RESEARCH ON RISKS AND CYBER THREATS AT THE ENTERPRISE AND DEVELOPMENT OF A SYSTEM TO ENSURE ITS INFORMATION SECURITY

Shapovalova Olena
Ph.D., Associate Professor
Department of Cybersecurity and Information Technologies
Karnauchenko Andriy
Master's degree student
Simon Kuznets Kharkiv National University of Economics,
Kharkiv, Ukraine

Information crime is becoming increasingly relevant as a specific type of illegal activity in cyberspace [1]. In the context of rapid digitalization and geopolitical instability, cybersecurity is becoming a critical factor for business survival. IT companies with research and development (R&D) departments are particularly at risk. Unlike the financial sector, where funds are the main asset, the main asset of R&D companies is intellectual property: source code, architectural solutions, and customer data.

The relevance of the study is due to the growing number of targeted attacks on supply chains and ransomware, which can instantly paralyze development processes. For medium-sized enterprises, which often do not have the budgets of large corporations, it is critically important to create an effective but economically sound protection system [2].

The aim of this work is to develop and design a comprehensive information security system for the IT company NovaTech Initiatives Ukraine based on a detailed analysis of risks and modern technological solutions.

The design of the protection system is based on a hybrid methodological approach. Analysis of existing standards has shown that for comprehensive protection, it is advisable to combine the process-oriented approach of ISO/IEC 27001 (for building an Information Security Management System — ISMS) [3] with specific technical controls and NIST frameworks (in particular, NIST SP 800-53 and Cybersecurity Framework) [4].

A qualitative-quantitative matrix method based on the recommendations of ISO/IEC 27005 was chosen for risk assessment. This approach allows risks to be classified by level (from low to critical) by comparing the probability of a threat occurring and its potential impact on business processes, which is optimal for medium-sized enterprises [5].

The practical part of the study is devoted to comprehensive audit of the IT infrastructure of the research object — NovaTech Initiatives Ukraine LLC. The audit, conducted using instrumental scanning (Tenable Nessus) and staff interviews, revealed a security status that can be characterized as reactive. Based on the audit results, the most critical vulnerabilities and key risks were identified and classified.

First, a flat network architecture was detected, in which all devices — including developers' workstations, database servers, and domain controllers — reside within a single logical segment. This configuration creates a critical risk in the event of compromise of any endpoint device.

Second, there is an absence of endpoint data encryption, in particular, full-disk encryption on corporate laptops. The unrestricted mobility of employees increases the likelihood of confidential R&D data leakage in the case of physical theft or loss of a device.

In addition, access to critical internal services is provided through single-factor authentication (password only), while the existing password complexity policy does not meet commonly accepted authentication requirements. This creates a high risk of user account compromise.

Due to the lack of proactive event monitoring, the processes of vulnerability detection, remediation, and software updating are not systematic and, therefore, cannot ensure reliable protection of information assets in the event of an incident. During the audit, a risk matrix was developed, identifying five critical and three high-level risks that require immediate response, including the risks of ransomware attacks and intellectual property leakage.

Based on the analysis of the current state of the organization's security posture, a target security architecture was designed in accordance with the principles of defense-in-depth and Zero Trust. The main components of the proposed system are as follows.

As part of the network architecture modernization, a transition from a flat network to a segmented topology was proposed. A dedicated demilitarized zone (DMZ) was implemented to host public services (website, VPN gateway), while the internal network was divided into isolated virtual local area networks (VLANs) according to functional responsibilities: R&D VLAN, Accounting VLAN, and Administration VLAN. To enhance the security level, inter-segment routing controlled by a next-generation firewall (NGFW) with strict access control lists (ACLs) was implemented. Formalized incident response playbooks were developed and adapted to the organizational structure of NovaTech Initiatives Ukraine. Detailed flowcharts were created for the scenarios "Ransomware Attack" and "Account Compromise", making it possible to standardize staff actions and significantly reduce response time to cyber threats (Fig. 1).

To mitigate the identified critical risks, a set of industrial-grade security solutions supported by technical enforcement mechanisms was selected. For data protection, mandatory deployment of Microsoft BitLocker was implemented on all corporate devices, with centralized storage of recovery keys in Active Directory, fully eliminating the risk of data leakage in the event of physical loss of a device.

