|  |  |
| --- | --- |
| **“AGREED”**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2022** | **“APPROVED”**  **CJSC KGC**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2022** |

Terms Of Reference

FOR Purchase of a technological process information management system (PIMS)

BISHKEK, 2022

**Content**

[1. General information 5](#_Toc104900860)

[1.1. Name 5](#_Toc104900861)

[1.2. Supplier and Contractor 5](#_Toc104900862)

[2. Basis, purpose and goals of the project 6](#_Toc104900863)

[2.1. Basis 6](#_Toc104900864)

[2.1. Purpose and objectives of the system 6](#_Toc104900865)

[3. PIMS system Requirements 7](#_Toc104900866)

[3.1. Requirements for the functionality of the software 7](#_Toc104900867)

[3.2. Non-functional software requirements 8](#_Toc104900868)

[3.2.1. Location of the data 8](#_Toc104900869)

[3.2.2. Performance requirements 8](#_Toc104900870)

[3.2.3. Requirements to integration with existing systems 8](#_Toc104900871)

[3.2.4. Requirements to the reporting system 8](#_Toc104900872)

[3.2.5. Using the mobile app on iOS or Android 9](#_Toc104900873)

[3.2.6. Modularity of applied software 9](#_Toc104900874)

[3.2.7. User Policies 9](#_Toc104900875)

[3.2.8. Usability and convenience of the user interface 9](#_Toc104900876)

[3.2.9. Interface and data language 10](#_Toc104900877)

[3.2.10. Directories module 10](#_Toc104900878)

[3.2.11. System class by recovery time and availability per year 10](#_Toc104900879)

[3.2.12. System Class by Recovery Priority 10](#_Toc104900880)

[3.2.13. Typical architectural template for Medium Speed (RC4) systems 10](#_Toc104900881)

[3.2.14. System class by support mode 13](#_Toc104900883)

[3.2.15. System documentation requirements 13](#_Toc104900884)

[3.2.16. Requirements for the role model of the system 13](#_Toc104900885)

[3.2.17. Information security requirements 14](#_Toc104900886)

3.2.17.1. Identification and authentication …………………………………………………………………..……… 14

3.2.17.2. Access control of access subjects to access objects …………………….………………………… 14

3.2.17.3. Restricting the software environment …………………………….……………………….…………… 15

3.2.17.4. Protecting machine media……………………………………………………………………………………… 15

3.2.17.5. Recording security events………………..…………………………………………………..………………..16

3.2.17.6. Antivirus protection ………………….………………………..………………………..………………………..16

3.2.17.7. Intrusion detection …………………..……………………………….………………………..……….……… 16

3.2.17.8. Control (analysis) of information security…………..………………………………………………… 16

3.2.17.9. Ensuring the integrity of information system and information………………..……..…….17

3.2.17.10. Ensuring information availability……………..…………………………….……………………………..17

3.2.16711. Protecting virtualization environment …………………………..………………………..………….18

3.2.17.12. Protection of technical equipment …………………………..…………………………………………..18

3.2.17.13. Protection of the information system, its means, communication, and data transmission systems …………………………………………………………………………………………………………………………….19

ABBREVIATIONS AND SYMBOLS

| **Terms** | **Definitions** |
| --- | --- |
| RPO | Recovery point objective - the allowable amount of possible data loss in the event of a malfunction (incident). |
| RTO | Recovery time objective - the acceptable recovery time of the information system in the event of a malfunction (incident). |
| DPC | Data processing center is a specialized designated room to host server and network equipment that ensures the smooth operation of the company's IT Systems. |
| DB | Data Backup is a consistent copy of data on removable media (hard disk,  floppy disk, etc.) designed to recovery data to its original or new location in  case of damage or destruction. |

1. General information
   1. Name

Full name– Terms of Reference for the Purchase of technological process information management system (PIMS)

* 1. Supplier and Contractor

Client: Kumtor Gold Company CJSC

Software supplier: organization selected by the Client for the software delivery under this TOR.

