Abstracts of Dissertations

Institute of Information and Communication Technologies

BULGARIAN ACADEMY OF SCIENCES

7 / 2025

MODELLING AND AUTOMATION OF STANDARDIZED INFORMATION SECURITY MANAGEMENT SYSTEMS

Todor Velev

МОДЕЛИРАНЕ И АВТОМАТИЗАЦИЯ НА СТАНДАРТИЗИРАНИ СИСТЕМИ ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА

Тодор Велев

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.*

e-ISSN: 1314-6351

BULGARIAN ACADEMY OF SCIENCES

Abstract of PhD Thesis

MODELLING AND AUTOMATION OF STANDARDIZED INFORMATION SECURITY MANAGEMENT SYSTEMS

Todor Velev Velev

Supervisor: Prof. Nina Dobrinkova

Approved by Supervising Committee:

Prof. Stefka Fidanova
Prof. Olympia Roeva
Prof. Leoneed Kirilov
Prof. Hristo Kostadinov
Assoc. Prof. Krassimira Ivanova

INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Department of Modelling and Optimization

I. GENERAL CHARACTERISTICS OF THE DISSERTATION

Relevance of the problem

In the modern information reality, characterized by the dynamic digitalization of all social and economic processes, information is becoming a strategic asset and at the same time an increasingly vulnerable resource. The daily exchange of huge amounts of data, the complex infrastructure of interconnected systems and the widespread use of cloud technologies and mobile devices lead to an increase in threats to information security. Cyberattacks, incidents of unauthorized access and data compromise are becoming more frequent, which poses challenges to organizations, both in the public and private sectors.

Traditional approaches to security, based primarily on manual processes, separate technical means or formal implementation of minimum requirements, no longer meet current risks. Against this background, international standards, such as ISO/IEC 27001, NIST, FISMA, GDPR and others, require a systematic, integrated and adaptive approach to information security management. They imply the construction of information security management systems (ISMS) that combine policies, procedures, technologies, human factors and organizational culture.

Automation of processes in ISMS is a new necessity, predetermined by the complexity and volume of data and information flows. Digital ISMS management platforms must provide traceability, control, continuous assessment and improvement, as well as the ability to integrate with new regulatory requirements and business changes. In this dynamic environment, information security is a task of high priority and increasing importance. Information security management systems are not adequate without automated platforms with elements of artificial intelligence to master the growing volume and types of information flows and interactions.

The relevance of this dissertation stems from a clearly identified need for a new, qualitatively different approach to the management of standardized SMIS. This approach should be based on a formalized, semantically rich model of the security domain and use this model to achieve a high degree of process automation. The development of an intelligent, integrated software environment (platform) based on such a model can dramatically increase the effectiveness, efficiency and adaptability of security management, while reducing costs and administrative burden on organizations.

Object and subject of the study

The object of research is standardized information security management systems (ISMS) and the possibilities for automation of functionalities and their management.

The subject of research is a Model of a software product, a complex Platform, that can model and automate any information security management system, built in accordance with an internationally recognized standard or standards in this field.

Goals and objectives

The goal of the dissertation is to develop and validate a platform model to manage and automate standardized information security management systems.

To achieve this goal, the following tasks have been formulated:

- Research and analysis of the theoretical foundations of standardized information security management systems in aspects:
  - Information security;
  - Information security standards;
  - Information Security Management Systems (ISMS);
  - Software applications for IS.
- Analysis of the processes, requirements and characteristics of the platform for management and automation of standardized information security management systems. The task is divided in accordance with the specified methodology into the following subtasks:
  - Research and analysis of work processes subject to automation and their corresponding information flows;
  - Determining the functional and non-functional requirements of the platform, through research and analysis of data, user groups and information security standards;
  - Identifying the general characteristics of the system.
- Design of an optimal platform model for modeling and automation of standardized information security management systems and its associated architecture.

Methods

To achieve the goals and objectives set in the dissertation, a combination of research methods was used, ensuring both theoretical depth and practical applicability of the results.

- **System analysis**

This method was applied to consider the ISMS as a complex, dynamic system of interconnected components, processes and activities. Through the systems analysis, the main elements of the ISMS, their dependencies, input and output parameters, as well as their interaction with the external environment of the organization were identified. The systems approach allowed for the structuring of the problem, its decomposition into smaller, manageable parts and their integration into a single platform model.

- **Comparative analysis**

An in-depth comparative analysis of various international standards (ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework), regulatory requirements (GDPR, NIS2), risk management methodologies (ISO 31000) and existing software solutions for ISMS was carried out. This analysis allowed the identification of good practices, common elements and gaps in current approaches, which served as the basis for formulating the requirements for the new platform.

- **Modeling**

The modeling method is central to the dissertation. The following techniques were used:

  - Conceptual modeling - for high-level definition of the components and logical structure of the proposed platform;
  - Architectural modeling - for designing the software architecture, including the selection of layers, modules, and technology stack;
  - Business Process Modeling (BPMN - Business Process Model and Notation) - used for a detailed description of key processes in an information security management system (e.g. risk assessment, incident management, audit) for the purpose of their standardization and preparation for automation;
  - Data modeling (ERD - Entity-Relationship Diagram) - is used to structure information, define objects, their attributes and relationships necessary for the platform's database.

- **Data analysis**

Used to collect, systematize, process, and interpret information related to cyber threat statistics, effectiveness of existing security measures, as well as data generated during prototype testing.

- **Literature review**

A thorough and systematic review of scientific and professional literature was conducted - books, scientific articles, conferences, reports, standards and good practices in the fields of information security, management systems, process modeling, software engineering and automation.

- **Expert assessment method**

When defining the requirements and validating the model and prototype, expert opinions and recommendations from specialists in the field of information security and auditing were indirectly taken into account. The combination of these methods provides a comprehensive approach to the problem, combining theoretical knowledge with practical application and validation of the proposed solutions.

II. VOLUME AND STRUCTURE

The dissertation is systematically organized into an introduction, three main chapters, main conclusions and inferences, appendices, and a comprehensive list of references. The total volume of the dissertation without appendices is 124 pages, which includes rich illustrative content of 29 figures (diagrams, schemes, screen shots) and 34 tables presenting data and classifications. The list of references contains 80 sources, demonstrating the breadth and depth of the literature review conducted.

III. CONTENT OF THE DISSERTATION

Introduction

The introduction clarifies the relevance of the problem and presents the methodological parameters of the dissertation, its structure, object, subject, goals and objectives.

CHAPTER 1 Standardized Information Security Management Systems

The first chapter of the dissertation aims to lay the theoretical foundations of the research. It provides a detailed review and analysis of existing approaches, standards and technologies in the field of information security management. The chapter is structured in such a way as to systematically identify the problems and gaps that the present work aims to address. A theoretical analysis has been made of the fundamental foundations on which the model of the Platform for Management and Automation of Standardized Information Security Management Systems is built, namely: Information Security; Information Security Standards; Information Security Management Systems (ISMS); and Software Applications for IS.

The chapter defines the terminology and aspects of information security, the methods, technologies and tools for information protection and the challenges that provoke the study. The evolution of information security from a purely technical aspect to a comprehensive management process is discussed. The need for a systematic approach to security management in organizations is presented, which goes beyond the framework of specific measures and ensures long-term sustainability.

Information security standards are analyzed, as well as the terminology, nature and objectives of standardization. The historical development of information security standards is examined, starting from early initiatives to the formation of international frameworks. The benefits of implementing standardized ISMS are discussed, including improving management processes, reducing risk, increasing customer and partner trust, and complying with regulatory requirements. The main elements, architecture and processes for the development and implementation of an ISMS are examined. This section provides a detailed overview, describing the key elements of an IMS according to the standard, including:

- Organizational context - understanding internal and external issues, stakeholders and scope of the EMS;

- Leadership - senior management commitment, policies and allocation of roles and responsibilities;
- Planning - addressing risks and opportunities, security objectives and plans to achieve them;
- Support - resources, competence, awareness, communication and documented information;
- Operational activity - operational planning and control, information security risk assessment, information security risk processing;
- Performance evaluation - monitoring, measurement, analysis, evaluation, internal audit and management review;
- Improvement - nonconformities and corrective actions, and continuous improvement. Special attention is paid to Annex A of ISO/IEC 27001, which contains a list of security controls categorized by domain.

Despite the significant benefits, implementing and maintaining an ISMS is associated with a number of challenges. The difficulties that often lead to delays, increased costs or unsuccessful certification are analyzed. The following are discussed:

- Lack of resources - insufficient staff, budget and time;
- Complexity of processes - a large number of documents, procedures and control points;
- Resistance to change - difficulties in changing the culture and work habits in the organization;
- Documentation management - voluminous and dynamic documentation that requires constant updating;
- Audit and compliance - complex internal and external audit processes requiring comprehensive evidence of compliance;
- Continuous improvement - keeping the ISMS in constant compliance with changing threats and business needs.

These challenges serve as a basis for arguing for the need for automation and modeling to address these problems.

The first chapter also analyzes the market for software tools to support ISMS. The functionalities of leading products are studied and the following common shortcomings are identified:

- Passive documentation orientation - most systems are "electronic repositories" for storing policies, procedures, and records. They support auditing, but not active, dynamic management.
- Lack of semantic understanding - data is stored in relational databases that do not manage the complex semantic relationships between assets, threats, controls, and business processes. This limits the possibilities for automated analysis and inference.
- Poor process automation - processes such as risk assessment are often reduced to filling

out spreadsheets that are then uploaded to the system. There is a lack of true automation based on logical rules.

- Low flexibility and extensibility - systems are usually built around one specific standard and are difficult to adapt to other frameworks or organization-specific requirements.

Main conclusions of Chapter 1

- ☞ Based on the analysis of information security, information security standards and information security management systems, it is concluded that a comprehensive approach is needed to address the described progressive challenges.
- ☞ From the study of the types and functional scope of software applications related to ISMS, the segmentation of products is identified. ISMS comprehensive management systems are mainly in aspects of certification, re-certification and maintenance of the necessary records and templates for the purposes of the audit process. There is a lack of comprehensive solutions that manage and control all work processes and information flows in the infrastructure and superstructure of the organization. The platform approach to building an adaptive system that models and automates standardized information security management systems is an innovative, generalized solution to the treated issues.
- ☞ In order to ensure the efficiency, usefulness and reliability of the platform, it is necessary to develop a model that is based on comprehensive monitoring, analysis and management of the document matrix, workflows and information flows and assets of the organization.

CHAPTER 2. Modeling a platform for management and automation of standardized information security management systems.

Chapter Two presents a methodology for researching and modeling an automated standardized information security management platform, and in accordance with it, an analysis of the processes, determination of requirements, and identification of the general characteristics of the system are carried out. The research and analysis, according to the proposed methodology, includes the following key steps:

- **Process analysis**

Research and analysis of the standardized work processes that the system should automate and the corresponding information flows.

The following standardized work processes have been identified and described:

- o Implementation of business processes IBP/Document management ;
- o Platform administration processes;
- o Defining and managing business processes;
- o Management of SUS;
- o Monitoring and control;
- o Audit.

- **Determining requirements**

To determine the functional and non-functional requirements, the following was performed:

- Research and analysis of user groups;

Users of a platform for the management and automation of standardized information security management systems are divided into 2 large groups:

- Users - companies and organizations that have implemented an Information Security Management System certified to an internationally recognized standard. These are users from all sectors of the economy, operating in all sections of the classifier of economic activities, including state and municipal organizations.
- Certification and consulting organizations - perform audits for the certification of ISMS and control audits to confirm compliance.

- Research and analysis of information security standards;

The study of the requirements of the standards was carried out according to their main groups of characteristics:

- Content of the standard - name, purpose, policies, scope, requirements, conditions, definitions, type and area of applicability.
- Infrastructure - procedures, processes, documents, controls, registers, deadlines, tools and functional algorithms.
- Superstructure (external environment) - correspondents, customers, suppliers, partners and institutions, related standards, possible integration opportunities, audits, etc.
- Resources - organizational structure and personnel, assets, tools and materials needed to plan, maintain and control standard mechanisms.

- Research and analysis of data.

A platform for the management and automation of standardized information security management systems, SUSI, operates with two main data groups, as follows:

- Data related to information security standards;
- Data related to the functional requirements for the Platform;

The result is shown in Appendix 3.

- **Defining the general characteristics of the platform**

The general characteristics of the platform were determined by studying good practices for user behavior, productivity, security and administration of information systems. Due to the specificity of the goals set and the subject matter studied, heuristic techniques were used for this task, such as:

- Best practices approach;
- Research and analysis of academic sources;
- SCAMPER technique;

- The Delphi Method

Unified Modeling Language – UML™ and Business Modeling – is used to describe the processes and requirements. Process Model and Notation (BPMN) standard for visual modeling of business processes in the form of diagrams like the ones shown below.