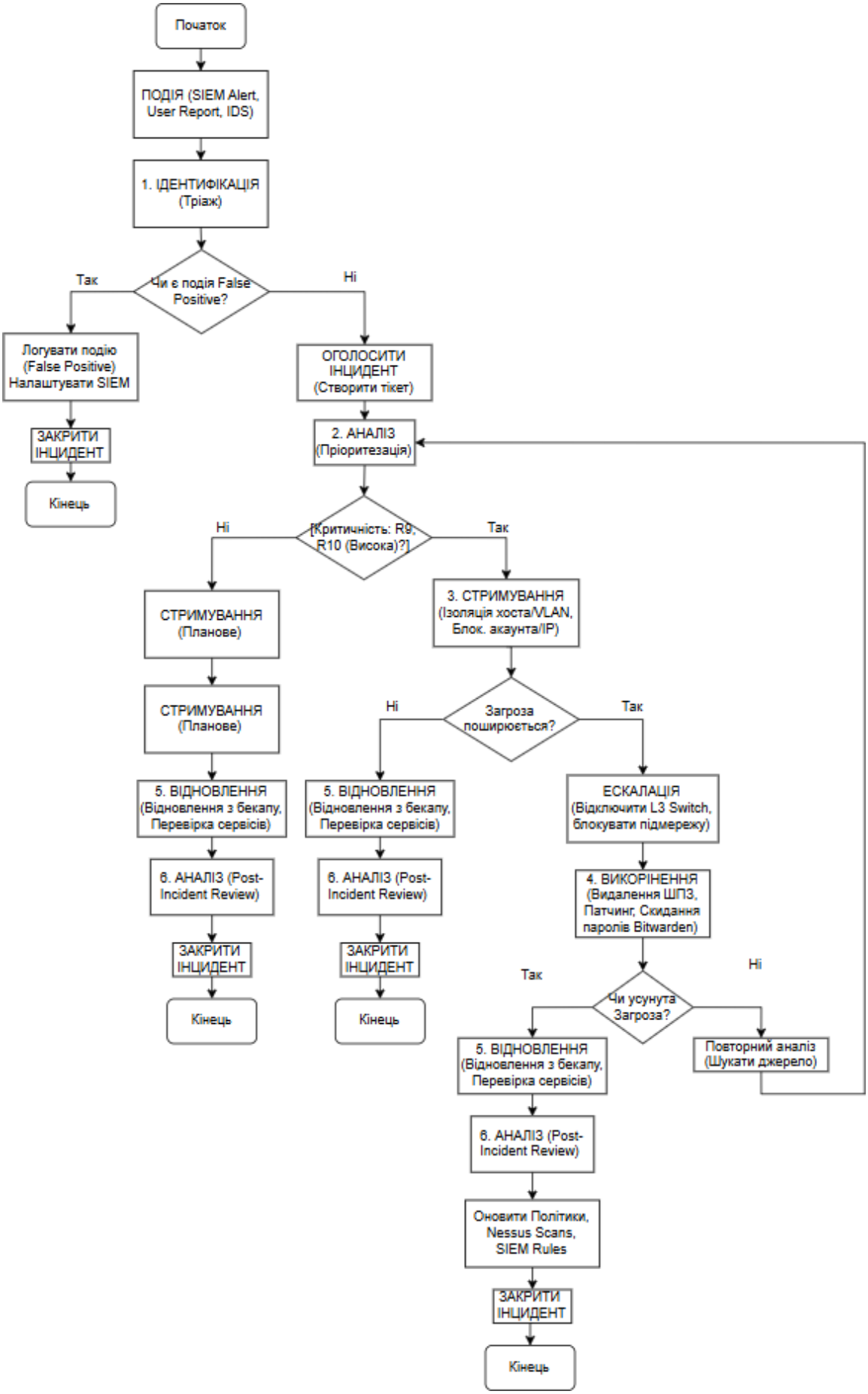

Fig. 1 – Algorithm for responding to cyber incidents

To improve access management, the Bitwarden Enterprise password manager was deployed, providing the generation of strong, unique passwords and enforcing multi-factor authentication (MFA) for access to corporate resources.

For vulnerability monitoring and remediation, the Tenable Nessus system was deployed with regular automated scanning of the infrastructure (both external perimeter and internal hosts), enabling proactive identification of emerging threats.

An innovative component of the study is the development of a proprietary software prototype for a cyberattack detection module (Web Application IDS/IPS) based on artificial intelligence technologies (Fig. 2).

