The development of technologies and computing resources not only expanded the spectrum of digital services in all areas of human activity, but also defined the spectrum of targeted cyber attacks. The object of the study is the process of ensuring the safety of critical business processes that ensure the continuity of production and/or functioning of the company/organization/enterprise as a whole. Targeted attacks are aimed at destroying not only the business structure, but also its individual components that determine critical business processes. Continuity of such business processes is a critical component of any company, organization or enterprise of any form of government, which critically affects the earning of profits or the organization of production processes. The proposed concept of determining the security level of critical business processes is based on the need to use multi-loop information protection systems. This allows to ensure the continuity of critical business processes through a timely objective assessment of the level of security and the timely formation of preventive measures. This approach is based on the proposed rules for determining the achievement of a given level of security, which are based on assessments of the integrity, availability and confidentiality of information arrays, as well as computer equipment in relation to various points of the organization's business processes. The use of threat integration on the internal and external contours of the protection system allows to ensure the necessary level of security and continuity of the production/technological process of critical business processes. The proposed practical implementation of the system security level assessment system in the declarative programming language Prolog, which allows to form requirements regarding the achievement of a given system security level depending on the state assessments of individual system components

Keywords: security concept, critical business process, multi-loop protection systems

UDC 681.32:007.5
DOI: 10.15587/1729-4061.2023.274301

DEVELOPMENT OF THE CONCEPT FOR DETERMINING THE LEVEL OF CRITICAL BUSINESS PROCESSES SECURITY

Serhii Yevseiev
Corresponding author
Doctor of Technical Sciences, Professor, Head of Department*
E-mail: Serhii.Yevseiev@gmail.com
Oleksandr Milov
Doctor of Technical Sciences, Professor*
Nataliia Zviertseva
Postgraduate Student
Department of Software Engineering and Management Intelligent Technologies**
Yurii Pribyliev
Doctor of Technical Sciences, Associate Professor
Department of Information Technology and Information Security***
Oleksandr Lezik
PhD, Associate Professor
Department of Tactics of the Air Defense Troops
Ivan Kozhedub Kharkiv National Air Force University
Dynamivska str., 3 a, Kharkiv, Ukraine, 61021
Olena Komisarenko
PhD, Associate Professor
Department of Information Systems and Technologies
National Transport University
M. Omelianovycha-Pavlenka str., 1, Kyiv, Ukraine, 02000
Andrii Nalyvaiko
PhD, Associate Professor, Leading Researcher
Centr of Military and Strategic Research***
Volodymyr Pogorelov
PhD, Associate Professor
Department of Information Technology Security
National Aviation University
Liubomyra Huzara, 1, Kyiv, Ukraine, 03058
Vitaliy Katsalap
PhD, Associate Professor
Department of Information Technology and Information Security***
Iryna Husarova
PhD, Associate Professor
Department of Applied Mathematics
Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166
*Department of Cyber Security**
**National Technical University "Kharkiv Polytechnic Institute"
Kyrpychova str., 2, Kharkiv, Ukraine, 61002
***The National Defence University of Ukraine named after Ivan Cherniakhovskyi
Povitroflotskiy ave., 28, Kyiv, Ukraine, 03049

Received date 02.12.2022
Accepted date 12.02.2023
Published date 28.02.2023

How to Cite: *Yevseiev, S., Milov, O., Zviertseva, N., Pribyliev, Y., Lezik, O., Komisarenko, O., Nalyvaiko, A., Pogorelov, V., Katsalap, V., Husarova, I. (2023). Development of the concept for determining the level of critical business processes security. Eastern-European Journal of Enterprise Technologies, 1 (9 (121)), 21–40. doi: https://doi.org/10.15587/1729-4061.2023.274301*

1. Introduction

Achieving the goals of their business by companies is possible only with the effective use of information technology. The downside of this use is increased vulnerability to cybersecurity threats. Vulnerability identification and risk assessment strongly require an information security risk assessment. The data used for identification procedures is in

Copyright © 2023, Authors. This is an open access article under the Creative Commons CC BY license

most cases uncertain, which makes it a challenge to identify risks and vulnerabilities. So-called "vulnerability identification errors" can occur if false positive vulnerabilities are discovered or if vulnerabilities remain unidentified (false negative). "Clear identification" in this context means that all identified vulnerabilities do pose a security risk to the organization.

In order to identify vulnerabilities in the information security (IS) risk assessment, security experts analyze the organization's assets. Due to the fact that the probabilities, consequences, and losses of vulnerabilities cannot be accurately determined [1], methods such as brainstorming, checklists, scenario analysis, impact analysis, and cause analysis are used to identify vulnerabilities [2]. These methods use undefined input to identify a vulnerability. However, it should be noted that business security needs are not properly considered; security checklists and standards used to identify vulnerabilities do not take into account company-specific security requirements [3]. Further, increasing uncertainty is the intentional behavior of an attacker when exploiting vulnerabilities for malicious purposes. This is explained by the fact that predicting human behavior is associated more with existing vulnerabilities and their consequences [4], rather than with preparation for future attacks. As a result, modern approaches identify risks and vulnerabilities under conditions of a high degree of uncertainty, which can lead to errors [5, 6].

Thus, studies that are devoted to the formation of the concept of building a security system for critical business processes, which is based on a multi-loop security system, are relevant. Eliminating vulnerability identification errors can help reduce the security costs of ineffective security measures and demonstrate that business security requirements are met.

2. Literature review and problem statement

An analysis of the main international standards [7–21] showed that the considered individual components of the information technology security assessment methodology are based on the security model – ensuring integrity, confidentiality and availability (integrity-confidentiality-availability models). This does not take into account an integral component of information flows – the authenticity service – he state of information, which provides confirmation of the authenticity of the source (authorized user and/or process) of information. The lack of a synergistic approach to risk analysis, a unified methodology for assessing information technology security in standards does not allow timely development of appropriate policies, new approaches and measures to ensure information security. In addition, the formation of new systems based on the integration of various technologies (Internet of things, mobile, smart, etc.) allows the formation of cyber-physical (socio-cyber-physical) systems. As a rule, such systems are formed in various data processing environments (desktop, cloud technologies), information is transmitted via various channels (wireless, Internet, mobile Internet channels), which requires the formation of multi-loop security systems. Thus, the imperfection of security mechanisms is based on the problem of objective risk analysis. In fact, risk is an integral assessment of how effectively existing protection tools are able to withstand attacks on critical business processes.

Despite the fact that many mechanisms and means of information protection have been developed, one of the highest priority tasks remains the task of evaluating the effectiveness of the process of ensuring the security of cyber-physical systems critical business processes based on appropriate metrics. Among the most common security metrics are their following taxonomies: Vaughn-Hennig-Siraj, NIST STS822, OCIPEP, OCTAVE, CISWG, Erkan Kahraman. However, taxonomy data does not take into account the requirements for assessing the continuity of business processes, combining mixed (targeted) threats with social engineering methods, computational and financial capabilities of attackers. The paper [22] addresses the issue and presents the results of a thorough review of the scientific literature on the concepts of systems, infrastructure and management. The results show that concept building faces a common problem in describing its key elements, structures and processes due to their recursive nature. The layered nature of critical infrastructure systems prompts management to systematically address the adaptation, emergence, and entropy properties that a complex system of systems exhibits. This confirms the need to form new approaches to ensuring the security of critical elements of the system's infrastructure, including the continuity of business processes.

The analysis [7–23] confirms the fact that in order to solve the problems of ensuring information security, along with formal methods for modeling processes and evaluating the effectiveness of the functioning of security systems, it is necessary to widely use more diverse methods. Such methods include methods of decomposition and structuring of components of systems and processes, informal methods for evaluating the effectiveness of functioning and decision-making. This means that the apparatus of system analysis must be used at all stages of the life cycle of information security systems of critical business processes [22]. A special place in the development of information technology security assessment methodology is occupied by the ISO/IEC 15408 standard "General criteria for assessing IT security", "General criteria". The standard defines general criteria that are used as the basis for evaluating the security properties of information products and technologies [7–9]. Common criteria are aimed at ensuring the comparability of the results of assessments obtained by different experts by introducing a common set of requirements for the security functions of information technology products and systems, as well as for the indicators of these functions. Using the analyzed standard, it is possible to solve a specific applied problem of choosing the appropriate requirements and IT security indicators [22]. In addition, potential security threats from the Unified Criteria, namely integrity, availability, confidentiality, are further proposed to be included as components in a new synergistic model of security threats. However, the proposed regulator has a significant drawback - the overload of the requirements base, which does not allow using small and medium-sized enterprises to ensure the security of business processes, does not take into account the hybridity of targeted attacks. The standards of the ISO 27XXX series [11–21] make it possible to form an information security management system, assess risks (computer incidents) and form security system mechanisms. However, the need to integrate security components is not taken into account: cybersecurity, information security, information security. In addition, they do not take into account changes in the threat vector, the formation of new (hybrid) cyber-physical systems

(socio-cyber-physical systems), the synthesis of technologies, which does not allow taking into account the need to form multi-loop security systems.

Practice shows that today it is possible to clearly distinguish two main groups of methods for assessing security risks [15, 16, 18–20]. The first group of methods allows to set the risk level by assessing the degree of compliance with a certain set of information security requirements. The second group of information security risk assessment methods is based on determining the probability of attacks, as well as the levels of their damage. In this case, the risk value is calculated separately for each threat and, in the general case, is presented as the product of the probability of a threat being realized by the amount of potential damage from this threat. The value of the damage is determined by the owner of the information, and the probability of the threat being realized is calculated by a group of experts conducting the audit procedure.

A distinctive feature of the methods of the first and second groups is the use of different scales to determine the magnitude of the risk. In the first case, the risk and all its parameters are expressed in numerical, that is, quantitative values. In the second case, qualitative scales are used.

Information security risk assessments are performed for risks identifying caused by vulnerabilities before they occur and to implement the required security functions. In [24] risk is defined as "the likelihood that a given threat will exploit the vulnerabilities of an asset or group of assets and thereby cause harm to an organization". This definition of risk is standard, generally accepted and quite general. The disadvantage of such a definition of risk can be considered (for the purposes of this study) the absence of its specification for the analysis of business processes being performed. A vulnerability can be defined as a "flaw" or weakness in a system's security procedures, design, implementation, or internal controls that can be implemented (accidentally triggered or intentionally exploited). Existing vulnerabilities can lead to security breaches or violations of system security policy [25, 26]. Here it is also necessary to clarify that the concept of vulnerability is also interpreted quite broadly, which makes it difficult to use it in the specific conditions of the functioning of the organization and its business processes. It should be noted that both the identification of information security risks and the proposal of appropriate security measures depend on the accurate identification of vulnerabilities. Accurate identification in this context means that the identified vulnerabilities can actually lead to a security breach and pose a security threat to the organization. Vulnerability identification errors occur when a vulnerability is either misidentified (false positive) or unidentified (false negative).

As a first step in any information security risk assessment, assets, threats, and vulnerabilities are identified according to standards that define basic security concepts.

These standards propose procedures and methods (such as brainstorming, checklists, scenario, impact and cause analysis) for identifying threats and vulnerabilities. In addition, critical business processes and information assets must be identified to determine the value of each asset to the organization.

