THE MINISTRY FOR DEVELOPMENT OF INFORMATION
TECHNOLOGIES AND COMMUNICATIONS OF
THE REPUBLIC OF UZBEKISTAN

TASHKENT UNIVERSITY OF INFORMATION TECNOLOGIES

As the manuscript

UDK 004.056

Oripov Pulatjon Xoldorali ugli

Developing the method of detection of attacks and controlling probability of risks in information system

5A330302 – Information security

Dissertation
is written for taking the degree
master academic

Scientific advisor:
d.t.s. Z.Z.Sharipov

CONTENT

INTRODUCTION

For solving the problems on the computerization of society, the development of information technology and security June 27, 2013y DP-1989 Decree of the President of the Republic of Uzbekistan "On measures for further development of the National Information and Communication System of the Republic of Uzbekistan" was adopted. The measures defined by the Decree, the establishment of national systems provide information, conditions for mass adoption in the economy and the life of every member of society, computer and information technologies increase the competitiveness of the domestic economy in the world market [1].

Rationale and relevance of the topic of the dissertation. In our country, under the leadership of the President acceleration of the development of information and communication technologies, the expansion of interactive services provided by public authorities to the population, the establishment of e-government are working actively. One of the latest guidelines in this area is Decree of the President of the Republic of Uzbekistan № PP-2158 on April 3, 2014 "On measures to further the implementation of information and communication technologies in the real economy" [2], which sets out a list of activities, with specific projects, performers and timing of their implementation planned for 2014-2015. Along with the acceleration of the development and implementation of information and communication technologies in various areas of the state, enough attention is paid to information security posed by information systems in our country. Evidence of this should be considered as the organization of a special state body coordinating those issues special government decision Decree of the Cabinet of Ministers № 250 of the PCM-16 September 2013 "On measures to further the implementation of information and communication technologies in the real economy" [3], in the light of implementation measures defined by these directives, one of the pressing issues on the current stage of development and implementation of information and communication technologies in our country, as well as solving problems of information security in general, and the construction of information security management systems (ISMS). One of the most important tasks is the definition of the ISMS security threats. A particular issue is the question of the definition of threats to information security risk identification and management, which is the subject of this work.

Degree researching of the problem.

Till now several researches have been done in this field, for instance: software CRAMM it is prepared by Great Britain, it includes analyzing of evaluation risks and risk management. In addition to, RiskWatch company's software which is based on analyze of probability attacks and estimating them , was created also we can take the method of controlling risks by Microsoft corporation.

The goal of the research. Analyses of determine attacks and risk management methods and development new algorithm module which was adopted Uzbek standards.

Hypothesis of the research, if the new algorithm implement for companies estimating the threats to those companies, controlling risks will be more expeditions and the algorithm, which we developed, will be effective method to treat attacks.

The tasks:

-Developing methodology based on International Standard BS7799 and national standard ISO 27005.

-Analyzing determination attacks and risk management methods in IT.

-Creating the algorithm which is based on detecting attacks and controlling risks

-Developing software focus on assessment asset's criticality degree

A brief review of literature on the subject of research following groups of sources can be carried out. The works of authors, who are Zegzhda P.D, Torokina A.A, Shirokov V.V, and Iwashko A.M, were devoted to the theory and practice of information security and the basics of engineering and technical protection of information, maintenance of information in the data processing systems. Mathematical methods of risk assessment, methods of reflecting on the change of the value of the risk, the procedures to ensure the construction of the risk management system of information security were considered in the works of Petrenko S.A, Simonov S.V Baranov A.V. and Berezin A.S. The greatest interest is derived from the work of Astakhov A, Lukatskii A.V, Vikhoreva S.V. and Kaspersky E, which consider various ways of classifying detection of attacks and threats. In addition to, we can see, in NISIT(National Institute of Standards and Technology), Microsoft corporation, company of RiskWatchs' scientific researches. In the works of Uzbek scientists Bekmuratov TF, Ganiev S.K and Karimov M.M, we investigated intelligent algorithms for constructing information security systems, the general theory of information security hardware and software to protect information.

Research methodology - system analysis, principles of management system of information security. Research methods: Theory of information protection, formalization of threat analysis and risk assessment information.

Researching of object. Business companies, state owned companies and any object who has information system.

Subject of research, Architucture of information systems, architecture of organizational protecting system, software-tools and device recourses, probability risks on organizations.

Scientific novelty of the research has created new model of algorithm which is different from other algorithms. The new model includes virtual system, which can be beneficial for the security of internal network. Difference of my model from others is that it has IDPS system that is able to check both internal and virtual system and send messages to ITA agent or administrator.

Publication, 2 thesis: Quality of probability risks assessment in information technologies, and one article: counting of assets value on protecting information.

In the first chapter of the dissertation, ways of providing security, international standard on controlling information security and risks BS7799-2:2009, national standard is ISO 27005:2011, recommendation of famous companies and software like methods which Microsoft companies suggested on controlling threats and software provided by RiskWatch company's on controlling threats have been learned.

The composition of work. This dissertation work consists of an introduction, three chapters, conclusion, literatures and appendix. In addition, there are 16 Figures, one table, 8 forms. Total dissertation pages are 96.

CHAPTER I.

RESEARCHES FOR CONTROL OF PROBABILITY THREATS IN INFORMATION SYSTEMS

Security Standards

Recognition for due care, due diligence and legal compliance, for the adequate protection of information assets, is a universally acknowledged business requirement for organizations of all types and sizes worldwide. Certification against well-known standards is the key to obtaining that recognition.

1.1. Overview international and national Standards of information security management. BS7799 standard.

BS7799 is actually "a comprehensive set of controls comprising best practices in information security". It is an internationally recognized information security standard.

The British Standard has been prepared for business managers and their staff to provide a model for setting up and managing an effective Security Management System (ISMS). The adoption of ISMS should be a strategic decision for an organization.

BS7799 gives recommendations for information security management for use by those who are responsible for initiating, documenting, implementing or maintaining security in their organization. BS7799 also specifies requirements for establishing, implementing and documenting systems of information security management.

The standard is intended to provide a common basis for developing organizational security standards and effective security management practices. It specifies requirements for security controls to be implemented according to the needs of individual organizations. In addition, this ensures that controls are effective–a valuable tool for both the IT Department and IT Audit community.

BS 7799 help to identify manage and reduce the range of threats to which information is continually exposed. Once compliance to, they provide organizations with the assurance and satisfaction of knowing that they are protecting their information using controls in common use by well-managed businesses. It is an excellent framework for developing or enhancing an organization’s security structure.

Certification and Compliance

Compliancy with BS7799-2 requires an organization to have implemented and documented their Information Security Management System (ISMS) in accordance with the control objectives set outlined in the BS7799-2:2002 documentation. BS7799-2 certification provides evidence and assurance that an organization has complied with the control objectives set out in the standards documentation. Certification outlines the scope of an organizations ISMS, and any exclusions to the control objectives.

In order to reach certification, organization must first achieve compliancy as set out in the BS 7799-2:2002 guideline. Once this has been achieved, the certification process requires an external review of by a BS7799 accredited auditor.

The auditor will work for a certified body or BSI; they will audit the organizations ISMS in line with the controls set out in the BS 7799-2:2002. On successful completion of the audit, organization will be awarded the BS7799-2 certificate.

The certificate will detail the scope of organizations ISMS and statement of applicability (SOA).

The model introduced by BSI, known as the “Plan-Do-Check-Act” (PDCA). This model can be applied to all ISMS processes.

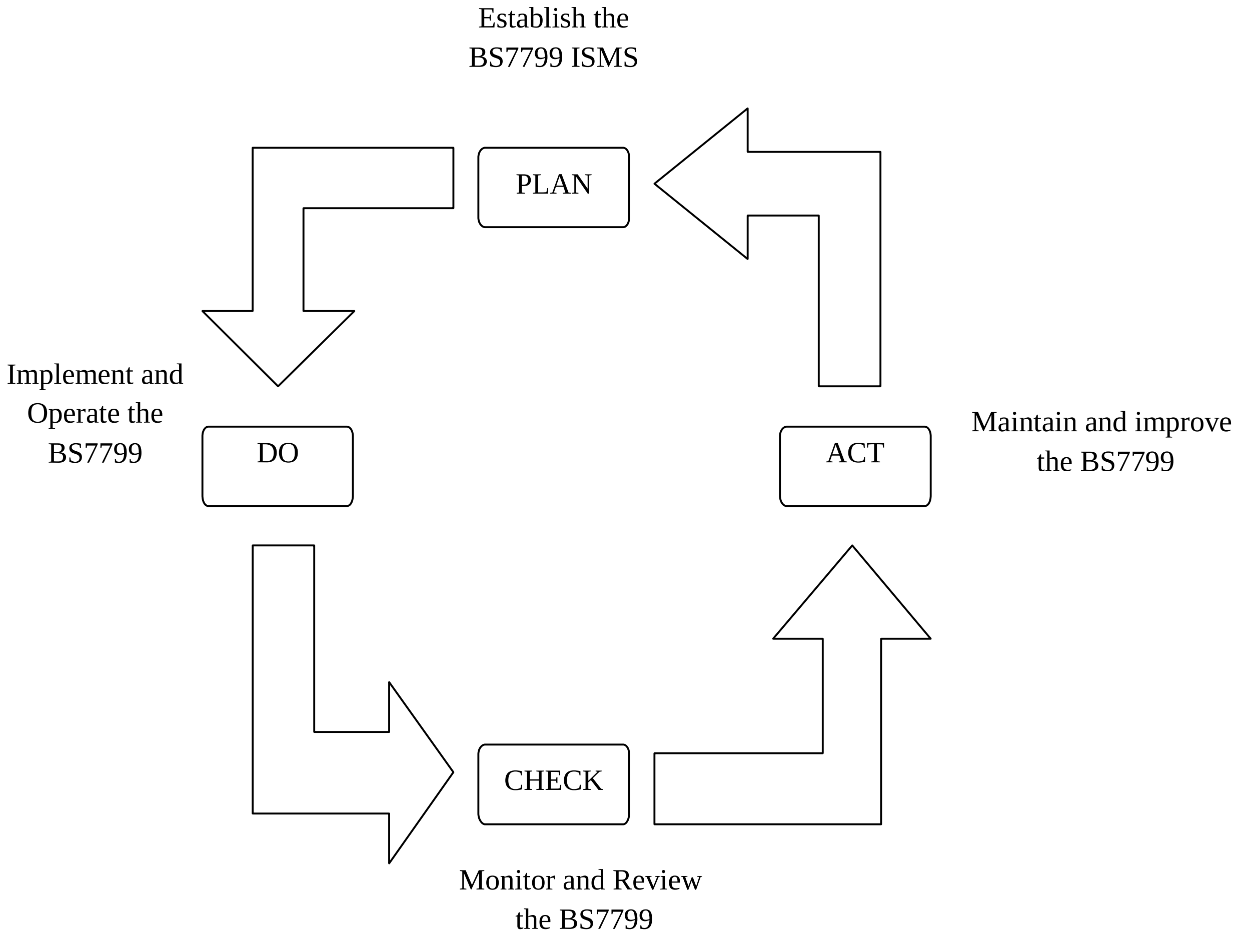


Figure 1. The module “Plan-Do-Check-Act”

Overview of BS7799 Implementation Process

1. Define the ISMS Scope (Boundary)
2. Define Information Security Policy
3. Define required Procedures and Guidelines
4. Perform Risk Assessment
5. Select objectives and controls to be implemented
6. Prepare statement of Applicability (SOA)
7. Regular Review and Internal Audits

Define the ISMS Scope:

Define the scope of the ISMS in terms of characteristics of the business, the organization, its location, assets and technology. The ISMS may cover all or part of an organization. Dependencies, interfaces and assumptions concerning the boundary with the environment need to be clearly identified. This is particularly relevant if only part of an organization is within the scope of the BS7799 ISMS.

Define Information Security Policy:

As building a good security, policy provides the foundations for the successful implementation of ISMS, without a doubt this major measure must be taken to reduce the risk of unacceptable use of any of the company's information resources.

The first step towards enhancing a company's security is the introduction of an enforceable security policy, informing staff on the various aspects of their responsibilities, general use of company resources and explaining how sensitive information must be handled. The policy will also describe in detail the meaning of acceptable use, as well as listing prohibited activities.

The development (and the proper implementation) of a security policy is highly beneficial as it will not only turn all of staff into participants in the company's effort to secure its Information’s but also help reduce the risk of a potential security breach through mistakes. These are usually issues such as revealing information to unknown (or unauthorized sources), the insecure or improper use of the Internet and many other activities.

The Information Security Policy contains the IT security objectives which the organization has set itself and the IT security strategy it pursues. In this way it constitutes both an aspiration and a statement that the IT security level specified is to be achieved at all levels of the organization.

The document acts as a "must read" source of information for everyone using in any way systems and resources defined as potential targets.

In order to realize the importance of a security policy, staff need to be aware and fully understand the consequences of violating the policy, thereby exposing critical systems to a malicious attacker, or causing unintended damage to other companies worldwide. Violations should be handled accordingly; those who in one way or the other violate the security policy should be made aware that they may face being put through a "trial period", which involves also the limited use of some of the company information assets until they can show they are able to act in a secure manner while using the corporate systems. They should also be aware that in some cases they also may risk being fired.

Define necessary Standards, Procedures and Guidelines:

Standards are definite requirements that an organization should put forth for everybody to follow. The standards should support the security policy and be measurable. It is good practice to document what the penalties are when standards are not met. Guidelines are recommended ideas for an enterprise. They can also be termed as ‘nice to haves’. It should be noted that the effectiveness of an organization’s security management will not be measured by the guidelines present. There, usually, are no penalties for not following the guidelines. However, there can be some incentives if the enterprise follows the guidelines.

Procedures are step by step description on how to meet the standards or guidelines so that the policy is supported. Procedures are usually targeted at the system level people who actually implement the control.

Perform Risk Assessment

Risk assessment is a fundamental prerequisite of BS7799-2. The standard does not require to use any particular approach, nor does it list any approved methods. Choose a method that is appropriate to organization and the scope of ISMS.

Whatever methodology choose to adopt, as an absolute minimum should ensure that it delivers the control environment that is documented within the policies and procedures of organization’s own information security manual.

As in any other sensitive procedure, Risk Analysis and Risk Management play an essential role in the proper functionality of the process. Risk Analysis is the process of identifying the critical information assets of the company and their use and functionality an important (key) process that needs to be taken very seriously. Essentially, it is the very process of defining exactly WHAT you are trying to protect, from WHOM you are trying to protect it and most importantly, HOW you are going to protect it.

The risk assessment documentation should explain which risk assessment approach has been chosen, and why this approach is appropriate to the security requirements, the business environment, and the size of the business and risk the organization faces. The approach adopted should aim to focus security effort and resources in a cost-effective and efficient way. The documentation should also cover the tools and techniques that have been chosen explain why they are suitable for the ISMS scope and risks, and how they should be used correctly to produce valid results.

The objective of a risk assessment, in the context of BS7799, is to balance the safeguards identified in the Statement of Applicability against the risk (i.e. probability) of failing to meet business objectives.

Implementing sound strategies for managing information security risks is vital given the scarcity of resources and budgets, and the need to keep abreast of organizations need to get services and products to market as quickly as possible.

Designing and implementing an appropriate risk management strategy requires the assistance of a number of people within an organization, such as staff from business areas, technology, personnel, finance, legal etc.

In order to be able to conduct a successful Risk Analysis, need to get well acquainted with the ways a company operates; if applicable, the ways of working and certain business procedures, which information resources are more important than others (prioritizing), and identifying the devices / procedures that could lead to a possible security problem.

List everything that is essential for the proper functionality of the business processes; like key applications and systems, application servers, web servers, database servers, various business plans, projects in development, etc.

A possible list of categories to look at would be:

- Hardware: All servers, workstations, personal computers, laptops, removable media (CD's, floppies, tapes, etc.), communication lines, etc.
- Software: Identify the risks of a potential security problem due to outdated software, infrequent patches and updates to new versions, etc. Also take into account the potential issues with staff installing various file sharing apps, entertainment or freeware software coming from unknown and untrustworthy sources.
- Personnel: Those who have access to confidential information, sensitive data, those who "own", administer or in any way modify existing databases.

What are the risks? Determine these by a consideration of the impacts that would occur if some threat exploits a weakness in defenses to compromise the security of an asset, and how likely is the impact to occur.

Risk assessment is systematic consideration of:

a) The valuation of the assets within the ISMS, including information about the valuation scale used when it is not monetary.

b) Identification of threats and vulnerabilities

c) The business harm likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets.

d) The realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented.

The results of this assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks.

It is important to carry out periodic reviews of security risks and implemented controls to:

a) take account of changes to business requirements and priorities;

b) consider new threats and vulnerabilities;

c) Confirm that controls remain effective and appropriate.

Reviews should be performed at different levels of depth depending on the results of previous assessments and the changing levels of risk that management is prepared to accept. Risk assessments are often carried out first at a high level, as a means of prioritizing resources in areas of high risk, and then at a more detailed level, to address specific risks.

Information Security Risk Management Stages in Risk Management Methodology:

monetary factors such as loss of reputation should also be taken into account.

It might not always be possible to reduce risks to an acceptable level within an acceptable cost, and then a decision should be made whether to add more controls, or accept the higher risks. When setting an acceptable level of risk the strength and cost of control should be compared with potential cost of an incident.

A number of controls can be considered as guiding principles providing a good starting point for implementing information security. They are either based on essential legislative requirements or considered to be common best practice for information security. Controls considered being essential to an organization from a legislative point of view.

Select Control Objectives and Controls to be implemented

Once security requirements have been identified, security controls should be selected and implemented to ensure risks are reduced to an acceptable level.

Controls can be selected from BS7799-2:2002 control sets, or new controls can be designed to meet specific needs as appropriate. It is necessary to recognize that some of the controls are not applicable to every information system or environment, and might not be practicable for all organizations.

Controls should be selected based on the cost of implementation in relation to the risks being reduced and the potential losses if a security breach occurs. Nonmonetary factors such as loss of reputation should also be taken into account.

It might not always be possible to reduce risks to an acceptable level within an acceptable cost, and then a decision should be made whether to add more controls, or accept the higher risks. When setting an acceptable level of risk the strength and cost of control should be compared with potential cost of an incident.

A number of controls can be considered as guiding principles providing a good starting point for implementing information security. They are either based on essential legislative requirements or considered to be common best practice for information security. Controls considered being essential to an organization from a legislative point of view.

