Developing a procedure for conducting a security audit of a software package for predicting storage system failures

Marina Bolsunovskaya[1], *Svetlana* Shirokova[2], *Aleksandra* Loginova[1,*], and *Mikhail* Uspenskij[3]

[1]Institute of Computer Science and Technology, Peter the Great St. Petersburg Polytechnic University, 195251, Polytechnicheskaya Street, 29, St. Petersburg, Russian Federation
[2]Institute of Industrial Management, Economics and Trade, Peter the Great St. Petersburg Polytechnic University, 195251, Polytechnicheskaya Street, 29, St. Petersburg, Russian Federation
[3]Scientific-research laboratory "Algorithms and systems for stream data processing", Peter the Great St. Petersburg Polytechnic University, Polytechnicheskaya Street, 29, St. Petersburg, Russian Federation

Abstract. The aim of the work is to develop a procedure for conducting an information security audit of the software system for predicting data storage failures in order to identify existing threats to information security, evaluate information security tools, and improve the efficiency of existing information security tools and introduce new ones. It is necessary to monitor the current situation to ensure information security in organizations where data storage systems are used. For this purpose, an audit system has been developed, including both organizational measures and software and hardware parts.

1 Introduction

To ensure fault tolerance of data storage systems (DSS), software systems for predicting DSS failures are used. Such systems provide the ability to perform diagnosis and prediction of the state of storage and storage components in real time.

The software package operates within the storage system on the base of the integration of management servers into a single cluster. To determine the state of a data storage system, the software package uses a set of parameters fixed by monitoring modules independently on each node of the cluster [1, 2].

At the moment, the task of ensuring information security in the operation of data storage systems at the disposal of individual nodes of the cluster is solved by maintaining a quorum using a scheme that provides data replication between all nodes of the cluster. Each of these nodes runs a separate instance of the monitoring software package. If one node is lost, others will not be able to get monitoring data from it, then the overall system state will not be

*Corresponding author: alexandra-lo@yandex.ru

complete. To eliminate uncertainty perhaps in the case when the lost node will recover and again become a member of the quorum. In the case when the lost node continued working and collecting data, after restoring it in the cluster, it will update the information it has about other components of the storage and transmit information about itself [3].

Logical blocks are used to synchronize data. A logical block is an observation where all parameters have the same interval. An observation contains the timestamp of the survey and the values of the parameters observed at the same polling interval.

The peculiarity of synchronization is the presence of a dynamic number of sources equal to the number of replicated databases [4]. This dynamics is due to the fact that the storage remains operational as long as there is a quorum. For example, if a quorum of five nodes has left two nodes for some reason, full replication must take place within the remaining three nodes.

Information collected by the node about itself in time when it did not participate in the quorum is also taken into account. When this node returns to the quorum, it fills in the missing information about the available quorum nodes and provides them with the missing information about itself so that all quorum nodes have the same information. The only source of node data is the node itself.

Using the information about the configuration of a storage system, which is currently being worked on, the node "knows" which nodes surround it, and "asks" each of these nodes all observations that have emerged from the time displayed in the last available observation of the requesting node about the respondents. To minimize the time to wait for the update from the node, a notification is sent that the node has new data along with the time stamp of the new record. The notification is sent to all quorum members.

The synchronization trigger is the fact that the most frequently performed monitoring is received. After receiving the results of the most frequent observation, a message is sent to the rest of the nodes that a new observation has appeared with the appropriate time stamp. The next step is for each node that receives the notification to determine what last monitoring it has from the node that sent the notification. If the notifying node has more recent data, the missing observations are queried. The query specifies the timestamp of the last available case. The server that originally sent the data, after receiving a request to send all its observations from a specific time stamp, searches for the corresponding observations. After finding one by one, in the order of increasing the timestamp, the server sends these changes to the node that requested them.

The task of ensuring the safety of individual software monitoring modules and software complex forecasting the state of the data storage and storage components is extremely important.

2 The purpose and the objectives of the study

The aim of the study is to identify existing vulnerabilities and possible security threats to it resources and to propose appropriate countermeasures to improve the existing level of security when using the software complex predicting storage failures [5-6].

To achieve this goal, it is necessary to analyze the existing types of audit of information systems and software systems, methods of identifying threats and countermeasures, to compare tem and to make an informed choice of them for a certain project.

At the next stage it is possible to carry out the security of the software complex audit, taking into account the selected methods. It will allow to identify and analyze existing threats to information security. On the basis of the study should be formed recommendations to address existing threats to information security of the software complex forecasting failures of data storage.

