Software integration of vulnerability databases into an isms to support risk-oriented decision-making*

Nataliya Maslova[1,2†], Valentyna Yashchuk[1,†], Olena Liubymenko[2,3*,†] and Andriy Ivanusa[1,†]

[1] Lviv State University of Life Safety, 35, Kleparivska St., Lviv, 79007, Ukraine
[2] Donetsk National Technical University, 76, Sambirska, St., Drohobych, Lviv region, 82100, Ukraine
[3] Lutsk National Technical University, 75, Lvivska street, Lutsk, Volyn region, 43018, Ukraine

Abstract

The paper addresses the problem of developing a Decision Support System (DSS) for vulnerability management based on the integration and analytical processing of data from heterogeneous cyber threat intelligence sources. A software-oriented approach is proposed that implements a vulnerability data processing pipeline, including data collection from open databases (CVE, NVD, KEV, EPSS), normalization, contextual enrichment, and subsequent analytical processing. A risk-oriented assessment model is developed, integrating indicators of technical severity, exploitability likelihood, presence of active exploitation, and asset criticality into a unified risk score. The proposed model enables context-aware differentiation of vulnerabilities and can serve as the analytical core of a DSS. The system architecture follows a modular data processing approach and supports integration with operational platforms (SIEM, SOAR, ITSM), allowing vulnerability data to be transformed into structured analytical indicators for decision-making. The results of the experimental study confirm the effectiveness of the proposed approach in terms of accurate risk differentiation and demonstrate its potential for automating data processing, including a reduction in vulnerability processing time of approximately 79%. The proposed approach can be applied to the development of intelligent DSS for data analysis and risk management in information systems.

Keywords

decision support system, data processing, vulnerability data integration, risk modeling, CVSS, EPSS, KEV, data pipeline, software architecture, cybersecurity analytics.

1. Introduction

Information technologies form the foundation of modern governmental, industrial, and socio-economic systems. The proliferation of complex digital infrastructures, including cloud services, containerized environments, and industrial control systems, leads to an expansion of the potential attack surface of information systems. Under such conditions, vulnerability management becomes a key factor in ensuring organizational cybersecurity.

Information Security Management Systems (ISMS) provide the organizational framework for managing cybersecurity risks and implementing protection measures for information assets. International standards ISO/IEC 27001 and ISO/IEC 27005 define the requirements for establishing and operating ISMS, as well as methodological approaches to information security risk assessment and treatment [1,2]. At the same time, effective vulnerability management requires the use of structured sources of information on software and system vulnerabilities.

Despite the availability of numerous vulnerability data sources, organizations often face challenges in integrating this data into information security management processes. Vulnerability

* CMIS -2026: Ninth International Workshop on Computer Modeling and Intelligent Systems, May 5, 2026, Zaporizhzhia, Ukraine
* Corresponding author.
† These authors contributed equally.
masgpp2@gmail.com (N. Maslova); v.yaschuk@ldubgd.edu.ua (V. Yashchuk); olena.liubymenko@donntu.edu.ua (O. Liubymenko); ivaaanusa@gmail.com (A. Ivanusa);
0000-0002-9078-0973 (N. Maslova); 0000-0003-2651-4918 (V. Yashchuk); 0000-0002-5935-6891 (O. Liubymenko); 0000-0001-9141-8039 (A. Ivanusa)

data originates from multiple sources, is represented in heterogeneous formats, and requires normalization, correlation with asset information, and further analytical processing. Study [3] emphasizes that integrating vulnerability databases into the ISMS environment is a critical factor in enhancing the cyber resilience of critical information systems.

In this context, there is a need to apply software technologies that enable automated collection, processing, and integration of vulnerability information into ISMS. Such approaches allow transforming raw vulnerability data into analytical information required for cybersecurity decision-making.

The aim of this study is to develop a software-oriented approach to integrating vulnerability databases into ISMS to support decision-making based on risk-oriented vulnerability assessment.

The study is aimed at achieving the following scientific and practical objectives:

- to develop a risk-oriented model for vulnerability prioritization that integrates CVSS, EPSS, KEV, and asset criticality;
- to formalize a DSS software architecture for processing and integrating vulnerability data;
- to experimentally demonstrate the ability of the model to provide context-aware risk differentiation.

The scientific novelty lies in the development of a risk-oriented approach to decision support in vulnerability management, integrating CVSS, EPSS, KEV, and asset criticality into a unified model and implemented within a software architecture integrated with SIEM, SOAR, and ITSM platforms. This approach enables the transformation of vulnerability data into context-aware risk indicators and bridges the gap between data accumulation and its practical use within ISMS.

2. Related Work and Problem Statement

Modern approaches to cybersecurity management emphasize the importance of systematic vulnerability management within Information Security Management Systems (ISMS). In addition to the ISMS requirements defined by ISO/IEC 27001 and ISO/IEC 27005, the ISO/IEC 27002 standard provides recommendations for implementing technical and organizational security controls, including those related to vulnerability management, incident response, and security monitoring [4]. Practical aspects of incident handling and cyber threat response are also addressed in NIST guidelines (SP 800-61, SP 800-137) [5,6]. In parallel, contemporary approaches to quantitative risk assessment, such as the FAIR (Factor Analysis of Information Risk) model, consider both the likelihood of threat realization and its impact on assets [7].

