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

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

Қўлёзма хуқуқида

УДК: 338.26.003.13

ZOKIROV ABDUMAVLON ABDURAUF UGLI

THE PROBLEMS OF THE EVALUATING INFORMATION RISKS AND THEIR SOLUTIONS

5A350301 – Economy and Management in the sphere of ICT

D I S S E R T A T I O N

Research supervisor:
PhD. Iminov T.K.

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКАЦИЯЛАРИНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

Факультет: АКТ соҳасида иқтисодиёт ва менежмент
Кафедра: АКТ соҳасида Иқтисодиёт
Ўқув йили: 2013-2015

Магистратура талабаси: А.А. Зокиров
Илмий раҳбар: Т.К. Иминов
Мутахассислиги: 5А350301- АКТ соҳасида иқтисодиёт ва менежмент

МАГИСТРЛИК ДИССЕРТАЦИЯСИ АННОТАЦИЯСИ

Мавзунинг долзарблиги: Мамлакатнинг иқтисодий тараққиёт мезонлари жамиятимиз ҳаётига кириб келаётган ахборот - коммуникация технологияларини самарали қўлланилиши билан характерланади. Шундай экан, корхоналарда ахборот ресурсларидан самарали фойдаланиш, унинг фаолиятида ахборот – коммуникация технологияларидан фойдаланган холда муваффақиятли фаолият олиб бориш, ахборот рискларини бошқариш ҳамда ахборот ресурслари захирасини ташкил этиш бугунги куннинг энг долзарб масалаларидан биридир. Иқтисодиётни модернизациялаш шароитида республикамиз алоқа корхоналари тизимининг ривожланиб бориши, алоқа корхоналарида турли янги хизматларнинг жорий этилиши, фаолият жараёнида интернет хизматларидан фойдаланишда керакли маълумотларга келтириши мумкин бўлган зарарнинг қийматини баҳолаш ва зарарни иқтисодий жиҳатдан қоплаш мазкур тадқиқот мавзуси бугунги кундаги долзарб масалалардан бирига бағишланганлини англатади.

Ўзбекистон ва жаҳон иқтисодиётининг келгуси тараққиёти рискларни бошқаришга боғлиқлиги бугунги кунда исталган соҳа ташкилоти у ёки бу турдаги ахборот технологиялардан фойдаланиши ва ахборот ресурсларга эга эканлиги ахборот хавфсизлигини таъминлаш учун зарурат туғдиради.

Ҳозирги кунда ахборот ҳар қандай моддий мулкдан қимматлироқ манба ҳисобланади. Корхонада мавжуд ахборот ресурсларини ва рискларини тўғри баҳолаш ва уларни хавфсизлигини таъминлаш долзарб масаладир.

Ишнинг мақсади ва вазифалари: Тадқиқотнинг мақсади ИКТ соҳасида фаолият олиб борадиган юридик шахслар ёки жисмоний шахсларнинг ахборот рискларини бошқаришда ва бахолашда енг мақбул ечимни аниқлашдан ва ахборот рискларини суғурта қилишни кенг тадбиқ қилишдан иборат. Тадқиқот ишининг вазифалари қуйидагилардан иборат:

- Ахборот рисклари ва уларни баҳолаш моҳиятининг очиб берилиши;
- Ахборот рискларини бахолаш методикасининг халқаро тажрибасини ўрганиб чиқиш;
- Ахборот рискларини суғурта қилишда ахборот рискларини бахолаш бўйича муаммоларни ўрганиш ва уларни бартараф этиш.

Тадқиқот объекти ва предмети: Тадқиқот ишида объект сифатида "ALSKOM" СК танлаб олинган. Иқтисодий фаолият давомида маълумотлар билан ишлаш, ахборот рисклари, уларни бахолаш ва бошқаришдаги мавжуд муаммолар ва уларнинг ечимларини аниқлашга қаратилган методикалар тадқиқот ишининг предмети ҳисобланади.

Тадқиқот услубияти ва услублари: Тадқиқотни олиб бориш жараёнида тарихий таҳлил, тизимли таҳлил, график усули, иқтисодий моделлаштириш, статистик таққослаш ва иқтисодий-математик услубларидан ўринли фойдаланилди.

Тадқиқот натижаларининг илмий жиҳатдан янгилик даражаси:
- Ахборот рисклари ва уларни баҳолаш моҳиятининг очиб берилган;
- Ахборот рискларини бахолаш методикасининг халқаро тажрибасини ўрганиб чиқилган;
- Ахборот рискларини суғурта қилишда ахборот рискларини бахолаш бўйича муаммолар ўрганиб чиқилган ва улар бартараф этилган.

Тадқиқот натижаларининг амалий аҳамияти ва татбиқи: Ҳозирги кунда ахборот ҳар қандай моддий мулкдан қимматлироқ манба ҳисобланади. Корхонада мавжуд ахборот ресурсларини ва рискларини тўғри баҳолаш ва уларни хавфсизлигини таъминлашда ва "ALSKOM" СК ва унинг филиалларида ахборот рискларини суғурталашни самарали ташкил этишда қўлланилиши мумкин

Иш тузилиши ва таркиби: Диссертация кириш қисмидан, уч боб, хулоса ҳамда фойдаланилган адабиётлар рўйхатидан ташкил топган. Умумий хажми 81 бетдан иборат.

Хулоса ва таклифларнинг қисқача умумлаштирилган ифодаси: Мамлакатнинг иқтисодий тараққиёт мезонлари жамиятимиз ҳаётига кириб келаётган ахборот - коммуникация технологияларини самарали қўлланилиши билан характерланади. Шундай экан, корхоналарда ахборот ресурсларидан самарали фойдаланиш, унинг фаолиятида ахборот – коммуникация технологияларидан фойдаланган холда муваффақиятли фаолият олиб бориш, ахборот рискларини бошқариш ҳамда ахборот ресурслари захирасини ташкил этиш бугунги куннинг энг долзарб масалаларидан биридир. Иқтисодиётни модернизациялаш шароитида республикамиз алоқа корхоналари тизимининг ривожланиб бориши, алоқа корхоналарида турли янги хизматларнинг жорий этилиши, фаолият жараёнида интернет хизматларидан фойдаланишда керакли

маълумотларга келтириши мумкин бўлган зарарнинг қийматини баҳолаш ва зарарни иқтисодий жиҳатдан қоплаш мазкур тадқиқот мавзуси бугунги кундаги долзарб масалалардан бирига бағишланганлини англатади. Ахборотнинг юридик ёки жисмоний шахслар учун жуда мухим ва қимматли эканлагини хисобга олган холда, унинг хавфсизлигини таъминлаш хам жуда долзарб масаладир. Ахборот рискларини тўғри бахолаш орқали эса, инсон ўзида бор маълумотнинг қийматини аниқлаш мумкин ва уни суғурта механизми орқали иқтисодий йўл билан ўз харажатларини тежаши ва рискларини бошқариши мумкин. Ана шу йўналишни янада ривожлантириш учун эса қўшимча таклифлар ишлаб чиқилган.

Илмий раҳбар _____

Магистратура талабаси _____

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

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

Faculty: Economy and management in the sphere of ICT
Chair: Economy in the sphere of ICT

Master’s student: Zokirov A.A.
Adviser: Iminov T.K.

Studying year: 2013-2015 Major: 5A350301– Economy and management in the sphere of ICT

THE ANNOTATION OF MASTERS DISSERTATION

The topicality of the worktheme:. The aspects of economic development of the country are characterized by effectively using information communication technologies which are coming into our public life. So, the most important issues are effectively usage of information resources, leading the successful activity by using the information communication technologies, the management of information risks and creating the information resources reserves. On condition of modernization if our economy the developing of the communication enterprises system, the implementing of the various new services, the evaluating the damages to information recourses by using the internet services and covering the damage in economic field mean the necessity of the topic.

The future development the world and Uzbekistan economy is related with risk management, nowadays any branch enterprise uses any kind of information communication technologies and they have to provide the information security.

Nowadays, the information resource is more expensive than any kind of poverty. The evaluating the information risks and providing the information recourses is necessary.

The purpose and objectives of the work: The goal of the dissertation is to determine the convenient solution for evaluating the information risks of legal and individuals and develop the insurance of information risks.

The objectives of the research are:

- Opening the essence of the information risks and evaluating;
- Learning the international methods of evaluating the information risks;
- Learning the problems of the evaluating the information risks and solve the issues.

The object and subject of the research: The subject of the study is the JSC "ALSKOM" insurance company. Working with information resources, evaluating the cost problems and their solutions are the subject of the work.

The methodology and methods of the research: Methods of historical analysis, induction, systems analysis, graphical approach, modeling, statistical comparison and economic modeling were used during the work with data for study.

The scientific novation degree of the research results: According to the research some novelties were given:

- There is opened the essence of the information risks and evaluating;
- There is learned the international methods of evaluating the information risks;

- There is learned the problems of the evaluating the information risks and solve the issues.

The practical importance and implementation of the research results: Nowadays, the information resource is more expensive than any kind of poverty. The evaluating the information risks and providing the information recourses are illustrated and they can be used in the JSC "ALSKOM" insurance company and its branches for effectively organizing the information risk insurance.

The structure and composition of the work consists of introduction, three chapters, conclusion and the list of reference. The dissertation is put in 81 pages.

The important results of the finished work: The most important issues are effectively usage of information resources, leading the successful activity by using the information communication technologies, the management of information risks and creating the information resources reserves. On condition of modernization if our economy the developing of the communication enterprises system, the implementing of the various new services, the evaluating the damages to information recourses by using the internet services and covering the damage in economic field mean the necessity of the topic.

By evaluating the information resources, person can determine the value of his information and he can manage the risks, insure his information in order to economize the expenses. And here is created the suggestions for development this direction for the future.

Research supervisor _____

Master student _____

TABLE OF CONTENTS:

INTRODUCTION

The relevance of research topic. Today step by step almost all organizations are trying to use the information communication technologies (ICT) in order to operate their works in our country. Widely the ICT system is involving all spheres and this is the demand of the tense, as our Government President said "…….not only we have to sort out the problems in information services operation, but also in short time duration we have to join the line of the countries that have a good degree of information communication implementing"[1]. Nowadays level of competitiveness of the economy largely depends on the ability to protect information from theft, unauthorized use, alteration, destruction and other IT-inherent risks. Operating experience of information systems and resources in various areas conclusively shows that there is different and very real threats (risks) loss of information, leading to a specific expressible material damage.

To protect and store data on the impact of information risks are different automated systems, which are designed to prevent unauthorized intrusion. However, to completely eliminate the risk of leakage or loss of information are impossible. This is due to the vulnerability of networks and errors provoked by human factor, as well as the rapid development of new technologies.

The degree of the problems research. In developed countries have already appreciated the relevance of the information security risks or disclosure of data or malfunction of electronic systems entails huge losses. Accordingly, it is increasing and the number of customer calls to the insurance companies that operate in conjunction with software vendors, in order to increase the reliability of information systems.

In order to determine the dependence of the rate of growth in the number of risks and economic development, we carried out a sociological survey. As a result, we

[1] I.A. Karimov, the magazine "Xalq So'zi" dated January 19, 2013.

established the legitimacy of our conclusion about this relationship. At the same time the results of the survey showed that 73% of the subjects of the ICT sector believe that external risk factors are the most dangerous, and the remaining 27% said that the most dangerous are the internal factors, particularly industrial and economic activities, the sphere of circulation of money and the scope of control.

One of the important results of the poll of managers and specialists on risk management actors of the ICT sector of Uzbekistan was the conclusion that in a conceptually important is not to avoid risk at all, which is practically impossible, and through good monitoring system analytical work movement elements to business elimination of their deviation from the desired path.

The value of information is the most important asset of the company that can lead to success and in addition, it could be the most confidential information. However, the Head of the organization is responsible to save the confidentiality. As the law "On Commercial Secrets" was signed on September 11, 2014 by the President of the Republic of Uzbekistan Islam Karimov.

Purposes and objectives of the research. The main purpose of the research is to open the theoretical and practical sides of the risk management and to clarify the meaning of the information recourses and also according to the foreign experience, to create the proposals for the implementing the new ways of evaluating the information recourses and importance of insurance for providing their security:

- To describe the essence of the information, risk and risk management;
- To develop the ways of creating the information security system and give the facts about the importance of information security;
- To determine the value of information and create the conditional method of evaluating the information in organizations;
- To give the suggestions for developing the information security using the insurance services in Uzbekistan.

The object of the research is the insurance company and other organizations that use the information communication technologies.

The subject of the research is the relation between information resources and insurance of information risks.

Theoretical and methodological base of the research. Theoretical base of the research consists of the native and foreign expert works on risk management and insurance the information risks. Methodological base of the research consists of Decrees and Resolutions of the President of Uzbekistan, some data of different organizations and other regulatory and legal**.**

The novelty of the research consists of that in this research there is worked on theoretical and practical directions for the risk management. The novelty is spreading the ways of information security with using the insurance services. The following facts are related to the novelty of the research:

- There is given the review for the developing the information security and suggested the acceptable methods of saving the information basis;
- There is studied the foreign experience in risk management and the possibility of implementing them in our Republic;
- There is studied the elements and services of insurance for providing the information security and suggested the proposals for improving the efficiency of risk management in all sphere in Uzbekistan.

