http://doi.org/10.35784/iapgos.6993 received: 26.12.2024 | revised: 30.11.2025 | accepted: 09.12.2025 | available online: 20.12.2025

ANALYSIS OF MODERN TOOLS, METHODS OF AUDIT AND MONITORING OF DATABASE SECURITY

Kateryna Mykhailyshyn[1], Oleh Harasymchuk[1], Oleh Deineka[1], Yurii Dreis[2], Volodymyr Shulha[3], Yuriy Pepa[3]

[1]Lviv Polytechnic National University, Lviv, Ukraine, [2]Mariupol State University, Kyiv, Ukraine, [3]State University of Information and Communication Technologies, Kyiv, Ukraine

Abstract. *The mismatch between modern technological innovations and traditional approaches to information security can significantly affect the effectiveness of database monitoring systems. This paper examines the ethical and legal aspects of database monitoring, taking into account current regulatory requirements and the importance of maintaining data confidentiality. The study also evaluates the use of each tool to determine their effectiveness in real-world conditions, the possibility of improving the functional characteristics of monitoring systems, their adaptation to new technologies and increasing the overall level of information protection.*

Keywords: databases, audit, monitoring, cybersecurity, data protection, security management

ANALIZA NOWOCZESNYCH NARZĘDZI, METOD AUDYTU I MONITOROWANIA BEZPIECZEŃSTWA BAZ DANYCH

Streszczenie. *Niedopasowanie nowoczesnych innowacji technologicznych do tradycyjnych podejść do bezpieczeństwa informacji może znacząco wpłynąć na skuteczność systemów monitorowania baz danych. W niniejszym artykule zbadano etyczne i prawne aspekty monitorowania baz danych, biorąc pod uwagę obecne wymogi regulacyjne i znaczenie zachowania poufności danych. W badaniu oceniono również wykorzystanie każdego narzędzia w celu określenia ich skuteczności w warunkach rzeczywistych, możliwości poprawy cech funkcjonalnych systemów monitorowania, ich dostosowania do nowych technologii i zwiększenia ogólnego poziomu ochrony informacji.*

Słowa kluczowe: bazy danych, audyt, monitorowanie, cyberbezpieczeństwo, ochrona danych, zarządzanie bezpieczeństwem

Introduction

With rapid digitalization and global information integration, the volume of data is growing rapidly, making it an extremely valuable asset and, consequently, making its security a critical aspect for any organization. Databases (DBs) are the main components of the information infrastructure, providing storage, management and access to critical data used to support the functioning of modern information systems. They form the basis for decision-making at all levels of organizational activity, from operational processes to strategic planning, and ensure the integrity, confidentiality and availability of business and security-critical data, which is becoming a top priority. That is why the issues of database security are receiving increased attention and various approaches and methods are being developed to protect them [3, 4, 15, 20, 24]. In this regard, audit and monitoring of databases [7, 9, 10, 12, 23] are of particular importance as security management tools. This research article is aimed at a comprehensive analysis of modern tools, methods of audit and monitoring of databases.

An important aspect is also the comparison of monitoring methods, in particular reactive and proactive approaches [14, 22], since each of them has its own characteristics, advantages and limitations in the context of database security. The study allows determining their effectiveness in different scenarios and identifying best practices for the optimal use of the method to improve the overall level of security of information systems. The study of the implementation of an audit and monitoring environment for modern information and communication systems and networks has already been the subject of numerous studies and scientific publications [2, 8, 16–18, 25, 29], which formulate basic rules and recommendations for access control and monitoring processes of information networks.

The general concept of modern works and studies on this issue shows that database audit and monitoring are important tools for ensuring the security and efficiency of information systems. They allow you to track user activity, identify potential threats and prevent unauthorized access to data. Regular audits help to identify vulnerabilities in the system, which allows you to respond to problems in a timely manner and improve the reliability of databases. In addition, monitoring allows you to track database performance, which is important to ensure stable and fast software operation. As a result, these measures help organizations comply with regulatory requirements and ensure data privacy.

The purpose of this article is to provide a detailed analysis and comparison of modern tools for auditing and monitoring database security, including SQL Server Audit, Oracle Audit Vault, IBM Guardium and others, in the context of growing cyber threats. It seeks to identify the strategic potential of integrating these tools with the latest technologies, such as machine learning and artificial intelligence, to create a comprehensive approach to database security and real-time anomaly and threat detection, providing recommendations for improving monitoring systems to increase the level of database protection in order to ensure confidentiality and integrity of information in the modern digital environment. The work will demonstrate testing of a prototype of such a monitoring system for a specific DBMS, which will allow us to evaluate the effectiveness and provide recommendations for the implementation of such systems in real-world conditions, taking into account ethical and legal aspects.

