https://orcid.org/0000-0002-9374-2833
https://orcid.org/0000-0002-8047-7647

UDC 004.772

**H.T. SAMOILENKO*, Yu.Yu.YURCHENKO***

# DEVELOPMENT OF AN INDIVIDUAL PROFILE OF ENTERPRISE PROTECTION

*State University of Trade and Economics, Kyiv, Ukraine

***Анотація.*** *У статті розглянуто існуючі моделі інформаційної безпеки, які є піграунтям для розробки індивідуального профілю захисту, та визначено особливості їх застосування. Забезпечення інформаційної безпеки на підприємстві полягає в розробці комплексної системи захисту інформації та контролі за джерелами виникнення потенційних загроз, необхідності здійснювати захист інформації відповідно до існуючих стандартів безпеки інформаційних технологій. Підготовка та розробка нормативної документації індивідуального профілю захисту є необхідними складовими відповідно до виду діяльності та потреб підприємства. У статті обгрунтовано необхідність розробки та подальшого застосування профілю захисту підприємства відповідно до сучасних стандартів у галузі інформаційної безпеки. Кількість профілів може бути не обмежена, вони розробляються для різних сфер застосування. До завдань реалізації політики безпеки підприємства входить розробка одного або декількох профілів захисту. Профіль захисту є основою для створення завдання безпеки, яке можна розглядати як технічний проєкт. У статті розглянуто складові поняття безпеки та визначено зв'язки і взаємодії між ними. Визначено вимоги, ризики (тобто події чи ситуації, які свідчать про можливість шкоди), активи та міри, що впливають на вразливість профілю захисту. Вимоги довіри безпеки включають розробку технологій, тестування, аналіз вразливостей, постачання, технічне обслуговування, експлуатаційну документацію тощо. Визначено дії, що несуть потенційні загрози безпеці умовного підприємтва. У статті запропоновано основні складові для побудови індивідуального профілю захисту умовного підприємства, зазначено зв'язки між ними. Виконано опис типів вимог відповідно до ієрархії «клас – сім'я – компонент – елемент». Визначено основні класи функціональних вимог до індивідуального профілю захисту.*

***Ключові слова:*** *моделі безпеки, реалізація політики безпеки, вимоги, вразливості, індивідуальний профіль захисту.*

***Abstract.*** *The article considers the existing models of information security, which are the basis for the development of an individual protection profile, and determines the features of their application. Ensuring information security at the enterprise is to develop a comprehensive system for protecting information and controlling the sources of potential threats, the need to protect information in accordance with existing standards for the security of information technology. Preparation and development of normative documentation of individual protection profile are necessary components in accordance with the type of activity and needs of the enterprise. The article substantiates the need to develop and further apply the company's protection profile in accordance with modern standards in the field of information security. The number of profiles may not be limited, they are developed for various applications. The task of implementing the company's security policy includes the development of one or more security profiles. The security profile is the basis for creating a security task that can be considered as a technical project. The article considers the components of the concept of security and defines the connections and interactions between them. Identified requirements, risks (i.e. events or situations that indicate the possibility of harm), assets and measures affecting the vulnerability of the security profile. Safety trust requirements include technology development, testing, vulnerability analysis, supply, maintenance, operational documentation, etc. Actions that pose potential threats to the security of conditional ingestion have been identified. The article proposes the main components for building an individual profile of protection of a conventional enterprise, indicates the links between them. A description of the types of requirements in accordance with the hierarchy «class – family – component – element» was executed. The main classes of functional requirements for individual protection profile are defined.*

© Samoilenko H.T., Yurchenko Yu.Yu., 2022

***Keywords:*** *security models, implementation of security policy, requirements, vulnerabilities, individual protection profile.*

DOI: 10.34121/1028-9763-2022-3-91-96

## 1. Introduction

The competitiveness of enterprises in various sectors depends on preserving their business customer base, business strategies, purchase price, and purchasing process. However, in recent years, the amount of sensitive information has been growing by leaps and bounds, and the selection of protective means against information leakage has become very difficult.

*The aim of the article* is to provide some models of analysis of information security and information protection and to develop an individual protection profile for a contingent enterprise.

## 2. Results of the research

The main purpose of the models is to create conditions for an objective assessment of the general state of the information system in terms of the degree of vulnerability or the level of data protection in it. From the very beginning, information security was also considered in terms of the possibility of applying modeling methods in it [1]. Below there are provided the most popular information security models.

