КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.927
UDC 004.056.5:004.7

**Svitlana Lehominova**
Doctor of Economic Sciences, Professor,
Head of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-4433-5123
*chiarasvitlana77@gmail.com*

**Tetiana Kapeliushna**
Doctor of Economic Sciences, Associate Professor,
Professor of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0001-7490-6751
*e-skr@ukr.net*

**Yurii Shchavinskyi**
Candidate of Technical Sciences
Associate Professor, Associate Professor of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-2319-8983
*yushchavinsky@ukr.net*

**Mykhailo Zaporozhchenko**
PhD, Associate Professor of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0003-0182-9497
*zaporozhchenkomm@gmail.com*

**Oleksandr Budzynskyi**
Postgraduate Student, the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0009-0002-2402-0711
*oleksandr.email@gmail.com*

# CONCEPT OF AUTOMATED RESPONSE TO THREATS IN CORPORATE DATABASES IN REAL-TIME MODE

**Abstract.** The article presents a concept of automated real-time threat response in corporate databases, developed with consideration of current trends in cyber threat evolution and the limitations of existing protection mechanisms. The relevance of the research is determined by the growing number of database attacks, among which the most common remain SQL injections, unauthorized privilege escalation, insider activities, and lateral movement within corporate networks. Traditional approaches to database security, primarily focused on access control and signature-based detection, do not provide sufficient response speed and fail to address the complexity of multi-vector attacks. The study defines the conceptual principles of system design, including continuous monitoring, multi-level analysis, adaptability, and integration with existing security platforms. The proposed architecture combines data collection mechanisms, artificial intelligence–based analytics modules for anomaly detection, a SOAR subsystem for dynamic response, and integration with SOC and SIEM solutions. This combination ensures the implementation of a closed security loop: monitoring → analysis → response → management and control. The practical validation of the concept is demonstrated through scenarios of detecting SQL injections and identifying anomalous employee behavior, which confirms the system's ability to effectively counter both external and internal threats in real time. The differences of the proposed model from traditional solutions, its advantages (response speed, flexibility, scalability), and limitations

(dependence on configuration, resource intensity) are analyzed. The obtained results have scientific novelty, which lies in the development of a concept for an integrated architecture of automated threat response in corporate databases. The practical significance lies in the possibility of implementing the proposed concept in corporate systems to enhance their resilience against modern cyber threats.

**Keywords:** cybersecurity; threat response concept; database security; machine learning.

## INTRODUCTION

Corporate databases, in the context of modern digital transformation, have become one of the key elements of the information infrastructure of organizations. They contain financial, commercial, personal, and other sensitive data, the loss or compromise of which can lead to significant economic damage, reputational harm, and legal liability [1]. The increasing number of multi-stage attacks, in which adversaries combine various techniques and gradually escalate privileges, highlights the urgency of timely incident detection and prevention. Traditional approaches to database (DB) security, which are primarily focused on classical methods of access control, logging, and signature-based anomaly detection, are increasingly proving insufficient. They are not always capable of ensuring real-time threat detection and rapid response. A significant limitation of such methods is their orientation toward post-factum response after an incident has occurred or toward identifying only known attack signatures. At the same time, modern threats are characterized by high dynamism, complexity, and the ability to bypass classical protection mechanisms. This necessitates a shift from static protection methods to dynamic detection systems with automated real-time response.

In this regard, an urgent task is the development of a concept that integrates modern methods of monitoring, analytics, and automated response into a unified architecture for protecting corporate databases. Therefore, researchers in the field of corporate DB security are actively seeking new approaches, since classical methods have already become standard practices that attackers have learned to bypass.

**Statement of the problem.** Despite significant progress in the field of database (DB) security, existing solutions have a number of critical limitations. First, most systems are focused on reactive threat detection, which occurs only after an attack has already taken place. Second, the integration between monitoring, analytics, and response modules is often fragmented, which reduces the effectiveness of comprehensive protection. Third, the lack of flexible mechanisms for adapting to new types of attacks creates risks of rapid obsolescence of traditional security tools.

Thus, there is a clear need to develop a conceptual model of automated real-time threat response in corporate databases. Such a model should provide continuous activity monitoring, intelligent analysis of potential incidents using machine learning algorithms, and dynamic application of security policies to prevent or minimize the consequences of attacks.