In [27], the allocation of critical business processes is justified by the fact that the limited budget for information security in organizations makes it necessary to effectively prioritize security requirements. The goal is to make the most of the available budget and achieve a balanced overall level of security, which should lead to the maximum return on investment. It is noted that many existing information security risk assessment approaches identify and assess risks to critical assets and are asset-centric approaches. They are limited in that it is difficult to track dependencies between assets and make realistic estimates of their value to the organization. The approach to security risk assessment presented in the paper is focused on business goals. Risks are identified and evaluated at the level of business processes and aggregated across all such processes depending on their criticality, role and importance for the organization as a whole. At the same time, both assets and processes that support or contribute to the achievement of the stated goals are practically not given due attention, which is a drawback of the proposed approach.

Reference [28] outlines the benefits of conducting a comprehensive risk assessment to help improve the effectiveness of responses to potential threats. The ultimate goal is primarily to identify, quantify and control the main threats that hinder the achievement of business goals. As part of this approach, a detailed risk assessment for a particular organization is carried out. It includes a comprehensive literature review analyzing several professional opinions on current information security issues. As an example, a case is considered when five important assets were identified in the risk register in relation to their owners. The work is accompanied by a qualitative analysis methodology to determine the magnitude of potential threats and vulnerabilities. The comparison of these parameters made it possible to assess the individual risk for each asset, threat and vulnerability. The risk appetite assessment helped to prioritize and determine acceptable risks. From the analysis, it was concluded that a person poses the greatest threat to information security due to intentional / unintentional human error. Finally, effective controls based on defense in depth were developed to mitigate the impact of identified risks from the risk register. The disadvantage of the approach proposed in [28] is the emphasis on assets, and the business processes used by them remain in the area of attention.

In [29], a description of the approach based on the systematic calculation of ratings is presented, which are additionally supported by logical arguments and evidence. The procedure combines the results of a threat assessment, a vulnerability assessment, and an impact assessment to arrive at a risk score for each asset for a specific threat. It is proposed to assess the risk rating according to the following formula:

$$\text{Risk\_Rating}(R)=\text{Threat\_Rating}(T)\times \\ \times\text{Vulnerability\_Rating}(V)\times\text{Impact\_Rating}(I).$$

It is expected that this systematic approach can assist decision makers in choosing a risk management strategy by ranking different threats according to their respective risk profile. Building a risk rating will allow to explore mitigation measures to reduce the risk to valuable assets and set a logical priority for implementation. In this paper business processes that use the corresponding assets are not considered, which should be considered a shortcoming of the proposed approach.

The paper [30] is focused on understanding the information an organization owns and how it should be used to sustain the business. The development of this understanding should help to manage information assets through change

effectively. The advantage of this work should be considered that, in addition to the definition of information assets, the need is stated:

– understand business motives and formulate business goals accordingly;

– understand business requirements for the use of information;

– present the relationship between business requirements and information assets in a way that is consistent with the declared goals.

It is argued that the reasons or "driving forces" for the implementation of the proposed approach may be different and, therefore, lead to different scales and goals. The scale can range from large-scale reviews of all organizational information to very focused assessments of specific changes in technology or business. It is stated that there are many benefits that can have a wide impact. These benefits include better change management, better understanding of information risk, and identification of potential savings and efficiency gains.

However, in this work, the emphasis is on information assets, while business processes, the implementation of which ensures the effective functioning of the organization's business, are "left out".

It should also be noted that the knowledge used by security experts is uncertain. Hazards, incidents or consequences statistics are missing, incomplete or possibly incorrect often. In addition, the vulnerabilities documented in the knowledge bases are not specific to the company's operations and security needs, which can lead to both ignoring vulnerabilities and identifying vulnerabilities that are not significant for a given organization.

Mistakes in identifying vulnerabilities can lead to unwanted losses on the one hand, and on the other hand, they can force a company to invest in security features that are not required. However, successfully and accurately identifying vulnerabilities can make a company more cost-effective in terms of security spending. This can prevent loss of image and/or finances [31], and also help demonstrate compliance with business safety requirements.

[31] examines the relationship between the increase in the number of security breaches affecting organizations and the costs associated with such incidents in order to mitigate their consequences by assessing exposure to risk and direct investment in IT security. However, due to the lack of standardized costing methods, the task of quantifying the internal costs of security breaches, as well as the costs of managing them, is one of the challenges of security risk analysis. Due to the fact that companies count the time spent by employees in the process of recovering a damaged IT resource and downtime, the cost of security breaches and loss of productivity is inflated. For these reasons, [31] proposes an approach to measure the negative economic impact associated with security incidents. The paper considers a method that involves the execution of alternative tasks that do not depend on the affected IT resources; therefore, employees' time is not considered completely free, and hence the overall costs are reduced. It has been demonstrated that the proposed method yields a lower overall cost than the company method in calculating the costs of information security breaches by reducing downtime. At the same time, as components of costs associated with downtime in work, they are usually not taken into account at all. The results showed how recovery procedures are performed in case of information security breaches. In other words, the impact of changing the parameters of running business processes (execution time and cost of performing a business operation) on the total cost of a business process has been demonstrated. However, consideration of information security violations from the point of view of business processes has not been explicitly performed, which, of course, should be considered a lack of work. The analysis [31] also leads to the conclusion that the business process model should provide for auxiliary operations that should be performed when the organization's security is violated.

Traditionally, protecting information and identifying information security risks requires appropriate processes that use scanning tools to identify threats and vulnerabilities. These methods use knowledge bases on security and vulnerability. The knowledge base can be either the security expert itself or any available sources that describe security best practices, security recommendations, or lists of vulnerabilities. However, these security knowledge bases are generic and not tailored to the security needs of a particular organization. However, accurately identifying vulnerabilities using this procedure is challenging, as it is nearly impossible to verify that all vulnerabilities have been correctly identified in a given environment.

The most popular and frequently used models based on the definition of risk as a threat are the following.

The model presented in [32] does not consider management as an element of the model; it also does not address security requirements that were not directly related to risks or assets.

The model [33] does not establish a link between the security requirement and asset control.

The paper [34] is devoted to the continuous analysis of the security of service-oriented systems during design and operation. Concepts and a process model are proposed for identifying security goals and requirements, assessing risks and documenting security measures. The purpose of the proposed concept is the ability to provide analysts with information about the security status of the system at any time during the design and operation processes. The main ideas are the interconnected identification and documentation of functional and security properties based on system models and a clear separation of business-oriented and technical information. It should be noted that the information used in the described approach is largely informal and non-executable.

In [35], a model based on the results of an exploratory qualitative study with the participation of experts is proposed. The purpose of the model is to identify potential rating variables that could be used to calculate a premium for insurance against cybersecurity risks. The proposed workflow involves conducting semi-structured qualitative interviews with a sample of 36 experts, followed by a set of indicators that are accessible and difficult to manipulate. The resulting set of indicators is then presented to the experts again to rank them according to their relative importance. The main disadvantage of this approach is the use of expert evaluation with all difficulties and disadvantages arising from this.

The works [34, 35] are made by the same author and can be considered as a representation of the same model, but from different points of view. Because of this, in the future they are considered as a single model. A common disadvantage of this model is that there is no direct relationship between security controls, security requirements, and assets.

A common disadvantage of these models [32–35] is that they are based on the definition of risk as a threat and vulnerability and do not take into account the security requirements

for risk definition. Therefore, these models lack relationships between risk, controls, security requirements, and assets. In addition, different terminology is used for some concepts.

Considering the security controls needed to identify a vulnerability requires that the focus be on the relationship between security requirements, assets, vulnerabilities, and risks. The risk or vulnerability is mitigated by the implementation and proper functioning of the appropriate security function. If the security function is not fully or correctly implemented, the risk or vulnerability is not reduced – the asset is at risk – and security requirements are not met. Failure to comply with security requirements will indicate a vulnerability. Therefore, it is anticipated that explicit security requirements assessment can be used to resolve vulnerability identification errors (false positives and false negatives) once the security needs business vulnerabilities are identified. The analysis carried out showed the following. A significant drawback of practical methods and techniques for analyzing computer incidents and mixed cyber attacks is that they do not allow the formation of the necessary preventive countermeasures at the initial stages of analysis. This, in turn, does not allow the formation of multi-loop protection systems. In addition, the disadvantages are only qualitative assessments that do not take into account the need for the continuity of critical business processes, and do not allow assessing the physical (financial) damage from the loss of not only confidential information, but also the suspension of critical business processes. Thus, an integrated approach is needed, which will allow forming the methodological foundations of the concept of determining the level of security of critical business processes.

3. The aim and objectives of the study

The aim of this study is to develop a concept for determining the level of security of critical business processes based on the paradigm: required security – business security needs – the identification of vulnerabilities in order to allow security experts to accurately identify vulnerabilities. Accuracy in this context means identifying flaws that could lead to a security breach or breach of security policy, and which thus pose a security risk to the organization.

To achieve the aim of research, it is necessary to solve the following objectives:

– to form a concept for determining the level of security, which is based on the concept of a critical business process and takes into account the points of execution of this business process;

– to form sets of rules for determining the achievability of a given security level, based on assessments of the integrity, availability and confidentiality of information arrays, as well as computer technology relative to various points of the organization's business processes;

– to develop a software implementation of a system for assessing the level of system security.

4. Materials and research methods

The use of the results of a quantitative risk assessment in the formation of an information security system (ISS) is due to several reasons.

Firstly, quantitative risk assessment allows to compare the benefits and costs of implementing GIS, thereby determining the effectiveness of investments in information security (ISec).

Secondly, many currently widely used standards in the field of information security and information technology (IT) are based on a risk-based approach.

It is also worth noting that there is a successful risk management practice in other areas, such as economics and finance, politics, ecology, production, and industrial safety. This allows to integrate risk management processes in certain areas into a single enterprise risk management system.

One of the main problems of existing approaches is the difficulty in obtaining objective quantitative assessments of IS risks, which require a large amount of initial data. Predicting individual risk parameters with acceptable accuracy is a very laborious task, and it is difficult to obtain an accurate quantitative estimate.

A significant influence on the formation of a list of critical business processes, which makes it difficult to create security systems, is exerted by the use of various technologies and elements within the framework of the integration and hybridity of technologies of socio-cyber-physical systems. Often, when assessing the risks that arise during the operation of an information system, causal relationships between identified risks are not taken into account.

An information system (IS) is understood as "a set of information contained in databases and information technologies and technical means that ensure its processing".

Based on the definition and analysis of cyber-physical systems, the following types of components of modern hybrid/complex IS can be distinguished: information assets (IA), software (SW), hardware (TS) and communication lines (CL). A structural diagram of the types of IS components is shown in Fig. 1.

Therefore, the set of IS components can also be represented as:

$$IS=\{IA, SW, HW, CC\}, \quad (1)$$

where IA is the set of information assets, SW is the set of software; HW is the set of hardware; CC is a set of communication channels.