Practical significance of the research. In world practice of risk management used such methods to reduce risks such as diversification or risk allocation, reservation of funds to cover unexpected losses, insurance risks, and others. Among them insurance as international practice shows, it is one of the effective methods of compensation losses.

The approbation of the research results. The main results of the research are given and discussed in the International Scientific Conference named "Actual Problems of Applied Mathematics and Information Technology, Al-Khwarizmi 2014" which was held in Samarkand, 15-17 September 2014.

And also for the results of research, into the informative site www.uzreport.uz there is replaced the article about the implementing the

information risk insurance and the interview was showed on Television on the channel UzreportTV.

Structure and volume of the research. In the introduction there are given the relevance of research topic, theoretical and methodological base of the research, the novelty of the research and practical significance of the research.

In chapter 1 “Theoretical foundations of risk management and information risk insurance”. There are given Information security of Business and risk management, Technology of Risk Analysis and its management and Information security in the field of Insurance.

In chapter 2 “Risk analysis in the field of information risk insurance and the methods of evaluating the information risks”. There are given the Analysis of the information risk insurance of the insurance company ALSKOM and the analysis of implementing the insurance for organizations in Uzbekistan and how it works in different enterprises and also the process of evaluating the loss value and its problems.

In chapter 3 “Challenges and recommendations on assessment cost of information systems and risks, their implementation of modern conditions”. There is given the issue about the implementing the method of information security.

To conclude, there are given main conclusions which are devoted to the research and facts in work.

CHAPTER 1. THEORETICAL FOUNDATIONS OF RISK MANAGEMENT AND INFORMATION RISK INSURANCE

1.1. Information security of Business and risk management

The high rate of ICT development in the country and their widespread use increases the vulnerability of economic entities in terms of information security. In this regard, the question becomes relevant the widespread introduction of the mechanism of information security risks, as an alternative method of providing IT-security.

Today, practically no sector of the economy that would not use information and communication technology, and everyday life for many of us associated with the use, creation, processing and storage of information resources. Information resources are becoming an important value, the risk of loss or damage which excites every information. That is why the development and implementation of the mechanism of protection of information resources is one of the urgent issues of modern society.

Currently, the problem of information security of corporate information systems (CIS) is increasingly discussed in the pages of a variety of computer publications. At the same time, as a rule, considerable attention is paid to the description of the various technical solutions, analyzing the advantages and disadvantages of the known hardware and software technology and information security. To a lesser extent affected by the issues and institutional arrangements to ensure information security of the company - the strategy and tactics of information security concept and security policy, plans for the protection of information resources of the company in terms of internal and external functioning of the ICC. This is taken for granted that this problem is certainly relevant to the representatives of the domestic business. However, behind the scenes there is a question: and what, in fact, the interests of Russian business representatives in solving this problem? For standard words that business-critical information should

be accessible, integrity and confidentiality, it is not enough, because the information - rather abstract concept; threats to its security are probabilistic in nature (as we know, until the thunder breaks out, no one will do nothing), to the same technical and organizational security solutions cost money! Apparently, the explanation for this phenomenon lies in the fact that this issue is discussed mainly among technical experts and specialists with explicit "technical roots." However, with the level of business management of the company there are potential threats to the company's information resources and the availability of critical technical vulnerabilities CIS "not visible", so the problem of information security CIS is very vague. But this is understandable formulation of the problem: whether to spend money on corporate information security system, which is useful for business is far from obvious? Moreover, you can often hear the question: "Why do we need information security? The same cannot earn! "Or, if you speak the language of business - why do we need to create another expensive facility? They have far too much! And this argument is rather difficult to argue. Especially if you do not own counterarguments, understandable to domestic business. Unfortunately, part of the Russian director and service chiefs automation (CIO), Executive Officer (CEO)[2], chief information security officer (CISO) of counterarguments are not, although intuitively absolutely sure of the need to solve this problem. So, what to do to information security was seen as one of the corporate business processes? In other words, how to present information security from a business perspective? Clearly, for this we must first try to identify the business problem of information security. One of the main engines of the market of business automation is the desire of the business to become more efficient and competitive through the use of modern information technologies and improve their own model. Such a desire is understandable: not too much left of real mechanisms to improve competitiveness, and they mostly have been exhausted, and information technology offer truly unlimited. The fact that in the automation business has great potential for its

[2] Chief Executive Officer; In fact, this position is largely dependent on the structure of a particular company. Therefore, it can be designated as the first man of the company, and only one of its directors performing certain duties

dynamic development has no doubt today, probably nobody. It is enough to compare the effectiveness and efficiency of work, such as corporate e-mail with the effectiveness and efficiency of a large army of secretaries and typists, quality and timing of the development of complex technical systems by CAD / CAM / CAE-systems, and using the traditional drawing board, and others. We can say that the business -problem CIS, as well as any other technical systems is to simplify, speed up and make easier the previously routine and therefore slow and riddled with errors of business processes. Or, more strictly speaking, any business working to a technical system, in principle, should provide businesses some type of service. Service can be quite varied: a blast furnace "provides services", melted steel, transport department - transporting loads, canteen - staff providing food, etc. Also, the ICC, as a purely technical system, offers your business the type of service - in this case the service information. And this service is to provide businesses need to make decisions right quality, at the right time and the right place, which is information for managing the business itself.

At its core, the information is gradually becoming one of the key elements of the business. After all, what is the information from a business perspective? In fact, this is nothing like a set of formalized (in the sense of structured, laid out on the shelves and available funds for research and presentation) Knowledge of the business itself. This information can be understood by not only some static information resources, such as the balance sheet for the previous year or the current settings of any equipment, but also the dynamic processes of information processing knowledge in the form of programmed business logic of the company in the medium of popular applications, as an electronic document management, ERP, CRM, directory service, and others.

Times of Henry Ford when managing the company independently nut screwed on an assembly line, are long gone. Today, the top management of any company essentially deals only with information - and use it to make decisions. It is clear that this kind of information is prepared a lot of the lower layers of a rather complex organizational system, which is called the modern enterprise. And the

lower layers of the system generally cannot have a clue about what they produce not only some products or services, but also information for guidance. In our opinion, the deeper meaning of the automation business is just to speed up and streamline the flow of information between the functional layers and layers of this system and to the management of the company is only the most necessary, accurate and structured in an easy to decide the form of the information. Note reliable information! Hence it is easy to conclude that the key business objectives of corporate information security system are guaranteeing the reliability of the information, or, in other words, the guarantee of confidentiality of the information service of CIS (figure 1).

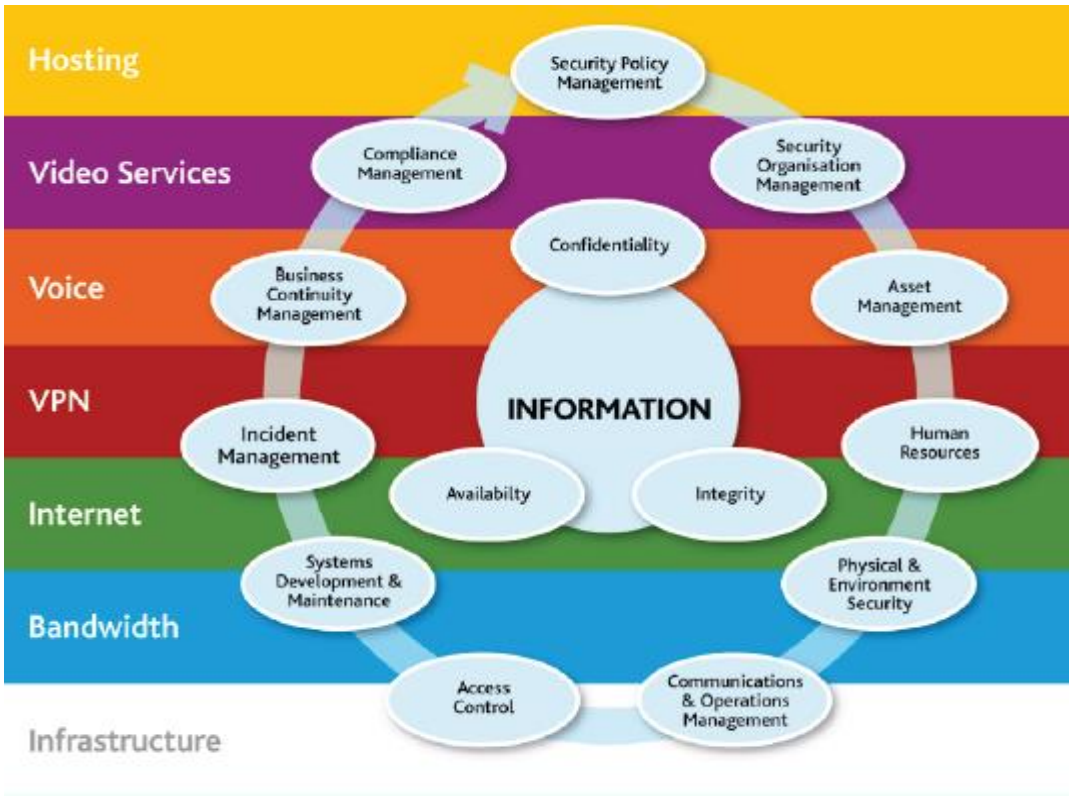

Figure 1. Information of the company.[3]

Let's try to ask any representative of the domestic business, whether it is ready to spend, say, one hundred thousand dollars for the purchase of, for example, five hundred firewalls and antivirus software licenses. Then ask the same question

[3] Insurance for cyber-risk management by Lawrence a. Gordon, martin p. Loeb, and Tashfeen Sohail

in another way: if he was ready to spend a hundred thousand dollars on the protection of information about itself and to protect the service, which is based on the management of the company? Most likely, the answer in the first case would be: a traditional Russian "no money", or, as in Odessa, with a question: "Why?". In the second case, response options greater: "In what terms' manage? Where were you before?". And even: "Why so little? Is my business worth so little? ". In addition, apparently, there will follow another interesting question: "And why a hundred thousand, not fifty, or, say, four hundred seventy-five?". And in this case, CIO, CEO, CISO just need to give a clear answer for the business, reasoned relevant economic calculations. That is in fact the cost of the study offer of the IB business.

Is it possible to carry out such an analysis and to justify the cost of corporate information security systems? The attentive reader must have noticed that lately in the press more and more often there are new topics for information security: Analysis of IS threats, an analysis of information risks, assessment of the total cost of ownership, return on investment evaluation of such a system, etc. All this is in the form of metrics and measures of information security is a economic tool refracted to the IB, which allows you to answer the question: Why a hundred thousand? And yet - this is a clear indication that the most "advanced" Russian CIO, CEO, and CISO already trying to answer it.

Let's see how you can justify the cost of corporate information security systems. In our view, such approaches are at least two. The first approach - we call it pseudoscientific - is to learn, and then to put into practice the necessary tools obtaining metrics and security measures, and for this to involve the company's management (as its owner) to the assessment of the value of the protected information, the definition of probability of potential threats and vulnerabilities and potential damage. In this case, the results of these assessments will largely depend on further activity of the CIO and CISO in the field of information security. If the information is not worth anything significant threats to the information assets of the company is not, and the potential damage is minimal -

and the management confirms (!) - The problem of information security can probably not do. If certain information is money, and the threat of potential damage is clear, it is understandable and within budget to the corporate information security system. It is significant that while it is possible to attract the company to realize the problems of information security and the construction of corporate information security system and to enlist their support. The second approach (called practical) is as follows: You can try to find the invariant of the reasonable cost of corporate information security systems. After all, there are similar invariants in other areas where significant business events are probabilistic. For example, in the auto insurance market, some general assessment of the reasonable cost of such services as insurance own car is of 5 to 15% of its market price - depending on the local conditions, culture and the driving experience of the driver, traffic, road conditions, etc.

By analogy with car insurance can never be engaged in information security in the company and do not rule out the possibility that the risk assumed to be quite rewarding. And you can spend on the creation of a corporate information security system a lot of money, and would still be some vulnerability that sooner or later lead to leakage or theft of confidential information. Therefore, experts-practitioners in the field of protection of the information found certain optimum, can feel relatively confident, - the cost of the IB should be approximately 10-20% of the value of the ICC - depending on the level of confidentiality of information. It is precisely the evaluation based on practical experience (best practice), you can count on. And to the question "Why to create adequate goals and objectives of the business of corporate information security systems requires a hundred thousand dollars?" Answer "Because today the cost of our CIS was one million dollars!". Obviously, the second approach is not without drawbacks. There will likely not be able to get the leadership deeply aware of the problem of information security. But we can safely predict the amount of budget for information security and to save on the services of external consultants.

Risk management is the acceptance of responsibility for recognizing, identifying, and controlling the exposures to loss or injury which are created by the activities of the University. By contrast, insurance management involves responsibility for only those risks which are actually insured against.

Some definitions are in order:

- Risk is uncertainty of loss.
- Peril is a source of loss (fire, windstorm, embezzlement, etc.).
- Hazard is a condition which increases the likelihood of loss (e.g., a known embezzler hired as an accountant).