1. Basis, purpose, and objectives of project
   1. Basis

The basis for purchase of the PIMS system is the need for operational administration of technological processes in real time - allowing for operational data accounting, planning and management of production resources, which will increase efficiency and productivity.

* 1. Purpose and objectives of the system

The purposes of the system are as follows:

1. A single source of reliable data that combines important information and enhances the capabilities of staff to ensure flawless, continuous operation of the company.
2. Provide data to users and related systems in the required volume in time and in the most appropriate format.
3. The ability to analyze and compare events.
4. Providing all authorized users with convenient access to factory status data and key elements.
5. The ability to compress and archive data without loss of completeness and quality.
6. Protection against loss and distortion during data storage.
7. Convenient visualization of historical trends and data in real time.
8. The possibility of safe operation by improving the quality and speed of response in emergency situations.
9. PIMS system Requirements
   1. Requirements for the functionality of the software
10. Data uploading capability (tags) from the DCS (Foxboro DCS) via the OPC server.
11. 2000 tags for online browsing and archive.
12. 5 licenses for simultaneous online work of users.
13. 1 User editing license;
14. Generating various reports (in excel format, by e-mail, on personal devices)
15. An application for trends, with the ability to select tags from the database and view, compare chronology of changes for analysis and troubleshooting.
16. The ability of the system to issue emergency event histories and save them for viewing.
17. Access to the system via the web, for Guidance through mobile applications (Chrome, MS Edge, FireFox).
18. Login control - if the user has logged in and made any changes, it must be saved and tracked.
19. Provide 5 interface pages of the system (mnemonic diagram).
20. Provide training for technical staff to continue configuring and editing the interface of the pages.
21. Manual data entry option.
22. 13. Minimize integration, in case of further transition to Foxboro EVO IDE software; discuss in the process of preliminary approval with the customer.

**The tag must contain the following data:**

* Tag name
* Metadata properties (technical units, descriptions, restrictions, etc.)
* Timestamp
* Values (boolean values, floating point numbers, integers, strings, etc)
  1. Non-functional software requirements
     1. Location of the data

The SaaS/On Premise solution should be deployed in Data Centers leased or purchased by KGC.

* + 1. Performance requirements

| № | Parameter | Value |
| --- | --- | --- |
|  | The number of users using the system at the same time per unit of time | 5-10 |
|  | Number of users editing data at the same time per unit of time | 1-2 |
|  | Average response time for on-screen form navigation operations | 500 ms |
|  | Average response time for data search/filtering operations | It should not exceed 30 seconds |

* + 1. Requirements for integration with existing systems

It is necessary to be able to implement automated data exchange from any PLC, DCS, SCADA, HMI, LIMS systems for their guaranteed delivery to a single repository. It is also necessary to support the exchange of information with top-level management systems (SAP/R3, Oracle Application, Baan, etc.)

* + 1. Requirements to the reporting system

The following reporting options should be available:

1. The capability to analyze information and generate web-based reports for access to reporting information, key indicators and technological data, through modern methods of trend analysis and collection of historical information in real time.
2. The data should be generated automatically (according to a schedule, by events) and in interactive (manual) mode and provide a selection of information according to the specified parameters.
3. There should be an option to upload reports to Excel, PDF, XML, CSV without a limit on the number of rows.
4. The capability to create an electronic document file with a report, enter the document for printing and the capability to send this report by mail.
5. Viewing comparative reports (make a selection by date, by status and by other necessary filters)

3.2.5. Using the mobile app on iOS or Android

Preference is given to architectural solutions for "thin client" mobile applications on iOS, Android.

To use an application with a "thin client", only standard software must be installed on the user's workstation, which does not require subsequent maintenance.

3.2.6. Modularity of applied software

The architecture of the system should be built from the most independent modules integrated with each other through universal interfaces (APIs) and services that implement functionality and data reception/transmission.

3.2.7. User Policies

The system should provide for the display of the necessary information for each role of the authorized user in their part. The system should be able to configure user rights to change roles, access rights to certain data segments.

3.2.8. Usability and convenience of the user interface

The system interface should provide a clear, intuitive representation of the structure of the posted information, a quick and logical transition to the relevant sections of the system.

