TERMS OF REFERENCE
FOR THE PURCHASE
OF UNDERGROUND MINING PLANNING SYSTEM

BISHKEK, 2021

Content

TERMS AND DEFINITIONS

Term	Definition
Planning of Mining Operations	A system of processes for determining the directions and sequence of mining operations, which is cyclical, based on the existing and predicted and periodically updated mining-geological, technical, and technological conditions, taking into account the company's performance targets in the long, medium and short term.
Long-term Planning	Planning of mining operations for five years or more with a breakdown of the first year of mining by quarters and the remaining years by years. The objective is to establish a mining strategy. Tasks: determine the volume and quality indicators planned for the extraction of minerals and identify the contents of useful components and harmful impurities in them, establish the procedure for stripping operations to ensure timely preparation and mining of the deposit reserves, determine the strategic directions of mining operations, determine the required amount of inventory and equipment.
Medium-term Planning	Planning of mining operations for 1 year with a breakdown by months. The objective is to determine the volume and quality indicators planned for the extraction of useful components, clarify the procedure for stripping operations to ensure timely preparation and mining of the deposit reserves, determine the directions of mining operations by month.
Short-term Planning	Planning of mining operations for a month with a breakdown by days. Objective: develop a plan of mining operations for the company's operational activities for the next month. Tasks: determine the volume and quality indicators planned for the extraction of useful components, determine the sequence of extraction units.
Mine Planning System	Software, regulatory documents and unified templates for input and output data, allowing the creation of standardized mining plans within the required time limits and periods of the company's activity.
Volume and Quality Indicators	Numerical indicators of the volume, tonnage, and content of the useful component in the rock mass extracted during mining operations, based on the geological block model.
Mining Plan Scenario	A set of mining and geological, technical, technological data and planning results, reflected in the set of files of certain software.

ABBREVIATIONS AND SYMBOLS

Term	Definition
DB	Drill & Blast
DB	Database
GMIS	Geological and Mining Information System
MPP	Mining and Processing Plant
GE	Geological Exploration
ETP	Engineering and Technical Personnel
IT	Information Technology
KPI	Key Performance Indicators
UMO	Underground Mining Operations
PC	Personal Computer
IO	Industrial Operation
SW	Software
CAD	Computer-Aided Design System
MC	Management Company
RPO	Recovery Point Objective - the allowable amount of possible data loss in the event of a failure (incident).
RTO	Recovery Time Objective - the allowable downtime of the information system in the event of a failure (incident).
DPC	Data Processing Center is a specialized dedicated premises hosting server and network equipment that ensures the uninterrupted 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 restore data to its original or new location in case of damage or destruction.

1. General Information

1.1. Name

Full name is “Terms of Reference for the purchase of underground mining planning system”.
Conventional name - Purchase of a planning system.

1.2. Supplier and Contractor

Client: Kumtor Gold Company CJSC
Software Supplier: the organization selected by the Client to supply software under this TOR.

2. Basis, purpose, and objectives of the purchase of a planning system

2.1. Basis

The basis for the implementation of a planning system is a request from the company's management to develop information transparency in planning underground mining operations, improve the quality of strategic and operational decisions, operate in a single information space, use common tools, increase the productivity of engineering and technical personnel and the reliability of mining planning results.

2.2. Purpose

Implementation of a unified contour of the information system for planning underground mining operations.
Mine Planning System shall:

1. Ensure the automation of the Company's technological processes in terms of planning underground mining operations.
2. Ensure the possibility of planning mining operations for various periods (five-year, year, month), based on geological block models, three-dimensional models of designed mine workings, resources, rules, and restrictions.

2.3. Project Objectives

Project Objectives:

1. Continuous improvement of production processes.
2. Improvement of the professional competence of employees in the use of mining planning software.
3. Optimization of the work of the company's mining service to increase the productivity of labor and the reliability of decisions made.
4. Reducing the influence of the "human factor" by automation of mining and geological production processes of planning, designing, and recording of the company's performance results.
5. Ensure automation of the following processes of underground mining planning (currently, there is no possibility to plan underground operations due to the lack of software with the required functionality).