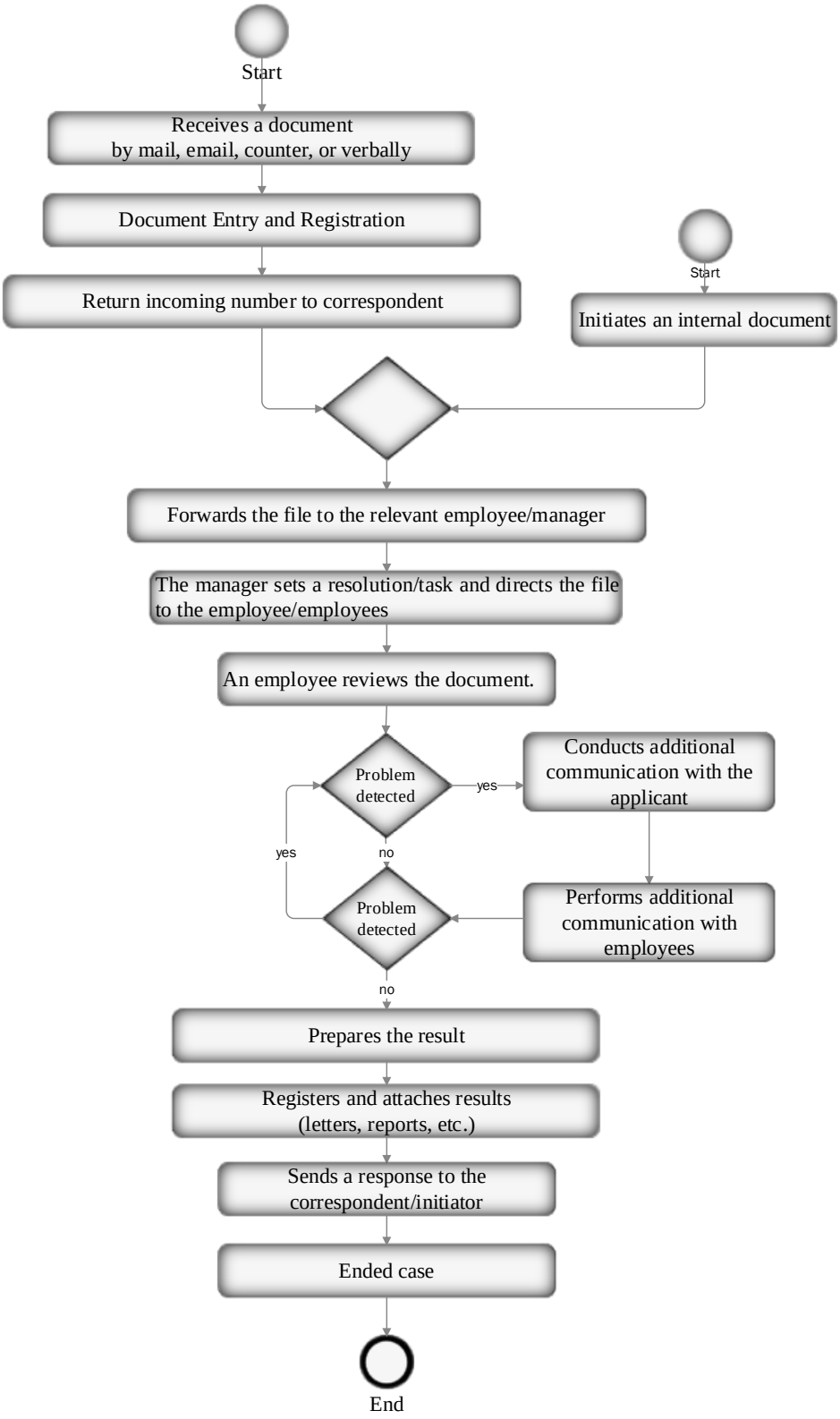


Figure 1 Document Management Process

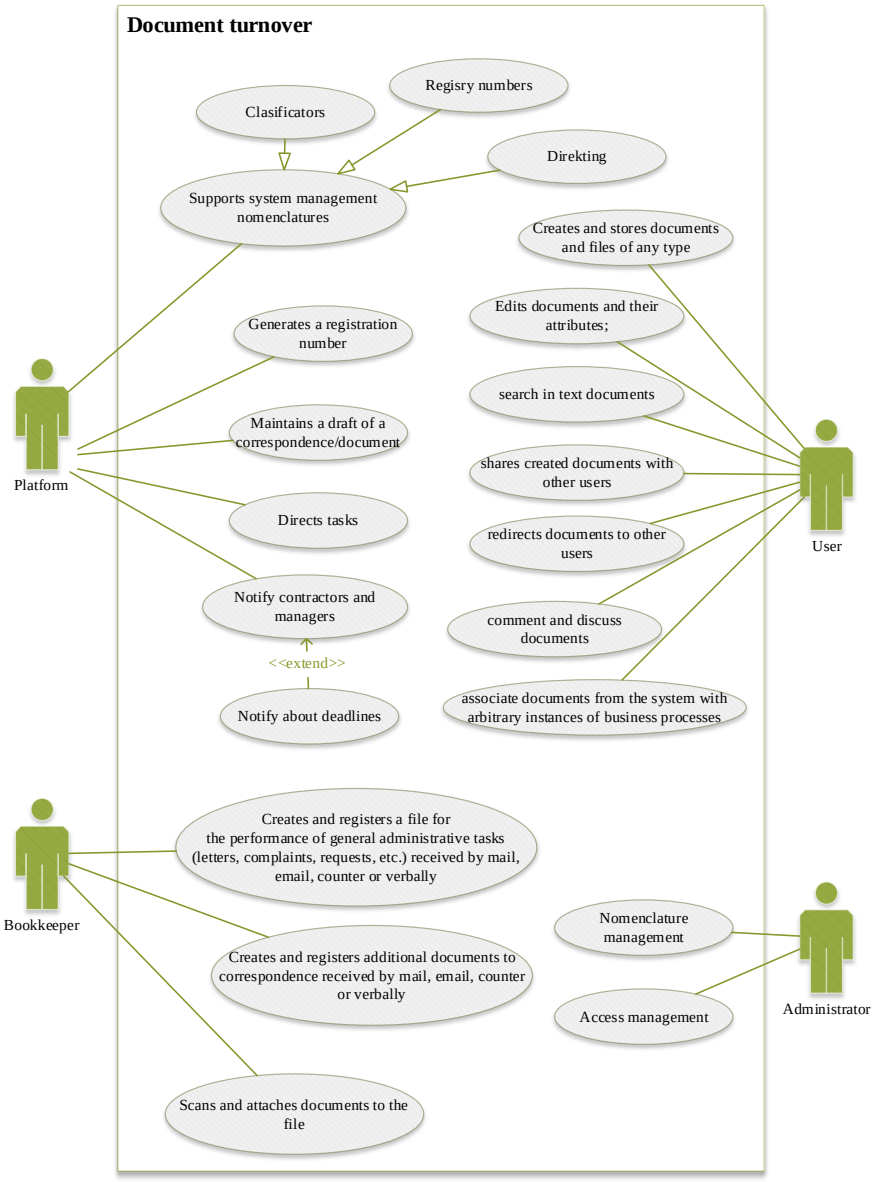


Figure 2 Document flow diagram of user cases

Main results of Chapter 2

- An analysis of the standardized work processes to be included in the Platform model, subject to automation, and the relevant information flows corresponding to them, has been carried out.
- Based on an analysis of the data, user groups and information security standards, the functional and non-functional requirements that must be reflected in the modeling of the Platform have been determined.
- Good practices for user behavior, productivity, security and administration of information systems were studied and the common characteristics of the Platform were identified.
- The necessary input parameters, attributes and constraints for modeling the platform for management and automation of standardized information security management systems have been defined.

CHAPTER 3. Platform model for modeling and automation of standardized information security management systems.

In the third chapter, the author's theory of a document matrix is presented, as a basis for operational management of an organization and the company. The modeling methodology and the conceptual model of the Platform are described. An optimized model of the subject of the dissertation has been developed, built according to the theoretical foundations and the research and analyses presented in Chapter 1 and Chapter 2. A logical and physical architecture for the implementation of the platform is proposed.

Document matrix

Every company, regardless of its size, carries out its activities in an internal and external working environment. The internal environment is determined by the company's resources (human, material and intangible) and by the work processes within it, related to the subject of activity. The external environment is the customers, suppliers, partners and government institutions with which the company works.

Information security management systems according to internationally recognized standards define, regulate, manage, monitor, record and archive the internal and external operating environment through the organization's document system and the corresponding data sets.

A document is a record that reflects in its development every action, norm, event, resource, attitude, process and intellectual production. In addition to the fact that nowadays documents are electronic and paper, they can be conditionally classified into several formal groups - Conventional records and Specialized documents.

The quantity of all these records, called documents, define and determine the company, its history, capacity, quality and competitive ability.

Documents themselves are not independent separate units. They are connected in **a document network specific to each company.** Each document is a final product, behind which stands a process of varying complexity and scope. Each document process consists of activities and stages and, as in any production, requires resources and materials. Resources and materials, in turn, are most often data sets and other documents that have their own processes and their own life cycle. The multitude of documents and the connections between them form the document network of the organization. Unlike the Internet, however, the document network of a company has defined paths, connections and forms (forms) and is connected to and indexes and manages the data sets (bases) of the organization.

For this reason, the system of company documents is considered not as the document network, **but as the document matrix** of the company.

The document matrix affects every element of the company's internal and external working environment and it is quite logical that it allows for maximum control over the

organization. The company document matrix is the basis of the management of any management system built according to internationally recognized standards. They are based on policies, work processes, procedures and numerous forms and records for their control.

When documents are digitized, the connections between them are visualized, and the matrix is dressed in appropriate functionality, an extremely effective system for monitoring, controlling, and managing all levels and resources in the company is obtained.

Platform concept

The platform for modeling and automation of standardized information security management systems is a modern, innovative, integrated information and operational system that models, digitizes, registers, manages, stores and controls work processes and related information and documentation in accordance with various internationally recognized information security standards.

The model is based on monitoring, analysis and management of the document matrix, workflows and information flows and assets of the organization. The platform covers all information units - documents (paper and electronic), audio and video communications, system, program and communication logs, etc. It monitors incoming, outgoing and internal information flows and manages them according to the workflows and standardized forms modeled in it.

Workflows and standardized forms are modeled according to the policies, procedures and templates of the information security management systems (ISMS). All records related not only to the elements of the ISMS, but also to the operational processes are formalized in the platform and are carried out only through it. The goal is to use the latest technological advances to digitize, index and revitalize the document matrix of the organization and enable operational efficiency of security management.

Information assets are introduced into the Platform as parameterized objects. Each control from the system of controls of the information security standards, according to which the ISMS is built, is associated with one or several predefined criteria of the platform. Each criterion is a formalized record with certain parameters of the registered information and frequency and method of verification. For each criterion, triggers for platform action are defined, according to possible values or events.

Controls are applied to an asset and/or process in accordance with the ISMS.

The mission of the platform is to integrate all document flows related to the work processes in the client organization. To connect the many application software products working in the field of information security and data arrays into a single information, communication and management system. The platform unites information sections and information flows into a single information space and provides an integrated environment for storage, management and exchange. This allows to effectively monitor

the movement of information structured into separate types of document units, to model the IMS and to implement reliable control.

The platform models the hierarchical structure of the organization, with the possibility of changes, allowing for adequate distribution of tasks according to the company's subordination. The system manages the movement of various types of documents, automating all phases of workflows.

According to the research and analysis presented in Chapter 2, the platform for modeling and automation of standardized information security management systems is implemented with the following components (modules):

- Module for defining and managing business processes DBP;
- Business Process Execution Module IBP;
- ISMS module;
- Audit and Control Module;
- The administrative module;

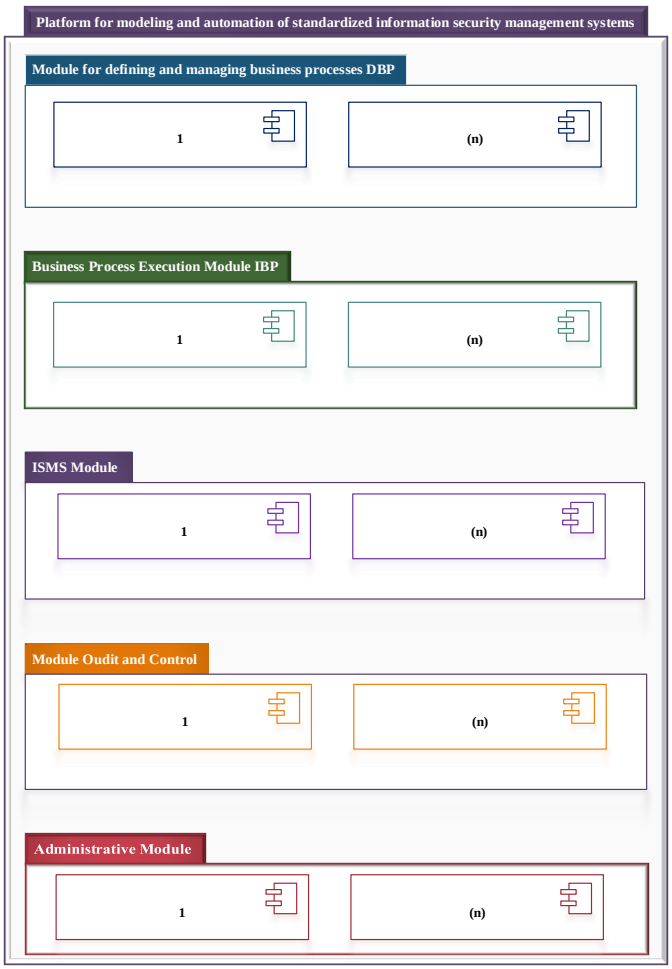


Figure 3 Platform Structure

The platform uses a single database in which the necessary information is entered and output through various interfaces, according to the information classes. The base arrays are managed by building specialized logic for each of them - standards, terms, processes, users,

procedures, routes, forms, controlled processes, and various unstructured data. The platform layer, the so-called middleware, implements the logic and exchange of information between the interfaces for entering information and the database. Another platform layer implements the connection of the functional modules and the database. The functional modules (components) perform a certain group of functions by providing interfaces for performing the necessary tasks. The platform builds its modules in the context of each client organization, as a set of components (functional modules) as shown in the figure.

