



Information Security Management Systems

Understanding how centralized security policies protect heterogeneous networks through clear principles and coordinated architecture

What We'll Cover Today

01

Core Requirements

What an information security management system must provide and its operating conditions

02

Nine Principles

The foundational principles that support the entire information security framework

03

Real Architecture

How Trusted Agent, GSM Server, and management console work together

04

Authentication Methods

From passwords to smart cards and system integration

05

Access Control

Proxy modules and application-level security

Why Management Systems Matter

The Challenge

As companies grow—opening branches, adding employees, deploying new servers and cloud services—managing security becomes exponentially harder.
Managing each machine separately is inefficient and error-prone.

The Solution

A coherent set of processes, policies, and technical tools working together.
Set a single policy once, and it automatically applies everywhere—no repetitive work on each device.

Operating Conditions

Real-world requirements for security systems that coexist with other critical infrastructure

Subsystem Compatibility

Security systems must not break workflows or conflict with other software like fire alarms, access control, or video surveillance

Uniform Reliability

All components need the same reliability standards—one weak module compromises the entire protection level

Fault Tolerance

If one subsystem fails, others continue working in degraded mode

Clear Control

Centralized or decentralized management with explicit access controls

Complete Logging

Every event is logged—the #1 requirement for auditing and incident investigation

Nine Foundational Principles

These principles emerge from decades of corporate experience—without them, systems eventually fail

Complexity

Protection at all levels: physical security, data cryptography, personnel policies, log auditing

Interaction

Cooperation with providers, authorities, and partners—incidents require collaboration

Centralized Management

Single policy point managing geographically distributed systems



Validity

Every investment justified; choose tools that work and meet standards

Improvement

System adapts as threats evolve, software updates, and requirements change

Legality

All tools and procedures operate within legal frameworks

Continuity

System operates 24/7; updates and reboots planned without compromising security

Specialization

Engage security professionals; don't rely solely on general IT departments



Three-Component Architecture

Like a factory: agents are machine tools, the management server is the dispatcher, and the console is the chief engineer's tablet



Trusted Agent

Program on every machine—client, server, or gateway. Checks identity, blocks dangerous traffic, keeps logs, requires authentication. Awaits server instructions.



Trusted GSM Server

Stores all security policies. Converts general policy to machine-specific rules and distributes them. Monitors agent health. Scales to 65,535 servers for heavy loads.



Trusted GSM Console

Administrator interface. Role-based views—directors see the big picture, branch employees see only their machines.

Authentication Methods

Multiple ways to verify identity, often combined for stronger security

Password

Classic and familiar, but vulnerable
with weak choices

Token

Physical key that can't be guessed;
emergency deactivation if stolen

Smart Card

Tiny computer storing private key that
never leaves the card

External Authentication

System queries another system like Active Directory

Multi-Factor Combinations

Two or three factors: password + token + fingerprint

Beyond Authentication: Access Control

The Challenge

Knowing who you are isn't enough—the system must decide what you can do.

Network Level

Can your computer connect to the server at all?

Application Level

Can you see all documents or just your own?

Proxy Modules

Special traps for requests. When you access the server, the proxy asks: "Can you do that?" If not, it blocks the request.



Control and Audit

Security is only partially technical—the other part is people who configure and monitor it



Event Logging

Every filter trigger, every access attempt—everything is logged for review



Administrator Monitoring

If an admin grants unauthorized access, it's visible in logs



Periodic Audit

Quarterly or annual reviews of changes and their justifications



Management Reporting

Leadership visibility into threats and applied countermeasures



Security questions

1. Name the three main components of the information security management architecture and their roles.
2. What is the difference between a Global Security Policy (GPB) and a local one?
3. What authentication methods do you know and which one is the most reliable?
4. Why is it important to log admin actions?
5. Give an example of how a proxy module can restrict user access to application data.
6. Which of the nine principles, in your opinion, is most often violated in practice and why?

List of references

1. ISO/IEC 17799:2000 (BS 7799:2000). Information technology — Code of practice for information security management.
2. ISO/IEC 27001:2013. Information security management systems — Requirements.
3. ISO/IEC 15408 (Common Criteria). Information technology — Security techniques — Evaluation criteria for IT security.
4. GOST R ISO / IEC 17799-2005. Information technologies. Safety precautions. Guide to Information Security management.
5. Baranov A. S. Informatsionnaya bezopasnost': kurs lektsii [Information Security: a course of lectures]. Moscow: Akademiya, 2021.
6. Gostev R. Managing security policies in corporate networks. St. Petersburg: PiterPubl., 2021.
7. TrustWorks Systems. Global Security Management Concept. White paper.