Abstracts of Dissertations

Institute of Information and Communication Technologies

BULGARIAN ACADEMY OF SCIENCES

1 / 2022

METHOD AND MODELS FOR DEVELOPMENT OF INFORMATION SECURITY SYSTEMS IN ORGANIZATIONS

Ivan Gaidarski

МЕТОД И МОДЕЛИ ЗА РАЗРАБОТКА НА СИСТЕМИ ЗА ИНФОРМАЦИОННА СИГУРНОСТ В ОРГАНИЗАЦИИ

Иван Гайдарски

Автореферати на дисертации

Институт по информационни и комуникационни технологии

БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ

ISSN: 1314-6351

Поредицата ***„Автореферати на дисертации на Института по информационни и комуникационни технологии при Българската академия на науките“*** *представя в електронен формат автореферати на дисертации за получаване на научната степен „Доктор на науките” или на образователната и научната степен „Доктор”, защитени в Института по информационни и комуникационни технологии при Българската академия на науките. Представените трудове отразяват нови научни и научно-приложни приноси в редица области на информационните и комуникационните технологии като Компютърни мрежи и архитектури, Паралелни алгоритми, Научни пресмятания, Лингвистично моделиране, Математически методи за обработка на сензорна информация, Информационни технологии в сигурността, Технологии за управление и обработка на знания, Грид-технологии и приложения, Оптимизация и вземане на решения, Обработка на сигнали и разпознаване на образи, Интелигентни системи, Информационни процеси и системи, Вградени интелигентни технологии, Йерархични системи, Комуникационни системи и услуги и др.*

The series ***Abstracts of Dissertations of the Institute of Information and Communication Technologies at the Bulgarian Academy of Sciences*** *presents in an electronic format the abstracts of Doctor of Sciences and PhD dissertations defended in the Institute of Information and Communication Technologies at the Bulgarian Academy of Sciences. The studies provide new original results in such areas of Information and Communication Technologies as Computer Networks and Architectures, Parallel Algorithms, Scientific Computations, Linguistic Modelling, Mathematical Methods for Sensor Data Processing, Information Technologies for Security, Technologies for Knowledge management and processing, Grid Technologies and Applications, Optimization and Decision Making, Signal Processing and Pattern Recognition, Information Processing and Systems, Intelligent Systems, Embedded Intelligent Technologies, Hierarchical Systems, Communication Systems and Services, etc.*

Редактори

Геннадий Агре
Институт по информационни и комуникационни технологии, Българска академия на науките
E-mail: agre@iinf.bas.bg

Райна Георгиева
Институт по информационни и комуникационни технологии, Българска академия на
E-mail: rayna@parallel.bas.bg

Даниела Борисова
Институт по информационни и комуникационни технологии, Българска академия на науките
E-mail: dborissova@iit.bas.bg

Editors

Gennady Agre
Institute of Information and Communication Technologies, Bulgarian Academy of Sciences
E-mail: agre@iinf.bas.bg

Rayna Georgieva
Institute of Information and Communication Technologies, Bulgarian Academy of Sciences
E-mail: rayna@parallel.bas.bg

Daniela Borissova
Institute of Information and Communication Technologies, Bulgarian Academy of Sciences
E-mail: dborissova@iit.bas.bg

e-ISSN: 1314-6351

BULGARIAN ACADEMY OF SCIENCES

Abstract of PhD Thesis

METHOD AND MODELS FOR DEVELOPMENT OF INFORMATIION SECURITY SYSTEMS IN ORGANIZATIONS

Ivan Kostadinov Gaidarski

Supervisor: Assoc. Prof. Rumen Andreev

Approved by Supervising Committee:

Prof. Ivan Garvanov
Prof. Radoslav Yoshinov
Prof. Rumen Trifonov
Prof. Todor Tagarev
Assoc. Prof. Svetozar Ilchev

IICT

INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Department of Communication Systems and Services

GENERAL DESCRIPTION OF THE PH.D. THESIS

Research topic and motivation

Information is one of the most valuable assets of modern organizations. Intellectual property, know-how, patents, customer and supplier lists - this information is vital for any organization and forms its competitive advantage. One of the most important challenges facing them is the protection of information in all its forms - electronic and physical. The information must be reliably protected both from external attacks - hackers or natural disasters, and from internal - current and former employees, partners and suppliers. Their right of access to the organization's resources such as systems, networks and data requires protection against unauthorized leakage of information to comply with new strategy, different from that of traditional protection against external threats to the organization [1, 2].

The main threats today are related to data and information assets. The more valuable the assets, the more attacks they are exposed to. New and existing vulnerabilities lead to higher attack success rates. Therefore, threats are highly dependent on the vulnerabilities that can be exploited by the attacking party. Any change in one of the factors leads to an increase in its scope. For example, increasing the capabilities of threat agents, respectively, leads to more successful identification and exploitation of vulnerabilities, and consequently to greater success of attacks [25]. The introduction of new information assets leads to an increase in the area under attack, respectively to new weaknesses / vulnerabilities, new methods of attack and new threats. The introduction of the latest technological innovations leads to weaknesses that are related to technological immaturity, improper use and improper integration with existing systems, low consumer awareness and more. This creates the ground for new threats to these assets [25]. In order to reduce successful attacks on information assets, it is necessary to perform an analysis of all elements in the chain of vulnerabilities-threats - attacks.

The organizations create, adopt and approve a unified security policy, procedures and processes for information security. They are the result of the influence of various factors - the territory in which the organization operates, regulatory regimes, sector-specific requirements, standards and good practices. One of the main factors that the organization must comply with is the national legislation in force in the territory of the country in which it is registered or operates - tax legislation, penal code, permit regimes and others. In the aspect of Information Security Systems (ISS), in the field of our interest are the normative acts, forming the basis of the state policy in the field of cyber security - cyber security, cyber defense activities and counteraction to cybercrime [57].

Information security uses a number of security approaches, each of which has a specific area of application that answers the question "Where?" And a certain functionality - "How?". For example, we can use the multilayer security model, consisting of several layers - external network, network perimeter, internal network, computer equipment, applications and data. Each protective layer is exposed to different threats and has a certain set of security approaches to protect against them. For the complex protection of the organization the approaches for information protection in network communication and the approaches for data protection in hierarchical organizational communication are combined. To our familiar approaches to information security in network communications we can add additional approaches, such as demilitarized zone, virtual private network, audit, penetration tests, vulnerability analysis, password hashing, filtering and others [29].

Each of these approaches has its role and peculiarities in the protection of certain assets, located in a certain layer and requiring certain efforts and resources. Information security (IS) is concerned with ensuring the security of these assets. The best approach to

this is to consider each asset in the context of the associated risk of loss and its value. The main goal of IS is to protect information in all its forms. As a result of the pervasive penetration of information technology, information security is relevant to more and more aspects of modern life, such as production, workflow, daily communication, shopping or entertainment [29]. The same applies to the vital sites of the critical infrastructure, providing electricity, water, telecommunications and transportation. They are entirely dependent on information technology and, above all, on ensuring its security [33]. Information security refers to the protection of assets - information, hardware, software, processes or combinations thereof. In order to assess what to protect, it is first necessary to determine which assets are valuable and for whom [4].

IS is a continuous process of aligning risk with the business objectives of the organization and minimizing residual risk. Organizations need to develop a comprehensive, risk-based IS strategy to protect their sensitive information. The development of effective information security systems requires a good knowledge of a number of scientific and scientifically applied areas such as Information Security and Cyber Security, Systems Design, Data Analysis, Large Data Arrays, Software Engineering and Systems Analysis. The methods and principles of these areas are particularly useful for developing an effective information security system that protects sensitive data.

The development and subsequent implementation of a modern information security system (ISS) is essential for the viability of the modern organization, which, in addition to ensuring the protection of its assets, is necessary to comply with a number of regulatory requirements, good practices and standards.

Objective and tasks of the Ph.D. Thesis

The objective of the dissertation is to create a method and models for development of information security systems, providing protection from internal threats (inside out direction) of sensitive information for different in nature and size organizations. The developed method should be applicable for the creation of ISS, implementing an approach for protection of sensitive data with Data Leak Prevention (DLP) solutions, suitable for application in organizations of different sizes, such as critical infrastructure, enterprises handling industrial secrets, trade or research organizations.

To achieve this goal, the following tasks have been formulated, which are in line with the different stages of ISS development:

1. Defining and classifying approaches for information security management and areas of application;
2. Analysis of the field of Information Security as part of the problem area of the Information Security System;
3. Description of the problem area of Information Security Systems in organizations through conceptual modeling;
4. Analysis and application of object-oriented approach in creating a project model of an information security system based on a conceptual model;
5. Defining an approach for transformation of the ISS project model into an implementation model;
6. Simulation of ISS and analysis of the generated test data

Methodology

To achieve the goals and objectives formulated in the dissertation, an object-oriented approach is used in the design and implementation of top-down software systems. This is a methodology widely used by software engineers, which aims to avoid dependence on the specific technical means included in the system and formulates a development method that achieves a high degree of formalization. The achieved result is usually a step towards achieving a reference model for creating a software system in a particular field.

List of publications

The publications on the dissertation have been reported and accepted for publication in the proceedings of three international conferences, one in specialized international journal with impact factor and one in an edition of an international academic publishing house.

[1] Gaidarski I., Model Driven Development of Information Security System, Problems Of Engineering Cybernetics And Robotics, Bulgarian Academy Of Sciences, 2021, Vol. 76, pp. 47-62, p-ISSN: 2738-7356; e-ISSN: 2738-7364, DOI: 10.7546/PECR.76.21.04

[2] Gaydarski, I., Minchev, Z., Andreev, R.. Model Driven Architectural Design of Information Security System. Advances in Intelligent Systems and Computing, Madureira A., Abraham A., Gandhi N., Silva C., Antunes M. (eds) Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018)., 492, Springer, 2019, ISBN:978-3-030-17064-6, ISSN:2194-5357, DOI:10.1007/978-3-030-17065-3_35, 349-359.

[3] Gaydarski, I., Minchev, Z., Conceptual Modeling of Information Security System and Its Validation Through DLP Systems. Proceedings of BISEC 2017, Belgrade Metropolitan University, 2017, ISBN:978-86-89755-14-5, DOI: 10.13140/RG.2.2.32836.53123, 36-40

[4] Gaydarski, I., Minchev, Z.. Virtual Enterprise Data Protection: Framework Implementation with Practical Validation. Proceedings of BISEC 2018, October 20, Belgrade, Serbia, Belgrade Metropolitan University, 2019, ISBN:978-86-89755-17-6, DOI:10.13140/RG.2.2.19996.33925, 10-15

[5] Gaydarski I., Kutinchev P., Holistic Approach to Data protection - identifying the weak points in the organization.. Proceedings of BdKCSE'2017 (7 December, 2017 Sofia), САИ, 2018, ISSN:2367-6450, 125-135

Project participation

As part of the development of the dissertation, the PhD student took part in the following research projects:

1. Research project on the topic: "Conceptual and simulation Modeling of Ecosystems for the Internet of Things (CoMEIN)", Contract H DN 02/1 of 13.12.2016, Competition for funding basic research - 2016, Mathematical sciences and informatics;

2. Program "Young Scientists and Doctoral Students at BAS" 2017, Research Department "Information and Communication Sciences and Technologies", Research Project ent. № 72-00-40-230 / 10.05.2017 on the topic "Modeling of architecture of information security systems in organizations." Contract N: DFNP – 17-101 / 28.07.2017. Funding: Program for support of young scientists and doctoral students of BAS-2017.

3. Research project on the topic: "Information and communication technologies for a

digital single market in science, education and security (ICTNOS)", Contract N: DO1-205 / 23.11.2018

Scientific and Scientific-applied contributions

1. A new classification of IS management approaches is proposed, depending on the type of communication and a detailed description of the foundation in the field of information security, based on its basic concepts;
2. A new method for developing information security systems in organizations has been proposed, which integrates model-based development of ISS by applying a top-down approach with a new method for analyzing the problem area of this type of systems. Characteristic of the proposed method is that it is technologically independent / condition to serve as a basis for creating a reference methodology for developing this type of systems /; flexible / allows expansion of an existing SIS with new functionality /; supports the interoperability of the SIS with an organization's existing information system by using the same approach to modeling both systems;
3. A multi-layered conceptual model of the problem area of information security systems has been developed as result of the application of two or more points of view in its description;
4. Architectural and functional models of information security systems have been constructed on the basis of an existing conceptual model of the problem space with the help of the object-oriented unified language for description of UML software systems;
5. Comparative analysis of existing DLP platforms for implementation based on the requirements described in the analysis model;
6. A model for the implementation of ISS in an organization using the DLP implementation platform "Cososys Endpoint Protector 5.0.2.1" is proposed
7. A simulation model of ISS based on object-oriented description of its architecture has been implemented using agent-based representation in NetLogo and I-SCIP-SA environments; Simulation study of ISS architecture by performing stochastic validation and interactive verification

Dissertation structure

The full volume of the PhD Thesis is 142 pages. It consists of an introduction, four chapters and a conclusion, a declaration of originality of the results, a bibliography and appendices. The dissertation includes 48 figures, 13 tables, 139 cited literature sources and 2 appendices.

The introduction addresses the actuality of the problem, the main threats in cyberspace, regulations and legal frameworks.

Chapter 1 presents the basic concepts and basic principles for providing information security (IS). Different approaches to IS management, the areas of their application, as well as the main scientific areas relevant for the development of IS systems are discussed. Our method for developing information security systems in organizations, the phases of which it consists, the models that are constructed in its application and its characteristics are presented. A framework for describing the architecture of the system is defined. The main goal and tasks of the dissertation are formulated.

Chapter 2 defines the basic concepts in IS by using our method for analysis in the field

of ISS, which takes into account the views of all stakeholders in its development. The aim is to apply the top-down approach when designing such a system, which makes it possible to reach solutions that are not related to a specific implementation and can be guiding in creating systems of this type. As a result, the analysis is the basis for creating a conceptual model of the problem area of the ISS.

Chapter 3 presents a presented method for designing an Information Security System, designed for organizations and aimed at protection against leakage of sensitive information from the inside out, ie. as a result of the actions of insiders with legitimate access to the resources of the organization and its data. The possibilities of object-oriented approach for creating a project model of ISS are considered. A way to transform the ISS conceptual model into an object-oriented design model by using the object-oriented UML description language is shown.

Chapter 4 describes an approach for creating a model for the implementation of the ISS through our proposed methodology for development of ISS. On the basis of a project object-oriented (OO) model, an OO realization model has been built, in accordance with the existing environment. An analysis of the problem area has been performed and based on the developed conceptual model, as a result of this analysis, the requirements to the architecture of the developed ISS have been specified. An analysis of existing DLP implementation platforms was performed and the most appropriate one was selected in accordance with the analysis model. It is shown how the method presented by us allows for modeling and implementation of new aspects of ISS without having to design the system from scratch. The results of tests of the extended ISS are also presented. An agent-based simulation model has been created by transforming an object-oriented project model. Based on the agent-based model, the operation of the ISS was simulated using the NetLogo (v.6.0.4) and I-SCIP-SA simulation environments. An analysis was performed on the basis of test data, as well as data from real situations.

Introduction

The introduction consists of the topicality of the problem and the main threats in IS. The current directions for research of threats in cyberspace, as well as security threats in the present and last year are considered. An overview of the main regulations and legal frameworks in the field of information security - an unified security policy, procedures, processes and standards for IS, adopted in organizations in order to comply with regulatory and legal requirements, standards and good practices for IS. An overview of the national legislation in the field of IS, operating in the territory of the state in which it is registered or operates - tax legislation, penal code, permit regimes. The structure of the dissertation is shown.

Chapter 1. Basic principles and method for development of information security system

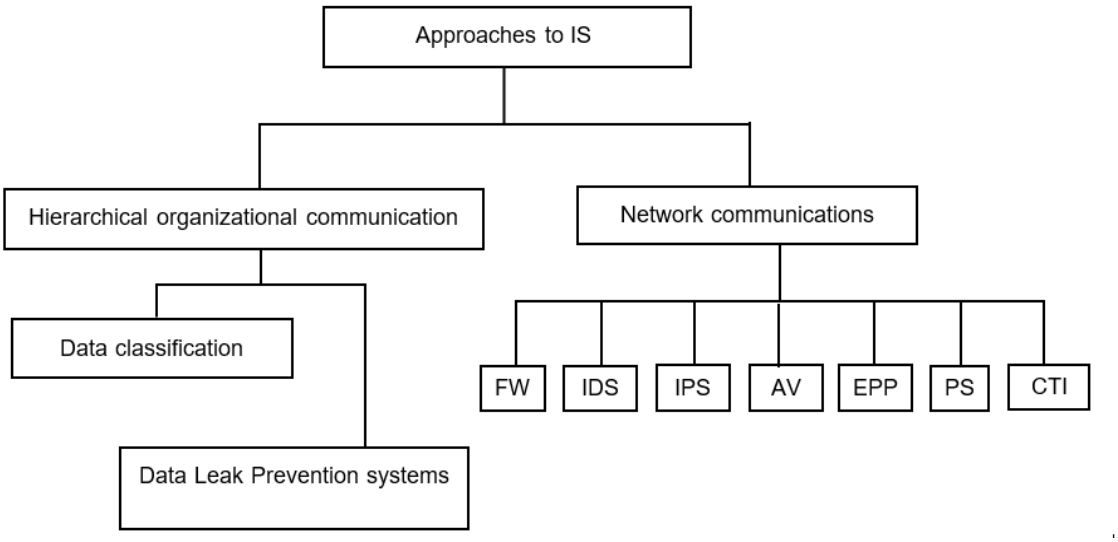
1.1 Basic principles for ensuring information security

This section presents the importance of the problems, related with information security and data protection, legal frameworks and regulations, providing IS, as well as the basic principles and security models for ensuring IS in an organization. We are discussing the major threats in cyberspace, the current threats for 2020 and 2021, and basic principles of IS, known as: Triad "Confidentiality, Integrity, Availability" (CIA Triad), the triple A (AAA) and the weakest link principles. We also consider basic protection models, such as perimeter protection, known as the "Lollipop model" and multi-layer model, known as "Onion model".

[2,21].

1.2 Approaches to information security management

In this subsection we systematize the existing approaches to IS in organizations, depending on the type of communication within the organization. We distinguish 2 types of communication: Network communications and Hierarchical organizational communication (Figure 3):



. Figure 3. Approaches to IS depending on the type of communication

1.3 Areas of application of the different approaches to information security

In this subsection we also consider the areas of application of the different approaches to protection. To illustrate, we use the multilayer protection model (Figure 2), consisting of several layers:

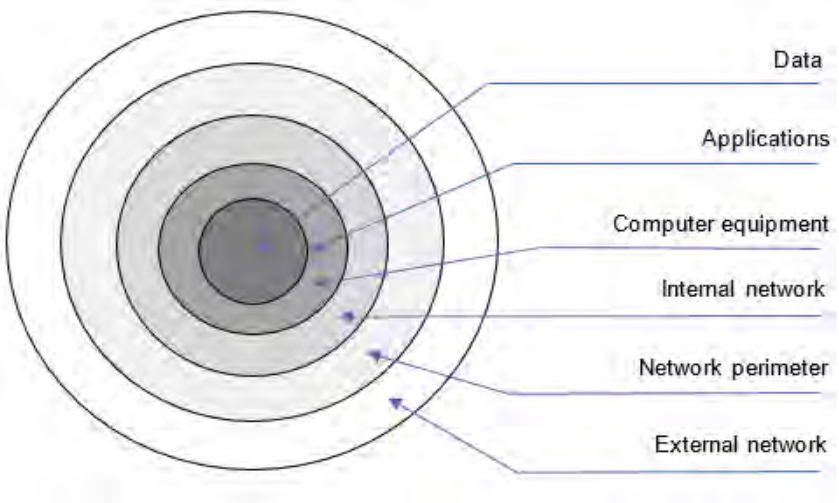


Figure 4. Multilayer protection model

Each protective layer is exposed to different threats and has a certain set of security approaches to protect against them (Table 1).

Areas of application	Approaches for IS
External network	Demilitarized Zone, Virtual Private Network, Logging, Audit, Penetration Tests, Vulnerability Analysis
Network perimeter	Firewall, Proxy Server, Logging, Packet Filtering, Static Packet Filtering, Dynamic Packet Filtering, Penetration Tests, Vulnerability Analysis
Internal network	IDS, IPS, Logging, Audit, Penetration Tests, Vulnerability Analysis.
Computer equipment	Authentication, Endpoint protection, Firewall, Password hashing, Logging, Audit, Penetration tests, Vulnerability analysis, DLP.
Applications	Content filtering, Data validation, Audit, Penetration tests, Vulnerability analysis, Data Classification
Data	Encryption, Access control, Data archiving, Penetration tests, Vulnerability analysis, Data classification, DLP.

Table 1. Security approaches and areas of application

For the complex protection of the organization's assets, the approaches for information protection in network communication and the approaches for data protection in hierarchical organizational communication are combined. In addition to the already known firewalls, IDS, IPS, Anti Virus, Endpoint Protection, Perimeter Security and Cyber Threat Intelligence, DLP and Data Classification, several additional security approaches have been added [29]: Demilitarized zone (DMZ), Virtual private network (VPN), Logging, Auditing, Penetration Testing, Vulnerability Analysis, Proxy, Packet Filtering, Static packet Filtering, Dynamic Packet Filtering (Dynamic packet Filtering), Password Hashing, Content Filtering, Data Validation, Encryption, Access Controls, Backups, etc.

1.4 Main scientific areas of importance for the development of information security systems

Here we look at the main scientific areas, needed to develop effective ISS: Cyber security, Systems design, Data analysis, Large data sets, Machine learning, Artificial Inteligence, Software engineering, System analysis.

Areas such as software engineering and systems analysis, the principles of which we use for our method for development ISS in organizations, are discussed in details. Particular attention is paid to the system development process (Figure 5), consisting of the main components and the links between them, considered in the context of ISS development:

- Problem area - defines the area in which the ISS problem is solved;
- Problem - implementation of a certain way of functioning of the ISS, which must work in a given environment;
- Implementation environment - represents the conditions under which the ISS is implemented;
- Stages - These are the stages through which the development of the ISS must pass;

- Creation of ISS models at different stages of development;
- Model transformation from one type to another.

The following stages of ISS development are distinguished:

- Collection of requirements - identification of possible risks, according to the understanding of consumers;
- Analysis - study of the problem area from the different perspectives of stakeholders;
- Design - design of the structure and processes in the system;
- Implementation - compliance of the ISS implementation with the specific implementation environment.

The models through the transformation of which the realization of a specific ISS is achieved are:

- A model for describing the risk that is managed by the ISS, based on the collected requirements to the system;
- ISS area model - a model obtained as a result of the analysis of the problem area;
- ISS design model - description of the architecture and functionality;
- Implementation model - implementation model of the designed ISS depending on the conditions under which it will operate.

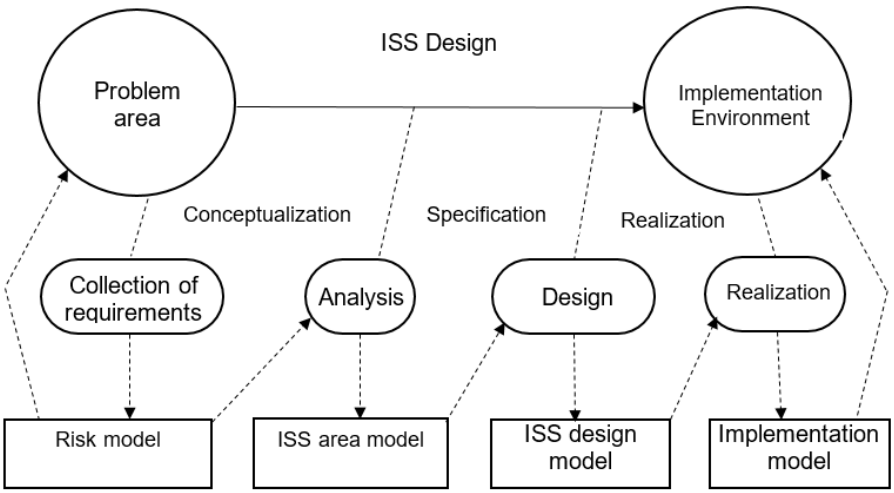


Figure 5. Systems development cycle

1.5 Method for development of information security systems in organizations

The method consists of the following phases (Figure 6):

1. Defining a framework for describing the ISS architecture, according to IEEE 1471 [67, 88, 89] and IEEE 42010 [67, 89] standards. The framework is formed from the many perspectives of stakeholders / observers.

2. Analysis of the problem area of the ISS, to determine the requirements for the system from different points of view. Based on this analysis, the requirements for the ISS are formed.

3. Building a conceptual model of the problem area from different points of view. Creating generalized and detailed conceptual models.

4. Integration of conceptual models created from different perspectives. The conceptual modeling approach allows easy and unified presentation at the level of ISS concepts from different points of view. This facilitates communication between the observers of the developed ISS, who are related to the respective points of view.

5. Transformation of a conceptual model of the problem area into an object-oriented project model.

6. Aspect-oriented transformation of design model into an object-oriented realization model and an agent-based simulation model.

The models that are constructed using the method are shown in Figure 7 [135,136]. Based on the analysis of the problem area, a conceptual model called "Guiding Model" is constructed, through which the desired system architecture is presented. The supporting model is not related to a specific implementation, but serves to describe the main components of the system architecture. The conceptual model reflects the problem area from different points of view. In turn, this model consists of a "Generalized Model" and a "Detailed Model".

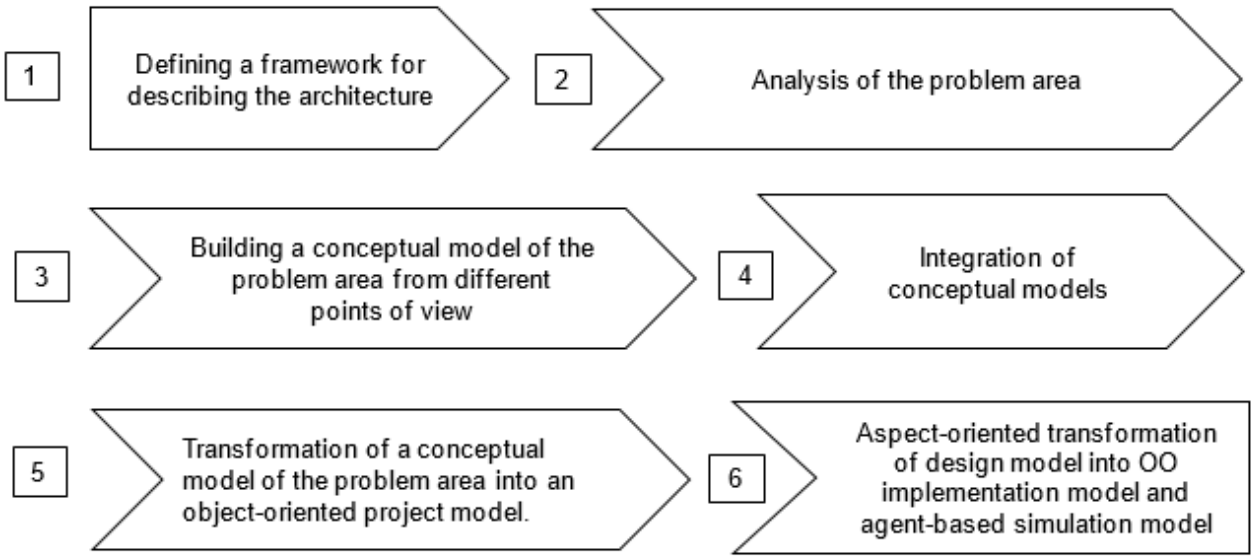
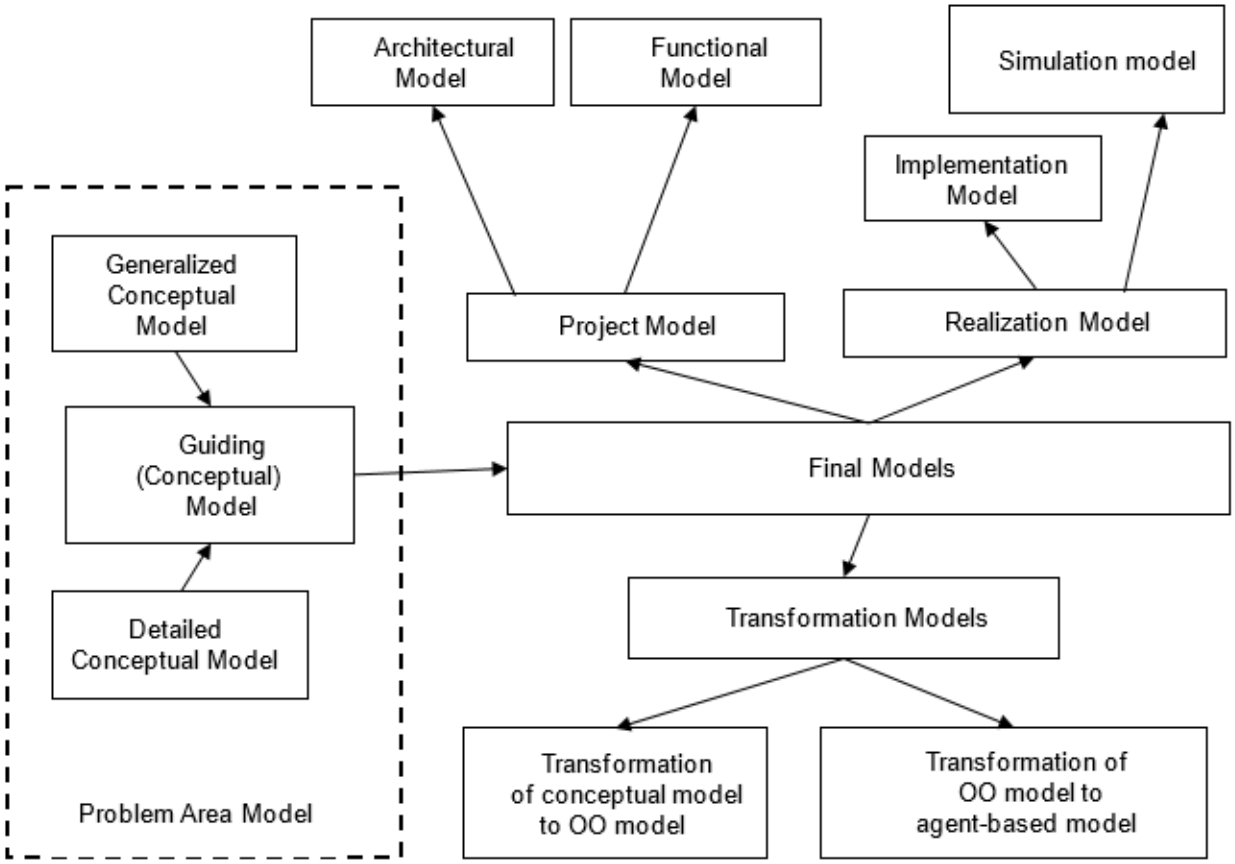


Figure 6. Method for development of ISS

Based on it, after a corresponding transformation, the following two main models are created - "Project Model" and "Realization Model". The Project model is object-oriented and consists of "Architectural" and "Functional" models, which present the description, respectively of the architecture and functionality of the system. "Realization model" represents a specific implementation of the system and can be done in two ways - by simulating a real system ("Simulation model") and by using specific existing systems, representing an environment for the implementation of ISS such as DLP ("Implementation Model"). The project model and the implementation model are representatives of the final models, which describe the system for the purposes of its development. Through the transformation models, the transformations between the models are presented - "Transformation of a conceptual model to an OO model" and "Transformation of an OO model to an agent-based model".



Fugure 7. Models for ISS development

Characteristics of the method:

- The method is model-based, as a result of applying a top-down approach;
- Model-to-model transformation is applied;
- Aspect-oriented transformation of a project model to an reazlization model depending on two areas of interest of the system implementer: object-oriented approach and agent-based approach.
- Technologically independent, which creates conditions to be the basis of a reference methodology for the development of ISS

The top-down approach, which is applied in the development of an information security system, is an “from the general to the specific” approach. It makes possible to implement and review common IS policies, procedures and processes in order to achieve certain objectives. It is suitable for establishing a reference methodology for the development of ISS, based on a framework for their design, as it is technologically independent.

1.6 Defining a framework for describing the system architecture

The implementation of the first stage is based on the guidelines for creating a framework for architectural description of systems presented in the standards IEEE 1471 [88] and ISO / IEC / IEEE 42010 [89].

These standards introduce concepts related to how to describe the architecture of a system [67]: Environment, Stakeholder, Concern, View, Viewpoint, Architecture of the system (System Architecture), Architectural description, Architectural framework, Architectural View, Architectural Viewpoint, Model kind.

These concepts are applicable in the analysis of the field "Information Security System" and provide a context for defining a common conceptual framework, allowing the

construction of conceptual models of ISS. Figure 8 shows the area of interest of the ISS, which is used as a framework for the analysis of the field of Information Security system in the present dissertation.

The development of complex systems involves many participants - each with their own perspective. These are the so-called "stakeholders". Each stakeholder has relevant skills, responsibilities, knowledge and experience that determine the attitude and requirements of the system. In a system that uses different technologies (software, hardware) and has a variety of regulatory and regulatory requirements, it is inevitable to intersect or overlap the different perspectives of the participants in the process of its development. An additional complicating circumstance is the fact that the knowledge of stakeholders is presented in different ways. The different requirements apply to different stages of the system development and each of them can be subject to different strategies. Thus, one of the important tasks in the process of system development is the coordination of stakeholders and the unified presentation of their requirements and contributions to the system. This problem is solved through our proposed method for developing information security systems in organizations as shown in Fig. 8.

Figure 8. ISS area of interest

The method takes into account and unifies the requirements of the various elements and viewpoints in the field of interest of the ISS, which we consider:

- "Information Security" Viewpoint - includes the basic concepts in information security (Threats, Vulnerabilities, Sources, Motivation, etc.), as well as the main approaches to the implementation of information security in organizations;
- "Risk analysis" Viewpoint - through risk analysis the requirements to ISS are determined;
- Communication Viewpoint - determines the way of communication, predetermining the approach to information protection;
- Technological Viewpoint. This Viewpoint includes different approaches in information and communication technologies such as object-oriented approach, agent-based approach and others..
- “Processing of Information” Viewpoint - including the three main types of data defined according to information security - Data-in-Rest, Data-in-Motion and Data-in-Use.

1.8 Conclusion

The chapter presents the basic principles and security models for ensuring information security. The presented approaches for IS management in organizations are divided into

two groups, depending on the type of communication in the organization, predetermining the respective approaches for IS: communication on the basis of equality - "Network communication" (Networks from/in organizations) and "Hierarchical organizational communication". The areas of application of the different approaches to information security are shown.

The main scientific fields of importance for the development of information security systems are presented. Special attention is paid to systems analysis and the system development cycle. The main components and connections between them are considered in the context of ISS development.

A framework for architectural description of systems based on IEEE 1471 and ISO / IEC / IEEE 42010 standards is presented.

The main goal and tasks of the dissertation are defined.

Chapter 1 describes the implementation of task 1, defined in "Objective and tasks of the Ph.D. Thesis": 1. Defining and classifying approaches for information security management and areas of application;

As a result of the research activity the following scientific and scientific-applied contributions have been achieved:

1. Classification of IS management approaches, depending on the type of communication.
2. A new method for developing information security systems in organizations is proposed, which is model-based. It is the result of the application of the top-down approach, i.e. from the general to the particular. Characteristic of the proposed method is that it is technologically independent, which allows it to serve as a basis for a reference methodology for the development of ISS

Chapter 2 Problem area analysis

2.1 Information security - basic concepts and approaches for implementation

In this point the basic concepts and approaches for realization of IS are considered.

2.1.1 Basic concepts in information security

Here we present the foundation of the field of information security, described through its basic concepts (Figure 9).

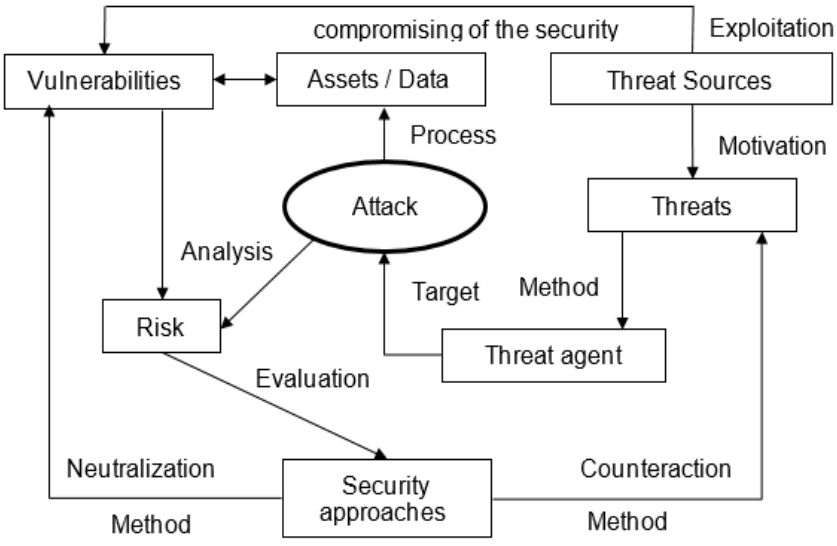


Figure 9. Vulnerabilities, threats and attacks

We define the basic concepts of IS: "Event", "Signals / Alarms", "Incident", "Breach", "Vulnerability", "Threat", "Threat Agent" , "Attack", "Data Breaches", "Data Loss".

2.1.2 Vulnerabilities. Threats. Sources and agents of the threat

This subsection examines in detail the terms "Vulnerabilities", "Threats", "Sources" and "Threat Agents" and their relationship.

2.1.3 Vectors, targets and nature of the threat

The terms "Vector", "Purpose" and "Character of the threat" are considered here. According to the threat vector, threats can be classified into external and internal.

"**External threats**"
The vector of the attack on external threats is “outside – in”, against the protected information assets. In the external threats is used the principle of the weakest link. The attacking party tries to find security vulnerabilities through which it can penetrate the secure network, servers or workstations and to take control of the information. Examples here are: Hacker Attacks, DoS Attacks, Worms, Trojans, Botnet, DoS and DDoS Attacks, Drive-by Exploits, and Code Injection (Code Injection Attacks) [25].

"**Internal threats**"
An incident caused by an internal threat occurs when an insider - employee, partner or third party provider with authorized access to information or systems, sensitive to the organization, intentionally or accidentally misuses this access, leading to negative consequences for the organization. There are many causes for incidents involving internal threats:

- Careless behavior of the insiders;
- Suppliers and external contractors;
- Too strict cybersecurity policies, leading to "Security Fatigue";
- Theft of electronic identity;
- Malicious users.

Internal threats can be divided into several main groups according to their source: Human Threat, User Activity, and Business Applications

2.1.4 Attacks and counteraction

In this subsection the categories of attacks, their mechanism and the approaches for their neutralization are considered in detail.