**Analysis of recent research and publications.** A large number of domestic and foreign researchers have addressed the pressing issues of countering cyber threats to corporate databases (DBs). In recent years, scientific studies have proposed a range of methods for automated threat detection and response. Research confirms the growing role of machine learning (ML) and deep learning (DL) in combating modern cyber threats [2], [3]. These studies have shown promising results, but also reveal limitations such as weak generalization, deviation from real-world conditions, and lack of flexible integration with DB access policies. For example, in [4] the authors noted that, compared to traditional methods and ML-based approaches, some concept explanations are interleaved to make the methods easier to understand.

The study [5] focuses on analyzing current security issues of corporate DBs within modern infrastructure, developing a model for detecting anomalous database access activity, and integrating

it into the AlienVault SIEM system for automated threat response. It was established that one of the main problems in DB security is the need for immediate detection of access anomalies and rapid response to threats against confidentiality, availability, and integrity.

In the context of growing use of IoT devices and mobile technologies in corporate environments, studies [6], [7] analyzed key information security threats and IT system vulnerabilities to objectively assess the level of protection of government networks and registries under conditions of modern information and cyber warfare. These studies justified the necessity of conducting penetration tests in IT systems.

In [8]–[10], researchers evaluated strategies with a focus on encryption methods, authentication mechanisms, and access control applied to strengthen data security. The authors emphasized the importance of integrating artificial intelligence (AI) and ML for enhanced threat detection, applying blockchain to improve data integrity, and adopting zero-trust architectures.

An important step forward was the method proposed in [11], where the author suggested the use of the Isolation Forest algorithm for behavioral analysis of SQL queries, risk assessment, and automated response. A strong feature of this study is the classification of threats (high/medium/low), which enables automated risk-level determination. However, despite its effectiveness, this approach has certain limitations: a focus mainly on individual SQL queries without considering broader context, lack of integration with modern XDR solutions, insufficient attention to data confidentiality during model training, and limited use of hybrid DL algorithms for detecting complex anomalies.

The study [12]–[15] developed a method for configuring and managing public accounts and subscriptions on platforms such as AWS, GCP, and Azure, which involves standardized configurations to ensure optimal performance and compliance with security requirements. A key component of this methodology is periodic scanning of cloud accounts and subscriptions for compliance with recognized standards, including NIST 800-53, ISO 27001, HIPAA, and PCI DSS.

The majority of researchers conclude that further studies are needed in methods of analysis and automation of response actions, which would improve the security of corporate DBs under dynamic cyber threats. Existing works form a foundation for optimizing algorithms to enhance response speed, expanding data sources, and improving SIEM analytics to increase the accuracy of threat prediction. At the same time, they are conducted without a unified framework that would combine AI, data security, scalability, and transparency of DB protection.

Despite progress, current solutions still contain important gaps, mainly contextual limitations, as most methods focus on individual events or queries without considering broader business context, user roles, or historical behavior. Rarely are hybrid approaches applied, combining traditional algorithms (e.g., Isolation Forest) with deep neural networks (LSTM, Transformers, GNN). There is little implementation of database-level response within unified cybersecurity platforms due to the lack of integration with XDR/SOC ecosystems. Additionally, in blockchain-based approaches, immutable and transparent logging of threat response actions is often absent.

Thus, there is a need to develop a comprehensive concept of automated real-time threat response in corporate DBs. Such a concept should combine: hybrid ML/DL models; adaptive response policies considering business context and user roles; confidential data processing mechanisms (confidential computing, federated learning); transparent incident auditing tools based on distributed ledgers; and integration with XDR and SOC instruments to enhance the effectiveness of responding to complex, multi-layered attacks.

**The purpose** of the article is to develop and justify a concept of automated real-time threat response in corporate databases, which combines activity monitoring, intelligent threat analysis, and dynamic enforcement of security policies to minimize the risks of unauthorized access and ensure the integrity of critical data.

## RESEARCH RESULTS

### Conceptual principles for building a real-time automated response system

Defining conceptual principles is essential for ensuring the integrity and consistency of the research. They form the methodological foundation that makes it possible to align technical, organizational, and legal aspects into a unified structure, ensuring the effectiveness and efficiency of the developed model. Conceptual principles serve as guidelines for practical implementation, creating a basis for adapting the system to changes in the external environment and to new challenges in the field of information and cybersecurity. They also enable the evaluation and comparison of results, as well as the assessment of their compliance with strategic objectives and reliability criteria, thus ensuring the practical relevance of the research.