BS7799-2:2002 Contains 36 Control Objectives and 127 Controls. And broadly divided into 10 Detailed Control Clauses:

1. Security Policy
2. Organization Security
3. Asset classification and control
4. Personnel Security
5. Physical & environmental security
6. Communications and operations management
7. Access control
8. Systems development and maintenance
9. Business continuity management
10. Compliance

Prepare statement of Applicability (SOA):

An organization will need to document the selected control objectives and controls, the reasons for selection and justification for the exclusion of any of the controls listed in the BS 7799-2:2002. Not all the controls described will be relevant to every situation, nor can they take account of local environmental or technological constraints, or be present in a form that suits every potential user in an organization. Organizations need to identify the most appropriate control objectives and controls to be implemented which are applicable to their own needs.

Having defined the SOA meant that the Organization could now focus on the areas of security that required improvements. This was a tremendous help and meant that the organization had a clear starting point and clear direction to take in addressing some of the security issues identified through the Risk Assessment.

The statement of applicability needs to be accessible to managers; personnel and any third party (auditors, etc.) authorized to have access to it.

Regular Review and Internal Audits

Auditing is the review and analysis of management, operational, and technical controls.

The security of information systems should be regularly reviewed. Such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with security implementation standards.

Properly defined Internal Audit will explain organizations current compliance position with respect to each section of BS 7799. A follow-up audit can determine the success which is achieved by the implementing appropriate actions.

1.2. National Risk management standard ISO 27005:2011

ISO 27005 has been prepared by International Standard Organization(ISO).Country of origin is International (place of business in Switzerland).

ISO 27005:2011 provides an iterative process for risk management, which advances to be the framework for several methodologies in the domain of risk management.

The risk management process, proposed by the standard, includes context establishment, risk assessment, risk treatment, risk communication, consultation, monitoring and review (see process in Figure 2).

The context establishment includes:

• Setting basic criteria such as the risk management approach, the risk evaluation criteria, the impact criteria and the risk acceptance criteria;

• Defining the scope and boundaries of the risk management;

• Defining the organization and the responsibilities for information security risk management.

The risk assessment consists of:

• The risk identification which has the aim to find possible sources of potential

– The assets within the defined scope;

– The threats and their sources;

– Existing and planned controls;

– Vulnerabilities that can be abused by threats having a negative impact to assets or to the organization;

– The consequences that a loss of confidentiality, integrity and availability may have on the assets.

– Business processes

• The risk analysis/estimation which includes:

– The selection of the risk analysis methodology which can be qualitative

(using a scale of qualifying attributes, e.g. Low, Medium and High), quantitative (using a scale with numerical values) or depending on the situation a mixture of both;

– Assessment of consequences and more precisely the business impact of a security incident with loss of confidentiality, integrity or availability of the assets;

– Assessment of incident likelihood by evaluating threats and vulnerabilities;

– Determination of the risk level for all relevant incident scenarios.

• The risk evaluation has the aim to compare the level of risk against the risk evaluation criteria and the risk acceptance criteria (defined in the context establishment).

– Vulnerabilities that can be abused by threats having a negative impact to assets or to the organization;

– The consequences that a loss of confidentiality, integrity and availability may have on the assets.

– Business processes

• The risk analysis/estimation which includes:

– The selection of the risk analysis methodology which can be qualitative

(using a scale of qualifying attributes, e.g. Low, Medium and High), quantitative (using a scale with numerical values) or depending on the situation a mixture of both;

– Assessment of consequences and more precisely the business impact of a security incident with loss of confidentiality, integrity or availability of the assets;

– Assessment of incident likelihood by evaluating threats and vulnerabilities;

– Determination of the risk level for all relevant incident scenarios.

• The risk evaluation has the aim to compare the level of risk against the risk

evaluation criteria and the risk acceptance criteria (defined in the context establishment).

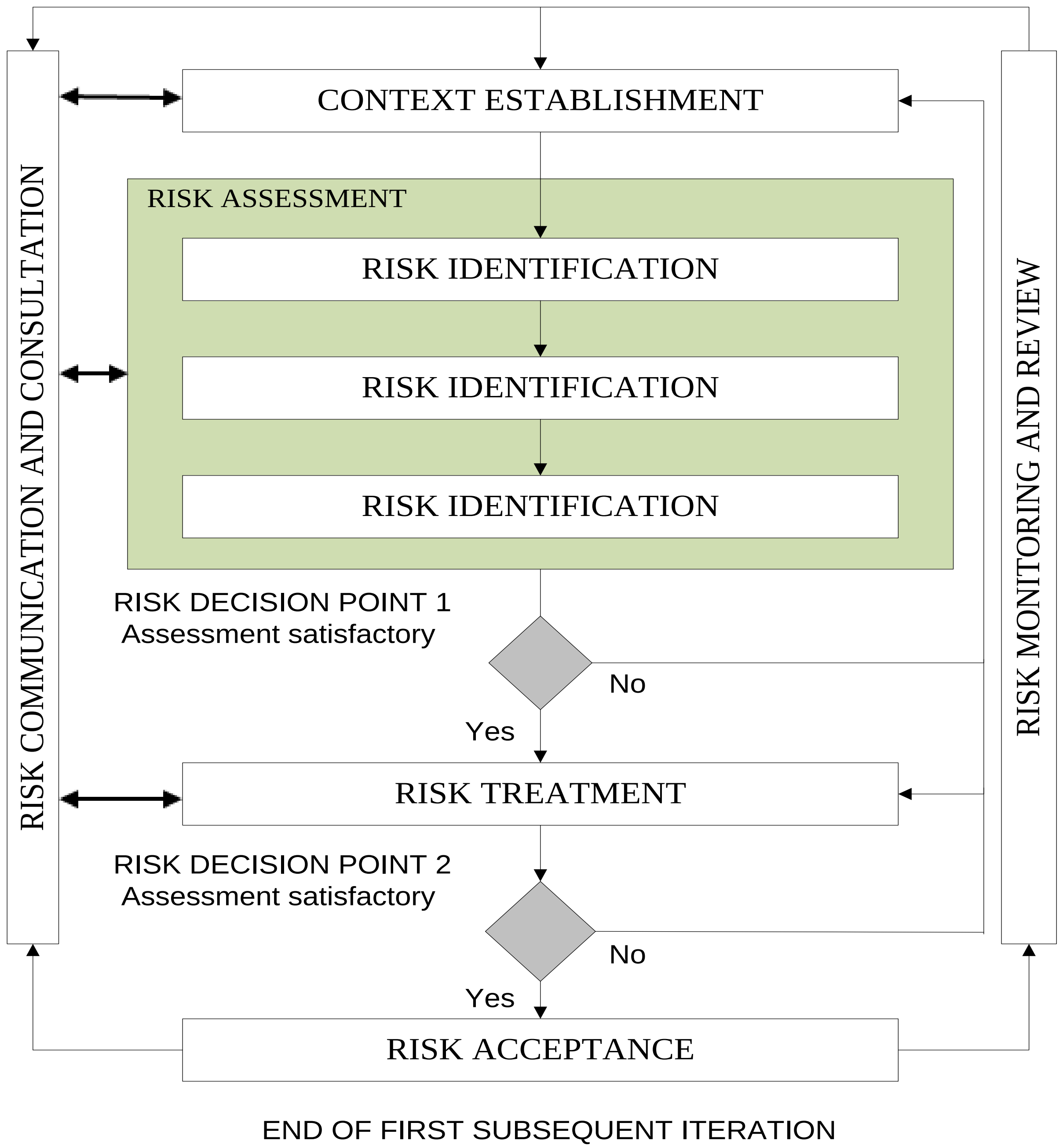


Figure 2: ISO/IEC 27005:2011 Information security risk management process

As shown in Figure 3, risk treatment will be done based on the results of the risk assessment. The risk treatment consists of four different options which should be selected by considering the outcome of the risk assessment, the expected cost for implementing these options and the expected benefits from these options.

The different options are:

- Risk modification: Reducing risk by introducing, removing or altering appropriated security controls such that the residual risk becomes acceptable;
- Risk retention: Accepting the risk without further action;
- Risk avoidance: Abandon the activity or condition that represents the source of the risk;
- Risk sharing: Sharing the risk with another party that can handle the particular risk (e.g. insurance, subcontractors, etc.)

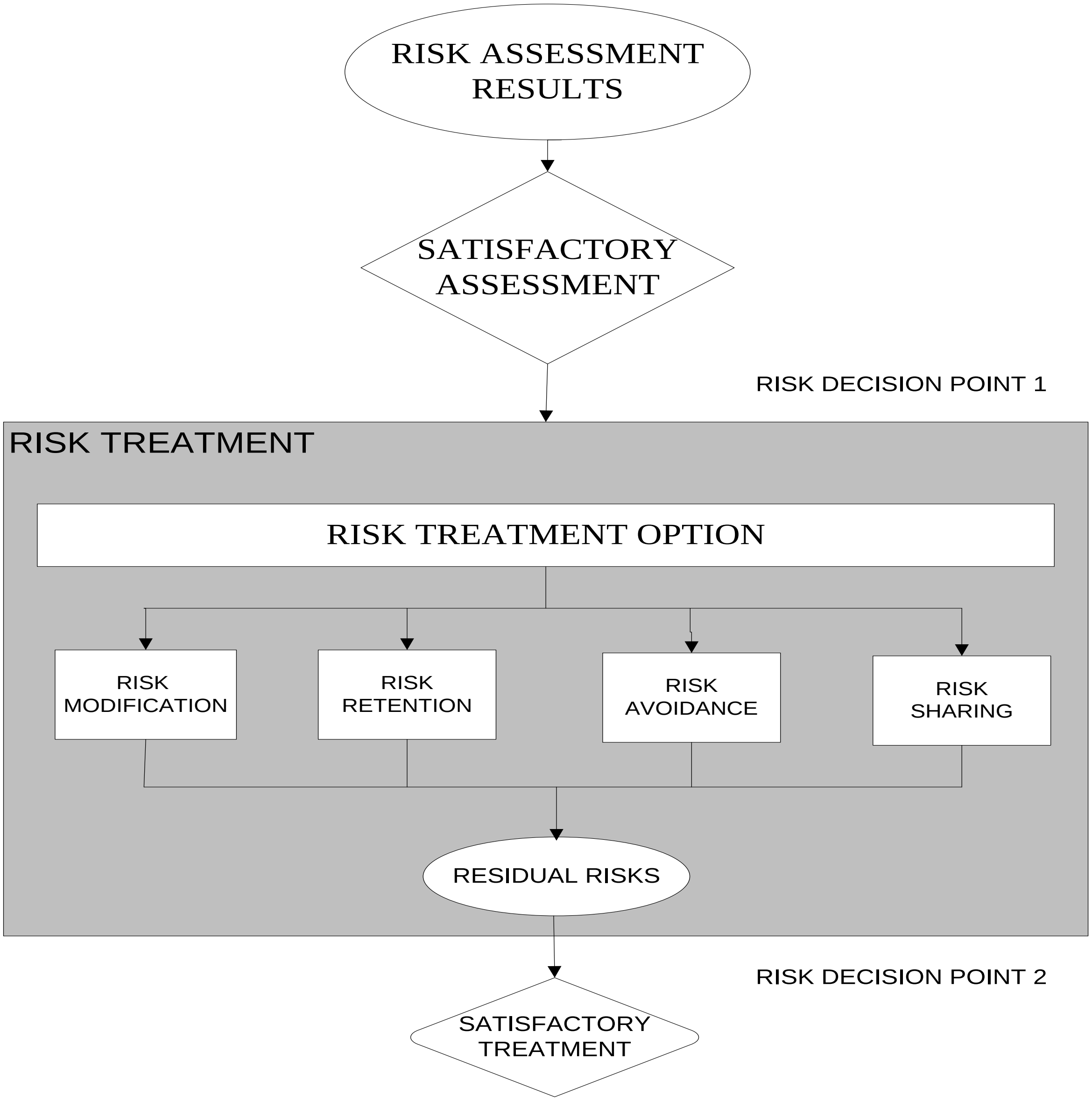


Figure 3: The risk treatment activity

After a satisfactory completion of the risk treatment, the residual risks have to be accepted by responsible managers. If accepted risks exceed the normal risk acceptance criteria there has to be a documented justification. The risk communication and consultation showed in the risk management process, represents the fact that information about the risks has to be shared between the decision-makers and other stakeholders. The communication of risks has to be done during the whole risk management process. Another important part of the risk management process is the Information security risk monitoring and review which consists in monitoring and reviewing the risks and their factors in order to identify changes and maintain an overview. This is important due to the fact that new threats, vulnerabilities or changes in likelihood or consequences can generate new risks or lead to a situation where an acceptable risk becomes unacceptable.

1.3. Risk controlling methods, introduced by Microsoft

Brief description of approaches to management of risks which are introduced by Microsoft Corporation is submitted below. Data description is based on documents “Leadership for the operation of risks” [5]. The management of risks is examined as one of the component of common control program, intended for company's manager and allowing to control the conducting business and to accept informed decision.

The control process of security risks, introduced by the Microsoft, includes following four stages:

1. Estimated risk.

Planning of information accumulation. Discussion of principal provisions of successful realization and recommendations preparation.

- collection of data on risk Process description of data collection and analysis.
- risk of prioritization. Detailed description of step on qualitative and quantitative risk assessment.

2. Decision support.

- definition of functional requirements. Definition of functional requirements for risk decrease.
- Choosing possible solutions for controlling. Description of approach to choose decisions on risk neutralization.
- decision survey. Verification of suggested elements of reasonableness check functional requirements.
- evaluation of risk decrease. Evaluation of decrease of liability impact or risk probability.
- cost estimation of decision. Evaluation of direct and indirect expense, connected with decisions on risk neutralization.

- choice of strategy of risk neutralization. Definition most of economic decision on risk neutralization by the analysis way of advantages and cost.

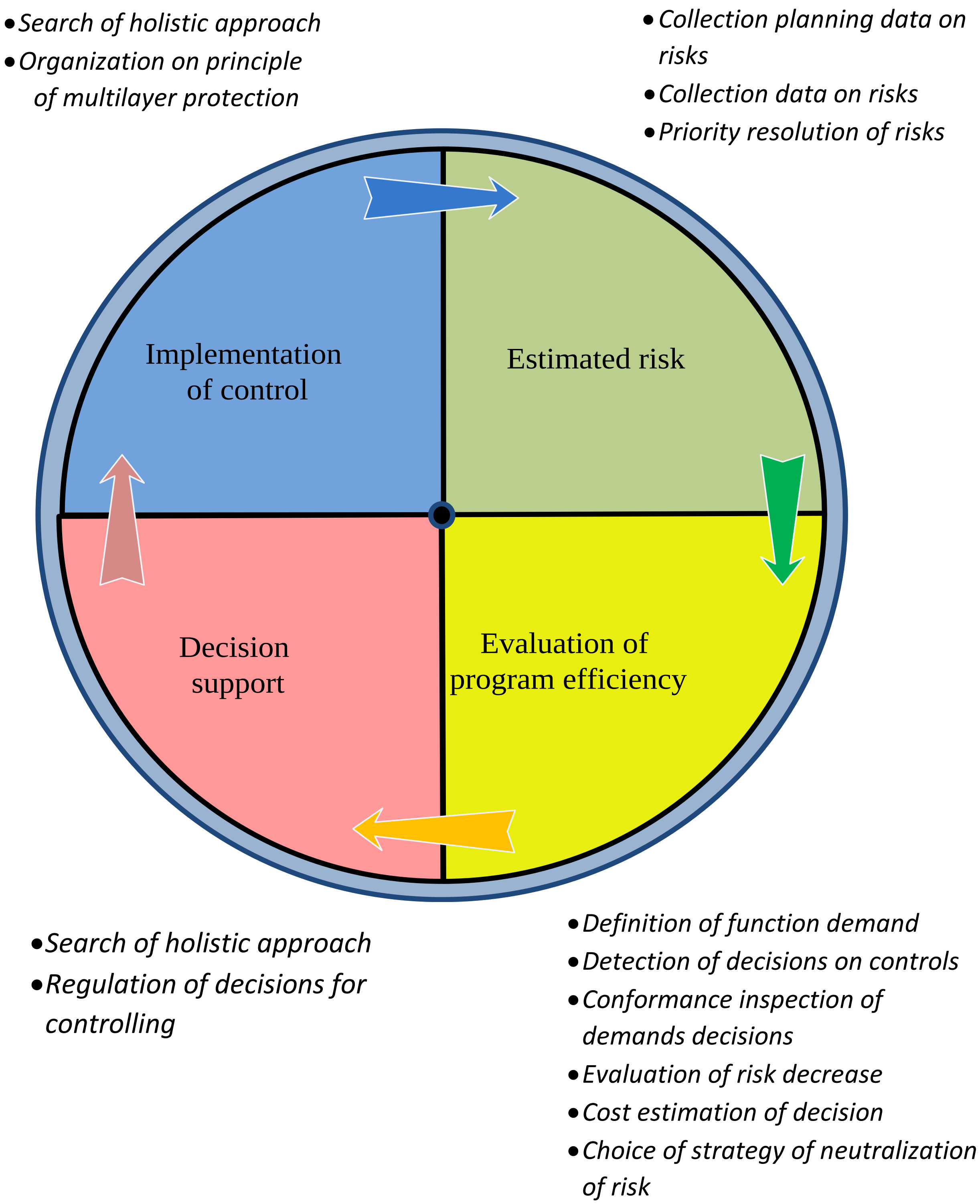
3. Implementation of control. Deployment and decision use for controlling, decreasing the risk for organization.

- *search of holistic approach.* Personal inclusion, processes and technologies in decision on risk neutralization.
- *organization on principle of multilayer protection.* Ordering of decisions on risk neutralization within enterprise.

4. Evaluation of program efficiency. The efficiency analysis of control process of risks and the verification them, provide whether control elements proper the level of security.

- development of a system of risk indices. Assessing level and risk change.
- evaluation of program efficiency. Evaluation of risk management software for emerging opportunities rationalization.

In leadership [5] the terms the management of risks and estimated risk is not interchangeable. Ruled by risks the common measures on risk decrease within organizations up to reasonable level are understood. The management of risks is the continuing process, but being produced by evaluations of most frequently is being done for annual interval. Under risk estimation means the process detection and risk prioritization for businesses which are the component part of risk management.



- *Search of holistic approach*
- *Organization on principle of multilayer protection*

- *Collection planning data on risks*
- *Collection data on risks*
- *Priority resolution of risks*

- *Search of holistic approach*
- *Regulation of decisions for controlling*

- *Definition of function demand*
- *Detection of decisions on controls*
- *Conformance inspection of demands decisions*
- *Evaluation of risk decrease*
- *Cost estimation of decision*
- *Choice of strategy of neutralization of risk*

Figure 4. Control process of security risks, prospective corporation Microsoft

With the description of risk what impact it has on business and how possible this event is are pointed out. The components, describing the risk are shown in fig. 5.