2.1.5 Approaches to Information security

Approaches to Information Security (AIS) are measures in the form of actions, processes or procedures taken to protect the information system from attacks on the Confidentiality, Integrity and Availability of the information system. The aim is to reduce the risk associated with information security [12]. The approaches are organizational, technological and technical, and are applied in accordance with the specifics of the Entity's activity [15] (Ordinance on the minimum requirements for network and information security). According to the time of its action, AIS can be logically grouped into several categories [2, 12, 13]: Preventive, Disclosure, Deterrent, Corrective, Restorative and Compensatory. AIS can have different physical realizations [2,12,13,14]: AIS for physical security, Administrative, Technological, Operational and Virtual.

2.2 Risk analysis

In this section we consider the concepts of risk, risk management, risk assessment and risk assessment methods. As part of the risk assessment, the processes of identifying threats and vulnerabilities and assessing assets are also considered. Risk suppression

processes and a periodic assessment process are also described.

2.3 Types of communications

Here are the types of communication in the organization in terms of approaches to implementation:

- *"Hierarchical organizational communication"*- communication within an organization based on the hierarchical structure of the organization;
- "*Network communication*" - communication that ensures equality between its participants.

Depending on the specifics of the two types of communication, different approaches to information security are used. In this dissertation the hierarchical organizational communication and the respective approaches for protection through Data Leak Prevention Systems (DLP), are considered.

From "Communication" viewpoint procedures and their formalization, formal and informal communication are distinguished as:

- *Formal communication* follows both the hierarchical structure of the organization and the horizontal communication between employees. It complies with set patterns specific to the organization, with priority given to messages sent by management down the structure;
- *Informal communication* is the daily communication between employees. It does not follow set patterns or a strict hierarchy, but it is vital to the organization because it carries out daily tasks.

2.4 Technological viewpoint in ISS design

In this subsection we consider different technological approaches for the development of an information security system: Object-oriented approach, Agent-based approach and Multi-agent systems.

2.5 Processing of Information viewpoint

Here we taking a look at the types of data processed, used and created by organizations. Each organization individually determines which data are vital to its functioning and which are secondary or supporting. By definition, sensitive data is data that an organization cannot afford to lose, disclose, or make available to unauthorized persons.

Depending on how the data is used, stored or transferred by the different systems and applications, 3 main states of the data are distinguished:

- Data at rest;
- Data in motion;
- Data in use.

2.6 Conclusion

The presented analysis in the field of information security systems is part of the applied approach for the development of such systems, known as "top-down". It provides an opportunity to review and implement common IS policies, procedures and processes in order to achieve certain objectives. It is suitable for creating a reference methodology for the development of ISS, based on defining a framework for their design.

An attempt has been made to make a comprehensive view of the ISS from several viewpoints: Information Security, Risk Analysis, Processing of Information, the appropriate

computer technology for system development and possible types of communication - object of information protection. Each viewpoint represents a perspective in which the area of existence of the system must be considered. The field of information security is described with the greatest attention and in the most detail, as it is the foundation of the information security systems.

Chapter 2 describes the implementation of task 2, defined in “Objective and tasks of the Ph.D. Thesis”: 2. Analysis of the field of Information Security as part of the problem area of the Information Security System;

As a result of the research activity for definition and classification of approaches for information security management and in the analysis of information security as a part of the field of information security systems the following scientific and scientific-applied contributions are achieved:

1. A new method for analysis of the field of information security systems has been created and applied.
2. A new approach for analysis of the problem area of the information security systems has been developed and applied;
3. A new detailed description of the foundation of the field of information security is presented, based on its basic concepts.

Chapter 3 Design of information security system in organizations. Analysis model. Project model.

The development of the ISS goes through the following stages (Figure 5):

1. Clarification of the requirements for the ISS,
2. System analysis of the requirements and construction of a model of the analysis coinciding with the model of the problem area
3. Creation of a ISS project model,
4. Building a realization model.

This subsection presents the process of defining a system framework for describing the ISS architecture. The system framework for defining the problem area of the ISS and subsequently the system architecture defines the boundaries within which the system is developed. The reference methodology for the development of ISS, proposed by us, is based on the framework for architectural description of software systems, described in the standards IEEE 1471 and IEEE 42010.

The architectural description marks the beginning of the creation of a ISS design model. It is used in the implementation of a real ISS, in the design of which the requirements of the different viewpoints in the field of interest of the ISS are taken into account and unified. The basic concepts underlying the framework for analysis of the field of ISS are presented in item 1.6 - Environment, Stakeholder, Area of interest, View, Perspective, System architecture, Architectural description, Framework for creating architectural description, Architectural view, Architectural point of view, Type of model are applicable in the analysis of the field Information Security. They define the general conceptual framework, allowing a multifaceted description of the problem area and defining the ISS architecture by using the potential of conceptual modeling [99, 100, 101].

3.1.1 Description of the approach

The essence of our approach is first to create a generalized model, and then on its basis and a detailed model of the problem area of the ISS. Thus, we disregard unnecessary

details and focus on the essential characteristics of the system. The process of conceptual modeling depends on the framework in which the basic concepts are formed.

Some of the requirements for the ISS are formed by the environment, which determines the conditions under which it will operate. These requirements are defined on the basis of our proposed method for analysis of the Problem Area and define a model of analysis. This analysis takes into account the views of all stakeholders in the development of the ISS, ensuring the complexity of IS approaches. The model of the problem area coincides with the model of the analysis. This model represents the desired system architecture. A distinction must be made between the architecture of the system and the description of the architecture, ie. Architectural model. While the definition of the system architecture reflects the model of the analysis, the architectural model is part of the design model.

For the purposes of designing on the basis of a created conceptual model, a description of the architecture and functionality of the ISS, which are components of the Project Model, is constructed. The construction of the Project Model is based on the use of object-oriented approach and object-oriented description language Unified Modeling Language (UML), providing tools for describing, analyzing, modeling and documenting the architecture and functionality of ISS [97, 98].

The project model consists of architectural model and functional model, described with the corresponding diagrams in UML. In constructing this model, the conceptual model is transformed into an object-oriented project model. The realization model can be implemented in two ways - through an agent approach, allowing simulation of the real system, or through the use of specific existing systems, representing an environment for the implementation of the ISS. Examples include DLP systems such as DeviceLock [95] and Cososys Endpoint Protector [96].

3.2 Analysis model

At this point, the creation of the analysis model is presented. The system is designed in a given Problem Area (PA) in which the problems and tasks for implementation by the ISS are presented. As result of the analysis of the PA, a description of the problem area is reached and a Model of the problem area (MPA) is created. MPA is essentially a model of the Analysis. The MPA and the analysis model are equivalent. This model represents the desired system architecture.

The following requirements are set for the ISS model of the problem area:

1. In accordance with the way of forming concepts, the conceptual modeling predetermines at least two stages in creating the MPA: construction of generalized model and construction of a detailed model;

2. The architecture of the ISS must correspond to the description of the Problem Area, where the tasks to be performed by the system are defined;

The result of using conceptual modeling in creating a Model of Analysis is a conceptual model, which is essentially an abstraction. Each concept is considered as a separate component. Therefore, this model also represents the architecture of the ISS.

3.2.1 Generalized model of the ISS problem area

As a result of the analysis of the problem area of the ISS, it can be summarized that the most important questions that a system must answer from the viewpoint of information security are: "What do we protect?", "Why do we protect?", "How are we protecting?" and "Where are we protecting?". The system framework for presenting the architecture of the ISS is essential for the development of the system because it identifies the main components needed to achieve its objectives [20, 125].

The components of the generalized model coincide with the tasks of the designed information security system. They reflect the relevant elements of the analysis of the field of Information Security. On this basis, we offer a meta-model, representing a generalized model of the problem area of the ISS. The model consists of six components corresponding to the basic concepts that represent the field of IS (Figure 14):

- “Endpoint protection” (Where do we protect?),
- “Protection of communications” (Where and What do we protect?),
- “Data protection” (What do we protect?),
- “Monitoring and Analysis”,
- “Management and Configuration” (How do we protect?),
- “Security model and policy” (Why do we defend?).

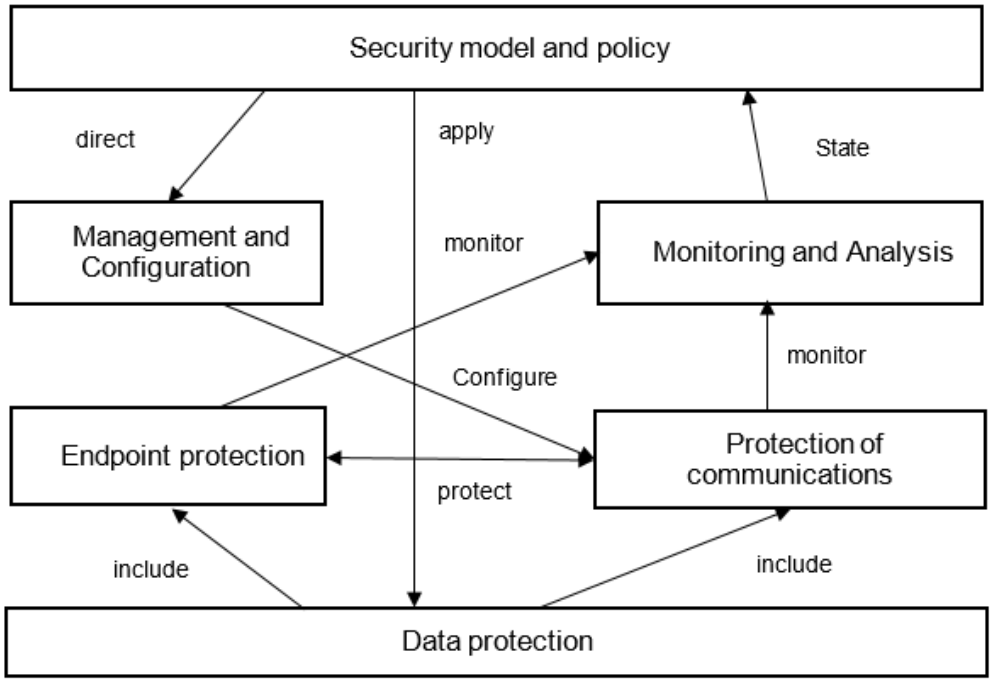
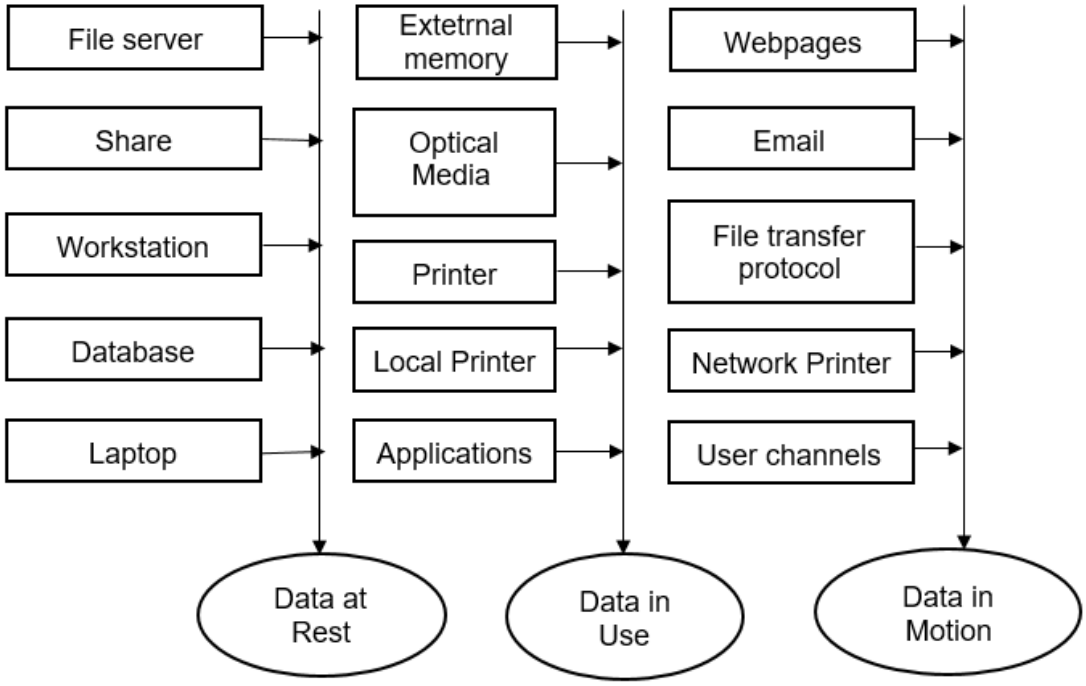


Figure 14. Generalized conceptual model of the ISS problem area

At any time, the data can be in one of the three states: "Data at rest" (stored on a storage device, archive or network partition), "Data in motion" (data involved in communication, data for the status of a module) or "Data in use" (all data used or processed in applications) [23]. For the formal presentation of the data in the ISS, we create a meta-model (Figure 15), which is based on the viewpoint "Processing of Information" in the area of interest of the ISS (Figure 8) [19]. In order to protect the different types of data, it is necessary to implement specific approaches to information security in the main blocks of the meta-model from the viewpoint "Information Security". Data must be protected against loss, theft, and unauthorized access or uncontrolled changes through the application of AIS, such as: Privacy Control, Integrity, Access Control, Isolation and Replication [17, 18].

In order to take into account the requirements of all stakeholders, i.e. viewpoints, our approach allows the creation of any number of conceptual meta-models that can be combined in one system. The result is a multi-layered conceptual meta-model of the ISS which contains meta-models representing the respective viewpoint.

The multilayer meta-model shown in Figure 16 presents the “Information Security” and “Processing of Information” viewpoints and the interrelationships between them. As a structure, the obtained conceptual meta-model corresponds to the Multilayer protection model of Figure 4.



.Figure 15. Meta-model "Processing of Information"

The set of Approaches to Information Security, used in the model ensures the implementation of the basic principles of information security such as "CIA Triad", "Principle of the triple A" and the weakest link principle. The main goal is to protect the data in the organization. Due to the complexity of protecting all possible data, we focus on protecting the organization's sensitive data, which is defined depending on the environment in which the system is designed. Regulatory, legal and other requirements are taken into account and efforts are limited to the protection of relatively small in volume, but critical for the work of the organization data. Regulatory, legal and other requirements are taken into account and efforts are limited to the protection of relatively small in volume, but critical to the work of the organization data. These data are defined as sensitive and the purpose of the ISS is to protect them. The components of the meta-model perform different security functionalities.

Depending on the requirements of the different stakeholders, meta-models for the different viewpoints can be added to the conceptual model in order to meet their requirements for the ISS. The resulting multilayer conceptual model is transformed into a real physical realization of ISS.

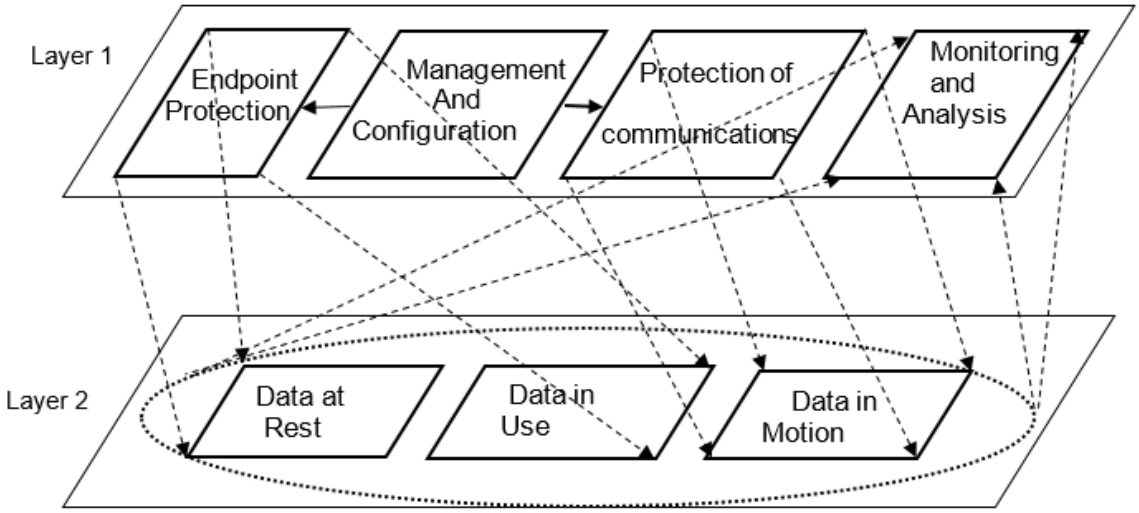


Figure 16. Multilayer conceptual model of ISS

3.2.2 Detailed presentation of the problem area

Here is the detailed presentation of the problem area. Based on the generalized ISS model, a detailed model of the ISS problem area is created. We consider the detailed conceptual models of two of the concepts shown - "Endpoint protection" (Figure 17) and "Communication protection. (Figure 18).

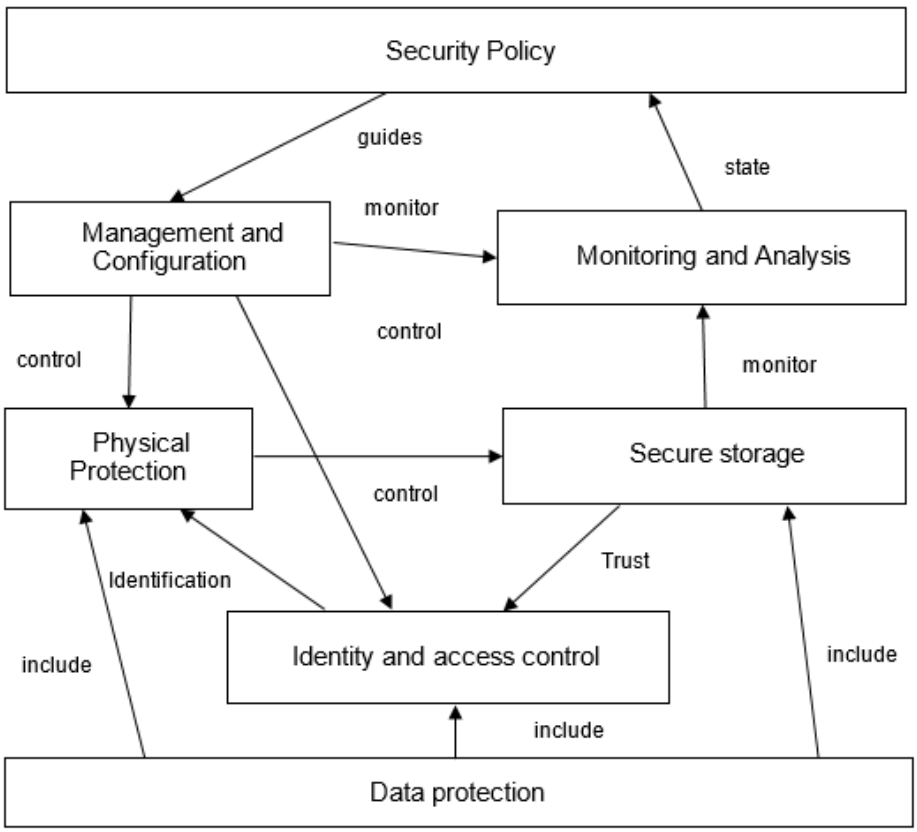


Figure 17. Detailed conceptual model of the “Endpoint protection” concept

Endpoints are elements of the ISS that have computing and communication capabilities: devices, workstations, servers, elements of the communication infrastructure, cloud infrastructure and others. They have different functions and security requirements and their

protection can be achieved with specific Approaches to Information Security (AIS).
To ensure the Availability, Confidentiality and Integrity of the endpoint, the concept of "Endpoint Protection" must ensure the implementation of certain functionalities that are provided by the components shown in Figure.17.

The concept of "Protection of communications" provides security of connected endpoints and communication channels. Figure 18 shows a detailed model of the concept.

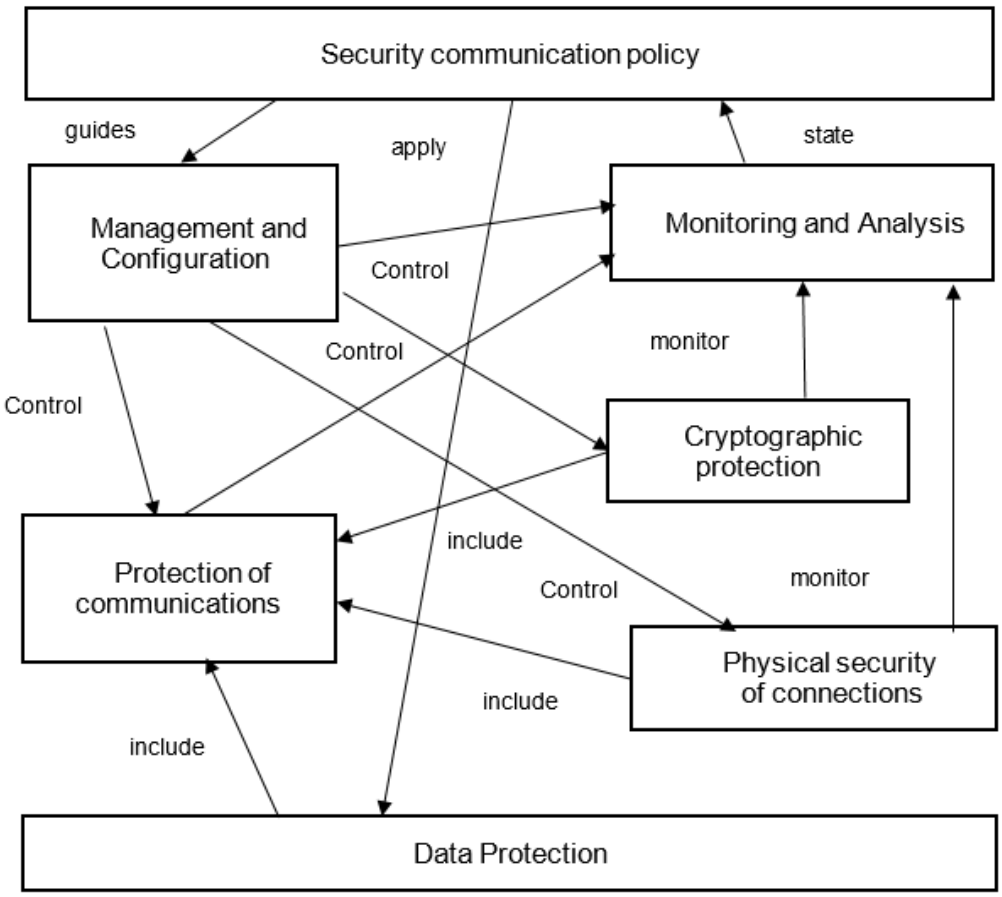


Figure 18. Detailed conceptual model of the “Protection of the Communications” concept

3.3. Project model of information security systems. Architectural and functional model

Approach to creating a project model

Based on the architectural description of the information security system, a project model of the system can be created. It allows the realization of real ISS. In the design of ISS, the requirements of the different viewpoints are summarized and taken into account. The ISS design approach is based on a model-to-model transformation. In our case we carry out the transformation:

Conceptual model → object-oriented (OO) model

The most appropriate way to describe OO models is to use an object-oriented description tool, such as the object-oriented UML language. This language allows system developers to describe the requirements for ISS and its components, to sketch, modify and manipulate the proposed architectures, to repeatedly use individual components of ISS, to communicate the information collected during the development of the system. UML provides standard notation for system analysis, design and implementation.

3.3.1 Object-oriented approach using object-oriented UML language

This subsection describes the general functionality and capabilities of the UML language, as well as the main types of diagrams (Figure 20). Through the different UML diagrams, different views of the system model can be represented.

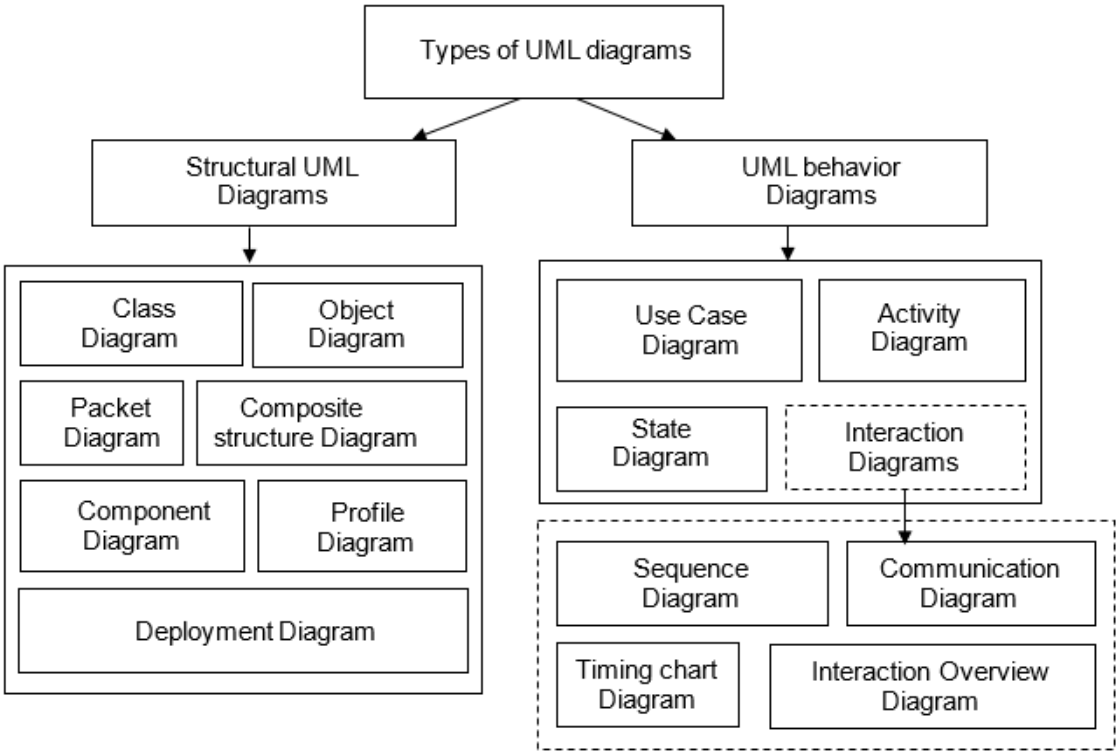


Figure 20. Types of UML diagrams

The static structure of the system can be represented by Structural Diagrams. These include the following main types: "Class Diagram", "Object Diagram", "Packet Diagram", "Composite Structure Diagram", "Component Diagram", “Deployment Diagram: and “Profile Diagram”.

Behavior Diagrams can represent the interactions and current states of components in a model, as well as to show how they change over time. These diagrams can be used to trace how the system operates in a real environment and to observe the effect of certain operations or events. These types of charts include "Use Case Diagrams", "Activity Diagrams", and “State Diagram".

The last type of UML diagrams are Interaction Diagrams. They are a subclass of Behavior Diagrams and are used to describe the interactions between the various elements in the model. This interaction is part of the dynamic behavior of the system. Such diagrams are: "Sequence Diagram", "Communication Diagram", "Timing Diagram" and “Interaction Overview Diagram".

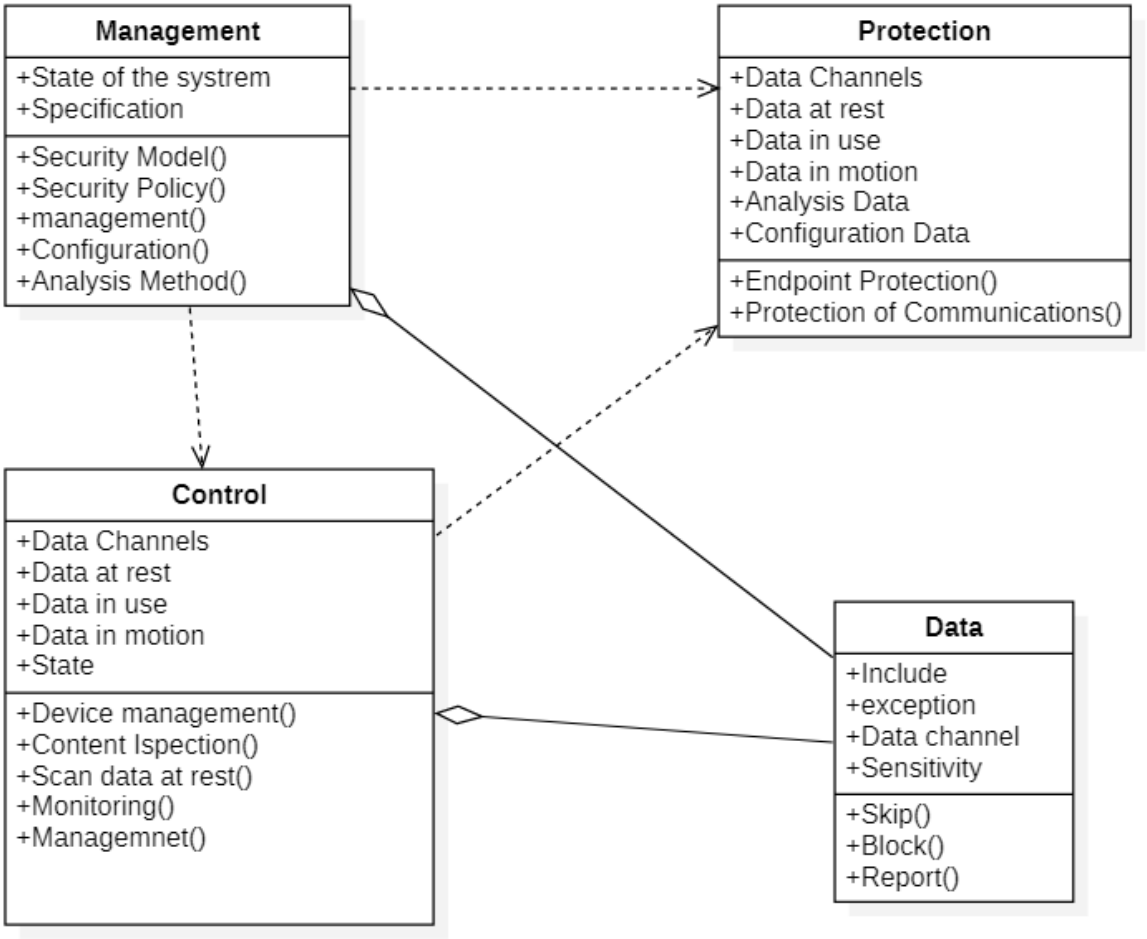
3.3.2 Architectural model of information security systems

The ISS architectural model is represented by static UML diagrams. To reflect the transformation of the generalized model of the ISS problem area from Figure 14 into an OO model, we use a "Class-diagram". To represent the object-oriented models of the detailed models of the concepts "Endpoint protection" (Figure 17) and "Protection of the Communications" (Figure 18) we use "Composite structure diagrams". A more detailed description of the architecture of the project model requires the use of "Object Diagram" and "Profile Diagram", which is currently not the task of the dissertation.

Based on the other static diagrams - "Packet diagram", "Component diagram" and "Deployment diagram", the Realization Model is built.

UML „Class Diagram“

The purpose of the Class Diagram is to show the static structure of the classifiers in the system. The diagram provides a basic notation that can be used by other UML diagrams. The class diagram consists of a set of classes and relationships between them [97]. The ISS concept represented by the generalized meta-model (Figure 14) can be described by a 'Class-diagram', as shown in Figure 21. We use the same concepts as in the meta-model, divided as methods of the four main classes.



Фигура 21. UML "Class diagram" of ISS

The "Endpoint Protection" and "Protection of the Communications" components correspond to the Endpoint Protection and Communications Protection methods in the Security class, and the Data Protection component is represented by the equivalent methods "Skip", "Block” and “Report” in the Data class. The Control class is an aggregation of the Endpoint Protection, Protection of the Communications, Data Protection, and Management and Configuration components.

UML "Composite structure diagram" of the class "Protection"

This type of diagram represents the internal structure of the respective class. The "Protection" class includes the "Endpoint Protection" and "Protection of Communications" methods, which provide data protection both at the endpoints and in the communication process. The class structure, expressed by a composite structure diagram, is shown in Figure 22.

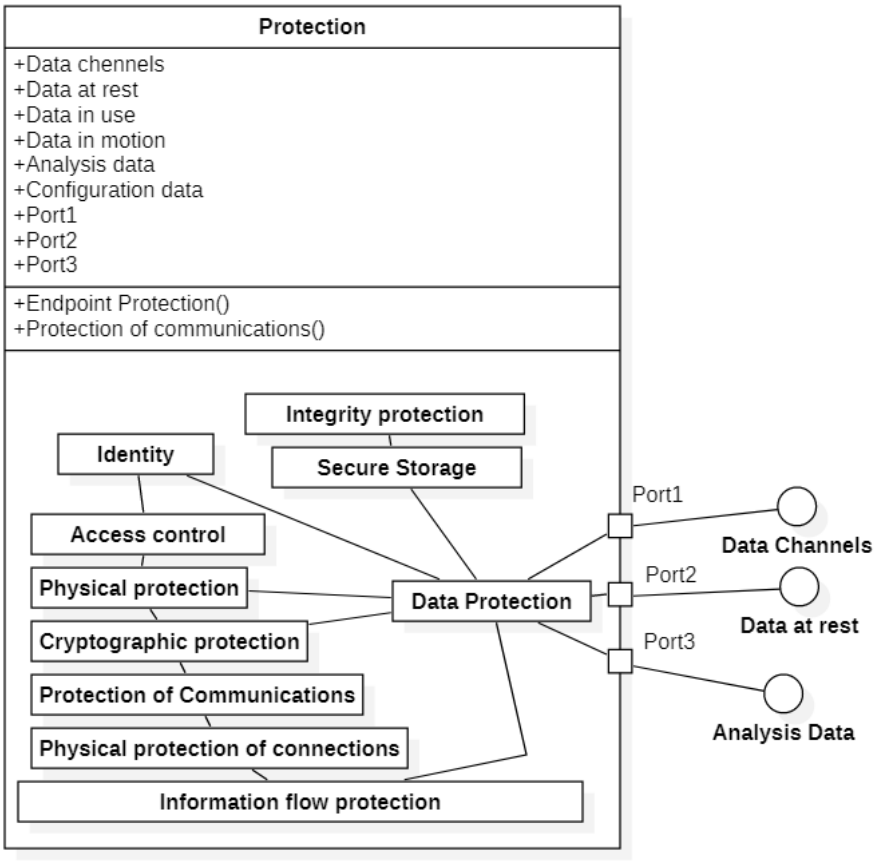


Figure 22. UML Composite structure diagram" of the class "Protection"

3.3.3 Functional model of information security systems

The functional model of ISS can be represented by dynamic UML diagrams: Behavior Diagrams and Interaction Diagrams. With their help can be described various aspects of the dynamic behavior of the system and the interaction of the various elements of the system with each other or with external entities. These diagrams are convenient for describing the results of the dynamic analysis of the ISS (Figure 23). The purpose of the analysis is to identify the possible variants of interaction, to describe them formally and to be embedded in the designed system so that it responds to the interaction according to the goals set in its design.

The ISS operates in a specific environment (1). In addition to providing the conditions for the functioning of the system, it also performs the interaction of the ISS with different entities - points of interaction (Pi1 .. PiN) in Figure 23. These entities outside the system interact with it in different ways, benefiting from the ISS. The modes of interaction can be described with a set of use case diagrams (2). These diagrams are the basis of the dynamic analysis and, accordingly, of the functional model of the ISS.

For each interaction of the ISS with an external entity / object, a basic use case diagram describing the main interaction and behavior as well as extended use case diagrams related to the basic diagram and extending the basic one can be compiled. Additional diagrams inherit the base diagram and add new aspects to the core interaction. Thus, a

set of use case diagrams is formed, related to one or more subjects and describing as fully as possible the interaction of the system with them. For each use case, the corresponding scenarios (3) describing the interaction and the expected response of the system are described. Each scenario can be analyzed using UML behavior diagrams. They can be interaction diagrams (4) (Sequence diagram, Communication diagram, Timing chart diagram, Interaction overview diagram) or Activity diagrams (5). The choice of (4) or (5) depends on the specifics of the system and the environment, so that its behavior can be most fully described. The next step is a description through state diagrams (6), through which we describe the change of state of the main elements of the ISS, summarizing its dynamic behavior.

The obtained set of UML diagrams describing the result of the dynamic analysis of the system forms the Functional model of the designed system. Each diagram describes the individual functionalities of the system, showing that the approach is applicable.

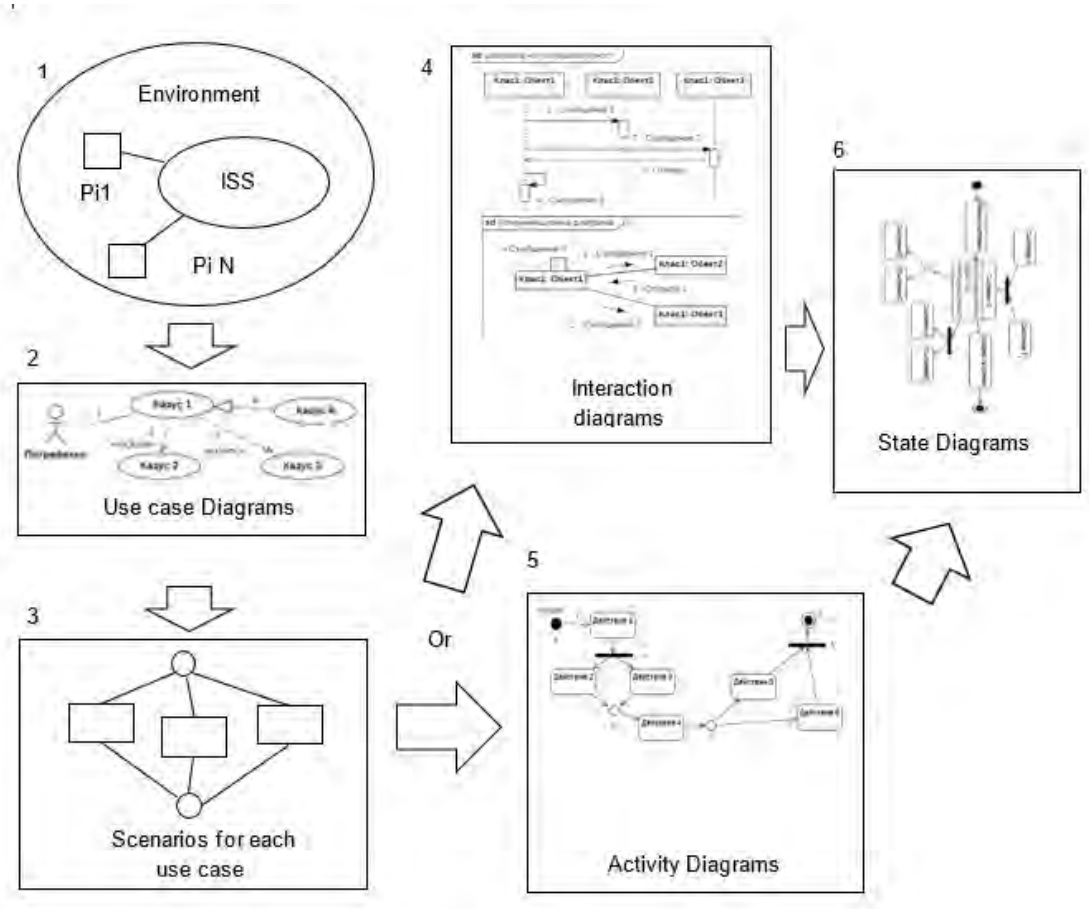


Figure 23. Approach to creating a functional model using dynamic UML diagrams

This subsection shows how different scenarios of interaction of the ISS with external entities can be described through the different dynamic diagrams. For example, a Use case diagram can conveniently describe different ways of communicating, such as sending an e-mail to a recipient external to the organization.

