Сучасний стек технологій для аналізу трафіку за допомогою SLIPS включає інструменти захоплення Zeek і Suricata та обробки даних у реальному часі. Використання алгоритмів типу Isolation Forest підтвердило свою ефективність для швидкого виявлення аномалій у вебтрафіку. Платформа SLIPS використовує Redis для швидкого обміну даними між модулями та пропонує інструменти візуалізації інцидентів, такі як Kalipso.

Особливе значення має відкритість датасетів, на яких тренується SLIPS, наприклад, Stratosphere IoT Dataset, що дозволяє дослідникам адаптувати систему під специфічні потреби Linux-серверів або IoT-інфраструктур.

Stratosphere Linux IPS представляє собою сучасний приклад інтелектуальної системи захисту, яка успішно поєднує статистичний аналіз з методами глибокого навчання. Застосування SLIPS дозволяє значно підвищити рівень виявлення складних кіберзагроз за рахунок аналізу довгострокової поведінки вузлів мережі. Перспективами подальшого розвитку є вдосконалення модулів аналізу зашифрованого трафіку та автоматизація реагування на інциденти IPS mode в хмарних середовищах.

1. IBM Security. Cost of a Data Breach Report 2025. IBM Corporation, 2025.
2. Alsoufi M. A., et al. Anomaly-based intrusion detection model using deep learning for IoT networks. Computer Modeling in Engineering & Sciences. – 2024. – Vol. 141, №1. – P. 823–845.
3. Chua W., et al. Web traffic anomaly detection using Isolation Forest. Informatics. – 2024. – Vol. 11, №4. – P. 83.
4. Garcia S. Stratosphere Linux IPS: Behavioral-based Intrusion Detection System. Stratosphere Laboratory, 2025. URL: https://github.com/stratosphereips/StratosphereLinuxIPS

## Cybersecurity for small and medium-sized businesses: a practical framework for organizations with limited resources

UDK 004.056.53

Iurii Zhurov

*SMB Cybersecurity Advisors LLC, iurii.zhurov@smbsecurityadvisors.com*

Over the past decade, the number of cyber incidents targeting small and medium-sized businesses (SMBs) has grown at an accelerating rate. According to the Verizon Data Breach Investigations Report (2024), 46% of cyberattacks in the United States are directed at SMBs, while 60% of businesses that suffer a significant cyber incident cease operations within six months [1]. At the same time, the SMB segment — over 33 million enterprises accounting for 44% of U.S. GDP [2] — remains critically underprotected. The root cause lies not in the absence of standards, but in their inapplicability under conditions of limited resources.

Existing information security frameworks — NIST Cybersecurity Framework 2.0, ISO/IEC 27001:2022, and CIS Controls v8 — were designed primarily for large organizations with dedicated security departments, certified personnel, and substantial implementation budgets. For SMBs that typically lack any dedicated cybersecurity specialist, full implementation of these standards is practically unfeasible.

The objective of this paper is to develop and validate a practice-oriented framework for risk assessment and information security policy implementation, adapted to the specific organizational and resource constraints of SMBs, enabling achievement of a baseline cybersecurity posture without dedicated security personnel or significant financial investment.

Analysis of existing approaches revealed a systemic gap between academic standards and the real capabilities of SMBs. Specifically, ISO/IEC 27001 implementation requires 6 to 18 months and external consultants; NIST CSF, despite its declared scalability, provides no concrete tools for organizations without an IT department; CIS Controls v8 encompasses 18 control groups, of which only a subset is adapted to the SMB level [3-5].

Based on this analysis, the SMB Cybersecurity Framework: Assessment, Policy & Implementation was developed. The framework implements a four-stage methodology: (1) asset inventory and threat identification accounting for the enterprise's industry-specific context; (2) risk prioritization using a likelihood × impact matrix; (3) implementation of a minimum viable set of security policies — password policy, access control, data protection, and incident response; (4) a phased implementation roadmap with 30/90/180-day horizons and an employee security awareness program.

