BULGARIAN ACADEMY OF SCIENCES
PROBLEMS OF ENGINEERING CYBERNETICS AND ROBOTICS • 2021 • Vol. **76**, pp. 47-62
p-ISSN: 2738-7356; e-ISSN: 2738-7364
https://doi.org/10.7546/PECR.76.21.04

# Model Driven Development of Information Security System

*Ivan Gaidarski*

*Institute of Information and Communication Technologies at*
*Bulgarian Academy of Sciences*
*Acad. Georgi Bonchev Str., bl.2, 1113 Sofia, Bulgaria*
*Emails: i.gaidarski@isdip.bas.bg, ivan.gaidarski@iict.bas.bg*

**Abstract:** It is vital for the modern organization to protect its information in all forms - electronic and physical. Traditionally, the threat to information systems comes from outside to inward direction. Nowadays, corporate information is more vulnerable to internal threats operating from the inside out by employees of the organization – "Insiders". In this article we discuss method for development of information security system (ISS), by using Model Driven Engineering, which is dealing with models and model transformation. We focus on protection of information that is sensitive to the organization, protecting it from leakage or theft by insiders. The development of the ISS take into account the legislation, standards and regulations in force in the respective territory for the protection of confidential or sensitive information. Model building and subsequent transformation is performed by using appropriate tools such as Conceptual modelling and standardized Unified Modeling Language (UML). In the process of development of the ISS we create the following models: Conceptual (Guiding Model) model, Project Model, and we carry out transformation of a Conceptual Model to a Project Object Oriented Model of ISS.

**Keywords:** *Conceptual, Information, Model, Protection, Transformation, UML*

## 1. Introduction

One of the most valuable assets of modern organizations is the information and data that organizations use, analyse and generate. They are vital to any organization and form its competitive advantage. Corporate information can cover all information related to business methods, intellectual property, finance, management systems, research and development projects, customer lists and trade secrets.

It is vital for the modern organization to protect corporate information in all its forms – electronic and physical. In order to protect corporate information, organizations create and adopt information security policies, procedures and processes. Part of the corporate information falls within the scope of various regulations, directives and standards, sector-specific requirements, national legislation in force in the territory of the country in which it is registered or operates. These are the General Data Protection Regulation (Regulation (EU) 2016/679), also known as the EU GDPR [1], Ordinance on the minimum requirements for network and information security, adopted on 26.07.2019, by the Council of Ministers of the Republic of Bulgaria [2], the National Cyber Security Strategy "Cyber Sustainable Bulgaria 2020", adopted by the Council of Ministers of the Republic of Bulgaria on 13 July 2016 [3], Law on Cyber Security, adopted by the National Assembly on 31.10. 2018 [4], Law on Protection of Classified Information [5], ISO/IEC 27001: 2017 [6-8], COBIT of ISACA (Information Systems Audit and Control Association) [9, 10], NIST "800 series" (The National Institute of Standards and Technology, USA) [11], Gramm-Leach-Bliley Act (GLBA) [12] for the financial sector, Sarbanes-Oxley Act (SOX) [13, 14] – for public companies in USA, Health Insurance Portability and Accountability Act (HIPAA) [15] for the health sector, Payment Card Industry (PCI) Data Security Standard SS) [16] for credit card operators.Another part of the corporate information does not fall within the scope of data protection laws, but its confidentiality is essential to maintain an organization's competitive advantage.

Traditionally, the threat to information systems in an organization comes from outside to inward direction, as a result of external attacks and breaches caused by malicious outsiders (hackers, bots, worms). Nowadays, corporate information is more vulnerable to internal threats operating from the inside out. Unscrupulous or leaving employees often try to take confidential information with them, hoping to use it for personal gain or for the benefit of their new employer, often a competitive business. At the same time, it is quite possible that employees are simply negligent in handling information and inadvertently cause it to leak outside the organization – data transfer through unauthorized messaging applications, file sharing in cloud services, personal email accounts and more.