The following UML diagrams forming the functional model are interaction diagrams describing the interaction of the Management, Control, and Data classes and the Management, Control, and Protection classes. The classes are part of the Class Diagram of the ISS architectural model (Figure 21). This type of diagram easily reflects specific interactions of individual classes, such as inspecting the flow of information passing

through a communication channel for the content of organization-sensitive data or verifying compliance with security policies by individual users.

"Sequence diagrams" visualize the time sequence of interactions between the elements of the system, carried out through messages between them.

In addition to interaction diagrams, the dynamic behavior of the system presented with scenarios and use cases can be analyzed by activity diagrams. Figure 28 shows a diagram of the activity of one of the methods of the class "Protection" - "Endpoint protection", showing the verification of whether the information passing through a data channel is sensitive according to the criteria of the organization. Similar activity diagrams can be created for all class diagram methods. In such a way, it is possible to describe different cases for interaction with the system in detail.

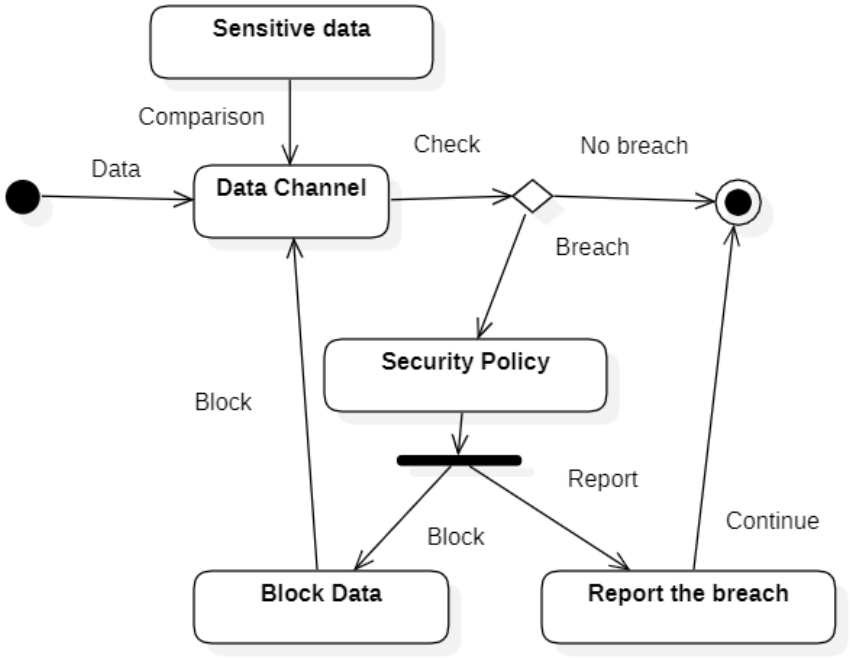


Figure 28. UML Activity diagram of the endpoint protection method

3.4 Conclusion

The third chapter presents an approach for designing ISS, designed for organizations and aimed at protection against leakage of sensitive information from the inside out, i.e. as a result of the action of insiders with legitimate access to the resources of the organization and its data. To determine the architecture of the system, the system framework presented in Chapter 2 is used, which helps us to specify the problem area of the SIS and to perform the relevant analysis.

This chapter presents a model of analysis that matches the model of the problem area. The construction of the model is based on the potential of conceptual modeling. As a result, a generalized conceptual model of the ISS problem area has been created. It is shown how the generalized model can be transformed into a multilayer when the analysis of more than one viewpoint in relation to the problem area of the system is taken into account. The presented multilayer meta model reflects the views "Information Security" and "Processing of Information". Based on the generalized conceptual model, a detailed conceptual model of its individual components is constructed. Detailed descriptions of the concepts "Endpoint Protection" and "Protection of Communications" are shown.

The process of creating an ISS project model is based on the implementation of the

"model to model" transformation. In this case, the conceptual model of the problem area of the system is used to create an object-oriented /OO/ project model. For this purpose, an object-oriented tool for describing models is used - the formal language UML. This language provides standard notation for systems design and implementation. It is shown that it allows system developers to present the requirements to the ISS and its components in a design model of the system, which consists of an architectural model and a functional model. It presents how individual aspects of the architectural model can be modeled, based on the respective conceptual models, using the following UML diagrams: "Class-diagram" and "Composite structure diagram". By modeling individual aspects of the functional model, it is shown how an object-oriented functional model can be compiled, based on the created conceptual models of the problem area. The following UML diagrams are used for this purpose: "Activity diagram", "State diagram", "Interaction overview diagrams", "Use case diagram", "Sequence diagram".

Through the applied method for analysis of the problem area, the possibilities for conceptual modeling and the approach for realization of the transformation “from model to model”, considered in Chapter 3, tasks 3 and 4, defined in "Objective and tasks of the Ph.D. Thesis":

> 3. Description of the problem area of Information Security Systems in organizations through conceptual modeling;
>
> 4. Analysis and application of object-oriented approach in creating a project model of an information security system based on a conceptual model;

As a result of the research activity for creation of a methodology for development of ISS through a model of analysis and project model the following scientific and scientific-applied contributions are achieved:

1 A conceptual model of the problem area of information security has been developed;
2 A multi-layered conceptual model of the problem area of ISS has been created as a result of the application of two or more viewpoints in its description;
3 An approach for creating architectural and functional models of ISS, based on an existing conceptual model of the problem space using the object-oriented unified language UML software systems is presented.

Chapter 4 Approaches to creating a model for the implementation of information security systems in organizations

According to the adopted methodology for the development of the ISS, on the basis of the project model a realization model should be created, which can be used for two purposes:

- Creating a realization model in accordance with the existing realization environment;
- Simulation of the operation of the designed ISS.

In order to achieve the first goal, as part of our proposed method, an analysis of the problem area is performed and based on the developed conceptual model, as a result of this analysis a platform for implementation is selected. The aim is to maintain the approach of object-oriented modeling. As a result, an object-oriented model of implementation must be created, which corresponds to the developed OO project model.

To achieve the second goal, the simulation environments NetLogo (v.6.0.4) and I-SCIP-SA are used, working on the basis of creating agent or multi-agent oriented models. This

requires the object-oriented project model described by UML to be transformed according to the requirements of the agent approach.

4.1 Comparative analysis of existing DLP platforms based on an analysis model

Information security policy affects the individual jobs in the organization in different ways. Employees in different positions (jobs) use different data and have the appropriate regulated access to them. This is described in the information security policy adopted by the organization, based on their job description. The IP policy also describes which operations with this data are allowed and which are not for the job. The access to organization-sensitive data for the respective positions is explicitly described.

The main goal of DLP systems is to protect data from leaks outside the organization. AIDS systems provide a flexible platform for the implementation of the adopted information security policy with regard to data protection. They offer appropriate tools to describe, implement and control:

- Different types of data,
- Defining and working with sensitive data for the organization,
- Allowed and prohibited operations with different types of data from the respective jobs,
- Description of different scenarios for working with data,
- Description of regulations for data handling and their observance and control.
- Analysis of the observance of the security policy in the organization.

DLP systems have the ability to adapt to different jobs according to the requirements of information security policy.

4.1.1 Applications of proposed by us method for specifying the ISS architecture

The ISS for organizations, designed by us is aimed at protection against leakage of sensitive information from the inside out by internal persons with legitimate access to data and resources of the organization. The architecture of the system is specified from the different points of view of the individual participants in the process of design and implementation of the ISS. A basic requirement for the system is to have an appropriate architecture that can be adapted to different information security policies, which set appropriate requirements for different users of information in an organization.

This requirement is fully satisfied by proposed new method for specifying the requirements for the architecture of the ISS.

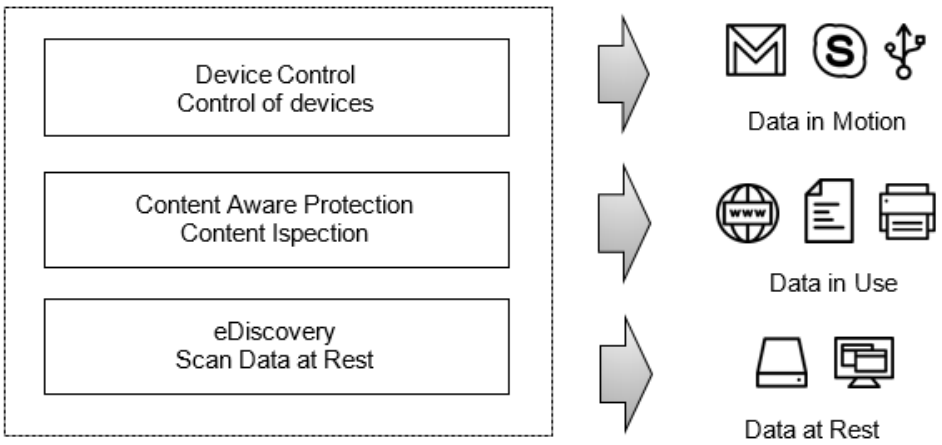
Based on the analysis of the problem area from different points of view and its subsequent conceptual modeling (Fig. 8), the requirements to the developed ISS are specified. This allows you to choose the right platform for its implementation. The first point to consider is the "Information Processing" point of view. It reflects the different types of data - data at rest, data in use and data in motion. Another point of view is the "Technology point of view", which reflects the ways of data protection and contains the supported platforms and technologies. It is of great importance to ensure operational. ISS compatibility, which builds on the addition of an existing ISS. The choice of platform for implementation is also used from the point of view of "Information Security", reflecting the requirements of the organization to data protection. They are described in the Information Security Policy. Based on the three points of view and the similar goals of the ISS designed by us and the systems for prevention of data leakage, a platform for realization of the DLP type is chosen. Using the conceptual meta-model from Fig.15, built from the point of view of "Information Processing", an analysis of leading DLP systems is performed (Cososys Endpoint Protector 5.0.2.1 [96], Symantec Data Loss Prevention 14.6 [137],

McAfee DLP Endpoint 9.3 .200 [138], Forcepoint DLP 8.9 [139], DeviceLock 8.2 [95]) and how they meet the requirements of the problem area.

As a result of the analysis, the most appropriate specific platform for implementation is selected. The DLP system chosen for the implementation of the ISS is part of its architecture. In our cases, based on the analysis, our choice falls on the DLP system Cososys Endpoint Protector 5.0.2.1 [96]. Apart from the advantage in terms of protection of basic data types (data at rest, data in use and data in motion), another major advantage is the provision of interoperability with other means and approaches to information security in the organization. An additional advantage of the chosen platform is its price. In the implementation of the SIS, the task of the selected DLP is only to ensure the protection of the organization's data from the inside out, without interfering with other means of protection.

4.2 DLP Implementation Platform Cososys Endpoint Protector 5.0.2.1

In addition to agent-oriented models for simulation purposes, the realization model can be created using the existing implementation environment. To achieve this goal, we choose an existing platform for building DLP systems Cososys EPP 5.0.2.1 [96]. To create the model we use the approach of object-oriented modeling. As a result, we create an object-oriented realization mode, which corresponds to the developed OO project mode.



Fifure 31. DLP „Cososys EndPoint Protector 5.0.2.1“ – Structure

The chosen implementation platform, Cososys EPP 5.0.2.1, consists of a hardware server and software modules Device Control, Content Aware Protection and eDiscovery. The hardware server provides centralized control of the DLP system, and the individual modules provide different functionality (Figure 31).

4.3 Object-oriented model of realization of information security systems in organizations

To create an OO realization model, we again use the UML toolkit. Through it we create the following diagrams:

- Packet diagram,
- Component diagram,
- Deployment diagram.

The packet diagram of the realization model (Figure 32) consists of the following main packages: "Device Control", "Content Aware Protection", "eDiscovery - Scanning at rest"

and "Reports and analysis “Corresponding to the main modules of the DLP system Cososys EPP 5.0.2.1. The DLP system is based on a client-server architecture. The workstations controlled by the system are called "Endpoints". At each endpoint, a client called an "agent" is installed, which controls the relevant data channels such as Lan network, wireless network, USB ports, Bluetooth ports, serial and parallel ports (Figure 33). The DLP system also controls the access of all devices using the channels and data ports - USB storage devices, printers, cameras, etc. The system communicates with the endpoint and enforces the adopted security policy, indicating WHO can use data channels and devices, WHEN to use them, HOW to use them (through what protocols and applications), WHAT data can be used and sent .

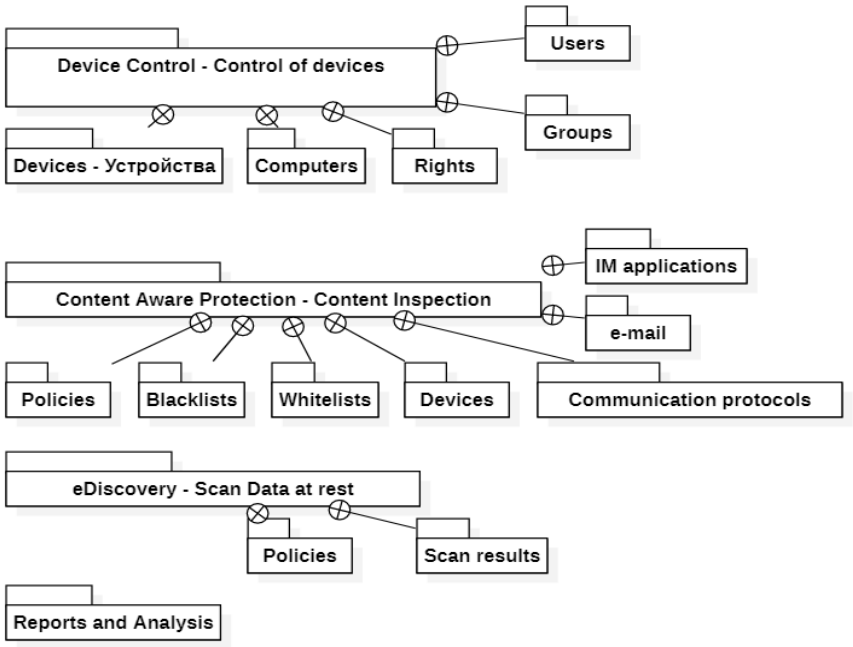


Figure 32. UML Packet diagram of DLP Cososys EPP 5.0.2.1

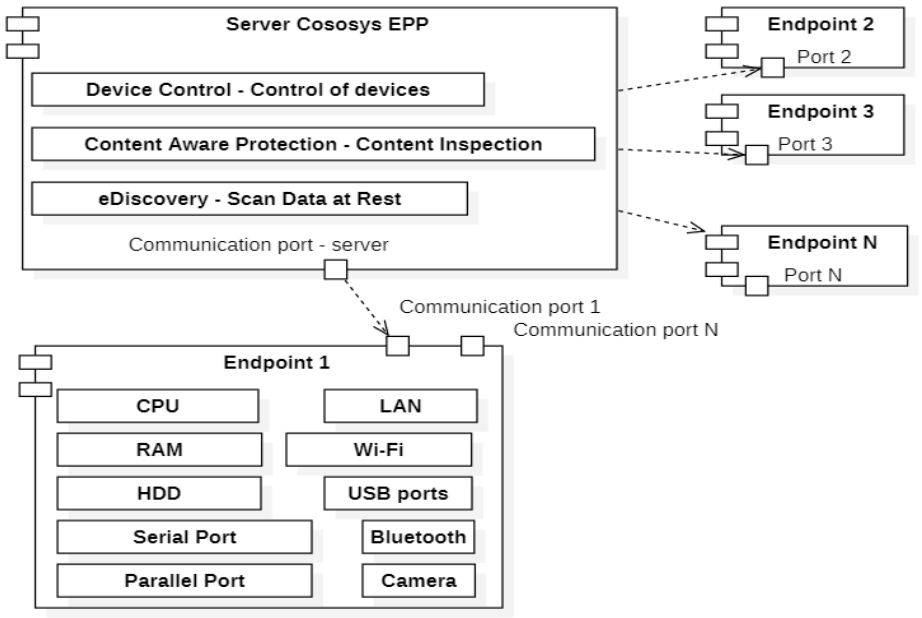


Figure 33. UML Component diagram of DLP Cososys EPP 5.0.2.1

The Deployment diagram models the physical implementation of the system components. Unlike the component diagrams used to describe individual components, deployment diagrams show how these components unfold in the real environment. An example diagram of an DLP system implementation is shown in Figure 34. Due to the fact that the ISS is usually a complex system composed of a large number of components, the diagram is simplified and shows several hardware components such as a DLP server connected to software agents, installed on consumer workstations. Through software agents, the DLP server monitors, controls and manages the data channels of endpoints (workstations and laptops) - LAN, wireless network, Bluetooth, USB ports, e-mail, chat communications and more. The DLP system is able to control the communication channels, to activate and deactivate the flow of data through them according to the context and the user. The data can be inspected by content, and in case of finding a violation - unauthorized leakage of data, it can be blocked and reported. The communication between the clients and the server is carried out through TCP/IP protocol.

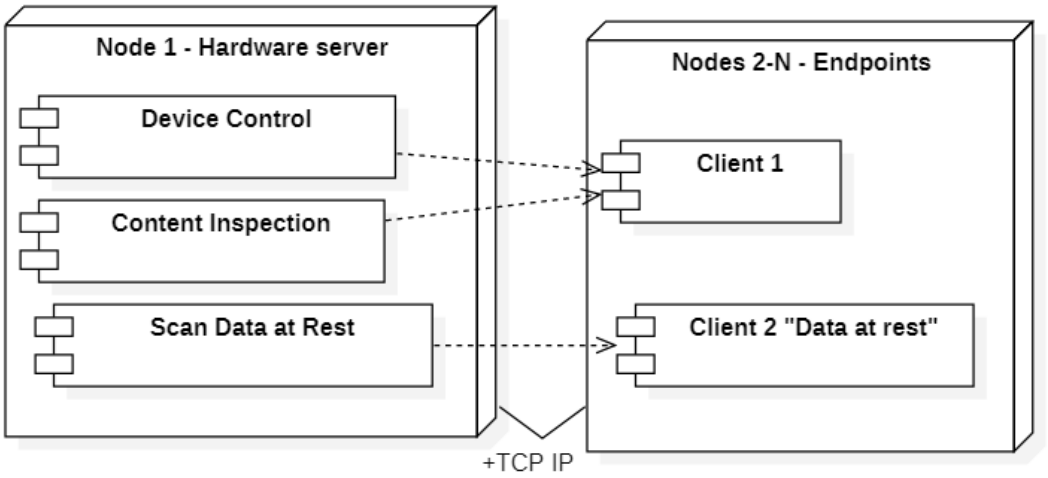


Figure 34. UML deployment diagrams of DLP

4.4 Extention of the existing ISS with new use cases to protect sensitive data for the organization

The method proposed by us, combined with the use of a flexible implementation platform such as DLP, provides an opportunity to further develop existing ISS through new data protection scenarios, not yet implemented in the organization. The method allows for modeling and implementation of new aspects of ISS without having to design the system from scratch. Another main advantage of the method and use of DLP is the preservation of interoperability with other elements of the existing ISS or of separate approaches and mechanisms for information security, already implemented in the organization.

This is the case with an organization that has a functioning ISS and effectively protects its infrastructure through various approaches to information security (AIS) with network communication - Fig.3. Following the entry into force of the General Data Protection Regulation (EU Regulation 2016/679), which regulates the protection of personal data of citizens of the European Union, the organization has to comply with it and introduce measures to protect personal data of customers and employees.

To this end, the following changes in the information security policy are necessary:

1. Compliance with the requirements of the GDPR for the protection of personal data,
2. Protection of information from inside-out.

Their implementation is based on the definition and protection of sensitive information for

the organization. Description of the necessary scenarios for the protection of personal and / or sensitive data and compile the dynamic UML diagrams necessary for the implementation of the scenarios, related to the description of the dynamic behavior of the system (Figure 23).

The described scenarios are then added to the existing ISS, through the selected DLP for the implementation of protection in real conditions, taking into account the individual jobs and the specifics of their work with data.

4.4.1 Results of tests performed on the expansion of an existing ISS with new use cases for the protection of sensitive data

Proposed by us method for designing of ISS, expands the capabilities of existing information security systems. The detailed description of the use cases for the protection of organization-sensitive data through design models using UML diagrams at the design stage enables the SIS to accurately meet the objectives set for internal security policies, regulations and confidentiality directives. The implementation of the ISS with the DLP platform provides intuitive policy making describing use cases through the proposed scenarios.

The functionally extended ISS is an effective tool for preventing and investigating incidents involving the leakage of sensitive information.

The project model gives a clear idea of the processes related to the processing and transfer of information in the organization.

As a result of tests conducted on the further development of the existing ISS through new uses for the protection of organization-sensitive data, the following has been identified (Fig. 35):

1. Reduction of incidents related to leakage of sensitive information (Chart 1),
2. Restriction of the information channels through which sensitive information can leak (Chart 2),
3. Increasing the visibility of sensitive information such as Data in rooms (Chart 3),
4. Improving compliance with internal security policies, legal regulations and confidentiality directives (Figure 4),
5. The rules for the protection of sensitive data drawn up under the scenarios of use shall be strictly and unconditionally implemented by the Functionally Extended ISS.

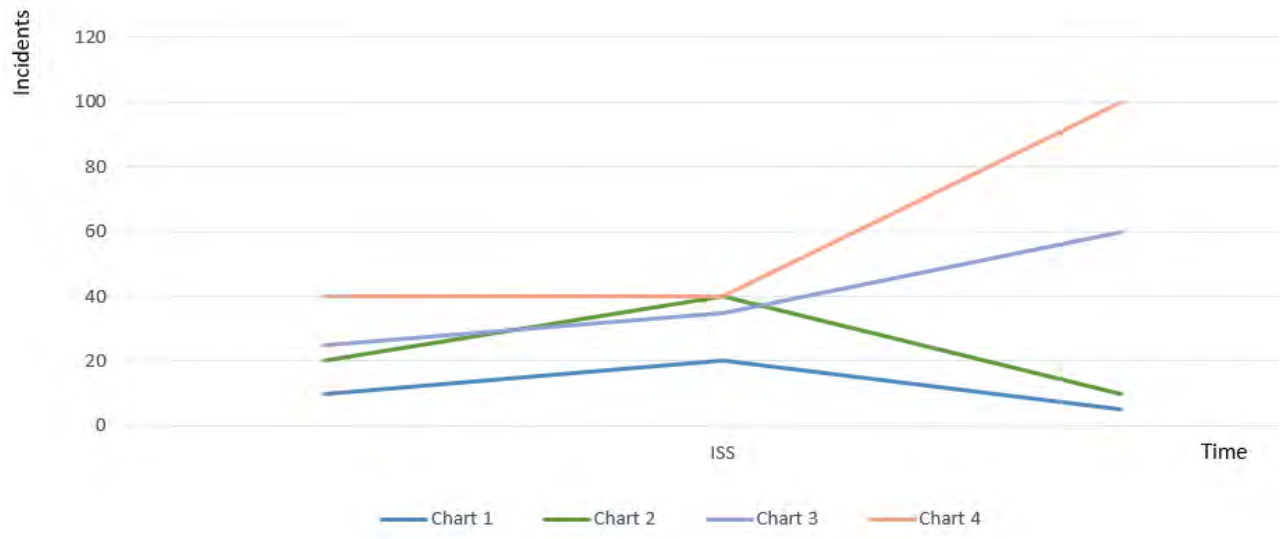


Figure 35. Summary of test results for the development of an existing ISS

4.5 Transformation of OO project model into agent-based realization model

Implementing a system with real components requires significant resources, time, serious effort and human capital to test and collect real data. For this reason, we need to simulate the operation of the designed system in the selected agent-based simulation environment. This requires transforming the created OO project system model into an agent-based realization model, the operation of which must be simulated.

In agent-based systems, the agent collects and processes information about the environment in which it operates and influences it based on decisions made by it and proactive activity. In ISS, we assume that individual agents performing independent tasks to protect an asset or information are part of the system. In order to achieve the objectives of the ISS, it must ensure the operation of several main types of agents, acting in a specific role and interacting between them: "Breaching Agent", "Protection Agent", "IS Policy Agent", "Monitoring agent", "Reporting agent", "Communication Agent", "Processing agent", "Storage agent", "Services agent ".

The transformation from the object-oriented project model of the ISS into an agent- -based realization model is based on the class-diagram of Figure 21. It is evident that the class "Control" contains objects that have the potential to become pro-active agents, making independent decisions. This class interacts with the other classes (Security, Data, and Management), which shape the environment of the agent class, which provides them with the information they need to work to make decisions. In addition, agents act on this environment in order to achieve the specific results for which the ISS is set up and receive information from them on which to base its decisions. We can assume that these classes form the environment with which the Control class interacts. We can define the class "Environment", consisting of the three classes Protection, Data and Management. The Control class then becomes a Control Agent, interacting with the new Environment class (Figure 36). On this basis, we assume that the "Control" class is transformed into an "Agent" class, which represents a set of agents, each of which has a specific purpose.

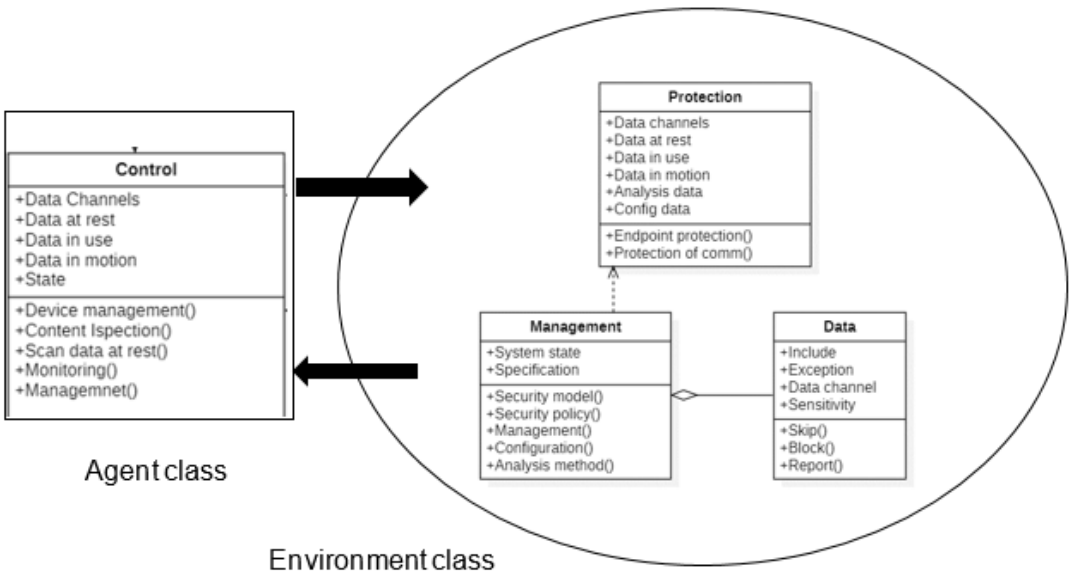


Figure 36. Agent and Environment classes

In accordance with the individual objectives and the need for certain roles, the class "Agent" includes: "Breaching Agent", "Protection Agent", "IS Policy Agent", "Monitoring agent", "Reporting agent", "Communication Agent", "Processing agent", "Storing agent", "Services agent" (Figure 36).

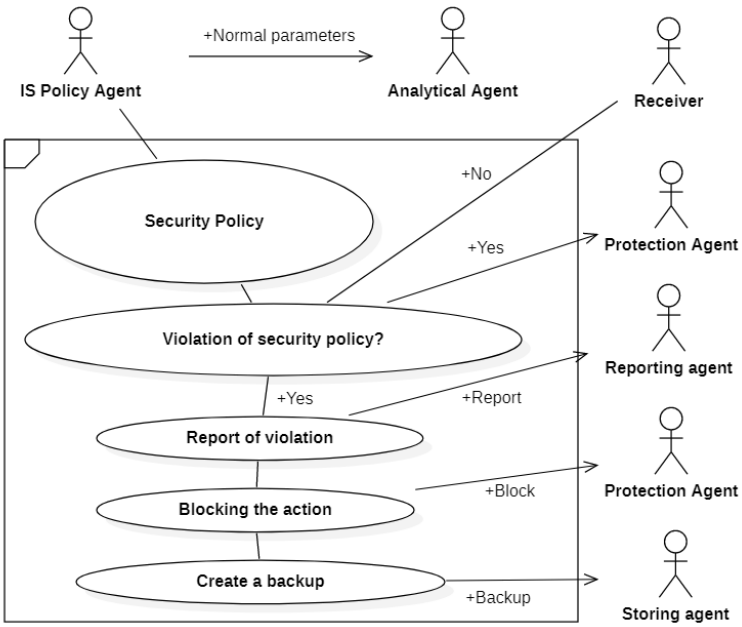


Figure 37. "IS Policy Agent" Use Case Diagram

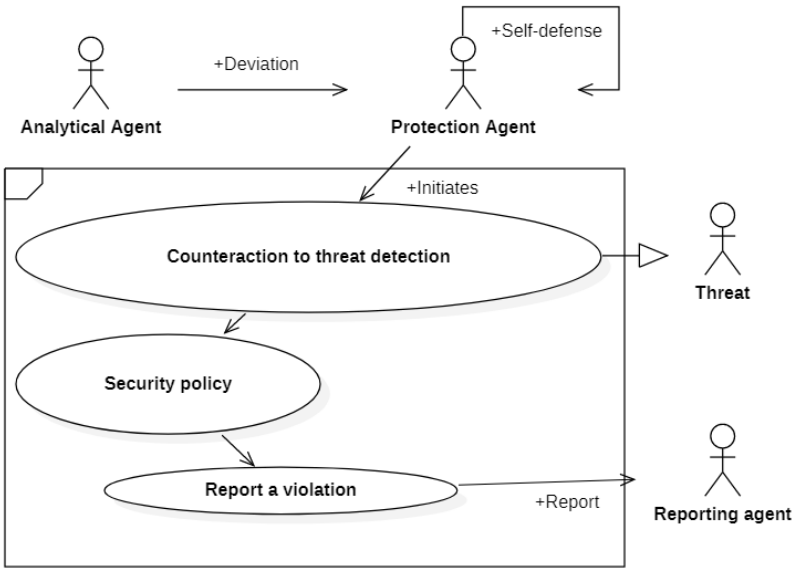


Figure 38. "Protection Agent" Use Case Diagram

To describe the role of each agent by using the UML language, a "use case" diagram is used, which describes the interaction of an agent with the environment, which in our case is considered as an OO system. For each of the listed agents, a diagram is created that describes the scenario in which it operates. To show how this is done, the 'use case' diagram is presented to the environment by the 'IS Policy Agent' and 'Protection Agent' agents. The other agents are described in a similar way, which creates an agent-based model of ISS implementation. This model is used to simulate the activity of the designed system. Figure 37 shows a use case diagram for an "IS Policy Agent" and Figure 38 shows a use case diagram for a "Protection Agent".

4.6 Simulation of information security systems and analysis of the generated test data

The implementation of the simulation of the ISS architectural model is performed on the

basis of agent- and multi-agent-oriented modeling in NetLogo and I-SCIP-SA environments, allowing mixed (expert, sensory and machine) evaluation of the proposed architectural meta ideas [102].

Experiments in NetLogo environment

NetLogo (Figure 39) is a multi-agent cross-platform simulation environment for simulating complex systems over time [47, 118]. The NetLogo environment is based on agent-based models for simulating the actions and interactions of multiple autonomous agents (individual or collective entities such as organizations or groups) working simultaneously. This makes it possible to study the relationships between micro-level models that arise from their interaction and to assess their impact on the system as a whole. Based on the meta-model in Figure 14, an agent-oriented model was created in the NetLogo environment (v.6.0.4).

The results of the simulations of this model are shown in Figure 40. In general, the interactions between the individual blocks are studied: “Protection Agent”, “Communication Agent”, "Breaching Agent”, “IS Policy Agent”, “Reporting Agent” , “Storing Agent”, “Monitoring Agent”, “Services Agent” and “Processing Agent”. By using elements of Game Theory, as well as a class of Monte Carlo methods for working with random samples, implemented in the NetLogo environment, the presentation of the agents was realized and the interactions between them were realized.

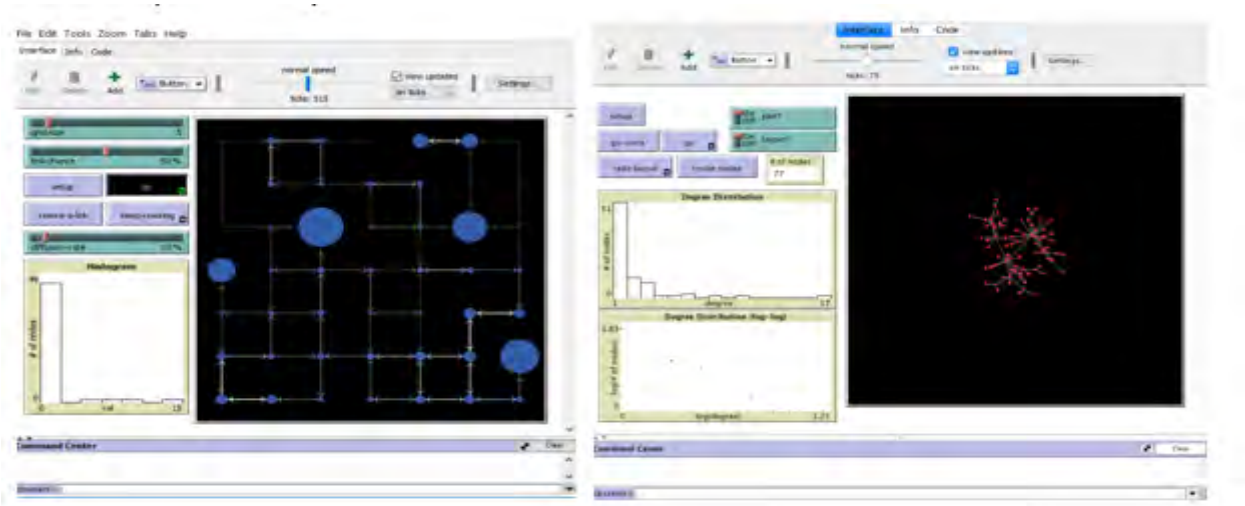


Figure 39. Screenshots from a simulation in a NetLogo environment

Experiments in I-SCIP-SA environment

In order to be closer to reality, allowing a mixed study of the proposed architectural solutions of the ISS, a multi-agent model [28] of the "system-of-systems" type [126] was developed in the I-SCIP-SA environment (Intelligent Scenario Computer Interface Program for System Analysis) [105]. The experience of [106] and the organization of the model proposed in [103] and implemented in [107], similar to the research in the NetLogo environment, were applied. The aim was to create an opportunity to identify future threats - internal and external in IS, used in a corporate environment, in accordance with the different states of the data used with active participation and the human factor. Mechanically, the results are presented through the object-link organization [108] and provide an opportunity to perform relevant initial and final holistic, classification assessments of the agents in the studied models.

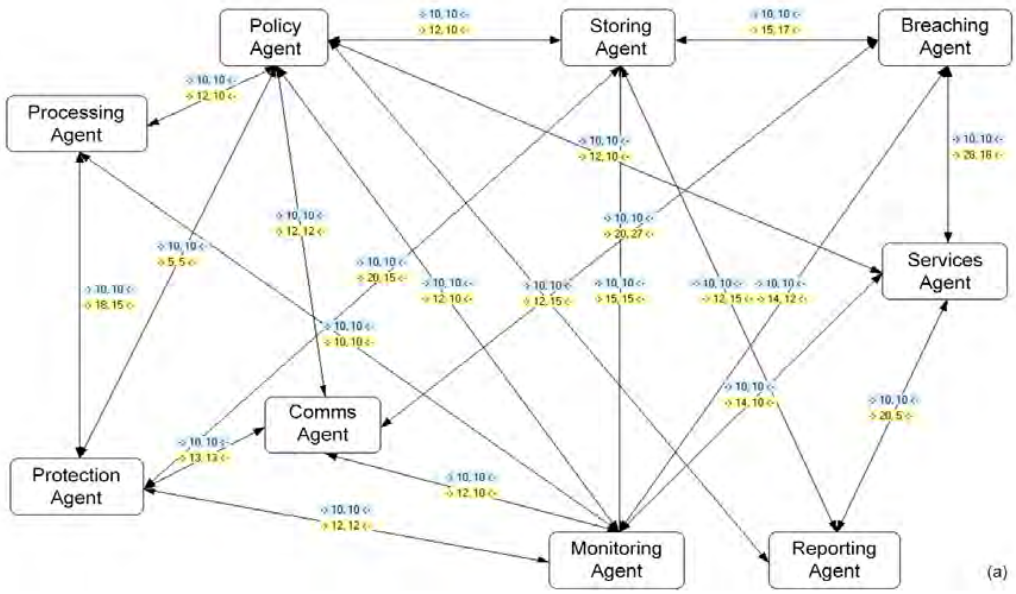


Figure 40. Multi-agent model of DLP system for proactive research of data leakage in corporate environment

Objects representing agents (graphically marked as named, rounded rectangles) have functionalities for both inter-agent communication and visualization of external (recorded or received in real time) data (Figure 40). Inter-agent communication channels are marked with two-way arrows, labeled with the values of weights (colored yellow) and time steps (colored blue), related to the direct (Influence) and feedback (Dependence) relationships between objects in the model. The data on the weights of the inter-agent connections forming trends can be derived from different simulation results in mixed reality, which are obtained as a result of solving mathematical models and external sources, both in real time and after the simulations.

The set of data sources can use: sensors, API functions for direct connection or using records in files of different origin (including expert or other simulation result), which provide the opportunity for proactive system analysis and holistic evaluation of objects in the model (in real time or after the simulation), according to the different data states ("Data in motion", "Data in use", "Data at rest").

The results of the system analysis are interpreted and aggregated in different ways, for example [109, 110, 111], using here “3D Sensitivity Diagram” - “3D Sensitivity diagram” (Figure 41), providing classification of agents (designated as indexed 3D). spheres) in four sectors (Active - Active, Passive - Passive, Critical - Critical and Buffering - Buffering objects, having respectively - "passive" - z <0 or "active" role - z ≥ 0 in relation to the sector in which they are located), in accordance with the processing and mixing of the initial expert assumptions and the resulting simulation results (for Influence - Influence - x, Dependence - Dependence - y and Sensitivity - z, measured as a percentage of the interval [0, 1]).

