Assessing Security Risks Method in E-Commerce System for IT Portfolio Management

Myroslava Bublyk[a], Victoria Vysotska[a], Lyubomyr Chyrun[b], Valentyna Panasyuk[c] and Oksana Brodyak[a]

[a] *Lviv Polytechnic National University, S,.Bandera street, 12, Lviv, 79013, Ukraine*
[b] *Ivan Franko National University of Lviv, University street, 1, Lviv, 79000, Ukraine*
[c] *Ternopil National Economic University, Lvivska Street, 11, Ternopil, 46004, Ukraine*

Abstract

The article analyses the main methods and means of assessing the risks of information security systems in the field of in e-commerce IT projects and programs and ways of reducing these risks. One of the problematic points in application portfolio management is ensuring the information security of the content analyzed. The human factor provides an increase in unauthorized access to important information, its distortion or loss. Timely analysis of the security risk assessment of the respective portfolios of e-commerce offers significantly increases the success of the implementation and implementation of the relevant IT projects and programs. The authors propose the prediction of the results of massive risk trials in e-commerce systems. Such predictions can still made with respect to repeated sampling, based on the classical definition of probability that is provided if the experiment is relatively limited in size. This situation is relatively rare in the IS. Most often, the IS has to deal with a non-repeated sample that investigates units of rare threats. Under such conditions, the distribution of the probability of occurrence of a threat (event) is subject to the hypergeometric law. The analysis clarifies the priority of information security, allowable residual risks and costs of information security measures. Then it concludes on the allowable residual levels of risk and the feasibility of using the specific security options. It has been experimentally confirmed on 10,000 samples out of 10 attacks that in 8507 samples, no more than 8 attacks can be expected, and the greatest load on the security system falls on 2-5 series of attacks.

Keywords 1

Risks Assessment, Information Security, IT projects and programs, E-Commerce System

1. Introduction

Portfolio management of IT projects is the application of traditional management to a large class of objects, managed using information technology capabilities [1]. An example of an IT portfolio would be planned initiatives, projects, and ongoing IT services (for example, such as application support in e-commerce systems) [2]. The goal of IT portfolio management will be to quantify the previously mysterious effects of IT, thereby measuring and objectively evaluating investment scenarios [3]. Portfolio management of IT projects initially had an exclusively project-oriented bias, but as it developed, it began to include stationary activities such as application support and technical support [4]. In most cases, portfolio management of IT projects is carried out through the creation of two portfolios [2-5]:

IntelITSIS'2021: 2nd International Workshop on Intelligent Information Technologies and Systems of Information Security, March 24–26, 2021, Khmelnytskyi, Ukraine
EMAIL: my.bublyk@gmail.com (M. Bublyk); victoria.a.vysotska@lpnu.ua (V. Vysotska); Lyubomyr.Chyrun@lnu.edu.ua (L. Chyrun); v.panasiuk@tneu.edu.ua (V. Panasyuk); brodyakoksana1976@gmail.com (O. Brodyak)
ORCID: 0000-0003-2403-0784 (M. Bublyk); 0000-0001-6417-3689 (V. Vysotska); 0000-0002-9448-1751 (L. Chyrun); 0000-0002-5133-6431 (V. Panasyuk); 0000-0002-9886-3589 (O. Brodyak)

1. Application Portfolio is the management of this portfolio focuses on comparing the cost of development an e-commerce system and its value to the organization. In addition to computed tangible benefits, this comparison can be based on intangible factors such as the level of maturity of the organization, the level of user familiarity with new applications and infrastructure, and external forces such as the emergence of new technologies and the withering away of old ones.
2. Project Portfolio. This type of portfolio management specifically deals with issues related to the cost of developing innovative capacity in terms of return on investment and the reduction of "duplicate" investments in situations with possible reorganization or takeover. In the latter case, the performance of IT project portfolio managers can judged in terms of data reliability, maintenance savings, and convenience for end users, and the relative cost of new investments to replace old programs.

The methodology for managing a portfolio of IT projects is more applicable to larger IT organizations, and in small organizations, planning and management departments can perform its functions. One of the problematic points in application portfolio management is ensuring the information security of the content analyzed. The human factor provides an increase in unauthorized access to important information, its distortion or loss [6-7]. Timely analysis of the security risk assessment of the respective portfolios of e-commerce offers significantly increases the success of the implementation and implementation of the relevant IT projects and programs.

Information security (IS) e-commerce (EC) systems mean the protection of information and the infrastructure that supports it from accidental or intentional influences of a natural or artificial nature, capable of harming the owners or users of information [1]. Any breach of e-commerce information security can addressed in terms of threats, vulnerabilities and attacks. Two important conclusions can draw from the provision of information security in e-commerce [2]:

- The treatment of information security issues for different categories of entities may vary significantly, such as security for closed government organizations and business entities [3];
- Information security is not solely about protecting information. This is a fundamentally broader concept [4]. The subject of information relations may suffer (material and / or moral damage) not only from unauthorized access to information but also from damage to the system, which will cause a break in work. For many open organizations (such as training organizations), protecting information is not a top priority.

2. Related Works Review

For protect the interests of the subjects of information relations, it is necessary to combine measures of the following levels [8]:

- Legislative (laws, regulations, standards, etc.);
- Administrative (actions of the general nature of the organization performed by management);
- Procedural (specific security measures that deal with people);
- Software and technical (specific technical measures).

The legislative level is the most important for securing the EC. To this level, we include the whole set of measures aimed at creating and supporting in society a negative (including responsibility and punishment) attitude towards the violations and violators of the IS EC [1]. Most people do not commit illegal acts not because it is not technically possible, but because it is condemned and / or punished by society because it is not accepted. The most important at the legislative level is the creation of a mechanism that allows harmonizing the process of drafting laws with the progress of information technologies. Naturally, laws cannot pre-empt life, but it is important that the backlog is not too large, since in practice, this leads to a decrease in the level of IS.

The basis of the **administrative level** measures, that is, the measures developed by the management of the organization, is the security policy for e-commerce [1]. Such a security policy refers to a set of documented management decisions aimed at protecting information and its associated resources. Security policy defines the organization's strategy in the field of information security, as well as the amount of attention and the amount of resources that management deems appropriate to allocate. It is based on an analysis of the risks that are real to an organization's e-

commerce system. Once the risks have analysed and the security strategy identified, a program has put in place to ensure information security. This program allocates resources, appoints responsible persons, establishes the procedure for monitoring the implementation of the program, etc. Developing a security policy is a subtle thing, as each organization has its own specifics. It is senseless to apply the practice of closed state organizations to commercial structures. In this area, it is advisable to use the basic principles of security policy making and templates for the most important types of organizations.

Procedural level includes safety measures implemented by people. Domestic organizations have a wealth of experience in drafting and implementing procedural (organizational) measures, but the problem is that they have come from a pre-computer past and therefore require substantial revision.

The following groups of procedural measures can distinguished [8]: personnel management; physical protection; support for working capacity; responding to a security regime violation; planning of restoration works. There for each group should be a set of regulations in each organization that define staff actions. In turn, the implementation of these regulations must put into practice.

Software and technical level. According to current beliefs, at least the following security mechanisms should exist within e-commerce systems [9]: identification and authentication of users; access control; logging and auditing; cryptography; shielding; ensuring high productivity. The range of interests of entities involved in the use of EC may divided into the following main categories [10]:

- Confidentiality (protection against unauthorized access);
- Integrity (timeliness and consistency of information, its protection against destruction and unauthorized change);
- Accessibility (opportunity to receive the necessary information service within a reasonable time).

This aspect of IS is the most practiced in our country. **Privacy**, laws, regulations, years of experience in relevant services are at stake. Modern hardware and software products for portfolio management of IT projects allow closing almost all potential channels of information outflow [11].