An important component of vulnerability management processes is the use of structured sources of vulnerability information. Global repositories such as CVE and NVD provide standardized descriptions of known software vulnerabilities and associated threats [8,9]. Additionally, the Known Exploited Vulnerabilities (KEV) catalog, maintained by CISA, contains a list of vulnerabilities actively exploited in real-world attacks, enabling more effective prioritization of remediation efforts [10].

Vulnerability severity is traditionally assessed using the Common Vulnerability Scoring System (CVSS), which provides standardized metrics for evaluating impact and exploitability [11]. Studies [12,13] highlight limitations of CVSS, noting that CVSS scores do not always reflect the real likelihood of exploitation, and reliance solely on base scores may lead to prioritization errors. To address this issue, the Exploit Prediction Scoring System (EPSS) was introduced, estimating exploitation likelihood based on statistical models and empirical attack data [14]. Research [13,15] demonstrates that combining CVSS metrics with EPSS significantly improves vulnerability prioritization in cybersecurity management.

Recent studies propose various approaches to vulnerability ranking and cyber risk assessment. Work [16] presents a systematic review of vulnerability prioritization methods and identifies key challenges related to integrating heterogeneous data sources and risk metrics. Study [17] demonstrates the potential of machine learning techniques to enhance CVSS-based prioritization

models. Meanwhile, [18] proposes an integrated vulnerability management model that combines vulnerability data with risk management and decision-making processes.

Another important research direction is the integration of vulnerability information with monitoring and incident response platforms. Modern cybersecurity infrastructures employ Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) systems to automate threat detection and response processes [19–22]. Study [23] shows that integrating these systems improves incident response efficiency and overall cybersecurity management.

Recent research also highlights the growing role of risk-oriented cybersecurity management models. Dynamic cyber risk management models enable continuous assessment of threats and vulnerabilities in complex digital environments [24]. Predictive models of vulnerability exploitation and analytical approaches to cyber risk assessment significantly enhance decision support capabilities in cybersecurity [25]. Statistical methods for cyber risk evaluation are also proposed to improve vulnerability prioritization based on quantitative risk indicators [26].

Previous studies by the authors have addressed certain aspects of integrating vulnerability information into ISMS environments. In [27], a conceptual model for integrating vulnerability databases into ISMS was proposed to enhance the cyber resilience of critical information systems. Study [28] examines mechanisms for incident response and coordination of cybersecurity centers. Work [29] proposes a multi-agent approach to web application firewall (WAF) security testing implemented using the JADE platform, demonstrating the potential of software technologies and intelligent systems for automating vulnerability detection and cyber threat analysis.

Despite significant progress in vulnerability management approaches, several limitations remain. Traditional methods based on CVSS provide a standardized assessment of technical severity but do not adequately reflect the real-world likelihood of exploitation or the operational context of information systems [11–13]. Extensions such as EPSS improve estimation of exploitation probability; however, they are often applied in isolation and do not account for asset criticality or evidence of active exploitation [13–15]. In addition, many existing approaches rely on fragmented data sources and lack integrated software architectures capable of automating data processing and supporting decision-making [16–18]. As a result, there is a gap between the availability of vulnerability data and its effective use in cybersecurity management processes. These limitations justify the need for integrated, risk-oriented approaches that combine multiple data sources within a unified analytical framework.

3. Software Architecture for Vulnerability Database Integration

Effective vulnerability management requires the integration of information from various cyber threat intelligence sources and its subsequent processing within Information Security Management Systems (ISMS). In modern conditions, the volume of vulnerability-related information is continuously increasing, which complicates its analysis and prioritization without the use of specialized software tools. Therefore, an important task is the development of a software architecture that enables automated collection, normalization, and analysis of vulnerability data to support cybersecurity decision-making.

The proposed architecture for integrating vulnerability databases is based on the use of open vulnerability information sources, data processing mechanisms, and security monitoring platforms. The primary objective of this architecture is to transform fragmented vulnerability data into structured analytical information that can be utilized within ISMS.

The main sources of vulnerability information include global vulnerability databases and systems for assessing their severity. The most widely used sources are:

- CVE (Common Vulnerabilities and Exposures) – a standardized list of known software vulnerabilities [8];
- NVD (National Vulnerability Database) – a database containing technical characteristics of vulnerabilities, CVSS metrics, and additional security attributes [9];

- KEV (Known Exploited Vulnerabilities) – a catalog of vulnerabilities actively exploited in real-world cyberattacks [10];
- CVSS (Common Vulnerability Scoring System) – a system for assessing vulnerability severity [11];
- EPSS (Exploit Prediction Scoring System) – a model for predicting the likelihood of vulnerability exploitation [14].

Studies show that combining CVSS and EPSS metrics improves the effectiveness of vulnerability prioritization and cyber risk management [13,15].

As shown in Table 1, different vulnerability data sources perform distinct functions within cybersecurity management processes.

Table 1
Vulnerability intelligence sources used in the proposed architecture

Source	Data type	Purpose
CVE	vulnerability identifiers	standardization of vulnerability descriptions
NVD	technical attributes	detailed vulnerability analysis
KEV	exploited vulnerabilities	prioritization of mitigation actions
CVSS	severity metrics	vulnerability impact assessment
EPSS	exploitation probability	prediction of attack likelihood

As shown in Table 1, different vulnerability information sources provide complementary data for vulnerability analysis and risk assessment. CVE and NVD offer baseline descriptions of vulnerabilities, while CVSS and EPSS metrics enable quantitative evaluation of vulnerability severity and exploitation likelihood.