Figure 41. Multi-agent model of DLP with additional classification initial estimates of agents in 3D Sensitivity Diagram

The proposed solution provides an opportunity for the proactive participation of the human factor in the decision-making process, ensuring a comprehensive consideration and assessment of the roles of DLP agents and the problem areas that arise. Multi-agent communication, in a system model, uses different organizational strategies such as: "leadership", as well as "negotiation" [112], depending on the selected simulation scenarios. The results of the analysis of the multi-agent model of the DLP system for proactive study of data leaks in the corporate environment show a clear need for balancing, providing expanded control over the communications and services used. However, this also hides a number of ambiguities, as the introduction of new technological solutions can lead to unexpected data leaks and security breaches. Therefore, monitoring, post-analysis and data storage in combination with real-time heuristic protection remain critical to the successful protection of today's corporate environment, taking into account the specifics of the data flows used.

Generation and analysis of test data

The implementation of this task is organized, on a selected multi-agent architecture of the ISS, in two steps: (a) stochastic validation of data leakage expectations, through expert assumptions and machine-generated ad-hoc data leakage selections; (b) interactive verification in a virtual corporate environment with the selected prototype of the ISS and cyber-attack vectors, realizing the expectations for leakage of corporate data under a certain playback scenario.

This chapter describes in detail a proactive stochastic solution for mixed validation on the proposed system model.

The verification of the results of the stochastic simulations was carried out empirically, using interactive simulation in transformed reality, organized within the exercises CYREX 2018, 2019 and 2020 [109, 117, 122, 123].

4.5 Conclusion

Chapter 4 describes approaches for creating a model for the implementation of the ISS

through proposed by us methodology for the development of ISS.

On the basis of a project object-oriented model, an OO realization model is built, consistent with the existing realization environment. After performing an analysis of the problem area and based on a conceptual model, the result of this analysis, the requirements for the architecture of the developed ISS are specified. The following is an analysis of existing DLP implementation platforms and selection of the most appropriate one in accordance with the analysis model.

The implementation model describes an existing platform for creating an information security system of DLP type "Cososys EndPoint Protector 5.0.2.1". For this purpose, the existing UML diagrams are used: "Batch diagram", "Component diagram" and "Deployment diagram".

The method presented by us allows for modeling and implementation of new aspects of ISS without having to design the system from scratch. To this end, it is sufficient to further develop the existing ISS by including new uses for the protection of sensitive data for the organization. The chapter presents an example with specific scenarios of new use cases, as well as tests of the extended expansion of the system.

In order to simulate the work of the designed ISS, an agent-based implementation model is built. For this purpose, a simulation model of the developed ISS is created, which can be implemented in a multi-agent cross-platform simulation environment for simulating complex systems over time. An approach for transformation from an object-oriented model to an agent-based model is presented.

The applied solution for conceptual UML meta-design of architectures using different classes of diagrams allows static and dynamic consideration of the functionalities of information security systems. More detailed studies of data leakage expectations have been performed simulated, based on mixed agent- and multi-agent-oriented solutions, providing great flexibility and proximity to reality.

The generation and analysis of test data is organized in two steps:

- Stochastic validation of data leakage expectations, through expert assumptions and machine-generated ad-hoc data leakage selections;
- Interactive verification in a virtual corporate environment with the selected prototype of the ISS and cyber attack vectors, realizing the expectations for leakage of corporate data in a certain scenario for playback..

The proposed practical validation and verification of a selected commercially available DLP system with flexible functionalities adapted to the meta architectures allow for a real combination of expert, sensor and machine simulated data. At the same time, it remains possible to compare them with the designed architectural functionalities, in terms of the real attack vectors in a mixed, futuristic virtual environment for selected scenario combinations.

The agent-oriented approach can show the dynamics of the system, which with other models cannot be represented. The agent-oriented model gives us a complete picture that neither the conceptual nor the object-oriented model can give. ISS simulation makes it possible to study the dynamics of the system in different scenarios. The scenarios are described and presented by case diagrams of use in the OO model and then simulated by the agent approach. The simulation can show the behavior of the system when the environment changes. Such is, for example, a change in legislation or regulations, giving certain priorities, the influence of internal or external to the organization, the emergence of a new type of threat or non-standard ways of data leakage. The results of the simulation help to predict both traditional and less common threats and to optimize the use of Approaches to Information Security (AIS).

Chapter 4 describes the implementation of tasks 5 and 6, defined in "Objective and tasks of the Ph.D. Thesis":

5. Defining an approach for transformation of the ISS project model into an implementation model;
6. Simulation of ISS and analysis of the generated test data

As a result of the performed research activity the following scientific and applied contributions are achieved:

1. UML model of ISS implementation in an organization using DLP platform "Cososys Endpoint Protector 5.0.2.1" is presented
2. Comparative analysis of existing DLP platforms for implementation based on the requirements described in the analysis model.
3. Design, implementation and testing of extension of existing ISS with support of new use cases.
4. Creating a simulation model of the architecture of an information security system of the type Data Leak Prevention /DLP/ based on a conceptual model and object-oriented description of its architecture using agent- and multi-agent representation in the environment NetLogo and I-SCIP-SA. Simulation study of the architecture of the DLP system for information security by performing stochastic validation and interactive verification.

Bibliography

1. Suryateja P.S., “Threats and Vulnerabilities of Cloud Computing: A Review”, International Journal of Computer Sciences and Engineering, Volume 6, Issue 3, published 30.03.2018
2. Rhodes-Ousley M., “Information Security the Complete Reference”, 2nd Edition, The McGraw-Hill, 2013
3. Diogenes Y., Ozkaya E., “Cybersecurity - Attack and Defence Strategies”, Packt Publishing Ltd., 2018
4. Pfleeger C. P.,.Pfleeger S.L, Margulies J., “Security in Computing”, 4th Edition, Prentice Hall, 2015
5. Ciampa M., “Security+ Guide to Network Security Fundamentals”, 4th Edition, Course Technology, Cengage Learning, 2015
6. CISSP Study Guide, https://www.sciencedirect.com/book/9781597499613/cissp-study-guide, last accessed 2021/08/11
7. The European Network and Information Security Agency (ENISA) (2012b), https://www.enisa.europa.eu/publications/ENISA_Threat_Landscape/at_download/fullReport, last accessed 2021/08/11
8. Landoll D., Information Security Policies, Procedures and Standards - A Practitioner’s Reference, CRC Press, Taylor & Francis Group, 2016, ISBN 978-1-4822-4591-2
9. Гайдарски И., Кутинчев П., Откриване на вътрешни заплахи и предотвратяване изтичането на чувствителна информация от организацията, Научна конференция "Необходима достатъчност за осигуряване на въздушния суверенитет на България и ролята на човешкия фактор", Военна Академия "Г.С.Раковски", 11.10.2018, София, България, ISBN 978-619-7478
10. Whitman M, Mattord H., Principles of Information Security, Fourth Edition

Course Technology, Cengage Learning, 2012
11. Gragido W., Pirc J.. Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats. Syngress, 2011.
12. Keung Y., “Information Security Controls”, Adv Robot Autom 2013, Department of Systems Engineering and Engineering Management, City University of Hong Kong, Kowloon Tong, Hong Kong
13. Bhaskar SM, Ahson SI (2008) Information Security: A practical Approach, Oxford: Alpha Science International Ltd.
14. Schweitzer JA, Managing Information Security: Administrative, Electronics, and Legal measures to Protect Business Information. Boston: Butterworths. 1990
15. Наредба за минималните изисквания за мрежова и информационна сигурност, https://www.mtitc.government.bg/sites/default/files/nar_minimalnite_iziskvaniq_mrejova_info_sigurnost-072019.pdf, last accessed 2021/08/11
16. Guide for Conducting Risk Assessments. NIST Special Publication 800-30 rev.1, NIST, September 2012, https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final, last accessed 2021/08/11
17. Guidelines on assessing DSP and OES compliance to the NISD security Requirements, ENISA, November 2018, https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements,last accessed 2021/08/11
18. Standards, Guidelines, Tools and Techniques, ISACA, May 2016, https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/standards-guidelines-tools-and-techniques , last accessed 2021/08/11
19. Шаньгин В.Ф. “Защита информации в компьютерниьх системах и сетях”, ДМК Пресс 2012, ISBN 978-5-94074-637-9
20. Hayden L., “IT Security Metrics: A Practical Framework for measuring Security & Protecting Data, 2010 by The McGraw-Hill, ISBN: 978-0-07-171341-2
21. Alhassan M, Adjei-Quaye A., Information Security in an Organization, International Journal of Computer (IJC), Global Society of Scientific Research and Researchers 2017, ISSN 2307-4523
22. Dimitrov W, Syarova S., Analysis of the functionalities of a Shared ICS Security Operations Center, International Conference “Big Data, Knowledge and Control Systems Engineering” 6th IEEE International Conference BdKCSE'2019, 21-22 November 2019, Sofia, Bulgaria
23. Accenture Security 2019 Cyber Threatscape Report, 2019 https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf, last accessed 2021/08/11
24. Insider Threat Report, Verizon 2019, https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf, last accessed 2021/08/11
25. ENISA Threat Landscape - Responding to the Evolving Threat Environment European Network and Information Security Agency (ENISA), 2012, https://www.enisa.europa.eu/publications/ENISA_Threat_Landscape/at_download/fullReport, last accessed 2021/08/11
26. ENISA Threat Landscape Report 2020 - 15 Top Cyberthreats and Trends, European Network and Information Security Agency (ENISA), 2019, https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020, last accessed 2021/08/11
27. Минчев З., Кутинчев П., Гайдарски И.. Топ 10 заплахи за киберпространство през 2019. IT4Sec Reports, Institute of ICT, Bulgarian Academy of Sciences, 2019, ISSN:1314-5614, DOI:10.11610/it4sec.0133, 133-1-133-12 Национално академично

издателство
28. Bollinger J., Enright B., Valites M., Crafting the InfoSec Playbook, O'Reilly Media, Inc., 2015, ISBN: 978-1-491-94940-5
29. Andress J., The basics of information security : understanding the fundamentals of InfoSec in theory and practice, Elsevier Inc. 2011
30. Taylor-Duncan L., Come in, We're Open – Keeping Your Company's IT Data Safe From Threats, Techni-Core productions, 2014
31. SysSec Red Book - Roadmap in the area of Systems Security, SysSec consortium, http://www.red-book.eu/, last accessed 2021/08/11
32. Минчев З., Гайдарски И., Кибер рискове, заплахи и мерки за защита, свързани с COVID-19, CSDM Views, Number 37, 2020, ISSN 1314-5622
33. Gaydarski I.,Discovery and Protection from Internal Threats in Critical Infrastructure's objects., Proceedings of BISEC 2019, Belgrade Metropolitan University, Belgrade Metropolitan University, приета за печат: 2019
34. Yassein M., Hmeidi I., Mohammad Al-Rousan Y., Arrabi D., Black Hole Attack Security Issues, Challenges & Solution In Manet, Conference: International Conference on Computer Science, Engineering and Information Technology (CSEIT-2018) Dubai, UAE, DOI: 10.5121/csit.2018.81815
35. Chandler J., Security in Cyberspace: Combatting Distributed Denial of Service Attacks, University of Ottawa, January 2003
36. Understanding Denial-of-Service Attacks, Cybersecurity & Infrastructure Security Agency, USA, https://www.us-cert.gov/ncas/tips/ST04-015, last accessed 2021/08/11
37. WASC Threat Classification v2.0, Web Application Security Consortium, 2010, http://projects.webappsec.org/f/WASC-TC-v2_0.pdf?ld=1 , last accessed 2021/08/11
38. LizaMoon Mass SQL-Injection Attack Infected at least 500k Websites, https://isc.sans.edu/forums/diary/LizaMoon+Mass+SQLInjection+Attack+Infected+at+least+500k+Websites/10642, last accessed 2021/08/11
39. Botnets: Measurement, Detection, Disinfection and Defence, European Network and Information Security Agency (ENISA), March 2011, https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence, last accessed 2021/08/11
40. DDoS Malware, Verisign 2013, https://www.informationweek.com/pdf_whitepapers/approved/1370027144_VRSNDDoSMalware.pdf , last accessed 2021/08/11
41. Nazario J., BlackEnergy DDoS Bot Analysis.. Arbor Networks, 2007, http://pds15.egloos.com/pds/201001/01/66/BlackEnergy_DDoS_Bot_Analysis.pdf, last accessed 2021/08/11
42. Tracking GhostNet: Investigating a Cyber Espionage Network. Information Warfare Monitor, March 2009, https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf, last accessed 2021/08/11
43. Shadows in the Cloud: An investigation into cyber espionage 2.0. Information Warfare Monitor and Shadowserver Foundation, 2010, https://citizenlab.ca/wp-content/uploads/2017/05/shadows-in-the-cloud.pdf, , last accessed 2021/08/11
44. Keizer, G., Is Stuxnet the 'best' malware ever?, Computerworld, September 2010. http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever, last accessed 2021/08/11
45. Gaydarski I., Kutinchev P., Holistic Approach to Data protection - identifying the weak points in the organization.. Proceedings of BdKCSE'2017 (7 December, 2017 Sofia), САИ, 2018, ISSN:2367-6450, 125-135
46. Gaydarski I, Minchev Z.. Challenges to Data Protection in Corporate Environment, Chapter 8, In Minchev Z., (Ed) Book "Future Digital Society Resilience in the Informational

Age", Sofia, Institute of ICT, Bulgarian Academy of Sciences, SoftTrade, December, 2018, ISBN 978-954-334-221-1, 82-100
47. Parsons, S., Gymtrasiewicz, P. and Wooldridge, M. (Eds). Game Theory and Decision Theory in Agent-Based Systems (Multiagent Systems, Artificial Societies, and Simulated Organizations), Springer, 2002.
48. Wahlstrom B. "Perspectives of Human Communication", Wm.C.Brown Publishers, 1992, ISBN 0-697-10704-3
49. Nwana, H. and Ndumu, D. An Introduction to Agent Technology, Software Agents and Soft Computing: Towards Enhancing Machine Intelligence, Concepts and Applications, Lecture Notes in Computer Science 1198, Springer, 3-26,1997.
50. Russel, S., Norving, P. Artificial Intelligence: A Modern Approach, Prentice Hall, New Jersey, 1995.
51. Wooldridge M, An Introduction To Multiagent Systems, John Wiley & Sons 2002, ISBN: 047149691X
52. Buecker A., Andreas P., Paisley S., Understanding IT Perimeter Security, Redpaper, IBM, November 2009, https://www.redbooks.ibm.com/redpapers/pdfs/redp4397.pdf, last accessed 2021/08/11
52. Santana G.,Cruz D., Modelling a network security systems using multi-agents systems engineering, Systems, Man and Cybernetics, 2003. IEEE International Conference, Vol.5, November 2003, DOI: 10.1109/ICSMC.2003.1245655
53. Guidelines for Data Classification, Carnegie Mellon University, https://www.cmu.edu/iso/governance/guidelines/data-classification.html,
last accessed 2021/08/11
54. Ahmed S., Karsiti M., Multiagent Systems ,In-Teh Croatia, 2009, ISBN 978-3-902613-51-6
55. Закон за киберсигурност, приет на 31 октомври 2018, 7 ноември 2018, https://www.mlsp.government.bg/uploads/3/zakonodatelstvo/za-kibersigurnost.pdf, last accessed 2021/08/11
56. Национална стратегия за киберсигурност „Кибер устойчива България 2020", Юли 2016, http://www.strategy.bg/StrategicDocuments/View.aspx?Id=1120, , last accessed 2021/08/11
57. Полимирова Д, Шаламанов В., Стоянов Н, Тагарев Т., Янакиев Я., Шарков Г., Папазов Я., Ризов В., Иванова К., Киберсигурност и възможности за приложение на иновативни технологии в работата на държавната администрация в България, Институт за публична администрация, 2019, ISBN 978-619-7262-14-8
https://www.ipa.government.bg/sites/default/files/01_ipa_study_v10.0._final_ed.pdf, last accessed 2021/08/11
58. Olivé A., Conceptual Modeling of Information Systems, January 2007, Springer DOI: 10.1007/978-3-540-39390-0
59. Mallikaarachchi V., Data Modeling for System Analysis, INFORMATION SYSTEMS ANALYSIS - IS 6840, University of Missouri, St. Louis, 2010
http://www.umsl.edu/~sauterv/analysis/Fall2010Papers/varuni/, last accessed 2021/08/11
60. Edgar T., Manz D., Research Methods for Cyber Security, Elsevier Inc. 2017, ISBN: 9780128053492
61. Saltzer J., Schroeder M., "The protection of information in computer systems," in Proceedings of the IEEE, vol. 63, no. 9, pp. 1278-1308, September 1975
62. Turing A., Computing Machinery and Intelligence, Mind, Volume LIX, Issue 236, October 1950, Pages 433–460, https://doi.org/10.1093/mind/LIX.236.433,
63. Laplante P., What Every Engineer Should Know about Software Engineerin, Boca Raton, CRC, 2007. ISBN 9780849372285
64. Cyber Kill Chain, Lockheed Martin https://www.lockheedmartin.com/en-

us/capabilities/cyber/cyber-kill-chain.html , last accessed 2021/08/11
65. Hutchins, E. M., Michael J. Cloppert, and Rohan M. Amin. “Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains.” Leading Issues in Information Warfare & Security Research Volume 1. 2011, pp. 80-106.
66. Finkelsetin A, Kramer J., Nuseibeh B., Finkelstein L., Goedicke M., Viewpoints - A Framework for Integrating Multiple Perspectives in System Developmen, International Journal of Software Engineering and Knowledge Engineering 02(01), November 2011
67. Hilliard R.,Emery D., Maier M., ANSI/IEEE 1471 and Systems Engineering, Systems Engineering 7(3):257 - 270, June 2004, DOI: 10.1002/sys.20008
68. Общ регламент относно защита на личните данни (Регламент (ЕС) 2016/679), https://cpdp.bg/?p=element&aid=991 , last accessed 2021/08/11
69. Националната стратегия за киберсигурност „Киберустойчива България 2020”, приета от Министерски съвет на Република България на 13 юли 2016 г., http://www.cyberbg.eu/, last accessed 2021/08/11
70. Актуализирана стратегия за национална сигурност на Република България, приета с Решение на Народното събрание от 14 март 2018 г, https://www.mod.bg/bg/doc/cooperation/20181005_Akt_strateg_NS_RB.pdf, last accessed 2021/08/11
71. Стратегията за национална сигурност на Република България, https://me.government.bg/bg/themes/bulgaria-s-national-security-strategy-904-0.html, last accessed 2021/08/11

72. Закон за управление и функциониране на системата за защита на националната сигурност, Ноември 2015, https://www.parliament.bg/bg/laws/ID/15270, last accessed 2021/08/11
73. Правилник за дейността, структурата и организацията на Държавна агенция “Електронно управление”, приет с постановление № 274 от 28 октомври 2016, https://dv.parliament.bg/DVWeb/showMaterialDV.jsp?idMat=108729, last accessed 2021/08/11
74. Закон за киберсигурност, приет от Народното събрание на 31 октомври 2018 г, https://parliament.bg/bg/laws/ID/78098, last accessed 2021/08/11
75. Закон за защита на класифицираната информация, 26.02.2019г. https://www.damtn.government.bg/wp-content/uploads/2019/06/zakon-za-klasifitsiranata-informacia.pdf, last accessed 2021/08/11
76. БДС EN ISO/IEC 27001:2017 „Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията", https://www.bds-bg.org/bg/project/show/bds:proj:102367, last accessed 2021/08/11
77. Директива 2016/1148 ЕС относно мерки за високо общо ниво на сигурност на мрежовите и информационни системи в Съюза, https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32016L1148, last accessed 2021/08/11
78. J. Hintzbergen, K. Hintzbergen, A. Smulders, and H. Baars, “Foundations of Information Security Based on ISO27001 and ISO27002,” 3rd Edition, Van Haren Publishing, 2015.
79. ISO 27001 Official Page, https://www.iso.org/isoiec-27001-information-security.html, last accessed 2021/08/11
80. COBIT Security Baseline: An Information Survival Kit, 2nd Edition, IT Governance Institute, 2007.
81. COBIT resources, http://www.isaca.org/COBIT/Pages/default.aspx, last accessed 2021/08/11
82. NIST Special Publications (800 Series), https://csrc.nist.gov/publications/sp800, last accessed 2021/08/11

83. Gramm-Leach-Bliley Act (GLBA) Resources, www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act, last accessed 2021/08/11
84. S. Anand, Sarbanes-Oxley Guide for Finance and Information Technology Professionals, 2nd, Wiley, Edition, 2006
85. Sarbanes-Oxley Act, https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry#sox2002, last accessed 2021/08/11
86. R. Herold and K. Beaver, "The Practical Guide to HIPAA Privacy and Security Compliance," 2nd Edition, CRC Press, 2014
87. PCI Security Standards, https://www.pcisecuritystandards.org/pci_security/ , last accessed 2021/08/11.
88. IEEE 1471, IEEE Recommended Practice for Architectural Description of Software-Intensive Systems, https://standards.ieee.org/standard/1471-2000.html, last accessed 2021/08/11
89. ISO/IEC/IEEE 42010:2011 – Systems and Software Engineering – Architecture Description, https://www.iso.org/standard/50508.html, last accessed 2021/08/11
90. Наков С., Колев В., Принципи на програмирането със C#, Издателство Фабер, Велико Търново 2018, ISBN: 978-619-00-0778-4
91. Горанов П., Тодорова Е., Георгиева Д., Концептуален модел на обектно-ориентирана библиотека от механични компоненти, Българско списание за инженерно проектиране, брой 35, януари 2018г, ISSN 1313-7530
92. Митрев Р., Компютърно моделиране и симулация, Пропелер, София, 2016г
93. A. Solvberg, Data and What They Refer to, Conceptual Modeling, Lecture Notes in Computer Science, vol 1565. Springer, Berlin, Heidelberg, 1999. https://doi.org/10.1007/3-540-48854-5_17
94. L. Vigotsky, Thought and Language, The M.I.T. Press, USA, 1962
95. DeviceLock Web Page, https://www.acronis.com/en-us/products/devicelock, last accessed 2021/08/11
96. CoSoSys Endpoint Protector Web Page, https://www.endpointprotector.com/, last accessed 2021/08/11
97. The Unified Modeling Language (UML) Web Page, https://www.uml-diagrams.org accessed 2021/08/11
98. A. Dennis, B. Wixom, and D. Tegarden, "System Analysis & Design – An Object-Oriented Approach with UML," 5th Edition, John Wiley & Sons, 2015, pp. 19-52.
99. Gaydarski, I., Minchev, Z., Andreev, R.. Model Driven Architectural Design of Information Security System. Advances in Intelligent Systems and Computing, Madureira A., Abraham A., Gandhi N., Silva C., Antunes M. (eds) Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018)., 492, Springer, 2019, ISBN:978-3-030-17064-6, ISSN:2194-5357, DOI:10.1007/978-3-030-17065-3_35, 349-359.
100. Gaidarski, I. K., Minchev, Z. B., Andreev, R. D.. Model Driven Approach for Designing of Information Security System. Journal of Information Assurance and Security, 13, MIR Labs, 2019, ISSN:1554-1010, 149-158,
101. Gaydarski, I., Minchev, Z., Conceptual Modeling of Information Security System and Its Validation Through DLP Systems. Proceedings of BISEC 2017, Belgrade Metropolitan University, 2017, ISBN:978-86-89755-14-5, DOI: 10.13140/ RG.2.2.32836.53123, 36-40
102. Gaydarski, I., Minchev, Z.. Virtual Enterprise Data Protection: Framework Implementation with Practical Validation. Proceedings of BISEC 2018, October 20, Belgrade, Serbia, Belgrade Metropolitan University, 2019, ISBN:978-86-89755-17-6,
103. Gaydarski, I., Minchev, Z., Andreev, R.. Model Driven Architectural Design of Information Security System. Advances in Intelligent Systems and Computing, Madureira A., Abraham A.,Gandhi N., Silva C., Antunes M. (eds) Proceedings of the Tenth

International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018)., 492, Springer, 2019, ISBN:978-3-030-17064-6, ISSN:2194-5357, DOI:10.1007/978-3-030-17065-3_35, 349-359.
104. Гайдарски И., Минчев З., „Моделиране, анализ, експериментална валидация и верификация на системи за информационна сигурност в корпоративна среда“, IT4SEC Reports, No. 132, 2019, стр. 1-29, ISSN 1314-5614
105. Minchev Z., “Methodological Approach for Modelling, Simulation & Assessment of Complex Discrete Systems,” In Proc. of National Informatics Conference Dedicated to 80-th Anniversary of Prof. Petar Barnev, Sofia, Bulgaria, Institute of Mathematics & Informatics, Bulgarian Academy of Sciences, 2016, pp. 102-110, DOI: 10.13140/RG.2.1.1865.4481
106. Boyanov L., Minchev Z., “Cyber Security Challenges in Smart Homes,” In Proceedings of NATO ARW “Best Practices and Innovative Approaches to Develop Cyber Security and Resiliency Policy Framework,” Ohrid, Macedonia, June 10-12, Published by IOS Press, NATO Science for Peace and Security Series - D: Information and Communication Security, Vol.38, 2013, pp. 99 – 114.
107. Gaydarski I., Minchev Z.. Challenges to Data Protection in Corporate Environment, Chapter 8, In Z. Minchev, (Ed) Book “Future Digital Society Resilience in the Informational Age”, Sofia, Institute of ICT, Bulgarian Academy of Sciences, SoftTrade, December, 2018, ISBN 978-954-334-221-1, 82-100
108. Chen P., “The Entity-Relationship Model-Toward a Unified View of Data,” ACM Transactions on Database Systems 1, 1976, pp. 9-36.
109. Minchev Z., “Data Relativities in the Transcending Digital Future,” In Proc. of BISEC 2018, Belgrade, Serbia, October 20, 2018 (in press)
110. Minchev Z., Dukov G., Cyber Intelligence Decision Support in the Era of Big Data, In ESGI 113 Problems & Final Reports Book, Chapter 6, Fastumprint, 2015, pp. 85-92.
111. Minchev Z., “Security Challenges to Digital Ecosystems Dynamic Transformation,” In Proc. of BISEC 2017, Belgrade, Serbia, October 18, 2017, pp. 6-10.
112. Sycara K., “Multiagent Systems,” AI Magazine, 19, No. 2, 1998, pp. 79-92.
113. Gaydarski, I., Kutinchev,P.. Using Big Data for Data Leak Prevention. proceedings of The International Conference “Big Data, Knowledge and Control Systems Engineering” (BdKCSE’2019)), IEEE Digital Library, 2020, ISSN:2367-645, DOI:10.1109/BdKCSE48644.2019.9010596
114. Data Breach Investigations Report 2021, Verizon, 2021,: https://www.verizon.com/business/resources/reports/dbir/, last accessed 2021/08/11
115. Forrester J., “World Dynamics,” Cambridge, Massachusetts, Wright-Allen Press, 1971.
116. Meadows D., Randers J., Meadows D., Limits to Growth: The 30-Year Update, Chelsea Green Publishing Company, 2004.
117. CYREX 2018 Web Page: http://securedfuture21.org/cyrex_2018/cyrex_2018.html , last accessed 2021/08/11
118. Jain L., Lim C., Knowledge Processing and Decision Making in Agent-Based Systems, Springer-Verlag Berlin Heidelberg 2009, ISBN 13:978-3-540-88049-3
119. БДС EN ISO/IEC 27002:2017 “Информационни технологии. Методи за сигурност. Кодекс за добра практика за управление на сигурността на информацията”, https://www.bds-bg.org/bg/project/show/bds:proj:102368, last accessed 2021/08/11
120. БДС EN ISO/IEC 27003:2020 “Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Указания”, https://www.bds-bg.org/bg/project/show/bds:proj:114396, last accessed 2021/08/11
121. БДС ISO/IEC 27004:2017 "Информационни технологии. Методи за сигурност.

Управление на сигурността на информацията. Наблюдение, измерване, анализ и оценяване", https://www.bds-bg.org/bg/project/show/bds:proj:102534, last accessed 2021/08/11
122. CYREX 2019 Web Page, http://securedfuture21.org/cyrex_2019/cyrex_2019.html, last accessed 2021/08/11
123. CYREX 2020 Web Page, http://securedfuture21.org/cyrex_2020/cyrex_2020.html, last accessed 2021/08/11
124. Gaidarski I., Minchev Z. (2021) Insider Threats to IT Security of Critical Infrastructures. In: Tagarev T., Atanassov K.T., Kharchenko V., Kacprzyk J. (eds) Digital Transformation, Cyber Security and Resilience of Modern Societies. Studies in Big Data, vol 84. Springer, Cham. https://doi.org/10.1007/978-3-030-65722-2_24
125. Schrecker S.,Soroush H., Molina J., Industrial Internet of Things Volume G4: Security Framework Paperback, Industrial Internet Consortium, September 19, 2016
126. Vester F., "The Art of Interconnected Thinking – Ideas and Tools for Dealing with Complexity," München, MCB – Verlag, 2007.
127. MITRE ATT&CK® Framework, https://attack.mitre.org/, last accessed 2021/08/11
128. NIST Cybersecurity Framework, https://www.nist.gov/cyberframework, last accessed 2021/08/11
129. Open Web Application Security Project, https://www.owasp.org/, last accessed 2021/08/11
130. Common Attack pattern Enumeration and Classification, http://capec.mitre.org/ , last accessed 2021/08/11
131. ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, https://www.iso.org/standard/50341.html, last accessed 2021/08/11
132. ISO 31000:2009 Risk management — Principles and guidelines, https://www.iso.org/standard/43170.html, last accessed 2021/08/11
133. Risk and Responsibility in a Hyperconnected World - Pathways to Global Cyber Resilience
http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf, last accessed 2021/08/11
134. Tagarev T., Polimirova D., Main Considerations in Elaborating Organizational Information Security Policies, Proceedings of the 20th International Conference on Computer Systems and Technologies CompSysTech '19, June 2019, DOI: 10.1145/3345252.3345302
135. Hilliard R.,Malavolta I., Muccini H., Pelliccione P., On the Composition and Reuse of Viewpoints across Architecture Frameworks, Joint Working IEEE/IFIP Conference on Software Architecture and European Conference on Software Architecture 2012, ISBN:978-1-4673-2809-8, DOI: 10.1109/WICSA-ECSA.212.21
136. Bezivin J., Jouault F., Valduriez P., "On the Need for Megamodels," in Proceedings of the OOPSLA/GPCE: Best Practices for Model-Driven Software Development workshop, 2004.
137 Symantec Data Loss Prevention Web Page, https://www.broadcom.com/products/cyber-security/information-protection/data-loss-prevention/, last accessed 2021/12/14
138 McAfee DLP Endpoint Web page, https://www.mcafee.com/enterprise/en-us/products/dlp-endpoint.html, last accessed 2021/12/14
139 Forcepoint DLP Web Page, https://www.forcepoint.com/product/dlp-data-loss-prevention/, last accessed 2021/12/14

БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ

АВТОРЕФЕРАТ НА ДИСЕРТАЦИЯ

за присъждане на образователна и научна степен "доктор" по научна специалност "Компютърни системи, комплекси и мрежи"

МЕТОД И МОДЕЛИ ЗА РАЗРАБОТКА НА СИСТЕМИ ЗА ИНФОРМАЦИОННА СИГУРНОСТ В ОРГАНИЗАЦИИ

Иван Костадинов Гайдарски

Ръководител: Доц. Румен Андреев

Научно жури:

Проф. Иван Гарванов
Проф. Радослав Йошинов
Проф. Румен Трифонов
Проф. Тодор Тагарев
Доц. Светозар Илчев

Институт по информационни и комуникационни технологии

Секция „Комуникационни системи и услуги"

Обща характеристика на дисертационния труд

Актуалност на темата

Информацията е един от най-ценните активи на съвременните организации. Интелектуалната собственост, ноу-хау, патенти, списъци с клиенти и доставчици – тази информация е жизненоважна за всяка организация и формират нейното конкурентно предимство. Едно от най-важните предизвикателства пред тях е защитата на информацията във всички и форми – електронна и физическа. Информацията трябва да бъде надеждно защитена както от външни атаки – хакери или природни бедствия, така и от вътрешни – настоящи и бивши служители, партньори и доставчици. Тяхното право на достъп до ресурсите на организацията като системи, мрежи и данни изисква защитата от нерегламентираното изтичане на информация да се съобразява със стратегия, различна от тази при традиционната защита срещу външни за организацията заплахи [1, 2].

Главните заплахи в наши дни са свързани с данните и информационните активи. Колкото са по-ценни активите, на толкова повече атаки са изложени. Новите и съществуващите уязвимости водят до по-висока успеваемост на атаките. Поради това заплахите силно зависят от уязвимостите, които могат да бъдат експлоатирани от атакуващата страна. Всяка промяна в един от факторите води до увеличаване на обхвата му. Например, увеличаването на възможностите на агентите на заплахата респективно водят до по-успешна идентификация и експлоатация на уязвимосттите, и съответно до по-голяма успеваемост на атаките [25]. Въвеждането на нови информационни активи води до увеличаване на атакуемата повърхност, съответно до нови слабости/уязвимости, нови методи за атака и нови заплахи. Въвеждането на последните технологични новости води до слабости, които са свързани с технологичната незрялост, неправилна употреба, неправилна интеграция със съществуващите системи, ниска информираност на потребителите и др. Това създава почва за нови заплахи, насочени към тези активи [25]. За да бъдат редуцирани успешните атаки към информационните активи е необходимо да бъде извършен анализ на всички елементи във веригата уязвимости-заплахи - атаки.

В организациите се създават, приемат и одобряват единна политика за сигурност, процедури и процеси за информационна сигурност. Те са резултат от влиянието на различни фактори – територията, на която организацията развива дейност, регулаторни режими, специфични за дадения сектор изисквания, стандарти и добри практики. Един от основните фактори, с който трябва да се съобрази организацията е националното законодателство, действащо на територията на държавата, в която тя е регистрирана или оперира – данъчно законодателство, наказателен кодекс, разрешителни режими и други. В аспекта на Системите за Информационна Сигурност (СИС), в областта на нашия интерес са нормативните актове, формиращи основата на държавната политика в областта на кибер сигурността - сигурност в кибер пространството, дейности по кибер отбрана и по противодействие на кибер престъпността [57].

Особено внимание трябва да се обърне на обработваните от организацията данни – често те подлежат на допълнителни регулации, необхващащи останалата дейност на организацията. Например за организация, базирана в Япония, Регламент (ЕС) 2016/679 не обхаща локалните лични данни, които тя обработва, освен ако тя не принадлежат на граждани на ЕС. Различните организации могат да дефинират и използват различни типове чувствителни данни в зависимост от своите нужди, законодателната рамка, действащите регулаторни режими – например регулации, приети политики за сигурност, нужни сертификации, специфични данни при участие в

определени проекти или обединения от няколко организации.

В информационната сигурност се използват редица подходи за защита, всеки от които има определена област на приложение, отговаряща на въпроса „Къде?“ и определена функционалност - „Как?“. За пример можем да използваме многослойния модел на защита, състоящ се от няколко слоя - Външна мрежа, Мрежов периметър, Вътрешна мрежа, Компютърно оборудване, Приложения и Данни. Всеки защитен слой е подложен на различни по характер заплахи и за защита от тях разполага с определен набор от подходи за сигурност. За комплексната защита на организацията се комбинират подходите за информационна защита при мрежова комуникация и подходите за защита на данни при йерархична организационна комуникация. Към познатите ни подходи за информационна защита при мрежови комуникации можем да добавим и допълнителни подходи, като демилитаризирана зона, виртуална частна мрежа, одит, тестове за проникване, анализ на уязвимости, хеширане на пароли, филтриране по и други [29].

Всеки един от тези подходи има своята роля и особености при защитата на определени активи, намиращи се в определен слой, и изискващи определени усилия и ресурси. Информационната сигурност (ИС) е свързана със осигуряване на безопасността на тези активи. Най-добрият подход за това е да се разгледа всеки актив в контекста на свързания с него риск от загуба и неговата стойност. Основна цел на ИС е защита на информацията във всичките ѝ форми. В резултат на повсеместното проникане на информационните технологии, информационната сигурност има отношение към все повече аспекти на съвременния живот, като производство, работен процес, ежедневна комуникация, пазаруване или забавления [29]. Същото важи и за жизненоважните обекти от критичната инфраструктура, осигуряващи електричество, вода, телекомуникации, транспорт. Те са изцяло зависими от информационните технологии и най-вече от осигуряването на тяхната безопасност [33]. Информационната сигурност се отнася до защитата на активи – информация, хардуер, софтуер, процеси или комбинации от тях. За да се прецени какво да се защитава, първо трябва да се определи кои активи са ценни и за кого [4].

Проектирането и последващото внедряване на съвременна система за информационна сигурност (СИС) е от съществено значение за жизнеността на съвременната организация, която, освен че трябва да осигури защита на своите активи е необходимо и да се съобразява с редица нормативни и регулационни изисквания, добри практики и стандарти.

Цел и задачи на дисертацията

Целта на дисертацията е създаване на метод и модели за разработване на системи за информационна сигурност, осигуряващи защита от вътрешни заплахи в посока отвътре-навън на чувствителна информация за различни по характер и размер организации. Разработеният метод трябва да е приложим за създаване на СИС, реализиращ подход за защита на чувствителни данни чрез използване на платформа от тип СПИД, подходящ за приложение в различни по големина организации, като обекти от критичната инфраструктура, предприятия, боравещи с индустриални тайни, търговски или научно-изследователски организации.За постигането на тази цел са формулирани следните задачи:

1. Определяне и класифициране на подходи за управление на информационна сигурност и области на приложение;
2. Анализ на областта „Информационна сигурност“ като част от проблемната област на Система за Информационна Сигурност;
3. Описание на проблемната област на Системите за Информационна Сигурност в организации чрез концептуално моделиране;

4. Анализ и приложение на обектно-ориентиран подход при създаване на проектен модел на система за информационна сигурност на базата на създаден концептуален модел;
5. Определяне на подход за трансформиране на проектния модел на СИС в модел на реализация;
6. Симулиране на СИС и анализ на генерираните тестови данни.

Методология

За постигане на формулираните в дисертационния труд цел и задачи е използван обектно-ориентиран подход при проектиране и реализация на софтуерни системи „отгоре-надолу“. Това е методология, използвана широко от софтуерните инженери, при която се цели да се избегне зависимостта от включените в системата конкретни технически средства и се формулира метод за разработване, постигащ висока степен на формализация. Постигнатият резултат обикновено представлява стъпка към постигане на референтен модел за създаване на програмна система в определена област.

Списък с авторски публикации по дисертацията

Публикациите по дисертацията са докладвани и приети за публикуване в сборниците на три международни конференции, едно в специализирано международно списание с импакт фактор и едно в издание на международно академично издателство.

[1] Gaidarski I., Model Driven Development of Information Security System, Problems Of Engineering Cybernetics And Robotics, Bulgarian Academy Of Sciences, 2021, Vol. 76, pp. 47-62, p-ISSN: 2738-7356; e-ISSN: 2738-7364, DOI: 10.7546/PECR.76.21.04

[2] Gaydarski, I., Minchev, Z., Andreev, R.. Model Driven Architectural Design of Information Security System. Advances in Intelligent Systems and Computing, Madureira A., Abraham A., Gandhi N., Silva C., Antunes M. (eds) Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018)., 492, Springer, 2019, ISBN:978-3-030-17064-6, ISSN:2194-5357, DOI:10.1007/978-3-030-17065-3_35, 349-359.