Integrity. It can divided static (understood as the immutability of information objects) and dynamic (concerning the specific execution of complex actions (transactions)) [12]. Almost all regulatory documents and national developments are of static integrity, although the dynamic aspect is no less important. An example of dynamic integrity is controlling the flow of financial messages (detecting theft, ordering or duplication of individual messages) [13].

Accessibility. E-commerce systems are created to receive certain information services. If, for one reason or another, it becomes impossible for the users to obtain these services, it obviously harms all subjects of information relations. Therefore, without contrasting accessibility to other aspects, we highlight it as the most important element of information security [14]. Particularly vividly, the leading role of accessibility is evident in e-commerce systems based on machine learning and neuron networks such as [15]:

- Support systems for electronic interaction of various services in the preparation of aviation, rail and road flights;
- Trading systems that are designed for the organization of Internet commerce and implement seller-buyer relationships; business-to-business system, where a scheme of fully automated interaction of business processes between two organizations is implemented. These may be auctions; financial, banking, tourist, medical, insurance, information services; online billing and more.

Outwardly less dramatic, but also very unpleasant, the consequences, both material and moral, can be the long-term inaccessibility of information services used by a large number of people: the sale of rail and air tickets, banking services, etc. Thus, information security should ensure: information confidentiality, data integrity - protection against crashes leading to information loss and unauthorized creation or destruction of data, as well as accessibility of information for all authorized users [16].

Appropriate definitions must given for all the functions and tasks of the EC. Next, determine the security mechanisms that implement these functions. The main mechanisms of information security are as follows [17]: managing access to information; identification and authentication; cryptography; shielding; ensuring data integrity and availability; support of the e-commerce system in case of failures, accidents, emergencies; tracking events that may threaten IS; access control in e-commerce

systems; logging of actions and events. If a description of subsystem requirements is used, the additional requirements specified in the requirements of the selected security profile (e-commerce security class against unauthorized access) should formulated. It is possible to use a mixed approach, in which additional requirements are described in terms of security features (services). However, in order to study security in e-commerce, there are currently four classes of data exchange in e-commerce: e-mail, e-data exchange, information transactions, and financial transactions [18].

3. Information Security Problems

In the theory of information security, there is a basic theorem of system security, which is proved for many types of mathematical models of protected systems and is formulated as follows: "If the initial state of the system is safe and all transitions of the system from state to state, then the system is safe." It is quite obvious that for a securely secured EC, the terms of this theorem must be maintained at all stages of the system life cycle. The basic security theorem of the system is transformed into the basic theorem of security for the software of the system: "If the software of the system starts its operations in a safe state and all transitions of the system from state to state are safe, then all states of the system are safe." Among the main requirements for conducting commercial operations are confidentiality, integrity, authentication, authorization, guarantees and secrecy [19]. The first four requirements are provided by hardware and software, but the fulfilment of the latter two - the achievement of safeguards and secrecy - is equally dependent on both the hardware and software of individuals and organizations, and compliance with laws that protect the consumer from possible fraud. In the real world, we pay a lot of attention to physical security, and in the e-commerce world, we have to take care of data, communications and transaction security. When dealing with the Internet and Intranet network systems, there are several possible threats to keep in mind [20]:

- Data is intentionally intercepted, read or modified;
- Users intentionally identify themselves incorrectly;
- The user gets unauthorized access from one network to another.

These threats are implemented through the following vulnerabilities [9]:

- TCP / IP service vulnerabilities - a number of TCP / IP services are dangerous and may compromised by reasonable attackers. Particularly vulnerable services used in Local Area Networks (LANs) to improve network management;
- Ease of watching channels and intercepting information - most internet traffic is not encrypted. E-mail, passwords, and transferable files can be intercepted using easily accessible applications. Attackers can then use passwords to break into e-commerce systems;
- Lack of policy is many networks can configured because of ignorance so that they will allowed to access by the Internet without being aware of possible abuse. A large number of networks allow for the use of more TCP / IP services than is required for the activities of their organization. Administrators of such networks do not attempt to restrict access to information from computers. This can help intruders gain access to the network;
- Configuration complexity - Host access control resources are often difficult to set up and control. Improperly configured tools often result in unauthorized access;
- Errors in configuring host or access control resources that are either poorly installed or so complex that they are barely manageable;
- The role and importance of administering the system, which are often overlooked when describing employees' job responsibilities (most administrators are part-time and poorly trained);
- Poor authentication;
- Possibility of easy observation of transmitted data;
- Possibility of easy camouflage under others;
- Flaws of LAN services and host mutual trust in each other;
- Complexity of configuration and security measures;
- Poor host-level security.

Three different categories of actors are interested in providing information security in e-commerce: government organizations, business entities, and individuals. From a philosophical point of view, it is

possible to speak of information as an abstract substance existing in itself, but for us neither storing nor transmitting information without a tangible medium is impossible [21]. Consequently [22]:

- Information as an object of ownership is copied (copied) at the expense of the tangible medium. The tangible property object is not copied. Indeed, if we consider two identical things, they consist of the same structures, but of materially different molecules. In addition, the information when copying remains the same, it's the same knowledge, the same semantics.
- Information as a property is easily moved to another property without noticeable infringement of the property of the information. Moving a tangible object to another property right is inevitable and usually causes the loss of that property to the primary property owner, that is, a clear violation of his property right.

The risk of copying and moving information is exacerbated by the fact that it is stored and processed in the reach of a large number of non-proprietary entities. These are, for example, automated systems, including information networks. Considering the peculiarities of information, we can conclude that as an object of property rights, information is no different from traditional objects of property rights [23]. Ownership includes three components of ownership: disposal; right of ownership; the right to use. The subject of ownership of the information may transfer some of its rights (dispositions) without losing them to other entities, for example - to the owner of the material storage medium (this is possession or use) or to the user (this is use and, possibly, possession). For information, the right of disposal implies an exclusive right (none other than the owner) to determine to whom this information may be made available for possession or use.

4. Main Components of the Security in the E-Commerce

Email is a cheap way to engage with your customers, business partners and use it to address a number of security issues [24]:

- E-mail addresses on the Internet are easy to fake;
- Emails can simply modified. The standard SMTP worksheet does not contain resources for checking their integrity;
- E-mail can read at each intermediate workstation;
- There is no guarantee of email delivery. Although some mail systems provide the ability to receive delivery messages, often such messages only mean that the recipient's mail server (and not necessarily the user itself) received the message.

4.1. Electronic Data Interchange (EDI)

The simplest form is the exchange of information between two business entities (trading partners) in a standardized format. The basic unit of exchange is a set of transactions that generally corresponds to a standard business document, such as a payment order or invoice for a product. Using standards based on X.9 and UN / EDIFACT, the business community has developed a group of standard transaction sets [25]. Each set of transactions consists of a large number of data elements required for a given business document, each of which has its own format and place among other data elements. Companies began to use EDI to reduce the time and cost of contacting suppliers. For example, in the automotive industry, large companies have required suppliers to use EDI for all transactions, which has saved a lot of paper, greatly accelerated the delivery process and reduced efforts to maintain the relevance of databases. Typically, EDI transactions used private global networks, which were cheaper than dedicated lines but provided reliable and secure delivery services. The Internet can provide the interoperability required for EDI at low cost. However, it does not provide the security services (integrity, privacy, interaction control) required for EDI. EDI transactions are vulnerable to modification, compromise or destruction when transmitted over the Internet. **Information transactions** are a major and expensive element of commerce. Business information can take several forms [26]:

- Static data such as historical information, maps, etc.;
- Corporate content such as phone numbers, addresses, organization structure, etc.;

- Information about products or services;
- Paid information such as news, periodicals, access to databases, etc.

Using the Internet to provide such services is much cheaper than using fax, telephone, or regular mail. Potential clients can search and receive information at the pace they need, and this will not require additional maintenance costs [27]. Usually, such information services use the WWW as a basic mechanism for providing information. The integrity and accessibility of the information provided are major security concerns that require the use of security tools and the creation of security policies [9].

