DOI: https://doi.org/10.53486/ser2025.31
International Scientific and Practical Conference, 4th Edition, March 27-28, 2023, Chișinău, Moldova

SECURING INFORMATION THROUGH DATA CLASSIFICATION

Fiodor TIMERCAN
PhD Candidate, University Lecturer
"Alexandru cel Bun" Armed Forces Military Academy, MOLDOVA
E-mail: timercantudor@yahoo.com
ORCID: 0009-0001-6769-3556

Abstract: *This paper explores the structured classification of information as a foundational element of information security, particularly within military and government systems. Using theoretical analysis and comparative review of access control mechanisms, the study identifies key strategies for mitigating data exposure risks. It distinguishes between subjective, objective, and technical information and analyzes their relevance to secure communication environments. The paper also discusses the evolution of access control post-9/11 and categorizes preventive, detective, and corrective security measures. Recommendations are proposed for policy development and implementation to enhance systemic resilience in the digital age.*

Keywords: *Network attacks, cryptographic, security, encryption, Virtual Private Networks, communication network.*

UDC: *004.056:004.67*

Classification JEL: *O3.*

1. Introduction

Our statements are supported by concerns regarding information protection and security, which date back thousands of years. At the risk of contradicting some previous periodizations, we can assert that the signals provided by different peoples over time lead us to the conclusion that the phenomenon of globalization in information protection and security systems began more than ten thousand years ago. Historical accounts - from Mesopotamian encryption methods to modern digital protocols - demonstrate the longstanding importance of securing sensitive data. Even the traditional system based on a central computer has become obsolete, as people across the world discuss the Internet, Intranet, Extranet, and the integration of personal computers (PDAs), various generations of mobile phones, and many other technologies. The modern dependence on cyberspace heightens the risk of disruption, necessitating robust classification systems.

2. Literature Review

Several sources address information classification and protection strategies. Arvin S. Quist (1993)[1] extensively explored classification systems. Anderson (2021)[2] and Miller (2002)[3] examined dependable system design and PC privacy respectively. Chen (2006)[4] discussed information sharing and security informatics. Andress (2002)[5] focused on integrating security policies with people and technology. Baker (1995)[6] and EU legal frameworks (EUR-Lex, 2025)[7] provide insights into national and institutional responses. However, a gap remains in integrating historical, typological, and strategic perspectives into a unified framework.

3. Methodology

This paper is structured as a conceptual analysis. It synthesizes previous literature and applies a typological approach to the classification of information. The analysis draws upon institutional practices, governmental strategies, and legislative frameworks, including

DOI: https://doi.org/10.53486/ser2025.31
International Scientific and Practical Conference, 4th Edition, March 27-28, 2023, Chișinău, Moldova

post-9/11 security shifts. No primary data collection is involved; the approach is qualitative, interpretive, and policy-oriented.

4. Results and Discussion

4.1. The beginnings of modern information classification

Regarding access to certain categories of information for the purpose of exercising control, the rules are clearer: an official may read documents from a specific category only if they have at least the authorization to access information from that category or a higher one. For example, an individual authorized to access "top secret" information can read confidential, secret, and top-secret information, whereas someone with access rights to secret information cannot access top-secret materials. The rule is that information can flow only upwards from confidential to secret and top secret while downward flow is only possible if an authorized person deliberately decides to reclassify it.

Additionally, rules for document storage have been established as follows: confidential documents are kept in locked cabinets in any government office, while documents in higher categories require specific types of safes, guarded doors, and control over copiers and other electronic equipment

Two fundamental strategies are practiced in national security:

1. Everything that is not prohibited is permitted.
2. Everything that is not permitted is prohibited.

In the United States, the first strategy governs access to government information. In many countries around the world, access to national information is controlled by state secrecy laws, following the second strategy. A loyal and dedicated employee does not discuss company affairs until they are certain that the matter can be made public. Two tactics are used to implement the fundamental strategy for protecting sensitive information:

- Discretionary access control;
- Legally regulated access control.

4.2. Information classification

When information was divided into two main categories classified and unclassified certain principles were considered. However, understanding these principles requires a preliminary approach to some key concepts. Governments start with a broader classification, dividing information into two main types:

- Subjective information;
- Objective information.

Previously, another classification was used: "operational" and "scientific" information. Some have even mentioned a third type of government-classified information “technical” information. However, in many sources, technical and scientific information are considered subsets of objective information.

Subjective Information

Subjective information has also been described as “true secrets,” while other authors have referred to it as "operational" or "operational secrets." However, the most appropriate term is subjective information or subjective secrets. This type of information is unique to the government, as it determines how key national activities will be conducted. As long as the government controls and protects the information on which it bases its decisions, adversaries cannot independently uncover it.

For example, in the military domain, subjective information includes the plan for invading another country (the timing and location of the invasion). The adversary cannot

DOI: https://doi.org/10.53486/ser2025.31
International Scientific and Practical Conference, 4th Edition, March 27-28, 2023, Chișinău, Moldova

generate such information independently; they can only obtain it through espionage or unauthorized disclosure.