Taking into account previous studies [5], the proposed concept is based on a set of principles that determine the effectiveness and reliability of the threat response system in corporate databases (Fig. 1).


*Fig. 1. Basic principles of the concept*

1) The principle of continuous monitoring requires the system to continuously collect and analyze data on queries, transactions, and user actions in the DBMS in real time, which minimizes the likelihood of missed incidents.

2) The principle of multi-level threat analysis requires that incident detection should combine signature-based methods (for rapid identification of known attacks), behavioral models (to detect deviations from normal activity), and intelligent AI/ML algorithms (for anomaly classification and threat prediction).

3) The principle of contextual risk assessment implies that the criticality of an event is determined not only by the technical characteristics of a query but also by its context (user role, behavioral history, time of access, nature of the data). This reduces the number of false positives.

4) The principle of adaptive response requires the system to apply different levels of actions depending on the threat, for example: high level — blocking the query/session; medium level — privilege restriction or enhanced monitoring; low level — SOC notification with the option of escalation.

5) The principle of integration with existing infrastructure solutions prescribes interaction with Database Activity Monitoring (DAM), SIEM, and SOAR systems for centralized incident management and event correlation across the organization.

6) The principle of transparent logging and auditing requires that all system actions be recorded in immutable logs with the possibility of verification (with the prospect of using blockchain mechanisms), ensuring transparency and compliance with regulatory requirements.

7) The principle of privacy protection and standards compliance lies in the necessity of collecting and processing monitoring data in accordance with data privacy principles (e.g., GDPR) and secure computing technologies (confidential computing, federated learning).

8) According to the principle of scalability and resilience, the system architecture must support horizontal scaling (distributed database monitoring) and ensure high availability even during massive attacks or failure of individual components.

The defined conceptual principles for building an automated threat response system for corporate databases in real-time require specification in the form of an architectural solution. Each principle is reflected in the functional levels of the system: the principle of continuous monitoring is implemented at the data collection level, the principle of multi-level analysis — in the analytics module using AI/ML and SIEM, the principle of dynamic response — in the SOAR subsystem, and the principle of integration and centralized management — at the management level and interaction with the SOC. Thus, the system architecture emerges as a materialization of the conceptual provisions, ensuring coherence between the theoretical foundation and practical implementation.

**Automated response system architecture**

Based on the identified principles, a system architecture has been developed that ensures their practical implementation. The proposed architecture of the real-time automated response system consists of four interconnected levels (Fig. 2).

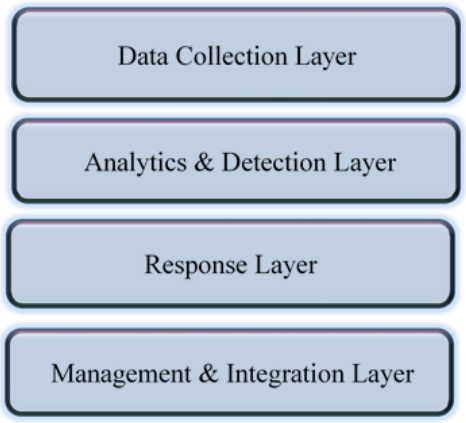


*Fig. 2. Automated response system architecture levels*

At the data collection layer (Data Collection Layer), the sources include database access logs (SQL, PostgreSQL, Oracle, etc.), system logs, network traffic, and transaction metadata.

Tools that can be used for data collection include Database Activity Monitoring (DAM), monitoring agents, and network traffic sensors, with the goal of ensuring continuous acquisition of raw data for further processing.

At the analytics and detection layer (Analytics & Detection Layer), AI/ML models (e.g., Isolation Forest, LSTM, Autoencoder) can be used to analyze user and transaction behavior patterns, detect deviations from the norm, and classify threat levels (low, medium, high), as well as to establish event correlation rules in SIEM.

At the response layer (Response Layer), to implement dynamic enforcement of security policies based assessed risk levels, SOAR platforms (e.g., IBM QRadar SOAR, TheHive) and orchestration modules should be used for automatic blocking of suspicious IP addresses, terminating sessions, modifying access policies, and executing verification scenarios.

At the management and integration layer (Management & Integration Layer), centralized control and integration with existing information security infrastructure should be provided by the SOC operator dashboard, reporting modules, and interfaces for integration with corporate systems (ERP, CRM).

Thus, the architecture combines DAM, SIEM, and SOAR solutions with AI/ML analytics, creating a closed loop: detection → analysis → response → management (including policy adaptation).