4.2. Financial transactions

One way or another, computers and networks have long used to handle financial transactions. Transferring money from account to account electronically is used for bank-to-bank transactions and ATMs for customer-bank transactions. The authorization of the buyer with the help of credit cards is performed on telephone lines and data networks [28]. For security purposes, these transactions are performed through private networks or encrypted. The use of private global networks (as for EDI) has limited the ability to interact [9]. And only the Internet provided a cheap opportunity to make financial transactions. There are three main classes of financial transactions and five important types of payment mechanism (Table 1) [1].

Table 1

Payments and financial transactions

Interaction	Cash	Check	Debit	Credit	Electronic funds transfer
Company-company		Main			Auxiliary
Company-client	Main	Auxiliary	Auxiliary	Auxiliary	
Client-client	Main	Auxiliary			

Using the Internet to perform these types of transactions allows you to replace the use of cash, checks, and credit cards with their electronic equivalents. The main definitions that apply to all classes of e-commerce security are exposure, vulnerability, attack, threat, management [29].

- **The exposure** is the form of a possible loss or loss to the EC. For example, exposures include unauthorized access to data or counteracting the authorized use of ECs.
- **The vulnerability** is some weakness of the security system, which can cause damage to the ECs.
- **An attack** is an action by an entity of a EC (user, program, process, etc.) that exploits the vulnerability of an e-commerce computer system to achieve goals that go beyond that entity's authorization on the computer system. That is, if, for example, a user does not have the right to read some of the data stored in the e-commerce system. In addition, it is interested to know them, and therefore he performs a number of known non-standard manipulations that provide access to this data (in the absence or insufficiently reliable) security work) or fail (if security work is reliable), then this user performs a EC attack.
- **The threat** to the EC is the conditions that create the potential for damage.
- **Management** in security terminology is called a security mechanism (action, device, procedure, technology, etc.) that reduces the vulnerability of the EC. It should understood that the damage to the EC is a broad concept as well. The loss includes not only the obvious damage to any of the components of the EC. Also the failure of the EC to be inoperable (such as de-energizing the premises where the hardware is located), various information leaks (e.g., illegal copying of programs, obtaining confidential data), and change of some physical and logical characteristics of the system (e.g., unauthorized addition of records to system files, etc.) Determining the possible damage to the EC is too complicated and depends on many conditions: for example, whether a lawyer is recognized in that country, so-called intellectual property or well-known Copyright, whether the courts are considering claims for moral damages suffered by a person or organization as a result of disclosure of confidential information by a third party, etc.

Ecommerce systems security issues can roughly divided into the following groups [1]:

- Problems of providing physical EC. These include the protection of systems against fire, flooding, other natural disasters, power failures, theft, damage, etc. [30].
- Problems of securing the logical security of the EC. This is to protect systems from unauthorized access. It is from intentional and unintentional errors in the actions of people and programs that could cause damage and more [31].
- Problems of ensuring the social security of the components of the EC. These include drafting legislation that regulates the use of ECs and defines the procedure for investigation and punishment for breaches of their security; the principles and rules of such an organization of customer service in the EC that would reduce the risk of system security breach, etc. [32].
- Problems of securing the ethical security of the EC. It may not seem that important to some, but many experts believe that the issue of securing users of a particular discipline and the formation of specific ethical rules that are binding on everyone who works with computers play a major role in securing EC [33]. For example, recently US National Science Foundation experts attempted to create a kind of "code of conduct" for an IS specialist, including e-commerce systems. In particular, it is stated that it was unethical to consider any intentional or unintentional acts that [1]:
    a. Disrupt the normal operation of computer systems;
    b. Cause additional resource costs (machine time, transmission lines, etc.);
    c. Destroy the integrity of information stored and processed on computer systems;
    d. Violate the interests of legal users;
    e. Cause unplanned expenditures of resources for additional control, restoration of system performance, removal of consequences of system security breach, etc.

According to the definition of IP, including e-commerce systems, its main components are hardware, mathematical (including software) and data (information) [34].

Theoretically, there are only four types of threats to these components [1]:

- **Interruption** is when an interruption occurs, a component of the system is lost (e.g. due to theft), becomes inaccessible (for example, due to blocking - physical or logical), or loses its working capacity [35];
- **Interception** is some third party has access to the component. Examples of interception are illegal copying of programs and data, unauthorized reading of data from computer network links, etc. [36];
- **Modification** is some third party not only gets access to the component, but also manipulates it. For example, modifications are unauthorized changes to data in databases or in general in files on a computer system; changing the algorithms of the programs used to perform some additional illegal processing. Sometimes modifications come out quickly enough (if not immediately), but subtler ones can remain undetected for a long time [37];
- **Imitation** is the intruder may add some false process to the system to perform the actions he needs, but not system-wide actions or fake entries in the system files or other users. For example, knowing the record format in a file that your payroll is accruing to your organization, you can put a fake entry in that file [38].

These are the basic theoretical principles necessary for further explain the whole problem of securing EC. To ensure these principles, it is necessary at the stage of design or selection of e-commerce systems to formulate requirements for the provision of information security mode in the implementation of the functions and tasks of e-commerce systems, as well as to develop the concept of IS policy [39]. At the same time, after compiling a list of functions and tasks of e-commerce systems, it is necessary to determine the requirements for providing the IS mode when implementing them. These requirements are formed in time: Availability; Integrity; Confidentiality. The development of the IS policy concept begins with the choice of the concept of e-commerce systems created / selected and conducted on the basis of the analysis of the following groups of factors [1-9]:

- Legal and contractual requirements;
- Requirements for providing the IS regime on the functions and tasks of e-commerce system;
- Threats (classes of risks) to which information resources are exposed.

As a result of the analysis, the general provisions of the IS regarding e-commerce systems in general are formulated [1-9]:

- Goals and priorities pursued by the organization in the field of IS;
- General directions in achieving these goals;
- Aspects of the IS program that need to be addressed at the organization level as a whole;
- Officials and their responsibilities for implementing the IS program.

Next, the development of the IS policy. The IS policy provides for the following steps:

- Risk analysis;
- Defining requirements for protection means;
- Choice of the main decisions on providing the IS regime;
- Developing plans to ensure the smooth running of the organization;
- Documentation of the IS policy.

Risk analysis involves the study and systematization of threats to IS, defining the requirements for security tools for IS [1] and is carried out in the following stages:

- Selection of elements of the e-commerce system and information resources for analysis. At this stage, critical system elements and critical information resources are selected that may be the target of the attack or may themselves be a potential source of maladministration [1-7].
- Development of risk assessment methodology. At this stage, the assessment of the maximum permissible and existing risk of threat for a certain period should obtained. Ideally, for each of the threats, the probability of its implementation over a period is obtained. This helps to correlate the possible loss with the cost of protection. In practice, for most threats it is impossible to obtain reliable data on the likelihood of a threat, and it has to be limited to qualitative estimates. Systematic analysis methods can used to develop risk assessment methodology.
- Threat analysis, identification of security weaknesses. A detailed list of threats is formed; a matrix of threats / elements of e-commerce systems or information resources is compiled. For each element of the matrix, a description of the possible impact of the threat on the respective element of the system or information resource is assigned. The list of threats and highlighted items is specified in the matrix assembly process.
- Risk analysis and assessment. This step involves the following steps:
    - Evaluation of the damage associated with the implementation of threats. An assessment is made of the damage that can be done by the organization to the implementation of security threats, taking into account the possible consequences of breach of confidentiality, integrity and accessibility of information;
    - An estimate of the costs of security-related activities and residual risk. A preliminary estimate of the direct costs of each event is taken into account, not including the costs of measures of a complex nature;
    - Cost / performance analysis. The costs of an information security system must weighed against the value of the protected information and other at-risk information resources, as well as the loss that may incurred by the organization through the implementation of threats.