From vital importance for the organization is the development of an information security system that protects information from the inside out by employees of the organization – the so-called "Insiders". Such are current and former employees, partners and suppliers. Their full or limited right of access to the organization's resources such as systems, networks and data requires protection against unauthorized leakage of information with different strategy from that of traditional protection against external threats to the organization [17, 18]. In addition, the organization must ensure the protection of its assets and

comply with a number of regulatory and regulatory requirements, good practices and standards affecting its activities and the data it uses. This must be taken into account and set in the design of the information security system of the organization.

The main goal of the article is to show the essence when developing an information security system (ISS), using the methods of Model-Driven Engineering, which is dealing with models and model transformation [19, 20]. The main efforts are focused on the development of an Information Security System to protect the sensitive information of an organization from leakage or theft by insiders. The proposed structure of the information security system takes into account the legislation, standards, and regulations in force in the respective territory for the protection of confidential or sensitive information. To realize such Information Security System, the following models are proposed: Conceptual model (Guiding Model), Project Model. The transformation of a conceptual model into a project-object-oriented model of the ISS has been carried out.

## 2. Model Driven Engineering

The development of the ISS is a complex task. It is necessary to take into account many requirements formed by the environment in which this system will operate, which are often contradictory and unclear. The different participants in the process of development and operation of the system also have different and often contradictory requirements.

One possible approach to dealing with complexity is to use models. Models provide a view to the system from a particular perspective, concentrating on important aspects of the system and abstracting from others. The advantage of the models is that they provide an easier understanding of the system by stakeholders in addition to an appropriate description of the system. Through the construction and transformation of models, a complete development of the system is possible, starting from the requirements and reaching its implementation.

Model Driven Engineering (MDE) is an approach that is based on models and their transformation [19]. Model building and subsequent transformation is performed by using appropriate description tools such as the standardized Unified Modeling Language (UML), as well as model transformation techniques and tools. MDE methods provide platform independence, providing abstractness of the system description, independent of specific platforms. The ISS can be simulated with appropriate tools and optimized. The approach allows the real system to be updated or rebuilt with a suitable specific platform when the initial requirements change.

The models provide a comprehensive description of the designed system, abstracting them and focusing on the aspects important for their functionality. Here are some definitions for models:

- The model can be considered as a simplified view of reality and is a set of statements about the studied system [21].
- A model is a set of formal elements describing a system that is developed for a specific purpose and that can be analyzed using various methods [21].
- The model is a set of statements defining an abstraction of the studied system or the problem addressed by it and fulfilling a certain goal [22].
- A metamodel is a model whose modeled system or problem addressed by it is a set of models and whose purpose is to define their abstract class [22].

The model must possess the following main characteristics [21]:

1. Accuracy. The model must provide an accurate description of the characteristics important for achieving the objectives of the system
2. Predictability. The use of models makes it possible to correctly predict the important properties of the modeled system. This can be achieved through formal analysis or simulation of the system represented by the model.
3. Comprehensibility. The description of the model must be understandable and intuitive, despite the fact that some of the details of the system are abstracted. It must be presented in an appropriate form or notation.
4. Abstraction. The model is a simplified abstract image of the corresponding system it represents.
5. Simplicity. The aim is to simplify and facilitate the design and analysis of the modeled system.

MDE uses models and the relationships between them as key artifacts for the system development process. Different models can be created and used for different aspects of the system. They serve as key building blocks of the developed system.

The other main component in the MDE methodology is the transformation of the models [20]. The concept of model transformation can be defined as generating a target model from a source model according to the definition of the transformation. The definition of transformation is a set of transformation rules that together describe how the output model can be transformed into a target model [23]. The transformation operation consists of describing how one or more constructs in the source model can be transformed into one or more constructs in the target model. Transformations are defined at the meta-model level and applied to models that correspond to these meta-models.

To define model transformation, MDE uses transformation templates described by formal languages. Transformation templates can be used to compare

constructs from the source meta-model with equivalent characteristics of the target meta-model. They can be customized and applied to models in accordance with the transformation rules defining the designs and elements of the models [20]. It can be said that the transformation of models is a tool for ensuring traceability in the development of models.