Characteristics of subjective information:

- *Small size* – The secret can often be expressed in just a few words, making it easy to steal and share.
- *Universal perceptibility* – No special training is needed to understand the secret; anyone can steal it.
- *Vulnerability to theft* – An adversary can steal it through espionage since it cannot be discovered independently.
- *Modifiable content* – The secret can be changed at the last moment; if a country learns that the enemy knows the timing and location of an invasion, these details can be altered.
- *Short lifespan* – Secrets quickly become obsolete; for example, once an invasion starts, the secret is no longer relevant, as the adversary has already learned it. Thus, secrets can only be protected for a limited period.

Objective Information

Objective information includes data that, even if discovered, developed, or controlled by the government, can already be known or independently discovered by another country. This category includes scientific information or scientific secrets. Such information cannot be absolutely controlled, as it is tied to the nature of things rather than secrecy. Scientists from different countries, working independently, may make identical discoveries. This type of information is also referred to as objective information or objective secrets.

Characteristics of Objective Information:

- *Complex and detailed* – Unlike a simple secret formula, scientific information often requires extensive reports for explanation, making it difficult to transmit easily.
- *Requires specialized knowledge* – It can only be understood by scientists or experts in the field.
- *Not arbitrarily controlled* – Others can discover the same information if they ask the right scientific questions.
- *Unchangeable* – It has an eternal character; a natural phenomenon has a single, definitive value.
- *Long-lasting secrecy* – While others may independently discover it, the process takes time, allowing the information to remain secret for an extended period.

Technical Information as an Objective Secret

A third type of information does not fit neatly into the subjective or objective categories technical information, which includes designs and technical implementations of new weapons. Unlike the scientific nature of theoretical research, technical information relates to practical applications and is classified as technical secrets or objective secrets.

While technical information shares characteristics with scientific information, there are key differences. Unlike scientific discoveries, which are natural phenomena, technical information refers to a method, process, technique, or equipment used to create a product. Essentially, technical information is applied science, used to exploit scientific discoveries.

However, in the field of information classification, scientific and technical information are often grouped together as a single type of objective information.

DOI: https://doi.org/10.53486/ser2025.31
International Scientific and Practical Conference,
4th Edition, March 27-28, 2023, Chișinău, Moldova

4.3. Access control in information systems

After September 11, 2001, the concept of access control within systems underwent a radical transformation, both in terms of enforcement methods and areas of application. Regarding methods, a major debate in the late 1990s focused on whether biometric identification systems should be introduced. At that time, biometrics was mainly associated with fingerprint collection for criminal investigations, and there was significant opposition, particularly from the banking sector. Other security tools were considered inconvenient or even dangerous and were therefore widely rejected. However, after the aforementioned date, attitudes changed dramatically, particularly concerning biometric identification, a trend that will be analyzed in detail later in this chapter.

The areas of application also expanded significantly, driven by system owners' and administrators' growing belief in the necessity of enhanced verification methods. As a result, stricter security measures were implemented in presidential, governmental, and public or private institutions, while airports significantly expanded their high-security zones.

Impact on Information Systems

Information systems also evolved significantly. A clear example is Microsoft's efforts in security enhancement, where almost every movement of personnel is monitored, relying on complete dependence on special access cards.

By the end of this chapter, readers should be able to:

- Acquire sufficient knowledge to determine and implement appropriate access control measures for a specific organization.
- Understand different access control models and how to combine them effectively.
- Gain expertise in identification and authentication methods necessary for organizational security.

4.5. Types of system access control

Security controls are implemented *to reduce risks and minimize potential losses* within a system. These controls fall into three primary categories:

Preventive Controls

- Purpose: Prevent security incidents from occurring.
  Examples:
  - ✓ Administrative: Security policies, employee training, background checks.
  - ✓ Technical: Firewalls, encryption, multi-factor authentication (MFA).
  - ✓ Physical: Locked server rooms, security guards, biometric access.

Detective Controls

- Purpose: Identify and detect anomalies or security breaches.
  Examples:
  - ✓ Administrative: Security audits, monitoring workplace activities.
  - ✓ Technical: Intrusion Detection Systems (IDS), log analysis, anomaly detection.
  - ✓ Physical: Security cameras, motion sensors, badge access logs.

Corrective Controls

- Purpose: Restore normal operations after an incident.
  Examples:
  - ✓ Administrative: Incident response plans, policy updates.
  - ✓ Technical: Patching vulnerabilities, restoring data from backups.
  - ✓ Physical: Replacing compromised locks, reinforcing physical barriers.

DOI: https://doi.org/10.53486/ser2025.31
International Scientific and Practical Conference,
4th Edition, March 27-28, 2023, Chișinău, Moldova

Security Control Pairings

For comprehensive protection, different types of controls are often combined:

- Preventive/Administrative – Employee security training.
- Preventive/Technical – Firewalls and access control lists.
- Preventive/Physical – Biometric security at entry points.
- Detective/Administrative – Internal security audits.
- Detective/Technical – Intrusion detection systems (IDS).
- Detective/Physical – Surveillance cameras monitoring sensitive areas.