The analysis clarifies the permissible residual risks and costs of information security measures, and then concludes on the permissible residual risk levels and the feasibility of applying specific security options. According to the results of the work, a document containing: Lists of IS threats, Risk assessments and recommendations to reduce the likelihood of their occurrence and the safeguards needed to counteract the threats.

5. Formation of Goals and Analysis of Scientific Results

When investigating the mechanisms of IS threats, the results of a separate risk assessment and recommendations are not significant. The study of the interaction of system, norm and situation is exploited by means of probability theory models, which involve the implementation of a mass experiment in which the same threat of IS (event) is repeated many times. These repetitive tests form series in which each event occurs or does not appear a certain number of times [1-5]. The choice of a

particular model for describing the risk assessment depends on the construction of the probabilistic test and, in particular, on the organization of selection from the list of its individual units.

Consider this a simple example. Let *N* events be taken from the list of IS threats, including *n* dangerous with serious consequences and m insignificant threats, and each of the events occurred at a certain interval of x_i times ($i = \overline{1,k}$, $k = n + m$, $N = \sum_{i=1}^{k} x_i$); the events took place without a certain interdependence, frequency and order. Tests involving the analysis of these events over a period can investigated using two schemes. Under the terms of the first scheme, each completed event is considered to repetitive after some time after the result of each trial is recorded in the protocol. With each subsequent study, the probability of occurrence of a particular event remains unchanged. (These probabilities are *n / N* and *m / N*, respectively.) A probabilistically threatening experiment that operates with the effects of mutually independent trials, in each of which threat events retain their unconditional probabilities, is called repeated sampling. In the implementation of the second scheme, completed events are counted as recurring. The probability of an event occurring in each subsequent trial depends on the results of the previous tests. Thus, we are dealing with dependent tests, and the probability of the result of each test is conditional. An experiment that runs on a sequence of dependent tests, each of which results in conditional probabilities, is called *a non-repetitive (or non-return) sample*. The real probabilistic threat experiment can carried out either by repeated or repeated sampling [1].

6. Proposed Methods and Materials

Investigating IS threats and conducting risk assessment uses a serial surveillance method. Its essence is that a group selects the units of threats from a fixed list: for example, 3-5 threats (events), etc. The units of threat that make up a series need not necessarily carried out one by one; they may also executed at intervals of time. When solving many theoretical and engineering problems, you often need to know the likelihood of a certain number of certain units of threat in a series. If the risk tests that form a series are considered to independent, then we can make the necessary predictions using three systems of independent tests designed in the theory of probability: *simple, polynomial, and Poisson.*

- *A simple scheme* involves only two results of the experiment: whether or not *A* appears. An example of such a scheme is a re-sampling from the list of threats to IS hazardous (*A*) and minor ($\overline{A}$) events.
- *In the polynomial scheme*, the test gives not two, but several results. Under this scheme, for example, an experiment is made to select from a list of threats of IS events of three types: with dangerous consequences, with medium consequences and minor ones.
- *In the Poisson scheme*, independent tests are performed on several sets (interruptions, interceptions, modifications, fakes), each of which has a different probability. Therefore, the likelihood of a risk outcome varies depending on which population is being tested.

The mathematical model of risk, which predicts the results of a simple test scheme, is the basis for constructing other probabilistic models, including those that are widely used in the study of the list of threats to IS.

6.1. A Simple Scheme of Independent Testing. The Bernoulli's Equation

Suppose that in some e-commerce systems, n threats are possible, in turn there are *m* dangerous threats and *n-m* insignificant ones. According to the re-sampling scheme, *N* independent tests are carried out, which consist of sequential randomly fulfilled threats from the list of possible ones. It is necessary to determine the probability of an event, which is that among the *N* threats made, *x* will be dangerous, and the order of the following dangerous and insignificant threats is indifferent.

We will consider the occurrence of a dangerous threat by event *A*, and the appearance of a minor threat by an event $\overline{A}$. We determine the probability of occurrence of dangerous and insignificant. By the classical definition of probability we have:

$$P(A) = m/n = p\,,.\; P(\overline{A}) = (n-m)/n = q$$

Now we find the probability that, for *N* independent trials, event A will appear exactly *x* times if the probability of occurrence of this event in each individual test is equal to *p*. To do this, let's put together all the possible schemas that will create a sequence of occurrence of *x* times of event *A* and times that this event does not occur, that is $AA\ldots A\,\overline{A}\;\overline{A}\ldots\overline{A}$. According to the multiplication theorem, the probability of occurrence of each scheme is $p^x q^{N-x}$, and the number of such schemes is equal to the number of compounds of *N* elements by *x*, that is C_N^x. It follows that the probability of occurrence of event *A* is equal to *x* times in a series of *N* independent trials is

$$P_N(x) = C_N^x p^x q^{N-x} = \frac{N!}{x!(N-x)!} p^x q^{N-x}, \tag{1}$$

where $p+q=1$. Note also that the probabilities (1) are equal to the corresponding members of the schedule by the formula binary expression $(q+p)^N$.

Using expression (1), called the Bernoulli formula, the probabilistic prediction of the results is performed in a simple independent test scheme.

All possible incompatible results of N experiments are the occurrence of 0, 1, 2, ..., *N* times of event *A*. Therefore, the sum of the quantities (2.1), which are separate values of probabilities at *x* = 0, 1, 2, ... , *N*, is equal to 1:

$$\sum_{x=0}^{N} P_N(x) = \sum_{x=0}^{N} C_N^x p^x q^{N-x} = (q+p)^N = 1$$

The probability distribution $P_N(x) = C_N^x p^x q^{N-x}$ at *x* = 0, 1, 2, ..., *N* is called the *binomial distribution* (or *binomial distribution law*) of probabilities. Often, in order to obtain sufficiently reliable results, a large number of independent tests have to carried out. In this case, the quantities *N* and *x* may be large enough, which makes the calculations according to the scheme just described very difficult. In such cases, the probability calculations $P_N(x)$ are made using approximate formulas.

Sometimes, to solve an information problem, it is not necessary to determine all the probabilities of the occurrence of an event 0,1,2,…,*N* times. Just indicate the most likely number of occurrences of this event. Consider the appropriate scheme. With increasing *x* magnitude $P_N(x)$ increases and with some x_0 (it is called a *modal value*) reaches its maximum value $P_N(x_0)$. After that with increasing *x*, the probability $P_N(x)$ decrease. To determine the modal value x_0, consider the behaviour of the function $P_N(x)$ by sequentially comparing two adjacent members of the distribution. Let $P_N(x_0)$ be the highest value of probability in distribution (1). Then the following two inequalities are satisfied:

$$P_N(x_0-1) \le P_N(x_0),\; P_N(x_0) \ge P_N(x_0+1). \tag{2}$$

Rewrite the first of inequalities (2) in the form

$$\frac{P_N(x_0)}{P_N(x_0-1)} = \frac{C_N^{x_0} p^{x_0} q^{N-x_0}}{C_N^{x_0-1} p^{x_0-1} q^{N-x_0+1}} = \frac{(N-x_0+1)p}{x_0 q} \ge 1. \tag{3}$$

Substituting in the last inequality *q* by *p*-1, we obtain

$$x_0 \le Np + p \tag{4}$$

Similarly, writing down the second of inequalities (2) in the form

$$\frac{P_N(x_0+1)}{P_N(x_0)} = \frac{C_N^{x_0+1} p^{x_0+1} q^{N-x_0-1}}{C_N^{x_0} p^{x_0} q^{N-x_0}} = \frac{(N-x_0)p}{(x_0+1)q} \le 1, \tag{5}$$

obsessed

$$x_0 \ge Np + p - 1 \tag{6}$$

Combining (4) and (6) results in double inequality

$$Np + p - 1 \le x_0 \le Np + p \tag{7}$$

Knowing the modal value x_0, we determine the binomial distribution probabilities we need. Calculating them starts with determining the maximum likelihood $P_N(x_0)$:

$$P_N(x_0) = C_N^{x_0} p^{x_0} q^{N-x_0} = \frac{N!}{x_0!(N-x_0)!} p^{x_0} q^{N-x_0} \tag{8}$$