The architecture for integrating vulnerability databases consists of several functional components that support data processing at different stages. The main architectural modules include (Fig. 1):

- Data Ingestion Layer – a module for collecting data from multiple sources (CVE, NVD, KEV, vendor advisories);
- Normalization Layer – a module for data normalization and standardization;
- Context Enrichment Layer – mapping vulnerabilities to organizational assets;
- Risk Scoring Module – calculating risk levels based on CVSS, EPSS, and asset criticality;
- Decision Support Layer – generating recommendations for vulnerability remediation prioritization;
- Security Integration Layer – integration with SIEM, SOAR, and ITSM systems.

As shown in Fig. 1, vulnerability information passes several processing stages before being used for decision support. First, vulnerability data is collected from external databases and normalized into a unified format. Then, the normalized data is enriched with contextual information about organizational assets, enabling more accurate risk assessment. The resulting risk indicators are used to support cybersecurity decision-making processes.

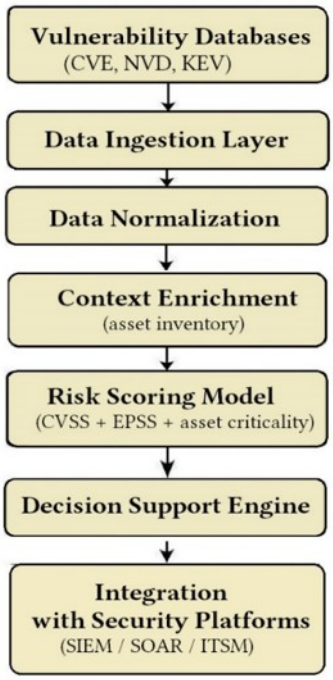

Figure 1: Architecture of Vulnerability Database Integration into ISMS.

One of the key functions of the architecture is vulnerability risk assessment. For this purpose, the following ranking model is proposed:

$$Risk=(CVSS/10) \times EPSS \times Asset\_Criticality \times KEV\_factor, \quad (1)$$

where

- CVSS / 10 is the normalized technical severity (0–1);
- EPSS is the probability of exploitation (0–1);
- Asset_Criticality is a weighting factor reflecting the importance of the information asset;
- KEV_factor indicates active exploitation, with a value of 1.2 if the vulnerability is present in KEV and 1.0 otherwise.

Normalization prevents dominance of a single parameter and ensures proper interpretation of the integrated risk score.

The coefficient values in the proposed risk model are selected to ensure a balanced influence of technical and contextual factors. The Asset_Criticality coefficient is defined within the range [0.5; 2], allowing differences in asset importance to be considered without excessive dominance in the overall risk score. This approach aligns with the principles of risk-based management defined in ISO/IEC 27005, which emphasizes the importance of asset value in risk assessment [2].

The KEV_factor is set to 1.2 when a vulnerability is listed in the Known Exploited Vulnerabilities catalog and 1.0 otherwise. This value is chosen as a moderate amplification factor that reflects confirmed exploitation in real-world attacks without dominating the model. This is consistent with modern quantitative risk assessment approaches, including FAIR, where both the likelihood of threat realization and its impact on assets are considered [7].

The selection of coefficients is also supported by sensitivity analysis results, which indicate the absence of dominance of individual parameters in the model.

Thus, the proposed architecture implements a Decision Support System (DSS) layer that transforms vulnerability data into actionable cybersecurity decisions. Similar risk-oriented approaches are widely used in modern cybersecurity management systems and contribute to improved vulnerability management [24,26].

The proposed model is heuristic and designed for practical integration rather than formal optimization. The practical implementation of the proposed architecture relies on several software components capable of supporting data collection, processing, enrichment, and integration with cybersecurity platforms. The main technological modules and their implementation technologies are presented in Table 2. As shown in Table 2, the proposed architecture combines mechanisms for vulnerability data collection with data normalization, contextual enrichment, and automated response components. Monitoring technologies such as Prometheus and Grafana enable continuous tracking of vulnerability management metrics and system performance.

Table 2
Software technologies used in the proposed architecture

Category	Technologies	Appointment
Data ingestion	REST APIs, JSON feeds, ETL pipelines	retrieval of CVE/NVD data
Data processing	Python, Spark, Elasticsearch	normalization and analysis
Security analytics	SIEM (Splunk, QRadar)	event correlation
Automation	SOAR (Cortex XSOAR, Shuffle)	automated playbooks
Risk analytics	ML-model, scoring engines	decision support
Visualization	Kibana, Grafana, Power BI	management dashboards

Unlike the approaches discussed above, the proposed architecture utilizes these sources as components of a unified data processing pipeline that ensures automated collection, normalization, and integration of vulnerability information.

One of the key technological components is the use of application programming interfaces (APIs) provided by vulnerability intelligence platforms. Public APIs of CVE and NVD databases enable automated retrieval of vulnerability records, including technical descriptions, CVSS metrics, information on affected software configurations, and references to mitigation recommendations [8,9]. Similarly, the Known Exploited Vulnerabilities (KEV) catalog maintained by CISA provides machine-readable data feeds that can be regularly synchronized with local cybersecurity monitoring systems [10].

Thus, the proposed approach integrates these sources into a single data processing workflow.

An important element of the integration architecture is the use of data collection and processing pipelines. Such pipelines are typically implemented using extract–transform–load (ETL) mechanisms, allowing data to be collected from multiple sources, transformed into unified formats, and stored in centralized repositories. In modern cybersecurity platforms, technologies such as Python-based data processing, RESTful APIs, messaging systems, and document-oriented databases are widely used to ensure scalable processing of vulnerability information.