By integrating these security controls effectively, organizations can ensure system security throughout its entire lifecycle.

Figure 1. Types of system access control
Source: author's elaboration

Preventive/Administrative Control

This approach focuses on the administrative responsibilities that contribute to achieving access control objectives. These mechanisms include organizational policies and procedures, background checks before hiring, employment termination practices (both normal and abnormal conditions), vacation planning, labeling or marking of special materials, more stringent supervision, training courses for security awareness, behavioral awareness, and procedures for signing contracts to obtain access to the informational system and network.

Preventive/Technical Control

The preventive-technical pairing focuses on using technologies to reinforce access control policies. Technical control, also called logical control, can be implemented through operating systems, applications, or an additional hardware/software component. Preventive/technical controls include protocols, encryption, smart cards, biometrics (for authentication purposes), software packages for local or remote access control, passwords, menus, antivirus software, and more.

Preventive/Physical Control

Mostly intuitive in nature, preventive/physical control measures aim to restrict physical access to areas containing sensitive system information. These areas are defined by a so-called security perimeter, under access control. This category includes fences, badges, multiple doors (after passing through one door, it locks automatically, and the next door requires knowledge of an opening system, trapping the person between two doors, hence referred to as "trap doors"), magnetic card entry systems, biometric identification

DOI: *https://doi.org/10.53486/ser2025.31*
International Scientific and Practical Conference, 4th Edition, March 27-28, 2023, Chișinău, Moldova

systems, security services, guard dogs, environmental control systems (temperature, humidity, etc.), building and access route blueprints, and specially designated areas for storing information media.

Detective/Administrative Control

Some of the detective/administrative controls overlap with reventive/administrative controls because they can be exercised to prevent potential security policy violations or to detect those in progress. This category includes security procedures and policies, background checks, vacation planning, marking or labeling special materials, more stringent supervision, and training to raise security awareness. Additionally, detective/administrative controls include those aimed at personnel rotation at workplaces, shared responsibility for tasks, and reviewing records for auditing purposes.

Detective/Technical Control

Detective/technical control measures aim to highlight security policy violations using technical means. These measures refer to intrusion detection systems and automated security violation reports, generated based on information collected for audit purposes. The reports can highlight deviations from "normal" operation or detect known signatures of unauthorized access episodes. Due to their importance, the information used in auditing must be protected at the highest level possible within the system.

Detective/Physical Control

Generally, these controls require human intervention to assess what the sensors or cameras provide in order to determine if there is a real threat to the system. In this case, control is exercised through video cameras, thermal detectors, smoke detectors, and motion detectors.

6. Conclusions

The classification of data is fundamental for national and organizational security. This study has shown that differentiating between subjective, objective, and technical types of information allows institutions to apply nuanced protection mechanisms. The typological understanding of data lays the groundwork for robust access control strategies - particularly in environments where digital vulnerability intersects with national interest.

Preventing all cyber-attacks is an unrealistic goal; however, the implementation of layered controls - preventive, detective, and corrective - ensures continuity and resilience in information systems. The evolution of access control systems post-9/11 demonstrates the critical role of adaptive policies and biometric technologies in enhancing security protocols.

Furthermore, institutional coordination, especially between the public and private sectors, must become a cornerstone of cyber governance. By building institutional capacity, raising awareness, and enforcing compliance frameworks, states and organizations can reduce the systemic risks associated with digital infrastructure.

Future research and practice should prioritize real-time threat detection capabilities and legal harmonization at transnational levels. Investments in education, cybersecurity certification, and interoperable policy frameworks are necessary to ensure sustainable digital resilience in an increasingly interconnected world.

7. References

1. QUIST, A. S. Security classification of information. 2nd ed. Tennessee: U.S. DEPARTMENT, 1993. DE-AC05-84OR21400.
2. ANDERSON, R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. UK: Cambridge University, 2021. ISBN: 978-1-119-64278-7.

DOI: *https://doi.org/10.53486/ser2025.31*
International Scientific and Practical Conference, 4th Edition, March 27-28, 2023, Chișinău, Moldova

3. MILLER, M. Security Engineering: Absolute PC Security and Privacy. San Francisco: Sybex, 2002. ISBN: 9780782141276.
4. CHEN, H. Intelligence and Security Informatics for International Security. Information Sharing & Data Mining. Springer, 2006. ISBN: 978-0-387-24379-5.
5. ANDRESS, M. Surviving Security: How to Integrate People, Process, and Technology. Indianapolis: Sams Publishing, 2002. ISBN: 978-0849320422.
6. BAKER, R. Network Security: How to Plan for It and Achieve It. New York: McGraw-Hill, 1995. ISBN: 978-0070051416.
7. EUR-LEX. Access to European Union law [online]. 2025. [viewed 19 March 2025]. Available from: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016L1148