[3] Gaydarski, I., Minchev, Z., Conceptual Modeling of Information Security System and Its Validation Through DLP Systems. Proceedings of BISEC 2017, Belgrade Metropolitan University, 2017, ISBN:978-86-89755-14-5, DOI: 10.13140/RG.2.2.32836.53123, 36-40

[4] Gaydarski, I., Minchev, Z.. Virtual Enterprise Data Protection: Framework Implementation with Practical Validation. Proceedings of BISEC 2018, October 20, Belgrade, Serbia, Belgrade Metropolitan University, 2019, ISBN:978-86-89755-17-6, DOI:10.13140/RG.2.2.19996.33925, 10-15

[5] Gaydarski I., Kutinchev P., Holistic Approach to Data protection - identifying the weak points in the organization.. Proceedings of BdKCSE’2017 (7 December, 2017 Sofia), САИ, 2018, ISSN:2367-6450, 125-135

Участие в проекти

В рамките на разработването на дисертационния труд докторантът е взел участие в следните научни проекти:

1. Научно-изследователски проект на тема: „Концептуално и симулационно Моделиране на Екосистеми за Интернет на Нещата (КоМЕИН)“, Договор № ДН 02/1 от 13.12.2016 г., Конкурс за финансиране на фундаментални научни изследвания – 2016 г., Математически науки и информатика;
2. Програма Млади учени и докторанти в БАН 2017, Научно направление „Информационни и комуникационни науки и технологии“, Научноизследователски проект вх. № 72-00-40-230/10.05.2017 г. на тема „Моделиране на архитектура на системи за информационна сигурност в организации.”.Договор N:ДФНП–17-101/ 28.07.2017. Финансиране: Програма за подпомагане на млади учени и докторанти на БАН–2017г.
3. Научно-изследователски проект на тема: „Информационни и комуникационни технологии за единен цифров пазар в науката, образованието и сигурността (ИКТвНОС)“, Договор N:ДО1-205/23.11.2018

Научни и Научно-приложни приноси:

1. Предложена е нова класификация на подходите за управление на ИС, в зависимост от вида комуникация и детайлно описание на фундамента на областта на информационната сигурност, основаващо се на нейните основни понятия;

2. Предложен е нов метод за разработване на системи за информационна сигурност в организации, който интегрира моделно-базирано разработване на СИС чрез прилагане на подхода „отгоре-надолу“ с нов метод за анализ на проблемната област на този вид системи. Характерно за предложеният метод е, че е технологично независим /условие да послужи за основа за създаване на референтна методология за разработване на този вид системи/; гъвкав /позволява разширяване на съществуваща СИС с нова функционалност/; подпомага постигането на оперативна съвместимост на СИС със съществуваща информационна система на организация чрез използване на един и същи подход за моделиране на двете системи;

3. Разработен е многослоен концептуален модел на проблемната област на системите за информационна сигурност като резултат от прилагането на две и повече от две гледни точки при нейното описание;

4. Конструирани са архитектурен и функционален модели на системите за информационна сигурност на базата на съществуващ концептуален модел на проблемното пространство с помощта на обектно-ориентирания унифициран език за описание на програмни системи UML;

5. Сравнителен анализ на съществуващи СПИД платформи за реализация на базата на изискванията, описани в модела на анализа;

6. Предложен е модел на реализация на СИС в организация, използваща СПИД платформа за реализация „Cososys Endpoint Protector 5.0.2.1“

7. Реализиран е симулационен модел на СИС на базата на обектно-ориентирано описание на архитектурата му чрез използване на агентно-базирано представяне в средите NetLogo и I-SCIP-SA; Симулационно изследване на архитектурата на СИС чрез извършване на стохастична валидация и интерактивна верификация.

Съдържание на дисертацията

Дисертационният труд е в обем от 142 страници, 48 фигури, 13 таблици, 139 цитирани литературни източника и 2 приложения. Състои се от увод, четири глави и заключение, декларация за оригиналност на резултатите, библиография и приложения.

В увода са разгледани актуалност на проблема, основни заплахи в киберпространството, регулации и законови рамки.

В Глава 1 са представени основните концепции и базовите принципи за осигуряването на ИС. Разгледани са различни подходи за управление на ИС, областите на тяхното приложение, както и основните научни области от значение за разработване на системи за ИС. Представен е наш метод за разработване на системи за информационна сигурност в организации, фазите от които се състои, моделите, които се конструират при прилагането му и неговите характеристики. Дефинирана е рамка за описание на архитектура на системата. Формулирани са основната цел и задачи на дисертацията.

В Глава 2 са дефинирани основните понятия в ИС чрез използване на наш метод за анализ на областта на СИС, при който се отчитат гледните точки на всички заинтересовани участници при нейното разработване. Целта е да се приложи подхода „отгоре-надолу при проектиране на такава система, което дава възможност да се достигне до решения, които не са свързани с конкретна реализация и могат да са насочващи при създаване на системи от този вид. В резултат, направеният анализ е основа за създаване на концептуален модел на проблемната област на СИС.

В Глава 3 е представен представен метод за проектиране на Системата за Информационна Сигурност, предназначена за организации и насочена към защита от изтичане на чувствителна информация отвътре-навън, т.е. в резултат от действие на вътрешни лица с легитимен достъп до ресурсите на организацията и до нейните данни. Разгледани са възможностите на обектно-ориентиран подход за създаване на проектен модел на СИС. Показан е начин за трансформиране на концептуалния модел на СИС в обектно-ориентиран проектен модел чрез използване на обектно-ориентирания език за описание UML.

В Глава 4 е описан подход за създаване на модел на реализация на СИС чрез предлаганата от нас методология за разработване на СИС. На базата на проектен обектно-ориентиран модел е изграден ОО модел на реализация, съобразен със съществуваща среда за реализация. Извършен е анализ на проблемната област и на базата на изграден концептуален модел, резултат от този анализ, са уточнени изискванията към архитектурата на разработваната СИС. Извършен е анализ на съществуващи платформи за реализация СПИД и избор на най-подходящата в съответствие с модела на анализа. Показано е как представеният от нас метод дава възможност за моделиране и реализация на нови аспекти от СИС без да се налага системата да се проектира отначало. Представени са и резултати от изпитания на разширена СИС. Създаден е агентно-базиран модел на реализация чрез трансформиране на обектно-ориентиран проектен модел. На базата на агентно-базирания модел е извършена симулация на работата на СИС чрез средите за симулиране NetLogo (v.6.0.4) и I-SCIP-SA. Извършен е анализ на базата на тестовите данни, както и на данни от реални ситуации..

Увод

Увода се състои от актуалност на проблема и основни заплахи в информационната сигурност. Разгледани са актуалните направления за изследване

на заплахи в киберпространството, както и заплахи за сигурността през последната година. Разгледани са и са систематизирани заплахи, свързани с КОВИД-19. Направен е преглед на основните регулации и законови рамки в областта на информационната сигурност – единна политика за сигурност, процедури, процеси и стандарти за ИС, приемани в организациите с цел съвместимост с регулаторни и законови изисквания, стандарти и добри практики за ИС. Направен е обзор на националното законодателство в облaстта на ИС, действащо на територията на държавата в която тя е регистрирана или оперира – данъчно законодателство, наказателен кодекс, разрешителни режими. Показана е структурата на дисертацията.

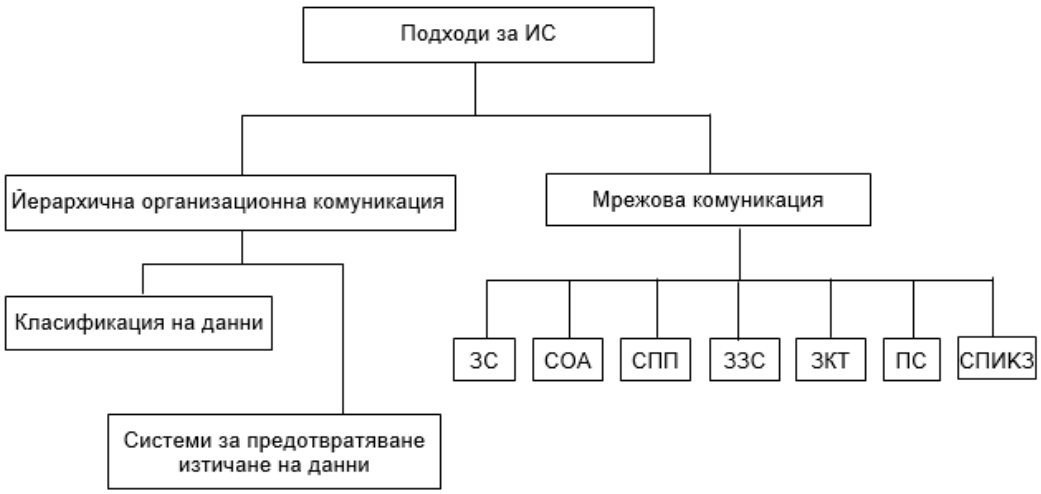
Глава 1. Базови принципи и метод за разработване на система за информационна сигурност

1.1 Базови принципи за осигуряване на информационна сигурност

В тази подточка са разгледани базовите принципи за осигуряване на информационна сигурност, известни като: Триада „Поверителност, Цялостност, Наличност“ (ПЦН Триада, CIA Triad), принципа на тройното А (ААА) и принцип на най-слабото звено. Разглеждаме и базовите защитни модели, като периметрова защита, известна като „Модел на близалката“(Lollipop model), многослоен модел, известен като „Луков модел“ (Onion model) и др.[2, 21].

1.2 Подходи за управление на информационна сигурност

В тази подточка са систематизирани съществуващите подходи за ИС в организации, в зависимост от вида на комуникацията. В организациите могат да се разграничат два вида комуникации, предопределящи подходите за ИС: комуникация на базата на равнопоставеност – „Мрежова комуникация“ (Мрежи от/в организации) и „Йерархична организационна комуникация“ (Фигура 3) [48].



Фигура 3. Подходи за ИС в зависимост от вида комуникация

1. Подходи за управление на ИС при мрежови комуникации:
    - Защитна стена (ЗС);
    - Системи за откриване на аномалии (СОА);
    - Системи за предотвратяване на проникване (СПП);
    - Защита от зловреден софтуер (ЗЗС);

- Защита на крайните точки (ЗКТ);
- Периметрова сигурност (ПС);
- Системи за предварителна информация за кибер-заплахи (СПИКЗ).

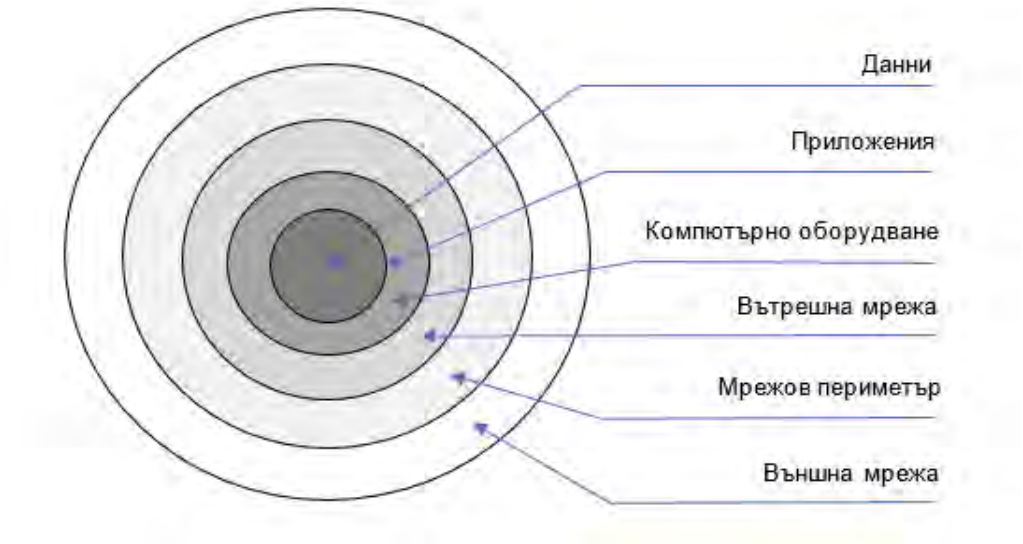
2. Подходи за управление на ИС при Йерархична комуникация в организация:

- Класификация на данни (КД);
- Системи за предотвратяване на изтичане на данни (СПИД).

Подходите за управление на ИС определят начина по който се реализират целите в една СИС.

1.3 Области на приложение на различните подходи за информационна сигурност

Тук са разгледани областите на приложение на различните подходи за защита. За илюстрация може да бъде използван многослойния модел на защита (Фигура 4), състоящ се от няколко слоя:



Фигура 4. Многослоен модел на защита

Всеки защитен слой е подложен на различни по характер заплахи и за защита от тях разполага с определен набор от подходи за сигурност (Таблица 1).

Области на приложение	Подходи за сигурност
Външна мрежа	Демилитаризирана зона, Виртуална частна мрежа, Създаване на дневници, Одит, Тестове за проникване, Анализ на уязвимости, Активна защита чрез примамки (Honepots)
Мрежов Периметър	Защитна стена, Прокси сървър, Създаване на дневници, Пакетна филтрация, Статична пакетна филтрация, Динамична пакетна филтрация, Тестове за проникване, Анализ на уязвимости, Активна защита чрез примамки (Honepots)
Вътрешна мрежа	СОА, СПП, Създаване на дневници, Одит, Тестове за

	проникване, Анализ на уязвимости.
Компютърно оборудване	Автентичност, Защита на крайните точки, Защитна стена, Хеширане на пароли, Създаване на дневници, Одит, Тестове за проникване, Анализ на уязвимости, СПИД.
Приложения	Филтриране по съдържание, Валидация на данни, Одит, Тестове за проникване, Анализ на уязвимости, КД.
Данни	Криптиране, Контрол на достъп, Архивиране на данни, Тестове за проникване, Анализ на уязвимости, Класификация на данни, СПИД, КД, структурни мерки за повишаване на устойчивостта (Resilience)

Таблица 1. Подходи за сигурност и области на приложение

За комплексната защита на организацията се комбинират подходите за информационна защита при мрежова комуникация и подходите за защита на данни при йерархична организационна комуникация. Освен вече познатите ни ЗС, СОА, СПП, ЗЗС, ЗКТ, ПС, СПИКЗ, КД и СПИД, са добавени няколко допълнителни подхода за сигурност [29]: Демилитаризирана зона (DMZ), Виртуална частна мрежа (VPN), Създаване на дневници (Logging), Одит (Auditing), Тестове за проникване (Penetration testing), Анализ на уязвимости (Vulnerability Analisys), Сървър - посредник (Proxy), Пакетна филтрация (Packet Filtering), Статична пакетна филтрация (Static packet Filtering), Динамична пакетна филтрация (Dynamic packet Filtering), Хеширане на пароли (Password Hashing), Филтриране по съдържание (Content Filtering), Валидация на данни (Data Validation), Криптиране (Encryption), Контрол на достъп (Access Controls), Архивиране на данни (Backup), структурни мерки за повишаване на устойчивостта (Resilience), Активна защита чрез примамки (Honepots).

1.4 Основни научни области от значение за разработката на системи за информационна сигурност

Тук са представени основните научни области, необходими за разработката на ефективни системи за информационна сигурност: информационна и кибер-сигурност, проектиране на системи, анализ на данни, големи масиви от данни, машинно самообучение, изкуствен интелект, софтуерно инженерство, и системен анализ.

Разгледани са подробно области като софтуерно инженерство и системен анализ, принципите на които използваме за разработка на нашия метод за проектиране на СИС в организации. Особено внимание е отделено на процеса на разработване на системи (Фигура 5), състоящ се от основни компонента и връзките между тях, разгледани в контекста на разработване на СИС:

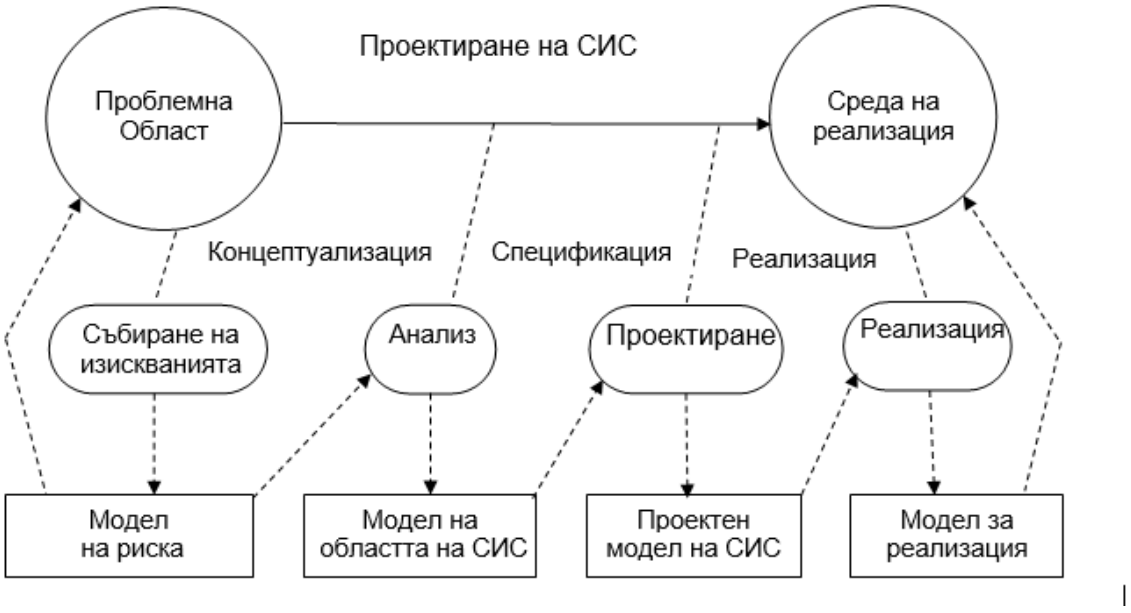
- Проблемна област - дефинира областта в която се решава проблема на СИС;
- Проблем - реализация на определен начин на функциониране на СИС, която трябва да заработи в дадена среда;
- Среда на реализация - представлява условията при които се реализира СИС;
- Етапи - Това са етапите през които трябва да премине разработката на СИС;
- Създаване на модели на СИС на различни етапи от разработката;
- Трансформиране на моделите от един вид в друг.

Различават се следните етапи на разработване на СИС:

- Събиране на изискванията – определяне на възможните рискове според разбирането на потребителите;
- Анализ - изследване на проблемната област от различни гледни точки на заинтересованите страни;
- Проектиране – проектиране на структурата и процесите в системата;
- Реализация – съобразяване на осъществяването на СИС с конкретната среда за реализация.

Моделите, чрез чиято трансформация се достига до реализацията на конкретна СИС са:

- Модел за описание на риска, които се управлява със СИС, на база на събраните изисквания към системата;
- Модел на областта на СИС – модел, получен в резултат на анализа на проблемната област;
- Проектен модел на СИС - описание на архитектурата и функционалността;
- Модел на реализация - модел за реализация на проектираната СИС в зависимост от условията при която тя ще работи.



Фигура 5. Цикъл на разработване на системи

1.5 Метод за разработване на системи за информационна сигурност в организации

Методът се състои от следните фази (Фигура 6):

1. Определяне на рамка за описание на архитектурата на СИС, съгласно стандартите IEEE 1471 [67, 88, 89] и IEEE 42010 [67, 89]. Рамката се формира от множеството от гледни точки на заинтересованите страни/наблюдатели.

2. Анализ на проблемната област на СИС, за определяне на изискванията към системата от различни гледни точки. На базата на този анализ се формират изискванията към СИС.

3. Изграждане на концептуален модел на проблемната област от различни гледни

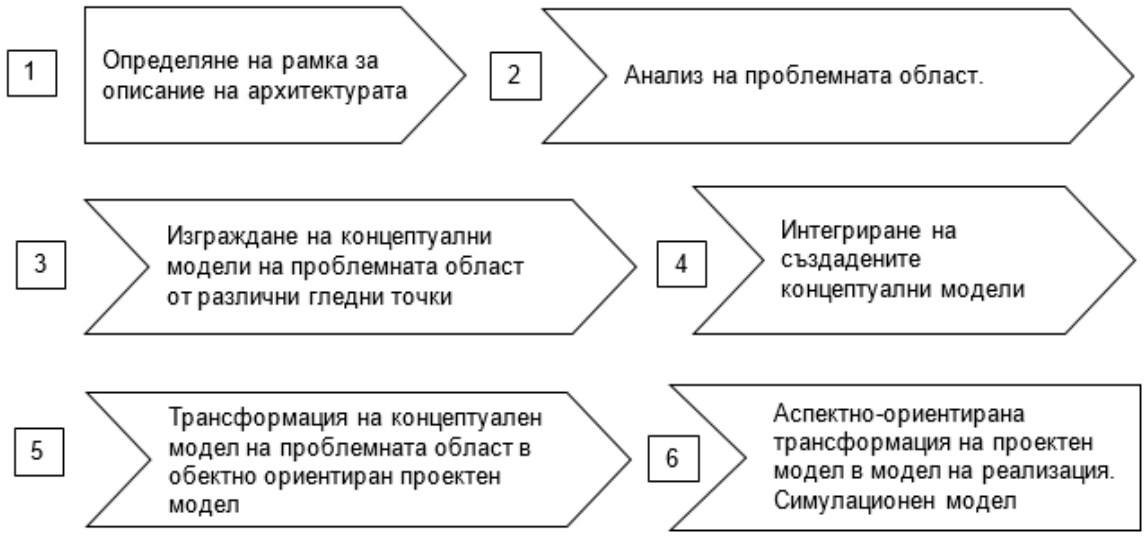
точки. Създаване на обобщен и детайлизирани концептуални модели.

4. Интегриране на концептуалните модели, създадени от различни гледни точки. Подходът на концептуалното моделиране позволява лесно и унифицирано представяне на ниво концепции на СИС от различни гледни точки. Това улеснява комуникацията между наблюдателите на разработваната СИС, които са свързани със съответните гледни точки.

5. Трансформация на концептуален модел на проблемната област в обектно ориентиран проектен модел.

6. Аспектно-ориентирана трансформация на проектен модел в обектно-ориентиран модел на реализация и агентно-базиран симулационен модел.

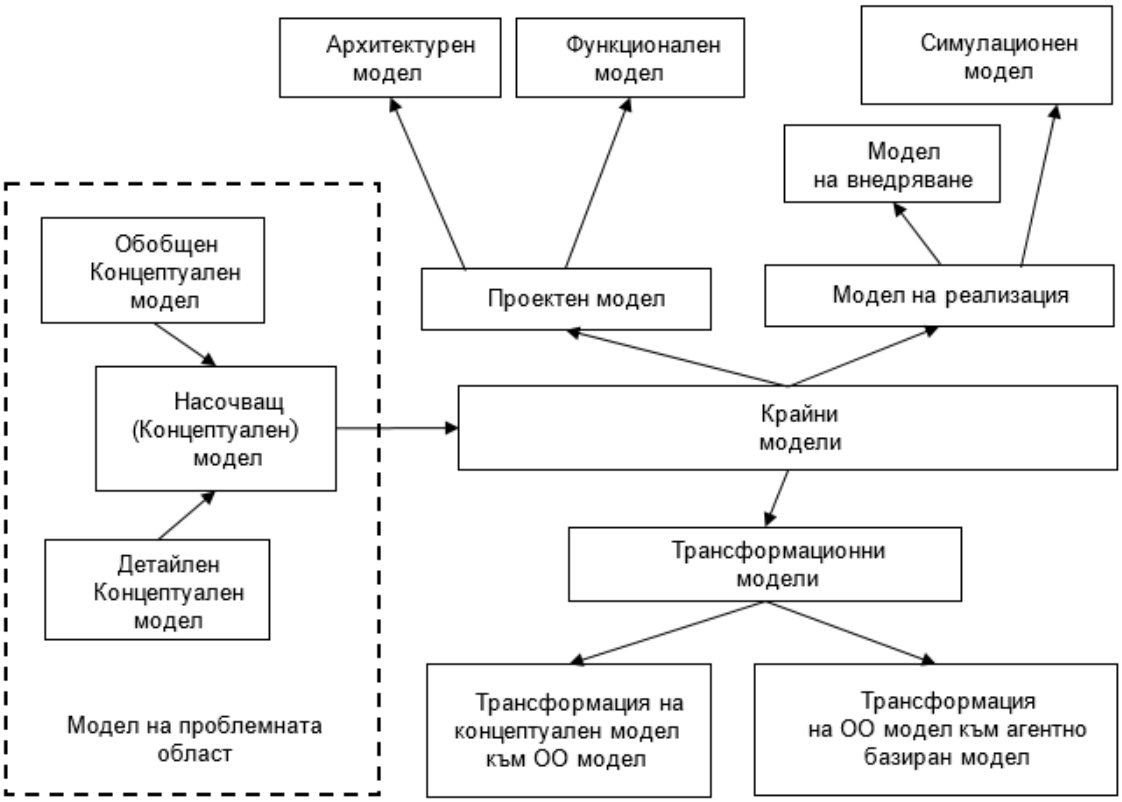
Моделите, които се конструират при прилагане на метода са показани на Фигура 7 [135,136]. На базата на анализ на проблемната област се конструира концептуален модел, наречен "Насочващ модел", чрез който се представя желаната архитектура на системата. Носочващият модел не е свързан с конкретна реализация, а служи за описание на основните компоненти от архитектурата на системата. Концептуалния модел отразява проблемната област от различни гледни точки. От своя страна този модел се състои от "Обобщен модел" и "Детайлен модел".



Фигура 6. Метод за разработване на СИС

На неговата база, след съответна трансформация се създават следващите два основни модела - "Проектен модел" и "Модел на реализация". Проектният модел е обектно-ориентиран и се състои от "Архитектурен" и "Функционален" модели, които представят описанието, съответно на архитектурата и функционалността на системата. "Модела на реализация" представя конкретна реализация на системата и може да се осъществи по два начина - чрез симулация на реална система ("Симулационен модел") и чрез използването на конкретни съществуващи системи, представляващи платформи за реализация на СИС, като СПИД ("Модел на внедряване"). Проектният модел и модела на реализация, са представители на крайните модели, които описват системата за целите на нейното разработване.

Чрез трансформационните модели, се представят трансформациите между моделите - "Трансформация на концептуален модел към ОО модел" и "Трансформация на ОО модел към агентно базиран модел".



Фигура 7. Модели за разработване на СИС

Характеристики на метода:

- Методът е моделно базиран, в резултат на прилагане на подход „отгоре-надолу“;
- Прилага се трансформация от „модел към модел“;
- Аспектно-ориентирана трансформация на проектен модел към модел на реализация в зависимост от две области на интерес на реализатора на системата: обектно-ориентиран подход и агентно-базиран подход.
- Технологично независим, което създава условия да е основа на референтна методология за разработване на СИС

Подходът „отгоре-надолу“, който се прилага при разработване на система за информационна сигурност е подход от общото към частното /конкретното/. Той дава възможност да се прилага и разглежда обща политика, процедури и процеси за ИС с цел постигне на определени цели, Той е подходящ за създаване на референтна методология за разработване на СИС, основана на определяне на рамка за тяхното проектиране, тъй като е технологично независим..

1.6 Дефиниране на рамка за описание на архитектура на системата

Осъществяването на първия етап, се базира на указанията за създаване на рамка за архитектурно описание на системи, представени в стандартите IEEE 1471 [88] и ISO/IEC/IEEE 42010 [89].

Тези стандарти въвеждат понятия, свързани с начина на описание на архитектурата на една система [67]: Околна среда (Environment), Заинтересована страна (Stakeholder), Област на интерес (Concern), Изглед (View), Гледна точка (Viewpoint),

Архитектура на системата (System Architecture), Архитектурно описание (Architectural description), Рамка на създаване на архитектурно описание (Architectural framework), Архитектурен изглед (Architectural View), Архитектурна гледна точка (Architectural Viewpoint), Вид на модела (Model kind).

Тези концепции са приложими при анализа на областта “Система за Информационна сигурност” и осигуряват контекст за дефиниране на обща концептуална рамка, позволяваща изграждането на концептуални модели на СИС. На Фигура 8 е показана областта на интерес на СИС, която се използва за рамка за анализ на областта на система за Информационна сигурност в настоящата дисертация.

Разработването на комплексни системи включва множество участници - всеки със своя собствена перспектива. Това са така наречените „заинтересовани страни“. Всяка заинтересована страна притежава съответни умения, отговорности, знания и опит, които определят отношението и изискванията към системата. При система, в която се използват различни технологии (софтуерни, хардуерни) и има разнообразни нормативни и регулаторни изисквания е неизбежно пресичането или припокриването на различните перспективи на участниците в процеса на нейното разработване. Допълнително усложняващо обстоятелство е факта, че знанията на заинтересованите страни се представят по различни начини. Различните изисквания се отнасят до различни етапи от разработването на системата и всяко от тях може да бъде подчинено на различни стратегии. Така една от важните задачи в процеса на разработка на системата е координацията на заинтересованите страни и унифицираното представяне на техните изисквания и приноси към системата.
Този проблем се решава чрез предлагания от нас метод за разработка на системи за информационна сигурност в организации.

Фигура 8. Област на интерес на СИС

Методът отчита и унифицира изискванията на различните елементи и гледни точки в областта на интерес на системата за информационна сигурност, която разглеждаме:

- Гледна точка „Информационна Сигурност“ – включва основните понятия в информационната сигурност (Заплахи, Уязвимости, Източници, Мотивация и

др.), както и основните подходи за реализиране на информационна сигурност в организации;
- Гледна точка „Риск анализ“ - чрез риск анализа се определят изискванията към СИС;
- Комуникационна гледна точка – определя начина на комуникиране, предопределящ подхода за защита на информацията.
- Технологична гледна точка. Тази гледна точка включва различни подходи при информационните и комуникационни технологии като обектно-ориентиран подход, агентен подход и други.
- Гледна точка „Обработка на информация“– включваща трите основни видове данни, дефинирани съгласно информационната сигурност – Данни в покой (Data-in-Rest), Данни в движение (Data-in-Motion) и Данни в употреба (Data-in-Use).

1.7 Заключение

В главата са представени основните базови принципи и защитни модели за осигуряване на информационна сигурност. Представените подходи за управление на ИС в организации, са разделени в две групи, в зависимост от вида на комуникацията в организацията, предопределящи съответните подходи за ИС: комуникация на базата на равнопоставеност – „Мрежова комуникация“ (Мрежи от/в организации) и „Йерархична организационна комуникация“. Показани са областите на приложение на различните подходи за информационна сигурност.

Представени са основните научни области от значение за разработване на системи за информационна сигурност. Обърнато е специално внимание на системния анализ и цикъла за разработване на системи. Основните компонента и връзки между тях, са разгледани в контекста на разработване на СИС.

Представена е рамка за архитектурно описание на системи, на базата на стандартите IEEE 1471 и ISO/IEC/IEEE 42010.

Дефинирани са основната цел и задачи на дисертацията.

Глава 1 описва изпълнението на задача 1, дефинирана в "Цел и задачи на дисертацията":

- Определяне и класифициране на подходи за управление на информационна сигурност и области на приложение;

В резултат на научноизследователската дейност са постигнати следните научни и научно-приложни приноси:

1. Предложена е нова класификация на подходите за управление на ИС, в зависимост от вида комуникация и детайлно описание на фундамента на областта на информационната сигурност, основаващо се на нейните основни понятия;
2. Предложен е нов метод за разработване на системи за информационна сигурност в организации, който интегрира моделно-базирано разработване на СИС чрез прилагане на подхода „отгоре-надолу“ с нов метод за анализ на проблемната област на този вид системи.

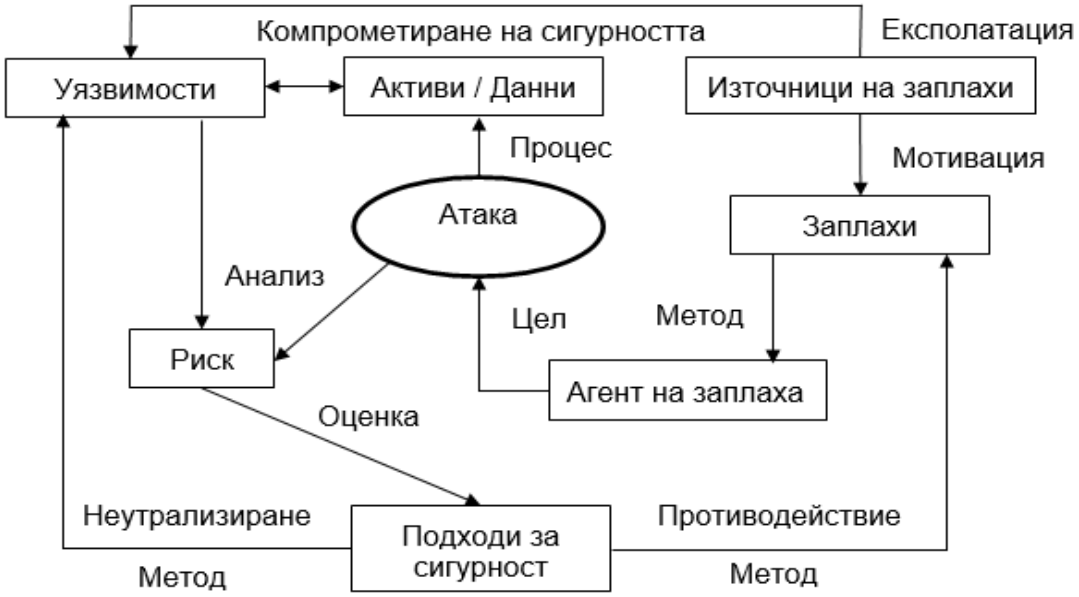
Глава 2. Анализ на проблемната област

2.1 Информационна сигурност - основни понятия и подходи за реализиране

В тази точка са разгледани основните понятия и подходи за реализиране на ИС.

2.1.1 Основни понятия в информационната сигурност

Тук представяме фундамента на областта на информационната сигурност, описан чрез нейните основни понятия (Фигура 9).



Фигура 9. Уязвимости, заплахи и атаки

Дефинираме основните понятия на ИС: „Събитие“, „Сигнали / Аларми“, „Инцидент“, „Нарушение“ (Breach), „Уязвимост“ (Vulnerability), „Заплаха“ (Threat), „Агент на заплаха“ (Threat Agent), „Атака“, „Изтичане на данни“ (Data Breaches), „Загуба на данни“ (Data Loss).

2.1.2 Уязвимости. Заплахи. Източници и агенти на заплахата

В тази поддточка подробно са разгледани понятията „Уязвимости“, „Заплахи“, „Източници“ и „Агенти на заплахата“ и тяхната взаимовръзка.

2.1.3 Вектори, цели и характер на заплахата

Тук са разгледани понятията „Вектор”, „Цел” и „Характер на заплаха”. Според вектора на заплаха, заплахите могат да се класифицират на външни и вътрешни.

„Външни заплахи“

Посоката на атаката при външните заплахи е отвън навътре, срещу защитените информационни активи. При външните заплахи се използва принципа на най-слабото звено. Атакуващата страна се опитва да намери пропуски в защитата чрез които да проникне в защитената мрежа, сървъри или работни станции и да поеме контрол върху информационните активи или инфраструктура. Такива са например: хакерски атаки, DoS атаки, Червеи (Worms), Троянски коне (Trojans), Бот-Мрежи (Botnet), Атаки за отказ на услуга - DoS и DDoS атаки, Заплаха тип Drive-by Exploits, и Инжектиране на код (Code Injection Attacks) [25].

„Вътрешни заплахи“

Инцидент, причинен от вътрешна заплаха възниква, когато вътрешно лице - служител, партньор или доставчик с оторизиран достъп до чувствителна за организацията информация или система, целенасочено или случайно злоупотреби с този достъп, като това води до отрицателни за организацията последствия. Съществуват множество причини за инциденти, свързани с вътрешни заплахи.

- Небрежно поведение на вътрешните лица;
- Доставчици и външни контрактори;
- Прекалено строги политики за киберсигурност – „Security Fatigue“;
- Кражба на електронна идентичност;
- Злонамерени потребители.

Вътрешните заплахи могат да се разделят на няколко основни групи според техния източник: Човешка заплаха, Активност на потребителите и Бизнес-приложения

2.1.4 Атаки и противодействие

В тази поддточка подробно са разгледани категориите атаки, техния механизъм и подходите за неутрализирането им.

2.1.5 Подходи за информационна сигурност

Подходите за информационна сигурност (ПИС) представляват мерки под формата на действия, процеси или процедури, предприети за защита на информационната система от атаките срещу Поверителността, Целостта и Наличността на информационната система. Целта е редуциране на риска, свързан с информационната сигурност [12]. Подходите са организационни, технологични и технически, и се прилагат в съответствие със спецификата на дейността на Субекта [15] (Наредба за минималните изисквания за мрежова и информационна сигурност). Според времето на своето действие, ПИС може да се групират логически в няколко категории [2, 12, 13]: Превантивни, Разкриващи, Възпиращи, Корективни, Възстановителни и Компенсативни.
ПИС могат да имат различна физическа реализация [2,12,13,14]: ПИС за физическа сигурност, Административни, Технологични, Оперативни и Виртуални.

2.2 Риск анализ

В тази точка разглеждаме понятията риск, управление на риска, оценка на риска.и методи за оценка на риска. Като част от оценката на риска са разгледани и процесите на идентифициране на заплахи и уязвимости и оценка на активите. Описани са и процесите на потискане на риска и периодичен процес на оценка

2.3 Видове комуникации

Тук са разгледани видовете комуникация в организацията от гледна точка на подходите за осъществяване:

- *„Йерархична организационна комуникация“* - комуникация в рамките на дадена организация основана на йерархичната структура на организацията;
- *„Мрежова комуникация“* - комуникация, осигуряваща равнопоставеност между участниците в нея.

В зависимост от спецификата на двата вида комуникация се използват различни подходи за информационна сигурност. В настоящата дисертация е разгледана йерархичната организационна комуникация и съответните подходи за защита чрез Системи за предотвратяване изтичането на данни (СПИД), познати още и като Data Leak Prevention.

От гледна точка на комуникационните процедури и тяхното формализиране се различават формална и неформална комуникация:

- *Формалната комуникация* следва както йерархичната структура на организацията, така и хоризонталната комуникация между служителите. Тя се съобразява със зададени шаблони, характерни за организацията, като приоритет имат съобщенията спускани от ръководството надолу по структурата;
- *Неформална комуникация* е ежедневната комуникация между служителите. Тя не следва зададени шаблони, нито строга йерархия, но има жизненоважно значение за организацията, защото чрез нея се извършват всекидневните задачи.

2.4 Технологична гледна точка при проектиране на СИС

В тази подточка са разглеждани различни технологични подходи за разработването на система за информационна сигурност: Обектно-ориентирания подход, Агентен подход и Мулти-агентни системи.