To perform this work, the following tasks will be performed:

- comparison of modern tools in terms of usability, performance and cost, including a comprehensive analysis of the functions of each system;
- consideration of reactive and proactive approaches, assessment of their application in real conditions;
- analyzing the role of machine learning and cloud platforms in audit and monitoring;
- assessment of regulatory requirements and data privacy for each tool.

The study examines modern tools for auditing and monitoring databases to assess their effectiveness, functionality and feasibility in various industries. In particular, the following were analyzed:

Structured Query Language Server Audit [19, 32] is a tool built into Microsoft SQL Server that allows for detailed auditing and monitoring of events such as data access and configuration changes.

Oracle Audit Vault [1, 31, 33, 34] is a comprehensive solution from Oracle that provides centralized auditing and monitoring of database activity, as well as threat protection by collecting and analyzing event logs from various sources within the corporate infrastructure.

Table 1. Comparative characteristics of security management tools

Tool	Productivity	Ease of use	Cost	Successful implementation cases
SQL Server Audit	High for SQL Server databases, performance impact is minimal if audit parameters are properly configured	Integration with SQL Server, easy to use for SQL administrators.	A Standard Edition license costs $3,717 per core, Enterprise Edition $14,256 per core. Express is available for small companies, which is free of charge.	Used in financial institutions - banks, insurance companies and investment firms for detailed audit of transactions.
Oracle Audit Vault	High, especially for Oracle databases, with the ability to scale	Flexible for auditing, allows for detailed customization of functions to meet user needs, requires considerable training to fully master.	OAV & Database Firewall costs $10,000 per processor licensed unit or $200 per user (min. 25).	Widely used in government agencies - the Ministry of Defense, Finance, and Justice to monitor access to confidential information.
IBM Guardium	High performance for large corporate environments, efficient under heavy loads.	User-friendly interface, flexible in configuration, but requires special knowledge in the field of information security and database administration.	Data Protection starts at $20,000 for a basic license. The cost increases with the size of the implementation, the number of protected databases and the additional modules required.	Used in international banks to protect data and comply with regulatory requirements.
Splunk	High, but may require significant resources such as CPU, RAM, and disk space to process large amounts of data.	Powerful interface focused on data analysis, but difficult to configure.	The license depends on the amount of data indexed daily. A standard license costs from $150 per gigabyte of data per day.	It is used in IT companies to monitor and analyze security logs.
Imperva Secure Sphere	High performance for real-time monitoring and protection.	Intuitive interface, a wide set of functions, such as in-depth user monitoring or automated incident response, but requires skills to configure.	Ranging from $25,000 to $100,000 per server depending on configuration, includes support and the option of additional features - web application protection.	Used in retail - Walmart, Target and Tesco to protect customer data and prevent information leaks.

IBM Guardium [30, 31] is a powerful data security management platform that provides the ability to monitor and audit databases, detect threats in real time, manage user privileges, and ensure compliance with regulatory standards.

Splunk [36, 37] is a tool for collecting, analyzing and monitoring data, including database logs, used for threat detection, auditing and regulatory compliance.

Imperva SecureSphere [35] is a database monitoring technology that includes protection against unauthorized access, auditing, user privilege control and anomaly detection.

To analyze and evaluate the effectiveness of these tools, we analyzed their performance, usability and cost, as well as analyzed successful cases of their implementation in various industries.

Comparative characteristics of security management tools are presented in Table 1.

Since existing solutions for auditing and monitoring databases often do not fully meet the rapidly changing conditions of cyber threats, further active work is underway to develop approaches in this area [5, 6, 11, 13, 27].

The analysis showed that all the tools under consideration demonstrate high performance in their respective environments. However, their functionality and requirements vary significantly depending on the specific needs of the organization. This result highlights the need for further adaptation and development of tools to ensure their effectiveness in a rapidly changing cyber environment.

1. Database security tools: overview and analysis

A comprehensive analysis of the functionality of key database security tools, such as SQL Server Audit, Oracle Audit Vault, IBM Guardium, Splunk and Imperva SecureSphere, allows us to assess their effectiveness and compliance with the requirements of modern information systems. These tools perform critical tasks, including change auditing, access monitoring, anomaly detection, and data leakage prevention, which are crucial for protecting confidential information and maintaining compliance with regulatory requirements. For a better understanding, let's analyse the main functions of information system control and oversight tools:

Structured Query Language Server (Fig. 1) Audit provides an audit of changes in databases, allowing you to track user actions and changes in table structures. The collected data is stored in audit logs, which makes it possible to detect unauthorized actions and ensure their proper control. Additionally, the tool monitors access to databases, tracking successful and unsuccessful attempts to log in to the system, which improves the protection of information resources.