With these definitions in mind, we can discuss the principles of risk management as they apply to the University. However, because of the diversification within the University, it is impossible to make one statement which will fit all situations equally. For instance, some departments are involved exclusively with education, others with research or patient care, and in some cases, with a combination of many operations and functions.

All departments are exposed to the perils of fire, theft, earthquake, burglary, work-incurred accidents, and liability for injury to the public. Some of these departments also have exposures involving possible loss of valuable papers and records, accounts receivables, loss of income and extra expenses to continue operations.

Therefore, an intelligent approach to risk management and insurance is necessary. Insurance is not purchased out of desire, but out of necessity. It isn't a commodity which is enjoyed or displayed or sought after by its owner. It is like headache tablets or spare tires; i.e., bought with the hope that they will never have to be used. Insurance should be the last line of defense and available after all other safeguards have failed.

Departments should not leave these things to chance, but follow good judgment and established procedures to control the risks and their costs.

A function of risk management is to organize and carry out a plan to control or reduce the risks to which the University is exposed. Departments can find

qualified help in the Insurance/Risk Management Department, Environmental Health & Safety Department, Police Department, Health Physics Department (Radiation Safety), Facilities Department, Employment/Employee Relations Departments, Omsbudperson and the Legal Office. With this assistance, they can follow certain procedures to control risks adequately and to obtain an objective loss prevention program. These steps are:

- ✓ Recognize and appraise the risk.
- ✓ Estimate the probability of loss due to the risk.
- ✓ Select the optimum method of treating the risk.
- ✓ Implement a plan to carry out the selected method.

The main concerns of most departments are the risks to property and people. Some examples of losses include:

LOSS BY DESTRUCTION - Property may be destroyed by fire, earthquake, flood, wind, breakage, or deterioration.

LOSS BY CONFISCATION - Property may be confiscated by an act of crime such as theft, embezzlement, robbery, burglary, forgery, and conversion.

LOSS OF USE - When property is destroyed or confiscated, the loss is often increased because of the indirect loss, e.g., loss of income, interruption of activities and extra expenses to continue operations. Much greater than the loss to physical property, is the loss of records and data which are vital to the operation of the University.

LOSS BY NEGLIGENCE - Liability claims are incurred when persons are injured or property of others is damaged or destroyed due to negligence.

LOSS OF EMPLOYEE/STUDENTS GOODWILL - Discrimination, sexual harassment, libel, slander, bad faith and unfair dealings will create liability situations and poor employee/student and public relations issues.

A function of risk management is to organize and carry out a plan to control or reduce the risks to which the University is exposed. Departments can find qualified help in the Insurance/Risk Management Department, Environmental Health & Safety Department, Police Department, Health Physics Department

(Radiation Safety), Facilities Department, Employment/Employee Relations Departments, Ombudsperson and the Legal Office. With this assistance, they can follow certain procedures to control risks adequately and to obtain an objective loss prevention program. These steps are:

- Recognize and appraise the risk.
- Estimate the probability of loss due to the risk.
- Select the optimum method of treating the risk.
- Implement a plan to carry out the selected method.

The main concerns of most departments are the risks to property and people. Some examples of losses include:

LOSS BY DESTRUCTION - Property may be destroyed by fire, earthquake, flood, wind, breakage, or deterioration.

LOSS BY CONFISCATION - Property may be confiscated by an act of crime such as theft, embezzlement, robbery, burglary, forgery, and conversion.

LOSS OF USE - When property is destroyed or confiscated, the loss is often increased because of the indirect loss, e.g., loss of income, interruption of activities and extra expenses to continue operations. Much greater than the loss to physical property, is the loss of records and data which are vital to the operation of the University.

LOSS BY NEGLIGENCE - Liability claims are incurred when persons are injured or property of others is damaged or destroyed due to negligence.

LOSS OF EMPLOYEE/STUDENTS GOODWILL - Discrimination, sexual harassment, libel, slander, bad faith and unfair dealings will create liability situations and poor employee/student and public relations issues.

METHODS FOR TREATING RISK

There are established and tested techniques by which risks may be controlled. 1) AVOIDING RISK - A risk may be avoided by not accepting or entering into the event which has hazards. This method has severe limitations because such a choice is not always possible, or if possible, it may require giving up some important advantages. Nevertheless, in some situations risk avoidance is

both possible and desirable. 2) SPREADING RISK - It is possible to spread the risk of loss to property and persons. Duplication of records and documents and, then, storing the duplicate copies elsewhere is an example of spreading the risk. A small fire in a single room can destroy the entire records of a department's operations. Placing people in a large number of buildings instead of a single facility will help spread the risk of potential loss of life or injury. 3) LOSS PREVENTION OR REDUCTION OF RISK - "An ounce of prevention is worth a pound of cure," according to an old saying. Today, this statement provides the guide for the control of risk. Risk may be reduced, eliminated, or certainly controlled by using a well-planned loss prevention program. These are some of the points a department should consider in its efforts to reduce loss: A. Utilize the services of the Insurance/Risk Management Department, Environmental Health & Safety Department, Police Department, Health Physics Department, Facilities Department, Employment/Employee Relations, Legal Office, Ombudsperson, HELP Center, and the Health Improvement Programs. B. Establish a system of accountability. Identify the causes and costs of losses and claims; study trends and patterns of repetitive accidents; form a safety or review committee to study incidents in order to better understand and control risks; include loss control as one of the more important goals and objectives of departments. C. Secure protection of money and records by preventing access to your accounts or computer systems, protect and safeguard codes and personal identification numbers, use high quality safes, vaults, and filing cabinets. When facilities are available for the storage of money or valuable equipment, access should be limited to as few people as possible. Cash handling procedures are reviewed by our internal auditors. Any large amounts of cash or checks must be deposited with the Cashier. Safe-keeping arrangements should be made for any other valuable equipment or materials. Change locks, and combination numbers when necessary to protect the integrity of access to secured areas. D. When selecting a site for storing valuable property, a number of items should be reviewed to reduce the possibility of loss. They include: (1) High water level - Avoid basements and areas where flood history exists. (2)

Heating system - Steam can be more damaging than water. (3) Construction of building - Safeguards and loss preventive systems built into the facility at time of construction (fire sprinkler system, security alarms, etc.) (4) Exposure - Surrounding area should be checked for hazardous exposures such as storage of flammable materials and chemicals. E. Housekeeping - Preventive Maintenance and good housekeeping procedures include, but are not limited to: (1) Educating and training staff in maintaining good housekeeping habits. (2) Arranging for preventive maintenance of equipment, tools, and building. 3) Controlling neatness and traffic flow patterns internally. F. Establish a safety program. There are basically two approaches to accident prevention: (1) Engineering risks, and (2) Personnel administration or human relations. The Engineering approach emphasizes mechanical causes of accidents, such as defective wiring, improper disposal of waste products and unguarded machinery. Safety engineering is an essential part of any accident prevention and loss reduction program. Yet, many times neglect, work attitudes, poor judgment or just plain carelessness by employees are the major causes of personal injuries and property damage. An effective program of education, training, and performance evaluation will aid in responding to the human element of accident prevention. Worker's compensation, disability and health insurance programs act as a cushion to the financial loss that may result from an accident to employees. There is, however, no way to truly compensate for the pain, suffering, dismemberment, and lost earnings or disfigurement and lost earnings that may result. Looking for ways to prevent injuries is the key. 4) RETENTION, ASSUMPTION OR ACCEPTANCE OF RISK - These methods are of particular interest to an operation as large as the University. Constant vigilance is needed to avoid accepting risks unintentionally through unawareness of the exposure. Some risks have to be retained because insurance cannot be purchased or the cost of insurance is not economically sound. Therefore, some risks should be retained, assumed, or accepted. Examples of these types of risks would be: earthquake, war, flood, accidental breakage, wear and tear etc. The importance and economic value of risk are reviewed in relationship to the

size of the operation, the probability and severity of loss. Before accepting a risk, consideration is first given to the potential amount of the loss and the effect the loss may have on the operations of the University. 5) TRANSFER OF RISK TO INSURANCE CARRIERS OR OTHERS - Risk may be transferred contractually to others. For example, when leasing facilities from others, the lease could require the lesser to assume all property and liability losses. Contracts to be entered into by the University must be reviewed by the appropriate University offices, e.g., procurement, sponsored projects, Legal and/or Risk Management. Only named individuals, approved by the Board of Trustees or delegated by a senior officer, may sign contracts or obligate the University under any written agreement. Many risks can and should be transferred to an insurance company. By doing so, that part of the risk is reduced to a certainty; i.e., the amount of the premium and deductible. The purchase of insurance is a tool that is used to help solve problems. However, the Director of Insurance/Risk Management recommends insurance only as a last method to solve a problem, not the first

Managing risk is a complex, multifaceted activity that requires the involvement of the entire organization—from senior leaders/executives providing the strategic vision and top-level goals and objectives for the organization; to mid-level leaders planning, executing, and managing projects; to individuals on the front lines operating the information systems supporting the organization's missions/business functions. Risk management is a comprehensive process that requires organizations to: (i) *frame* risk (i.e., establish the context for risk-based decisions); (ii) *assess* risk; (iii) *respond* to risk once determined; and (iv) *monitor* risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations. Risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk-based decision making is integrated into every aspect of the organization. The following sections briefly describe each of the four risk management components.

The first component of risk management addresses how organizations *frame* risk or establish a risk context—that is, describing the environment in which risk-based decisions are made. The purpose of the risk framing component is to produce a *risk management strategy* that addresses how organizations intend to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions. The risk frame establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within organizations. Establishing a realistic and credible risk frame requires that organizations identify: (i) risk assumptions (e.g., assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time); (ii) risk constraints (e.g., constraints on the risk assessment, response, and monitoring alternatives under consideration); (iii) risk tolerance (e.g., levels of risk, types of risk, and degree of risk uncertainty that are acceptable); and (iv) priorities and trade-offs (e.g., the relative importance of missions/business functions, trade-offs among different types of risk that organizations face, time frames in which organizations must address risk, and any factors of uncertainty that organizations consider in risk responses). The risk framing component and the associated risk management strategy also include any strategic-level decisions on how risk to organizational operations and assets, individuals, other organizations, and the Nation, is to be managed by senior leaders/executives.

The first component of risk management addresses how organizations *frame* risk or establish a risk context—that is, describing the environment in which risk-based decisions are made. The purpose of the risk framing component is to produce a *risk management strategy* that addresses how organizations intend to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions. The risk frame establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within organizations.

Establishing a realistic and credible risk frame requires that organizations identify: (i) risk assumptions (e.g., assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time); (ii) risk constraints (e.g., constraints on the risk assessment, response, and monitoring alternatives under consideration); (iii) risk tolerance (e.g., levels of risk, types of risk, and degree of risk uncertainty that are acceptable); and (iv) priorities and trade-offs (e.g., the relative importance of missions/business functions, trade-offs among different types of risk that organizations face, time frames in which organizations must address risk, and any factors of uncertainty that organizations consider in risk responses). The risk framing component and the associated risk management strategy also include any strategic-level decisions on how risk to organizational operations and assets, individuals, other organizations, and the Nation, is to be managed by senior leaders/executives.

The second component of risk management addresses how organizations *assess* risk within the context of the organizational risk frame. The purpose of the risk assessment component is to identify: (i) threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations or the Nation; (ii) vulnerabilities internal and external to organizations;(iii) the harm (i.e., consequences/impact) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) the likelihood that harm will occur. The end result is a determination of risk (i.e., the degree of harm and likelihood of harm occurring). To support the risk assessment component, organizations identify: (i) the tools, techniques, and methodologies that are used to assess risk; (ii) the assumptions related to risk assessments; (iii) the constraints that may affect risk assessments; (iv) roles and responsibilities;
(v) how risk assessment information is collected, processed, and communicated throughout organizations; (vi) how risk assessments are conducted within organizations; (vii) the frequency of risk assessments; and (viii) how threat information is obtained (i.e., sources and methods).

The third component of risk management addresses how organizations *respond* to risk once that risk is determined based on the results of risk assessments. The purpose of the risk response component is to provide a consistent, organization-wide, response to risk in accordance with the organizational risk frame by: (i) developing alternative courses of action for responding to risk; (ii) Evaluating the alternative courses of action; (iii) determining appropriate courses of action consistent with organizational risk tolerance; and (iv) implementing risk responses based on selected courses of action. To support the risk response component, organizations describe the types of risk responses that can be implemented (i.e., accepting, avoiding, mitigating, sharing, or transferring risk). Organizations also identify the tools, techniques, and methodologies used to develop courses of action for responding to risk, how courses of action are evaluated, and how risk responses are communicated across organizations and as appropriate, to external entities (e.g., external service providers, supply chain partners).

The fourth component of risk management addresses how organizations *monitor* risk over time. The purpose of the risk monitoring component is to: (i) verify that planned risk response measures are implemented and information security requirements derived from/traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, and standards, and guidelines, are satisfied; (ii) determine the ongoing effectiveness of risk response measures following implementation; and (iii) identify risk-impacting changes to organizational information systems and the environments in which the systems operate. To support the risk monitoring component, organizations describe how compliance is verified and how the ongoing effectiveness of risk responses is determined (e.g., the types of tools, techniques, and methodologies used to determine the sufficiency/correctness of risk responses and if risk mitigation measures are implemented correctly, operating as intended, and producing the desired effect with regard to reducing risk). In addition, organizations describe how

changes that may impact the ongoing effectiveness of risk responses are monitored.