## 3. Method for Development of Information Security System

Our efforts are focused on the design of SIS, designed for organizations and aimed at protection against leakage of sensitive information from inside to outside by insiders with legitimate access to the resources of the organization and its data.

The proposed by us method for developing an information security system includes the following phases:

1. 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.
2. Building a conceptual model of the problem area from different points of view. Creating generalized and detailed conceptual models.
3. Transformation of a conceptual model of the problem area into an object-oriented project model.
4. 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 Fig. 1 [24, 25].

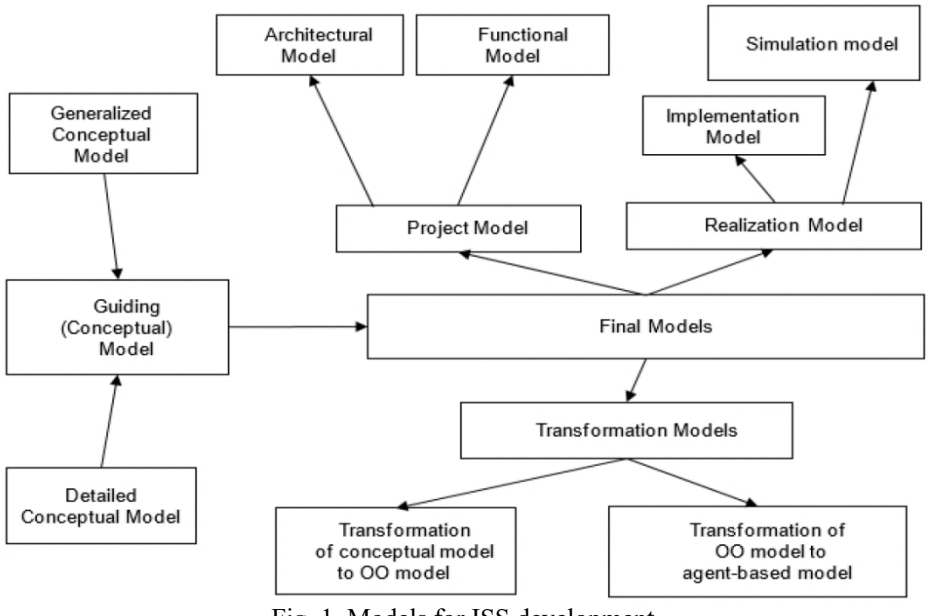


Fig. 1. Models for ISS development

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".

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 ("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".

We will consider in detail the creation of a Conceptual (Guiding Model) model and Project Model, as well as the transformation of a Conceptual Model to a Project Object Oriented Model.

## 4. Models and model transformation

### 4.1. Conceptual (Guiding) model.

The system is designed in a given Problem Area (PA) in which are presented the problems and tasks for implementation by the ISS. As a result of PA analysis, a PA Model equivalent to an Analysis Model or Domain Analysis Model is constructed. The aim is to clarify the requirements for the ISS from the point of view of all stakeholders in the development of the ISS. These requirements are formed by the environment that determines the conditions under which the system will operate. The PA model represents the desired system architecture, so it is also called a Guiding Model.

The principles of Conceptual Modeling are used for the construction of the Conceptual (Guiding) model. They are based on the guidelines for creating a framework for the architectural description of systems presented in the IEEE 1471 [26] and ISO / IEC / IEEE 42010 [27] standards. These standards introduce concepts related to how to describe the architecture of a system [1]: Environment,

Stakeholder, Concern, View, Viewpoint, System Architecture, Architectural description, Architectural framework and Model kind.

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. 2.


Fig. 2. 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.

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. The conceptual model consists of 2 parts: "Generalized model" and "Detailed model".

### 4.1.1. Generalized Conceptual Model of the ISS Problem Area

The most important questions that a system must answer from the point of view of information security are: "What do we protect?", "Why do we protect?", "How do we protect?" and "Where do we protect?".