A destructive state is understood as an undesirable and unplanned state of an IS component in which it finds itself as a result of the implementation of one or more threats. During the analysis of various regulatory documents on information security, the theory of reliability and a survey of specialists in the field of IT and information security, the main destructive states were identified for each type of IS components:

1) information asset (IA):

– unavailable (accessibility violated);

– compromised (violated confidentiality);

– changed (integrity is broken);

2) software (SW):

– unavailable (failure occurred);

– hacked (unauthorized access (UA) obtained by an attacker or user privileges increased);

– changed (unauthorized change of code and/or configuration);

3) technical tool (HW):

– unavailable (a temporary failure has occurred);

– inoperable (a failure has occurred requiring repair or replacement);

– lost (there was a loss or theft from the rightful owner);

4) communication channels (CC):

– unavailable (failure or failure has occurred);

– hacked (acquired UA by an attacker).

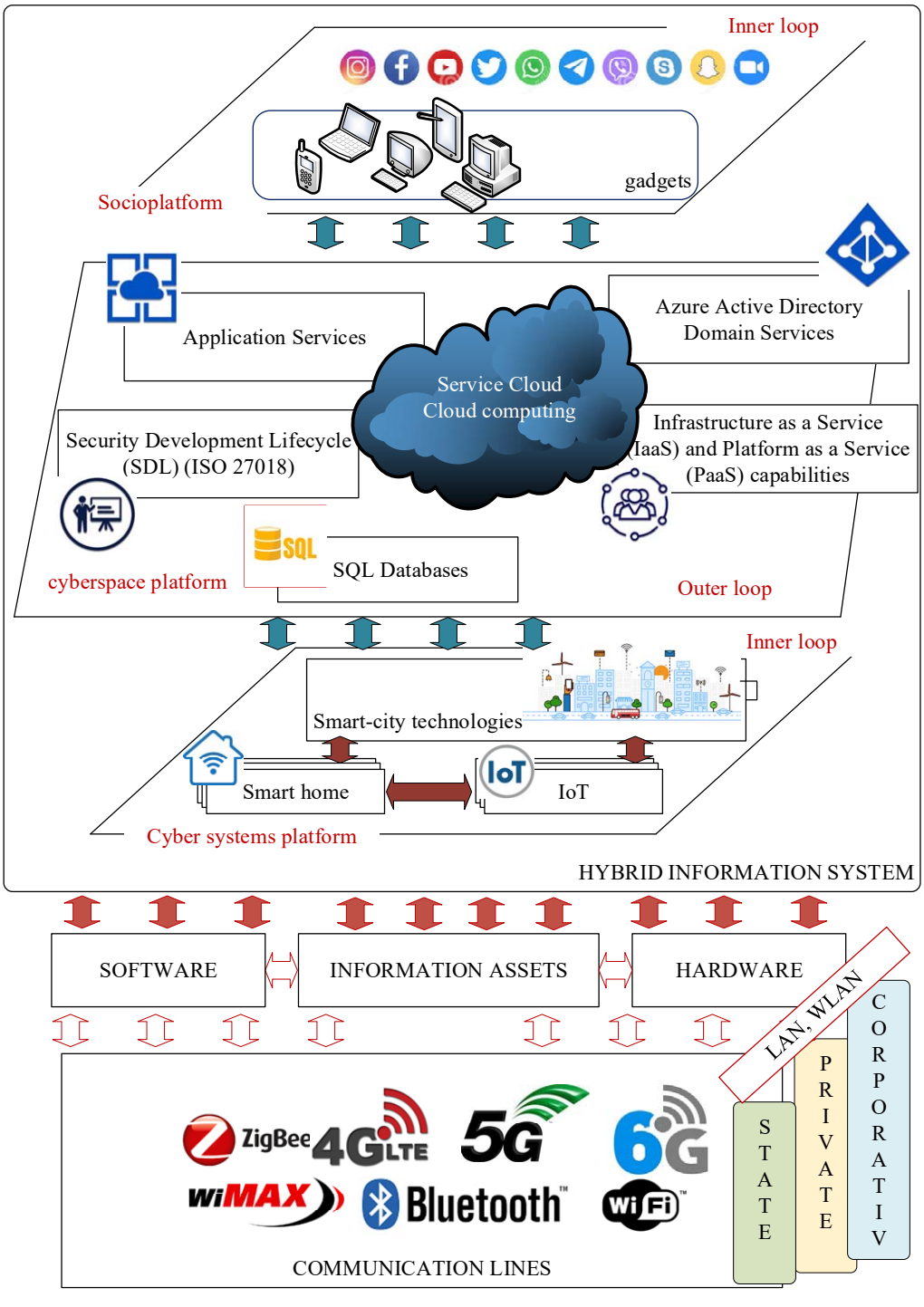

Fig. 1. Structural diagram of the types of components of the information system

A transition is understood as a change in the state of an IS component from normal to destructive as a result of a threat. The reasons for the transition of the IS component to a destructive state can be:

– the impact of the source of threats on the IS component;

– the completed transition of the associated IS component to the destructive state.

The source of threats is understood as the subject of access, a material object or a physical phenomenon that causes a threat to information security. The set of threat sources includes sources of four types:

$$ST=\{ND, TS, UV, IV\}, \quad (2)$$

where ST are sources of threats, ND are natural and man-made disasters; TS – technical means and systems; UV – unintentional violators; IV – intentional violators (intruders).

The study is based on information security models that describe the concepts used (e.g. assets, vulnerabilities and security requirements) in managing and assessing information security risks. The subject of the research is the development of the Concept for determining the level of security of critical business processes in the context of modern mixed cyber threats. The object of research is the process of ensuring the security of critical business processes.

Asset-related concepts describe critical assets and their security, while risk-treatment-related concepts describe se-

curity solutions, requirements, and security features used to mitigate risks. The main trends and approaches to determining the level of security are demonstrated in Fig. 2.

To build an integral security system for hybrid information systems, it is not enough to use only the principles that regulate in international regulators. An integrated approach is needed not only for the analysis of information assets, but also for the definition of critical (continuous) business processes that ensure the achievement of the goals of the company and/or organization. This approach requires the consideration of new approaches based on the integration of known methods and methods for assessing risks and computer vulnerabilities, taking into account the synergy and hybridity of targeted threats to elements of the IS infrastructure. In addition, it is necessary to form new requirements for assessing the security level of hybrid ISs, which are not only logically but also physically separated in space, use different technologies, and form both cyber-physical and socio-cyber-physical systems. This approach to building cyber-physical systems requires building security systems for each of the circuits/systems. This creates the need for multi-loop security systems with an integrated approach that takes into account both individual threats to the loops (internal and external) and their synergy for the attacker to build mixed (targeted) attacks.

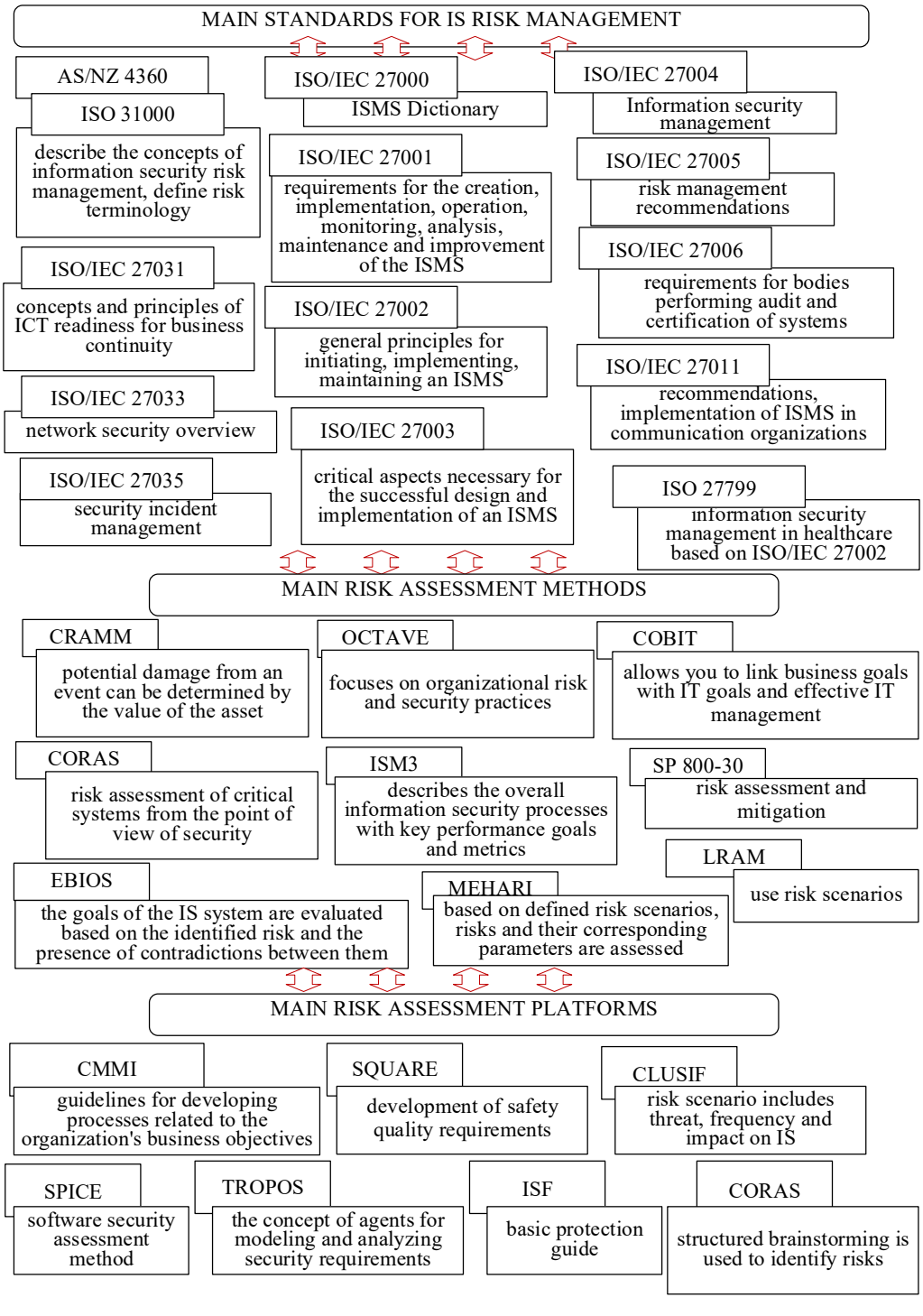

Fig. 2. Basic approaches to information security risk management

As a rule, when assessing security risks, after identifying the assets, the threats that may arise are determined. However, there are problems associated with the fact that it is impossible to determine whether the lists of threats, vulnerabilities or security controls used are complete and comprehensive.

When determining "real" risks for a company, there are many uncertainties in assessing probabilities as risk values. To illustrate the challenges of assessing risk in an uncertain environment, consider calculating the likelihood of a hypothetical encryption vulnerability on a web server. Let the web server need to determine the probabilities of the following outcomes:

– the offender exploits an encryption vulnerability in a web server;

– a hacker or criminal exploits an encryption vulnerability on a web server;

– a hacker or criminal will not be able to exploit any vulnerability.

More data is needed to determine the likelihood of detected web server threats and the parameters associated with this scenario need to be taken into account. The following data should be identified in the probability assessment and assessed for their availability:

– the number of known exploits for the web server version;

– the number of unprotected exploits for the web server version;

– criticality of exploits;

– the level of detection of all vulnerabilities by an attacker;

– coefficient of successful use;

– number of users of the web server application;

– the ratio of friendly and malicious users accessing the web server;

– impact on controls.