To enhance the analytical value of vulnerability data, it is further enriched with contextual information obtained from asset inventories, configuration management databases (CMDB), and software component repositories. This contextual enrichment enables mapping vulnerabilities to specific information assets within an organization's infrastructure.

Integration with operational cybersecurity platforms is another key element of the proposed architecture. Vulnerability information can be transmitted to Security Information and Event Management (SIEM) systems for event correlation and threat detection, as well as to Security Orchestration, Automation and Response (SOAR) platforms for automating incident response processes [19,23]. In addition, integration with IT Service Management (ITSM) systems enables automatic creation of remediation tasks for system administrators and cybersecurity specialists.

Recent studies also emphasize the growing role of intelligent and automated technologies in cybersecurity. In particular, multi-agent security testing systems and automated penetration testing platforms can leverage vulnerability database information for proactive security assessment and identification of new vulnerabilities [29]. These technologies complement traditional vulnerability management tools and contribute to the automation of cybersecurity processes.

Thus, the use of modern software technologies enables the development of integrated vulnerability data processing platforms that support continuous cybersecurity monitoring, automated risk assessment, and effective decision support within ISMS environments.

4. Software Implementation of the Vulnerability Processing Pipeline

The practical implementation of the proposed architecture involves the development of an automated vulnerability information processing system that ensures the collection, normalization, analytical processing, and utilization of data from various cyber threat intelligence sources. Such a system enables automation of monitoring processes for newly discovered vulnerabilities and supports risk-oriented decision-making within Information Security Management Systems.

During implementation, the software system for vulnerability data processing operates as a sequence of interconnected software components that perform different stages of data processing (Fig. 2). In a simplified form, this system can be represented as a sequential vulnerability data processing workflow, encompassing data collection, normalization, analytical processing, and integration with cybersecurity management systems.

In general, the software system for vulnerability data processing can be represented by the following scheme:

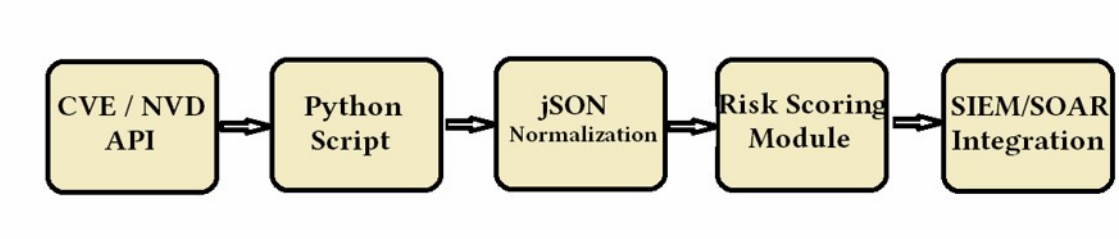

Figure 2: Example of a Vulnerability Processing Pipeline.

In this structure, individual elements perform different functional roles. In particular, data ingestion scripts (Python ingestion scripts) act as software components for collecting information from open vulnerability sources. The risk scoring module implements algorithms for vulnerability analysis and ranking. Integration with SIEM and SOAR platforms ensures the transfer of analytical results to operational cybersecurity systems for further response.

Together, these components form a unified automated vulnerability data processing system that transforms data from vulnerability databases into practically applicable analytical information for cybersecurity decision support.

Vulnerability information obtained from different sources has heterogeneous formats and varying metadata structures. Therefore, one of the key stages of the processing system is data normalization.

At this stage, the following operations are performed:

- processing and analysis of JSON vulnerability records;
- extraction of CVE identifiers and related attributes;
- matching software configurations using CPE identifiers;
- removal of duplicate vulnerability records.

After normalization, vulnerability data is enriched with contextual information obtained from organizational asset inventories and configuration management databases (CMDB). This enables mapping vulnerabilities to specific software components or information systems used within the organization.

The next stage of the processing system involves assessing the risk associated with identified vulnerabilities. For this purpose, a risk-oriented ranking model is used, combining CVSS, EPSS, vulnerability exploitation status in the KEV catalog, and asset criticality.

Based on these parameters, an integrated risk score is calculated and used to rank vulnerabilities according to their potential impact on organizational information assets. This approach enables prioritization of remediation actions and directs cybersecurity resources toward the most critical threats.

The following code fragment (Fig.3) illustrates a simplified implementation of the vulnerability risk scoring module. In this implementation, the CVSS score is normalized to the range [0;1] and combined with EPSS, asset criticality, and KEV status to compute an integrated risk score.

```
def calculate_risk(cvss, epss, asset_criticality, kev):
    return round((cvss / 10) * epss * asset_criticality * (1.2 if kev
else 1.0), 2)

if __name__ == "__main__":
    cve = input("CVE ID: ")
    risk = calculate_risk(
        float(input("CVSS (0-10): ")),
        float(input("EPSS (0-1): ")),
        float(input("Asset criticality: ")),
        input("KEV (yes/no): ").lower() == "yes"
    )
    print(f"{cve} risk: {risk}")
```

Figure 3: Example of a Vulnerability Risk Assessment Module.

The parameters used in the fragment are as follows:

- cvss — normalized technical severity of the vulnerability;
- epss — probability of exploitation;
- asset_criticality — importance of the asset;
- kev_status — indication of active exploitation.

