


# Improving the Efficiency of Risk Assessment and Documentation Processing to Ensure Information Security of Oilfield Services Companies

Krasnov A.E. <sup>1</sup> <sup>a</sup> and Lystsev K.S. <sup>2</sup> <sup>b</sup>

<sup>1</sup> Doctor of Physical and Mathematical Sciences, Professor of the Federal State Budgetary Educational Institution of Higher Education Russian State Social University

<sup>2</sup> Postgraduate student of the Federal State Budgetary Educational Institution of Higher Education Russian State Social University

krasnovmgutu@yandex.net , Konstantin.Lystsev@bk.ru

Keywords : oilfield services companies, management, information security, automation, protection, sustainability.

Abstract : Information security is of paramount importance in modern society . studies regions Oilfield service companies were selected as a potential site for automation of information security processes , as their activities encompass all the key elements of modern commercial manufacturing companies. The study identified key elements of information security at oilfield service companies, as well as the specific features and objectives of a local information security system.

## 1 INTRODUCTION

Oilfield service companies represent a broad class of companies implementing a variety of operating models – from the performance of strictly defined types of work to integrated software solutions and field operators.

As a rule, oilfield service companies ensure the parallel implementation of many interconnected operations, from planning, exploration, production, to the development of automated control systems (ACS) for production and technological processes (TP).


The oilfield services industry is complex, and to ensure successful exploration, drilling, production, and distribution of oil and gas, it is necessary to effectively manage operations not only at the oilfield but also at the development sites and establish automated production and process control systems. Operations management plays a critical role in achieving operational efficiency, reducing costs, and improving safety. Oilfield services operations encompass a wide range of activities, including drilling, well completions , production, transportation, and maintenance. Managing these


operations requires highly coordinated efforts and the use of advanced technologies to optimize productivity and reduce costs. According to a recent report, the global oilfield services market was valued at \$257.5 billion in 2019 and is expected to grow at a CAGR of 3.7% from 2020 to 2027. The report also highlights the growing demand for efficient and cost-effective oilfield operations as a key market driver.

Thus, the study of the practice of ensuring information security of oil service enterprises has significant practical potential.

One of the most significant challenges in managing oil field operations is the sheer scale of the operations. Oil field operations involve a vast network of equipment, personnel, and processes, making them difficult to manage effectively. Furthermore, oil field operations are often conducted in remote and challenging environments, which can create associated risks. Thus, the vast majority of oilfield service companies worldwide are implementing programs to address functional gaps in the technologies they currently use to manage their businesses.

The oil and gas sector faces unique challenges due to its geographical dispersion . Infrastructure.

<sup>a</sup>  <https://orcid.org/0000-0002-4075-4427>

<sup>b</sup>  <https://orcid.org/0009-0005-6513-6587>

Production facilities are often located at significant distances from each other—fields can be located in hard-to-reach regions, hundreds of kilometers from processing plants and logistics hubs. This spatial dispersion of hydrocarbon production, transportation, and processing facilities requires special approaches to organizing the management and control of technological processes.

Remote drilling rigs, including offshore platforms located in the open sea or land wells in the Arctic and other hard-to-reach regions, pose particular challenges. These facilities often operate with limited communication channels, making it difficult to transmit data in real time. Unstable internet, dependence on satellite communications, and high latency create significant technological barriers to the implementation of digital solutions.

Modern oilfield services companies face exceptional complexity in their IT and telecommunications infrastructure, shaped by years of technological evolution. This complexity presents a significant challenge amid the industry's digital transformation, requiring specialized approaches to modernizing and integrating various systems.

One of the key challenges is the simultaneous coexistence of legacy systems and modern digital solutions. Many industrial facilities continue to use process control systems developed decades ago, which, despite their obsolescence, remain critical to the continuity of production processes.

These systems often run on legacy hardware and operating systems, which creates significant challenges when integrating them with modern IoT platforms and cloud services.

However, complete replacement of such systems is often impossible due to the need for a continuous production cycle, which forces the search for compromise solutions in the form of intermediate software layers and specialized gateways.

