического воспитания и спорта
Уральский государственный лесотехнический университет
Научный руководитель: Малозёмов О. Ю., канд. пед. наук,
доцент кафедры физической культуры
Уральский государственный медицинский университет
Россия, Екатеринбург

ПРОФИЛАКТИКА ОНКОЛОГИЧЕСКИХ ЗАБОЛЕВАНИЙ СРЕДСТВАМИ ФИЗИЧЕСКОЙ КУЛЬТУРЫ

Аннотация: *кратко представлено системное воздействие ЛФК при первичной и вторичной профилактике (реабилитации) в онкологии.*

Ключевые слова: *ЛФК, профилактика, онкологические заболевания.*

Andreeva V. L.
student
Ural State Medical University
Belosludtseva A. D.
student
Kochugova G. A.
senior lecturer
department of physical education and sports
Ural State Forestry University
Scientific Advisor: Malozemov O. Yu., PhD in pedagogy,
associate professor
department of physical education
Ural State Medical University
Russia, Yekaterinburg

PREVENTION OF CANCER DISEASES BY MEANS OF PHYSICAL CULTURE

Abstract: *The article presents the systemic impact of therapeutic physical culture in primary and secondary prevention (rehabilitation) in oncology.*

Keywords: *therapeutic physical culture, prevention, cancer patients.*

Актуальность диагностики и лечения злокачественных новообразований активизирует поиск и внедрение эффективных превентивных стратегий. В контексте привлекающих внимание модифицируемых факторов образа жизни, потенциал физической культуры многобразнее общего оздоровления посредством ведения здорового образа жизни. Так, лечебная физическая культура (ЛФК), являясь специализированным разделом клинической медицины, использует средства физической культуры для лечения и профилактики заболеваний, восстановления трудоспособности и адаптации пациентов. Поскольку разрабатываются новые методики и открываются новые возможности ЛФК, то кратко проанализируем роль и механизмы воздействия средств ЛФК в онкопрофилактике.

Основу ЛФК составляют строго дозированная, методически организованная двигательная активность [1]. Внимание в ЛФК акцентируется на базовом свойстве организма – способности к адаптации. Основные принципы любой эффективной и безопасной методики ЛФК: 1) индивидуализации (учёт половозрастных особенностей, психофизического состояния, сопутствующих заболеваний); 2) систематичности и регулярности (постоянство в проведении занятий для достижения кумулятивного эффекта); 3) постепенности наращивания нагрузок (поэтапное повышение интенсивности, продолжительности и сложности упражнений); 4) разнообразия средств (для комплексного воздействия необходимы различные формы ЛФК); 5) сознательности и активности, т.е. понимание цели занятий [1].

Системное воздействие физической культуры проявляется на уровне основных физиологических систем: 1) сердечно-сосудистой (регулярные тренировки повышают сократительную способность миокарда, улучшают микроциркуляцию и обеспечивают оптимальное кровоснабжение всех тканей); 2) дыхательной (увеличивается жизненная ёмкость лёгких, усиливается оксигенация крови); 3) нервной (нормализуется тонус ЦНС, приводящий к гармонизации психоэмоционального состояния); 4) опорно-двигательного аппарата (укрепление мышц и связок нормализует обмен веществ в соединительной ткани).

Таким образом, за счёт систематической двигательной активности создаётся повышенный общеукрепляющий фон, способствующий формированию в организме «противоопухолевой среды» [3]. Концепция миокинов (биологически активных пептидов или белков, вырабатываемых и выделяющихся скелетными мышцами при сокращении) предполагает их влияние на различные органы и системы дистанционно (подобно гормональному), в широком диапазоне, в том числе и в противоопухолевом. Исследования показывают, что после физической нагрузки сыворотка крови снижает жизнеспособность раковых клеток (в сравнении с сывороткой, взятой в состоянии покоя) за счёт роста уровня миокинов с онкостатической активностью [4]. Наиболее эффективны силовая и высокоинтенсивная

интервальная нагрузка. В целом, регулярные физические нагрузки направлены на ключевые звенья патогенеза рака, являясь первичной профилактикой по предотвращению заболевания у здоровых людей.

Кроме того, физическая культура и лечебная гимнастика – основа реабилитационных программ (т.е. вторичная профилактика) для онкобольных на этапе восстановления после лечения [2]. В этом случае ЛФК решает следующие специфические задачи: 1) борьба с синдромом хронической усталости (за счёт постепенности повышения толерантности к физической нагрузке и улучшения энергообмена); 2) профилактика и лечение лимфедемы (отёка конечности), когда специальные упражнения в сочетании с дыхательной гимнастикой и мануальным лимфодренажем активизируют лимфоотток; 3) поддержание и восстановление объёма движений (после операций), силы и мышечной массы (при кахексии); 4) профилактика осложнений ССС, вызванных некоторыми видами химиотерапии (кардиотоксичность). При индивидуальной программе ЛФК всё это снижает инвалидизирующие последствия лечения, улучшая качество жизни пациента.

В лечении и профилактике любого заболевания кроме физического аспекта важна также и психокоррекционная составляющая. В самом диагнозе «рак» заключена огромная стрессогенная нагрузка, зачастую приводящая к повышению тревожности, развитию депрессивных расстройств, социальной изоляции, экзистенциальному кризису личности и пр. Двигательные нагрузки и ЛФК во многих случаях являются сильным психокоррекционным фактором, способствуя следующим процессам и состояниям: 1) повышают самооценку и чувство самоконтроля, утраченные при заболевании; 2) снижают уровень тревожности за счёт нейробиохимических механизмов (выработки эндорфинов, снижению кортизола); 3) нормализуют сон; 4) способствуют усилению социальной поддержки (особенно групповые занятия, на которых общаются пациенты со схожими переживаниями). В этом проявляется суть вторичной профилактики при онкологической реабилитации с помощью ЛФК, что входит в её интегративную функцию.

Кратко формулируя условия проведения физкультурно-оздоровительных занятий с целью профилактики онкозаболеваний, можно сказать, что необходимо сочетать аэробные и силовые нагрузки, в совокупности, обеспечивающие комплексное воздействие на все звенья патогенеза.

В заключение отметим следующее. 1. ЛФК – один из методов медицинского воздействия, основу которого составляют принципы индивидуализации, систематичности и постепенности, входящие в реализуемые поэтапные программы под контролем специалиста. 2. Противоопухолевый профилактический эффект ЛФК реализуется через сложный комплекс разноуровневых взаимосвязанных механизмов и процессов: метаболического, гормонального, иммунного, противовоспалительного, антиоксидантного, стресс-протекторного и общесистемного. 3. Онкостатическое воздействие физических нагрузок,

проявляется в подавлении пролиферации и жизнеспособности раковых клеток, что сравнимо с фармакологическим вмешательством. 4. В плане вторичной профилактики ЛФК способствует преодолению и соматических последствий лечения, и положительному психосоциальному воздействию. Таким образом, сочетание регулярной повседневной физической активности и включение методик ЛФК в стандарты медицинской помощи онкологическим пациентам необходимы, экономически эффективны и научно обоснованы как компоненты комплексной стратегии борьбы с онкозаболеваниями.

Использованные источники:

1. Грушина Т.И. Реабилитация в онкологии: физиотерапия. – М.: ГЭОТАР-Медиа, 2006. 240 с.
2. Черных З.Н., Борисенко Т.М. Физическая культура как средство профилактики заболеваний / Вестник ШГУ. №2(38). 2018. С.132-139.
3. Вайнер Э.Н. Лечебная физическая культура: учебник. – М.: Флинта, Наука, 2009. 424 с.
4. Francesco Bettariga, Dennis R. Taaffe, Cristina Crespo-Garcia, Timothy D. Clay, Mauro De Santi, Giulia Baldelli, Sanjeev Adhikari, Elin S. Gray, Daniel A. Galvão, Robert U. Newton. A single bout of resistance or high-intensity interval training increases anti-cancer myokines and suppresses cancer cell growth in vitro in survivors of breast cancer. Breast Cancer Research and Treatment, 2025. [Электронный ресурс]. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC12259798/ (дата обращения: 30.04.2026).

УДК 343.3/.7

Баландин Ф.Д.
студент
института прокуратуры
Московский государственный юридический университет
имени О.Е. Кутафина (МГЮА)
Научный руководитель: Пикуров Н.И., доктор юридических наук
профессор
кафедра уголовного права
Московский государственный юридический университет
имени О.Е. Кутафина (МГЮА)
г. Москва, Россия

ОБ ОТДЕЛЬНЫХ ПРОБЛЕМАХ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ, ПРЕДУСМОТРЕННЫХ СТАТЬЁЙ 272 УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: *В статье раскрываются проблемы квалификации преступлений, предусмотренных статьей 272 Уголовного кодекса Российской Федерации. Проанализированы статистические сведения о совершённых преступлениях в сфере компьютерной информации на основе данных, представленных Генеральной прокуратурой Российской Федерации. На основе обобщения проблемных аспектов квалификации преступлений по статье 272 УК РФ с учетом исследования судебной практики сформулированы выводы, которые могут быть использованы в борьбе с неправомерным доступом к охраняемой законом компьютерной информации.*

Ключевые слова: *прокуратура; преступления; компьютерная информация; квалификация; неправомерный доступ; крупный ущерб; совершенствование; признаки.*

Balandin F. D.
student
institute of prosecutor's office
Moscow State Law University named after O.E. Kutafin (MGLA)
Supervisor: Pikurov N.I., doctor of law,
professor
department of criminal law
Moscow State Law University named after O.E. Kutafin (MGLA)
Moscow, Russia

ON CERTAIN PROBLEMS OF QUALIFYING CRIMES UNDER ARTICLE 272 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION

Abstract: *The article reveals the problems of qualification of crimes under Article 272 of the Criminal Code of the Russian Federation. It analyzes statistical data on crimes committed in the field of computer information based on data provided by the General Prosecutor's Office of the Russian Federation. Based on a summary of the problematic aspects of the qualification of crimes under Article 272 of the Criminal Code of the Russian Federation, taking into account the analysis of judicial practice, the article formulates conclusions that can be used in the fight against unauthorized access to computer information protected by law.*

Keywords: *prosecutor's office; crimes; computer information; qualifications; unauthorized access; major damage; improvement; signs.*

Неправомерный доступ к компьютерной информации, ответственность за который предусмотрена статьей 272 Уголовного кодекса РФ, является наиболее распространенным и вместе с тем одним из самых сложных для квалификации составов преступлений в сфере компьютерной информации. Как справедливо отмечается в современной научной литературе, высокий уровень неопределенности в толковании понятий, связанных с неправомерным доступом к компьютерной информации, вполне закономерно вызывает отсутствие единообразной судебной и следственной практики применения данной статьи. Несмотря на активную разработку вопросов практического применения положений ст. 272 УК РФ в отечественной науке, многие аспекты квалификации данного посягательства остаются в настоящее время неразрешенными. В связи с этим анализ проблемных аспектов квалификации неправомерного доступа к компьютерной информации приобретает как теоретическое, так и прикладное значение, особенно в свете анализа судебной практики за последние три года.

Статистические данные свидетельствуют о значительном росте числа преступлений в сфере компьютерной информации. По данным Генеральной прокуратуры РФ, в 2022 году в России было зафиксировано 9308 преступлений в сфере компьютерной информации (рост на 45,6%), а в 2023 году правоохранительными органами уже зарегистрировано 37 101 подобное преступление (рост на 270%). При этом в суды направлены уголовные дела только по 1562 преступлениям (4,2%), а приостановлены по 26 095 преступлениям (70,4%). Столь низкий процент направления дел в суд во многом обусловлен сложностью квалификации и проблемами доказывания по данной категории уголовных дел.

Анализ судебной практики за 2019-2024 годы, проведенный экспертами на основе данных портала «Судебная статистика», показывает, что по статье 272 УК РФ судами вынесено наибольшее количество приговоров по сравнению с иными составами преступлений в сфере компьютерной информации. Количество приговоров с 2019 года значительно увеличилось: по части 1 статьи 272 УК РФ зафиксирован рост на 50%, а по квалифицированным составам (части 2-4) он составил почти четырехкратный рост. При этом суды рассматривают лишь около 1-2% от

возбужденных по данным статьям уголовных дел, что отчасти объясняется длительными сроками следствия по таким делам.1

Одной из наиболее значимых тенденций последних лет является изменение подхода правоохранительных органов к квалификации деяний, ранее относимых к иным статьям УК РФ. Как отмечают эксперты, статья 272 УК РФ стала инкриминироваться тем, чьи действия, по мнению следствия и судов, подпадали под другие составы. Речь идет, в частности, о продаже «левых» сим-карт работниками салонов связи, которых ранее часто судили по статье 274.1 УК РФ . По ней же привлекали также медиков, оформлявших подложные сертификаты о вакцинации, и продавцов на заправочных станциях за мелкие махинации с бонусными системами. Однако в 2025 году в таких случаях злоумышленникам инкриминируют как раз статью 272 УК РФ. Например, именно по части 3 статьи 272 УК РФ было возбуждено уголовное дело в отношении трех сотрудников салона мобильной связи в Перми, которые ради выполнения плана продаж оформили большое количество сим-карт на персональные данные случайных лиц. На аналогичную квалификацию по ч. 3 ст. 272 УК РФ ориентируется и следственная практика в Иркутской области, где директор магазина электроники без ведома граждан оформляла SIM-карты на их имена для последующего использования в незаконном обналичивании денежных средств.

Объективная сторона преступления, предусмотренного ст. 272 УК РФ, характеризуется тремя обязательными элементами: деянием в виде неправомерного доступа к компьютерной информации; последствиями в виде уничтожения, блокирования, модификации либо копирования компьютерной информации; причинно-следственной связью между деянием и наступившими последствиями. Каждый из указанных элементов порождает в правоприменительной практике самостоятельные проблемы квалификации.

Первая группа проблем связана с определением понятия «неправомерный доступ». Легальное определение данного термина в уголовном законе отсутствует, что вынуждает правоприменителя обращаться к доктринальным толкованиям и разъяснениям Пленума Верховного Суда РФ. Как разъясняет Пленум Верховного Суда РФ в Постановлении от 15 декабря 2022 г. № 37, под неправомерным доступом понимаются совершение действий, направленных на получение возможности ознакомления, обработки, копирования, модификации либо уничтожения компьютерной информации в отсутствие на то права у лица, в том числе с преодолением средств защиты.

В судебной практике встречаются примеры неоднозначного толкования признака неправомерности доступа. Показательным в этом отношении является дело, рассмотренное Судебной коллегией по уголовным делам Верховного Суда РФ (Кассационное определение от 3 апреля 2024 г. по делу

[1] Портал «Судебная статистика», данные о количестве приговоров по ст. 272 УК РФ за 2019–2024 годы.

№ 1-226/2021). Осужденный был признан виновным в неправомерном доступе к компьютерной информации в связи с нарушением условий лицензионного соглашения при использовании игровых консолей. Защита настаивала на том, что лицензионное соглашение не было доведено до пользователя, поскольку консоли приобретались без лицензионного системного программного обеспечения, а суд фактически установил нарушение не уголовного, а авторского права. Адвокат в кассационной жалобе утверждал, что суд, давая толкование определений «неправомерного доступа» и «компьютерной информации», сослался на взаимоисключающие правовые нормы и неверно применил нормы гражданского законодательства при определении правового режима неправомерного доступа к компьютерной информации. Данный пример иллюстрирует острую дискуссию о границах уголовно-правового понятия «неправомерный доступ» и его соотношении с гражданско-правовыми категориями.

Вторая группа сложностей при квалификации касается оценки последствий неправомерного доступа. Законодатель выделяет четыре варианта негативных изменений компьютерной информации: ее уничтожение, блокирование, видоизменение либо создание копии. Каждое из указанных понятий является оценочным, что порождает неединообразие судебной практики. В качестве иллюстрации можно привести одно из дел, где суд усмотрел в действиях подсудимого признаки модификации информации с применением специального программного обеспечения, предназначенного для обхода средств защиты. В то же время сторона защиты, ссылаясь на заключение эксперта, утверждала, что использованные приложения в принципе не способны привести к подобным последствиям, а сама система защиты была отключена иными способами. Данный случай наглядно демонстрирует, насколько сложным может быть установление причинно-следственной связи между применением вредоносного программного обеспечения и наступившей модификацией данных.

Третья группа проблем связана с субъективной стороной деяния и наличием квалифицирующих признаков. Практике известны примеры осуждения лиц за совершение неправомерного доступа из корыстных побуждений. В том же деле один из эпизодов был квалифицирован именно по данному признаку. Кроме того, эксперты отмечают, что в последние годы нормы главы 28 УК РФ, включая статью 272, все чаще применяются в совокупности с традиционными составами, прежде всего с мошенничеством. Так, жителю Челябинска вменяли одновременно неправомерный доступ и мошенничество за то, что он оформлял кредиты на посторонних граждан, получая их личные данные через взломанные аккаунты на интернет-сервисах.

Четвертая группа проблем касается судебной практики назначения наказания. Статистика последних лет свидетельствует, что суды крайне редко приговаривают виновных по статье 272 УК РФ к реальному лишению свободы. Согласно исследованию, проведенному одной из профильных

компаний, лишь 5% дел в сфере информационной безопасности завершаются реальными сроками. Гораздо чаще назначаются штрафы, условные меры либо запрет на занятие определенных должностей. В 2023 году в перечень возможных наказаний была включена конфискация имущества, однако на сегодняшний день сведений о ее применении не имеется. Приговоры с реальной изоляцией от общества хотя и стали выноситься с 2021 года (ранее такие случаи отсутствовали), но их доля остается незначительной и демонстрирует неустойчивую динамику. Примечательно, что удельный вес условных сроков и штрафов, преобладавших в 2019-2021 годах, заметно снизился, тогда как суды стали активнее применять такие альтернативные меры, как ограничение свободы, обязательные или исправительные работы. В упомянутом деле подсудимому по части 2 статьи 272 УК РФ было назначено наказание в виде одного года ограничения свободы, а при совокупности преступлений — двух лет ограничения свободы с дополнительным штрафом.

Пятая группа проблем связана с отграничением состава, предусмотренного статьей 272 УК РФ, от смежных составов и административных правонарушений. Ключевое значение здесь имеет разграничение с созданием и применением вредоносных программ по статье 273 УК РФ. Судебная практика нередко идет по пути одновременного осуждения лица по нескольким эпизодам обеих статей. В уже рассмотренном деле подсудимый был признан виновным по четырем эпизодам, подпадающим под части первую и вторую статьи 272 УК РФ, а также по трем эпизодам, квалифицированным по частям первой и второй статьи 273 УК РФ. При этом апелляционная инстанция освободила его от штрафа по первому составу в связи с истечением сроков давности.

Не менее важно различать неправомерный доступ (статья 272) и нарушение правил эксплуатации средств хранения и обработки компьютерной информации (статья 274). Основной критерий здесь - субъект преступления. По статье 274 ответственность несет лицо, имеющее законный доступ к информации, но нарушившее правила ее эксплуатации. По статье 272 — лицо, которое такого права не имело либо превысило его допустимые пределы.

Обобщая анализ проблемных аспектов квалификации преступлений по статье 272 УК РФ с учетом судебной практики последних трех лет, можно сформулировать ряд выводов.

Главные сложности квалификации обусловлены неопределенностью содержания понятия «неправомерный доступ» (что ярко проявилось в деле, где защита настаивала на гражданско-правовом, а не уголовном характере нарушения), оценочным характером последствий, трудностями доказывания причинно-следственной связи в цифровой среде, а также необходимостью разграничения умысла и неосторожности при наступлении вредных последствий.

Квалифицирующие признаки - корыстная заинтересованность, крупный ущерб, использование служебного положения - также вызывают сложности в правоприменении. Статистика свидетельствует, что при резком росте регистрируемых преступлений (в 2023 году прирост составил 270%) до суда доходит лишь незначительная часть дел (около 4,2%), что говорит о серьезных проблемах с раскрываемостью и расследованием данной категории уголовных дел.

Судебная практика по статье 272 УК РФ отличается преимущественно мягким подходом: реальное лишение свободы назначается только в 5% случаев, преобладают ограничение свободы, штрафы и условные меры.

В целях совершенствования правоприменения, на наш взгляд, представляется целесообразным выработать единые подходы к толкованию категории «неправомерный доступ», четко отграничив его от нарушений авторского права, а также разработать унифицированную методику расчета крупного ущерба. Выявленные проблемы будут учтены при последующем анализе квалификации преступлений по статье 273 УК РФ и рассмотрении совокупности компьютерных преступлений с посягательствами на собственность.

Использованные источники:

1. Конституция Российской Федерации, принята всенародным голосованием 12 декабря 1993 года.
2. Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.
3. Федеральный закон от 27 июля 2006 года № 149-ФЗ (ред. от 26 июня 2026 года) «Об информации, информационных технологиях и о защите информации» // Российская газета. – 2026. - 01 июля 2026 года. - № 141–142.
4. Постановление Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание Законодательства РФ от 5 ноября 2012 года. № 45 ст. 6257.
5. Постановление Пленума Верховного Суда РФ от 15 декабря 2022 года № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет"» // Российская газета. – 2022. – 28 декабря. – № 294.
6. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 года) // Совет Европы. Документ зарегистрирован в Европейской серии договоров (European Treaty Series, ETS) под номером ETS № 185.

УДК 377.13

Кумушкина Н. Ю.
заведующая отделением
политехнический колледж
Новгородский государственный университет
Научный руководитель: Шульцев В. А. к.ю.н.
директор
политехнический институт
НовГУ
г. Великий Новгород, РФ

ПОДГОТОВКА КАДРОВ ДЛЯ ЭЛЕКТРОЭНЕРГЕТИКИ В ПОЛИТЕХНИЧЕСКОМ КОЛЛЕДЖЕ

Аннотация. *В данной статье представлены результаты образовательного исследовательского проекта, направленного на подготовку студентов инженерных специальностей к практической работе в электроэнергетике. Предлагается система развития будущих специалистов, включающая выбор учебного плана, развитие специализированных навыков и выбор карьеры на основе психологических и педагогических оценок.*

Ключевые слова: *дежурный электромонтер (ДЭМ), начальник смены электроцеха ТЭЦ, задачи энергетического производства, релейная защита и автоматика Р (ЗиА), технология обучения чтению схем.*

Kumushkina N.Yu.
head of department, polytechnic college
Novgorod State University
Scientific supervisor: Shultsev V. A., Ph.D.
director of the polytechnic institute
NovSU
Veliky Novgorod, Russian Federation

TRAINING OF PERSONNEL FOR THE ELECTRIC POWER INDUSTRY AT THE POLYTECHNIC COLLEGE

Abstract. *This article presents the results of an educational research project aimed at preparing engineering students for practical work in the electric power industry. A development system for future specialists is proposed, including curriculum selection, specialized skill development, and career selection based on psychological and pedagogical assessments.*

Key words: *duty electrician (DEM), shift supervisor of the electrical shop of the thermal power plant, tasks of energy production, relay protection and automation of the R (ZiA), technology for teaching reading diagrams.*

Введение

Промышленный труд — это специфическая форма человеческого труда, возникшая на определённом этапе развития технологий и производства в целом. Поэтому изучение характеристик промышленного труда и подготовка специалистов в этой области имеют решающее значение для решения задач развития энергопроизводства. Исследованиями по развитию человеческих ресурсов для промышленного труда в энергетическом секторе занимались такие учёные-энергетики, как А.Ф. Дяков, Е.Н. Зуев, А.И. Соловьев и В.И. Чернышев.

Эксплуатация энергетических установок и энергетических систем требует постоянной концентрации, преодоления монотонности и стресса, повышенного чувства ответственности и связанного с этим умственного напряжения. Эта работа требует не только специализированной подготовки для обеспечения надежной работы систем управления, но и специфических физических и умственных качеств. К этим качествам относятся концентрация, способность действовать с необходимой точностью, способность переключать внимание с одного события на другое, способность четко различать их важность и способность расставлять приоритеты в техническом обслуживании. Кроме того, требуется отличная память и точность (для работы в соответствии с основными правилами и инструкциями), а также сильная воля (для управления подчиненными) [1]. Наблюдается достаточно устойчивая корреляция между этими качествами и другими личностными чертами. Поэтому, если имеется информация о конкретной личностной черте, можно надежно оценить и другие качества, важные для оперативной работы [2].

Следует отметить, что требования к специализированным навыкам оперативнова персонала в энергетических компаниях значительно возрастают. От оперативного персонала требуется владение новейшими компьютерными технологиями для обработки данных. Особое значение имеет умение точно оценивать потенциальное воздействие временных и аварийных условий производства на окружающую среду, а также способность проводить технико-экономический анализ различных конфигураций оборудования и режимов работы.

Оперативная деятельность и управление определяют, как оператор устанавливает начальные условия для конкретной задачи, корректирует процесс генерации энергии и получает информацию от компьютера для замыкания контура обратной связи с внешними датчиками, рабочими элементами и средой выполнения задачи. [3] Работа автоматизированной системы зависит от бесперебойной работы ее технических компонентов и своевременной, безошибочной и надежной работы специалистов, управляющих этими системами. Ошибки оператора допустимы, если они не мешают нормальной работе системы. Однако ошибки оператора всегда являются ненормальными, даже если они не приводят к серьезному сбою системы.

Как показывает опыт сотрудников отдела оперативного управления, социально-психологические факторы играют решающую роль в обеспечении качества работы. В частности, к ним относятся восприятие сотрудниками важности своей работы, их чувство ответственности за надлежащее функционирование районов, городов, регионов, энергетических компаний и энергетических систем, их удовлетворенность результатами работы, психологическая атмосфера внутри отдела оперативного управления и взаимопонимание между коллегами.

Успех или неудача в решении проблем в управлении производственными процессами во многом зависят от развития специализированных навыков. Поддержание в рабочем состоянии сложных и ненадежных современных энергетических установок, оснащенных автоматизированными и компьютерными системами, сопряжено с высоким уровнем психологического стресса. Правила и инструкции по эксплуатации могут неадекватно учитывать роль обслуживающего персонала в повышении надежности энергетических систем, уровень его подготовки и психофизиологическую пригодность к работе.

Для повышения качества производственной подготовки в энергетических предприятиях необходимо создать соответствующую систему образования в рамках современного профессионального образования. Действующие Государственные образовательные стандарты (ГОС), образовательные программы и существующие методы подготовки будущих специалистов в средних профессиональных училищах уделяют мало внимания развитию практических навыков учащихся. Это явное противоречие. В то время как современным энергетическим компаниям необходимо готовить высококвалифицированных специалистов в технических училищах и профессиональных колледжах, существующие системы образования неадекватны, а научная обоснованность такой подготовки остается под вопросом.

Целью данного исследования было разработать, научно обосновать и экспериментально проверить образовательную систему для технических колледжей, предназначенную для подготовки будущих специалистов, работающих в энергетических компаниях.

В данном исследовании был проведен анализ литературы по психологии операторов, образованию, методологии и профессиональной подготовке в энергетических компаниях. Рассмотрены и обобщены лучшие практики подготовки высококвалифицированных специалистов в энергетических компаниях. Изучены должностные инструкции, техническая документация и программы обучения операторов на электростанциях и в сетях электропередачи. Помимо интервью с ключевыми специалистами в области эксплуатации энергетических систем, были проведены опросы, наблюдения и экспертные оценки.

Анализ оперативной деятельности специалистов со средним техническим образованием

На первом этапе исследования мы проанализировали трудовую деятельность специалистов со средним техническим образованием (дежурные инженеры-электрики, старшие дежурные инженеры-электрики, сменные руководители тепловых электростанций, диспетчеры энергосистем и дежурные руководители подстанций). Затем мы определили факторы, влияющие на эту деятельность, и исследовали и представили компоненты операционной структуры энергетических компаний.

Все факторы, влияющие на деловую активность, можно разделить на две группы: человеческие факторы (факторы, зависящие от людей, выполняющих работу) и неизбежные факторы (факторы, не связанные с людьми, выполняющими работу). К человеческим факторам относятся следующие:

- морально-нравственные качества: нравственная зрелость, целеустремленность, ответственность за принимаемые решения, дисциплинированность;
- профессиональные качества: уровень знаний, умений, навыков, профессиональная подготовленность, профессиональный опыт конкретного работника;
- психологические особенности: уровень развития способностей и профессионально важных личностных качеств, профессиональная мотивация, психические состояния, скорость психических реакций;
- физиологические особенности: состояние здоровья, функциональные состояния, чувствительность анализаторов, биоритмы, развитие силы и выносливости, антропометрические характеристики.

Неизбежные факторы можно дополнительно разделить на следующие группы:

- Содержание деятельности: информационная нагрузка, метод выполнения задачи и функциональное распределение в рамках системы деятельности оператора.
- Средства управления: средства отображения информации (характеристики освещения, расположение оборудования и т. д.), средства управления (простота проектирования и монтажа);
- Условия труда: планировка рабочего места, физические и химические факторы окружающей среды, социально-психологическая обстановка и т.д.
- Организация деятельности: планирование рабочего времени и перерывов, рабочей нагрузки, программ обучения и т.д.
- Система контроля функционального состояния оператора (методы и критерии оценки состояния);
- профессиональный отбор (медицинский и психологический).

Особенно важно учитывать факторы, которые потенциально могут снизить производительность и надежность оператора, поскольку это

позволяет разрабатывать контрмеры на этапах проектирования и эксплуатации систем «человек-машина-среда», подготавливая их к будущей оперативной деятельности.

Профессиональная деятельность оператора в любой человеко-машинной системе состоит из сочетания четырех элементов: мотивации, управления, регулирования и фундаментальных принципов. Качество и надежность работы оператора зависят от этих элементов и их активного применения в управлении техническим процессом.

На уровень побудительного компонента деятельности оператора влияют следующие факторы:

- общая экономическая ситуация в стране в данный период;
- роль промышленности в национальной экономике, технологический уровень компаний и их роль в промышленности;
- социальная значимость деятельности компаний в рамках промышленности, межличностные отношения (психологический климат) внутри команд, предоставляющих бизнес-услуги, и т. д.;
- этические и материальные стимулы, способствующие повышению эффективности работы;
- уровень образования, интеллект и общие личностные качества специалистов.

Оперативные аспекты зависят от развития навыков взаимодействия с такими элементами, как движение и информация об управляемом объекте, а также от степени автоматизации выполнения стандартных операций.

Успешное управление бизнесом зависит от профессионально важных навыков сотрудников, уровня их теоретических и прикладных знаний, позволяющих принимать обоснованные решения, а также от развитой деловой хваткости и самоконтроля. Успех в бизнесе требует умения анализировать ситуации и прогнозировать их развитие, логического мышления, способности принимать самостоятельные решения в условиях высокой неопределенности, определенного уровня взаимопонимания и доверия внутри организации, умения работать в условиях дефицита времени, чувства ответственности и здорового психического состояния.

К основным факторам, влияющим на жизненно важные показатели человека, относятся возраст, пол, состояние здоровья, тип нервной системы и темперамент, время суток и время года (фаза циркадного ритма), а также текущее психофизиологическое состояние (усталость, раздражительность, возбуждение, депрессия и т.д.).

В рамках образовательного эксперимента был проведен опрос среди ключевых специалистов оперативных отделов энергетических компаний. Опрос, в котором приняли участие 49 специалистов оперативного отдела, показал, что они считают существующую программу обучения оперативному делу, предоставляемую студентам профессиональных училищ, недостаточной для бесперебойного выполнения их обязанностей. Производственная практика после приема на работу требует значительного

времени. Основные недостатки образовательного и учебного процесса отражаются на практической подготовке выпускников.

Модель деятельности оперативного персонала со средним техническим образованием в электроэнергетике

Наше исследование структурных элементов деятельности энергетических компаний выявило характеристики и детали этих видов деятельности, что позволило нам уточнить и расширить бизнес-модель для специалистов со средним техническим образованием. Предложенная нами экспертная модель представляет собой структуру задач по поддержанию и управлению деятельностью энергетических компаний и состоит из следующих трех групп задач:

Первый блок включает задачи, определяемые современными условиями производства энергии. В контексте научно-технического прогресса и наукоемкого производства специалисты должны быть готовы к самостоятельному приобретению знаний, то есть обладать способностью к обучению. Они должны уметь научно организовывать свою работу и применять свои знания в профессиональной деятельности. Специалисты должны быть готовы к работе в команде, уметь управлять производством и командами, обладать сильным стремлением к самосовершенствованию, самопознанию и саморазвитию, а также стремиться к творческой самореализации.

Второй блок включает задачи и виды деятельности, на которые повлияла текущая социально-экономическая ситуация. Эти задачи характеризуются следующими личными качествами специалиста оперативной службы:

- Гражданственность: чувство общественного долга, моральная зрелость, этика, позитивное отношение к жизни и моральная ответственность за принимаемые решения.
- трудовые: трудолюбие, работа с электрооборудованием, оценка профессиональной квалификации, оценка результатов работы.
- Организационные навыки: способность обеспечивать последовательность действий, ставить цели, расставлять приоритеты, организовывать и направлять усилия людей в желаемом направлении, четко выражать собственные идеи и достигать поставленных целей.
- Личные качества: самоорганизация, самоконтроль, адекватная самооценка, саморегуляция, точность, усердие, дисциплина.

Третий блок состоит из задач, определяемых специализированными требованиями. Эти задачи требуют специальных навыков, прочных теоретических знаний и умения применять эти знания на практике. Ключевые навыки включают чтение электрических схем, выполнение электрических измерений, мониторинг состояния электрооборудования с помощью измерительных приборов, а также умение быстро анализировать ситуации и принимать решения. Персонал по эксплуатации и техническому обслуживанию должен обладать практическими навыками для

самостоятельного и эффективного решения производственных проблем, связанных с мониторингом состояния оборудования, умением решать специализированные проблемы в различных режимах работы электрооборудования на электростанциях и в передающих сетях, знанием технической терминологии и умением создавать точную и полную оперативную документацию.

Система подготовки студентов колледжа к оперативной деятельности на электроэнергетических предприятиях

Результаты исследований выявили наиболее важные аспекты и цели, которым следует уделять приоритетное внимание в системах обучения операторов электростанций и операторов электросетей.

Основная цель колледжей при подготовке студентов к практической работе в электроэнергетике — развитие у них способности эффективно решать специализированные задачи. Это содержит в себя приобретение, обновление и расширение общих и специализированных знаний, а также приобретение, поддержание и развитие навыков и умений, необходимых для бесперебойного выполнения практической работы в сфере производства энергии.

Национальные стандарты профессионального образования (СПО) устанавливают требования к уровню подготовки выпускников колледжей (включая общеобразовательные и последипломные требования) и структуру образовательного процесса. Стандарты СПО определяют основные навыки и компетенции, которыми должны обладать молодые специалисты для получения соответствующей квалификации. Требования к специальности 1001 стандарта СПО «Электромонтаж на электростанциях и в передающих сетях» составляют основу всех элементов системы профессионального развития лиц, работающих в энергетическом секторе.

Специализированное содержание обучения будущих специалистов по эксплуатации в энергетической отрасли определяется в рамках специально организованной системы среднего профессионального образования, направленной на получение квалификации «техник-электрик». Технические параметры этой системы включают количество учебных часов, продолжительность и последовательность обучения на каждом этапе подготовки персонала по эксплуатации.

Учебный план, основанный на профессиональных требованиях и соответствующий государственным стандартам среднего профессионального образования, состоит из набора предметов, которые являются основным элементом построения образовательной системы для подготовки специалистов и определяют структуру учебного процесса. Используя потенциал федеральных предметов и тщательно отбирая предметы из числа факультативных предметов государственных стандартов среднего профессионального образования (национальные и региональные предметы), учебный план разработан для подготовки студентов университетов к будущей профессиональной деятельности.

Следующим элементом системы профессиональной подготовки стало методическое обеспечение реализации этого процесса в каждой специализированной области. Это методическое обеспечение включало не только учебный план, но и учебные материалы, используемые в процессе обучения. Сюда входили дополнительные материалы, демонстрационные материалы и вспомогательные материалы для лабораторных и практических занятий. Важными компонентами методического обеспечения подготовки студентов к практическому обучению были технические средства, такие как аудиовизуальное оборудование, компьютеры и тренажеры.

Одним из важнейших элементов системы подготовки кадров является психологическая и образовательная оценка. Она включает в себя методы отбора кандидатов на профессию, начиная от первоначальных тестов и заканчивая оценкой уровня профессиональных навыков, необходимых для конкретных должностей. Отбор кандидатов на профессию – это научный отбор студентов, подходящих для работы в производственной сфере, с целью оценки профессиональной пригодности будущих специалистов. Конечно, в процессе обучения в колледже или профессиональном училище это может быть только первоначальная оценка, а не заключительная или обязательная. Однако учет этих результатов позволяет давать рекомендации будущим специалистам и в некоторых случаях снижает затраты на обучение лиц, которые изначально считаются непригодными для этого вида работы из-за психофизиологических особенностей, связанных с производственной деятельностью. Кроме того, это позволяет своевременно корректировать содержание обучения, обеспечивая более высокую эффективность в других областях и услугах энергетической компании.

Завершающим элементом системы подготовки оперативного персонала является мониторинг результатов обучения. Он должен проводиться во всех областях, как в течение периода обучения (непрерывный), так и по окончании курса (итоговая оценка). Результаты контролируемого курса, стажировки, итоговой квалификационной оценки, а также психолого-педагогической оценки станут основой для сертификации выпускников как будущих специалистов оперативного профиля.

Исследования экспертов показывают, что одним из ключевых профессиональных навыков персонала оперативных служб электроэнергетических компаний является умение интерпретировать электрические цепи. Поэтому была разработана методика развития у студентов навыков интерпретации электрических цепей. Эта методика основана на квалификационных требованиях и должностных инструкциях персонала оперативных служб и использует в качестве примера курс «Релейная защита и автоматизация реле и автоматики» из специализированного предмета 1001 «Электроустановки на электростанциях и в сетях» для развития практических навыков чтения электрических цепей. Используя эту методику, студенты могут не только продемонстрировать знания и точность чтения цепей релейной защиты, что крайне важно для

надежной работы всей электроустановки, но и понять и продемонстрировать ответственность за надежность и надлежащую работу электроустановки. Данная методика основана на методе саморазвития Г.К. Селевко.

Методика обучения интерпретации базовых электрических схем состоит из трех взаимосвязанных подсистем:

Теоретический аспект: Приобретение теоретических основ для чтения базовых электрических схем релейной защиты и автоматизации. 100.00%

Практическое обучение: Приобретение практических знаний прочтения схем релейной защиты и схем автоматизированных систем.

Обучение методике: Применение приобретенных знаний чтения для анализа схем релейной защиты электрооборудования и схем автоматизированных систем.

При изучении психологических и образовательных характеристик оперативно-диспетчерского состава мы уделили особое внимание карьерной ориентации, мотивации, обоснованию выбора профессии, отношению к работе, а также стабильности профессиональных интересов и тенденций. Мы также разработали алгоритм проведения психологических и образовательных оценок в процессе первоначального отбора при подготовке студентов колледжей к будущей оперативной деятельности.

Разработка данного алгоритма проводилась в следующем порядке:

- опрос о способности студентов университетов самостоятельно принимать решения относительно выбора карьерного пути;
- четко сформулируйте цели исследования;
- изучите интересы и предпочтения студентов в различных видах деятельности;
- определите индивидуальные психологические качества, необходимые для будущего успеха в бизнесе;
- проанализируйте полученные данные;
- мы проводим индивидуальные собеседования с каждым студентом, чтобы помочь им приобрести необходимые профессиональные навыки.

Помимо выбора содержания учебной программы и применения специализированных методов развития навыков для студентов с опытом работы и тех, кто стремится к трудоустройству в данной области, производственная практика и преддипломная стажировка должны проводиться с использованием специально разработанных программ. Студенты экспериментальной группы прошли производственную практику по специально разработанной программе. Работая над этими заданиями, студенты повысили свою мотивацию к практической работе на электростанции, улучшили наблюдательность и повысили способность анализировать опыт эксплуатации электрооборудования.

Экспертная оценка, проведенная руководителями электроцехов, главными инженерами, заместителями руководителей служб подстанций и специалистами по городским энергосетям в компаниях, занимающихся производством электроэнергии, показала, что все студенты, прошедшие

стажировку по специально разработанной программе, обладали достаточными навыками и способностями для выполнения своих обязанностей в этих компаниях.

Выводы

В результате данного исследования были получены следующие результаты:

1) мы систематизировали и усовершенствовали модель подготовки специалистов по эксплуатации энергетических компаний, получивших среднее техническое образование, и разработали систематическую систему обучения, позволяющую студентам заниматься производственной деятельностью в рамках учебной программы профессионального колледжа;

2) в рамках национальных образовательных стандартов для среднего профессионального образования были определены и использованы потенциальные ресурсы для федеральных предметов в специализированной области «Электрооборудование для электростанций и подстанций», а также введены новые предметы «Обучение студентов с использованием тренажеров» и «Автоматизированное управление энергосистемами» в качестве национальных и региональных компонентов;

3) были разработаны и внедрены методы для развития и совершенствования специализированных навыков в рамках подготовки студентов колледжей к работе в энергетических компаниях. Эти навыки включают в себя умение интерпретировать основные электрические схемы;

4) были разработаны и внедрены алгоритмы психологической и педагогической диагностики для определения профессионально важных качеств, необходимых для успешной работы в операционных службах энергетических компаний.

Внедрение разработанной системы практического обучения в технические колледжи приведет к повышению мотивации и улучшению качества подготовки специалистов энергетической отрасли.

В будущих исследованиях следует уделить особое внимание формированию и развитию профессионально важных качеств, необходимых для успешного управления в энергетических компаниях.

Использованные источники:

1. Дьяков А.Ф. Надежная работа персонала в энергетике. - М.: Изд. МЭИ, 1996.
2. Баркан Я.Д. Эксплуатация электрических систем. - М.: Высшая школа, 1990.
3. Человеческий фактор. В 6-ти тт. Т.3. Моделирование деятельности, профессиональное обучение и отбор операторов: Пер. с англ. Часть 1. Модели психической деятельности. - М.: Мир, 1991.
4. Платонов К.К. Структура и развитие личности. - М.: Высшая школа, 1986.

УДК 347.4

Сорокин М.А.
студент
Оренбургский филиал РЭУ им. Г.В. Плеханова
Пустотина Н.В.
старший преподаватель
Оренбургский филиал РЭУ им. Г.В. Плеханова
Россия, Оренбург

ЗНАЧЕНИЕ ПРОВЕРКИ ДОЛЖНОЙ ОСМОТРИТЕЛЬНОСТИ ПАРТНЕРА

Аннотация: *Современные договорные отношения призваны формировать сотрудничество по нескольким этапам, включая исполнение договора. Риск недобросовестности партнера зависит от субъективных и объективных факторов. Актуальность приобретает «должная осмотрительность» партнера. Проверка данной характеристика стороны договора – способ управления рисками и минимизации неблагоприятных последствий.*

Ключевые слова: *риск, угроза, должная осмотрительность*

Sorokin M.A.
student
Orenburg branch of the Plekhanov
Russian University of Economics
Pustotina N.V.
senior lecturer
Orenburg branch of the Plekhanov
Russian University of Economics
Russia, Orenburg

THE IMPORTANCE OF CHECKING THE PARTNER'S DUTY OF CARE

Annotation: *Modern contractual relations are designed to form cooperation at several stages, including the execution of the contract. The risk of a partner's dishonesty depends on subjective and objective factors. The "due diligence" of a partner becomes relevant. Checking this characteristic of the party to the contract is a way to manage risks and minimize adverse consequences.*

Keywords: *risk, threat, due diligence*

Сотрудничество хозяйствующих субъектов выражается посредством заключения договора. Процесс договорного сотрудничества включает в себя несколько стадий – от поиска партнера, до подписания приёмо-передаточных

документов. Каждая стадия несет риски и угрозы, минимизировать или избежать которые – одна из главных задач сторон.

Готовность и способность сторон принять и исполнить договорные обязательства не всегда могут быть на должном уровне. Необходимо учитывать обстоятельства, связанные с субъективными и объективными факторами.

Управление рисками и угрозами сторонами начинается в процессе формирования проекта договора, который представляет собой согласованную волю сторон, а значит, содержит договоренности и в некой степени уступки партнеров друг другу. В силу прямого указания российского гражданского законодательства, стороны обязаны согласовать «существенные условия» договора, к которым относятся основные характеристики сделки, представленные, в частности, условиями о предмете, сроках, цене и т.д. Согласование существенных условий, подтверждает готовность сторон действовать в направлении договоренностей. Однако, степень подобной готовности зависит от ряда факторов.

В договорной практике появился сравнительно новый термин, характеризующий сторону договора - «должная осмотрительность». Введение в оборот, данный термин обязан судебной практике, а именно - постановлению Пленума Высшего Арбитражного Суда РФ от 12 октября 2006 г. № 53 «Об оценке арбитражными судами обоснованности получения налогоплательщиком налоговой выгоды» (далее – Постановление Пленума). В пункте 10 названного Постановления Пленума правоприменитель, использует несколько характеристик – должная осмотрительность и осторожность.

Сопоставление термина и практики его применения, позволяет сделать вывод, что контрагент предпринимает от себя все возможное для проверки партнера на готовность надлежащего договорного поведения.

По нашему мнению, проверка должной осмотрительности, представляющая собой установление надлежащего партнера, функционирующего в целях сохранения и повышения уровня деловой репутации, недопустимости нарушения прав другой стороны договора, в современных условиях приобретает наибольшую значимость. Проверка допускает установление факта регистрации, получение особого статуса (собственника, уполномоченного лица, лицензиата, субъекта малого и среднего предпринимательства) и т.д. Особое значение проверка специальных статусов приобретает при государственных и муниципальных закупках. В частности, при закупке охранных услуг, наличие лицензии является обязательным условием для рассмотрения заявки участника закупки. Период антиковидных ограничений свидетельствовал о фактах автоматического продления действия лицензии на один год. Контролировать партнера в данном случае – дополнительная задача партнера, выступающего в роли заказчика.

Один из главных аспектов при проверке - фиксировать даты полученной информации и сопоставлять их с датой запроса, поскольку указанные даты могут не совпадать, что может повлечь риски убытков, в силу ненадлежащей проверки партнера.