From the data that is needed to determine the probabilities, it is possible to form a diagram of dependencies between the parameters (Fig. 3), which can be used to estimate the probability.

Analysis of Fig. 3 showed that attackers accessing a website fall into two groups – hackers and criminals. The sublevels below hackers and criminals are the same. Each was assigned a Vulnerability Detection Rate, meaning the likelihood that they successfully discovered vulnerabilities. The following is the ratio of exploited vulnerabilities. Only a few vulnerabilities can be exploited because they have not been fixed. The next level concerns whether the hacker/criminal is capable of exploiting unprotected vulnerabilities. The last level of the tree is the likelihood that this vulnerability will be exploited. Some vulnerabilities are likely to be exploited more than others. This example assumes independence of variables (for example, hacker, criminal, encryption and SQL vulnerability). However, it is often difficult to determine whether the parameters are independent. This is due to the fact that it is necessary to know:

– the intentions of the attacker (for example, what is the difference between a hacker and a criminal);

– technical details of vulnerabilities (for example, details about encryption and a problem with SQL);

– environment (eg administrative and technical security functions applied);

– parameters and their relationship with each other.

Estimates for each parameter of the tree, obtained as a result of expert evaluation, are presented in Fig. 3. Most of the probability values in the dependency tree are only expert estimates that do not claim to be reliable. Rather, these artificial values are used to demonstrate how individual values affect the overall likelihood, and also to provide a statement about the likelihood of a hacker and a criminal using a web server.

Before presenting the detailed results of the probability score for a hacker and a criminal, one would expect the web server to be of medium risk. The results for probabilities since the start of this analysis are as follows:

– the offender uses an encryption vulnerability on the web server, probability=0.144 %;

– a hacker exploits an encryption vulnerability on a web server, probability=0.384 %;

– a hacker or criminal uses an encryption vulnerability on a web server, probability=0.528 %;

– a hacker or criminal will not exploit any vulnerability, probability=97.36 %.

Before defining risk based on security requirements, it is necessary to compare models to see if the relationship between risk and security requirements is defined. Before the comparison, it is necessary to give the basic definitions of the elements that will be used for an information security model based on these three models using similar terminology. The main definitions of the elements are as follows.

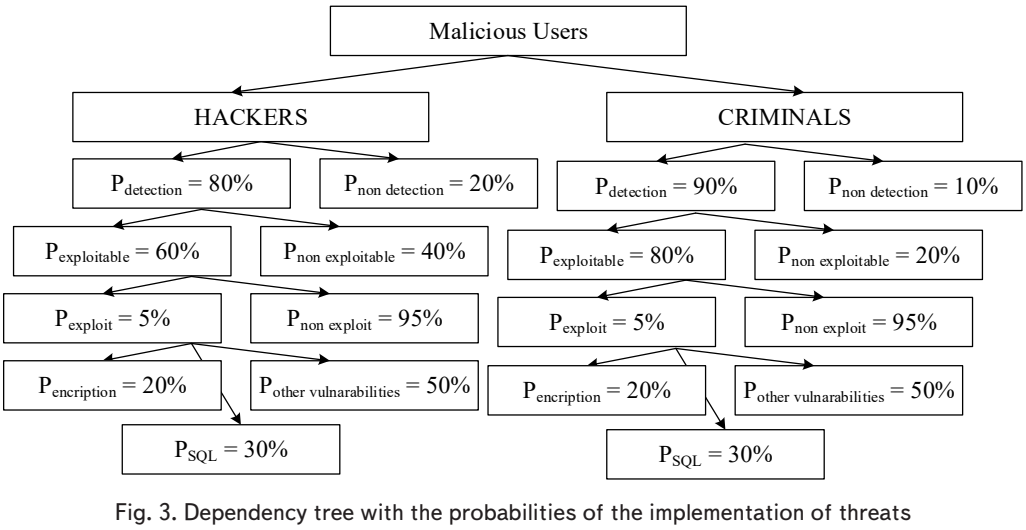

Fig. 3. Dependency tree with the probabilities of the implementation of threats

The security goal is determined by the business requirements that are affected by the risks. Business requirements describe security needs in terms of business operations, where a business operation is a set of activities that are defined and can be modeled as a business process. A security requirement is a refinement and additional specification of a security goal and represents constraints on the functions of a system where these constraints implement one or more security goals [19]. It is necessary to enter the following definitions:

– risk treatment is the process of selecting and implementing security functions to modify risk based on security requirements;

– security function is security requirements in the form of administrative, physical or technical controls and are applied to an asset in order to comply with a security requirement;

– assurance is an assessment of the security function and is used to determine whether the security requirements are met;

– assuranceis an assurance that security features reduce risks to assets and that assets are protected as required;

– an asset may consist of hardware, software, information systems, or any physical means used to fulfill an organization's business requirements. An information asset is a refinement of an asset that is made up of data;

– risk is a combination of a likely event and its impact, which can lead to a violation of safety objectives;

– an impact is an adverse change in an event that violates the safety objectives of an asset;

– an event is a threat that exploits a form of vulnerability;

– a vulnerability is a weakness in an asset or control associated with a security objective;

– a threat is a potential attack or incident that could lead to an adverse impact on an asset;

– the business process model is a detailed description of the business process, including the activities, agents, artifacts, and roles involved in the modeling notation;

– an artifact is a product that was created or changed as a result of a technological action;

– a role is a set of actions that has been assigned to the participants in the process to determine the functional responsibility.

5. Results of the development of the concept of determining the level of security of critical business processes

5. 1. Formation of the concept of determining the level of security

The formation of the concept of determining the level of security is focused on eliminating the shortcomings inherent in the most popular and widely used models. For this purpose, a comparative analysis of the models was carried out, the results of which are summarized in tables.

The elements that used in the most popular models [32–35] are compared in Table 1 with respect to the elements used in the extended information security model. The comparison shows that the models are built on the same basic principles. But the models lack elements such as assurances and business requirements, which links security risk assessment to the realm of business process management.

Table 2 shows which links between risks/vulnerabilities and security objectives/requirements are present and which are not present in these models.

Table 1

Comparison of model elements and risk concepts

Model elements	Model [34, 35]	Model [33]	Model [32]
Threat	Threat	Threat	Threat
Vulnerability	Agent	Vulnerability	Vulnerability
Event	Incident	Event	Not used
Impact	Threat	Impact	Likelihood and Consequence
Risk	Threat	Risk	Risk
Risk treatment	Security solution	Risk treatment	Not used
Element/Asset	Model element	Asset	Asset
Security function	Security Control	Control	Security Policy
Security Requirement	Security Requirement	Security Requirement	Security Requirement
Security objective	Business Security Objective	Security criterion	Target of evaluation
Assurance	Not used	Not used	Not used
Business requirements	Not used	Not used	Not used
Business process modelling	Not used	Not used	Not used

Table 2

Comparison of the use of security requirements

Relations	Model [34, 35]	Model [33]	Model [32]
Risk to security objective	–	+	–
Risk to security requirement	–	+	–
Risk to business requirements	–	–	–
Vulnerability to security objective	–	–	–
Vulnerability to security requirement	+	–	–

A proposed method applies existing models such as information assets and security requirements to business process models (BPM). Business process models describe the actions of a process in an organization to achieve a goal. From BPM, information assets, participants, and computer system facilities for risk assessment can first be determined. The criticality of each information asset can be defined by business process objectives in the form of security objectives. After that, the security requirements specifying the security objectives can be identified and used to argue for the correctness of the procedure for correctly identifying vulnerabilities. Security features related to business process activities that use an information asset are compared with security requirements to identify vulnerabilities.

The proposed approach provides an assessment of security requirements within business process models to identify vulnerabilities, eliminate identification errors (false positives, false negatives and true positives) of vulnerabilities, regardless of the business processes used. However, it should be noted that not all vulnerability identification errors can be eliminated by applying this approach. The difference between the proposed method and existing approaches lies in the explicit assessment of

security requirements in a business context (in business process models) to accurately identify vulnerabilities. Eliminating vulnerability identification errors will reduce the amount of money spent on the implementation of ineffective security measures, which is the result of meeting business security requirements.

The concept of determining the level of security is based on an extended model of information security (Fig. 4), based on the models considered earlier and representing these relationships.

The need to introduce an extended information security model into consideration is caused by the fact that none of the analyzed models considers the relationship between risk, security requirements, security controls and assets. This extended information security model proposes to consider risk in terms of security requirements because it provides a combined view of concepts related to risk, risk treatment, and security requirements.

This extended information security risk model uses model elements and relationships between elements from the previously mentioned models. Rectangles are used to represent elements, and text-annotated arrows are used to describe relationships between elements. In the model that follows, adds elements for elements such as assurances, business requirements, and business process modeling that are not present in existing models. Labeled arrows between elements such as vulnerability and risk are added to describe the context of the relationship and to clarify the relationship between concepts related to risk, risk treatment, assets, and security requirements. Labels are used to describe relationships between elements.

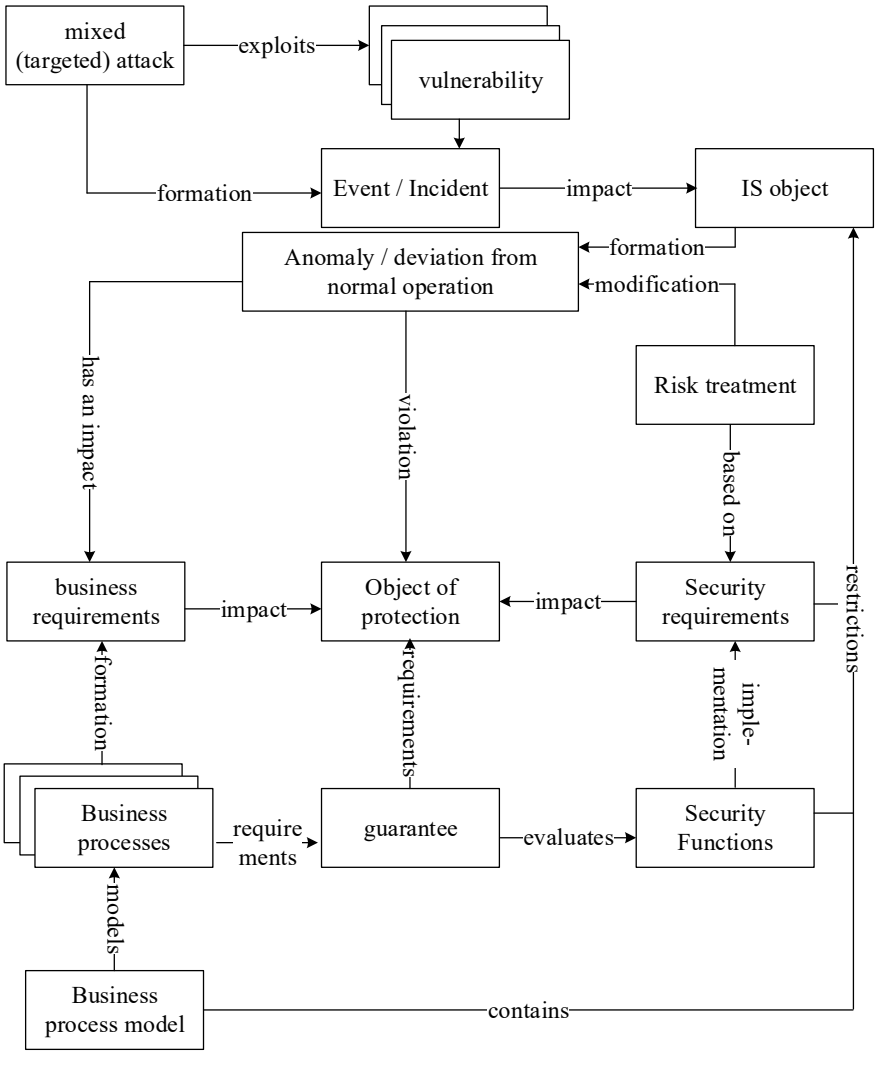

Fig. 4. Extended information security risk model

Compared to existing models, this extended information security risk model provides a combined representation of concepts related to risk, risk treatment, asset requirements, and security, similar to models [32–35]. The difference is that risk treatment and asset-related concepts are linked through risk and security requirements, and not just through risk itself. Model elements such as risk, vulnerability, security objective, security requirements, security controls, and asset are linked together, showing that risks and vulnerabilities affect security objectives, security requirements, and assets. Models [32, 33] do link risks to security objectives and requirements, but they use this relationship to indicate that security requirements reduce risk and that the significance of the risk is determined by the security criterion. Models [36–38] associate threats with security requirements. This indicates a breach, but misses the link between security requirements and controls, and also lacks the concept of vulnerabilities in the model.