Along with the need to ensure the reliable operation of the IT infrastructure, oilfield service companies have an obligation to comply with the requirements of Federal Law 187 "On Critical Information Infrastructure", since they are subjects of this federal law.

Thus, when ensuring the information security of oilfield service companies, a complex task arises: on the one hand, ensuring the reliable functioning of the IT infrastructure, the uninterrupted operation of services and communications, on the other hand, fulfilling the requirements of legislation on critical information infrastructure. Both of these tasks must

be carried out under conditions of limited financial, technical and human resources.

To solve the described problems, it seems rational to apply an approach to assessing and calculating the risks of negative consequences and, as a result, prioritizing protection measures, as well as automating labor-intensive document management processes associated with the implementation of the requirements of Federal Law 187 "On Critical Information Infrastructure."

## **2 APPLICATION OF METHODS FOR STUDYING STABILITY COEFFICIENTS IN PLANNING INFORMATION SECURITY MEASURES**

Modern approaches to assessing the sustainability of oil and gas infrastructure are undergoing a significant transformation, requiring the development of specialized metrics that take into account the unique characteristics of the industry.

Traditional vulnerability and risk assessment methods used in corporate IT systems are not effective enough for complex industrial environments, leading to the need to modify existing ones and create new resilience indicators.

In the work of Krasnov A.E. and co-authors, a concept of sustainability of critical information infrastructures is proposed, which can be effectively applied in the oilfield services industry after the following modifications.

The introduction of industry-specific importance coefficients for various asset categories is particularly important. Unlike traditional approaches, where resource criticality is assessed primarily based on stored data, the oil and gas sector uses a multidimensional assessment system that takes into account the technological significance of equipment, its impact on the production chain, environmental risks, and the economic consequences of downtime.

For each type of asset – from wellhead pressure sensors to central control systems – specialized weighting factors are developed to reflect their role in ensuring the continuity of production processes c.

These coefficients are regularly revised to take into account changes in technological schemes and the emergence of new types of cyber threats specific to critical infrastructure ( Krasnov , Sidorov , 2023 ).

Taking into account incident response time parameters is becoming a key aspect in assessing the resilience of industrial systems. In the oil and gas industry, where many processes require immediate response, traditional threat detection and response time metrics (MTTD and MTTR) are supplemented by Mean Time to Impact (MTTI) metrics. Time To Impact ) d( **Table 1**) with implementations.

Table 1: Key data sources ( Smith , 2023 ).

Indicator	Standard/Source	Example value for oil and gas
MTTD	NIST SP 800-61 Rev. 2	<15 min for SCADA
MTTR	API TR 1173	<4 hours for sensors
MTTI	Dragos Report 2023	<30 min for pipelines

Differentiated timeframes are being developed for various types of incidents—from cyberattacks on control systems to physical damage to equipment. Particular attention is paid to cascading effects, where a delay in responding to one incident can lead to a series of subsequent failures. For critical systems, strict recovery time standards are being introduced, taking into account both technological limitations and industrial safety requirements.

Adapting risk calculation formulas to the specifics of technological processes requires a deep understanding of the production characteristics of the oil and gas industry. Traditional risk assessment models are supplemented by factors specific to industrial environments: the likelihood of failure of obsolete equipment, the risk of unintentional personnel intervention, and the specifics of working in extreme climatic conditions.

Table 2: Risks and measures to counter the influence of the human factor in solving information security problems of oilfield service companies.

Threat type	Scenario	Protective measures
<b>Personnel errors</b>	Accidental shutdown of critical systems or incorrect settings	- Mandatory training - Automated configuration checks
<b>Insider threats</b>	Intentional data transfer or sabotage by employees	- Access control (RBAC) - Action monitoring (UEBA systems)

<b>Social engineering</b>	Phishing , pretexting to obtain credentials	- Multi-factor authentication (MFA) - Regular tests
---------------------------	---	--

Thus, *the adapted critical information infrastructure resilience model* represents an effective tool for building an information security system for oilfield service companies in the context of digital transformation, allowing for a comprehensive consideration of industry specifics and modern cyber threats .