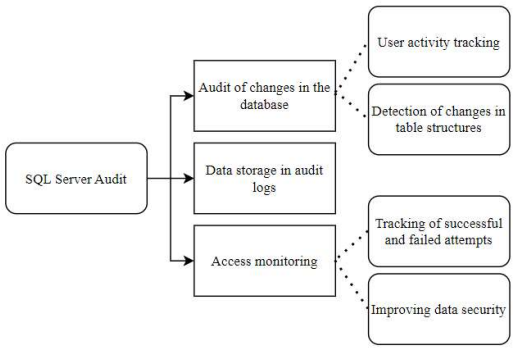

Fig. 1. SQL Server Audit functionality

Oracle Audit Vault (Fig. 2) consolidates audit logs from numerous systems, providing an opportunity to monitor user activity in Oracle databases. By processing the collected information, Oracle Audit Vault is able to detect anomalous actions or security policy violations. The proactive risk management provided by this tool prevents data leaks by automatically responding to illegal actions, which increases the overall level of protection.

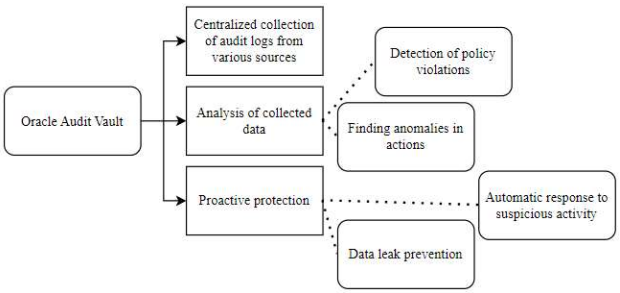

Fig. 2. Oracle Audit Vault functionality

IBM Guardium (Fig. 3) is noted for its ability to detect anomalies using analytical approaches to identify user behavior patterns that may indicate potential security threats. The tool collects data from various databases and analyses it in real time, which allows for a quick response to incidents. In addition, Guardium provides access monitoring, which reduces the risk of unauthorized actions.

Splunk (Fig. 4) specializes in collecting and indexing logs from various sources, including databases, allowing organizations to conduct in-depth analysis of user activity, detect anomalies, and respond quickly to threats. The data collected by the tool can be presented in the form of reports for further analysis.

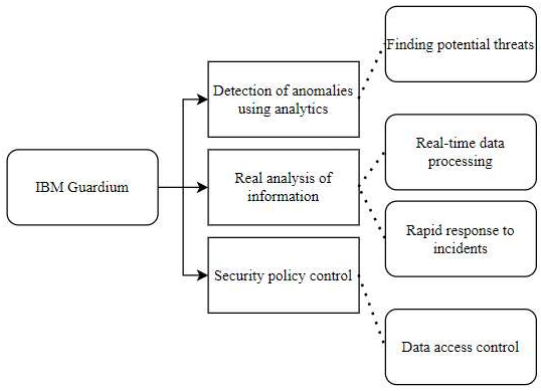

Fig. 3. IBM Guardium functionality

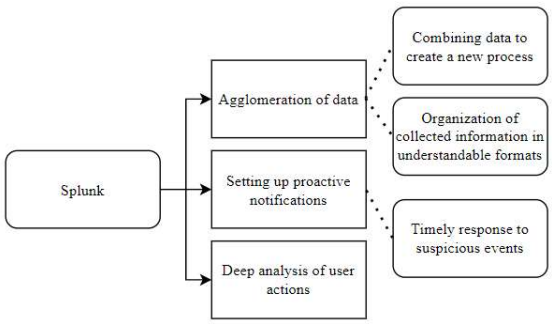

Fig. 4. Splunk functionality

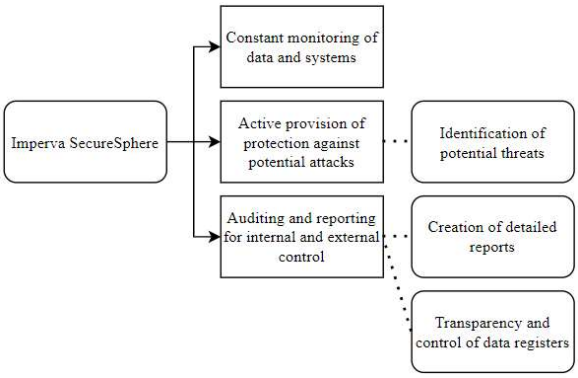

Fig. 5. Imperva SecureSphere functionality

Imperva SecureSphere (Fig. 5) is a tool that provides continuous database monitoring and real-time protection against attacks. It collects data on all system activities, analyses it to detect threats, and implements proactive protection. In addition, SecureSphere provides extensive auditing and reporting capabilities, enabling detailed reports for internal controls and external auditors, which increases the clarity and regulation of data registers.

The functionality of each tool is realized through the processing of significant amounts of data generated during system operation. This data may include audit logs, user actions, configuration changes, and other important indicators. The collected information is analyzed using built-in analytical mechanisms to detect anomalies, ensure compliance with security policies and prevent potential threats. The results of the analysis are usually presented in the form of reports, dashboards, or automatic alerts to ensure prompt response to incidents and maintain a high level of security. To achieve maximum security efficiency, it is important not only to record events after they occur, but also to predict their possible consequences. That's why we believe that moving to a comparison of reactive and proactive monitoring strategies allows us to understand how these approaches can complement each other to ensure comprehensive database protection.