### 2.1. ADEPT-50 model

One of the first attempts to use a mathematical model to describe the defense mechanism was the ADERT-50 model first published in 1970. It includes four types of security-related objects: users, tasks, terminals, and files. Each of them is described by a specific four-dimensional structure (the authors called it a tuple) (A, C, F, M) which contains the basic parameters of security.

### 2.2. HRU model

The HRU model was first proposed in 1971, and its creation (by M. Harrison, W. Ruzzo, J. Ullman) was an important step in the development of data protection theory. The HRU model is used to analyze the security system which implements a discretionary security policy and its main element – the access matrix. A protection system is a state machine that operates in accordance with certain rules of transition.

### 2.3. Take-Grant model

The Take-Grant model of distribution of access rights, proposed in 1976, is used to analyze systems of discretionary delimitation, provide access in the first place, and analyze the ways of distribution of access rights in such systems. Access graphs and rules of their transformations are used as the main elements of the model. It aims at answering the question of the possibility of obtaining access rights by the system entity to the object in the state described by the access graph. Subsequently, the Take-Grant model was developed as an extended Take-Grant model considering the ways of information flows in systems with the discretionary delimitation of access.

### 2.4. Bella-LaPadula model

This model implies the provision of all participants in the process of data protection and the documents with special tags, for example, «secret», «top secret», etc., called a security level. All levels of security are regulated by the established relationship domination. Access control is based on the security levels of the interacting parties based on two simple rules:

– an authorized person (entity) has the right to read only those documents whose security level does not exceed his personal level of security;

– the authorized person (entity) has the right to enter information only in those documents whose security level is not lower than his personal security level.

### 2.5. Integrity models

There are two models of integrity – the Clark Wilson model and the Biba model. The first one was proposed in 1987 as a result of an analysis of paper-based paperwork practices that are effective in providing data integrity. It is descriptive and does not contain rigorous mathematical constructions. The Biba model was developed in 1977 as a modification of the BellaLaPadula model and focused on ensuring data integrity.

### 2.6. Models of general type

In general models, the main issue is not only the access of subjects to objects but also other aspects of security including:

– a model of the protection process;

– a protection system model;

– a model of protection functions;

– a full overlap model;

– an information and analytical model for assessing data protection against threats of unauthorized access.

Security includes protecting assets from threats. The developers of the standard say that all kinds of threats should be considered, but in the field of security, the greatest attention is paid to those related to human actions. Fig. 1 illustrates the relationship between high-level security concepts. The preservation of assets is the responsibility of their owners, to whom they are valuable. Existing or suspected infringers may also attach value to these assets and seek to use them against the interests of the owner. Violators' events lead to threats. As mentioned above, the dangers are realized due to the vulnerabilities in the system.