### 3 AUTOMATION OF DOCUMENT FLOW WITHIN THE FRAMEWORK OF THE REQUIREMENTS OF FEDERAL LAW 187 "ON CRITICAL INFORMATION INFRASTRUCTURE"

The work of information security (IS) specialists requires special attention and a responsible approach to a range of problems arising from the various characteristics of technological processes and production, including those at oilfield service companies.

Various tools are used to automate the process of searching and analyzing regulatory documents by information security specialists and to support management decision-making. The most promising and comprehensive approach is the use of expert information and analytical systems (EIAS).

An expert information and analytical system for decision-making in the field of information security was created to automate work with legislative and regulatory frameworks in the field of information security. Thanks to its extensive functionality, it enables employees to conduct a variety of work with relevant documents. The system provides managers and employees with a convenient and effective tool for searching and analyzing documents defining information security requirements for decision-making in emerging situations.

In addition, the system includes a database of prepared expert recommendations, instructions, supporting documents, and templates in accordance

with the standard procedure being solved at the enterprise.

The EIAS uses various methods and algorithms to analyze information security documents, including user query recognition, keyword and phrase analysis, and determination of compliance with regulatory requirements ( Krasnov , 2023 ). This significantly reduces the time and effort required to search and analyze information security documents.

The developed system can be characterized as an expert information-analytical system (EIAS), since it is not limited by information-analytical technologies, but has limitations in terms of expert system technologies:

It does not use an explanation mechanism; production technologies are used in the inference;

Does not use calculus and propositional logic.

Uses static data entered by the user.

Moreover, the products are based not on a formal chain of conclusions, but on rules determined by experts, i.e., the hidden logic of their conclusions based on knowledge of situations, which additionally classifies the system as static, since changes in the process of solving standard procedures are not expected.

The developed EIAS "Themis" ( Krasnov , Lyscev , CHekanov , 2024 ) combines several tools in the field of information security:

1. Reference systems such as ConsultantPlus , Garant, and others are among the most widely known

and actively used tools of this type. They allow for precise searches for necessary information based on an updated database and provide a wide range of documents.

2. Document lists, such as the "Handbook of Russian Federation Legislation in the Field of Information Security," provide practical, comprehensive, and up-to-date information. They help navigate regulatory documents in a cataloging format.

3. A map of legislation in the field of information security, reflecting the hierarchy of laws and regulations , which helps to easily find connections between them

However, the listed tools are not without their shortcomings, and the developed EIAS allows for a comprehensive approach to identifying and resolving information security situations at enterprises using a knowledge base of experts.

The developed system has a number of structural components:

Database (DB) (legislative and regulatory documents of the Russian Federation);

Knowledge base (expert solutions);

Inference machine ( Rodichev , 2023 );

System interface.

The interaction of the elements is shown in the diagram:

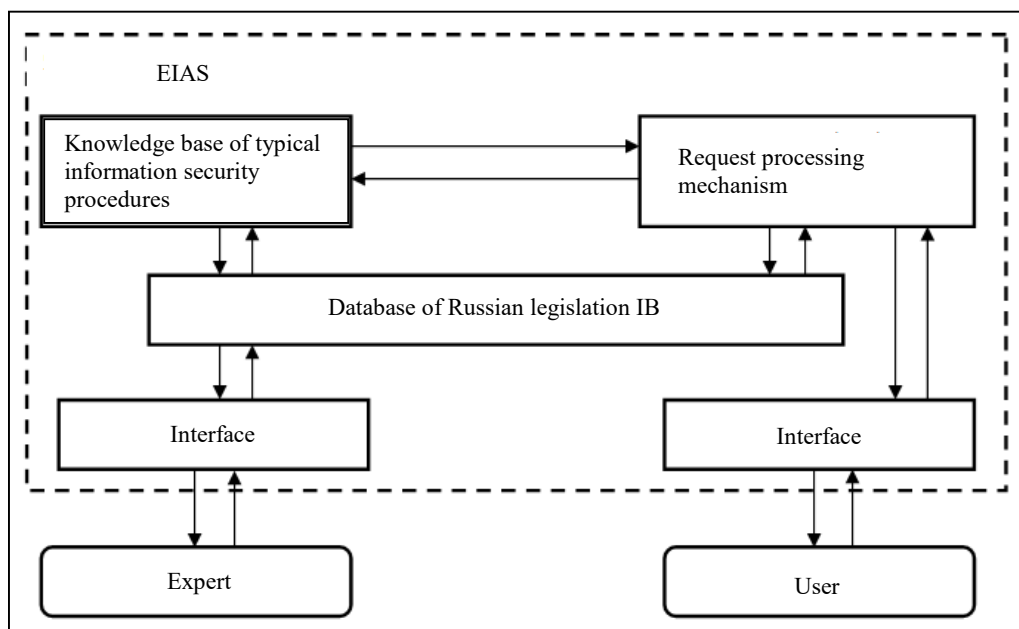


Figure 1: Schematic diagram of the EIAS elements.

The expert and user interact with system elements through an interface. The expert participates in the preparation, structuring, and systematization of the EIAS database and knowledge base.

System structure:

The structure of the expert information and analytical system is based on the regulatory acts of the Russian Federation, which govern information security in various areas.

1. "Information":
  - 1.1. Restricted access information;
  - 1.2. Publicly available information;
  - 1.3. Information to which access cannot be restricted;
2. "Information Security":
  - 2.1 Physical protection;
  - 2.2. Hardware protection;
  - 2.3. Software protection;
  - 2.4. Organizational protection;
  - 2.5. Psychological protection;
  - 2.6. Legal protection;
3. "Audit":
  - 3.1. Certification of hardware and software systems;
  - 3.2. Internal audit;
  - 3.3. External audit;

4. "Control":
  - 4.1. Access control;
  - 4.2. Network control;
  - 4.3. Control of policies and procedures;
  - 4.4 Event control;
  - 4.5. Information security control;
5. "Management":
  - 5.1 Risk management;
  - 5.2. Security program management;
  - 5.3. Resource management;
  - 5.4. Personnel management;
  - 5.5. Incident Management;
6. "Threats":
  - 6.1 Threat Model;
  - 6.2. Intruder model;
  - 6.3 Malicious software;
  - 6.4 Network attacks.

Structuring and presenting groups allows users to focus on general concepts in the field of information security and find the required Russian Federation documents.

The relationship between groups and subgroups of the implemented EIAS database is determined by the identified semantic relationships of its documents and is presented as follows:

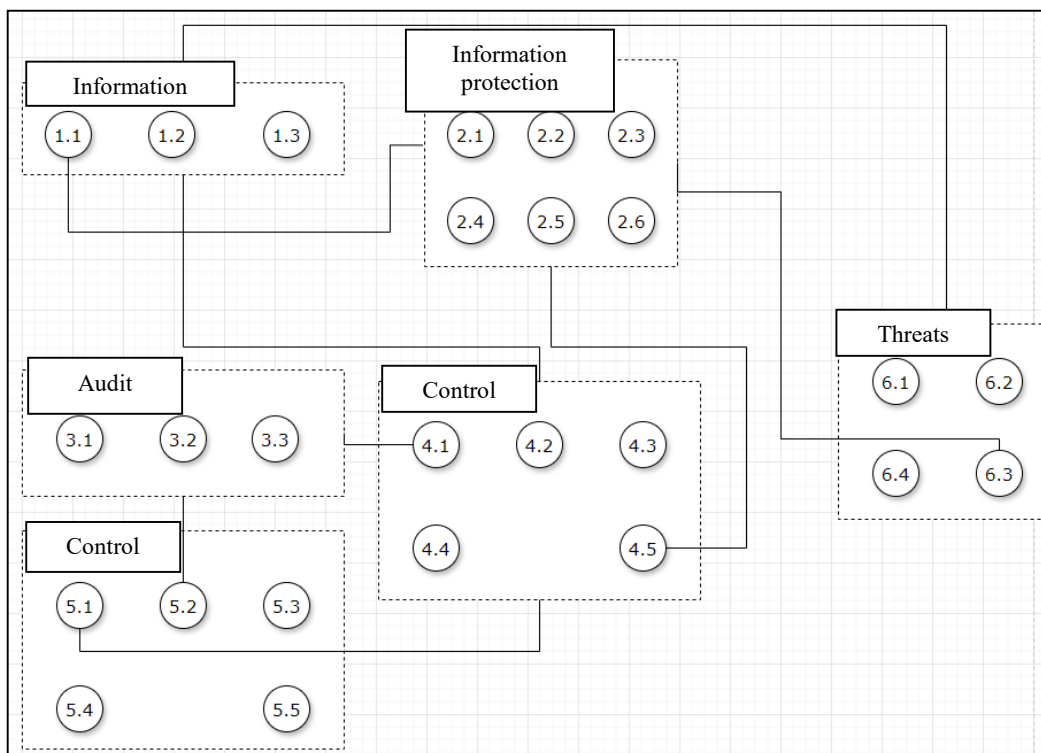


Figure 2: Database structure.

1. The Information group is associated with:  
"Information Security";  
"Control";  
"Threats."
2. The "Information Security" group is associated with:  
"Information" ( sub-block "Restricted access information");  
"Control" ( sub-block "Information security control");  
"Threats" ( sub-block "Malware").
3. The Audit group is associated with:  
"Control" ( subblock "Access control");  
"Management" ( sub-block "Security Program Management").
4. The Control group is associated with:  
"Information Security" ( sub-block "Information Security Control");  
"Management" ( sub-block "Risk Management").
5. The Management group is associated with:  
"Control" ( sub-block "Risk management").
6. The "Threats" group is associated with:  
"Information Security" ( sub-block "Malware").

The presented structure allows us to reflect a holistic picture of the interrelations of groups and subgroups of identified areas in the field of information security.

## 4 ARCHITECTURE OF EIAS

The architecture of an expert information-analytical system based on a database is a set of relational tables interconnected by keys:

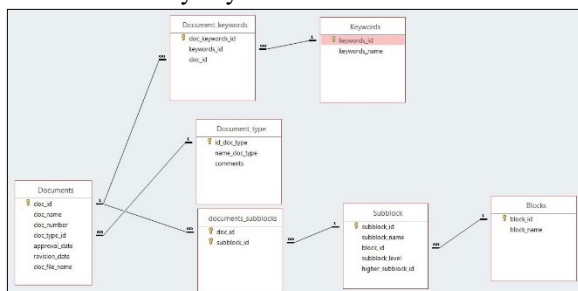


Figure 3: Architecture of the EIAS database.

The schema includes the " Keywords " table, which contains keywords (semantic components), and the " Document\_type " table, which specifies the type of regulatory document. The " Blocks ," " Subblocks ," and " documents\_subblocks " tables describe the document groups and subgroups represented by the database structure.

The structure of the EIAS can be modified and expanded, while the architecture remains unchanged. This feature allows the EIAS to be characterized as invariant and applicable in various fields.

## 5 FEATURES OF THE WORK OF OILFIELD SERVICE COMPANIES

An oilfield services company (OFS) is a company that provides various services and equipment for the extraction, production, and transportation of oil and gas. These services may include well drilling and repair, construction and maintenance of oil and gas fields, geophysical surveys, equipment and materials procurement, technical support, and other related services. Oilfield services companies are a vital component of the oil and gas industry, providing the necessary resources and expertise for the efficient operation of this sector.

Oil and gas services are a means of ensuring a country's energy and environmental security. For example, in the United States and China, primarily national companies are permitted to perform this type of work. This is due to the strategic importance for national security of the information obtained through these services regarding the status and prospects of the country's mineral resources (results of geological exploration, seismic surveys, drilling, and geophysical well logging onshore and offshore). These services ensure the required level of oil and gas production and transportation (field development design and construction, well repair, field automation, enhanced oil recovery , pipelines, offshore platform construction, etc.) and serve as the informational foundation for environmental safety onshore, offshore, and in the subsoil during oil and gas production.