There are several classifications of audit types, for example, methods and tools used in the audit, based on the auditor's affiliation to the surveyed company. Based on a detailed comparison, it was decided to focus on the method of comprehensive audit.

Comprehensive audit of information security of enterprises implies the following tasks:

Study of information systems and business processes of the enterprise (as objects of protection), formation and analysis of the model of interaction of information systems used to support business processes.

Identification of the most important components and nodes of information systems to support business processes.

Definition of requirements to the existing information, analysis of structure, functions and features of the existing information security system, analysis of standard means of protection, research of software and hardware.

Testing of the threats to information security.

Assessment of risks associated with the implementation of threats to information security.

Development of recommendations for improvement current level of information security and formulation of proposals to reduce information security risks.

3 The information security audit methodology

If we consider the software system (software complex) for predicting failures of date storage as an information system, the process of information security audit of such system would be represented by the following sequence of stages:

- initiating an audit procedure;
- gathering information for the audit;
- data analysis;
- development of recommendations and preparation of the report [7-10].

On the basis of information security standards can be defined a basic set of requirements for the security of the software product, which are divided into the following groups:

1. Physical control of access to premises and monitoring of premises.
2. Hardware of the software complex.
3. Network support of the software complex functioning.
4. System software.
5. Application software.
6. Organizational support.

In the course of analysis of existing approaches to the prevention of unauthorized physical access to the premises and information was found that it is necessary to establish means of processing of critical information in safe areas protected by certain security perimeters, with appropriate protection bariers and access control. Means of processing critical information, which includes data monitoring the state of storage, must be physically protected from unauthorized access, damage and interference. To protect against such threats, there are:

- e-passes;
- recording the date and time of entry and exit;
- restriction or limitation of access to places where relevant information is processed or stored [11, 14, 16].

Below we describe the rules of risk response in ensuring the security of the software complex forecasting data storage failures, operating in automated control mode, for example, monitoring the actions of the user.

- Current status: the system automatically logs user activity. It records the user name, log in / log out date and time, and the actions to be performed. Logs are stored for 1 month on removable media.

- Recommendations: audit logs that record user actions, unexpected events, and information security events should be kept for agreed periods to help with future investigations and access control.
- Comments and potential threats: no system of the notification about the completion of the space on the media are written to the log, currently, available space is checked manually.
- Recommendations: for convenience, it is recommended to implement a system that automatically selects those from all user action logs that can potentially pose a threat to information security (for example, copy critical monitoring data from the database) [12].

Such regulations have been worked out for all steps of planning, management, control and security of information systems. When choosing a method of risk analysis, it is necessary to take into account the characteristics of the information system [13], the environment in which it operates, the applicability of this method to the information system under consideration and other aspects [14, 15].

4 Risk assessment of the project

4.1 The procedure of risk assessment and analysis for the software complex for predicting storage failures

When conducting an audit, it is not enough to simply assess the risks, it is necessary to analyze the result and, if necessary, take appropriate measures, that is, risk response, for example.

The following steps are implemented in the course of risk assessment and analysis for the software complex for predicting storage failures:

1. Identification of key aspects that require additional measures to ensure the safety of the software complex for predicting data storage failures.
2. An analysis of some of the key aspects to be protected in the first place;
3. Formation of a set of possible threats to information security and vulnerabilities, due to which these threats can be implemented.
4. Assessment of the likelihood of security threats.
5. Assessment of the level of damage.
6. Calculation of risks (qualitatively and / or quantitatively).
7. Analysis of the results.

At the risk management stage, recommendations are made to eliminate risks-threats, reduce them or transfer responsibility to third parties [2, 4, 16].

With regard to the software complex forecasting data storage failures the risk management stage may concern:

- information resources ensuring the implementation of monitoring processes;
- system and application software;
- hardware (servers, workstations, switches, storage disks);
- premises where information is stored and processed.
- It is proposed to consider the following types of damage:
- disclosure, deletion, modification, unavailability of data;
- damage or destruction of equipment;
- violation of the integrity of the software.

It is also worth noting that the risk assessment can be performed in two stages:

- Qualitative assessment;
- Quantification.

At a qualitative assessment the levels of damage from the implementation of the attack are estimated, as well as the levels of the threat of the attack itself.

Information security risk is calculated as the probability of threats of harm caused to the company as a result of its implementations. Management then determines the level of acceptable risk and therefore acceptable and unacceptable risk. For unacceptable risks, it is necessary to perform additional actions to reduce them, for example.

