

ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ/INFORMATICS AND INFORMATION PROCESSES

DOI: https://doi.org/10.60797/IRJ.2026.170.50 EDN: SOSJEF

MULTI-LEVEL DATA PROTECTION METHODOLOGY FOR 1C INFORMATION SYSTEMS

Research article

Yunusova V.S.[1], Lapteva M.G.[2], Tolmacheva A.V.[3], Panchenko O.V.[4,*]

[1] Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan, Russian Federation

[2, 3, 4] Kazan National Research Technological University, Kazan, Russian Federation

* Corresponding author (panchenkoov[at]corp.knrtu.ru)

Suggested: 08.06.2026; Accepted: 06.07.2026; Published: 17.08.2026

Abstract

The growing volume of processed information, the tightening of personal-data protection requirements (Federal Law No. 152-FZ, the requirements of the FSTEC and FSB of Russia), and the drive toward import substitution and the migration of corporate information systems to domestic software make it relevant to develop data-protection methods adapted to the architecture of the 1C platform, which occupies a dominant position in the Russian corporate segment. The aim of this work is to develop and experimentally verify a practically applicable protection methodology that takes into account the operating modes of 1C databases (file-based and client-server) and the typical architectural solutions of corporate IT infrastructures while maintaining an acceptable level of performance. The methodological basis comprises a comparative analysis of existing approaches, threat modeling using the STRIDE methodology, and experimental verification in an isolated test environment. A multi-level methodology is proposed that combines organizational, technical, and educational measures based on classical information-security principles and the platform's built-in mechanisms — the role-based rights model, record-level access restriction (RLS), the registration log, and scheduled jobs — and employs multi-factor authentication, cryptographic protection compliant with GOST R 34.12-2015, and SIEM-based monitoring. Validation on a copy of a working database over two months showed that the share of blocked unauthorized-access attempts rose from 52% to 97% (a relative increase of about 87%) and that the average incident-response time fell from 14 to 4 minutes, while the system response time increased by only 6–9%. The theoretical significance of the work lies in systematizing the multi-level approach as applied to the 1C platform, and its practical significance in providing a validated regulation ready for implementation.

Keywords: data protection, information security, 1C platform, multi-level protection, database, multi-factor authentication, access control, role-based model, STRIDE threat modeling, cryptographic protection, GOST R 34.12-2015, monitoring, database administration.

МЕТОДОЛОГИЯ МНОГОУРОВНЕВОЙ ЗАЩИТЫ ДАННЫХ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ «1С»

Научная статья

Юнусова В.С.[1], Лаптева М.Г.[2], Толмачева А.В.[3], Панченко О.В.[4,*]

[1] Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань, Российская Федерация

[2, 3, 4] Казанский национальный исследовательский технологический университет, Казань, Российская Федерация

* Корреспондирующий автор (panchenkoov[at]corp.knrtu.ru)

Предложена: 08.06.2026; Принята: 06.07.2026; Опубликована: 17.08.2026

Аннотация

Рост объемов обрабатываемой информации, ужесточение требований к защите персональных данных (Федеральный закон № 152-ФЗ, требования ФСТЭК и ФСБ России), а также стремление к импортозамещению и переходу корпоративных информационных систем на отечественное программное обеспечение обусловливают актуальность разработки методов защиты данных, адаптированных к архитектуре платформы «1С», занимающей доминирующее положение в российском корпоративном сегменте. Целью данной работы является разработка и экспериментальная проверка применимой на практике методологии защиты, учитывающей режимы работы баз данных «1С» (файловый и клиент-сервер) и типичные архитектурные решения корпоративных IT-инфраструктур при сохранении приемлемого уровня производительности. Методологическая основа включает сравнительный анализ существующих подходов, моделирование угроз с использованием методологии STRIDE и экспериментальную проверку в изолированной тестовой среде. Предложена многоуровневая методология, сочетающая организационные, технические и образовательные меры, основанные на классических принципах информационной безопасности и встроенных механизмах платформы — модели прав на основе ролей, ограничении доступа на уровне записей (RLS), журнале регистрации и запланированных заданиях — и использующая многофакторную аутентификацию, криптографическую защиту в соответствии с ГОСТ Р 34.12-2015 и мониторинг на основе SIEM. Тестирование на копии рабочей базы данных в течение двух месяцев показало, что доля заблокированных попыток несанкционированного доступа выросла с 52 до 97% (относительный рост составил около 87%), а среднее время реагирования на инциденты сократилось с 14 до 4 минут, при этом время отклика системы увеличилось лишь на 6–9%. Теоретическая значимость работы заключается в систематизации многоуровневого подхода, примененного к платформе «1С», а практическая — в предоставлении проверенного на практике регламента, готового к внедрению.

Ключевые слова: защита данных, информационная безопасность, платформа «1С», многоуровневая защита, база данных, многофакторная аутентификация, контроль доступа, роль-ориентированная модель, моделирование угроз по методу STRIDE, криптографическая защита, ГОСТ Р 34.12-2015, мониторинг, администрирование баз данных.

Introduction

Digital infrastructure has long ceased to be a mere auxiliary element of business: today it largely determines how quickly and accurately an enterprise makes management decisions, serves its customers, and maintains its internal records. The rapid growth in the volume of processed information, the widening range of automated processes, and the pervasive spread of network services generate a steady demand for IT solutions capable of combining high performance with reliable data protection [1]. In the Russian corporate environment, one of the most widely used products of this kind is the 1C platform, which covers accounting and financial management, document management, logistics, human-resource management, and warehouse operations [2].