The navigation elements of the system interface should provide an unambiguous understanding of their meaning by the user and provide navigation through all sections of the system accessible to the user and display relevant information.

The user interface should be user-friendly and convenient. The system interface must take into account the context of use: where, under what circumstances, and with what devices the user will interact with the system. The interface should be adaptive, i.e., provide a high degree of usability not only on wide desktop screens, but also on portable (mobile versions of the application on iOS and Android), tablet and web devices (Mac OS, Android, Linux, Windows). The system interface, including graphs and diagrams, must adapt to the screen resolution.

Interface elements (menu items, buttons, input fields in forms, drop-down lists, etc.) must adapt in size to the device on which the system is viewed and to the main use case of this device.

It should also have hints and pointers to functional components. The system designed for data processing must have manual and automatic data processing functions, such as copying, duplication, import/export in Excel, PDF, XML, CSV formats. The data should be output using extensive graphical and functional capabilities that provide users with the functions of interaction, monitoring, analysis and management of production processes. If an error or failure occurs, the software should issue an appropriate information message/notification that is understandable to the user.

3.2.9. Interface and data language

The system must support the display of the interface in Russian and English. When logging in, it should display an option to select a language suitable for the user.

3.2.10. Directories module

The system must have a separate module or modes for editing the system directory. The directory editing module/mode should be able to add new directories, if necessary, without interfering or involving additional development at the code level.

* + 1. System class by recovery time and availability per year

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Fault tolerance Template Code | The name of the fault tolerance template | | Description of the template | The System class code using this template | Regulated % of System availability per year (SLA) | Max. allowable system downtime per year | \*Restore in case of a local  system failure | | | \*Restore in case of a fall of the main DPC | | | | The number of necessary sets of equipment to ensure the declared fault tolerance | | | |
|  | | |  | | | |
| RTO | RPO | | RTO | | RPO | |
| <RC 4> | Medium Speed | Systems whose unavailability affects the inability to generate income in the long term, or significantly affects the efficiency of a large number of employees of the company | | | | BO | 99,5% | | up to 1d 19h 50 m | | 1-12h | | 1-12h | | up to 5 days | Up to 24 hours | Two sets of servers and one storage in the main DPC |

* + 1. System Class by Recovery Priority

|  |  |  |
| --- | --- | --- |
| **System Class Code** | **The name of the System class** | **Description of classifiers** |
| BO | Business Operational | Systems whose unavailability affects the inability to generate income in the long term, or significantly affects the efficiency of a large number of KGC employees. In other words, these are systems that support various operations of the KGC company. The unavailability of these Systems for 1 day does not lead to significant financial losses. |

* + 1. Typical architectural template for Medium Speed (RC4) systems

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Fault tolerance Template Code** | **The name of the fault tolerance template** | **Description of the template** | **Recovery in case of a local system failure** | | **Recovery in case of a fall of the main DPC** | |
| **RTO** | **RPO** | **RTO** | **RPO** |
| RC4 | Mean speed | Systems whose unavailability affects the inability to generate income in the long term, or significantly affects the efficiency of a large number of employees of the company | 1-12h | 1-12h | Up to 5days | Up to 24h |

RC4 class systems are **BO (Business Operational)** systems in terms of recovery priority, and **HA (High Availability)** systems in terms of failure handling type.

# TECHNOLOGICAL SOLUTION FOR RC4 IT SYSTEMS:

To protect data from loss and logical distortion, a strategy of DB and recovery from tapes and/or disks will be applied. At the same time, it will be necessary to perform a full DB on a magnetic tape weekly and perform an incremental DB every day (and not just archive backup copies of the log) on a tape.