In the case of quantitative risk assessment, the scale of assessment the probability of the implementation of information security threats is compared to the numeric probability values from 0 to 1, where very low probability is estimated as [0… 0.25], but very high as [0.75… 1]. The damage is expressed in money terms.

The risk itself is calculated as a product of probability implementation of the threat to information security in the amount of damage incurred [10, 14, 16].

Next the selected and justified for the project of creating software complex for predicting failures of DSS methods of risk management will be presented.

The most common of them are: risk reduction to the permitted level through the use of various technical and organizational means; taking a risk if it has an acceptable level; transfer of risks to a third party.

4.2 Identifying possible threats

Possible threats to servers and / or storage systems designed to store and process information could be as follows:

- damage or destruction by an attacker;
- refusal for technical reasons;
- the destruction of a natural disaster, for example, made by fire.

Possible threats for the software complex for predicting failures of DSS, performing data processing monitoring of a data storage, are:

- unintentional modification or deletion of information from monitoring databases and system logs;
- leakage of confidential information as a result of copying;
- destruction or damage of electronic media, resulting in data loss.

It is important to assess the likelihood of threats, assess the damage, using previously used countermeasures and make recommendations to reduce the risk.

To reduce the risks described above, the following measures may be recommended:

- the RAID technology (technology resiliency);
- important information reservation;
- conducting of the monitoring of a server room condition for determine a failure of any critical equipment.

Consider a few risks. Damage or destruction of the server and/or storage by an attacker. The probability of this is risky, but the amount of damage, if this threat is realized, will be great. To reduce the risk, the following safety measures should be taken by implementing passive and active monitoring systems: restricting access to the server room by using electronic passes; using video cameras to monitor the perimeter; hiring a security guard to monitor perimeter security.

The risk of destruction of servers and/or DSS in fire. This risk also has a critical level in terms of the cost of damage. To reduce the risk is recommended: reduce possible damage by creating backup copies of information for individual servers and / or storage; introduction of system of monitoring of the environment, including for detecting smoke and /or increasing the temperature of the air, and alarm system; introduction of fire extinguishing system (gas fire extinguishing system).

To reduce risks in case of unintentional modification or deletion of information from the monitoring database, the following measures are recommended: back up critical information for individual servers or external storage; implementation of history storage functionality database changes monitoring with the possibility of data recovery; implementation of active monitoring.

After the audit of information security on the basis of the approaches proposed by the authors [17-20] was compiled a list of recommendations. All these recommendations could be grouped as follows: recommended organizational measures; recommended software and technical measures.

4.2.1 Recommended measures of the organizational level

The recommended measures of the organizational level include:

- regular analysis of security policies;
- appointment of responsible for security of valuable software and hardware and information resources;
- inclusion in the duties of all employees of the organization-information security;
- regular dissemination of information about incidents and viruses;
- creation of a forum to discuss various issues related to information security;
- short-term training on information security for all employees of the organization;
- updating the anti-virus database every day.

4.2.2 Recommended technical measures

The recommended technical measures include:

- frequently monitor new vulnerabilities in the software;
- regularly monitor the integrity of critical data and the software that processes it;
- organizational and physical security measures for backups should be appropriate for the level of protection of these primary media;
- updating software and install security updates as often as possible;
- making documentation of user rights corresponding to the tasks assigned to them;
- regular checking of the adequacy of the rights assigned to the user;
- regular use of vulnerability scanner to track changes in software security;
- ensuring compliance of the information system with the security standard;
- using only of certified tools for local and network security.

After analyzing the data in two different ways (using a risk-based approach and an approach based on information security standards), recommendations were developed to change the information security system to improve the level of protection of storage.

It should be taken into account that in order to create an effective security system, the cost of purchasing hardware and software, their integration and maintenance of security must exceed the cost of protected information. At the same time, the use of a software complex for predicting data storage failures, in which the results of monitoring the status of individual servers and /or storage as a whole are utilized, will provide a new level of information security, including:

monitoring performance degradation of individual servers and / or the storage system as a whole;

comprehensive automatic monitoring of the technical condition of individual servers and / or data storage systems in real time for different operating modes.