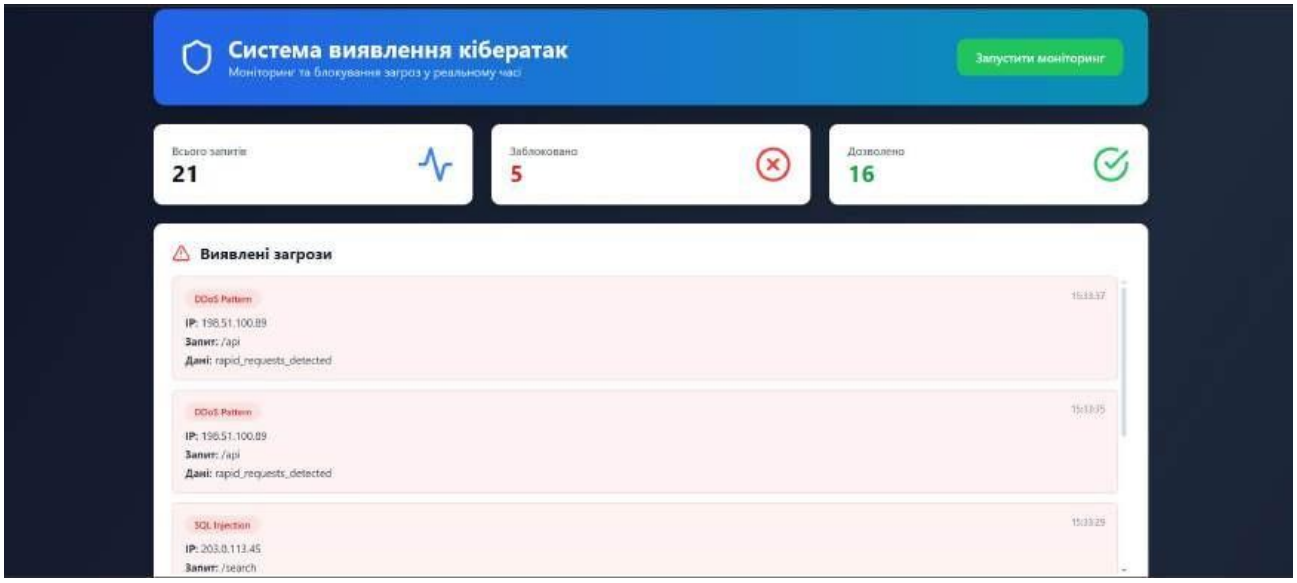

Fig. 2 – Main panel of the “Cyberattack Detection System”

The module is integrated into the web traffic flow and analyzes incoming HTTP requests in real time. Its key feature is the use of a language model to analyze the request payload for patterns of sophisticated attacks (such as SQL Injection, Cross-Site Scripting (XSS), Command Injection, etc.) that are difficult to detect using traditional signature-based methods. The module supports automatic blocking of malicious IP addresses, thereby enhancing the proactive nature of protection.

A critical aspect of security system implementation is the justification of its economic feasibility for the business. In this study, an effectiveness assessment was conducted using the Annualized Loss Expectancy (ALE) method and the Return on Security Investment (ROSI) indicator.

The results of the calculations showed that, prior to system implementation, with a high probability of a critical attack (estimated at 30% per year) and potential losses from a single incident amounting to $125,000 (equivalent to 2–3 days of downtime of the R&D department), the expected annual loss (ALE) was $37,500.

After the implementation of the system and the deployment of a comprehensive set of protective measures, the probability of a successful attack was reduced to 5%, which decreased the ALE to $6,250.

Regarding the economic effect, the annual investment costs for security tools (Nessus and Bitwarden licenses) amount to approximately $5,300. The net annual

savings resulting from the system implementation equal $25,950, while the Return on Security Investment (ROSI) is approximately 490%.

Thus, the proposed system is not only technically necessary but also a highly cost- effective investment that pays for itself by preventing even a single serious incident.

As a result of the conducted research, a scientific and practical problem of developing a comprehensive cybersecurity system for a medium-sized IT enterprise was solved. The transition from a flat, unsecured infrastructure to a layered defense system, incorporating network segmentation, modern access control and encryption mechanisms, as well as the implementation of innovative monitoring modules, makes it possible to significantly reduce business risks.

The proven economic efficiency confirms the feasibility and practical applicability of the proposed approach under real operating conditions of R&D companies.

References

1. Wikipedia Information crime URL: https://uk.wikipedia.org/wiki/Інформаційні_злочини (Date of access: 27.10.2025).

2. How computer viruses work: their mechanisms and methods of combating them URL: https://itproger.com/ua/news/kak-ustroeni-kompyuternie-virusi-ih-mehanizmi- i-metodi-borbi (Date of access: 27.10.2025).

3. ISO/IEC 27001 standard URL:https//zakon.isu.net.ua/sites/default/files/ normdocs/dstu_iso_iec_27001_2023.pdf (Date of access: 27.10.2025).

4. NIST Risk Management Framework (RMF) URL: https://en.wikipedia.org/ wiki/Risk_Management_Framework (Accessed 27.10.2025).

5. General Data Protection Regulation (GDPR) URL: https://gdpr-info.eu/ (Date of access: 27.10.2025).