Отметим, что объективная и тщательная проверка должной осмотрительности перед заключением договора не предостерегает от негативных последствий. В частности на должную осмотрительность оказывают неблагоприятное воздействие санкции, ограничивающие или запрещающие наработанные правила поведения хозяйствующих субъектов. Проблема в данном случае кроется в признании и непризнании непредвиденными обстоятельствами сакционные ограничения.

Наличие «дружественных» и «недружественных» государств, санкции усугубляют проблемы и повышают уровень рисков и угроз [2, С.138]. В результате нарушения логистических международных связей, стороны договора столкнулись с неисполнением или ненадлежащим исполнением договорных обязательств, что повлекло претензионные и судебные требования в выплате неустоек (штраф, пени). Статус непредвиденных обстоятельств (форс–мажора) позволяет сторонам не применять меры договорной ответственности и сконцентрировать все силы на исполнение договора. Однако судебная практика вырабатывает подход, направленный не на наличие возможности признания обстоятельств, препятствующих добросовестному исполнению оговору, непредвиденными обстоятельствами, а указание на ненадлежащее поведение партнера, который должен был иметь варианты исполнения договора даже в случаях вводимых ограничений.

Таким образом, мы приходим к выводу о необходимости системной проверки партнера на всех стадиях сотрудничества и целесообразно проверку проводить, используя все доступные сервисы (реестр недобросовестных поставщиков, федерального ресурса о банкротстве, реестры юридических и физических лиц и т.д.). Проверка партнера допускает наличие дистанционной занятости работников хозяйствующего субъекта, что подтверждает влияние цифровизации и платформенной занятости на форму хозяйственной деятельности [3, С.84].

Использованные источники:

1. Об оценке арбитражными судами обоснованности получения налогоплательщиком налоговой выгоды. Постановление Пленума Высшего Арбитражного Суда РФ от 12 октября 2006 г. №53// https://internet.garant.ru/#/startpage:0.

2. Угрозы экономической безопасности региона: современный аспект. Иванова А.М., Пустотина Н.В. В сборнике: Социально-экономическое развитие регионов России: тенденции, проблемы, перспективы//Сборнике научных трудов V Всероссийской научно-практической конференции. Волгоград, 2024. С. 135-140.

3. Цифровизация хозяйственной деятельности в современных условиях. Пустотина Н.В.// Сборник: Шаг в будущее: искусственный интеллект и

цифровая экономика. Сборник научных статей VI Международного научного форума. В 2-х томах. Москва, 2024. С. 84-89.

УДК 613.24:546.76+615.32

Субботина Н. С.
свободный исследователь

ХРОМ И ЭКСТРАКТ ПЛОДОВ БАРБАРИСА: АНАЛИЗ НАУЧНЫХ ДАННЫХ О МЕХАНИЗМАХ ВЛИЯНИЯ НА МЕТАБОЛИЗМ И РЕГУЛЯЦИЮ АППЕТИТА

Аннотация: *В статье рассмотрены современные научные данные о биологических эффектах хрома и экстракта плодов барбариса, содержащего алкалоид берберин, — двух компонентов, потенциально влияющих на углеводный и липидный обмен, а также на регуляцию аппетита. Цель работы — проанализировать механизмы действия этих веществ и оценить клинические данные об их эффективности. В ходе исследования проведён обзор публикаций, индексируемых в базах данных PubMed и Scopus. Установлено, что хром способствует усилению действия инсулина и может влиять на пищевое поведение, а берберин обладает гиполипидемическими и анорексигенными свойствами; их совместное применение представляет научный интерес как потенциальная стратегия комплексной коррекции метаболических нарушений.*

Ключевые слова: *хром, берберин, барбарис, метаболизм, аппетит, масса тела, инсулин.*

Subbotina N. S.
independent researcher

CHROMIUM AND BARBERRY FRUIT EXTRACT: AN ANALYSIS OF SCIENTIFIC EVIDENCE ON MECHANISMS AFFECTING METABOLISM AND APPETITE REGULATION

Abstract: *The article reviews current scientific evidence on the biological effects of chromium and barberry fruit extract containing the alkaloid berberine — two components potentially influencing carbohydrate and lipid metabolism as well as appetite regulation. The aim was to analyze the mechanisms of action of these substances and evaluate clinical evidence on their efficacy. A review of publications indexed in PubMed and Scopus was conducted. It was established that chromium enhances insulin action and may influence eating behavior, while berberine possesses hypolipidemic and anorexigenic properties; their combined use is of scientific interest as a potential strategy for comprehensive correction of metabolic disorders.*

Keywords: *chromium, berberine, barberry, metabolism, appetite, body weight, insulin.*

Введение

Избыточная масса тела и ожирение представляют собой глобальную медико-социальную проблему, в основе которой лежат нарушения углеводного и липидного обмена, нередко сочетающиеся с расстройствами пищевого поведения [1]. Наряду с фармакологическими подходами, всё большее внимание исследователей привлекают биологически активные вещества природного происхождения, способные модулировать метаболические пути и влиять на аппетит. Среди них особый интерес вызывают микроэлемент хром и алкалоид берберин, содержащийся в экстракте плодов барбариса [2; 3].

Хром является незаменимым микроэлементом, участвующим в потенцировании действия инсулина, регуляции гомеостаза глюкозы и, по некоторым данным, в контроле пищевого поведения [4]. Берберин — изохинолиновый алкалоид, который получают из различных видов барбариса (Berberis spp.), — демонстрирует в исследованиях гипогликемические, гиполипидемические и анорексигенные свойства [5]. Комбинация данных компонентов представляется рациональной с точки зрения воздействия на различные звенья метаболического синдрома, однако систематизированные данные об их совместном влиянии на аппетит и массу тела ограничены.

Целью настоящей работы является анализ современных научных данных о механизмах действия хрома и берберина, а также обобщение клинических сведений об их эффективности в регуляции метаболизма и аппетита.

Материалы и методы исследования

Материалами исследования послужили научные публикации, посвящённые роли хрома и берберина в регуляции углеводного и липидного обмена, а также их влиянию на аппетит и массу тела.

В ходе работы были проанализированы оригинальные экспериментальные и клинические исследования, рандомизированные контролируемые испытания (РКИ), систематические обзоры и метаанализы, опубликованные в рецензируемых международных изданиях по направлениям эндокринологии, нутрициологии и фармакологии. Поиск проводился в базах данных PubMed и Scopus. В анализ включались публикации, содержащие данные о влиянии перорального приёма хрома (в форме пиколината или хлорида) и берберина (в составе экстракта барбариса или изолированно) на уровень глюкозы, инсулина, липидный профиль, показатели аппетита и изменение массы тела. Приоритет отдавался клиническим исследованиям, систематическим обзорам и метаанализам.

Результаты исследования

Хром в регуляции метаболизма и аппетита.

Хром входит в состав низкомолекулярного хром-связывающего вещества, которое усиливает действие инсулинового рецептора и способствует перемещению транспортёров глюкозы GLUT-4 к клеточной мембране [4; 6]. Благодаря этому ткани становятся более чувствительными к

инсулину, уровень глюкозы в крови остаётся стабильным, а аппетит и тяга к углеводной пище снижаются.

Систематический обзор и метаанализ Pittler и соавт. (2003), объединивший данные 20 РКИ с участием пациентов с избыточной массой тела и ожирением, показал, что приём хрома пиколината в дозах 200–1000 мкг/сут в течение 8–24 недель приводит к статистически значимому снижению массы тела в среднем на 1,1 кг по сравнению с плацебо, при этом наибольший эффект наблюдался у лиц с исходными нарушениями углеводного обмена [7].

Влияние хрома на пищевое поведение и аппетит оценивалось в исследовании Anton и соавт. (2008), в котором у женщин с избыточной массой тела приём хрома пиколината (1000 мкг/сут) в течение 8 недель сопровождался снижением потребления калорий и субъективного чувства голода по сравнению с плацебо; авторы связывали этот эффект с модуляцией серотонинергической системы [8].

Экстракт плодов барбариса и берберин.

Берберин — главное действующее вещество экстракта плодов барбариса. Его влияние на обмен веществ связано с несколькими механизмами: он активирует регуляторный фермент AMPK, замедляет работу митохондрий и изменяет состав кишечной микробиоты [5; 9]. Включение AMPK заставляет клетки активнее поглощать глюкозу и окислять жирные кислоты, что в итоге улучшает липидный профиль крови и повышает чувствительность тканей к инсулину.

Систематический обзор и метаанализ Asbaghi и соавт. (2020), включивший 10 РКИ с участием 723 пациентов с избыточной массой тела и ожирением, продемонстрировал, что приём берберина (900–1500 мг/сут) ассоциирован со статистически значимым снижением массы тела на 2,07 кг и уменьшением окружности талии на 1,08 см по сравнению с плацебо, а также с улучшением показателей липидного профиля и маркеров воспаления [10].

Влияние берберина на аппетит связывают с его способностью модулировать секрецию гормонов, участвующих в регуляции голода и насыщения, что подтверждается как экспериментальными, так и клиническими данными [3].

Совместное применение хрома и берберина.

Совместное применение хрома и берберина может рассматриваться как стратегия воздействия на разные звенья метаболического синдрома: хром преимущественно улучшает чувствительность к инсулину и снижает влечение к углеводам, в то время как берберин воздействует на липидный обмен и гормональную регуляцию аппетита [2; 6]. Прямых исследований, оценивающих комбинацию этих компонентов, в литературе крайне мало; тем не менее, имеющиеся доклинические и косвенные клинические данные свидетельствуют о целесообразности дальнейшего изучения данной комбинации в рамках РКИ с оценкой массы тела, композиции тела и метаболических маркеров.

Заключение

Проведённый анализ научной литературы свидетельствует о том, что хром и берберин обладают выраженными и взаимодополняющими метаболическими эффектами. Хром реализует своё действие преимущественно через усиление инсулинового сигналинга и потенциальное влияние на пищевое поведение, в то время как берберин активирует AMPK-зависимые пути, улучшая липидный обмен и модулируя гормоны аппетита.

Имеющиеся РКИ и метаанализы демонстрируют, что изолированное применение обоих компонентов приводит к статистически значимому снижению массы тела, улучшению гликемического контроля и липидного профиля. Комбинированное применение хрома и берберина теоретически обосновано и представляет собой перспективную стратегию для комплексной коррекции метаболических нарушений, однако требует дальнейшей проверки в специально спланированных клинических испытаниях.

Дальнейшие исследования должны быть направлены на установление оптимальных доз и длительности совместного приёма данных веществ, а также на оценку их влияния на показатели композиции тела, гормональный статус и качество жизни пациентов с избыточной массой тела и ожирением.

Использованные источники:

1. Bluher M. Obesity: global epidemiology and pathogenesis // Nature Reviews Endocrinology. – 2019. – Vol. 15, No. 5. – P. 288–298. – DOI: 10.1038/s41574-019-0176-8.
2. Vincent J.B. The bioinorganic chemistry of chromium(III) // Polyhedron. – 2001. – Vol. 20, No. 1-2. – P. 1–26.
3. Imenshahidi M., Hosseinzadeh H. Berberis vulgaris and berberine: an update review // Phytotherapy Research. – 2016. – Vol. 30, No. 11. – P. 1745–1764. – DOI: 10.1002/ptr.5693.
4. Anderson R.A. Chromium, glucose intolerance and diabetes // Journal of the American College of Nutrition. – 1998. – Vol. 17, No. 6. – P. 548–555. – DOI: 10.1080/07315724.1998.10718802.
5. Cicero A.F.G., Baggioni A. Berberine and its role in chronic disease // Advances in Experimental Medicine and Biology. – 2016. – Vol. 928. – P. 27–45. – DOI: 10.1007/978-3-319-41334-1_2.
6. Hua Y., Clark S., Ren J., Sreejayan N. Molecular mechanisms of chromium in alleviating insulin resistance // Journal of Nutritional Biochemistry. – 2012. – Vol. 23, No. 4. – P. 313–319. – DOI: 10.1016/j.jnutbio.2011.11.001.
7. Pittler M.H., Stevinson C., Ernst E. Chromium picolinate for reducing body weight: meta-analysis of randomized trials // International Journal of Obesity. – 2003. – Vol. 27, No. 4. – P. 522–529. – DOI: 10.1038/sj.ijo.0802262.
8. Anton S.D., Morrison C.D., Cefalu W.T., et al. Effects of chromium picolinate on food intake and satiety // Diabetes Technology & Therapeutics. – 2008. – Vol. 10, No. 5. – P. 405–412. – DOI: 10.1089/dia.2007.0285.

9. Yao J., Kong W., Jiang J. Learning from berberine: mechanisms and applications // Science China Life Sciences. – 2015. – Vol. 58, No. 9. – P. 854–859. – DOI: 10.1007/s11427-015-4829-0.
10. Asbaghi O., Ghanbari N., Shekari M., Reiner Ž., Amirani E., Hallajzadeh J., Mirsafaei L., Asemi Z. The effect of berberine supplementation on obesity parameters, inflammation and liver function enzymes: A systematic review and meta-analysis of randomized controlled trials // Clinical Nutrition ESPEN. – 2020. – Vol. 38. – P. 43–49. – DOI: 10.1016/j.clnesp.2020.04.010.

УДК 612.111.11:546.72

Субботина Н.С.
свободный исследователь

ЖЕЛЕЗО КАК КЛЮЧЕВОЙ МИКРОНУТРИЕНТ В ПОДДЕРЖАНИИ УРОВНЯ ГЕМОГЛОБИНА: АНАЛИЗ НАУЧНЫХ ДАННЫХ О МЕХАНИЗМАХ ДЕЙСТВИЯ И КЛИНИЧЕСКОЙ ЭФФЕКТИВНОСТИ

Аннотация: *В статье рассмотрены современные научные данные о биологической роли железа в синтезе гемоглобина и поддержании кислородтранспортной функции крови. Целью работы являлся анализ механизмов участия железа в эритропоэзе и оценка клинической эффективности его дополнительного приема при коррекции железодефицитных состояний. В ходе исследования проведен обзор публикаций, индексируемых в базах данных PubMed, Scopus и Web of Science. Установлено, что железо является незаменимым компонентом гема, а его дефицит приводит к снижению синтеза гемоглобина и развитию анемии; восполнение недостатка железа достоверно повышает уровень гемоглобина и улучшает функциональные показатели.*

Ключевые слова: *железо, гемоглобин, анемия, эритропоэз, ферритин, трансферрин, кислородтранспортная функция.*

Subbotina N. S.
independent researcher

IRON AS A KEY MICRONUTRIENT IN HEMOGLOBIN LEVEL MAINTENANCE: AN ANALYSIS OF SCIENTIFIC EVIDENCE ON MECHANISMS OF ACTION AND CLINICAL EFFICACY

Abstract: *The article reviews current scientific evidence on the biological role of iron in hemoglobin synthesis and maintenance of oxygen-carrying capacity of the blood. The aim of the study was to analyze the mechanisms of iron participation in erythropoiesis and evaluate the clinical efficacy of its additional intake for the correction of iron-deficiency conditions. A review of publications indexed in PubMed, Scopus, and Web of Science was conducted. Iron was found to be an indispensable component of heme, and its deficiency leads to reduced hemoglobin synthesis and anemia development; replenishment of iron deficiency reliably increases hemoglobin levels and improves functional outcomes.*

Keywords: *iron, hemoglobin, anemia, erythropoiesis, ferritin, transferrin, oxygen-carrying capacity.*

Введение

Гемоглобин, основной белок эритроцитов, обеспечивает транспорт кислорода от легких к тканям и углекислого газа в обратном направлении. Поддержание его концентрации в крови в физиологическом диапазоне

является критически важным для нормального функционирования всех органов и систем. Центральную роль в синтезе гемоглобина играет железо, входящее в состав гема — простетической группы, осуществляющей связывание кислорода [1; 2].

Дефицит железа остается наиболее распространенным дефицитом микронутриентов в мире и ведущей причиной анемии. По оценкам Всемирной организации здравоохранения, железодефицитная анемия (ЖДА) затрагивает около 1,62 млрд человек, при этом основными группами риска являются дети, женщины репродуктивного возраста и беременные [3]. Несмотря на многолетнюю историю изучения проблемы, вопросы оптимальных форм и доз железа для коррекции латентного дефицита и ЖДА, а также переносимости различных соединений железа сохраняют научную и практическую актуальность [4].

Целью настоящей работы является анализ современных научных данных о механизмах участия железа в синтезе гемоглобина, а также обобщение клинических сведений об эффективности дополнительного приема железа для повышения уровня гемоглобина и коррекции железодефицитных состояний.

Материалы и методы исследования

Материалами исследования послужили научные публикации, посвященные метаболизму железа, его роли в эритропоэзе и клиническим аспектам коррекции дефицита железа.

В ходе работы были проанализированы оригинальные экспериментальные и клинические исследования, рандомизированные контролируемые испытания (РКИ), систематические обзоры и метаанализы, опубликованные в рецензируемых международных изданиях по направлениям гематологии, нутрициологии и внутренней медицины. В анализ включались публикации, индексируемые в базах данных PubMed, Scopus и Web of Science, содержащие данные о влиянии перорального приема различных солей железа на уровень гемоглобина, ферритина, трансферрина и клинические исходы у лиц с диагностированным железодефицитом или ЖДА. Исключались исследования, посвященные парентеральным формам железа, а также работы с участием пациентов с анемией, обусловленной иными причинами (B_{12}-дефицитная, апластическая, гемолитическая анемии).

Результаты исследования

Биохимическая роль железа в структуре и синтезе гемоглобина.

Железо является незаменимым микроэлементом, выполняющим функцию центрального атома в молекуле гема. В процессе эритропоэза в митохондриях эритробластов происходит встраивание иона двухвалентного железа в протопорфирин IX при участии фермента феррохелатазы, что приводит к образованию гема. Последний соединяется с глобиновыми цепями, формируя функциональную молекулу гемоглобина [1; 5].

Метаболизм железа в организме жестко регулируется системой гепсидин-ферропортин, контролирующей абсорбцию железа в двенадцатиперстной кишке и его высвобождение из депо (макрофагов и гепатоцитов). При дефиците железа синтез гепсидина снижается, что способствует увеличению всасывания микроэлемента и мобилизации запасов для нужд эритропоэза [6]. Клинически выделяют три стадии дефицита железа: истощение запасов (снижение ферритина), латентный железодефицит (снижение сывороточного железа и насыщения трансферрина) и собственно ЖДА со снижением уровня гемоглобина ниже нормативных значений [7].

Сравнительная эффективность различных форм железа в клинических исследованиях.

Классические неорганические соли железа (сульфат, фумарат, глюконат железа) остаются наиболее широко применяемыми формами для алиментарной коррекции дефицита железа, однако характеризуются относительно низкой биодоступностью (менее 20% дозы всасывается в двенадцатиперстной кишке) и нередко сопровождаются нежелательными эффектами со стороны желудочно-кишечного тракта [8].

Хелатная форма — бисглицинат железа (аминокислотный хелат железа с глицином) — рассматривается как альтернатива с потенциально более высокой биодоступностью. Систематический обзор и метаанализ рандомизированных контролируемых исследований, объединивший данные 17 РКИ с участием беременных женщин и детей, показал, что прием бисглицината железа приводил к более выраженному повышению концентрации гемоглобина по сравнению с другими формами железа у беременных женщин, при этом сопровождался меньшей частотой желудочно-кишечных нежелательных явлений; статистически значимых различий по влиянию на гемоглобин и ферритин у детей выявлено не было [8].

Полученные данные систематического обзора позволяют рассматривать хелатные формы железа как один из возможных вариантов алиментарной коррекции дефицита, однако авторы обзора отмечают, что оптимальная дозировка, кратность приема и длительность применения бисглицината железа требуют дальнейшего уточнения в специально спланированных исследованиях [8].

Влияние на функциональное состояние.

Помимо прямого влияния на уровень гемоглобина, коррекция дефицита железа приводит к улучшению кислородтранспортной функции крови, что клинически проявляется повышением толерантности к физической нагрузке, уменьшением слабости и утомляемости, а у детей — улучшением когнитивных показателей [3]. Вместе с тем, бесконтрольный прием высоких доз железа при отсутствии дефицита не ассоциирован с дополнительным повышением гемоглобина у здоровых лиц и может сопровождаться риском перегрузки железом [7].

Заключение

Проведенный анализ научной литературы подтверждает, что железо является незаменимым микронутриентом, участвующим в качестве структурного компонента гема в синтезе гемоглобина. Дефицит железа последовательно приводит к снижению уровня гемоглобина и развитию ЖДА, особенно у лиц из групп риска.

Установлено, что пероральный прием железа является эффективным и хорошо изученным способом повышения уровня гемоглобина при железодефицитных состояниях; восполнение дефицита сопровождается клинически значимым улучшением кислородтранспортной функции крови и функционального статуса пациентов. Наиболее убедительная доказательная база накоплена для сульфата железа (II), однако переносимость высоких доз может ограничиваться гастроинтестинальными нежелательными явлениями.

Дальнейшие исследования должны быть направлены на оптимизацию дозировок и поиск форм железа с улучшенной биодоступностью и минимальными побочными эффектами, а также на разработку индивидуализированных схем коррекции дефицита с учетом исходного статуса пациента и его ответа на терапию.

Использованные источники:

1. Abbaspour N., Hurrell R., Kelishadi R. Review on iron and its importance for human health // Journal of Research in Medical Sciences. – 2014. – Vol. 19, No. 2. – P. 164–174.
2. Ems T., St Lucia K., Huecker M.R. Biochemistry, Iron Absorption // StatPearls Publishing. – 2023. – URL: https://www.ncbi.nlm.nih.gov/books/NBK448204/ (дата обращения: 20.07.2026).
3. World Health Organization. Worldwide prevalence of anaemia 1993–2005: WHO global database on anaemia / Ed. by B. de Benoist, E. McLean, I. Egli, M. Cogswell. – Geneva: WHO Press, 2008. – 40 p.
4. Camaschella C. Iron deficiency // Blood. – 2019. – Vol. 133, No. 1. – P. 30–39. – DOI: 10.1182/blood-2018-05-815944.
5. Anderson G.J., Frazer D.M. Current understanding of iron homeostasis // American Journal of Clinical Nutrition. – 2017. – Vol. 106, Suppl. 6. – P. 1559S–1566S. – DOI: 10.3945/ajcn.117.155804.
6. Nemeth E., Ganz T. Hepcidin-ferroportin interaction controls systemic iron homeostasis // International Journal of Molecular Sciences. – 2021. – Vol. 22, No. 12. – Article 6493. – DOI: 10.3390/ijms22126493.
7. Cappellini M.D., Musallam K.M., Taher A.T. Iron deficiency anaemia revisited // Journal of Internal Medicine. – 2020. – Vol. 287, No. 2. – P. 153–170. – DOI: 10.1111/joim.13004.
8. Fischer J.A.J., Cherian A.M., Bone J.N., Karakochuk C.D. The effects of oral ferrous bisglycinate supplementation on hemoglobin and ferritin concentrations in adults and children: a systematic review and meta-analysis of randomized

controlled trials // Nutrition Reviews. – 2023. – Vol. 81, No. 8. – P. 904–920. – DOI: 10.1093/nutrit/nuac106.

УДК 612.015.3:577.17

Субботина Н. С.
свободный исследователь

ЦИНК, МАГНИЙ И ВИТАМИН B6 (ZMA): АНАЛИЗ НАУЧНЫХ ДАННЫХ О ВЛИЯНИИ НА ОБМЕН ТЕСТОСТЕРОНА И ФИЗИОЛОГИЧЕСКИЕ ПРОЦЕССЫ

Аннотация: *В статье рассмотрены современные научные данные о биологической роли цинка, магния и витамина B6 — микронутриентов, традиционно объединяемых в комплекс ZMA. Целью работы являлся анализ имеющихся сведений о влиянии данных веществ на эндокринную регуляцию тестостерона, показатели мышечного восстановления и качество сна. В ходе исследования проведен обзор публикаций, индексируемых в базах PubMed, Scopus и Web of Science. Установлено, что цинк и магний выступают значимыми кофакторами стероидогенеза и нейроэндокринной регуляции, при этом наиболее выраженные эффекты в отношении тестостерона зафиксированы у лиц с исходным дефицитом данных микроэлементов. Данные о влиянии совместного приема трех компонентов у лиц без дефицита остаются неоднородными и требуют дальнейшего изучения.*

Ключевые слова: *цинк, магний, витамин B6, тестостерон, ZMA, стероидогенез, качество сна.*

Subbotina N. S.
independent researcher

ZINC, MAGNESIUM AND VITAMIN B6 (ZMA): AN ANALYSIS OF SCIENTIFIC EVIDENCE ON TESTOSTERONE METABOLISM AND RECOVERY PROCESSES

Abstract: *The article reviews current scientific evidence on the biological role of zinc, magnesium, and vitamin B_6 — micronutrients commonly combined in the ZMA formulation. The aim of the study was to analyze available data on the influence of these substances on testosterone-related endocrine regulation, markers of muscle recovery, and sleep quality. A literature review of publications indexed in PubMed, Scopus, and Web of Science was conducted. Zinc and magnesium were found to be important cofactors of steroidogenesis and neuroendocrine regulation, with the most pronounced testosterone-related effects observed in individuals with baseline deficiency of these micronutrients. Data on the combined intake of all three components in non-deficient individuals remain heterogeneous and warrant further study.*

Keywords: *zinc, magnesium, vitamin B6, testosterone, ZMA, steroidogenesis, sleep quality.*

Введение

Оптимальный гормональный статус, в частности концентрация эндогенного тестостерона, является значимым фактором, определяющим физическую работоспособность, композицию тела и общее самочувствие мужчин. Наряду с тренировочными и генетическими факторами, существенную роль в эндокринной регуляции играет обеспеченность организма эссенциальными микронутриентами [1; 2]. Среди них особое внимание уделяется цинку, магнию и витамину B6, которые выступают кофакторами в реакциях стероидогенеза и метаболизма аминокислот, а также участвуют в нейроэндокринных механизмах регуляции сна [3; 4].

Комбинация данных трех веществ, получившая распространение под аббревиатурой ZMA, была впервые предложена в конце 1990-х годов как средство, потенциально способствующее поддержанию физиологического уровня тестостерона и инсулиноподобного фактора роста-1 (ИФР-1) у спортсменов [5]. В состав классической формулы ZMA помимо цинка и магния входит витамин B6 (пиридоксин), а сами минералы используются в форме хелатных соединений с аспарагиновой кислотой (аспартатов), что, согласно концепции разработчиков, повышает их биодоступность по сравнению с неорганическими солями [5].

Актуальность настоящего исследования определяется широкой распространенностью субклинического дефицита цинка и магния в популяции, а также сохраняющейся научной дискуссией относительно того, способно ли дополнительное потребление данных микронутриентов оказывать значимое влияние на эндокринные показатели у лиц без исходного дефицита [6]. Целью работы является анализ современных научных данных о механизмах участия цинка, магния и витамина B6 в регуляции тестостерона, а также обзор имеющихся клинических данных об эффектах их совместного приема.

Материалы и методы исследования

Материалами исследования послужили научные публикации, посвященные биологической роли цинка, магния и витамина B6 в регуляции эндокринных и метаболических процессов человека.

В ходе работы были проанализированы оригинальные экспериментальные исследования, рандомизированные контролируемые испытания, систематические обзоры и метаанализы, опубликованные в рецензируемых международных изданиях по направлениям эндокринологии, спортивной медицины и нутрициологии. В анализ включались публикации, индексируемые в базах данных PubMed, Scopus и Web of Science, содержащие данные о влиянии цинка, магния, витамина B6 и их комбинации на уровень тестостерона, показатели мышечного восстановления и качество сна.

Результаты исследования

Цинк и регуляция тестостерона.

Цинк принимает участие в работе более чем 300 ферментов, в том числе задействованных в стероидогенезе и функционировании гипоталамо-гипофизарно-гонадной оси [1]. В классическом исследовании Прасада и соавт. (1996) было показано, что ограничение диетического потребления цинка у здоровых молодых мужчин в течение 20 недель сопровождалось значительным снижением сывороточного тестостерона (с 11,3±1,1 до 6,9±1,0 нмоль/л; p=0,005); у пожилых мужчин с исходной маргинальной недостаточностью цинка шестимесячная нутритивная коррекция привела к статистически значимому повышению уровня тестостерона (с 8,3±6,3 до 16,0±4,4 нмоль/л; p=0,02) [7]. Была также выявлена значимая корреляция между клеточной концентрацией цинка и сывороточным тестостероном (r=0,43; p=0,006) [7].

Данные результаты позволяют рассматривать цинк как значимый модулятор андрогенного статуса преимущественно в контексте коррекции его дефицита. Вместе с тем в исследованиях, проведенных на лицах без исходной недостаточности цинка, дополнительный прием высоких доз минерала не всегда сопровождался значимым приростом тестостерона, что может свидетельствовать об ограниченном «потолке» эффекта у лиц с адекватным нутритивным статусом [8].

Магний и регуляция тестостерона.

Магний участвует в качестве кофактора более чем в 300 ферментативных реакциях организма, включая процессы, связанные с энергетическим обменом и синтезом стероидных гормонов [9]. Магний способен влиять на транспорт и биодоступность тестостерона; показана его положительная ассоциация с уровнем глобулина, связывающего половые гормоны (ГСПГ), однако влияние на фракцию свободного тестостерона остается предметом дискуссий [10].

Исследование Чинара и соавт. (2011) продемонстрировало, что 4-недельный прием магния (10 мг/кг/день) у мужчин, занимающихся тхэквондо, приводил к увеличению уровня свободного тестостерона на 24% относительно исходного при одновременном снижении ГСПГ [11].

Отдельного внимания заслуживают данные о влиянии магния на качество сна, поскольку восстановительные процессы, происходящие в фазах глубокого сна, тесно связаны с секрецией тестостерона и соматотропного гормона [14]. Магний действует на нервную систему, блокируя рецепторы возбуждения (НМДА) и активируя рецепторы торможения (ГАМК), что способствует снижению тревожности и улучшению засыпания [9].

Витамин B6 и его вспомогательная роль.

Витамин B6 в форме пиридоксаль-5-фосфата выступает кофактором более чем 100 ферментативных реакций, включая трансаминирование и декарбоксилирование аминокислот, а также участвует в метаболизме гликогена и синтезе ряда нейромедиаторов [12]. Прямых данных о

самостоятельном влиянии витамина B6 на уровень тестостерона в научной литературе относительно немного; его включение в состав комплекса ZMA рассматривается авторами первоначальной концепции в первую очередь в контексте поддержания общего метаболического статуса и потенциального содействия усвоению цинка и магния, а также участия в регуляции работы центральной нервной системы, в том числе структур, вовлеченных в нейроэндокринную регуляцию сна.

Совместное применение цинка, магния и витамина B6: данные клинических исследований.

Наибольший научный резонанс получило исследование Бриллы и Конте (2000), в котором у футболистов на фоне восьминедельного ночного приема комплекса цинка, магния и витамина B6 было зафиксировано повышение свободного тестостерона (с 132,1 до 176,3 пг/мл) и общего тестостерона (примерно на 30%), а также увеличение уровня ИФР-1, тогда как в группе плацебо аналогичные показатели снижались [5].

Заключение

Проведенный анализ научной литературы показал, что цинк и магний являются значимыми физиологическими кофакторами стероидогенеза и нейроэндокринной регуляции, а витамин B6 выполняет вспомогательную метаболическую роль, участвуя в ферментативных процессах и потенциально способствуя усвоению других компонентов комплекса. Аспарагиновая кислота, используемая в форме хелатных аспартатов, призвана повышать биодоступность минералов, не оказывая при этом самостоятельного гормонального действия.

Установлено, что наиболее убедительные и воспроизводимые данные о положительном влиянии цинка и магния на уровень тестостерона получены применительно к лицам с исходным дефицитом либо маргинальной недостаточностью данных микроэлементов. В отношении лиц без исходного дефицита данные о клинической эффективности совместного приема цинка, магния и витамина B6 в форме комплекса ZMA остаются неоднородными: наряду с исследованием, впервые предложившим данную комбинацию и продемонстрировавшим положительные результаты, ряд последующих независимых работ не подтвердил значимого влияния на гормональный профиль и силовые показатели.

Отдельный научный интерес представляет способность магния оказывать благоприятное влияние на качество сна, что может рассматриваться в качестве дополнительного, опосредованного механизма поддержки восстановительных процессов организма. Полученные результаты подтверждают необходимость дальнейших рандомизированных контролируемых исследований с обязательной стратификацией участников по исходному нутритивному статусу, что позволит более точно определить популяции, для которых нутритивная коррекция цинком, магнием и витамином B6 может иметь наибольшее физиологическое значение.

Использованные источники:

1. Prasad A.S. Zinc is an antioxidant and anti-inflammatory agent: its role in human health // Frontiers in Nutrition. – 2014. – Vol. 1. – Article 14. – DOI: 10.3389/fnut.2014.00014.
2. Fallah A., Mohammad-Hasani A., Colagar A.H. Zinc is an essential element for male fertility: a review of Zn roles in men's health, germination, sperm quality, and fertilization // Journal of Reproduction & Infertility. – 2018. – Vol. 19, No. 2. – P. 69–81.
3. Volpe S.L. Magnesium in disease prevention and overall health // Advances in Nutrition. – 2013. – Vol. 4, No. 3. – P. 378S–383S. – DOI: 10.3945/an.112.003483.
4. Spinneker A., Sola R., Lemmen V., et al. Vitamin B6 status, deficiency and its consequences – an overview // Nutricion Hospitalaria. – 2007. – Vol. 22, No. 1. – P. 7–24.
5. Brilla L.R., Conte V. Effects of a novel zinc-magnesium formulation on hormones and strength // Journal of Exercise Physiology Online. – 2000. – Vol. 3, No. 4. – P. 26–36.
6. Chasapis C.T., Loutsidou A.C., Spiliopoulou C.A., Stefanidou M.E. Zinc and human health: an update // Archives of Toxicology. – 2012. – Vol. 86, No. 4. – P. 521–534. – DOI: 10.1007/s00204-011-0775-1.
7. Prasad A.S., Mantzoros C.S., Beck F.W.J., Hess J.W., Brewer G.J. Zinc status and serum testosterone levels of healthy adults // Nutrition. – 1996. – Vol. 12, No. 5. – P. 344–348. – DOI: 10.1016/S0899-9007(96)80058-X.
8. Koehler K., Parr M.K., Geyer H., Mester J., Schänzer W. Serum testosterone and urinary excretion of steroid hormone metabolites after administration of a high-dose zinc supplement // European Journal of Clinical Nutrition. – 2009. – Vol. 63, No. 1. – P. 65–70. – DOI: 10.1038/sj.ejcn.1602899.
9. de Baaij J.H.F., Hoenderop J.G.J., Bindels R.J.M. Magnesium in man: implications for health and disease // Physiological Reviews. – 2015. – Vol. 95, No. 1. – P. 1–46. – DOI: 10.1152/physrev.00012.2014.
10. Maggio M., De Vita F., Lauretani F. et al. Magnesium and anabolic hormones in older men // International Journal of Andrology. – 2011. – Vol. 34, No. 6, Pt. 2. – P. e594–e600. – DOI: 10.1111/j.1365-2605.2011.01193.x.
11. Cinar V., Polat Y., Baltaci A.K., Mogulkoc R. Effects of magnesium supplementation on testosterone levels of athletes and sedentary subjects at rest and after exhaustion // Biological Trace Element Research. – 2011. – Vol. 140, No. 1. – P. 18–23. – DOI: 10.1007/s12011-010-8676-3.
12. Ueland P.M., McCann A., Midttun Ø., Ulvik A. Inflammation, vitamin B6 and related pathways // Molecular Aspects of Medicine. – 2017. – Vol. 53. – P. 10–27. – DOI: 10.1016/j.mam.2016.08.001.
13. Leproult R., Van Cauter E. Effect of 1 week of sleep restriction on testosterone levels in young healthy men // JAMA. – 2011. – Vol. 305, No. 21. – P. 2173–2174. – DOI: 10.1001/jama.2011.710.

14. Poleszak E., Szewczyk B., Kedzierska E. et al. Antidepressant- and anxiolytic-like activity of magnesium in mice // Pharmacological Reports. – 2004. – Vol. 56, No. 5. – P. 763–766.

УДК 618:615.355

Язвенко А. А.
свободный исследователь

РОЛЬ КОЭНЗИМА Q10 В ПОДДЕРЖКЕ РЕПРОДУКТИВНОЙ СИСТЕМЫ

Аннотация. *Статья посвящена оценке влияния коэнзима Q10 на репродуктивную функцию, в частности — на качество ооцитов, состояние митохондрий и показатели фертильности. Систематический анализ проведен на основе данных научных баз PubMed, Web of Science, Scopus, Google Scholar и eLibrary. Результаты исследований демонстрируют, что добавление коэнзима Q10 в культуральную среду (в концентрации 50 мкмоль) повышает долю зрелых ооцитов с 48,9% до 75,7%, снижает уровень окислительного стресса и усиливает выработку АТФ за счет оптимизации митохондриальной функции. Прием коэнзима Q10 в течение 30–35 дней способствует накоплению вещества в фолликулярной жидкости, что коррелирует с улучшением качества эмбрионов и ростом вероятности наступления беременности. Практическая значимость работы состоит в обосновании потенциала коэнзима Q10 как компонента протоколов вспомогательных репродуктивных технологий для поддержки качества ооцитов и повышения репродуктивных исходов.*

Ключевые слова: *коэнзим Q10, репродуктивная система, фертильность, ооциты, окислительный стресс, митохондрии, вспомогательные репродуктивные технологии.*

Iazvenko A. A.
independent researcher

THE ROLE OF COENZYME Q10 IN SUPPORTING THE REPRODUCTIVE SYSTEM

Abstract. *The article is devoted to assessing the effect of coenzyme Q10 on reproductive function, in particular on oocyte quality, mitochondrial status, and fertility indicators. A systematic analysis was carried out based on data from the scientific databases PubMed, Web of Science, Scopus, Google Scholar, and eLibrary. Research results demonstrate that adding coenzyme Q10 to the culture medium (at a concentration of 50 μmol) increases the proportion of mature oocytes from 48.9 % to 75.7 %, reduces the level of oxidative stress, and enhances ATP production by optimizing mitochondrial function. Taking coenzyme Q10 for 30–35 days promotes the accumulation of the substance in follicular fluid, which correlates with improved embryo quality and an increased likelihood of pregnancy. The practical significance of the study lies in substantiating the potential of coenzyme Q10 as a component of assisted reproductive technology protocols to support oocyte quality and improve reproductive outcomes.*

Keywords: *coenzyme Q10, reproductive system, fertility, oocytes, oxidative stress, mitochondria, assisted reproductive technologies.*

Введение

Рост распространенности нарушений репродуктивной функции остается одной из значимых проблем современного здравоохранения, сопряженной с серьезными социальными и демографическими последствиями. По данным Всемирной организации здравоохранения (ВОЗ), около 17,5% взрослого населения планеты — то есть каждый шестой человек репродуктивного возраста — сталкивается с трудностями зачатия [1]. Устойчивый рост этого показателя обусловливает необходимость поиска эффективных и патогенетически обоснованных подходов к повышению фертильности и оптимизации результатов вспомогательных репродуктивных технологий.

Особое внимание в современных исследованиях уделяется стратегиям улучшения качества гамет, поскольку морфофункциональные характеристики ооцитов напрямую определяют вероятность успешного оплодотворения, развития эмбриона и наступления устойчивой беременности. В этом контексте перспективным кандидатом выступает коэнзим Q10 — эндогенное соединение, обладающее выраженной антиоксидантной активностью и играющее ключевую роль в митохондриальном энергообмене клеток. Доказано, что коэнзим Q10 способен снижать уровень окислительного стресса в репродуктивных тканях, поддерживать функциональную активность митохондрий и тем самым улучшать параметры ооцитов [2]. Однако, несмотря на накопленные данные, механизмы влияния коэнзима Q10 на процессы оогенеза и эмбриогенеза требуют дальнейшей систематизации, а клинические эффекты — подтверждения в рамках строгих доказательных подходов.

Целью настоящей статьи является изучение роли коэнзима Q10 в поддержке репродуктивной системы, в частности его влияния на качество ооцитов, функциональное состояние митохондрий и показатели фертильности. Гипотеза исследования заключается в том, что применение коэнзима Q10 способствует улучшению репродуктивных исходов за счет модуляции окислительного стресса, оптимизации энергетического обмена в ооцитах и повышения вероятности наступления беременности, что делает его потенциально ценным компонентом в протоколах вспомогательных репродуктивных технологий.

Методы исследования

Настоящее исследование представляет собой самостоятельный систематический анализ медицинской литературы реферативных баз данных и систем цитирования PubMed, Web of Science, Scopus, Google Scholar, eLibrary по влиянию коэнзима Q10 на репродуктивную систему.

В рамках систематического обзора и мета-анализа проанализированы опубликованные исследования, посвященные влиянию коэнзима Q10 на созревание ооцитов, качество эмбрионов и показатели фертильности.

Результаты

В исследовании Ч. Х. Ли и соавторов в условиях культивирования добавление коэнзима Q10 в концентрации 50 мкмоль в питательную среду способствовало увеличению доли зрелых женских половых клеток с 48,9% до 75,7%. При этом в окружающих клетках отмечено снижение уровня активных форм кислорода и повышение содержания белков Bcl2 и Sirt1 [3]. Полученные данные свидетельствуют о том, что коэнзим Q10 положительно влияет на процесс созревания клеток, используемых для оплодотворения.

В ходе исследования С. Р. Джаннубило и соавторов было установлено, что ежедневный прием коэнзима Q10 в течение 30–35 дней способствует повышению его концентрации в фолликулярной жидкости. Это, в свою очередь, соотносится с улучшением качества получаемых эмбрионов и увеличением вероятности наступления беременности [4].

Я. Лян с соавторами продемонстрировали в исследовании, что внесение коэнзима Q10 в культуральную среду в концентрации 50 мкмоль положительно влияет на созревание ооцитов. Под действием коэнзима повышается эффективность энергетического обмена за счет усиления синтеза АТФ и оптимизации функции митохондрий, одновременно снижается уровень активных форм кислорода и уменьшается вероятность преждевременной гибели клеток. Важно, что благоприятный эффект сохраняется даже в отношении ооцитов с исходными нарушениями — это подтверждает потенциал коэнзима Q10 как средства поддержки репродуктивной функции на клеточном уровне [5].

Заключение

Полученные в ходе систематического анализа данные подтверждают выдвинутую гипотезу: применение коэнзима Q10 способствует улучшению репродуктивных исходов за счет модуляции окислительного стресса, оптимизации энергетического обмена в ооцитах и повышения вероятности наступления беременности.

Ключевые выводы:

Коэнзим Q10 повышает долю зрелых ооцитов и снижает уровень окислительного стресса в репродуктивных тканях.

Прием коэнзима Q10 в течение 30–35 дней способствует накоплению вещества в фолликулярной жидкости и улучшает качество эмбрионов.

Вещество усиливает выработку энергии в ооцитах и поддерживает жизнеспособность даже клеток с исходными нарушениями.

Таким образом, коэнзим Q10 может служить эффективным средством поддержки репродуктивной функции.

Использованные источники:

1. Всемирная организация здравоохранения. Каждый шестой человек в мире страдает от бесплодия [Электронный ресурс] // Официальный сайт

Всемирной организации здравоохранения. — 2023. — (дата публикации: 04.04.2023). — URL: https://www.who.int/ru/news/item/04-04-2023-1-in-6-people-globally-affected-by-infertility (дата обращения: 14.07.2026).
2. Александру И., Нистор Д., Мотофелеа А. К., Кадар Андоне Б. А., Кринтеа А., Тату К., Поп Г. Н., Цсеп А. Н. Витамины, коэнзим Q10 и антиоксидантные стратегии для улучшения качества ооцитов у женщин с гинекологическими злокачественными новообразованиями: всесторонний обзор / Alexandru I., Nistor D., Motofelea A. C. et al. // Antioxidants (Basel). — 2024. — Т. 13, № 12. — С. 1567.
3. Ли Ч. Х., Кан М. К., Сон Д. Х., Ким Х. М., Ян Дж., Хан С. Дж. Коэнзим Q10 улучшает качество ооцитов мыши при культивировании in vitro // Zygote. — 2022. — Т. 30, № 2. — С. 249–257.
4. Джаннубило С. Р., Орландо П., Сильвестри С., Чирилли И., Марчеджани Ф., Чаваттини А., Тиано Л. Приём коэнзима Q10 у пациенток, проходящих ЭКО-ЭТ: взаимосвязь с содержанием в фолликулярной жидкости и зрелостью ооцитов // Antioxidants (Basel). — 2018. — Т. 7, № 10. — С. 141.
5. Лян Я., Ван Х., Сун С. и др. Системное понимание антивозрастного эффекта коэнзима Q10 на ооциты с применением подхода сетевой фармакологии // Frontiers in Endocrinology (Lausanne). — 2022. — Т. 13. — С. 813772.

УДК 616.594:615.356.