The main areas of oil services are drilling, hydraulic fracturing , routine and major well repairs, and geological exploration.

The data presented demonstrates that oilfield services are a critically important, independent segment of the oil industry, ensuring the required level of oil and gas production. Furthermore, due to their technological advancement, high degree of mechanization, and automation, oilfield services are critical information infrastructure. Given this, studying the specifics of information security at oilfield services companies has significant scientific and practical potential.

Working conditions at oilfield service companies are characterized by continuous work, a high degree of mechanization, and automation. Work is carried out in isolated, developed areas—fields, typically located at considerable distances from populated areas.

The above factors lead to enterprises using shift work and maintaining a large staff.

Vertically integrated oil companies have established a rigorous pass control system at their oil fields, and therefore maintain a continuous document flow between them and oilfield service companies for obtaining passes. Furthermore, in addition to their own employees, oilfield service companies are responsible for preparing permit documents for subcontractors.

Internal local documents of oil companies and federal legislation requirements establish strict requirements for personnel training, health status, and the frequency of medical examinations.

These factors demonstrate the particular importance of protecting personal data for oilfield service companies.

The statistics provided reflect that the oilfield services market is highly competitive, which is why two important areas are emerging in the information security segment.

First, protecting commercial information. Competing companies take different approaches to organizing production, using financial instruments, and optimizing costs. This information is critical to the company and must be protected.

Second, ensuring the uninterrupted operation of communication channels and software. Oilfield service companies are highly mobile, regularly relocating to new projects and locations, which requires the establishment of remote offices and projects. Furthermore, oilfield services are characterized by high technology, advanced automation, and the extensive use of various software.

Oilfield service companies are included in the list of enterprises defined by Federal Law No. 187 of July 26, 2017, "On Critical Information Infrastructure." Therefore, additional information security requirements are established. Compliance with federal legislation requires ongoing information gathering on the introduction of new fixed assets into production, regular categorization of facilities, threat assessment, threat modeling, and planning of mitigation measures and methods. Furthermore, this area requires ongoing collaboration with government agencies, such as the Federal Service for Technical

and Export Control (FSTEC) and the National Center for Cyber Security (NCCI).

The listed areas of information security are fundamental, but not exhaustive. All of them require administrative regulation and oversight, as well as the accumulation and processing of large amounts of information.

Thus, oilfield service companies are demanding of the following list of information blocks:

1. Federal Legislative Framework. Currently, the Russian Federation has adopted and enforced numerous laws and regulations that, in one way or another, regulate information security issues. This section may also include industry-specific legislation for a specific enterprise that addresses information security issues. Important regulatory acts include, for example, Federal Law No. 149-FZ of July 27, 2006, "On Information, Information Technology, and Information Protection" and Federal Law No. 187-FZ of July 26, 2017, "On the Security of the Critical Information Infrastructure of the Russian Federation."

2. Local company regulations governing information security: policies, procedures, instructions, and orders. This section may also include local regulatory documents on information security for vertically integrated oil companies, which are typically appendices to service contracts.

3. Critical information infrastructure. As noted above, oilfield service companies, according to their OKVED classification, are considered critical information infrastructure. This, in accordance with Federal Law No. 187 of July 26, 2017, "On Critical Information Infrastructure," requires a number of activities. These include the establishment and operation of standing categorization committees, categorization of fixed assets, correspondence and interaction with authorized government agencies (the Ministry of Energy of the Russian Federation, the Federal Security Service of the Russian Federation, and the Federal Service for Technical and Export Control), threat assessment, model development, etc.

4. Personal data protection. Personal data protection issues are regulated by Federal Law No. 152 of July 27, 2006, "On Personal Data."

5. Protection of commercial information. Provided in accordance with Federal Law No. 98 of July 29, 2004, "On Commercial Secrets."