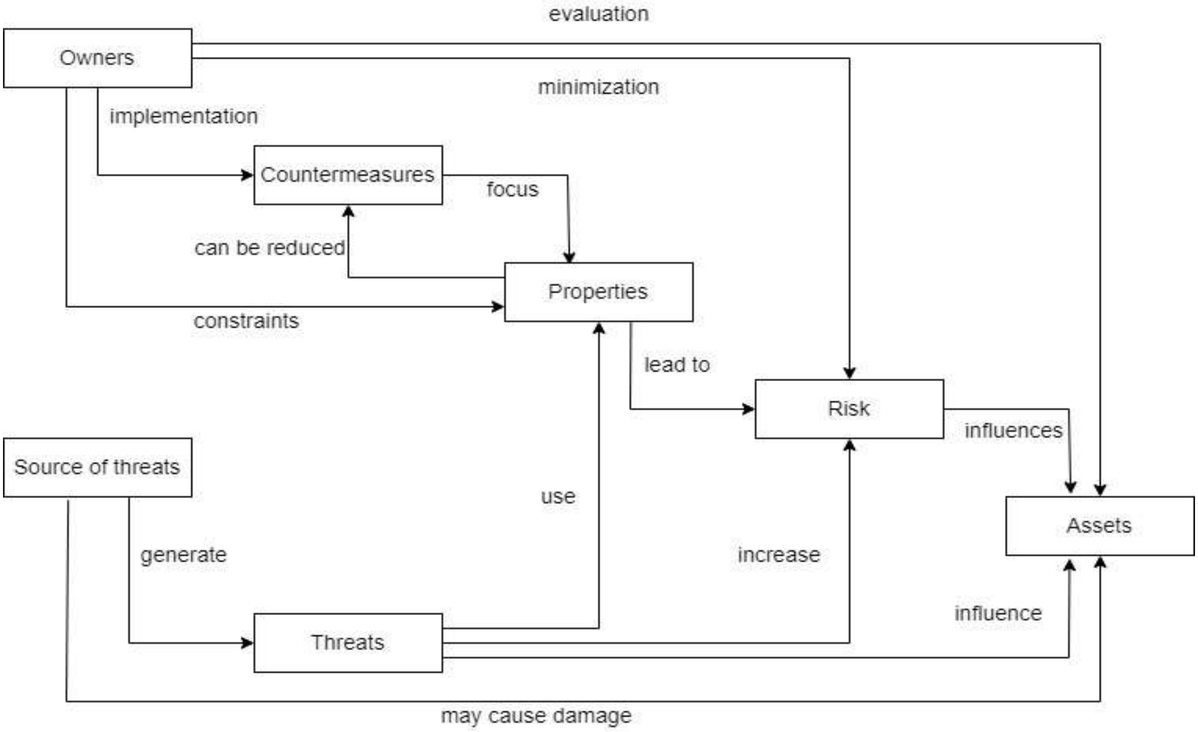

Figure 1 – Security concepts and their interrelation [adapted by the authors]

Asset owners analyze possible threats to determine which of them can be implemented in relation to the system under consideration. The analysis identifies risks (i.e. events or situations that suggest the possibility of harm) and analyzes them. Asset owners take countermeasures to reduce vulnerabilities and enforce security policies. However, even after the implementation of these countermeasures, residual vulnerabilities and, consequently, residual risk may persist.

One of the most common modern standards in the field of information security is ISO/IEC 15408 [2]. It was developed to meet the needs of three groups of professionals: developers, certification experts, and users of the object of assessment. In the standard, the latter means «an assessed product of information technology (IT) or a system with the guidance of the administrator and the user». Such objects include, for example, operating systems, applications, information systems, etc. «General criteria» imply the existence of two types of security requirements – functional and trust. Functional requirements apply to security services such as access control, audit, etc. Security trust requirements include technology development, testing, vulnerability analysis, supply, maintenance, operational documentation, and others.

## 3. Materials and methods

The description of both types of requirements is made in a single style: they are organized in a hierarchy «class – family – component – element». The term «class» is used for the most common grouping of safety requirements, and the element is the lowest, indivisible level of safety requirements [3]. The standard identifies 11 classes of functional requirements:

– security audit;
– communication (data transmission);
– cryptographic support (cryptographic protection);
– protection of user data;
– identification and authentication;
– security management;
– privacy (confidentiality);
– protection of security functions of the object;
– use of resources;
– access to the object of assessment;
– trusted route/channel.

The main structures defined by the «Common Criteria» are the protection profile and security objectives. The protection profile is an independent set of safety requirements for a certain category that meets customer's specific needs. The profile consists of components or packages of functional requirements and one of the levels of guarantee [4]. The structure of the protection profile is presented in Fig. 2.

The profile defines the «model» of the security system or its individual module. The number of profiles is not potentially limited, they are developed for different applications (for example, the profile «Specialized means of protection against unauthorized access to confidential information»).

The protection profile is the basis for creating a security task that can be considered a technical project for the development. The security task may include the requirements of one or more security profiles. It also describes the level of functionality of the means and mechanisms of the implemented protection and provides a justification for the degree of their adequacy. Based on the results of evaluations, catalogs of certified security profiles and products (operating systems, information security tools, etc.) are created, which are later used in the evaluation of other objects.