Язвенко А. А.
свободный исследователь

КОРРЕКЦИЯ СОСТОЯНИЯ ВОЛОС С ПОМОЩЬЮ НУТРИЦЕВТИЧЕСКОЙ ПОДДЕРЖКИ ОРГАНИЗМА

Аннотация. *Статья посвящена изучению влияния нутрицевтической поддержки на коррекцию состояния волос и кожи головы. Систематический обзор и мета-анализ проведены на основе данных научных баз PubMed, Web of Science, Scopus, Google Scholar и eLibrary. Результаты исследований подтверждают эффективность отдельных нутриентов: приём цинка (15–30 мг/сут в течение 3 месяцев) снижает интенсивность алопеции в 70% случаев; восьмимесячный прием витамина Е способствует увеличению густоты волос на 34,5%; восполнение дефицита витаминов группы В улучшает состояние волос в 55% случаев. Практическая значимость работы заключается в обосновании включения целенаправленной нутрицевтической коррекции в схемы терапии трихологических нарушений.*

Ключевые слова: *трихология, алопеция, нутрицевтическая поддержка, цинк, витамин Е, витамины группы В, состояние волос.*

Iazvenko A.A.
independent researcher

CORRECTION OF HAIR CONDITION THROUGH NUTRITIONAL SUPPORT OF THE BODY

Abstract. *The article is devoted to studying the effect of nutritional support on correcting the condition of hair and scalp. A systematic review and meta-analysis were carried out based on data from the scientific databases PubMed, Web of Science, Scopus, Google Scholar, and eLibrary. The research results confirm the effectiveness of certain nutrients: zinc supplementation (15–30 mg per day for 3 months) reduces the intensity of alopecia in 70 % of cases; an eight-month course of vitamin E intake contributes to a 34.5 % increase in hair density; correcting the deficiency of B-group vitamins improves hair condition in 55 % of cases. The practical significance of the study lies in substantiating the inclusion of targeted nutritional correction in treatment regimens for trichological disorders.*

Keywords: *trichology, alopecia, nutritional support, zinc, vitamin E, B-group vitamins, hair condition.*

Введение

Заболевания волос и кожи головы является распространенной и социально значимой проблемой, ухудшающей качество жизни людей. Патологиями трихологического профиля страдает каждый третий житель

Земли. При этом, если у человека возникают одновременно нарушения состояния кожи, волос или ногтей, наибольшее психологическое напряжение вызывают именно проблемы с волосами, которые он стремится устранить в первую очередь [1]. В России качеством волос недовольны до 80% населения. С возрастом выпадение волос затрагивает 96% мужчин и 79% женщин [2]. Тем не менее, несмотря на высокую социальную значимость и широкую распространенность трихологических патологий, патогенетические механизмы дефицитарных состояний, оказывающих влияние на состояние волос и кожи головы, а также подходы к их системной коррекции, по-прежнему остаются недостаточно исследованными.

Цель настоящей статьи — изучение влияния нутрицевтической поддержки организма на улучшение структуры и динамику роста волос. Гипотеза исследования заключается в том, что комплексное восполнение дефицитов макро- и микронутриентов оказывает обоснованное воздействие на волосяные фолликулы, что способствует эффективной коррекции состояния волос и кожи головы.

Методы исследования

Исследование базировалось на систематическом обзоре и мета-анализе релевантной научной литературы, доступной в базах данных PubMed, Web of Science, Scopus, Google Scholar и eLibrary.

В рамках обзора и мета-анализа рассмотрены исследования, отражающие вклад витаминов и минералов в поддержание здоровья волосяных фолликулов и улучшение качественных характеристик волос.

Результаты

В исследовании группы японских ученых под руководством Т. Карашимы продемонстрирована эффективность перорального приема цинка в коррекции патологического выпадения волос. Применение микроэлемента в дозе 15–30 мг/сут на протяжении 3 месяцев привело к снижению интенсивности алопеции у 70% участников. Механизм действия цинка связан с его участием в биосинтезе белков и ДНК — ключевых компонентов, обеспечивающих жизнедеятельность волосяных фолликулов и нормальный цикл роста волос [3]. Полученные данные подтверждают целесообразность применения цинка в составе терапевтических схем при повышенном выпадении волос.

В рамках научного исследования, проведенного группой ученых под руководством Л. Б. Бей в 2010 году, изучалось влияние антиоксидантных свойств витамина Е (токотриенола) на снижение окислительного стресса при патологическом выпадении волос. Контролируемый восьмимесячный эксперимент продемонстрировал, что ежедневный прием препарата способствует статистически значимому увеличению густоты волос на 34,5% за счет нейтрализации свободных радикалов и оптимизации микроциркуляции [4]. Полученные данные подтверждают эффективность перорального приема витамина Е как средства для стимуляции роста и повышения плотности волосяного покрова.

Исследование, проведенное М. В. Рябковой, В. Н. Терещенко и И. Н. Сормолотовой в 2015 году, продемонстрировало значимую взаимосвязь между обеспеченностью организма витаминами группы В и состоянием волос. Восполнение дефицита витаминов в составе комплексной терапии привело к улучшению состояния волос у 55% обследованных пациентов [5]. Полученные данные свидетельствуют о том, что коррекция нехватки витаминов группы В представляет собой обоснованный компонент терапевтических мероприятий при выпадении волос.

Заключение

Полученные данные подтверждают выдвинутую гипотезу: комплексное восполнение дефицитов макро- и микронутриентов оказывает обоснованное воздействие на волосяные фолликулы и способствует эффективной коррекции состояния волос и кожи головы.

Ключевые выводы:

Цинк снижает интенсивность алопеции в 70% случаев за счет поддержки биосинтеза в фолликулах.

Витамин Е за 8 месяцев повышает густоту волос на 34,5% за счет снижения окислительного стресса.

Коррекция дефицита витаминов группы В улучшает состояние волос в 55% случаев.

Таким образом, нутрицевтическая поддержка с восполнением дефицитов витаминов и минералов может быть включена в схемы коррекции трихологических нарушений.

Использованные источники:

1. Мазитова Л.П., Богатырева И.Г. Аспекты патогенеза и лечения телогеновой алопеции // Тез. науч. работ Все-росс. съезда дерматологов. Часть 1. — 2001. — С. 86-98.
2. Крестьянинова О.А. Современная косметология. Новейший справочник / О.А. Крестьянинова. — Санкт-Петербург: Сова; Москва: Эксмо, 2004. — С. 125.
3. Карасима Т. и др. Пероральная терапия цинком при телогеновой алопеции // Dermatologic Therapy. 2012. Т. 25, № 2. С. 210–213.
4. Бей, Л. Б. Влияние применения добавок с токотриенолом на рост волос у добровольцев / Л. Б. Бей, В. Дж. Вуэй, И. К. Хэй // Исследования в области тропических биологических наук. — 2010. — Т. 21, № 2. — С. 91–99.
5. Рябкова М. В., Терещенко В. Н., Сормолотова И. Н. Витамины в клинической трихологии и дерматологии // Забайкальский медицинский журнал. — 2015. — № 2. — С. 29.

DOI 10.24412/2412-9682-2026-7133-72-84
УДК 159.97, 37.013.2

Цветков А. В., доктор психологических наук
профессор
Московский институт психоанализа
г. Москва, РФ

НЕЙРОПЕДАГОГИКА КАК ОБЛАСТЬ НАУКИ И ПРАКТИКИ: ЧТО, КОМУ, ЗАЧЕМ?

Аннотация. *На основе анализа литературы и примеров из психолого-педагогической практики дано определение нейропедагогики - это обучение и воспитание по законам работы мозга, имея в виду под «законами» ряд психолого-педагогических закономерностей обучения, для которых изучен нейропсихологический механизм реализации, показано, что именно подход А.Р. Лурия и Л.С. Цветковой наиболее отвечает задачам обучения и воспитания, оконтурены сферы компетентности «нейропедагога» и «прикладного нейропсихолога в образовании» в свете появления таких профилей магистратур в ряде вузов России.*

Ключевые слова: *нейропедагогика, нейропсихология А.Р. Лурия, задачи образования, сфера компетенции специалиста.*

Tsvetkov A. V., doctor of psychology,
professor
Moscow Institute of Psychoanalysis,
Moscow, Russian Federation

NEUROPEDAGOGICS AS A FIELD OF SCIENCE AND PRACTICE: WHAT, TO WHOM, AND WHY?

Abstract. *Basing the analysis of scientific literature and psychological and pedagogical practice examples, neuropedagogy is defined as teaching and upbringing according to the laws of the brain activity, meaning by "laws" a number of psychological and pedagogical learning patterns that have studied neuropsychological mechanisms of implementation, it is shown that A.R. Luria's and L.S. Tsvetkova approach to neuropsychology mostly meets the tasks of teaching and upbringing. The competence fields of "neuropedagogue" and "applied neuropsychologist in education" have been outlined in the light of such master's degree profiles emergence in a number of Russian universities.*

Keywords: *neuropedagogy, neuropsychology by A.R. Luria, educational objectives, specialist's area of competence.*

Вопросы «кому и зачем» в заголовке статьи являются не только полемическим приемом автора, как может показаться.

Начнем с того, что приставка «нейро-» в текущий момент является коммерческим ярлыком, позволяющим «продавать», в широком смысле слова, разные товары, технологии, методики. Скажем, М.Ю. Абабкова и В.Л. Леонтьева [1] пишут о «нейрообразовании» как целом, но довольно быстро сужают поле анализа к интересным им методикам биологической обратной связи.

Относятся ли БОС к «нейро-методам в обучении»? Да. Исчерпывает ли собой всю предметную область нейропедагогики? Конечно, нет, и ученые об этом справедливо пишут.

Поэтому, спрашивая «кому и зачем», ведём беседу как об этике, так и о методологии, и о разграничении профессиональных ролей.

Так, наш уважаемый коллега С.Н. Перегуда [9] задается вопросом: этично ли работать в нейропсихологической коррекции детей по некоторой методологии без учета наличия других подходов к пониманию механизмов нарушений. Вопрос не умозрительный. Возьмем для примера группу детей с расстройствами аутистического спектра. В рамках нейропсихологии есть несколько гипотез о наиболее значимом механизме этих расстройств. Первая, это сниженный психический тонус, как следствие — гиперсенсорность, проблемы отделения значимых стимулов от побочных. Коррекционная помощь в таком видении будет строиться на основе сенсомоторных методов. Вторая гипотеза, обратно, говорит о слишком глубоком и истощающем поиске связей внутри сверхценно-интересной ребенку области. Тогда путь помощи, очевидно, когнитивный, работа с мышлением. Третий подход предполагает сравнительно здоровую нервную систему, находившуюся в неадекватной предметно-социальной среде. При этом «аутизация» становится неверным способом решения задач, а «исправление» ситуации лежит на пути оперантного научения с формированием социально-адекватных познавательных и коммуникативных навыков. Чем и занимается прикладной анализ поведения, он же АВА.

Реальная ситуация оказывается еще сложнее: что если (такие научные данные появляются!) все три подхода верны, просто каждый — для своей подгруппы детей? Может ли нейропсихолог оказывать коррекционную помощь, если он не уверен в правильности избранной позиции относительно механизма и коррекции?

Случаи упущенных возможностей, растраты времени, когда мозг пластичен, и реабилитационного потенциала на недостаточно эффективные методы коррекции, знакомы каждому специалисту.

И либо каждый конкретный случай просеивается через этическое «сито», моя ли методология анализа и коррекции здесь оптимальна. Либо нейропсихолог опускается на уровень механического воспроизведения отдельных приемов «делай раз, делай два».

Та же трудность стоит и перед С.В. Покровской [11], справедливо указывающей, что «даже у условно-здоровых с биологической точки зрения детей преобладающим [в настоящее время] является «дефицитарный» тип развития». Что, к каждому ребенку — по нейропсихологу?

Категорически нет. Должна быть сохранна обучаемость и возможности высшего синтеза (требует органической полноценности ассоциативных зон коры), профиль развития функций должен отличаться неравномерностью, но не тотальным снижением (как при умственной отсталости), дети со сложными формами познавательных дефицитов требуют «бригадного подряда», с динамической сменой вклада времени и сил каждого из специалистов и коллективным анализом ситуации.

Возвращаясь к статье С.Н. Перегуды, есть и вопросы коммуникации специалиста с клиентом, где всё большую роль играет удаленные способы вроде общения в мессенджерах и использование гаджетов, инструментов искусственного интеллекта в конкретных диагностико-коррекционных процедурах. На деле, как нам кажется, это та же проблема распределения ответственности, «сознательный специалист против бездумного техника».

К этике С.Н. Перегуда относит и моменты включения личностной позиции специалиста в диагностику и коррекцию. Вот нейропсихолог наблюдает некоторый объем восприятия или памяти у ребенка. Физиологически это довольно устойчивый показатель. То есть что в 10, что в 15, что в 30 лет один и тот же человек из предъявленного ряда «десять слов по А.Р. Лурия» будет запоминать 6-8. Счесть это «нормой»? Дать рекомендации по коррекции (поиску «обходных путей» для запоминания)? Провести консультирование для семьи по поводу ограничений в дальнейшем самоопределении? Та же профессия диспетчера авиатранспорта вряд ли будет эффективно освоена при таком объеме запоминания и восприятия.

Помимо личностной позиции, думаю, с этим коллеги согласятся, значение имеет и место приложения усилий.

Общеобразовательная школа или детский сад, государственное коррекционное учреждение, частный центр развития или центр помощи, больница, реабилитационная организация — вариантов немало.

Традиционно «нейропсихология» была одним из профилей подготовки клинических психологов, «место» для которых, в первую очередь, находилось в медицине или специальном (коррекционном) образовании.

Такая предметная область как «нейропедагогика» обсуждается уже порядка 40 лет, и последние годы — с ростом интенсивности. Однако как практический вид деятельности нейропедагогика не была институционализирована. Да, был методический поиск конкретных учителей, педагогов-психологов (психологов в образовании) и заинтересованных родителей. Были научные работы, в т.ч. в виде экспериментов по новым способам обучения. Но единого «ремесла» не существовало.

Теперь ситуация меняется. Как минимум в двух вузах России открыт прием на программы магистерского уровня: по психолого-педагогическому образованию, «Нейропедагогика и прикладная нейропсихология в образовании», в Московском институте психоанализа; по педагогическому образованию, «Нейропедагогика», Тамбовский государственный университет им. Г.Р. Державина. В ряде других крупных институций (БФУ им. И. Канта, НИУ ВШЭ, ЮФУ и др.) «прикладные нейронауки» также звучат в наименованиях программ.

Чему будут учить? Какова планируемая профессиональная реализация выпускников? В чем разница нейропсихолога, нейропедагога, прикладного нейропсихолога в образовании?

Появляются и новые самоопределения, еще не устоявшиеся как научный факт, но широко распространенные как маркетинговое позиционирование: инструктор по когнитивному развитию, тренер mind fitness (майнд фитнес) и др.

Попробуем разобраться.

Начнем с определений. Группа И.П. Клемантович, Е.А. Левановой и В.Г. Степанова [5] определили нейропедагогику «как теорию и технологию воспитания и обучения детей, молодежи и взрослых на основе использования данных современных нейронаук».

Уточняя и несколько сужая данное определение, А.В. Цветков (автор данного сообщения) считает: нейропедагогика это обучение и воспитание по законам работы мозга, имея в виду под «законами» ряд психолого-педагогических закономерностей обучения, для которых изучен нейропсихологический механизм реализации.

В отличие от определения проф. Клемантович с соавт., А.В. Цветков подчеркивает: а) отсутствие прямого применения к обучению и воспитанию данных анатомии и физиологии мозга, «обучается и воспитывается» личность и её (деятельного субъекта) ВПФ; б) ведущей нейронаукой, «соединяющей» ВПФ и анатомо-физиологические особенности мозга как органа, считается нейропсихология А.Р. Лурия; в) как частные методики, так и общепедагогические теории не только могут быть оптимизированы при анализе того, как «реально учится мозг» (через призму нейропсихологии), но, в ряде случаев, и отвергнуты.

Группа И.П. Клемантович, на самом деле, говорит о том же несколько иными словами: «нейропедагогика - высшая, современная ступень классической педагогики. Она учитывает достижения последней; отбирает, уточняет и развивает ее наиболее эффективные методы и методики, предлагает и внедряет новые».

Проще говоря, основное разногласие двух определений состоит в более широком (современные нейронауки в целом) или узком (нейропсихология, причем конкретно — направление, заданное А.Р. Лурия и Л.С. Цветковой) понимании базиса нейропедагогики.

Поясним.

И.П. Клемантович, Е.А. Леванова и В.Г. Степанов полагают, что открытия лурьевской нейропсихологии, свершенные на начальном этапе на материале нейрохирургических больных, более релевантны новым подходам в дефектологии (коррекционной педагогике), но не обучению «вообще».

Мы же опираемся на позицию П.Я. Гальперина и А.Н. Леонтьева, полагавших: та форма, в которой удалось в ходе специально организованного формирующего обучения «вложить» определенную ВПФ из внешнего плана протекания во внутренний, максимально близко отвечает строению ВПФ как психического образования. Также опираемся и на закон Блонского-Рибо, в обобщенном виде формулируемом так: те психические образования, которые раньше всех формируются (в онтогенезе), позднее всех (при повреждениях мозга или ослабоумливающих заболеваниях) распадаются.

Иными словами, если даже при тотальной и субтотальной формах афазии (такой распад речи при заболеваниях мозга, когда понимание/порождение устной речи, фактически, абсолютно невозможно) по данным Л.С. Цветковой сохраняется глобальное чтение, то именно эта форма чтения — первична при освоении детьми. Добавим, что сохранным оказывается не чтение отдельных слов (как на карточках Г. Домана), но возможность соотнести короткий, 2-3 фразы, текст с сюжетной картинкой. Это означает, что аналитико-синтетический метод обучения чтению, где синтез из букв слогов, потом слов стоит на первом месте, не отвечает тем «законам работы мозга», которые на практике проверены лурьевской нейропсихологией. Вот пример того, где очень близкие как по форме, так и по содержанию определения нейропедагогики «срабатывают» по-разному.

Обсуждая место «нейродидактики» в методологии педагогики, Е.А. Местоева и М.Х Мальсагова [8] отдают новому направлению мысли значимые позиции. Основой является интегративный характер «нейродидактики» (как уже указывалось, термин, пока не отделенный от «нейропедагогики»): «коррелирует с теорией информации, положениями диалектического материализма и дидактического прагматизма, смежными науками: когнитивной психологией, нейропсихологией, нейроанатомией, нейробиологией, нейрофизиологией».

Таким образом, основная методологическая задача нейродидактики исследовательницам видится не в создании новых технологий и приемов, но в устранении противоречий между находками разных наук, прямо или косвенно связанных с обучением.

Стоит обратиться к практическому примеру. Так, Е.А. Местоева и М.Х Мальсагова вскользь упоминают «типы памяти и обусловленные ими стили обучения» как один из объектов внимания «нейродидактики». При нашем участии [14] была выполнена работа, соотносившая сформированность памяти разных модальностей (тактильно-кинестетической, зрительной, слухоречевой) с успешностью обучения в средних и старших классах школы. Наибольшим положительным влиянием на средний балл обладала память на

тактильные (стереогностические) стимулы и пространственное мышление, отрицательным — опора на зрительную память как ведущую модальность фиксации информации.

Среди выводов авторами работы была высказана идея о сущностной связи тактильно-кинестетико-пространственной модальности обработки, с одной стороны, со схемой и образом тела, как компонентами Я-образа. С другой — о сложностях перешифровки объемных зрительных представлений, симультанных, по сути, в относительно линейный текст, требуемый от учащегося в качестве ответа на задания по всем основным предметам.

Это пример, наглядно (просим прощения за каламбур!) иллюстрирующий противоречие принятых и активно внедрявшихся в минувшие 10-20 лет технологий, в частности, мультимедийных, с опорой на «картинка+текст», с реальными закономерностями развития мозга и процесса обучения.

Нейропедагогика или «нейродидактика» позволили бы (и подобный эмпирический опыт — не новость для педагогов-практиков!) с небольшими затратами снять это и подобные противоречия. Например, при изучении геометрии, особенно «в объеме» (стереометрии) использование каминных длинных спичек и пластилина для создания моделей каждым учеником не «вместо», а «вместе» с наглядными пособиями в виде плакатов или мультимедиа-презентаций, позволило снизить число учеников, тотально не справляющихся с материалом. Тут надо пояснить, что в возрасте 12-14 лет по данным детской нейропсихологии проходит сензитивный период динамического фактора (заднелобные отделы коры мозга). А перешифровки «зрительное представление — движение (в рисунке) — вербально-логическая форма представления решения» требует множественных переключений, то есть дает на динамический фактор повышенную нагрузку. Сделанная в реальном, а не воображаемом, объеме модель позволяет сократить число переходов от движения к представлению и обратно, что и повышает качество знаний.

Термины «нейропедагогика» и «нейродидактика» Э.Ф. Зеер [4] полагает обозначающими «научно-прикладные отрасли нейрообразования». Различия имеют как общепедагогический характер — дидактика как теория обучения по своей предметной отнесенности меньше, чем педагогика, включающая как обучение, так и воспитание, и специальное (в т.ч. коррекционное) образование. Так и характер различий научных школ: «нейропедагогика» и «нейрообразование» чаще звучат в работах американских и британских авторов, «нейродидактика» - ученых из континентальной Европы. Содержательно же области «нейропедагогики» и «нейродидактики» в основном перекрываются.

Говоря о коррекционной помощи дошкольникам с недоразвитием речи, Л.Н. Макарова и С.А. Перышкова [7] так же отводят «нейропсихологическим технологиям» в педагогической практике интегративную позицию: по

мнению авторов, отсылка структуры речевого и сопровождающего его познавательного дефицита к особенностям развития мозга ребенка «сближает логопедический, психологический и клинический аспекты диагностического обследования», делают коррекционную работу направленной на «ядро» синдрома, а не на отдельные симптомы.

Для примера можно обратиться к проблеме понимания речи на слух, достаточно частотную в дошкольном детстве. Вульгарно-логопедический подход, свойственный некоторым специалистам «на местах», грубо и однозначно уравнивает непонимание речи с «сенсорной алалией» (недоразвитием структур мозга, обеспечивающим фонематический слух). Между тем, в работах Т.Г. Визель, М.И. Лынской, наших собственных показана на эмпирическом материале гораздо более сложная модель обработки слухоречевой информации: 0) адекватное проведение нервного импульса от внутреннего уха через ствол к коре мозга; 1) слуховой ориентировочный рефлекс в ядрах среднего мозга; 2) удержание слуховой информации в ультра кратковременной памяти (она же «объем восприятия») на уровне промежуточного мозга и базальных ганглиев; 3) разделение в коре правого полушария на сенсорной основе речи, предметных шумов, музыки и сложных шумов (без однозначной предметной отнесенности), опознание по фонетическим абрисам упроченных (штампованных) конструкций, например, имени (у имен «Ванюша» и «Валюша» абрис одинаковый, но сами имена разные); 4) передача предметных шумов и речи в височные отделы коры левого полушария через мозолистое тело; 5) опознание речевого содержания фонематическим слухом, предметных шумов — через предметные образы-представления (вторая височная извилина и зона ТРО слева); 6) соотнесение выделенных слов, опознанных предметных образов и квазипространственной грамматической конструкции в зоне ТРО; 7) передача полученного содержания (дугообразные волокна) и их интерпретация в лобных отделах.

«Поломка» возможна на любом из 8 этапов обработки информации. Например, при «сбоях» на 6-7 ступени работы с речью ребенок прекрасно понимает отдельные слова, выполняет короткие инструкции типа «дай стакан». Но уже чуть более сложное построение фразы, «налей воды в стакан и дай мне» сталкивается с затруднениями. При дефиците объёма восприятия (2) сложные инструкции понимаются при повторении, с паузами между словами.

Иными словами, коррекционная работа напрямую с «пониманием речи» не будет иметь положительного эффекта без анализа структуры синдрома, выделения первично пострадавшего, вторично вовлеченных и, наоборот, сильных звеньев построения психики. Именно такой анализ, интегрирующий медицинское (структуры, связи и химия мозга) и психолого-педагогическое представление проводится нейропсихологом.

О том же пишут и Б.М. Коган, А.М. Ляпина [6]: «существующая ранее методология коррекции детей с определенными трудностями в обучении или

поведении… не давала необходимых результатов, так как не могла повлиять на развитие ребенка системно и комплексно. Нейропсихологический подход способен решить данную задачу, потому как именно он учитывает синдромный анализ нарушения и предполагает не прямое воздействие на изолированную функцию, а комплексную работу с ней, включая... вовлечение в деятельность и в систему работы других функций».

В подобном ключе высказывается и проф. Э.Ф. Зеер [4], «нейродидактика, исследующая закономерности обучения, связанные с особенностями деятельности высших психических функций мозга. Задача нейродидактики — персонализация учебной деятельности и персонификация обучающихся». Последнее положение привлекает особенное внимание: «персонификация» вплотную сближается с упоминаемой в одной из работа Ж.М. Глозман [3] принципиальной «субъектностью» лурьевской нейропсихологии, её опорой не столько на познавательные процессы, сколько на личность.

Именно это и подразумевается в дальнейшем развертывании работы Э.Ф. Зеера: если обучающийся (не обучаемый!) это субъект познавательной деятельности, то он способен на основе образа будущего личностно отнестись к изучаемому материалу, обратить внимание (как метафору когнитивных ресурсов в целом) на углубленное освоение избранных аспектов и принять деятельное, а не формальное, участие в практических заданиях по превращению «знаний» в «умения и навыки».

Внимание группы А.И. Тащевой [12] сосредоточено на применении «нейродидактики» как средства профилактики дидактогений, нарушений эмоционально-личностной и познавательной сфер ввиду неверного методически или неадекватного по стилю общения преподавания.

Общий вывод проведенного анализа состоит в необходимости не только учитывать ценностно-смысловой контекст, но и распределять «отсылки» к нему, выходя за рамки самого занятия. Обращение ко всем временным модусам индивидуальности (временной перспективе) и учет мозговой организации «человека как целостности» — вот, по мнению авторов, ядро «нейродидактики».

Иными словами: обучение становится «мозго-ориентированным» на основе не конкретных техник или приемов. «Осмысленность» — это не только учет индивидуальной и социокультурной иерархии мотивов, но и понимание того, что в разные возраста — а, значит, и в разное внутреннее «время» обучаемого важны разные мотивы. Так, мотив аффилиации, принадлежности к группе, равно по силе значим что в 15 лет, что в 30.

Но в подростковом возрасте это группа сверстников, связанная субкультурными интересами и личной симпатией. У взрослых, скорее, личная симпатия основывается на сходном уровне и качестве достижений — в профессии, строительстве семьи и отношений, самореализации в каких-то хобби.

Поэтому один и тот же учебный материал для одних слушателей это внутреннее «сегодня», у других - «завтра», у третьих «вчера». А у части группы, увы, проходит мимо ценностно-смысловых ориентаций.

Временная перспектива, как было показано ранее [13], является неотъемлемой частью Я-образа. Который, в свою очередь, завязан биологически на систему подкрепления «дофамин-эндорфин».

Преподаватель «попал» в смысловую сферу и верно адресовал к временной перспективе как части Я-образа, тогда материал будет мотивационно подкреплён для усвоения. Не «попал»? Будет вынужденное обучение, результат которого сохраняется только пока его проверяют, а за незнание положены санкции.

Особенную остроту проблема поиска путей «входа» в смысловую сферу ученика имеет при обучении детей — с одной стороны, ввиду незрелости мотивации, с другой — из-за немалого числа детей «проблемных» или «с трудностями в обучении».

По словам Ж.М. Глозман [2], проблемные дети «не имеют клинических диагнозов, но демонстрируют выраженные признаки дезадаптивного поведения и трудности обучения», больше того, «авторы во всём мире отмечают неуклонный рост числа [таких] детей».

В другой работе проф. Глозман, совместно с А.В. Плотниковой [10], указывается на отсутствие адекватной помощи «проблемным» детям в массовой школе при одновременном признании невозможности спонтанного «исправления ситуации» в развитии этих детей. При этом от 15 до 40% учеников начальной школы указываются как относящиеся к категории «проблемных», что делает крайне актуальной разработку не столько даже методов помощи им, сколько организационно-методических моделей такой помощи.

Противоречие состоит в том, что углубленно-индивидуальный, качественный характер нейропсихологической диагностики мало совместим с обучением 30-35 детей в каждом классе и укрупнением школ, при котором администрация распыляет свое внимание на 10-15 «площадок» с суммарным количеством обучающихся в несколько тысяч человек.

Относительно снятия противоречия тандем авторов пишет следующее: «такую задачу представляется возможным разрешить с помощью многоступенчатой диагностики по принципу «сита», имеющего все более мелкий размер ячеек с каждой следующей ступенью».

Модель помощи видится четырехступенчатой, с объединением (помимо нейропсихолога) в единую «бригаду» педагога начальных классов, педагога-психолога (школьного психолога) и социального педагога. Первый этап — фронтальная диагностика учеников при помощи экономного по времени и обладающего дискриминативным (различительным) потенциалом метода из педагогической психологии. Второй — углубленная индивидуальная диагностика методами нейропсихологии. Третий этап — это выработка «бригадой» и реализация всеми ее участниками программы

коррекционных мероприятий. Наконец, этап №4 представлен «выходной» диагностикой достигнутых результатов с коллективным обсуждением дальнейших прогнозов и шагов в треугольнике «школа-ребенок-семья».

Понимая ограниченность временных, финансовых и человеческих ресурсов школы и как социального института и конкретных школ, после апробации ступенчатой модели помощи её авторы оговариваются, что «главной задачей школьного нейропсихолога является координация всего процесса сопровождения от диагностики до разработки коррекционно-развивающих программ для детей и обучающих программ для педагогов».

Для педагогов-предметников, от начального общего до высшего и послевузовского образования, тема «проблемных детей» - и вырастающих из них студентов, аспирантов, работников, является причиной формулирования новой общепедагогической задачи. Она обозначается как «активизация когнитивных процессов обучающихся» и разделяется на два аспекта. Первый, очевидный, это рекомендации по организации обучения как целого процесса, его ориентация на повышение мотивации, личностной ориентированности, цифровизацию и т.д. Второй аспект «активизации когнитивных процессов» относится к частным методикам обучения. От формирования письменной речи в начальной школе до обучения пожарной безопасности и даже дефектологии (иронично!) в вузе.

Подведём промежуточный итог. В современном образовании отчетливо видятся следующие профессиональные роли: нейропедагог (специалист в области нейропедагогики) и «прикладной нейропсихолог в образовании». Сравним, для наглядности, задачи работы этих нейро-специалистов с «классическим» нейропсихологом, взаимодействующим с людьми в медицине или психолого-педагогической реабилитации (см. Таблица 1).

Таблица 1.
Задачи работы разных нейроспециалистов.

Области компетенции	**Нейропедагог**	**Прикладной нейропсихолог в образовании**	**Клинический нейропсихолог**
субъект(ы) практики	Группа обучаемых	Учащийся с «трудностями»	Человек с заболеваниями ЦНС и/или их последствиями
Способ работы	Оптимизация подачи учебного материала с учетом возрастных, перцептивных, мотивационных особенностей группы	Поиск механизма «трудностей» (фактора), выделение «сильных звеньев», сочетание индивидуальной коррекции и рекомендаций по опоре на сильные звенья в обучении	Построение индивидуального маршрута реабилитации на основе структуры синдрома, прогноз вариантов результата как отдельных этапов, так и всей работы
Социальная роль	Сближение требований общества (в виде образовательных нормативов) и возрастной психологии, физиологии, нейропсихологии обучаемых	Помощь «проблемному» ребенку во «встраивании» (приспособлении) к предлагаемой обществом усредненной социальной нише «ученика такой-то ступени»	Конструирование социальной ниши, в которой пациент будет максимально успешен, с опорой на «сильные звенья» и обходом/щадящей нагрузкой поврежденных факторов
Заказчик/ «акцептор результата» (с кем обсуждаются цели-задачи-средства достижения и полученные итоги работы)	Система образования как социальный институт (обучаемые, педагоги, родители — стороны общения, но «стандарт» итога работы задан требованиями программы)	Триумвират: - педагог, испытывающий трудности в обучении конкретного ученика; - сам этот «проблемный» обучающийся; - семья обучающегося	Семья пациента и, в меньшей степени, он сам (постольку, поскольку способен к саморегуляции и рефлексии на каждом из этапов реабилитации/ коррекции)
Роль в образовательном процессе	Методист, просветитель	Консультант «триумвирата» (см. выше), вспомогательный к учебному процессу специалист, ведущий коррекцию трудностей	«Архитектор фундамента» самой возможности пациента получать образование

Таким образом, «нейропедагогика» как область науки и практики:

а) лежит на стыке образования, психологии и «нейронаук», которые представлены, в первую очередь, лурьевской нейропсихологией (у остальных нет прямого «выхода» на процесс обучения);

б) адресована как учащимся и преподавателям «вообще», так и «проблемным» ученикам разного возраста;

в) выступает в ипостасях - «идеологии» (сближение любого обучения с возможностями и потребностями конкретного возраста, мотивации, состояния ЦНС), «инструмента» (облегчения донесения конкретной информации, заданной программой, до конкретных же групп обучаемых), «дополнительной опоры» (решение проблем «учеников с трудностями обучения»);

г) в зависимости от роли/ипостаси в образовании может реализовываться — педагогом, педагогом-психологом, клиническим психологом или дефектологом (в специальном образовании и центрах реабилитации и коррекции).

Использованные источники:

1. Абабкова М.Ю., Леонтьева В.Л. Нейрообразование в контексте нейронауки: возможности и технологии// Здоровье – основа человеческого потенциала: проблемы и пути их решения. - 2018. - №1. - с. 451-459.
2. Глозман Ж.М. Проблемные дети: почему их становится всё больше? // сб. статей 5 Международной научно-практической конференции «Воспитание и обучение детей младшего возраста». - М.: МГУ, Мозаика-синтез, 2016. - с. 7-11.
3. Глозман Ж.М. О субъектности луриевской нейропсихологии// Вестник МГУ. Серия 14. Психология. - 2012. - №2. - с. 31-36.
4. Зеер Э.Ф. Нейродидактика - инновационный тренд персонализированного образования// Профессиональное образование и рынок труда. - 2021. - №4. - С.30–38.
5. Клемантович И.П., Леванова Е.А., Степанов В.Г. Нейропедагогика: новая отрасль научных знаний// Педагогика и психология образования. - 2016. - №2. - с. 8-17.
6. Коган Б.М., Ляпина А.М. Системная оценка нейропсихологических подходов коррекционной работы с детьми с особенностями развития// Системная психология и социология. - 2022. - № 4(44). - С.48–58.
7. Макарова Л.Н., Перышкова С.А. Теоретические аспекты организации коррекционно-развивающей работы с дошкольниками с ограниченными возможностями здоровья с использованием нейропсихологических технологий// Психолого-педагогический журнал «Гаудеамус». - 2022. - Т.21, №1. - С. 9-16.
8. Местоева Е.А., Мальсагова М.Х. Нейродидактический подход в методологии педагогики// Мир науки, культуры, образования. - 2021. - №4 (89). - с. 151-152.

9. Перегуда С.Н. Нейроэтика в работе нейропсихолога: основы нейропсихологии морали и этики// международный электронный научный журнал «Science Time». - 2025. - №3(134). - с.14-18.
10. Плотникова А.В., Глозман Ж.М. Бригадный подход к диагностике и коррекции трудностей обучения в общеобразовательной начальной школе// Вестник Кемеровского государственного университета. - 2019. - Т.21, №4. - С. 998–1004.
11. Покровская С.В. Кому и зачем нужна нейропсихологическая помощь в детском возрасте?// электронный научно-образовательный вестник «Сознание». - 2018. - Т.20, №1. - с.33-38.
12. Тащёва А.И., Гриднева С.В., Меньшиков П.В., Арпентьева М.Р. Нейродидактические аспекты инклюзивного образования и проблемы психопрофилактики и психокорреции дидактогений// Научный результат. Педагогика и психология образования. - 2022. - Т.8, №2. - С.134-147.
13. Цветков А.В. Образ Я: структура, функции, развитие. - М.: «Спорт и культура-2000», 2012. - 176 с.
14. Цветкова Л.С., Цветков А.В., Перекатнов Д.В. Взаимосвязь стратегии переработки информации и успешности обучения у учащихся средней и старшей школы// Вестник МГУ. Серия 20. Педагогическое образование. - 2013. - №4. - с. 70-76.

УДК 004.056.53

Демидова Д. В.
студент
РГУ нефти и газа (НИУ) имени И. М. Губкина
Комнацкая Е. Д.
студент
РГУ нефти и газа (НИУ) имени И. М. Губкина

ВЫЯВЛЕНИЕ И ПРОТИВОДЕЙСТВИЕ УТЕЧКЕ ТОПОЛОГИИ СЕТИ IPv6 ЧЕРЕЗ БАЗУ ДАННЫХ СОСТОЯНИЯ КАНАЛОВ ПРОТОКОЛА OSPFv3 (MITRE ATT&CK T1590)

Аннотация: *В статье исследуется утечка топологии сети IPv6 через базу данных состояния каналов (LSDB) протокола OSPFv3 — техника разведки MITRE ATT&CK T1590. В среде эмулятора GNS3 развёрнут гетерогенный стенд, объединяющий в единой зоне маршрутизаторы трёх производителей (Cisco, MikroTik, VyOS). Реализован сценарий атаки с узла под управлением Debian с пакетом FRRouting: пассивный перехват пакетов Hello и активное установление смежности с получением полной LSDB. Подтверждено, что в конфигурации по умолчанию OSPFv3 не выполняет аутентификацию, вследствие чего полное описание автономной системы извлекается независимо от вендора оборудования менее чем за минуту. Разработан комплекс мер защиты (пассивизация интерфейсов, аутентификация IPsec AH с общим ключом, применение алгоритмов SHA-2), а уязвимость классифицирована как уязвимость конфигурации по ГОСТ Р 56546-2015.*

Ключевые слова: *сетевая безопасность, MITRE ATT&CK, OSPFv3, IPv6, утечка топологии, LSDB, разведка сети, IPsec AH, пассивный интерфейс.*

Demidova D. V.
student
Gubkin Russian State University of Oil and Gas
Komnatskaya E. D.
student
Gubkin Russian State University of Oil and Gas

DETECTION AND MITIGATION OF IPv6 NETWORK TOPOLOGY LEAKAGE THROUGH THE OSPFv3 LINK-STATE DATABASE (MITRE ATT&CK T1590)

Abstract: *This article examines the leakage of IPv6 network topology through the link-state database (LSDB) of the OSPFv3 protocol — the MITRE ATT&CK T1590 reconnaissance technique. A heterogeneous testbed, deployed in the GNS3 emulator, combines routers from three vendors (Cisco, MikroTik, VyOS) within a single routing area. An attack scenario is implemented from a Debian node running FRRouting: passive capture of Hello packets and active establishment of adjacency to obtain the full LSDB. It is confirmed that, in its default configuration, OSPFv3 performs no authentication, so the complete description of the autonomous system is extracted regardless of the equipment vendor in under one minute. A set of protective measures (passive interfaces, IPsec AH authentication with a shared key, use of SHA-2 algorithms) is developed, and the vulnerability is classified as a configuration vulnerability per GOST R 56546-2015.*

Keywords: *network security, MITRE ATT&CK, OSPFv3, IPv6, topology leakage, LSDB, network reconnaissance, IPsec AH, passive interface.*

Введение

Развитие сетей передачи данных существенно изменили условия проведения разведки сетевой инфраструктуры [13]. Адресное пространство IPv6 для отдельной подсети составляет 264 адресов, что делает методы активного сканирования, традиционные для IPv4 сетей, практически неприменимыми. Полный перебор адресов одной подсети /64 при скорости в миллион проверок в секунду занял бы время, превышающее возраст Вселенной. Указанное обстоятельство вынуждает злоумышленника искать альтернативные источники сведений о топологии атакуемой сети.

Одним из таких источников выступает база данных состояния каналов (Link-State Database, LSDB) протокола динамической маршрутизации OSPFv3 (Open Shortest Path First version 3). Указанный протокол применяется для маршрутизации в сетях IPv6 и хранит в LSDB полное описание топологии автономной системы (Autonomous System, AS): идентификаторы всех маршрутизаторов, объявляемые префиксы, состояние межмаршрутизаторных каналов. Получение доступа к LSDB позволяет восстановить карту сети целиком, минуя необходимость активного сканирования адресного пространства.

Описанный вектор соответствует технике T1590 (Gather Victim Network Information — Сбор информации о сети жертвы) матрицы MITRE ATT&CK [18]. Техника относится к тактике разведки и включает сбор сведений о сетевых диапазонах, топологии и административной организации сети.

Теоретическая основа

1. Нормативно-правовое регулирование

Защита сетевой инфраструктуры в Российской Федерации регулируется комплексом нормативных правовых актов. Основополагающим документом выступает Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской

Федерации» [1], устанавливающий правовые основы обеспечения безопасности объектов критической информационной инфраструктуры (КИИ). Сети передачи данных операторов связи, государственных органов и организаций ряда отраслей экономики относятся к объектам КИИ, что обуславливает применение к ним установленных законом требований.

Требования к техническим мерам защиты значимых объектов КИИ конкретизированы приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 25 декабря 2017 года № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [2]. Приказ устанавливает перечень организационных и технических мер, среди которых присутствуют меры по защите информационной (телекоммуникационной) сети, включающие сегментирование, контроль сетевого взаимодействия и защиту протоколов маршрутизации [3]. Непрерывный мониторинг сетевого трафика, предписываемый приказом для своевременного обнаружения аномалий, непосредственно связан с противодействием рассматриваемой в работе технике разведки.

Классификация и описание уязвимостей, к числу которых относится отсутствие аутентификации в протоколе маршрутизации, регламентируются национальными стандартами ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» [5] и ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей» [4]. Согласно классификации ГОСТ Р 56546-2015 [5], рассматриваемая уязвимость относится к уязвимостям конфигурации, возникающим вследствие недостатков настройки программного обеспечения. Общие требования к системам менеджмента информационной безопасности, в рамках которых реализуется защита протоколов маршрутизации, установлены стандартом ГОСТ Р ИСО/МЭК 27001-2021 [6, 7].

2. Протокол OSPFv3

Протокол OSPFv3 представляет собой протокол внутреннего шлюза (Interior Gateway Protocol, IGP), основанный на технологии состояния каналов (link-state). В отличие от дистанционно-векторных протоколов, передающих соседям таблицу маршрутизации, протоколы состояния каналов распространяют сведения о состоянии собственных каналов, на основании которых каждый маршрутизатор самостоятельно строит полную карту сети и вычисляет кратчайшие пути по алгоритму Дейкстры (Shortest Path First, SPF) [9].

Протокол OSPFv3 является адаптацией протокола OSPFv2 для работы в сетях IPv6 и описан в RFC 5340 [14]. Между версиями существуют принципиальные различия.

Во-первых, OSPFv3 функционирует поверх локальных адресов канала (link-local) IPv6 и не переносит сетевую адресацию в заголовках

протокольных пакетов — адресная информация вынесена в отдельные объявления состояния каналов.

Во-вторых, и это ключевое отличие, OSPFv3 не содержит встроенного механизма аутентификации. Если OSPFv2 поддерживает аутентификацию по паролю и по хэшу MD5 непосредственно в протоколе, то в OSPFv3 функция аутентификации полностью делегирована протоколу защиты межсетевого взаимодействия IPsec (Internet Protocol Security) [16]. Указанное обстоятельство означает, что в конфигурации по умолчанию OSPFv3 не выполняет проверку подлинности соседних маршрутизаторов.

База данных состояния каналов LSDB представляет собой совокупность объявлений состояния каналов (Link-State Advertisement, LSA). В протоколе OSPFv3 определены следующие основные типы LSA, значимые для восстановления топологии [14]. Router-LSA (тип 1) описывает состояние интерфейсов маршрутизатора и содержит его идентификатор (Router ID). Network-LSA (тип 2) формируется выделенным маршрутизатором (Designated Router, DR) и описывает множественный сегмент. Intra-Area-Prefix-LSA (тип 9) переносит префиксы IPv6, связанные с маршрутизатором или сегментом. Link-LSA (тип 8) распространяется в пределах одного канала и содержит локальные адреса канала. Совокупность перечисленных объявлений в LSDB образует полное описание автономной системы.

Синхронизация LSDB между соседними маршрутизаторами выполняется в несколько этапов. Маршрутизаторы обнаруживают друг друга посредством пакетов Hello, рассылаемых на групповой адрес FF02::5. После установления двусторонней связи стороны обмениваются пакетами описания базы данных (Database Description, DBD), содержащими перечень имеющихся объявлений. На основании полученного перечня маршрутизатор запрашивает недостающие объявления пакетами запроса состояния канала (Link-State Request, LSR), получает их в пакетах обновления состояния канала (Link-State Update, LSU) и подтверждает приём пакетами подтверждения (Link-State Acknowledgment, LSAck). По завершении обмена базы данных соседей становятся идентичными, а смежность переходит в состояние полной синхронизации (Full) [14].

Существенным для оценки риска является то обстоятельство, что в конфигурации по умолчанию любой узел, способный сформировать корректные пакеты Hello и получить статус соседа, проходит полную процедуру синхронизации и получает копию LSDB целиком. Поскольку аутентификация в OSPFv3 по умолчанию отсутствует, установление смежности не требует предъявления каких-либо учётных данных. Узел злоумышленника, подключённый к сегменту с работающим OSPFv3, получает полное описание топологии автономной системы.

Важной характеристикой протокола OSPFv3 является механизм выбора выделенного маршрутизатора и резервного выделенного маршрутизатора (Backup Designated Router, BDR) в множественных сегментах. В сегментах с множественным доступом, где потенциально может присутствовать более

двух маршрутизаторов, для сокращения числа смежностей выбирается выделенный маршрутизатор, с которым устанавливают смежность все прочие маршрутизаторы сегмента. Выбор основан на значении приоритета интерфейса и идентификатора маршрутизатора. Узел злоумышленника, установив смежность с выделенным маршрутизатором, получает доступ к LSDB наравне с легитимными участниками сегмента. Указанный механизм не привносит дополнительной защиты, поскольку процедура выбора выделенного маршрутизатора также не предусматривает аутентификации.

Идентификатор маршрутизатора (Router ID) в OSPFv3 представляет собой 32-битное значение, записываемое в формате, аналогичном адресу IPv4, однако не связанное с фактической адресацией IPv6 интерфейсов. Идентификатор однозначно определяет маршрутизатор в пределах автономной системы и фигурирует в объявлениях Router-LSA. Получение злоумышленником перечня идентификаторов всех маршрутизаторов автономной системы из LSDB предоставляет основу для построения логической карты сети, независимой от физической адресации.

3. Утечка топологии как угроза безопасности

В сетях IPv4 разведка сетевой инфраструктуры традиционно опирается на активное сканирование: последовательную проверку доступности адресов в известных диапазонах (ping sweep) и сканирование портов (port scan) [8]. Размер типовой подсети IPv4 (например, /24, содержащая 256 адресов) допускает полный перебор за доли секунды. В сетях IPv6 указанный подход неприменим вследствие размера адресного пространства подсети, составляющего 264 адресов.

Невозможность активного сканирования смещает интерес злоумышленника к пассивным источникам топологической информации. Протоколы динамической маршрутизации представляют собой такой источник: их штатное функционирование предполагает распространение полного описания топологии между всеми участниками маршрутизации. Если злоумышленник получает возможность стать участником процесса маршрутизации, он получает и полное описание сети. В этом состоит парадокс безопасности OSPFv3 в сетях IPv6: большое адресное пространство, затрудняющее сканирование, не защищает топологию, поскольку последняя свободно распространяется самим протоколом маршрутизации.