6. IT infrastructure protection, including ongoing security assessment, anti-virus policy, implementation of NCCI recommendations, availability of updates, etc. Compliance with the recommendations of the Federal Standard GOST R ISO/IEC 27001-2021 "Information technology.

Methods and means of ensuring information security. Information security management systems. Requirements" ( Rodichev , 2023 ) is important here.

Because many information security documents must be developed and approved in accordance with federal laws and standards, automating the work of document development specialists remains a pressing issue.

In these circumstances, the practical question arises of how to store, exchange, accumulate statistics, process, and make accessible to oilfield service company employees in these information blocks. What technologies and tools should be used to ensure reliable information storage, systematization, and transmission, as well as development in the face of staff turnover?

## **6 ADAPTATION OF THE DEVELOPED INTELLIGENT SYSTEM TO THE ACTIVITIES OF INFORMATION SECURITY SPECIALISTS AT OILFIELD SERVICE ENTERPRISES**

An analysis of the needs of oilfield service companies highlighted important aspects of specialists' work with information security regulations. The database developed by the EIAS includes these regulations and enables navigation and analysis in this area. However,

according to the stated objectives, there is no solution for automating document preparation.

This requires the inclusion of an additional automated document generation module in the developed EIAS. This module will allow experts to generate templates in accordance with Russian legislation for subsequent automated processing and storage of received documents by EIAS users.

The algorithm for the automated document generation module is presented as follows:

The user fills out a form with the organization's data;

The entered data is substituted into the corresponding places in the document using a simple replacement algorithm;

The user has the opportunity to save a set of prepared documents in accordance with the entered data, provided that the required fields are fully filled in.

A specific feature of the implementation is that experts need to prepare template forms with the .doc extension in advance and designate the locations for the user-entered data.

Data can be static, such as the organization's name, the manager's full name, etc., or dynamic, such as time stamps or the document's preparation date. Furthermore, data can be simple or complex, allowing for multiple values to be specified, generating tables in the resulting document.

The new general structure of the EIAS is as follows:

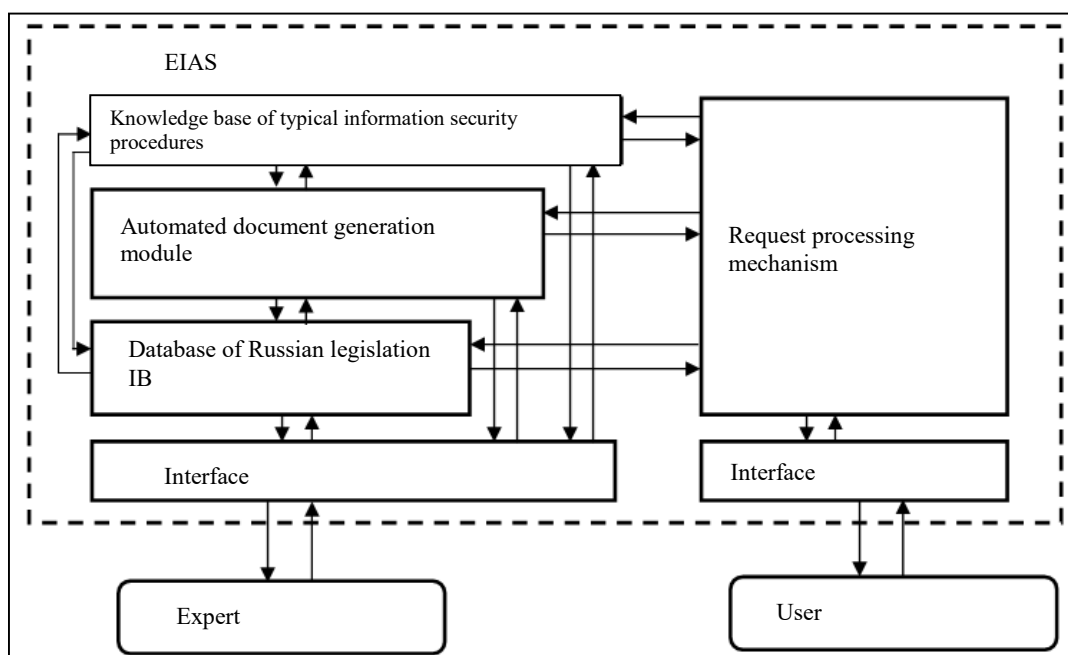


Figure 4: Modified structure of the EIAS.