5 Conclusions

In the course of this work, the following tasks has been solved:

1. The analysis of existing measures and algorithms for information security was made.
2. The review and comparison of existing types of information security audit were carried out.
3. The review of existing approaches to the analysis of information security risks was carried out.
4. Information required for information security audit was collected.
5. The obtained data were analyzed using two approaches: on the basis of information security standards and on the basis of risk analysis approach.
6. Recommendations to reduce the risks of information security threats have been developed. Implementation of the developed countermeasures to eliminate information security vulnerabilities will reduce risks and ensure the protection of important data stored in an information system, as well as prevent possible financial losses and damage to an organization as a whole.
7. The analysis software for predicting failures of storage systems with purpose to ensure a new level of information security monitoring system of storage conditions and the proper software package predict failure of the storage system.

The research is carried out with the financial support of the Ministry of Science and Higher Education of Russia Federation within the framework of the Federal Program “Research and Development in Priority Areas for the Development of the Russian Science and Technology Complex for 2014-2020”. The unique identifier is RFMEFI58117X0023.

References

1. S. V. Zapechnikov. Information counter threats of terrorism, **6-P**, 123-128 (2016)
2. A. Zakharov The basic data storage systems and their features [Osnovnye systemy khraneniya dannykh i ih osobennosti] URL: http://www.itworkroom.com/main-shd/ (2014)
3. A.V. Igumnov, S. E. Sarajishvili. St. Petersburg Polytechnic University Journal of Engineering Science and Technology Series “Informatics. Telecommunications. Management”, **2 (193)** (St. Petersburg.: Publishing house of Polytechnical Institute), 99-109 (2014)
4. V. R. Klimov. Modern problems of design, production and operation of radio systems [Sovremennye problemy proektirovaniya, proizvodstva i ekspluatacii radiotekhnicheskikh system], **1-2 (9)**, 148-150 (2015)
5. B. Zhu [et al.] *Proc. IEEE 29th Symposium on Mass Storage Systems and Technologies (MSST)*, **1–5** (2013)
6. A. Wildani [et al.] *Proc. IEEE International Symposium on Modeling, Analysis Simulation of Computer and Telecommunication Systems*, **1–11** (2009)
7. R. Wood. Journal of magnetism and magnetic materials, **321(6)**, 555–561 (2009)
8. K. Warwick, M. T. Tham. Failsafe control systems (London: Chapman & Hall) (1991)
9. Q. Xin, T.J.E. Schwarz, E.L. Miller. *Proc. 13th IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems*, **125–134** (2005)
10. A. A. Denisov. Modern problems of system analysis [Sovremennye problemy systemnogo analiza], **293** (2008)

11. V. N. Volkova, V. N. Kozlov, V. E. Mager, L. V. Chernenkaya. *Proc. Int. Conf. SCM-2017* (St. Petersburg: ETU "LETI"), 183-186 (2017)
12. V. N. Volkova, A.V. Loginova, S.V. Shirokova, E.A. Kozlovskaya. *Proc. of the 19th International Conference on Soft Computing and Measurements, SCM 2016* (Saint Petersburg Electrotechnical University (SPbETU) "LETI" 25-27 May 2016), 470-473, DOI: 10.1109/SCM.2016.75198162016 (2016)
13. A. S. Makarov, M. V. Bolsunovskaya, S. V. Shirokova, M. B. Uspenskij, A. A. Kuz'michjov. *Proc. Int. Conf. SCM-2018* (St. Petersburg: ETU "LETI"), 61-64 (2018)
14. V. N. Volkova, A. A. Denisov Methods of organization of complex examinations [Metody organizacii slozhnykh ekspertiz] (St. Petersburg: St. Petersburg Polytechnic University Publ.) (2010)
15. V. N. Volkova, Yu. Yu. Cherny. *Proc. Int. Conf. SARC-2016*, 95-108 (2016)
16. V.N. Volkova, A. A. Denisov. Systems theory and system analysis: textbook for universities (2nd edition revised and expanded) [Teoriya sistem i sistemnyj analiz] (Moscow: Yurait Publ.), **616** (2016)
17. Reed-Solomon Codes Part 1 Theory in simple language *In "Algorithms" Blog of YADRO company* URL:https://habrahabr.ru/company/yadro/blog/336286/ (2018)
18. I. Iliadis, V. Venkatesan. *Proc. The Eighth International Conference on Communication Theory, Reliability, and Quality of Service (CTRQ 2015)* (Barcelona, Spain), 6-12 (2015)
19. M. C. Kurt. *Fault-tolerant programming models and computing frameworks* (ProQuest Dissertations Publishing) (2015)
20. F. Mahdisoltani, I. Stefanovici, B. Schroeder. *Proc. 2017 USENIX Annual Technical Conference* (Santa Clara, CA), 391–402 (2017)