The rest of the probabilities are calculated using the following recurrent formulas, which are based on expressions (3) and (5):

- If $x < x_0$

$$\left.\begin{aligned} P_N(x_0-1) &= \frac{x_0}{N-(x_0-1)} \cdot \frac{q}{p} \cdot P_N(x_0), \\ P_N(x_0-2) &= \frac{x_0-1}{N-(x_0-2)} \cdot \frac{q}{p} \cdot P_N(x_0-1), \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ P_N(x_{\min}+1) &= \frac{x_0+2}{N-x_{\min}-1} \cdot \frac{q}{p} \cdot P_N(x_{\min}+2), \\ P_N(x_{\min}) &= \frac{x_{\min}+1}{N-x_{\min}} \cdot \frac{q}{p} \cdot P_N(x_{\min}+1), \end{aligned}\right\} \tag{9}$$

- If $x > x_0$

$$\left.\begin{aligned} P_N(x_0+1) &= \frac{N-x_0}{x_0+1} \cdot \frac{p}{q} \cdot P_N(x_0), \\ P_N(x_0+2) &= \frac{N-(x_0+1)}{x_0+2} \cdot \frac{p}{q} \cdot P_N(x_0+1), \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ P_N(x_{\max}-1) &= \frac{N-(x_{\max}-2)}{x_{\max}-1} \cdot \frac{p}{q} \cdot P_N(x_{\max}-2), \\ P_N(x_{\max}) &= \frac{N-(x_{\max}-1)}{x_0+1} \cdot \frac{p}{q} \cdot P_N(x_{\max}-1), \end{aligned}\right\} \tag{10}$$

where is that: $x_{\min} \geq 0$ and $x_{\min} \geq 0$.

6.2. Polynomial Scheme

If the risk test has several results, then their probabilistic prediction is performed using a polynomial scheme. Her mathematical model is constructed like this. Suppose that some risk test may have one of *k* different incompatible outcomes A_1, A_2,..., A_k. We denote the probability of each of them respectively by $P(A_1) = p_1$, $P(A_2) = p_2$,..., $P(A_k) = p_k$. Since the event A_1 + A_2 + ... + A_k is reliable, then $p_1 + p_2 + \cdots + p_k = 1$. Let's run *N* independent tests and determine the probability that an event A_1 will occur x_1 times, an event A_2 – x_2 times, ..., an event A_k – x_k times where $x_1 + x_2 + \cdots + x_k = N$. The specified result is obtained in different ways, each of which corresponds to different rearrangements of x_1 result A_1, x_2 times, result A_2,..., x_k times of result A_k. The probability of occurrence of each such combination is equal to $p_1^{x_1} p_2^{x_2} \cdots p_k^{x_k}$. The total number of such combinations is equal to the product $C_N^{x_1} C_N^{x_2} \cdots C_N^{x_k}$ that is expressed

$$\frac{N!}{x_1! x_2! \cdots x_k!}.$$

Hence, for *N* independent tests, the probability of obtaining x_1 the result A_1, x_2 times the result A_2,..., x_k the result A_k is equal to

$$P_N(x_1, x_2, \ldots, x_k) = \frac{N!}{x_1! x_2! \cdots x_k!} \cdot p_1^{x_1} p_2^{x_2} \cdots p_k^{x_k}, \quad (11)$$

where $0 \le x_i \le N$ and $\sum_{i=1}^{k} x_i = N$. In the partial case when $k = 2$ we have $P_N(x_1, x_2) = \frac{N!}{x_1! x_2!} \cdot p_1^{x_1} p_2^{x_2}$.

Given that $x_1 + x_2 = N$, $p_1 + p_2 = 1$ and denoting x_1 by x, x_2 - through $N - x$, p_1 - through p, and p_2 - through q, we come to the expression

$$P_N(x) = \frac{N!}{x!(N-x)!} p^x q^{N-x} = C_N^x p^x q^{N-x},$$

that is, to the Bernoulli formula for a simple system of independent test schemes. Consequently, the Bernoulli formula is a partial case of (11).

Like the simple scheme, the polynomial scheme is used in repeated risk sampling, provided the values $N, x_1, x_2, \ldots, x_k$ are not very large. Under these conditions, the use of the scheme in question provides valuable information not only for the probabilistic construction of algorithms for systematic analysis of the list of IS threats in e-commerce systems. These algorithms also allow you to determine the optimal consistency of risk assessment and the implementation of recommendations to reduce the likelihood of their occurrence and the safeguards required to eliminate threats to e-commerce systems.

6.3. Poisson Scheme

In practice, IS often has to deal with such a set of threats, in which the transactions that make it belong to different types of threats (Fig. 1). As the list of threats is built based on different norms, each unit of threats has its own a priori probability in each list. As a result, the probability of occurrence and non-occurrence of certain units varies from experience to experience in e-commerce systems.

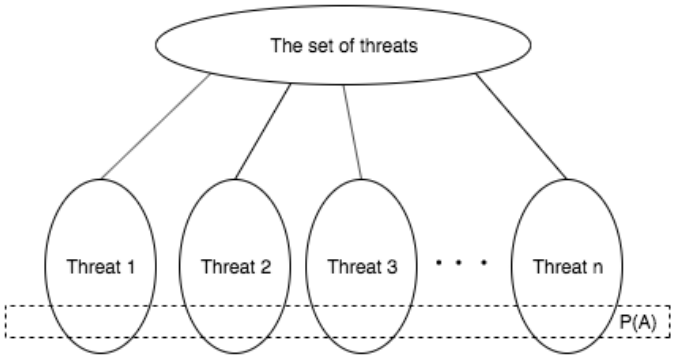

Figure 1: The Poisson scheme

This situation, depicted in the figure, is described by *the Poisson scheme*. The formal presentation of this scheme is based on the following considerations. Let *N* be independent trials, in which either event *A*. may or may not occur. The probabilities of occurrence of event *A* in 1, 2, ..., *N* trials are respectively equal $p_1, p_2, \ldots, p_N$, and the probabilities are not $q_1 = 1 - p_1$, $q_2 = 1 - p_2$, $q_N = 1 - p_N$. It can be shown that the probability of occurrence of result *A* in a series of *N* trials is *x* times equal

$$P_N(x) = p_1 p_2 p_3 \ldots p_x q_{x=1} \ldots q_N + p_1 q_2 p_3 \ldots q_{N-1} p_N + \cdots + q_1 q_2 q_3 \ldots q_{N-x} p_{N-x+1} p_{N-x+2} \ldots p_N \quad (12)$$

Thus, the required probability is the sum of all possible products, in each of which *p* with different indices is contained exactly *x* times, and *q* with different indices is included $N - x$ times. To create all possible products of *x* probabilities p_i and $N - x$ probabilities q_i $(i = 1, 2, \ldots, N)$, we create a product of binomials

$$(q_1 + p_1 t)(q_2 + p_2 t) \cdots (q_N + p_N t) = \prod_{i=1}^{N} (q_i + p_i t) \quad (13)$$

where *t* is some arbitrary parameter.

Multiply binomials and erect similar terms, then obtain equality

$$\prod_{i=1}^{N}(q_i + p_i t) = \sum_{x=0}^{N} P_N(x) t^x,$$

in which the coefficient for t^x is nothing but the expression (11).