As the volume of stored information grows, so do the risks associated with breaches of its confidentiality, integrity, and availability. Even a single incident — a leak of customers' personal data, the substitution of source documents, or the loss of access to a working database — can result in serious financial losses, regulatory sanctions, and reputational damage for an organization. This makes the development of holistic protection methods that take into account the architecture of specific information systems and the features of the corporate IT environment a practically urgent task.

The range of threats faced by 1C-based information systems is extremely broad: malware, the actions of external attackers, administration errors, hardware failures, unintentional actions by employees, and vulnerabilities in both the applied solutions and the platform itself. The task of the database administrator is to ensure protection throughout the entire life cycle of the system — from the initial allocation of access rights to the continuous monitoring of user activity and the handling of incidents [3]. At the same time, common protection methods often prove insufficiently adapted to the specifics of 1C — to its operating modes (file-based and client-server), to its built-in authentication mechanisms, and to its scheduled jobs — which gives rise to a situation in which formal compliance with requirements does not guarantee actual security [4].

This work is devoted to analyzing the approaches to data protection currently used in 1C systems, identifying their weaknesses, and building on this basis a more balanced methodology that combines organizational, technical, and software mechanisms. The key principle underlying the study is multi-layeredness: in our view, sustainable protection cannot be achieved by purely technological or purely regulatory means taken separately; a combination of tools, procedures, and staff competencies working in concert is required.

The study covers the entire cycle of work — from a review and comparison of known solutions to the development of an original methodology, its verification in a test environment, and an assessment of the resulting effect. The ultimate goal is a tangible increase in the security of corporate data stored in 1C databases and a reduction in the probability of the successful realization of both external and internal threats.

The relevance of the topic is driven by several simultaneously acting trends. The first is the steady growth in the number and sophistication of cyber threats: the number of incidents involving unauthorized access to corporate databases increases year on year, and the attacks themselves are increasingly targeted [5]. The second is the tightening of regulatory requirements for handling information, primarily personal data: Federal Law No. 152-FZ "On Personal Data", the orders of the FSTEC of Russia, and the requirements of the FSB of Russia for protection tools set a mandatory level of measures, non-compliance with which entails administrative and, in some cases, more serious liability [6]. The third trend is technological in nature — the drive toward import substitution and the migration of corporate information systems to domestic software [7], in which the 1C platform occupies a dominant position. Taken together, these factors turn the development of a 1C-adapted data protection methodology from a narrow technical problem into a practically significant and sought-after task.

The object of the study is the process of administering and protecting the database management system used by the 1C platform.

The subject of the study is the interconnected set of organizational, software-technical, and educational means of ensuring the confidentiality, integrity, and availability of data, considered in relation to the operating modes and built-in mechanisms of the 1C platform during the administration of systems of this class.

The aim of the work is to develop and experimentally verify a practically applicable protection methodology that takes into account both the features of 1C database operation and the typical architectural solutions of corporate IT infrastructures, while ensuring a tangible increase in data security with an acceptable level of system performance.

Achieving this aim involves solving the following tasks:

1) to carry out a critical review of current protection methods and assess the actual level of data security in a typical 1C administration scenario;

2) to identify the strengths and weaknesses of these methods, as well as their characteristic residual risks;

3) to formulate a comprehensive methodology combining organizational, technical, and educational measures;

4) to conduct testing and validation of the methodology under conditions that model real corporate operation;

5) to prepare practical recommendations and a regulation suitable for implementing the methodology at an enterprise.

The methodological basis of the work comprises a comparative analysis of existing approaches to database protection, threat modeling using the STRIDE methodology, the design of a comprehensive methodology based on classical information-security principles, and the experimental verification of the proposed solutions in an isolated test environment with subsequent validation on a copy of a working 1C database.

The scientific novelty of the work is as follows. First, the typical multi-level protection model is adapted to the architecture and operating modes of the 1C platform — file-based and client-server — relying on its built-in mechanisms: the role-based rights model, record-level access restriction, the registration log, and scheduled jobs. Second, organizational, technical, and

educational measures are combined into a single verified methodology, whereas in most known solutions they are applied in isolation [8]. Third, based on validation on a copy of a working database, a quantitative assessment of the balance between the level of security and system performance has been obtained, which makes it possible to reasonably recommend the methodology for practical implementation [9].

Analysis of Existing Database Security Methods

Examining the methodological approaches to database protection in the course of administering 1C applied solutions is not a formal introductory section but a substantive starting point of the study. The modern information environment exists amid a constant escalation of cyber threats, and this background cannot be ignored. 1C databases store information that is critically important for the operation of any organization: financial aggregates, information about counterparties and employees, elements of trade secrets, and operational business-process data. For this reason, the protection of such databases cannot be limited to any single layer or technology — it requires constant revision and a comprehensive approach.

The methods used today can conveniently be grouped into three large directions that differ in the nature of the means employed.

The first direction consists of organizational measures: the development of local regulations on data protection, the assignment of personal responsibility for compliance with them, and regular staff training. Security policies here play the role of a framework — they formalize the rules of access to information resources, describe the procedure for processing data, and regulate actions in the event of an incident.

The second direction comprises technical means of protection. These include cryptographic mechanisms, access-control tools, and the regular updating of software. Encryption practically rules out the possibility of reading data without a key even if it is intercepted; a properly configured access-control system shuts out users who lack the necessary privileges; and timely software updates close known vulnerabilities and reduce the system's susceptibility to external attacks.