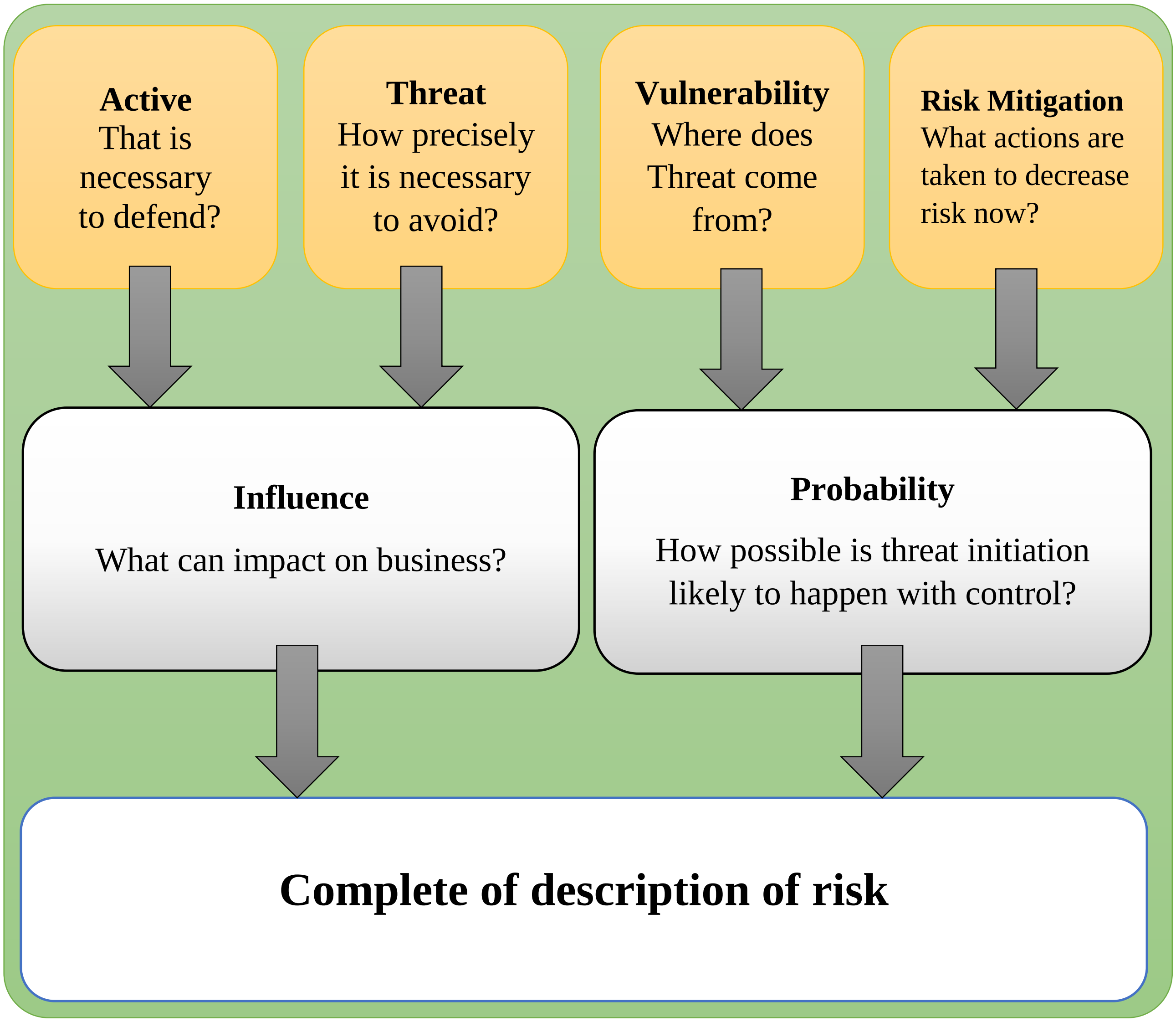

Active
That is necessary to defend?
Threat
How precisely it is necessary to avoid?
Vulnerability
Where does Threat come from?
Risk Mitigation
What actions are taken to decrease risk now?
Influence
What can impact on business?
Probability
How possible is threat initiation likely to happen with control?
Complete of description of risk

Figure 5. Components "complete formulating" of risks

On pioneering stage of estimating risk gives a meaning in accordance with this scale: "high", "average" and "low". After that, for discovered quintessence risks quantitative assessment is held. At length prospective of Microsoft the technique of estimated risk will be considered henceforth the sections of educational course.

Before introduction into organization of control process of security risks, prospective corporation the Microsoft, it is necessary to check the maturity level of organization from the point of view management of security risks Organization, in which the ceremonial policies or the processes, managerial of security risks are absent, it will be very hard at once to introduce all aspects pending process. If will find themselves, that the maturity level is fairly low, pending the process it is possible to root consistent. Stages over several months (for example exploitation way of pilot project in individual unit over several complete cycles is process data) . Having demonstrated the effectiveness of control process of security risks, prospective corporation the Microsoft, as an example of this pilot project, the management team of security risks can pass on to introduction process data in other units, gradually covering all organization.

The scale, set out in table, estimates the maturity level.

Level	Condition	Definition
0	Is absent	The policy or the process are not documented. Earlier organization did not know about business risks, connected with management risks, and did not consider this problem
1	Highly specialized	Some members of the Organization recognize the relevance management of risks, however the directing operations of risks are highly specialized. The policies and the processes in organization is not documented, the processes is not fully retried. Due to projects for the operation of risks are chaotic and not manageable, and received results are not measured by and is free of audit
2	Retried	Organizations it is known on the management of risks The control process of risks is retried, but is developed slightly. The process is documented not in full, however corresponding operations are being done regularly, and

		the organization seeks to introduce the comprehensive control process of risks with engagement of top management. In organization the ceremonial training and the informing for the operation of risks aren't held; the responsibility for performance respective measures was laid on individual members of the staffs
3	Presence certain process	The organization adopted the ceremonial decision on intense introduction management of risks for management of protection program of information. In organization the basic process with clearly specific purposes and achievement process of documentation and appraisal of the results is worked out. The training of all personals basis of management of risks is held. The organization actively introduces documentation of the control processes of risks.
4	Controlled by	At all organization levels deep understanding management of risks is available. In organization there is the control procedure of risks and well-defined the process, the information on the management of risks, the available detailed training has wide distribution, there is also the initial forms of measurements of efficiency indices. Risk management software the sufficient volume of resources is outlined, the results management of risks exert positive effect at work of many organizational units, and the management team of security risks can continually improve their processes and the means. In organization

		some technological means, assistant in management of risks, however the most (unless the overwhelming majority) procedures of estimated risk, the determinations of elements of inspection and analysis of advantages are being used and cost is being done by hand.
5	Optimized	The organization separated on management of security risks the considerable resources, and the members of the staffs try to forecast, what problems can meet during the later month and years and in which way by them is needed will decide. The control process of risks has been deeply studied and to a great extent automated by the using of various media (developed at organization or acquired at strange designers). When problem initiation in security system the primary cause of occurred problem is being revealed and actions required for risk decrease its repeated initiation are taken. The organization members of the staffs can undergo training, providing different levels of preparation

1.4. Based on management threats of RISKWATCH software

The company of RISKWATCH developed the own technique of risk analysis and the family software, in which the it in that or other action is realized [8, 10, 20].

In family of RISKWATCH enter the program products for carrying out of distinctive types of security audit:

- RISKWATCH for Physical Security - for the analysis of physics integrated circuit protection;
- RISKWATCH for Information Systems - for information risks
- HIPAA-WATCH for Healthcare Industry - to assess conformities with a standard of HIPAA (US Healthcare Insurance Portability and Accountability Act), Topical in basic to health care facilities, employee on the territory US;
- RISKWATCH RW17799 for ISO 17799 - to assess appropriateness IS standard demands of international standard of ISO 17799.

In method of RISKWATCH as of criterion to assess and management of risks expected annual losses (Annual Loss Expectancy, ALE) and call-back evaluation of investments (Return On Investment, ROI) are being used. RISKWATCH are oriented at the exact quantitative assessment of losses correlation from security risks and cost of creation of protection system. At the foundation of product of RISKWATCH the technique of risk analysis is situated, which consists of four stages.

First stage - definition of subject of research. Here are described such parameters, as the organization type, the composition explored system (broadly), basic the demands in the area of security With a view to facilitating analytics work, in gauges, corresponding the organization type ("Commercial information system", "state / military information system" and etc.), is the categories lists protected resources, losses, threats, vulnerabilities and measures for the protection. Of them is needed to select by that real are present in organization (the figure 6.).

For example of losses category:

- delay and denial of service;

- information disclosure;

- direct losses (for example from facility killing by the fire);

- life and health (personal, customers and etc.);

- data change;

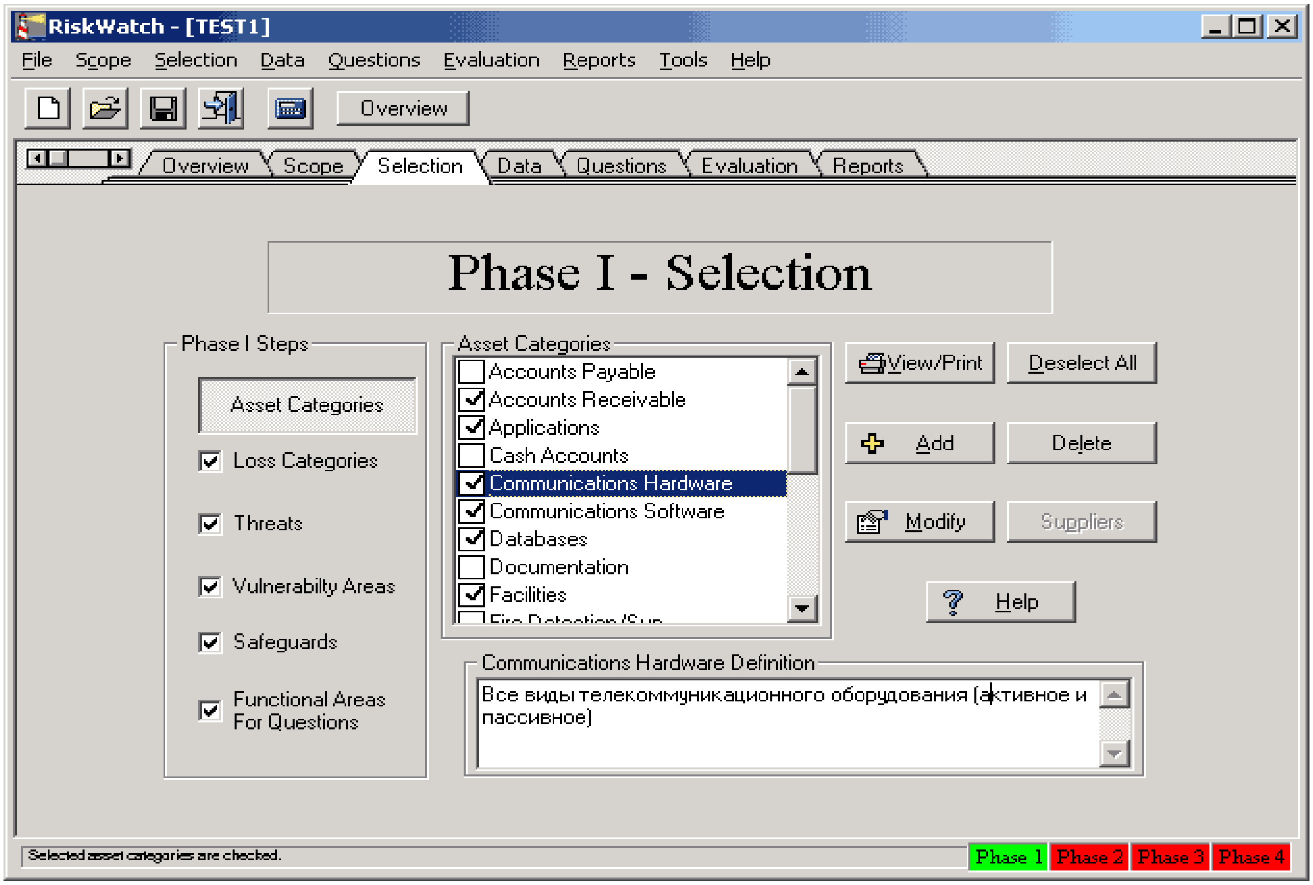
- indirect losses (for example costs for recovery);

- reputation.

Second stage - data entry, describing particular system characteristics. Data may be introduced by hand or to importation from reports, created by the instrumental tools for research of vulnerability of computer networks. At that stage, in particular, the resources, the losses and the incidents classes at length is described. The incidents classes are achieved by comparison category of losses and resources category.

To identify eventual vulnerabilities the questionnaire is being used, the base of which contains over 600 problems. The problems are linked to resources categories. Arise frequency of each outlined threats, the vulnerability degree and the resources value also is set. If for chosen class of threat in system is annual average evaluation

The initiations (LAFE and SAFE), them are being used they (the figure.7). All this is being used in future for effect calculation from introduction of protection facilities.


RiskWatch - [TEST1]
File Scope Selection Data Questions Evaluation Reports Tools Help
Overview
Overview Scope Selection Data Questions Evaluation Reports
View/Print
Deselect All
Add
Delete
Modify
Suppliers
Help
Phase 1 Phase 2 Phase 3 Phase 4

Phase I - Selection

Phase I Steps

- Asset Categories
- ☑ Loss Categories
- ☑ Threats
- ☑ Vulnerabilty Areas
- ☑ Safeguards
- ☑ Functional Areas For Questions

Asset Categories

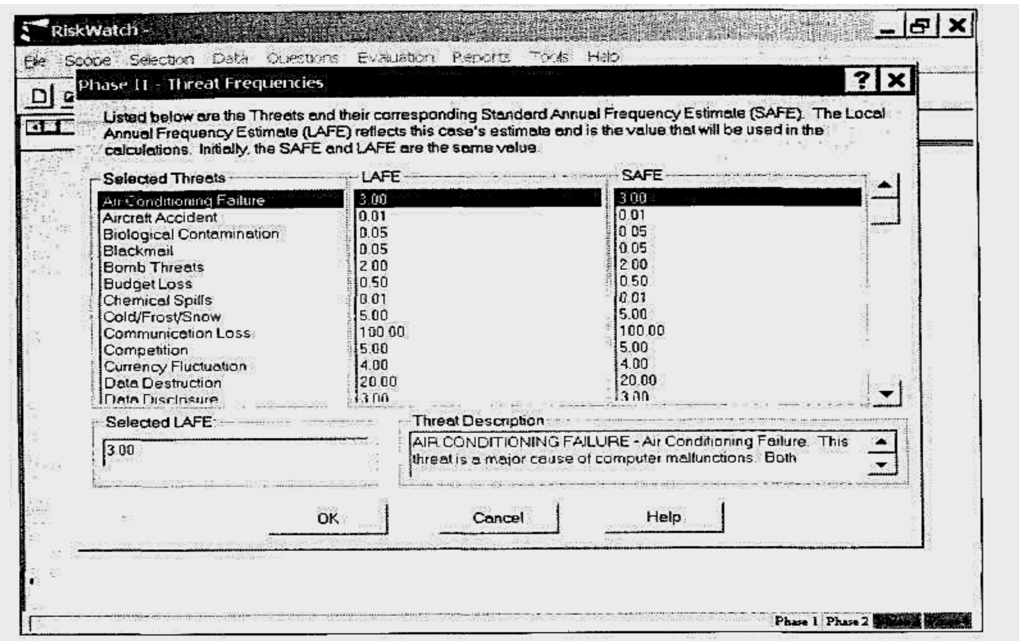
- □ Accounts Payable
- ☑ Accounts Receivable
- ☑ Applications
- □ Cash Accounts
- ☑ Communications Hardware
- ☑ Communications Software
- ☑ Databases
- □ Documentation
- ☑ Facilities
- □ Fire Detection/Sup

Communications Hardware Definition

Все виды телекоммуникационного оборудования (активное и пассивное)

Selected asset categories are checked.

Figure 6. Classification protected resources.


RiskWatch -
File Scope Selection Data Questions Evaluation Reports Tools Help
OK
Cancel
Help
Phase 1 Phase 2

Phase II - Threat Frequencies

Listed below are the Threats and their corresponding Standard Annual Frequency Estimate (SAFE). The Local Annual Frequency Estimate (LAFE) reflects this case's estimate and is the value that will be used in the calculations. Initially, the SAFE and LAFE are the same value.

Selected Threats	LAFE	SAFE
Air Conditioning Failure	3.00	3.00
Aircraft Accident	0.01	0.01
Biological Contamination	0.05	0.05
Blackmail	0.05	0.05
Bomb Threats	2.00	2.00
Budget Loss	0.50	0.50
Chemical Spills	0.01	0.01
Cold/Frost/Snow	5.00	5.00
Communication Loss	100.00	100.00
Competition	5.00	5.00
Currency Fluctuation	4.00	4.00
Data Destruction	20.00	20.00
Data Disclosure	3.00	3.00

Selected LAFE: 3.00

Threat Description: AIR CONDITIONING FAILURE - Air Conditioning Failure. This threat is a major cause of computer malfunctions. Both

Figure 7. Evaluations example of assignment of LAFE and SAFE for one of threats.

Third stage - quantitative risk assessment. At that stage the risks profile is calculated, and the actions of ensuring the safety are chosen. The communications between at first shall be established .Resources, losses, threats and vulnerabilities, outlined on previous steps examining. In essence, the risk is estimated by means of mathematical expectation of losses over a year. For example if the server cost $150000, and the fire will delete odds on it for a year, is equal to zero. That expected losses will amount to $1500.

The calculation formula (m = p*v, the where m-mathematic expectation, p - the probability of appearance of threat, V - the cost of funds) suffered some changes, by the fact that RISKWATCH uses certain the American institute of standards of NIST evaluation, called LAFE and SAFE. LAFE (Local Annual Frequency Estimate) - shows, how many once a year at an average of data threat is realized in a given place (for example in city). SAFE (Standard Annual Frequency Estimate) - shows, how many once a year at an average of data threat is realized in that "world part" (for example to North America). Shall be introduced also the correction index, which permits to take into account, that in the result of the implementation of threat protected the resource may be been destroyed not in full, and in part only.