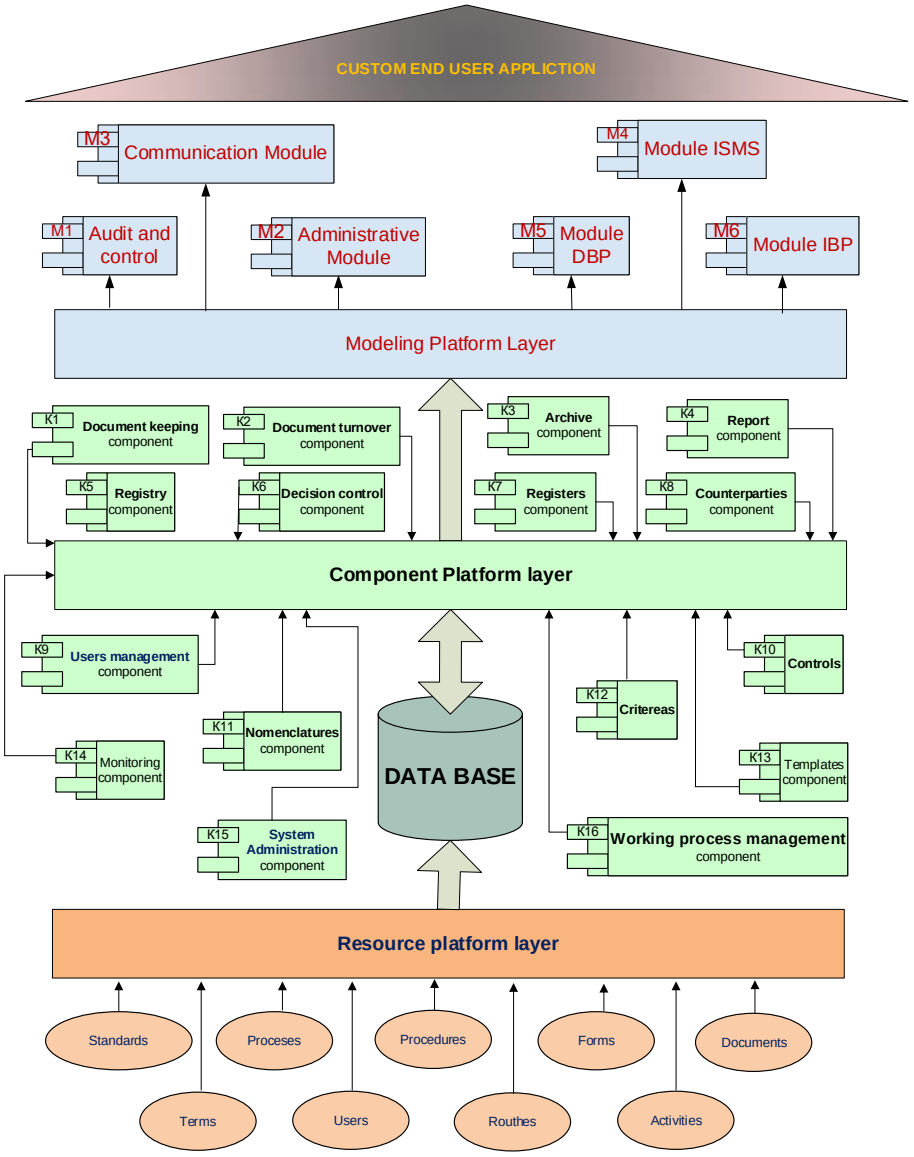


Figure 4 Conceptual architecture of the model

The system has a registration and control part, in which the organization's indexes are entered and all incoming-outgoing and internal operational documents (events) are registered in accordance with them. Document numbers are automatically generated according to a pre-set stereotype. Deadlines for execution can be set for each registered document, which it controls. The platform also functions as a communicator, informing in various ways (e-mail, SMS, sound and visual) about various controlled events, overdue deadlines and tasks to be performed. The electronic system models the operational procedures and process maps

created in the company according to the relevant standard, ensuring the informationally correct compliance with all work processes, filling in the relevant forms and blanks, monitoring of work processes and control of decisions. It guarantees the highest possible levels of security, reliability and information protection. It provides the opportunity for each user to identify themselves not only with a username and password, but also with a private electronic signature. Each employee/user has pre-defined profiles, roles, access rights and functionality corresponding to their job description. The system dynamically generates personalized screens upon user login, providing an intuitive user interface and navigation.
The modules of the Platform build the models related to the management of various types of internationally recognized standards with a rich set of tools: standardized processes; pre-developed scenarios and stagings; a set of predefined forms; developed conventional registers; specialized registers; internal communication environment; systems for evaluation, control and audit support; and others.

Modeling methodology

Based on functional and non-functional requirements, business processes and the specification of user cases defined in the previous chapter, after the research and analysis, an optimal set of information descriptors was developed, distributed into logical information classes and subclasses.

The set of descriptors generated by the research and analysis is decomposed into logical information classes, in accordance with their functional orientation in the description of the standards. Information classes are considered as program objects and sub-objects. They are described by their attributes, which are called information identifiers. Their representation is unified by using a specific technical format that defines the format of representation of the values of each attribute of the information objects. The technical format of the information classes and their attributes is described by the syntax of the Unified Modeling Language (UML).

For the design of the platform, UML class diagrams are used. which depict the structure of the system by modeling its classes, properties, operations and relationships between objects. A class diagram is a visual notation used to build and visualize object-oriented systems. It is a static structural diagram demonstrating the properties of the platform, classes, operations and relationships between objects for the description and design of the system. Class diagrams are a form of structural diagrams, as they determine what should be included in the modeled system. Information identifiers are modeled in 3 levels of information classes structured in modules of the platform. As an example, I apply a model of one main SUSI module.

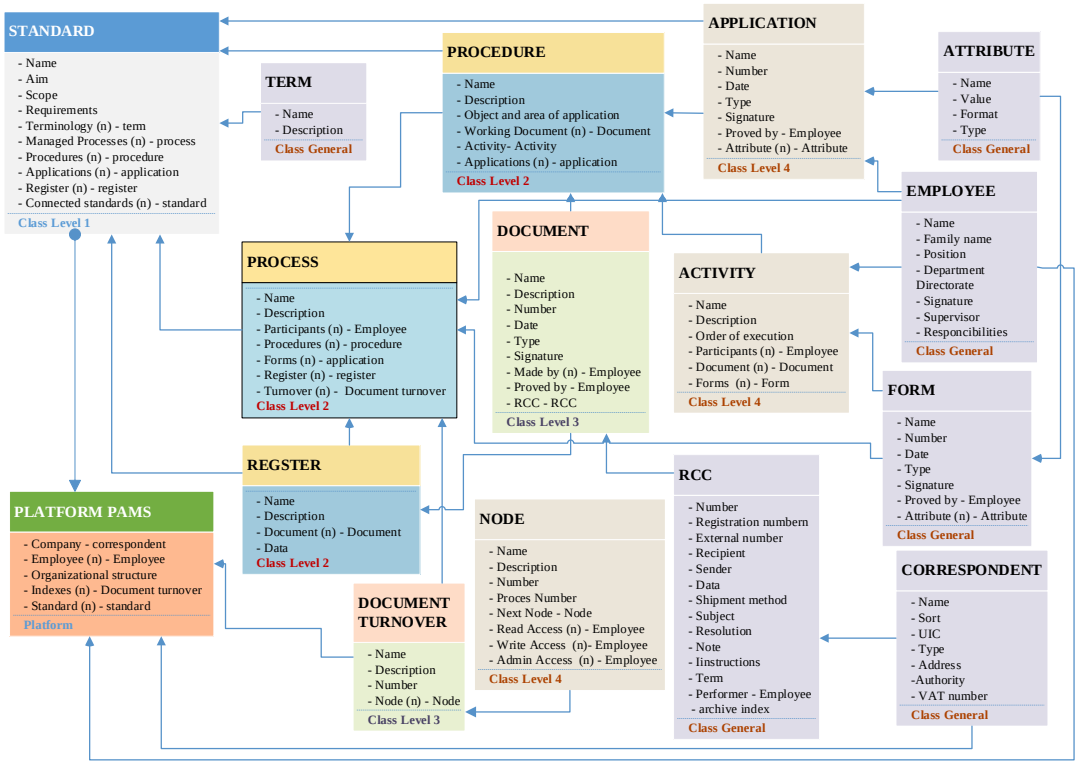


Figure 5 SUSI module

The identifiers for each class are described in detail in a tabular form.

Table 1Organizational Unit (Structure)

Description		
Type	**Name/ Format**	**Description**
Class	Organizational unit: () Structure	Organizational Unit (Structure) is a base class of the Administrative Module, related to describing the structure of the organization and its corresponding modeling in the Platform.
Attribute	Name: Nvarchar (400)	Name of the organizational structural unit.
Attribute	Type: Type	The structure type is a predefined nomenclature – directorate, department, sector and position.
class	Parent Organizational Unit: Structure	Name of the parent organizational unit to which the structure belongs (if any)
Subclass	Rights (n): Right	A list of rights on the information objects that the organizational unit and all its substructures have. A set of rights are defined for each information object from the classifier - Example: for the information object "Incident Register" the right to read, the right to register and the right

		to edit.
Subclass	Templates: Template	Templates are a set of rights that can be applied to any information object and added as a structural unit in a set.
Subclass	Users: User (n)	A list of employees of the organization who have been added to the organizational structure.

System architecture

The platform for modeling and automation of standardized information security management systems is implemented as a centralized web-based system with a service-oriented architecture (SOA), combining the main modules, which in turn use an infrastructure of standardized services to implement processing for specific types of information.

Service-oriented architecture (Service- oriented Architecture) is a model specifically designed to reduce costs, increase flexibility and simplify the presentation of business and operations of different parts of the activity. A basic principle of SOA is the structuring of business activities into services, which allows for their rapid identification and reuse of already existing functionalities, as well as avoiding their duplication during development. Standardization of the behavior of these services leads to limiting the unexpected impacts of changes, as well as to their successful prediction and avoidance. Service-oriented architecture (SOA) is a collection of independent software elements that provide software functionality to other applications as a service.

Main advantages of the SOA approach:

- Independence from supplier, product or technology;
- The service is a self-contained functional unit.

The Services can be combined with other software applications to provide full functionality of a larger software application.

Logical architecture

The platform architecture can be decomposed into separate layers (levels), communicating with each other via strictly defined interfaces. The main advantage of this approach is that it allows significant changes to be made to individual layers without affecting the others, which leads to extreme flexibility. The layers are defined to group elements that vary independently. In centralized platforms, a proven model is the separation of the following layers:

Database layer;

Business logic layer;

User interface layer (presentation layer);

Each layer is subsequently decomposed into separate modules, with communication between the modules being carried out via strictly specified interfaces. The division into clearly defined layers and the separation of the database layer from the business logic layers allows for the overall solution to be compatible with both the existing infrastructure in the organization and with a virtual infrastructure.