The third direction is monitoring and auditing. Its task is to record deviations from the system's normal behavior and to suppress threats before they are fully realized. This includes observing user actions, analyzing event logs, and applying automated audit tools that make it possible to recognize anomalies, detect attempts at unauthorized access, and reconstruct the course of incidents. It is fundamentally important that data collection in itself is meaningless — value is gained only from its systematic analytical processing.

The starting point for building a protection system is a correct assessment of the threats affecting the database infrastructure. By their source, they are conventionally divided into internal and external. Internal threats, as practice shows, most often arise from the human factor — whether poor staff training, the violation of regulations, or unintentional errors. External threats are associated with the deliberate actions of attackers: network attacks, the spread of malware, and the use of social-engineering methods.

To systematize possible threat scenarios and subsequently assess risks, special models are used. Among them, the STRIDE model has become especially widespread, combining six characteristic types of threats:

- S — Spoofing (identity spoofing);
- T — Tampering (violation of integrity);
- R — Repudiation (denial of actions performed);
- I — Information Disclosure;
- D — Denial of Service (violation of availability);
- E — Elevation of Privilege.

An effective security methodology must take into account the evolution of threats and follow changes in the arsenal of protection tools. In essence, this is not a one-off project but a continuous process of adaptation: an analytical review of new risks, the adjustment of measures, and the introduction of up-to-date tools — all of this should become regular practice (Table 1).

Table 1 - Comparison of methods

DOI: https://doi.org/10.60797/IRJ.2026.170.50.1

Direction	Goals and objectives	Advantages	Limitations	Main measures
Organizational	Establishing access regulations; defining procedures for interaction and response	A clear management structure; greater staff discipline and awareness	Dependence on the human factor; the need for regular training	Security policies; appointment of responsible persons; training sessions
Technical	Protecting information and preventing unauthorized access	A high degree of protection; the possibility of automation	Additional costs; the need for qualified maintenance	Encryption; access control; software updates
Monitoring and auditing	Detecting threats; analyzing anomalies; preventing attacks	Timely response; the possibility of incident analysis	Possible false positives; resource demands	Monitoring systems; action auditing; IDS/IPS

Among the architectural approaches to building protection, the most widespread is the multi-level model, in which security is ensured sequentially at the physical, network, and application layers.

• The physical layer is responsible for protecting the server infrastructure: controlled access to technical premises, video-surveillance systems, alarms, and organizational measures for admitting employees and contractors.

• The network layer is provided by firewalls, intrusion-detection systems, VPN connections, and the encryption of network traffic; multi-factor authentication is mandatory for remote connection to 1C databases [10].

• The application layer is oriented directly toward business logic: the correct configuration of roles and rights, protection against SQL injection, the secure development of 1C configurations, and the consistent application of the principle of least privilege [11].

Backup and, more broadly, recovery mechanisms play an integral role in this scheme: they are precisely what minimize damage in any incident — from a hardware failure to a successful attack. The factor of staff training is no less significant: incident statistics consistently show that a substantial proportion of information-security breaches are associated not with sophisticated targeted attacks but with errors or negligence on the part of employees (Table 2).

Table 2 - Comparative characteristics of data protection measures

DOI: https://doi.org/10.60797/IRJ.2026.170.50.2

Approach	Advantages	Disadvantages
Physical protection	Protection of equipment from theft and damage	Does not protect against internal threats
Access management	Control of actions and restriction of user rights	Configuration complexity, risk of errors
Encryption	A high level of data integrity	Reduced performance, the need for key management
Backup	The possibility of data recovery	Risk of backup leaks
Monitoring and auditing	The possibility of detecting violations	High costs and resource demands
Staff training	Improved literacy and attentiveness	Requires time and a systematic approach

Development of the Database Security Methodology

Designing a methodology for protecting a 1C database at an enterprise is one of the central tasks within the broader scope of managing corporate information resources. Its successful implementation requires simultaneously taking into account technical and organizational aspects and relying on the classical principles of information security [12], [13].

The basic element of the methodology is a set of data-protection principles whose observance increases the system's resilience to potential threats. The first and perhaps most significant of them is confidentiality — restricting access to information to a circle of specially authorized persons. In the 1C system, this principle is implemented through the combination of authentication and authorization mechanisms, the configuration of roles and access rights, and record-level access restriction (RLS), which makes it possible to differentiate the visibility of data down to specific table rows.

The second principle is data integrity: information in the database must be kept in a correct, internally consistent state. Its maintenance is ensured by record-versioning mechanisms, verification of the operations performed, and regular backups, which in 1C can conveniently be automated using scheduled jobs, making it possible to restore the database to a working state in the event of an incident.

The third principle is availability: the information system must operate continuously, and any downtime that disrupts the course of business processes should be minimized. This is achieved by maintaining the serviceability of the server equipment, building a fault-tolerant architecture, and using prompt post-failure recovery procedures.

The fourth principle is accounting and auditing. It requires the mandatory recording of the actions of users and administrators in system logs; in the 1C platform, this role is performed by the built-in registration log, which reflects login events, data changes, and operations with access rights. Regular analysis of these logs makes it possible to notice deviations from the usual picture of work and to recognize potential incidents before they escalate into serious ones.

The fifth principle is the minimization of privileges. According to it, a user should have exactly the set of privileges necessary to perform their job duties — no more and no less. Any excessive rights turn into a potential entry point for an attacker or a source of unintentional error.

Finally, the principle of protection against threats covers the arsenal of directly technical means: antivirus suites, firewalls, intrusion detection and prevention systems (IDS/IPS), as well as the physical protection of the premises housing the server equipment.