2.5 Обработка на информация

Тук са разгледани видовете данни, обработвани, използвани и създавани от организациите. Всяка организация индувидуално определя кои данни са жизненоважни за нейното функциониране и кои са второстепенни или поддържащи. По дефиниция чувствителните данни са тези данни, които дадена организация не може да си позволи да загуби, да бъдат разкрити или да станат достояние на неоторизирани лица.

В зависимост от това как данните се използват, съхраняват или пренасят от различните системи и приложения се разграничават 3 основни състояния:

- Данни в покой;
- Данни в движение;
- Данни в употреба.

2.6 Заключение

Представеният анализ на областта на системите за информационна сигурност е част от приложения подход за разработване на такива системи, известен като „отгоре-надолу“. Той дава възможност да се разглежда и прилага обща политика, процедури и процеси за ИС с цел постигне на определени цели. Подходящ е за създаване на референтна методология за разработване на СИС, основана на определяне на рамка за тяхното проектиране.

Направен е опит да се осъществи един цялостен поглед върху СИС от няколко гледни точки: Информационна Сигурност, Риск анализ, Обработка на информацията, Подходящи компютърни технологии за разработване на системата и възможни видове комуникация – обект на информационна защита. Всяка гледна точка представлява перспектива, в която трябва да се разглежда областта на съществуване на системата. Най-голямо внимание и най-детайлно е описана областта на информационната сигурност, тъй като тя е фундамента на системите за информационна сигурност.

Взаимосвързаността на отделните гледни точки довежда до интересни резултати. Например съвместното прилагане на комуникационната гледна точка и тази на информационната сигурност довежда до създаване на нова квалификация на подходите за управление на информационната сигурност, която е представена в глава 1 на дисертационния труд. Взаимозависимостта между гледните точки Информационна сигурност и Обработка на информацията довежда до въвеждането на нови понятия и нов аспект за оценка на информацията – чувствителност. Същото може да се каже и за влиянието на гледната точка Информационна сигурност върху

технологията, известна като Агентен подход.

Глава 2 описва изпълнението на задача 2, дефинирана в "Цел и задачи на дисертацията":

- Анализ на областта на Информационна сигурност като част от проблемната област на Система за Информационна Сигурност;

В резултат на научноизследователската дейност за определяне и класифициране на подходи за управление на информационната сигурност и при анализа на информационната сигурност като част от областта на системите за информационна сигурност са постигнати следните научни и научно-приложни приноси:

1. Предложен е нов метод за разработване на системи за информационна сигурност в организации, който интегрира моделно-базирано разработване на СИС чрез прилагане на подхода „отгоре-надолу“ с нов метод за анализ на проблемната област на този вид системи. Характерно за предложеният метод е, че е технологично независим /условие да послужи за основа за създаване на референтна методология за разработване на този вид системи/; гъвкав /позволява разширяване на съществуваща СИС с нова функционалност/; подпомага постигането на оперативна съвместимост на СИС със съществуваща информационна система на организация чрез използване на един и същи подход за моделиране на двете системи;
2. Предложено е детайлно описание на фундамента на областта на информационната сигурност, основаващо се на нейните основни понятия.

Глава 3 Проектиране на система за информационна сигурност в организации. Модел на анализа. Проектен модел.

В тази глава е описан метод за проектиране на система за информационна сигурност чрез създаване на Модел на анализа и Проектен модел. Концентрираме се в проектирането на СИС, предназначена за организации и насочена към защита от изтичане на чувствителна информация отвътре-навън от вътрешни лица с легитимен достъп до ресурсите на организацията и до нейните данни.

3.1 Системна рамка за описание на архитектурата на системи за информационна сигурност в организации

Разработването на СИС преминава през следните етапи (Фигура 5):

1. Уточняване на изискванията към СИС,
2. Системен анализ на изискванията и конструиране на модел на анализа съвпадащ с модел на проблемната област
3. Създаване на проектен модел на СИС,
4. Изграждане на модел на реализация.

В тази подточка е представен процеса на дефиниране на системна рамка за описание на архитектурата на СИС. Системната рамка за определяне на проблемната област на СИС и в последствие архитектурата на системата определя границите, в които тя се разработва системата. Референтната методология за разработване на СИС, предлагана от нас е основана на рамката за архитектурно описание на програмни системи, описана в стандартите IEEE 1471 и IEEE 42010. Архитектурното описание поставя началото на създаване на проектен модел на СИС. Той се използва при реализация на реална СИС, при проектирането на която се отчитат и унифицират изискванията на различните гледни точки в областта на интерес на СИС. Базовите концепции, залегнали в основата на рамката за анализ на областта на система за Информационна сигурност са представени в т.1.6 - Околна

среда, Заинтересована страна, Област на интерес, Изглед, Гледна точка, Архитектура на системата, Архитектурно описание, Рамка на създаване на архитектурно описание, Архитектурен изглед, Архитектурна гледна точка, Вид на модела са приложими при анализа на областта Информационна Сигурност. Те определят общата концептуална рамка, позволяваща многоаспектно описание на проблемната област и определяне на архитектурата на СИС чрез използване на възможностите на концептуалното моделиране [99, 100, 101].

3.1.1 Описание на подхода

Същността на нашия подход е първоначално създаване на обобщен модел, а след това на неговата основа и детайлен модел на проблемната област на СИС. Така ние се абстрахираме от излишните подробности и се фокусираме върху съществените характеристики на системата. Процесът на концептуално моделиране зависи от рамката, в която се формират основните понятия.

Част от изискванията към системата за информационна сигурност се формират от околната среда, определяща условията при които тя ще оперира. Тези изисквания се дефинират въз основа на предложеният от нас метод за анализ на Проблемната област и определят модел на анализа. Този анализ взима предвид гледните точки на всички заинтересовани участници в разработването на СИС, гарантирайки комплексност на подходите за ИС. Моделът на проблемната област съвпада с модела на анализа. Този модел представя желаната архитектура на системата. Трябва да се прави разлика между архитектура на системата и описание на архитектурата, т.е. архитектурен модел. Докато определянето на архитектурата на системата отразява модела на анализа, то архитектурният модел е част от проектния модел.

За целите на проектирането на базата на създаден концептуален модел се конструира описание на архитектурата и функционалността на СИС, които са компоненти на Проектния модел. Изграждането на Проектния модел се базира на използването на обектно-ориентиран подход и обектно-ориентиран език за описание Unified Modeling Language (UML), предоставящ инструменти за описание, анализиране, моделиране и документиране на архитектурата и функционалността на СИС [97, 98].

Проектният модел се състои от архитектурен модел и функционален модел, описвани със съответните диаграми в UML. При конструирането на този модел, концептуалният модел се трансформира в обектно-ориентиран проектен модел. Моделът на реализация може да се осъществи по два начина - чрез агентен подход, позволяващ симулация на реалната система, или чрез използването на конкретни съществуващи системи, представляващи среда за реализация на СИС. Такива са например системите за предотвратяване изтичане на данни СПИД като DeviceLock [95] и Cososys Endpoint Protector [96].

3.2 Модел на анализа

В тази точка е представено създаването на модела на анализа. Системата се проектира в дадена Проблемна област (ПО) в която се представят проблемите и задачите за реализиране от СИС. В резултат на анализ на ПО се достига до описание на проблемната област и създаване на Модел на проблемната област (МПО), което е по същество и модел на Анализа. Моделът на проблемната област и Моделът на анализа са еквивалентни. Този модел представя желаната архитектура на системата.

Към МПО на СИС се поставят следните изисквания:

1. В съответствие с начина на формиране на понятия концептуалното моделиране предопределя поне два етапа при създаване на модела на проблемната област: конструиране на обобщен модел и конструиране на детайлен модел;
2. Архитектурата на СИС трябва да съответства на описанието на Проблемната област, където са определени задачите, които трябва да изпълнява системата;

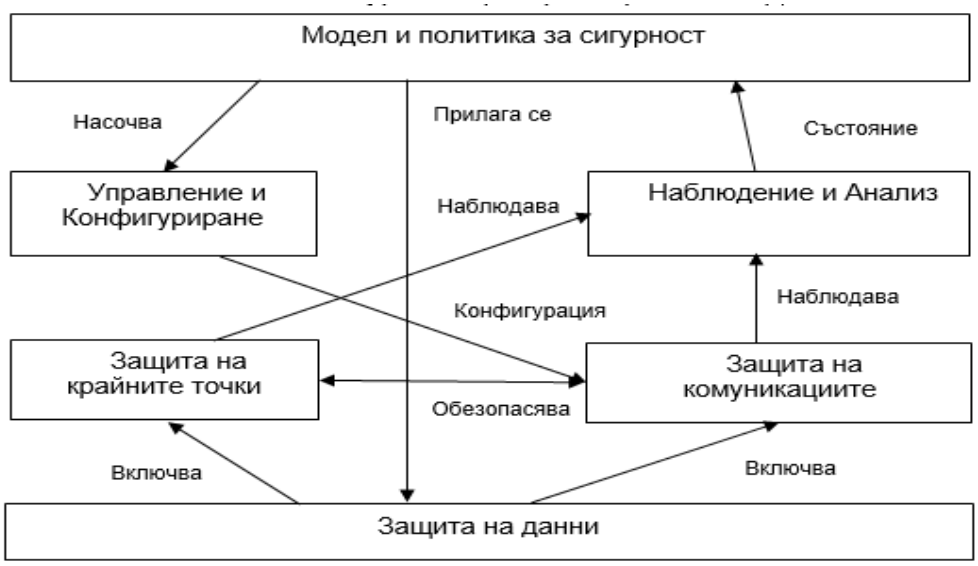
Резултатът от използване на концептуалното моделиране при създаване на Модел на анализа е концептуален модел, който представлява в своята същност абстракция, Всяка една концепция се разглежда като отделен компонент. Затова този модел представя и архитектурата на СИС.

3.2.1 Обобщен модел на проблемната област на СИС

В резултат на извършения анализ на проблемната област на СИС може да се обобщи, че най-важните въпроси, на които трябва да отговори една система от гледна точка на информационната сигурност са: „Какво защитаваме?“, „Защо защитаваме?“, „Как защитаваме?“ и „Къде защитаваме?“. Системната рамка за представяне на архитектурата на СИС е от съществено значение за разработването на системата, защото посочва основните компоненти, необходими за постигане на поставените и цели [20, 125].

Компонентите на обобщения модел съвпадат със задачите от ПО на проектираната система за информационна сигурност. Те отразяват съответните елементи от анализа на областта Информационна Сигурност. На тази база предлагаме мета-модел, представляващ обобщен модел на проблемната област на СИС. Моделът се състои от шест компонента, отговарящи на основните концепции, които представят областта ИС (Фигура 14) :

- “Защита на крайните точки” (Къде защитаваме?),
- “Защита на комуникациите” (Къде и Какво защитаваме?),
- “Защита на данни” (Какво защитаваме?),
- “Наблюдение и Анализ”,
- “Управление и Конфигуриране” (Как защитаваме?),
- “Модел и политика за сигурност” (Защо защитаваме?).

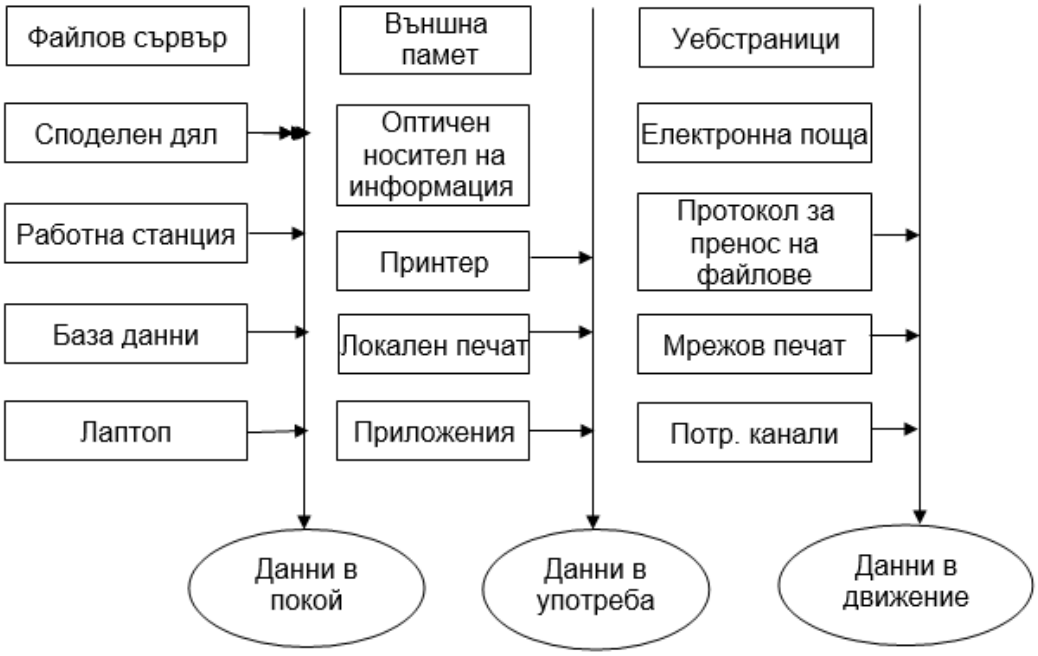


Фигура 14. Обобщен концептуален модел на проблемната област на СИС

Във всеки един момент данните могат да бъдат в едно от трите състояния: „Данни в покой“ (съхранен на запаметяващо устройство, архив или мрежов дял), „Данни в движение“ (данни участващи в комуникация, данни за състоянието на даден модул) или „Данни в употреба“ (всички данни използвани или обработвани в приложения) [23]. За формално представяне на данните в СИС създаваме мета-модел (Фигура 15), които се базира на гледната точка „Обработка на информация“ в областта на интерес на СИС (Фигура 8) [19]. За да се защитят различните типове данни е необходимо да се внедрят специфични подходи за информационна сигурност в основните блокове на мета-модела от гледна точка „Информационна сигурност“. Данните трябва да бъдат защитени срещу загуба, кражба, неоторизиран достъп и неконтролирани промени чрез прилагане на ПИС, като например: контрол на Поверителност, Цялостност, контрол на достъпа, изолация и репликация [17, 18].

С цел да се вземат предвид изискванията на всички заинтересовани страни, т.е. различните гледни точки, нашият подход позволява създаването на произволен брой концептуални мета-модели, които могат да бъдат комбинирани в една система. Резултата е многослоен концептуален мета-модел на СИС който съдържа мета-модели, представляващи съответните гледни точки.

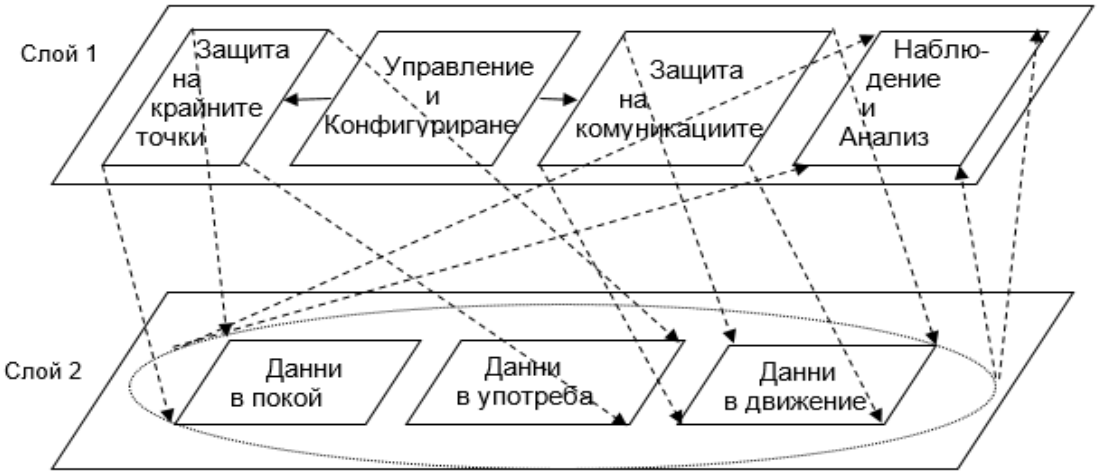
Показаният на Фигура 16 многослоен мета-модел представя гледните точки “Информационна сигурност” и “Обработка на информация” и взаимовръзките между тях. Като структура получения концептуален мета-модел съответства на Многослойния модел на защита от Фигура 4.



Фигура 15. Мета-модел “Обработка на информация”

Съвкупността от подходите за ИС, използвани в модела осигурява изпълнението на базовите принципи за информационна сигурност като „ПЦН Триада“, „Принцип на тройното А“ и „Принцип на най-слабото звено“. Основната цел е защита на данните в организацията. Поради сложността на защитата на всички възможни данни, ние се фокусираме в защита на чувствителните за организацията данни, които се дефинират в зависимост от околната среда в която се проектира системата. Отчитат се нормативни, законови, регулаторни и други изисквания и усилията се свеждат до защита на сравнително малки по обем, но критични за работата на организацията

данни. Отчитат се нормативни, законови, регулаторни и други изисквания и усилията се свеждат до защита на сравнително малки по обем, но критични за работата на организацията данни. Тези данни са дефинирани като чувствителни и целта на СИС е да бъдат защитени. Отделните компоненти на мета-модела изпълняват различни функционалности по защита.

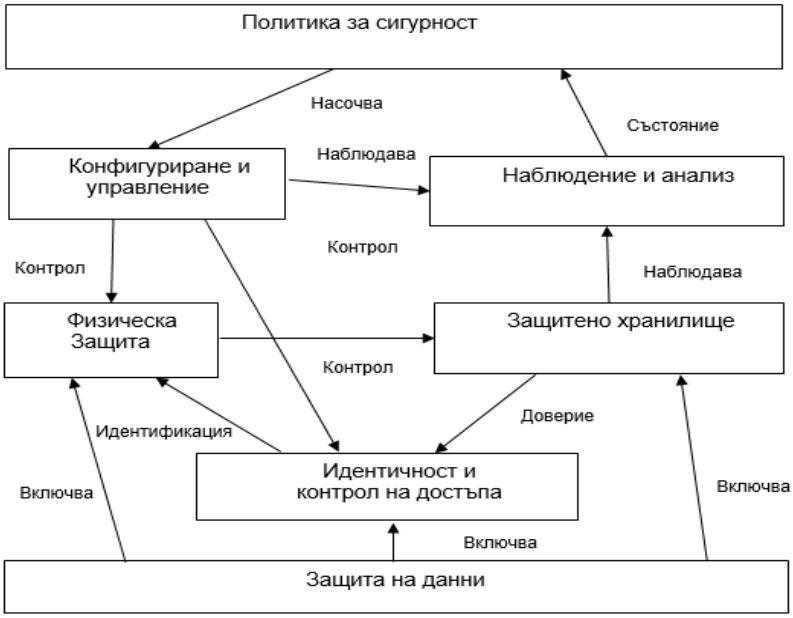


Фигура 16. Многослоен концептуален модел на СИС

В зависимост от изискванията на различните заинтересовани страни, към концептуалния модел могат да бъдат добавени мета-модели за различните гледни точки, с цел задоволяване на техните изисквания към СИС. Полученият многослоен концептуален модел се трансформира в реална физическа реализация на СИС.

3.2.2 Детайлно представяне на проблемната област

Тук е разгледано детайлното представяне на проблемната област**.** На основата на обобщения модел на СИС се създава детайлен модел на проблемната област на СИС. Разглеждаме детайлните концептуални модели на две от показаните концепции – *„Защита на крайните точки“* (Фигура 17) и *„Защита на комуникациите.* (Фигура 18).

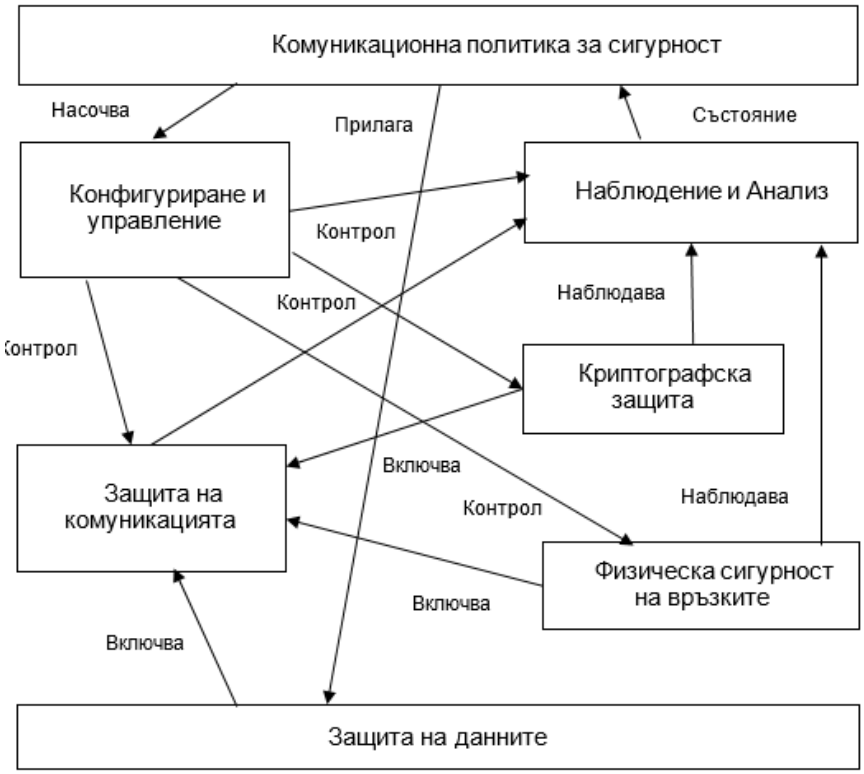


Фигура 17. Детайлен концептуален модел на концепцията „Защита на крайните точки“

Крайните точки са елементи на СИС, които имат изчислителни и комуникационни възможности: устройства, работни станции, сървъри, елементи на комуникационната инфраструктура, облачна инфраструктура и др. Те имат различни функции и изисквания за сигурност и тяхната защита може да бъде постигната със специфични подходи за информационна сигурност /ПИС/.

За да осигури Наличността, Поверителността и Цялостността на крайната точка, концепцията *„Защита на крайните точки“* трябва да осигури изпълнението на определени функционалности, които се осигуряват от компонентите показани на Фигура.17.

Концепцията *„Защита на комуникациите*“осигурява сигурност на свързаните крайни точки и комуникационните канали. На Фигура 18 е показан детайлен модел на концепцията.



Фигура 18. Детайлен концептуален модел на концепцията „*Защита на комуникациите*“

3.3. Проектен модел на системи за информационна сигурност. Архитектурен и функционален модел

Подход за създаване на проектен модел

На базата на архитектурното описание на системата за информационна сигурност може да бъде създаден проектен модел на системата. Той дава възможност за реализация на реална СИС, като при нейното проектиране се взимат предвид и се обобщават изискванията на различните гледни точки в областта на интерес на СИС. Подходът на проектиране на СИС е базиран на трансформация „модел-към-модел“. В нашият случай осъществяваме трансформацията:

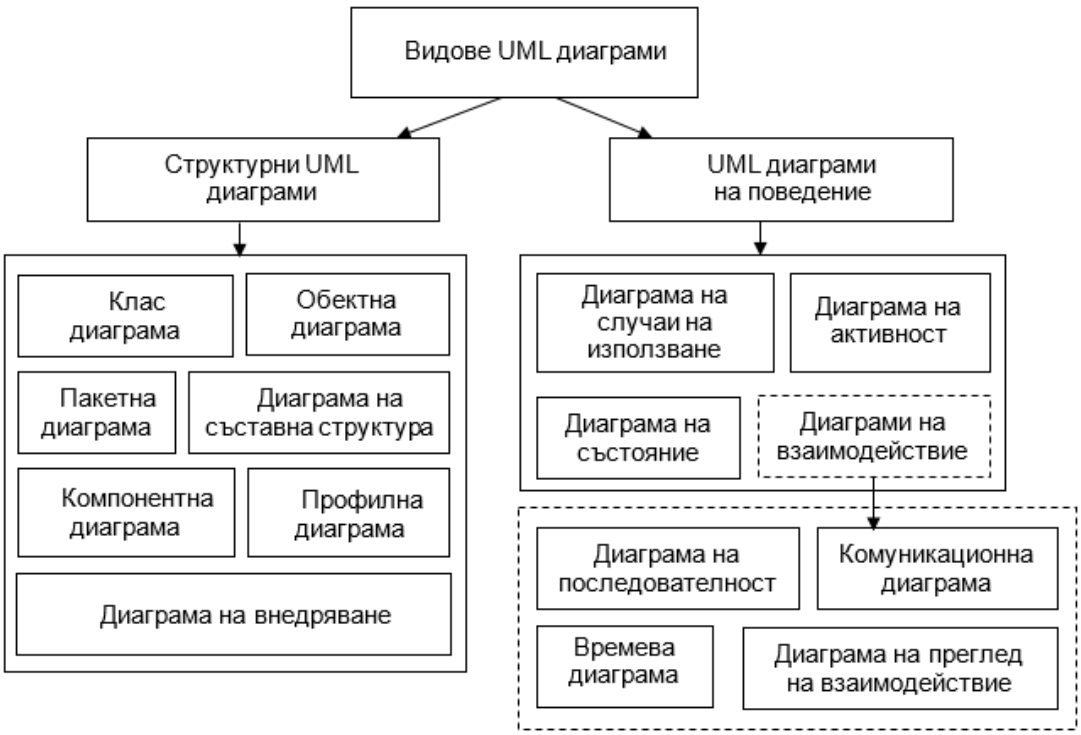
концептуален модел → обектно-ориентиран (ОО) модел

Най-подходящият начин за описание на ОО моделите е използването на обектно-ориентиран инструмент за описание, какъвто е обектно-ориентирания език UML. Този език позволява на системните разработчици да описват изискванията към СИС

и нейните компоненти, да скицират, модифицират и манипулират предложените архитектури, да използват многократно отделни компоненти на СИС, за комуникиране на информацията, събрана по време на разработването на системата. UML осигурява стандартна нотация за анализ, проектиране и внедряване на системи.

3.3.1 Обектно-ориентиран подход чрез използване на обектно-ориентиран език UML

В тази подточка са описани общата функционалност и възможности на езика за описание UML, както и основните видове диаграми (Фигура 20). Чрез различните UML диаграми, може да бъдат представени различни изгледи на системния модел.



Фигура 20. Видове UML диаграми

Чрез структурните диаграми (Structural Diagrams), може да бъде представена статичната структура на системата. Те включват следните основни типове: „Клас-диаграма“ (Class Diagram), Обектна диаграма“ (Object Diagram), „Пакетна диаграма“ (Package Diagram), „Диаграма на съставна структура“ (Composite Structure Diagram), „Компонентна диаграма“ (Component Diagram), „Диаграма на внедряване“ (Deployment Diagram), „Профилна диаграма“ (Profile Diagram).

Чрез „*Диаграмите за поведение*“ *(Behaviour Diagrams),* могат да се представят взаимодействието и моментните състояния на компонентите в модела, както и да се покаже как те се изменят с течение на времето. Чрез тези диаграми може да се проследи как системата действа в реална среда и да се наблюдава ефекта от дадени операции или събития. Този вид диаграми включват „Диаграми на употреба“ (UseCase Diagrams), „Диаграми на активност“ (Activity Diagrams), „Диаграма на състояние“ (State chart Diagram).

Последният тип UML диаграми са „Диаграмите за взаимодействие“ (Interaction Diagrams). Те са подклас на „Диаграмите за поведение“ и се използват за описание на взаимодействията между различните елементи в модела. Това взаимодействие е част от динамичното поведение на системата. Такива диаграми са: „Диаграма на

последователност“ (Sequence Diagram), „Диаграма за Сътрудничество“ (Collaboration Diagram), „Комуникационна диаграма“ (Communication Diagram), „Времева диаграма“ (Timing Diagram), „Диаграма за преглед на взаимодействие“ (Interaction Overview Diagram).

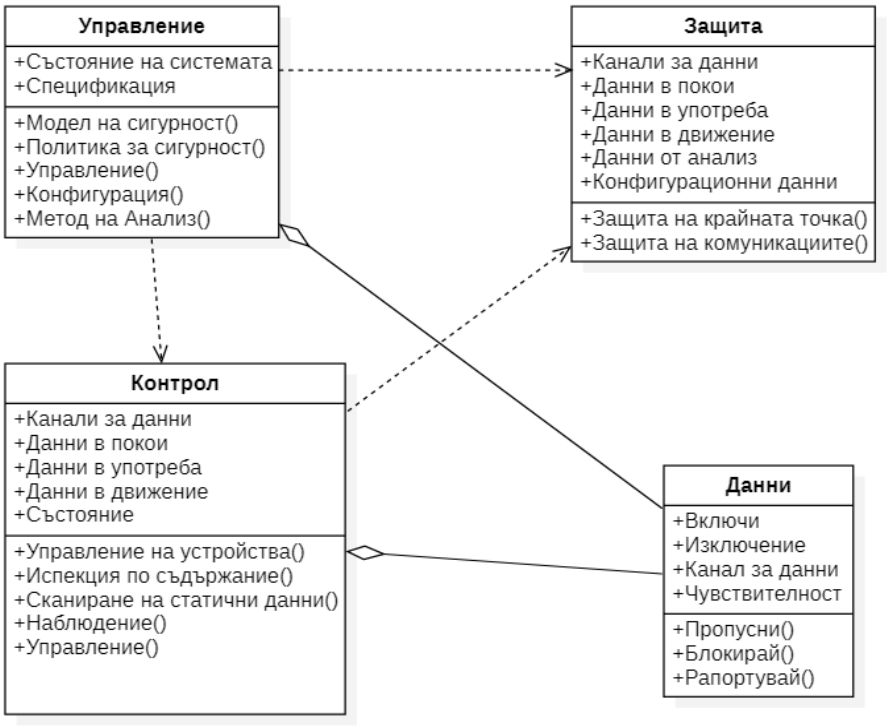
3.3.2 Архитектурен модел на системи за информационна сигурност

Архитектурният модел на СИС се представя чрез статични UML диаграми. За да се отрази трансформацията на обобщения модел на проблемната област на СИС от Фигура 14 в ОО модел използваме „Клас-диаграма“. За представяне на обектно-ориентираните модели на детайлните модели на концепциите „Защита на крайните точки“ (Фигура 17) и „Защита на комуникациите“ (Фигура 18) използваме „Диаграми на съставна структура“. По-детайлното описание н архитектурата на проектния модел изисква използването и на „Обектна диаграма“ и „Профилна диаграма“ което в момента не е задача на дисертационния труд.

На базата на останалите статични диаграми – „Пакетна диаграма“, „Компонентна диаграма“ и „Диаграма на внедряване“ се изгражда Модела на реализация.

UML „Клас-диаграма“

Целта на „Клас-диаграмата“ е да покаже статичната структура на класификаторите в системата. Диаграмата осигурява основна нотация, която може да се използва от други UML диаграми. Клас-диаграмата се състои от набор класове и връзки между класовете [97]. Концепцията на СИС, представена чрез обобщения мета-модел (Фигура 14) може да бъде описана чрез „Клас-диаграма“, както е показано на Фигура 21. Използваме същите понятия като в мета-модела, разделени като методи на четирите основни класа.



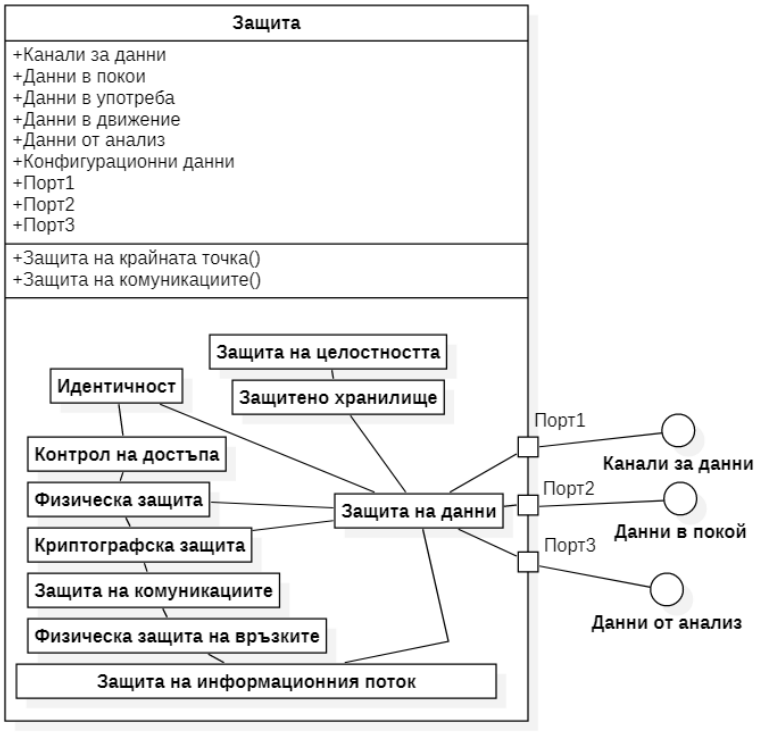
Фигура 21. UML „Клас диаграма“ на СИС

На компонентите „Защита на крайните точки” и “Защита на комуникациите” отговарят методите “Защита на крайната точка” и „Защита на комуникациите” в класа „Защита“, компонента „Защита на данни” е представен с еквивалентните методи „Пропусни”, „Блокирай” и „Рапортувай” в класа „Данни“. Клас „Контрол“ е агрегация от

компонентите „Защита на крайните точки”, “Защита на комуникациите”,„Защита на данни” и „Управление и Конфигуриране“.

UML „Диаграма на съставна структура“ на клас “Защита”

Чрез този вид диаграма се представя вътрешната структура на съответния клас. Класът „Защита“ включва методите “Защита на крайната точка” и “Защита на комуникациите”, осъществяващи защитата на данни както в крайните точки, така и в процеса на комуникация. Структурата на класа, изразена чрез диаграма на съставна структура е показана на Фигура 22.



Фигура 22. UML „Диаграма на съставна структура” на клас “Защита“.

3.3.3 Функционален модел на системи за информационна сигурност

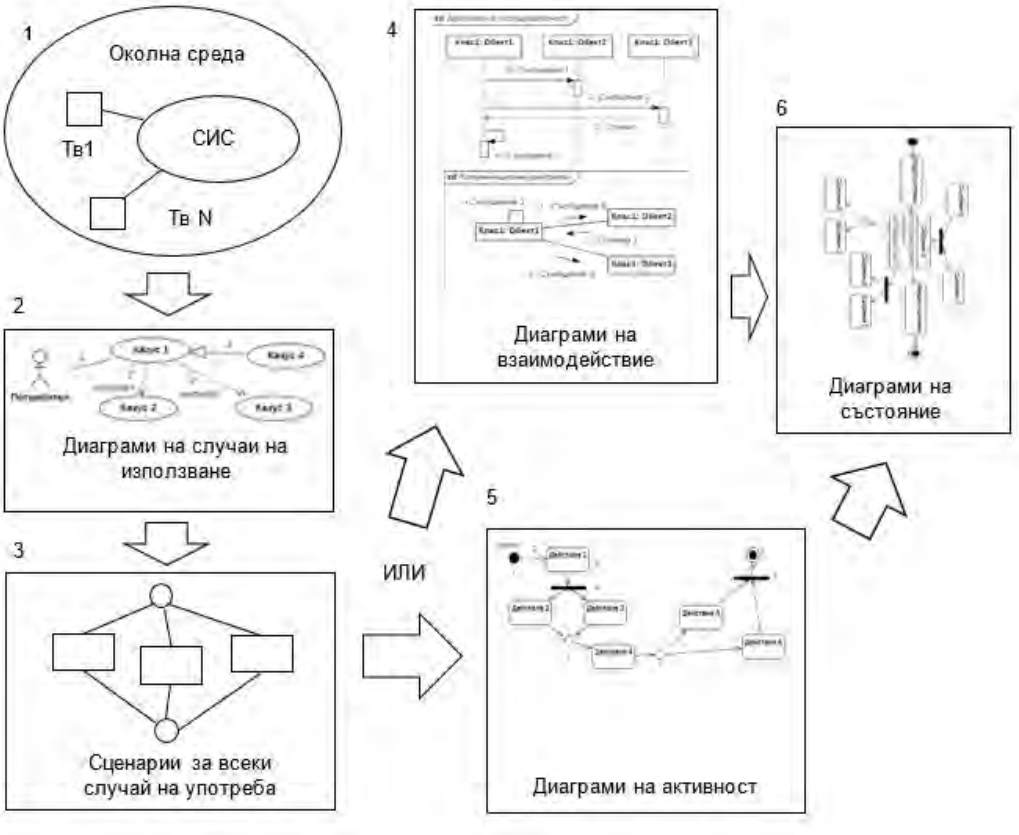
Функционалният модел на СИС може се представи чрез динамични UML диаграми: Диаграми на поведение и Диаграми на взаимодействие. Чрез тях може да се опишат различни аспекти от динамичното поведение на системата и взаимодействието на различните елементи на системата един с друг или с външни субекти. Те са удобни за описание на резултатите от динамичния анализ на системата за информационна сигурност (Фигура 23). Целта на анализа е да се идентифицират възможните варианти на взаимодействие, те да бъдат описани формално и да бъдат заложени в проектираната система, така че тя да реагира на взаимодействието според заложените при нейното проектиране цели.

СИС функционира в определена Околна среда (1). Освен че тя предоставя условията за функциониране на системата, в нея се извършва и взаимодействието (интеракцията) на СИС с различни субекти – точки на взаимодействие (Тв1 .. ТвN) от Фигура 23. Тези външни за системата субекти взаимодействат с нея по различни начини, извличайки полза от СИС. Начините на взаимодействие могат да бъдат описани с набор от диаграми на случаи на използване (2). Тези диаграми стоят в основата на динамичния анализ и съответно на функционалния модел на СИС.

За всяко взаимодействие на СИС със външен субект/обект може да бъде

съставена както базова диаграма на случаи на използване, описваща основното взаимодействие и поведение, така и разширени диаграми на случаи на използване, свързани с базовата диаграма и разширяващи базовата. Допълнителните диаграми наследяват базовите диаграми и добавят нови аспекти към основното взаимодействие. Така се формира набор от диаграми на случаи на използване, свързани с един или повече субекти и описващи възможно най-пълно взаимодействието на системата с тях. За всеки случай на използване се описват съответните сценарии (3), описващи взаимодействието и очакваната реакция на системата. Всеки сценарии може да бъде анализиран чрез използването на UML диаграми на поведение. Те могат да бъдат диаграми на взаимодействие (4) (Диаграма на последователност, Комуникационна диаграма, Времева диаграма, Диаграма на преглед на взаимодействие) или Диаграми на активност (5). Изборът на (4) или (5) зависи от спецификата на системата и на околната среда, така че най-пълно да бъде описано нейното поведение. Следващата стъпка е описание чрез диаграми на състояние (6), чрез които описваме промяната на състоянието на основните елементи на СИС, обобщавайки динамичното и поведение.

Полученият набор от UML диаграми, описващи резултата от динамичния анализ на системата формира Функционалния модел на проектираната система. Всяка диаграма описва отделни функционалности на системата, показвайки че подхода е приложим.