We open the brackets on the left-hand side of the equality and reduce such terms, then we obtain all probabilities $P_N(0)$, $P_N(1)$, $P_N(2)$, ..., $P_N(N)$, which act as coefficients, respectively, at t^0, t^1, t^2, ..., t^N. The sum of all probabilities $P_N(x)$ is 1:

$$\sum_{x=0}^{N} P_N(x) = 1.$$

In particular, if $p_1 = p_2 = \ldots = p_N = p$, $q_1 = q_2 = \ldots = q_N = q$, we have

$$(q + pt)^N = \sum_{x=0}^{N} C_N^x p^x q^{N-x} t^x,$$

where the Bernoulli's Equation comes from.

The Poisson scheme, like the two previous schemes, is appropriate to use in the risk test when we can arrange re-sampling and the values of *N* and *x* are not very large. Defining the requirements for security measures and choosing the main solutions for securing the IS regime. Defining the requirements for protection means the following steps:

- Formulation of IS requirements based on an analysis of IP functions and tasks taking into account the risk analysis performed. Security requirements are formulated in terms of functions and security mechanisms;
- Selecting a security profile (e-commerce security system against unauthorized access (NSD)).
    a. In the choice of the basic decisions on providing the IS regime, the complex of measures is structured according to the levels:
        i. Administrative (ensuring the development and implementation of the IS program);
        ii. Organizational (organization of staff work and regulation of its actions);
        iii. Software-technical (software-technical implementation of security mechanisms).
    b. At the administrative level, security for IS should be developed:
        i. The system of support to the management of the organization of measures for the provision of IS, the fulfilment of legal and contractual requirements in the field of IS;
        ii. Procedure for informing employees of the basic concepts of the IS concept, requirements for training the staff of the rules of the IS;
        iii. The system of control over the implementation of the adopted decisions and responsible officials.
    c. At the organizational level, the security of IS should consider:
        i. The organizational structure of the service responsible for maintaining the IS regime, the division of responsibilities;
        ii. A set of preventive measures (prevention of the appearance of viruses, prevention of unintentional actions that lead to the violation of IS);
        iii. Organization of access of employees of third-party organizations to the resources of the e-commerce system;
        iv. Users/staff Access Organization to specific e-commerce system resources;
        v. Policy on particular aspects: remote access to e-commerce system, use of open resources, use of non-certified software (software), etc.
    d. At the software and hardware level of the IS software and hardware are considered that meet the set requirements. If the requirements are formulated in terms of security functions (services), the security mechanisms and their corresponding software and hardware implementations options are considered [16-17]. If the requirements are formulated on IP subsystems, options for hardware and software implementation of these subsystems are considered. When considering different options, we recommend that you consider the following:

i. Managing access to information and services, taking into account the requirements for the distribution of responsibilities and resources;
ii. Logging events for daily monitoring or special investigations;
iii. Check and ensure the integrity of critical data at all stages of their processing;
iv. Protection of confidential data from unauthorized access, including the use of encryption tools;
v. Backup of critical data;
vi. Restoration of the e-commerce system after failures, especially for systems with high accessibility requirements;
vii. Protection against making unauthorized additions and changes;
viii. Providing controls, for example, using programs in selective control and alternative software for repetition of critical computations.

7. Experimental Results and Discussions

For determine the characteristics of a period of systematic attacks on the ECS was randomly selected 100 time intervals of 10 attacks each [1]. The frequencies of successful attacks in these series are given in Table 2. It is necessary to calculate the theoretical binomial distribution of probabilities of x successful attacks in one series [1].

Table 2

The frequencies of successful attacks and the remaining values of the expected number of samples

Number of occurrences of the event x	Empirical frequencies of sampling S_x	$P_N(x)$	S_x^T
10	2	0.0	0
9	1	0.0001	0
8	2	0.0014	0
7	4	0.0090	1
6	11	0.0368	4
5	27	0.1029	10
4	33	0.2001	20
3	15	0.2668	27
2	4	0.2335	23
1	1	0.1211	12
0	0	0.0282	3
	ΣS_x =100	1.0	100

Here $S = 100$, $N = 10$. Using the products of x and S_x given in the table 1 [1], we find

$$p = \frac{\sum xS_x}{NS} = \frac{0\cdot 0+1\cdot 1+2\cdot 4+3\cdot 15+\cdots+8\cdot 2+9\cdot 1+10\cdot 0}{10\cdot 100} = \frac{440}{1000} = 0.44.$$

Let's take $p \approx 0.44$ and $q \approx 0.56$, then based on $Np+p-1 \le x_0 \le Np+p$ we have

$$10\cdot 0.44-0.56 < x_0 < 10\cdot 0.44-0.56+1, \text{ or } 3.84 < x_0 < 4.84,$$

whence it follows that x_0=4. Then $P_N(x_0) = P_{10}(4) = C_{10}^4 \cdot 0.3^4 \cdot 0.7^6$. From here we find that $P_{10}(4) = 0.2001$. Therefore, $S_x^T = SP_{10}(4) = 100\cdot 0.2001 \approx 20.01$. The remaining values of the expected number of samples are given in the table 3 and on Fig. 2-4 [1].

Attacks of 9-10 in the series have almost no effect on the result. Therefore, we can neglect them. Here instead of determining, and then summing up the probabilities of 0, 1, 2, ..., 8 attacks (this is nine terms) [1], let's determine the probability of 9 or 10 attacks (two terms):

$$P_{10}(9)+P_{10}(10) = 0.1493.$$

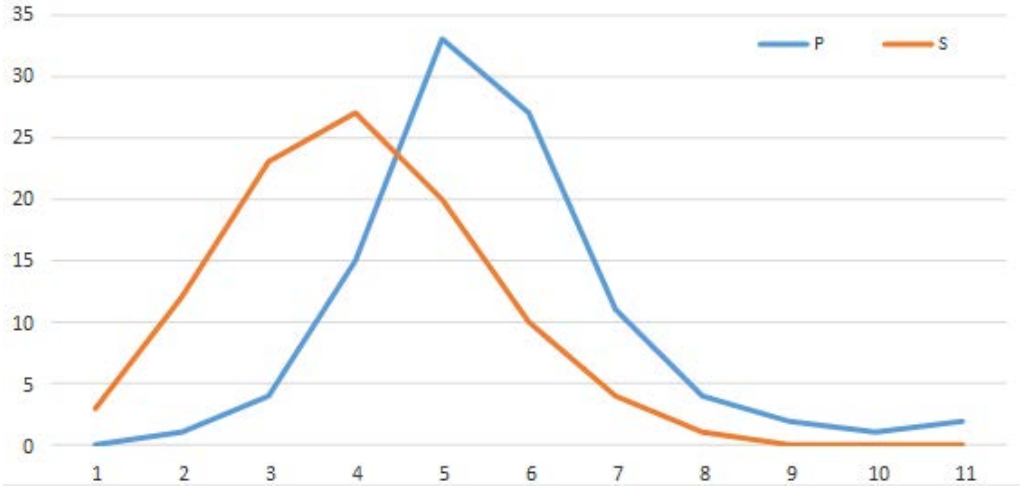

Figure 2: Graphic of the dependence of the values of the expected number of attacks series samples