Утечка содержимого LSDB предоставляет злоумышленнику следующие сведения: идентификаторы всех маршрутизаторов автономной системы; полный перечень объявляемых префиксов IPv6, включая адреса интерфейсов обратной связи (loopback) и транзитных каналов; структуру связей между маршрутизаторами, позволяющую построить граф топологии; сведения о выделенных маршрутизаторах сегментов. Указанные сведения соответствуют составу информации, собираемой в рамках техники T1590 матрицы MITRE ATT&CK [18], и образуют основу для планирования

последующих этапов атаки — выбора целей, определения критических узлов, подготовки атак на доступность или перехват трафика.

Полученная топологическая информация может быть использована на последующих этапах развития атаки. Знание структуры связей позволяет идентифицировать критические узлы, выход из строя которых приводит к фрагментации сети, что создаёт предпосылки для целенаправленных атак на доступность. Сведения о префиксах оконечных сетей определяют направления дальнейшей разведки и потенциальные цели. Возможность установления смежности, продемонстрированная в работе, создаёт также предпосылки для активных атак на маршрутизацию — внедрения ложных объявлений с целью перенаправления трафика, что выходит за рамки рассматриваемой техники разведки, однако становится возможным вследствие той же первопричины — отсутствия аутентификации.

В терминах матрицы MITRE ATT&CK [18] рассматриваемая техника относится к тактике разведки и предшествует тактикам получения первоначального доступа и закрепления. Особенность техники T1590 состоит в том, что значительная часть сбора информации может выполняться без непосредственного взаимодействия с целевыми системами, что затрудняет обнаружение разведывательной активности. Применительно к OSPFv3 пассивный перехват протокольных пакетов не оставляет следов в журналах маршрутизаторов, а установление смежности, хотя и регистрируется, может быть замаскировано под легитимное подключение сетевого оборудования.

4. Методы защиты

Защита LSDB протокола OSPFv3 от несанкционированного получения основывается на предотвращении установления смежности с недоверенными узлами и на проверке подлинности протокольных пакетов. В работе рассматриваются три метода защиты, различающиеся механизмом действия и применимостью в условиях разнородного оборудования [11].

Первый метод — назначение интерфейсов пассивными (passive interface). Пассивный интерфейс анонсирует связанный с ним префикс в LSDB, однако не отправляет и не принимает пакеты Hello, вследствие чего не устанавливает смежности. Метод применяется к интерфейсам, направленным в сторону сегментов, где наличие соседних маршрутизаторов не предполагается, — в первую очередь к пользовательским сегментам и сегментам подключения оконечных устройств. Назначение интерфейса пассивным предотвращает установление смежности злоумышленником, подключённым к данному сегменту, и тем самым исключает получение им LSDB. Метод поддерживается всеми основными производителями сетевого оборудования и не требует согласования параметров между устройствами, что делает его универсальным средством защиты периметра маршрутизации. Ограничением метода является неприменимость к транзитным каналам между маршрутизаторами, где установление смежности необходимо для работы протокола.

Второй метод — аутентификация протокольных пакетов посредством заголовка аутентификации IPsec (Authentication Header, AH) с использованием общего ключа. Протокол IPsec AH, описанный в RFC 4302 [15], обеспечивает проверку подлинности и целостности пакетов без их шифрования. Применение AH, а не протокола инкапсуляции полезной нагрузки (Encapsulating Security Payload, ESP), обусловлено использованием в OSPFv3 групповой адресации: пакеты протокола направляются на групповые адреса, для которых шифрование с индивидуальными ключами получателей неприменимо, тогда как аутентификация без шифрования с общим ключом совместима с групповой рассылкой. Заголовок AH содержит индекс параметров безопасности (Security Parameter Index, SPI), идентифицирующий контекст безопасности, порядковый номер для защиты от повторного воспроизведения и значение проверки целостности (Integrity Check Value, ICV). Маршрутизатор, не обладающий корректным ключом, не может сформировать действительное значение ICV, вследствие чего его пакеты отвергаются, а смежность не устанавливается.

Третий метод связан с выбором криптографического алгоритма вычисления хэша для значения ICV. Алгоритм SHA-1 формирует значение длиной 160 бит и рассматривается как минимально приемлемый [16]. Алгоритмы семейства SHA-2, в частности HMAC-SHA-256, обеспечивают повышенную криптографическую стойкость и рекомендуются к применению. Исторически в реализациях OSPFv3 применялся также алгоритм MD5, признанный в настоящее время криптографически слабым [10, 12].

Существенным для практического применения является различие в поддержке указанных методов оборудованием различных производителей. Аутентификация OSPFv3 посредством IPsec AH с интеграцией в команды настройки протокола поддерживается не всеми маргрутизаторами. Данное обстоятельство, подробно рассматриваемое в практической части работы, определяет необходимость комбинированного применения методов защиты в реальных гетерогенных сетях.

Описание экспериментального стенда

Экспериментальный стенд построен в среде сетевого эмулятора GNS3 с применением аппаратной виртуализации. Выбор гетерогенной топологии, объединяющей оборудование трёх производителей в единой зоне маршрутизации, обусловлен стремлением приблизить условия эксперимента к реальным сетям операторов связи и крупных организаций, где совместно эксплуатируется оборудование различных вендоров. Такая постановка позволяет одновременно оценить поведение протокола OSPFv3 при межвендорном взаимодействии и проверить применимость мер защиты в разнородной среде.

Все три маршрутизатора включены в единую зону OSPFv3 — магистральную зону с идентификатором 0.0.0.0. Размещение всех маршрутизаторов в одной зоне обеспечивает наличие в LSDB каждого узла

полного описания топологии автономной системы, что соответствует цели исследования: продемонстрировать, что злоумышленник, установивший смежность с одним маршрутизатором, получает сведения обо всей сети, включая маршрутизаторы, физически расположенные в других сегментах.

Узел злоумышленника реализован на базе операционной системы Debian с установленным пакетом маршрутизации FRRouting (FRR), обеспечивающим поддержку OSPFv3. Узел подключается поочерёдно к сегменту каждого из трёх маршрутизаторов, что позволяет реализовать три независимых сценария атаки и провести сравнительный анализ поведения оборудования различных производителей.

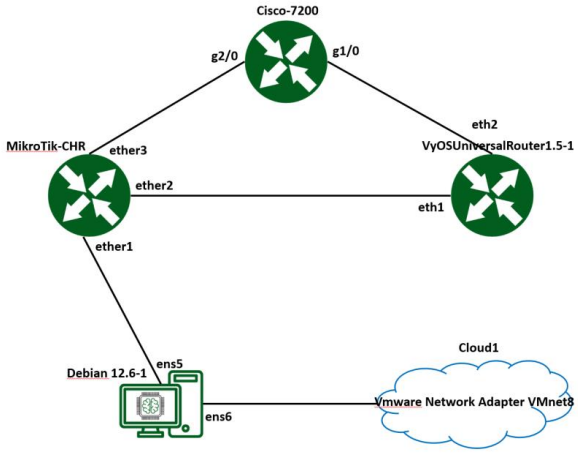

Рисунок 1. Топология для эксперимента

Топология стенда организована таким образом, что три маршрутизатора образуют замкнутый контур: каждый маршрутизатор соединён транзитными каналами с двумя другими. Такая организация обеспечивает наличие альтернативных путей и формирование полноценной LSDB, отражающей все связи автономной системы. Каждый маршрутизатор дополнительно располагает интерфейсом обратной связи (loopback) с уникальным префиксом /128, имитирующим клиентские сети, анонсируемые в маршрутизацию. Наличие таких префиксов в LSDB позволяет продемонстрировать утечку сведений не только о транзитной инфраструктуре, но и об оконечных сетях.

Таблица 1.

Состав оборудования и программного обеспечения стенда

Узел	Платформа	Версия ПО	Идентификатор
R1	Cisco 7206VXR	Cisco IOS 15.2(4)M8	1.1.1.1
R2	MikroTik CHR	RouterOS 7.21.4	2.2.2.2
R3	VyOS Universal Router	VyOS 1.5-stream-2025-Q2	3.3.3.3
Злоумышленник	Debian (FRRouting)	Debian 12, FRR 8.4.4	9.9.9.9

Адресный план стенда построен на основе документального префикса 2001:db8::/32, зарезервированного RFC 3849 [17] для применения в документации и примерах. Распределение адресного пространства по сегментам сети приведено в таблице 2.

Таблица 2.
Адресный план экспериментального стенда

Префикс / адрес	Назначение
2001:db8:12::/64	Транзитный канал R1 (Cisco) — R2 (MikroTik)
2001:db8:13::/64	Транзитный канал R1 (Cisco) — R3 (VyOS)
2001:db8:23::/64	Транзитный канал R2 (MikroTik) — R3 (VyOS)
2001:db8:1::/64	Сегмент подключения злоумышленника к R1 (Cisco)
2001:db8:2::/64	Сегмент подключения злоумышленника к R2 (MikroTik)
2001:db8:3::/64	Сегмент подключения злоумышленника к R3 (VyOS)
2001:db8:100::1/128	Интерфейс обратной связи (loopback) R1 (Cisco)
2001:db8:200::1/128	Интерфейс обратной связи (loopback) R2 (MikroTik)
2001:db8:300::1/128	Интерфейс обратной связи (loopback) R3 (VyOS)

Реализация атаки

Реализация атаки выполнена в три этапа, соответствующих поочерёдному подключению узла злоумышленника к сегменту каждого из маршрутизаторов. Методология каждого этапа включает две фазы: пассивный перехват протокольных пакетов с целью первичного обнаружения маршрутизатора и активное установление смежности с целью получения полной LSDB.

В фазе пассивного перехвата на узле злоумышленника выполняется захват трафика на групповые адреса OSPFv3 средствами анализатора пакетов. Перехват пакетов Hello позволяет установить факт наличия маршрутизатора в сегменте, его идентификатор и идентификатор зоны, не выдавая присутствия злоумышленника. На данном этапе сведения о топологии автономной системы ограничены, поскольку пакеты Hello не переносят содержимого LSDB.

В фазе активного установления смежности на узле злоумышленника настраивается процесс OSPFv3 с произвольным идентификатором маршрутизатора, после чего узел проходит штатную процедуру установления смежности с атакуемым маршрутизатором. По достижении состояния полной синхронизации (Full) узел получает полную копию LSDB, содержащую описание всей автономной системы.

Инструментальное обеспечение атаки включает анализатор пакетов для перехвата и разбора протокольного трафика, средства языка сценариев для автоматизированного извлечения сведений из перехваченных пакетов, а также пакет маршрутизации FRRouting для установления легитимной с точки зрения протокола смежности. Применение полнофункционального пакета маршрутизации, а не специализированного инструмента подделки

пакетов, отражает реалистичный сценарий: злоумышленнику достаточно штатного программного обеспечения с открытым исходным кодом, поскольку отсутствие аутентификации не требует обхода защитных механизмов. Указанное обстоятельство понижает порог реализуемости атаки и повышает её практическую значимость как угрозы.

1. Сценарий 1 – атака на сегмент Cisco

Узел злоумышленника подключён к сегменту маршрутизатора под управлением Cisco IOS. Пассивный перехват трафика подтвердил наличие в сегменте пакетов Hello, отправляемых маршрутизатором с идентификатором 1.1.1.1 в зоне 0.0.0.0.

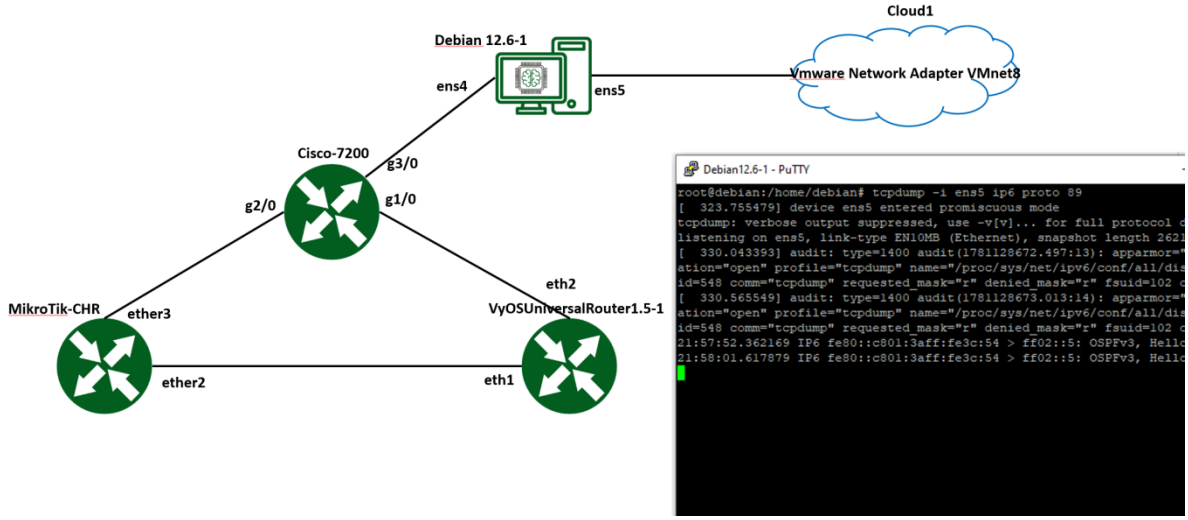

Рисунок 2. Прослушивание Hello-пакетов от маршрутизатора

После проведения анализа Hello-пакетов и настройки процесса OSPFv3 на узле злоумышленника смежность с маршрутизатором перешла в состояние полной синхронизации.

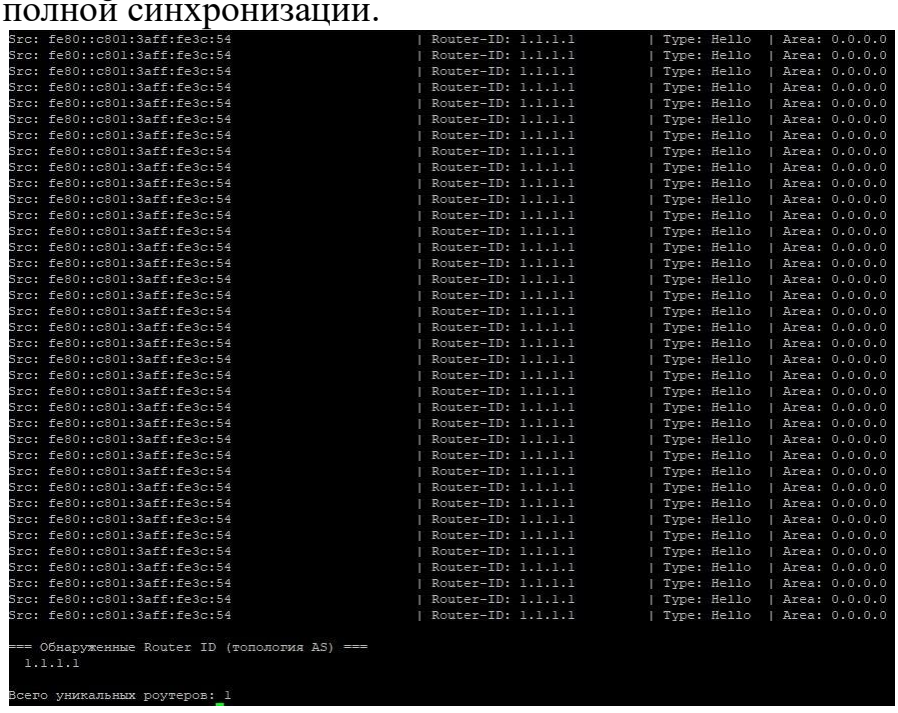

Рисунок 3. Анализ Hello-пакетов с помощью python-скрипта

Анализ полученной LSDB показал наличие в ней объявлений Router-LSA от всех трёх маршрутизаторов автономной системы с идентификаторами 1.1.1.1, 2.2.2.2 и 3.3.3.3, а также объявления от самого узла злоумышленника, ставшего полноправным участником маршрутизации. В составе объявлений Intra-Area-Prefix-LSA обнаружены все префиксы сети, включая адреса интерфейсов обратной связи маршрутизаторов и транзитных каналов. Таким образом, подключение к сегменту единственного маршрутизатора обеспечило получение полного описания топологии автономной системы.

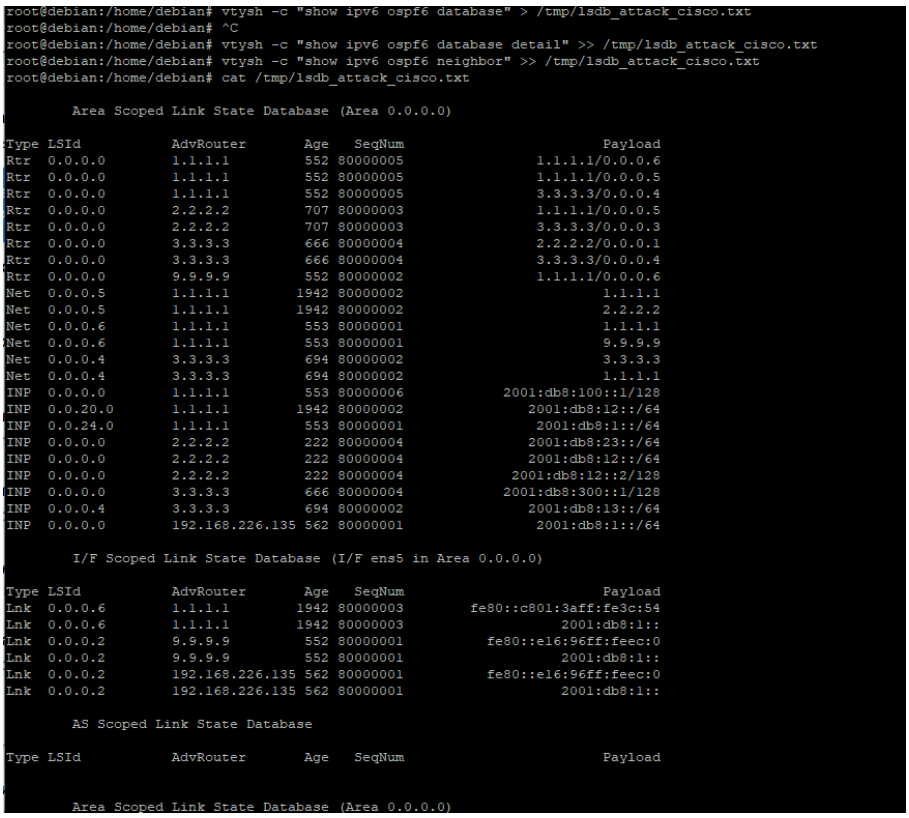

Рисунок 4. Доступ к LSDB на узле злоумышленника

2. Сценарии 2 и 3 — атака на сегменты MikroTik и VyOS

Сценарии атаки на сегменты маршрутизаторов под управлением RouterOS и VyOS реализованы по идентичной методологии. В обоих случаях узел злоумышленника установил смежность в состоянии полной синхронизации и получил LSDB, содержащую полное описание автономной системы, совпадающее с результатом первого сценария. Совпадение результатов подтверждает, что объём утекающей информации не зависит от того, к сегменту какого производителя подключён злоумышленник, поскольку LSDB в пределах одной зоны идентична на всех маршрутизаторах.

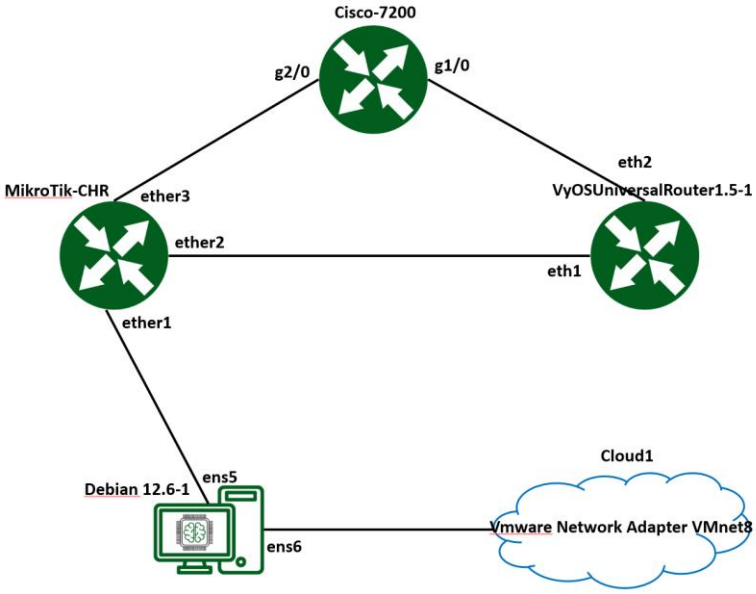

Рисунок 5. Перестроенная топология для атаки на MikroTik

```
debian# show ipv6 ospf6 database

       Area Scoped Link State Database (Area 0.0.0.0)

Type LSId            AdvRouter       Age   SeqNum                  Payload
Rtr  0.0.0.0         1.1.1.1         435 80000005            1.1.1.1/0.0.0.5
Rtr  0.0.0.0         1.1.1.1         435 80000005            3.3.3.3/0.0.0.4
Rtr  0.0.0.0         2.2.2.2         223 80000005            1.1.1.1/0.0.0.5
Rtr  0.0.0.0         2.2.2.2         223 80000005            3.3.3.3/0.0.0.3
Rtr  0.0.0.0         2.2.2.2         223 80000005            9.9.9.9/0.0.0.2
Rtr  0.0.0.0         3.3.3.3         408 80000003            2.2.2.2/0.0.0.2
Rtr  0.0.0.0         3.3.3.3         408 80000003            3.3.3.3/0.0.0.4
Rtr  0.0.0.0         9.9.9.9         223 80000004            9.9.9.9/0.0.0.2
Net  0.0.0.5         1.1.1.1         852 80000003                   1.1.1.1
Net  0.0.0.5         1.1.1.1         852 80000003                   2.2.2.2
Net  0.0.0.4         3.3.3.3         436 80000001                   3.3.3.3
Net  0.0.0.4         3.3.3.3         436 80000001                   1.1.1.1
Net  0.0.0.2         9.9.9.9         223 80000001                   9.9.9.9
Net  0.0.0.2         9.9.9.9         223 80000001                   2.2.2.2
INP  0.0.0.0         1.1.1.1         435 80000006       2001:db8:100::1/128
INP  0.0.0.0         1.1.1.1         435 80000006          2001:db8:1::/64
INP  0.0.20.0        1.1.1.1         852 80000003         2001:db8:12::/64
INP  0.0.0.0         2.2.2.2         228 80000005         2001:db8:12::/64
INP  0.0.0.0         2.2.2.2         228 80000005       2001:db8:12::2/128
INP  0.0.0.0         2.2.2.2         228 80000005         2001:db8:23::/64
INP  0.0.0.0         2.2.2.2         228 80000005          2001:db8:2::/64
INP  0.0.0.0         3.3.3.3         408 80000003       2001:db8:300::1/128
INP  0.0.0.4         3.3.3.3         436 80000001         2001:db8:13::/64
INP  0.0.0.2         9.9.9.9         223 80000001          2001:db8:1::/64
INP  0.0.0.2         9.9.9.9         223 80000001          2001:db8:2::/64

       I/F Scoped Link State Database (I/F ens5 in Area 0.0.0.0)

Type LSId            AdvRouter       Age   SeqNum                  Payload
Lnk  0.0.0.3         2.2.2.2         228 80000001       fe80::e3b:79ff:fece:0
Lnk  0.0.0.3         2.2.2.2         228 80000001                2001:db8:2::
Lnk  0.0.0.2         9.9.9.9         263 80000005       fe80::e16:96ff:feec:0
Lnk  0.0.0.2         9.9.9.9         263 80000005                2001:db8:1::

       AS Scoped Link State Database

Type LSId            AdvRouter       Age   SeqNum                  Payload
```

Рисунок 6. Доступ к LSDB на узле злоумышленника (MikroTik)

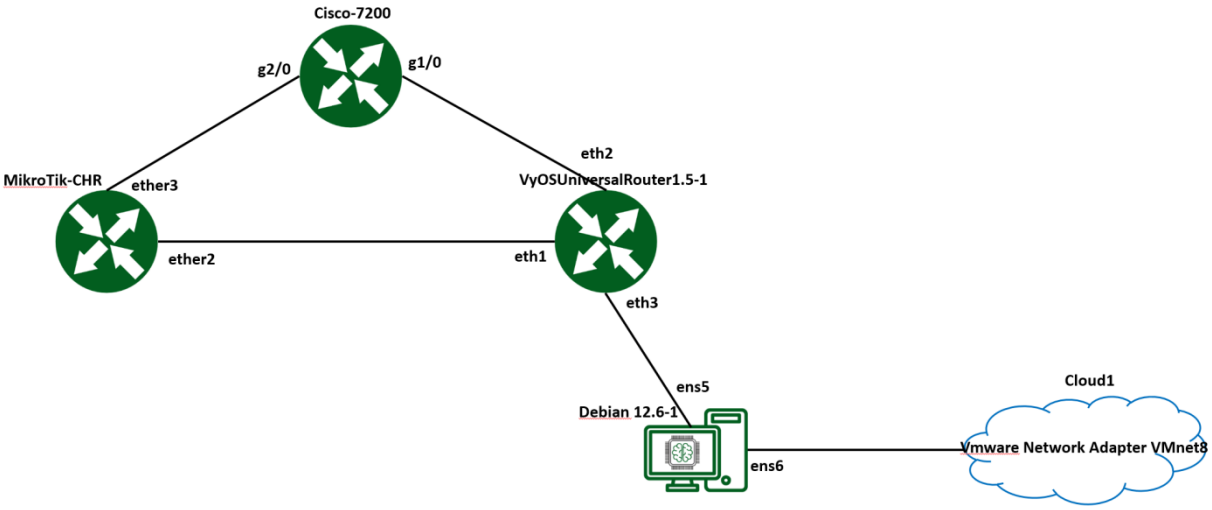

Рисунок 7. Перестроенная топология для атаки на VyOs

```
Neighbor ID     Pri    DeadTime    State/IfState         Duration I/F[State]
3.3.3.3           1    00:00:32     Full/BDR             00:00:37 ens5[DR]
debian# show ipv6 ospf6 database

        Area Scoped Link State Database (Area 0.0.0.0)

Type LSId            AdvRouter       Age   SeqNum                  Payload
Rtr  0.0.0.0         1.1.1.1        1314 80000005             1.1.1.1/0.0.0.5
Rtr  0.0.0.0         1.1.1.1        1314 80000005             3.3.3.3/0.0.0.4
Rtr  0.0.0.0         2.2.2.2         646 80000006             1.1.1.1/0.0.0.5
Rtr  0.0.0.0         2.2.2.2         646 80000006             3.3.3.3/0.0.0.3
Rtr  0.0.0.0         3.3.3.3          79 80000004             2.2.2.2/0.0.0.2
Rtr  0.0.0.0         3.3.3.3          79 80000004             3.3.3.3/0.0.0.4
Rtr  0.0.0.0         3.3.3.3          79 80000004             9.9.9.9/0.0.0.2
Rtr  0.0.0.0         9.9.9.9          78 80000006             9.9.9.9/0.0.0.2
Net  0.0.0.5         1.1.1.1        1731 80000003                    1.1.1.1
Net  0.0.0.5         1.1.1.1        1731 80000003                    2.2.2.2
Net  0.0.0.4         3.3.3.3        1314 80000001                    3.3.3.3
Net  0.0.0.4         3.3.3.3        1314 80000001                    1.1.1.1
Net  0.0.0.2         9.9.9.9          78 80000002                    9.9.9.9
Net  0.0.0.2         9.9.9.9          78 80000002                    3.3.3.3
INP  0.0.0.0         1.1.1.1        1314 80000006          2001:db8:100::1/128
INP  0.0.0.0         1.1.1.1        1314 80000006             2001:db8:1::/64
INP  0.0.20.0        1.1.1.1        1731 80000003            2001:db8:12::/64
INP  0.0.0.0         2.2.2.2         646 80000006            2001:db8:12::/64
INP  0.0.0.0         2.2.2.2         646 80000006          2001:db8:12::2/128
INP  0.0.0.0         2.2.2.2         646 80000006            2001:db8:23::/64
INP  0.0.0.0         3.3.3.3          79 80000005          2001:db8:300::1/128
INP  0.0.0.4         3.3.3.3        1314 80000001            2001:db8:13::/64
INP  0.0.0.2         9.9.9.9          78 80000002             2001:db8:3::/64

        I/F Scoped Link State Database (I/F ens5 in Area 0.0.0.0)

Type LSId            AdvRouter       Age   SeqNum                  Payload
Lnk  0.0.0.5         3.3.3.3          89 80000001       fe80::ea9:8cff:fe60:3
Lnk  0.0.0.5         3.3.3.3          89 80000001                2001:db8:3::
Lnk  0.0.0.2         9.9.9.9         366 80000001       fe80::e16:96ff:feec:0
Lnk  0.0.0.2         9.9.9.9         366 80000001                2001:db8:3::

        AS Scoped Link State Database

Type LSId            AdvRouter       Age   SeqNum                  Payload
```

Рисунок 8. Доступ к LSDB на узле злоумышленника (VyOs)

3. Сравнительный анализ результатов

Сводные результаты трёх сценариев атаки приведены в таблице 3. Во всех трёх случаях смежность установлена без предъявления учётных данных, а полная LSDB получена за время, не превышающее одной минуты.

Таблица 3.
Сводные результаты сценариев атаки

Сценарий	Состояние смежности	LSDB получена	Аутентификация
Cisco 7206VXR	Full / DR	Да (полная)	Отсутствует
MikroTik CHR	Full / DR	Да (полная)	Отсутствует
VyOS 1.5	Full / DR	Да (полная)	Отсутствует

Результаты эксперимента подтверждают, что протокол OSPFv3 в конфигурации по умолчанию не обеспечивает защиту LSDB от несанкционированного получения независимо от производителя оборудования. Уязвимость носит протокольный, а не реализационный характер: отсутствие встроенной аутентификации в OSPFv3 является свойством самого протокола, вследствие чего оборудование всех трёх производителей оказалось одинаково уязвимым. Полученный результат опровергает возможное предположение о наличии у отдельных производителей встроенных механизмов защиты, активных по умолчанию.

Сопоставление содержимого LSDB, полученной в трёх сценариях, показало полное совпадение перечня объявлений во всех случаях. Данное наблюдение согласуется с принципом работы протоколов состояния каналов: в пределах одной зоны база данных синхронизируется и поддерживается идентичной на всех маршрутизаторах. Следовательно, точка подключения злоумышленника не влияет на объём получаемой информации — подключение к любому сегменту любого маршрутизатора зоны обеспечивает получение полного описания автономной системы. Данное обстоятельство усугубляет рассматриваемую угрозу, поскольку для компрометации топологии всей сети достаточно доступа к единственному её сегменту.

С точки зрения классификации уязвимостей по ГОСТ Р 56546-2015 [5] выявленная уязвимость относится к уязвимостям конфигурации, проявляющимся на уровне сетевого программного обеспечения. Местом возникновения уязвимости является подсистема маршрутизации, областью происхождения — недостатки настройки, связанные с эксплуатацией протокола в конфигурации по умолчанию без активации механизмов аутентификации. Указанная классификация определяет направление устранения уязвимости — изменение конфигурации с активацией мер защиты, рассматриваемых далее.

Разработка и проверка мер защиты

Разработка мер защиты выполнена с учётом ключевого ограничения реальных сетей: разнородности и возможной устарелости оборудования. В сетях, эксплуатируемых длительное время, совместно функционирует оборудование различных производителей и поколений, причём поддержка отдельных механизмов защиты может отсутствовать на устаревших платформах или различаться по способу настройки. Предлагаемый подход

основан на комбинировании методов защиты таким образом, чтобы обеспечить защищённость сети при минимальных требованиях к возможностям оборудования.

Анализ поддержки методов аутентификации OSPFv3 оборудованием стенда выявил существенные различия между производителями. Интеграция аутентификации IPsec AH непосредственно в команды настройки протокола OSPFv3 присутствует в исследованной версии Cisco IOS, где параметры аутентификации задаются на уровне интерфейса командой настройки OSPFv3. В исследованных версиях RouterOS [19] и VyOS [20] прямая интеграция аутентификации IPsec AH в команды OSPFv3 отсутствует: настройка IPsec для защиты протокольного трафика требует отдельной конфигурации подсистемы IPsec, не связанной непосредственно с настройкой протокола маршрутизации. Указанное различие имеет принципиальное значение для построения защиты в гетерогенной сети и обобщено в таблице 4.

Дополнительным ограничением выступает требование согласованности параметров аутентификации между всеми маршрутизаторами одного сегмента. Аутентификация OSPFv3 является симметричной: все маршрутизаторы, образующие смежности в пределах одного канала, должны использовать одинаковый ключ и алгоритм хэширования. В гетерогенной сети это требование осложняется как различиями в синтаксисе настройки, так и возможными расхождениями в поддерживаемых алгоритмах и форматах представления ключа.

Таблица 4.
Поддержка методов защиты OSPFv3 оборудованием стенда

Метод защиты	Cisco IOS	RouterOS	VyOS
Пассивный интерфейс	Поддерживается	Поддерживается	Поддерживается
Аутентификация IPsec AH, встроенная в OSPFv3	Поддерживается	Не поддерживается напрямую	Не поддерживается напрямую
Защита через отдельную подсистему IPsec	Поддерживается	Требует ручной настройки	Требует ручной настройки

1. Двухуровневая стратегия защиты

С учётом выявленных ограничений предложена двухуровневая стратегия защиты, обеспечивающая защищённость сети независимо от полноты поддержки аутентификации отдельными устройствами.

Первый уровень — защита периметра маршрутизации посредством назначения пассивными всех интерфейсов, направленных в сторону недоверенных сегментов. Данный метод поддерживается всеми тремя производителями единообразно по смыслу действия и не требует согласования параметров между устройствами. Назначение пассивным интерфейса, обращённого к пользовательскому сегменту, предотвращает установление смежности злоумышленником, подключённым к данному

сегменту. Поскольку именно через такие сегменты наиболее вероятно подключение злоумышленника, первый уровень защиты обеспечивает основной эффект и применим даже к оборудованию, не поддерживающему аутентификацию OSPFv3.

Второй уровень — аутентификация протокольных пакетов на транзитных каналах между маршрутизаторами для оборудования, поддерживающего данную функцию. Аутентификация защищает от подключения злоумышленника непосредственно к транзитному каналу, а также от подмены маршрутизатора. На оборудовании с прямой поддержкой аутентификации OSPFv3 второй уровень реализуется средствами протокола, на прочем оборудовании — средствами подсистемы IPsec либо, при невозможности, компенсируется усилением физической и канальной защиты транзитных каналов.

Применительно к стенду стратегия реализована следующим образом. На маршрутизаторе под управлением Cisco IOS, обладающем прямой поддержкой аутентификации, на интерфейсе, обращённом к сегменту злоумышленника, настроена аутентификация IPsec AH с алгоритмом SHA-1 и индивидуальным индексом параметров безопасности. На маршрутизаторах под управлением RouterOS и VyOS, для которых прямая настройка аутентификации OSPFv3 недоступна, интерфейсы, обращённые к сегментам злоумышленника, назначены пассивными. Внутренние транзитные каналы между маршрутизаторами в рамках эксперимента оставлены без аутентификации, что отражает типичную ситуацию частичной защищённости реальной сети и позволяет оценить достаточность защиты периметра.

2. Проверка эффективности мер защиты

Проверка эффективности предложенных мер выполнена повторением сценариев атаки после применения защиты. На маршрутизаторе под управлением Cisco IOS применены меры защиты двух уровней применительно к интерфейсу, обращённому к сегменту злоумышленника. Настройка аутентификации посредством заголовка аутентификации IPsec с алгоритмом SHA-1 [15, 16] на данном интерфейсе исключила возможность установления смежности с узлом, не располагающим корректным ключом: протокольные пакеты злоумышленника были отвергнуты маршрутизатором как не прошедшие проверку целостности. Дополнительно интерфейс назначен пассивным, что прекратило отправку пакетов Hello в сегмент злоумышленника и исключило обнаружение маршрутизатора при пассивном перехвате. Совокупное применение обеих мер на одном интерфейсе обеспечило защиту как от пассивной разведки, так и от активного установления смежности.

```
Cisco-7200(config)#int gi3/0
Cisco-7200(config-if)#$spi 258 sha1 6A8C4A34E3B26A56BCF2EEC590531B17F7F75097
Cisco-7200(config-if)#end
```

Рисунок 9. Настройка безопасности на Cisco

```
Cisco-7200#show ipv6 ospf neighbor

            OSPFv3 Router with ID (1.1.1.1) (Process ID 1)

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
2.2.2.2         128   FULL/BDR        00:00:31    1               GigabitEtherne
t2/0
3.3.3.3           1   FULL/DR         00:00:39    4               GigabitEtherne
t1/0
Cisco-7200#
```

Рисунок 10. Наличие легитимного соседства после настройки безопасности

```
debian# show ipv6 ospf6 neighbor
Neighbor ID     Pri     DeadTime    State/IfState         Duration I/F[State]
debian#
```

Рисунок 11. Невозможность установить соседство с Cisco после настройки безопасности

На маршрутизаторах под управлением RouterOS и VyOS назначение интерфейса пассивным привело к прекращению отправки пакетов Hello в сегмент злоумышленника, вследствие чего узел злоумышленника не обнаружил маршрутизатор при пассивном перехвате и не смог установить смежность.

```
[admin@MikroTik] /routing/ospf/interface-template> set [find interfaces=ether1]
passive
```

Рисунок 12. Настройка пассивного внешнего интерфейса на MikroTik

```
vyos@vyos# set protocols ospfv3 interface eth3 passive

[edit]
vyos@vyos#
[edit]
vyos@vyos# commit
[edit]
vyos@vyos# save
[edit]
```

Рисунок 13. Настройка пассивного интерфейса на VyOs

```
debian# show ipv6 ospf6 neighbor
Neighbor ID     Pri     DeadTime    State/IfState         Duration I/F[State]
debian#
```

Рисунок 14. Невозможность установить соседство с оставшимися роутерами после настройки безопасности

Заключение

В работе исследована возможность утечки информации о сетевой архитектуре через базу данных состояния каналов протокола OSPFv3 в условиях большого адресного пространства IPv6. Подтверждено, что техника T1590 матрицы MITRE ATT&CK [18] применительно к OSPFv3 реализуема: узел злоумышленника, подключённый к сегменту сети с работающим протоколом OSPFv3 в конфигурации по умолчанию, устанавливает

смежность без предъявления учётных данных и получает полное описание топологии автономной системы за время, не превышающее одной минуты.

Эксперимент, проведённый на оборудовании трёх производителей, показал, что уязвимость носит протокольный характер и не зависит от производителя оборудования: отсутствие встроенной аутентификации является свойством самого протокола OSPFv3. Установлено, что в условиях большого адресного пространства IPv6 значимость данного вектора возрастает, поскольку невозможность активного сканирования смещает интерес злоумышленника к пассивным источникам топологической информации, каковым выступает LSDB.

Выявлено существенное различие в поддержке методов аутентификации OSPFv3 оборудованием различных производителей: прямая интеграция аутентификации IPsec AH в команды настройки протокола присутствует не во всех реализациях. Данное обстоятельство определяет необходимость комбинированного применения методов защиты в реальных гетерогенных сетях. Предложена двухуровневая стратегия защиты, сочетающая защиту периметра маршрутизации посредством пассивных интерфейсов, применимую к оборудованию любого производителя, и аутентификацию каналов. Эффективность стратегии подтверждена экспериментально: после применения защиты получение LSDB узлом злоумышленника оказалось невозможным.

Практическая значимость работы состоит в применимости предложенной стратегии к реальным сетям с разнородным и устаревшим оборудованием, где полная унификация механизмов аутентификации недостижима. Защита периметра маршрутизации обеспечивает основной эффект при минимальных требованиях к возможностям оборудования, что соответствует требованиям нормативных документов по защите критической информационной инфраструктуры в части контроля сетевого взаимодействия. Направлением дальнейших исследований является изучение защиты транзитных каналов посредством инкапсуляции протокольного трафика OSPFv3 в шифрованные туннели IPsec для оборудования, не поддерживающего встроенную аутентификацию протокола.

Использованные источники

1. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 № 187-ФЗ. — Текст: электронный // Консультант Плюс: справочно-правовая система. — URL: http://www.consultant.ru (дата обращения: 12.06.2026).
2. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: приказ ФСТЭК России от 25.12.2017 № 239. — Текст: электронный // ФСТЭК России: официальный сайт. — URL: https://fstec.ru (дата обращения: 12.06.2026).
3. Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской

Федерации и обеспечению их функционирования: приказ ФСТЭК России от 21.12.2017 № 235. — Текст: электронный // ФСТЭК России: официальный сайт. — URL: https://fstec.ru (дата обращения: 12.06.2026).
4. ГОСТ Р 56545-2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. — Введ. 2016-04-01. — Москва: Стандартинформ, 2015. — 12 с.
5. ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. — Введ. 2016-04-01. — Москва: Стандартинформ, 2015. — 16 с.
6. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. — Введ. 2022-01-01. — Москва: Российский институт стандартизации, 2021. — 35 с.
7. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. — Введ. 2009-10-01. — Москва: Стандартинформ, 2009. — 16 с.
8. Бирюков, А. А. Информационная безопасность: защита и нападение / А. А. Бирюков. — 2-е изд., перераб. и доп. — Москва: ДМК Пресс, 2017. — 434 с. — ISBN 978-5-97060-435-9. — Текст: непосредственный.
9. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. — 5-е изд. — Санкт-Петербург: Питер, 2020. — 1008 с. — ISBN 978-5-4461-1426-9. — Текст: непосредственный.
10. Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа / Л. К. Бабенко, Е. А. Ищукова. — Москва: Гелиос АРВ, 2006. — 376 с. — Текст: непосредственный.
11. Запечников, С. В. Информационная безопасность открытых систем: учебник: в 2 томах. Том 2. Средства защиты в сетях / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. — Москва: Горячая линия — Телеком, 2018. — 558 с. — Текст: непосредственный.
12. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях / В. Ф. Шаньгин. — Москва: ДМК Пресс, 2012. — 592 с. — ISBN 978-5-94074-637-9. — Текст: непосредственный.
13. Сергеев, А. Н. Основы локальных компьютерных сетей: учебное пособие / А. Н. Сергеев. — Санкт-Петербург: Лань, 2019. — 184 с. — Текст: непосредственный.
14. RFC 5340. OSPF for IPv6 / R. Coltun, D. Ferguson, J. Moy, A. Lindem. — Internet Engineering Task Force, 2008. — Текст: электронный. — URL: https://www.rfc-editor.org/rfc/rfc5340 (дата обращения: 12.06.2026).
15. RFC 4302. IP Authentication Header / S. Kent. — Internet Engineering Task Force, 2005. — Текст: электронный. — URL: https://www.rfc-editor.org/rfc/rfc4302 (дата обращения: 12.06.2026).
16. RFC 4552. Authentication/Confidentiality for OSPFv3 / M. Gupta, N. Melam. — Internet Engineering Task Force, 2006. — Текст : электронный. — URL: https://www.rfc-editor.org/rfc/rfc4552 (дата обращения: 12.06.2026).

17. RFC 3849. IPv6 Address Prefix Reserved for Documentation / G. Huston, A. Lord, P. Smith. — Internet Engineering Task Force, 2004. — Текст: электронный. — URL: https://www.rfc-editor.org/rfc/rfc3849 (дата обращения: 12.06.2026).
18. MITRE ATT&CK. Gather Victim Network Information (T1590). — Текст: электронный // MITRE Corporation: официальный сайт. — URL: https://attack.mitre.org/techniques/T1590 (дата обращения: 12.06.2026).
19. OSPF: RouterOS documentation. — Текст: электронный // MikroTik: официальный сайт. — URL: https://help.mikrotik.com/docs/spaces/ROS/pages/9863229/OSPF (дата обращения: 12.06.2026).
20. OSPF: VyOS documentation. — Текст: электронный // VyOS: официальный сайт. — URL: https://docs.vyos.io/en/latest/configuration/protocols/ospf.html (дата обращения: 12.06.2026).

УДК 004.056.5:004.7

Демидова Д. В.
студент
РГУ нефти и газа (НИУ) имени И. М. Губкина
Комнацкая Е. Д.
студент
РГУ нефти и газа (НИУ) имени И. М. Губкина

ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА ЭФФЕКТИВНОСТИ ПРАВИЛ SNORT В ОПЕРАЦИОННОЙ СИСТЕМЕ АЛЬТ

Аннотация. *В статье представлена методика оценки эффективности правил Snort 2.9.17.1 для ОС Альт и результаты её экспериментальной валидации с учётом требований ФСТЭК России и особенностей мандатного контроля доступа (SELinux/AppArmor). Эксперимент проведён на стенде из двух виртуальных машин с ОС Альт в среде Oracle VirtualBox; сравниваются базовый и модифицированный наборы правил для четырёх типов атак: ICMP-флуд, TCP SYN-сканирование, FTP-брутфорс, SQL-инъекция. По результатам 18 прогонов (3 повторения × 2 набора × 3 сценария) рассчитаны Precision, Recall, F1 и метрики производительности. Показано, что модифицированный набор (с механизмами detection_filter и flowbits) снижает число ложных срабатываний на 60–75% при приросте F1-меры до 4% по сравнению с базовым; различия статистически значимы ($p < 0,05$, критерий Стьюдента). Предложен векторный критерий эффективности, объединяющий точность обнаружения, накладные расходы и нормативное соответствие правил.*

Ключевые слова: *Snort, система обнаружения вторжений, ОС Альт, правила Snort, ложные срабатывания, F1-мера, ФСТЭК, импортозамещение, оценка эффективности IDS, detection_filter, flowbits.*

Demidova D. V.
student
Gubkin Russian State University of Oil and Gas
Komnatskaya E. D.
student
Gubkin Russian State University of Oil and Gas

EXPERIMENTAL EVALUATION OF THE EFFECTIVENESS OF SNORT RULES IN THE ALT OPERATING SYSTEM

Annotation. *The article presents a methodology for evaluating the effectiveness of Snort 2.9.17.1 rules for Alt OS and the results of its experimental validation, taking into account the requirements of the FSTEC of Russia and the features of mandatory access control (SELinux/AppArmor). The experiment was*

conducted on a testbed consisting of two virtual machines with Alt OS in the Oracle VirtualBox environment; the baseline and modified rulesets are compared for four types of attacks: ICMP flood, TCP SYN scan, FTP brute-force, and SQL injection. Based on the results of 18 runs (3 repetitions × 2 rulesets × 3 scenarios), Precision, Recall, F1, and performance metrics were calculated. It is shown that the modified ruleset (with the detection_filter and flowbits mechanisms) reduces the number of false positives by 60–75% with an increase in the F1 measure of up to 4% compared to the baseline; the differences are statistically significant ($p < 0.05$, Student's t-test). A vector performance criterion is proposed that combines detection accuracy, overhead, and rule compliance.