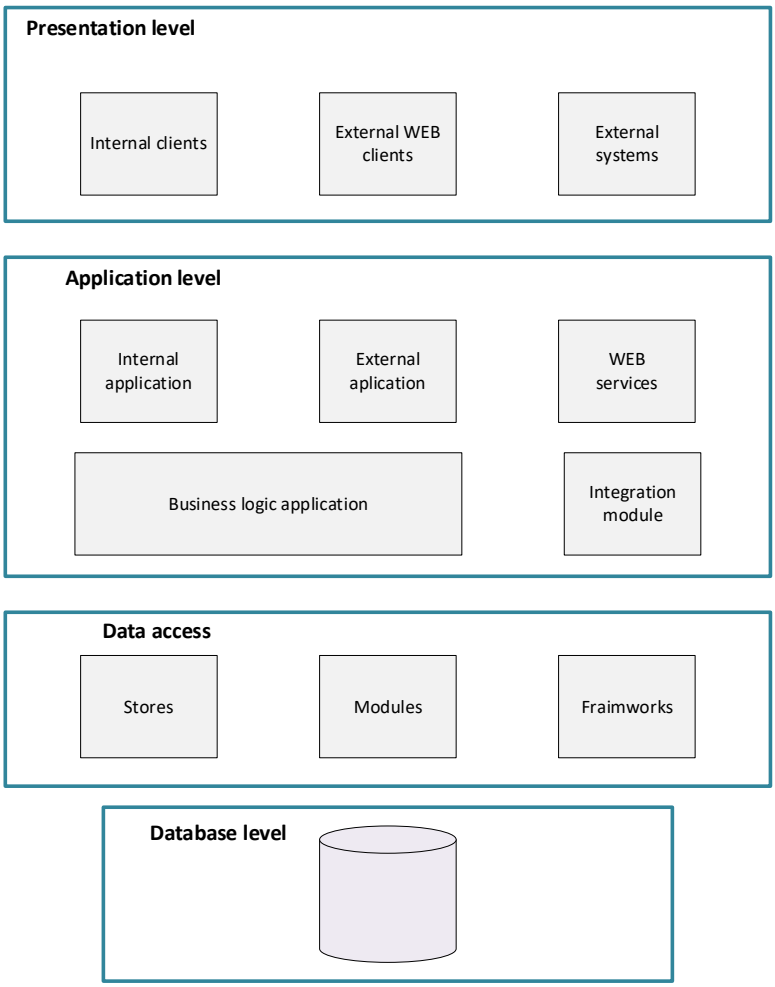


Figure 6 System architecture of the Platform implementation – three-tier MVC architecture

Physical architecture

The platform is based on a flexible architecture that can be deployed in both a physical environment and a virtualized (cloud) environment, or another hybrid solution.

The platform adapts to the organization's existing hardware, network and application environment, and has two main physical components:

- An application server that executes requests to the system's web application through which users work with the system.
- Server for managing the system's databases.

Considerations for maximum separation and ensuring information security predetermine the separation of servers in the so-called DMZ or "demilitarized zone" - an area of the network that is isolated from the rest of the internal network, separated from the external environment by an external firewall, but also by an internal firewall, so that a possible breach does not pose a risk to the server with the system application or the server storing its databases.

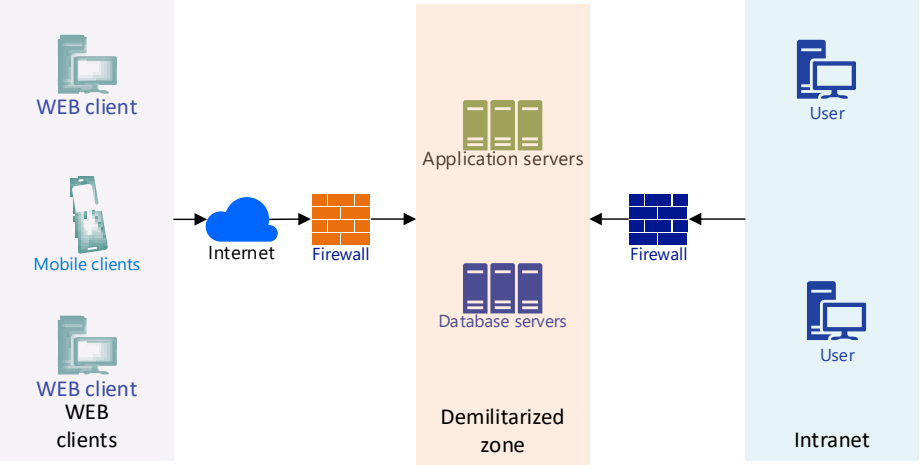


Figure 7 Physical architecture

Main conclusions to Chapter 3

- **The Document Matrix** is introduced as a basis for operational management of the company and the conceptual model of the Platform.
- According to the described modeling methodology and the results of the previous chapters, a model of the Platform for Modeling and Automation of Standardized Information Security Management Systems has been built.
- A logical and physical architecture for the implementation of the platform is proposed.
- The UML code of the model is presented in **Appendix 5 (Plant UML)**
- The implementation of the Platform in modules with Python in OOP style is presented **in Appendix 6.**
- The database implementation is given in **Appendix 7** ORM (Object-Relational Mapping) implementation via (SQL Alchemy standard in Python).

IV. MAIN FINDINGS AND CONCLUSIONS

Scientific contributions

- An algorithm and methodology for research and modeling of an automated standardized information security management platform are proposed;
- The author's theory of **a document matrix is presented** as a basis for operational management of an organization and a company.

Scientific and applied contributions

- An analysis of information security management systems is presented in aspects: Information security; Information security standards; Information security management systems (ISMS); IS software applications.
- Work processes and flows that are subject to automation through the developed platform have been identified, defined and analyzed;
- Functional and non-functional requirements are defined after research and analysis of data, user groups and information security standards;
- The general characteristics of the system are identified, using heuristic methods;
- A model of a complex platform for modeling and automation of standardized information security management systems has been developed. The model is based on monitoring, analysis and management of the document matrix, workflows and information flows and assets of the organization.
- A platform architecture is proposed that is in line with modern requirements for modularity, automation, and standards compatibility.

Directions for future research

The results achieved in the dissertation work outline the following directions for future research:

- Development of the Platform with integration with artificial intelligence that analyzes:
  - Information units and records;
  - System, program and communication logs;
  - The information generated by the control criteria.
- Based on the analyses performed with AI, the platform's functionalities can be further developed in aspects:
  - Offering optimization of the SUS;
  - Display of abnormal parameters and activities outside the norm;
  - Calculating probabilistic events and predicting risk factors.
- Information security management systems can be modeled with neural networks managed by the Platform. This is an approach to increasing the effectiveness and

efficiency of critical information security management systems.

- The generative unsupervised neural network - Boltzmann machine (Boltzmann Machine) uses techniques on input data to analyze the normal states of the IMS to predict undesirable situations. Internationally recognized standards define a set of security controls for monitoring, auditing, and managing the IMS. They are divided into categories, and each of them has standardized attributes. The neural units of the Boltzmann machine are based on the IMS security control infrastructure.
- Integrating neural networks into an ISMS can significantly improve an organization's ability to detect, predict, and respond to security anomalies. NNs are widely used in almost all areas of information and cybersecurity, but for modeling the behavior of an ISMS as a complete complex system, they are an innovative method for reducing costs and time, as well as preventing or mitigating damage.

Approbation of the results

The main results obtained in the development of the dissertation work have been reported in three publications and at specialized international conferences.

Articles and citations

1. Velev T., Dobrinkova N., "Unified innovative Platform for administration and automated management of internationally recognized standards", Book Title: "Digital Transformation, Cyber Security and Resilience of Modern Societies", book series "Studies in Big Data", Springer. DOI:10.1007/978-3-030-65722-2 _5, eBook ISBN: 978-3-030-65722-2, ISBN: 978-3-030-65721-5, (https:// www.scopus.com /pages/publications/85129091048) ISSN: 2197-6503, vol. 84, p. 75
2. Velev T, "Heuristic essentials for modeling and optimization of a platform for automation and management of standardized information security management systems" , 28–29 October 2021, Sofia , Bulgaria , 2021 Big Data, Knowledge and Control Systems, Engineering (BdKCSE) IEEE | DOI: 10.1109/BDKCSE53180.2021.9627263 , ISBN:978-1-6654-1042-7, https:// ieeexplore.ieee.org /document/9627277 ;
3. Velev T., Dobrinkova N., "The logical model of unify, innovative Platform for Automation and Management of Standards (PAMS)" 1st International Scientific Conference Digital Transformation, Cyber Security and Resilience " DIGILIENCE2019, Sofia 2-4 October 2019. ISIJ Digital Transformation, Cyber Security and Resilience, ISSN 0861-5160 (print), ISSN 1314-2119 (online), vol. 43, no. 1 (2019): 113-120, 2019, p.113-p.120 https://doi.org/10.11610/isij.4310
   - Citation 1: Wang, Z., Guan, X., Zeng, Y., Liang, X. and Dong, S., "Utilizing data platform management to implement "5W" analysis framework for preventing and controlling corruption in grassroots government". Heliyon Volume 10, Issue 7, 15 April 2024, e28601, DOI: 10.1016/j.heliyon.2024.e28601, 2024 (Scopus referenced: https: // www.scopus.com/pages/publications/85188751354)

Conferences

- International Conference on Big Data, Knowledge and Control Systems Engineering BdKCSE'2018, (21-22 November 2018), report: "Unified innovative Platform for

administration and automated management of internationally recognized standards"

- DIGILIENCE 2019: Digital Transformation, Cyber Security and Resilience Central Military Club Sofia, Bulgaria, October 2-4, 2019, report: " The logical model of unify, innovative Platform for Automation and Management of Standards (PAMS)"

Projects

Part of the research in the dissertation is from project No. BG161PO003-1.1.06–0036-C0001 "Unified platform for administration, automation and management of internationally recognized standards", implemented in cooperation by the teams of **Perfect Plus EOOD (head Todor Velev) and IICT - BAS (head Svetozar Marg e nov).** The project is for industrial research of a high-tech innovative product in the field of information technologies with a duration of 22 months.

A large part of the results has been tested in the project "Development and implementation of a Unified System for Management, Control and Analysis of Activities (ESUKAD) for the needs of the Bulgarian Institute of Metrology (BIM)", led by Todor Velev.

Acknowledgements

I express my gratitude to my supervisor, Prof. Dr. Nina Dobrinkova, for valuable guidance, professional competence and assistance in the preparation of the dissertation. I am grateful for the help and advice of my colleagues from the Institute of Computer Science and Technology of the Bulgarian Academy of Sciences and from Solent. University of Southampton.

Applications

Appendix 1 Basic terminology in standardization
Appendix 2 Certification (auditing) organizations
Appendix 3 Data Exploration
Appendix 4 Up-to-dateness and change of documents and records management.
Appendix 5 UML model code (Plant UML)
Appendix 6 Platform implementation with Python
Appendix 7 ORM (Object-Relational Mapping) implementation – SQL Alchemy

БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ

АВТОРЕФЕРАТ НА ДИСЕРТАЦИЯ

за присъждане на образователна и научна степен "доктор" по докторска програма „Информатика"

МОДЕЛИРАНЕ И АВТОМАТИЗАЦИЯ НА СТАНДАРТИЗИРАНИ СИСТЕМИ ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА

Тодор Велев Велев

Ръководител: Проф. Нина Добринкова

Научно жури:

Проф. Стефка Фиданова
Проф. Олимпия Роева
Проф. Леонид Кирилов
Проф. Христо Костадинов
Доц. Красимира Иванова

Институт по информационни и комуникационни технологии

Секция „Моделиране и оптимизация"

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИЯТА

Актуалност на проблема

В съвременната информационна действителност, характеризираща се с динамична цифровизация на всички обществени и икономически процеси, информацията се превръща в стратегически актив и в същото време – във все по-уязвим ресурс. Ежедневният обмен на огромни масиви от данни, сложната инфраструктура от взаимосвързани системи и повсеместното използване на облачни технологии и мобилни устройства водят до нарастване на заплахите за сигурността на информацията. Зачестяват кибератаките, инцидентите с неоторизиран достъп и компрометиране на данни, което поставя предизвикателства пред организациите, както в публичния, така и в частния сектор.

Традиционните подходи към сигурността, базирани предимно на ръчни процеси, отделни технически средства или формално изпълнение на минимални изисквания, вече не отговарят на актуалните рискове. На този фон международните стандарти, като ISO/IEC 27001, NIST, FISMA, GDPR и други, изискват системен, интегриран и адаптивен подход към управлението на информационната сигурност. Те предполагат изграждане на системи за управление на сигурността на информацията (СУСИ), които съчетават политики, процедури, технологии, човешки фактор и организационна култура.

Автоматизацията на процесите в СУСИ е нова необходимост, предопределена от сложността и обема на данните и информационните потоци. Дигиталните платформи за управление на СУСИ трябва да осигуряват проследимост, контрол, непрекъсната оценка и подобрение, както и възможност за интеграция с нови нормативни изисквания и бизнес промени. В тази динамична среда информационната сигурност е задача с висок приоритет и нарастващо значение. Системите за управление на информационната сигурност не са адекватни без автоматизирани платформи с елементи на изкуствен интелект, които да овладеят нарастващите по обем и видове информационни потоци и взаимодействия.

Актуалността на настоящия дисертационен труд произтича от ясно идентифицирана необходимост от нов, качествено различен подход към управлението на стандартизирани СУСИ. Този подход трябва да се основава на формализиран, смислово богат модел на областта на сигурността и да използва този модел за постигане на висока степен на автоматизация на процесите. Разработването на интелигентна, интегрирана програмна среда (платформа), базирана на такъв модел, може драстично да повиши резултатността, ефикасността и приспособимостта на управлението на сигурността, като същевременно намали разходите и административната тежест върху организациите.

Обект и предмет на изследването

Обектът на изследване са стандартизираните системи за управление на сигурността на информацията (СУСИ) и възможностите за автоматизация на функционалностите и управлението им.