Measures to improve users' digital literacy are also among the mandatory components of the methodology: without sufficient staff competencies, the effectiveness of even the most carefully designed technical solutions is noticeably reduced.

One of the core components of protection is authentication — the procedure for confirming a user's identity when logging into the system. The 1C platform natively supports password protection; additionally, biometric methods and two-factor

authentication (2FA) may be used. Passwords must meet strength requirements and be changed periodically [14], and the account must be automatically locked after three consecutive unsuccessful login attempts [15].

Two-factor authentication provides an additional barrier: to confirm their identity, the user must present two independent factors. The general scheme of its operation is shown in Figure 1.

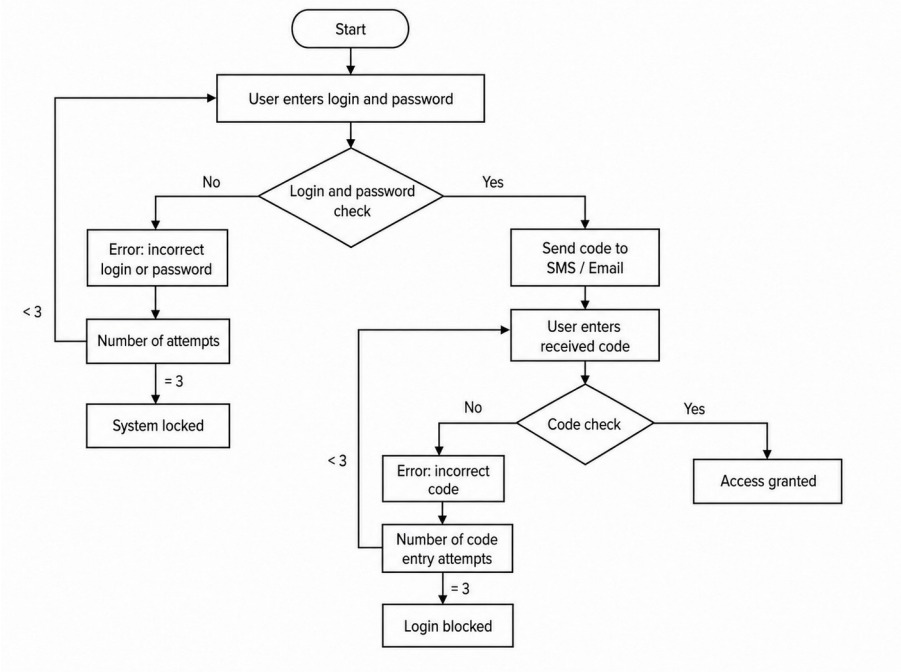

Figure 1 - Two-factor authentication scheme in 1C
DOI: https://doi.org/10.60797/IRJ.2026.170.50.3

Two-factor authentication is based on a combination of factors of three different types: something the user knows (login and password), something they possess (a smartphone or a hardware token), and something that characterizes them (a fingerprint, an iris pattern, or facial features). The login scenario is structured as follows. The user enters their credentials, and the system checks their correctness. If the data are correct, a one-time confirmation code is sent to a previously registered device; if not, the user receives an error notification. The system compares the entered code with its reference value. On a match, it grants access to the database; on a mismatch, it records a failed attempt; after three consecutive unsuccessful attempts, the account is temporarily locked.

After authentication, authorization comes into effect — the mechanism that determines which actions are permitted to a particular user [16]. Its correctness is directly related to compliance with the principle of least privilege and requires maintaining an up-to-date register of users and conducting periodic checks. Another essential layer of protection is cryptographic mechanisms: they guarantee the integrity of information even when an attacker gains direct physical access to the storage media. In Russian practice, certified cryptographic information protection tools (CIPF) are used for this purpose, implementing algorithms compliant with GOST R 34.12-2015 ("Kuznyechik" and "Magma") [17], [18], which ensures conformity with regulatory requirements.

The protection system must also include a monitoring and auditing loop aimed at detecting suspicious activity. SIEM platforms have proven themselves well in this role: they collect events from many sources in real time, correlate them, and signal anomalies. No less important is the organization of secure log storage, which ensures the immutability of the recorded entries and thereby their evidentiary value. Incident-response procedures are built on monitoring data, covering the identification of an event, the collection of initial information, the temporary restriction of access, the elimination of the root cause, and the subsequent restoration of normal system operation.

The effectiveness of a security strategy is ultimately determined by the quality of interaction among the IT service, information-security specialists, and the organization's management. Forming an appropriate corporate culture and providing systematic staff training strengthen the system's resilience to external influences and noticeably reduce the overall level of risk.

Testing and Validation of the Developed Methodology

Verifying the operability and effectiveness of the developed methodology is the final but by no means formal stage of the study. It is at this stage that it becomes clear how applicable the proposed solutions are under conditions as close as possible to real operation, and which of them require refinement. So as not to put the enterprise's working system at risk, all experiments are conducted in a specially prepared test environment isolated from production.

The aim of testing is to obtain a well-rounded assessment of the effectiveness of the proposed measures as applied to a 1C database across several groups of indicators: resilience to external and internal influences, data integrity, stability of operation, and ease of administration. The initial system configuration without the proposed protection measures is taken as a baseline for comparison, which makes it possible to assess precisely the contribution of the methodology. The test environment should

replicate the configuration of the enterprise's real IT infrastructure while remaining isolated from the production environment. The most successful solution is a virtualized server platform with an up-to-date copy of the working 1C database deployed on it, on which characteristic attacks and abnormal situations are reproduced according to controlled scenarios corresponding to the threat types of the STRIDE model.