As indicated in the four components of risk management described above, organizations also consider external risk relationships, as appropriate. Organizations identify external entities with which there is an actual or potential risk relationship (i.e., organizations which could impose risks on, transfer risks to, or communicate risks to other organizations, as well as those to which organizations could impose, transfer, or communicate risks). External risk relationships include, for example, suppliers, customers or served populations, mission/business partners, and/or service providers. For organizations dealing with advanced persistent threats (i.e., a long-term pattern of targeted, sophisticated attacks) the risk posed by external partners (especially suppliers in the supply chain) may become more pronounced. Organizations establish practices for sharing risk-related information (e.g., threat and vulnerability information) with external entities, including those with which the organizations have a risk relationship as well as those which could supply or receive risk-related information (e.g., Information Sharing and Analysis Centers [ISAC], Computer Emergency Response Teams [CERT]).

Figure 2 illustrates the risk management process and the information and communications flows among components. The black arrows represent the *primary* flows within the risk management process with risk *framing* informing all the sequential step-by-step set of activities moving from risk *assessment* to risk *response* to risk *monitoring*. For example, one of the primary outputs from the risk framing component is a description of the sources and methods that organizations use in acquiring threat information (e.g., open source, classified intelligence community reports). The output regarding threat information is a primary input to the risk assessment component and is communicated accordingly to that component. Another example is illustrated in the primary output from the risk assessment component—that is, a determination of risk. The output from the risk assessment component is communicated to the risk response component and is

received as a primary input for that component. Another primary input to the risk response component is an output from the risk framing component—the risk management strategy that defines how the organization should respond to risk. Together, these inputs, along with any additional inputs, are used by decision makers when selecting among potential courses of action for risk responses.

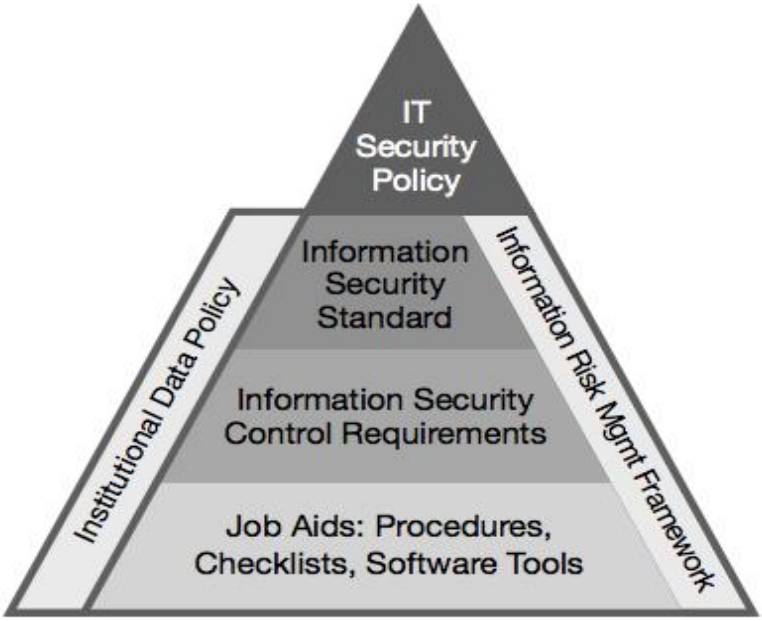

Figure 2: Risk Management and information flows[4].

The bidirectional nature of the arrows indicates that the information and communication flows among the risk management components as well as the execution order of the components, may be flexible and respond to the dynamic nature of the risk management process. For example, new legislation, directives, or policies may require that organizations implement additional risk response measures immediately. This information is communicated directly from the risk framing component to the risk response component where specific activities are carried out to achieve compliance with the new legislation, directives, or policies, illustrating the very dynamic and flexible nature of information as it moves through the risk management process. Chapter Three provides a complete

[4] Risk Management in the Insurance Business Sector, Claudio Fernandez Published by MFC Artes Graficas, S.L

description of the organization-wide risk management process including specifications for inputs/preconditions, activities, and outputs/post conditions.

To integrate the risk management process throughout the organization, a three-tiered approach is employed that addresses risk at the: (i) *organization* level; (ii) *mission/business process* level; and (iii) *information system* level. The risk management process is carried out seamlessly across the three tiers with the overall objective of continuous improvement in the organization's risk-related activities and effective inter-tier and intra-tier communication among all stakeholders having a shared interest in the mission/business success of the organization. Figure 3 illustrates the three-tiered approach to risk management along with some of its key characteristics.

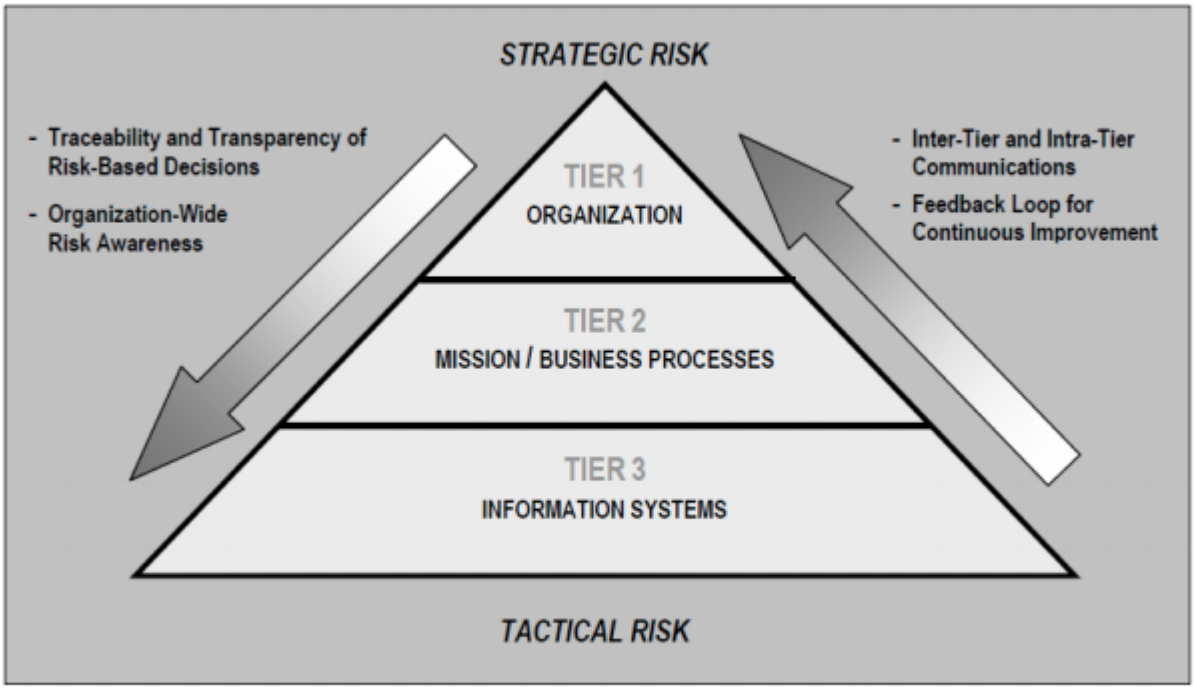

Figure 3: Risk Management 3-Tiered Approach[5].

Tier 1 addresses risk from an *organizational* perspective. Tier 1 implements the first component of risk management (i.e., risk framing), providing the context for all risk management activities carried out by organizations. Tier 1 risk management activities directly affect the activities carried out at Tiers 2 and 3. For example, the missions and business functions defined at Tier 1 influence the design

[5] Risk Management in the Insurance Business Sector, Claudio Fernandez Published by MFC Artes Graficas, S.L

and development of the mission/business processes created at Tier 2 to carry out those missions/business functions. Tier 1 provides a prioritization of missions/business functions which in turn drives investment strategies and funding decisions, thus, affecting the development of enterprise architecture (including embedded information security architecture) at Tier 2 and the allocations and deployment of management, operational, and technical security controls at Tier 3. Other examples of Tier 1 activities that affect Tier 2 and Tier 3 activities include the selection of common controls, the provision of guidance from the risk executive (function) to authorizing officials, and the establishment of the order of recovery for information systems supporting critical missions and business operations. Section 2.3 provides a more detailed description of the specific activities associated with Tier 1.

Tier 2 addresses risk from a *mission/business process* perspective and is informed by the risk context, risk decisions, and risk activities at Tier 1. Tier 2 risk management activities include: (i) defining the mission/business processes needed to support the missions and business functions of organizations; (ii) prioritizing the mission/business processes with respect to the strategic goals and objectives of organizations; (iii) defining the types of information needed to successfully execute the mission/business processes, the criticality/sensitivity of the information, and the information flows both internal and external to organizations; (iv) incorporating information security requirements into the mission/business processes; and (v) establishing an enterprise architecture with embedded information security architecture that promotes cost-effective and efficient information technology solutions consistent with the strategic goals and objectives of the organization and measures of performance. Tier 2 activities directly affect the activities carried out at Tier 3. For example, the information security architecture portion of the enterprise architecture developed at Tier 2 influences and guides the allocation of information protection needs which, in turn, influences and guides the allocation of the security controls to specific components of organizational information systems at Tier 3. Enterprise

architecture decisions at Tier 2 affect the design of information systems at Tier 3 including the types of information technologies acceptable for use in developing those systems. The activities carried out at Tier 2 can also provide useful feedback to Tier 1, possibly resulting in revisions to the organizational risk frame or affecting risk management activities carried out at Tier 1, for example those performed by the risk executive (function). Section 2.4 provides a more detailed description of the specific activities associated with Tier 2.

Tier 3 addresses risk from an *information system* perspective and is guided by the risk context, risk decisions and risk activities at Tiers 1 and 2. Tier 3 risk management activities include: (i) categorizing organizational information systems; (ii) allocating security controls to organizational information systems and the environments in which those systems operate consistent with the organization's established enterprise architecture and embedded information security architecture; and (iii) managing the selection, implementation, assessment, authorization, and ongoing monitoring of allocated security controls as part of a disciplined and structured system development life cycle process implemented across the organization. At Tier 3, information system owners, common control providers, system and security engineers, and information system security officers make risk-based decisions regarding the implementation, operation, and monitoring of organizational information systems. Based on these day-to-day operational risk-based decisions, authorizing officials make follow-on risk-based decisions on whether or not the information systems are initially authorized to operate within the designated environments of operation or continue to receive authorization to operate on an ongoing basis. These ongoing risk-based decisions are informed by the risk management process with guidance from the risk executive (function) and the various architectural considerations supporting the mission/business processes. In addition, the activities at Tier 3 provide essential feedback to Tiers 1 and 2. New vulnerabilities discovered in an organizational information system, for example, may have systemic implications that extend organization-wide. Those same vulnerabilities may trigger changes to

the enterprise architecture and embedded information security architecture or may require an adjustment to the organizational risk tolerance.

Risk Management Strategy. An organizational *risk management strategy*, one of the key outputs of risk framing, addresses how organizations intend to assess, respond to, and monitor risk—the risk associated with the operation and use of organizational information systems. The risk management strategy makes explicit the specific assumptions, constraints, risk tolerances, and priorities/trade-offs used within organizations for making investment and operational decisions. The risk management strategy also includes any strategic-level decisions and considerations on how senior leaders/executives are to manage information security risk to organizational operations and assets, individuals, other organizations, and the Nation. An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk response strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The use of a risk executive (function) can facilitate consistent, organization-wide application of the risk management strategy. The organization-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad-based and comprehensive.

An important Tier 1 risk management activity and also part of risk framing, is the determination of *risk tolerance*. Risk tolerance is the level of risk or degree of uncertainty that is acceptable to organizations and is a key element of the organizational risk frame. Risk tolerance affects all components of the risk management process—having a direct impact on the risk management decisions made by senior leaders/executives throughout the organization and providing important constraints on those decisions. For example, risk tolerance affects the nature and extent of risk management oversight implemented in organizations, the extent and rigor of risk assessments performed, and the content of

organizational strategies for responding to risk. With regard to risk assessments, more risk-tolerant organizations may be concerned only with those threats that peer organizations have experienced while less risk-tolerant organizations may expand the list to include those threats that are theoretically possible, but which have not been observed in operational environments. With regard to risk response, less risk-tolerant organizations are likely to require additional grounds for confidence in the effectiveness of selected safeguards and countermeasures or prefer safeguards and countermeasures that are more mature and have a proven track record. Such organizations may also decide to employ multiple safeguards and countermeasures from multiple sources (e.g., antivirus software at clients and servers that are provided by different vendors). Another example illustrating the impact of risk tolerance on risk response is that risk tolerance can also affect the organizational requirements for trustworthiness provided by specific information technologies. Two organizations may choose the same information technologies, but their relative degree of risk tolerance may impact the degree of assessment required prior to deployment.