* Analysis of initial data, such as: geological models, open-pit mining frameworks, underground mining frameworks of previous periods. The official block model provided by geologists is used.
* Construction of chambers' frameworks in accordance with geomechanical, technological and economic parameters, based on the data of a consulting company.
* Design of opening and stoping mining workings.
* Determination of the sequence of construction of workings and development of chambers, work schedule.
* Simulation of the advance of mining workings with their possible productivity (how many meters per day or year, for the required period), to solve tactical planning tasks, for example:

drilling equipment to mine horizontal and vertical workings, as well as to haul the rock mass by load-haul-dump trucks from stoping and development workings.

6. Improving the quality of control and analysis of mining operations.
7. Improving the accuracy of recoverable reserves forecasting at all stages of the deposit development.
8. Reducing the planned vs actual variation by increasing the variability and quality of planning.
9. Reducing the costs of late decision-making.
10. Timely identification of risks.
11. Improving the safety of mining operations.
12. Reducing operating costs by automation of mine planning processes.
13. Achieving the main strategic objectives of the company by increasing the variability and quality of long-term planning.

3. Requirements for underground mining planning system

1. Development of long-term, medium-term, and short-term plans of mining operations within the designed mining contours with the possibility to adjust.
2. Planning of drifting, stoping and auxiliary operations (drilling, blasting).
3. Development of scenarios of mining plans based on geological block models and three-dimensional models of workings.
4. Perform resource-based planning taking into account the performance of equipment or equipment complexes.
5. Perform planning taking into account the target quality of the ore supplied to the Mill.
6. Perform planning taking into account priorities, geometric and logical limits of the sequence of mining and operation of equipment complexes.
7. Analysis of planning results using 3D animation of the mining sequence, visualization of spreadsheets, diagrams, Gantt charts and graphs based on planning results, with the possibility to customize their visualization in interactive mode.

3.1. Requirements for software functionality

The system shall contain the following modules:

1. Planning of underground mining operations with equipment arrangement.
2. Planning of preparatory underground operations with equipment arrangement.
3. Planning of stockpiles (burdening) with equipment arrangement.
4. System administration to differentiate user access rights.

The list of requirements for the software functionality is provided below.

1.	Availability of 3D visualization of planning objects (frameworks, workings, sections, drifts) and animation of the mining sequence based on the established rules of the mining sequence.
2.	Possibility to set a filter for selecting drifts and workings by name, part of name, z mark, name of the assigned equipment, custom attributes in 3D modeling.
3.	Storing planning settings and software results in the form of scenarios.
4.	Using volume-quality characteristics from the attributes of frame models (specific gravity of ore, mineral reserves).
5.	Calculation of volume and quality indicators based on the introduced block models and frameworks: the amount of ore, the content of useful components, the volume of ore extracted (section * length). A reference book of block model parameters is required.
6.	Possibility to use multiple block models in one scenario.
7.	Possibility to use block models with sub-blocking.
8.	Possibility to use block models with partial percentage.
9.	Possibility to create custom calculations by composing formula expressions from mandatory and custom parameters.
10.	User interface and software help in Russian and English.

11.	Possibility to develop long-term (strategic plan, life of mine), medium-term (year, month) and short-term (day, week) mining plans. Initial data: settings of the block model. Preparatory work: Axes of workings, optimization of frameworks. Planning settings: setting the parameters of stope workings. Setting up the sequence of auxiliary operations. Concept of the materials flow chart. Setting up the mining sequence. Mining technology - chamber development system (cutting a split drift, breaking a stope chamber, backfilling of a split drift and a chamber, a mined panel after backfilling). Setting up the equipment performance. Setting up auxiliary operations. Setting up the equipment operation calendars. Visualization of the mining plan.
12.	Planning of drifting operations. Possibility to name drifting workings and assign grouping attributes. Possibility to customize the direction of drifting operations in the mine working (possibility to set the direction, sequence of mine workings, priority). Possibility to assign a sequence of drifting operations manually.
13.	Functionality to calculate volume-quality indicators in drifting working at predetermined cross-sections of different volumes (cross-section * length = volume, volume * specific gravity = mass).
14.	Functionality to enter the fact of working drifting (meters of drifting, percentage of completion) to determine the position from which the formation of the plan begins.
15.	Planning of stoping operations (possibility to enter a sequence of mining operations by chambers and equipment performance).
16.	Possibility to assign the names of the stope workings and assign grouping attributes (the specified period of working, the direction of stoping operations).
17.	Possibility to set up auxiliary operations: drilling, blasting, backfilling operations.
18.	Possibility of a schematic representation of the company's ore flows along the materials movement chain from the mining areas to the Mill.
19.	Possibility to configure soft priorities for the distribution of performance between workings.
20.	Possibility to add mining and auxiliary equipment or equipment complexes with their performance parametes. A hardware manual is required.
21.	Possibility to customize the designation of equipment (main and auxiliary) by mine workings both interactively in the 3D interface and in tabular form.
22.	Possibility to customize the working calendars of the equipment.
23.	Functionality to set dates and events, in case of which the input parameters of planning are changed.
24.	Functionality to enter the fact of stoping operations (tons extracted, percentage of completion) to determine the position from which the formation of the plan begins.
25.	Possibility to perform resource-based planning taking into account the entered performance of equipment or equipment complexes.
26.	Possibility to plan ore burdening, taking into account intermediate stockpiles and ore delivery directly from mining areas.