The testing process is structured in three sequential stages:

1. Functional verification — checking the operability of all components included in the methodology. At this stage, the correct operation of the authentication, authorization, backup, cryptographic-protection, and monitoring mechanisms is verified.

2. Load testing — measuring the performance and stability margin of the system as the number of simultaneous users grows, the flow of transactions increases, and typical queries become more complex.

3. Assessment of the ergonomics of administration and user work — collecting feedback from IT specialists and ordinary users through surveys, interviews, and comparison with the system's operation logs.

Upon completion of all three stages, the results are brought together, interpreted, and formalized as an analytical report.

Validation Results

Following the testing procedure described above, the data obtained were subjected to analytical processing. Among the strengths of the developed methodology are its ability to suppress unauthorized-access attempts and to reduce the system's susceptibility to user errors; the obvious costs include increased server load, the need for additional staff training, and a certain complication of administration.

Validation was carried out over two months on a copy of the organization's working 1C database, which made it possible to assess the effectiveness of the methodology under conditions as close as possible to the working environment. The key indicators recorded were the proportion of blocked unauthorized-access attempts, the average incident-response time, and the average system response time during typical operations; all values were compared with the initial configuration taken as the baseline. To obtain reproducible estimates, a fixed battery of 500 simulated unauthorized-access attempts spanning the six STRIDE threat categories was replayed in ten independent test runs against both the baseline configuration and the system protected by the proposed methodology, and the figures reported below are averaged over these runs. The share of successfully blocked unauthorized-access attempts rose from 52 ± 3% in the baseline configuration to 97 ± 1% with the proposed measures in place — that is, a relative increase of about 87% (an absolute gain of roughly 45 percentage points). The average incident-response time was reduced from 14 to 4 minutes. For typical user operations, the average response time increased by 6–9% depending on the type of operation (on average, from 0.45 to 0.49 s) — an increase that falls within the acceptable range and is practically imperceptible to users in everyday work. The tests confirmed the effectiveness of the combined approach that brings together multi-factor authentication, backup, monitoring, and auditing. At the same time, the connection of cryptographic mechanisms predictably increased the server load, which required additional configuration optimization. The resulting balance between the increase in security and the moderate decrease in performance makes it possible to recommend the methodology for implementation in the enterprise's production environment.

Implementation of the Methodology at an Enterprise

The practical implementation of a 1C database protection methodology is perhaps the most critical part of the entire effort: it is here that theoretical constructs collide with the reality of the enterprise, and the effectiveness of the proposed measures is entirely determined by the accuracy of their execution. Implementation is not only the installation and configuration of technical means but also systematic work with people, forming within the team a culture of secure handling of information. The starting point is a diagnosis of the current state of the protection system: an audit of existing regulations, an inventory of the tools used, the identification of bottlenecks, and a check against regulatory requirements. The resulting picture becomes the basis for a list of the necessary technical and organizational improvements.

Next, a detailed implementation plan is drawn up: stages are identified, deadlines are stipulated, and areas of responsibility are distributed among the project participants. A responsible person is appointed for each key area — technical administration, monitoring, training, and oversight of regulation compliance. After this, the technical part proper begins: updating the applied solutions, deploying additional protection tools, configuring monitoring tools, updating software, and introducing data-recovery procedures. All work is carried out sequentially and in a coordinated order, which makes it possible to avoid prolonged downtime and to reduce the risk of disrupting normal system operation.

A special place in implementation is occupied by staff training: the level of security is directly related to the discipline of following the rules. The training program combines theoretical and practical parts. For technical specialists, the emphasis is on the intricacies of administration, security issues, and the procedure for responding to incidents; for ordinary users, on the rules of safe work, the creation of strong passwords, the recognition of forged messages, and the prevention of information leaks. The formats can vary: lectures, seminars, online courses, workshops, and a concluding test. After formal training, it is advisable to deploy a consulting-support system — it allows employees to promptly obtain clarifications on emerging questions and not to accumulate unresolved problems.

For greater clarity of the development and implementation of security policies, the entire process is formalized as a flowchart that records the order in which the training and regulatory measures are carried out (Figure 2).