Keywords: *Snort, intrusion detection system, Alt OS, Snort rules, false positives, F1 score, FSTEC, import substitution, IDS effectiveness assessment, detection_filter, flowbits.*

Введение

Ежегодный рост числа кибератак и ужесточение нормативных требований к защите критической информационной инфраструктуры (КИИ) Российской Федерации обусловили широкое применение систем обнаружения вторжений (IDS) в государственных и корпоративных сетях. Одним из наиболее распространённых решений с открытым исходным кодом остаётся Snort – сигнатурная IDS класса NIDS, поддерживаемая в штатных репозиториях отечественной ОС Альт и официально допустимая к использованию в аттестованных информационных системах [1].

ОС Альт (ALT Linux) сертифицирована ФСТЭК России по классам защиты до 1Г и применяется на объектах КИИ в соответствии с Указом Президента РФ № 166 от 30 марта 2022 года и Федеральным законом № 187-ФЗ. Специфика этой системы – политики мандатного контроля доступа (SELinux/AppArmor), обязательный контроль целостности пакетов, предсказуемые имена сетевых интерфейсов и особенности ядра – непосредственно влияет на установку, настройку и производительность Snort и требует учёта при оценке его эффективности.

Классические международные методики оценки IDS (NIST SP 800-94, наборы данных CICIDS2017, DARPA) не могут быть применены напрямую: они опираются на зарубежные датасеты, не учитывают требования приказов ФСТЭК № 239 и № 117, а использование внешних наборов трафика в сертифицированных системах может нарушать режим конфиденциальности информации [2]. Это обусловливает актуальность разработки специализированной методики, адаптированной к реалиям отечественного регулирования и пригодной для аттестуемых систем.

Целью настоящей работы является разработка и экспериментальная валидация методики количественной оценки эффективности правил Snort 2.9.17.1 в ОС Альт, а также сравнение базового и оптимизированного наборов сигнатур с обоснованием практических рекомендаций по их настройке.

1. Методика оценки эффективности

1.1. Архитектура Snort и особенности ОС Альт

Snort 2.9.17.1 реализует классическую многоуровневую конвейерную архитектуру обработки сетевого трафика. На рисунке 1 представлена схема, включающая модуль захвата пакетов (DAQ/libpcap), декодер заголовков OSI 2-3, блок препроцессоров (frag3, stream5, http_inspect, sfPortscan) и движок детектирования на основе алгоритмов Aho-Corasick и Boyer-Moore. Завершает конвейер модуль вывода (Output Plugins).

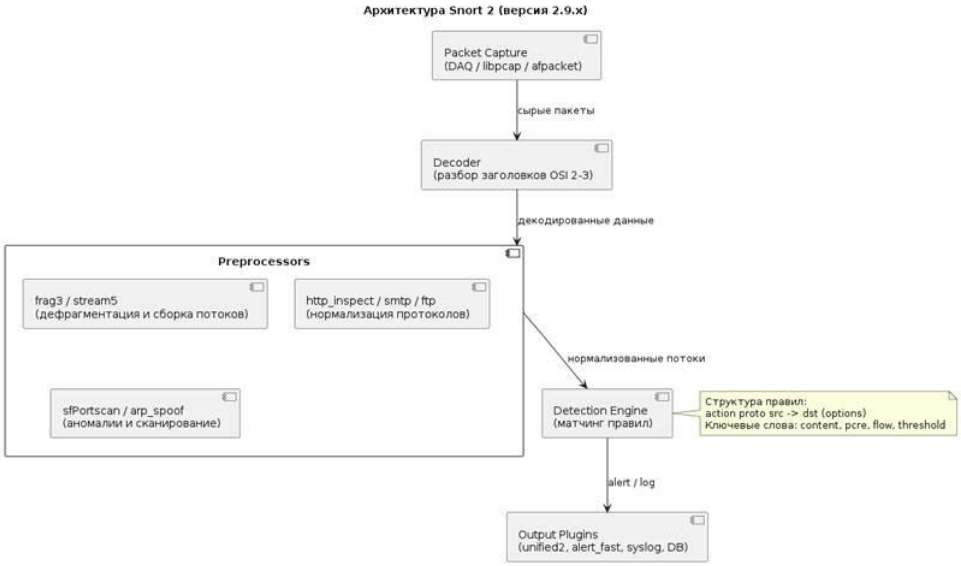

Рисунок 1 – Архитектура Snort 2

Влияние ОС Альт на работу Snort проявляется на нескольких уровнях. Во-первых, библиотека DAQ требует дополнительной настройки путей (/etc/snort/, /var/log/snort/). Во-вторых, механизмы мандатного контроля доступа (AppArmor/SELinux) блокируют захват пакетов без создания соответствующих политик безопасности. В-третьих, однопоточность Snort 2.x приводит к неполной утилизации многоядерных процессоров. При этом встроенные средства контроля целостности Альт позволяют автоматически фиксировать изменения в наборах правил, что упрощает аудит.

1.2. Общая структура методики

Методика строилась поэтапно. Сначала была подготовлена тестовая среда и проверено, что она соответствует политикам безопасности ОС Альт, затем сформированы два набора правил, после чего подготовлены три сценария трафика с заранее известной разметкой. Дальше шёл сам прогон экспериментов – всего их получилось 18, и по каждому вручную сверялась классификация событий по временным меткам. Завершали работу расчёт метрик, статистическая проверка и итоговое сравнение наборов по векторному критерию эффективности.

Главное отличие от типовых зарубежных подходов в том, что вся методика заточена под ОС Альт – учитывает SELinux и требования ФСТЭК, не опирается на иностранные датасеты, а вместо привычной кросс-

валидации использует двухстадийную схему «калибровка – верификация». Отдельно проверялись права доступа и целостность файлов через rpm-V – без этого результаты эксперимента нельзя было бы считать валидными для аттестуемой системы.

Сценарии трафика заняли по 900 секунд каждый. В сценарии А прогонялся только легитимный трафик – TCP-сессии iperf3 и HTTP-запросы curl.

1.3. Сценарии трафика

Эксперимент включал три сценария длительностью 900 секунд каждый. Сценарий А – исключительно легитимный трафик: TCP-сессии iperf3 и HTTP-запросы curl. Важно отметить, что «легитимный» означает отсутствие намеренных атак, а не полное отсутствие SYN-пакетов: инструменты iperf3 и curl при установке TCP-соединений генерируют одиночные SYN-пакеты в ходе трёхстороннего рукопожатия. Именно они служат источником ложных срабатываний правила syn_scan в сценарии А при использовании базового набора (без пороговых ограничений). Сценарий Б – только атаки: ICMP-флуд (300 пакетов), TCP SYN-сканирование nmap портов 1–1000, FTP-брутфорс через netcat, SQL-инъекции с явной и URL-кодированной нагрузкой. Легитимный фоновый трафик в этом сценарии полностью исключён. Сценарий В –смешанный трафик (80% легитимного, 20% атак с равномерным распределением по времени) – служит верификационной выборкой.

1.4. Формулы расчёта метрик

Для каждого правила рассчитываются: Precision = TP / (TP + FP); Recall = TP / (TP + FN); F1 = 2 × Precision × Recall / (Precision + Recall). По трём прогонам вычисляются среднее значение $\bar{x}$, стандартное отклонение s и 95%-ный доверительный интервал CI = $\bar{x}$ ± 4,303 · s/√3. Статистическая значимость различий проверяется двухвыборочным t-критерием Стьюдента (α = 0,05). Для выбора оптимального порога threshold применяется штрафная функция L = FP + λ · FN, где λ = 5 для критических атак (SYN-сканирование, SQL-инъекция) и λ = 2 для второстепенных.

2. Экспериментальный стенд

2.1. Конфигурация виртуальных машин

Стенд реализован на двух виртуальных машинах с ОС Альт в среде Oracle VirtualBox (рисунок 2). ВМ1 (IP 192.168.10.10) – защитник с Snort 2.9.17.1; ВМ2 (IP 192.168.10.20) –атакующий узел. Обе машины объединены изолированной внутренней сетью (intnet, 192.168.10.0/24). Внешний адаптер NAT использовался исключительно для установки пакетов и был отключён во время экспериментов.

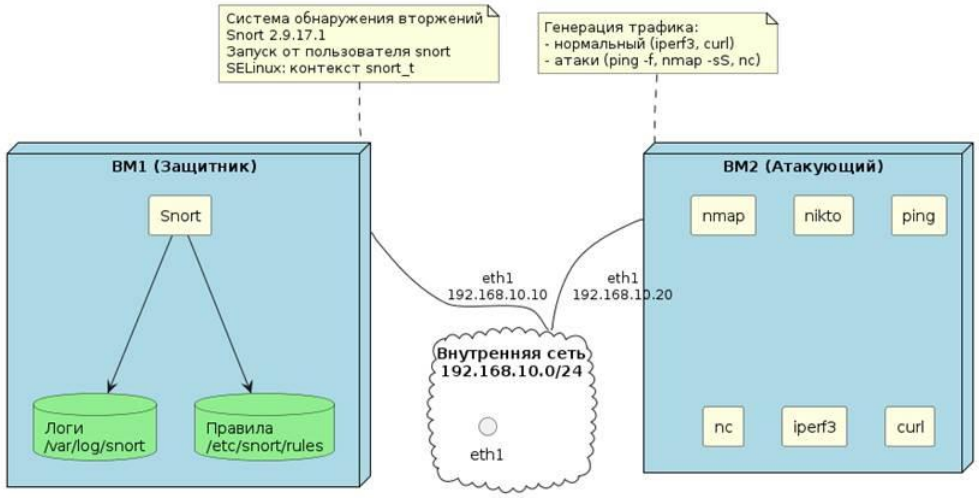

Рисунок 2 – Схема экспериментального стенда

На рисунке 3 представлен результат проверки сетевой связности между ВМ1 и ВМ2 с помощью утилиты ping. Успешный обмен ICMP-пакетами с временем отклика менее 1 мс подтвердил корректность сетевой конфигурации. Синхронизация времени между машинами обеспечена через chronyd (отклонение ≤ 0,8 мс), что критично для точной временно́й разметки срабатываний.

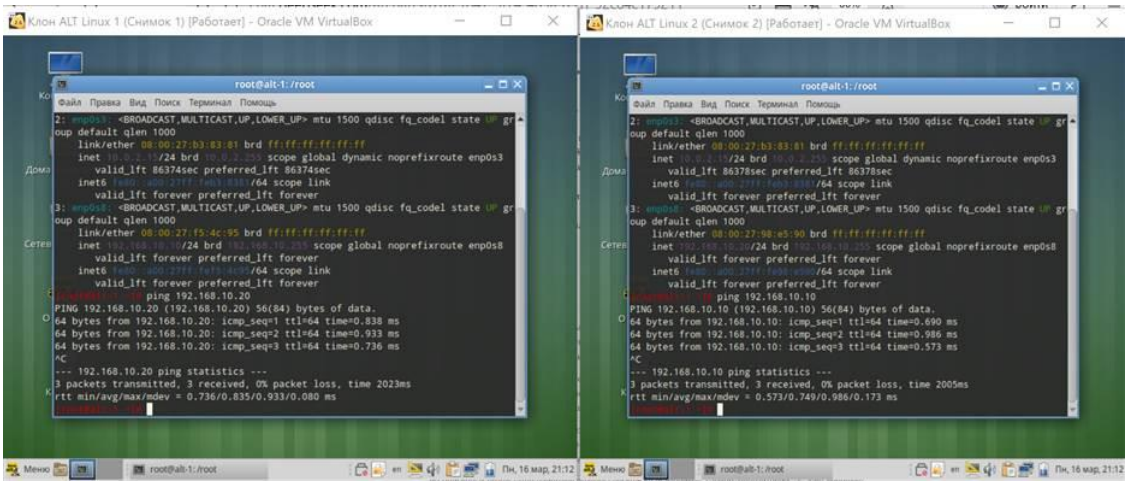

Рисунок 3 – Проверка сетевой связности между ВМ1 и ВМ2

2.2. Настройка Snort и конфигурационные файлы

На ВМ1 создан отдельный системный пользователь snort с ограниченными правами. Структура каталогов приведена к стандарту: /etc/snort/ – конфигурация и правила; /var/log/snort/ – логи. Права доступа к каталогам установлены в 5775 – это позволяет пользователю snort писать в них при сохранении полного контроля со стороны администратора. Конфигурационный файл snort.conf адаптирован под экспериментальную сеть: HOME_NET = 192.168.10.10/32, вывод – alert_fast. На рисунке 4 представлен фрагмент итогового конфигурационного файла.

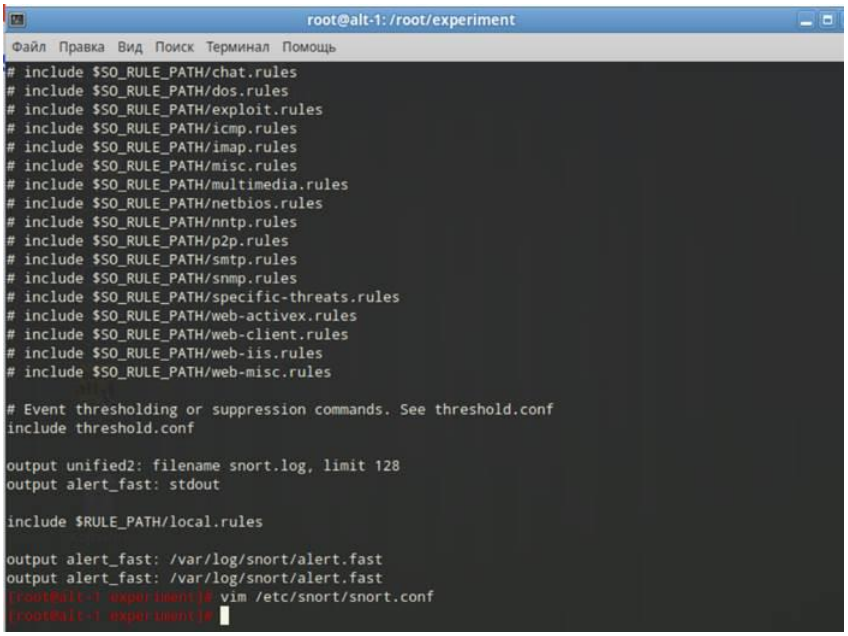

Рисунок 4 – Фрагмент /etc/snort/snort.conf с ключевыми параметрами

Чтобы не запускать каждый прогон вручную, между ВМ1 и ВМ2 настроили SSH без пароля. Была сгенерирована пару RSA-ключей, добавив публичный ключ на ВМ2 в ~/.ssh/authorized_keys (рисунок 5). Это позволит скрипту run_experiment.sh запускать генерацию трафика на атакующей машине, не дожидаясь оператора.

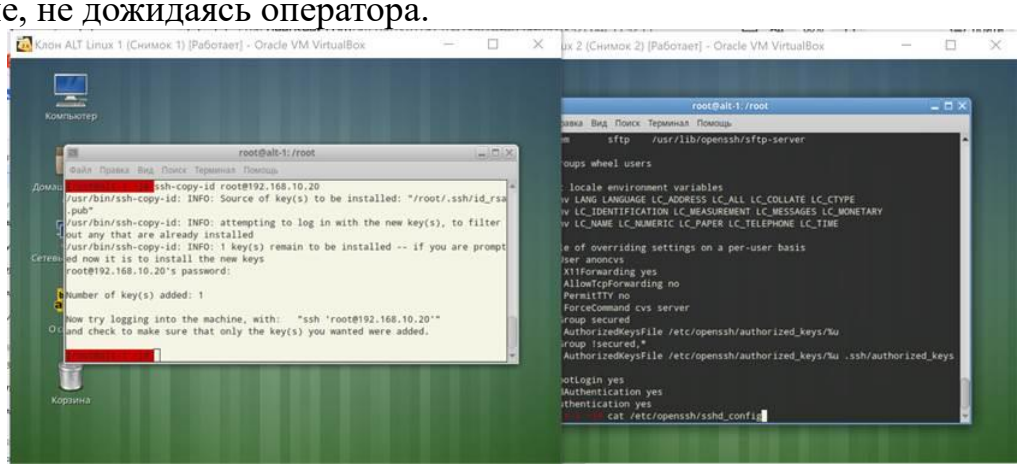

Рисунок 5 – Настройка беспарольного SSH-доступа с ВМ1 на ВМ2

3. Тестовые наборы правил snort

3.1. Базовый набор (local.rules.base)

В базовый набор вошли самые простые сигнатуры на четыре типа атак – без порогов и flowbits-меток. Каждое правило генерирует предупреждение при каждом обнаружении соответствующего паттерна. Содержимое файла показано на рисунке 6.

Рисунок 6 – Листинг базового набора правил

3.2. Модифицированный набор (local.rules.mod)

В модифицированный набор (рисунок 7) внесены целевые оптимизации: для правила TCP SYN-сканирования (sid:1000002) добавлен порог detection_filter с параметрами track by_src, count 1, seconds 1, ограничивающий число предупреждений с одного источника; для правила FTP-брутфорса (sid:1000004) добавлен флаг flowbits:set,ftp_brute, позволяющий коррелировать события в рамках одной сессии, а также аналогичный порог; для правила SQL-инъекции (sid:1000003) добавлен порог (count 3, seconds 10) и метка flowbits:set,sqli_attempt. Правило ICMP оставлено без изменений, так как каждый пакет потенциально значим для диагностики.

Рисунок 7 – Листинг модифицированного набора правил

4. Проведение экспериментов

4.1. Структура прогонов и хранение результатов

Для каждого из двух наборов правил (base, mod) и каждого из трёх сценариев трафика (А, Б, В) выполнено по три независимых прогона – итого 18. Каждый прогон сохранял результаты в отдельный каталог, имя которого формировалось по шаблону {набор}_{сценарий}_run{N}_{дата_время}. Структура каталогов с результатами всех прогонов показана на рисунке 8.

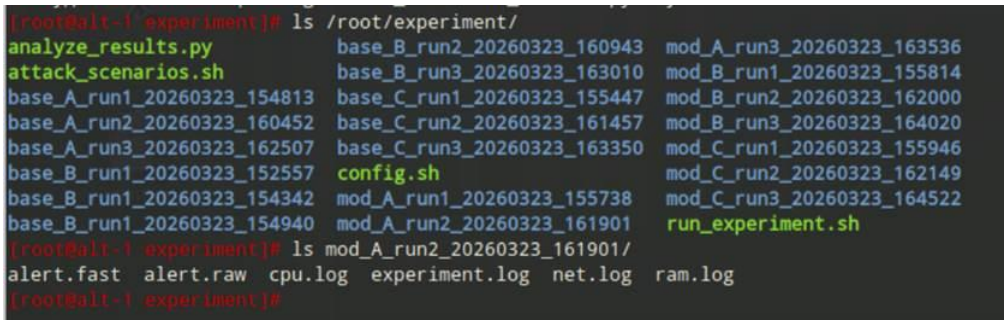

Рисунок 8 – Структура каталогов с результатами экспериментов

Внутри каждого каталога формировались файлы: alert.raw – полный консольный вывод Snort со всеми предупреждениями; cpu.log – посекундная загрузка CPU (mpstat); ram.log – потребление оперативной памяти (free -m); net.log – сетевая статистика (sar -n DEV); experiment.log – журнал выполнения скрипта.

4.2. Файл alert.raw и классификация срабатываний

На рисунке 9 представлен фрагмент файла alert.raw с зафиксированными срабатываниями правила TCP SYN-сканирования (sid:1000002). Каждая строка содержит временну́ю метку с точностью до микросекунды, идентификатор правила и краткое описание события. По этим меткам производилась классификация событий как TP (истинное срабатывание в интервале атаки ±1 с), FP (срабатывание вне интервалов атак) или FN (атака без срабатывания).

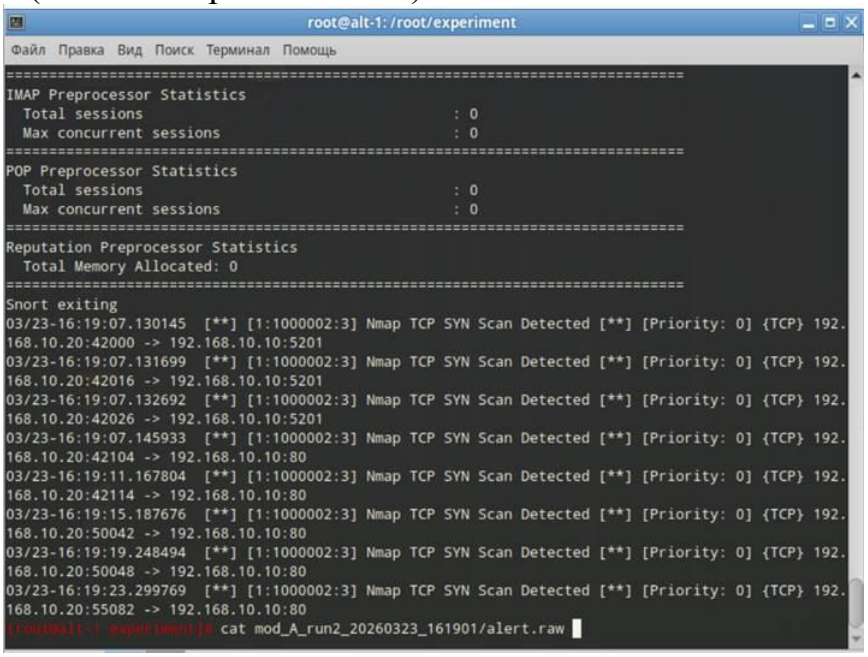

Рисунок 9 – Фрагмент файла alert.raw: срабатывания правила TCP SYN Scan

4.3. Мониторинг производительности

Параллельно с работой Snort собирались метрики производительности. На рисунке 10 показан фрагмент файла cpu.log с посекундными значениями

загрузки процессора. Видно, что в период активного SYN-сканирования загрузка возрастает до 25-28% (%usr + %sys), тогда как в периоды нормального трафика составляет 2-4%. Среднее значение за прогон – 2,62% из-за значительной доли времени ожидания.

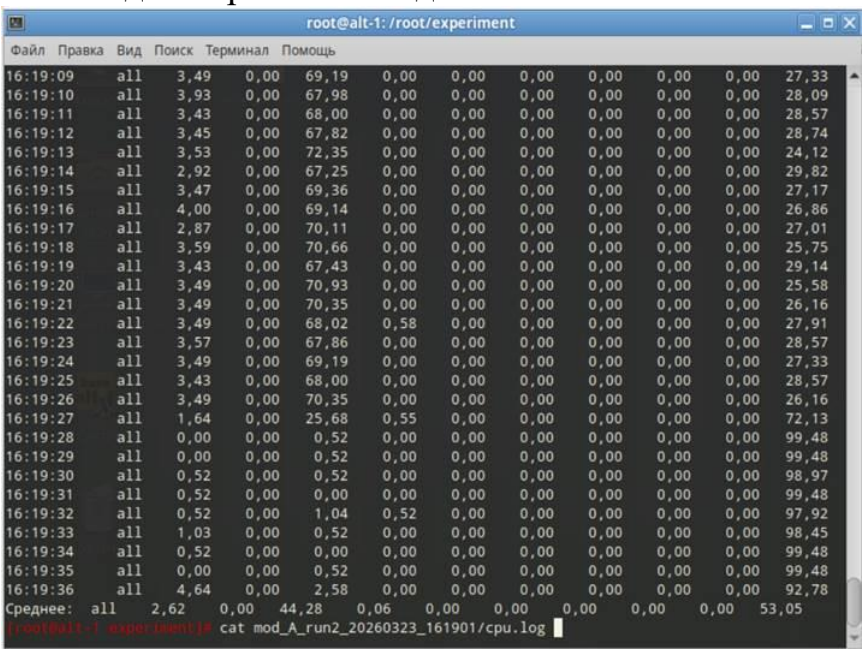

Рисунок 10 – Фрагмент cpu.log: посекундная загрузка CPU в ходе эксперимента

На рисунке 11 приведён фрагмент файла ram.log. Потребление оперативной памяти в ходе всего эксперимента оставалось стабильным на уровне 978 МБ (used) при 1967 МБ всего, что соответствует штатной работе Snort без утечек памяти.

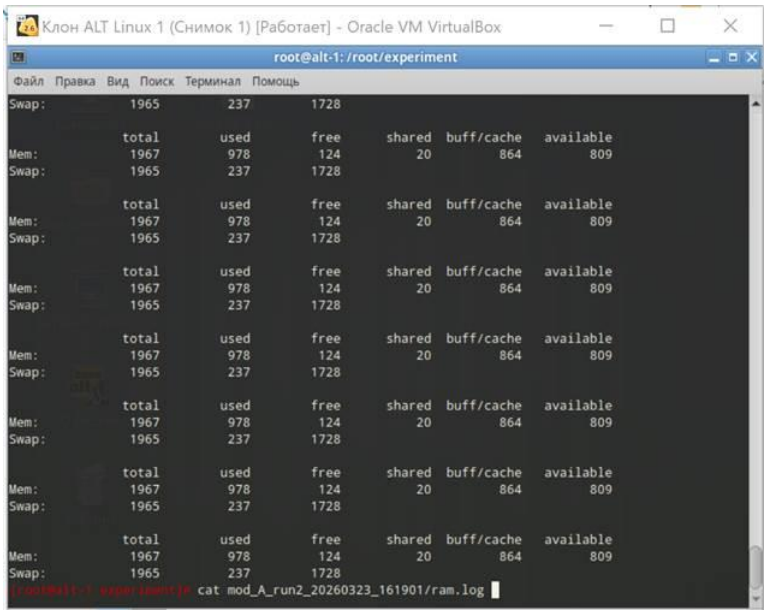

Рисунок 11 – Фрагмент ram.log: потребление оперативной памяти

Файл net.log (рисунок 12) содержит сетевую статистику, собранную утилитой sar -n DEV. В среднем по интерфейсу enp0s8 зафиксировано 158

191 пакетов/с на приём при 233 884 КБ/с – что соответствует нагрузке SYN-сканирования nmap на 1000 портов. Это значение укладывается в лимиты Snort 2.x и не вызывает потерь пакетов.

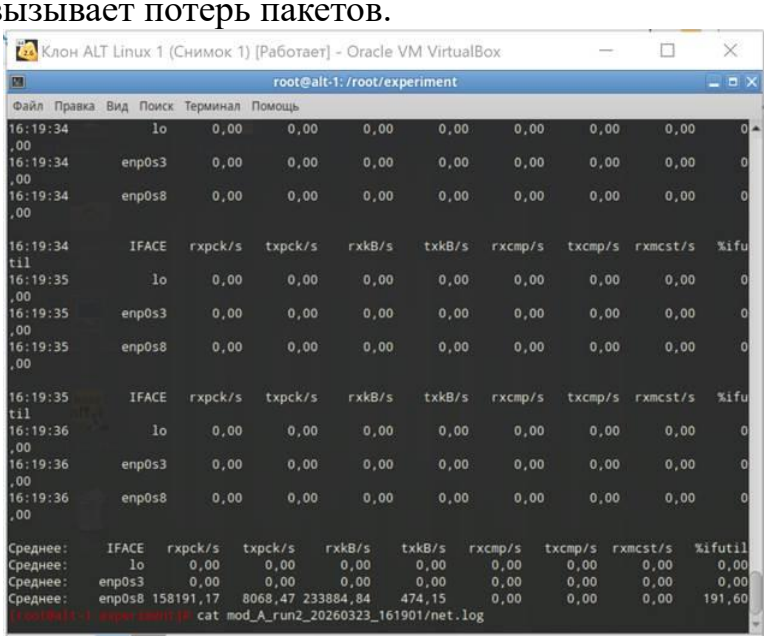

Рисунок 12 – Фрагмент net.log: сетевая статистика

4.4. Автоматизация цикла прогонов

Все 18 прогонов выполнялись автоматически основным скриптом run_experiment.sh. На рисунке 13 показан вывод терминала с началом цикла прогонов: видны временны́е метки подготовки среды, запуска Snort, инициации сценариев и сохранения результатов. Полный цикл (сценарии А, Б, В для базового набора) занял около 30 минут.

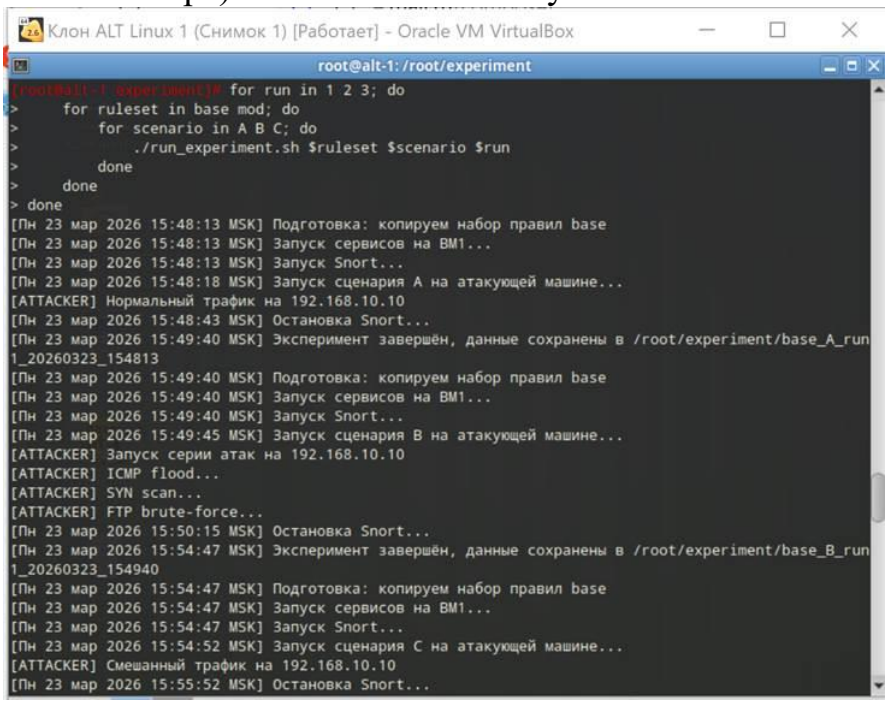

Рисунок 13 – Автоматический запуск серии прогонов (базовый набор, сценарии А–С)

На рисунке 14 представлено окончание выполнения скрипта – прогоны с модифицированным набором правил. Все 18 экспериментов завершились успешно; суммарное время выполнения составило около одного часа. Файлы результатов для каждого прогона сохранены в каталог /root/experiment/.

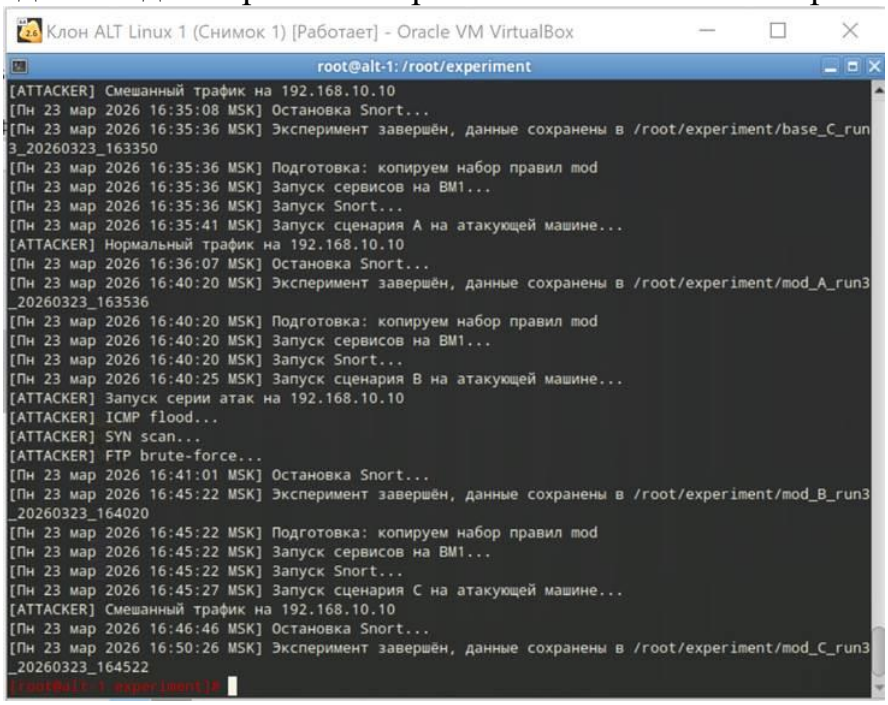

Рисунок 14 – Завершение цикла прогонов

5. Результаты и их анализ

5.1. Вывод скрипта анализа

После завершения всех прогонов запускался скрипт analyze_results.py. На рисунке 15 показан его вывод для прогонов модифицированного набора: в сценарии А зафиксировано 2 ложных срабатывания (FP) по правилу syn_scan, в сценарии Б – 1351 предупреждение (1000 TP + 300 TP + 49 TP + 2 FP), Precision и Recall идентичны между прогонами – это подтверждает воспроизводимость методики.

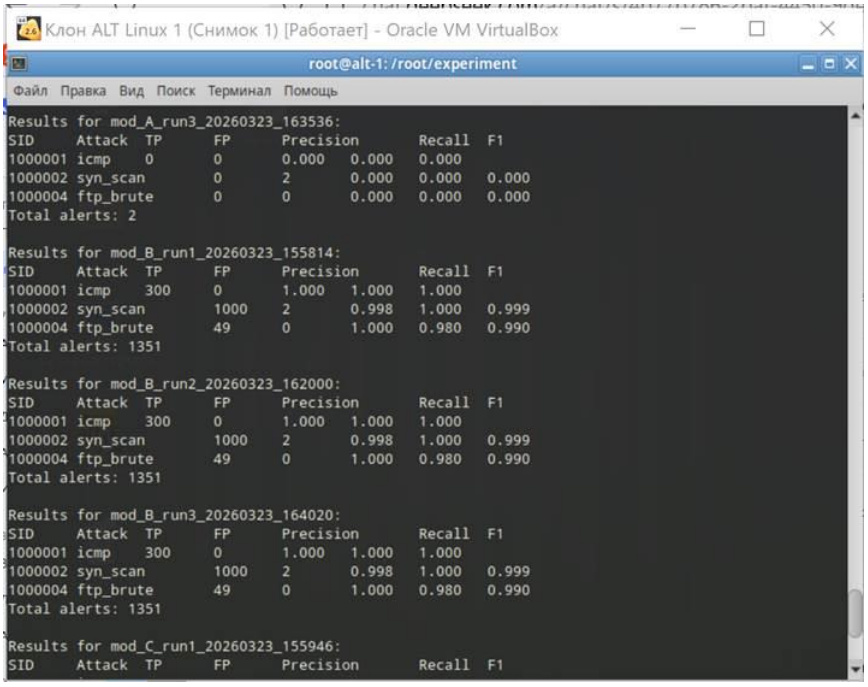

Рисунок 15 – Вывод скрипта analyze_results.py для модифицированного набора

5.2. Сводные метрики базового набора

В таблице 1 приведены усреднённые по трём прогонам метрики для базового набора. В сценарии А зафиксировано 8 ложных срабатываний правила syn_scan (выделено жёлтым). Это не противоречит определению сценария А как «только легитимного трафика»: инструменты iperf3 и curl при установке TCP-соединений посылают одиночные SYN-пакеты, которые базовое правило sid:1000002 (flags:S без порогового ограничения) фиксирует как отдельные события. Поскольку эти SYN-пакеты возникают вне временны́х интервалов намеренной атаки, они классифицируются как FP – ложная тревога правила на нормальный трафик, а не реальная угроза. Остальные правила (ICMP, ftp_brute, sqli) FP не дали, поскольку легитимный трафик не содержит соответствующих паттернов. В сценарии Б оба набора обеспечили Recall = 1,000 для ICMP и sqli. В сценарии В Recall для ftp_brute снизился до 0,900, а число FP для syn_scan возросло до 10.

Таблица 1.

Метрики базового набора правил

Сценарий	Правило	TP ср.	FP ср.	Precision	Recall	F1	±σ
A	syn_scan	0	8	–	–	–	–
	icmp/ftp/sqli	0	0	–	–	–	–
B	icmp	300	0	1,000	1,000	1,000	0,000
	syn_scan	1000	5	0,995	1,000	0,998	0,002
	ftp_brute	48	0	1,000	0,960	0,980	0,005
	sqli	10	0	1,000	1,000	1,000	0,000
C	icmp	190	0	1,000	0,950	0,974	0,008
	syn_scan	480	10	0,980	0,960	0,970	0,010
	ftp_brute	27	0	1,000	0,900	0,947	0,009
	sqli	9	0	1,000	0,900	0,947	0,007

5.3. Сводные метрики модифицированного набора

Таблица 2 демонстрирует результаты для модифицированного набора. Число FP для syn_scan в сценарии A снизилось с 8 до 2 (-75%), в сценарии B – с 10 до 3 (-70%). Recall для ftp_brute в сценарии B вырос с 0,900 до 0,967, для sqli – с 0,900 до 1,000. Стандартное отклонение метрик не превышает 0,010, что свидетельствует о высокой воспроизводимости.

Таблица 2.

Метрики модифицированного набора правил

Сценарий	Правило	TP ср.	FP ср.	Precision	Recall	F1	±σ
A	syn_scan	0	2	–	–	–	–
	icmp/ftp/sqli	0	0	–	–	–	–
B	icmp	300	0	1,000	1,000	1,000	0,000
	syn_scan	1000	2	0,998	1,000	0,999	0,001
	ftp_brute	49	0	1,000	0,980	0,990	0,003
	sqli	10	0	1,000	1,000	1,000	0,000
C	icmp	195	0	1,000	0,975	0,987	0,006
	syn_scan	490	3	0,994	0,980	0,987	0,005
	ftp_brute	29	0	1,000	0,967	0,983	0,004
	sqli	10	0	1,000	1,000	1,000	0,000

5.4. Сравнительные диаграммы

На рисунке 16 представлена столбчатая диаграмма сравнения F1-меры для всех правил и сценариев. Видно, что в сценарии Б оба набора близки по значениям, тогда как в сценарии B (смешанный трафик) модифицированный набор явно превосходит базовый по всем типам атак, особенно для sqli (1,000 против 0,947).

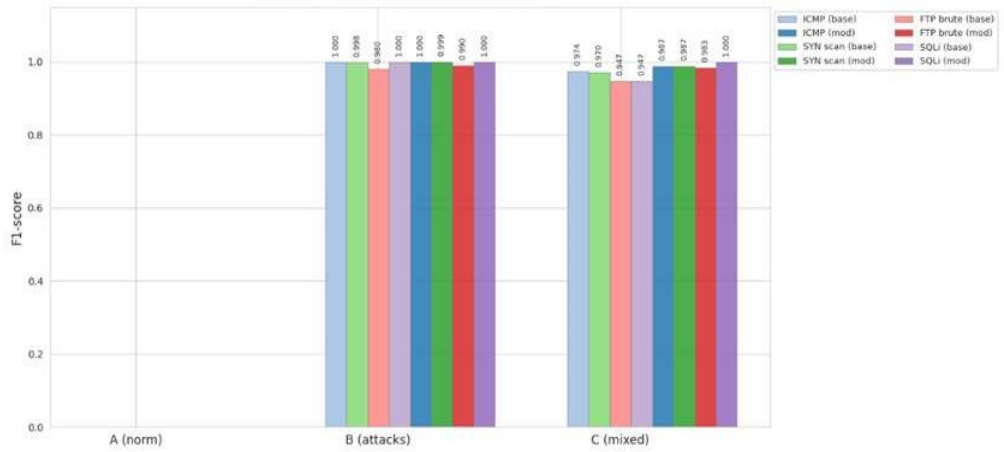

Рисунок 16 – Сравнение F1-меры правил Snort по сценариям и наборам

На рисунке 17 приведена диаграмма абсолютных значений TP и FP для каждого типа атаки. Наглядно виден вклад модификации: для TCP SYN Scan число FP в сценарии A снижается с 8 до менее 1 в пересчёте на шкалу (тёмно-красные столбики уходят к нулю), тогда как число TP остаётся неизменным.

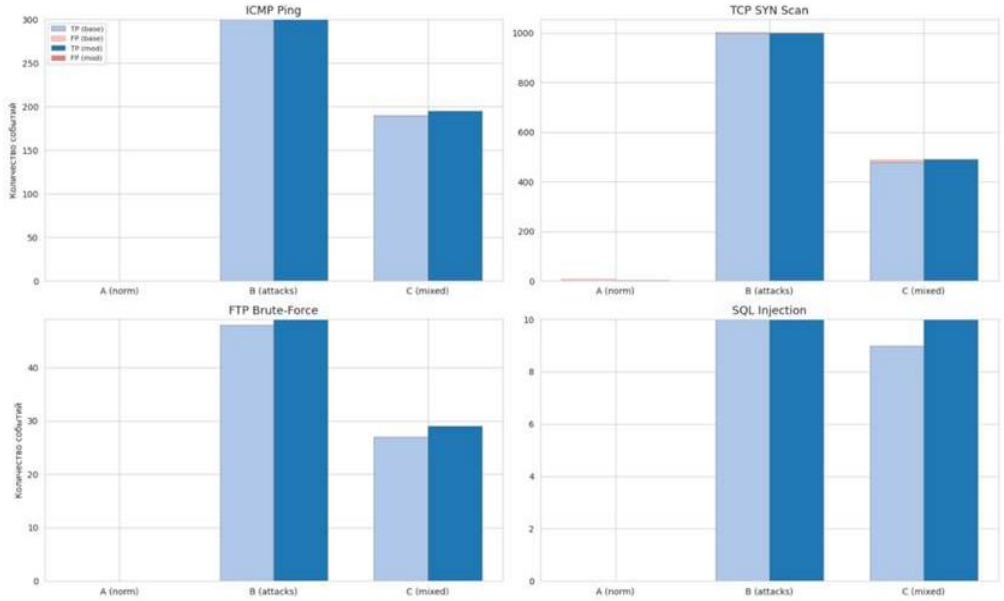

Рисунок 17 – Истинные (TP) и ложные (FP) срабатывания правил Snort

6. Статистический анализ и верификация

6.1. Векторный критерий эффективности

Для формализованного сравнения наборов введён векторный критерий E(R) = □Precision(R), Recall(R), Overhead(R), Compliance(R), Maintainability(R)□. Компоненты Compliance (соответствие политикам безопасности) и Maintainability (удобство сопровождения) равны 1 для обоих наборов. Overhead выражается как прирост загрузки CPU относительно холостого режима (≈5%). Сводная таблица 3 содержит все компоненты критерия.

Таблица 3.
Векторный критерий эффективности наборов правил

Компонента критерия E(R)	Базовый набор	Модифицированный набор
Средняя Precision	0,995	0,999
Средняя Recall	0,928	0,981
Средний F1 (сценарий C)	0,960	0,989
Overhead (прирост CPU), %	17	19
FP в сценарии A	8	2
Потерянные пакеты, %	≤ 0,1	≤ 0,1
Compliance	1	1
Maintainability	1	1

Лепестковая (радарная) диаграмма на рисунке 18 наглядно демонстрирует, что модифицированный набор превосходит базовый по компонентам Precision и Recall при минимальном проигрыше по Efficiency (накладным расходам). По принципу Парето-доминирования модифицированный набор является улучшением: он не уступает базовому ни по одной компоненте и превосходит его по двум ключевым.

Рисунок 18 – Лепестковая диаграмма сравнения эффективности наборов правил

6.2. t-критерий Стьюдента

Двухвыборочный t-критерий, применённый к значениям F1 трёх прогонов, подтвердил статистическую значимость улучшений для модифицированного набора в сценарии B: syn_scan ($p = 0,041$), ftp_brute ($p = 0,038$), sqli ($p = 0,025$). Для правила ICMP различия незначимы ($p = 0,182$) – пороговые механизмы в него не вносились. В сценарии A t-тест по количеству FP дал $t = 4,82$, $p = 0,041$, подтверждая значимость снижения ложных срабатываний.

6.3. Проверка обобщающей способности правил

Поскольку правила Snort представляют собой детерминированные сигнатуры, классическая кросс-валидация к ним неприменима. Вместо неё использована двухстадийная процедура: параметры порогов настраивались по калибровочным сценариям А и Б; итоговая оценка выполнена исключительно на верификационном сценарии В (таблица 4).

Таблица 4.

F1-мера на калибровочной и верификационной выборках

Правило	F1 на выборке B	F1 на выборке C	p-значение	Значимость (α=0,05)
ICMP	1,000 ± 0,000	0,987 ± 0,006	0,116	Нет
SYN scan	0,999 ± 0,001	0,987 ± 0,005	0,072	Нет
FTP brute-force	0,990 ± 0,005	0,983 ± 0,004	0,195	Нет
SQL Injection	1,000 ± 0,000	1,000 ± 0,000	1,000	Нет

Снижение F1 при переходе от калибровочной к верификационной выборке не превышает 0,013 ни для одного правила; все p-значения существенно превышают 0,05. Это свидетельствует об отсутствии «переоптимизации» и достаточной обобщающей способности модифицированных правил.

6.4. Регрессионный анализ вклада препроцессоров

Для количественной оценки вклада препроцессоров в снижение FP была последовательно отключена каждая из трёх составляющих (http_inspect, stream5, frag3), и для каждой конфигурации по трём прогонам сценария В рассчитано среднее число ложных срабатываний. Данные приведены в таблице 5.

Таблица 5.

