



# Lecture 3: Types of Measures to Ensure Information Security

A Classification of Controls

# Agenda

01

## The Three Pillars of Security

---

Legal, Organizational, and Technical

02

## Hardware Security Measures

---

Protecting against physical threats

03

## Software Security Measures

---

Tools for data protection

04

## Functional Classification of Controls

---

Preventive, Detective, Corrective

05

## Key Takeaways

---

Integrated and layered defense

# The Three Pillars of Security

Security requires a systematic, integrated approach.



## Legal

Laws, standards, and accountability

## Organizational

Policies, personnel, and recovery plans

## Technical

Controls, networks, and system protections

### Legal Measures

Laws, standards, and responsibility for computer crimes.

### Organizational Measures

Physical security, personnel selection, disaster recovery, segregation of duties.

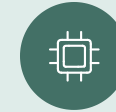
### Technical Measures

Hardware and software tools for protection (e.g., access control, redundancy).

# Technical Measures: Hardware Security (Part 1 – Availability)



**Power Failure Protection**  
Uninterruptible Power Supplies (UPS) and redundant power supplies ensure continuous operation.



**Processor Failure Protection**  
Redundancy and symmetric multiprocessing allow systems to continue working if one processor fails.



**Storage Device Failure Protection**  
Backup systems(tapes,off-sitestorage) and mirroring (RAID 1) provide data safety.

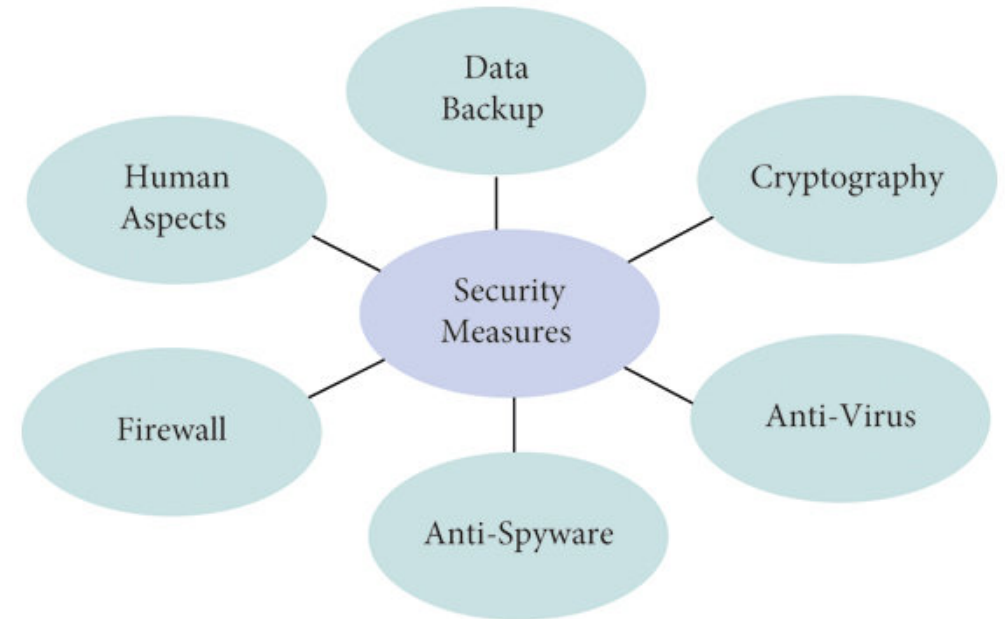
# Technical Measures: Hardware Security (Part 2 – Confidentiality)

Threat: Spurious Electromagnetic Radiation (PEMI)

Signals from monitors, CPUs, and printers can be intercepted from a distance, leading to information leakage.

Protection Methods:

- Shielding (rooms or equipment)
- Filtering (on power lines)
- Grounding



# Information Security Software Categories

Specialized programs provide essential data protection functions.

## → Data Archiving Tools

For secure storage and retrieval of historical data.

## → Antivirus Software

Detects and removes malicious software.

## → Cryptographic Tools

Encryption for data confidentiality and integrity.

## → User Identification & Authentication

Verifies user identities before granting access.

## → Access Controls

Manages permissions for resources and data.

## → Logging and Audit Tools

Records system activities for security monitoring and incident investigation.

# Key Takeaways: A Layered Defense

Security is not a single product; it's a layered system of controls.



A legal policy needs organizational procedures, and technical tools require physical security.

# Hardware Security: The Foundation

Software security is irrelevant if physical hardware fails.



## Power Outages

UPS systems protect against power loss.



## Disk Failures

RAID and backups prevent data loss.



## Electromagnetic Eavesdropping

Shielding protects against data leakage.

Protecting against physical threats is the foundational layer for all other security.



# Functional Classification of Controls

Measures can be classified by their function relative to a security incident.

1

## Preventive Controls

Stop threats from succeeding (e.g., access controls, encryption, UPS, physical locks).

2

## Detective Controls

Identify and report incidents in progress or after occurrence (e.g., logging, antivirus scans, fire alarms).

3

## Corrective Controls

Remediate incident impact and restore systems (e.g., backup restoration, mirrored drives, disaster recovery plans).

# Controls Map to Threats

Technical measures directly counter specific threats.

Availability

UPS and redundancy.

Confidentiality

Access control and cryptography.



Integrity

Backups and mirroring.

This framework ensures a comprehensive defense strategy.

**Control questions:**

- What areas of information protection measures do you know?
- List the main software and hardware tools for protecting computer information.
- What are the means of protection against power failures?
- What are the means of protection against malfunctioning processors and storage devices?
- What are the means of protection against information leaks due to the formation of electromagnetic radiation?
- What relates to information security software?

**Recommended literature:**

- Partyka T.L., Popov I.I. Information Security. Textbook for students of vocational schools. M.: FORUM: INFRA - M, 2002.
- Raghavan, S. Cyber Security: Concepts, Methodologies, Tools, and Applications; IGI Global: Hershey, PA, USA, 2022.
- Stallings, W.; Brown, L. Computer Security: Principles and Practice, 4th ed.; Pearson: London, UK, 2021.
- Pfleeger, C.; Pfleeger, S.; Margulies, J. Security in Computing, 6th ed.; Pearson: London, UK, 2022.
- Kim, D.; Solomon, M.G. Fundamentals of Information Systems Security, 4th ed.; Jones & Bartlett Learning: Burlington, MA, USA, 2021.
- Whitman, M.; Mattord, H. Principles of Information Security, 8th ed.; Cengage Learning: Boston, MA, USA, 2023.