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 Information Security (Fig. 3): 1) "Endpoint protection" (Where do we protect?), 2) "Protection of communications" (Where and What do we protect?), 3) "Data protection" (What do we protect?), 4) "Monitoring and Analysis", 5) "Management and Configuration" (How do we protect?), 6) "Security model and policy" (Why do we defend?).

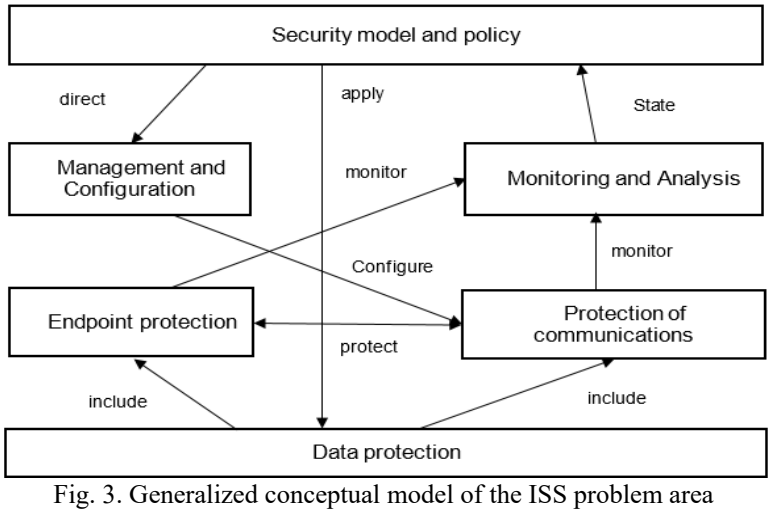


Fig. 3. Generalized conceptual model of the ISS problem area

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) [28].

For the formal presentation of the data in the ISS, we create a meta-model (Fig. 4), which is based on the viewpoint “Processing of Information” in the area of interest of the ISS (Fig. 2) [29].

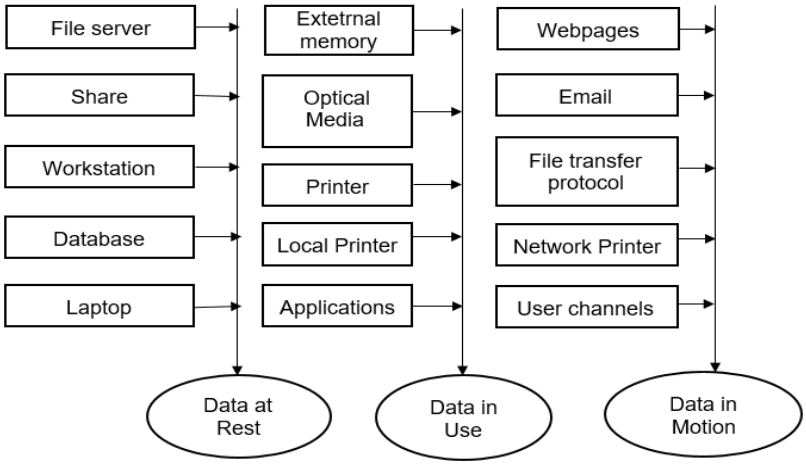


Fig. 4. Meta-model “Processing of Information”

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 (Fig. 5).