27.	Possibility to perform planning taking into account the target quality of the ore supplied to the Mill.
28.	Visualization of planning results - 3D model.
29.	Possibility of 3D sequence animation of mining the areas and auxiliary operations, the developed calendar plan.
30.	Versioning of changes.

3.2. Non-functional software requirements

3.2.1. Performance Requirements

№	Parameter	Value
1.	Number of users simultaneously working with the system per time unit	5
2.	Average response time for display navigation operations	<= 8 sec.
3.	Average response time for data search/filter operations	<= 60 sec.

3.2.2. Requirements for integration with existing systems

It is necessary to have a possibility to implement automated data exchange (block model, frame models of stope workings, axes of workings, cross-sections of drifting working based on a string file) with existing systems via RESTful API.

It is necessary to have a possibility to implement automatic uploading of graphical planning results: in the form of polygonal models of workings with period identifiers, in the form of frame models with period identifiers, in the form of numerical data into the corresponding blocks of the geological block model in DXF, DWG, SURPAC, DATAMINE, MICROMINE, VULKAN formats.

3.2.3. System reporting requirements

Visualization of reports on mining, extraction, planning results for a given period of time (from 1 hour).

Visualization of graphs on mining, extraction, planning results, with the possibility to customize graph formats (bar charts, pile charts, line charts, area charts).

Visualization of the workflow in the form of a Gantt chart.

3.2.4. System class in terms of recovery time and availability per year

Fault Tolerance Template Code	Fault Tolerance Template Name	Template Description	System Class Code using this template	Regulated % of System availability per year (SLA)	Max. allowable System downtime per year	* Recovery in the event of a local system failure		* Recovery in the event of the main DPC failure		Number of required equipment sets to ensure the declared fault tolerance
						RTO	RPO	RTO	RPO	

RC5	Low Speed	All other systems not classified as RC1, RC2, RC3, RC4	OP, TE	99%	up to 3 days 15 hours 40 minutes	up to 72 hours	up to 24 hours	up to 4 weeks	up to 24 hours	One set of servers and SANs in the main DPC

3.2.5. System class by recovery priority

System Class Code	System Class Name	Description of classifiers
OP	Office Productivity	Office applications that ensure the efficient work of company personnel.

3.2.6. Typical architectural template for Low Speed (RC5) system

Fault Tolerance Template Code	Fault Tolerance Template Name	Template Description	* Recovery in the event of a local system failure		Recovery in the event of the main DPC failure	
			RTO	RPO	RTO	RPO
RC5	Low Speed	All other systems not classified as RC1, RC2, RC3 or RC4	up to 72 hours	up to 24 hours	up to 4 weeks	up to 24 hours

RC4 recovery priority class systems are OP (Office Productivity) or TE (Test) Systems.