There is no correct level of organizational risk tolerance. Rather, the degree of risk tolerance is:

(i) Generally indicative of organizational culture; (ii) potentially different for different types of losses/compromises; and (iii) highly influenced by the individual subjective risk tolerance of senior leaders/executives. Yet, the ramifications of risk decisions based on risk tolerance are potentially profound, with less risk-tolerant organizations perhaps failing to achieve needed mission/business capabilities in order to avoid what appears to be unacceptable risk; while more risk-tolerant organizations may focus on near-term mission/business efficiencies at the expense of setting themselves up for future failure. It is important that organizations exercise due diligence in determining risk tolerance—recognizing how fundamental this decision is to the effectiveness of the risk management program.

To summarize, risk management considerations can be addressed as an integral part of the enterprise architecture by:

- Developing a segment architecture linked to the strategic goals and objectives of organizations, defined missions/business functions, and associated mission/business processes;
- Identifying where effective risk response is a critical element in the success of organizational missions and business functions;
- Defining the appropriate, architectural-level information security requirements within organization-defined segments based on the organization's risk management strategy;
- Incorporating an information security architecture that implements architectural-level information security requirements;
- Translating the information security requirements from the segment architecture into specific security controls for information systems/environments of operation as part of the solution architecture;
- Allocating management, operational, and technical security controls to information systems and environments of operation as defined by the information security architecture; and
- Documenting risk management decisions at all levels of the enterprise architecture.

Enterprise architecture provides a disciplined and structured approach to achieving consolidation, standardization, and optimization of information technology assets that are employed within organizations. Risk reduction can be achieved through the full integration of management processes organization - wide, thereby providing greater degrees of security, privacy, reliability, and cost-effectiveness for the missions and business functions being carried out by organizations. This integrated approach of incorporating the organization's risk management strategy into enterprise architecture gives senior leaders/executives the opportunity to make more informed risk-based decisions in dynamic operating environments—decisions based on trade-offs between fulfilling and improving organizational missions and business functions and managing the many types and sources of risk that must be considered in their risk management responsibilities.

1.2. The essence of information risk insurance as a method of information security

The published documents of various organizations and the situation described above standards for the protection of information on issues of information risk analysis and management contain a number of important details that it is necessary to specify the development of workable techniques. The required degree of specialization of these parts depends on the maturity level of the organization, its specific activity and other factors. Thus, it is impossible to offer any single acceptable to all local companies and organizations, a universal technique to match a concept of risk management. In each particular case it is necessary to adapt the general procedure of risk analysis and management of the specific needs of the enterprise, taking into account the specifics of its operations and business. Let us first consider the typical questions and problems arising in the development of such techniques possible approaches to solving these problems, and then discuss examples of adaptation and development of appropriate corporate procedures (figure 4).

Risk Identification. In any method necessary to identify risks as an option - their components (threats and vulnerabilities). Naturally in this case it is the requirement of completeness of the list. The challenge of making the list and the proof of its completeness depends on what is required to detail the list. At a basic level of safety (the third level of maturity of the organization) specific requirements for detailed classes are usually absent, so it is sufficient to use any suitable in this case, the standard list of risk classes. An estimate of the risk is not considered that it is acceptable for certain varieties of techniques baseline. Lists of classes of risks are contained in a number of manuals, specialized in risk analysis. Example -German standard BSI [346], which has a catalog of threats in relation to the various elements of information technology. The advantage of such lists is their completeness: classes are usually a little (scores), they are quite extensive and cover all obviously there are many risks. The drawback - the complexity of

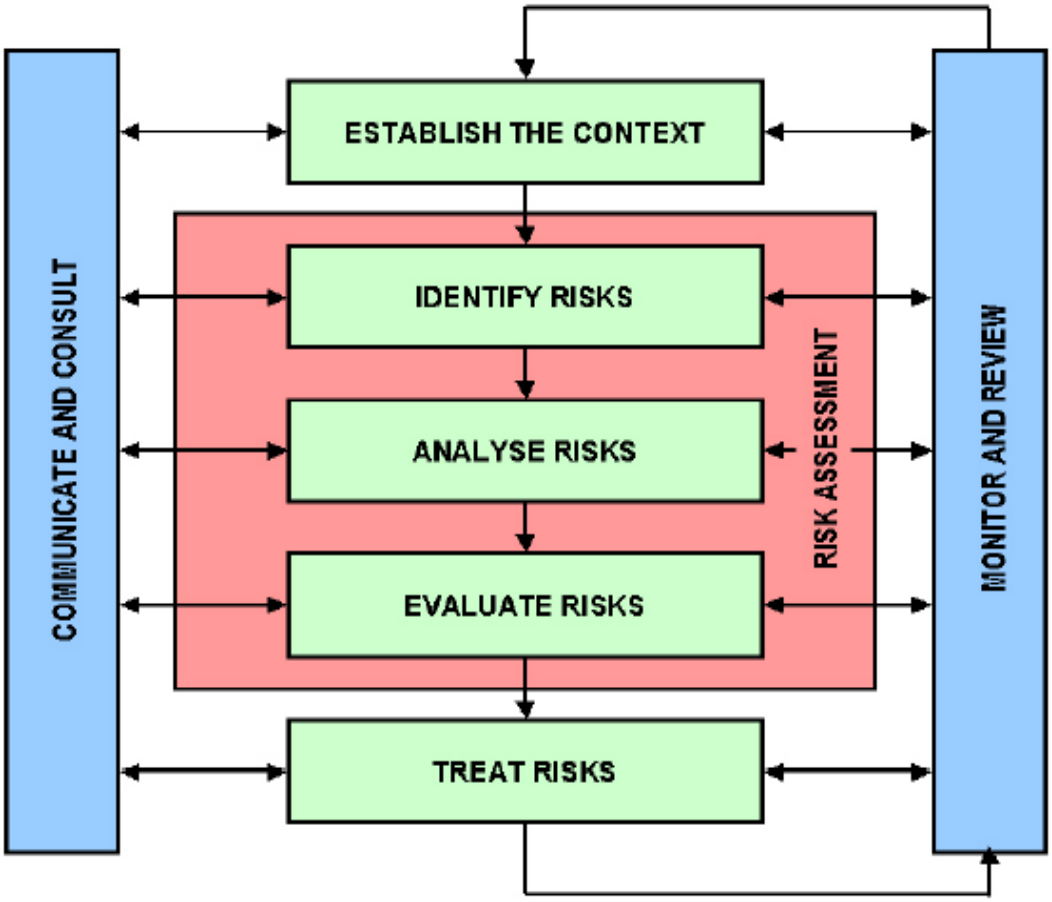

FIGURE 4: Risk Management Process.[6]

assessing the level of risk and efficiency for a wide range of countermeasures, since such calculations it is more convenient to carry out on a narrower (specific) classes account risks. For example, the class of risk "router failure" can be divided into many subclasses, including possible forms of failure (vulnerability) on a particular router equipment failure.

Assessing the risks. When assessing the risks it is recommended to consider the following aspects:

- The scale and the criteria by which you can measure the risk;
- Assessment of the probability of events;
- Risk measurement technology.

[6] Information Risk Management. Economically viable safety / Petrenko SA, Simonov SV - M .: IT Co., DMK Press, 2004. - 384 p

Scales and criteria that are measured risks. To measure any property you must select the scale. The scales can be direct (natural) or indirectly (derivatives). Examples of direct scales are scales for measuring physical quantities such as scales for measuring the liquid volumes in liters, scales for measuring the length in meters. In some cases, direct scales do not exist, we have to use a direct dial other related properties of interest to us, or to define new scale. Example - a scale for measuring the subjective properties of the "value of the information resource." This value can be measured in units' derived scales, such as the cost of resource recovery, recovery time and other resources. Another option - to define a scale for peer review, for example having three values:

- Low-value information resource from it do not depend on mission-critical tasks, and it can be restored with a small investment of time and money;
- The average value of the resource: it depends on a number of important tasks, but in case of loss, it can be restored in a time not exceeding the permissible critical, but the cost recovery - high;
- A valuable resource: depend on it critical tasks in the event of loss recovery time exceed the allowable critical or extremely high cost.

To measure the risk exists natural scale. The risks can be assessed by objective or subjective criteria. An example of an objective criterion is the probability of failure of any equipment, such as a PC, over a certain period of time. An example of a subjective criterion - the owner of an information resource assessment of risk of failure of the PC. In the latter case, usually developed qualitative scale with multiple gradations, such as: low, medium, high. The risk analysis techniques usually used subjective criteria, measured in units of value because:

- Assessment must reflect the subjective point of view of the owner of information resources;
- To consider the different aspects - not only technical, but also organizational, psychological, etc.

For the subjective evaluation of the example risk assessment of a failure of the PC, you can either use a direct peer review, or to define a function that

transforms objective data (probability) in a subjective scale of risks. Subjective scales are quantitative and qualitative, but in practice it is usually applied to the qualitative scale of 3-7 grades. On the one hand, it is easy and convenient, on the other - requires competent approach to data processing.

Objective and subjective probability. The term "probability" has several different meanings. Most often there are two interpretations, which are designated by a combination of "objective evidence" and "subjective probability". Under the objective (sometimes called physical) likely understood the relative frequency of occurrence of any event in the total number of observations, or the ratio of favorable outcomes to the total number of observations. This concept is used in analyzing the results of a large number of observations of past and received as a consequence of the models that describe some of the processes. Under the subjective probability is meant a measure of confidence some person or group of people is that this event will actually take place. As a measure of confidence in the possibility of occurrence subjective probability can be formally represented by different ways: a probability distribution on the set of events, a binary relation on a set of events that do not fully specify the probability distribution binary relation or in other ways. Most often subjective probability is a probability measure derived by experts. It is in this sense that we will understand the subjective probability in the future. The subjective probability in modern works in the field of system analysis is not just to determine a measure of confidence on the set of events, and is linked with the system of preferences of the decision maker (DM), and eventually to a utility function that reflects their preferences from a variety of alternatives. The close relationship between subjective probability and utility is used in the construction of certain methods to obtain subjective probabilities.

Obtaining estimates of subjective probability. The process of obtaining a subjective probability is usually divided into three phases: preparatory phase, obtaining estimates, phase analysis of the estimates.

First stage. During this stage the object of study - a lot of events, and perform a preliminary analysis of the properties of the set (set dependent or independent events, discrete and continuous random variables, generating a given set of events). On the basis of this analysis, select one of the suitable methods (overview of the main techniques of the definition of subjective probability. At the same stage, the preparation of an expert or group of experts to familiarize them with the method and test their understanding of the task.

The second stage. It consists in the application of the method chosen in the first phase. The result of this phase is a set of numbers that reflects the subjective opinion of an expert or group of experts on the probability of an event, but cannot always be considered as the final distribution, as is often contradictory.

The third stage. At this stage, we study the survey results. If the probabilities provided by experts are not consistent with the axioms of probability, then it draws attention of experts and answers clarified in order to bring them into line with the chosen system of axioms.

Information security in the field of Insurance

Legislation in the field of information security is a branch of the national legislation, which has a long and complex process of development and which continues to grow. Law-making and practice in this regard plays a huge role. The presence of a significant number of legal acts in this area and an active legislative process, inadequate legal regulation of social relations in the sphere of information also confirm the need for a systematic analysis of the legislation in this area; development in accordance with the state policy of development of legislation on the use of information and communication technologies (ICT), as well as policies for the protection of information. A fundamental piece of legislation for the protection of information is the Law of the Republic of Uzbekistan "About principles and guarantees of freedom of information", which are the basic concepts such as "information", "information sphere", "confidential information", "information security," "protection of information ". The Oliy Majlis passed about 75 laws related to some extent to the information, information services and

information technology, in particular, in 2005 the Law "On electronic payments", and "On protection of information in automated banking systems." The adoption of these laws helped the transition of the banking system to a new legal level, as well as provided protection of the rights of the owner information. In 2007, the Law of the Republic of Uzbekistan dated December 25, 2007, № Law-137 "On amendments and additions to some legislative acts of the Republic of Uzbekistan in connection with the strengthening of responsibility for committing illegal acts in the field of information and data" of the Criminal Code was amended by the Head XX1 "Computer crime".

However, these laws are only a small fraction of the regulatory - legal acts that should govern activities information and information technology, including in the field of information security. One of the areas of protection of information rights and freedoms of the individual and the state is the organizational - legal security of their information security. Canning legal basis for the development of information on the legal framework that has been created is impossible. In a society such changes occur, which on the one hand, the increasing potential of information and communication technologies (ICT) as part of the world economy, the international and domestic markets, provide capacity-building of information, on the other - form such socially significant structures that give it more complex targets for the use of these technologies. For the Republic today is the task of forming and implementation of national administrative and other reforms. In particular, it is the development of e-government and government online services. In connection with the establishment in accordance with the Resolution of the Cabinet of Ministers №250 Centre for the Development of "Electronic Government" and the Center for information security that are more deeply investigate the processes, law is also intended to respond to this development factor.

Today the private and public sectors face financial and reputational damage, competitive inroads, and significant regulatory sanctions when confidential information is inadequately protected. Clearly enough reasons as to why cyber

security must be prioritized regardless of what sector one conducts their organization.

Besides the weekly round, or of late what seems to be becoming more of a daily occurrence of cyber attacks just as much continues to happen offline as well. “Unencrypted” mobile devices continue to get lost which in turn increases the number of data breaches that we all read about in the media headlines on what seems like a weekly basis.