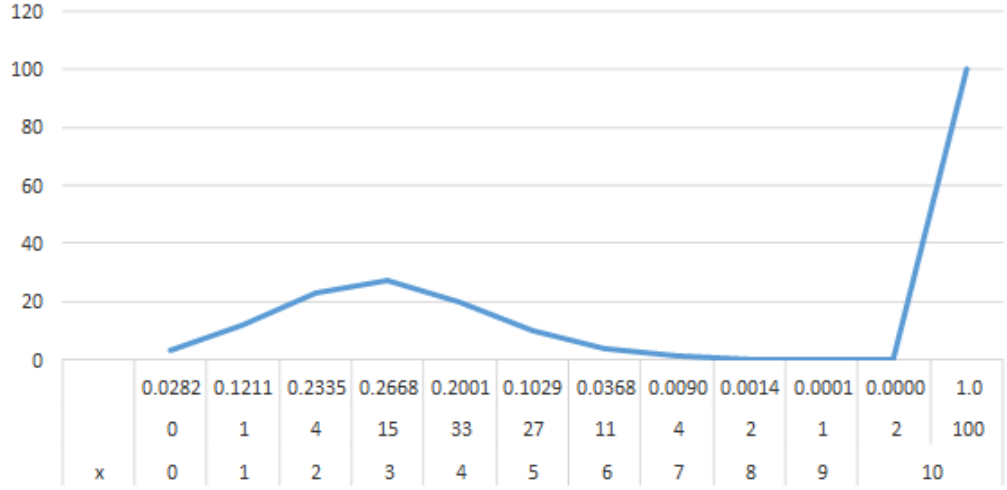

Figure 3: Graphic of the binomial probability distribution of a series of attacks

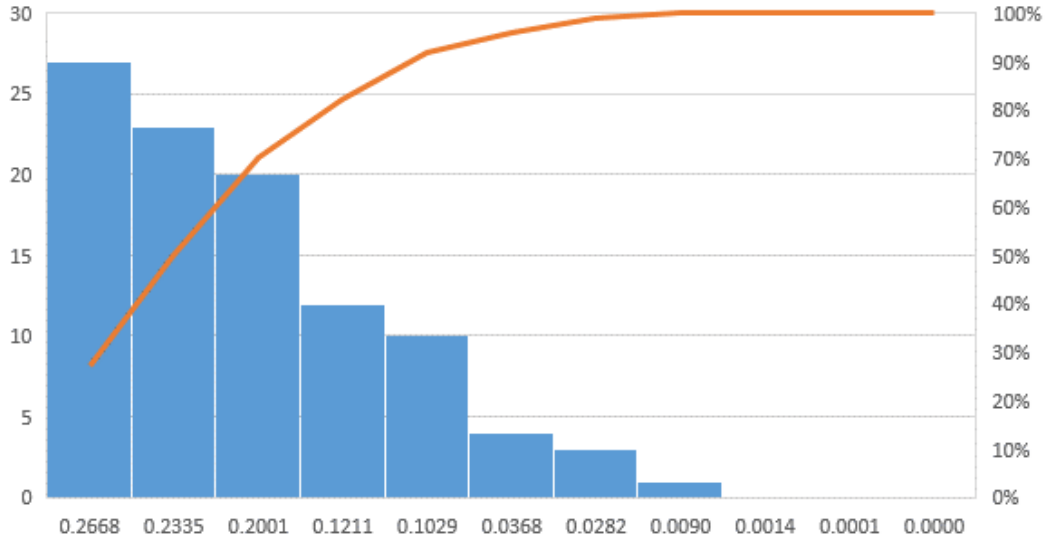

Figure 4: Pareto diagram of the distribution of a series of attacks in descending order, and on the auxiliary axis - the line of the set of values as a percentage of the total

Then the required value is calculated by the formula

$$P_{10}(x \le 8) = 1 - \left(P_{10}(9) + P_{10}(10)\right) = 1 - 0.1493 = 0.8507 .$$

In other words, if we take 10,000 samples of 10 attacks, then in 8507 samples we can expect the appearance of no more than 8 attacks and the greatest load on the security system goes to 2-5 attacks

series. By systematizing the statistics of periods of such attacks, it is possible to predict the following system loads and improve security levels in ECS.

8. Conclusion

The authors developed an approach to the analysis of qualitative (absolute frequency of attacks series on the system per a certain period) and quantitative (relative frequency of attacks series on the system per a certain period) characteristics to assess the information security risks in e-commerce systems. One of the problematic points in application portfolio management is ensuring the information security of the content analyzed. The human factor provides an increase in unauthorized access to important information, its distortion or loss. Timely analysis of the security risk assessment of the respective portfolios of e-commerce offers significantly increases the success of the implementation and implementation of the relevant IT projects and programs. It is proposed to use the method of the sequential monitoring to study information security threats and conduct risk assessments. In this case, the mathematical model of risk, which provides the results of the test for the hypergeometric law, is the basis for the construction of other probabilistic models, including those that are widely used in the study of threats to information security.

It is necessary and sufficient for ensure the protection of e-commerce information that changing the states of the system will only cause their security if the initial state was secure. To date, it may be to protect information submitted electronically from the following methods of influence: read requests, write, modify, create an object without maintaining consistency, destroy, and change its current security level. In order to effectively protect information in e-commerce systems, software hardware is used to protect the software against unauthorized access and copying.

The authors propose the prediction of the results of massive risk trials in e-commerce systems. Such predictions can still made with respect to repeated sampling, based on the classical definition of probability that is provided if the experiment is relatively limited in size. This situation is relatively rare in the IS. Most often, the IS has to deal with a non-repeated sample that investigates units of rare threats. Under such conditions, the distribution of the probability of occurrence of a threat (event) is subject to the hypergeometric law. The analysis clarifies the priority of information security, allowable residual risks and costs of information security measures. Then it concludes on the allowable residual levels of risk and the feasibility of using the specific security options. It has been experimentally confirmed on 10,000 samples out of 10 attacks that in 8507 samples, no more than 8 attacks can be expected, and the greatest load on the security system falls on 2-5 series of attacks.

In the future, it is expected to investigate the attacks series on information systems depending on period (day, week, month and season).

References

[1] A. Gozhyj, I. Kalinina, V. Vysotska, S. Sachenko, R. Kovalchuk, Qualitative and Quantitative Characteristics Analysis for Information Security Risk Assessment in E-Commerce Systems, CEUR WS 2762 (2020) 177-190.

[2] A.Y. Berko, K.A. Aliekseyeva, Quality evaluation of information resources in web-projects, 136(10) (2012) 226-234.

[3] L. Chyrun, I. Turok, I. Dyyak, Information Model of the Tendering System for Large Projects, CEUR WS 2604 (2020) 1224-1236.

[4] R. Yurynets, Z. Yurynets, D. Dosyn, Y. Kis, Risk Assessment Technology of Crediting with the Use of Logistic Regression Model, CEUR WS 2362 (2019) 153-162.

[5] M. Dyvak, N. Porplytsya, V. Brych, O. Tulai, Y. Shpak, Modeling of Dynamics of the Company's Share in the Solid Fuel Market. Proceedings of the 9th International Conference on Advanced Computer Information Technologies, ACIT, 2019, pp. 354-357. doi: 10.1109/ACITT.2019.8779973

[6] K. Karoui, Security novel risk assessment framework based on reversible metrics: a case study of DDoS attacks on an E-commerce web server, International Journal of Network Management, 26(6) (2016) 553-578. doi: 10.1002/nem.1956