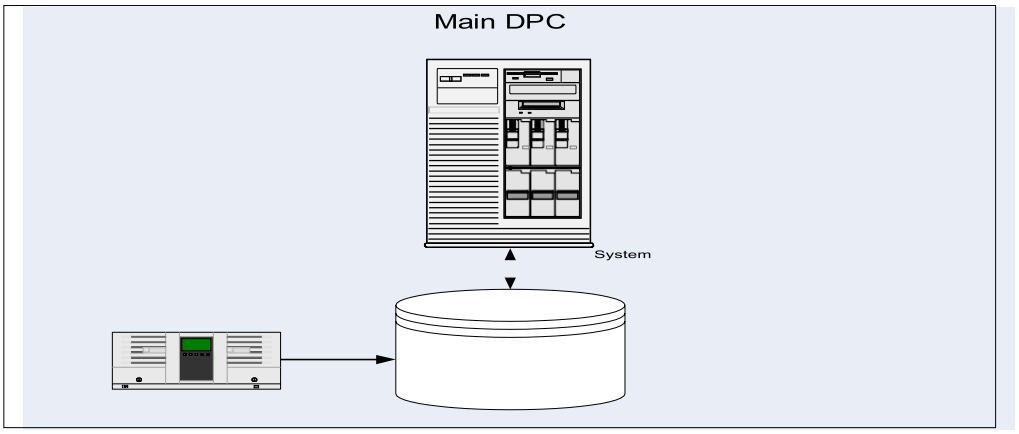
Technological solution for RC5 IT-System:
The same data protection strategy can be used as for RC4 recovery priority data.
The following data backup technologies can be used:

1. DB in LAN or SAN network.
2. DB on magnetic tapes.

For RC4 Class Systems, the following requirements shall be taken into account:

1. it is allowed to use mid/entry-level SANs connected via SAN/DAS, and internal disks assembled in a RAID group can also be used.
2. a complete DB on the tape should be performed at least once a week.
3. the applications are likely not to be clustered.
4. Hardware redundancy is not used for this Class Systems.

Configuration without redundancy



3.2.7. System class by Support Mode

Code	Name	Description
S11x7	S11x7	IT system, accompanied by IT in the mode of 11 hours a day and 7 days a week.

3.2.8. System documentation requirements

Based on the results of the project implementation, the Contractor shall develop, agree, and submit the following documents to the Client:

- TERMS OF REFERENCE
- Specification (Composition and description of the program. Information about the logical structure and the functioning 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, limitations for the application).
- Test program and methodology (test object; test purpose; program requirements; software documentation requirements; test composition and procedure with indication of technical and software tools used during tests, as well as the procedure for conducting tests; test methods with indication of test results (lists of test examples)).
- Testing protocols (unit, integration, performance, vulnerability stress tests).
- Developer's Guide (Information for checking, ensuring the functioning and setting up the program, API library of classes and functions with a description of signatures, semantics of functions).
- Application Administrator Guide.
- User's Manual.

3.2.9. Requirements for the system role model

During the project implementation, the CRUD (Create, Read, Update, Delete) matrix shall be implemented in the system.

Action / Role	Creation of user guides	Access control	Planning	Reporting
Planner 1			CRU	CRU
Planner 2			CR	CR
Admin	CRU			
Information security officer		CRU		

3.2.10. Information security requirements

3.2.10.1. Identification and Authentication

Identification and authentication of the subject and object access through integration with the Active Directory.

Management of identifiers, including the creation, assignment, destruction of identifiers.

Management of authentication means, including storage, issuance, initialization, blocking of authentication means and taking measures in case of loss and (or) compromise of authentication means.

Feedback protection when entering authentication information.

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

3.2.10.2. Access control of access subjects to access objects

Management (creating, activating, blocking, and deleting) of user accounts, including external users.

Implementation of the required methods (discretionary, mandatory, role-based, or other method), types (read, write, execute or another type) and access control rules.

Management (filtering, routing, connection control, unidirectional transmission, and other management methods) 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 the minimum necessary rights and privileges to users, administrators and persons ensuring the functioning of the information system.

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

When the user enters the information system, he/she shall be warned that information protection measures have been implemented in the information system, and that it is necessary to comply with the information processing rules set up by the operator.

Notifying the user after a successful login to the information system about his/her previous login to the information system.

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

Blocking the access session to the information system after the set time of inactivity of the user or at his/her request.

Support and preservation of security attributes (security tags) 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.

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

Providing a trusted download of computer technology.

3.2.10.3. Limiting the software environment

Managing the launch (accesses) of software components, including the definition of the components to be launched, setting the parameters for launching components, monitoring the launch of software components.