The following data backup technologies can be used:

1. DB over LAN or SAN network.
2. DB of data to disk memory.
3. DB for tapes.

RC4 Class System Recovery Diagram (Medium Speed)



**The main DPC**

The Active system

**PACK ARD**

Standby System

**PACK ARD**

SD

SD

POWERED

POWERED

Tape Library

**HE WLE TT**

**PA CK AR D**

**H EWLE TT**

**PA CK AR D**

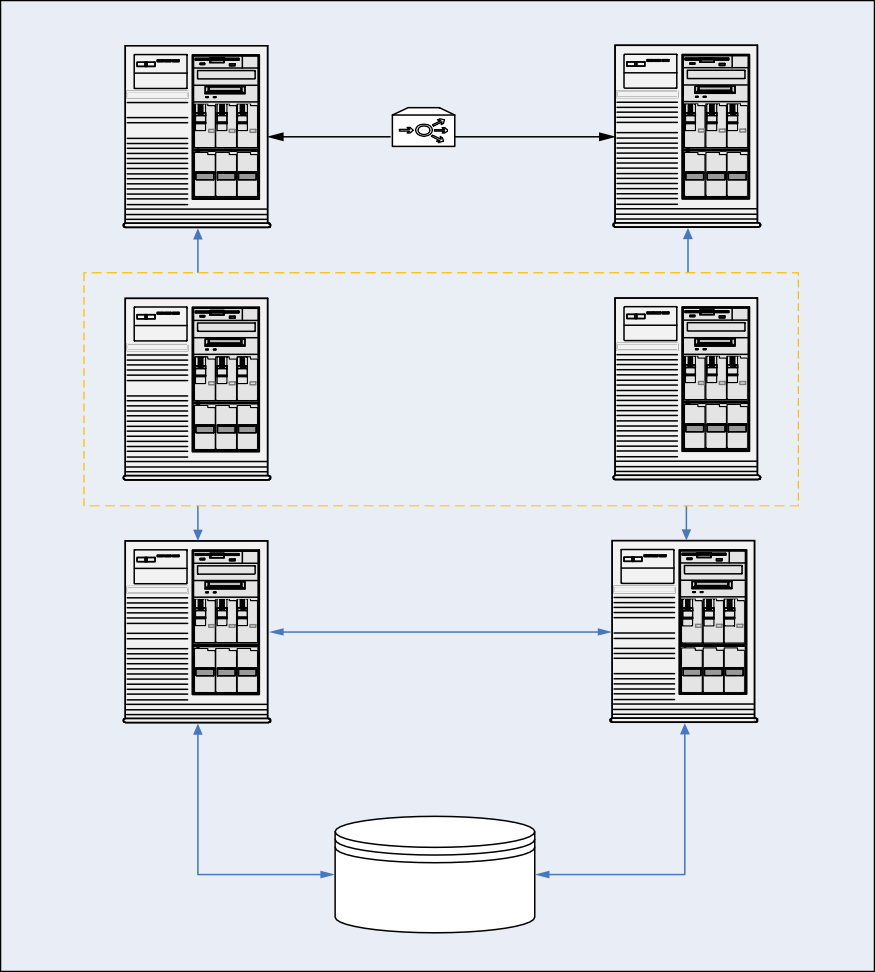
Storage

The following requirements must be taken into account for RC4 class systems:

1. 1) at least once a week, a complete DB should be performed, and at least once a day, an incremental DB should be performed.
2. The DB should be carried out on a local media server on the local network.
3. the backup image must exist in at least two copies.
4. it is necessary to test the recovery of these Systems, according to the approved and signed DB test plan.
5. allocation of a single network connection used for DB purposes for application servers >2 Tb (for physical servers).
6. The use of "clustering" technology is possible.
7. they can use SAN-connected disk drives of 2-3 levels (more likely, internal hard drives).
8. the server and network equipment are located within the same data DPC.
9. mandatory use of the Web balancer in the HA diagram.
10. a valid contract (technical support) is required for software and hardware maintenance by the Software/hardware Vendor (response time is 24 hours or less).