The final stage of the automated vulnerability data processing system involves integrating the results of analytical processing with operational cybersecurity systems. The obtained results can be transmitted to the following systems:

- SIEM platforms, which correlate vulnerability information with security events and enable detection of exploitation attempts;
- SOAR platforms, which automate incident response processes and execute vulnerability remediation workflows;
- IT Service Management (ITSM) systems, which support the creation and tracking of vulnerability remediation tasks.

Integration of the vulnerability data processing system with these platforms enables automation of vulnerability management processes and information security processes as a whole (Fig.4).

Figure 4 presents a generalized architecture for integrating the vulnerability data processing system with operational cybersecurity platforms. After collecting data from CVE, NVD, KEV, and EPSS sources, the data is normalized and risk assessment is performed. The resulting outputs are passed to the decision support module, which determines vulnerability remediation priorities. Through the integration layer, the results can be transmitted to SOAR platforms for automated response or to ITSM systems for creating remediation tasks.

Branching at the integration stage is determined by decision rules defined in the DSS module, which map vulnerability priorities to corresponding event correlation processes in SIEM, response scenarios in SOAR, or remediation workflows in ITSM systems.

Playbooks, tickets, and correlation rules serve as mechanisms for automated response, task management, and event correlation in SOAR, ITSM, and SIEM platforms, respectively. The integration layer acts as an intermediate software component that ensures data exchange and transformation between the DSS module and external cybersecurity platforms. Data transfer is implemented using REST APIs and webhook mechanisms, supporting both request-driven and event-driven interactions.

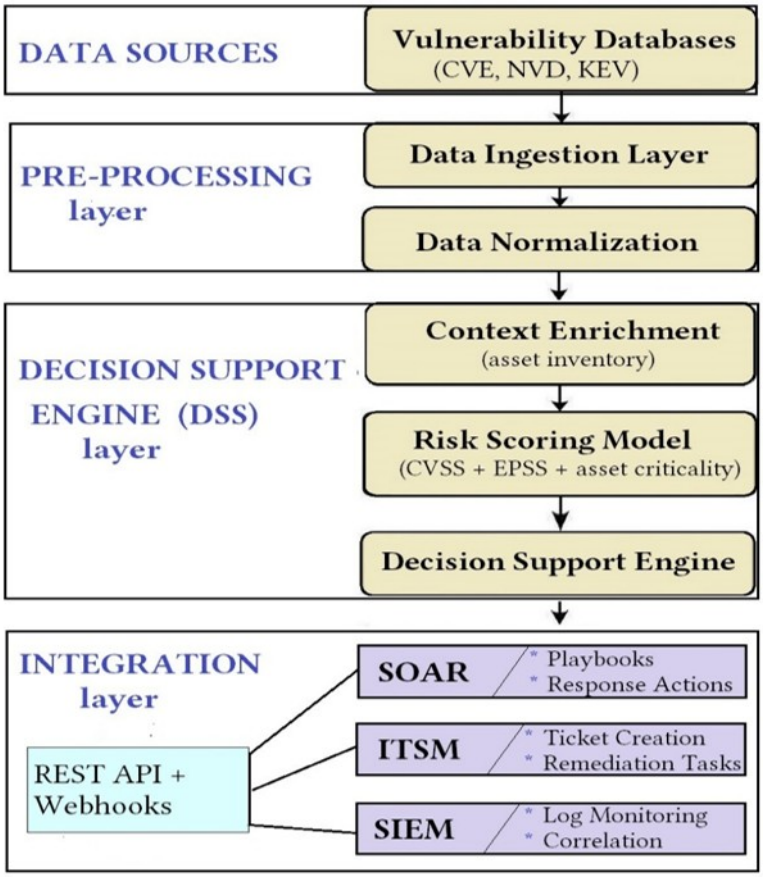

Figure 4: Architecture of integration of the automated vulnerability information processing system with IT service response and management platforms.

It should be noted that integration scripts for SIEM depend on the specific security platform, as different SIEM systems use distinct APIs, event formats, and data ingestion mechanisms.

Overall, the proposed architecture is platform-independent and enables integration with various SIEM and SOAR systems through standardized API interfaces.

Thus, the automated vulnerability data processing system transforms vulnerability database data into analytical information that can be used to support managerial decision-making in cybersecurity. It serves as a technological foundation for implementing a Decision Support System (DSS) in vulnerability management processes within ISMS.

5. Results

The experimental evaluation is based on vulnerability datasets obtained from publicly available cyber threat intelligence sources, including the Common Vulnerabilities and Exposures (CVE) list [8], the National Vulnerability Database (NVD) [9], the Known Exploited Vulnerabilities (KEV) catalog maintained by CISA [10], and Exploit Prediction Scoring System (EPSS) probability scores provided by FIRST [14].

The dataset includes vulnerability records affecting widely used software systems and platforms, such as Apache Log4j (CVE-2021-44228), Microsoft Outlook (CVE-2023-23397), MOVEit Transfer (CVE-2023-34362), Spring Framework (CVE-2022-22965), and F5 BIG-IP (CVE-2022-1388), which are commonly referenced in cybersecurity research and real-world incidents. Similar datasets based on CVE/NVD and EPSS are widely used in studies on vulnerability prioritization and cyber risk assessment [13–15].

In this study, a representative subset of vulnerabilities is used to illustrate the proposed approach. Although the dataset size is limited, it reflects typical vulnerability analysis scenarios

and allows demonstrating the key properties of the model, including context-aware risk differentiation and the effects of automation.