Formula (1) and (3) show the variants of index calculation of ale

ALE = Asset Value Exposure Factor* Frequency (1)*

Where *Asset Value* - cost pending asset (data, programs, instrument and etc.);
Exposure Factor - coefficient action - shows, how much of (in percentage terms) from asset value, are placed at risk;
Frequency - arise frequency of undesired event;
ALE - this estimate expected annual losses for one particular asset from sale of one threat. When the total assets and action are identified by and is collected together, that appears the possibility to appraise the common risk for IS, as the sum of all particular values.

It is possible to introduce findings “expected annual the accident rate” (Annualized Rate Of Occurrence - ARO) and “expected the single damage” (Single Loss Expectancy - SLE), that may call off as the margin of original cost and its the residual cost after accident (although the similar evaluation method is applicable not in all instances, for example it not is appropriate for estimated risk, related to violation information confidentiality). Then, for separately taken combination Threat resource is applicable the formula (2)

$$ALE = ARO*SLE \; (2)$$

Additionally is being considered scenario "that if”, which permits to describe

- Analogous situation granting of introduction of protection facilities. Comparing expected loss.
- Granting of introduction of safeguard measures and without them can be estimated the effect from such events.
- RISKWATCH includes of base with evaluations of LAFE and SAFE, and also with generalized.
- Description of different types of protection facilities.
- The effect from introduction of protection facilities quantitatively are described by means of.
- Finding of ROI (Return On Investment - the investments call-back), which shows the return on.

Made investments for a certain period of time. Is calculated it from the formula:

$$RIO = \sum_i NVP(Benefits)_i - \sum_j NVP(Costs_j) \; (3)$$

Where $Costs_j$ - costs of introduction and maintaining defence j- protective measures; benefits - evaluation that benefit (expected the loss reduction), which bring the introduction of data of measure for the protection; NPV (net present value) - pure present value.

Fourth stage - report generation. Reports types:

Brief results. (Complete and summary accounts about elements, described on stage 1 and 2. (Report from cost protected resources and expected losses from sale

Threats.

- Report about threats and countermeasures.
- Report of ROI (fragment - on figure 8).
- Report on results of security audit.

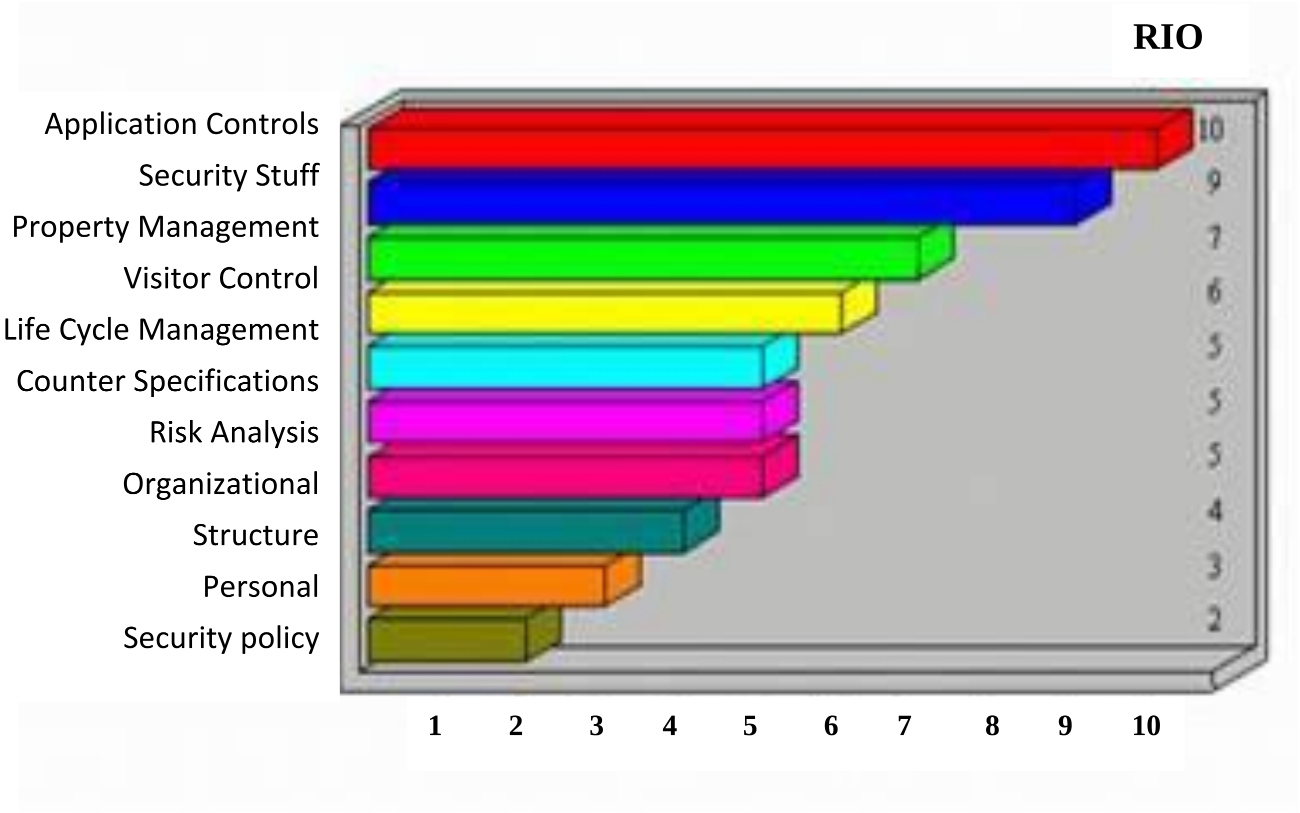


Figure 8. Schedule example of finding of ROI
for different measures for the protection.

So that, pending the means makes it possible to estimate not only that risks
Which now exist at enterprise, but as well that the advantage, which may produce the introduction physics, technological, program and away means and defense mechanisms. Prepared reports and schedules give the material, enough for adoption of decisions on the change of system of enterprise safety provision.

CHAPTER II.

ANALIZE OF DETECTION ATTAKCS

METHODS AND RISK ASSESSMENT

2.1. Intrusion Detection and Risk Management

The concept of risk is fundamental to any field of human activity. Whatever we did, there is always a chance that the objectives of our work, for whatever reasons, will not be achieved. Our very existence is associated with serious risks as a result of which we can bear more or less serious damage. Thus, a risk is the possibility of incurring losses.

In the field of information security risk assessment plays the same pivotal role, as in all other areas of human activity. Due to the inadequate assessment of the risks associated with the implementation of information security threats in today's high-tech society, the state, organizations and individuals have very significant damage, that hardly anyone ever calculates successfully.

The magnitude of the risk is determined by the probability of successful execution of the threat and the magnitude of the damage that will be caused as a result. Possible damage can not always be expressed in monetary units, and the probability of success of the threat does not measure precisely. Therefore, our assessment of risks are approximate. Their accuracy depends on how well we focus on the current situation correctly imagine the nature and methods of threats, as well as on our ability to analyze and evaluate their impact.

Assess the risks, you must decide what to do with them. This process is called risk management. Risk management involves the assessment of the cost of the implementation of countermeasures, which should be less than the possible damage. The difference between the cost of taking countermeasures and the magnitude of potential damage should be greater, the less chance of damage.

Countermeasures can reduce risk levels with different ways:

- Reducing the likelihood of the threats to security;

- Eliminating or reducing the vulnerability of their value;

- Reducing the amount of potential damage;

- Promoting resource recovery automated system (AS), which was damaged;.

- Identifying attacks and other security breaches.

2.2. Network attacks

With the increasing dependence of the world economy and government from the Internet the level of risk associated with network attacks increases on the resources of networks connected to the Internet. Attacks across the WAN are powerful means of information warfare between states, the commission of crimes in the financial and other sectors, including acts of terrorism. For example, September 22, 2001 by the American Institute of studying security technologies (Institute for Security Technology Studies At Dartmouth College) published a report entitled "Cyber attacks during the war against terrorism» (Cyber Attacks During The War on Terrorism: A Predictive Analysis). By this method, in other conflicts between countries cyber attacks can also be seen which are in the internet.

- Unauthorized access to Internet-resources of the United States and allied countries, which result in damage to the critical elements of the information infrastructure and the integrity of vital information.

The main conclusions of the analysis:

- Physical attacks immediately followed by the increasing number of network attacks;

- The quantity, complexity and coordination of network attacks is increasing steadily;

- Network attacks directed against a particularly critical network resources, which include servers and active network equipment connected to the Internet.

The study allowed to recommend as a priority security measures during the war against terrorism are following:

- Improving documentation (logging) and alarming (alert) in systems of detecting network attacks;

- Immediate reporting about suspicious activity to law enforcement authorities for the purpose of investigation and preventive measures;

- Adherence to standards and best practices in the field of information and physical security, regular software updates, virus protection, installation of the systems of detecting attacks and Firewall;

- The adoption of the recommended measures to protect against known software implementation attacks (exploites) and backup of critical information resources;

- Application of methods of filtering IP-packets (ingress and egress filtering) on the router and Firewall to protect against DoS-attacks.

As seen from the recommendations, along with the standard means of protection, without which normal functioning of the AC (such as Firewall, backup and antivirus software), you still need IDS (attack detection system) - the main means of struggle against network attacks.

Currently, IDS are becoming increasingly adopted the practice of the security of corporate networks. However, there are a number of problems which will inevitably encounter the organization deploying the system at identifying attacks. These problems make it very difficult, and sometimes even stop the process of implementation of IDS. Here are some of them:

- The high cost of commercial IDS;

- Low efficiency of modern IDS, characterized by a large number of false positives and Rationality failures (false positives and false negatives);

- Demanding and often unsatisfactory performance of IDS are already at a speed of 100 Mbit/s networks;

- Underestimation of the risks associated with network attacks;

- Lack of organization methods of risk analysis and management, enabling management to adequately assess risk and value to justify the cost of implementing countermeasures;

- The need for highly qualified experts to identify attacks, without which the implementation and deployment of IDS.

For many countries it is also characterized by a slight dependence of the information infrastructure of enterprises from the Internet and financing measures to ensure information security as a residual that is not conducive to the acquisition of expensive remedies to deal with network attacks.

Nevertheless, the process of implementation in practice of maintaining the IDS IS(Information security) continues.

Organizing estimating IT intellectuality of experts would be prosperious. While existing international system can used. For instance, The American Institute of SANS established a program of professional certification experts to identify attacks - GIAC Certified Intrusion Analyst (GCIA).

At the heart of most of the errors in decision-making, including the protection against network attacks is wrong risk assessment. The accuracy of the identification and assessment of risks associated with any activity, acts as the main characteristics of vocational education expert in the subject area. In the absence of an adequate assessment of the risks is difficult to answer questions about where to start building a system of information security, what resources and what threats from the need to protect and what countermeasures are considered a priority. It is also difficult to solve the problem of necessity and sufficiency of a set of counter-measures and the adequacy of the existing risks.

Thus, the question of assessing the risks associated with network attacks, and is considered the most important in the first place.

2.2.1. Detecting attacks as a method of risk management.

Detecting attacks today is one of the methods of risk management. Activities to detect network attacks using network IDS is to monitor network traffic between the attacker and the attacked system, finding and analysis of suspicious traffic, assessing the level of seriousness of the attack and the magnitude of the risk associated with its implementation, as well as deciding on the response to the attack. Search suspicious traffic, and often determine the level of severity of the attack IDS performed automatically. The most common method of intrusion detection signature analysis is used in all commercial IDS and are discussed below. An estimate of the risk associated with network attacks, requires the participation of an expert. On the basis of risk assessment addressed the issue of responding to the attack. If the risk is small, it is possible that the attack does not deserve attention. At the same time, in some cases, you may need to take immediate response.

Consider the methodology for assessing the risks associated with the implementation of network attacks, adopted in SANS / GIAC.

2.2.2. Assessment of the severity of a network attack

The attacks of varying degrees of severity require different levels of response. Attack Severity (Severity) is determined by the risk as a result of its implementation. The magnitude of the risk, in turn, depends on the probability of a successful attack and the magnitude of possible damage, and the amount of potential damage - on the degree of criticality of resources (Criticality), which is directed against an attack. On the likelihood of successful implementation of the attack (Lethality) affects the effectiveness of the methods and the magnitude of the vulnerability of the protection system, through which it is undertaken. The size of the vulnerability is directly related to the efficiency of countermeasures on the system (System countermeasures) and network layer (Network countermeasures), used to counteract this type of threat.

The formula for finding the level of seriousness of the attack is follows:

$$S=(Vr+Ve) - (Cs+Cn) \quad (4)$$

(S=SEVERITY, Vr=CRITICALITY, Ve=LETHALITY,

Cs= SYSTEM COUNTERMEASURES, Cn=NETWORK COUNTERMEASURES).

This formula can be used to estimate the risk of attacks detected using IDS, when analyzing the results of the monitoring network traffic. Typically, interest only those attacks for which the amount of risk exceeds a certain threshold value.

Severity of attack (S) installed on a numerical scale from -10 to +10.

S{-10,10} - the magnitude of risk associated with the implementation of a network attack.

The criticality of the network resource (Vr) is determined by the 5-point scale based on the purpose of the network resources and performs its functions. In practice guided by the following scale:

- 5 - Firewall, DNS-server, a router;

- 4 - mail gateway;

- 2 - Workstation UNIX;

- 1 - PC Windows,

To determine the probability of successful implementation of the attack and the possible damage (Ve) adopted the following scale:

- 5 - an attacker can gain root access on the remote system;

- 4 - a denial of service as a result of network attacks;

- 3 - receiving an unprivileged user on a remote system, such as by intercepting the password transmitted across the network in clear text;

- 2 - the disclosure of confidential information to unauthorized network access, such as an attack on a null session of Windows;

- 1 - the probability of the success of these attacks is very small.

The effectiveness of the countermeasures system level (Cs) can be assessed on the following scale:

- 5 - modern operating systems, are loaded all the software correction (packs), there are additional (cash) network protection (eg, tcp wrappers, or secure shell);

- 3 - an old version of the operating system is not installed some software correction;

- 1 - no specialized protective equipment, password policy is not generated, passwords are transmitted across the network in unencrypted view.

The following scale is used to assess the effectiveness of countermeasures network layer (Cn):

- 5 - Firewall, which implements the principle of minimizing the privileges, the only entry point to the network;

- 4 - Firewall and the presence of additional network entry points;

- 2 - Firewall, allowing whatever is not explicitly prohibited (permissive access control policy).

As already noted, this method of estimating the risks associated with network attacks, used in SANS / GIAC when analyzing suspicious pieces of network traffic (detects), detected by the network IDS.

2.3. Determine threats and risk management tools

2.3.1. Firewall system.

It is now becoming apparent failure of traditional firewall to protect networks from threats from the Internet, because they do not provide protection against a class of security threats (including by threats directed against themselves Firewall). Traditional data protection, including the Firewall, is only effective against known vulnerabilities. They are unlikely to prevent hackers to find new ways to implement attacks. For this purpose special funds intended to identify attacks - IDS. Moreover, it is often must to observe the situation when the installation Firewall only reduces the overall security of the corporate network against threats from the Internet. Misconfigured firewall protection system creates a "hole", sometimes more than his absence.

The same principle is true with respect to the Firewall and any other remedies.

Adding a new remedy increases the overall security of the system only under the condition that the existing security practices should not be changed in the direction of weakening protection mechanisms.

Establishing Firewall, network administrators, relying on protection mechanisms implemented by the Firewall, often refuse any additional measures to maintain protection against threats from the external network, which are necessary in the absence of Firewall. As a result, the overall security of the network against external attacks may either increase or remain the same, or (and this is very likely) deteriorate. This occurs because network administrators and users tend to trust implicitly Firewall and overestimate its role in protecting the network from external threats by the Internet. They present themselves as a kind of Firewall shield covering them from the rain, hail, snow, storms and other bad weather. At the same time forget that there are many holes shield, and sometimes it may even resemble a sieve. "Holes" in the shield needs to communicate with the outside world hostile. By mistake, and it is not possible can be opened not the "hole" or "holes" are too high, besides the "holes" in the shield is sometimes possible to break out.

Therefore, to ensure an adequate level of protection should be required to supplement the Firewall special tools detect attacks. On this topic there is already a lot of publications, so no need to once again defend this thesis, illustrating it with plenty of examples from the sad experience of Russian and foreign companies. However, setting the Firewall, the management of Russian companies is not in a hurry to allocate funds for the purchase and operation of systems for identifying attacks.

An analysis of suspicious traffic. The signatures as the main mechanism for identifying attacks.

IDS systems detect attacks solve the problem of monitoring information system on a network, system and application levels to detect security breaches and rapid response. Network IDS serve as a source of data for analysis of network packets, a IDS system level (host - host based) analyze security audit log records the OS and applications. At the same methods of analysis (detect attacks) are common to all classes of IDS.

It was suggested that a lot of different approaches to solving the problem of intrusion detection (in the general case we are talking about intentional activity, including, in addition to the attacks, the actions performed within the given powers, but violate the rules of security policy). However, any existing IDS can be divided into two main classes: one statistical analysis employed, while others - signature analysis.

Statistical methods are based on the assumption that the activity of the attacker is always accompanied by some anomalies, changing the profile of the behavior of users, software and hardware.

The primary method of detecting attacks, accepted in most modern commercial products, a signature analysis. The relative simplicity of this method makes it possible to successfully implement it in practice. IDS, applying signature analysis usually do not "know" about the rules of the security policy implemented by the Firewall (so in this case it is not about intentional activity, but only about the attacks). The basic principle of their operation - a comparison occurring in the system / network events with the signatures of known attacks - the same as that used in the anti-virus software.

General criteria for evaluation of IT security (ISO 15408) contains a set of requirements FAU_SAA entitled "Analysis of the data security audit» (Security audit analysis). These requirements determine the functionality of IDS, looking for malicious activity as statistical methods, and signature analysis.

Component FAU_SAA2 «Identifying anomalous activity, based on application profiles» (Profile based anomaly detection) involves the detection of abnormal activity using profiles of determining dangerous in terms of security of users' actions and identify these actions. In order to establish the degree of danger or that actions are evaluated by appropriate "rating confidence" to the users. The greater the risk of a user action, the higher the "rating confidence". When the "rating confidence" reaches the critical value, provided security policy taken action to respond to the malicious activity.

Components FAU_SAA3 «Simple attack heuristics» (Simple attack heuristics) and FAU_SAA4 «Complex attack heuristics» (Complex attack heuristics) provide for the implementation of signature analysis to search for malicious activity. In the event of an attack FAU_SAA4 signature sets the sequence of events, is a sign of violation of the rules of the system security policy.