2. Methods of database monitoring: comparing reactive and proactive strategies

The strategies used to protect data and ensure the smooth functioning of information systems are also known as reactive and proactive approaches to database monitoring. It's worth taking a closer look at each method to understand their role in ensuring data protection and ensuring that digital platforms are up and running reliably.

A reactive approach to database monitoring involves taking active steps only after an undesirable event or threat has already occurred. The focus is on identifying and responding to incidents that have already occurred. This method includes several key stages:

- ***Incident detection***. The focus is on detecting problems or anomalies only after they occur.
- ***Event analysis.*** Processes that occurred in databases are collected and stored in logs and analyzed to identify the causes and consequences of incidents.
- ***Audit.*** The collected material is used for retrospective analysis, i.e., to understand what happened and take appropriate measures to avoid similar problems in the future.

The proactive approach to database monitoring, unlike the reactive approach, is aimed at preventing threats. It is achieved by continuously monitoring activity, analyzing behavioral patterns, and detecting anomalies in real time in systems. The key stages of the proposed method include the following:

- ***Threat prediction.*** Monitoring uses analytical tools to identify potential vulnerabilities before they actually occur.
- ***Behavioral pattern analysis.*** Systems use algorithms and models to identify atypical behavioral patterns that may indicate potential threats.
- ***Incident prevention.*** Based on the predictions and data obtained, measures are taken, such as setting up security systems and implementing access control policies, to prevent possible vulnerabilities.
- ***Rapid response.*** The system automatically takes measures to eliminate threats or reduce their impact.

When choosing an approach to monitoring data management systems, it is important to consider whether the system is reactive, proactive, or a combination of both. For a better understanding of how different tools implement these approaches, Table 2 shows the features of the strategies in a comparative form for popular database monitoring tools.

This mapping provided us with a clear picture of how different tools implement control and security approaches. Depending on your specific security requirements and organizational needs, the choice between these systems can have a significant impact on the effectiveness of managing and protecting data in your infrastructure. The decision should take into account not only the current needs of the organization, but also its ability to adapt to rapid changes in the cybersecurity environment.

Table 2. Visualizations of the choice between reactive and proactive approaches

Tool	Reactive approach	Proactive approach	A combined approach
IBM Guardium	Collection and storage of event data for further auditing.	x	x
Imperva SecureSphere	Collection of audit logs for further analysis.	x	x
Oracle Audit Vault	x	Real-time activity monitoring, anomaly detection, automatic response.	x
Splunk	x	Continuous monitoring and operational protection, as well as automatic actions.	x
SQL Server Audit	Deep analysis of event data and retention for further action.	Setting up proactive alerts to prevent threats.	Support for both approaches.

With this in mind, it is a logical step to explore the opportunities offered by the latest technologies, such as the use of artificial intelligence and machine learning in detecting database threats. These technologies can significantly increase the level of protection by providing proactive detection and response to potential threats.

3. Opportunities for integrating artificial intelligence and machine learning into database audit and monitoring tools

Artificial intelligence is opening up new horizons in database security, allowing threats to be prevented before they can cause damage [21, 28]. Thanks to the ability to analyze large amounts of data in real time, a self-learning tool is able to detect anomalies in user and system behavior that may signal potential threats. This allows not only to detect known threats but also to learn from new ones, adapting the security system to new challenges. Combined with the integration of cloud technologies that provide scalability, reliability, and efficient resource management, these approaches create powerful database audit and monitoring solutions that can withstand modern threats. Cloud platforms allow you to securely store and process large amounts of data, providing quick access to it at any time. In addition, cloud technologies provide high fault tolerance and automatic backup capabilities, making them an integral element of modern database security systems.

The transition to using database auditing and monitoring tools such as SQL Server Audit, Oracle Audit Vault, IBM Guardium, Splunk, and Imperva SecureSphere requires a thorough analysis of their capabilities in terms of integration with machine intelligence technologies and cloud solutions.

SQL Server Audit has rather limited integration with artificial intelligence, so it requires additional solutions to implement advanced threat detection technology, such as Azure Machine Learning, which actually supports machine learning. Instead, this tool allows you to use cloud services for greater analytics and monitoring capabilities. For example, companies in the Ukrainian market that work with large amounts of data often use Microsoft products, such as Microsoft Azure and Power BI, to ensure security and analyze data in real time.