Фигура 23. Подход за създаване на функционален модел чрез динамични UML диаграми

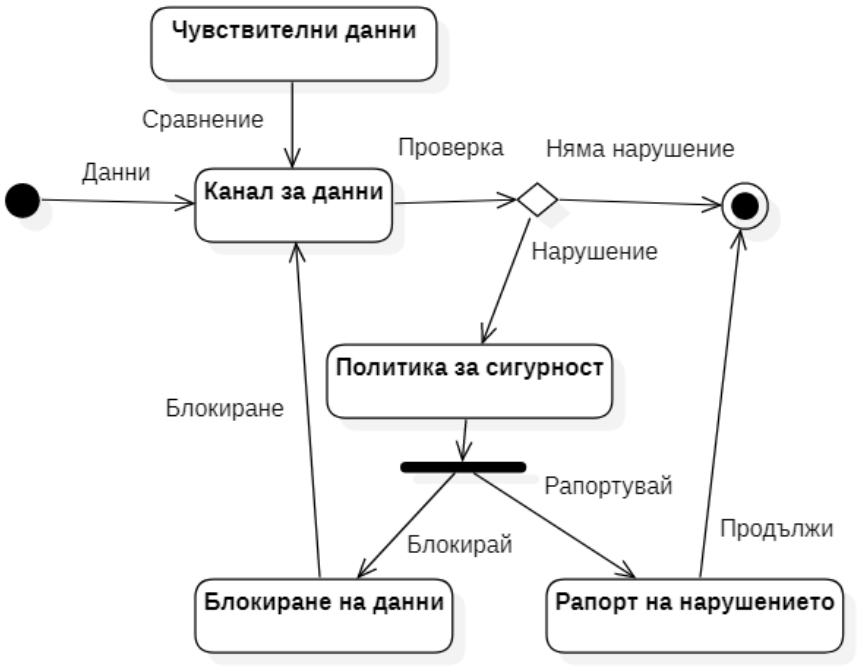
В настоящата подточка е показано как чрез различните динамични диаграми може да се опишат различни сценарии на взаимодействие на СИС с външни за нея субекти. Така например с „Диаграма на случай на използване“ удобно могат да бъдат описани разлчни начини на комуникация, например изпращане на електронна поща

до външен за организацията получател.

Следващите UML диаграми, формиращи функционалния модел са диаграми на взаимодействие, описващи взаимодействието на класовете „Управление“, „Контрол“ и „Данни“ и класовете „Управление“, „Контрол“ и „Защита“. Класовете са част от Клас-диаграмата от архитектурния модел на СИС (Фигура 21). Чрез този вид диаграми лесно се отразяват специфични взаимодействия на отделните класове, например инспекцията на потока от информация, преминаващ през даден комуникационен канал за съдържание на чувствителни за организацията данни или проверка на спазването на политиката за сигурност от отделните потребители.

Чрез „Диаграми на последователност“ се визуализира времевата последователност на взаимодействията между елементите на системата, осъществени чрез съобщения между тях.

Освен с диаграмите на взаимодействие, динамичното поведение на системата, представено със сценариите и случаите на използване могат да се анализират чрез диаграми на активност. На Фигура 28 е представена диаграма на активност на един от методите на клас „Защита“ – “Защита на крайна точка”, показваща проверка дали информацията, преминаваща през даден канал за данни е чувствителна според критериите на организацията. Подобни диаграми на активността могат да се създадат за всички методи от клас-диаграмата. По този начин е възможно да се опишат подробно различни случаи за взаимодействие със системата.



Фигура 28. UML Диаграма на активност на метода “Защита на крайна точка”

3.4 Заключение

В трета глава е представен подход за проектиране на Системата за Информационна Сигурност, предназначена за организации и насочена към защита от изтичане на чувствителна информация отвътре-навън, т.е. в резултат от действие на вътрешни лица с легитимен достъп до ресурсите на организацията и до нейните данни. За определянето на архитектурата на системата се използва представената в глава 2 системна рамка, която ни помага да се уточни проблемната област на СИС и да се извърши съответния анализ.

Представен е модел на анализа, който съвпада с модела на проблемната област. Изграждането на модела се основава на възможностите на концептуалното моделиране. В резултат е създаден обобщен концептуален модел на проблемната област на СИС. Показано е как обобщеният модел може да се трансформира в многослоен, когато се вземе под внимание анализа на повече от една гледни точки спрямо проблемната област на системата. Представеният многослоен мета модел отразява гледните точки „Информационна Сигурност“ и „Обработка на информацията“. На основата на обобщения концептуален модел се конструира детайлен концептуален модел на отделните негови компоненти. Показани са детайлни описания на концепциите „Защита на крайните точки“ и „Защита на комуникациите“.

Процесът на създаване на проектен модел на СИС е базиран на осъществяване на трансформацията „от модел към модел“. В случая се използва концептуалния модел на проблемната област на системата за създаване на обектно-ориентиран /ОО/ проектен модел. За целта се използва обектно-ориентиран инструмент за описание на модели – формалния език UML. Този език осигурява стандартна нотация за проектиране и внедряване на системи. Показано е, че той позволява на системните разработчици да представят изискванията към СИС и нейните компоненти в проектен модел на системата, който се състои от архитектурен модел и функционален модел. Представено е как могат да се моделират отделни аспекти на архитектурния модел, основани на съответните концептуални модели чрез използване на следните UML диаграми: „Клас-диаграма“ и „Диаграма на съставна структура“. Чрез моделиране на отделни аспекти на функционалния модел е показано как може да се състави обектно-ориентиран функционален модел, базиран на създадените концептуални модели на проблемната област. За целта се използват следните UML диаграми: „Диаграма на активност“, „Диаграма на състоянието“, „Диаграми на преглед на взаимодействие“, „Диаграма на случай на употреба“ , „Диаграма на последователност“.

Чрез приложения метод за анализ на проблемната област, възможностите за концептуално моделиране и подхода за осъществяване на трансформацията „от модел към модел”, разгледани в Глава 3 успешно се изпълняват задачи 3 и 4, дефинирани в "Цел и задачи на дисертацията":

- Описание на проблемната област на Системите за Информационна Сигурност в организации чрез концептуално моделиране;
- Анализ и приложение на обектно-ориентиран подход при създаване на проектен модел на система за информационна сигурност на базата на създаден концептуален модел.

В резултат на научноизследователската дейност за създаване на методология за разработване на СИС чрез модел на анализа и проектен модел се постигат следните научни и научно-приложни приноси:

1. Разработен е многослоен концептуален модел на проблемната област на системите за информационна сигурност като резултат от прилагането на две и повече от две гледни точки при нейното описание;

2. Конструирани са архитектурен и функционален модели на системите за информационна сигурност на базата на съществуващ концептуален модел на проблемното пространство с помощта на обектно-ориентирания унифициран език за описание на програмни системи UML;

Глава 4. Подходи за създаване на модел на реализация на системи

за информационна сигурност в организации

Съгласно възприетата методология за разработване на СИС, на базата на проектния модел трябва да се създаде модел на реализация, които може да се използва за две цели:

- Създаване на модел на реализация, съобразен със съществуваща среда за реализация;
- Симулиране работата на проектираната СИС;

За постигането на първата цел, като част от предложеният от нас метод, се извършва анализ на проблемната област и на базата на изградения концептуален модел, резултат от този анализ се избира платформа за реализация. Целта е да се запази подхода на обектно-ориентираното моделиране. В резултат трябва се създаде обектно-ориентиран модел на реализация, които съответства на разработения ОО проектен модел.

За постигането на втората цел се използват средите за симулиране NetLogo (v.6.0.4), и I-SCIP-SA, работещи на базата на създаване на агентно или мулти-агентно ориентирани модели. Това изисква обектно-ориентирания проектен модел, описан със средствата на UML да бъде трансформиран съгласно изискванията на агентния подход.

4.1 Сравнителен анализ на съществуващи платформи СПИД на базата на модел на анализа

Политиката за информационна сигурност касае по различен начин отделните работни места в организацията. Служителите на различни позиции (работни места) използват различни данни и имат съответния регламентиран достъп до тях. Това се описва в приетата в организацията политика за информационна сигурност, на базата на длъжностната им характеристика. В политиката за ИС се описва и какви операции с тези данни са разрешени и какви не са за даденото работно място. Изрично е описан достъпът до чувствителни за организацията данни за съответните позиции.

Основната цел на СПИД е опазването на данни от изтичане извън организацията. СПИД представят гъвкава платформа за реализация на приетата политика за информационна сигурност по отношение на защита на данните. Те предлагат подходящи инструменти за описание, изпълнение и контрол на:

- Различни типове данни,
- Дефиниране и работа с чувствителни за организацията данни,
- Разрешени и забранени операции с различни типове данни от съответните работни места,
- Описание на различни сценарии за работа с данните,
- Описание на регулации за работа с данни и тяхното спазване и контрол.
- Анализ на спазването на политиката за сигурност в организацията.

СПИД имат възможност за адаптиране към различните работни места според изискванията на политиката за информационна сигурност.

4.1.1 Приложения на предложеният от нас метод за уточняване на архитектурата на СИС

Проектираната от нас СИС е предназначена за организации и насочена към защита от изтичане на чувствителна информация в посока отвътре-навън от вътрешни лица с легитимен достъп до данни и ресурси на организацията. Архитектурата на системата се уточнява от различните гледни точки на отделните

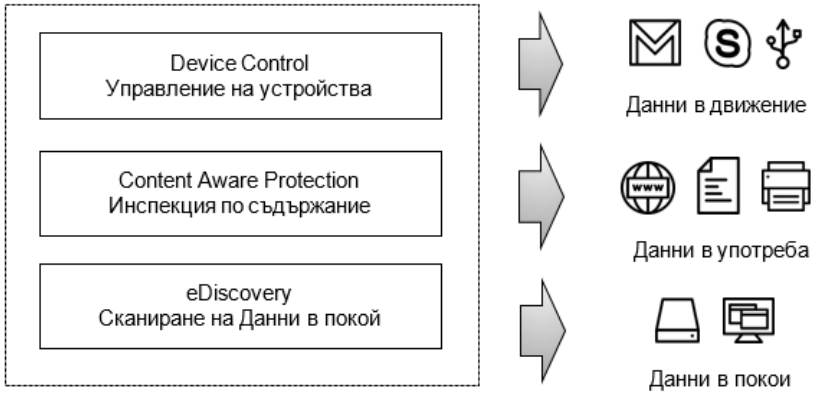
участници в процеса на проектиране и реализация на СИС. Базово изискване към системата е да притежава подходяща архитектура, която да се адаптира към различни политики за информационна сигурност, които поставят съответни изисквания към различни потребители на информация в дадена организация.

Това изискване се удовлетворява напълно от предложения от нас нов метод за уточняване на изискванията към архитектурата на СИС.

На базата на анализ на проблемната област от различни гледни точки и нейното последващо концептуално моделиране (Фиг.8), се конкретизират изискванията към разработваната СИС. Това дава възможност за избор на подходяща платформа за нейната реализация. Първата гледна точка, която се взима в предвид е гледната точка „Обработка на информация“. Тя отразява различните видове данни – данни в покой, данни в употреба и данни в движение. Друга гледна точка е „Технологична гледна точка“, отразяваща способите за защита на данните и съдържаща поддържаните платформи и технологии. Тя е от голямо значение за осигуряване на оперативна съвместимост на СИС, която се изгрзжда като допълнение към вече съществуваща СИС. За избора на платформа за реализация се използва и гледна точка „Информационна сигурност“, отразяваща изискванията на организацията към защитата на данните. Те са описани в политиката за Информационна сигурност. На базата на трите гледни точки и сходните цели на проектираната от нас СИС и системите за предотвратяване изтичането на данни, се избира платформа за реализация от тип СПИД. Използвайки концептуалният мета-модел от Фиг.15, изграден от гледната точка „Обработка на информация“ се извършва анализ на водещи СПИД (Cososys Endpoint Protector 5.0.2.1 [96], Symantec Data Loss Prevention 14.6 [137], McAfee DLP Endpoint 9.3.200 [138], Forcepoint DLP 8.9 [139], DeviceLock 8.2 [95]) и как те изпълняват изискванията на проблемната област.

Като резултат от анализа е избрана най-подходящата за нашите цели конкретна платформа за реализация. СПИД избрана за реализация на СИС е част от нейната архитектура. В нашия случаи, на базата на анализа изборът ни пада върху СПИД Cososys Endpoint Protector 5.0.2.1 [96]. Освен предимствата по отношение на защитата на основните типове данни (данни в покой, данни в употреба и данни в движение), друго сериозно предимство е осигуряването на оперативна съвместимост с останалите средства и подходи за информационна сигурност в организацията. Допълнително предимство на избраната платформа е нейната цена. При реализацията на СИС, задачата на избраната СПИД е единствено осигуряване на защита на данните на организацията в посока отвътре-навън, без да пречи на останалите средства за защита.

4.2 Платформа за реализация СПИД Cososys Endpoint Protector 5.0.2.1



Фигура 31. СПИД „Cososys EndPoint Protector 5.0.2.1“ – Структура

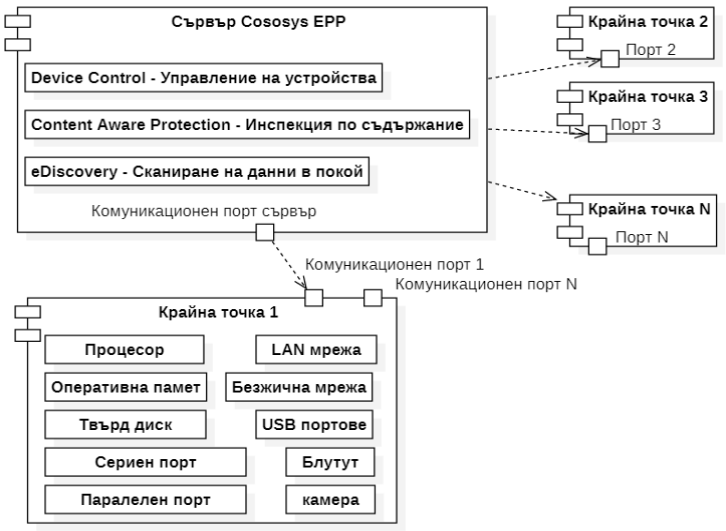
Освен агентно-ориентирани модели с цел симулация, модела на реализация може да бъде създаден чрез използването на съществуващата среда за реализация. За постигането на тази цел избираме съществуваща платформа за изграждане на СПИД Cososys EPP 5.0.2.1 [96]. За създаването на модела е използван подхода на обектно-ориентираното моделиране. В резултат е създаден обектно-ориентиран модел на реализация, които да съответства на разработения ОО проектен модел. Избраната платформа за реализация Cososys EPP 5.0.2.1, се състои от хардуерен сървър и софтуерни модули Device Control, Content Aware Protection и eDiscovery. Хардуерния сървър осигурява централизираното управление на СПИД, а отделните модули осуряват различна функционалност (Фигура 31).

4.3 Обектно-ориентиран модел на реализация на системи за информационна сигурност

За създаването на ОО модел на реализация отново използваме нструментариума на езика UML. Чрез него създаваме следните диаграми:

- Пакетна диаграма,
- Компонентна диаграма,
- Диаграма на внедряване.

Фигура 32. UML Пакетна диаграма на СПИД Cososys EPP 5.0.2.1

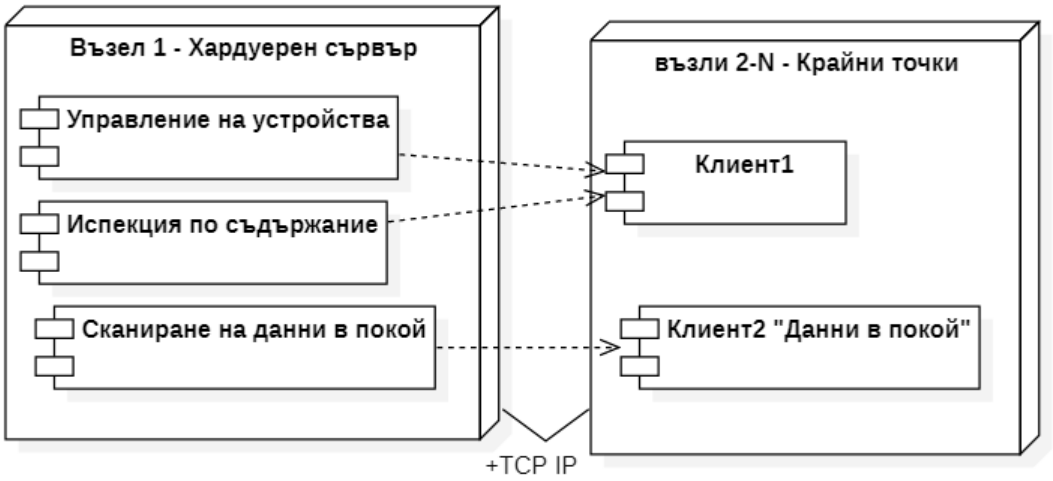


Фигура 33. UML Компонентна диаграма на Cososys EPP 5.0.2.1

Пакетната диаграма от модела на реализация (Фигура 32) е съставена от следните основни пакети: “Device Control – Управление на устройства“, „Content Aware Protection – Инспекция по съдържание“, „eDiscovery – Сканиране на Данни в покой“ и „Доклади и анализи“, отговарящи на основните модули на СПИД Cososys EPP 5.0.2.1.

СПИД Cososys EPP 5.0.2.1 е изградена на базата на „клиент-сървър“ архитектура. Контролираните от системата работни станции се наричат „Крайни точки“. На всяка крайна точка се инсталира клиент, наречен „агент“, които контролира съответните канали за данни като Lan мрежа, безжична мрежа, USB портове, Блутут портове, серийни и паралелни портове (Фигура 33). СПИД контролира и достъпа на всички устройства, използващи каналите и портовете за данни – USB запаметяващи устройства, принтери, камери и т.н. Системата комуникира с крайната точка като и налага за изпълнение приетата политика за сигурност, указваща КОИ може да използва каналите за данни и устройствата, КОГА да ги използва, КАК да ги използва (чрез какви протоколи и приложения), КАКВИ данни може да използва и изпраща.

Чрез диаграмата на внедряване се моделира физическото внедряване на системните компоненти. За разлика от компонентните диаграми, използвани за описание на отделните компоненти, диаграмите на внедряване показват как тези компоненти се разгръщат в реалната среда. Примерна диаграма на внедряване на СПИД система е показана на Фигура 34. Поради факта че СИС обикновена е сложна система, съставена от голям брой компоненти, диаграмата е опростена и показва няколко хардуерни компоненти като СПИД (DLP) сървър, който е свързан със софтуерните агенти, работещи на потребителските работни станции. Чрез софтуерните агенти, СПИД сървъра наблюдава, контролира и управлява каналите за данни на крайните точки (работни станции и лаптопи) – LAN мрежа, безжична мрежа, Блутут, USB портове, електронна поща, чат комуникации и др. СПИД е в състояние да контролира комуникационните канали, да активира и деактивира потока от данни през тях според контекста и потребителя. Данните могат да бъдат инспектирани по съдържание, като при констатиране на нарушение – неоторизирано изтичане на данни, то може да бъде блокирано и докладвано. Комуникацията между клиентите и сървъра се осъществява чрез TCP/IP протокол.



Фигура 34. UML Диаграма на внедряване на СПИД

4.4. Разширяване на съществуваща СИС с нови случаи на използване за защита на чувствителни данни за организацията

При реализацията на политики за информационна сигурност в организацията, главно внимание се обръща на различните позиции (работни места). Длъжностната характеристика на работното място определя използването на информационната система. Начините на използване на ИС от служителите на организацията дефинират съвкупност от случаи на употреба (use cases). Случаите на употреба, свързани с използване, обработка или комуникация на данни, обект на защита в организацията могат да бъдат описани в СИС, която да следи как съответния служител спазва политиката за сигурност.

Изборът на СПИД като платформа за реализация на СИС дава възможност за гъвкава настройка на системата със съответните изисквания към работните места - с каква информация е допустимо да работи и какви операции са разрешени.

Реализацията на СИС се описва чрез модела на реализация. Той се конструира чрез обектно-ориентирано моделиране от обектно-ориентиран проектен модел на СИС. За целта се използват UML диаграми според представеният от нас метод. Чрез тях се описват конкретни случаи на използване (use cases) чрез които могат да бъдат постигнати и удовлетворени поставените пред СИС цели. Използвайки случаите на използване не е необходимо да се реализира реална, пълномащабна СИС. Достатъчно е описаните случаи да покриват поставените цели за различните работни места в организацията. Чрез сценариите, описани в случаите на използване се осигурява възможност на СИС да се адаптира към нови изисквания на организацията и съответните работни места. Наборът от описани случаи на използване, описващ различни сценарии на взаимодействие на СИС с околната среда и потребителите (Фиг.23) дават възможност на системата да удовлетвори изискванията на различни по своя характер, дейност и големина организации.

Представеният метод, съчетан с използването на гъвкава платформа за реализация като СПИД осигурява възможност за доразвиване на съществуващи СИС чрез нови сценарии за защита на данни, нереализирани досега в организацията. Метода дава възможност за моделиране и реализация на нови аспекти от СИС без да се налага системата да се проектира отначало. Друго основно предимства на метода и използването на СПИД е запазването на оперативната съвместимост с останалите елементи на съществуващата СИС или на отделни подходи и механизами за информационна сигурност, реализирани вече в

организацията.

Такъв е случаят с организация, притежаваща функционираща СИС и предпазваща ефективно нейната инфраструктура чрез различни подходи за информационна сигурност (ПИС) с мрежова комуникация – Фиг.3. След влизането в сила на Общия регламент относно защита на личните данни - Регламент (ЕС) 2016/679 (GDPR), регламентиращ защитата на личните данни на граждани на Европейския Съюз, се налага организацията да се съобрази с него и да въведе мерки за защита на личните данни на клиенти и служители.

За целта са наложителни следните промени в политиката за информационна сигурност

1. Спазване на изискванията на GDPR за опазване на лични данни,
2. Опазване на информацията от изнасяне в посока отвътре-навън.

Тяхната реализация се базира на определянето и опазването на чувствителната за организацията информация. Описват се необходимите сценарии за защита на лични и/или чувствителни данни и се съставят необходимите за изпълнението на сценариите динамични UML диаграми, свързани с описанието на динамичното поведение на системата (Фигура 23). Няколко такива сценария са показани в Таблица 2. След това така описаните сценарии се добавят към съществуващата СИС, чрез избраната СПИД за реализация на защитата в реални условия, съобразявайки се с отделните работни места и спецификата на работата им с данни.

Сценарий 1	
Ключови контроли	Контрол на лични/чувствителни данни чрез политики и правила за IBAN, ЕГН, ID, Credit Card Numbers.
Описание	Контрол на трансфера на лични/чувствителни данни, съдържащи IBAN, ID, Credit Card Numbers чрез външни запаметяващи устройства (USB флаш памети).
Сценарий	Копиране на данни върху външно запаметяващо устройство (USB флаш памет). СИС проверява дали копираните файлове съдържат чувствителни за организацията данни. Ако данните са чувствителни, политиката за сигурност определя дали потребителя има право да копира файловете, съдържащи тези данни. Проверява се дали според политиката за сигурност потребителя има право да използва този външен носител. Например в организацията може да е регламентирано използването само на служебни оторизирани флаш памети или само на криптирани USB носители. В този случаи се дефинира „бял списък“ от разрешени за използване преносими Flash памети. За всеки потребител се определя персонална Flash памет която може да бъде използвана само от него. При нарушаване на политиката за сигурност копирането на файла се забранява и се изготвя доклад за нарушението. Възможно е да се създаде резервно копие на файла (документа) за по-нататъшно разследване.
Проектни модели описващи Сценарий 1	Виж Приложение 1 1. Диаграма на случай на използване (Use Case Diagram) – Фигура 1.1

(UML диаграми)	2. Диаграма на взаимодействие или Диаграма на активност – Фигура 1.2 3. Диаграми на състояние – Фигура 1.3.1 и 1.3.2
Сценарий 2	
Ключови контроли	Принудително криптиране на данни, пренасяни чрез USB флаш памети.
Описание	Криптиране на лични/чувствителни данни, съдържащи IBAN, ID, Credit Card Numbers при пренасяне на данни чрез външни запаметяващи устройства (USB флаш памети).
Сценарий	При копиране на файлове върху външно запаметяващо устройство (USB флаш памет).се проверява дали политиката за сигурност разрешава тази операция от този потребител, с тези данни. След това се проверява дали външното запаметяващо устройство е хардуерно криптирано. Ако то е хардуерно криптирано, операцията се разрешава и се прави резервно копие, ако политиката за сигурност го изисква. Ако устройството не е хардуерно криптирано се активира вграденият в СПИД модул за софтуерно криптиране и файловете се криптират принудително. След това операцията за копиране се разрешава, като се копира криптиран файл. Чрез този сценарии се гарантира че при загуба или кражба на външното запаметяващо устройство (USB флаш памет) GDPR е спазен.
Проектни модели описващи Сценарий 2 (UML диаграми)	Виж Приложение 1 1. Диаграма на случай на използване (Use Case Diagram) – Фигура 2.1 2. Диаграма на взаимодействие или Диаграма на активност – Фигура 2.2 3. Диаграми на състояние – Фигура 2.3
Сценарий 3	
Ключови контроли	Контрол на лични/чувствителни данни чрез политики и правила за IBAN, ЕГН, ID, Credit Card Numbers.
Описание	Контрол на трансфера на лични и чувствителни данни, съдържащи IBAN, ID, Credit Card Numbers чрез електронна поща (email).
Сценарий	Изпращане на данни чрез електронна поща (email). СИС проверява дали изпращаната електронна поща съдържа чувствителни за организацията данни. Ако данните са чувствителни, политиката за сигурност определя дали потребителя има право да изпраща пощата, съдържаща тези данни. Проверява се дали според политиката за сигурност потребителя има право да изпраща електронна поща до адресата. Например в организацията може да е регламентирано изпращането на електронна поща до оп-

	ределени адреси от определени потребители. В този случаи се дефинира „бял списък“ от разрешени адреси на електронна поща. При нарушаване на политиката за сигурност изпращането на електронното писмо се забранява и се изготвя доклад за нарушението. Възможно е да се създаде резервно копие на файла (документа) за по-нататъшно разследване.
Проектни модели описващи Сценарий 3 (UML диаграми)	Виж Приложение 1 1. Диаграма на случай на използване (Use Case Diagram) – Фигура 3.1 2. Диаграма на взаимодействие или Диаграма на активност – Фигура 3.2 3. Диаграми на състояние – Фигура 3.3

Таблица 2. Сценарии на нови случаи на употреба на съществуваща СИС

4.4.1 Резултати от проведени изпитания на реализирано разширяване на съществуваща СИС с нови случаи на използване за защита на чувствителни данни

Цел на изпитанията

Изпитание на предложените сценарии за разширяване възможностите на съществуваща СИС за предотвратяване изтичане на информация в държавни и частни структури.

Обхват на проучването

До момента проучването обхваща 7 организации – 5 държавни и 2 частни.
Размер на субектите: Мащабни добре структурирани държавни и частни субекти.

Методология

Проведени са срещи с представители на проявили интерес държавни и частни субекти, на които е обсъдена нуждата от разширяване възможностите на системите за информационна сигурност. Дискутирани са различни инструменти за защита на чувствителна информация, в зависимост от спецификата на дейността, нормативните изисквания и размера на субекта. След проведените срещи се стига до извода, че най-голяма е нуждата от внедряването на решения от типа СПИД.

В два от субектите са направени подробни тестове и Доказване на концепцията (POC - Proof Of Concept) на решения от тип СПИД. За провеждане на тестовете и POC са съгласувани и одобрени тестови сценарии, представени със случаи на използване (use cases) за защита на чувствителна информация, съответстваща на нормативните уредби и вътрешни правила на субекта. Наблюдавани са и съвместимостта с наличните към момента инструменти и решения за ИТ сигурност, използвани в организациите.

Нормативна база

Закон за киберсигурност в Р.България [57, 74], Наредба за минималните изисквания за мрежова и информационна сигурност [15], EU GDPR [68], ISO 27001 и 27002 [8, 78, 79] и други спицифични наредби за субектите.

Описание на проведените изпитания

За осъществяване на специфичните за средата тестове, одобрените правила и сценарии са основани на извадки от ключови контроли, използващи функционалността на приложеното решение от тип СПИД.

Резултати и заключения от изпитанията

Използвайки предложеният от нас метод за проектиране на СИС, се разширяват

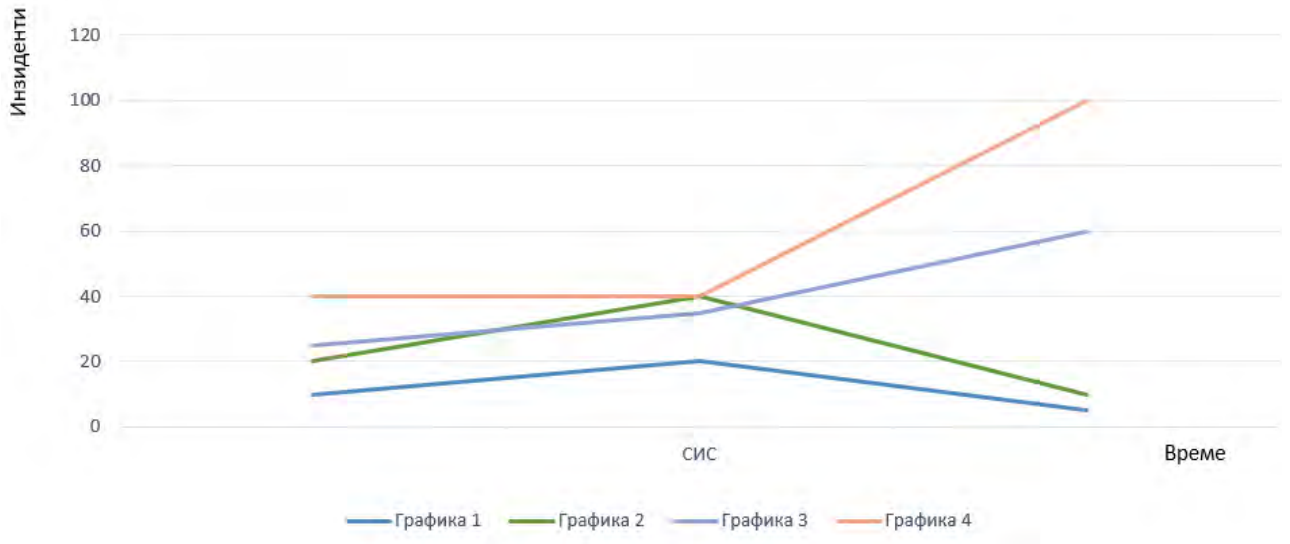
възможностите на съществуващите системи за информационна сигурност. Детайлното описание на случаите на употреба за защита на чувствителни за организацията данни чрез проектните модели с помощта на UML диаграми още на етап проектиране осигуряват възможност на СИС точно да изпълнява поставените цели, свързани с политиките за вътрешна сигурност, правните разпоредни и директивите за поверителност. Реализирането на СИС с платформа СПИД осигурява интиутивно създаване на политики, описващи случаите на употреба чрез предложените сценарии.

Функционално разширената СИС е ефикасен инструмент за предотвратяване и разследване на инциденти, свързани с изтичане на чувствителна информация.

Проектния модел дава ясна представа за процесите, свързани с обработка и трансфер на информация в организацията.

В резултат на проведените изпитания на доразвитие на съществуваща СИС чрез нови случаи на употреба за защита на чувствителни за организацията данни (Таблица 11), е установено следното:

1. Намаляване на инцидентите, свързани с изтичане на чувствителна информация (Графика 1 от Фиг. 35).
2. Ограничаване на информационните канали по които е възможно изтичането чувствителна информация (Графика 2 от Фиг. 35)
3. Повишаване видимостта на чувствителната информация от тип Данни в покои (Графика 3 от Фиг. 35)
4. Подобряване на съответствието с политиките за вътрешна сигурност, правните разпоредби и директивите за поверителност (Графика 4 от Фиг. 35)
5. Правилата за защита на чувствителни данни, изготвени по сценариите на случаите на употреба се изпълняват стриктно и безотказно от Функционално разширената СИС.



Фигура 35. Обобщени резултати от изпитания на доразвитието на съществуваща СИС

4.5 Трансформиране на ОО проектен модел в агентно-базиран модел на реализация

Внедряването на система с реални компоненти изисква значителни средства,

време, сериозни усилия и човешки капитал за нейното тестване и събиране на реални данни. Поради тази причина се налага да симулираме действието на проектираната система в избраната агентно-базирана симулационна среда. Това изисква да се трансформира създадения ОО проектен модел на системата във агентно-базиран модел на реализацията, чието действие трябва да се симулира.

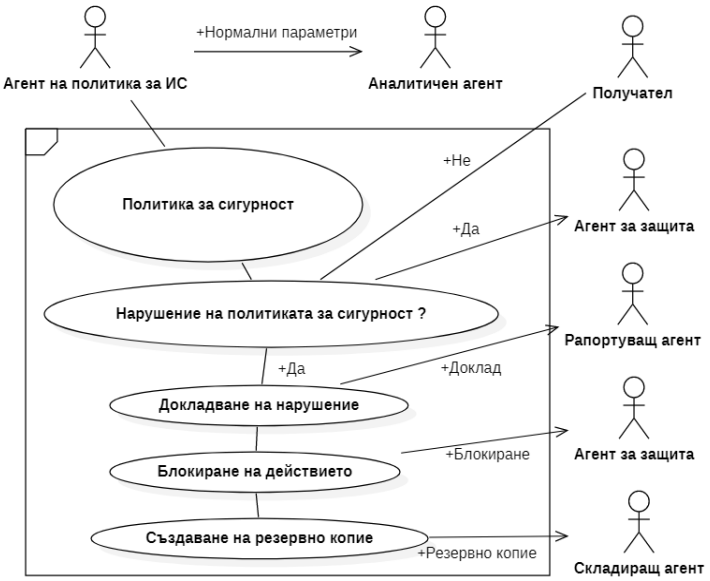
В агентно-базираните системи, агентът събира и обработва информация за околната среда, в която действа, и въздейства върху нея на базата на взети от него решения и про-активна дейност. При СИС допускаме, че отделни агенти изпълняващи самостоятелни задачи по защита на даден актив или информация са част от системата. За да се постигнат целите на СИС, тя трябва да осигури дейността на няколко основни вида агенти, изпълняващи определена роля и извършващи интеракции между тях: *„Агент по нарушенията“, „Агент за Защита“, „Агент на политика за ИС“, „Агент за наблюдение“, „Рапортуващ агент“,„Комуникационен Агент“,„Обработващ агент“, „Складиращ агент“,„Агент за реализация на услуги“.*

Трансформацията от обектно-ориентирания проектен модел на СИС в агентно-базиран модел на реализация се основава на клас-диаграмата от Фигура 21. Видимо е че клас "Контрол" съдържа в себе обекти, които имат потенциал да се превърнат в про-активни агенти, взимащи самостоятелни решения. Този клас взаимодейства с останалите класове (Защита, Данни и Управление), които оформят околната среда на класа агенти, която осигурява необходимата им за работа информация за вземане на решения. Освен това агентите въздействат на тази околна среда с цел постигане на конкретни резултати за които СИС е създадена и получава от тях информация, на чиято база взима решенията. Можем да приемем че тези класове формират околната среда, с която класа "Контрол" взаимодейства. Можем да дефинираме клас "Околна среда", съставен от трите класа Защита, Данни и Управление. Тогава класа "Контрол" става Агент "Контрол", взаимодействащ с новия клас "Околна среда" (Фигура 36). На тази база приемаме, че класът "Контрол" се трансформира в клас “Агент“, които представя съвкупност от агенти, всеки от които има определена цел.

Фигура 36. Класове „Агент“ и „Околна среда“

В съответствие с отделните цели и нуждата от определени роли, класът „Агент“ обхваща: „Агент по нарушенията“, „Агент за Защита“, „Агент на политика за ИС“, „Агент за наблюдение“, „Рапортуващ агент“, „Комуникационен агент“, „Обработващ

агент“, „Складиращ агент“ и „Агент за реализация на услуги“ (Фигура 36).



Фигура 38. Диаграма на случай на използване при „Агент на политика за ИС“

Фигура 39. Диаграма на случай на използване при „Агент за защита“

За да се опише ролята на всеки агент чрез използване на ОО език UML се използва диаграма „случай на използване“, която описва взаимодействието на даден агент с околната среда, която в нашия случай се разглежда като ОО система. За всеки един от изброените агенти се създава такава диаграма, която описва сценария по които той действа. За да покажем как става това се представя диаграмата „случай на използване“, на околната среда от агентите „Агент на политика за ИС“ и „Агент за защита“. По аналогичен начин са описани и останалите агенти, с което се създава агентно-базиран модел на реализация на СИС. Този модел се използва при симулиране дейността на проектираната система. На Фигура 37 е показана диаграма на случай на използване за „Агент на политика за ИС“, а на Фигура 38 - диаграма на случай на използване за „Агент за Защита“.

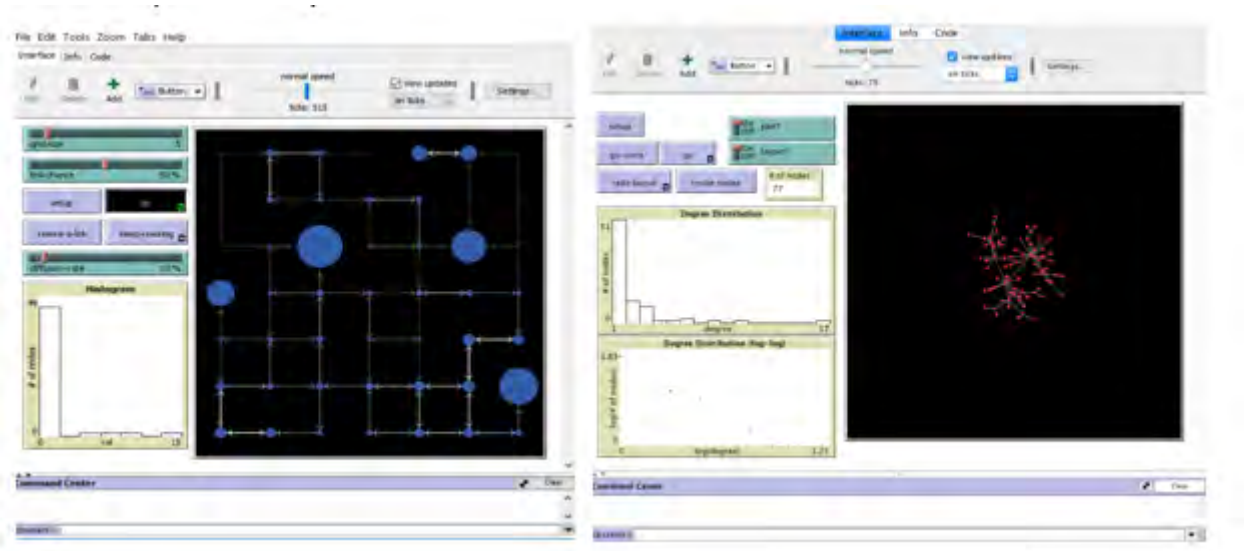
4.6 Симулиране на системи за информационна сигурност и анализ на генерираните тестови данни

Реализацията на симулацията на архитектурния модел на СИС извършваме на базата на агентно- и мулти-агентно ориентирано моделиране в средите NetLogo и I-SCIP-SA, позволяващи смесена (експертна, сензорна и машинна) оценка на предложените архитектурни мета идеи [102].