Предмет на изследване е Модел на програмен продукт комплексна Платформа, която да моделира и автоматизира произволна система за управление на сигурността на информацията, изградена в съответствие с международно признат стандарт или стандарти в тази област.

Цели и задачи

Целта на дисертационната работа е да разработи и апробира модел на платформа, която да управлява и автоматизира стандартизирани системи за управление на сигурността на информацията.

За реализиране на тази цел са формулирани следните задачи:

- Изследване и анализ на теоретичните основи на стандартизирани системи за управление на сигурността на информацията в аспекти:
  - Сигурност на информацията;
  - Стандарти за информационна сигурност;
  - Системи за управление на сигурността на информацията СУСИ;
  - Софтуерните приложения за ИС.
- Анализ на процесите, изискванията и характеристиките на платформата за управление и автоматизация на стандартизирани системи за управление на сигурността на информацията. Задачата е разделена в съответствие с посочената методика на следните подзадачи:
  - Изследване и анализ на работни процеси, подлежащи на автоматизация и съответстващите им информационните потоци;
  - Определяне на функционалните и нефункционалните изисквания на платформата, чрез изследване и анализ на данните, на потребителските групи и на стандартите за информационна сигурност;
  - Идентифициране на общите характеристики на системата.
- Проектиране на оптимален модел на платформа за моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията и прилежащата му архитектура.

Методи

За постигането на поставените цели и задачи в дисертационния труд е използвана комбинация от научноизследователски методи, осигуряващи както теоретична задълбоченост, така и практическа приложимост на резултатите.

- **Системен анализ**

Този метод е приложен за разглеждане на СУСИ като комплексна, динамична система от взаимосвързани компоненти, процеси и дейности. Чрез системния анализ са идентифицирани основните елементи на СУСИ, техните зависимости, входни и изходни параметри, както и взаимодействието им с външната среда на организацията. Системният подход позволи структурирането на проблема, декомпозирането му на по-малки, управляеми части и интегрирането им в единен модел на платформа.

- **Сравнителен анализ**

Извършен е задълбочен сравнителен анализ на различни международни стандарти (ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework), регулаторни изисквания (GDPR, NIS2), методологии за управление на риска (ISO 31000) и съществуващи софтуерни решения за СУСИ. Този анализ позволи идентифицирането на добри практики, общи елементи и пропуски в текущите подходи, което послужи като основа за формулиране на изискванията към новата платформа.

- **Моделиране**

Методът на моделирането е централен за дисертацията. Използвани са следните техники:

  - Концептуално моделиране - за дефиниране на високо ниво на компонентите и логическата структура на предложената платформа;
  - Архитектурно моделиране - за проектиране на софтуерната архитектура, включително избор на слоеве, модули и технологичен стек;
  - Моделиране на бизнес процеси (BPMN - Business Process Model and Notation) - използван е за детайлно описание на ключови процеси в СУСИ (напр. оценка на риска, управление на инциденти, одит) с цел тяхната стандартизация и подготовка за автоматизация;
  - Моделиране на данни (ERD - Entity-Relationship Diagram) - приложен е за структуриране на информацията, дефиниране на обекти, техните атрибути и взаимовръзки, необходими за базата данни на платформата.

- **Анализ на данни**

Използван за събиране, систематизиране, обработка и интерпретиране на информация, свързана със статистически данни за киберзаплахи, ефективност на съществуващи мерки за сигурност, както и данни, генерирани по време на тестове на прототипа.

- **Литературен обзор**

Извършен е задълбочен и систематичен преглед на научна и професионална литература – книги, научни статии, конференции, доклади, стандарти и добри практики в областите на информационната сигурност, системите за управление, моделирането на процеси, софтуерното инженерство и автоматизацията.

- **Метод на експертните оценки**

При дефинирането на изискванията и валидацията на модела и прототипа, индиректно са взети предвид експертни мнения и препоръки от специалисти в областта на информационната сигурност и одита.

Комбинацията от тези методи осигурява всеобхватен подход към проблема, съчетавайки теоретичното познание с практическото приложение и валидация на предложените решения.

II. ОБЕМ И СТРУКТУРА

Дисертационният труд е систематично организиран в увод, три основни глави, основни изводи и заключения, приложения, и изчерпателен списък с използвана литература. Общият обем на дисертацията без приложенията е 124 страници, което включва богато илюстративно съдържание от 29 фигури (диаграми, схеми, екранни изгледи) и 34 таблици, представящи данни и класификации. Списъкът с използваната литература съдържа 80 източника, демонстриращи широтата и задълбочеността на извършения литературен обзор.

III. СЪДЪРЖАНИЕ НА ДИСЕРТАЦИЯТА

Увод

В увода е изяснена актуалността на проблема и са представени методическите параметри на дисертационния труд, структурата, обектът, предметът, целите и задачите.

ГЛАВА 1 Стандартизирани системи за управление на сигурността на информацията

Първа глава на дисертационния труд има за цел да положи теоретичните основи на изследването. Тя извършва подробен преглед и анализ на съществуващите подходи, стандарти и технологии в областта на управлението на сигурността на информацията. Главата е структурирана така, че да изведе систематично проблемите и пропуските, които настоящата работа цели да разреши.

Направен е теоретичен анализ на фундаменталните постаменти върху които се изгражда модела на Платформата за управление и автоматизация на стандартизирани системи за управление на сигурността на информацията, а именно: Сигурност на информацията; Стандарти за информационна сигурност; Системи за управление на сигурността на информацията СУСИ; и Софтуерни приложения за ИС.

В главата са дефинирани терминологията и аспектите на информационната сигурност, методите, технологиите и инструментите за защита на информацията и предизвикателствата, провокиращи изследването. Обсъжда се еволюцията на информационната сигурност от чисто технически аспект до всеобхватен управленски процес. Представя се необходимостта от систематичен подход за управление на сигурността в организациите, който да излезе извън рамките на конкретните мерки и да осигури дългосрочна устойчивост. Анализирани са стандартите за информационна

сигурност, както и терминологията, същността и целите на стандартизацията. Разглежда се историческото развитие на стандартите за информационна сигурност, като се започне от ранни инициативи до формирането на международни рамки. Обсъждат се ползите от внедряването на стандартизирани СУСИ, включително подобряване на управленските процеси, намаляване на риска, повишаване на доверието на клиенти и партньори, и спазване на регулаторни изисквания

Изследвани са основните елементи, архитектурата и процесите по разработка и внедряване на СУСИ. Тази секция прави детайлен преглед като се описват ключовите елементи на СУСИ съгласно стандарта, включително:

- Контекст на организацията - разбиране на вътрешни и външни проблеми, заинтересовани страни и обхват на СУСИ;
- Лидерство - ангажираност на висшето ръководство, политики и разпределение на роли и отговорности;
- Планиране - адресиране на рискове и възможности, цели за сигурност и планове за постигането им;
- Поддръжка - ресурси, компетентност, осведоменост, комуникация и документирана информация;
- Оперативна дейност - оперативно планиране и контрол, оценка на риска за информационната сигурност, обработка на риска за информационната сигурност;
- Оценка на изпълнението - мониторинг, измерване, анализ, оценка, вътрешен одит и преглед от ръководството;
- Подобрение - несъответствия и коригиращи действия, и непрекъснато подобрение. Специално внимание се обръща на Приложение А на ISO/IEC 27001, което съдържа списък с контроли за сигурност, категоризирани по домейни.

Въпреки значителните ползи, внедряването и поддържането на СУСИ е свързано с редица предизвикателства. Анализират се трудностите, които често водят до забавяне, повишени разходи или неуспешно сертифициране. Обсъждат се:

- Липса на ресурси - недостатъчен персонал, бюджет и време;
- Сложност на процесите - голям брой документи, процедури и контролни точки;
- Съпротивление на промяна - трудности при промяна на културата и работните навици в организацията;
- Управление на документацията - обемна и динамична документация, която изисква постоянно актуализиране;
- Одит и съответствие - сложни процеси за вътрешен и външен одит, изискващи изчерпателни доказателства за съответствие;
- Непрекъснато подобрение - поддържане на СУСИ в постоянно съответствие с променящите се заплахи и бизнес нужди.

Тези предизвикателства служат като основа за аргументиране на необходимостта от автоматизация и моделиране, които да адресират тези проблеми.

В първа глава се анализира също и пазара на софтуерни инструменти за подпомагане на СУСИ. Проучени са функционалностите на водещи продукти и са идентифицирани следните общи недостатъци:

- Ориентация към пасивна документация - повечето системи са "електронни хранилища" за съхранение на политики, процедури и записи. Те подпомагат одита, но не и активното, динамично управление.
- Липса на смислово разбиране - данните се съхраняват в релационни бази данни, които не управляват сложните семантични връзки между активи, заплахи, контроли и бизнес процеси. Това ограничава възможностите за автоматизирани анализи и изводи.
- Слаба автоматизация на процесите - процеси като оценката на риска често се свеждат до попълване на електронни таблици, които след това се качват в системата. Липсва истинска автоматизация, базирана на логически правила.
- Ниска гъвкавост и разширяемост - системите обикновено са изградени около един конкретен стандарт и трудно се адаптират към други рамки или специфични за организацията изисквания.

Основни изводи към Глава 1

- ☞ Въз основа на направения анализ на сигурността на информацията, стандартите за информационна сигурност и системите за управление на сигурността на информацията се налага извода, че е необходим комплексен подход за справяне с описаните прогресиращи предизвикателства.
- ☞ От изследването на видовете и функционалния обхват на софтуерните приложения, свързани със СУСИ се идентифицира сегментацията на продуктите. Системите за цялостно управление на СУСИ са предимно в аспекти сертификация, ре сертификация и поддържане на необходимите записи и шаблони за целите на одитния процес. Липсват цялостни решения които да управляват и контролират всички работни процеси и информационни потоци в инфраструктурата и суперструктурата на организацията. Платформения подход за изграждане на адаптивна система, моделираща и автоматизираща стандартизирани системи за управление на сигурността на информацията е иновативно, генерализирано решение на третираната проблематика.
- ☞ С цел да се гарантира ефективност, полезност и надеждност на платформата е необходимо да се разработи модел, който се базира на цялостен мониторинг, анализ и управление на документната матрица, работните процеси и информационните потоци и активи на организацията.

ГЛАВА 2. Моделиране на платформа за управление и автоматизация на стандартизирани системи за управление на сигурността на информацията.

Във Втора глава е представена методология за изследване и моделиране на автоматизирана стандартизирана платформа за управление на сигурността на информацията и съобразно нея е извършен анализ на процесите, определяне на изискванията и идентифициране на общите характеристики на системата.

Изследването и анализа, съобразно предложената методология включва следните ключови стъпки:

- **Анализ на процесите**

Изследване и анализиране на стандартизираните работни процеси, които системата да автоматизира и кореспондиращите с тях информационните потоци.

Идентифицирани и описани са следните стандартизирани работни процеси:

- Изпълнение на бизнес процеси ИБП/Документооборот ;
- Процеси по администрация на платформата;
- Дефиниране и управление на бизнес процеси;
- Управление на СУСИ;
- Мониторинг и контрол;
- Одит.

- **Определяне на изискванията**

За определяне на функционалните и нефункционалните изисквания се извърши:

- Изследване и анализ на потребителските групи;

Потребителите на платформа за управление и автоматизация на стандартизирани системи за управление на сигурността на информацията са обособени в 2 големи групи:

- Ползватели - компании и организации внедрили Система за управление на информационната сигурност, сертифицирана по международно признат стандарт. Това са ползватели от всички сектори на икономиката, изпълняващи дейност във всички раздели на класификатора на икономическите дейности, включително държавни и общински организации.
- Сертификационни и консултантски организации - извършват одити при сертифицирането на СУСИ и контролни одити за потвърждаване на съответствието.

- Изследване и анализ на стандартите за информационна сигурност;

Изследването на изискванията на стандартите се извърши съобразно техните основни групи характеристики:

- Съдържание на стандарта - име, цел, политики, обхват, изисквания, условия, определения, вид и област на приложимост.
- Инфраструктура - процедури, процеси, документи, контроли, регистри, срокове, инструменти и функционални алгоритми.
- Суперструктура (външна среда) - кореспонденти, клиенти, доставчици, партньори и институции, свързани стандарти, възможни възможности за интеграция, одити, и т.н.
- Ресурси - организационна структура и персонал, активи, инструменти и материали, необходими за планиране, поддържане и контрол на стандартните механизми.

  - Изследване и анализ на данните.