Oracle Audit Vault is distinguished by its advanced functionality, including integration with Oracle Cloud solutions, which provides high scalability and reliability. A significant advantage is the ability to integrate with artificial intelligence solutions that use machine learning to analyze events and detect threats. Oracle Machine Learning offers a variety of machine learning algorithms that can be used to analyze data in the field of database security. For example, a clustering algorithm is used to group user actions, where each cluster represents a specific type of behavior. A sudden change in user activity from their usual cluster can be an indicator of a potential threat. Another example is the use of an isolated forest model to automatically detect anomalous transactions, which may indicate unauthorized access attempts or fraud.

IBM Guardium is one of the leading database security solutions thanks to its powerful integration capabilities with artificial intelligence and cloud platforms. Its high status is confirmed by numerous cybersecurity honors and awards, such as recognition in the Gartner Magic Quadrant report as a leader in the Data Security category. Guardium supports real-time analytics and uses machine learning to improve the accuracy of threat detection. For example, the solution can integrate with IBM Watson to analyze large amounts of data and detect anomalies, which increases the efficiency of threat detection and response.

Splunk specializes in processing large volumes of structured and unstructured data in real time. Its power allows you to manage data from a variety of sources, such as event logs, network traffic, database transactions, and even data from the Internet of Things. It is capable of processing data at scales ranging from a few gigabytes to terabytes per day, making it particularly useful for large organizations and enterprises with extensive infrastructure. Splunk Cloud provides the ability to deploy and manage infrastructure in the cloud, allowing businesses to focus on data analytics rather than hardware management. It also integrates with popular cloud platforms such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform, enabling global analytics.

Imperva SecureSphere provides powerful protection and monitoring of SQL injection and network traffic monitoring to detect suspicious activity with its advanced features. SecureSphere protects web applications such as cross-site XSS and web form attacks and provides advanced auditing and reporting capabilities, including security event logging and compliance. Threat analysis in SecureSphere is supported by machine learning. The solution uses behavioral modelling to create user and system profiles, which allows it to detect anomalies that may indicate potential threats. This allows for a proactive response to possible incidents and ensures a high level of security.

Another important application is classification data context via ML and AI. Integrating artificial intelligence (AI) and machine learning (ML) into database audit and monitoring tools enhances the ability to detect and respond to security incidents. By comparing classified data with audit logs, AI-driven tools can identify anomalies and potential security breaches more effectively. For instance, if a user typically accesses public data but suddenly attempts to access highly-confidential data, this behavior can be flagged as suspicious.

The use of AI and ML in data classification and audit processes provides several advantages: ***Enhanced Threat Detection***: AI algorithms can analyze vast amounts of data in real-time, identifying patterns and anomalies that may indicate security incidents.

Proactive Security Measures: Machine learning models can predict potential threats based on historical data, allowing organizations to implement preventive measures.

Scalability: Cloud-based AI solutions can scale to handle large volumes of data, ensuring comprehensive monitoring across extensive infrastructures.

Compliance: Implementing a robust data classification and audit framework can help organizations meet regulatory requirements and pass audits such as ISO27001 or SOC2 Type 2. These standards require stringent data protection measures, and AI-driven tools can provide the necessary oversight and reporting capabilities.

The use of artificial intelligence and machine learning significantly expands the capabilities of modern tools. They allow not only to detect known threats but also to adapt to new challenges by analyzing user and system behavior in real time. Integration with cloud technologies ensures scalability and reliability, which is critical in today's dynamic cyber threat environment. That is why the right choice and implementation of these tools ensures not only effective monitoring, but also a proactive approach to database security, which is the basis for a reliable data infrastructure in any organization. The issue of responding to leaks and ensuring data confidentiality is a logical extension of the study, as even the best monitoring solutions must be complemented by effective incident response measures. It is worth considering how measures are implemented in practice and what tools are most effective in ensuring privacy and preventing data leaks.

4. Response to data breaches and data privacy

Ensuring confidentiality and prompt response to data breaches are key aspects of modern database monitoring systems. A comparative analysis of the tools used for monitoring is worthwhile, with a particular focus on their ability to protect data from unauthorized access and respond effectively to security incidents. Table 3 below illustrates how different tools deal with

these challenges, providing an opportunity to assess their effectiveness in different scenarios.

To summarize our research, it is worth noting that all the database monitoring tools under consideration demonstrate a high level of confidentiality and efficiency in data protection. They are powerful solutions that provide reliable protection of information in various environments, be it on-premises or cloud infrastructures. Despite the fact that some of them have suffered data breaches, the companies that developed them have taken timely and effective measures to resolve problems and improve their systems. They are constantly improving, using advanced technologies such as machine learning and encryption to increase security and adapt to new threats. This makes them indispensable tools in ensuring data protection and privacy in today's environment.