**Reservation within the main DPC:**

**High Availability**



Main DPC

Web

Server №1

Web

Server №2

Web-balancer

Clustering

Application

Server №1

Application Server №2

Database

Server №1

Active\Active or Active\ Standby

Database Server №2

Storage

Automatic switching/ Manual switching

* + 1. System class by support mode

|  |  |  |
| --- | --- | --- |
| **Code** | **Name** | **Description** |
| S11x7 | S11x7 | An IT system supported by IT in the mode of 11 hours a day and 7 days a week. |

* + 1. System documentation requirements

Based on the results of the project, the Contractor must develop, coordinate and transfer the following documents to the Customer:

* • Terms of reference (functional and non-functional requirements with a description of services for integration with other systems)
* • Description of the most frequently used rules for processing external correspondence - external and internal (best practice), possibly using a hardware and software package. A possible plan for the regulatory part of external correspondence.
* • Specification (Composition and description of the program. Information about the logical structure and operation of the program. Technical architecture. Description of the application: Information about the purpose of the program, the scope of application, the methods used, the class of tasks to be solved, restrictions for use). Solution architecture (logical structure of the application, broken down into modules; functional architecture; database structure and scheme; application integration scenario; scheme of system deployments in a fault-tolerant architecture, broken down by environments-development, test, preprod, prod).
* Sizing on system hardware, by media breakdown (processing, test, teacher, prod).
* The test program and methodology (the object of the tests; the purpose of the tests; requirements for the program; requirements for software documentation; the composition and procedure of tests indicating the technical and software tools used during the tests, as well as the procedure for conducting tests; test methods indicating the results of the tests (lists of test examples)).
* Testing protocols (unit, integration, performance, stress tests, vulnerability tests).
* Developer's Guide (Information for checking, ensuring the functioning and configuration of the program, API library of classes and functions with a description of signatures, semantics of functions).
* System Administration requirements (Installation, version updates, etc.)
* Application Administrator's Guide.
* User's Guide.
  + 1. Requirements for the role model of the system

During the implementation of the project, the CRUD matrix (Create, Read, Update, Delete) should be implemented in the system. During the implementation of the system, roles, actions and accesses will be reviewed.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Activity  Role | Creation of directories, configuration of business processes | Resolution Approval | Execution | Control | Reporting |
| Chief |  | RU | R | R | R |
| Secretary |  |  | CRU |  | CRU |
| Performer |  |  | U |  | R |
| Controller |  | R | R | RU | R |
| Administrator | CRU |  |  |  |  |
| Information Security Officer |  | CRU |  |  |  |

* + 1. Information security requirements
       1. Identification and authentication

Identification and authentication of access subjects and access objects through integration with Active Directory.

Identity management, including the creation, assignment, and deleting of identifiers.

Managing authentication tools, including storing, issuing, initializing, blocking authentication tools, and taking action in case of loss and/or compromise of authentication tools.

Protection of feedback when entering authentication information (Process of exchange and confirmation of authentication codes, confirmation of authorization by the reverse side) for external counterparties.

Identification and authentication of file system objects, launched and executable modules, objects of database management systems, objects created by application and special software, and other access objects.

* + - 1. Access control of access subjects to access objects

Management (establishment, activation, blocking and deleting) of user accounts, including external users.

Implement the required methods (discretionary, mandatory, role-based, or otherwise), types (read, write, execute, or other type), and access control rules.

Control (filtering (limitation of the data set), routing, connection control, unidirectional transmission and other methods of management) of information flows between devices, segments of the information system, as well as between information systems.

Separation of powers (roles) of users, administrators and persons ensuring the functioning of the information system.

Assignment of minimum necessary rights and privileges to users, administrators and persons ensuring the functioning of the information system.

Limitation of unsuccessful attempts to enter the information system (access to the information system).

Warning the user when he logs in to the information system that information protection measures have been implemented in the information system, and about the need to comply with the rules of information processing established by the operator.

Limiting the number of concurrent access sessions for each user account of the information system.

Blocking the session of access to the information system after the specified time of inactivity (inaction) of the user or at his request.

Maintaining and preserving security attributes (security labels) associated with information during its storage and processing.

Implementation of secure remote access of access subjects to access objects through external information and telecommunication networks.

Regulation and control of the use of wireless access technologies in the information system.

Management of interaction with information systems of third-party organizations (external information systems).

Provision of trusted boot of computer equipment.

* + - 1. Restricting the software environment

Launch (access) management of software components, including the definition of the components to be launched, the configuration of component launch parameters, and the control over the launch of software components.