**Practical justification of the concept**

The architecture of the automated threat response system for corporate databases in real-time, developed based on conceptual principles, functions as a multi-level integrated model that combines monitoring, analysis, and response mechanisms.

At the first level — data collection — continuous monitoring of all database queries and user activity is performed using Database Activity Monitoring (DAM) agents, network sensors, and event logs. This ensures completeness of input information for subsequent analysis.

The second level is the analytics layer, where data is processed using machine learning algorithms and anomaly detection modules. The system evaluates each query in real-time based on multiple criteria (SQL query structure, execution context, action frequency, user behavior profile) and assigns a dynamic risk level (low, medium, high). A SIEM platform is used for event correlation, enabling detection of complex multi-vector attacks.

The third level is the response layer, where the SOAR (Security Orchestration, Automation, and Response) subsystem is employed. Depending on the threat level, the system applies predefined policies: for high risk — automatic blocking of a suspicious query or IP address; for medium risk — restriction of user privileges or forced re-authentication; for low risk — sending a warning to the SOC analyst.

The fourth level is management and integration, providing centralized control, data visualization, and information exchange with other security systems. Integration with the SOC creates a unified information space where all incidents are recorded, reports are generated, and opportunities for further analysis of response effectiveness are provided.

Thus, the architecture ensures a closed security loop: monitoring → analysis → response → management and control, minimizing the time between threat detection and the implementation of countermeasures.

**Concept application scenario**

To illustrate the practical implementation of the concept according to the proposed closed security loop, it is necessary to examine the system’s operation using the example of a classic SQL injection attack aimed at gaining unauthorized access to a corporate database. The results of the scenario analysis are summarized in Table 1.

*Table 1*

**Classic SQL injection attack scenario**

| Safety cycle | Actions |
|---|---|
| Request Monitoring | At the data collection level, the DAM agent records the SQL query sent from the web application to the database. The query contains suspicious constructs characteristic of SQL injections (e.g., OR 1=1 or the insertion of additional UNION SELECT operators). |
| Risk Analysis and Assessment | The machine learning algorithm classifies the query as a deviation from normal behavior by comparing it with the user's behavioral profile and statistics of legitimate queries. The system assigns a high threat level to the query. |
| Automated Response | The SOAR subsystem automatically blocks the execution of the query and logs the incident in the SIEM. Additionally, the source IP address of the attack is added to a blacklist, preventing repeated attempts. |
| Governance and Control (SOC Alerts and Audits) | The SOC analyst receives a notification with detailed information: the query content, source data, attack time, and the actions taken. This allows for a rapid assessment of the situation and informed decisions regarding further actions (e.g., initiating a web application review or adding additional rules to the security system). |

The proposed system provides real-time operational response to SQL injection attempts, minimizing the risk of data compromise and reducing the workload on the security team.

In corporate databases, a significant portion of incidents involves actions by legitimate users who have authorized access but abuse it. The system's operation in the case of an internal threat is presented in Table 2.

*Table 2*

**Insider threat scenario**

| Safety cycle | Actions |
|---|---|
| Request Monitoring | The DAM agent records the actions of an employee who normally executes 10–15 standard SQL queries to reference tables during working hours. However, outside of working hours, the system detects a series of atypical queries aimed at exporting a large volume of data from a confidential customer table. |
| Risk Analysis and Assessment | The User and Entity Behavior Analytics (UEBA) module compares the user's actions with their profile and group statistics. The ML algorithm detects significant deviations:<br>– unusual access time;<br>– abnormal query volume;<br>– execution of queries beyond the user's typical role.<br>The queries are assigned a high threat level. |
| Automated Response | The SOAR subsystem blocks the user's further actions and temporarily restricts their database access. If necessary, forced session termination is applied. |
| Governance and Control (SOC Alerts and Audits) | The SOC receives an alert containing the user ID, access time, nature of the queries, and an automatically generated risk assessment. The analyst can initiate an internal investigation or enforce stricter access policies. |

This scenario demonstrates the system's ability to detect and block insider actions by users who technically have legitimate access but use it in violation of security policies. Thus, the concept ensures protection not only against external attacks but also against internal threats, which is critically important for modern corporate environments.