5. Summary

To provide a detailed analysis and comparison of modern tools discussed in this article, despite their individual characteristics, have demonstrated high functionality and efficiency in ensuring data security. An analysis of their capabilities has shown that all these tools have a high level of confidentiality and are able to adapt to modern threats through the use of cloud solutions and artificial intelligence and machine learning technologies. The use of both reactive and proactive monitoring approaches allows the tools to effectively detect and respond to threats. They provide timely information protection through innovative methods of detecting anomalies in real time. The use of machine learning combined with flexible encryption methods helps to increase the level of data protection and minimize the risk of leaks. While some tools have experienced data breaches, which has been a challenge for the companies developing them, the corresponding improvements in technology and security policies have demonstrated their ability to effectively address the issues and improve. Testing of a prototype monitoring system for a specific DBMS was demonstrated, which showed the reliability and effectiveness of the tools under consideration in the context of modern security requirements. This research article is a valuable source for information security professionals, providing a comprehensive analysis of modern tools and techniques for monitoring and verifying database security.

The results obtained can be used by specialists to make an informed choice of optimal solutions, in accordance with specific conditions and needs. In addition, the formulated recommendations for improving monitoring systems can be applied in practice to significantly increase the level of database protection, which is extremely important for ensuring the confidentiality and integrity of information in the modern digital environment. Thus, a comprehensive analysis of the functionality and adaptation to new conditions allowed us to formulate recommendations for improving database monitoring systems. And the use of the latest technologies and flexibility in responding to cyber threats are key aspects that allow to increase the level of information protection and ensure its safety in the dynamic conditions of the modern digital world.

Table 3. Comparison of monitoring tools in the field of data protection

Tool	Data storage	Known leak	Leakage response	Level of confidentiality
SQL Server	In a database, files, on disk, or in cloud storage. The storage configuration is defined by the administrator. The method of protection is the use of data encryption during disk recording. That is, if physical access to the storage is obtained, the data will remain encrypted and unreadable without the appropriate encryption keys.	No large-scale leaks have been recorded.	The system automatically notifies administrators and generates backups for disaster recovery.	The right level of privacy that allows you to configure access control policies, encryption and authentication [25].
Oracle Audit Vault	Large volumes on local servers and in the cloud thanks to integration with Oracle Cloud. Local – on protected Oracle servers that support high fault tolerance and availability. In the cloud – on special secure storages, where they are distributed to ensure scalability and quick access.	No large-scale leaks have been recorded.	Built-in security mechanisms are used – automatic detection of anomalies using multi-factor authorization and secure data transmission channels.	A high level of encryption using the AES-256 algorithm, where access is strictly controlled based on roles and policies, which allows protection even in the event of unauthorized access to the infrastructure.
IBM Guardium	In local environments – stored on secure servers or virtual machines using RAID technologies using SSL/TLS protocols and on cloud platforms – automatically encrypted before saving.	No large-scale leaks have been recorded.	If a threat is detected, the system automatically generates a notification and can take actions such as blocking access, restricting user rights or starting additional checks.	High level by using AES-256. Access is granted only to authorized users, and is controlled through policies – who can view, modify or delete data.
Splunk	Processes data in local environments – on server clusters that can be distributed to ensure high availability and resistance to failures, as well as in cloud platforms – AWS, Azure, or Google Cloud, where data can be automatically stored in protected AWS S3 object storage.	In 2020, part of the source code of their software was placed on a third-party server due to the compromise of the credentials of one of the employees.	An internal investigation was conducted, which led to improved access policies, added MFA for all employees, and improved internal procedures. security new rules for the protection of confidential information have been developed, access control to critical systems and data has been strengthened.	A sufficient level, the AES-256 encryption algorithm is implemented, and there is the possibility of setting roles and privileges for users and groups.
Imperva SecureSphere	Local – on servers or appliances that are integrated with the company's existing IT infrastructure. In the cloud – in AWS, Microsoft Azure or Google Cloud, where data is automatically encrypted before being transferred to storage	No large-scale leaks have been recorded	Implements proactivity to protect and respond to threats. Uses attack signatures to detect and block suspicious activity, continuous monitoring of events with the ability to automatically respond	High level thanks to integration with cloud platforms and the use of machine learning

References

[1] Cinar O. et al.: Database Security in Private Database Clouds. International Conference on Information Science and Security (ICISS), Pattaya, Thailand, 2016, 1–5 [http://doi.org/10.1109/ICISSEC.2016.7885847].

[2] Deineka O. et al.: Designing Data Classification and Secure Store Policy According to SOC 2 Type II. CEUR Workshop Proceedings, 2024, 3654, 398–409 [https://ceur-ws.org/Vol-3654/short7.pdf].

[3] Devara S. R., Azad C.: Improved Database Security Using Cryptography with Genetic Operators. SN Computer Science 4(5), 2023, 570 [http://doi.org/10.1007/s42979-023-01990-z].

[4] Dou K. et al.: Research on Mainstream Data Base Security Analysis Technology of Big Data Platform. IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C). Hainan, China, 2021, 994–998 [http://doi.org/10.1109/QRS-C55045.2021.00150].