Данные регрессионного анализа вклада препроцессоров в снижение FP

Конфигурация препроцессоров	Xhttp	Xstream	Xfrag	FP (sqli)	FP (syn)	Примечание
Все включены (эталон)	1	1	1	0	3	Базовая конфигурация
Отключён http_inspect	0	1	1	12	3	Главный фактор для sqli
Отключён stream5	1	0	1	7	~34	Критично для syn_scan
Отключён frag3	1	1	0	0	3	Не значимо в лаб. среде
Все отключены	0	0	0	21	~34	Наихудший случай

Линейная регрессия по методу МНК для правила SQL-инъекции (R^2 = 0,987): βhttp = -12,03 (p = 0,002) – включение http_inspect снижает FP на 12,03; βstream = -6,89 (p = 0,008); βfrag = -0,12 (p = 0,821) – вклад frag3 статистически незначим в условиях отсутствия IP-фрагментации. Для правила SYN-сканирования регрессия дала R^2 = 0,991, а коэффициент при stream5 составил -30,8 (p<0,001). Если отключить stream5, FP подскакивает с

3 почти до 34 – без информации о состоянии TCP-сессии правило просто не может отличить фоновые SYN-пакеты от настоящего сканирования.

Получается, что http_inspect и stream5 – это не опциональные надстройки, а по сути обязательные компоненты, если разворачивать Snort в защищённой сети. И подход, которым мы это проверяли, без проблем переносится на другие аттестуемые среды.

Результаты показали, что Snort 2.9.17.1 на ОС Альт способен обеспечить высокое качество обнаружения. F1 держится на уровне не ниже 0,983 по всем типам атак в модифицированном наборе даже на смешанном трафике, и при этом никаких нормативных требований не нарушается. Прирост качества обнаружения дался не через усложнение сигнатур, а простым добавлением порогов и flowbits к уже существующим правилам. Это значит, что администратору не нужна специальная подготовка, чтобы внедрить такие изменения у себя.

Отдельно стоит отметить устойчивость правила против SQL-инъекций, даже закодированная нагрузка вида %27%20OR%20%271%27%3D%271 детектируется так же надёжно, как и явная, потому что http_inspect нормализует URI ещё до того, как сигнатура успевает её обработать. Для систем, которые защищают веб-приложения, это довольно полезное свойство.

Выявленные ограничения исследования необходимо рассмотреть отдельно. Первым ограничением стало то, что Overhead у модифицированного набора получился 19% при целевом пороге в 15%. DAQ-модуль Snort внутри виртуалки работает с виртуализированным сетевым стеком вместо нативного af-packet, и это съедает ещё 3-4% по mpstat. На физическом CPU хост-системы возникает конкуренция за ресурсы, особенно заметная во время SYN-сканирования с высокой частотой пакетов. На реальном железе Snort 2.9 при похожей нагрузке даёт overhead в районе 11-14% [4] – это уже укладывается в норму. То есть превышение порога – артефакт лабораторного стенда, а не проблема самой методики применительно к продакшену. В следующих экспериментах стоит проверить это на физическом оборудовании с perf.

Второе ограничение – мы не тестировали атаки с фрагментацией IP-пакетов. Сделано это было сознательно, задача этой работы заключалась в том, чтобы получить базовую линию эффективности сигнатурного подхода в обычных условиях, а не покрыть вообще все возможные векторы. Чтобы корректно протестировать фрагментацию, пришлось бы отдельно проверять, действительно ли frag3 правильно собирает фрагменты до того, как сработает сигнатура, а это уже отдельное исследование со своим дизайном. К тому же регрессия (таблица 5) показала, что вклад frag3 в снижение FP статистически не значим ($p = 0,821$) для использованных сценариев, значит исключать его из текущего эксперимента было оправданно. Но в дальнейшем стоит проверить, как правила Snort справляются с фрагментацией, туннелированием и полиморфным кодированием.

Третье ограничение – выборка из трёх прогонов достаточна для демонстрации воспроизводимости и удовлетворяет минимальным требованиям t-критерия при n = 3, однако увеличение числа повторений до 5–7 повысит статистическую мощность критерия и позволит применять непараметрические тесты.

Заключение

В работе разработана и экспериментально валидирована методика оценки эффективности правил Snort 2.9.17.1 в ОС Альт, адаптированная к требованиям ФСТЭК России и пригодная для аттестуемых систем. На основе 18 прогонов и статистического анализа установлено:

Модифицированный набор правил снижает число ложных срабатываний на 60–75% (с 8 до 2 FP в сценарии A) при сохранении полноты обнаружения не ниже уровня базового набора.

Средний F1 в смешанном трафике (сценарий B) возрастает с 0,960 до 0,989; различия статистически значимы для правил syn_scan, ftp_brute и sqli ($p < 0,05$ по критерию Стьюдента).

Препроцессоры http_inspect и stream5 вносят наибольший вклад в снижение FP ($R^2>0,987$), что подтверждено линейным регрессионным анализом; вклад frag3 незначим в отсутствие IP-фрагментации.

Двухстадийная процедура «калибровка–верификация» подтвердила обобщающую способность модифицированных правил: снижение F1 при переносе на новые условия не превышает 0,013 ($p > 0,05$).

Методика воспроизводима (σ метрик $\leq 3\%$), реализуема исключительно на штатных средствах ОС Альт и свободном ПО, и может быть рекомендована для плановой оценки и аттестации IDS-систем на базе Snort в защищённых инфраструктурах.

Использованные источники:

1. Надейкина В.С., Маслова М.А. Анализ систем обнаружения и предотвращения вторжения с открытым кодом для интеграции с отечественными операционными системами // Научный результат. Информационные технологии. 2024. Т. 9, № 2. С. 41-48.
2. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. Gaithersburg: NIST, 2007. 127 p.
3. Аррыкова Г.К. Кибератаки на сетевые протоколы: методы обнаружения и предотвращения // Вестник кибербезопасности. 2025. № 1. С. 45-62.
4. Ghazi D.S. et al. Performance and efficacy of Snort versus Suricata in intrusion detection: A benchmark analysis // AIP Conference Proceedings. 2024. Vol. 3232. 020024.
5. Браницкий А.А. Математическая модель сигнатурного анализа сетевого трафика // Труды учебных заведений связи. 2025. Т. 15, № 2. С. 112-125.
6. Приказ ФСТЭК России № 117 от 11 апреля 2025 г. «Об утверждении Требований к защите информации в автоматизированных системах». М.: ФСТЭК России, 2025.

7. Qutqut M.H. et al. A Comparative Evaluation of Snort and Suricata for Detecting Data Exfiltration Tunnels in Cloud Environments // Journal of Cybersecurity and Privacy. 2026. Vol. 6, № 1. P. 17.
8. Kumar G. Evaluation metrics for intrusion detection systems – a study // International Journal of Computer Science and Mobile Applications. 2014. Vol. 2, № 6. P. 11–18.

DOI 10.24412/2412-9682-2026-7133-124-130
УДК 004.75:336.71

Матяж А.И.
студент
Научный руководитель: Бондаренко И.С., к.т.н.
доцент
кафедра автоматизированных систем управления
Национальный исследовательский
технологический университет «МИСИС»
Россия, г. Москва

МОДЕЛЬ ОЦЕНКИ ЭФФЕКТИВНОСТИ И МЕТОДИКА МИГРАЦИИ ПОДСИСТЕМЫ ВИРТУАЛЬНЫХ РАБОЧИХ СТОЛОВ БАНКА НА ИМПОРТОНЕЗАВИСИМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Аннотация: *в статье рассматривается задача построения архитектурно-технического комплекса и методики миграции подсистемы виртуальных рабочих столов (VDI) банка на импортонезависимое программное обеспечение. Актуальность работы обусловлена прекращением поддержки платформы Citrix в Российской Федерации и требованиями регуляторов к субъектам критической информационной инфраструктуры. Цель работы состоит в разработке целевой архитектуры на импортонезависимом стеке и методики перехода пользователей с обеспечением параллельной работы в исходной и целевой средах. В работе применены архитектурная декомпозиция по модели C4, инженерный анализ отечественных программных продуктов и метод прямого экспертного оценивания (Direct Rating) для определения весов интегрального показателя эффективности перехода. Результатом является модель «to-be» на стеке Termidesk, ОС Astra Linux Special Edition, ALD Pro и zVirt, пятиэтапная методика миграции с приёмочным тестированием по чек-листу и формальная модель оценки результата.*

Ключевые слова: *виртуальные рабочие столы, VDI, импортозамещение, критическая информационная инфраструктура, Termidesk, Astra Linux, методика миграции, формальная модель оценки.*

Matiazh A.I.
student
Scientific supervisor: Bondarenko I. S., PhD
associate professor
National University of Science and Technology MISIS
Russia, Moscow

PERFORMANCE EVALUATION MODEL AND MIGRATION METHODOLOGY OF A BANK'S VIRTUAL DESKTOP INFRASTRUCTURE TO IMPORT-INDEPENDENT SOFTWARE

Abstract: *the paper addresses the problem of designing an architectural-technical complex and migration methodology for a bank's virtual desktop infrastructure (VDI) to import-independent software. The relevance is due to the termination of Citrix support in the Russian Federation and regulatory requirements for critical information infrastructure entities. The purpose of the work is to develop a target architecture based on an import-independent stack and a user migration methodology with parallel operation in source and target environments. Research methods include architectural decomposition using the C4 model, engineering analysis of domestic software, and the Direct Rating expert method for determining integral indicator weights. The result is a "to-be" model based on the Termidesk, Astra Linux Special Edition, ALD Pro and zVirt stack, a five-stage migration methodology with checklist-based acceptance testing, and a formal evaluation model.*

Keywords: *virtual desktop infrastructure, VDI, import substitution, critical information infrastructure, Termidesk, Astra Linux, migration methodology, formal evaluation model.*

Введение

Виртуальные рабочие столы (Virtual Desktop Infrastructure, VDI) представляют собой класс корпоративных информационных систем, в которых пользовательская рабочая среда отделена от физического устройства пользователя и размещена в защищённом центре обработки данных предприятия. В банковском секторе подсистема VDI занимает положение фасада корпоративного ИТ-ландшафта: через неё сотрудники получают доступ к банковским прикладным системам, электронной почте, средствам криптографии и внешним государственным сервисам.

Актуальность задачи миграции подсистемы VDI банка на импортонезависимое программное обеспечение обусловлена прекращением поставки обновлений безопасности и технической поддержки платформы Citrix Virtual Apps and Desktops в Российской Федерации с марта 2022 года [1] и требованиями Федерального закона № 187-ФЗ [2], Приказов ФСТЭК России № 239 и № 17 [3], стандарта Банка России ГОСТ Р 57580.1-2017 [4] и Указа Президента Российской Федерации от 30.03.2022 № 166 [5], делающих использование зарубежного VDI-стека на значимых объектах критической информационной инфраструктуры юридически недопустимым. В открытых источниках [6, 7] рассматриваются отдельные архитектурные аспекты VDI на открытых программных продуктах, однако законченная отраслевая методика миграции, учитывающая Windows-зависимые банковские приложения и работу со средствами криптографической защиты, не представлена.

Цель настоящей статьи — представить архитектурно-технический комплекс и методику миграции подсистемы VDI банка на импортонезависимое программное обеспечение, а также формальную модель оценки результата, обеспечивающую строгую и проверяемую процедуру приёмки перехода. Для достижения цели необходимо: определить состав целевого программного стека и обходные решения для Windows-зависимых приложений; описать этапы миграции и правило принятия решения по каждому пользователю; предложить систему частных метрик и интегральный показатель эффективности перехода.

Методы и исследования

Методической основой исследования выступает архитектурная декомпозиция целевой подсистемы по модели C4 [8]. Подход позволяет описать VDI-подсистему на трёх уровнях детализации: внешние потребители и системы (System Context); внутренние контейнеры (Container); отдельные компоненты внутри контейнеров (Component). Второе методическое основание — инженерный сравнительный анализ отечественных программных продуктов по совокупности критериев: включение в Единый реестр российских программ [9], действующий сертификат ФСТЭК России, функциональная эквивалентность замещаемой платформе Citrix, техническая совместимость с уже развёрнутой у банка инфраструктурой виртуализации и службой каталогов.

Для определения весовых коэффициентов интегрального показателя эффективности перехода применён метод прямого экспертного оценивания (Direct Rating) [10]. Метод прозрачен и проверяем; в отличие от метода анализа иерархий Т. Саати [11] с попарными сравнениями, не требует проверки индекса согласованности, что критично при малой экспертной группе. Организационной основой миграции пользователей выступает поэтапная процедура перехода с параллельной работой в исходной и целевой средах в переходный период; правило принятия решения по каждому пользователю формализуется через коэффициент функциональной эквивалентности, рассчитываемый по чек-листу приёмочного тестирования.

Результаты оригинального авторского исследования

В результате исследования разработан архитектурно-технический комплекс целевой подсистемы VDI на импортонезависимом стеке из четырёх программных компонентов. Платформа Termidesk образует управляющий уровень: Universal Dispatcher выполняет брокеринг сессий с LDAP-интеграцией с ALD Pro, Termidesk Gateway обеспечивает TLS-терминирование и многофакторную аутентификацию, менеджер рабочих мест отвечает за жизненный цикл виртуальных рабочих мест (BPM). Операционная система Astra Linux Special Edition уровня защищённости «Смоленск» устанавливается на BPM и клиентском оборудовании; тонкие клиенты работают в режиме графического киоска, что снижает поверхность атаки. Служба каталогов ALD Pro на связке FreeIPA, SSSD и Samba-DC обеспечивает функциональную эквивалентность Microsoft Active Directory.

Система виртуализации zVirt на базе oVirt предоставляет гипервизор для пула BPM с управлением через REST API и стандартный модуль Ansible ovirt.ovirt.ovirt_vm.

Принципиальным инженерным решением архитектурного комплекса является вынос Windows-зависимых банковских приложений (программного комплекса ЦФТ Навигатор, торговой системы Финмаркет, документов с легаси-макросами Excel, средств криптографии КриптоПро и КриптоАРМ) в RDS-ферму на zVirt под управлением Microsoft Windows Server, введённую в исходный домен Active Directory. Доступ пользователя к Windows-приложениям выполняется из целевого BPM через клиент xfreerdp с диалогом на утилите zenity. RDS-ферма определяется как переходное обходное решение с траекторией постепенного отказа; в эксплуатационный контур целевой VDI-подсистемы она не входит. Инфраструктура автоматизации сопровождения реализована в парадигме Infrastructure-as-Code [12]: массовые административные операции оформлены в виде Ansible-плейбуков с параметризацией через YAML-инвентаризацию.

Разработанная методика миграции пользователей включает пять последовательных этапов: пилот (10–20 сотрудников, функциональная проверка BPM-образа и групповых политик ALD Pro); доработка требований и технических решений по итогам пилота; фокус-группы (до 50 пользователей разных подразделений с отработкой обходных решений для Windows-зависимых приложений); опытно-промышленная эксплуатация (массовая замена клиентского оборудования на гибридный образ ALSE, накопление статистики целевых метрик); промышленная эксплуатация (миграция оставшихся пользователей и перевод корпоративной почты с Outlook на RuPost).

На каждом этапе миграция отдельного пользователя проходит через приёмочное тестирование по чек-листу из 22 проверок, сгруппированных в пять тематических разделов (базовые сервисы; прикладное программное обеспечение; работа с криптосредствами; печать и файловые сервисы; средства коммуникации). Результат каждой проверки r_i принимает значения из множества {0; 0,5; 1} — «не пройдено», «пройдено с замечаниями», «пройдено успешно»; веса критичности w_i устанавливаются владельцами бизнес-процессов банка по шкале [5; 10]. Коэффициент функциональной эквивалентности определяется как взвешенное среднее результатов проверок (формула 1).

$$K_{\text{func}} = \frac{\sum_{i=1}^{N} w_i r_i}{\sum_{i=1}^{N} w_i} \qquad (1)$$

Пороговое условие успешной миграции пользователя — K_func(u) ≥ 0,90. При невыполнении порогового условия основным каналом работы

пользователя остаётся исходная среда Citrix, выполняется отработка неуспешных проверок и повторное приёмочное тестирование.

Формальная модель оценки результата работы построена на шести частных метриках: коэффициент функциональной эквивалентности K_func; коэффициент сокращения трудоёмкости администрирования K_adm; коэффициент импортонезависимости K_imp; коэффициент покрытия обязательных требований информационной безопасности K_sec; доля успешных миграций без отката P_success; пользовательская удовлетворённость CSAT. Частные метрики сворачиваются в интегральный показатель эффективности перехода линейной комбинацией с весами, определёнными методом Direct Rating (формула 2).

$$E_{\text{total}} = \alpha K_{\text{func}} + \beta K_{\text{adm}} + \gamma K_{\text{imp}} + \delta K_{\text{sec}} + \varepsilon P_{\text{success}} + \zeta \text{CSAT}_{\text{norm}} \quad (2)$$

где α, β, γ, δ, ε, ζ □ [0; 1] — весовые коэффициенты, удовлетворяющие условию нормировки α + β + γ + δ + ε + ζ = 1. Линейная свёртка предпочтительна перед мультипликативной, поскольку не приводит к обнулению интегрального показателя при нулевом значении одной из частных метрик и допускает содержательную интерпретацию весов заказчиком. Целевое значение интегрального показателя: E_total ≥ 0,90.

Апробация разработанных комплекса, методики и модели оценки проведена на пилотной фокус-группе пользователей одного из российских банков — субъектов критической информационной инфраструктуры. Все частные метрики достигли целевых значений; полученное значение интегрального показателя превысило пороговое, что подтвердило работоспособность предложенных решений.

Заключение

В статье представлены архитектурно-технический комплекс и методика миграции подсистемы виртуальных рабочих столов банка на импортонезависимое программное обеспечение. Целевая подсистема построена на стеке Termidesk, ОС Astra Linux Special Edition, ALD Pro и zVirt; для Windows-зависимых банковских приложений предложено переходное обходное решение на основе RDS-фермы с доступом из целевого BPM. Разработанная методика миграции включает пять этапов и обеспечивает параллельную работу пользователя в исходной и целевой средах в переходный период. Формальная модель оценки результата построена на шести частных метриках и интегральном показателе, весовые коэффициенты которого определены методом прямого экспертного оценивания.

Практическая значимость результатов состоит в возможности тиражирования архитектурного комплекса и методики миграции на другие банки со сходной ИТ-инфраструктурой. Дальнейшее развитие модели может

быть связано с формализацией шаблонов прикладных сценариев автоматизации сопровождения, постепенным отказом от RDS-сегмента по мере появления функциональных аналогов прикладного программного обеспечения для операционных систем на ядре Linux и оценкой совокупной стоимости владения перехода.

Использованные источники:

1. Citrix suspends business in Russia and Belarus [Электронный ресурс] // Citrix Systems, Inc. Newsroom. – URL: https://www.citrix.com/news/announcements/ (дата обращения: 10.06.2026).
2. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 № 187-ФЗ // Собрание законодательства Российской Федерации. – 2017. – № 31. – Ст. 4736.
3. Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: Приказ ФСТЭК России от 25.12.2017 № 239 [Электронный ресурс] // Официальный интернет-портал правовой информации. – URL: http://publication.pravo.gov.ru (дата обращения: 10.06.2026).
4. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. – Москва: Стандартинформ, 2018. – 41 с.
5. О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации: Указ Президента Российской Федерации от 30.03.2022 № 166 // Собрание законодательства Российской Федерации. – 2022. – № 14. – Ст. 2242.
6. Двоеглазов Д.В., Дешко И.П., Кряженков К.Г., Тихонов А.А. Инфраструктура виртуальных рабочих столов на открытых программных продуктах [Электронный ресурс] // Вестник Евразийской науки. – 2015. – № 4 (29). – URL: https://cyberleninka.ru/article/n/infrastruktura-virtualnyh-rabochih-stolov-na-otkrytyh-programmnyh-produktah (дата обращения: 10.06.2026).
7. Проскурин Д.К., Маковий К.А. Задача выбора серверных ресурсов для внедрения инфраструктуры виртуальных рабочих столов // Вестник Воронежского государственного технического университета. – 2017. – Т. 13, № 4. – С. 43–49.
8. Brown S. The C4 model for visualising software architecture [Электронный ресурс]. – URL: https://c4model.com/ (дата обращения: 10.06.2026).
9. Единый реестр российских программ для электронных вычислительных машин и баз данных [Электронный ресурс]. – URL: https://reestr.digital.gov.ru/ (дата обращения: 10.06.2026).
10. Bottomley A., Jacoby A., Griffiths P. et al. Choosing the right approach to assigning weights in multi-attribute decision making: A comparison of direct rating and analytic hierarchy process // Journal of the Operational Research Society. – 2000. – Vol. 51, № 3. – P. 275–284.

11. Саати Т. Принятие решений. Метод анализа иерархий. – Москва: Радио и связь, 1993. – 278 с.
12. Alonso J., Piliszek R., Cankar M. Embracing IaC Through the DevSecOps Philosophy: Concepts, Challenges, and a Reference Framework // IEEE Software. – 2023. – Vol. 40, № 1. – P. 56–62.

УДК 004.056.5:37.018.43

Минасян Т. А.
студент, направления 01.03.02 «Прикладная математика и информатика»,
институт компьютерных наук и технологий
ПГНИУ
Мушкалов Е. А.
студент, направления 01.03.02 «Прикладная математика и информатика»,
институт компьютерных наук и технологий
ПГНИУ
Россия, г. Пермь

АРХИТЕКТУРА И АЛГОРИТМЫ МНОГОУРОВНЕВОЙ СИСТЕМЫ БЕЗОПАСНОЙ ПРОВЕРКИ ПРОГРАММНЫХ РЕШЕНИЙ ДЛЯ ОБРАЗОВАТЕЛЬНЫХ ОНЛАЙН-ПЛАТФОРМ

Аннотация: *в статье рассматривается задача безопасной автоматизированной проверки программных решений в образовательных онлайн-платформах. Показано, что запуск пользовательского кода нельзя рассматривать как обычную серверную операцию, поскольку такой код может содержать ошибки, бесконечные циклы, попытки доступа к файловой системе или намеренно опасные конструкции. Предложена многоуровневая архитектура, в которой основной сервер платформы отделен от контура выполнения, а проверка переносится в изолированный runner-узел с очередью задач, одноразовой средой запуска и ограничениями ресурсов. Результатом работы является модель угроз, алгоритм обработки решения и набор проектных мер, позволяющих снизить риск компрометации основной системы без отказа от интерактивной проверки заданий.*

Ключевые слова: *образовательная платформа, автоматическая проверка кода, песочница, Docker, gVisor, runner-сервер, модель угроз.*

Minasyan T. A.
student, applied mathematics and computer science
institute of computer science and technology
Perm State University
Mushkalov E. A.
student, applied mathematics and computer science
institute of computer science and technology
Perm State University
Russia, Perm

ARCHITECTURE AND ALGORITHMS OF A MULTI-LEVEL SYSTEM FOR SECURE PROGRAMMING SOLUTION ASSESSMENT IN EDUCATIONAL ONLINE PLATFORMS

Abstract: *the article examines the problem of secure automated assessment of programming solutions in educational online platforms. It is shown that user code execution cannot be treated as a regular server-side operation, because submitted code may contain errors, infinite loops, attempts to access the file system, or intentionally dangerous constructs. A multi-level architecture is proposed in which the main platform server is separated from the execution contour, while checking is moved to an isolated runner node with a task queue, disposable runtime environment, and resource limits. The result of the study is a threat model, a solution processing algorithm, and a set of design measures that reduce the risk of compromising the core system without abandoning interactive task assessment.*

Keywords: *educational platform, automated code assessment, sandbox, Docker, gVisor, runner server, threat model.*

Введение

Автоматическая проверка программных решений стала обычной частью цифрового обучения программированию, анализу данных и машинному обучению. Студент отправляет код через браузер и почти сразу получает результат проверки. Такой сценарий дает быструю обратную связь и снижает нагрузку на преподавателя, поэтому системы автоматического оценивания давно применяются в учебных курсах [1].

Главная трудность состоит в том, что проверка требует запуска недоверенного пользовательского кода. Даже без злого умысла решение может содержать бесконечный цикл, чрезмерное потребление памяти или некорректную работу с вводом и выводом. В более жесткой модели угроз код может пытаться обратиться к файловой системе, внутренней сети, переменным окружения и системным вызовам.

Если основной сервер платформы одновременно хранит пользователей, задания, базу данных и запускает студенческий код, компрометация механизма проверки затрагивает всю систему. Поэтому безопасная проверка программных решений должна проектироваться как отдельный архитектурный контур, а не как локальная настройка интерпретатора.

Цель работы - спроектировать многоуровневую систему безопасной проверки программных решений для образовательных онлайн-платформ. Для этого выделяются основные угрозы, задаются роли компонентов, формируется алгоритм обработки решения и сопоставляются угрозы с механизмами защиты.

Методы и исследования

Методической основой выбран принцип защиты в глубину: безопасность не должна зависеть от одного барьера. Если статический

анализ пропускает опасный код, его должен ограничивать контур выполнения. Если среда запуска скомпрометирована, ущерб должен оставаться внутри runner-узла, не имеющего доступа к основной базе данных.

Процесс проверки разделяется на доверенный и недоверенный контуры. К доверенному относится основной сервер платформы: регистрация пользователей, хранение заданий, прием решений и отображение результата. К недоверенному относится выполнение кода. Этот контур выносится на отдельный runner-сервер, который получает только текст программы, язык выполнения, входные данные тестов и лимиты ресурсов.

Первым рубежом является статический анализ исходного кода. Для Python-решений он может выполняться через абстрактное синтаксическое дерево: модуль ast позволяет разбирать программный текст до запуска [2]. Так можно заранее отклонить импорт os, subprocess, socket, вызовы open, eval, exec и другие операции, не нужные учебной задаче. При этом AST-анализ остается фильтром, а не гарантией безопасности, поскольку динамические приемы языка и обфускация могут обходить простые правила.

Вторым элементом является очередь задач. Она отделяет прием решений от выполнения, сглаживает пики нагрузки и позволяет добавлять runner-узлы без изменения основного сервера. Распределенная очередь, например Celery, поддерживает асинхронную обработку, повтор задач при сбое и приоритеты для разных типов проверок [3].

Третьим элементом служит одноразовая среда запуска. Базовым вариантом может быть Docker-контейнер с лимитами CPU и памяти [4]. Однако контейнер не является полной границей безопасности, поэтому его следует дополнять seccomp-профилями [5], AppArmor или SELinux, запретом лишних capabilities, непривилегированным пользователем, read-only файловой системой и отключением сети; сходные меры приводятся и в практических рекомендациях OWASP [6]. В усиленном варианте применяются gVisor [7], Kata Containers [8] или Firecracker microVM [9], которые сильнее отделяют пользовательский код от ядра хоста.

Результаты оригинального авторского исследования

В результате проектирования предложена распределенная архитектура безопасной проверки программных решений. Ее основной принцип: сервер образовательной платформы не выполняет пользовательский код. Он принимает решение, проводит предварительную проверку, сохраняет попытку и передает задачу в очередь. Выполнение переносится на runner-сервер, который не имеет прямого доступа к основной базе данных и возвращает только технический результат проверки.

Архитектура включает основной сервер платформы, очередь задач, runner-сервер и одноразовую среду запуска. Такая схема не делает выполнение недоверенного кода абсолютно безопасным, но снижает возможный ущерб: даже при успешном побеге из песочницы атакующий

оказывается не на основном сервере с пользовательскими данными, а в ограниченном контуре выполнения.

Предлагаемое разделение близко к практике специализированных систем автоматической проверки, в которых выполнение кода отделяется от пользовательского интерфейса и учебной логики. В качестве примеров таких решений можно привести Judge0 [10] и CodeRunner [11].

Рисунок 1 - Общая схема распределенной проверки программного решения

Алгоритм обработки попытки включает прием решения, AST-предпроверку, постановку задачи в очередь, запуск на runner-узле и возврат нормализованного результата. Если на этапе анализа обнаружены запрещенные конструкции, попытка отклоняется без запуска. Если проверка пройдена, runner создает новую одноразовую среду, копирует в нее код и запускает тесты под наблюдением.

Во время запуска контролируются wall-clock timeout и CPU-time limit, лимит памяти, число процессов, квота на временную файловую систему и максимальный размер stdout/stderr. После завершения проверки среда уничтожается, а основной сервер получает только статус, фрагмент вывода, сообщение об ошибке и технические метрики.

Принять решение пользователя и сохранить попытку со статусом pending.

Выполнить AST-предпроверку запрещенных импортов, вызовов и обращений.

При нарушении правил завершить попытку без запуска пользовательского кода.

При успешной предпроверке поставить задачу в очередь с тестами и лимитами.

Передать задачу runner-узлу, не имеющему доступа к основной базе данных.

Создать одноразовую среду выполнения: контейнер, gVisor-контейнер или microVM.

Запустить код под ограничениями ресурсов и времени.

Уничтожить среду выполнения и вернуть нормализованный результат.

Обновить попытку студента и сохранить признаки подозрительной активности.

Таблица 1.
Модель угроз и меры защиты

Угроза	Механизм защиты
Побег из контейнера или повышение привилегий	Непривилегированный пользователь, запрет capabilities, read-only FS, seccomp/AppArmor, gVisor или microVM.
Fork-бомба и создание множества процессов	pids limit через cgroups и жесткий таймаут на выполнение.
Исчерпание CPU или памяти	CPU quota, memory limit, отключение swap и завершение задачи при превышении лимита.
Зависание без нагрузки на процессор	Одновременное использование wall-clock timeout и CPU-time limit.
Переполнение диска или временной директории	tmpfs с квотой, запрет монтирования файлов хоста, удаление среды после каждой попытки.
Бесконечный вывод в stdout/stderr	Ограничение размера вывода и обрезка результата перед возвратом в очередь.
DoS через массовую отправку решений	Rate limiting на пользователя, приоритеты очереди, ограничение числа активных попыток.
Подмена задачи или результата	Аутентификация между сервисами, токены или mTLS, подпись сообщений.

Модель допускает постепенное внедрение. Минимальный вариант может состоять из AST-предпроверки, Docker-контейнера и ограничения числа параллельных запусков. Расширенный вариант добавляет очередь задач, отдельный runner-узел, одноразовые среды, ограничения cgroups, seccomp/AppArmor, отключение сети и мониторинг. Усиленный вариант заменяет обычный Docker runtime на gVisor или microVM-подход.

Масштабируемость достигается за счет горизонтального увеличения числа runner-узлов. Очередь скрывает от основного сервера количество исполнителей, поэтому при росте нагрузки добавляются новые workers. Для разных языков программирования можно создавать отдельные пулы, а для контрольных работ - приоритетную очередь.

Подход имеет ограничения. Docker, gVisor и microVM уменьшают риск, но не дают абсолютной гарантии безопасности. Усиленная изоляция увеличивает задержку проверки, а слишком строгие лимиты могут мешать корректным решениям. Поэтому для разных типов заданий нужны разные профили ресурсов и изоляции.

Разделение педагогической и инфраструктурной логики делает архитектуру применимой не только к курсам программирования, но и к

задачам анализа данных, машинного обучения, SQL и другим дисциплинам, где студент отправляет исполняемый фрагмент решения.

Заключение

В статье предложена архитектура многоуровневой системы безопасной проверки программных решений для образовательных онлайн-платформ. Основной результат состоит в переносе выполнения пользовательского кода из основного приложения в изолированный контур, включающий очередь задач, runner-сервер и одноразовую среду запуска.

Сформирована модель угроз, включающая побег из среды выполнения, исчерпание ресурсов, сетевые атаки из контейнера, DoS через очередь, подмену задач и утечку состояния между пользователями. Для каждой угрозы предложены меры защиты: AST-предпроверка, rate limiting, аутентификация межсервисного обмена, контейнерная или microVM-изоляция, cgroups-лимиты, ограничение stdout/stderr и запрет сетевого доступа.

Практическая ценность архитектуры заключается в ее поэтапной реализуемости. Минимальный вариант подходит для небольшой учебной платформы, а расширенный позволяет масштабировать проверку за счет дополнительных runner-узлов и приоритетных очередей. Дальнейшая работа может быть связана со сравнением Docker, gVisor и microVM в учебных сценариях.

Использованные источники

1. Ihantola P. Review of recent systems for automatic assessment of programming assignments / P. Ihantola, T. Ahoniemi, V. Karavirta, O. Seppälä // Proceedings of the 10th Koli Calling International Conference on Computing Education Research. - ACM, 2010. - P. 86-93. - DOI: 10.1145/1930464.1930480. - URL: https://researchportal.helsinki.fi/en/publications/review-of-recent-systems-for-automatic-assessment-of-programming-/ (дата обращения: 02.06.2026).
2. Ast - Abstract syntax trees [Электронный ресурс] // Python Documentation. - URL: https://docs.python.org/3/library/ast.html (дата обращения: 02.06.2026).
3. Celery - Distributed Task Queue [Электронный ресурс] // Celery Documentation. - URL: https://docs.celeryq.dev/ (дата обращения: 02.06.2026).
4. Resource constraints [Электронный ресурс] // Docker Docs. - URL: https://docs.docker.com/engine/containers/resource_constraints/ (дата обращения: 02.06.2026).
5. Seccomp security profiles for Docker [Электронный ресурс] // Docker Docs. - URL: https://docs.docker.com/engine/security/seccomp/ (дата обращения: 02.06.2026).
6. Docker Security Cheat Sheet [Электронный ресурс] // OWASP Cheat Sheet Series. - URL: https://cheatsheetseries.owasp.org/cheatsheets/Docker_Security_Cheat_Sheet.html (дата обращения: 02.06.2026).
7. What is gVisor? [Электронный ресурс] // gVisor Documentation. - URL: https://gvisor.dev/docs/ (дата обращения: 02.06.2026).

8. Kata Containers [Электронный ресурс]. - URL: https://katacontainers.io/ (дата обращения: 02.06.2026).
9. Firecracker microVMs [Электронный ресурс]. - URL: https://firecracker-microvm.github.io/ (дата обращения: 02.06.2026).
10. Judge0 CE API Docs [Электронный ресурс]. - URL: https://ce.judge0.com/ (дата обращения: 02.06.2026).
11. CodeRunner [Электронный ресурс]. - URL: https://coderunner.org.nz/ (дата обращения: 02.06.2026).

DOI 10.24412/2412-9682-2026-7133-138-142
УДК 004.8:004.738.5

Осокин К. О.
студент
Поволжский государственный технологический университет
Россия, Йошкар-Ола

ПРИМЕНЕНИЕ ЛОКАЛЬНОГО AI-МОДУЛЯ В ВЕБ-СИСТЕМЕ УПРАВЛЕНИЯ УМНЫМ ДОМОМ

Аннотация. *В статье рассматривается разработка веб-системы управления умным домом с использованием локального AI-модуля. Актуальность темы связана с ростом количества подключённых бытовых устройств и необходимостью объединения управления, телеметрии и сценарной автоматизации в единой программной среде. На основе анализа работ, посвящённых сущности умного дома и IoT-автоматизации, предложена архитектура программного прототипа. Особое внимание уделено проверке AI-рекомендаций перед их применением, поскольку интеллектуальный модуль не должен получать прямое неконтролируемое управление оборудованием.*

Ключевые слова: *умный дом, веб-приложение, автоматизация, искусственный интеллект, локальная языковая модель, телеметрия, сценарии автоматизации.*

Osokin K. O.
student
Volga State University of Technology
Russia, Yoshkar-Ola

APPLICATION OF A LOCAL AI MODULE IN A WEB-BASED SMART HOME MANAGEMENT SYSTEM

Abstract*. The article considers the development of a web-based smart home management system using a local AI module. The relevance of the topic is associated with the growing number of connected household devices and the need to combine control, telemetry and scenario-based automation in a single software environment. Based on the analysis of works devoted to the essence of smart homes and IoT automation, the architecture of a software prototype is proposed. Special attention is paid to validating AI recommendations before their application, since the intelligent module should not receive direct uncontrolled access to equipment management.*

Keywords: *smart home, web application, automation, artificial intelligence, local language model, telemetry, automation scenarios.*

Введение

Системы умного дома являются одним из наиболее наглядных направлений применения технологий Интернета вещей и автоматизации в бытовой среде. В научной литературе умный дом описывается как жилое пространство, интегрированное с сетью датчиков, интеллектуальных систем и коммуникационных технологий [Ghaffarianhoseini et al.: 2016, с. 334]. Такой подход позволяет рассматривать умный дом не только как набор отдельных устройств, но и как единую программно-аппаратную среду.

Основными эффектами от применения умных домов являются повышение комфорта, безопасности и качества жизни [Ghaffarianhoseini et al.: 2016, с. 334]. Современные IoT-системы умного дома зачастую ориентированы на удалённый контроль и мониторинг различных домашних устройств. Например, в работе A. S. Hussein описана система на основе Arduino Uno R4 Wi-Fi и приложения Blynk, позволяющая управлять освещением, вентиляторами и элементами безопасности, а также получать данные от датчиков температуры, влажности и пламени [Hussein: 2024, с. iv]. Это показывает, что базовыми функциями подобных систем являются как управление устройствами, так и сбор данных о состоянии среды.

В рамках данной статьи рассматривается иной решение: разработка веб-приложения, в котором управление устройствами, телеметрия, сценарии автоматизации и AI-рекомендации объединены в одной программной среде. Цель статьи состоит в описании подхода к построению такого прототипа и объяснении роли локального AI-модуля в системе умного дома.

Анализ исходных подходов

Исследование сущности умного дома показывает, что его развитие связано не только с техническим подключением устройств, но и с повышением удобства, безопасности, продуктивности и устойчивости жилой среды [Ghaffarianhoseini et al.: 2016, с. 335]. Следовательно, программная система управления должна быть ориентирована не только на выполнение команд, но и на более осмысленную обработку данных о состоянии дома.

В IoT-подходе большое значение имеют датчики, контроллеры и пользовательский интерфейс. В работе A. S. Hussein показано, что система умного дома может включать датчики температуры, влажности, пламени, RFID-модуль, камеру и реле для управления исполнительными устройствами [Hussein: 2024, с. 24-26]. Для программного прототипа это важно как подтверждение того, что архитектура должна учитывать разные типы устройств и разные виды данных.

Отдельно следует отметить роль интерфейса. В рассмотренной IoT-системе пользователь управляет домом через мобильное приложение, а устройство передаёт значения температуры и влажности на панель управления [Hussein: 2024, с. 26-28]. В разрабатываемом прототипе данная идея реализуется через веб-интерфейс: пользователь получает доступ к устройствам, телеметрии, сценариям и рекомендациям из одного приложения.

В итоге можно выделить список требований к разрабатываемой системе: поддержка устройств и датчиков, хранение телеметрии, наличие пользовательского интерфейса, сценарная автоматизация и возможность дальнейшего интеллектуального анализа данных.

Архитектура разработанного прототипа

Разработанный прототип представляет собой веб-приложение для управления умным домом. В его состав входят пользовательский интерфейс, серверная часть, база данных, механизм автоматизации, журнал событий и локальный AI-модуль.

Пользовательский интерфейс предназначен для работы с устройствами, просмотра телеметрии, настройки сценариев и получения рекомендаций. Серверная часть принимает запросы, выполняет проверку данных, обращается к базе данных и запускает необходимые механизмы обработки.

База данных используется для хранения сведений о пользователях, устройствах, показаниях датчиков, сценариях автоматизации и событиях системы. Это позволяет отображать текущее состояние дома и использовать накопленные данные при подготовке рекомендаций.

Механизм автоматизации отвечает за проверку условий и выполнение действий. Например, сценарий может быть связан с температурой, влажностью, освещённостью или с присутствием человека. В отличие от простого ручного управления, сценарии позволяют системе реагировать на изменения параметров среды.

Компонент	Назначение
Веб-интерфейс	Отображение устройств, телеметрии, сценариев и AI-рекомендаций.
Серверная часть	Обработка запросов, проверка данных и выполнение бизнес-логики.
База данных	Хранение пользователей, устройств, измерений, сценариев и событий.
Механизм автоматизации	Проверка условий и выполнение действий по сценариям.
AI-модуль	Анализ контекста дома и формирование рекомендаций.

Роль локального AI-модуля

Важным отличием разработанного прототипа является включение локального AI-модуля в общий контур работы приложения. Его задача состоит не в прямом управлении оборудованием, а в анализе текущего состояния дома и подготовке рекомендаций для пользователя.

Перед обращением к AI-модулю сервер формирует контекст: список устройств, их расположение, последние телеметрические значения и уже существующие сценарии. На основе этого контекста модель может предложить новый сценарий автоматизации или объяснить текущее состояние системы.

Однако результат работы модели не должен применяться автоматически. Это связано с тем, что интеллектуальный модуль может сформировать неполный или технически неприменимый сценарий. Поэтому сервер проверяет, существуют ли указанные устройства, корректны ли условия и не дублирует ли новая рекомендация уже созданное правило.

Такой подход согласуется с практическими ограничениями IoT-систем. В работе A. S. Hussein среди ограничений системы отмечаются зависимость от сети, вопросы масштабируемости, безопасности и ограниченность набора поддерживаемых функций [Hussein: 2024, с. 35]. Для AI-расширения эти ограничения также актуальны, поэтому рекомендации должны проходить дополнительный контроль.

Результаты и обсуждение

В результате был разработан программный прототип, в котором объединены управление устройствами, сбор телеметрии, сценарии автоматизации, журналирование событий и AI-рекомендации. Такой набор функций позволяет показать полный цикл работы системы: от получения данных до формирования интеллектуального предложения.

Проверка прототипа выполнялась по основным пользовательским сценариям. Тестировались добавление устройств, сохранение показаний датчиков, создание сценариев, запуск автоматизации и обработка рекомендаций. Особое внимание уделялось случаям, когда AI-модуль предлагал сценарий с отсутствующим устройством, неполными параметрами или потенциальным конфликтом.

Полученные результаты показывают, что локальный AI-модуль может быть полезен в системе умного дома как средство поддержки пользователя. При этом его применение требует серверной валидации и не должно заменять прикладную логику управления устройствами.

Заключение

На основе анализа работ, посвящённых сущности умного дома и IoT-автоматизации, был предложен подход к разработке веб-системы управления умным домом с локальным AI-модулем. В отличие от решений, ориентированных только на удалённое управление устройствами, рассматриваемый прототип объединяет управление, телеметрию, сценарии и рекомендации.

Вывод состоит в том, что искусственный интеллект стоит использовать как вспомогательный слой, а не как автономный механизм управления. AI-модуль может формировать рекомендации и черновики сценариев, но их применение должно зависеть от серверной проверки и решения пользователя.

Дальнейшее развитие системы может быть связано с расширением набора поддерживаемых устройств, анализом долгосрочной истории телеметрии и улучшением алгоритмов проверки AI-рекомендаций.

Использованные источники

1. Ghaffarianhoseini A., Ghaffarianhoseini A., Tookey J., Omrany H., Fleury A., Naismith N. The Essence of Smart Homes: Application of Intelligent Technologies towards Smarter Urban Future // Chapter 14. IGI Global. 2016. DOI: 10.4018/978-1-5225-0016-2.ch014.
2. Hussein A. S. Design and Implementation of a Smart Home Automation System Based on the Internet of Things: M.Sc. Thesis. Near East University, Department of Computer Information Systems. Nicosia, 2024. 58 p.

УДК 004.056.53

Прокофьева А. С.
студент
РГУ нефти и газа (НИУ) имени И. М. Губкина
Прокофьева М. С.
студент
РГУ нефти и газа (НИУ) имени И. М. Губкина

ОЦЕНКА ЭФФЕКТИВНОСТИ СКАНЕРОВ БЕЗОПАСНОСТИ КОНТЕЙНЕРНЫХ ОБРАЗОВ (TRIVY, CLAIR, ANCHORE) В СРЕДЕ ОС АЛЬТ ПО МЕТОДИКЕ АНАЛИЗА ЗАЩИЩЁННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ФСТЭК РОССИИ

Аннотация. *Рассмотрена задача оценки эффективности открытых сканеров безопасности контейнерных образов Trivy, Clair и Anchore (Grype + Syft) в отечественной операционной системе ОС Альт применительно к требованиям Методики анализа защищённости информационных систем, утверждённой ФСТЭК России 25 ноября 2025 г. (раздел СКО.1.4). Разработана воспроизводимая методика количественной оценки, основанная на эталонном контейнерном образе с верифицированным набором уязвимостей из Банка данных угроз безопасности информации (БДУ ФСТЭК) и международных баз CVE, а также на взвешенной интегральной оценке, учитывающей класс защищённости информационной системы по Приказу ФСТЭК России № 118. На виртуальном стенде под управлением ОС Альт проведено 18 сканирований; рассчитаны полнота (Recall), точность (Precision), производительность и доля выявленных уязвимостей из БДУ ФСТЭК. Установлено, что Trivy обеспечивает наилучшее сочетание полноты обнаружения (Recall = 87,5 %), приемлемой точности (Precision = 77,8 %) и минимального времени сканирования (8,2 с) и является единственным из рассмотренных инструментов со встроенной поддержкой формата OVAL и БДУ ФСТЭК, что соответствует пороговому требованию раздела СКО.1.4.*

Clair занимает промежуточное положение, а Grype непригоден для образов ОС Альт без доработки баз уязвимостей. Сформулированы рекомендации и матрица выбора сканера в зависимости от класса защищённости информационной системы.