In the model [33], vulnerabilities and assets are linked through security policy to security requirements, but risk treatment concepts are not explicitly specified. The advanced information security model shows the impact of risks and vulnerabilities on security objectives, security requirements, and assets. That is why it can help to better understand the relationship between concepts related to risk, assets, security requirements and risk treatment. Thus, it will allow for a better integration of these concepts into existing approaches to risk assessment. In addition, it is used as a basis for determining risk in terms of security requirements. This is made possible by the relationship between risk and vulnerabilities, security objectives and associated security requirements, and not just in terms of threats and vulnerabilities.

Taking into account the remarks made, it can be argued that the extended information security risk model is the basis for determining the risk in terms of security requirements. Further, the definition of risk is developed based on the relationship between risk, vulnerabilities, goals and security requirements.

Risks and vulnerabilities violate security objectives arising from business requirements by failing to ensure the confidentiality, integrity, and availability of information. This can be detrimental to the organization. In an extended information security risk model, this is depicted as a relationship, labeled "violating," between a risk or vulnerability and a security goal. If a security requirement is not implemented, implemented

incorrectly, or not followed, it will adversely affect the security goal and ultimately business requirements. This is because security requirements refine the purpose of security by defining the requirements for ensuring the confidentiality, integrity, and availability of information. Therefore, non-compliance with security requirements can be expected to be detrimental to the organization and therefore constitutes a security risk to the organization as a whole.

The link between a risk or vulnerability and a security goal is that the former can violate the security goal specified by the security requirements and implemented through the security functions, thereby harming the organization. Therefore, risk can also be defined as "non-compliance with safety requirements that causes harm to the organization". Therefore, both a risk and a vulnerability can be identified by the deviation or non-compliance with the security requirements by the implemented security functions. Security functions are implemented by administrative, physical and technical controls that meet security requirements. This means that the correct implementation and operation of security functions in relation to compliance with security requirements is key to preventing risk to the organization, as well as to identify risks and vulnerabilities.

Business process models can be used to assess risks, vulnerabilities, and security features that describe the operation and core values of an organization. Process actions describe what process participants or agents must do. An agent can be a person or a system performing an action. According to [39], business process models describe the processes of value creation in an organization and can be considered as a place where risks materialize, information is generated and security functions are performed.

It is the business process model that contains the information assets. Within a business process, information is processed to achieve the purpose of the process. The information is used by the actors (e. g., people) and systems (e. g., application or network) of the process because such information represents a business transaction. Information assets are subject to security requirements to ensure that the purpose of the process is achieved. The security requirements of an information asset depend on the purpose of the business process, the context and significance of the information related to the company, product, service or person, and represent a constraint. The security requirements are implemented through the security functions for the information asset. Security features provide protection in terms of confidentiality, integrity, and availability of an information asset. Security features such as authentication mechanisms ensure compliance with information asset security requirements (Fig. 5).

Information assets are key because, when processed in a business context, they bind business and security goals to their requirements and it is to them that security functions are applied. The correlation between information assets, business process models, security requirements, and security functions can be used in risk assessment to identify vulnerabilities. The security requirements can be assessed using the security functions applied to the information asset. The security of an information asset can be assessed in the context of a business process by the activities of the value-creating processes that use the information. By using these elements in an assessment, it can be ensured that the required security can be implemented and that the organization is not at risk.

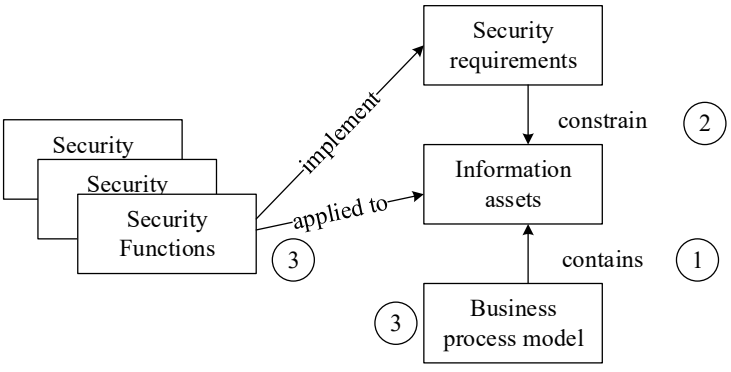

Fig. 5. Correlation of concepts and the order of use of concepts

The proposed security breach risk assessment approach uses correlations between security requirement elements, information assets, business process models, and security functions to identify vulnerabilities.

Initially, the list of information assets is formed on the basis of business process models (1). Information assets can be identified by information used in critical business processes. Information assets are characterized by the security requirements that can be defined for them and represent constraints (2). Artifacts such as business process and security objectives, security policies, or security best practices can be used to define security requirements. These information asset security requirements are analyzed and evaluated in the process activities of the business process model (3) against the implemented security functions applied to information assets (3) to identify vulnerabilities (Fig. 5). To determine if the information assets are appropriate for the implemented security functions, the security requirements of the asset must be evaluated in each activity of the business process model where the information assets are used.

The benefit of evaluating information asset security requirements using a business process model is that the basis for the assessment-the security requirements that provide true value-is defined and explicitly evaluated in the operational business context. Assertion about the security of information assets can be provided by the results of risk assessment of processes and information assets, which show only really relevant vulnerabilities. This statement can be formulated as not only vulnerabilities are defined, but also security needs and the need to fulfill them. As a result, security vulnerabilities and security operations can be identified more precisely than simply based on security best practices for any individual asset. In addition, interdependencies between information assets and/or processes can also be taken into account, since the security requirements of information assets are systematically assessed during the implementation of a business process. The difference from other approaches that use parts of business process models, information assets, or security requirements is that vulnerability identification for an information asset is based on an explicit assessment of the security requirements of the asset, taking into account the actions of business processes and the implementation of security functions.

The structure of the characteristics of security requirements that define the security needs of an information asset, taking into account the processing of information, containers that process information, as well as the processes required for the security of containers, is presented in Table 3.

Table 3

Security Requirements for Information Assets

Information asset	Security services	IT Security Processes
Processing		
Data	Integrity, Confidentiality and availability security objectives rating.	n/a
Containers		
Primary Systems	Integrity, confidentiality and availability requirements for the systems that processes information.	IT security processes that ensure the security of systems.
Organization/ People	Integrity, confidentiality and availability requirements for the actors or the processes that handle the information.	IT security processes that ensure security in the organization.
Environment/ Physical	Integrity, Confidentiality and availability requirements for the environment where the information is physically available.	IT security processes that ensure security for facilities and the workplace.

Thus, to implement the proposed concept, it is necessary to determine not only possible mixed (targeted) cyber attacks, but also to form a set of rules for determining the achievability of the required security level. This approach ensures the integration of preventive measures for possible computer incidents/vulnerabilities, mixed (targeted) attacks, and will also automate the process of their formation, taking into account business goals. In addition, the proposed solution allows to create and take into account critical business processes, conduct modeling based on the Prolog program.

5. 2. Formation of a set of rules for determining the achievability of a given security level

The set of rules for determining the achievability of a given security level is proposed to be formed as follows. First of all, it is necessary to perform the identification of vulnerabilities, which is performed as follows.

The first step assesses the degree of implementation of security functions at the processing level and their compliance with the security objectives of information assets (second step). The second step evaluates the information asset containers (i. e., systems, actors, and environment) and security requirements.

Implemented security functions are evaluated to determine conformity with the security objectives. However, before the security functions can be assessed, it is necessary to determine where in the business process information assets are created, processed and transferred. These business process points are defined as entry points (EPs), processing points (PPs), and communication points (CCs). Entry points (EPs) describe the actions by which available information is made available for processing by entering the system. Processing points (PPs) describe activities in which information is stored permanently in electronic form or modified (processed). Communication channels (CC) describe activities in which information is transferred between the activities of a process.

Information can be transferred across organizational boundaries, geographic locations, or across departments. EP, PP and CC can be identified by keywords (eg enter, process, save, send) of business process operation descriptions. Entry points, processing points and communication channels determine the input, storage, processing and transmission of information. Through these process points, the security objectives of processing an information asset are evaluated.

For each EP, PP and CC, the degree of implementation of security services (functions) (such as access control, authorization, data verification, communication, encryption, performance) is determined. These security functions are subject to evaluation because they are closely related to the security objectives by definition. For example, integrity concerns the protection of accuracy and completeness; therefore, access control, authorization, and data validation are checked to ensure integrity.

Confidentiality is concerned with preventing unauthorized disclosure of information, so access control, authorization, communication, and encryption are checked to ensure confidentiality.

Availability means that the assets are available and therefore the implemented contingency measures and system performance are checked to ensure availability.

All possible ratings defined for access control (AC), authorization (A), input validation (D), communication (C), and encryption (E) [38] are shown in Table 4. For each level, its rating and abbreviation are determined, for example. AC0 means access control level 0; A2 stands for authorization level 2. After defining the implementation levels of the security function, it is necessary to determine whether the security objective of the information asset is met at each of the EPs, PPs and CCs where the information asset is used.

In the next step, the security function implementation rating for each EP, PP and CC is assessed against the information asset's security objective level. The set of security functions is evaluated taking into account the action on the information and the security goal to be achieved. EPs are only evaluated for integrity through security, access control, and data validation features. PPs are evaluated based on integrity and confidentiality through security, access control, authorization, and data validation features. CCs are evaluated for integrity and confidentiality through the use of communication security and encryption features.