2.3.2. About IDPS technology

IDPS(intrusion Detection and Prevention System)s. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. IDPSs are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDPSs have become a necessary addition to the security infrastructure of nearly every organization. IDPSs typically record information related to observed events, notify security administrators of important observed events, and produce reports. Many IDPSs can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g., reconfiguring a firewall), or changing the attack's content.

2.3.3. Intrusion Detection and Prevention Principles

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Incidents have many causes, such as malware (e.g., worms, spyware), attackers gaining unauthorized access to systems from the Internet, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized. Although many incidents are malicious in nature, many others are not; for example, a person might mistype the address of a computer and accidentally attempt to connect to a different system without authorization.

An intrusion detection system (IDS) is software that automates the intrusion detection process. An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. This section provides an overview of IDS and IPS technologies as a foundation for the rest of the publication. It first explains how IDS and IPS technologies can be used. Next, it describes the key functions that IDS and IPS technologies perform and the detection methodologies that they use. Finally, it provides an overview of the major classes of IDS and IPS technologies. IDS and IPS technologies offer many of the same capabilities, and administrators can usually disable prevention features in IPS products, causing them to function as IDSs. Accordingly, for brevity the term intrusion detection and prevention systems(IDPS)is used throughout the rest of this guide to refer to both IDS and IPS technologies. Any exceptions are specifically noted.

An overview of IDPS technologies. IDPS provides a high-level description of the security capabilities of the technologies, including the methodologies they use to identify suspicious activity.

2.3.4. Components and Architecture

This section describes the major components of IDPS solutions and illustrates the most common network architectures for these components.

Typical Components

The typical components in an IDPS solution are as follows: Sensor or Agent. Sensors and agents monitor and analyze activity. The term sensor is typically used for IDPSs that monitor networks, including network-based, wireless, and network behavior analysis technologies. The term agent is typically used for host-based IDPS technologies. Management Server. A management server is a centralized device that receives information from the sensors or agents and manages them. Some management servers perform analysis on the event information that the sensors or agents provide and can identify events that the individual sensors or agents cannot. Matching event information from multiple sensors or agents, such as finding events triggered by the same IP address, is known as correlation. Management servers are available as both appliance and software-only products. Some small IDPS deployments do not use any management servers, but most IDPS deployments do. In larger IDPS deployments, there are often multiple management servers, and in some cases there are two tiers of management servers. Database Server. A database server is a repository for event information recorded by sensors, agents, and/or management servers. Many IDPSs provide support for database servers. Console. A console is a program that provides an interface for the IDPS's users and administrators. Console software is typically installed onto standard desktop or laptop computers. Some consoles are used for IDPS administration only, such as configuring sensors or agents and applying software updates, while other consoles are used strictly for monitoring and analysis. Some IDPS consoles provide both administration and monitoring capabilities.

2.4. The analysis of network traffic and content analysis

There are two not mutually exclusive approach to identify network attacks: network traffic analysis and content analysis. In the first case study only the headers of network packets in the second - their contents.

Of course, the most complete control of information interactions is provided only by analyzing the entire contents of the network packet, including headers and data area. However, from a practical point of view, this task difficult because of the huge amount of data that had to be processed. Modern IDS begin to experience serious performance problems even at a speed of 100 Mb / s networks. Therefore, in most cases it is expedient to resort to detect attacks to the analysis of network traffic, in some cases, combining it with the content analysis.

Conceptually, the signature of a network attack is virtually identical to the signature of the virus. It is a set of features that allow to distinguish the network attack from other types of network traffic. Thus, the following features may be considered as attack signatures:

- Examples of attack signatures used in the analysis of traffic (network packet headers):

- title TCP-package set the destination port 139 and the flag GLD (Out of Band), which is a sign of attack ala WinNuke;

- simultaneously conflicting flags TCP pack-ta: SYN and FIN. Through this combination of flags in many programs attackers manage to bypass filters and monitors, checks only the installation of a single SYN-flag;

- an example of attack signatures used in the analysis of the content:

- "GET. Cgi-bin / etc / passwd". The appearance of a line in the HTTP-data package indicates the presence of exploits such as phf, php or aglimpse.

Methods of analysis of content have one major drawback. They do not work when the attack program (DDoS, trojans) are turning to encrypted traffic. For example, Back Orifice trojan or Barbwire DDoS-commands transmitted between client and server (manager and agent) is encrypted by an algorithm blowfish. Methods for detection of such attacks are limited to the analysis of network packet headers.

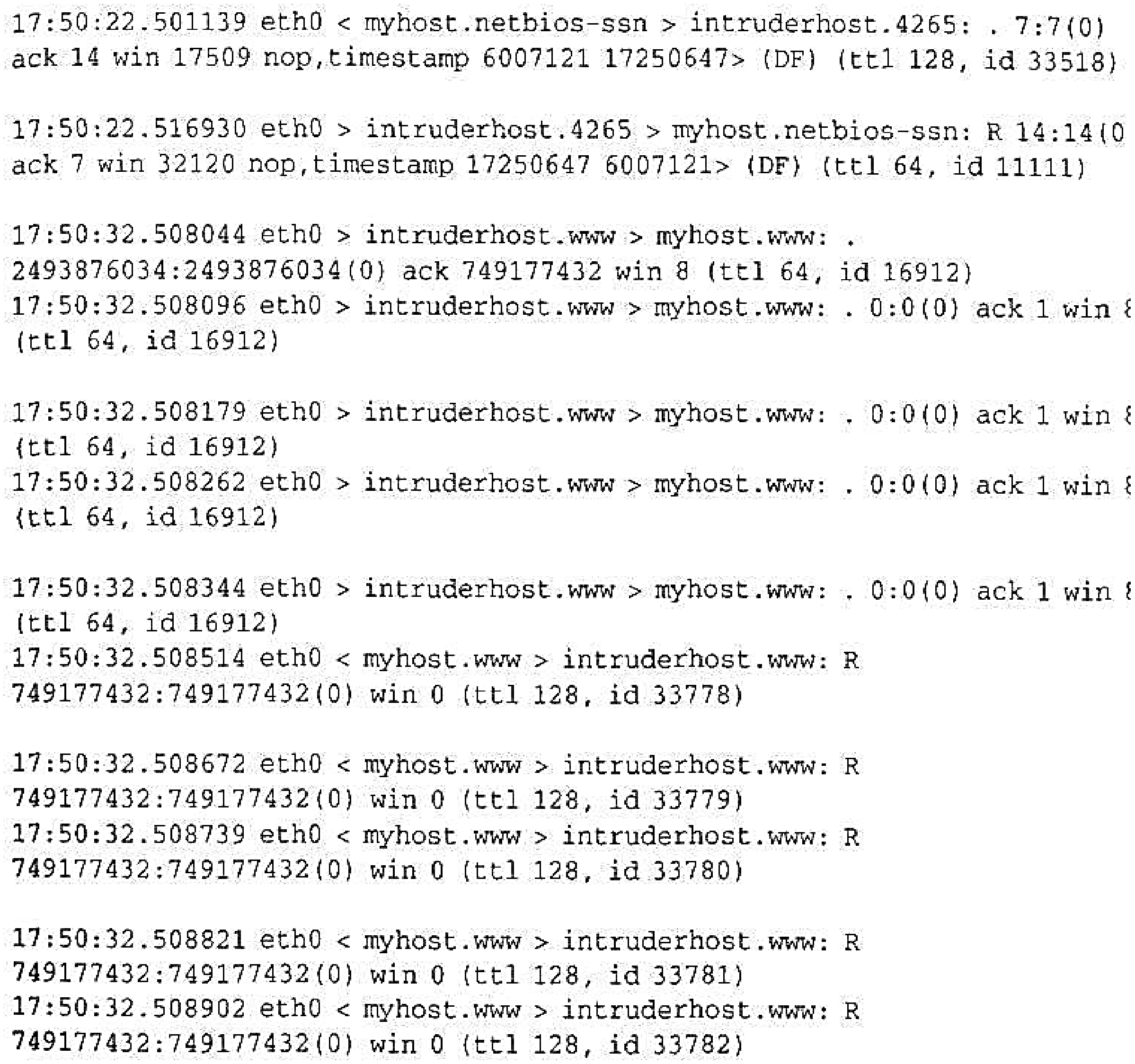
2.4.1. An example of the analysis of suspicious traffic

We show how to manage the risks associated with network attacks is implemented in practice. First, you need to install and configure any system for monitoring network traffic, such as NFR, NetProwler, Tcpdump + Shadow, etc.Then you can proceed to the analysis of suspicious traffic, events and all types of network attacks, assess and manage risks.

As an example of suspicious traffic, deserves the attention of experts, consider the fragment of the event log program Tcpdump - Listing 1.

Листинг 1

```
7:50:22.499014 eth0 > intruderhost.4265 > myhost.netbios-ssn: S
2828114481:2828114481(0) win 32120 sackOK,timestamp 17250647 0,nop,wscale
0> (DF) (ttl 64, id 11091)

17:50:22.499428 eth0 < myhost.netbios-ssn > intruderhost.4265: S
1070635944:1070635944(0) ack 2828114482 win 17520 nop,wscale
0,nop,nop,timestamp 0 0,nop,nop,sackOK> (DF) (ttl 128, id 33514)

17:50:22.499462 eth0 > intruderhost.4265 > myhost.netbios-ssn: . 1:1(0)
ack 1 win 32120 nop,timestamp 17250647 0> (DF) (ttl 64, id 11093)

17:50:22.500379 eth0 > intruderhost.4265 > myhost.netbios-ssn: P 1:13(12)
ack 1 win 32120 urg 12 nop,timestamp 17250647 0>>>> NBT (DF) (ttl 64, id
11095)
          4500 0040 2b57 4000 4006 78e4 c0a8 0aae
          c0a8 0a7e 10a9 008b a891 9a32 3fd0 9ba9
          8038 7d78 7dcb 000c 0101 080a 0107 3957
          0000 0000 796f 7520 6172 6520 6465 6164
           E^@ ^@ @  + W  @^@  @^F  x.. .... ^J..
          .... ^J ~ ^P.. ^@.. .... .. 2  ?.. ....
          .. 8  } x  }.. ^@^L ^A^A ^H^J ^A^G  9 W
          ^@^@ ^@^@  y o u   a r e   d e a d

17:50:22.500791 eth0 > intruderhost.4265 > myhost.netbios-ssn: F 13:13(0)
ack 1 win 32120 nop,timestamp 17250647 0> (DF) (ttl 64, id 11097)

17:50:22.500873 eth0 < myhost.netbios-ssn > intruderhost.4265: FP 1:6(5)
ack 13 win 17509 nop,timestamp 6007121 17250647>>>> NBT (DF) (ttl 128, id
33517)
          4500 0039 82ed 4000 8006 e154 c0a8 0a7e
          c0a8 0aae 008b 10a9 3fd0 9ba9 a891 9a3e
          8019 4465 7642 0000 0101 080a 005b a951
          0107 3957 8300 0001 8f

           E^@ ^@ 9 ....  @^@ ..^F .. T .... ^J ~
          .... ^J.. ^@.. ^P..  ?.. .... .... .. >
          ..^Y  D e  v B ^@^@ ^A^A ^H^J ^@ [ .. Q
          ^A^G  9 W ..^@ ^@^A
          ..

17:50:22.500920 eth0 > intruderhost.4265 > myhost.netbios-ssn: . 14:14(0)
ack 7 win 32120 nop,timestamp 17250647 6007121> (DF) (ttl 64, id 11098)
```



```
17:50:22.501139 eth0 < myhost.netbios-ssn > intruderhost.4265: . 7:7(0)
ack 14 win 17509 nop,timestamp 6007121 17250647> (DF) (ttl 128, id 33518)

17:50:22.516930 eth0 > intruderhost.4265 > myhost.netbios-ssn: R 14:14(0
ack 7 win 32120 nop,timestamp 17250647 6007121> (DF) (ttl 64, id 11111)

17:50:32.508044 eth0 > intruderhost.www > myhost.www: .
2493876034:2493876034(0) ack 749177432 win 8 (ttl 64, id 16912)
17:50:32.508096 eth0 > intruderhost.www > myhost.www: . 0:0(0) ack 1 win 8
(ttl 64, id 16912)

17:50:32.508179 eth0 > intruderhost.www > myhost.www: . 0:0(0) ack 1 win 8
(ttl 64, id 16912)
17:50:32.508262 eth0 > intruderhost.www > myhost.www: . 0:0(0) ack 1 win 8
(ttl 64, id 16912)

17:50:32.508344 eth0 > intruderhost.www > myhost.www: . 0:0(0) ack 1 win 8
(ttl 64, id 16912)
17:50:32.508514 eth0 < myhost.www > intruderhost.www: R
749177432:749177432(0) win 0 (ttl 128, id 33778)

17:50:32.508672 eth0 < myhost.www > intruderhost.www: R
749177432:749177432(0) win 0 (ttl 128, id 33779)
17:50:32.508739 eth0 < myhost.www > intruderhost.www: R
749177432:749177432(0) win 0 (ttl 128, id 33780)

17:50:32.508821 eth0 < myhost.www > intruderhost.www: R
749177432:749177432(0) win 0 (ttl 128, id 33781)
17:50:32.508902 eth0 < myhost.www > intruderhost.www: R
749177432:749177432(0) win 0 (ttl 128, id 33782)
```

This format is useful for practical work in the exam on the degree GCIA (GIAC Intrusion Analyst) in the SANS / GIAC.

Data source. Test LAN.

IDS, generated message about the attack. Tcpdump v.3.6.2.

The format of the message data. Tcpdump uses the following format to display the TCP packets:

- Time (hh: mm: ss.microseconds);

- Network interface name [ethO in our case];

- Source IP address. source port> destination IP address. destination port;

- TCP flags ["" - indicates that all the flag bits set to 0, "P" - PUSH flag, "F" - FIN flag, "S" - SYN flag, "R" - RESET flag];

- Beginning sequence number: ending sequence number (data bytes transfered);

- Ack the sequence number of the next block of data expected from the other end of the TCP connection;

- Win the number of bytes free in the receive buffer for receipt of data from the other end of the TCP connection;

- <Nop, nop, timestamp 6007121 17250647> - tcp options:

- Then - NO operation [pad options to 4-byte boundaries];

- Timestamp - carries a timestamp for each segment;

- (DF) do not fragment flag set;

- (Ttl time to live value, id IP identifier).

The probability of a fake IP-address of the sender of the attacking party. In this case, between the parties has been established the communication session, so the probability of fake IP-addresses is small. However, we can not exclude the possibility of introducing an attacker in a session (session hijacking) - in the case of interaction between Windows prediction number TCP-packet is trivial. To carry out this type of attack the attacker host must be connected to the communication link between the communicating parties (man-in-the-middle).

Description of attack. This fragment suggests the attack traffic "denial of service" against Windows port NetBIOS, known as WinNuke.

The attack is performed by sending out-of-band data on port 139 of the attacked host, which often leads to "hang» Windows-system. And other operating systems may be vulnerable to this type of attack, such as SCO OpenServer as it is exposed.

The expected result of this type of DoS-attacks - "freeze" of the targeted system.

The mechanism of the attack. Program implementing this type of attack can be found on the Internet. When the Windows-system receives a packet with the flag URGENT, it expects that this will be followed by the flag data. The lack of data after the flag URG leads her into confusion. This feature of Windows-systems (for which no corresponding software correction) contributes to the success of DoS-attacks Winnuke. Service Netbios (TCP port 139) is known as the most susceptible to this vulnerability, and most often attacked. However, the potential is not impossible the success of this type of attack and through other ports.

Such an attack can be made both remotely and locally (i.e. on the same machine on which the program runs Winnuke).

System Windows. The success of this attack against the Windows causes the system to hang and the appearance of "blue screen of death." The consequences of the attack are usually in the loss of unsaved user documents (changes).

Windows, Windows for Workgroups. In the event of the success of the attacks against the systems Windows for Workgroups, or Windows, the screen displays an error message on the program - "blue screen", notifies the user that the application is not responding. The consequences of the attack: a user typically loses any unsaved documents (changes).

Links to sources of information about the attack/vulnerability. Description Winnuke attacks can be found at the following links:

- http: //support.microsoft.som/support, http://ciac.llnl.gov/ciac/bulletins

Objectives of attack and the motivation of the attacking side (targeting and targeted attacks). Asked about the purpose and motivation of the attacking side, there are two answers:

1. This attack is a targeted and directed against a specific system containing the corresponding vulnerability.

2. It scans the network in search of systems that are experiencing this specific vulnerability.

For the correct answer you need additional study of event logs and IDS on the DOE to ascertain the event in history.

The magnitude of the risk. The magnitude of the risk (Severity), associated with the event, is calculated as follows:

(Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity.

We evaluate:

- Criticality of the attacked host - Criticality: 2 (host Windows);

- The possible consequences - Lethality: 0 (Windows hosts are not vulnerable to this issue, therefore, there are no consequences);

- The effectiveness of countermeasures system level - Sys Counters: 5 (installed the latest software correction);

- The effectiveness of countermeasures network layer - Net Counters: 5 (target host is located behind a filtering router and a firewall on the internal network).

Then Severity: (2 + 1) - (5 + 5) = -7.

Thus, the level of risk in this case is considerably less than 0 (event not worthy of serious attention of experts).

Advice on protection. Since the magnitude of the risk is very small, about the defense in this case, do not worry. In general, however, you can give the following recommendations for the protection of:

- The best way to protect against this kind of attacks from the external network is traditionally recognized as the use of DOE. Blocking Netbios service on the router and the firewall, performing the function of external corporate network gateway, is a common practice;

- Periodic network scanning using the scanner - a good preventive measure against such attacks (of course, if the database vulnerability scanner regularly updated);

- If the results of a network scan revealed Windows-systems vulnerable to this type of attack, then they need to install the software corrections by Microsoft, which can be found at:

http://support.microsoft. com / support /

Conclusions Chapter II.

1. The analysis of the properties and attributes determining threats, the methods efficiency signs of threats as well as threats management methods, including automated systems and computers.

2. Considered a quantitative approach in more detail by the example of the method for determining and managing threats. For the application of sustainability assessment methods for assessing and managing the risks identified the necessary characteristics and threats.

3. The existing different methods of intrusion detection analysis of suspicious traffic forming two mutually complementary types - quantitative and qualitative. Shown distinctive side and the transition from one species to another in order to manage risks.

CHAPTER III.

VALUATION OF ASSETS AND METHOD OF MANAGING PROBABILITY RISKS IN INFORMATION SYSTEM

3.1. Valuation of assets

Increased dependency on networked information systems, expanded internal communication facilities, explosive growth of Internet, closer ties with business partners, driven further by e-business, e-government initiatives and facilitated by the advances in information and communication technologies created many new opportunities, but also an environment with more risks than ever before.