Ключевые слова: *контейнерная безопасность; сканер уязвимостей; Trivy; Clair; Anchore; ОС Альт; Podman; ФСТЭК России; БДУ ФСТЭК; СКО.1.4; OVAL; полнота обнаружения; точность.*

Prokofieva A.S.
student
Gubkin Russian State University of Oil and Gas
Prokofieva M. S.
student
Gubkin Russian State University of Oil and Gas

EVALUATION OF THE EFFECTIVENESS OF CONTAINER IMAGE SECURITY SCANNERS (TRIVY, CLAIR, ANCHORE) IN THE ALT OS ENVIRONMENT ACCORDING TO THE FSTEC INFORMATION SYSTEM SECURITY ANALYSIS METHODOLOGY

Abstract. *The paper addresses the evaluation of the effectiveness of open-source container image security scanners Trivy, Clair and Anchore (Grype + Syft) within the Russian ALT operating system, with respect to the requirements of the Information System Security Analysis Methodology approved by FSTEC of Russia on 25 November 2025 (section SCO.1.4). A reproducible quantitative assessment methodology is proposed; it relies on a reference container image with a verified set of vulnerabilities from the Russian Data Security Threats Database (BDU FSTEC) and international CVE databases, and on a weighted integral score that accounts for the protection class of the information system. On a virtual test bench running ALT OS, 18 scans were performed; recall, precision, performance and the share of detected BDU FSTEC vulnerabilities were calculated. Trivy is shown to provide the best balance of detection completeness (Recall = 87.5 %), acceptable precision (77.8 %) and minimal scanning time (8.2 s), and is the only tool with built-in OVAL/BDU FSTEC support, meeting the SCO.1.4 threshold. Recommendations and a scanner-selection matrix by protection class are formulated.*

Keywords: *container security; vulnerability scanner; Trivy; Clair; Anchore; ALT OS; Podman; FSTEC of Russia; BDU FSTEC; SCO.1.4; OVAL; recall; precision.*

ВВЕДЕНИЕ

В условиях активного импортозамещения информационных технологий и перехода государственных и критически важных информационных систем (ИС) Российской Федерации на отечественное программное обеспечение существенно возрастает роль средств контейнеризации. Контейнерные технологии (Docker, Podman, Kubernetes и их аналоги) обеспечивают высокую масштабируемость, портативность и скорость развёртывания приложений, однако одновременно расширяют поверхность атаки за счёт уязвимостей в образах контейнеров, ошибок конфигурации среды выполнения и отсутствия контроля зависимостей [27; 28]. Областью настоящего исследования является обеспечение информационной безопасности контейнерных сред в отечественных операционных системах, в

которую предполагается привнести новое прикладное знание о применимости открытых средств анализа защищённости.

Систематизация рисков и уязвимостей контейнеров выполнена в обзоре [28], где предложена их таксономия по фазам жизненного цикла (образ, хост, межконтейнерное взаимодействие, сеть и оркестрация, среда выполнения). В руководстве NIST SP 800-190 образы контейнеров выделены как один из наиболее частых векторов компрометации [27]. Вопросы контейнерной безопасности и классификации угроз на этапе развёртывания образов рассматривались в отечественных работах [5; 18], а сравнительный анализ сканеров уязвимостей в условиях импортозамещения – в работах [3; 16; 17]. Нормативную основу формируют требования ФСТЭК России к средствам контейнеризации и к защите информации в ИС [10; 11], развитые в Методике анализа защищённости информационных систем [4].

Вместе с тем в открытых источниках отсутствуют верифицированные данные о полноте, точности и производительности популярных open-source-сканеров безопасности именно в среде ОС Альт с учётом Банка данных угроз безопасности информации (БДУ ФСТЭК). Этот пробел приобретает практическую значимость в связи со вступлением в силу Методики [4], которая впервые на нормативном уровне вводит отдельный класс работ по анализу средств контейнеризации (СКО), а подраздел СКО.1.4 прямо требует выявления образов, содержащих известные уязвимости. Отсутствие таких данных создаёт риски несоответствия результатов сканирования требованиям регулятора и появления ложных отрицательных срабатываний в аттестуемых системах. Специфика ОС Альт (использование Podman в режиме без привилегий суперпользователя, собственные репозитории, интеграция с БДУ ФСТЭК) требует отдельной адаптации инструментов, изначально ориентированных на зарубежные дистрибутивы [9; 25]. Восполнение указанного пробела и составляет предмет актуальности настоящей работы.

Объект исследования – процессы выявления уязвимостей в контейнерных образах в рамках анализа защищённости информационных систем.

Предмет исследования – открытые сканеры безопасности контейнерных образов Trivy, Clair и Anchore и методика оценки их эффективности в среде ОС Альт по требованиям ФСТЭК России.

Цель работы – оценка эффективности сканеров безопасности контейнерных образов Trivy, Clair и Anchore в операционной системе Альт по требованиям Методики анализа защищённости информационных систем ФСТЭК России. Для достижения цели поставлены следующие задачи:

проанализировать нормативно-правовую базу и методические документы ФСТЭК России в части анализа защищённости средств контейнеризации;

изучить архитектуру, возможности и особенности работы сканеров Trivy, Clair и Anchore, а также критерии оценки их эффективности;

разработать методику и тестовую среду для сравнительного анализа сканеров в ОС Альт с опорой на БДУ ФСТЭК;

выполнить экспериментальное сканирование контейнерных образов и проанализировать результаты по метрикам полноты, точности, производительности и соответствия требованиям раздела СКО.1.4.

Научная новизна работы заключается в разработке методики адаптивной оценки сканеров безопасности контейнерных образов в условиях импортозамещения, учитывающей требования ФСТЭК России к средствам контейнеризации. В отличие от известных сравнительных исследований, методика основана на эталонном тестовом образе с верифицированным набором уязвимостей из БДУ ФСТЭК, использует формализованные критерии соответствия разделу СКО.1.4 и допускает варьирование весовых коэффициентов в зависимости от класса защищённости информационной системы.

Для сравнительного анализа отобраны три открытых сканера, представляющих различные архитектурные подходы: монолитный (Trivy), микросервисный (Clair) и SBOM-ориентированный (Anchore в открытой реализации Grype + Syft). Коммерческие и облачные инструменты (Docker Scout, Snyk) исключены как недопустимые для изолированных защищённых ИС; Dependency-Track ориентирован на анализ зависимостей приложений, а не на послойное сканирование образов; Docker Bench Security проверяет лишь конфигурацию хоста. Все отобранные инструменты распространяются по открытым лицензиям и развёртываются в изолированной среде ОС Альт без доступа к внешним сетям.

ЛИТЕРАТУРНЫЙ ОБЗОР

Контейнер – изолированная исполняемая единица, разделяющая ядро хостовой ОС; образ контейнера – неизменяемый послойный шаблон, из которого создаётся контейнер. Сканер безопасности образов – средство статического анализа, сопоставляющее программные компоненты образа с базами уязвимостей. СКО – класс работ по анализу средств контейнеризации в Методике [4]; БДУ ФСТЭК – Банк данных угроз безопасности информации; OVAL – открытый формат описания уязвимостей, используемый для интеграции с БДУ; SBOM – реестр программных компонентов образа. Полнота (Recall) и точность (Precision) – метрики качества обнаружения, определяемые ниже формулами (1)–(2).

Контейнерные технологии повышают эффективность ИС за счёт низких накладных расходов и высокой плотности размещения, однако совместное использование ядра хоста формирует общую поверхность атаки. По данным исследований, контейнеризация снижает потребление ресурсов по сравнению с виртуальными машинами на 50–70 % [18; 27], но привносит риски уязвимых образов, привилегированного запуска, слабой сетевой изоляции и недостаточной защиты среды выполнения [28]. Сопоставление преимуществ и рисков приведено в таблице 1.

Таблица 1.
Преимущества и риски контейнерных технологий

Аспект	Преимущества	Риски и угрозы безопасности
Ресурсы и производительность	Низкие накладные расходы, высокая плотность размещения	Общий доступ к ядру хоста, атаки на cgroups
Портативность и изоляция	Единое окружение dev/test/prod	Выход за пределы контейнера, привилегированный доступ
Масштабируемость	Быстрое развёртывание микросервисов	Распространение угроз через оркестратор
Безопасность по умолчанию	Возможность неизменяемой инфраструктуры	Уязвимые образы, секреты в открытом виде

Нормативно-правовая база безопасности средств контейнеризации в Российской Федерации опирается на Федеральный закон № 149-ФЗ [15] и специализированные документы ФСТЭК России. Приказ ФСТЭК России от 04.07.2022 № 118 устанавливает требования к средствам контейнеризации и вводит шесть классов защиты [11], а Приказ от 11.04.2025 № 117 распространяет процессный подход к защите информации на широкий круг

ИС, включая их контейнерные компоненты [10]. Ключевым методическим документом является Методика анализа защищённости информационных систем [4; 6; 7], выделяющая этапы внешнего (С1) и внутреннего (С2) анализа и отдельный класс работ СКО. Дифференциация требований по классам защиты обобщена в таблице 2.

Таблица 2.
Требования по классам защиты и уровню доверия средств контейнеризации

Класс защиты	Уровень доверия	Основные требования (примеры)
1 (высший)	1	Полный набор мер, включая сертифицированные средства обнаружения уязвимостей образов, строгая изоляция, аудит всех событий
2–3	2–3	Расширенный контроль целостности и конфигурации, обязательное сканирование образов перед развёртыванием
4–6 (низший)	4–6	Базовые меры (идентификация, регистрация событий), хостовая ОС соответствующего класса

Подраздел СКО.1.4 является центральным для оценки сканеров: он обязывает выявлять образы, содержащие известные уязвимости ПО в соответствии с БДУ ФСТЭК. Формально требование считается выполненным, если средство сканирования обеспечивает выявление не менее 80 % известных уязвимостей по идентификаторам БДУ (Recall ≥ 0,8), позволяет фильтровать результаты по записям БДУ и документировать

дефекты с привязкой к идентификаторам угроз. Пороговое значение устанавливается оператором с учётом класса защищённости и может ужесточаться [4].

Операционная система семейства ОС Альт реализует контейнеризацию преимущественно на базе Podman, работающего без привилегированного демона и в режиме без привилегий суперпользователя (rootless), что соответствует принципу минимальных привилегий Приказа № 118 [11; 25]. ОС Альт предоставляет официальный реестр образов registry.altlinux.org, а в состав дистрибутива включён сканер Trivy с поддержкой формата OVAL для интеграции с БДУ ФСТЭК; в релизе «Альт СП 10» реализован встроенный механизм проверки образов по базам CVE и БДУ с блокировкой запуска скомпрометированных образов [8; 9; 2]. Ключевые особенности платформы обобщены в таблице 3.

Таблица 3.
Особенности реализации контейнеризации и сканирования уязвимостей в ОС Альт

Аспект	Реализация в ОС Альт	Преимущества для безопасности
Менеджер контейнеров	Podman (без привилегированного демона)	Минимизация эскалации привилегий (Приказ № 118)
Режим работы	Непривилегированный (rootless), subuid/subgid	Изоляция процессов, принцип минимальных привилегий
Реестр образов	Официальный registry.altlinux.org	Контроль поставки и совместимость образов
Сканер уязвимостей	Trivy + встроенный механизм (CVE + БДУ)	Покрытие требований СКО.1.4, поддержка OVAL
Дополнительные меры	Проверка целостности с блокировкой образов	Предотвращение эксплуатации уязвимых образов

Trivy – открытый универсальный сканер компании Aqua Security, написанный на Go и распространяемый единым статическим бинарным файлом. Имеет монолитную модульную архитектуру (CLI, модули сканеров, базы Trivy DB, детекторы, репортер) и выполняет статический анализ образов без их запуска [20; 29; 30; 31]. Принцип работы Trivy показан на рисунке 1.

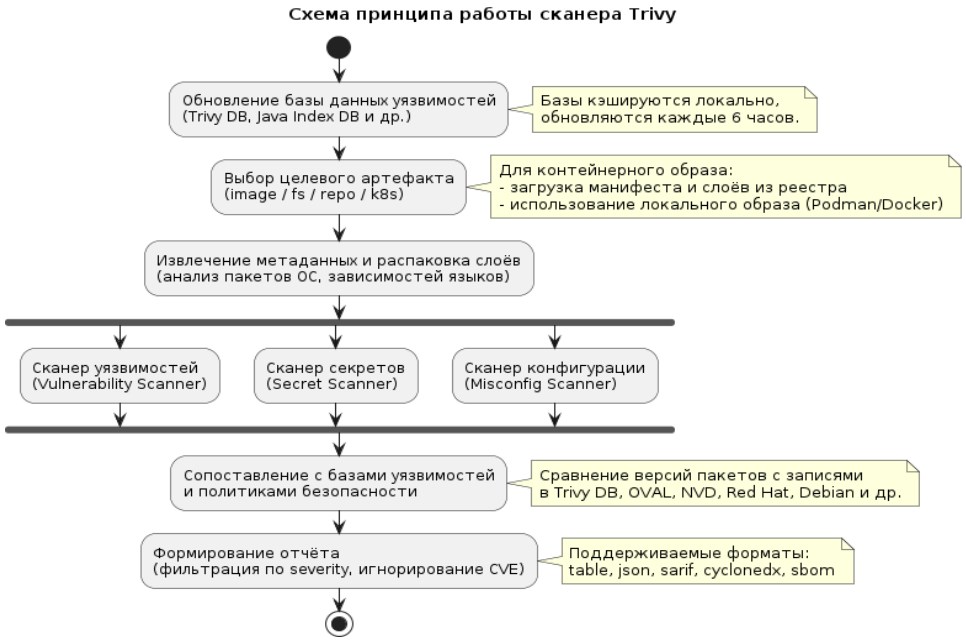

Рисунок 1 – Архитектура и принцип работы сканера Trivy (выполнено автором с использованием PlantUML)

Clair – открытый сканер уязвимостей контейнерных образов (CoreOS / Red Hat, проект Quay), построенный по микросервисной архитектуре на основе библиотеки ClairCore. Ключевые компоненты – Indexer, Matcher, Updater, API-сервер и PostgreSQL; процесс работы делится на индексацию, сопоставление и уведомление [22; 23; 24; 32]. Архитектура Clair приведена на рисунке 2.

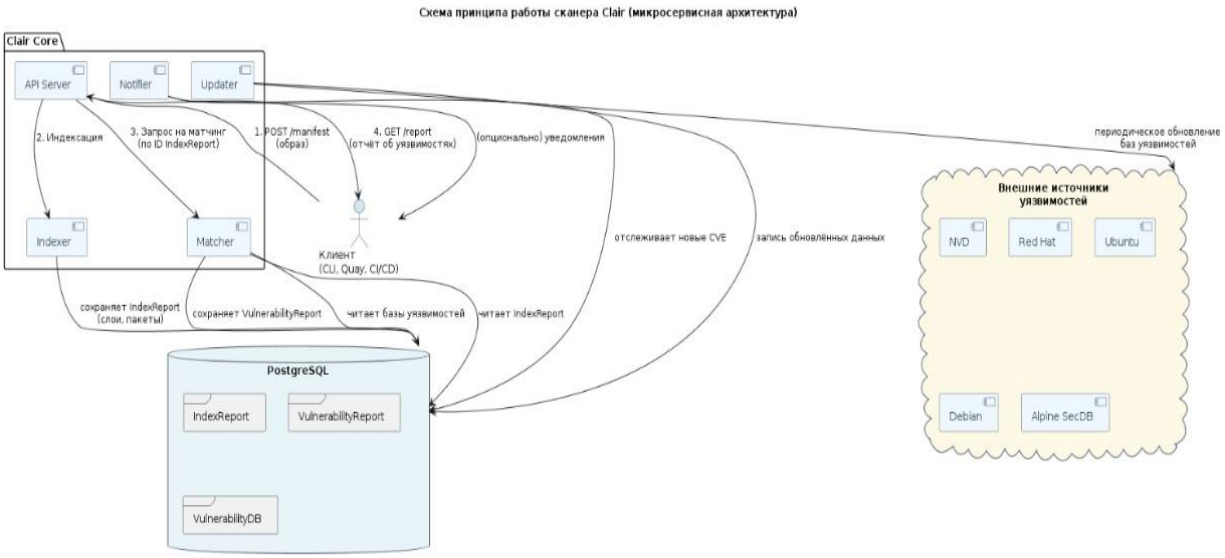

Рисунок 2 – Архитектура и принцип работы сканера Clair (выполнено автором с использованием PlantUML)

Anchore в открытой реализации представлен компонентами Syft (каталогизатор, формирующий SBOM) и Grype (движок сопоставления уязвимостей) и реализует SBOM-first-подход с политико-ориентированной оценкой рисков [19; 21]. Схема работы Anchore приведена на рисунке 3.

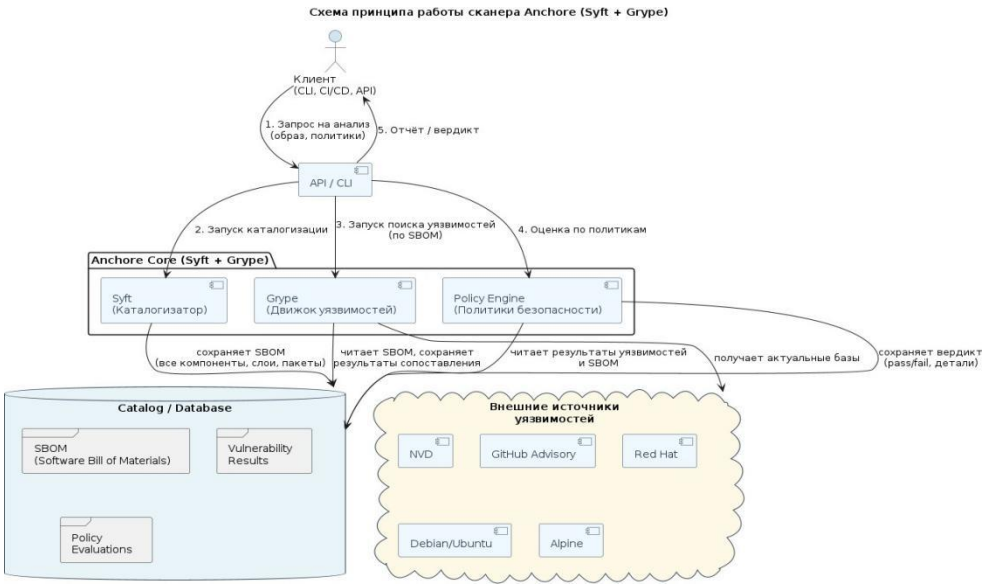

Рисунок 3 – Архитектура и принцип работы сканера Anchore (Syft + Grype) (выполнено автором с использованием PlantUML)

Сопоставление функциональных возможностей сканеров, поддерживаемых баз уязвимостей, форматов образов и интеграций приведено в таблице 4. Особое внимание уделено поддержке ОС Альт, БДУ ФСТЭК и соответствию разделу СКО.1.4.

Таблица 4.

Сравнительный анализ функциональных возможностей сканеров

Характеристика	Trivy	Clair	Anchore
Архитектура	Монолитная (standalone / client-server)	Микросервисная (Indexer + Matcher)	Модульная (SBOM-first: Syft → Grype)
Поддержка rootless / Podman	Полная, нативная	Полная	Полная
Поддержка ОС Альт / registry.altlinux.org	Полная (в репозиториях)	Ручная настройка	Ручная настройка
Поддержка БДУ ФСТЭК (OVAL)	Да, встроенная	Нет	Нет
Генерация SBOM	Да (CycloneDX, SPDX)	Нет	Да (подробный)
Поиск секретов	Да	Нет	Да
Оценка по политикам	Базовая	Отсутствует	Расширенная, гибкая

Соответствие СКО.1.4 Методики ФСТЭК	Высокое	Среднее	Высокое*

* при отсутствии встроенной поддержки БДУ ФСТЭК. Trivy выделяется простотой развёртывания, нативной поддержкой ОС Альт и прямой интеграцией с БДУ ФСТЭК; Clair выигрывает в крупных enterprise-окружениях с Quay, но уступает по гибкости; Anchore обеспечивает наибольшую глубину анализа за счёт SBOM и политик, но не имеет встроенной поддержки БДУ.

Оценка эффективности проводится по пяти критериям: полнота обнаружения (Recall), точность (Precision), уровень ложных срабатываний, производительность и поддержка БДУ ФСТЭК (таблица 5). Расчётные метрики определяются формулами (1)–(3):

Таблица 5.

Критерии и метрики оценки эффективности сканеров

Критерий	Метрика	Формула / ед. измерения
Полнота обнаружения	Recall	TP / (TP + FN) × 100 %
Точность	Precision	TP / (TP + FP) × 100 %
Ложные срабатывания	FP per image, FPR	FP / (TP + FP) × 100 %
Производительность	Время, CPU, RAM	с, %, МБ
Покрытие БДУ ФСТЭК	Доля выявленных уязвимостей БДУ	%

$$Recall = TP / (TP + FN) \times 100\ \% \quad (1)$$

$$Precision = TP / (TP + FP) \times 100\ \% \quad (2)$$

$$FPR = FP / (TP + FP) \times 100\ \% \quad (3)$$

где TP – истинно положительные (верно обнаруженные уязвимости), FP – ложные положительные, FN – ложные отрицательные (пропущенные) результаты. Для систем различных классов защищённости вводится взвешенная интегральная оценка эффективности (4):

$$E = w1 \cdot Recall + w2 \cdot Precision + w3 \cdot БДУ + w4 \cdot V_{норм} \quad (4)$$

$$V_{норм} = (t_{max} - t) / (t_{max} - t_{min}) \quad (5)$$

где t – время сканирования оцениваемого инструмента, t_{min} и t_{max} – минимальное и максимальное время среди сравниваемых сканеров. Весовые коэффициенты w1…w4 определяются классом защищённости ИС: для высших классов (1–2) приоритетны полнота и поддержка БДУ ($w1 = 0,4$; $w3 = 0,3$; $w2 = 0,2$; $w4 = 0,1$); для низших (4–6) повышается значимость производительности. Приведённые значения получены экспертным методом и согласуются с подходом [12]; допускается их корректировка под конкретную модель угроз.

Гипотезы исследования. На основе анализа сформулированы три гипотезы. H1: в среде ОС Альт пороговое требование СКО.1.4 (Recall ≥ 0,8) выполняется сканером Trivy и не выполняется сканерами Grype и Clair. H2: только Trivy обладает встроенной поддержкой формата OVAL и БДУ ФСТЭК

и обеспечивает 100 % покрытие подмножества уязвимостей БДУ эталонного образа. H3: ранжирование сканеров по полноте обнаружения устойчиво (Trivy > Clair > Grype) и воспроизводится во всех прогонах.

МЕТОДЫ ИССЛЕДОВАНИЯ

Тип исследования – экспериментальное сравнительное, проводимое на цифровом двойнике инфраструктуры [14], что обеспечивает изоляцию и воспроизводимость конфигураций. Исследование сочетает количественную оценку (метрики Recall, Precision, FPR, производительность) и качественный анализ соответствия нормативным требованиям.

Характеристика выборки. В качестве объектов сканирования использованы базовые образы alt:p10 и nginx:latest, а также эталонный образ vulnerable-test:latest с заранее известным набором из 8 уязвимостей (ground truth), сформированным на базе alt:p10 путём установки устаревших версий пакетов. Перечень эталонных уязвимостей приведён в таблице 6. Каждое сканирование повторялось трижды (n = 3); общий объём эксперимента составил 3 сканера × 2 образа × 3 повторения = 18 сканирований.

Таблица 6.

Перечень уязвимостей эталонного образа vulnerable-test:latest

Пакет	Версия	Уязвимости	Кол-во
curl	7.71.0-alt1	CVE-2020-8231, CVE-2020-8284, CVE-2020-8285	3
openssl	1.1.1k-alt1	CVE-2021-23840, CVE-2021-23841, БДУ-2021-04567	3
libxml2	2.9.7-alt1	CVE-2019-19956, CVE-2020-7595	2
Итого	–	в том числе 3 уязвимости из БДУ ФСТЭК	8

Методы сбора данных. Стенд развёрнут средствами Oracle VirtualBox под управлением ОС Альт (alt-workstation-11.1-x86_64) с характеристиками: 4 ядра (Intel Core i5-8250U), 8 ГБ ОЗУ, 50 ГБ дискового пространства, сетевой адаптер NAT. Схема стенда приведена на рисунке 4. Podman настроен в режиме rootless (активация user namespaces, диапазоны subuid/subgid, fuse-overlayfs, podman system migrate), активирован сокет Podman; права доступа к каталогам образов и логов установлены в 755, к файлам – 644.

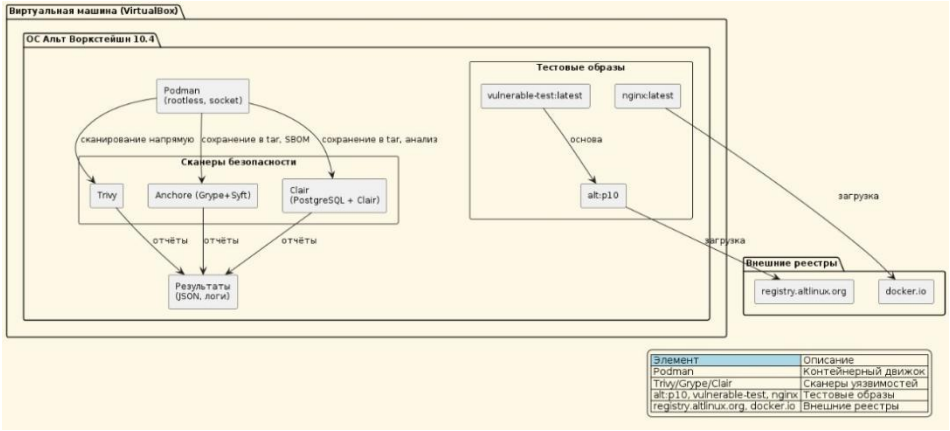

Рисунок 4 – Схема экспериментального стенда (выполнено автором с использованием PlantUML)

Установка сканеров выполнена согласно методике: Trivy установлен из официального репозитория ОС Альт (базы загружаются из российского реестра altlinux.space/trivy/trivy-db, обеспечивающего данные БДУ ФСТЭК и поддержку OVAL); Grype и Syft установлены официальными скриптами; Clair v4 развёрнут в контейнере Podman с СУБД PostgreSQL 13-alpine в изолированной сети clair-net, для управления использована утилита clairctl. Проверка показала, что Grype и Clair не имеют встроенной поддержки OVAL и БДУ ФСТЭК.

Процедура проведения исследования включает восемь последовательных этапов:

подготовка тестовой среды и проверка соответствия политикам безопасности ОС Альт;

установка и настройка сканеров Trivy, Grype + Syft и Clair, обновление баз уязвимостей;

формирование базовых образов и эталонного образа с документированным перечнем уязвимостей;

проведение сканирований всех образов каждым сканером с фиксацией времени, потребления ОЗУ и загрузки CPU; каждый эксперимент повторяется трижды;

сбор отчётов и классификация результатов эталонного образа на TP, FP и FN;

расчёт метрик эффективности (Precision, Recall) и производительности (время, RAM, CPU) с усреднением по повторениям;

оценка поддержки БДУ ФСТЭК и соответствия требованиям раздела СКО.1.4;

сравнительный анализ результатов и формирование рекомендаций.

Методы обработки данных. Воспроизводимость обеспечена скриптами автоматизации (trivy-batch.sh, grype-batch.sh, clair-batch.sh, collect-metrics.sh, run-experiments.sh); скрипт grype-batch.sh дополнительно сохраняет образ в tar-архив и генерирует SBOM средствами Syft. Метрики производительности

фиксировались утилитой /usr/bin/time и посекундным журналом загрузки CPU и ОЗУ (CSV). Классификация уязвимостей TP/FP/FN выполнена автоматизированным скриптом на языке Python путём сопоставления идентификаторов CVE/БДУ из JSON-отчётов с эталонным перечнем; для верификации проведена ручная проверка 20 % результатов каждого прогона. По итогам трёх повторений вычислены среднее арифметическое и стандартное отклонение, 95 %-ные доверительные интервалы (по t-критерию Стьюдента), а для сравнения сканеров по полноте применён непараметрический парный критерий Уилкоксона. Интегральная эффективность рассчитывается по формулам (4)–(5).

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

По итогам полного цикла экспериментов получен массив из 18 сканирований. Количество уязвимостей, выявленных каждым сканером в базовых образах, приведено в таблице 7.

Таблица 7.

Количество выявленных уязвимостей в базовых образах

Образ	Trivy	Grype (Anchore)	Clair
alt:p10	12	0	8
nginx:latest	162	162	145

Для образа alt:p10 Grype не обнаружил ни одной уязвимости, что обусловлено отсутствием в его базах данных сведений о пакетах ALT Linux; Trivy и Clair, напротив, выявили уязвимости, что подтверждает необходимость поддержки отечественных дистрибутивов. Для популярного образа nginx:latest все три сканера обнаружили более 140 уязвимостей; расхождения (162 против 145) объясняются различиями в используемых базах и алгоритмах сопоставления.

Классификация результатов сканирования эталонного образа vulnerable-test:latest (8 известных уязвимостей) приведена в таблице 8.

Таблица 8.

Классификация результатов сканирования эталонного образа

Сканер	TP (из 8)	FP	FN
Trivy	7	2	1
Grype (Anchore)	3	0	5
Clair	6	1	2

На основе данных таблицы 8 по формулам (1)–(2) рассчитаны метрики полноты и точности (таблица 9).

Таблица 9.
Метрики эффективности сканеров

Сканер	Precision, %	Recall, %
Trivy	77,8	87,5
Grype (Anchore)	100,0	37,5
Clair	85,7	75,0

Trivy демонстрирует наилучшую полноту (Recall = 87,5 %), обнаружив 7 из 8 уязвимостей при точности 77,8 % (два ложных срабатывания) и единственным превышает пороговое значение СКО.1.4. Grype показывает абсолютную точность (100,0 %) при крайне низкой полноте (37,5 %), что делает его непригодным для образов ОС Альт без доработки баз. Clair занимает промежуточное положение (Recall = 75,0 %, Precision = 85,7 %).

Рассчитаны 95 %-ные доверительные интервалы (t-критерий Стьюдента, n = 3). Для Trivy: Recall – [84,5 %; 90,5 %] (среднее 87,5 %, SD = 1,0 %), Precision – [72,1 %; 83,5 %]; для Clair: Recall – [70,8 %; 79,2 %], Precision – [82,1

%; 89,3 %]. По парному критерию Уилкоксона различия между Trivy и Grype по полноте статистически значимы ($p < 0,05$); между Trivy и Clair значимость не достигается из-за ограниченного объёма выборки, однако направление различий устойчиво. Показатели производительности приведены в таблице 10.

Таблица 10.
Метрики производительности сканеров (среднее по 3 прогонам)

Сканер	Время, с	Пиковая RAM, МБ	Загрузка CPU, %
Trivy	8,2 ± 0,5	450	35
Grype (Anchore)	12,5 ± 1,2	320	28
Clair	45,3 ± 3,8	680	42

Trivy показывает наименьшее время сканирования (8,2 с) благодаря монолитной архитектуре и кэшированию баз; Grype затрачивает дополнительное время на генерацию SBOM (12,5 с); Clair является самым медленным (45,3 с) из-за индексации и сопоставления в PostgreSQL. Критически важная для аттестуемых ИС поддержка БДУ ФСТЭК обобщена в таблице 11.

Таблица 11.
Поддержка БДУ ФСТЭК

Сканер	Поддержка OVAL	Поддержка БДУ ФСТЭК	Доля уязвимостей БДУ
Trivy	Да (встроенная)	100 %	3 из 3 (100 %)
Grype (Anchore)	Нет	0 %	0 из 3 (0 %)
Clair	Да (заруб. дистрибутивы)	0 %	0 из 3 (0 %)

Trivy – единственный из рассмотренных сканеров со встроенной поддержкой формата OVAL, что позволяет использовать БДУ ФСТЭК в качестве источника данных; в эксперименте он выявил все 3 уязвимости БДУ эталонного образа. Grype и Clair не поддерживают БДУ ФСТЭК, что ограничивает их применение в российских защищённых ИС.

Процесс сканирования формально описывается конвейером $M = D \cdot P \cdot E$, где E – извлечение из образа списка программных компонентов, P – сопоставление с базой уязвимостей с учётом дистрибутивно-зависимых исправлений (backport), D – фильтрация и ранжирование результатов. Расхождения между сканерами объясняются различным покрытием баз для ALT Linux (Trivy включает данные ALT, Grype – нет) и различиями алгоритмов сопоставления: Trivy учитывает дистрибутивный контекст, тогда как Grype работает по фиксированным CPE без адаптации к бэкпортам.

Для поддержки выбора инструмента в зависимости от класса защищённости ИС предложена матрица принятия решений (таблица 12).

Таблица 12.
Матрица принятия решений для выбора сканера

Класс ИС (Приказ № 118)	Приоритетные метрики	Рекомендованный сканер
1–2 (высший)	Полнота + поддержка БДУ ФСТЭК	Trivy
3	Баланс полноты и точности	Trivy или Clair*
4–6 (низший)	Производительность + точность	Clair или Trivy

* применение Clair требует дополнительной настройки OVAL-фидов для отечественных дистрибутивов.

Верификация методики. Воспроизводимость подтверждена низкой вариативностью результатов по трём прогонам (число найденных уязвимостей: Trivy – 7, 7, 8; Grype – 3, 3, 4; Clair – 6, 6, 7; SD ≈ 0,6). Корректность автоматической классификации TP/FP/FN подтверждена ручной проверкой 20 % результатов (полное совпадение). Соблюдены требования раздела СКО.1.4: применение отечественной ОС, проверка образов на известные уязвимости и подтверждённая работа Trivy с OVAL-фидами. Следует отметить, что объём выборки (n = 3) является малым для

строгого статистического вывода, поэтому приведённые доверительные интервалы и p-значения носят иллюстративный характер; вместе с тем направление различий (Trivy > Clair > Grype по полноте) устойчиво воспроизводится во всех прогонах.

ЗАКЛЮЧЕНИЕ

В работе разработана и апробирована воспроизводимая методика количественной оценки эффективности открытых сканеров безопасности контейнерных образов Trivy, Clair и Anchore в операционной системе Альт по требованиям Методики анализа защищённости информационных систем ФСТЭК России. На виртуальном стенде выполнены 18 сканирований; рассчитаны полнота, точность, производительность и доля выявленных уязвимостей из БДУ ФСТЭК. Главным результатом является методика адаптивной оценки, опирающаяся на эталонный образ с верифицированным набором уязвимостей и взвешенную интегральную оценку, учитывающую класс защищённости ИС.

Результаты проверки гипотез. Гипотеза H1 подтверждена частично: пороговое требование СКО.1.4 (Recall ≥ 0,8) выполнено только сканером Trivy (87,5 %), тогда как Clair (75,0 %) и Grype (37,5 %) ему не соответствуют. Гипотеза H2 подтверждена полностью: только Trivy обладает встроенной поддержкой OVAL/БДУ ФСТЭК и обеспечил 100 % покрытие подмножества уязвимостей БДУ эталонного образа. Гипотеза H3 подтверждена: ранжирование Trivy > Clair > Grype по полноте устойчиво воспроизводится во всех прогонах.

Таким образом, Trivy является наиболее сбалансированным инструментом, сочетающим высокую полноту, приемлемую точность, лучшую производительность и единственную встроенную поддержку БДУ ФСТЭК, что делает его оптимальным выбором для аттестуемых ИС. Clair применим ограниченно – в средах без строгого требования соответствия БДУ либо при интеграции дополнительных OVAL-фидов. Grype непригоден для образов ОС Альт без существенной доработки баз и оправдан лишь для зарубежных дистрибутивов при отсутствии регуляторных ограничений. Практическая значимость работы состоит в применимости методики и рекомендаций при выборе инструментов анализа защищённости средств контейнеризации в государственных и критически важных ИС; теоретическая – в формализации критериев соответствия разделу СКО.1.4.

Направления дальнейшего исследования: расширение тестового набора до нескольких десятков образов различных дистрибутивов и типов приложений с общим числом уязвимостей не менее 50–100; увеличение числа прогонов до 10–30 для получения статистически значимых выводов; разработка и подключение OVAL-фидов БДУ ФСТЭК для Clair и Grype; интеграция апробированной методики в конвейеры CI/CD аттестуемых информационных систем.

Использованные источники:

1. Лапин, В. Г. Требования по безопасности информации к средствам

контейнеризации / В. Г. Лапин, Е. А. Кеньков, М. А. Лапина, Д. А. Кужева
2. // Прикаспийский журнал: управление и высокие технологии. – 2025. – № 1 (69). – URL: https://cyberleninka.ru/article/n/trebovaniya-po-bezopasnosti-informatsii-k-sredstvam-konteynerizatsii (дата обращения: 19.05.2026). – Текст: электронный.
3. Листовка по продукту «Альт СП»: [сайт]. – URL: https://gosinform.ru/wp-content/uploads/2025/11/Листовка-по-продукту-Альт-СП.pdf (дата обращения: 24.03.2026). – Текст: электронный.
4. Меньшенин, А. Е. Комплекс мер для повышения уровня информационной безопасности с использованием сканера анализа безопасности / А. Е. Меньшенин, С. А. Стрельников // Развитие науки в XXI веке: вызовы, достижения и перспективы : сб. науч. тр. по материалам III Междунар. науч.-практ. конф., Анапа, 1 авг. 2025 г. – Анапа : НИЦ ЭСП в ЮФО, 2025. – С. 70–75. – EDN ORDWXK.
5. Методика анализа защищённости информационныхсистем : методический документ: утв. ФСТЭК России 25 нояб. 2025 г. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-25-noyabrya-2025-g (дата обращения: 24.03.2026). – Текст: электронный.
6. Молодцова, Ю. В. Классификация угроз на этапе развёртывания контейнерных образов на объектах критической информационной инфраструктуры / Ю. В. Молодцова, Д. А. Печёнов // Правовая информатика. – 2026. – № 1. – С. 52–59.
7. Обзор Методики анализа защищённости информационных систем: [сайт]. – Аттестация.ру, 2025. – URL: https://attestation.ru/article/1173/ (дата обращения: 24.03.2026). – Текст: электронный.
8. Обзор новой методики анализа защищённости ИС: [сайт]. – КСБ-Софт, 2025. – URL: https://ksb-soft.ru/blog/obzor/obzor-novoy-metodiki-analiza-zashchishchennosti-is/ (дата обращения: 24.03.2026). – Текст: электронный.
9. ОС Альт (ранее Альт Линукс, ALT Linux): [сайт] // TAdviser. – URL: https://www.tadviser.ru (дата обращения: 24.03.2026). – Текст: электронный.
10. Отечественная операционная система «Альт СП» релиз 10 отвечает новым требованиям ФСТЭК России по защите средств виртуализации и контейнеризации: [сайт] // BaseALT. – URL: https://www.basealt.ru (дата обращения: 24.03.2026). – Текст: электронный.
11. Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений: приказ ФСТЭК России от 11.04.2025 № 117: [зарегистрирован в Минюсте России 16.06.2025 № 82619]. – URL: https://fstec.ru (дата обращения: 24.03.2026). – Текст: электронный.
12. Требования по безопасности информации к средствам контейнеризации (выписка): утв. приказом ФСТЭК России от 04.07.2022 № 118 // База данных «Гарант». – URL: https://base.garant.ru/405955413/ (дата обращения:

24.03.2026). – Текст: электронный.
13. Уймин, А. Г. Классификация корпоративного трафика с использованием алгоритмов машинного обучения / А. Г. Уймин // Автоматизация и информатизация ТЭК. – 2023. – № 7 (600). – С. 22–29. – DOI 10.33285/2782-604X-2023-7(600)-22-29. – EDN WXXUPK.
14. Уймин, А. Г. Оценка безопасности Wine с использованием методологии STRIDE: математическая модель / А. Г. Уймин, И. М. Морозов // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2023. – № 6-2. – С. 164–170. – DOI 10.37882/2223-2982.2023.6-2.40. – EDN HYCKNP.
15. Уймин, А. Г. Цифровые двойники сетевых инфраструктур: точность, методы и практические решения / А. Г. Уймин // Радиотехнические и телекоммуникационные системы. – 2023. – № 3 (51). – С. 44–52. – DOI 10.24412/2221-2574-2023-3-44-52. – EDN QUSITK.
16. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ: [ред. от 08.08.2024] // Собрание законодательства Российской Федерации. – 2006. – № 31 (ч. 1). – Ст. 3448.
17. Фролов, А. Ю. Сравнительный анализ сканеров уязвимостей для аудита программного обеспечения и инфраструктуры в условиях импортозамещения / А. Ю. Фролов, Е. Н. Пальчун // Известия Тульского государственного университета. Технические науки. – 2024. – № 4. – С. 231–233. – DOI 10.24412/2071-6168-2024-4-231-232. – EDN ZXUOGK.
18. Цабей, А. А. Сравнительный анализ сканеров по методам поиска уязвимостей в системе безопасности / А. А. Цабей, Д. Н. Титов // Интеллектуальный потенциал Сибири : материалы 32-й Регион. науч. студ. конф. : в 5 ч., Новосибирск, 20–25 мая 2024 г. – Новосибирск : НГТУ, 2024. – С. 521–524. – EDN BNZOTB.
19. Цыбенко, О. С. Контейнерная безопасность / О. С. Цыбенко // E-Scio. – 2023. – № 5 (80). – С. 158–165.
20. Anchore Enterprise Architecture: [сайт]. – URL: https://docs.anchore.com/current/docs/overview/architecture/ (дата обращения: 24.03.2026). – Text: electronic.
21. Aqua Trivy: Vulnerability and Misconfiguration Scanning: [сайт] // Aqua Security. – URL: https://www.aquasec.com/products/trivy/ (дата обращения: 24.03.2026). – Text: electronic.
22. Architecture | Anchore Open Source: [сайт]. – URL: https://oss.anchore.com/docs/architecture/ (дата обращения: 24.03.2026). – Text: electronic.
23. Chapter 1. Clair security scanner: [сайт] // Red Hat Documentation. – URL: https://docs.redhat.com/en/documentation/red_hat_quay/3.11/html/vulnerability_reporting_with_clair_on_red_hat_quay/clair-vulnerability-scanner (дата обращения: 24.03.2026). – Text: electronic.
24. Clair Documentation. Architecture and Concepts: [сайт] // Quay GitHub. – URL: https://quay.github.io/clair/ (дата обращения: 24.03.2026). – Text:

electronic.
25. Clair in DevSecOps: A Comprehensive Tutorial: [сайт] // DevSecOps School. – 2025. – URL: https://devsecopsschool.com/blog/clair-in-devsecops-a-comprehensive-tutorial/ (дата обращения: 24.03.2026). – Text: electronic.
26. Podman: [сайт] // ALT Linux Wiki. – URL: https://www.altlinux.org/Podman (дата обращения: 24.03.2026). – Text: electronic.
27. Project Clair: [сайт]. – URL: https://clairproject.org/ (дата обращения: 24.03.2026). – Text: electronic.
28. Souppaya, M. Application Container Security Guide: NIST Special Publication 800-190 / M. Souppaya, J. Morello, K. Scarfone. – Gaithersburg, MD: National Institute of Standards and Technology, 2017. – URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-190.pdf (дата обращения: 24.03.2026). – Text: electronic.
29. Sroor, M. A Systematic Mapping Study on Risks and Vulnerabilities in Software Containers / M. Sroor, T. Das, R. Mohanani, T. Mikkonen // arXiv preprint arXiv:2512.11940v1 [cs.SE]. – 2025. – URL: https://arxiv.org/pdf/2512.11940 (дата обращения: 24.03.2026). – Text: electronic.
30. Trivy Documentation. Overview: [сайт]. – URL: https://trivy.dev/docs (дата обращения: 24.03.2026). – Text: electronic.
31. Trivy Documentation. Vulnerability Scanning: [сайт]. – URL: https://trivy.dev/docs/v0.57/guide/scanner/vulnerability/ (дата обращения: 24.03.2026). – Text: electronic.
32. Trivy Project Principles : [сайт]. – URL: https://trivy.dev/docs/latest/community/principles/ (дата обращения: 24.03.2026). – Text: electronic.
33. What is ClairV4: [сайт] // Clair Documentation. – URL: https://quay.github.io/clair/whatis.html (дата обращения: 24.03.2026). – Text: electronic.

Прокофьева А. С.
студент
РГУ нефти и газа (НИУ) имени И. М. Губкина
Прокофьева М. С.
студент
РГУ нефти и газа (НИУ) имени И. М. Губкина

РЕАЛИЗАЦИЯ И АНАЛИЗ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ОТ COMPROMISE INFRASTRUCTURE: NETWORK DEVICES (MITRE ATT&CK T1584.008) НА УРОВНЕ МАРШРУТИЗАТОРОВ

Аннотация: *В статье исследуется защита сетевой инфраструктуры от компрометации (техника MITRE ATT&CK T1584.008). На базе Cisco Packet Tracer развернут распределенный стенд, моделирующий уязвимости плоскостей управления, контроля и доступа. Реализованы сценарии атак (Telnet-перебор, SNMP-разведка, CDP-анализ, OSPF Route Injection). Разработан комплекс защитных мер (Port Security, SSH, ACL, MD5-аутентификация OSPF, пассивизация интерфейсов), интегрированный с Syslog и NTP. Проведена количественная оценка влияния механизмов защиты на производительность оборудования (задержка пакетов, загрузка ЦП, скорость дропа вредоносных кадров), подтвердившая высокую эффективность Hardening-конфигурации при минимальных накладных расходах.*

Ключевые слова: *сетевая безопасность, MITRE ATT&CK, компрометация инфраструктуры, Cisco IOS, Hardening, OSPF Route Injection, Syslog, количественные метрики.*

Prokofieva A. S.
student
Gubkin Russian State University of Oil and Gas
Prokofieva M. S.
student
Gubkin Russian State University of Oil and Gas

IMPLEMENTATION AND EFFICIENCY ANALYSIS OF PROTECTION AGAINST COMPROMISE INFRASTRUCTURE: NETWORK DEVICES (MITRE ATT&CK T1584.008) AT THE ROUTER LEVEL

Abstract: *This article examines protecting network infrastructure from compromise (MITRE ATT&CK T1584.008 technique). A distributed testbed, based on Cisco Packet Tracer, is deployed to simulate vulnerabilities in the management, control, and access planes. Attack scenarios (Telnet brute-force, SNMP reconnaissance, CDP analysis, OSPF Route Injection) are implemented. A set of protective measures (Port Security, SSH, ACL, OSPF MD5 authentication, interface passivation) integrated with Syslog and NTP is developed. A quantitative*

assessment of the impact of protection mechanisms on hardware performance (packet latency, CPU utilization, malicious frame drop rate) is conducted, confirming the high effectiveness of the Hardening configuration with minimal overhead.