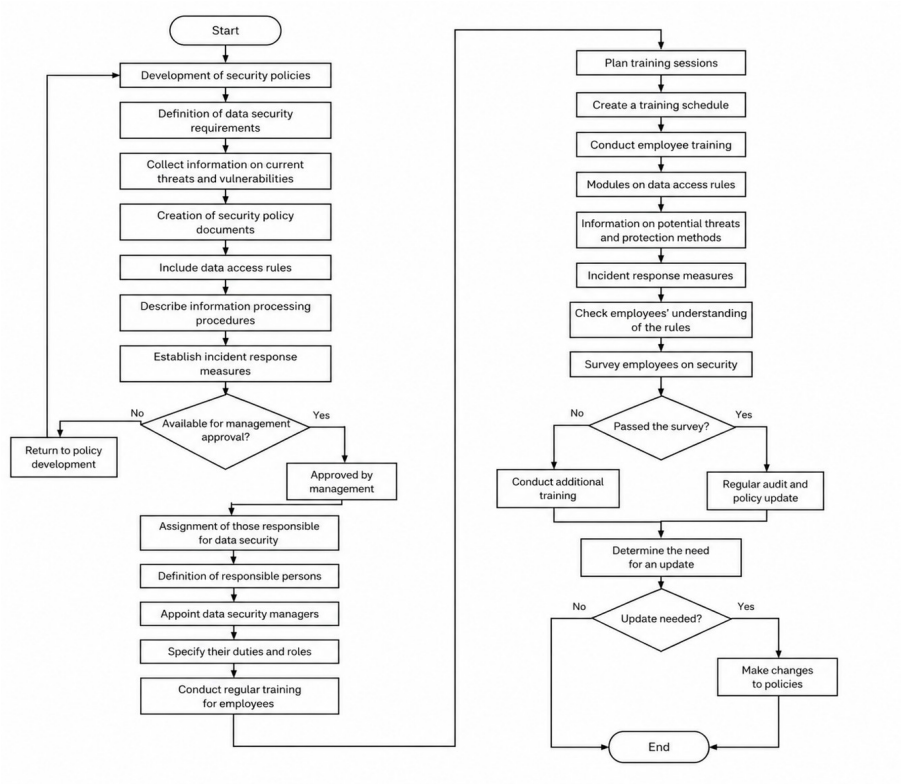

Figure 2 - Flowchart of security policy development and implementation
DOI: https://doi.org/10.60797/IRJ.2026.170.50.4

The process of implementing the information-security methodology itself is conveniently represented as a sequence of steps unfolding over time. It begins with the launch of a formal implementation procedure and the development of a security policy, within which the list of current threats is outlined and the requirements, access rules, the procedure for handling data, and response measures are recorded. The prepared package of documents is agreed upon with management, after which responsible persons and their functions are assigned. This is followed by training events that conclude with a check of staff knowledge; if the results are unsatisfactory, the training cycle is repeated. Once the plan is approved, a working group is formed — it includes information-security specialists, 1C administrators, and representatives of the departments that use the system. On this basis, work regulations and detailed instructions on access, backup, authentication, and monitoring are developed.

Next comes the turn of technical work: cryptographic mechanisms are selected and configured, the rights-differentiation and authentication system is set up, monitoring with log keeping is deployed, and a schedule for software updates and testing is drawn up. In parallel, the vulnerability-auditing procedure and the incident-response order are refined, and staff training is conducted. Each block of measures — technical and organizational — must undergo testing followed by the collection of user feedback, which makes it possible to adjust the implementation process in a timely manner.

After all elements of the methodology have been deployed, the task of continuously monitoring its effectiveness becomes critically important. This includes analyzing access logs and system events, conducting periodic penetration tests, assessing the clarity and convenience of the regulations for employees, surveying users and administrators, and checking against current standards and regulatory requirements. The assessment scale should be two-dimensional: quantitative indicators (the proportion of blocked unauthorized-access attempts, the average incident-response time, the average system response time) should be complemented by qualitative ones — staff satisfaction and the degree of actual compliance with the established rules.

Thus, the implementation of the methodology is not a one-time campaign but a multi-stage and recurring process that requires consistency of action and constant oversight. For the result to be sustainable, the effectiveness of the measures applied must be regularly reviewed and the methodology promptly adapted to changes in the technological landscape and the emergence of new threats.

Conclusion

The study conducted on the topic "A Multi-Level Data Protection Methodology for 1C Information Systems" made it possible to formulate and validate a set of theoretical propositions and practical solutions aimed at improving the reliability of storing and processing corporate data. A review of existing approaches showed their strengths and weaknesses and, most importantly, revealed an obvious gap: the insufficient adaptation of typical methods to the architectural features of the 1C platform.

All the stated tasks have been solved. A critical review of current protection methods was carried out and the actual level of data security in a typical 1C administration scenario was assessed; their strengths and weaknesses, as well as their characteristic residual risks, were identified; a comprehensive methodology combining organizational, technical, and

educational measures was formulated; its testing and validation were conducted under conditions modeling real operation; and practical recommendations and a regulation suitable for implementation at an enterprise were prepared.

It has been established that ensuring data security in 1C administration is impossible without a comprehensive approach that combines technical, organizational, regulatory, and educational measures. In the course of development, the key elements of protection were identified: the differentiation of access levels, the creation and storage of backups, the use of encryption, and tools for monitoring and incident response. Particular attention was paid to the principles of authentication, authorization, and control of user actions.

The practical part of the work included testing and validation of the developed methodology under conditions modeling a real operating environment. The results obtained are convincing: the share of successfully blocked unauthorized-access attempts rose from 52% to 97% (a relative gain of about 87%), the average incident-response time was reduced from 14 to 4 minutes, while the increase in the average response time was only 6–9%. Taken together, the implementation of the proposed measures appreciably reduced the probability of data loss, integrity violations, and unauthorized access to data.

The final stage of the study was the implementation of the methodology in the enterprise's operations — with the preparation of regulatory documents, staff training, and the deployment of a monitoring and control system. This stage demonstrated an essential point: information security is inextricably linked not only with technology but also with the human factor. Forming a culture of secure behavior among users and an awareness of their own responsibility is not a declarative but a key element of a sustainable protection system.

In the end, the developed methodology represents a holistic, practically applicable solution that makes it possible to adapt existing security mechanisms to the specifics of administering 1C databases. Its theoretical significance lies in systematizing the multi-level approach as applied to this platform, and its practical significance in the availability of a proven regulation ready for implementation. It should be borne in mind that validation was carried out at a single organization, so further verification of the methodology on various configurations and in different industries remains a separate task; nevertheless, the work done confirms its relevance amid the growth of cyber threats and the tightening of requirements for protecting corporate information resources.