[5] Dreis Yu. et al.: Model to Formation Data Base of Internal Parameters for Assessing the Status of the State Secret Protection. Cybersecurity Providing in Information and Telecommunication Systems 3654, 2024, 277–289 [https://ceur-ws.org/Vol-3654/paper23.pdf].

[6] Falchenko S. et al.: Method of Fuzzy Classification of Information with Limited Access. IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020). Kyiv, Ukraine, 2020, 255–259 [http://doi.org/10.1109/ATIT50783.2020.9349358].

[7] Flores D. A. et al.: Implementing Chain of Custody Requirements in Database Audit Records for Forensic Purposes. IEEE Trustcom/BigDataSE/ICESS, 2017, 675–682 [http://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.299].

[8] Hong S. et al.: Data Auditing for Intelligent Network Security Monitoring. IEEE Communications Magazine 61(3), 2023, 74–79 [http://doi.org/10.1109/MCOM.003.2200046].

[9] Huang Q. et al.: A Logging Scheme for Database Audit. Second International Workshop on Computer Science and Engineering. Qingdao, China, 2009, 390–393 [http://doi.org/10.1109/WCSE.2009.837].
[10] Huijie W.: A Security Framework for Database Auditing System. 10th International Symposium on Computational Intelligence and Design. Hangzhou, China, 2017, 350–353 [http://doi.org/10.1109/ISCID.2017.64].
[11] Ivanichenko Y. et al.: Restricted Information Identification Model. Cybersecurity Providing in Information and Telecommunication Systems 3288, 2022, 89–95 [https://ceur-ws.org/Vol-3288/short5.pdf].
[12] Kehe Wu et al.: The Design and Implementation of Database Audit System Framework. IEEE 5th International Conference on Software Engineering and Service Science, 2014 [http://doi.org/10.1109/ICSESS.2014.6933628].
[13] Korchenko O. et al.: Tuple Model for Forming a Database of Primary Parameters for Assessing the State Secret Protection Status. Ukrainian Scientific Journal Infjrmation Security 28(1), 2022, 35–42 [http://doi.org/10.18372/2225-5036.28.16911].
[14] Lakhdhar Y. et al.: Active, Reactive and Proactive Visibility-Based Cyber Defense for Defending Against Attacks on Critical Systems. International Wireless Communications and Mobile Computing (IWCMC). Limassol, Cyprus, 2020, 439–444 [http://doi.org/10.1109/IWCMC48107.2020.9148400].
[15] Liegang Han et al.: HDTSM: Hybrid Dynamic Token-based Security Mechanism for Database Protection in E-Government Service Systems. International Conference on Artificial Intelligence and Automation Control (AIAC), 2023, 94–98 [http://doi.org/10.1109/AIAC61660.2023.00029].
[16] Martseniuk Y. et al.: Automated Conformity Verification Concept for Cloud Security. CEUR Workshop Proceedings 3654, 2024, 25–37 [https://ceur-ws.org/Vol-3654/paper3.pdf].
[17] Martseniuk Y. et al.: Shadow IT risk analysis in public cloud infrastructure. Cyber Security and Data Protection 2024, 22–31 [https://ceur-ws.org/Vol-3800/paper3.pdf].
[18] Martseniuk Y. et al.: Universal Centralized Secret Data Management for Automated Public Cloud Provisioning. Cybersecurity Providing in Information and Telecommunication Systems 2, 2024, 72–81 [https://ceur-ws.org/Vol-3826/paper7.pdf].
[19] Motwani R. et al.: Auditing SQL Queries. IEEE 24th International Conference on Data Engineering. Cancun, Mexico, 2008, 287–296 [http://doi.org/10.1109/ICDE.2008.4497437].
[20] Mousa A. et al.: Database Security Threats and Challenges. 8th International Symposium on Digital Forensics and Security (ISDFS). Beirut, Lebanon, 2020, 1–5 [http://doi.org/10.1109/ISDFS49300.2020.9116436].
[21] Ozkan-Okay M. et al.: A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. IEEE Access 12, 2024, 12229–12256 [http://doi.org/10.1109/ACCESS.2024.3355547].
[22] Paradisi M.: Proactive and Predictive Risk Management in Aviation Safety: A Corporate Strategic Approach. IEEE International Workshop on Technologies for Defense and Security (TechDefense). 2023, 34–39 [http://doi.org/10.1109/TechDefense59795.2023.10380870].
[23] Semančik L.: Recording of Data Monitoring Access to Databases Using Triggers. Communication and Information Technologies (KIT). Vysoke Tatry, Slovakia, 2019, 1–5 [http://doi.org/10.23919/KIT.2019.8883478].
[24] Seok-Woo Lee et al.: Database Security System Based on User Identification. Journal of Digital Contents Society 25(4), 2024, 1079–1085 [http://doi.org/10.9728/dcs.2024.25.4.1079].
[25] Shevchenko S. et al.: Protection of Information in Telecommunication Medical Systems Based on a Risk-Oriented Approach, Cybersecurity Providing in Information and Telecommunication Systems 3421, 2023, 158–167 [https://ceur-ws.org/Vol-3421/paper16.pdf].
[26] Shevchuk D. et al.: Designing Secured Services for Authentication, Authorization and Accounting of Users (short paper). CPITS II, 2023, 217–225 [https://ceur-ws.org/Vol-3550/short4.pdf].
[27] Skladannyi P. et al.: Model to Formation Data Base of Secondary Parameters for Assessing Status of the State Secret Protection. Conference Cyber Security and Data Protection, Lviv, Ukraine, 3800, 2024, 1–11 [https://ceur-ws.org/Vol-3800/paper1.pdf].
[28] Wang Y. et al.: The Overview of Database Security Threats' Solutions: Traditional and Machine Learning. Journal of Information Security 12, 2021, 34–55 [http://doi.org/10.4236/jis.2021.121002].
[29] Yongzheng Wu et al.: A User-Level Framework for Auditing and Monitoring. 21st Annual Computer Security Applications Conference (ACSAC'05). Tucson, USA, 2005, 101–105 [http://doi.org/10.1109/CSAC.2005.8].
[30] GDE DSM Installation Guide v3.0.0.2. [https://www.ibm.com/support/pages/system/files/inline-files/$FILE/GDE_DSM_Install_Guide_v3.0.0.2_v1_0.pdf].
[31] IBM Security Guardium Data Protection – Incident management. [https://icore.kz/upravlenie-inczidentami/ibm-security-guardium-data-protection].
[32] Integrity Oracle Security Blog – What is Oracle Audit Vault. [https://www.integrigy.com/oracle-security-blog/what-oracle-audit-vault].
[33] Microsoft Learn – SQL Server Audit (Database Engine). [https://learn.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-database-engine?view=sql-server-ver16].
[34] Oracle Documentation Audit Vault and Database Firewall. [https://docs.oracle.com/en/database/oracle/audit-vault-database-firewall/20/sigli/index.html#GUID-E11B3C13-8BD4-449F-8E9E-27B9898D778D].
[35] SecureSphere Management Solutions. [https://www.imperva.com/resources/datasheets/DS_SecureSphere_Management_Solutions.pdf].
[36] Splunk – The Essential Guide to Data. [https://www.splunk.com/en_us/pdfs/ebooks/the-essential-guide-to-data.pdf].
[37] What Is Splunk & What Does It Do? A Splunk Intro. [https://www.splunk.com/en_us/blog/learn/what-splunk-does.html].