A recently conducted Zurich survey[7] stated that as awareness grows, information security and cyber risk continues to represent at least a moderate threat for a majority of risk professionals, who more and more are adopting an enterprise-wide approach to information security and cyber liability risk management. Due to improved awareness, cyber insurance also is increasingly becoming a part of more organizations cyber risk management strategies. We all know that life offers no guarantees and that “when one door closes, another one opens.” This holds true for cyber security, especially with today’s evolving threat environment and the force of attacks that continue to knock on the doors of countless networks. Enter “cyber insurance.” While cyber insurance cannot stop incidents or prevent them from happening, it can help respond to incidents when they do happen. When a security incident or a data breach happens, most cyber insurance policies have a team of experts already in place to help determine how your incident happened, whether or not any sensitive (PII) Personally Identifiable Information or (PHI) Personal Health Information has been exposed and helps determine if the security breach needs to be reported. Cyber insurance offers the private and public sector the ability to mitigate the residual risk, losses and associated costs of a security incident and/or data breach. Cyber insurance protects against the liability that comes from compensating others because cyber security has failed.

In today's world, where technology is a key element in the structure of any company, increasingly raises the question of protection of digital data. Despite the

[7] (Information Security, Cyber Liability & Risk Management: The Second Annual Survey on the Current State of and Trends in Information Security and Cyber Liability Risk Management, by Zurich)

large number of antivirus software, passwords and system access restriction information stored on electronic media, it is still exposed to various risks, whether it is a server failure or accidental destruction of the necessary data.

Insurance of information risks - insurance, which compensates for losses in emergency situations and natural disasters.

Therefore, as the object of insurance may be:

- Information resources - information in any electronic form (databases, libraries and archives in electronic form on the technical media of any kind), software and systems under development or exploitation;
- Financial assets - cash in electronic form in the form of entries in the accounts (client-bank), securities in electronic (book-entry) form.

As a supplement to the basic insurance protection can insure consequential damages or expenses associated with the onset of the following insurance cases:

- Losses from temporary suspension of business activities in the insurance case - it lost profit for the period of downtime, operating costs to maintain business during downtime. This remuneration of employees, mandatory contributions and not dependent on the production of payments facility;
- Additional costs for disaster recovery of business:

a) Temporary rental of equipment;

b) The use of third-party processing services of organization;

c) The urgent replacement of equipment and software;

d) The cost of investigating the circumstances of the insured event;

e) The costs of protecting the reputation of the insurer.

Insurance amount (liability limit) on the objects of insurance is determined based on the value of information systems in accordance with the "Methodology for calculation of the value of the information systems of information risks."

However, the threat of the companies is not limited to natural disasters. As you know, there is no absolute protection, and to create a system with a 100% guarantee against various threats impossible. A number of these threats is increasing with cosmic speed. Various statistical reports punctually is born,

predicting steady growth of viruses, worms and DoS-attacks that threaten to absolutely any company having access to the Internet. It would seem that the building has no fire and servers are running normally, but the data on them destroyed as a result of a virus outbreak. What to do? Property insurance will not help here, since blow inflicted on information assets. The consequence of such an attack can serve as a simple in operation and the inability of the affected company's services to its customers. And it's not only lost profit, churn and cost recovery of goodwill, and possible actions by customers, shareholders and others. One element of protection against such threats is the insurance of information risks, to which attention is being paid at the moment around the world.

Unlike property insurance covers the risks of information: software, including billing systems, Web-server, ERP-systems and means of protection; electronic data stored in databases, file servers and other media (CD-ROM, DVD, tape streamer, etc.); financial assets in an electronic form, including on the client-bank. If the insurance object is not no secret, the event which marks the arrival of an advance payment from the insurance company for the time being remains a dark horse, and it's time to move on to the notion of "insured event". His attempt to prevent any - and the insurance company do not want to pay for someone else's mistakes, and the insurer whose business is still suffering, despite the reimbursement of incurred losses. Do not forget that any encroachments on the company's assets carry with them and uncontrolled losses, such as loss of business reputation, decline in the value of the company, the reduction of orders and customer churn, the prosecution and the personal responsibility of the company's management.

The above-mentioned losses are uninsurable, which include the destruction of or damage to insured assets as described above, as a result of the following events:

The action of viruses, worms and Trojan are the most common type of information threats faced by different data from 85 to 93% of all companies. These threats and bring maximum losses for companies.

Computer attacks from outside intruders (hackers). It should be noted that some insurance companies (JSC "Ingosstrakh") refers to this event is not only the attacks, but the threat of their commission.

Embezzlement of funds in electronic form outside intruders. Such theft can occur by means of fraudulent financial orders sent electronically to the insurer or on behalf of the insured, and by modifying the software (for example, the attack "salami"), and even by directly entering commands, for example, in the "Internet Bank".

Unauthorized actions by their own employees. System failures due to errors in their design, development, construction, installation, configuration and operation. In this event very clearly fit into various errors of staff (including unintentional), which nullify all measures to protect enterprise resources.

The insured event is also a result of the temporary cessation of activity of any of these insurance claims.

Before the insurance company will take over the risk insured, it must ensure that the network is not an insurable company leaky sieve, and the first attack does not lead to the loss. In other words, a prerequisite for the information security risks is to conduct a special examination of the risk analysis of the insurance object. This expertise, in Russian sounding as well as in English - "Survey" (from the English "survey" - "inspection"), carried out by experts in the field of information security, which render their verdict on the level of protection of insured companies.

The peculiarity of this expertise is that it is performed by independent experts, broken or in insurable or an insurance company. It is believed that this will allow the insurance company to get a more accurate picture of the insurer, and the last - to assess its system of protection from the point of view of an independent disinterested expert. We must remember that the involvement of Russian experts is several times cheaper than their Western counterparts, who prefer an hourly wage. Half of the cost of survey of the insurance company compensated at the conclusion of the relevant contract of insurance.

However expertise is not a guarantee of the contract. The fact that the results of the analysis may require the implementation of additional technical and organizational security measures to reduce the risks of damage to corporate resources. Not all companies can go the extra costs and without insurance contract will not be, because the probability of occurrence of the insured event becomes too high. Says head of information "Industrial-insurance company" I. Parafeynikov: "We are ready to insure these risks, but in this case the insured are requirements to carry out a series of organizational and technical measures to reduce our risk, and this, of course, dramatically increases the price of the issue, so many companies believe that the information risks to insure our own peril."

As soon as an insured event occurs, the insurance company leaves in place and assessing the damage, and then comes the moment of payment of insurance compensation. However, no payments are made at the same time, and during the term of the insurance policy (usually 1 year).

The cost of this service is calculated individually for each client, but usually does not exceed 5% of the insurance policy in the limit of liability insurance company. The parameters that affect the insurance rates are used: The cost of insured resources. The higher it is, the lower the rate of insurance. For example, Lloyd determines the premium of $ 20,000 (5%) in the value of information in the $ 1 million and $ 75,000 (0.75%) with an increase in the value of the information to 10 million dollars.

Used remedies show that the known systems of protection, the lower the rate of insurance. Statistics attacks for similar companies in the industry. However, the insurance rate may be reduced to 3% or even 1.5%. It is enough to implement the recommended examination as a result of protective measures. The hardest part - is to determine the limit of liability, ie, the amount that would be required to pay the insurance company as a result of the insured event. In turn, this sum is divided into two components: the cost of information resources the amount of losses from discontinued operations as a result of the insured event. It should be added that many insurance companies set the lower limit of the insured amount below which

it cannot go down. For example, Ingosstrakh, this sum is equal to US $ 50,000, from Western companies; this strap is much higher due to increased overhead costs of various insurance activities. The upper limit of damages is limited to no one, although there is an unspoken boundary (for example, in the West, it is equal to $ 100 million), above which require closer contact with the insurance company and a clear study of all legal and technical issues. On average, the limit of liability in the international market of information security risks is ranging from one hundred thousand to $ 5 million. For Russia, this figure has not been determined due to the absence of necessary statistics.

Widespread this type of insurance was in the 90s of the last century due to the widespread use of computers and the Internet in all areas of human activity. Currently, insurance services offer information risks many insurance companies, in particular:

- Lloyd - service Internet Asset and Income Protection Coverage by Lloyd;
- AIG - service net Advantage Suite;
- Marsh - Net Secure service.

At the same time there was a practice under which insurance companies work closely with the developers of remedies and companies specializing in information security. After conducting of survey experts recommend the insurer to apply the remedies developer having a corresponding relationship with the insurance company. In case of using such means insurance rate is reduced as compared with the standard, for example, from 2.5% to 1.5%. Of course, the insurance company does not recommend any remedy, but only the well known and proven. For example, such an alliance exists between the company Internet Security Systems and Marsh, between Counterpane Internet Security, and Lloyd, etc. As a rule, customers of insurance companies are not very large firms wishing to protect themselves from potential losses resulting from an insured event. Individuals not included in the area of interest of insurance companies and it is natural - a little profit and the cost of doing deals abound.

Conclusion for Chapter 1. The benefits of insurance as a method of protection against information risks are obvious. This is not only a way of pecuniary damage. The use of insurance involves the analysis of the object of insurance, as well as a complete and thorough audit of information security systems of the enterprise prior to the conclusion of an insurance contract. In this interest as a policyholder, that it is important not to overpay premiums and the insurer who does not want to take insurance "unfinished" system. This insurance carries a stimulating function, ie enterprise, improving their information security system, is able to lower their insurance costs.

In general insurance information risk allows covering the risks associated with virtually any hardware and software systems for the collection, transmission, storage and processing. A number of organizations of communication and information have already realized the economic benefits of information security risks and are active users of the insurance services.

CHAPTER 2. RISK ANALYSIS IN THE FIELD OF INFORMATION RISK INSURANCE AND THE METHODS OF EVALUATING THE INFORMATION RISKS

2.1. Existing methods for evaluating the cost of information systems and damage caused by the impact of information risks

Information security has increasingly become an important topic for small and big organizations alike. Although awareness and efforts towards security have increased, unfortunately, this increase does not appear to be mitigating the number or cost of incidents from either internal or external sources. One reason for the problem is that the technology is changing faster than what financially-strapped businesses and information technology (IT) departments can handle. Most organizations are not only increasing the size of their networks but also adding new types of connectivity and complexity. For example, acquisition and implementation of different types of systems because of back-end business process integration with suppliers and other partners and front-end process integration with clients and customers. In some cases, this kind of integration is forced due to mergers and acquisitions. In several instances, market's competitive pressures on hardware and software vendors forces them to implement security features and test products prior to product release in a shortened time span and compromise security. A lot of times security is an afterthought and it turns out to be an add-in into existing systems and applications which is difficult, expensive, and, in some cases, impossible without serious operational impact. Even if security mechanisms exist, there is another fundamental problem involving the implementation of controls.

Most organizations do not invest in a thorough risk assessment process before implementing controls. This could result in some threats being overlooked, and also financial and other resources applied wrongly to threats that either do not exist or do not have serious impact (Anderson 1998). Risk is generally defined as a threat or potential for loss. Risk to some degree is unavoidable but what is needed

is an approach to risk that enables organizations to systematically identify information systems risks, prioritize those risks, and take appropriate steps to manage them. Risk assessment is the analysis of the likelihood of loss due to a particular threat against a specific asset in relation to any safeguards to determine vulnerabilities. Assets can be both physical like hardware and virtual like data that has value to an organization. Risk management can be defined as a "systematic process for the identification, analysis, control and communication of risks" (Paul 2000). The risk assessment is one element 485 within the broader set of risk management activities. It provides a basis for establishing appropriate policies and selecting cost-effective techniques to implement these policies. It also offers a means of providing decision makers with the information needed to understand factors that can negatively influence operations and outcomes, and make informed judgments concerning the extent of actions needed to mitigate the risk. All risk assessment methods (GAO Report 1999) generally include the following steps:

1. Identifying threats that could harm, and thus, adversely affect critical operations and assets.
2. Estimating the likelihood/probabilities that such threats will materialize based on historical information and/or the judgment of knowledgeable individuals.
3. Identifying and ranking the value, sensitivity, and criticality of the operations and assets that could be affected.
4. Estimating the potential losses or damages including recovery costs.
5. Identifying cost-effective actions to mitigate risk, which include information security policies as well as technical and physical controls.

There are two common approaches used in risk assessment: a quantitative approach and a qualitative approach. A quantitative approach estimates the monetary costs of risk and risk mitigation techniques based on the likelihood that a damaging event will occur, the costs of potential losses, and the costs of actions that could be taken. When reliable data on likelihood and costs are not available, a qualitative approach can be taken by defining risk in more subjective terms.

Insurance company JSC «ALSKOM» established in September 1996. The internal policy of the Company allows us to maintain a high position in the insurance market and annually increase the number of policyholders. In accordance with the license of the Ministry of Finance of the Republic of Uzbekistan Series SF №00164 dated 10 January 2012 on the implementation of the insurance business, the Company sells more than 50 types of insurance. Reliability Service confirmed rated "uzA + - very high financial reliability" rating assigned to the company «SAIPRO» in 2011.