A recent CERT Coordination Center paper [7] gives an overview of attack trends as follows:

automation; speed of attack tools,

increasing sophistication of attack tools,

faster discovery of vulnerabilities,

increasing permeability of firewalls,

increasing asymmetric threat,

increasing threat from infrastructure attacks.

Let me give two striking examples for the mentioned trends: Code-Red (CRv2) infected more than 359,000 computers worldwide in less than 14 hours [6]. CERT/CC reports 2,437 vulnerabilities in 2001, almost six times more than 417 in 1999 [CST02], not to mention the unknown vulnerabilities

Facing with these emerging challenges and considering other aspects like the generally more widespread insider threat and the non-technical information security leaks, managers and information security professionals should evaluate the specific risks to their organization to ensure an appropriate level of security enabling a seamless flow of their business operations.

In the present competitive environment however, most managers tend not to rely on some general statistics or projections, when it comes to invest in information security measures which may reduce IT performance or employee productivity, while not providing any tangible benefits. While these organizations may suffer serious losses due to security breaches, others may not be sure whether they over-protect their assets by supporting security initiatives, which may also result in loss of competitive advantage. The tool that should fine-tune and justify the required security measures and pave the way for informed management decisions is risk analysis and management.

3.1.1. Risk analysis and management

Risk, the possibility of damage or loss, is described mostly in dependencies of threat and vulnerability, or impact and probability. The general framework developed in 1992 NIST workshops cited in [8] formalized six concepts in risk analysis: "(1) assets, (2) vulnerabilities, (3) threats, (4) impacts, (5) likelihoods, and (6) safeguards."

There is a wide consensus among information security professionals that there can be no 100% security, or in other words no zero risk. Even assuming that a complete risk elimination is possible, this would rather be hindered by budget constraints or in most cases not attempted since measures would cost more than the asset value to be protected. Thus the emphasis of dealing with risks in this context moves from risk avoidance to risk management.

Basically risk analysis and risk management are defined as follows:

Risk analysis involves the identification and assessment of the levels of risks calculated from the known values of assets and the levels of threats to, and vulnerabilities of, those assets.

Risk management involves the identification, selection and adoption of

countermeasures justified by the identified risks to assets and the reduction of those risks to acceptable levels.

Thus the measure of risk can be determined as a product of threat, vulnerability and asset values:

Risk = Asset x Threat x Vulnerability

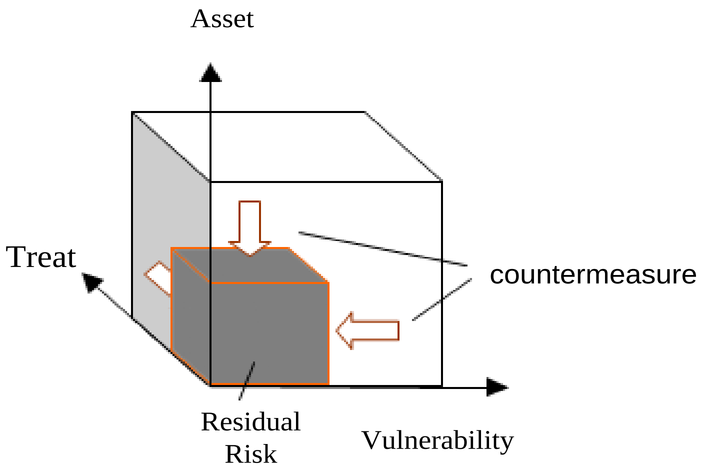


Figure 9: Risk as a function of asset value, threat and vulnerability.

The risk elements and their corresponding countermeasures can best be visualized with a cuboid (Figure 9). The system has an initial level of risk before any countermeasures are applied. Countermeasures, assuming that their values are assigned by the same parameters that are used for threat, vulnerability and asset valuation, can reduce risk, i.e. by reducing threat (e.g. locked doors, firewalls), reducing vulnerability (e.g. awareness, patches, hotfixes) or reducing asset value (e.g. encryption). After calculating the results from each combination of threat, vulnerability, asset and countermeasure the residual risk is determined. Here the impact element is covered in asset value, the likelihood in threat and vulnerability values.

Considering their business environment and resources available the decision makers in an organization may then implement one or more of the following risk management strategies:

- risk mitigation (reducing the risks with applying selected countermeasures),

- risk acceptance (accepting the residual risk or even the initial level if the countermeasures are more costly than the asset values),
- risk transfer (transferring the risk to another organization, e.g. by insurance or outsourcing).

The option of eliminating assets may also be mentioned here in case of very high risk, unavailable or unaffordable countermeasures as well as impossible risk transfer.

Today most current risk analysis methodologies start with identifying and valuing assets, followed by identifying threats likely to occur to them with related vulnerabilities. Finally, risk is determined for combinations of identified assets, threats and vulnerabilities to propose appropriate countermeasures. During this process two different measurement schemes can be applied to risk elements; quantitative or qualitative. Quantitative approach articulates risk in numerical terms, i.e. expected monetary loss and probability (e.g. annual loss expectancy, ALE). Qualitative approach has no numeric value and is usually opinion based. Results are summarized in words like “low”, “medium” and “high”. Advantages and disadvantages of both approaches are listed in several works including [KRA99].

There are a wide range of threats and vulnerabilities as well as different business environments and solutions with the need for balancing organizational and technical issues. This makes the implementation of risk analysis and measurement methodologies difficult and their outcome dependent on the experience of the persons involved, which causes inconsistence and sometimes-unsatisfactory results. Moreover, they require big amount of information to be gathered and a number of – by quantitative methods especially complex - calculations to be made. In order to address these problems automated tools are developed to raise the productivity by minimizing work and analysis time, as well as normalize differences of personal experience. There are a number of risk management packages listed in [NIS91], which gives an idea on different implementations, although the information is not up-to-date.

Developed software based on has took results by learning methods

It may be regarded as a benchmark to organizations for risk and contingency management considering the input from a number of government and private sector security experts in the tool.

3.1.2. The new software product “Risklarni baxolash” overview below.

The essential elements of data collection, analysis and output results, that should be present in an automated risk analysis tool are covered in the three stages of a “Risklarni baxolash” review:

- identifying and valuing assets,
- identifying threats and vulnerabilities, calculating risks,
- identifying and prioritizing countermeasures.

“Risklarni baxolash” tool guides the review with a process-flow oriented interface(Figure 10).

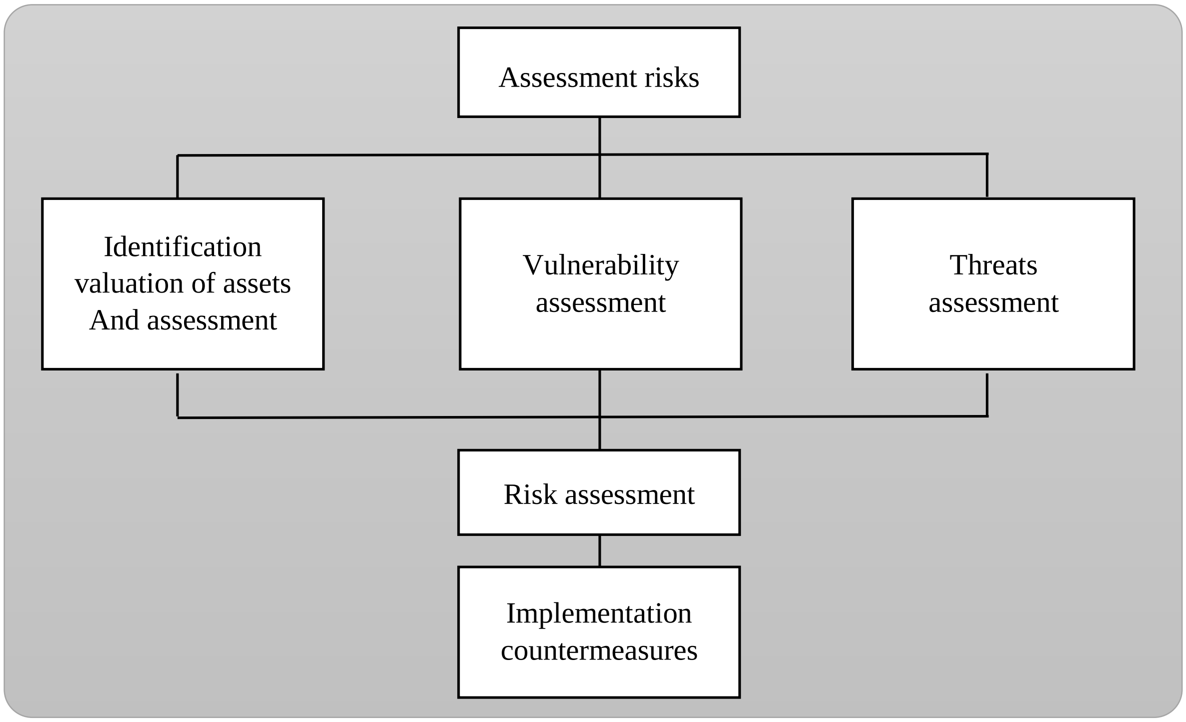

Assessment risks
Identification valuation of assets And assessment
Vulnerability assessment
Threats assessment
Risk assessment
Implementation countermeasures

Figure 10 “Risklarni baxolash” Overview Screen.

First step:

Identification and Valuation of Assets

- Asset values to an organization are central in determining the risks and the required security level. Three types of assets that make up the information are identified: data, application software and physical assets
- The valuation of information assets is regarded sometimes as a speculative activity, since it depends on who (e.g. sensitive information in hands of a competitor or a script -kiddie) and when (e.g. expirable passwords) possesses them. In "Risklarni baxolash" the reviewer conducts interviews with "data owners" (e.g. business unit managers) to value data assets, which raises the level of organizational acceptance of the review. This part of valuation is more difficult, since it may be hard to identify data (or business process) owners sometimes, or the interviewees may need some guidance for estimations, which may also be regarded as an followed process.

We can define every physic and intellectual tool's critically costs by following form.
Meanly,
We indicate every asset's (physic and intellectual) cost's-$\boldsymbol{A_i}$
After then count all assets (physic and intellectual) costs by followed form

$$\sum_{i=1}^{n} A_i \quad (5)$$

Every asset's critical coefficient is defined by

$$\partial = \frac{A_i}{\sum_{i=1}^{n} A_i} \quad (6)$$

Second step:

Threats and vulnerability assessment

In addition to asset values, the other two key components of a "Risklarni baxolash" risk analysis are levels (likelihoods of occurring) of threat and vulnerability. Threats and vulnerabilities are investigated against selected asset groups, which are put together to stay in reasonable review time frames. “Risklarni baxolash” has predefined tables for threat asset it involves two group elements:

Users/threat group.

use of another company employee ID (Masquerade);

using someone else's identity provider (Masquerade);

unauthorized use of another's identity (masquerade);

unauthorized access to the application;

the introduction of malicious software;

unauthorized use of system resources;

the use of telecommunications for the unauthorized access by employees of the organization;

the use of telecommunications for the unauthorized access by the service provider;

the use of telecommunications for the unauthorized access by outsiders;

errors in routing;

server failure;

network server failure;

failure of memory devices;

failure printers;

Malfunction network distributing components;

failure gateways;

failure or network management control servers;

failure of network interfaces;

failure of network services;

power failure;

failure of air conditioners;

failures of the system and network software;

failure of application software;

user error;

fire;

flooding;

natural disasters;

lack of staff;

theft by employees;

Theft by outsiders;

intentional unauthorized actions of employees;

intentional unauthorized actions of outsiders;

An exhaustive assessment of every threat to every asset group does not make sense and is not feasible, so the reviewer chooses here suitable threats and assets according to customer needs. On the vulnerability front, it should be noted that “Risklarni baxolash” is targeting a managerial level risk assessment, thus detailed technical, system specific vulnerabilities which may be identified by vulnerability scanners are not addressed by the tool.

Third step:

Organizational vulnerability

In the following 13 organizational components are took by statistics center, its help to us estimate organizational protecting system.

1. Enable ports (yes/no);

2. Password (yes/no);

3.Remote control(yes/no);

4.Firewall(yes/no);

5.USB/DVD Rom(yes/no);

6.UPS(yes/no);

7.Blocked case(yes/no);

8.Autoload software(yes/no);

9.Excessive software(yes/no);

10.Internet connecting(yes/no);

11.Social networks(yes/no);

12.External e-mail(yes/no);

13.Antivirus(yes/no);

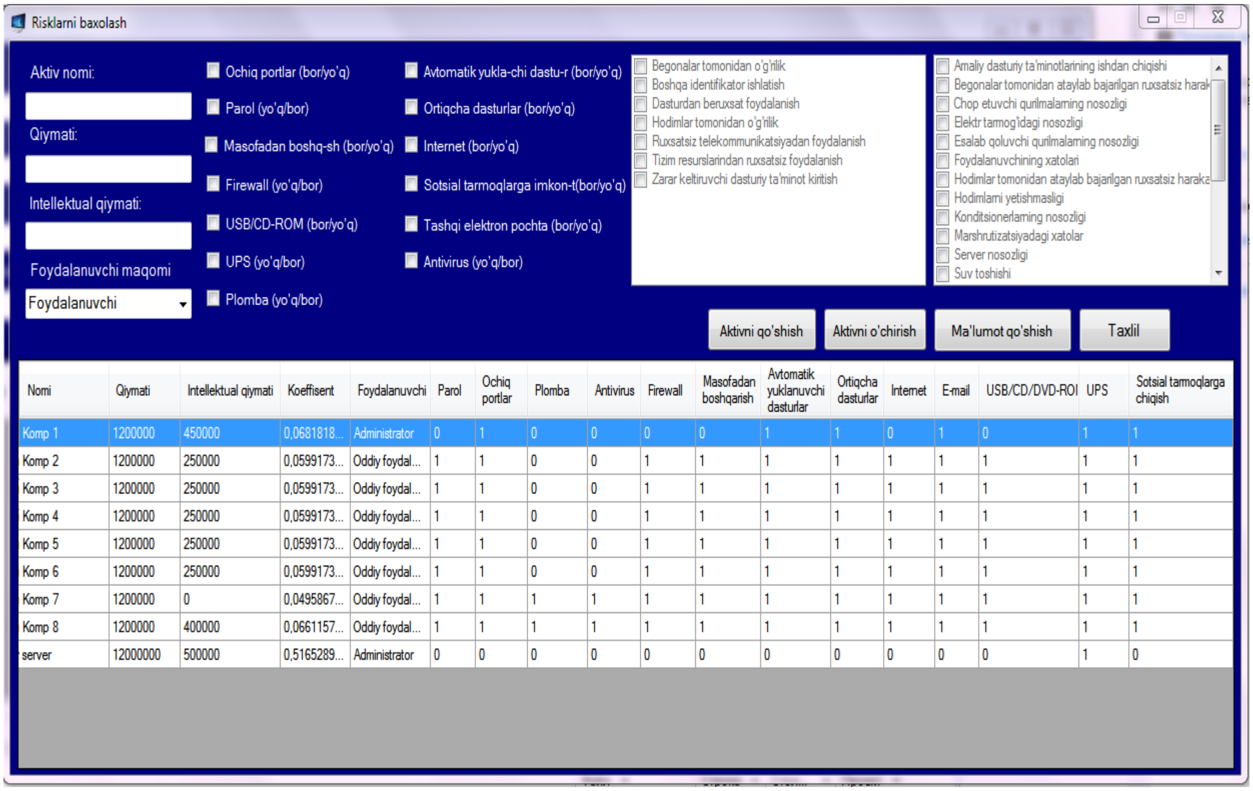
By given information we can estimate of every organization's is organized security system level. First of all, we should compare between protection system of the companies with the result of experts standards, and it help to us estimate the level of enterprises protection system. Result of the process is showed by per cent. The form gave the following:

$$\delta = \frac{n}{14} \quad (7)$$

Where n −the number of implemented protecting components.

3.1.3. The part of program.

The program is created by C#, which object oriented programming language. It consist of the number of windows. As well as the results of assessment is given by bar graph.