To further improve the protection system, the authors consider it advisable:

1) to conduct regular audits of the state of information security and to promptly update the methods used;

2) to maintain a high level of staff competencies through systematic training and practical exercises;

3) to introduce modern technological solutions and automated control tools that meet the requirements of industry and state standards.

Ensuring the security of 1C databases is not a task with a one-time solution but a continuous process based on a comprehensive approach, the ability to adapt to new threats, and the constant improvement of the tools and procedures applied.

Конфликт интересов

Не указан.

Рецензия

Борисов А.Н., Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань Российская Федерация
DOI: https://doi.org/10.60797/IRJ.2026.170.50.5
Сообщество рецензентов Международного научно-исследовательского журнала
DOI: https://doi.org/10.60797/IRJ.2026.170.50.6

Conflict of Interest

None declared.

Review

Borisov A.N., Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan Russian Federation
DOI: https://doi.org/10.60797/IRJ.2026.170.50.5
Community of Reviewers of the International Research Journal
DOI: https://doi.org/10.60797/IRJ.2026.170.50.6

Список литературы / References

1. Ковалев В.Е. Внедрение ERP-систем малыми и средними компаниями в России: барьеры и перспективы / В.Е. Ковалев, К.В. Новикова, В.Д. Добровлянин // Управленец. — 2023. — Т. 14. — № 6. — С. 77–90. — DOI: 10.29141/2218-5003-2023-14-6-6. — EDN: EPLGEJ.

2. Smolentseva L.V. Application of the Information System "1C: Enterprise" in the Cooperative Sector of the Economy / L.V. Smolentseva, L.A. Gainulova, A.M. Akhmedova [et al.] // Cooperation and Sustainable Development. — 2021. — DOI: 10.1007/978-3-030-77000-6_110.

3. Ivanov O. 1C software vulnerabilities description / O. Ivanov, D. Silnov. — Art. 01059. — DOI: 10.1051/shsconf/20173501059.

4. Initiative J.T.F.T. Risk management framework for information systems and organizations: a system life cycle approach for security and privacy / J.T.F.T. Initiative. — 2018. — DOI: 10.6028/nist.sp.800-37r2.

5. Gusev A. New cyberattacks vectors of Russian critical infrastructure enterprises: domestic private banking sector view within AI protection methods / A. Gusev // Procedia Computer Science. — 2020. — № 169. — P. 314–319. — DOI: 10.1016/j.procs.2020.02.189.

6. Российская Федерация. Законы. О персональных данных: федер. закон: [от 27 июля 2006 года № 152-ФЗ (с учётом всех внесённых изменений)] // Собрание законодательства Российской Федерации. — 2006. — № 31. — Ст. 3451.

7. О мерах по обеспечению технологической независимости и безопасности критически важной информационной инфраструктуры Российской Федерации: Указ Президента Российской Федерации от 30 марта 2022 года № 166 //

Официальный интернет-портал правовой информации. — URL: http://publication.pravo.gov.ru/Document/View/0001202203300001 (дата обращения: 17.04.2026).

8. Gupta B. Security, privacy and forensics in the enterprise information systems / B. Gupta, D. Agrawal // Enterprise Information Systems. — 2021. — № 15. — P. 445–447. — DOI: 10.1080/17517575.2020.1791364.

9. Li Y. Role-Based Access Control Model for Inter-System Cross-Domain in Multi-Domain Environment / Y. Li, Z. Du, Y. Fu [et al.] // Applied Sciences. — 2022. — DOI: 10.3390/app122413036.

10. Park J.-H. A Proposal for a Zero-Trust-Based Multi-Level Security Model and Its Security Controls / J.-H. Park, S. Park, H. Youm // Applied Sciences. — 2025. — DOI: 10.3390/app15020785.

11. Logrippo L. Multi-level models for data security in networks and in the Internet of things / L. Logrippo // J. Inf. Secur. Appl. — 2021. — № 58. — Art. 102778. — DOI: 10.1016/j.jisa.2021.102778.

12. Zalozhnev A. Information Security Control Engineering for an Industrial Company with "1C" Software / A. Zalozhnev, D.V. Chistov // 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET). — 2023. — P. 1–6. — DOI: 10.1109/icecet58911.2023.10389577.

13. Stepanova A.E. Vulnerability Research of Software Products 1C Enterprise / A.E. Stepanova, A. Vladimirov, A.P. Klarin // 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2014–2017. — 2020. — DOI: 10.1109/eiconrus49466.2020.9038990.

14. Hasan S.S.U. A Review on Secure Authentication Mechanisms for Mobile Security / S.S.U. Hasan, A. Ghani, A. Daud [et al.] // Sensors (Basel, Switzerland). — 2025. — № 25. — DOI: 10.3390/s25030700.

15. Rui Z. A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification / Z. Rui, Z. Yan // IEEE Access. — 2018. — № 7. — P. 5994–6009. — DOI: 10.1109/access.2018.2889996.

16. Sahyudi M. Analisis Implementasi Sistem Keamanan Basis Data Berbasis Role-Based Access Control (RBAC) pada Aplikasi Enterprise Resource Planning / M. Sahyudi, E.R. Susanto // SATESI: Jurnal Sains Teknologi dan Sistem Informasi. — 2025. — DOI: 10.54259/satesi.v5i1.3997.

17. Ishchukova E. Fast Implementation and Cryptanalysis of GOST R 34.12-2015 Block Ciphers / E. Ishchukova, L. Babenko, M. Anikeev // Proceedings of the 9th International Conference on Security of Information and Networks. — 2016. — DOI: 10.1145/2947626.2947657.