Платформа за управление и автоматизация на стандартизирани системи за управление на сигурността на информацията СУСИ, оперира с две основни групи данни, като следва:

- Данни свързани със стандартите за информационна сигурност;
- Данни свързани с функционалните изисквания за Платформата;

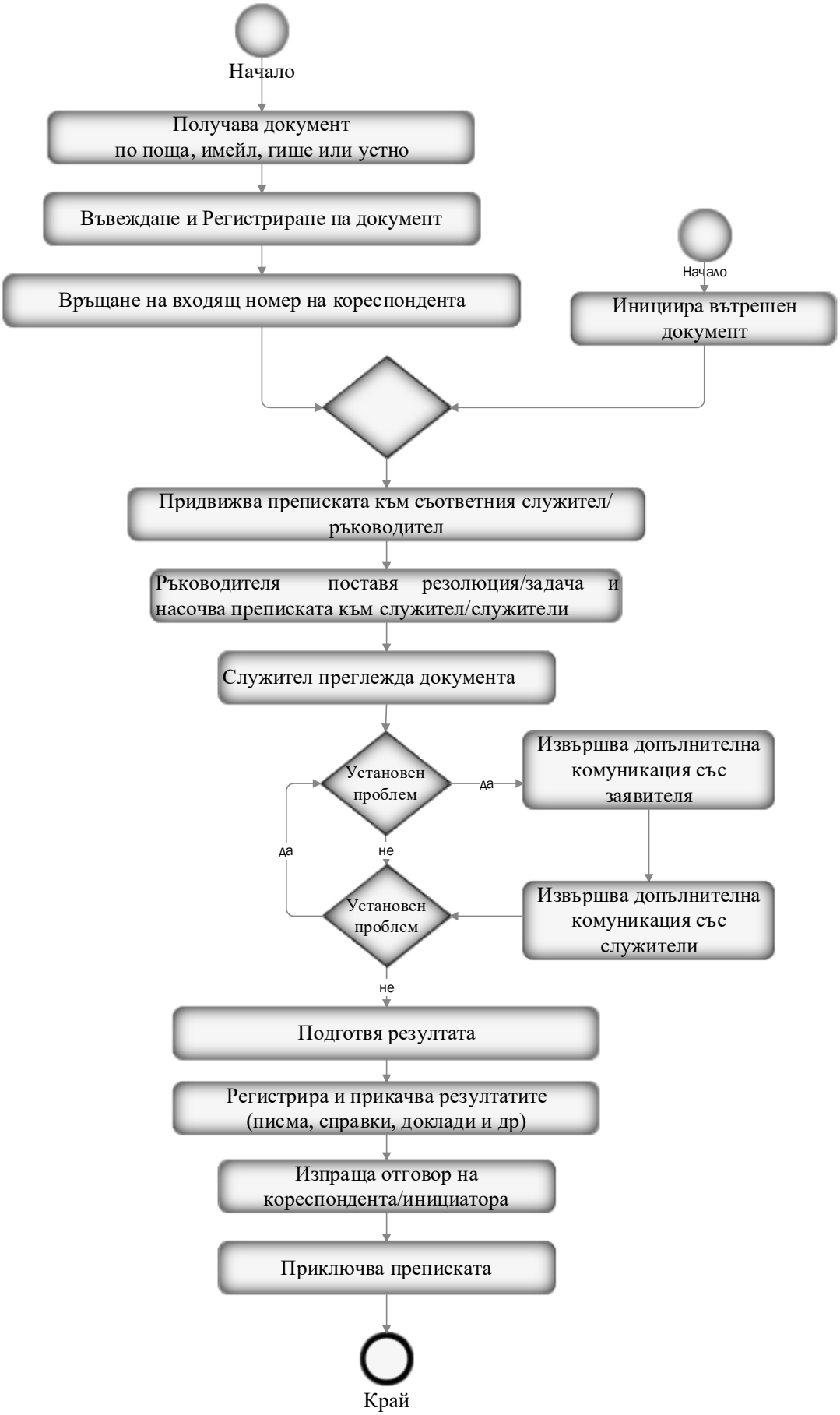
Резултата е показан в Приложение 3.

- **Определяне на общите характеристики на платформата**

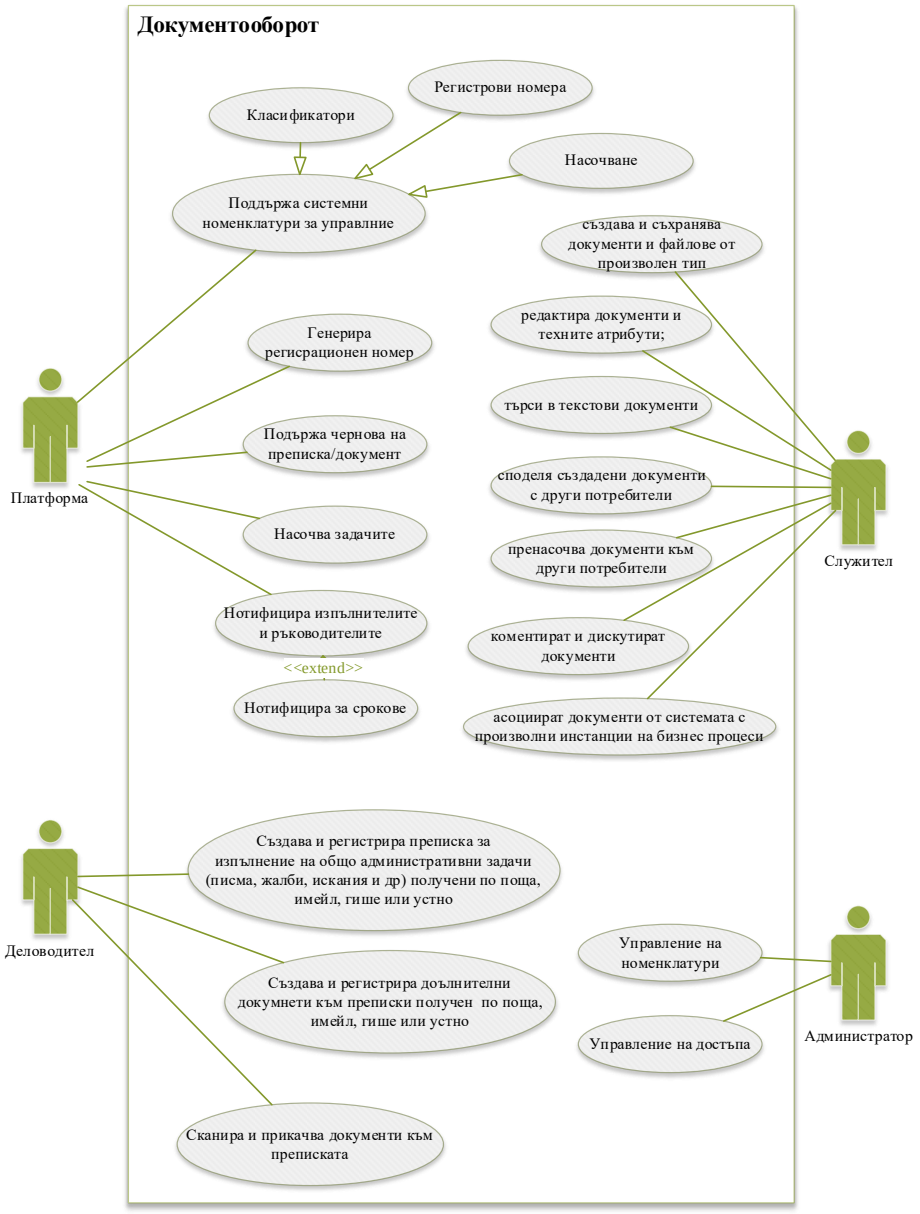
Общите характеристики на платформата са определени чрез изследване на добрите практики за потребителско поведение, продуктивност, сигурност и администрация на информационните системи. Поради спецификата на поставените цели и изучаваната материя за тази задача са използвани евристични техники като:

- Подход най-добри практики;
- Проучване и анализ на академични източници;
- Техника SCAMPER;
- Методът Делфи

За описание на процесите и изискванията е използван е унифицираният език за моделиране – UML™ и Business Process Model and Notation (BPMN) стандарта за визуално моделиране на бизнес процеси под формата на диаграми като показаните по-долу.



Фигура 1 Процес Документооборот



Фигура 2 Документооборот диаграма на потребителските случаи

Основни резултати от Глава 2

- Извършен е анализ на стандартизираните работни процеси, които да бъдат включени в модела на Платформата, подлежащи на автоматизация и съответните, кореспондиращите с тях информационните потоци.
- Въз основа на анализ на данните, на потребителските групи и на стандартите за информационна сигурност са определени функционалните и нефункционалните изисквания, които трябва да бъдат отразени при моделирането на Платформата.
- Изследвани са добрите практики за потребителско поведение, продуктивност, сигурност и администрация на информационните системи и са идентифицирани общите характеристики на Платформата.

ГЛАВА 3. Модел на платформа за моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията.

В трета глава е представена авторската теория за документна матрица, като основа за оперативно управление на организация и компанията. Описаната е методиката за моделиране и концептуалният модел на Платформата. Изработен е оптимизиран модел на предмета на дисертацията, изграден съобразно теоретичните постаменти и направените изследвания и анализи, представени в Глава 1 и Глава 2. Предложена е логическа и физическа архитектура за реализация на платформата.

Документна матрица

Всяка компания независимо от мащаба си изпълнява своята дейност във вътрешна и външна работна среда. Вътрешната среда се определя от ресурсите на компанията (човешки, материални и нематериални) и от работните процеси в нея, свързани с предмета на дейност. Външната среда са клиентите, доставчиците, партньорите и държавните институции с които компанията работи.

Системите за управление на сигурността на информацията по международно признатите стандарти дефинират, регламентират, управляват, наблюдават, регистрират и архивират вътрешната и външната среда на функциониране, чрез системата от документи на организацията и кореспондиращите масиви от данни.

Документа е запис, чрез който се отразява в неговото развитие всяко действие, норма, събитие, ресурс, отношение, процес и интелектуално производство. Освен че в днешно време документите са електронни и хартиени те могат условно да се класифицират в няколко формални групи - Конвенционални записи и Специализирани документи

Количеството от всички тези записи, наречени документи, дефинират и определят компанията, нейната история, капацитет, качество и конкурентно способност.

Документите сами по себе си не са независими отделни единици. Те са свързани в специфична за всяка фирма **документна мрежа**. Всеки документ е краен продукт, зад който стои процес от различна сложност и обхват. Всеки документен процес се състои от дейности и етапи и както във всяко производство се нуждае от ресурси и материали. Ресурсите и материалите от своя страна са най-често масиви от данни и други документи, които имат своите процеси и своя жизнен цикъл. Множеството документи и връзките между тях образуват документната мрежа на организацията. За разлика от Интернет мрежата обаче документната мрежа на една компания има дефинирани пътища, връзки и форми (формуляри) и е свързана и индексира и управлява масивите (базите) от данни на организацията.

По тази причина системата от фирмени документи се разглежда не като документната мрежа, **а като документна матрица** на компанията.

Документната матрица засяга всеки елемент от вътрешната и външна работна среда на фирмата и е съвсем логично тя да дава възможност за максимален контрол върху организацията. Фирмената документна матрица е в основата на управлението на всяка система за управление, изградена по международно признати стандарти. Те са базирани на политики, работни процеси, процедури и множество форми и записи за контрола им.

Когато документите се цифровизират, връзките между тях се визуализират и матрицата се облече в подходяща функционалност, то се получава изключително ефективна система за мониторинг, контрол и управление на всички нива и ресурси в компанията.

Концепция на платформата

Платформата за моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията е съвременна, иновативна, интегрирана информационно-оперативна система, която моделира, дигитализира, регистрира, управлява, съхранява и контролира работните процеси и свързаната с тях информация и документация в съответствие с различни международно признати стандарти за информационна сигурност.

Модела се базира на мониторинг, анализ и управление на документната матрица, работните процеси и на информационните потоци и активи на организацията. Платформата обхваща всички информационни единици - документи (хартиени и електронни), аудио и видео комуникации, системни, програмни и комуникационни логове и др.. Мониторира входящите, изходящите и вътрешните информационни потоци и ги управлява, съобразно моделираните в нея работни процеси и стандартизирани форми.

Работните процеси и стандартизираните форми са моделирани, съобразно политиките, процедурите и шаблоните на системите за управление на сигурността на информацията (СУСИ). Всички записи, свързани не само с елементите на СУСИ, а и с оперативните процеси се формализират във платформата и се извършват само чрез нея. Целта е да се използват най-новите технологични постижения, за да се цифровизира, индексира и съживи документната матрица на организацията и да позволи оперативна ефективност на управление на сигурността.

Информационните активи се въвеждат в Платформата като параметризирани обекти. Всеки контрол от системата от контроли на стандартите за информационна сигурност, съобразно които е изградена СУСИ се асоциират с един или няколко предварително дефинирани критерия на платформата. Всеки критерий е формализиран запис с определени параметри на регистрираната информация и честота и начин на проверка. За всеки критерий се дефинират тригери на действие на платформата, съобразно възможни стойности или събития.