Management of the installation of software components, including the definition of components to be installed, configuration of component installation parameters, control over the installation of software components.

Installation of only authorized software and (or) its components.

Manage temporary files, including hold, allow, redirect writes, delete temporary files.

* + - 1. Protecting machine media

Accounting of computer data carriers.

Control of access to computer data carriers.

Control of the movement of computer data carriers outside the controlled area (if necessary).

Exclusion of the possibility of unauthorized familiarization with the content of information stored on computer carriers, and (or) the use of information carriers in other information systems.

Control of the use of interfaces for input (output) of information on computer data carriers. Control of input (output) of information to computer data carriers.

Control of the connection of computer data carriers.

Deleting (erasure) of information on computer media when they are transferred between users, to third-party organizations for repair or disposal, as well as control of deleting (erasure).

* + - 1. Recording security events

Define the security events to be logged and how long they should be retained.

Determination of the composition and content of information on security events to be recorded.

Collecting, recording, and storing information about security events for a set retention time.

Responding to failures in the registration of security events, including hardware and software errors, failures in information collection mechanisms, and reaching the limit or overflow of memory capacity.

Monitoring (viewing, analyzing) the results of security event registration and responding to them.

Generation of timestamps and/or synchronization of system time in the information system.

Protection of information about security events.

Providing the ability to view and analyze information about the actions of individual users in the information system.

* + - 1. Antivirus protection

Implement antivirus protection or integrate with existing protection systems.

* + - 1. Intrusion detection

When intrusions are detected (Denial-of-service attack), alarm and block actions.

Updating the of decision rules database (if there is a top detection level, optional).

* + - 1. Control (analysis) of information security

Identification, analysis of vulnerabilities in the information system and prompt elimination of newly identified vulnerabilities.

Control of the installation of software updates, including software updates of information security tools.

Monitoring the performance, configuration parameters and correct functioning of software and information security tools.

Control of the composition of hardware, software and information security tools.

Control of the rules for generating and changing user passwords, creating and deleting user accounts, implementing access control rules, user powers in the information system.

* + - 1. Ensuring the integrity of information system and information

Monitoring the integrity of software, including software of information security tools.

Control of the integrity of information contained in the databases of the information system.

Ensuring the possibility of restoring software, including software for information security tools, in the event of emergency situations.

Detection and response to the receipt of unsolicited electronic messages (letters, documents) and other information not related to the functioning of the information system (spam protection).

Control of the content of information transmitted from the information system (containerized, based on the properties of the object of access, and content, based on the search for information prohibited for transfer using signatures, masks and other methods), and exclusion of illegal transfer of information from the information system.

Restriction of users' rights to enter information into the information system.

Control of the accuracy, completeness and correctness of data entered into the information system.

Control of erroneous actions of users to enter and (or) transmit information and warn users about erroneous actions.

* + - 1. Ensuring information availability

Use of fault-tolerant technical means.

Redundancy of hardware, software, information transmission channels, means of ensuring the functioning of the information system.

Monitoring of trouble-free operation of technical facilities, detection and localization of malfunctions, taking measures to restore failed facilities and their testing.

Periodic backup of information to backup computer data carriers.

Ensuring the possibility of restoring information from backup computer data carriers (backup copies) within a set time interval.

Clustering of the information system and (or) its segments.

Control of the state and quality of the provision of computing resources (capacities) by the authorized person, including the transfer of information.

* + - 1. Protecting virtualization environment

Identification and authentication of access subjects and access objects in the virtual infrastructure, including administrators of virtualization management tools.

Control access of access subjects to access objects in the virtual infrastructure, including inside virtual machines.

Logging security events to the virtual infrastructure.

Management (filtering, routing, connection control, unidirectional transmission) of information flows between the components of the virtual infrastructure, as well as along the perimeter of the virtual infrastructure.

Trusted boot of virtualization servers, virtual machine (container), virtualization management servers.

Manage the movement of virtual machines (containers) and the data processed on them.

Control the integrity of the virtual infrastructure and its configurations.