Table 4

EP, PP and CC rating criteria

EP/PP measures			CC measures	
Access control& accountability	Authorization (access right)	Data input validation	Communication	Encryption
AC0: Unauthenticated user	A0: none	D0: None	C0: External unauthenticated partner	E0: None
AC1: internal user	A1: Read	D1: Manual	C1: External authenticated partner	E1: Weak encryption
AC2: authenticated user	A2: Execute/process	D2: Downstream validation	C2: Internal network partner	E2: Standard encryption
AC3: System user	A3: Write/update	D3: Value verification	C3: Internal authenticated partner	E3: Strong encryption
EP/PP security level	A4: Full control	D4: Value verification and completeness	CC security level	

Availability is assessed for EPs, PPs, and CCs that use the systems, based on system performance and contingency measures taken. The evaluation of the security function implementation rating against the information asset security objective rating is supported by a predefined set of rules for checking compliance. For example, an access control score in EP1 (entry point 1) evaluated as AC0 (access control level 0) is compared to the defined rules for security goal integrity level 2. Fig. 5 shows a fragment of a complete set of rules defined to ensure the integrity and confidentiality of security goals [40]. Scores for EP/PP and CC can be "good" (fair – requirements met), "poor" (not enough – requirements not met), "n/a" (not applicable), or "n" (unknown – not rated).

The rules can be read as follows for the first level of integrity and access control to security functions (each cell represents one or more rules) (Table 5):

– AC0: If an EP is rated AC0, then the Data Entry Review score must be at least D2 for that EP. PP AC0 rating is ok;

– AC1 and AC2: If the EP is rated AC1 or AC2, the data entry validation rating must be at least D1. PP rating AC1/AC2 is ok;

– AC3: EP rating AC3 is acceptable. The PP AC3 rating is ok.

The assessment of the integrity and confidentiality of information asset security objectives is based on the same security functions and follows the same procedure. Different categories such as "performance" and "measures" are used for the accessibility of a security goal. Scores how often accessibility requirements have been met in the past, with a performance rating. Implemented continuity measures are rated with a "measure" rating. The difference from the integrity and confidentiality assessment is that only system containers are considered in the availability assessment. Rule sets are not static and can be changed as required by company policy. The rules were defined using the knowledge of security experts and taking into account the dependencies of the security functions on the level of the security goal.

Table 5

Security goal rule set table (excerpt)

Security Objective		Integrity		
		Level 1	Level 2	Level 3
Access Control				
Unauthenticated user	AC0	EP and ≥D2	EP and D4	EP failed
		PP	PP and ≤A1	PP and ≤A1
Internal user	AC1	EP and ≥D1	EP and ≥D2	EP failed
		PP	PP and ≤A2	PP and ≤A1
Authenticated user	AC2	EP and ≥D1	EP and ≥D1	EP and ≥D2
		PP	PP and AS and≥D1	PP and (A3 or A4 and D4)
System user	AC3	EP	EP	EP
		PP	PP	PP
Authorization				
None	A0	PP	PP	PP
Read	A1	PP	PP	PP
Execute/process	A2	PP	PP≥AC1	PP and ≥AC2
Write/update	A3	PP and ≥D3	PP and D4	PP and (AC2 and D4)
			AC2 and≥D1	AC3
Full control	A4	PP and ≥03	PP and D4	PP and (AC2 and D4)
			AC2 and D2	AC3
Data validation				
None	D0	EP failed	EP failed	EP failed
Manual	D1	EP and ≥AC1	EP and AC2	EP failed
Downstream reasonableness validation	D2	EP	EP and ≥AC1	EP and AC2
Value verification	D3	EP	EP and AC2	EP and AC2
Value verification and completeness	D4	EP	EP	EP and AC2
Communication				
External unauthenticated partner	C0	CC and ≥E1	CC failed	CC failed
External authenticated partner	C1	CC	CC and ≥E2	CC and E3
Internal network partner	C2	CC	CC	CC and ≥E2
Internal authenticated partner	C3	CC	CC	CC
Encryption				
None	E0	CC failed	CC failed	CC failed
weak encryption	E1	CC	CC failed	CC failed
Standard encryption	E2	CC	CC	CC failed
strong encryption	E3	CC	CC	CC

In the next step, the containers of information assets (e. g., information systems, personnel, environment) are evaluated in terms of information asset security requirements. Security requirements for containers of information assets are evaluated at each technological operation in which information is processed. This is done in the form of EP, PP and CC using information gathering methods such as on-site interviews and document reviews. The identified EPs, PPs, and CCs are evaluated by the security assessor based on evidence that the security requirements for the system, organization, or physical environment are met. This evidence may be obtained from the system configuration, system specification, company security policy, technical documentation, or implementation examples. IT security processes are assessed through system testing, verification, and review of process performance documentation. Assessing the IT security process helps identify technical issues and ensure safe operations; it also defines an organization's ability to detect, prevent, or mitigate security problems. The security of an IT process is determined by whether problems are identified in the implementation of the business process or not.

The next step is to specify the information asset security requirements. First, an appropriate security goal rating for integrity, confidentiality, and availability must be selected based on the information asset's security needs. Second, the security requirements of the container must be specified; a description of what needs to be protected, as well as a specific implementation in the containers that process the information. The company's security policy, organizational procedures, and security best practices can be used to identify and define security requirements.

5. 3. Software implementation of the system security level assessment system

The generated set of rules can be considered as the basis for the implementation of situational management of the security system, and in particular, the business process security management system [41, 42].

Dependencies between access control and authorization, as well as data validation in relation to input or processing of information, arranged in the form of a set of rules (Table 5), were implemented in SWI-Prolog to support automatic evaluation generation [43].

Prolog is a declarative programming language based on facts and rules. The procedures for working with them are implemented in the programming language itself and do not require programming costs. Prolog was also chosen because it is possible to generate logical search specifications to determine when a security function implementation becomes true with respect to the security goal level. This characteristic of Prolog can also be used to determine what security functions are needed (if not known) to meet the security goal level. In addition, it is easily possible to change the rule base in Prolog or improve the rules as needed (for example, if additional security features need to be evaluated or if new facts are available). That is why Prolog is a suitable tool for the initial creation of a means of manipulating the properties of objects and relations between them, which is the main subject of our study.

The purpose of the Prolog program is to support automatic evaluation of security goals. In Prolog, the logic of a program is expressed in terms of facts and rules. The program begins with a request that the Prolog engine tries to satisfy by checking the available facts and rules. Facts and rules are the rules for determining the security goal presented earlier. For each security objective (integrity, confidentiality, and availability), a security rating (level 1–3) was assigned to EP, PP, CC facts. These facts are checked by Prolog rules to determine if the request is true. For rule set table rules representing a condition, a fact is used, for example, PP is ok (true) when the security function "authorization" evaluates to A0. When programming in Prolog, this is displayed as auth(a0). For rules that are a conditional statement, a fact with arguments is used, e.g. PP is ok (true) when the security feature "authorization" is rated A0 and "access" is rated AC1 – auth_access(a0, acl). To represent dependencies between conditions in a conditional statement, rules were used to define integrity, confidentiality, and availability. In other words, both of the above facts are combined by a logical union ("and", represented by a comma) in the rule: integ(A, Ac): auth(A), auth_access(A,Ac).

Prolog's rules and logical conjunctions allow to combine facts and conditional statements. They can include or exclude conditions or form a new condition.

The program consists of three main parts:

– facts representing individual conditions for safety purposes and process points;

– evaluation rules for the safety of process points;

– interface for requesting information about the assessment required by the user.

The program starts by asking for a security goal assess (*X*=confidentiality, integrity or availability) and its rating (*Lev*=level 1 to 3). The so(*X*, *Lev*) rule then queries the process point type (*Pp*=*ep*, *pp* or *cc*) and, depending on the security target entry, invokes the integ(*Pp*, *Lev*), conf(*Pp*, *Lev*) or avail(*Lev*) rule . With integ (*Pp*, *Lev*) and conf(*Pp*, *Lev*), the EP and PP security feature ratings are requested for access control (*Ac*=*ac*0 to *ac*3), authorization (*A*=*a*1 to *a*4) and data validation (*D*=*d*1 to d4). For CC, only ratings for encryption (*E*=*e*0 to *e*3) and communication (*C*=*c*0 to *c*3) are requested. With avail (*Lev*), the performance (*P*=*p*1 to *p*4) and measures (*M*=*m*1 to *m*4) rating of the EP, PP and CC systems are requested. An entry can only be granted for one EP, PP or CC. Thereafter, depending on which security objective has been specified, the appropriate availability, integrity, or confidentiality evaluation rules are invoked on the process point type, as explained below. The program evaluates only one security objective for one process point.

A fragment of the program for implementing the request execution is shown in Fig. 6.

```
/*Assessment and query security objective and the
security objective level */
assess:-     write('Please     type     SO     integrity,
confidentiality,
availability:'),nl,read(X),write('Please type level 1 to
3:'),nl,read(Lev),so(X,Lev).
```

Fig. 6. Fragment of the program for implementing the security level request

After the user has specified the security functions for an EP, PP, or CC, evaluation rules are called to evaluate whether the security goal is met.

Integrity is assessed for EP, PP and CC. To determine the integrity, rules were proposed, an example, one of which is shown in Fig. 7.

In the body of each of the rules, it is checked whether one variable or a combination of all variables is true with respect to certain facts. For example, for EP, it is checked whether the

evaluation of the safety function Ac or D is true, or Ac and D are true. Lev contains the security goal level and is only used to distinguish between facts defined for different security goal levels.

Privacy is only assessed for PP and CC; EP is not subject to confidentiality requirements in terms of processing. An example of a privacy definition record for a PP is shown in Fig. 8.

The main part of each rule tests whether one variable or a combination of all variables is true with respect to certain facts. For PP, whether the evaluation of the safety function

```
integ_EP(Lev,Ac,D):- (ep_int_data(Lev,D);
ep_int_access(Lev,Ac); ep_int_data_access(Lev,Ac,D)).
```

Fig. 7. Example of a rule for determining the integrity of the data of a security function

```
conf_PP(Lev,Ac,A):- (pp_conf_access(Lev,Ac);
pp_conf_auth(Lev,A); pp_conf_access_au th (Lev, Ac, A)).
```

Fig. 8. Confidentiality Rule for a Processing Point

Ac or A is true, or whether Ac and A are true at the same time. The Lev variable reflects the level of the security goal and is only used to distinguish between facts defined for different levels of the security goal.

Accessibility is assessed without distinction between EP, PP and CC and therefore directly on established facts. The avail_EPPPCC (Lev, P, M) rule checks performance ratings and measurements using the facts defined for the availability level. The Lev variable reflects the level of the security goal and is only used to distinguish between facts defined for different levels of the security goal. Certain facts describe the true integrity, confidentiality, and availability condition at EP, PP, and CC regarding the implementation of the security function. Facts are used by the evaluation rules to test the truth of a statement for EP, PP, or CC. Facts are arranged as follows:

Name_of_the_fact (Security objective level, security function rating).

The rating of the security function rule can be one or more arguments. An example of a fact description for indicating data integrity at an EP, depending on the level1 and d2 values specified in the security level request dialog, is as follows:

/*Facts for verifying integrity for EP*/ep_int_ data(level1, d2).

Thus, the proposed software product provides the possibility of modeling security services, taking into account the proposed concept of determining the level of security of critical business processes.