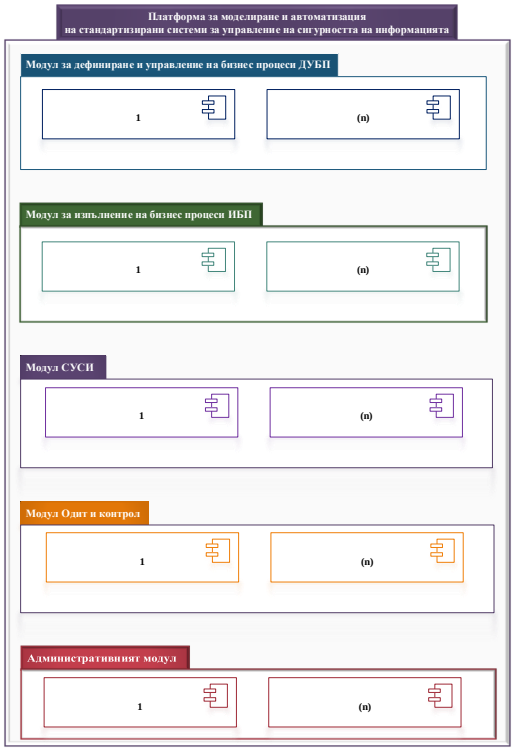
Контролите се прилагат към актив и/или процес в съответствие със СУСИ.

Мисията на платформата е да интегрира всички документи потоци, свързани с работните процеси в клиентската организация. Да свърже множеството приложни софтуерни продукти, работещи в сферата на информационната сигурност и масивите от данни в една единна информационно-комуникационна и управленска система. Платформата обединява информационните сечения и информационните потоци в единно информационно пространство и осигурява интегрирана среда за съхранение, управление и обмен. Това позволява да се следи ефективно движението на информацията, структурирана в отделни типове документни единици, да се моделира СУСИ и да се осъществява надежден контрол.

Платформата моделира йерархичната структура на организацията, с възможност за изменения, като позволява адекватно разпределение на задачите съобразно субординацията на компанията. Системата управлява движението на разнообразни типове документи, като автоматизира всички фази на работните потоци.

Съгласно извършените изследвания и анализи, представени в Глава 2 Платформата за моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията се реализира със следните компоненти (модули):

- Модул за дефиниране и управление на бизнес процеси ДУБП;
- Модул за изпълнение на бизнес процеси ИБП;
- Модул СУСИ;
- Модул Одит и контрол;
- Административният модул;



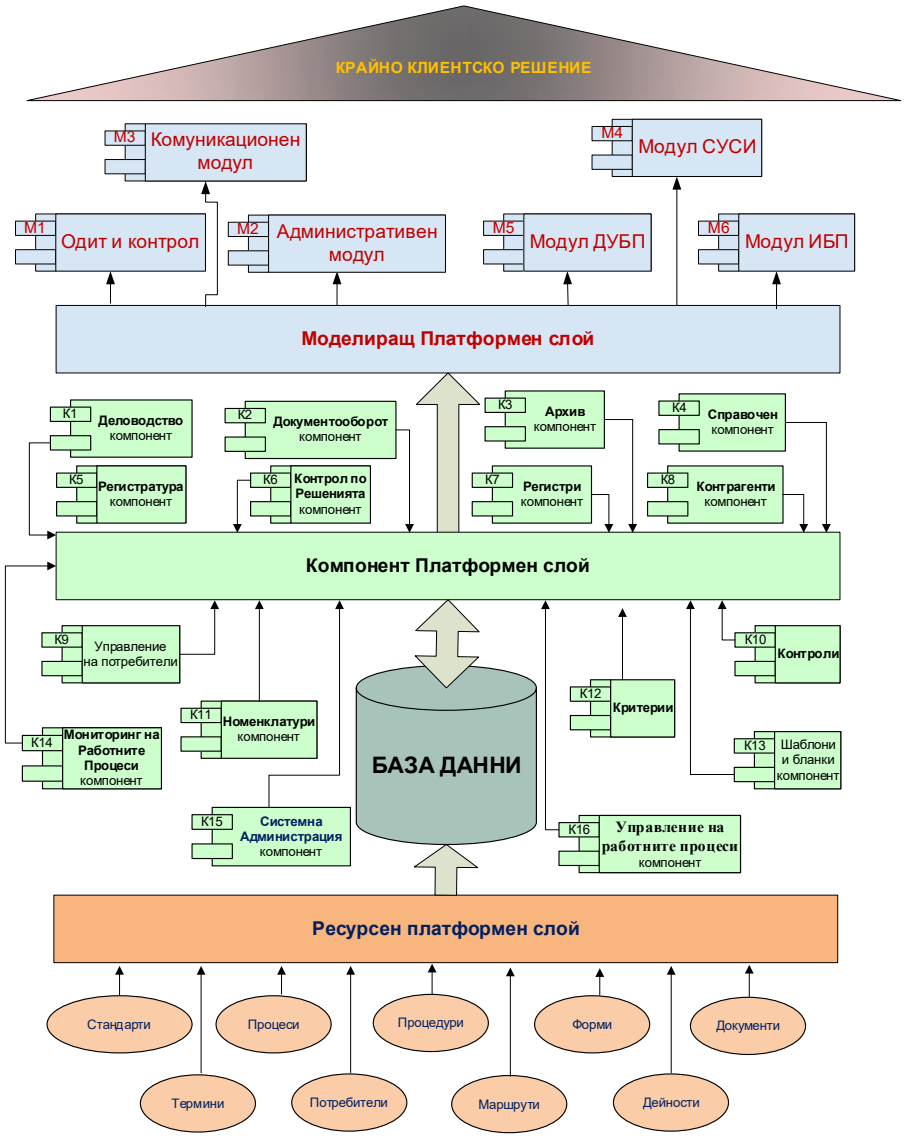
Фигура 3 Структура на Платформата

Платформата използва единна база от данни в която чрез различни интерфейси се въвежда и извежда необходимата информация, съобразно информационните класове. Базовите масиви се управляват чрез изграждане на специализирана логика за всеки от тях – стандарти, термини, процеси, потребители, процедури, маршрути, форми, контролирани процеси, и различни неструктурирани данни.

Платформения слой, така наречения мидълуер, реализира логиката и обмена на информация между интерфейсите за въвеждане на информация и базата от данни. Друг платформен слой, реализира връзката на функционалните модули и базата от данни. Функционалните модули (компоненти) изпълняват определена група от функции, чрез предоставяне на интерфейси за осъществяване на необходимите задачи. Платформата изгражда модулите си в контекста на всяка клиентска организация, като набор от компоненти (функционални модули) както е показано на фигурата.

Системата притежава регистрационно-контролна част, в която се въвеждат индекси на организацията и се регистрират в съответствие с тях всички входящо-изходящи и вътрешно оперативни документи (събития). Автоматично се генерират номера на документите съгласно предварително заложен стереотип. Към всеки регистриран документ могат да се задават срокове за изпълнение, които тя контролира. Платформата функционира и като комуникатор, като информира по различни начини (е-мейл, SMS, звуково и визуално) за различни контролирани събития, просрочени срокове и задачи за изпълнение. Електронната система моделира създадените в компанията по съответния стандарт оперативни процедури и процесни карти, като осигурява информационно коректното спазване на всички работни процеси, попълване на съответните формуляри и бланки, мониторинг на работните процеси и контрол на решенията. Тя гарантира възможно най-високи нива на сигурност, надеждност и защита на информацията. Осигурява възможност всеки потребител да се идентифицира не само с потребителско име и парола, а и с частен електронен подпис. Всеки служител/потребител има предварително дефинирани профили, роли, права на достъп и функционалност, съответстваща на длъжностната му характеристика. Системата генерира динамично персонални екрани при влизането на потребителя, като му предоставя интуитивен потребителски интерфейс и навигация.

Модулите на Платформата изграждат моделите, свързани с управление на различи типове международно признати стандарти с богат инструментариум: **типизирани процеси**; **предварително разработени сценарии и постановки**; набор от предварително дефинирани форми; разработени конвенционални регистри; специализирани регистри; вътрешна комуникационна среда; системи за оценка, контрол и подпомагане на одита; и други.



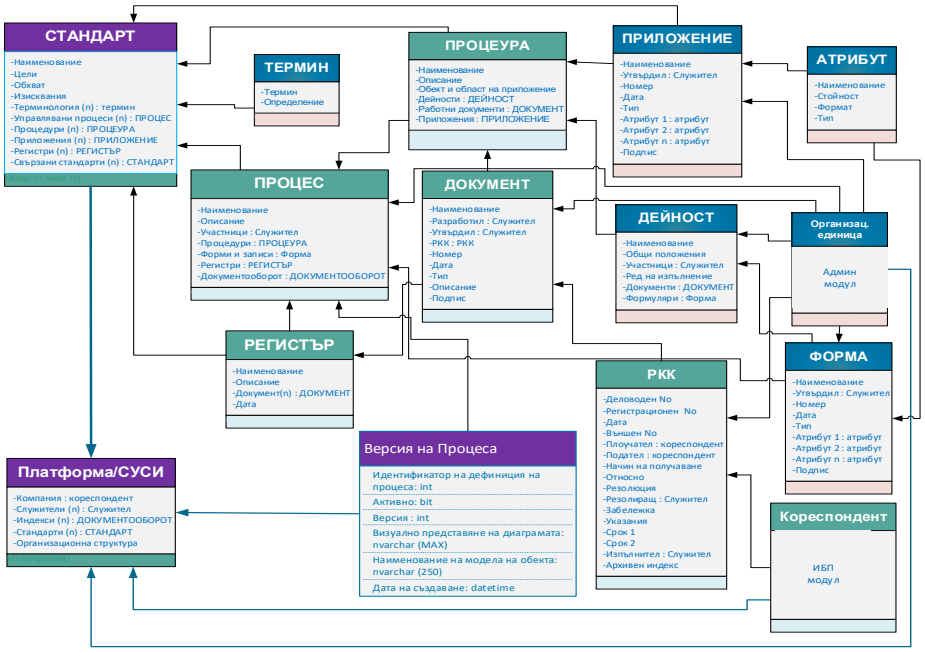
Фигура 4 Концептуална архитектура на модела

Методика за моделиране

Въз основа на функционални и нефункционални изисквания, бизнес процесите и спецификацията на потребителски случаи, дефинирани в предходната глава след направеното изследване и анализ, се разработи оптимален набор от информационни определители, разпределени в логически информационни класове и подкласове.

Наборът от дескриптори, генериран от извършените изследвания и анализи е декомпозиран на логически информационни класове, в съответствие с тяхната функционална ориентация в описанието на стандартите. Информационните класове се разглеждат като програмни обекти и подобекти. Те се описват чрез своите атрибути, които се наричат информационни идентификатори. Тяхното представяне е унифицирано чрез използване на специфичен технически формат, който определя формата на представяне на стойностите на всеки атрибут на информационните обекти. Техническият формат на информационните класове и техните атрибути се описва от синтаксиса на унифициран език за моделиране (UML).

За дизайна на платформата се използват UML клас диаграми. които изобразяват структурата на системата чрез моделиране на нейните класове, свойства, операции и връзки между обекти. Клас диаграмата е визуална нотация, използвана за изграждане и визуализиране на обектно-ориентирани системи. Тя е статична структурна диаграма, демонстрираща свойствата на платформата, класовете, операциите и връзките между обекти за описание и дизайн на системата. Диаграмите на класове са форма на структурни диаграми, тъй като те определят какво трябва да бъде включено в моделираната система. Информационните идентификатори са моделирани в 3 нива информационни класове структурирани в модули на платформата. За пример прилагам модел на един основен модул СУСИ.



Фигура 5 Модул СУСИ

Идентификаторите за всеки клас са описани подробно в табличен вид.

Таблица 1 Организационна единица (Структура)

Описание		
Тип	**Наименование/ Формат**	**Описание**
Клас	Организационна единица: () Структура	Организационна единица (Структура) е базов клас на Административния модул, отнасящ се към описване на структурата на организацията и кореспондиращото и моделиране в Платформата.
Атрибут	Наименование: Nvarchar (400)	Наименование на организационната структурна единица.
Атрибут	Тип: Тип	Типът на структурата е предефинирана номенклатура – дирекция, отдел, сектор и длъжност.

клас	Родителска Организационна единица: Структура	Наименование на родителската организационна единица към която принадлежи структурата. (ако има такава)
Подклас	Права (n): Право	Списък от права върху информационните обекти които има организационната единица и всички нейни подструктури. Определят се набор от права за всеки информационен обект от класификатора – Пример: за информационен обект „Регистър на инцидентите“ право на четене, право на регистриране и право на редакция.
Подклас	Шаблони: Шаблон	Шаблоните са набор от права които могат да се прилагат към всеки информационен обект и да се добавят за структурно звено в комплект.
Подклас	Потребители: Потребител (n)	Списък от служители на организацията които са добавени към организационната структура.

Системна архитектура

Платформата за моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията се реализира като централизирана уеб базирана система с архитектура ориентирана към услугите (SOA), комбинираща в себе си основните модули, които от своя страна използват инфраструктура от стандартизирани услуги за реализация на обработката за конкретните типове информация.