Given the wide range and the specific nature of the risks your company offer the insurance product "Insurance of information risks." This product in 2008 and 2009, recognized as the best innovative insurance product, and our company was awarded the highest award of the national insurance market - "Oltin Soyabon." Terms and methodology developed by specialists of insurance companies on the basis of the requirements of the global insurance practice.

This insurance product is registered with the Patent Office of the Republic of Uzbekistan, and therefore the exclusive right to use the developed methodological basis of the information security risks belongs to «ALSKOM».

The following regulations have been developed for the insurance of information risks.

1. The rules of information security risks. The rules establish the procedure and conditions of insurance.

2. The method of calculating the value of the information systems of information risk, which is a calculation of the value of natural resources determined by the price recovery in the event of failure.

3. Methods of assessing the damage and determining the amount of insurance compensation, which provides for the definition of risk assessment of the damage and threats, as well as possible damage in case of insurance of information risks and ensure the practical realization of the insurance compensation if information risk.

4. Instructions for the examination (audit) of information systems security. This instruction regulates the examination of information systems to identify flaws in the system of information protection or to investigate the incident involving the loss of information.

These regulations were approved by the order of the Uzbek Agency for Communication and Information December 1, 2008 and entered into force. This insurance product is registered with the Patent Office of the Republic of Uzbekistan, and therefore the exclusive right to use the developed methodological basis of the information security risks belongs to «ALSKOM»(figure 5).

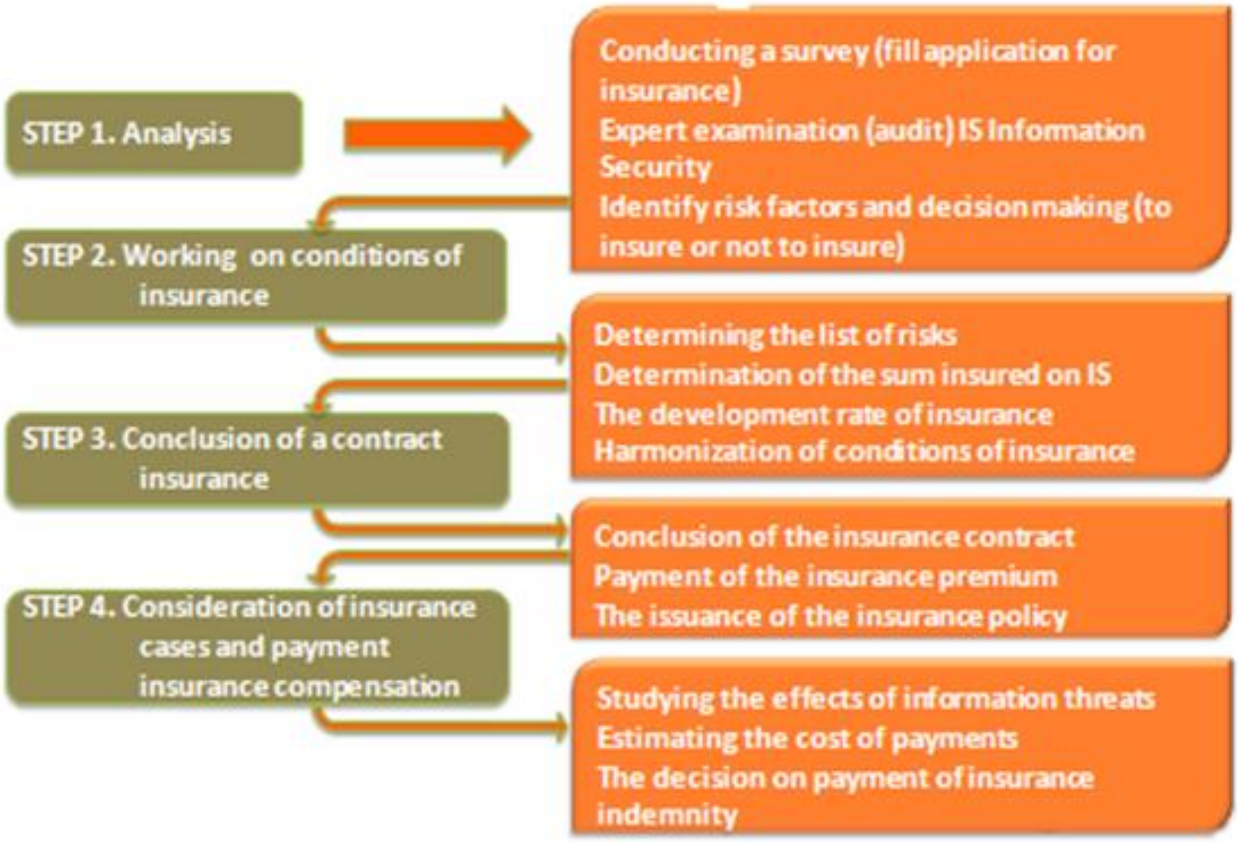

Figure 5: The procedure for the implementation of information security risks[8]

1-stage. Analysis. An analysis of the potential insurers is the initial step in the process of insurance in which the insurer's decision to enter into an insurance contract. This is possible during the preparation of the potential policyholder to answer some questions. To this end, experts «ALSKOM» developed the

[8] "The rule of information risk insurance", 2009. JSC "ALSKOM" insurance company

questionnaire-application for insurance. It should be noted that the application form is the basis for a contract of insurance, so the information recorded in it are essential for risk assessment.

Further detailed examination will be conducted, ie, audit of information security information system of the insurer, through the involvement of independent experts. Experts on the basis of the analysis the level of security of information systems in accordance with the "Guidelines for the examination (audit) security of information systems" provide the policyholder and the insurer on conclusion of the level of information security of information systems of the insured. On the basis of this conclusion, the insurer proceeds to the next stage, the stage of development of insurance conditions.

2-stage. Working conditions of insurance.

2.1. At this stage in the first place with the agreement of the insured is determined by the list of risks to be insured. They can be insured all risks or individual, at the option of the policyholder.

In developed products cover the losses associated with the loss, destruction or damage of data, loss of securities and cash in an electronic form as a result of the following events:

- Failures (the failure of) information systems due to errors in their design, development, construction, installation, configuration, maintenance, or operation;
- Intentional wrongful actions of the insured committed by them alone or in collusion with third parties for the purpose of harm to the insured or to obtain an illegal financial gain;
- Computer attacks against the insured by third parties;
- Intentional wrongful acts of third parties aimed at unauthorized modification, copy, damage, destruction of electronic data, permanent or temporary disablement of the information systems of the insured;
- Actions of computer viruses - malicious computer code fragments, or electronic instructions, can independently or when they are activated users replicate and

spread in information systems and networks (this includes also "Trojan horses", "worms", "logic bombs");

- Theft of cash and securities in electronic form as a result of unauthorized access by third parties to the information system, including implementation through: a) entering into a fraudulent electronic commands policyholder information systems;

b) unauthorized modification of computer code (program) of the insured; c) fraudulent transfer (fraudulent) electronic orders allegedly issued on behalf of the insurer, bank or depository insured.

2.2. The next step is to determine the object of insurance and the insurance sums on them. It should be noted that the information is the property of its owner if it is documented information created at his expense, acquired them legally. Therefore all the provisions of property insurance provided for by the legislation of Uzbekistan are applicable to this type of insurance.

Therefore, as the object of insurance may be:

- Information resources - information in any electronic form (databases, libraries and archives in electronic form on the technical media of any kind), software and systems under development or exploitation;

- Financial assets - cash in electronic form in the form of entries in the accounts (client-bank), securities in electronic (book-entry) form.

As a supplement to the basic insurance protection can insure consequential damages or expenses associated with the onset of the following insurance cases:

- Losses from temporary suspension of business activities in the insurance case - it lost profit for the period of downtime, operating costs to maintain business during downtime, ie This remuneration of employees, mandatory contributions and not Dependent on the production of payments facility;

- Additional costs for disaster recovery of business:

a) Temporary rental of equipment;

b) The use of third-party processing services of organizations;

c) The urgent replacement of equipment and software;

d) The cost of investigating the circumstances of the insured event;

e) The costs of protecting the reputation of the insurer.

Insurance amount (liability limit) on the objects of insurance is determined based on the value of information systems in accordance with the "Methodology for calculation of the value of the information systems of information risks."

2.3. Further, the insurer starts to develop insurance rates. Insurance rate is the rate of insurance premium, which is paid by the insured to the insurer under the insurance contract. Insurance rate is set individually for each risk. Its size depends on the level of information security of information systems and the degree (amount) of risk determined on the basis of the analysis of information security IS insured.

3-phase. Conclusion of the insurance contract. After the development and harmonization of conditions of insurance with the insurer between the insurer and the insured is the insurance contract. Terms and conditions of the insurance contract are determined by the "Rules of insurance of information risks."

Further, the insurer shall pay the contractual calculated insurance premium. After paying the insurance premium the insurer gives the insured an insurance policy, the facts show the entry of liability of the insurer to pay the insurance indemnity.

4-Stage. Consideration of insurance claims and payment of insurance compensation. In the insurance case involved an expert organization that studies the impact of information threats and identify damages in accordance with the "Guidelines for assessment of the damage and determine the amount of insurance compensation" Revealed damages are awarded SC «ALSKOM» within the sum insured established in the insurance contract.

Methods of calculating the cost of information systems.

The cost of an information system is defined as the aggregate of the cost of:

- Information Resources - a database, libraries, archives in electronic form, documented information;
- Information and communication technologies:

a) Computer hardware (servers, workstations);

b) Telecommunications and networking equipment (equipment of local area networks, antennas, fiber-optic communication lines;

c) Peripherals (printers, scanners, uninterruptible);

d) Software (software products, tools and systems, resource planning insurer, as well as finance and accounting system);

e) The development and implementation of mechanisms to counter information risks.

Evaluation of the information system is carried out on the basis of costs that are required for restoration:

- Information resources;
- Information and communication technologies;
- Mechanisms to counter the risks of information.

To calculate the cost of recovery of information systems in the insurance case, possible damage to the following benchmarks:

1. The sum of all costs for the restoration of information resources:

1.1. The cost of restoring the database

1.2. The cost of restoring the electronic library

1.3 The cost of restoring the archive in electronic form

1.4 The cost of restoring the documented information

2. The sum of all costs Sun-emergence of information technologies and means of communication:

2.1. The cost of the restoration - the purchase of computer equipment

2.2. The cost of rehabilitating the telecommunication and network equipment

2.3. The cost of the restoration - the purchase of equipment

2.4. The cost of the restoration - the purchase of software

3. Development costs (acquisition) and the introduction of new mechanisms opposite to information risks

4. Insurance amount - the limit of liability for all information risks

4.1. Insurance amount - the limit of liability for information risk

5. Franchise.

Methods of assessing information risks.

To assess the risks of information system security of each Insured valuable resource is determined by analyzing the threats acting on a particular resource, and vulnerabilities through which these threats can be realized.
In order to assess the risk of the information necessary to analyze the threats acting on the information system vulnerabilities, which can be realized through threats. Threats are divided into:

- Technological nature;
- Organizational nature.

Technological threats mean effects are divided into:

- Physical;
- Software (logical).

The next stage of classification is the cause of the threat.
The reasons for the implementation of physical threats are:

- Actions of the offender (person);
- Force majeure;
- Equipment failure and internal life support systems.

Whatever the reason, the physical impact on the threat:

- Information resource;
- A communication channel.

Software threat due to the impact of share on:

- Threats from local offender;
- Threats from a remote intruder.

One of the main issues in the insurance of information risks is to determine the sum insured. The sum insured, the amount of money within which the insurer is liable for the fulfillment of its obligations under the insurance contract shall be determined by agreement between the parties and shall not exceed the cost of information systems.

Cost information systems are determined by the following formula:

$$C_{uc} = \sum_{i=1}^{n} C_{umc} + \sum_{i=1}^{k} C_{ПО} + C_{up} \quad (2.1)$$

where:

C_{uc} - The cost of an information system in terms of money;

C_{umc} - Book value of information technology, in terms of money;

$C_{ПО}$ - The book value of the software in terms of money;

C_{up} - The value of the information resource, in terms of money;

n - the number of information technology;

k - the number of the software.

When calculating the cost of information resources are taken into account the costs associated with the establishment and commissioning of information resources. The amount of the costs incurred is calculated on the basis of the balance sheet.

Calculations to determine the value of information resources are based on the following formula:

$$C_{up} = (ЗПС * П) * m \quad (2.2)$$

where:

C_{up} - The value of the information resource, in terms of money;

$ЗПС$ - The average monthly wage IT-specialist in monetary terms;

П - period of the information resources (from the date of entry to audit);

m - number of employees working on the information resource.

It should be noted that the above method is used to determine the value of information systems entities. The question of determining the value of the information systems of individuals today is difficult due to the individuality of their information systems. In simple words, the information owner can cost a lot of money, but for the other person does not have a value.

Taking this into account, as well as to improve and wide application of information security risks in the practice should consider the development and approval of the Ministry for the development of information technologies and communications of a clear program of information security risks.