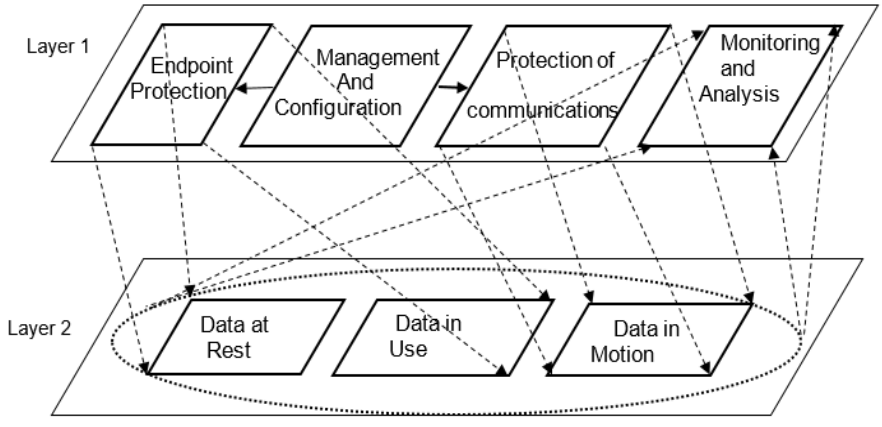


Fig. 5. Multilayer conceptual model of ISS

### 4.1.2. Detailed conceptual model 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 model of the concepts "Endpoint protection" (Fig. 6).

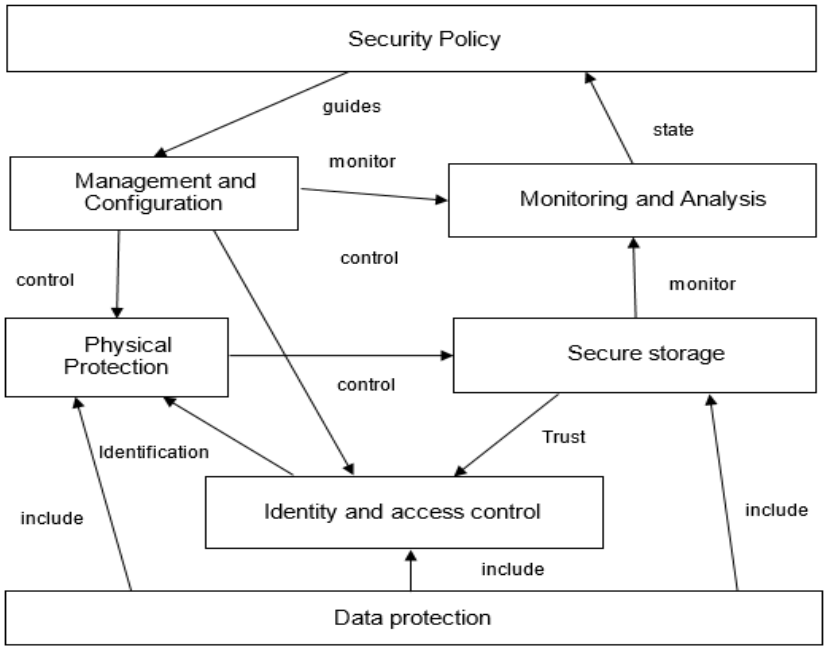


Fig. 6. Detailed conceptual model of the "Endpoint protection" concept

## 4.2. Project Model

On the basis of architectural description of ISS and the created conceptual model, a description of the architecture and functionality of the ISS is constructed, which are components of the design model. The construction of the design model is based on the use of object-oriented approach and object-oriented description language Unified Modeling Language (UML), providing tools for describing, analysing, modelling and documenting the architecture and functionality of ISS [30, 31]. The design model consists of an architectural model and a functional model, described with the corresponding diagrams in UML. The creation of a project model is based on the "model-to-model" transformation. In our case we carry out the following transformation:

***Conceptual model → Object-oriented project model***

Fig. 7 shows the main types of UML diagrams. Using different UML diagrams, different views of the system model can be represented.