Each vulnerability record contains structured attributes, including CVSS severity metrics, EPSS exploitation probability, KEV exploitation status, and contextual information related to asset criticality derived from asset inventories or configuration management databases (CMDB). The use of such multi-source datasets enables comprehensive analysis of vulnerabilities by combining technical severity, exploitation likelihood, and operational context.

The results of the experimental study are aimed at evaluating two aspects of the proposed approach:

- the ability of the model to provide risk differentiation;
- the efficiency of automation in vulnerability processing.

The system automatically processes vulnerability records, performs normalization, enriches them with contextual information about organizational information assets, and computes integrated risk scores in accordance with the proposed risk-oriented vulnerability ranking model.

To evaluate the effectiveness of the proposed model, a comparison with a baseline approach based on CVSS scores is performed. Table 3 presents the prioritization results obtained using both CVSS-based ranking and the proposed risk-oriented model.

Table 3
Comparison of CVSS-based and proposed model prioritization

Vulnerability	CVSS	EPSS	KEV	Asset	CVSS Rank	Proposed Rank	Risk Level
CVE-2021-44228 (Log4Shell)	10.0	0.97	Yes	High	1	1	Critical
CVE-2023-23397 (Microsoft Outlook)	9.8	0.89	Yes	Medium	2	2	Critical
CVE-2023-34362 (MOVEit Transfer)	9.8	0.85	Yes	High	2	2	Critical
CVE-2022-30190 (Follina)	7.8	0.45	No	High	4	4	Medium
CVE-2021-34527 (PrintNightmare)	8.8	0.32	No	Medium	3	5	Medium
CVE-2020-11023 (jQuery XSS)	4.8	0.04	No	Medium	6	6	Low

The conducted sensitivity analysis shows that EPSS and asset criticality have the greatest impact on the integrated risk score, while the KEV factor acts as a corrective coefficient. This confirms the balanced nature of the proposed model.

Thus, in contrast to CVSS-oriented approaches, the proposed model reduces the risk of misprioritization and improves the validity of decision-making, confirming its suitability as the analytical core of a DSS.

The results are integrated with operational cybersecurity platforms (SIEM, SOAR, ITSM). In the experiment, data was transmitted to the Splunk SIEM platform via REST API in JSON format, enabling near real-time usage. The transmitted events included the CVE identifier, CVSS and EPSS values, KEV status, asset information, risk level, and remediation priority, enabling correlation with telemetry data and supporting automated incident response.

To evaluate the impact of automation on vulnerability management processes, a controlled illustrative experiment was conducted, comparing vulnerability processing time in manual and automated modes. The test data consisted of typical vulnerability analysis scenarios based on open sources (CVE/NVD), including data collection, analysis, risk assessment, and prioritization stages.

In the manual mode, analysis involved sequential processing by an analyst, whereas the automated mode utilized the proposed vulnerability data processing system. The experimental results are presented in Table 4.

Table 4
Comparative Analysis of Vulnerability Processing Time

Scenario	CVE ID	Manual processing (min)	Automated processing (min)
1	CVE-2021-44228	25.4	5.2
2	CVE-2022-22965	30.1	6.3
3	CVE-2023-34362	20.7	4.1
4	CVE-2023-23397	35.6	7.4
5	CVE-2022-1388	28.3	5.8
6	CVE-2021-34527	32.9	6.9

The presented values are illustrative and reflect simulated task execution conditions, allowing demonstration of the potential efficiency gains of the proposed approach. As shown in Table 4, the use of an automated approach significantly reduces vulnerability processing time compared to manual analysis. The greatest effect is achieved through automation of data collection, information normalization, and risk-oriented prioritization.

On average, the automated approach in the experiment reduced processing time from 28.83 to 5.95 minutes, corresponding to an approximately 4.85× speedup, or a 79.4% reduction in processing time. This demonstrates the potential of the proposed system to reduce the workload of cybersecurity professionals and improve the efficiency of vulnerability management processes. However, this result is illustrative and supports the implementation effectiveness rather than constituting the primary contribution of the study.

The obtained results indicate that the proposed model not only automates vulnerability data processing but also enables context-aware prioritization of remediation actions. Unlike approaches based solely on CVSS scores, the proposed system incorporates exploitation probability (EPSS), KEV status, and asset criticality, allowing for a more accurate assessment of actual risk levels.

This enables the system to function as a Decision Support System (DSS) that transforms vulnerability database data into structured analytical information suitable for cybersecurity decision-making.

An important advantage of the approach is the integration of vulnerability assessment results with operational cybersecurity platforms. The transmission of structured events to SIEM, SOAR, and ITSM systems enables direct use of analytical results in monitoring, incident response, and remediation management processes, ensuring the transition from risk assessment to actionable measures.

The controlled illustrative experiment further demonstrates that automation of data collection, normalization, and analysis processes can significantly reduce vulnerability processing time. At the same time, the main value of the proposed approach lies not only in accelerating processing but also in improving decision-making quality through multi-factor risk assessment.

6. Discussion

The proposed approach to integrating vulnerability databases into Information Security Management Systems demonstrates the potential of software technologies to improve the validity of cyber risk management processes. The developed automated vulnerability data processing system ensures integration of data from multiple sources, their normalization, analytical processing, and transmission of results to operational cybersecurity platforms.