Thus, an important additional component of the EIAS for adaptation to oilfield service companies is the automated document generation module. This new functionality enables automated generation of necessary documents and management of information security processes at the enterprise (Krasnovu, Chekanov, Lyscev, 2024).

This study examined the problems of ensuring information security at oilfield service enterprises and proposed an approach to adapting the developed expert information and analytical system for enterprises in this area.

An analysis of existing tools for information security specialists revealed the need to use an integrated approach, as implemented in the developed EIAS.

An analysis of the activities of oilfield service companies revealed a high volume of confidential information and a complex set of tasks determined by the specifics of technological processes and production and regulated by Russian Federation legislation.

Additionally, the work identifies priority areas of activity for information security specialists at oilfield service companies, such as ensuring compliance with Russian legislation, protecting confidential data, developing local regulatory documents, and others.

To adapt the EIAS to the operations of oilfield service companies, it is proposed to supplement it with a module for automated document generation in accordance with Russian legislation and industry specifics. This will improve the efficiency of information security specialists, minimize human error in document preparation, and ensure compliance with regulatory requirements.

Thus, the results of the conducted study demonstrate the relevance and practical significance of the application of the developed EIAS for oilfield service enterprises in order to improve the level of information security and determine the directions for the development of similar systems for enterprises of any profile.

## REFERENCES

- Internet publication "Neftegaz.RU". "Rol' i appointment oil and gas service ." [https://neftegaz.ru/analysis/oil\\_gas/329673-rol-i-naznachenie-neftegazovogo-servisa/?ysclid=lo4cqtilfq226323446](https://neftegaz.ru/analysis/oil_gas/329673-rol-i-naznachenie-neftegazovogo-servisa/?ysclid=lo4cqtilfq226323446)
- Informational service « Consultant plyus » [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_48699/](https://www.consultant.ru/document/cons_doc_LAW_48699/)

- Krasnov , AV, Sidorov , KL, 2023. Cyberphysical industrial safety objects of the TEK. Publisher : " Nedra ", 412 p. Chapter 4. Dynamic correction coefficients criticality (pp. 178–210).
- Smith, J., 2023. Real-Time Incident Response Metrics for ICS. *ZHurnal : IEEE Transactions on Industrial Cybersecurity*, Vol. 1(2), pp. 89–102.
- GOST R 58404-2023. Methods ocenki cyber resilience TEK objects . Section : 6.4 Normativy time recovery for critical sistem (s. 78–85). Tablica : Differentiated temporary frames for tips incidents ( Appendix V). Regime access : <https://techexpert.ru/document/721048664> (data obrashcheniya 30.06.2025).
- Krasnov , AE, 2023. Automation support acceptance managerial solutions in the region informational security na basis technologies expert system. *Information education i science* . No. 2(58). P. 81-89.
- Krasnov , AE, Lyscev , KS, Chekanov , IR, 2024. "To the question ob automation processa provision informational security oil service enterprises . Potential , areas application .» , « Modern science : current problems theories i practices . Series " Natural and technical sciences », No. 5 .  
Informational service « Consultant plyus » [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_48699/](https://www.consultant.ru/document/cons_doc_LAW_48699/)
- Rodichev , YU.A., 2023. « Information bezopansot !. Nacional'nye standards Russian Federation ". Publishing house " Piter " St. Petersburg.
- Krasnovu , AE, Chekanov , IR, Lyscev , KS, 2024. « Adaptaciya expert informational and analytical systems support acceptance solutions in the region informational security for oil service enterprises » « Modern science : current problems theories i practices . Series « Natural i technical sciences », No. 8.