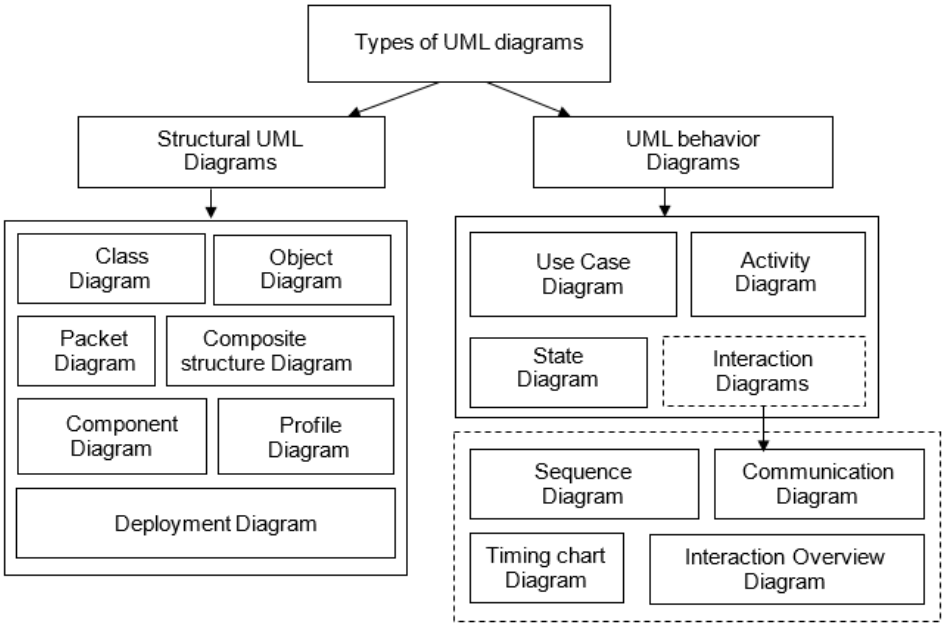


Fig. 7. Types of UML diagrams

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”, “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”.

### 4.2.1 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 Fig. 3 into

an OO model, we use a Class-diagram. To represent the object-oriented models of the detailed models of the concepts “Endpoint protection” (Fig. 6) and “Protection of the Communications”, Composite structure diagram can be used. Based on the other static diagrams – Packet diagram, Component diagram and Deployment diagram, the Realization Model can be constructed.

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. It consists of a set of classes and relationships between them [30]. The ISS concept represented by the generalized meta-model (Fig. 3) can be described by a Class-diagram, as shown in Fig. 8.

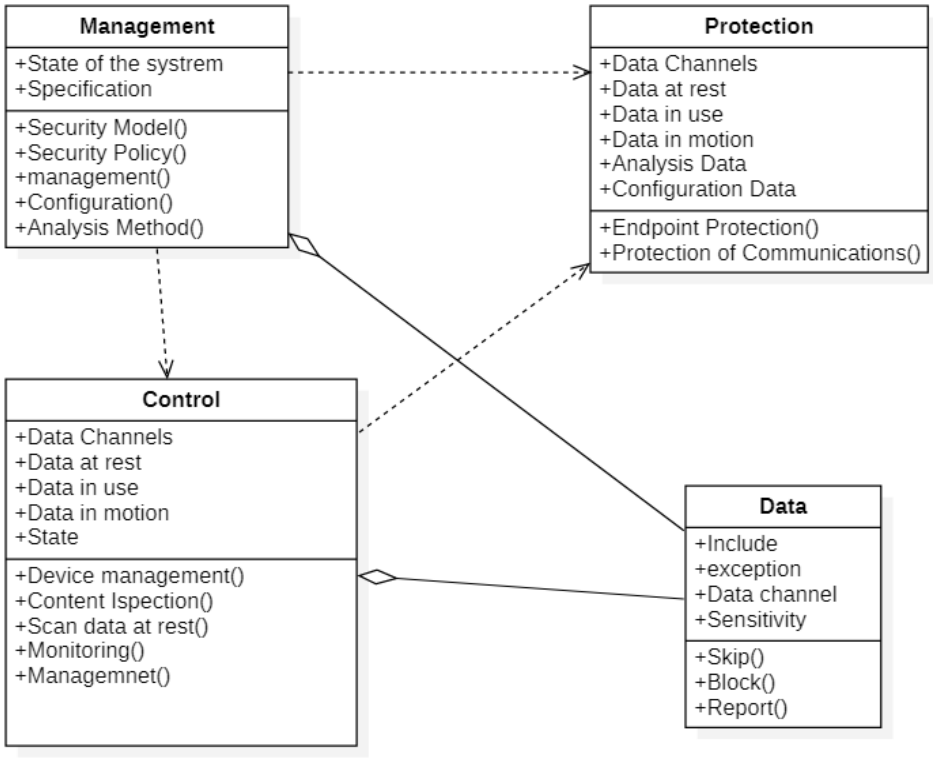


Fig. 8. UML “Class diagram” of ISS

We use the same concepts as in the meta-model, divided as methods of the four main classes. 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.