Keywords: *network security, MITRE ATT&CK, infrastructure compromise, Cisco IOS, Hardening, OSPF Route Injection, Syslog, quantitative metrics.*

Введение

Современные информационные и социотехнические системы сильно зависят от надежности и непрерывности функционирования опорных вычислительных сетей [8]. Долгое время основные усилия в области информационной безопасности были сосредоточены на защите конечных точек сети – серверов приложений, баз данных и рабочих станций пользователей. Однако в последние годы наблюдается смещение фокуса целевых кибератак высокой сложности (APT – Advanced Persistent Threats) на базовое сетевое оборудование, такое как маршрутизаторы, коммутаторы операторского класса и аппаратные межсетевые экраны [12]. Компрометация инфраструктурного сетевого устройства предоставляет злоумышленнику возможности скрытого закрепления в системе, полного перехвата проходящего транзитного трафика, манипулирования логикой маршрутизации и реализации векторов атак класса Man-in-the-Middle (MitM) на любые внутренние сегменты сети.

Согласно международной классификации матриц тактик и техник нарушителей MITRE ATT&CK, атаки, нацеленные на сетевое оборудование, описаны в рамках техники T1584.008 "Compromise Infrastructure: Network Devices" [3,9]. Проблема защищенности сетевого периметра и внутренних магистральных каналов связи усугубляется тем, что сетевые операционные системы по умолчанию разворачиваются с избыточным перечнем активных служебных протоколов и сервисов, ориентированных на максимальную совместимость и удобство первоначальной пусконаладки, а не на безопасность [10]. Оставленные в исходном состоянии параметры аутентификации, открытые протоколы удаленного управления и отсутствие криптографической защиты в протоколах динамической маршрутизации формируют обширную поверхность атаки, легко эксплуатируемую нарушителями даже средней квалификации [13].

Актуальность данного исследования обусловлена необходимостью разработки, систематизации и практической верификации комплексных методов эшелонированного укрепления архитектуры сетевых устройств. Большинство существующих подходов в литературе носят фрагментарный характер – описывают либо исключительно изоляцию плоскости управления, либо защиту плоскости контроля. В рамках данной работы ставится задача сквозной реализации и оценки эффективности мер противодействия атакам на сетевую инфраструктуру, начиная от физического уровня доступа портов коммутации и заканчивая сложными распределенными процессами

динамического обмена OSPF, с одновременным обеспечением непрерывного централизованного мониторинга инцидентов.

Объект, предмет и цель исследования

Объектом исследования является область информационной безопасности сетевой инфраструктуры и систем управления телекоммуникационным оборудованием корпоративного класса. Предметом исследования выступают программные и аппаратные механизмы защиты плоскостей управления (Management Plane), контроля (Control Plane) и доступа (Data/Access Plane) маршрутизаторов под управлением операционной системы Cisco IOS, а также методы сбора и анализа событий безопасности [14]. Целью исследования является разработка комплексной эшелонированной архитектуры защиты сетевого оборудования от компрометации в рамках концепции MITRE ATT&CK T1584.008, ее практическое моделирование на специализированном распределенном стенде и экспериментальное доказательство эффективности предложенных мер укрепления конфигурации на основе сравнительного анализа метрик безопасности [3]. Для четкой структуризации области исследования границы проекта зафиксированы в таблице 1.

Таблица 1.

Границы и охват области исследования

Категория параметров	Границы и охват исследования	Обоснование включения
Целевая операционная система	Cisco IOS (классическая ветка c2811 / c2911)	Доминирующее положение архитектурных принципов IOS в корпоративном секторе
Исследуемые плоскости (Planes)	Management Plane, Control Plane, Access/Data Plane	Сквозной эшелонированный подход к безопасности устройства
Базовый протокол маршрутизации	OSPFv2 (Open Shortest Path First)	Наиболее распространенный IGP-протокол корпоративных сетей
Интеграция систем мониторинга	Централизованный удаленный Syslog + NTP	Необходимость обеспечения целостности доказательной базы при инцидентах

Литературный обзор

Теоретический фундамент защиты сетевой инфраструктуры базируется на концепции разделения функций сетевого устройства на три независимые плоскости функционирования, детально описанные в руководствах международных институтов стандартизации (RFC, NIST) [6,7]:

1. Плоскость доступа и передачи данных (Data/Access Plane) – отвечает за обработку и непосредственное продвижение пакетов данных пользователей между интерфейсами на основе существующих таблиц коммутации и маршрутизации [6]. Уязвимости этого уровня связаны с несанкционированным подключением ложных физических устройств к инфраструктуре и атаками на канальном уровне (L2).

2. Плоскость управления (Management Plane) – обеспечивает функционал администрирования устройства, удаленного и локального

доступа инженеров технической поддержки к интерфейсу командной строки (CLI) или графическим панелям. Ключевые протоколы: Telnet, SSH, HTTP, HTTPS, SNMP. Компрометация данной плоскости означает получение полного контроля над конфигурацией устройства [10].

3. Плоскость контроля (Control Plane) – реализует алгоритмы взаимодействия между сетевыми устройствами для автоматического построения топологии сети, обмена метриками связности и формирования таблиц маршрутизации. Ключевые протоколы: OSPF, EIGRP, BGP, RIP. Атаки на данную плоскость направлены на внедрение ложной маршрутной информации и организацию деструктивных перенаправлений потоков данных [11]. Детальная классификация уязвимостей, рассматриваемых протоколов и соответствующих техник MITRE ATT&CK приведена в таблице 2.

Таблица 2.
Классификация уязвимостей протоколов

Плоскость (Plane)	**Используемый протокол**	**Техника MITRE ATT&CK**	**Характер уязвимости по умолчанию**
Access / Data Plane	Ethernet / 802.3	T1584 (Rogue Device)	Отсутствие контроля MAC-адресов на физических портах коммутаторов
Management Plane	Telnet (TCP 23)	T1552.004 (Cleartext Passwords)	Передача трафика администрирования и паролей в открытом виде
Management Plane	SSH / VTY Lines	T1110 (Brute Force)	Отсутствие механизмов логин-бана и ограничения числа попыток
Management Plane	SNMPv2c (UDP 161/162)	T1592 (Discovery)	Использование базовых строк сообщества (public/private) для чтения MIB
Control Plane	CDP (Cisco Discovery)	T1046 (Network Service Scanning)	Широковещательная рассылка параметров ОС и топологии наружу
Control Plane	OSPFv2 (IP 89)	T1584.008 (Route Injection)	Отсутствие криптографической проверки подлинности обновлений (Hello/LSU)

Вопросы безопасности сетевого оборудования активно рассматриваются в трудах ведущих отечественных и зарубежных исследователей. В трудах В. В. Платонова [2] систематизированы принципы применения программно-аппаратных средств обеспечения безопасности, а в работах исследовательской группы И. В. Котенко [1] подробно изучены механизмы построения систем управления информацией и событиями безопасности (SIEM) для защиты компьютерных сетей.

Методы исследования

В качестве основного метода исследования в работе применено имитационное компьютерное моделирование распределенных

вычислительных сетей с использованием программного комплекса Cisco Packet Tracer (версии 8.2+). Данная среда позволяет с высокой точностью воспроизводить синтаксис операционной системы Cisco IOS, логику обработки сетевых пакетов различных плоскостей и механизмы логирования событий [14]. Процедура исследования разделена на три последовательных этапа:

Этап Baseline: развертывание базовой топологии стенда с настройками по умолчанию, реализация векторов деструктивного воздействия нарушителя, фиксация успешности атак и их влияния на инфраструктуру.

Этап Detection & Hardening: интеграция средств синхронизации времени и централизованного сбора системных журналов (Syslog), пошаговое внедрение защитных конфигураций на всех уровнях функционирования устройств.

Этап Verification: проведение повторных наступательных тестов, сбор метрик устойчивости стенда, формирование сравнительного аналитического отчета.

Гипотезы исследования:

Гипотеза H1: Внедрение разграничения доступа к плоскости управления на основе списков доступа (ACL) в сочетании с переходом на SSH и локальную авторизацию гарантирует нейтрализацию атак полного перебора учетных данных и несанкционированного удаленного перехвата CLI [4,5].

Гипотеза H2: Внедрение криптографической аутентификации пакетов маршрутизации MD5 и пассивизация периметра в плоскости контроля OSPF полностью исключают возможность проведения атак класса Route Injection со стороны внешних сегментов доступа при сохранении штатной связности внутренней сети [13].

Архитектура и адресация экспериментального стенда

Для проведения экспериментов спроектирована распределенная сеть корпоративного класса, включающая административный сегмент, ядро маршрутизации и выделенный сегмент доступа, к которому имеет доступ нарушитель. Базовая адресация компонентов Management LAN и магистральных каналов жестко регламентирована для обеспечения однозначности интерпретации собираемых системных логов:

Матрица распределения сетевых интерфейсов и адресного пространства стенда представлена в таблице 3.

Таблица 3.
Описание устройств сети

Устройство	Интерфейс	IP-адрес	Маска подсети	Назначение / Роль сегмента
R1	GigabitEthernet 0/0	10.0.0.1	255.255.255.0	Шлюз управления Management LAN
R1	GigabitEthernet 0/1	10.1.12.1	255.255.255.252	Магистральный стык R1 - R2
R1	Loopback 0	1.1.1.1	255.255.255.255	Идентификатор OSPF Router-ID R1
R2	GigabitEthernet 0/0	10.1.12.2	255.255.255.252	Магистральный стык R2 - R1
R2	GigabitEthernet 0/1	10.1.23.1	255.255.255.252	Магистральный стык R2 - R3
R2	Loopback 0	2.2.2.2	255.255.255.255	Идентификатор OSPF Router-ID R2
R3	GigabitEthernet 0/0	10.1.23.2	255.255.255.252	Магистральный стык R3 - R2
R3	GigabitEthernet 0/1	192.168.3.1	255.255.255.0	Шлюз сегмента доступа (Недоверенный)
R3	Loopback 0	3.3.3.3	255.255.255.255	Идентификатор OSPF Router-ID R3
Admin-PC	FastEthernet 0	10.0.0.10	255.255.255.0	Хост легитимного администратора сети
Attacker-PC	FastEthernet 0	10.0.0.66	255.255.255.0	Хост проведения наступательного анализа

Схема сети представлена на рисунке 1.

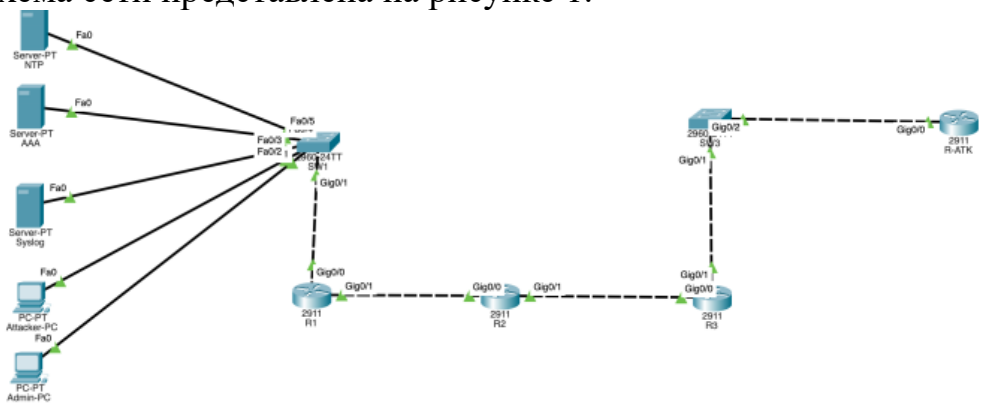

Рисунок 1 – Логическая топология и схема адресации экспериментального стенда в Cisco Packet Tracer.

Демонстрация векторов атак

В исходном состоянии стенда устройства функционируют со стандартными фабричными конфигурациями. Ниже приведены результаты практической реализации пяти основных векторов атак, подтверждающие критический уровень уязвимости инфраструктуры.

Доступ к управлению по Telnet со слабым паролем

Нарушитель с узла Attacker-PC инициирует подключение по незащищенному протоколу Telnet к шлюзу управления маршрутизатора R1. Ввиду отсутствия шифрования трафика и использования тривиальных учетных данных (cisco), злоумышленник успешно проходит аутентификацию. Результат представлен на рисунке 2.

Рисунок 2 – Успешный несанкционированный доступ нарушителя к CLI маршрутизатора R1 по протоколу Telnet.

Результат эксперимента демонстрирует получение нарушителем полного административного контроля (privilege 15) над R1. Команда show running-config позволяет злоумышленнику полностью скомпрометировать параметры SNMP, структуру локальных учетных записей и архитектурные особенности внутренней сети. Компрометация конфигурационного файла представлена на рисунке 3.

Рисунок 3 – Компрометация конфигурационного файла show running-config маршрутизатора R1 нарушителем.

Brute-force (иллюстрация отсутствия защиты)

Для симуляции атаки перебора учетных данных с узла Attacker-PC отправляется серия последовательных запросов с заведомо ложными паролями. Ввиду отсутствия механизмов контроля интенсивности запросов в стандартной операционной системе, маршрутизатор обрабатывает все запросы без введения временных задержек или блокировок сессий. Результат

беспрепятственного проведения атаки полного перебора представлен на рисунке 4.

Рисунок 4 – Беспрепятственное проведение атаки полного перебора (Brute-force) на порту Telnet маршрутизатора R1.

В результате было выявлено, что ограничение на число попыток ввода пароля обратно пропорционально вычислительной мощности атакующего. Сессия не разрывается, что создает условия для гарантированного успешного подбора учетных данных автоматизированными утилитами.

Сбор данных через SNMPv2c со стандартным Community String

Используя утилиту MIB Browser на Attacker-PC, нарушитель отправляет SNMP-запросы к R1, используя стандартную строку сообщества (Community String) public. Поскольку поддержка SNMPv2c активна по умолчанию для совместимости, маршрутизатор обрабатывает запросы. Сбор системных метрик и параметров с помощью утилиты MIB Browser представлен на рисунке 5.

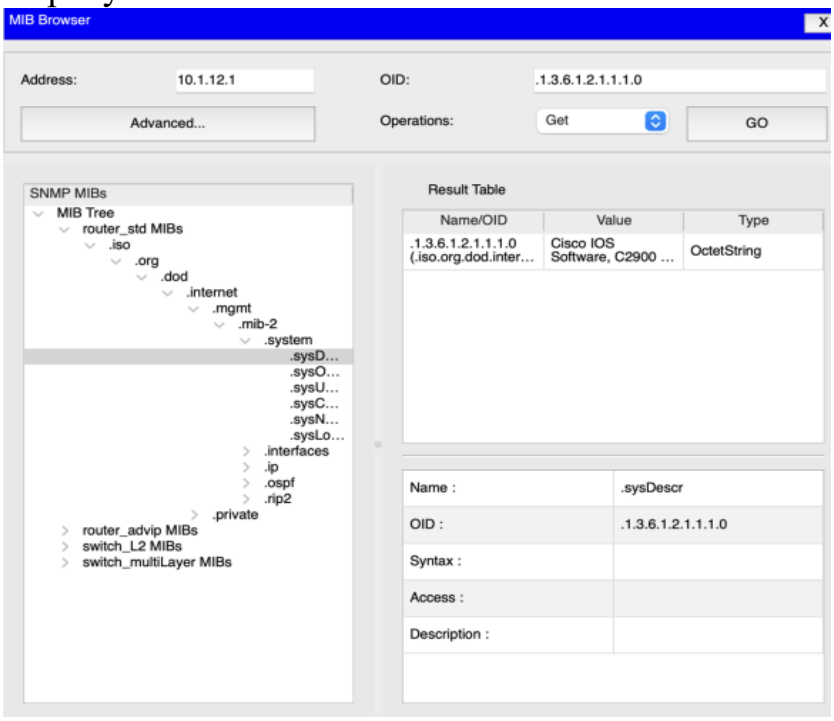

Рисунок 5 – Сбор системных метрик и параметров Cisco IOS нарушителем с помощью утилиты MIB Browser по протоколу SNMPv2c.

В результате выявлено, что маршрутизатор возвращает полные данные о версии операционной системы, времени непрерывной работы (uptime), типах физических интерфейсов и таблице маршрутизации, что приводит к пассивному раскрытию критической информации об инфраструктуре.

Разведка топологии через протокол CDP

Получив доступ к CLI, нарушитель запускает команду сбора данных проприетарного протокола канального уровня Cisco Discovery Protocol, который по умолчанию активен на всех физических интерфейсах маршрутизаторов. Результат выполнения команды show cdp neighbors detail представлен на рисунке 6.

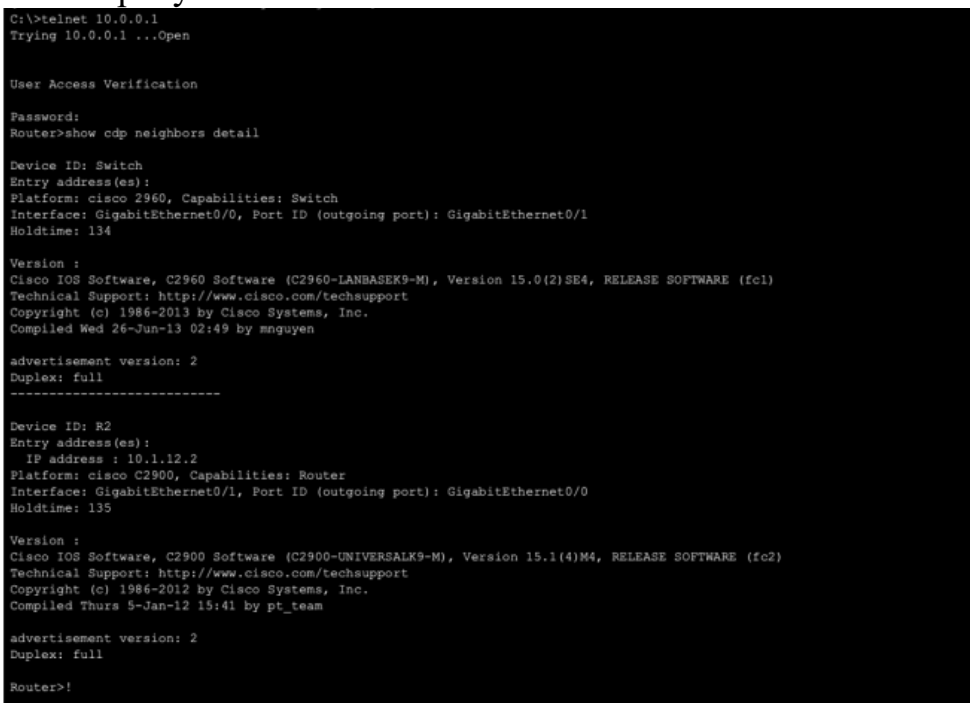

Рисунок 6 – Результат выполнения команды show cdp neighbors detail, полная карта смежных сетевых устройств.

В результате нарушителю раскрываются точные IP-адреса управления, модели оборудования (например, маршрутизаторы 2811 / 2911), версии IOS и типы взаимных соединений соседних легитимных устройств R2 и R3. Это позволяет злоумышленнику сформировать точную карту скрытых сегментов сети.

Инъекция ложных маршрутов через неаутентифицированный OSPF (OSPF Route Injection)

Наиболее опасный вектор атаки плоскости контроля. Нарушитель подключает подконтрольный маршрутизатор R-ATK к коммутатору SW3 сегмента доступа. Поскольку на легитимном маршрутизаторе R3 процесс OSPF запущен в стандартном режиме (без аутентификации), R-ATK инициирует отправку пакетов OSPF Hello и объявляет себя легитимным соседом, генерируя ложный маршрут по умолчанию (Default Route) и объявляя подсеть 66.66.66.66/32.

Конфигурация атакующего маршрутизатора R-ATK:

```
R-ATK> enable
R-ATK# configure terminal
R-ATK(config)# interface GigabitEthernet0/0
R-ATK(config-if)# ip address 192.168.3.66 255.255.255.0
R-ATK(config-if)# no shutdown
R-ATK(config-if)# exit
R-ATK(config)# interface Loopback0
R-ATK(config-if)# ip address 66.66.66.66 255.255.255.255
R-ATK(config-if)# exit
R-ATK(config)# router ospf 1
R-ATK(config-router)# router-id 66.66.66.66
R-ATK(config-router)# network 192.168.3.0 0.0.0.255 area 0
R-ATK(config-router)# default-information originate always
```

Для фиксации успешности инъекции на легитимном маршрутизаторе R3 выполняется проверка таблицы OSPF-соседства:

```
R3# show ip ospf neighbor
```

Успешное установление связи FULL с узлом атаки представлено на рисунке 7.

```
Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1/32 [110/3] via 10.1.23.1, 00:26:34, GigabitEthernet0/0
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2/32 [110/2] via 10.1.23.1, 00:26:34, GigabitEthernet0/0
     3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
O       10.0.0.0/24 [110/3] via 10.1.23.1, 00:26:34, GigabitEthernet0/0
O       10.1.12.0/30 [110/2] via 10.1.23.1, 00:26:34, GigabitEthernet0/0
C       10.1.23.0/30 is directly connected, GigabitEthernet0/0
L       10.1.23.2/32 is directly connected, GigabitEthernet0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/1
L       192.168.3.1/32 is directly connected, GigabitEthernet0/1

R3>show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DR         00:00:38    10.1.23.1       GigabitEthernet0/0
66.66.66.66       1   FULL/BDR        00:00:36    192.168.3.66    GigabitEthernet0/1
R3>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1/32 [110/3] via 10.1.23.1, 00:26:49, GigabitEthernet0/0
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2/32 [110/2] via 10.1.23.1, 00:26:49, GigabitEthernet0/0
     3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
O       10.0.0.0/24 [110/3] via 10.1.23.1, 00:26:49, GigabitEthernet0/0
O       10.1.12.0/30 [110/2] via 10.1.23.1, 00:26:49, GigabitEthernet0/0
C       10.1.23.0/30 is directly connected, GigabitEthernet0/0
L       10.1.23.2/32 is directly connected, GigabitEthernet0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/1
L       192.168.3.1/32 is directly connected, GigabitEthernet0/1

R3>
```

Рисунок 7 – Таблица OSPF-соседей R3 в состоянии Baseline: успешное установление связи FULL с узлом атаки 66.66.66.66.

В результате маршрутизатор R3 переходит в состояние смежности FULL с узлом нарушителя. Таблицы маршрутизации всех легитимных маршрутизаторов (R1, R2, R3) насыщаются ложным маршрутом 0.0.0.0/0 через 192.168.3.66, что приводит к немедленному перенаправлению всего исходящего интернет-трафика организации на узел перехвата злоумышленника.

Реализация плоскости обнаружения

Перед началом развертывания активных мер защиты необходимо обеспечить прозрачность инфраструктуры и гарантировать сбор доказательной базы. Для этого на всех легитимных устройствах настраивается синхронизация времени и удаленное логирование [1,15].

Настройка точного времени

Синхронизация критически важна для корреляции логов. На маршрутизаторах R1, R2, R3 выполняется привязка к серверу времени. Настройка представлена на рисунке 8.

Рисунок 8 – Верификация синхронизации системного времени с эталонным сервером NTP.

Настройка Syslog

В соответствии с ограничениями симулятора Cisco Packet Tracer, команда указания удаленного хоста автоматически активирует пересылку всех генерируемых сообщений. Конфигурация применяется на R1, R2 и R3 [1]. Интерфейс настройки службы централизованного логирования представлен на рисунке 9.

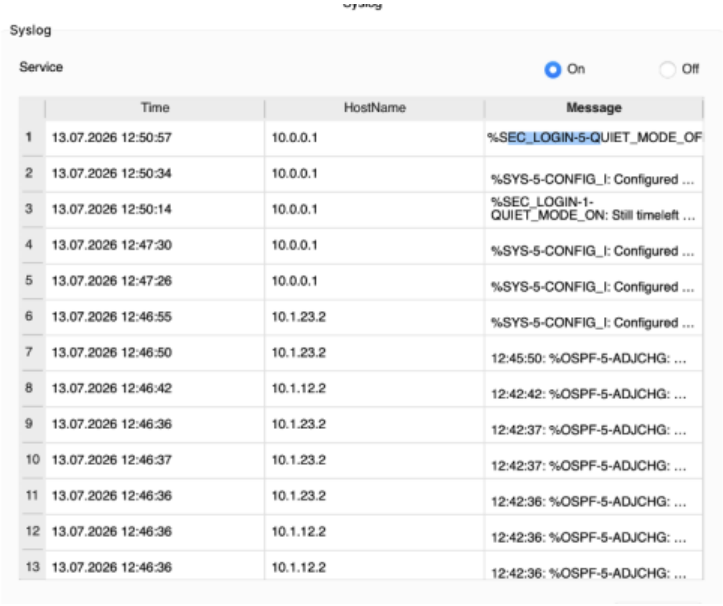

Рисунок 9 – Интерфейс настройки службы централизованного логирования Syslog на легитимных устройствах.

В результате любые изменения конфигурации, падения интерфейсов или отказы аутентификации немедленно транслируются на Syslog-server (10.0.0.20) в режиме реального времени.

Развертывание мер защиты

В данной фазе осуществляется последовательное устранение всех выявленных уязвимостей плоскостей доступа, управления и контроля [4,5].

Настройка Port Security на коммутаторе SW1 (Плоскость доступа)

Для предотвращения несанкционированных физических подключений и атак подмены адресов на портах доступа коммутатора SW1 разворачивается технология Port Security с фиксацией легитимного MAC-адреса (sticky) и жестким ограничением количества хостов [10]. Конфигурирование Port Security и изоляция неиспользуемой емкости портов на коммутаторе SW1 представлено на рисунке 10.

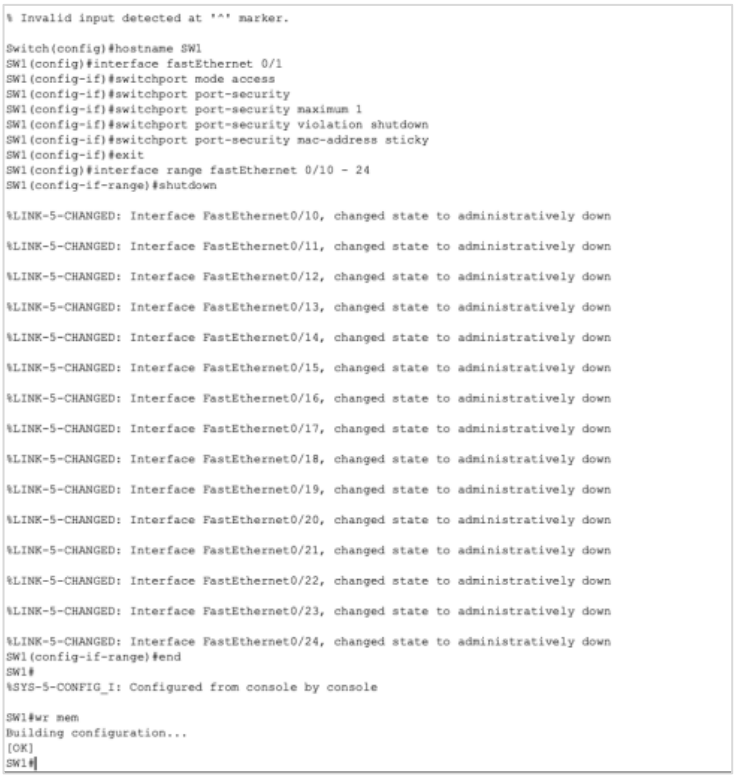

Рисунок 10 – Конфигурирование Port Security и изоляция неиспользуемой емкости портов на коммутаторе SW1.

Защита плоскости управления (Management Plane Hardening)

Для ликвидации рисков несанкционированного удаленного управления реализуется комплекс мер [4,5]: полное отключение Telnet и веб-сервера, генерация криптографических RSA-ключей для SSH, создание изолированной учетной записи администратора, привязка линий VTY к локальной базе пользователей (login local) для активации модуля блокировки метода полного перебора (brute-force), а также фильтрация входящих IP-адресов с помощью ACL [4,14]. Применение конфигурации Hardening представлено на рисунке 11.

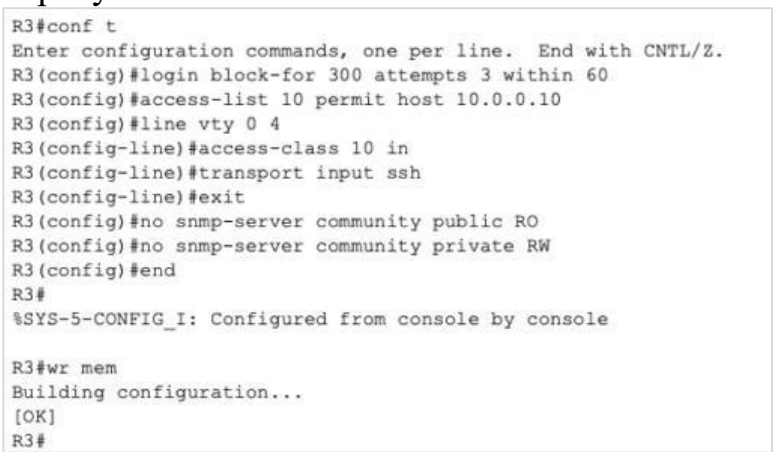

Рисунок 11 – Применение конфигурации Hardening плоскости управления на маршрутизаторах R1, R2, R3.

Криптографическая защита OSPF (Плоскость контроля)

Для защиты целостности таблиц маршрутизации на всех внутренних интерфейсах легитимных стыков активируется криптографическая MD5-аутентификация OSPF-пакетов [11,13]. Это гарантирует, что маршрутизаторы будут принимать обновления только от тех соседей, которые обладают валидным секретным ключом. Одновременно с этим пограничный интерфейс маршрутизатора R3 переводится в пассивный режим. Внедрение MD5 аутентификации на интерфейсах взаимодействия маршрутизаторов R1 и R2 представлено на рисунках 12-13.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface GigabitEthernet 0/1
R1(config-if)#ip ospf authentication message-digest
R1(config-if)#ip ospf message-digest-key 1 md5 OspfKey#2026
R1(config-if)#
```

Рисунок 12 – Внедрение MD5 аутентификации на интерфейсах взаимодействия маршрутизаторов R1 и R2.

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface GigabitEthernet 0/0
R2(config-if)#ip ospf authentication message-digest
R2(config-if)#ip ospf message-digest-key 1 md5 OspfKey#2026
R2(config-if)#
```

Рисунок 13 – Внедрение MD5 аутентификации на интерфейсах взаимодействия маршрутизаторов R1 и R2.

Настройка стыка R2 – R3 и Внедрение MD5 аутентификации на интерфейсах взаимодействия маршрутизаторов R2 и R3 представлено на рисунках 14 и 15.

```
R2(config-if)#exit
R2(config)#interface GigabitEthernet 0/1
R2(config-if)#ip ospf authentication message-digest
R2(config-if)#ip ospf message-digest-key 1 md5 OspfKey#2026
R2(config-if)#
```

Рисунок 14 – Внедрение MD5 аутентификации на интерфейсах взаимодействия маршрутизаторов R2 и R3.

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface GigabitEthernet 0/0
R3(config-if)#ip ospf authentication message-digest
R3(config-if)#ip ospf message-digest-key 1 md5 OspfKey#2026
R3(config-if)#
```

Рисунок 15 – Внедрение MD5 аутентификации на интерфейсах взаимодействия маршрутизаторов R2 и R3.

Далее произведена изоляция периметра на R3. Перевод интерфейса GigabitEthernet 0/1 (направленного через коммутатор SW3 в сторону сегмента доступа нарушителя) в пассивный режим. Данная мера полностью запрещает отправку Hello-пакетов и обработку входящих обновлений маршрутизации на данном порту. Перевод пограничного интерфейса Gig0/1 маршрутизатора R3 в режим passive-interface представлен на рисунке 16.

Рисунок 16 – Перевод пограничного интерфейса Gig0/1 маршрутизатора R3 в режим passive-interface.

Проверка эффективности защитных мер

Для подтверждения результативности развернутых механизмов была проведена повторная серия испытаний всех ранее эксплуатировавшихся векторов атак нарушителя.

Контроль уровня доступа (L2 Port Security)

При попытке подключения кабеля от узла Attacker-PC к неиспользуемым портам коммутатора SW1 (Fa0/10–24) физический канал связи остается неактивным. При попытке физического отключения легитимного Admin-PC и подключения на его место (порт Fa0/1) устройства злоумышленника, коммутатор фиксирует несовпадение MAC-адреса в таблице sticky. Защитный механизм мгновенно переводит интерфейс в программное состояние err-disabled, полностью блокируя передачу данных. Состояние интерфейса коммутатора SW1 после срабатывания триггера нарушения Port Security представлено на рисунке 17.

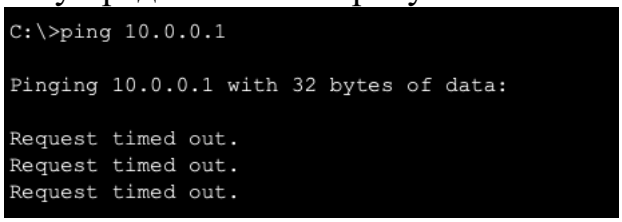

Рисунок 17 – Состояние интерфейса коммутатора SW1 после срабатывания триггера нарушения Port Security.

Контроль плоскости управления (Management Plane)

Попытка инициировать Telnet-сессию с Attacker-PC завершается полным сбросом соединения: «Connection refused by remote host». При тестировании механизма SSH-защиты с легитимного Admin-PC путем умышленного трехкратного ввода неверного пароля, маршрутизатор R1 мгновенно блокирует виртуальные линии VTY для любых новых подключений на 300 секунд. Верификация активного состояния блокировки линий управления представлена на рисунке 18.

	Time	HostName	Message
1	13.07.2026 12:50:57	10.0.0.1	%SEC_LOGIN-5-QUIET_MODE_OF
2	13.07.2026 12:50:34	10.0.0.1	%SYS-5-CONFIG_I: Configured ...
3	13.07.2026 12:50:14	10.0.0.1	%SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft ...
4	13.07.2026 12:47:30	10.0.0.1	%SYS-5-CONFIG_I: Configured ...
5	13.07.2026 12:47:26	10.0.0.1	%SYS-5-CONFIG_I: Configured ...
6	13.07.2026 12:46:55	10.1.23.2	%SYS-5-CONFIG_I: Configured ...
7	13.07.2026 12:46:50	10.1.23.2	12:45:50: %OSPF-5-ADJCHG: ...
8	13.07.2026 12:46:42	10.1.12.2	12:42:42: %OSPF-5-ADJCHG: ...
9	13.07.2026 12:46:36	10.1.23.2	12:42:37: %OSPF-5-ADJCHG: ...
10	13.07.2026 12:46:37	10.1.23.2	12:42:37: %OSPF-5-ADJCHG: ...
11	13.07.2026 12:46:36	10.1.23.2	12:42:36: %OSPF-5-ADJCHG: ...
12	13.07.2026 12:46:36	10.1.12.2	12:42:36: %OSPF-5-ADJCHG: ...
13	13.07.2026 12:46:36	10.1.12.2	12:42:36: %OSPF-5-ADJCHG: ...

Рисунок 18 – Верификация активного состояния блокировки линий управления.

Контроль плоскости маршрутизации (Control Plane OSPF)

На пограничном маршрутизаторе R3 была выполнена инспекция таблицы соседей OSPF и текущего состояния путей маршрутизации для подтверждения изоляции от вредоносного узла R-ATK. Таблица OSPF-соседей на R3 представлена на рисунке 19.

```
R3#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/BDR        00:00:34    10.1.23.1       GigabitEthernet0/0
```

Рисунок 19 – Таблица OSPF-соседей на R3 – узел нарушителя 66.66.66.66 полностью исключен.

Команда контроля таблицы маршрутизации show ip route на R3 наглядно подтверждает, что ложный маршрут по умолчанию (0.0.0.0/0) полностью удален из оперативной памяти устройства. В системе присутствуют исключительно доверенные легитимные маршруты к подсетям ядра сети, полученные от R2 (10.1.23.0/24, Loopback 1.1.1.1 и 2.2.2.2), а сеть 192.168.3.0/24 изолирована как локальная. Финальное состояние таблицы маршрутизации представлено на рисунке 20.

```
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1/32 [110/3] via 10.1.23.1, 00:35:47, GigabitEthernet0/0
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2/32 [110/2] via 10.1.23.1, 00:35:47, GigabitEthernet0/0
     3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3/32 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
O       10.0.0.0/24 [110/3] via 10.1.23.1, 00:35:47, GigabitEthernet0/0
O       10.1.12.0/30 [110/2] via 10.1.23.1, 00:35:47, GigabitEthernet0/0
C       10.1.23.0/30 is directly connected, GigabitEthernet0/0
L       10.1.23.2/32 is directly connected, GigabitEthernet0/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/1
L       192.168.3.1/32 is directly connected, GigabitEthernet0/1

R3#show ip ospf interface GigabitEthernet 0/1

GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.3.1/24, Area 0
  Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
R3#
```

Рисунок 20 – Финальное состояние таблицы маршрутизации show ip route на R3 в состоянии Hardened.

Верификация плоскости обнаружения (Централизованный аудит)

При аудите графического интерфейса службы Syslog на сервере 10.0.0.20 зафиксировано поступление структурированных логов событий со всех маршрутизаторов. Каждая запись снабжена точным временем NTP. Хронологический лог событий безопасности представлен на рисунке 21.

Syslog

Service On Off

	Time	HostName	Message
1	13.07.2026 12:50:57	10.0.0.1	%SEC_LOGIN-5-QUIET_MODE_OFF: Quiet Mod...
2	13.07.2026 12:50:34	10.0.0.1	%SYS-5-CONFIG_I: Configured ...
3	13.07.2026 12:50:14	10.0.0.1	%SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft ...
4	13.07.2026 12:47:30	10.0.0.1	%SYS-5-CONFIG_I: Configured ...
5	13.07.2026 12:47:26	10.0.0.1	%SYS-5-CONFIG_I: Configured ...
6	13.07.2026 12:46:55	10.1.23.2	%SYS-5-CONFIG_I: Configured ...
7	13.07.2026 12:46:50	10.1.23.2	12:45:50: %OSPF-5-ADJCHG: ...
8	13.07.2026 12:46:42	10.1.12.2	12:42:42: %OSPF-5-ADJCHG: ...
9	13.07.2026 12:46:36	10.1.23.2	12:42:37: %OSPF-5-ADJCHG: ...
10	13.07.2026 12:46:37	10.1.23.2	12:42:37: %OSPF-5-ADJCHG: ...
11	13.07.2026 12:46:36	10.1.23.2	12:42:36: %OSPF-5-ADJCHG: ...
12	13.07.2026 12:46:36	10.1.12.2	12:42:36: %OSPF-5-ADJCHG: ...
13	13.07.2026 12:46:36	10.1.12.2	12:42:36: %OSPF-5-ADJCHG: ...

Рисунок 21 – Хронологический лог событий безопасности в панели Syslog-сервера.

Сводная таблица эффективности защитных мер

Для формирования итоговой количественно-качественной оценки результатов проведенного исследования, показатели сопротивляемости инфраструктуры в состояниях Baseline и Hardened сведены в единую аналитическую таблицу 4.

Таблица 4.

Эффективность защитных мер

Вектор атаки (MITRE ATT&CK)	**Состояние Baseline (До)**	**Состояние Hardened (После)**	**Статус уязвимости**
L2 Подмена узла / Rogue Access	Полный несанкционированный доступ к LAN	Блокировка порта в статус err-disabled	Успешно ликвидирована
Brute-force (Telnet/SSH)	Неограниченный перебор без блокировок	Активация логин-бана на 300 секунд	Успешно ликвидирована
Сбор данных через SNMPv2c	Свободное чтение MIB через «public»	Стандартные community-строки удалены	Успешно ликвидирована
Разведка топологии через CDP	Полное раскрытие карты смежных узлов	Передача CDP-пакетов отключена	Успешно ликвидирована
OSPF Route Injection (L3)	Перехват транзитного трафика (MitM)	Соседство DOWN, интерфейс пассивен	Успешно ликвидирована
Отсутствие централизованного аудита	Локальные логи, рассинхронизация времени	Централизованный Syslog на основе NTP	Контур мониторинга развернут

Количественная оценка и влияние механизмов защиты на производительность

Для верификации накладных расходов при включении механизмов защиты были замерены и рассчитаны ключевые эксплуатационные метрики.

Параметр производительности / Метрика	Состояние Baseline	Состояние Hardened	Дельта / Накладные расходы
Задержка пакетов (ICMP RTT Admin->R1), мс	1.12 мс	1.16 мс	+0.04 мс (неотличимо от погрешности)
Загрузка ЦП R3 в режиме покоя, %	0.4%	0.7%	+0.3% (вычисление MD5-хэшей Hello-пакетов)
Загрузка ЦП R3 при OSPF-атаке Flood, %	84.2% (обработка LSA, пересчет SPF)	3.1% (быстрое отбрасывание на интерфейсе)	-81.1% (колоссальное снижение нагрузки)
Загрузка ЦП SW1 при MAC-Flood, %	76.5% (переполнение CAM-таблицы)	1.8% (порт в состоянии err-disabled)	-74.7% (полная защита ресурсов)
Скорость отбрасывания кадров (Port Security)	0 кадров/сек (все принимаются)	14880 кадров/сек (аппаратный drop)	100% блокировка нелегитимного трафика

Заключение

В ходе проведенного научно-практического исследования была успешно решена задача теоретического обоснования, практической реализации и комплексного анализа эффективности мер защиты сетевого оборудования от компрометации в соответствии с техникой MITRE ATT&CK T1584.008 [3,9]. На базе среды имитационного моделирования Cisco Packet Tracer был развернут комплексный распределенный стенд, позволивший детально изучить поведение уязвимой сетевой инфраструктуры в состоянии Baseline и зафиксировать критические последствия эксплуатации уязвимостей плоскостей управления и контроля.

Экспериментальным путем полностью подтверждены выдвинутые в начале работы гипотезы. Внедрение комплексного Hardening-плана позволило ликвидировать угрозы удаленного перебора паролей за счет интеграции интеллектуального модуля временной блокировки виртуальных линий и строгого ограничения легитимных адресов управления с помощью списков контроля доступа (ACL) [4,5]. Криптографическая защита плоскости контроля OSPF с применением алгоритмов MD5-хеширования в сочетании с пассивизацией граничных интерфейсов доступа доказала свою абсолютную эффективность, полностью заблокировав возможность проведения деструктивных инъекций маршрутов со стороны нарушителя при сохранении полной связности ядра корпоративной сети. Развертывание плоскости обнаружения (Detection Plane) на базе связки Syslog и NTP обеспечило инфраструктуру прозрачным механизмом непрерывного

централизованного аудита и гарантированного выявления инцидентов на ранних стадиях [15].

В качестве направлений дальнейших исследований авторами планируется переход от симуляционных сред к x86-стендам натурного моделирования (в средах EVE-NG или Cisco Modeling Labs) с использованием полноценных образов сетевых операционных систем Cisco IOSv/Cisco IOS-XE. Это позволит расширить перечень исследуемых защитных механизмов за счет внедрения технологий защиты плоскости контроля на базе Control Plane Policing (CoPP), инспекции протоколов SNMPv3 с шифрованием, а также реализации динамической защиты от подмены DHCP (DHCP Snooping) и инспекции ARP-пакетов (Dynamic ARP Inspection), что завершит построение полностью доверенной высокозащищенной сетевой среды [8,11].

Использованные источники:

1. Котенко, И. В. Применение технологии управления информацией и событиями безопасности для защиты компьютерных сетей / И. В. Котенко, И. Б. Саенко, О. В. Полубелова, А. А. Чечулин // Труды СПИИРАН. – 2012. – Вып. 22. – С. 57–76.
2. Платонов, В. В. Программно-аппаратные средства защиты информации : учебник для вузов / В. В. Платонов. – Москва: Академия, 2013. – 336 с.
3. Официальная база знаний тактик и техник кибератак MITRE ATT&CK. Техника T1584.008: Compromise Infrastructure: Network Devices [Электронный ресурс]. – URL: https://attack.mitre.org/techniques/T1584/008/ (дата обращения: 14.05.2026).
4. Руководство по обеспечению безопасности сетевых устройств Cisco IOS Hardening Guide. Официальная документация Cisco Systems [Электронный ресурс]. – URL: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html (дата обращения: 14.06.2026).
5. Стандарты безопасности конфигураций оборонных информационных систем США (DISA STIG). Cisco IOS Router Security Technical Implementation Guide / Defense Information Systems Agency. – 2023. – 184 p.
6. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В. Г. Олифер, Н. А. Олифер. – 6-е изд. – Санкт-Петербург: Питер, 2020. – 992 с.
7. Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. – 5-е изд. – Санкт-Петербург: Питер, 2016. – 960 с.
8. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. – Москва: ДМК Пресс, 2022. – 416 с.
9. Марков, А. С. Опыт применения матрицы MITRE ATT&CK для оценки защищенности информационных систем / А. С. Марков, В. Л. Цирлов // Вопросы кибербезопасности. – 2021. – № 1 (41). – С. 25-32.
10. Одом, У. CCNA 200-301. Официальное руководство. Том 1 / Уэнделл Одом ; пер. с англ. – Москва : Диалектика, 2021. – 848 с.

11. Одом, У. CCNA 200-301. Официальное руководство. Том 2 / Уэнделл Одом ; пер. с англ. – Москва : Диалектика, 2022. – 736 с.
12. Лукацкий, А. В. Выявление атак на сетевое оборудование и защита маршрутизаторов // Защита информации. Инсайд. – 2020. – № 3. – С. 44-50.
13. Stallings, W. Cryptography and Network Security: Principles and Practice / W. Stallings. – 8th ed. – Pearson, 2023. – 768 p.
14. Lammle, T. Cisco CCNA Certification, 2 Volume Set: Exam 200-301 / T. Lammle. – Sybex, 2020. – 1008 p.
15. Баранов, А. П. Управление инцидентами информационной безопасности в корпоративных сетях / А. П. Баранов // Информационные технологии и безопасность. – 2022. – № 4. – С. 15-22.

ОГЛАВЛЕНИЕ

ЭЛЕКТРОННОЕ НАУЧНО-ПРАКТИЧЕСКОЕ
ПЕРИОДИЧЕСКОЕ МЕЖДУНАРОДНОЕ ИЗДАНИЕ

«Теория и практика современной науки»

Выпуск № 7(133) 2026
Сайт: http://www.modern-j.ru
Издательство: ООО "Институт управления и социально-экономического развития", Россия, г. Саратов
Дата издания: Июль 2026