Kateryna Mykhailyshyn
e-mail: kateryna.mykhailyshyn.kb.2022@lpnu.ua

Student at the Department of Information Protection, Lviv Polytechnic National University, Lviv, Ukraine.
Research interests: cybersecurity, cloud technology, ethical hacking, security isolation, DevSecOps, SDLC, AI security, risk management.

https://orcid.org/0009-0009-4835-6958

Ph.D. Oleh Harasymchuk
e-mail: oleh.i.harasymchuk@lpnu.ua

Ph.D., associate professor at the Department of Information Protection, Lviv Polytechnic National University, Lviv, Ukraine.
Cybersecurity, pseudo-random number generators, large language models, security standards, information protection systems, authentication and authorized access systems, database and knowledge systems.

https://orcid.org/0000-0002-8742-8872

M.Sc. Oleh Deineka
e-mail: deinekaoleg.86@gmail.com

Postgraduate of Cyber Security Department of Information Protection, Lviv Polytechnic National University, Lviv, Ukraine.
Research interests: big data, data governance, artificial intelligence, AI agents, large language models, security standards, cybersecurity.

https://orcid.org/0009-0005-9156-3339

Ph.D. Yurii Dreis
e-mail: y.dreis@mu.edu.ua

Ph.D., associate professor at the Department of Analytics System and Information Technology, Mariupol State University, Kyiv, Ukraine.
Research interests: information security, protection information with limited accesses, consequence assessment, risk analysis.

https://orcid.org/0000-0003-2699-1597

Prof. Volodymyr Shulha
e-mail: info@duikt.edu.ua

Doctor of historical sciences, senior researcher, Rector of the State University of Information and Communication Technologies, State University of Information and Communication Technologies, Kyiv, Ukraine.
Research interests: information security auditing, information and personal data protection, cybersecurity.

https://orcid.org/0000-0003-4356-7288

Ph.D. Yuriy Pepa
e-mail: yurka14@ukr.net

Ph.D., professor of the Department of Technical Systems of Cybersecurity, State University of Information and Communication Technologies, Kyiv, Ukraine.
Research interests: cybersecurity, telecommunication systems, intelligent robotic systems, decision-making systems, radio electronic devices, antenna technology.

https://orcid.org/0000-0003-2073-1364