A distinguishing feature of the proposed approach is its prioritization of organizational over purely technical security measures. Practical consulting experience demonstrates that the vast majority of successful cyber incidents against SMBs are enabled by organizational vulnerabilities — absence of policies, inadequate access control, low staff awareness — rather than technical infrastructure deficiencies. Addressing organizational vulnerabilities is a necessary precondition for the effectiveness of any technical security controls.

A comparative analysis of the proposed framework against existing approaches is presented in Table 1.

Table 1

Comparative analysis of information security frameworks

| ***Criterion*** | *NIST CSF 2.0* | *ISO/IEC 27001* | *CIS Controls v8* | *SMB Framework (proposed)* |
|---|---|---|---|---|
| **SMB-oriented** | No | No | Partially | 209 |
| **No dedicated security staff required** | No | No | Partially | 220 |
| **Minimal budget** | No | No | Partially | Yes |
| **Phased implementation** | Yes | No | Yes | Yes |
| **Staff awareness training** | Partially | Partially | Yes | Yes |
| **Open access** | Yes | No | Yes | Yes |
| **Implementation complexity (1-10, lower is better)** | 7 | 9 | 6 | 2 |

The framework is distributed in open access and designed for independent implementation by SMB enterprises without external specialist involvement. Application of the approach across enterprises in multiple sectors confirmed its

practical feasibility and effectiveness in achieving a baseline cybersecurity posture under constrained resources.

The following conclusions can be drawn from this research: 1) existing information security frameworks exhibit a systemic gap with the actual needs of SMBs, making their full implementation impractical under resource constraints; 2) the proposed framework provides a practically achievable path to baseline cybersecurity, bridging the gap between academic standards and the real capabilities of small businesses; 3) prioritizing organizational security measures over technical ones is the key principle of effective cybersecurity for SMBs; 4) a phased approach with a 30/90/180-day horizon enables enterprises to systematically build their security posture in accordance with available resources.

1. Verizon Data Breach Investigations Report 2024. Basking Ridge: Verizon, 2024. 100 p.
2. U.S. Small Business Administration. Small Business Facts. Washington: SBA, 2024.
3. NIST Cybersecurity Framework 2.0. National Institute of Standards and Technology. Gaithersburg: NIST, 2024. 32 p.
4. ISO/IEC 27001:2022. Information security management systems — Requirements. Geneva: ISO, 2022. 19 p.
5. CIS Controls Version 8. Center for Internet Security. East Greenbush: CIS, 2021. 114 p.

## Аналіз векторів загроз корпоративній безпеці засобами автоматизованого інструмента OSINT

УДК 004.056

Владислав Загороднюк[1], Артем Соколов[2]

*Національний університет «Одеська політехніка»,*
*[1]10252811@stud.op.edu.ua, [2]sokolov.a.v@op.edu.ua*

Експоненційне зростання обсягів даних з відкритих джерел вимагає перегляду підходів до забезпечення корпоративної кібербезпеки [1]. Традиційні методи моніторингу демонструють низьку ефективність, оскільки фізично не здатні впоратися з потоками інформації та генерують багато хибних тривог. Автоматизація підготовки кібератак зловмисниками зумовлює потребу в симетричних рішеннях, що робить превентивну стратегію безпеки критично важливим фундаментом для бізнесу [2].

Метою роботи є розробка автоматизованого інструмента OSINT, який використовує передові архітектури штучного інтелекту, зокрема багатоагентні моделі та Retrieval-Augmented Generation (RAG), для виявлення та комплексного аналізу векторів загроз.

До ключових векторів загроз належать: 1) експлуатація зовнішньої поверхні атаки (тіньове IT); 2) глибоке ШІ-профілювання для атак соціальної інженерії; 3) масові витоки конфіденційних даних у публічних репозиторіях.

Наукова новизна дослідження полягає в інтеграції багатоагентної архітектури LangGraph із великою мовною моделлю Gemini 3.1, яка виступає як