Risklarni baxolash

Aktiv nomi:

Qiymati:

Intellektual qiymati:

Foydalanuvchi maqomi: Foydalanuvchi

□ Ochiq portlar (bor/yo'q)
□ Parol (yo'q/bor)
□ Masofadan boshq-sh (bor/yo'q)
□ Firewall (yo'q/bor)
□ USB/CD-ROM (bor/yo'q)
□ UPS (yo'q/bor)
□ Plomba (yo'q/bor)

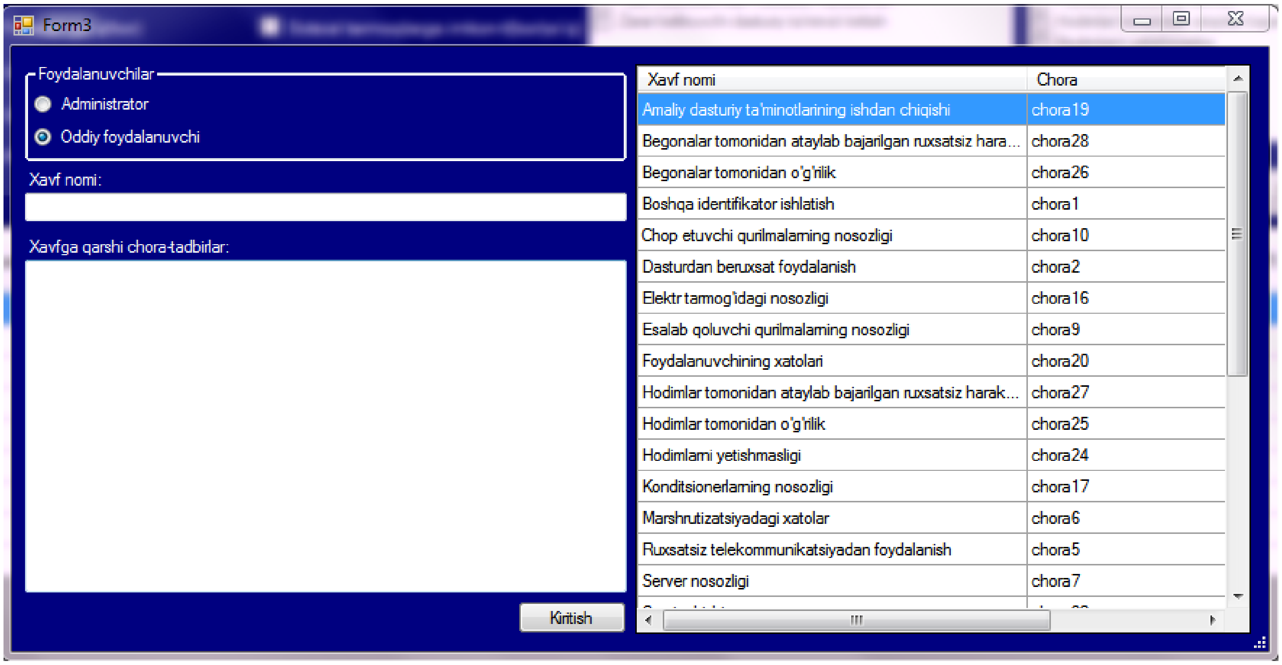
□ Avtomatik yukla-chi dastu-r (bor/yo'q)
□ Ortiqcha dasturlar (bor/yo'q)
□ Internet (bor/yo'q)
□ Sotsial tarmoqlarga imkon-t(bor/yo'q)
□ Tashqi elektron pochta (bor/yo'q)
□ Antivirus (yo'q/bor)

□ Begonalar tomonidan o'g'rilik
□ Boshqa identifikator ishlatish
□ Dasturdan beruxsat foydalanish
□ Hodimlar tomonidan o'g'rilik
□ Ruxsatsiz telekommunikatsiyadan foydalanish
□ Tizim resurslarindan ruxsatsiz foydalanish
□ Zarar keltiruvchi dasturiy ta'minot kiritish

□ Amaliy dasturiy ta'minotlarining ishdan chiqishi
□ Begonalar tomonidan ataylab bajarilgan ruxsatsiz harak
□ Chop etuvchi qurilmalarning nosozligi
□ Elektr tarmog'idagi nosozligi
□ Esalab qoluvchi qurilmalarning nosozligi
□ Foydalanuvchining xatolari
□ Hodimlar tomonidan ataylab bajarilgan ruxsatsiz haraka
□ Hodimlarni yetishmasligi
□ Konditsionerlarning nosozligi
□ Marshrutizatsiyadagi xatolar
□ Server nosozligi
□ Suv toshishi

Nomi	Qiymati	Intellektual qiymati	Koeffisent	Foydalanuvchi	Parol	Ochiq portlar	Plomba	Antivirus	Firewall	Masofadan boshqarish	Avtomatik yuklanuvchi dasturlar	Ortiqcha dasturlar	Internet	E-mail	USB/CD/DVD-ROI	UPS	Sotsial tarmoqlarga chiqish
Komp 1	1200000	450000	0,0681818...	Administrator	0	1	0	0	0	0	1	1	0	1	0	1	1
Komp 2	1200000	250000	0,0599173...	Oddiy foydal...	1	1	0	0	1	1	1	1	1	1	1	1	1
Komp 3	1200000	250000	0,0599173...	Oddiy foydal...	1	1	0	0	1	1	1	1	1	1	1	1	1
Komp 4	1200000	250000	0,0599173...	Oddiy foydal...	1	1	0	0	1	1	1	1	1	1	1	1	1
Komp 5	1200000	250000	0,0599173...	Oddiy foydal...	1	1	0	0	1	1	1	1	1	1	1	1	1
Komp 6	1200000	250000	0,0599173...	Oddiy foydal...	1	1	0	0	1	1	1	1	1	1	1	1	1
Komp 7	1200000	0	0,0495867...	Oddiy foydal...	1	1	1	1	1	1	1	1	1	1	1	1	1
Komp 8	1200000	400000	0,0661157...	Oddiy foydal...	1	1	1	1	1	1	1	1	1	1	1	1	1
server	12000000	500000	0,5165289...	Administrator	0	0	0	0	0	0	0	0	0	0	0	1	0

Figure 11. The main window.



Form3

Foydalanuvchilar
○ Administrator
● Oddiy foydalanuvchi

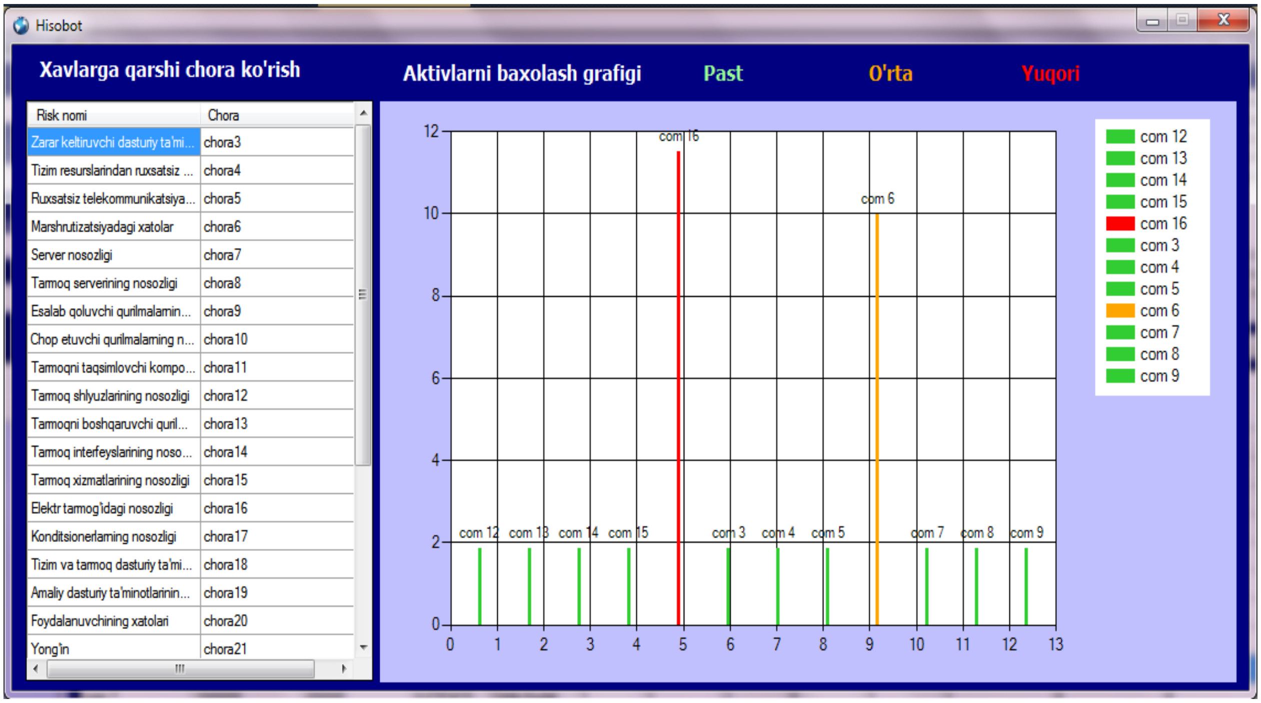
Xavf nomi:

Xavfga qarshi chora-tadbirlar:

Xavf nomi	Chora
Amaliy dasturiy ta'minotlarining ishdan chiqishi	chora19
Begonalar tomonidan ataylab bajarilgan ruxsatsiz hara...	chora28
Begonalar tomonidan o'g'rilik	chora26
Boshqa identifikator ishlatish	chora1
Chop etuvchi qurilmalarning nosozligi	chora10
Dasturdan beruxsat foydalanish	chora2
Elektr tarmog'idagi nosozligi	chora16
Esalab qoluvchi qurilmalarning nosozligi	chora9
Foydalanuvchining xatolari	chora20
Hodimlar tomonidan ataylab bajarilgan ruxsatsiz harak...	chora27
Hodimlar tomonidan o'g'rilik	chora25
Hodimlarni yetishmasligi	chora24
Konditsionerlarning nosozligi	chora17
Marshrutizatsiyadagi xatolar	chora6
Ruxsatsiz telekommunikatsiyadan foydalanish	chora5
Server nosozligi	chora7

Figure 12. “Risklarni boshqarish” By this form we can insert:

- probability of threats on the companies
- countermeasure probability threats .



Xavlarga qarshi chora ko'rish

Risk nomi	Chora
Zarar keltiruvchi dasturiy ta'mi...	chora3
Tizim resurslarindan ruxsatsiz ...	chora4
Ruxsatsiz telekommunikatsiya...	chora5
Marshrutizatsiyadagi xatolar	chora6
Server nosozligi	chora7
Tarmoq serverining nosozligi	chora8
Esalab qoluvchi qurilmalarnin...	chora9
Chop etuvchi qurilmalarning n...	chora10
Tarmoqni taqsimlovchi kompo...	chora11
Tarmoq shlyuzlarining nosozligi	chora12
Tarmoqni boshqaruvchi quril...	chora13
Tarmoq interfeyslarining noso...	chora14
Tarmoq xizmatlarining nosozligi	chora15
Elektr tarmog'idagi nosozligi	chora16
Konditsionerlarning nosozligi	chora17
Tizim va tarmoq dasturiy ta'mi...	chora18
Amaliy dasturiy ta'minotlarinin...	chora19
Foydalanuvchining xatolari	chora20
Yong'in	chora21

Figure 13. “Risklarni boshqarish” the form of result

As can be seen from the diagram is that the following consequences of estimating probability threats on assets:

- The red line shows us the level of high degree threats on the assets.
- The yellow line shows us the level of medium degree threats on assets.
- The green line shows us the level of low degree threats on assets.

3.2. Uses of IDPS Technologies

IDPSs are primarily focused on identifying possible incidents. For example, an IDPS could detect when an attacker has successfully compromised a system by exploiting a vulnerability in the system. The IDPS could then report the incident to security administrators, who could quickly initiate incident response actions to minimize the damage caused by the incident. The IDPS could also log information that could be used by the incident handlers.

Many IDPSs can also be configured to recognize violations of security policies. For example, some IDPSs can be configured with firewall rule set-like settings, allowing them to identify network traffic that violates the organization’s security or acceptable use policies. Also, some IDPSs can monitor file transfers and identify ones that might be suspicious, such as copying a large database onto a user’s laptop. Many IDPSs can also identify reconnaissance activity, which may indicate that an attack is imminent. For example, some attack tools and forms of malware, particularly worms, perform reconnaissance activities such as host and port scans to identify targets for subsequent attacks. An IDPS might be able to block reconnaissance and notify security administrators, who can take actions if needed to alter other security controls to prevent related incidents. Because reconnaissance activity is so frequent on the Internet, reconnaissance detection is often performed primarily on protected internal networks.

In addition to, identifying incidents and supporting incident response efforts, organizations have found other uses for IDPSs, including the following: Identifying security policy problems. An IDPS can provide some degree of quality control for security policy implementation, such as duplicating firewall rule sets and alerting when it sees network traffic that should have been blocked by the firewall but was not because of a firewall configuration error.

Documenting the existing threat to an organization. IDPSs log information about the threats that they detect. Understanding the frequency and characteristics of attacks against an organization’s computing resources is helpful in identifying the appropriate security measures for protecting the resources. The information can also be used to educate management about the threats that the organization faces. Deterring individuals from violating security policies. If individuals are aware that their actions are being monitored by IDPS technologies for security policy violations, they may be less likely to commit such violations because of the risk of detection. Because of the increasing dependence on information systems and the prevalence and potential impact of intrusions against those systems, IDPSs have become a necessary addition to the security infrastructure of nearly every organization.

3.2.1. Key Functions of IDPS Technologies

There are many types of IDPS technologies, which are differentiated primarily by the types of events that they can recognize and the methodologies that they use to identify incidents. In addition to monitoring and analyzing events to identify undesirable activity, all types of IDPS technologies typically perform the following functions:

Recording information related to observed events. Information is usually recorded locally, and might also be sent to separate systems such as centralized logging servers, security information and event management (SIEM) solutions, and enterprise management systems. Notifying security administrators of important observed events. This notification, known as an alert, occurs through any of several methods, including the following: e-mails, pages, messages on the IDPS user interface, Simple Network Management Protocol (SNMP) traps, syslog messages, and user-defined programs and scripts. A notification message typically includes only basic information regarding an event; administrators need to access the IDPS for additional information.

Producing reports. Reports summarize the monitored events or provide details on particular events of interest. Some IDPSs are also able to change their security profile when a new threat is detected. For example, an IDPS might be able to collect more detailed information for a particular session after malicious activity is detected within that session. An IDPS might also alter the settings for when certain alerts are triggered or what priority should be assigned to subsequent alerts after a particular threat is detected. IPS technologies are differentiated from IDS technologies by one characteristic: IPS technologies can respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which can be divided into the following groups: The IPS stops the attack itself. Examples of how this could be done are as follows:

- Terminate the network connection or user session that is being used for the attack
- Block access to the target (or possibly other likely targets) from the offending user account, IP address, or other attacker attribute
- Block all access to the targeted host, service, application, or other resource.

The IPS changes the security environment. The IPS could change the configuration of other security controls to disrupt an attack. Common examples are reconfiguring a network device (e.g., firewall, router, switch) to block access from the attacker or to the target, and altering a host-based firewall on a target to block incoming attacks. Some IPSs can even cause patches to be applied to a host if the IPS detects that the host has vulnerabilities. The IPS changes the attack's content. Some IPS technologies can remove or replace malicious portions of an attack to make it benign. A simple example is an IPS removing an infected file attachment from an e-mail and then permitting the cleaned e-mail to reach its recipient. A more complex example is an IPS that acts as a proxy and normalizes incoming requests, which means that the proxy repackages the payloads of the requests, discarding header information. This might cause certain attacks to be discarded as part of the normalization process. Another common attribute of IDPS technologies is that they cannot provide completely accurate detection. When an IDPS incorrectly identifies benign activity as being malicious, a false positive has occurred. When an IDPS fails to identify malicious activity, a false negative has occurred. It is not possible to eliminate all false positives and negatives; in most cases, reducing the occurrences of one increases the occurrences of the other. Many organizations choose to decrease false negatives at the cost of increasing false positives, which means that more malicious events are detected but more analysis resources are needed to differentiate false positives from true malicious events. Altering the configuration of an IDPS to improve its detection accuracy is known as tuning. Most IDPS technologies also offer features that compensate for the use of common evasion techniques. Evasion is modifying the format or timing of malicious activity so that its appearance changes but its effect is the same. Attackers use evasion techniques to try to prevent IDPS technologies from detecting their attacks. For example, an attacker could encode text characters in a particular way, knowing that the target understands the encoding and hoping that any monitoring IDPSs do not. Most IDPS technologies can overcome common evasion techniques by duplicating special processing performed by the targets. If the IDPS can "see" the activity in the same way that the target would, then evasion techniques will generally be unsuccessful at hiding attacks.

3.2.2. Common Detection Methodologies

IDPS technologies use many methodologies to detect incidents. The primary classes of detection methodologies: signature-based, anomaly-based, and stateful protocol analysis, respectively. Most IDPS technologies use multiple detection methodologies, either separately or integrated, to provide more broad and accurate detection.

- **Signature-Based Detection**

A signature is a pattern that corresponds to a known threat. Signature-based detection is the process of comparing signatures against observed events to identify possible incidents.

Examples of signatures are as follows:

- A telnet attempt with a username of “root”, which is a violation of an organization’s security policy.
- An e-mail with a subject of “Free pictures!” and an attachment filename of “freepics.exe”, which are characteristics of a known form of malware.
- An operating system log entry with a status code value of 645, which indicates that the host’s auditing has been disabled.

Signature-based detection is very effective at detecting known threats but largely ineffective at detecting previously unknown threats, threats disguised by the use of evasion techniques, and many variants of known threats. For example, if an attacker modified the malware in the previous example to use a filename of “freepics2.exe”, a signature looking for “freepics.exe” would not match it. Signature-based detection is the simplest detection method because it just compares the current unit of activity, such as a packet or a log entry, to a list of signatures using string comparison operations. Signature-based detection technologies have little understanding of many network or application protocols and cannot track and understand the state of complex communications. For example, they cannot pair a request with the corresponding response, such as knowing that a request to a Web server for a particular page generated a response status code of 403, meaning that the server refused to fill the request. They also lack the ability to remember previous requests when processing the current request. This limitation prevents signature-based detection methods from detecting attacks that comprise multiple events if none of the events contains a clear indication of an attack.

- **Anomaly-Based Detection**

Anomaly-based detection is the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. An IDPS using anomaly-based detection has profiles that represent the normal behavior of such things as users, hosts, network connections, or applications. The profiles are developed by monitoring the characteristics of typical activity over a period of time.

For example, a profile for a network might show that Web activity comprises an average of 13% of network bandwidth at the Internet border during typical workday hours. The IDPS then uses statistical methods to compare the characteristics of current activity to thresholds related to the profile, such as detecting when Web activity comprises significantly more bandwidth than expected and alerting an administrator of the anomaly. Profiles can be developed for many behavioral attributes, such as the number of e-mails sent by a user, the number of failed login attempts for a host, and the level of processor usage for a host in a given period of time.

The major benefit of anomaly-based detection methods is that they can be very effective at detecting previously unknown threats. For example, suppose that a computer becomes infected with a new type of malware. The malware could consume the computer’s processing resources, send large numbers of e-mails, initiate large numbers of network connections, and perform other behavior that would be significantly different from the established profiles for the computer. An initial profile is generated over a period of time (typically days, sometimes weeks) sometimes called a training period. Profiles for anomaly-based detection can either be static or dynamic. Once generated, a static profile is unchanged unless the IDPS is specifically directed to generate a new profile. A dynamic profile is adjusted constantly as additional events are observed. Because systems and networks change over time, the corresponding measures of normal behavior also change; a static profile will eventually become inaccurate, so it needs to be regenerated periodically. Dynamic profiles do not have this problem, but they are susceptible to evasion attempts from attackers. For example, an attacker can perform small amounts of malicious activity occasionally, then slowly increase the frequency and quantity of activity. If the rate of change is sufficiently slow, the IDPS might think the malicious activity is normal behavior and include it in its profile. Malicious activity might also be observed by an IDPS while it builds its initial profiles. Inadvertently including malicious activity as part of a profile is a common problem with anomaly-based IDPS products. (In some cases, administrators can modify the profile to exclude activity in the profile that is known to be malicious.) Another problem with building profiles is that it can be very challenging in some cases to make them accurate, because computing activity can be so complex. For example, if a particular maintenance activity that performs large file transfers occurs only once a month, it might not be observed during the training period; when the maintenance occurs, it is likely to be considered a significant deviation from the profile and trigger an alert. Anomaly-based IDPS products often produce many false positives because of benign activity that deviates significantly from profiles, especially in more diverse or dynamic environments. Another noteworthy problem with the use of anomaly-based detection techniques is that it is often difficult for analysts to determine why a particular alert was generated and to validate that an alert is accurate and not a false positive, because of the complexity of events and number of events that may have caused the alert to be generated.