The presented scenario examples (SQL injection and internal threat) allow the following conclusions to be drawn:

– the system provides real-time threat detection, through continuous monitoring and query analytics, it can quickly identify both external and internal incidents;

- AI/ML models enhance detection accuracy, and user behavior and query anomaly analysis allow differentiation between legitimate actions and potentially dangerous ones, reducing false positives;
- automated response minimizes risks and reaction time; blocking suspicious queries or restricting user privileges occurs without operator intervention, significantly reducing the likelihood of data compromise;
- the architecture enables protection of databases from external attacks (SQL injections), internal threats (access abuse), and potentially more complex scenarios, such as lateral movement within the network;
- integration with the SOC and logging ensures control and auditability; all system actions are recorded and notify SOC analysts, supporting transparency, facilitating investigations, and improving security policies.

The proposed architecture concept for corporate database cybersecurity has several significant advantages. First, it is based on an integrated approach combining monitoring, user behavior analysis, and automated incident response. This reduces the time between threat detection and appropriate action, enhancing the resilience of the corporate infrastructure against attacks. Second, the architecture is designed for adaptability, i.e., the ability to update algorithms and security rules based on new attack scenarios and external intelligence data (OTX, STIX/TAXII). Third, the implementation of the multi-layered protection principle minimizes the risk of system compromise even if one layer of defense is bypassed.

Compared to existing approaches, which are mostly based on static access control or solely on IDS/IPS tools, the proposed architecture stands out due to its synergistic combination of monitoring, anomaly detection, and automated response technologies. This creates conditions for dynamic database security management, rather than mere passive log collection or isolated attack blocking.

At the same time, the concept has certain limitations. First, system effectiveness largely depends on correct rule configuration and proper training of anomaly detection models; insufficient preparation may result in false positives or missed threats. Second, implementing the architecture requires additional computing resources, which may be critical for organizations with limited infrastructure. Third, integration with existing corporate security processes may require changes to access policies and incident response procedures, necessitating organizational effort and staff training.

## CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH

The article proposes a concept for automated real-time threat response in corporate databases. It is based on the principles of continuous monitoring, multi-level analysis, dynamic response, and integration with existing information security management systems. The proposed architecture combines data collection modules, AI/ML-based analytical mechanisms, a SOAR subsystem, and SOC integration, providing a closed security management loop: monitoring → analysis → response → management and control.

The practical justification of the concept is demonstrated through scenarios involving the detection of SQL injections and insider threats, confirming the system’s ability to quickly identify and neutralize incidents. A comparison with existing approaches demonstrates that the proposed model offers advantages in response speed, flexibility, and scalability, though it requires careful configuration and sufficient resources.

The results have both scientific and practical significance. The scientific novelty lies in the development of an integrated architecture concept for automated threat response in corporate databases. The practical significance lies in the potential application of this concept to the design of modern systems to protect corporate environments from internal and external attacks.

Future research will focus on applying simulations to test the architecture's resilience against new types of attacks, exploring organizational aspects of implementing automated response system interaction with SOC personnel, and developing methodological recommendations for training staff on the use of the new architecture.

## REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Almaiah, M. A., Saqr, L. M., Al-Rawwash, L. A., Altellawi, L. A., Al-Ali, R., & Almomani, O. (2024). Classification of cybersecurity threats, vulnerabilities and countermeasures in database systems. *Computers, Materials & Continua*, 1–10. https://doi.org/10.32604/cmc.2024.057673
2. Raji, A. N., Olawore, A. O., Ayodeji, A., & Joseph, J. (2023). Integrating artificial intelligence, machine learning, and data analytics in cybersecurity: A holistic approach to advanced threat detection and response. *World Journal of Advanced Research and Reviews, 20*(3), 2005–2024. https://doi.org/10.30574/wjarr.2023.20.3.2741
3. Guo, Y. (2022). A review of machine learning-based zero-day attack detection: Challenges and future directions. *Computer Communications, 198*, 175–185. https://doi.org/10.1016/j.comcom.2022.11.001
4. Wang, Y., Xi, J., & Cheng, T. (2021). The overview of database security threats' solutions: Traditional and machine learning. *Journal of Information Security, 12*(1), 34–55. https://doi.org/10.4236/jis.2021.121002
5. Shchavinskyi, Y., & Budzynskyi, O. (2025). Analysis of current problems of security of corporate databases in the conditions of modern infrastructure and ways to solution them. *Cybersecurity: Education, Science, Technique, 3*(27), 390–405. https://doi.org/10.28925/2663-4023.2025.27.726
6. Kostiuk, Y., Bebeshko, B., Kriuchkova, L., Lytvynov, V., Oksanych, I., Skladannyi, P., & Khorolska, K. (2024). Information protection and data exchange security in wireless mobile networks with authentication and key exchange protocols. *Cybersecurity: Education, Science, Technique, 1*(25), 229–252. https://doi.org/10.28925/2663-4023.2024.25.229252
7. Kyrychok, R. V., Skladannyi, P. M., Buriachok, V. L., Hulak, H. M., & Kozachok, V. A. (2016). Problems of ensuring control over the security of corporate networks and ways to solve them. *Scientific Notes of the Ukrainian Research Institute of Communications, 3*(43), 48–61. https://journals.dut.edu.ua/index.php/sciencenotes/article/view/772/716
8. Adenubi, A. O., & Oduroye, P. A. (2024). Data security in big data: Challenges, strategies, and future trends. *International Journal of Research in Education Humanities and Commerce, 5*(2), 1–15. https://doi.org/10.37602/ijrehc.2024.5201
9. Bao, R., Chen, Z., & Obaidat, M. S. (2018). Challenges and techniques in big data security and privacy: A review. *Security and Privacy, 1*(4), e13. https://doi.org/10.1002/spy2.13
10. Li, X., Wang, Z., Leung, V. C. M., Ji, H., Liu, Y., & Zhang, H. (2021). Blockchain-empowered data-driven networks. *ACM Computing Surveys, 54*(3), 1–38. https://doi.org/10.1145/3446373
11. Budzynskyi, O. (2025). Method of detecting vulnerabilities and automated response in corporate database protection systems. *Modern Information Security, 62*(2). https://doi.org/10.31673/2409-7292.2025.029259
12. Matseniuk, Y., & Partyka, A. (2024). The concept of automated compliance verification as the foundation of a fundamental cloud security model. *Computer Systems and Networks, 6*(1), 108–123. https://doi.org/10.23939/csn2024.01.108
13. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). *Information and communication systems security* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
14. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Information security systems* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
15. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). *Enterprise information and cyber security* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

**Легомінова Світлана Володимирівна**
доктор економічних наук, професор, завідувачка кафедри управління
кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID:0000-0002-4433-5123
*chiarasvitlana77@gmail.com*

**Капелюшна Тетяна Вікторівна**
доктор економічних наук, доцент, професор кафедри управління
кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID:0000-0001-7490-6751
*e-skr@ukr.net*

**Щавінський Юрій Віталійович**
канд. техн. наук, доцент, доцент кафедри управління
кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0000-0002-2319-8983
*yushchavinsky@ukr.net*

**Запорожченко Михайло Михайлович**
доктор філософії, доцент кафедри управління
кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0000-0003-0182-9497
*zaporozhchenkomm@gmail.com*

**Будзинський Олександр Володимирович**
аспірант кафедри управління
кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0002-2402-0711
*oleksandr.email@gmail.com*

# КОНЦЕПЦІЯ АВТОМАТИЗОВАНОГО РЕАГУВАННЯ НА ЗАГРОЗИ В КОРПОРАТИВНИХ БАЗАХ ДАНИХ У РЕЖИМІ РЕАЛЬНОГО ЧАСУ

**Анотація.** У статті представлено концепцію автоматизованого реагування на загрози в корпоративних базах даних у режимі реального часу, розроблену з урахуванням сучасних тенденцій розвитку кіберзагроз та обмежень існуючих засобів захисту. Актуальність дослідження обумовлена зростанням кількості атак на бази даних, серед яких найбільш поширеними залишаються SQL-ін'єкції, несанкціоноване підвищення привілеїв, інсайдерські дії та бічне переміщення у корпоративних мережах. Традиційні підходи до захисту баз даних, орієнтовані переважно на контроль доступу та сигнатурне виявлення, не забезпечують достатньої швидкості реагування і не враховують складність багатовекторних атак. У роботі визначено концептуальні принципи побудови системи, серед яких безперервний моніторинг, багаторівневий аналіз, адаптивність та інтеграція з існуючими платформами безпеки. Запропонована архітектура поєднує засоби збору даних, модулі аналітики на основі штучного інтелекту для виявлення аномалій, підсистему динамічного реагування SOAR та інтеграцію з SOC і SIEM-рішеннями. Таке поєднання забезпечує реалізацію замкненого циклу безпеки: моніторинг → аналіз → реагування → управління і контроль. Практичне обґрунтування концепції продемонстровано на прикладі сценаріїв виявлення SQL-ін'єкцій та ідентифікації аномальної поведінки співробітників, що підтверджує здатність системи ефективно протидіяти як зовнішнім, так і внутрішнім загрозам у режимі реального часу. Проаналізовано відмінності запропонованої моделі від традиційних рішень, її переваги (швидкість реагування, гнучкість, масштабованість) та обмеження (залежність від налаштувань, ресурсомісткість). Отримані результати мають наукову новизну, яка полягає у формуванні концепції інтегрованої архітектури автоматизованого реагування на загрози в