One of the key advantages of the proposed approach is the use of a risk-oriented prioritization model that combines multiple vulnerability characteristics. Unlike traditional approaches based

solely on CVSS scores, the proposed model also considers exploitation probability (EPSS), the presence of vulnerabilities in the KEV catalog, and asset criticality. This enables more accurate prioritization of remediation actions and reduces the likelihood of underestimating the most critical weaknesses in information systems.

An important feature of the proposed architecture is its modularity and platform independence. The integration layer ensures interaction with various monitoring and incident response platforms, including SIEM, SOAR, and IT Service Management systems. Due to the use of API-oriented integration mechanisms, the system can adapt to different cybersecurity environments without significant changes to the core architecture.

The obtained results confirm that the proposed system performs the functions of a Decision Support System (DSS), as it transforms heterogeneous vulnerability data into structured analytical indicators suitable for managerial decision-making.

The results presented in Section 4 indicate that automation of vulnerability data processing reduces the time required for analysis and prioritization. In particular, the controlled illustrative experiment demonstrated a potential reduction in processing time by a factor of 4.85.

At the same time, the proposed approach has certain limitations. The system's effectiveness largely depends on the completeness and timeliness of data obtained from external vulnerability sources. In addition, the accuracy of risk assessment may vary depending on the quality of information about organizational assets and the correctness of their classification by criticality level. Another limitation is that the reported time evaluation is based on a controlled illustrative experiment rather than a full-scale real-world deployment.

A promising direction for future research is the extension of the system's analytical capabilities through the use of machine learning methods for predicting vulnerability exploitation and adaptive cyber risk prioritization. Another important direction is the integration of the system with cyber resilience management platforms and strategic cybersecurity management frameworks.

Conclusions

The paper addresses the problem of effective use of vulnerability database information in organizational information security management processes. The growing number of known vulnerabilities and the speed of their exploitation in real-world cyberattacks necessitate the automation of analysis, prioritization, and integration processes within cybersecurity management systems.

The study proposes an approach to integrating vulnerability databases into Information Security Management Systems based on a software system for automated vulnerability data processing. A system architecture has been developed that ensures automated data collection from open vulnerability sources, normalization, contextual enrichment, and analytical processing.

Particular attention is given to the development of a risk-oriented vulnerability prioritization model that combines CVSS severity metrics, EPSS exploitation probability, KEV exploitation status, and the criticality of organizational information assets. Experimental evaluation results demonstrate that the proposed approach enables risk-based differentiation of vulnerabilities and supports integration of analytical results with SIEM, SOAR, and ITSM platforms.

A controlled illustrative experiment showed that automation of data collection, normalization, and prioritization processes has the potential to reduce vulnerability processing time from 28.83 to 5.95 minutes, corresponding to an approximately 4.85× speedup. This confirms the practical value of the proposed architecture as a technological foundation for a Decision Support System within ISMS.

The key result and scientific novelty of the study lie in the development of a risk-oriented decision support approach for vulnerability management, integrating CVSS, EPSS, KEV, and asset criticality into a unified model implemented within a software architecture integrated with SIEM, SOAR, and ITSM. This enables transformation of vulnerability data into context-aware risk indicators and bridges the gap between data accumulation and its practical use within ISMS.

Unlike traditional approaches primarily based on CVSS, the proposed model incorporates exploitation likelihood, evidence of active attacks, and asset criticality, thereby improving risk assessment accuracy.

Future research may focus on extending the analytical capabilities of the system through the application of machine learning methods for predicting vulnerability exploitation, as well as on integrating the system with cyber resilience management platforms and strategic cybersecurity management frameworks.

Acknowledgements

We would like to express our sincere gratitude to all members of the research group whose dedicated and diligent work made a significant contribution to this study. We are also grateful to the staff of the Departments of Information Security Management and Applied Mathematics and Computer Science for their constructive ideas and professional recommendations, which greatly contributed to improving the presented results and their integration into the educational process. Special thanks are extended to the university administration for providing favorable conditions for conducting this research and supporting scientific initiatives. We hope that the presented results will serve as a foundation for further research and contribute to strengthening the cyber resilience of critical systems.

Declaration on Generative AI

During the preparation of this work, GPT-4 was used exclusively for language editing (grammar, spelling, and style). The authors bear full responsibility for the content of the publication.

References

[1] International Organization for Standardization, ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, ISO, Geneva, 2022.

[2] International Organization for Standardization, ISO/IEC 27005:2022 Information security risk management, ISO, Geneva, 2022.

[3] V. Yashchuk, A. Ivanusa, N. Maslova, R. Tkachuk, and T. Brych, "Integration of vulnerability databases into ISMS – a path to enhancing cyber resilience of critical systems," in Resilient Systems: Secure Digital Technologies and Critical Infrastructure. Proceedings of the 1st International Scientific and Practical Conference, Donetsk National Technical University, Drohobych, 2025, pp. 60–66.

[4] International Organization for Standardization, ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls, ISO, Geneva, 2022.

[5] National Institute of Standards and Technology (NIST), Computer Security Incident Handling Guide (SP 800-61 Rev. 2), Gaithersburg, MD, 2012. URL: https://nvlpubs.nist.gov

[6] National Institute of Standards and Technology (NIST), Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (SP 800-137), Gaithersburg, MD, 2011. URL: https://nvlpubs.nist.gov

[7] The Open Group, The Open FAIR™ Body of Knowledge (O-RA, O-RT Standards), Version 2.0, The Open Group, 2020. URL: https://www.opengroup.org/open-fair

[8] MITRE Corporation, Common Vulnerabilities and Exposures (CVE), URL: https://cve.mitre.org , accessed 2026.