18. Smyslov V. Using GOST Ciphers in the Encapsulating Security Payload (ESP) and Internet Key Exchange Version 2 (IKEv2) Protocols / V. Smyslov // RFC. — 2022. — 9227. — P. 1–22. — DOI: 10.17487/rfc9227.

Список литературы на английском языке / References in English

1. Kovalev V.E. Vnedrenie ERP-sistem malimi i srednimi kompaniyami v Rossii: bareri i perspektivi [ERP systems in small and medium-sized enterprises: Barriers and prospects] / V.E. Kovalev, K.V. Novikova, V.D. Dobrovlyanin // Upravlenets [The Manager]. — 2023. — Vol. 14. — № 6. — P. 77–90. — DOI: 10.29141/2218-5003-2023-14-6-6. — EDN: EPLGEJ. [in Russian]

2. Smolentseva L.V. Application of the Information System "1C: Enterprise" in the Cooperative Sector of the Economy / L.V. Smolentseva, L.A. Gainulova, A.M. Akhmedova [et al.] // Cooperation and Sustainable Development. — 2021. — DOI: 10.1007/978-3-030-77000-6_110.

3. Ivanov O. 1C software vulnerabilities description / O. Ivanov, D. Silnov. — Art. 01059. — DOI: 10.1051/shsconf/20173501059.

4. Initiative J.T.F.T. Risk management framework for information systems and organizations: a system life cycle approach for security and privacy / J.T.F.T. Initiative. — 2018. — DOI: 10.6028/nist.sp.800-37r2.

5. Gusev A. New cyberattacks vectors of Russian critical infrastructure enterprises: domestic private banking sector view within AI protection methods / A. Gusev // Procedia Computer Science. — 2020. — № 169. — P. 314–319. — DOI: 10.1016/j.procs.2020.02.189.

6. Russian Federation. Laws. O personalnikh dannikh [On Personal Data]: Federal Law: [No. 152-FZ of 27 July 2006 (as amended)] // Sobranie zakonodatelstva Rossiiskoi Federatsii [Collected Legislation of the Russian Federation]. — 2006. — № 31. — Art. 3451. [in Russian]

7. O merakh po obespecheniyu tekhnologicheskoi nezavisimosti i bezopasnosti kriticheski vazhnoi informatsionnoi infrastrukturi Rossiiskoi Federatsii [On measures to ensure the technological independence and security of the critical information infrastructure of the Russian Federation]: Decree of the President of the Russian Federation No. 166 of 30 March 2022 // Ofitsialnii internet-portal pravovoi informatsii [Official Internet Portal of Legal Information]. — URL: http://publication.pravo.gov.ru/Document/View/0001202203300001 (accessed: 17.04.2026). [in Russian]

8. Gupta B. Security, privacy and forensics in the enterprise information systems / B. Gupta, D. Agrawal // Enterprise Information Systems. — 2021. — № 15. — P. 445–447. — DOI: 10.1080/17517575.2020.1791364.

9. Li Y. Role-Based Access Control Model for Inter-System Cross-Domain in Multi-Domain Environment / Y. Li, Z. Du, Y. Fu [et al.] // Applied Sciences. — 2022. — DOI: 10.3390/app122413036.

10. Park J.-H. A Proposal for a Zero-Trust-Based Multi-Level Security Model and Its Security Controls / J.-H. Park, S. Park, H. Youm // Applied Sciences. — 2025. — DOI: 10.3390/app15020785.

11. Logrippo L. Multi-level models for data security in networks and in the Internet of things / L. Logrippo // J. Inf. Secur. Appl. — 2021. — № 58. — Art. 102778. — DOI: 10.1016/j.jisa.2021.102778.

12. Zalozhnev A. Information Security Control Engineering for an Industrial Company with "1C" Software / A. Zalozhnev, D.V. Chistov // 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET). — 2023. — P. 1–6. — DOI: 10.1109/icecet58911.2023.10389577.

13. Stepanova A.E. Vulnerability Research of Software Products 1C Enterprise / A.E. Stepanova, A. Vladimirov, A.P. Klarin // 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2014–2017. — 2020. — DOI: 10.1109/eiconrus49466.2020.9038990.

14. Hasan S.S.U. A Review on Secure Authentication Mechanisms for Mobile Security / S.S.U. Hasan, A. Ghani, A. Daud [et al.] // Sensors (Basel, Switzerland). — 2025. — № 25. — DOI: 10.3390/s25030700.

15. Rui Z. A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification / Z. Rui, Z. Yan // IEEE Access. — 2018. — № 7. — P. 5994–6009. — DOI: 10.1109/access.2018.2889996.

16. Sahyudi M. Analisis Implementasi Sistem Keamanan Basis Data Berbasis Role-Based Access Control (RBAC) pada Aplikasi Enterprise Resource Planning / M. Sahyudi, E.R. Susanto // SATESI: Jurnal Sains Teknologi dan Sistem Informasi. — 2025. — DOI: 10.54259/satesi.v5i1.3997.

17. Ishchukova E. Fast Implementation and Cryptanalysis of GOST R 34.12-2015 Block Ciphers / E. Ishchukova, L. Babenko, M. Anikeev // Proceedings of the 9th International Conference on Security of Information and Networks. — 2016. — DOI: 10.1145/2947626.2947657.

18. Smyslov V. Using GOST Ciphers in the Encapsulating Security Payload (ESP) and Internet Key Exchange Version 2 (IKEv2) Protocols / V. Smyslov // RFC. — 2022. — 9227. — P. 1–22. — DOI: 10.17487/rfc9227.