6. Discussion of the results of applying the concept of determining the level of security of critical business processes

The paper proposes an approach related to the joint use of security requirements and business process models. The security requirements reflect the security needs of the business and determine whether a given vulnerability poses a security threat to the business. Information asset security requirements are evaluated in the context of the business process model to determine if the security functions are implemented and working correctly. The security requirements assessment considers systems, people, and the physical parts of business processes, as well as IT processes.

It is shown that risk assessment techniques can benefit from an explicit assessment of the security requirements in the business context during risk identification in order to eliminate vulnerability identification errors and determine the value of the security criterion.

To determine the security level of critical business processes, consider the block diagram of the concept, which is shown in Fig. 9. To identify threats and form multi-loop security systems, taking into account the integration of technologies and the formation of hybrid – cyber-physical/socio-cyber-physical systems, it is possible to use the classifier and expert evaluation proposed in [44, 45].

The security level assessment should take into account organizational, software, technical, informational, technological and even financial issues, providing a view of the risk on a company-wide scale. These components of the functioning of the organization can be combined within the business process model. So the block diagram of a business process reflects the technological aspects of the organization's functioning, linking individual operations with "input-output" links. Such links in the proposed model correspond to connection points (CC). The business transaction itself is assigned a process point (PP). The business operation is executed based on the data received from the "control" input, which defines the normative basis of the process. The performer of a business transaction is identified by the "engine" input. Business processes as a whole are defined within the framework of the concept in the part "Formation of security contours", individual components – within the part "Assessment of the degree of implementation of security services". The task of the desired level of security for the entire system of business processes of the organization is carried out in the "Evaluation of cyber threats" part of the proposed concept. Thus, within the framework of the proposed concept, the corresponding actions related to determining the achievability of a given security level are divided into levels of the concept.

As an example, a conditional example of making a payment in online banking is considered.

The use of the proposed concept begins with the definition of critical business processes (online payment execution process). The following information assets are defined for the selected business process: customer and payment data. Customer data is stored and processed, as well as payment data necessary for transactions. The criteria and indicators for identifying these information assets are decision points and actions in the process, such as "Enter personal and payment data", "Verify personnel and payment data", or "Save personnel, contract and payment data".

The next step is to specify the information asset security requirements. First, an appropriate security goal rating for integrity, confidentiality, and availability must be selected based on the information asset's security needs. Second, the security requirements of the container must be specified; a description of what needs to be protected, as well as a specific implementation in the containers that process the information. The company's security policy, organizational procedures, and security best practices can be used to identify and define security requirements.

The security requirements defined for customer and payment data are presented in Tables 6, 7.

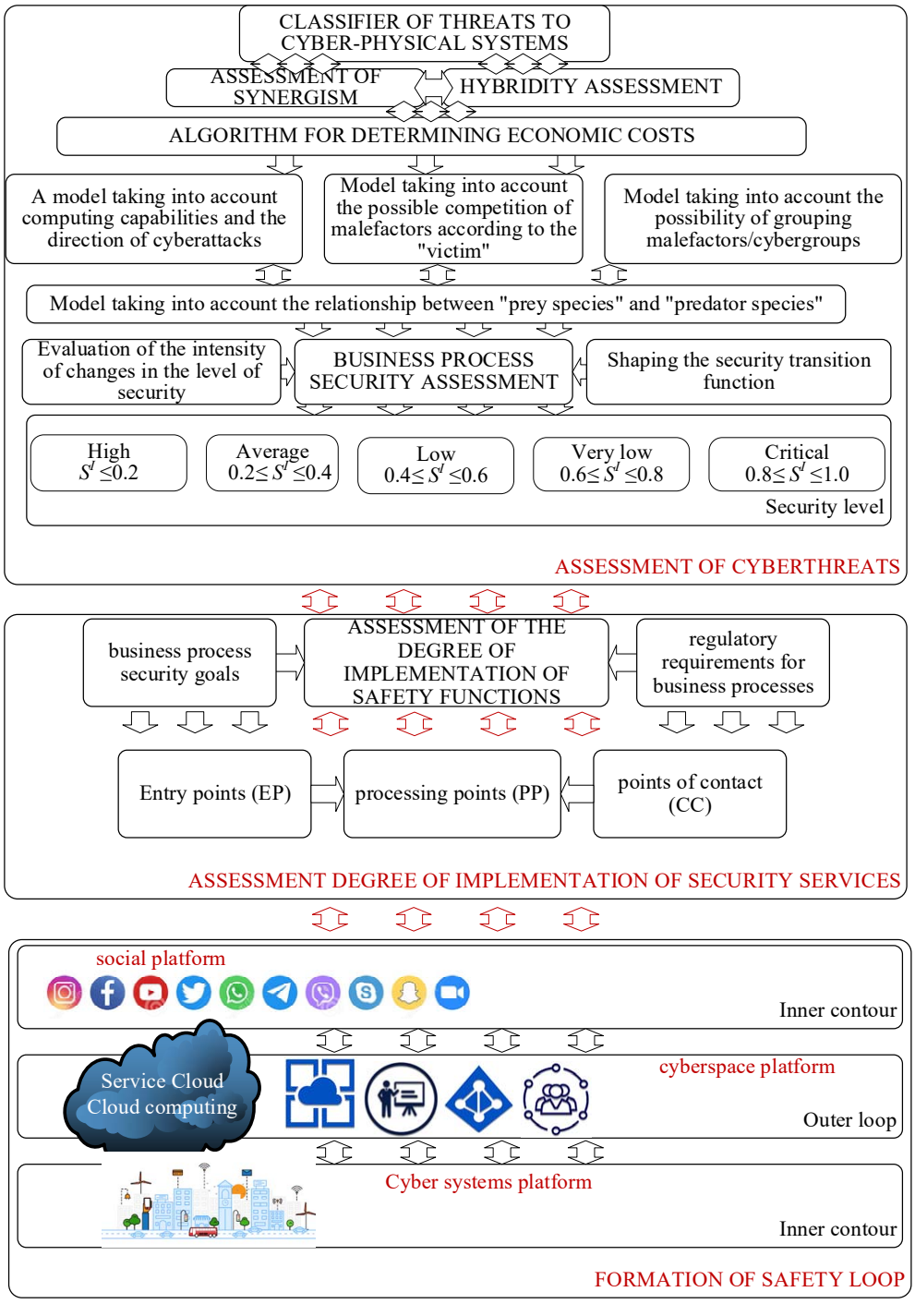

Fig. 9. Structural diagram of the Concept for determining the level of security of critical business processes

The degree of implemented security functions in the processing of information and their compliance with the security objectives of information assets is assessed. Information asset containers (systems, actors, and environment) are evaluated based on information asset security requirements. The points where information assets are created, processed or transferred (business process points EP, PP and CC) are also defined. For each EP, PP, and CC, the extent to which the security function is implemented (including access control, authorization, data validation, and communication security) is defined.

Container security requirements are assessed in terms of security at each technological operation in which data is processed (points EP, PP, CC). Evidence of whether the security requirements for the banking system, organization, or cyber-physical environment are met can be obtained from the system configuration or specification, company security policy, process documentation, or other implementation examples.

A Prolog program is used to determine whether the required security level is reachable. An example of a dialog when determining the security level of the analyzed system, security functions, setting indicators for the analyzed business process is shown in Fig. 10. As a result of the dialogue, a decision is formed on the possibility of achieving the specified security level with the value of the specified parameters.

Table 6

Customer data security requirements

Information asset: Customer data	Integrity	Confidentiality	Availability	IT Security Processes
Processing				
Data	I-L2	C-L2	A-L3	n/a
Containers				
Primary Systems	Address data has to be verified in the system. Data in the system should be protected against unauthorised access and modification. 192-bit AES encryption if data is transferred	Access should be given only to company people. Changes have to be logged	Within one business day	Access Management (authorizations). IT Security Management (Security of systems). Continuity management and Disaster Recovery. Change Management
Organization. People. Process	Personnel entering data should verify their entries as well as the data received	People of the departments should be aware of confidentiality	Core people within one business day	Access Management IT. Security training
Physical	None	Documents should be locked away and disposed of securely	Within one business day	IT Security training. Facility Management. Continuity Management

Table 7

Payment data security requirements

Information assets: payment data	Integrity	Confidentiality	Availability	IT Security Processes
Processing				
Data	I-L2	C-L2	A-L2	n/a
Containers				
Primary Systems	Address data has to be verified in the system. Data in the system should be protected against unauthorized access and modification. 192-bit AES encryption if data is transferred	Access should be given only to company people. Changes have to be logged	Within one business day	Access Management (authorizations). IT Security Management (Security of systems). Continuity management and Disaster Recovery. Change Management
Organization. People. Process	Personnel entering data should verify their entries as well as the data received	People of the departments should be aware of confidentiality	Core people within one business day	Access Management. IT Security training
Physical	None	Documents should be locked away and disposed of securely	Within one business day	IT Security training. Facility Management. Continuity Management

```
Welcome to SWI-Prolog (threaded, 64 bits, version 9.0.3)
SWI-Prolog comes with ABSOLUTELY NO WARRANTY. This is free
software.
Please run ?- license. for legal details.

For online help and background, visit https://www.swi-prolog.org
For built-in help, use ?- help(Topic). or ?- apropos(Word).

?- assess.
Please type: integrity, confidentiality, availability:
|: integrity.
Please type level 1 to 3:
|: level2.
Please type ep,pp,cc
|: ep.
Access rating(ac0-ac3)?
|: ac2.
Authorisation rating (a0-a4)?
|: a3.
Data validation rating(d0-d4)
|: d3.

true .
```

Fig. 10. An example of a dialogue with the program for setting the security level of the analyzed system and determining the possibility of its achievability

Making a decision on the impossibility of achieving the desired level of system security with unsatisfactory parameters of the analyzed business process is shown in Fig. 11.

```
?- assess.
Please type SO integrity, confidentiality, availability:
|: integrity.
Please type level 1 to 3:
|: level3.
Please type ep,pp,cc
|: ep.
Access rating(ac0-ac3)?
|: ac0.
Authorisation rating (a0-a4)?
|: a0.
Data validation rating(d0-d4)
|: d0.

false.
```

Fig. 11. Dialogue in case of receiving a decision on the impossibility of achieving the desired level of security

The research has some limitations, which are as follows.

Publicly available knowledge of threats and vulnerabilities is needed to define and specify security requirements; if a particular threat or vulnerability is not well known, it is unlikely to be identified. This is because the security expert does not identify the vulnerability and therefore it may not be properly reflected in the security requirements specification. The same is true for any procedure for identifying vulnerabilities, if the vulnerabilities are not known at all. In all methods, only known vulnerabilities can be identified.

Security requirements can be defined in general terms, but vulnerability identification will be more effective if security requirements are defined more precisely in terms of threats and vulnerabilities. Vulnerability identification depends on the precise definition of security requirements, which can be established by the business process owner or security expert. However, the proposed approach lacks a formal process for checking the correctness and completeness of the specifications.

The business process models used for this approach must be accessible and up-to-date so that they reflect current business operations. However, if the simulated process does not match the business operations, the vulnerabilities may not be correctly identified. But when evaluating the discrepancy between the process model and the current implementation, this will be pointed out.