корпоративних базах даних. Практичне значення полягає у можливості впровадження розробленої концепції у корпоративні системи для підвищення їх стійкості до сучасних кіберзагроз.

**Ключові слова:** кібербезпека; концепція реагування на загрози; безпека баз даних; машинне навчання.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Almaiah, M. A., Saqr, L. M., Al-Rawwash, L. A., Altellawi, L. A., Al-Ali, R., & Almomani, O. (2024). Classification of cybersecurity threats, vulnerabilities and countermeasures in database systems. *Computers, Materials & Continua*, 1–10. https://doi.org/10.32604/cmc.2024.057673
2. Raji, A. N., Olawore, A. O., Ayodeji, A., & Joseph, J. (2023). Integrating artificial intelligence, machine learning, and data analytics in cybersecurity: A holistic approach to advanced threat detection and response. *World Journal of Advanced Research and Reviews, 20*(3), 2005–2024. https://doi.org/10.30574/wjarr.2023.20.3.2741
3. Guo, Y. (2022). A review of machine learning-based zero-day attack detection: Challenges and future directions. *Computer Communications, 198*, 175–185. https://doi.org/10.1016/j.comcom.2022.11.001
4. Wang, Y., Xi, J., & Cheng, T. (2021). The overview of database security threats' solutions: Traditional and machine learning. *Journal of Information Security, 12*(1), 34–55. https://doi.org/10.4236/jis.2021.121002
5. Shchavinskyi, Y., & Budzynskyi, O. (2025). Analysis of current problems of security of corporate databases in the conditions of modern infrastructure and ways to solution them. *Cybersecurity: Education, Science, Technique, 3*(27), 390–405. https://doi.org/10.28925/2663-4023.2025.27.726
6. Kostiuk, Y., Bebeshko, B., Kriuchkova, L., Lytvynov, V., Oksanych, I., Skladannyi, P., & Khorolska, K. (2024). Information protection and data exchange security in wireless mobile networks with authentication and key exchange protocols. *Cybersecurity: Education, Science, Technique, 1*(25), 229–252. https://doi.org/10.28925/2663-4023.2024.25.229252
7. Kyrychok, R. V., Skladannyi, P. M., Buriachok, V. L., Hulak, H. M., & Kozachok, V. A. (2016). Problems of ensuring control over the security of corporate networks and ways to solve them. *Scientific Notes of the Ukrainian Research Institute of Communications, 3*(43), 48–61. https://journals.dut.edu.ua/index.php/sciencenotes/article/view/772/716
8. Adenubi, A. O., & Oduroye, P. A. (2024). Data security in big data: Challenges, strategies, and future trends. *International Journal of Research in Education Humanities and Commerce, 5*(2), 1–15. https://doi.org/10.37602/ijrehc.2024.5201
9. Bao, R., Chen, Z., & Obaidat, M. S. (2018). Challenges and techniques in big data security and privacy: A review. *Security and Privacy, 1*(4), e13. https://doi.org/10.1002/spy2.13
10. Li, X., Wang, Z., Leung, V. C. M., Ji, H., Liu, Y., & Zhang, H. (2021). Blockchain-empowered data-driven networks. *ACM Computing Surveys, 54*(3), 1–38. https://doi.org/10.1145/3446373
11. Budzynskyi, O. (2025). Method of detecting vulnerabilities and automated response in corporate database protection systems. *Modern Information Security, 62*(2). https://doi.org/10.31673/2409-7292.2025.029259
12. Matseniuk, Y., & Partyka, A. (2024). The concept of automated compliance verification as the foundation of a fundamental cloud security model. *Computer Systems and Networks, 6*(1), 108–123. https://doi.org/10.23939/csn2024.01.108
13. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). *Information and communication systems security* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
14. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Information security systems* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
15. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). *Enterprise information and cyber security* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.