Data backup, backup of hardware, software of the virtual infrastructure, as well as communication channels within the virtual infrastructure.

Implementation and management of antivirus protection in the virtual infrastructure.

Splitting the virtual infrastructure into segments (segmentation the virtual infrastructure) to process information by an individual user and/or group of users.

* + - 1. Protection of technical equipment

Protection of information processed by technical means from its leakage through technical channels.

Organization of a controlled zone, within which stationary technical means processing information, and information security means, as well as means of ensuring functioning, are permanently located.

Control and management of physical access to technical means, means of information protection, means of ensuring functioning, as well as to the premises and structures in which they are installed, excluding unauthorized physical access to means of information processing, means of information protection and means of ensuring the functioning of the information system and premises and structures in which they are installed.

Placement of devices for displaying (displaying) information, excluding its unauthorized viewing.

Protection from external influences (environmental influences, instability of power supply, air conditioning and other external factors).

3.2.11.13. Protection of the information system, its means, communication, and data transmission systems

Separation in the information system of the functions of management (administration) of the information system, management (administration) of the information protection system, functions of information processing and other functions of the information system.

Prevents high-priority processes from being delayed or interrupted by low-priority processes.

Ensuring the protection of information from disclosure, modification and imposition (introduction of false information) during its transmission (preparation for transmission) through communication channels that go beyond the controlled area, including wireless communication channels.

Provision of a trusted channel, route between the administrator, the user and information security tools (security functions of information security tools).

Prevent unauthorized remote activation of video cameras, microphones, and other peripherals that can be activated remotely, and notify users when such devices are activated.

Transfer and control of the integrity of security attributes (security labels) associated with information when exchanging information with other information systems.

Control of authorized and exclusion of unauthorized use of mobile code technologies, including registration of events related to the use of mobile code technologies, their analysis and response to violations related to the use of mobile code technologies.

Control of authorized and exclusion of unauthorized use of voice transmission technologies, including registration of events related to the use of speech transmission technologies, their analysis and response to violations related to the use of speech transmission technologies.

Control of authorized and exclusion of unauthorized transmission of video information, including registration of events related to the transmission of video information, their analysis and response to violations related to the transmission of video information.

Confirmation of the origin of the source of information obtained in the process of determining network addresses by network names or determining network names by network addresses.

Ensuring the authenticity of network connections (interaction sessions), including for protection against substitution of network devices and services.

Prevent a user from denying that they have sent information to another user.

Exclusion of the possibility of the user denying the fact of receiving information from another user.

Use of terminal access devices for information processing.

Protection of archive files, settings for information protection tools and software, and other data that are not subject to change in the process of information processing.

Identification, analysis and blocking of hidden information transmission channels in the information system bypassing the implemented information protection measures or within permitted network protocols.

Dividing the information system into segments (segmentation of the information system) and ensuring the protection of the perimeters of the segments of the information system.

Ensuring the download and execution of software from read-only computer media and monitoring the integrity of this software.

Process isolation (program execution) in a dedicated memory area.

Protection of wireless connections used in an information system.

Exclusion of the user's access to information that arose as a result of the actions of the previous user through registers, RAM, external storage devices and other resources of the information system common to users.

Protection of the information system from threats to information security aimed at refusing to serve the information system.

Protection of the perimeter (physical and (or) logical boundaries) of the information system during its interaction with other information systems and information and telecommunication networks.

Termination of network connections when they are terminated or after the time interval of network connection inactivity specified by the operator.

Use of various types of system-wide, applied and special software in an information system or its segments (creation of a heterogeneous environment).

Use of application and special software that can function in environments of various operating systems.

Creation (emulation) of false information systems or their components designed to detect, register and analyze the actions of violators in the process of implementing threats to information security.

Reproduction of false and (or) concealment of true individual information technologies and (or) structural and functional characteristics of the information system or its segments, ensuring the imposition of a false idea on the violator of true information technologies and (or) structural and functional characteristics of the information system.

Transfer of the information system or its devices (components) to a predetermined configuration that ensures information protection in the event of failures (malfunction) in the information protection system of the information system.

Protection of mobile technical means used in the information system.