Експерименти в средата NetLogo

NetLogo (Фигура 39) е мулти-агентна крос-платформена симулационна среда за симулиране на сложни системи във времето [47, 118]. Средата NetLogo е основана на агентно-базирани модели за симулиране на действията и взаимодействията на множество автономни агенти (индивидуални или колективни субекти като организации или групи), работещи едновременно. Това дава възможност да се изследват връзките между модели на микро ниво, които възникват от при тяхното взаимодействие и оценка на въздействието им върху системата, като цяло. На базата на мета-модела от Фигура 14 е създаден агентно-ориентиран модел в средата NetLogo (v.6.0.4).

Резултатите от симулациите на този модел са показани на Фигура 40. Като цяло са изследвани взаимодействията между отделните блокове: “Агент за Защита ”, “Комуникационен Агент”, “Агент по нарушенията”, “Агент на политика за ИС”, “Рапортуващ агент”, “Складиращ агент”, “Агент за наблюдение”, “Агент за реализация на услуги” и “ Обработващ агент”. Чрез използване на елементи от Теория на игрите, като и клас от методите Монте Карло за работа със случайни извадки, имплементирани в средата NetLogo, е осъществено представянето на агентите и са реализирани интеракциите между тях.



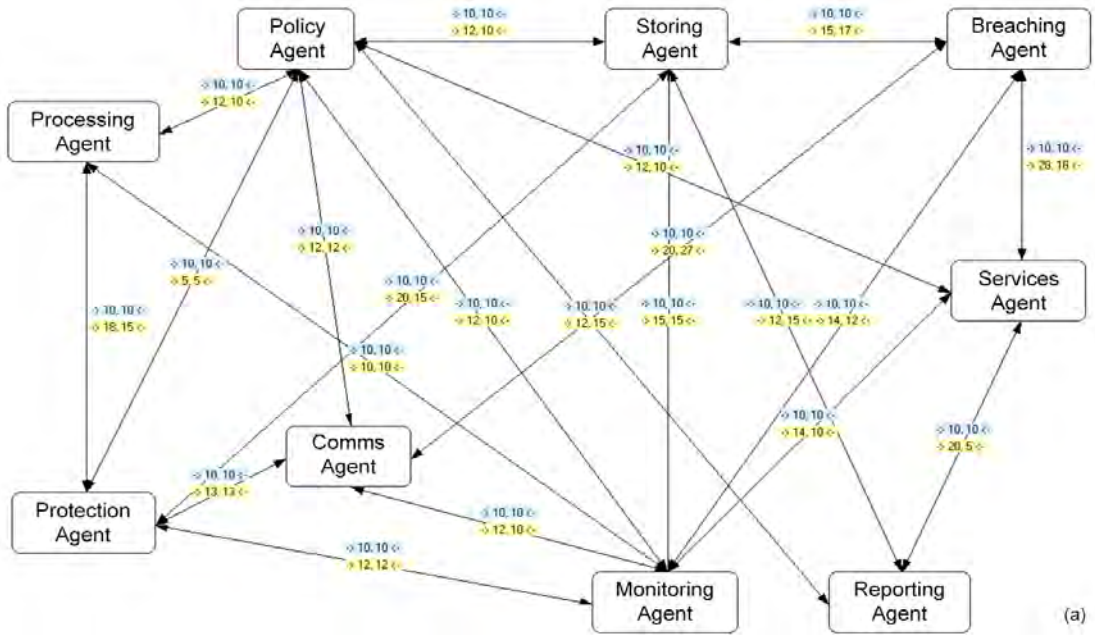
Фигура 40. Екранни снимки от симулация в среда на NetLogo

Експерименти в средата I-SCIP-SA

С цел по-голяма близост до реалността, позволяваща смесено изследване на предложените архитектурни решения на СИС е разработен мулти-агентен модел [28] от тип „система-от-системи“ [126] в средата I-SCIP-SA (Intelligent Scenario Computer Interface Program for System Analysis) [105]. При това е приложен опита от [106] и организацията от модела, предложен в [103] и реализиран в [107], аналогични на изследванията в средата NetLogo. Целта е да се създаде възможност за идентифицирането на бъдещи заплахи – вътрешни и външни в ИС, използвани в

корпоративна среда, в съответствие с различните състояния на използваните данни с активното участие и на човешкия фактор. Машинно, резултатите са представени посредством организацията „обект-връзка“ [108] и предоставят възможност за извършването на релевантни начални и крайни холистични, класификационни оценки на агентите в изследваните модели.

Обектите, представящи агенти (графично означени като именувани, заоблени правоъгълници) имат функционалности както за между-агентна комуникация, така и за визуализация на външни (записани или получавани в реално време) данни (Фигура 40). Между-агентните комуникационни канали са отбелязани с двупосочни стрелки, етикирани със стойностите на теглата (оцветени в жълто) и времевите стъпки (оцветени в синьо), отнесени към правите (Influence) и обратните (Dependence) връзки между обектите в модела. Данните за теглата на между-агентните връзки, образуващи трендове могат да произхождат от различни симулационни резултати в смесената реалност, които са получени като резултат от решаването на математически модели и външни източници, както в реално време, така и след провеждане на симулациите.



Фигура 41. Мулти-агентен модел на СПИД за проактивно изследване изтичане на данни в корпоративна среда

Множеството на източниците на данни може да използва: сензори, API функции за директна връзка или използващи записи във файлове с различен произход (вкл. експертен или друг симулационен резултат), които осигуряват възможност за проактивен системен анализ и холистична оценка на обектите в модела (в реално време или след симулацията), в съответствие с различните състояния на данните („данни в движение“, „данни в употреба“, „данни в покой“).

Резултатите от системния анализ са интерпретирани и агрегирани по различни начини, например [109, 110, 111], като тук се използва “3D Диаграма на чувствителността” – “3D ДЧ” (Фигура 41), осигуряваща класификация на агентите (означени като индексирани 3D сфери) в четири сектора (Активни – Active, Пасивни – Passive, Критични – Critical и Буферни – Buffering обекти, имащи съответно – „пасивна“ – $z < 0$ или „активна“ роля – $z \geq 0$ по отношение на сектора в който са разположени), в съответствие с обработката и смесването на първоначалните експертни допускания и резултантните симулационни резултати (за Влияние –

Influence – x, Зависимост – Dependence – y и Чувствителност – Sensitivity – z, измерени в проценти от интервала [0, 1]).

Фигура 41. Мулти-агентен модел на СПИД с допълнителни класификационни начални оценки на агентите в 3D ДЧ

Предложеното решение предоставя възможност за проактивно участие на човешкия фактор в процеса на вземане на решения, гарантирайки цялостно разглеждане и оценка на ролите на СПИД (DLP) агентите и проблемните места, възникващи при това. Мулти-агентната комуникация, в системния модел използва различни организационни стратегии от типа: „лидерство“ – “prominence”, както и „преговори“ – “negotiation” [112], в зависимост от избраните симулационни сценарии. Получените резултати от анализа на мулти-агентния модел на СПИД за проактивно изследване на изтичанията на данни в корпоративна среда показват ясна необходимост от балансиране, осигуряващо разширен контрол върху използваните комуникации и услуги. Това обаче крие и редица неясноти, тъй като въвеждането на нови технологични решения може да доведе до неочаквани изтичания на данни и пробиви в сигурността. Следователно мониторинга, пост-анализа и складирането на данни в комбинация с евристичната защита в реално време остават критични за успешната защита на съвременната корпоративна среда, при отчитане особеностите на използваните потоци от данни.

Генериране и анализ на тестови данни

Изпълнението на тази задача е организирано, върху избрана мулти-агентна архитектура на СИС, на две стъпки: (а) стохастична валидация на очакванията за изтичания на данни, посредством експертни допускания и машинно генерирани ad-hoc селекции за изтичания на данни; (б) интерактивна верификация във виртуална корпоративна среда с избрания прототип на СИС и вектори на кибер-атаки, реализиращи очакванията за изтичане на корпоративни данни по определен сценарий за проиграване.

В настоящата глава подробно е описано проактивно стохастично решение за смесена валидация върху предложения системен модел.

Верифицирането на резултатите от стохастичните симулации е проведена емпирично, с използване на интерактивна симулация в трансформирана реалност, организирана в рамките на ученията CYREX 2018, 2019 и 2020 [109, 117, 122, 123].

4.5 Заключение

В глава 4 са описани подходи за създаване на модел на реализация на СИС чрез предлаганата от нас методология за разработване на СИС.

На базата на проектен обектно-ориентиран модел е изграден ОО модел на реализация, съобразен със съществуваща среда за реализация. След извършване на анализ на проблемната област и на базата на изграден концептуален модел, резултат от този анализ, са уточнени изискванията към архитектурата на разработваната СИС. Направен е анализ на съществуващи платформи за реализация СПИД и е избрана най-подходящата в съответствие с модела на анализа.

Моделът на реализация описва съществуваща платформа за реализация на СИС от тип СПИД „Cososys EndPoint Protector 5.0.2.1“. За целта се използват съществуващите UML диаграми: „Пакетна диаграма“, „Компонентна диаграма“ и „Диаграма на внедряване“.

Представеният метод дава възможност за моделиране и реализация на нови аспекти от СИС без да се налага системата да се проектира отначало. За целта е достатъчно да се доразвие съществуваща СИС чрез включване на нови случаи на употреба за защита на чувствителни данни за организацията. В главата е представен пример с конкретни сценарии на нови случаи на употреба (use cases), както и проведени изпитания на реализираното разширение на системата.

За да се симулира работата на проектираната СИС е изграден агентно-базиран модел на реализация. За целта е създаден симулационен модел на разработваната СИС, който може да се реализира в мулти-агентна крос-платформена симулационна среда за симулиране на сложни системи във времето. Представен е подход за трансформиране от обектно-ориентиран модел в агентно-базиран модел.

Приложеното решение за концептуално UML мета-проектиране на архитектури с използване на различни класове диаграми, позволява статично и динамично разглеждане на функционалностите на системите за информационна сигурност. По-детайлни изследвания на очакванията за изтичания на данни са извършени симулационно, на основата на смесени агентно- и мултиагентно- ориентирани решения, осигуряващи голяма гъвкавост и близост до реалността.

Генерирането и анализа на тестови данни е организирано на две стъпки:

- Стохастична валидация на очакванията за изтичания на данни, посредством експертни допускания и машинно генерирани ad-hoc селекции за изтичания на данни;
- Интерактивна верификация във виртуална корпоративна среда с избрания прототип на СИС и вектори на кибер атаки, реализиращи очакванията за изтичане на корпоративни данни по определен сценарий за проиграване.

Предложените практическа валидация и верификация на избрана комерсиално достъпна СПИД платформа за реализация с гъвкави функционалности, адаптирани към мета архитектурите, дават възможност за реално съчетаване на експертни, сензорни и машинно симулирани данни. При това остава възможно и тяхното сравнение с проектираните архитектурни функционалности, по отношение на реалните вектори за атака в смесена, футуристична виртуална среда за избрани сценарийни комбинации.

Чрез агентно-ориентирания подход може да се покаже динамиката на системата, която с другите модели не може да бъде представена. Агентно-ориентирания модел ни дава цялостна картина, която нито концептуалния, нито обектно-ориентирания модел може да даде. Симулацията на СИС дава възможност да бъде изследвана динамиката на системата при различни сценарии. Сценариите са описани и предс-тавени чрез диаграми на случаи на използване в ОО модел и след това симулирани чрез агентния подход. Симулацията може да покаже поведението на системата при промяна на околната среда. Такава е например промяна на законодателство или нормативна база, даващо определени приоритети, влиянието на вътрешни или външни за организацията лица, поява на нов тип заплахи или нестандартни начини за изтичане на данни. Резултатите от симулацията помагат да се предвидят както традиционните, така и по-рядко срещани заплахи и да се оптимизира използването на ПИС.

Глава 4 описва изпълнението на задачи 5 и 6, дефинирани в "Цел и задачи на дисертацията":

- Развитие на съществуващи СИС на базата на проектиране и реализация на нови случаи на употреба, отнасящи се до чувствителни данни.
- Определяне на подход за трансформиране на проектния модел на СИС в модел на реализация;
- Симулация на СИС на базата на модела на реализация. Генериране и анализ на тестови данни.

В резултат от изпълнената научноизследователската дейност се постигат следните научно-приложни приноси:

1. Предложен е UML модел на реализация на СИС в организация, използваща СПИД платформа за реализация „Cososys Endpoint Protector 5.0.2.1“
2. Сравнителен анализ на съществуващи СПИД платформа за реализация на базата на изискванията, описани в модела на анализа.
3. Проектиране, реализация и тестване на разширение на съществуващи СИС с поддържането на нови случай на употреба.
4. Реализиран е симулационен модел на СИС на базата на обектно-ориентирано описание на архитектурата му чрез използване на агентно-базирано представяне в средите NetLogo и I-SCIP-SA; Симулационно изследване на архитектурата на СИС чрез извършване на стохастична валидация и интерактивна верификация.

Библиография

1. Suryateja P.S., “Threats and Vulnerabilities of Cloud Computing: A Review”, International Journal of Computer Sciences and Engineering, Volume 6, Issue 3, published 30.03.2018
2. Rhodes-Ousley M., “Information Security the Complete Reference”, 2nd Edition, The McGraw-Hill, 2013
3. Diogenes Y., Ozkaya E., “Cybersecurity - Attack and Defence Strategies”, Packt Publishing Ltd., 2018
4. Pfleeger C. P.,.Pfleeger S.L, Margulies J., “Security in Computing”, 4th Edition, Prentice Hall, 2015
5. Ciampa M., “Security+ Guide to Network Security Fundamentals”, 4th Edition, Course Technology, Cengage Learning, 2015

6. CISSP Study Guide, https://www.sciencedirect.com/book/9781597499613/cissp-study-guide, last accessed 2021/08/11
7. The European Network and Information Security Agency (ENISA) (2012b), https://www.enisa.europa.eu/publications/ENISA_Threat_Landscape/at_download/fullReport, last accessed 2021/08/11
8. Landoll D., Information Security Policies, Procedures and Standards - A Practitioner's Reference, CRC Press, Taylor & Francis Group, 2016, ISBN 978-1-4822-4591-2
9. Гайдарски И., Кутинчев П., Откриване на вътрешни заплахи и предотвратяване изтичането на чувствителна информация от организацията, Научна конференция "Необходима достатъчност за осигуряване на въздушния суверенитет на България и ролята на човешкия фактор", Военна Академия "Г.С.Раковски", 11.10.2018, София, България, ISBN 978-619-7478
10. Whitman M, Mattord H., Principles of Information Security, Fourth Edition
Course Technology, Cengage Learning, 2012
11. Gragido W., Pirc J.. Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats. Syngress, 2011.
12. Keung Y., "Information Security Controls", Adv Robot Autom 2013, Department of Systems Engineering and Engineering Management, City University of Hong Kong, Kowloon Tong, Hong Kong
13. Bhaskar SM, Ahson SI (2008) Information Security: A practical Approach, Oxford: Alpha Science International Ltd.
14. Schweitzer JA, Managing Information Security: Administrative, Electronics, and Legal measures to Protect Business Information. Boston: Butterworths. 1990
15. Наредба за минималните изисквания за мрежова и информационна сигурност, https://www.mtitc.government.bg/sites/default/files/nar_minimalnite_iziskvaniq_mrejova_info_sigurnost-072019.pdf, last accessed 2021/08/11
16. Guide for Conducting Risk Assessments. NIST Special Publication 800-30 rev.1, NIST, September 2012, https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final, last accessed 2021/08/11
17. Guidelines on assessing DSP and OES compliance to the NISD security Requirements, ENISA, November 2018, https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements,last accessed 2021/08/11
18. Standards, Guidelines, Tools and Techniques, ISACA, May 2016, https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/standards-guidelines-tools-and-techniques , last accessed 2021/08/11
19. Шаньгин В.Ф. "Защита информации в компьютерниьх системах и сетях", ДМК Пресс 2012, ISBN 978-5-94074-637-9
20. Hayden L., "IT Security Metrics: A Practical Framework for measuring Security & Protecting Data, 2010 by The McGraw-Hill, ISBN: 978-0-07-171341-2
21. Alhassan M, Adjei-Quaye A., Information Security in an Organization, International Journal of Computer (IJC), Global Society of Scientific Research and Researchers 2017, ISSN 2307-4523
22. Dimitrov W, Syarova S., Analysis of the functionalities of a Shared ICS Security Operations Center, International Conference "Big Data, Knowledge and Control Systems Engineering" 6th IEEE International Conference BdKCSE'2019, 21-22 November 2019, Sofia, Bulgaria
23. Accenture Security 2019 Cyber Threatscape Report, 2019
https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf, last accessed 2021/08/11

24. Insider Threat Report, Verizon 2019, _https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf, last accessed 2021/08/11
25. ENISA Threat Landscape - Responding to the Evolving Threat Environment European Network and Information Security Agency (ENISA), 2012, https://www.enisa.europa.eu/publications/ENISA_Threat_Landscape/at_download/fullReport, last accessed 2021/08/11
26. ENISA Threat Landscape Report 2020 - 15 Top Cyberthreats and Trends, European Network and Information Security Agency (ENISA), 2019, https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020, last accessed 2021/08/11
27. Минчев З., Кутинчев П., Гайдарски И.. Топ 10 заплахи за киберпространство през 2019. IT4Sec Reports, Institute of ICT, Bulgarian Academy of Sciences, 2019, ISSN:1314-5614, DOI:10.11610/it4sec.0133, 133-1-133-12 Национално академично издателство
28. Bollinger J., Enright B., Valites M., Crafting the InfoSec Playbook, O'Reilly Media, Inc., 2015, ISBN: 978-1-491-94940-5
29. Andress J., The basics of information security : understanding the fundamentals of InfoSec in theory and practice, Elsevier Inc. 2011
30. Taylor-Duncan L., Come in, We're Open – Keeping Your Company's IT Data Safe From Threats, Techni-Core productions, 2014
31. SysSec Red Book - Roadmap in the area of Systems Security, SysSec consortium, http://www.red-book.eu/, last accessed 2021/08/11
32. Минчев З., Гайдарски И., Кибер рискове, заплахи и мерки за защита, свързани с COVID-19, CSDM Views, Number 37, 2020, ISSN 1314-5622
33. Gaydarski I.,Discovery and Protection from Internal Threats in Critical Infrastructure's objects., Proceedings of BISEC 2019, Belgrade Metropolitan University, Belgrade Metropolitan University, приета за печат: 2019
34. Yassein M., Hmeidi I., Mohammad Al-Rousan Y., Arrabi D., Black Hole Attack Security Issues, Challenges & Solution In Manet, Conference: International Conference on Computer Science, Engineering and Information Technology (CSEIT-2018) Dubai, UAE, DOI: 10.5121/csit.2018.81815
35. Chandler J., Security in Cyberspace: Combatting Distributed Denial of Service Attacks, University of Ottawa, January 2003
36. Understanding Denial-of-Service Attacks, Cybersecurity & Infrastructure Security Agency, USA, https://www.us-cert.gov/ncas/tips/ST04-015, last accessed 2021/08/11
37. WASC Threat Classification v2.0, Web Application Security Consortium, 2010, http://projects.webappsec.org/f/WASC-TC-v2_0.pdf?ld=1 , last accessed 2021/08/11
38. LizaMoon Mass SQL-Injection Attack Infected at least 500k Websites, https://isc.sans.edu/forums/diary/LizaMoon+Mass+SQLInjection+Attack+Infected+at+least+500k+Websites/10642, last accessed 2021/08/11
39. Botnets: Measurement, Detection, Disinfection and Defence, European Network and Information Security Agency (ENISA), March 2011, https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence, last accessed 2021/08/11
40. DDoS Malware, Verisign 2013, https://www.informationweek.com/pdf_whitepapers/approved/1370027144_VRSNDDoSMalware.pdf , last accessed 2021/08/11
41. Nazario J., BlackEnergy DDoS Bot Analysis.. Arbor Networks, 2007, http://pds15.egloos.com/pds/201001/01/66/BlackEnergy_DDoS_Bot_Analysis.pdf, last accessed 2021/08/11

42. Tracking GhostNet: Investigating a Cyber Espionage Network. Information Warfare Monitor, March 2009, https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf, last accessed 2021/08/11
43. Shadows in the Cloud: An investigation into cyber espionage 2.0. Information Warfare Monitor and Shadowserver Foundation, 2010, https://citizenlab.ca/wp-content/uploads/2017/05/shadows-in-the-cloud.pdf, , last accessed 2021/08/11
44. Keizer, G., Is Stuxnet the 'best' malware ever?, Computerworld, September 2010. http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever, last accessed 2021/08/11
45. Gaydarski I., Kutinchev P., Holistic Approach to Data protection - identifying the weak points in the organization.. Proceedings of BdKCSE'2017 (7 December, 2017 Sofia), САИ, 2018, ISSN:2367-6450, 125-135
46. Gaydarski I, Minchev Z.. Challenges to Data Protection in Corporate Environment, Chapter 8, In Minchev Z., (Ed) Book "Future Digital Society Resilience in the Informational Age", Sofia, Institute of ICT, Bulgarian Academy of Sciences, SoftTrade, December, 2018, ISBN 978-954-334-221-1, 82-100
47. Parsons, S., Gymtrasiewicz, P. and Wooldridge, M. (Eds). Game Theory and Decision Theory in Agent-Based Systems (Multiagent Systems, Artificial Societies, and Simulated Organizations), Springer, 2002.
48. Wahlstrom B. "Perspectives of Human Communication", Wm.C.Brown Publishers, 1992, ISBN 0-697-10704-3
49. Nwana, H. and Ndumu, D. An Introduction to Agent Technology, Software Agents and Soft Computing: Towards Enhancing Machine Intelligence, Concepts and Applications, Lecture Notes in Computer Science 1198, Springer, 3-26,1997.
50. Russel, S., Norving, P. Artificial Intelligence: A Modern Approach, Prentice Hall, New Jersey, 1995.
51. Wooldridge M, An Introduction To Multiagent Systems, John Wiley & Sons 2002, ISBN: 047149691X
52. Buecker A., Andreas P., Paisley S., Understanding IT Perimeter Security, Redpaper, IBM, November 2009, https://www.redbooks.ibm.com/redpapers/pdfs/redp4397.pdf, last accessed 2021/08/11
52. Santana G.,Cruz D., Modelling a network security systems using multi-agents systems engineering, Systems, Man and Cybernetics, 2003. IEEE International Conference, Vol.5, November 2003, DOI: 10.1109/ICSMC.2003.1245655
53. Guidelines for Data Classification, Carnegie Mellon University, https://www.cmu.edu/iso/governance/guidelines/data-classification.html,
last accessed 2021/08/11
54. Ahmed S., Karsiti M., Multiagent Systems ,In-Teh Croatia, 2009, ISBN 978-3-902613-51-6
55. Закон за киберсигурност, приет на 31 октомври 2018, 7 ноември 2018, https://www.mlsp.government.bg/uploads/3/zakonodatelstvo/za-kibersigurnost.pdf, last accessed 2021/08/11
56. Национална стратегия за киберсигурност „Кибер устойчива България 2020", Юли 2016, http://www.strategy.bg/StrategicDocuments/View.aspx?Id=1120, , last accessed 2021/08/11
57. Полимирова Д, Шаламанов В., Стоянов Н, Тагарев Т., Янакиев Я., Шарков Г., Папазов Я., Ризов В., Иванова К., Киберсигурност и възможности за приложение на иновативни технологии в работата на държавната администрация в България, Институт за публична администрация, 2019, ISBN 978-619-7262-14-8 https://www.ipa.government.bg/sites/default/files/01_ipa_study_v10.0._final_ed.pdf, last accessed 2021/08/11

58. Olivé A., Conceptual Modeling of Information Systems, January 2007, Springer DOI: 10.1007/978-3-540-39390-0
59. Mallikaarachchi V., Data Modeling for System Analysis, INFORMATION SYSTEMS ANALYSIS - IS 6840, University of Missouri, St. Louis, 2010 http://www.umsl.edu/~sauterv/analysis/Fall2010Papers/varuni/, last accessed 2021/08/11
60. Edgar T., Manz D., Research Methods for Cyber Security, Elsevier Inc. 2017, ISBN: 9780128053492
61. Saltzer J., Schroeder M., "The protection of information in computer systems," in Proceedings of the IEEE, vol. 63, no. 9, pp. 1278-1308, September 1975
62. Turing A., Computing Machinery and Intelligence, Mind, Volume LIX, Issue 236, October 1950, Pages 433–460, https://doi.org/10.1093/mind/LIX.236.433,
63. Laplante P., What Every Engineer Should Know about Software Engineerin, Boca Raton, CRC, 2007. ISBN 9780849372285
64. Cyber Kill Chain, Lockheed Martin https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html , last accessed 2021/08/11
65. Hutchins, E. M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains." Leading Issues in Information Warfare & Security Research Volume 1. 2011, pp. 80-106.
66. Finkelsetin A, Kramer J., Nuseibeh B., Finkelstein L., Goedicke M., Viewpoints - A Framework for Integrating Multiple Perspectives in System Developmen, International Journal of Software Engineering and Knowledge Engineering 02(01), November 2011
67. Hilliard R.,Emery D., Maier M., ANSI/IEEE 1471 and Systems Engineering, Systems Engineering 7(3):257 - 270, June 2004, DOI: 10.1002/sys.20008
68. Общ регламент относно защита на личните данни (Регламент (ЕС) 2016/679), https://cpdp.bg/?p=element&aid=991 , last accessed 2021/08/11
69. Националната стратегия за киберсигурност „Киберустойчива България 2020", приета от Министерски съвет на Република България на 13 юли 2016 г., http://www.cyberbg.eu/, last accessed 2021/08/11
70. Актуализирана стратегия за национална сигурност на Република България, приета с Решение на Народното събрание от 14 март 2018 г, https://www.mod.bg/bg/doc/cooperation/20181005_Akt_strateg_NS_RB.pdf, last accessed 2021/08/11
71. Стратегията за национална сигурност на Република България, https://me.government.bg/bg/themes/bulgaria-s-national-security-strategy-904-0.html, last accessed 2021/08/11

72. Закон за управление и функциониране на системата за защита на националната сигурност, Ноември 2015, https://www.parliament.bg/bg/laws/ID/15270, last accessed 2021/08/11
73. Правилник за дейността, структурата и организацията на Държавна агенция "Електронно управление", приет с постановление № 274 от 28 октомври 2016, https://dv.parliament.bg/DVWeb/showMaterialDV.jsp?idMat=108729, last accessed 2021/08/11
74. Закон за киберсигурност, приет от Народното събрание на 31 октомври 2018 г, https://parliament.bg/bg/laws/ID/78098, last accessed 2021/08/11
75. Закон за защита на класифицираната информация, 26.02.2019г. https://www.damtn.government.bg/wp-content/uploads/2019/06/zakon-za-klasifitsiranata-informacia.pdf, last accessed 2021/08/11
76. БДС EN ISO/IEC 27001:2017 „Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията", https://www.bds-bg.org/bg/project/show/bds:proj:102367, last accessed 2021/08/11

77. Директива 2016/1148 ЕС относно мерки за високо общо ниво на сигурност на мрежовите и информационни системи в Съюза, https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32016L1148, last accessed 2021/08/11
78. J. Hintzbergen, K. Hintzbergen, A. Smulders, and H. Baars, “Foundations of Information Security Based on ISO27001 and ISO27002,” 3rd Edition, Van Haren Publishing, 2015.
79. ISO 27001 Official Page, https://www.iso.org/isoiec-27001-information-security.html, last accessed 2021/08/11
80. COBIT Security Baseline: An Information Survival Kit, 2nd Edition, IT Governance Institute, 2007.
81. COBIT resources, http://www.isaca.org/COBIT/Pages/default.aspx, last accessed 2021/08/11
82. NIST Special Publications (800 Series), https://csrc.nist.gov/publications/sp800, last accessed 2021/08/11
83. Gramm-Leach-Bliley Act (GLBA) Resources, www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act, last accessed 2021/08/11
84. S. Anand, Sarbanes-Oxley Guide for Finance and Information Technology Professionals, 2nd, Wiley, Edition, 2006
85. Sarbanes-Oxley Act, https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry#sox2002, last accessed 2021/08/11
86. R. Herold and K. Beaver, “The Practical Guide to HIPAA Privacy and Security Compliance,” 2nd Edition, CRC Press, 2014
87. PCI Security Standards, https://www.pcisecuritystandards.org/pci_security/ , last accessed 2021/08/11.
88. IEEE 1471, IEEE Recommended Practice for Architectural Description of Software-Intensive Systems, https://standards.ieee.org/standard/1471-2000.html, last accessed 2021/08/11
89. ISO/IEC/IEEE 42010:2011 – Systems and Software Engineering – Architecture Description, https://www.iso.org/standard/50508.html, last accessed 2021/08/11
90. Наков С., Колев В., Принципи на програмирането със C#, Издателство Фабер, Велико Търново 2018, ISBN: 978-619-00-0778-4
91. Горанов П., Тодорова Е., Георгиева Д., Концептуален модел на обектно-ориентирана библиотека от механични компоненти, Българско списание за инженерно проектиране, брой 35, януари 2018г, ISSN 1313-7530
92. Митрев Р., Компютърно моделиране и симулация, Пропелер, София, 2016г
93. A. Solvberg, Data and What They Refer to, Conceptual Modeling, Lecture Notes in Computer Science, vol 1565. Springer, Berlin, Heidelberg, 1999. https://doi.org/10.1007/3-540-48854-5_17
94. L. Vigotsky, Thought and Language, The M.I.T. Press, USA, 1962
95. DeviceLock Web Page, https://www.acronis.com/en-us/products/devicelock, last accessed 2021/08/11
96. CoSoSys Endpoint Protector Web Page, https://www.endpointprotector.com/, last accessed 2021/08/11
97. The Unified Modeling Language (UML) Web Page, https://www.uml-diagrams.org accessed 2021/08/11
98. A. Dennis, B. Wixom, and D. Tegarden, “System Analysis & Design – An Object-Oriented Approach with UML,” 5th Edition, John Wiley & Sons, 2015, pp. 19-52.
99. Gaydarski, I., Minchev, Z., Andreev, R.. Model Driven Architectural Design of Information Security System. Advances in Intelligent Systems and Computing, Madureira A., Abraham A., Gandhi N., Silva C., Antunes M. (eds) Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018).,

492, Springer, 2019, ISBN:978-3-030-17064-6, ISSN:2194-5357, DOI:10.1007/978-3-030-17065-3_35, 349-359.
100. Gaidarski, I. K., Minchev, Z. B., Andreev, R. D.. Model Driven Approach for Designing of Information Security System. Journal of Information Assurance and Security, 13, MIR Labs, 2019, ISSN:1554-1010, 149-158,
101. Gaydarski, I., Minchev, Z., Conceptual Modeling of Information Security System and Its Validation Through DLP Systems. Proceedings of BISEC 2017, Belgrade Metropolitan University, 2017, ISBN:978-86-89755-14-5, DOI: 10.13140/ RG.2.2.32836.53123, 36-40
102. Gaydarski, I., Minchev, Z.. Virtual Enterprise Data Protection: Framework Implementation with Practical Validation. Proceedings of BISEC 2018, October 20, Belgrade, Serbia, Belgrade Metropolitan University, 2019, ISBN:978-86-89755-17-6,
103. Gaydarski, I., Minchev, Z., Andreev, R.. Model Driven Architectural Design of Information Security System. Advances in Intelligent Systems and Computing, Madureira A., Abraham A.,Gandhi N., Silva C., Antunes M. (eds) Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018)., 492, Springer, 2019, ISBN:978-3-030-17064-6, ISSN:2194-5357, DOI:10.1007/978-3-030-17065-3_35, 349-359.
104. Гайдарски И., Минчев З., „Моделиране, анализ, експериментална валидация и верификация на системи за информационна сигурност в корпоративна среда“, IT4SEC Reports, No. 132, 2019, стр. 1-29, ISSN 1314-5614
105. Minchev Z., “Methodological Approach for Modelling, Simulation & Assessment of Complex Discrete Systems,” In Proc. of National Informatics Conference Dedicated to 80-th Anniversary of Prof. Petar Barnev, Sofia, Bulgaria, Institute of Mathematics & Informatics, Bulgarian Academy of Sciences, 2016, pp. 102-110, DOI: 10.13140/RG.2.1.1865.4481
106. Boyanov L., Minchev Z., “Cyber Security Challenges in Smart Homes,” In Proceedings of NATO ARW “Best Practices and Innovative Approaches to Develop Cyber Security and Resiliency Policy Framework,” Ohrid, Macedonia, June 10-12, Published by IOS Press, NATO Science for Peace and Security Series - D: Information and Communication Security, Vol.38, 2013, pp. 99 – 114.
107. Gaydarski I., Minchev Z.. Challenges to Data Protection in Corporate Environment, Chapter 8, In Z. Minchev, (Ed) Book “Future Digital Society Resilience in the Informational Age”, Sofia, Institute of ICT, Bulgarian Academy of Sciences, SoftTrade, December, 2018, ISBN 978-954-334-221-1, 82-100
108. Chen P., “The Entity-Relationship Model-Toward a Unified View of Data,” ACM Transactions on Database Systems 1, 1976, pp. 9-36.
109. Minchev Z., “Data Relativities in the Transcending Digital Future,” In Proc. of BISEC 2018, Belgrade, Serbia, October 20, 2018 (in press)
110. Minchev Z., Dukov G., Cyber Intelligence Decision Support in the Era of Big Data, In ESGI 113 Problems & Final Reports Book, Chapter 6, Fastumprint, 2015, pp. 85-92.
111. Minchev Z., “Security Challenges to Digital Ecosystems Dynamic Transformation,” In Proc. of BISEC 2017, Belgrade, Serbia, October 18, 2017, pp. 6-10.
112. Sycara K., “Multiagent Systems,” AI Magazine, 19, No. 2, 1998, pp. 79-92.
113. Gaydarski, I., Kutinchev,P.. Using Big Data for Data Leak Prevention. proceedings of The International Conference “Big Data, Knowledge and Control Systems Engineering” (BdKCSE’2019)), IEEE Digital Library, 2020, ISSN:2367-645, DOI:10.1109/BdKCSE48644.2019.9010596
114. Data Breach Investigations Report 2021, Verizon, 2021,: https://www.verizon.com/business/resources/reports/dbir/, last accessed 2021/08/11
115. Forrester J., “World Dynamics,” Cambridge, Massachusetts, Wright-Allen Press, 1971.

116. Meadows D., Randers J., Meadows D., Limits to Growth: The 30-Year Update, Chelsea Green Publishing Company, 2004.
117. CYREX 2018 Web Page: http://securedfuture21.org/cyrex_2018/cyrex_2018.html , last accessed 2021/08/11
118. Jain L., Lim C., Knowledge Processing and Decision Making in Agent-Based Systems, Springer-Verlag Berlin Heidelberg 2009, ISBN 13:978-3-540-88049-3
119. БДС EN ISO/IEC 27002:2017 “Информационни технологии. Методи за сигурност. Кодекс за добра практика за управление на сигурността на информацията”, https://www.bds-bg.org/bg/project/show/bds:proj:102368, last accessed 2021/08/11
120. БДС EN ISO/IEC 27003:2020 “Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Указания”, https://www.bds-bg.org/bg/project/show/bds:proj:114396, last accessed 2021/08/11
121. БДС ISO/IEC 27004:2017 "Информационни технологии. Методи за сигурност. Управление на сигурността на информацията. Наблюдение, измерване, анализ и оценяване", https://www.bds-bg.org/bg/project/show/bds:proj:102534, last accessed 2021/08/11
122. CYREX 2019 Web Page, http://securedfuture21.org/cyrex_2019/cyrex_2019.html, last accessed 2021/08/11
123. CYREX 2020 Web Page, http://securedfuture21.org/cyrex_2020/cyrex_2020.html, last accessed 2021/08/11
124. Gaidarski I., Minchev Z. (2021) Insider Threats to IT Security of Critical Infrastructures. In: Tagarev T., Atanassov K.T., Kharchenko V., Kacprzyk J. (eds) Digital Transformation, Cyber Security and Resilience of Modern Societies. Studies in Big Data, vol 84. Springer, Cham. https://doi.org/10.1007/978-3-030-65722-2_24
125. Schrecker S.,Soroush H., Molina J., Industrial Internet of Things Volume G4: Security Framework Paperback, Industrial Internet Consortium, September 19, 2016
126. Vester F., “The Art of Interconnected Thinking – Ideas and Tools for Dealing with Complexity,” München, MCB – Verlag, 2007.
127. MITRE ATT&CK® Framework, https://attack.mitre.org/, last accessed 2021/08/11
128. NIST Cybersecurity Framework, https://www.nist.gov/cyberframework, last accessed 2021/08/11
129. Open Web Application Security Project, https://www.owasp.org/, last accessed 2021/08/11
130. Common Attack pattern Enumeration and Classification, http://capec.mitre.org/ , last accessed 2021/08/11
131. ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, https://www.iso.org/standard/50341.html, last accessed 2021/08/11
132. ISO 31000:2009 Risk management — Principles and guidelines, https://www.iso.org/standard/43170.html, last accessed 2021/08/11
133. Risk and Responsibility in a Hyperconnected World - Pathways to Global Cyber Resilience http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf, last accessed 2021/08/11
134. Tagarev T., Polimirova D., Main Considerations in Elaborating Organizational Information Security Policies, Proceedings of the 20th International Conference on Computer Systems and Technologies CompSysTech '19, June 2019, DOI: 10.1145/3345252.3345302
135. Hilliard R.,Malavolta I., Muccini H., Pelliccione P., On the Composition and Reuse of Viewpoints across Architecture Frameworks, Joint Working IEEE/IFIP Conference on

Software Architecture and European Conference on Software Architecture 2012, ISBN:978-1-4673-2809-8, DOI: 10.1109/WICSA-ECSA.212.21
136. Bezivin J., Jouault F., Valduriez P., “On the Need for Megamodels,” in Proceedings of the OOPSLA/GPCE: Best Practices for Model-Driven Software Development workshop, 2004.
137 Symantec Data Loss Prevention Web Page, https://www.broadcom.com/products/cyber-security/information-protection/data-loss-prevention/, last accessed 2021/12/14
138 McAfee DLP Endpoint Web page, https://www.mcafee.com/enterprise/en-us/products/dlp-endpoint.html, last accessed 2021/12/14
139 Forcepoint DLP Web Page, https://www.forcepoint.com/product/dlp-data-loss-prevention/, last accessed 2021/12/14

Abstracts of Dissertations

Number 1, 2022

INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGIES
BULGARIAN ACADEMY OF SCIENCES

БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ
ИНСТИТУТ ПО ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

Брой 1, 2022

Автореферати на дисертации