### 4.2.2 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. 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.

In addition to interaction diagrams, the dynamic behavior of the system presented with scenarios and use cases can be analyzed by activity diagrams. Fig. 9 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.

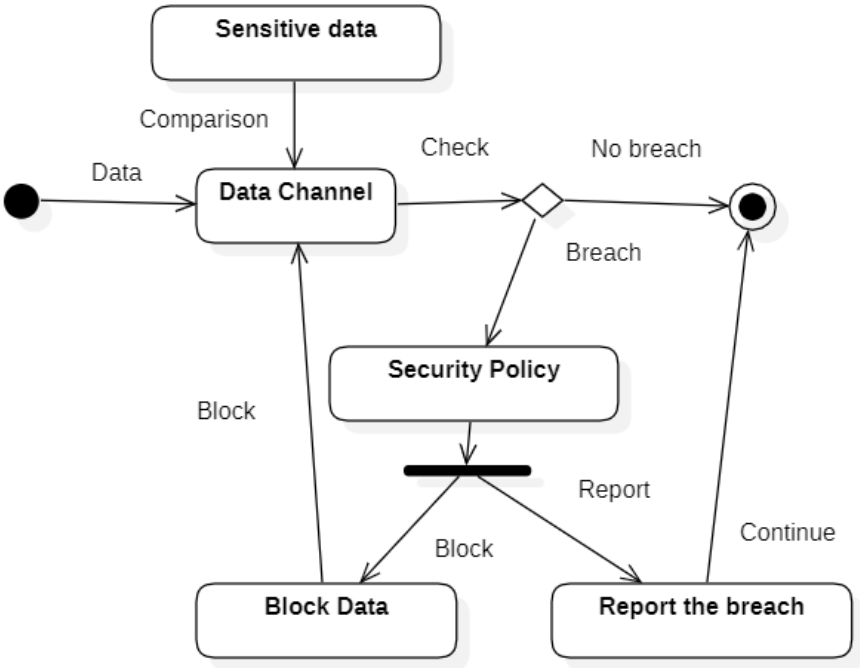


Fig. 9. UML activity diagram of the endpoint protection method

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.

## 5. Conclusion

The proposed method for development of ISS is based on the principles of the Model Driven Engineering, i.e. dealing with models and model transformations. The top-down approach, which is applied in our method, is an approach from the general to the specific. It makes possible to implement and review common data protection policies, procedures and processes in order to achieve certain objectives.

With the proposed method we discusing the development of ISS, designed for organizations and aimed at protection against leakage of sensitive information from inside to outside by insiders with legitimate access to the resources of the organization and its data. It also take into account the legislation, standards and regulations in force in the respective territory for the protection of confidential or sensitive information.

Here are the most important characteristics of the proposed method:

- The method is model-based, as a result of applying a top-down approach;
- Model-to-model transformation is applied;
- Technologically independent, which creates conditions to be the basis of a reference methodology for the development of ISS

The proosed method is suitable for establishing a reference methodology for the development of ISS based on a framework for their design, as it is technologically independent.

## References


1. Hilliard, R., Emery, D., Maier, M.: ANSI/IEEE 1471 and Systems Engineering. Systems Engineering 7(3), 257-270 (2004). https://doi.org/10.1002/sys.20008.
2. 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 2021/08/05.
3. Националната стратегия за киберсигурност „Киберустойчива България 2020”, приета от Министерски съвет на Република България на 13 юли 2016, http://www.cyberbg.eu/ , last accessed 2021/08/05.
4. Закон за киберсигурност, приет от Народното събрание на 31 октомври 2018, https://parliament.bg/bg/laws/ID/78098, last accessed 2021/08/05.