[7] R. Lynnyk, V. Vysotska, Y. Matseliukh, Y. Burov, L. Demkiv, A. Zaverbnyj, A. Sachenko, I. Shylinska, I. Yevseyeva, O. Bihun, DDOS Attacks Analysis Based On Machine Learning in Challenges of Global Changes, CEUR WS 2631 (2020) 159-171.
[8] O. Trach, S. Fedushko, Determination of Measures of Counteraction to the Social-Oriented Risks of Virtual Community Life Cycle Organization, volume 1080 of Advances in Intelligent Systems and Computing, 2020, pp. 680-695. doi: 10.1007/978-3-030-33695-0_46
[9] Y. Matseliukh, V. Vysotska, M. Bublyk, Intelligent System of Visual Simulation of Passenger Flows, CEUR WS 2604 (2020) 906-920.
[10] H. Tsague, B. Twala, Investigation of carrier mobility degradation effects on mosfet leakage simulations, International Journal of Computing, 15(4) (2016) 237-247.
[11] Z. Li, Z. Li, Y. Shen, G. Zhang, Application of Combined Evaluation Method Based on Comprehensive Weight and Gray-fuzzy Theory in Network Security Risk Assessment, in: Proceedings of the International Conference on Computing Technology, Information Security and Risk Management, CTISRM, 2016, p. 38.
[12] T. I. Buldakova, D. A. Mikov, Comprehensive approach to information security risk management, CEUR WS 2081 (2017) 21-26.
[13] M. F. Ak, M. Gul, AHP–TOPSIS integration extended with Pythagorean fuzzy sets for information security risk analysis, Complex & Intelligent Systems 5(2), (2019) 113-126. doi: 10.1007/s40747-018-0087-7
[14] B. Rusyn, R. Torska, M. Kobasyar, Application of the cellular automata for obtaining pitting images during simulation process of their growth, volume 242 of Advances in Intelligent Systems and Computing, 2014, pp. 299-306. doi: 10.1007/978-3-319-02309-0_32
[15] V. Morozov, O. Kalnichenko, O. Mezentseva, The method of interaction modeling on basis of deep learning the neural networks in complex IT-projects, International Journal of Computing 19(1) (2020) 88-96. doi: 10.47839/ijc.19.1.1697
[16] O. Chereshnyuk, V. Panasyuk, S. Sachenko, A. Banasik, I. Golyash, Fuzzy-multiple Approach in Choosing the Optimal Term for Implementing the Innovative Project, in International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 2017, pp. 533-537. doi: 10.1109/IDAACS.2017.8095138
[17] A. P. H. de Gusmão, L. C. e Silva, M. M. Silva, T. Poleto, A. P. C. S. Costa, Information security risk analysis model using fuzzy decision theory, International Journal of Information Management 36(1) (2016) 25-34. doi: 10.1016/j.ijinfomgt.2015.09.003
[18] Z. Wu, L. Wang, Trustworthiness Measurement of E-commerce Systems Using Fuzzy Hybrid Multi-criteria Analysis, Trustcom/BigDataSE/ISPA 1 (2015) 668-675. doi: 10.1109/Trustcom.2015.433
[19] A. G. Kravets, N. Salnikova, K. Dmitrenko, M. Lempert, Industrial Cyber-Physical Systems: Risks Assessment and Attacks Modeling, Cyber-Physical Systems: Industry 4.0 Challenges, Springer, Cham. 2020, pp. 197-210. doi: 10.1007/978-3-030-32648-7_16
[20] A. Elzamly, B. Hussin, A comparison of fuzzy and stepwise multiple regression analysis techniques for managing software project risks: Implementation phase, International Management Review 10(1) (2014) 43-54. doi: 10.3844/jcssp.2014.1725.1742
[21] R. J. Chapman, The rules of project risk management: Implementation guidelines for major projects, Routledge, 2019, ISBN: 9780367209322
[22] M. Loosemore, E. Cheung, Implementing systems thinking to manage risk in public private partnership projects, International Journal of Project Management 33(6) (2015) 1325-1334. doi: 10.1016/j.ijproman.2015.02.005
[23] Y. Liu, H. Ma, Z. Liu, H. Hui, Research on the evaluation system of E-commerce specialty based on TOPSIS and analytic hierarchy process, Revista de la Facultad de Ingenieria 32(4) (2017) 626-632.
[24] A. A. Al-Bakri, M. I. Katsioloudes, The factors affecting e-commerce adoption by Jordanian SMEs, Management Research Review 38(7) (2015) 726-749. doi:10.1108/MRR-12-2013-0291
[25] Y. Priyadi, Suhardi, The Designing of Measurement Instrument for Information Technology Risk Assessment as a Risk Management Strategy Recommendation at SBUPE Bandung, International Journal of Science and Research 4(4) (2015) 3058-3063. doi: 10.21275/sub153803

[26] H. Beheshti, M. Alborzi, Using fuzzy logic to increase the accuracy of e-commerce risk assessment based on an expert system, Engineering, Technology & Applied Science Research 7(6) (2017) 2205-2209. doi: 10.48084/etasr.1479
[27] A. P. H. de Gusmão, M. M. Silva, T. Poleto, L. C. e Silva, A. P. C. S. Costa, Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory, International Journal of Information Management 43 (2018) 248-260. doi: 10.1016/j.ijinfomgt.2018.08.008
[28] Y. Li, H. Zhao, L. Zhu, Research on the Construction of E-commerce Security Risk Assessment Model Based on Cloud Computing, in: Proceedings of the 11th International Conference on Measuring Technology and Mechatronics Automation, ICMTMA, 2019, pp. 589-592. doi: 10.1109/ICMTMA.2019.00135
[29] M. Alali, A. Almogren, M. M. Hassan, I. A. Rassan, M. Z. A. Bhuiyan, Improving risk assessment model of cyber security using fuzzy logic inference system, Computers & Security 74 (2018) 323-339. doi: 10.1016/j.cose.2017.09.011
[30] S. Islam, H. Mouratidis, E. R. Weippl, An empirical study on the implementation and evaluation of a goal-driven software development risk management model, Information and Software Technology 56(2) (2014) 117-133. doi:10.1016/j.infsof.2013.06.003
[31] Z. Song, Y. Sun, J. Wan, L. Huang, J. Zhu, Smart e-commerce systems: current status and research challenges, Electronic Markets 29(2) 2019 221-238. doi: 10.1007/s12525-017-0272-3
[32] D. Maček, I. Magdalenić, N. B. Ređep, A Systematic Literature Review on the Application of Multicriteria Decision Making Methods for Information Security Risk Assessment, International Journal of Safety and Security Engineering 10(2) (2020) 161-174. doi: 10.18280/ijsse.100202
[33] A. Rzheuskyi, O. Kutyuk, O. Voloshyn, A. Kowalska-Styczen, V. Voloshyn, L. Chyrun, S. Chyrun, D. Peleshko, T. Rak, The Intellectual System Development of Distant Competencies Analyzing for IT Recruitment, Advances in Intelligent Systems and Computing, 2018, Springer, Cham, 2020, pp. 696-720. doi: 10.1007/978-3-030-33695-0_47
[34] V. Andrunyk, V. Pasichnyk, N. Antonyuk, T. Shestakevych, A Complex System for Teaching Students with Autism: The Concept of Analysis. Formation of IT Teaching Complex, volume 1080 of Advances in Intelligent Systems and Computing, Springer Nature Switzerland AG, Springer, Cham, 2020, pp. 721-733. doi: 10.1007/978-3-030-33695-0_48
[35] M. Bublyk, O. Rybytska, A. Karpiak, Y. Matseliukh, Structuring the fuzzy knowledge base of the IT industry impact factors, in: Proceedings of the Computer sciences and information technologies (CSIT), 2018. doi: 10.1109/STC-CSIT.2018.8526760
[36] O. Garasym, L. Chyrun, N. Chernovol, A. Gozhyj, V. Gozhyj, I. Kalinina, B. Rusyn, L. Pohreliuk, M. Korobchynskyi, Network Security Analysis Based on Consolidated Threat Resources, CEUR WS 2604 (2020) 1004-1018.
[37] S. Sachenko, S. Rippa, I. Golyash, Improving the Information Security Audit of Enterprise Using XML Technologies. Proceedings of the Inretnational Conference on Intelligent Data Acquisition and Advanced Computing Systems:Technology and Applications, 2011, pp. 933-937. doi: 10.1109/IDAACS.2011.6072879
[38] O. Kehret, A. Walz, A. Sikora, Integration of hardware security modules into a deeply embedded TLS stack, International Journal of Computing 15(1) 2016 22-30. doi: 10.47839/ijc.15.1.827
[39] V. Kharchenko, Y. Ponochovnyi, A. Abdulmunem, A. Boyarchuk, Security and availability models for smart building automation systems, International Journal of Computing 16(4) (2017) 194-202. doi: 10.47839/ijc.16.4.907