- **Stateful Protocol Analysis**

Stateful protocol analysis is the process of comparing predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations. Unlike anomaly-based detection, which uses host or network-specific profiles, stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used. The “stateful” in stateful protocol analysis means that the IDPS is capable of understanding and tracking the state of network, transport, and application protocols that have a notion of state. For example, when a user starts a File Transfer Protocol (FTP) session, the session is initially in the unauthenticated state. Unauthenticated users should only perform a few commands in this state, such as viewing help information or providing usernames and passwords. An important part of understanding state is pairing requests with responses, so when an FTP authentication attempt occurs, the IDPS can determine if it was successful by finding the status code in the corresponding response.

Once the user has authenticated successfully, the session is in the authenticated state, and users are expected to perform any of several dozen commands. Performing most of these commands while in the unauthenticated state would be considered suspicious, but in the authenticated state performing most of them is considered benign. Stateful protocol analysis can identify unexpected sequences of commands, such as issuing the same command repeatedly or issuing a command without first issuing a command upon which it is dependent. Another state tracking feature of stateful protocol analysis is that for protocols that perform authentication, the IDPS can keep track of the authenticator used for each session, and record the authenticator used for suspicious activity. This is helpful when investigating an incident. Some IDPSs can also use the authenticator information to define acceptable activity differently for multiple classes of users or specific users. The “protocol analysis” performed by stateful protocol analysis methods usually includes reasonableness checks for individual commands, such as minimum and maximum lengths for arguments. If a command typically has a username argument, and usernames have a maximum length of 20 characters, then an argument with a length of 1000 characters is suspicious. If the large argument contains binary data, then it is even more suspicious. Stateful protocol analysis methods use protocol models, which are typically based primarily on protocol standards from software vendors and standards bodies(e.g., Internet Engineering Task Force [IETF] Request for Comments [RFC]). The protocol models also typically take into account variances in each protocol’s implementation. Many standards are not exhaustively complete in explaining the details of the protocol, which causes variations among implementations. In addition, many vendors either violate standards or add proprietary features, some of which may replace features from the standards. For proprietary protocols, complete details about the protocols are often not available, making it difficult for IDPS technologies to perform comprehensive, accurate analysis. As protocols are revised and vendors alter their protocol implementations, IDPS protocol models need to be updated to reflect those changes. The primary drawback to stateful protocol analysis methods is that they are very resource-intensive because of the complexity of the analysis and the overhead involved in performing state tracking for many simultaneous sessions. Another serious problem is that stateful protocol analysis methods cannot detect attacks that do not violate the characteristics of generally acceptable protocol behavior, such as performing many benign actions in a short period of time to cause a denial of service. Yet another problem is that the protocol model used by an IDPS might conflict with the way the protocol is implemented in particular versions of specific applications and operating systems, or how different client and server implementations of the protocol interact.

3.2.3. Types of IDPS Technologies

There are many types of IDPS technologies. For the purposes of this document, they are divided into the following four groups based on the type of events that they monitor and the ways in which they are deployed:

- Network-Based, which monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity. It can identify many different types of events of interest. It is most commonly deployed at a boundary between networks, such as in proximity to border firewalls or routers, virtual private network (VPN) servers, remote access servers, and wireless networks.
- Wireless, which monitors wireless network traffic and analyzes its wireless networking protocols to identify suspicious activity involving the protocols themselves. It cannot identify suspicious activity in the application or higher-layer network protocols (e.g., TCP, UDP) that the wireless network traffic is transferring. It is most commonly deployed within range of an organization's wireless network to monitor it, but can also be deployed to locations where unauthorized wireless networking could be occurring. Network Behavior Analysis (NBA), which examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware (e.g., worms, backdoors), and policy

violations (e.g., a client system providing network services to other systems). NBA systems are most often deployed to monitor flows on an organization’s internal networks, and are also sometimes deployed where they can monitor flows between an organization’s networks and external networks (e.g., the Internet, business partners’ networks). NBA products are discussed in more detail in Section 6. Host-Based, which monitors the characteristics of a single host and the events occurring within that host for suspicious activity. Examples of the types of characteristics a host-based IDPS might monitor are network traffic (only for that host), system logs, running processes, application activity, file access and modification, and system and application configuration changes. Host-based IDPSs are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information. Section 7 contains additional information on host-based IDPSs. Some forms of IDPS are more mature than others because they have been in use much longer. Network based IDPS and some forms of host-based IDPS have been commercially available for over ten years. Network behavior analysis software is a some what newer form of IDPS that evolved in part from products created primarily to detect DDoS attacks, and in part from products developed to monitor traffic flows on internal networks. Wireless technologies are a relatively new type of IDPS, developed in response to the popularity of wireless local area networks (WLAN) and the growing threats against WLANs and WLAN clients.

3.2.4. Firewalls and Routers

Firewalls (network-based and host-based) and routers filter network traffic based on TCP/IP characteristics such as the source and destination IP addresses, the transport layer protocol (e.g., TCP, UDP, ICMP), and basic protocol information (e.g., TCP or UDP port numbers, ICMP type and code). Most firewalls and routers log which connections or connection attempts they block; the blocked activity is often generated by unauthorized access attempts from automated attack tools, port scanning, and malware. Some network-based firewalls also act as proxies. When a proxy is used, each successful connection attempt actually results in the creation of two separate connections: one between the client and the proxy server, and another between the proxy server and the true destination. Many proxies are application-specific, and some actually perform some analysis and validation of common application protocols, such as HTTP. The proxy may reject client requests that appear to be invalid (which could include some forms of attacks) and log information regarding these requests. Ways in which firewalls and routers complement IDPSs include the following:

Network-based firewalls and routers often perform network address translation (NAT), which is the process of mapping addresses on one network to addresses on another network. NAT is most often accomplished by mapping private addresses from an internal network to one or more public addresses on a network that is connected to the Internet. Firewalls and routers that perform NAT typically record each NAT address and mapping. IDPS users may need to make use of this mapping information to identify the actual IP address of a host behind a device performing NAT.

If IDPSs and other security controls (e.g., antivirus software) cannot stop a new network-borne threat, such as a network service worm or denial of service attack, firewalls or routers might have to be temporarily reconfigured to block the threat.

Routers are often used as data sources for NBA deployments. Limitations of firewalls and routers in the context of IDPS include the following:

Firewalls and routers cannot detect most types of malicious activity.

Firewalls and routers typically log relatively little information, such as the basic characteristics of denied connection attempts only, and they rarely record the content of any packets. NBA technologies and some network-based IDPSs can log much more information about network traffic than firewalls and routers do.

3.3. Development new algorithm module

The results of analyzes created new algorithm of determining attacks and risk management in Information system. Iit consists of checking system, virtual system and IDPS technology. In the following model shows of it

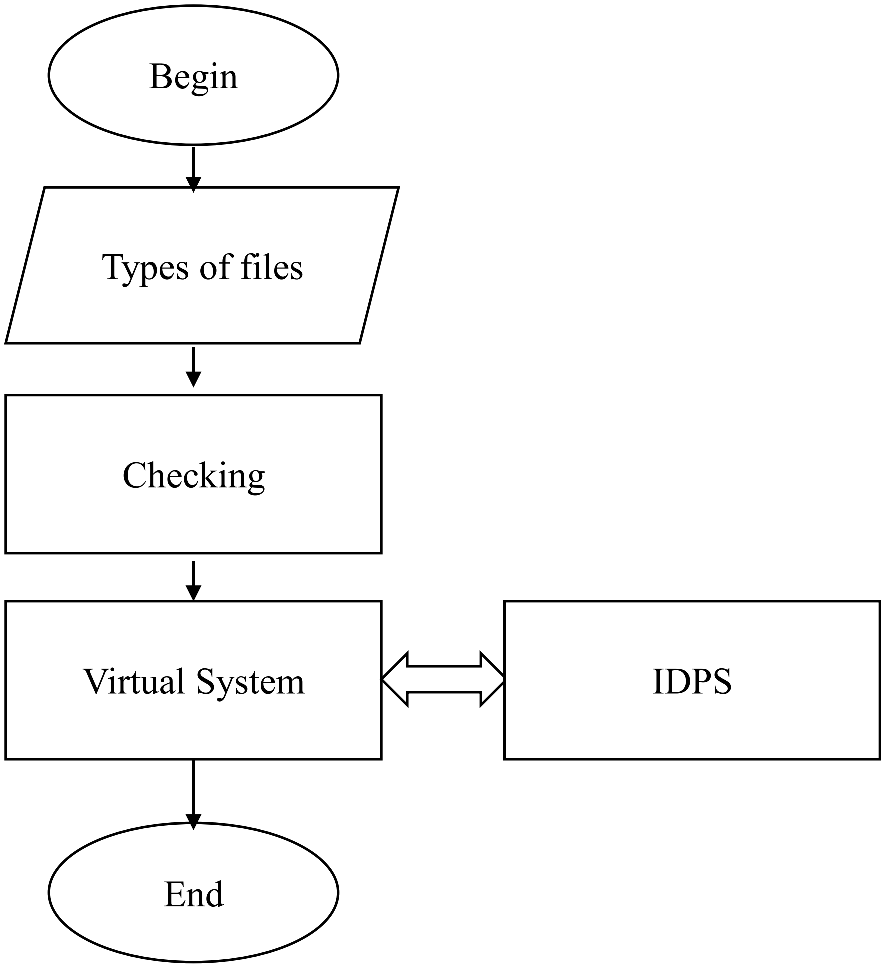


Figure 14.Structure of new algorithm module.

IDPS technology checking following types of file:

- File syslog, containing the data from the kernel OS and applications that are registered through the system syslog

- File wtmp, including information about the users registered in the system and running processes them;

- File btmp, where there is information about all failed login attempts;

- Accounting system user processes pacct, recording a variety of information related to their operation and use of system resources

In addition to these sources of information is a file in which data is stored in binary format, you can connect additional data sources that use the text format for storing data, such as file / var / adm / messages, and any other text files, event logs, operating system and applications.

- ➢ Checking system

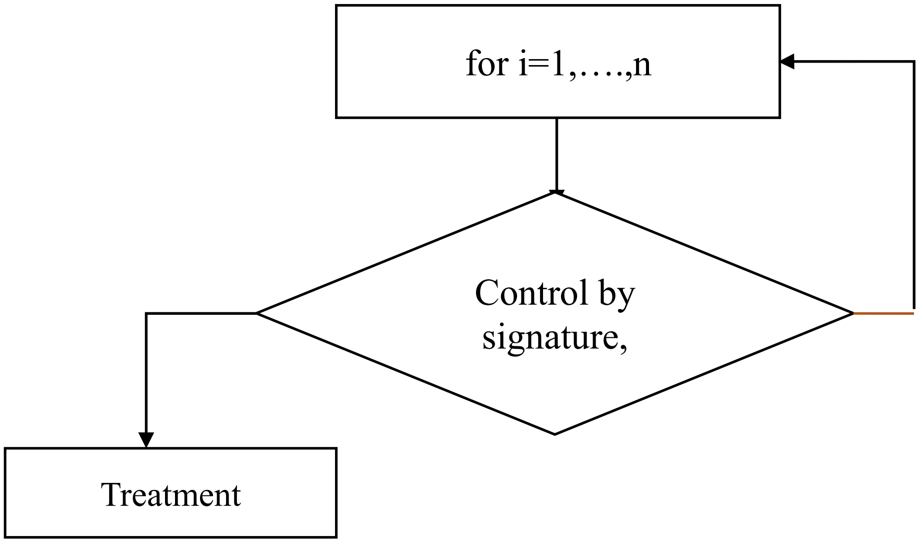


Figure 15. The model the process of checking system as Firewall system

- ➢ IDPS technology:
- Signature analyze
- Anomalous analyze

- Stateful traffic protocol;

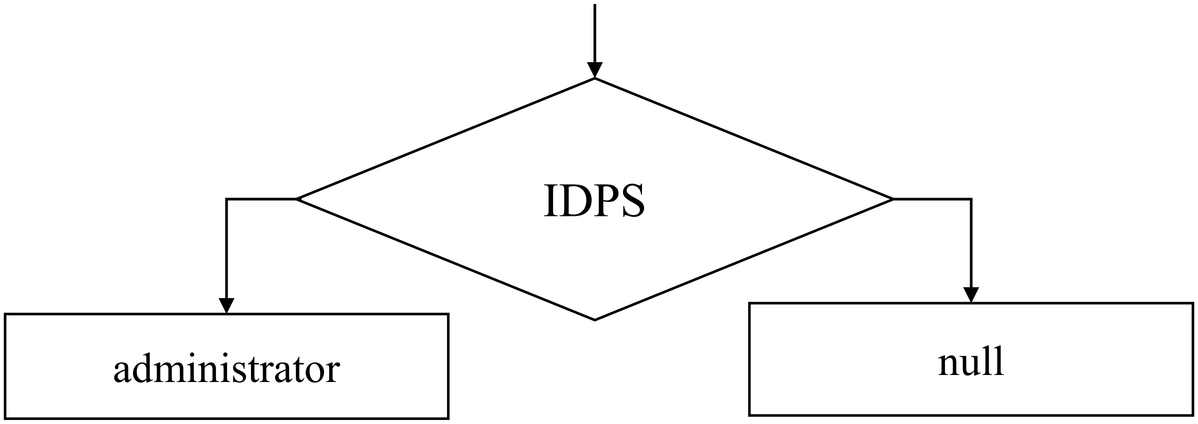


Figure 16. The model of the process of IDPS(Intrusion Detection and Prevention System)

Closing

Researches have shown that there are several threats to information security management. Each method is based on the Threat Management certain sign, and sometimes on a few signs. The analysis showed that not all methods of management of threats can be obtained by simple calculations. Besides, not every control method allows to obtain an effective method of preventing threats. Also in the analysis were defined requirements management techniques uniquely allows information to prevent risks, which allowed to formulate the problem of research.

Thus, researches have yielded the following results:

1. Analysis of the properties and signs of threat detection, the methods efficiency signs of threats as well as threats management methods, including automated systems and computers.

2. The existing different methods of intrusion detection analysis of suspicious traffic forming two mutually complementary types - quantitative and qualitative. Shown distinctive side and the transition from one species to another in order to manage risks.

3. Analysis of the properties and signs of classification of threats, the methods of hazard assessment of threats, as well as the classification of objects of protection, including automated systems and computers.

4. As part of the research and analysis of the practical application of the technology method of evaluating the threats to information risk, propose an algorithm for solving the problem: threat assessment - identifying features and characteristics of threats - the definition of quality and (or) quantitative indicators - risk assessment of asset information system.

5. The damage is considered as a category of threat assessment listed manifestations of possible damage, which consists of three groups, produced rankings ways to show the

types of threats on the degree of danger of indirect indicators using the expert-analytical method for the ten-point scale.

6. The developed algorithm asset valuation information system, the technique of valuation of assets. Implemented software for calculating critical threats to information system assets.

7. This estimate allows to evaluate the risk in terms of justification of the cost of implementing risk management systems.

8. The algorithm of the risk management information system comprises the following parameters:

• Signature-based method for the analysis of threats;

• Anomalous method of analyzing dangerous traffic;

• Analysis of suspicious traffic using heuristic analysis, in case of threat signatures to supplement the transfer of hazardous signature database;

• The decision to block dangerous traffic is assigned to an expert group with the purpose to prevent false information protection system;

• The effectiveness of methods of valuation of assets information system;

• Effectiveness study the cost of implementing a risk management system;

• Effectiveness of risk management techniques.

Due to the proposed sequence of the task: analysis of risk management - identifying features and characteristics of the existing risk management practices - to develop an algorithm information risk management - defining quality and (or) quantitative indicators - risk assessment asset information system information, the opportunity, rationale for the introduction of expenditure the risk management system. The resulting algorithm allows risk management capabilities prevent accidental triggering of the system of protection of information resources and complement the signature database of information threats.

REFERENCES

1. June 27, 2013y DP-1989 Decree of the President of the Republic of Uzbekistan "On measures for further development of the National Information and Communication System of the Republic of Uzbekistan".
2. Decree of the President of the Republic of Uzbekistan № PP-2158 on April 3, 2014 "On measures to further the implementation of information and communication technologies in the real economy".
3. Decree of the Cabinet of Ministers № 250 of the PCM-16 September 2013 "On measures to further the implementation of information and communication technologies in the real economy".
4. Petrenko S.A. “Risk management of company” Express-electronika . - № 2-3. - 2002. - C. 106-113.
5. Руководство по управлению рисками безопасности. Группа разработки решений Майкрософт по безопасности и соответствию регулятивным нормам и Центр Microsoft security center of excellence. URL:http://www.microsoft.com/rus/technet/security/guidance
6. “CAIDA Analysis of Code -Red.” 15 August 2001. URL: http://www .caida.org/anal ysis/security/code-red/
7. “Overview of Attack Trends.” 19 February 2002. URL: http://www .isall iance.org/resources/papers/
8. RiskWatch users manual. URL: http://www.riskwatch.com.
9. Craft R, Wyss G, Vandewart R, Funkhouser D. “An Open Framework for Risk Management.” 21st National Information Systems Security Conference Proceedings. October 1998. URL: http://csrc.nist.gov/nissc/1998/proceedings/paper
10. Александрович Г.Я., Нестеров С.А., Петренко С.А. Автоматизация оценки Информационных рисков компании. // Защита информации. Конфидент. 2003, № 2. С.78-8.

11. Brewer, Dr. David. “Risk Assessment Models and Evolving Approaches.” IAAC workshop, London. July 2000.
URL:http://www.gam massl.co.uk/topics/IAAC.htm

12. Karen S, Peter M. “Guide to Intrusion Detection and Prevention Systems (IDPS)” (February 2007)

13. Zeki Y. “A qualitative risk analysis and management tool–CRAMM” SANS Institute

14. Нестеров С.А. “Анализ и управление рисками в сфере информационной безопасности”. Санкт-Петербург 2007.

15. Lili S.R, “An Information Systems Security Risk Assessment Model under Dempster-Shafer Theory of Belief Functions”
University of New Jersey, Spring 2006.

16. P.X.Oripov, A.I.Ubaydullayev “Quality of probability risks assessment in information technologies” Department of Information security, TUIT

17. P.X.Oripov, A.I.Ubaydullayev “ ” Department of Information security, TUIT

18. P.X.Oripov, E.Q.Qaxramonov “ ” Department of Information security, TUIT

19. Information Systems Security: A Practitioner's Reference Second Edition, by Philip E. Fites, Martin P. Kratz

20. Taylor L. Risk analysis tools & how they work. URL: http://www.riskwatch.com

21. Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security

22. http://www.securityauditor.net/iso17799/(ISO 17799 Security Standard)

23. http://www.gammassl.co.uk/bs7799/works.html(How 7799 Works)