

Limitation and Regulation of Access to Information to Achieve Information Security in the Interaction of National Security Systems in Crisis Situations Related to Cyber Security and Cyber Defence

Veselina Gagamova^{1,*}, Milena Ivanova², Ivan Hristozov³, Violeta Vasileva⁴
 G. S. Rakovski National Defence College, 82 Evlogi i Hristo Georgievi Blvd., 1504 Sofia, Bulgaria^{1,3}
 Council of Ministers of the Republic of Bulgaria, 1 Dondukov Blvd., 1594 Sofia, Bulgaria²
 Future Innovation Labs⁴
 v.gagamova@rndc.bg

Abstract: Achieving information security in the organization is related to the implementation of certain standard security procedures. The set of methods and tools for information security and communication and information systems (CIS) are the tools for implementing these procedures. The subject of the research is the subsystem for limiting and regulating access to information and communication and information systems, which is necessary for the analysis and simulation modelling of the interaction of national security systems in crisis situations related to cybersecurity and cyber defence.

Keywords: INFORMATION SECURITY, CRISIS MANAGEMENT, STANDARD SECURITY PROCEDURES

1. Introduction

The modern trend in crises affecting national security or the welfare of citizens is related to their common characteristic - the fact that their roots and impacts are exclusively connected to the physical domains of land, air, sea or space. In the last two decades, a new domain has evolved - "Cyberspace", which can still rely on and consists of physical assets (server, router, etc.) and also contains a new virtual dimension - the web space. The online world has been conquered society as a whole with the increasing number of online services and connectivity. This in turn becomes a strength as well as a weakness. Communication and Information Systems (CIS) and technology are a critical factor in the economy and society that now rely on the Internet for many different ways and levels. Cybersecurity incidents, whether intentional or accidental, are growing at an alarming rate and affect many areas. Such cyber security incidents could lead to the disruption of essential services such as water, healthcare, electricity or mobile services [1].

Achieving information security in the organization is related to the implementation of certain standard security procedures. They cover a variety of security areas, including continuous functional planning, system-on-access control, system development and maintenance, physical and environmental protection, compliance, personnel protection, organizational protection, computer and operations management, classification and control of assets as well as security and protection policy. Instrumentation for the implementation of these standard procedures is the complex of methods and tools for information security and CIS, structured in an organizational aspect. They are part of the general model for information security and CIS in organizations. The goal is to build a system for their guaranteed functioning, in the information storage and processing centres, communication networks and data transmission networks, as well as their monitoring and control. As a result of the accumulated experience, the protection methods are defined as activities for the protection of the information and elements of the CIS with the aim of preventing access to them. Methods of protecting CIS may include **restricting** and managing access to information and elements of CIS; coding (encryption) of information; **regulation** of access to information and elements of CIS. The essence and content of these methods are integrated and specified within subsystems for restricting and regulating access and subsystem crypto protection and protection from computer viruses and hackers [2, 3].

The subject of the research is the subsystem for restricting and regulating access to information and CIS in the organization.

The restriction and regulation of access to information and CIS is related to **unregulated access** to data in the organization. Unregulated access to the information and CIS may occur in the following cases:

- In direct contact with the objects of access;

- Creation and use of software and technical means of contact with the objects of access, by bypassing the means of protection;

- Modification of the means of protection so as to make contact with the objects of access;

- Implementation of mechanisms that disrupt the structure and functions of the technical or software means so that contact with the access objects is made.

We will focus specifically on the features related to the limitation and regulation of access to information and CIS in the organization.

2. Limiting unauthorized access to information in the organization

The restriction of unregulated access to information is ensured by:

- A system for distinguishing the subjects from the objects of access;

- Means of ensuring split access.

The system for distinguishing the subjects from the objects of access is related to:

- Introduction and implementation of rules for distinguishing the access of the subjects and their processes from the data;

- Implementation of rules for distinguishing the access of subjects and their processes from devices that generate copies of information media;

- Isolation of the programs and processes implemented in the interest of one subject from the others;

- Management of data flows in order to prevent records of data on media not conforming to the marking;

- Implementation of rules to control the exchange of data between CIS subjects.

The means of providing split access are connected to:

- Identification and recognition of subjects and maintenance of the relationship between them and the processes performed for them;

- Registration of the actions of the subjects and their processes;

- Provision of opportunities to exclude and include new subjects and objects of access and to change their rights;

- Reacting to unauthorized access attempts, for example, by signalling-blocking-recovery, after such an attempt;

- Testing;
- Clearing the operational memory and the working areas of the magnetic media after the end of the work of the users;
- • Report of the output printed, graphic and other forms of displaying the information;
- • Control over the overall program and informational part of the means for providing shared access.

There are several possible ways to limit unregulated access to information. More significant of them are:

- Construction of a distributed system for distinguishing access with a protection core built into the software and technical complex;
- Access differentiation system built into the operating system, DBMS or application programs;
- Embedding a system for distinguishing access in network management tools or at the application level;
- Using cryptographic conversions or direct access control methods;
- Software or technical implementation of an access differentiation system.

Technical means to limit unregulated access to information are characterized by the following:

- Degree, completeness and quality of the scope of rules for distinguishing access implemented in the system;
- Composition and quality of the means ensuring the system for distinguishing access;
- Guarantees for the correct functioning of a system for distinguishing access and providing means.

The completeness, quality and scope of the access differentiation rules are assessed by the presence of clear and consistent measures for reliable identification embedded in the access differentiation system. The possibilities of controlling the various access procedures are also considered.