[9] National Institute of Standards and Technology, National Vulnerability Database (NVD), URL: https://nvd.nist.gov , accessed 2026.

[10] Cybersecurity and Infrastructure Security Agency, Known Exploited Vulnerabilities Catalog, URL: https://www.cisa.gov/known-exploited-vulnerabilities-catalog , accessed 2026.

[11] FIRST (Forum of Incident Response and Security Teams), Common Vulnerability Scoring System (CVSS) v3.1 Specification, FIRST, 2019.
[12] L. Bracciale et al., "Quantifying medical device cybersecurity risk with CVSS BTE," Scientific Reports, 2025. doi: 10.1038/s41598-025-26898-x
[13] S. Azizi et al., "Vulnerability scoring metric of CVSS needs to be adjusted per each product: Analysis and improvements," Journal of Information Security and Applications, 2025. doi: 10.1080/19393555.2025.2498466
[14] FIRST (Forum of Incident Response and Security Teams), Exploit Prediction Scoring System (EPSS) Model, URL: https://www.first.org/epss, accessed 2026.
[15] J. Jacobs, S. Romanosky, B. Edwards et al., "Enhancing vulnerability prioritization: Data-driven exploit predictions with community-driven insights," arXiv:2302.14172, 2023. doi: 10.48550/arXiv.2302.14172
[16] Y. Jiang, N. Oo, Q. Meng, H. W. Lim, and B. Sikdar, "A survey on vulnerability prioritization: Taxonomy, metrics, and research challenges," arXiv:2502.11070, 2025. URL: https://arxiv.org/abs/2502.11070
[17] A. Balsam, M. Walkowski, M. Nowak, J. Oko, and S. Sujecki, "Automatic CVSS-based vulnerability prioritization and response with context information and machine learning," Applied Sciences, vol. 15, no. 16, p. 8787, 2025. doi: 10.3390/app15168787
[18] N. Shimizu and M. Hashimoto, "Vulnerability management chaining: An integrated framework for efficient cybersecurity risk prioritization," arXiv:2506.01220, 2025. doi: 10.48550/arXiv.2506.01220
[19] S. Ramakrishnan and D. R. Chittibala, "Enhancing cyber resilience: Convergence of SIEM, SOAR, and AI in 2024," International Journal of Computing and Engineering, vol. 5, no. 2, pp. 36–44, 2024. doi: 10.47941/ijce.1754
[20] P. W. Singer and A. Friedman, Cybersecurity and cyberwar: What everyone needs to know, Oxford University Press, Oxford, 2014 (online 2020). doi: 10.1093/wentk/9780199918096.003.0001
[21] V. Mavroeidis and S. Bromander, "Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence," in Proc. European Intelligence and Security Informatics Conference (EISIC), 2017, pp. 91–98. doi: 10.1109/EISIC.2017.20
[22] A. Ahmad, S. B. Maynard, and S. Park, "Information security strategies: Towards an organizational multi-strategy perspective," Journal of Intelligent Manufacturing, vol. 25, pp. 357–370, 2014. doi: 10.1007/s10845-012-0683-0
[23] V. G. Bilali et al., "A SOAR platform for standardizing, automating operational cyber threat intelligence sharing," Proc. ACM, 2024. doi: 10.1145/3664476.3670939
[24] S. Islam, N. Basheer, S. Papastergiou, M. Ciampi, and S. Silvestri, "Intelligent dynamic cybersecurity risk management framework with explainability and interpretability of AI models for enhancing security and resilience of digital infrastructure," Journal of Reliable Intelligent Environments, vol. 11, no. 3, pp. 1–25, 2025. doi: 10.1007/s40860-025-00253-3
[25] M. Mahbub, M. S. A. Khan, M. S. Mia et al., "A novel vulnerability exploit prediction system using the relational vulnerability-vendor network," ACM Transactions on Privacy and Security, 2025. doi: 10.1145/3724133
[26] M. Angelelli, A. Guarino et al., "A robust statistical framework for cyber-vulnerability prioritisation under partial information in threat intelligence," Expert Systems with Applications, vol. 242, p. 124572, 2024. doi: 10.1016/j.eswa.2024.124572
[27] V. Yashchuk, A. Ivanusa, N. Maslova, R. Tkachuk, and T. Brych, "Conceptualization of integrative use of vulnerability databases in the context of system management of information security," Bulletin of Lviv State University of Life Safety, vol. 31, pp. 126–139, 2025. doi: 10.32447/20784643.31.2025.13

[28] V. Yashchuk, "Methods for ensuring information system security and cyber incident response by cybersecurity centers," Scientific Collection InterConf+, vol. 45, no. 201, pp. 632–641, 2024. doi: 10.51582/interconf.19-20.05.2024

[29] N. Maslova, O. Liubymenko, Y. Dorohyi, and A. Ivanusa, "Multi-agent WAF pentesting on the JADE platform," in Proc. 8th International Workshop on Computer Modeling and Intelligent Systems (CMIS-2025), Zaporizhzhia, Ukraine, CEUR Workshop Proceedings, CEUR-WS.org, (2025) CEUR Workshop Proceedings, 3988, p. 282 – 295. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-105010210059&partnerID=40&md5=776df03a12e67ec203c1105aea 558112