However, despite these limitations, the automation of the security level assessment has a number of advantages. First of all, errors associated with the application of the developed concept are eliminated. Also, the software implementation of the concept allows to repeatedly play situations related to changing the requirements for individual components of the business process, obtaining an assessment of the achievability of the specified security level of the business process as a whole. Incorporating process points (EP, PP or CC), safety requirements and related evaluation results into the modeling process can be useful in several ways. First of all, to visualize the impact of vulnerabilities on the result of a business process or their impact on the actions of the assessment process, as well as for security analysis, allowing to identify weak links in the system under study.

An analysis of the practical implementation of the proposed approach showed that in the conditions of synergy and hybridity of mixed threats, business goals, and assessment of critical business processes, it is possible to form multi-loop security systems. Thus, the relationship between business goals, objects/elements of the infrastructure of hybrid information systems, security services is objectively formed, taking into account the requirements of regulators, the goals and functionality of the critical (continuous) business processes of the company/organization/enterprise. The main limitation is the integration of the proposed software solution into software applications that implement the analysis of computer incidents and cyber threats.

7. Conclusions

1. Hybrid (cyber-physical/socio-cyber-physh ical) information systems are boosted in the conditions of rapid development of computing resources and technologies, integration of various components of high technologies. This requires a new approach to providing not only security services, but also the multi-loop protection systems. The proposed concept of determining the level of security is based on the concept of a critical business process and takes into account the points of execution of this business process, as well as the hybridity and synergy of modern threats.

2. Sets of rules for determining the achievability of a given level of security based on estimates of the integrity, availability and confidentiality of information arrays, as well as computer technology relative to various points of the organization's business processes, have been formed. This approach provides an objective link between business goals, infrastructure objects/elements of hybrid information systems, security services, taking into account the requirements of regulators, the goals and functionality of critical (continuous) business processes of a company/organization/enterprise.

3. A system for assessing the level of system security has been developed, implemented in the declarative programming language Prolog, which, in dialogue with the user, generates a response on the achievability of a given level of system security, depending on the assessments of the state of individual system components reported to it.

Conflict of interest

The authors declare that there is no conflict of interest regarding this study, including financial, personal nature, authorship or other nature that could affect the research and its results presented in this article.

Financing

The study was conducted without financial support.

Data Availability

The manuscript has no associated data.

References

1. Fenz, S., Ekelhart, A. (2011). Verification, Validation, and Evaluation in Information Security Risk Management. IEEE Security & Privacy Magazine, 9 (2), 58–65. doi: https://doi.org/10.1109/msp.2010.117
2. IEC 31010:2019. Risk management – Risk assessment techniques. ISO. Available at: https://www.iso.org/standard/72140.html
3. Shaikh, F. A., Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. Computers & Security, 124, 102974. doi: https://doi.org/10.1016/j.cose.2022.102974
4. Haag, S., Siponen, M., Liu, F. (2021). Protection Motivation Theory in Information Systems Security Research. ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 52 (2), 25–67. doi: https://doi.org/10.1145/3462766.3462770
5. Li, Y., Xin, T., Siponen, M. (2022). Citizens' Cybersecurity Behavior: Some Major Challenges. IEEE Security & Privacy, 20 (1), 54–61. doi: https://doi.org/10.1109/msec.2021.3117371
6. Chen, S., Xiao, H., He, W., Mou, J., Siponen, M., Qiu, H., Xu, F. (2021). Determinants of Individual Knowledge Innovation Behavior. Journal of Organizational and End User Computing, 33 (6), 1–24. doi: https://doi.org/10.4018/joeuc.20211101.oa27
7. ISO/IEC 15408-1:2009. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. ISO. Available at: https://www.iso.org/standard/50341.html
8. ISO/IEC 15408-2:2008. Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components. ISO. Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46414
9. ISO/IEC 15408-3:2008. Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components. ISO. Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46413
10. ISO/IEC 13335-1:2004. Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management. ISO. Available at: https://www.iso.org/ru/standard/39066.html
11. ISO/IEC 27005:2008. Information technology – Security techniques – Information security risk management. ISO. Available at: https://www.iso.org/ru/standard/42107.html
12. ISO/IEC 18028-1:2006. Information technology – Security techniques – IT network security – Part 1: Network security management. ISO. Available at: https://www.iso.org/ru/standard/40008.html
13. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. ISO. Available at: https://www.iso.org/standard/54534.html
14. ISO/IEC 27002:2013. Information technology – Security techniques – Code of practice for information security controls. ISO. Available at: https://www.iso.org/standard/54533.html
15. ISO/IEC 27003:2017. Information technology – Security techniques – Information security management systems – Guidance. ISO. Available at: https://www.iso.org/ru/standard/63417.html
16. ISO/IEC 27006:2015. Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems. ISO. Available at: https://www.iso.org/standard/62313.html
17. ISO/IEC 27032:2012. Information technology – Security techniques – Guidelines for cybersecurity. ISO. Available at: https://www.iso.org/ru/standard/44375.html
18. ISO/IEC 27035-1:2023. Information technology – Information security incident management – Part 1: Principles and process. ISO. Available at: https://www.iso.org/ru/standard/78973.html
19. ISO/IEC 27035-2:2023. Information technology – Information security incident management – Part 2: Guidelines to plan and prepare for incident response. ISO. Available at: https://www.iso.org/ru/standard/78974.html
20. ISO/IEC 27035-3:2020. Information technology – Information security incident management – Part 3: Guidelines for ICT incident response operations. ISO. Available at: https://www.iso.org/ru/standard/74033.html
21. ISO/IEC 27000:2018. Information technology – Security techniques – Information security management systems – Overview and vocabulary. ISO. Available at: https://www.iso.org/standard/73906.html
22. Große, C. (2023). A review of the foundations of systems, infrastructure and governance. Safety Science, 160, 106060. doi: https://doi.org/10.1016/j.ssci.2023.106060
23. Gorbenko, I. D., Potiy, A. V., Tereschenko, P. I. (2000). Kriterii i metodologiya otsenki bezopasnosti informatsionnykh tekhnologiy. Radiotekhnika, 114, 25–38. Available at: https://openarchive.nure.ua/items/409b6535-c863-4544-b651-801fc67b239a/full
24. The ISO/IEC Directives are published in two parts. Part 1: Procedures for the technical work. Part 2: Principles and rules for the structure and drafting of ISO and IEC documents. Available at: https://www.iso.org/sites/directives/current/part1/index.xhtml
25. Scarfone, K., Jansen, W., Tracy, M. (2008). Guide to general server security. National Institute of Standards and Technology (NIST). Available at: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf
26. Stoneburner, G., Goguen, A., Feringa, A. (2002). Risk management guide for information technology systems. National Institute of Standards and Technology (NIST). doi: https://doi.org/10.6028/nist.sp.800-30
27. Khanmohammadi, K., Houmb, S. H. (2010). Business Process-Based Information Security Risk Assessment. 2010 Fourth International Conference on Network and System Security. doi: https://doi.org/10.1109/nss.2010.37

28. Kuzminykh, I., Ghita, B., Sokolov, V., Bakhshi, T. (2021). Information Security Risk Assessment. Encyclopedia, 1 (3), 602–617. doi: https://doi.org/10.3390/encyclopedia1030050
29. Liu, C., Tan, C.-K., Fang, Y.-S., Lok, T.-S. (2012). The Security Risk Assessment Methodology. Procedia Engineering, 43, 600–609. doi: https://doi.org/10.1016/j.proeng.2012.08.106
30. Identifying Information Assets and Business Requirements. The National Archives. Available at: https://cdn.nationalarchives.gov.uk/documents/identify-information-assets.pdf
31. Martin, C., Kadry, A., Abu-Shady, G. (2014). Quantifying the financial impact of it security breaches on business processes. 2014 Twelfth Annual International Conference on Privacy, Security and Trust. doi: https://doi.org/10.1109/pst.2014.6890934
32. Lund, M. S., Solhaug, B., Stølen, K. (2011). Model-Driven Risk Analysis. Springer, 460. doi: https://doi.org/10.1007/978-3-642-12323-8
33. Matulevičius, R. (2017). Domain Model for Information Systems Security Risk Management. Fundamentals of Secure System Modelling, 17–30. doi: https://doi.org/10.1007/978-3-319-61717-6_2
34. Innerhofer-Oberperfler, F., Mitterer, M., Hafner, M., Breu, R. (2010). Security Analysis of Service Oriented Systems. Web Services Security Development and Architecture, 33–56. doi: https://doi.org/10.4018/978-1-60566-950-2.ch002
35. Innerhofer-Oberperfler, F., Breu, R. (2010). Potential Rating Indicators for Cyberinsurance: An Exploratory Qualitative Study. Economics of Information Security and Privacy, 249–278. doi: https://doi.org/10.1007/978-1-4419-6967-5_13
36. Alkubaisy, D., Piras, L., Al-Obeidallah, M. G., Cox, K., Mouratidis, H. (2022). A Framework for Privacy and Security Requirements Analysis and Conflict Resolution for Supporting GDPR Compliance Through Privacy-by-Design. Evaluation of Novel Approaches to Software Engineering, 67–87. doi: https://doi.org/10.1007/978-3-030-96648-5_4
37. Pullonen, P., Tom, J., Matulevičius, R., Toots, A. (2019). Privacy-enhanced BPMN: enabling data privacy analysis in business processes models. Software and Systems Modeling, 18 (6), 3235–3264. doi: https://doi.org/10.1007/s10270-019-00718-z
38. Malina, L., Dzurenda, P., Ricci, S., Hajny, J., Srivastava, G., Matulevicius, R. et al. (2021). Post-Quantum Era Privacy Protection for Intelligent Infrastructures. IEEE Access, 9, 36038–36077. doi: https://doi.org/10.1109/access.2021.3062201
39. Rikhardsson, P., Rohde, C., Christensen, L., Batt, C. E. (2021). Management controls and crisis: evidence from the banking sector. Accounting, Auditing & Accountability Journal, 34 (4), 757–785. doi: https://doi.org/10.1108/aaaj-01-2020-4400
40. Koeze, R. (2017). Designing a Cyber Risk Assessment Tool for Small to Medium Enterprises. TUDelft. Available at: https://repository.tudelft.nl/islandora/object/uuid:8ffae35d-0695-4eb9-b488-471bd1c9e10d/datastream/OBJ/download
41. Milov, O., Khvostenko, V., Natalia, V., Korol, O., Zviertseva, N. (2022). Situational Control of Cyber Security in Socio-Cyber-Physical Systems. 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). doi: https://doi.org/10.1109/hora55278.2022.9800049
42. Milov, O., Yevseiev, S., Zviertseva, N., Zviertsev, H., Motalyhin, Y. (2022). Pseudo-Physical Logics in Control of Cyber Security Systems. 2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). doi: https://doi.org/10.1109/ismsit56059.2022.9932711
43. SWI-Prolog. Available at: https://www.swi-prolog.org/
44. Pohasii, S., Yevseiev, S., Zhuchenko, O., Milov, O., Lysechko, V., Kovalenko, O. et al. (2022). Development of crypto-code constructs based on LDPC codes. Eastern-European Journal of Enterprise Technologies, 2 (9 (116)), 44–59. doi: https://doi.org/10.15587/1729-4061.2022.254545
45. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S. et. al.; Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.) (2021). Synergy of building cybersecurity systems. Kharkiv: PC TECHNOLOGY CENTER, 188. doi: https://doi.org/10.15587/978-617-7319-31-2