When evaluating the quality of the access differentiation system, the means of identification of the subjects and the order of reporting the actions and the means of binding the subjects to the processes are taken into account. The effectiveness of access differentiation is evaluated by:

- The method of design and implementation of the access differentiation system and the means that provide it (formal and informal verification);
- The composition and quality of the means preventing the circumvention of the access differentiation system (integrity maintenance and recovery after failures, accidents and unauthorized access attempts, capabilities for testing, control and diagnostics during operation)

To improve access control, when the option is available, it is recommended to use multi-factor authentication for the products and services that the organization uses. In practice, this means that the following methods are used for each successful identification:

- something that is known, for example a username and password;
- something that is available (owned), for example, a code received on a registered mobile device, another application or e-mail, as well as an electronic identifier;
- something that is, for example, biometric data, usually a fingerprint.

It is also mandatory to use strong passwords.

Passwords are still a primary way to authenticate employees, but they are easy to guess and hack. A strong password is strictly personal (not shared), **complex** (a combination of uppercase letters, lowercase letters, a symbol and numbers) and **unique** (i.e. do not use the same password for other personal services, for example social networks or personal mail, where the password can be leaked on the Internet).

Passwords remain a major cybersecurity concern, and according to the The European Union Agency for Cybersecurity, ENISA, 56% of the time the same password is used for different services or products, while 44% of devices aren't even protected by a strong password.

A good practice and convenience for employees is to use a **password manager**, an application that generates unique strong passwords for each application/web address and stores them in a safe that can be unlocked with a single password. Then, the employee does not need to remember many and different passwords or use the same password in multiple sites.

It is recommended that employees be encouraged to use a passphrase. This not only ensures better protection, but also makes it easier to remember. Administrative passwords can be stored in special storage for emergency situations or to provide a backup if some of the administrators are unavailable. However, they must be kept in a secure location and accessible only to authorized personnel.

3. Regulating the access control to the information

One of the key levels in achieving limited, authorized access to an organization's data is the implementation of appropriate access control measures and tools. An organization must ensure that its computer network supports the ability to centrally enforce access control, of the type provided by modern network systems such as Microsoft Active Directory. This allows the organization to ensure that those who have access to its systems and data can be centrally managed and controlled. In this regard, appropriate software **measures and means of access control** are implemented, such as [4]:

- Software security, through access control levels to information;
- Modern software products to increase the level of protection of access to databases;
- Means of monitoring the traffic and testing for possible attacks;
- Software means to protect the server with the databases;
- Software products for regulating user access to databases;
- Software products for password management;
- Resources for distribution and management of users;
- Monitoring of active processes related to the database;
- Access management.

It should be noted that software measures and means of access control need to be examined consistently in future research

3. Conclusion

In conclusion, it can be summarized that the specified measures and techniques for limiting access to information and communication and information systems are only part of what must be planned and implemented. Such measures are carried out in the entire complex of organizational, administrative, programmatic, technical and physical means of protection

Acknowledgements

This publication was financed by the Ministry of Education and Science in implementation of the National Scientific Program – Security and Defence that is funded by Ministry of Education and Science of the Republic of Bulgaria in implementation of National Strategy for the Development of Scientific Research 2017-2030 and was adopted by Decision of the Council of Ministers No. 731 of October 21, 2021.

4. References

1. Jochen Rehrl and Galia Glume, Editors, Handbook on, CSDP Missions and Operations, the Common Security and Defence Policy of the European Union, ed. Jochen Rehrl and Galia Glume, Federal Ministry of Defence and Sports of the Republic of Austria, Published by: Directorate for Security Policy of the Federal Ministry of Defence and Sports of the Republic of Austria, Vienna/Austria, ISBN: 978-3-902275-42-4, Armed Forces Printing Centre, Vienna/Austria, 2015
2. Milena Ivanova, Veselina Aleksandrova, Sigurnost na informatsiyata i komunikatsionnitate i informatsionni sistemi s prilozhenie v otbranata na darzhavata i sigurnostta na obshtestvoto, Savremenni aspekti na sigurnostta – predizvikelstva, podhodi, reshenia, Godishna studentska nauchna sesia 27 septemvri 2023 g., s. 134-142, izd. Voenna akademija „Georgi Stoykov Rakovski“, izdatel, 2023 g., ISSN: 2738-7526. / Милена Иванова, Веселина Александрова, Сигурност на информацията и комуникационните и информационни системи с приложение в отбраната на държавата и сигурността на обществото, Съвременни аспекти на сигурността – предизвикателства, подходи, решения, Годишна студентска научна сесия 27 септември 2023 г., с. 134-142, изд. Военна академия „Георги Стойков Раковски“, издател, 2023 г., ISSN: 2738-7526.
3. Veselina Aleksandrova, Milena Ivanova, Violeta Vasileva, Technology for Organizing the Security of Information and Communication and Information Systems, In:Proceedings of the 11th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE – 2021), volume:100, Publishing Complex – UNWE, Sofia, Bulgaria, p. 305-310, ISSN 2367-7635 (PRINT), ISSN 2367-7643 (ONLINE), Issued for Publication: September 15TH, 2023, Indexed by EBSCO HOST, ProQuest, URL: <https://icaictsee.unwe.bg/past-conferences/ICAICTSEE-2021.pdf>
4. Petrov R., Osnovi na etichnoto hakerstvo, Izd. Infovizhan, 2019g, ISBN 978-619-7442-33-5. / Петров Р., Основи на етичното хакерство, Изд. Инфовижън, 2019г, ISBN 978-619-7442-33-5.