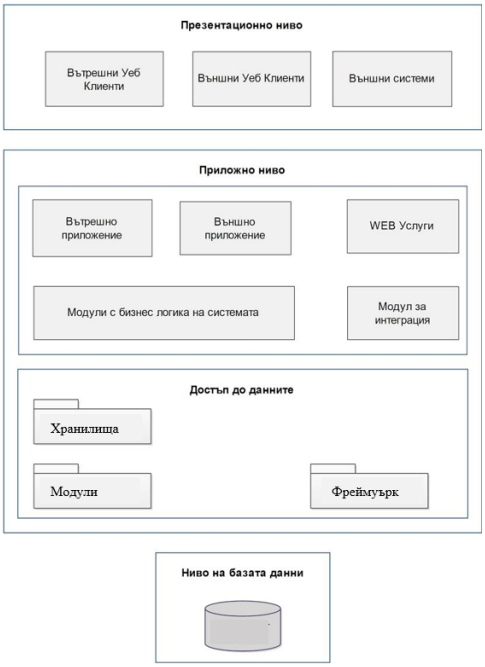
Ориентираната към услуги архитектура (Service-oriented Architecture) е модел, специално предназначен да намали разходите, да увеличи гъвкавостта и да опрости представянето на бизнеса и операциите на различни части от дейността. Основен принцип на SOA е структурирането на бизнес дейностите в услуги, което дава възможност за тяхното бързо идентифициране и преизползване на вече съществуващите функционалности, както и избягване на дублирането им по време на разработка. Стандартизацията на поведението на тези услуги води до ограничаване на неочакваните въздействия при промени, както и до успешното им прогнозиране и избягване. Архитектура ориентирана към услугите (SOA) е съвкупност от независими софтуерни елементи, предоставящи като услуга софтуерна функционалност на други приложения.

Основни предимства на SOA подхода:

- Независимост от доставчик, продукт или технология;
- Услугата е самостоятелна функционална единица.

Услугите могат да бъдат комбинирани с други софтуерни приложения, за да се осигури пълна функционалност на по-голямо софтуерно приложение.

Логическа архитектура



Фигура 6 Системна архитектура на реализацията на Платформата – трислойна архитектура MVC

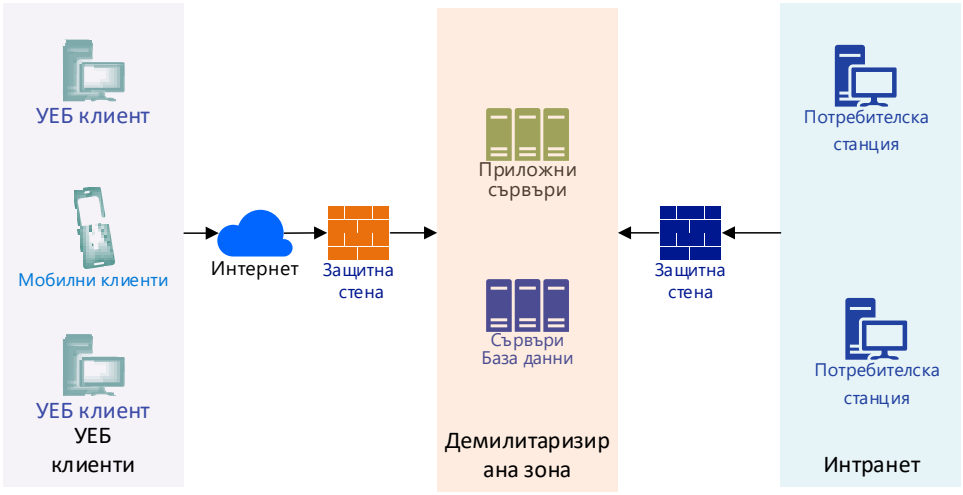
Архитектура на платформата може да бъде декомпозирана на отделни слоеве (нива), комуникиращи помежду си по строго определени интерфейси. Основно предимство при този подход е, че позволява в отделните слоеве да бъдат извършвани значителни промени без това да оказва влияние на останалите, което води до изключителна гъвкавост. Слоевете са определени така, че да групират елементите, които варират независимо. При централизираните платформи доказан модел е разделянето на следните слоеве:

- Слой на базата данни;
- Слой на бизнес логиката;
- Слой на потребителския интерфейс (презентационен слой);

Всеки слой в последствие се декомпозира на отделни модули, като комуникацията между модулите се осъществява по строго специфицирани интерфейси. Разделението на ясно разграничени слоеве и обособяването на слоя на базата данни от слоевете на бизнес логиката позволява да се осигури възможността цялостното решение да бъде съвместимо както със съществуващата инфраструктура в организацията, така и с виртуална инфраструктура.

Физическа архитектура

Платформата се базира на гъвкава архитектура, която ще може да се разгръща както в физическа среда, така и във виртуализирана (облачна) среда, или друго хибридно решение.



Фигура 7 Физическа архитектура

Платформата се адаптира към съществуващата хардуерна, мрежова и приложна среда в организацията, като има два основни физически компонента:

- Приложен сървър, изпълняващ заявките към уеб приложението на системата, чрез който потребителите работят със системата.
- Сървър за управление на базите данни на системата.

Съображенията за максимално добро обособяване и осигуряване на информационна сигурност предопределят отделяне на сървърите в т. нар. DMZ или „демилитаризирана зона“ – зона от мрежата, която е изолирана от останалите части на вътрешната мрежа, отделена от външната среда с външна защитна стена, но и с вътрешна защитна стена, така че евентуален пробив да не доведе до риск за сървъра с приложението на системата или сървъра съхраняващ неговите бази данни.

Основни изводи към Глава 3

- Въвежда се авторската теория за **Документна матрица**, като основа за оперативно управление на компанията и концептуалния модел на Платформата.
- Съобразно описаната методика за моделиране и резултатите от предходните глави е изграден модел на Платформата за моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията.
- Предложена е логическа и физическа архитектура за реализация на платформата.
- UML кода на модела е представен в **Приложение 5 (Plant UML)**
- Реализацията на Платформата по модули с Python в ООП стил е представено **в Приложение 6.**
- Реализацията на базата данни е дадена в **Приложение 7** ORM (Object-Relational Mapping) реализация чрез (SQL Alchemy стандарт в Python).

IV. ОСНОВНИ ИЗВОДИ И ЗАКЛЮЧЕНИЯ

Научни приноси

- Предложени са алгоритъм и методология за изследване и моделиране на автоматизирана стандартизирана платформа за управление на сигурността на информацията;
- Представена е авторската теория за **документна матрица**, като основа за оперативно управление на организация и компания.

Научно-приложни приноси

- Представен е анализ на системите за управление на сигурността на информацията в аспекти: Сигурността на информацията; Стандартите за информационна сигурност; Системите за управление на сигурността на информацията СУСИ; Софтуерните приложения за ИС.
- Определени, дефинирани и анализирани са работни процеси и потоци, които подлежат на автоматизация чрез разработваната платформа;
- Дефинирани са функционалните и нефункционалните изисквания след извършено изследване и анализ на данните, на потребителските групи и на стандартите за информационна сигурност;
- Идентифицирани са общите характеристики на системата, с използването на евристични методи;
- Разработен е модел на комплексна платформа за **моделиране и автоматизация на стандартизирани системи за управление на сигурността на информацията.** Модела се базира на мониторинг, анализ и управление на документната матрица, работните процеси и информационните потоци и активи на организацията.
- Предложена е архитектура на платформата, която е в съответствие със съвременните изисквания за модулност, автоматизация и съвместимост със стандарти.

Насоки за бъдещи изследвания

Постигнатите резултати в дисертационната работа очертават следните насоки за бъдещи изследвания:

- Развитие на Платформата с интеграция с изкуствен интелект, който анализира:
  - Информационните единици и записи;
  - Системните, програмни и комуникационни логове;
  - Информацията генерирана от критериите по контролите.
- Въз основа на извършените анализи с АИ могат да се доразвият функционалностите на платформата в аспекти:
  - Предлагане на оптимизация на СУСИ;
  - Показване на аномалии параметри и активности извън норма;

- Изчисляване на вероятностни събития и предвижда рискови фактори.

- Системите за управление на сигурността на информацията могат да се моделират с невронни мрежи, управлявани от Платформата. Това е подход за повишаване на ефективността и ефикасността на критични системи за управление на информационната сигурност.
- Генеративната неконтролирана невронна мрежа - машина на Болцман (Boltzmann Machine) използва техники върху входните данни за анализиране на нормалните състояния на СУСИ, за да предвиди нежеланите ситуации. Международно признатите стандарти определят набор от контроли за сигурност за наблюдение, одит и управление на СУСИ. Те са разпределени в категории и всяка от тях има стандартизирани атрибути. Невронните единици на машината на Болцман са базирани на инфраструктурата за контрол на сигурността на СУСИ.
- Интегрирането на невронни мрежи в СУСИ може значително да подобри способността на организацията да открива, прогнозира и реагира на аномалии в сигурността. НМ се използват до голяма степен в почти всички области на информационната и киберсигурност, но за моделиране на поведението на СУСИ като цялостна сложна система, те са иновативен метод за намаляване на разходите и времето, както и за предотвратяване или смекчаване на щетите.

Апробация на резултатите

Основните резултати, получени при разработката на дисертационната работа, са докладвани в три публикации и на специализирани международни конференции.

Статии и цитирания

1. Velev T., Dobrinkova N., “Unified innovative Platform for administration and automated management of internationally recognized standards”, Book Title: “Digital Transformation, Cyber Security and Resilience of Modern Societies”, book series “Studies in Big Data”, Springer. DOI:10.1007/978-3-030-65722-2_5, eBook ISBN: 978-3-030-65722-2, ISBN: 978-3-030-65721-5, (https://www.scopus.com/pages/publications/85129091048) ISSN: 2197-6503, 2021, vol. 84, p. 61 – p. 75
2. Velev T, “Heuristic essentials for modeling and optimization of a platform for automation and management of standardized information security management systems”, 28–29 October 2021, Sofia, Bulgaria, 2021 Big Data, Knowledge and Control Systems, Engineering (BdKCSE) IEEE | DOI: 10.1109/BDKCSE53180.2021.9627263, ISBN:978-1-6654-1042-7, https://ieeexplore.ieee.org/document/9627277;
3. Velev T., Dobrinkova N., “The logical model of unify, innovative Platform for Automation and Management of Standards (PAMS)” 1st International Scientific Conference Digital Transformation, Cyber Security and Resilience" DIGILIENCE2019, Sofia 2-4 October 2019. ISIJ Digital Transformation, Cyber Security and Resilience, ISSN 0861-5160 (print), ISSN 1314-2119 (online), vol. 43, no. 1 (2019): 113-120, 2019, p.113-p.120 https://doi.org/10.11610/isij.4310
   - Citation 1: Wang, Z., Guan, X., Zeng, Y., Liang, X. and Dong, S., “Utilizing data platform management to implement “5W” analysis framework for preventing and

controlling corruption in grassroots government". Heliyon Volume 10, Issue 7, 15 April 2024, e28601, DOI: 10.1016/j.heliyon.2024.e28601, 2024 (Scopus referenced: https://www.scopus.com/pages/publications/85188751354)

Конференции

- International Conference on Big Data, Knowledge and Control Systems Engineering BdKCSE'2018, (21-22 November 2018), доклад: "Unified innovative Platform for administration and automated management of internationally recognized standards"
- DIGILIENCE 2019: Digital Transformation, Cyber Security and Resilience Central Military Club Sofia, Bulgaria, October 2-4, 2019, доклад: "The logical model of unify, innovative Platform for Automation and Management of Standards (PAMS)"

Проекти

Част от изследванията в дисертационния труд са от проект № BG161PO003-1.1.06–0036-C0001 "Унифицирана платформа за администрация автоматизация и управление на международно признати стандарти", изпълняван в сътрудничество от екипите на **Перфект Плюс ЕООД (ръководител Тодор Велев) и ИИКТ – БАН (ръководител Светозар Маргенов).** Проектът е за индустриално изследване на високотехнологичен иновативен продукт в областта на информационните технологии с продължителност 22 месеца.

Голяма част от резултатите са апробирани в проект „Разработка и въвеждане в експлоатация на Единна система за управление, контрол и анализ на дейностите (ЕСУКАД) за нуждите на Българския институт по метрология (БИМ)", ръководен от Тодор Велев.

Благодарности

Изказвам своята благодарност на научният си ръководител проф. д-р Нина Добринкова, за ценни напътствия, професионална компетентност и съдействие при подготовката на дисертационния труд. Благодаря за помощта и съветите на колегите от ИККТ на БАН и от Solent University Southampton .

Приложения

Приложение 1 Основна терминология в стандартизацията
Приложение 2 Сертификационни (одитиращи) организации
Приложение 3 Изследване на данните
Приложение 4 Актуалност и промяна на документите и управление на записите.
Приложение 5 UML код на модела (Plant UML)
Приложение 6 Реализация на Платформата с Python
Приложение 7 ORM (Object-Relational Mapping) реализация – SQL Alchemy

Abstracts of Dissertations

Number 7, 2025

INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

BULGARIAN ACADEMY OF SCIENCES

БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ

ИНСТИТУТ ПО ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

Брой 7, 2025

Автореферати на дисертации