Managing the installation of software components, including determining the components to be installed, configuring the installation parameters of components, monitoring the installation of software components.

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

Managing temporary files, including ban, permission, redirection of records, deletion of temporary files.

3.2.10.4. Protection of computer storage media

Accounting for computer data carriers.

Access control to computer storage media.

Control of the movement of computer data carriers outside the controlled area.

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

Control of the use of the information input (output) interfaces on computer storage media.

Control of the information input (output) on computer storage media.

Monitoring the connection of computer storage media.

Destruction (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 destruction (erasure).

3.2.10.5. Security Event Recording

Determination of security events to be recorded and their storage periods.

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

Collection, recording and storage of information about security events for a specified storage period.

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

Monitoring (viewing, analyzing) the results of recording security events 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 possibility to view and analyze information about the actions of individual users in the information system.

3.2.10.6. Anti-virus protection

Implementation of anti-virus protection or integration with the existing ones.

Updating the database of signs of malicious computer programs (viruses).

3.2.10.7. Intrusion detection

Intrusion detection.

Updating the base of decisive rules.

3.2.10.8. Control (analysis) of information security

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

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

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

Control of the composition of technical means, 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 permissions in the information system.

3.2.10.9. Ensuring the integrity of the information system and information

Control of the software integrity, including information security software.

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

Providing the possibility to restore software, including information security software, in the event of emergency situations.

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

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

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

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

Control of erroneous actions of users in entering and (or) transmitting information and warning users about erroneous actions.

3.2.10.10. Ensuring the information availability

Use of fault-tolerant technical means.

Reservation of technical means, software, information transmission channels, means of ensuring the functioning of the information system.

Monitoring the trouble-free functioning of technical means, detecting, and localizing functioning failures, taking measures to restore the failed means, and testing them.

Periodic backup of information on backup computer storage media.

Providing the possibility to restore information from backup computer storage media (backups) within a specified time interval.

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

Monitoring the status and quality of the provision of computing resources (capacities) by an authorized person, including information transfer.

3.2.10.11. Securing virtualization environment

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

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

Recording security events in the virtual infrastructure.

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

Trusted loading of virtualization servers, virtual machines (containers), virtualization management servers.

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

Monitoring the integrity of the virtual infrastructure and its configurations.

Backing up data, backing up hardware, virtual infrastructure software, as well as communication channels within the virtual infrastructure.

Implementation and management of antivirus protection in a virtual infrastructure.

Dividing the virtual infrastructure into segments (segmenting the virtual infrastructure) for processing information by an individual user and (or) a group of users.

3.2.10.12. Protection of technical means

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 protection means, as well as functioning ensuring means, are permanently located.

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

Placement of information output (display) devices, excluding its unauthorized viewing.

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

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

Separation of information system management (administration) functions, information security system management (administration), information processing functions and other information system functions.

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

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

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

Prohibition of unauthorized remote activation of video cameras, microphones and other peripheral devices that can be activated remotely and notifying users about the activation of such devices.

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

Control of authorized and exclusion of unauthorized use of mobile code technologies, including recording 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 speech transmission technologies, including recording 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 video information transmission, including recording of events related to the video information transmission, their analysis and response to violations related to the video information transmission.

Confirmation of the origin of the information source 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 to protect against substitution of network devices and services.

Exclusion of the possibility of denial by the user of the fact of sending information to another user.

Exclusion of the possibility of denial by the user of the fact of receiving information from another user.

Use of terminal access devices for information processing.

Protection of archived files, settings of information and software, and other data security tools that cannot be changed during information processing.

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

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

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

Isolation of processes (program execution) in the allocated memory area.

Protection of wireless connections used in the information system.

Exclusion of user's access to information resulting from the actions of the previous user through registries, RAM, external storage devices and other information system resources shared by users.

Protection of the information system from information security threats aimed at denial of the information system service.

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

Termination of network connections upon their completion or upon expiration of the time interval of inactivity of the network connection specified by the operator.

Use of various types of system-wide, applied, and special software in the 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, record, and analyze the actions of violators in the process of implementing information security threats.

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 about the true information technologies and (or) the structural and functional characteristics of the information system.

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

Protection of mobile technical means used in the information system.