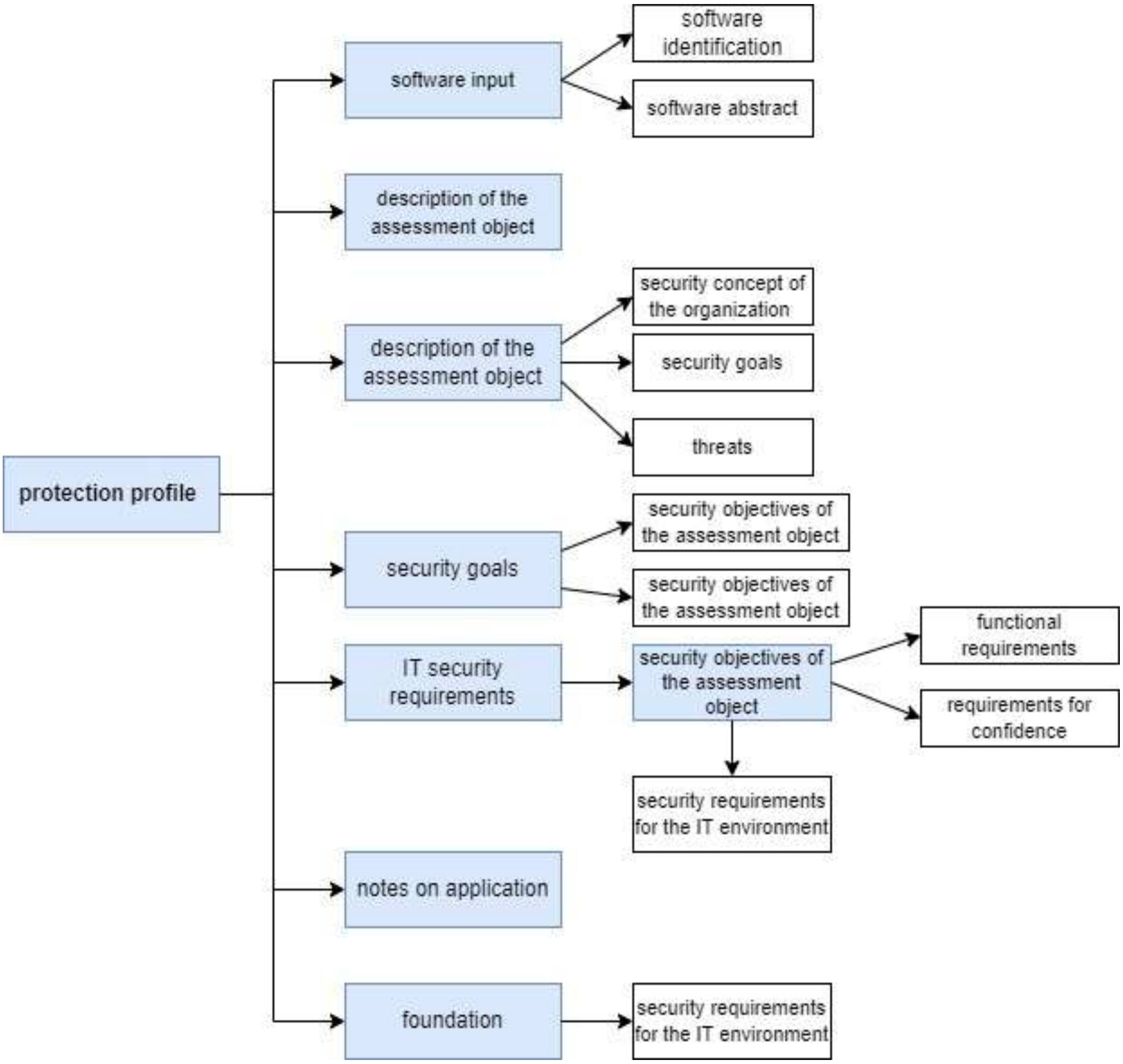
protection profile
software input
software identification
software abstract
description of the assessment object
description of the assessment object
security concept of the organization
security goals
threats
security goals
security objectives of the assessment object
security objectives of the assessment object
IT security requirements
security objectives of the assessment object
functional requirements
requirements for confidence
security requirements for the IT environment
notes on application
foundation
security requirements for the IT environment

Figure 2 – Individual protection profile [adapted by the authors]

## 4. Conclusions

Today, the problem of data protection is acute for every company because it directly affects the stability of its operation and further development. Thus, the need to develop and further implement a reliable profile of enterprise protection is quite critical. The protection profile is the basis for creating a security task considered a technical project for the development of hardware and software implementation. The security task may include the requirements of one or more security profiles. It also describes the level of functional capabilities of means and protection mechanisms, and provides justification for the degree of their adequacy. As a result of the evaluations, catalogs of certified security profiles and products (operating systems, information security tools, etc.) are created, which are later used in the evaluation of other objects.

The individual profile of enterprise protection can be divided into two parts: development of regulatory documentation and hardware and software implementation.

The article considers the most popular models of information security used to develop an individual protection profile. Accordingly, the normative documentation of the individual protection profile describes the information security model that will be used in the future. Preparation and development of regulatory documentation of the individual profile of protection must be performed in accordance with the profile of activities and needs of the enterprise. Thus, to ensure smooth operation of the enterprise it is necessary to use an individual data protection profile.

## REFERENCES

1. Скабцов Н. Аудит безопасности информационных систем. СПб.: Питер, 2018. 272 с.
2. Common Criteria Services – ISO 15408.
3. Диогенес Ю., Озкайя Е. Кибербезопасность: стратегии атак и обороны / пер. с англ. Д.А. Беликова. М.: ДМК Пресс, 2020. 326 с.
4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Юбилейное издание. СПб.: Питер, 2020. 1008 с.

*Стаття надійшла до редакції 06.06.2022*