5. Закон за защита на класифицираната информация, 26.02.2019, https://www.damtn.government.bg/wp-content/uploads/2019/06/zakon-za-klasifitsiranata-informacia.pdf , last accessed 2021/08/05.
6. 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 2021/08/05.
7. Hintzbergen, J., Hintzbergen, K., Smulders, A., Baars, H.: Foundations of Information Security Based on ISO27001 and ISO27002. 3rd Edition, Van Haren Publishing (2015).
8. ISO 27001 Official Page, https://www.iso.org/isoiec-27001-information-security.html, https://www.iso.org/isoiec-27001-information-security.html, last accessed 2021/08/05.
9. COBIT Security Baseline: An Information Survival Kit. 2nd Edition, IT Governance Institute (2007).
10. COBIT resources, http://www.isaca.org/COBIT/Pages/default.aspx, last accessed 2021/08/05.
11. NIST Special Publications (800 Series), https://csrc.nist.gov/publications/sp800, last accessed 2021/08/05.
12. Gramm-Leach-Bliley Act (GLBA) Resources, www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act, last accessed 2021/08/05.
13. Anand, S.: Sarbanes-Oxley Guide for Finance and Information Technology Professionals, 2nd Edition, Wiley (2006).
14. Sarbanes-OxleyAct, https://www.investor.gov/introduction-investing/investing-basics/role-sec/laws-govern-securities-industry#sox2002, last accessed 2021/08/05.
15. Herold, R., Beaver, R.: The Practical Guide to HIPAA Privacy and Security Compliance, 2nd Edition, CRC Press (2014).
16. PCI Security Standards, https://www.pcisecuritystandards.org/pci_security/ , last accessed 2021/08/05.
17. Suryateja, P.S.: Threats and Vulnerabilities of Cloud Computing: A Review, International Journal of Computer Sciences and Engineering 6(3), 297-302 (2018).
18. Rhodes-Ousley, M.; Information Security the Complete Reference. 2nd Edition, The McGraw-Hill (2013).
19. Kent, S.: Model Driven Engineering. In IFM '02: Proceedings of the Third International Conference on Integrated Formal Methods, pp. 286–298. London, UK, Springer-Verlag (2002).
20. Topçu, O., Durak, U., Oğuztüzün, H., Yilmaz, L.: Distributed Simulation: A Model Driven Engineering Approach, Springer International Publishing Switzerland (2016). http:/doi.org/10.1007/978-3-319-03050-0_2.

21. Devedic, V., Djuric, D., Gasevic, D.: Model Driven Engineering and Ontology Development, Springer-Verlag Berlin Heidelberg (2009).
22. Perrouin, G.: Architecting Software Systems Using Model Transformations and Architectural Frameworks, University of Namur (2007).
23. Kleppe, A., Bast, W., Warmer, J.: Mda Explained, the Model Driven Architecture: The Model Driven Architecture: Practice and Promise. Addison-Wesley Professional (2003).
24. 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). http:/doi.org/10.1109/WICSA-ECSA.212.21
25. 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).
26. IEEE 1471, IEEE Recommended Practice for Architectural Description of Software-Intensive Systems, https://standards.ieee.org/standard/1471-2000.html, last accessed 2021/08/05.
27. ISO/IEC/IEEE 42010:2011 – Systems and Software Engineering – Architecture Description, https://www.iso.org/standard/50508.html, last accessed 2021/08/05.
28. Accenture Security 2019 Cyber ThreatScape Report https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf , last accessed 2021/08/05.
29. Шаньгин, В.Ф.: Защита информации в компьютерньх системах и сетях. ДМК Пресс (2012).
30. The Unified Modeling Language (UML) Web Page, https://www.uml-diagrams.org/ , last accessed 2021/08/05.
31. Dennis, A., Wixom, B., Tegarden, D.: System Analysis & Design - An Object-Oriented Approach with UML, 5th Edition, John Wiley & Sons, 19-52 (2015).