2.2. The practice of information risks insurance in Uzbekistan and the experience of information risk insurance in foreign countries

Currently, information security in enterprises irrespective of their activities is very relevant. Efforts and money spent does not give the expected results. Adopted by many government decisions and normative documents in the field of information security, but does not work properly take monitoring compliance with applicable standards and requirements. At the level of the company's management is not supported initiatives to ensure information security and responsible for information security cannot justify the need to introduce mechanisms for the protection of information. Not implemented information security management system, and there does no understand in general. This means that selective and inconsistent implementation of security tools cannot provide the necessary level of protection. These problems are the main reasons for the decrease level of information security. To save the reputation and business information, businesses need to integrate physical and information security into a single organization-wide process - the process of enterprise information security management as part of an overall enterprise management system.

The process of continuous improvement usually requires an initial investment in the documentation of activities, formalizing an approach to risk management, the definition of methods for analyzing and allocating resources. These measures are used to bring the cycle into effect. They do not necessarily have to be completed before they are activated under review.

For the effective functioning of the information security management system is necessary to ensure the conditions for a continuous cyclic process, including the

degree of awareness of the need to protect information and tasking; data collection and analysis on the state of information security in the company; risk assessment; Planning measures for handling risks; realization and implementation of appropriate control mechanisms, roles and responsibilities, training and motivation of personnel, operational work on the implementation of protective measures; monitoring of the operation control mechanisms, assess their effectiveness, and appropriate corrective action.

Foreign experience of information risk insurance.

November 2, 1989 Internet was first attacked by a virus. At the same time it was first used the word "hacker" and had begun research into ways to protect against viruses and prevent them. Insurance of information risks - a relatively new type of insurance, is still slightly prevalent in Russia. This article examines the existing international experience, which can be used successfully in our country.

The development of e-commerce and information technology over the past twenty five years, accompanied by the growth and complexity of the components of the criminal forms and methods used by hackers. At the same time, despite all the efforts (among whom were successful) fight hackers and viruses, their number grew. There is reason to believe that this situation is not about to change, and huge economic damage done by hackers, further increase.

The number of cyber crimes, despite the continuous development of information security tools, is not reduced. Using electronic technology for 2014 hackers and insiders has damaged the global economy of $ 27 billion versus $ 18 billion a year earlier (an increase of 50%). For reference, in 2011 the cyber criminals managed to steal from businesses and other organizations approximately $ 12.5 billion. The increased level of boldness and imagination of the perpetrators can only envy. Contribute to this growth, including numerous online forums where you can learn and basic knowledge, and "higher education" in this area. There you can collect from bricks designer tools for hacking, type the command, get detailed

information about the victim. And then it all depends on the scale of the individual offender and the degree of confidence in their impunity.

The jeopardized system management port does not interfere with the normal work of the personnel, but regularly supplied information on the whereabouts of the containers of fruit, where they were accomplices in South and Central America have added carefully before sending a cargo of drugs. Before the arrival of representatives of the Customs Service, these containers unsuspecting crane on the instructions of a computer system port promptly stashed out of sight in the other places.

On the actual scope of activity of the computer underground can only occasionally be judged by the results of trials of accidentally fell into the hands of justice, "genius." Moreover, burglars and thieves of banks other personal information on their background gradually fade into the background of its popularity

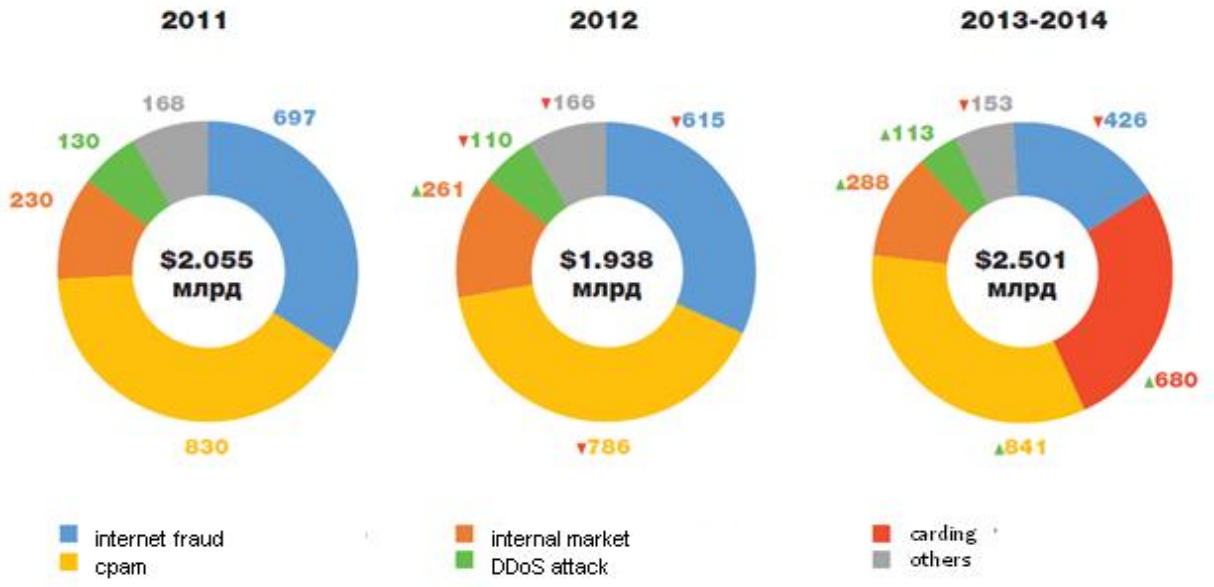

Figure 6: The dynamics of the loss of Russian business by cybercriminals for 2011-2014, $ Billion[9]

[9] Rates for cybercriminals, taken from the internet resources.

Like a thimble, hackers rather complicated algorithms changed the location of the Bonded cargo wharves and warehouses, as long as they were allegedly not mistakenly loaded on cars, and the documents of the present, but the remaining cargo in the port, export away until the real owners of bananas and pineapples. The alarm was raised only after the port began to systematically disappear without a trace hundreds of containers due to the prohibitive raging appetites of organizers of the scam. And later uncovered the scale of smuggling introduced into shock even seasoned drug police.

Lloyd's of London, one of world's largest insurance firms, has partnered with San Jose, California-based Counterpane Security, Inc. to offer insurance against business losses due to mischief by hackers.

Counterpane said the insurance program will protect against the loss of revenues and information assets caused by Internet and e-commerce security breaches. The firm will offer one program for its clients, and another that its clients can offer to their own customers.

Counterpane chief technology officer Bruce Schneier said, "This is not for your home user, this is for Yahoo!, this is for CDUniverse, which lost all those credit card numbers in January. It's threat avoidance. This, along with monitoring, is just another arrow in your quiver."

Lloyd's of London, one of world's largest insurance firms, has partnered with San Jose, California-based Counterpane Security, Inc. to offer insurance against business losses due to mischief by hackers.

Counterpane said the insurance program will protect against the loss of revenues and information assets caused by Internet and e-commerce security breaches. The firm will offer one program for its clients, and another that its clients can offer to their own customers.

Counterpane chief technology officer Bruce Schneier said, "This is not for your home user, this is for Yahoo!, this is for CDUniverse, which lost all those credit card numbers in January. It's threat avoidance. This, along with monitoring, is just another arrow in your quiver."

Ransom Insurance

Counterpane says its customers will have exclusive access to two previously unavailable insurance programs. The first program, Internet Access and Income Protection Coverage, is designed for Counterpane clients. The second, Internet Asset and Income Protection Warranty Plan, is a program that Counterpane clients can offer to their customers. Both plans cover damages, lost revenues and special costs. The cyber-damage protection portion covers the cost to repair and replace data and/or software to the same standard following a hacker attack that damages, destroys, alters, corrupts or otherwise misuses the customer's electronic devices.

The revenue protection portion covers financial losses following a service interruption or service impairment caused by a hacker maliciously blocking access to a customer's site.

The extortion protection part of the plan covers the costs of a specialist consultant's assistance in a security crisis and any subsequent negotiation, including payment of a ransom demand.

The insurance products will be underwritten by insurance brokers Frank Crystal & Co. and SafeOnline. Businesses needing more than $100 million (US$) in protection can negotiate additional coverage directly with Lloyd's.

Reluctant Insurers

According to Lloyd's, hackers can cause millions of dollars worth of damage, and insurance companies have historically been unwilling to insure against those losses. Said Bronek Masojada, CEO of Lloyd's insurer Hiscox, "Until now, the insurance industry has not had sufficient assurance of risk control from security companies."

Masojada said that Counterpane showed Lloyd's that it was able to substantially reduce its clients' exposure to risk through security monitoring. Because of Counterpane's monitoring services, Lloyd's was able to "broaden the coverage and increase the amount and availability of our insurance to Counterpane and their customers," Hiscox said.

According to the Insurance Information Institute, a non-profit organization sponsored by the property/casualty insurance industry, e-commerce insurance has been available for some time. However, many dot-com companies were either not aware of its existence or did not feel a need for it until after the denial-of-service (DoS) attacks on Yahoo! and other major Web sites last February.

The DoS attacks reportedly sparked a flood of calls to insurance brokerages. The Insurance Information Institute said that sales of e-commerce insurance policies could exceed the $2.5 billion now spent on directors' and officers' liability insurance policies.

The organization said that an e-commerce policy "can include loss of business income, public relations, intellectual property, difference in conditions, interruption of service and electronic publishing liability. In general, companies with revenues of $1 billion or less can expect to pay premiums of about $25,000 to $125,000 for at least $25 million in coverage. Coverage limits can be as high as $200 million."

The Institute notes that DoS attacks and other e-commerce risks are not covered by typical business insurance policies, but rather by e-commerce insurance policies which will usually cover the cost of computer consultants and lost income during the time an e-commerce site is down. Lost income can include lost sales for e-tailers and lost "click-throughs" for content provider sites.

A report out last week from Jericho, New York-based Reality Research predicted that businesses worldwide will lose more than $1.5 trillion this year due to computer viruses spreading through the Internet. Computer Economics, Inc. has estimated that the "I LOVE YOU" virus, which was released earlier this year and spread via e-mail, affected 45 million computer files and cost companies $2.61 million.

2.3. The analysis of implementing the information risk insurance in Uzbekistan

Today, practically no sector of the economy that would not use information and communication technology, and everyday life for many of us associated with the use, creation, processing and storage of information resources. Information resources are becoming an important value, the risk of loss or damage which excites every connoisseur information. That is why the development and implementation of the mechanism of protection of information resources is one of the urgent issues of modern society. Today in the world there are a number of methods of protection of information systems. One of the new methods of information security is the insurance of information risks.

Legislation in the field of information security is a branch of the national legislation, which has a long and complex process of development and which continues to grow. Law-making and practice in this regard plays a huge role. The presence of a significant number of legal acts in this area and an active legislative process, inadequate legal regulation of social relations in the sphere of information also confirm the need for a systematic analysis of the legislation in this area; development in accordance with the state policy of development of legislation on the use of information and communication technologies (hereinafter - ICT), as well as policies for the protection of information.

A fundamental piece of legislation for the protection of information is the Law of the Republic of Uzbekistan "About principles and guarantees of freedom of information", which are the basic concepts such as "information", "information sphere", "confidential information", "information security," "protection of information ". The Oliy Majlis passed about 75 laws related to some extent to the information, information services and information technology, in particular, in 2005 the Law "On electronic payments", and "On protection of information in automated banking systems." The adoption of these laws helped the transition of the banking system to a new legal level, as well as protection of the rights of the

owner provided information. In 2007, the Law of the Republic of Uzbekistan dated December 25, 2007, № ZRU-137 "On amendments and additions to some legislative acts of the Republic of Uzbekistan in connection with the strengthening of responsibility for committing illegal acts in the field of information and data" of the Criminal Code was amended by the Head XX1. "Computer crime" However, these laws are only a small fraction of the regulatory - legal acts that should govern activities information and information technology, including in the field of information security. One of the areas of protection of information rights and freedoms of the individual and the state is the organizational - legal security of their information security. Canning legal basis for the development of information on the legal framework that has been created is impossible. In a society such changes occur, which on the one hand, the increasing potential of information and communication technologies (ICT) as part of the world economy, the international and domestic markets, provide capacity-building of information, on the other - form such socially significant structures that give it more complex targets for the use of these technologies. For the Republic today is the task of forming and implementation of national administrative and other reforms. In particular, it is the development of e-government and government online services. In connection with the establishment in accordance with the Resolution of the Cabinet of Ministers №250 Centre for the Development of "Electronic Government" and the Center for information security that are more deeply investigate the processes, law is also intended to respond to this development factor.

With the development of information and communication technologies (ICT), any business activity is closely linked to the receipt, storage, processing and use of various information. Uncertainties and risks associated with entrepreneurship are one of its characterizing features. Today the level of competitiveness of the economy largely depends on the ability to protect information from theft, unauthorized use, alteration, destruction and other IT-inherent risks. Operating experience of information systems and resources in various areas conclusively shows that there is different and very real threats (risks)

loss of information, leading to a specific expressible material damage. To protect and store data on the impact of information risks are different automated systems, which are designed to prevent unauthorized intrusion, however, to completely eliminate the risk of leakage or loss of information impossible. This is due to the vulnerability of networks and errors provoked by human factor, as well as the rapid development of new technologies. In world practice of risk management used such methods to reduce risks such as diversification or risk allocation, reservation of funds to cover unexpected losses, insurance risks, and others. Among them insurance as international practice shows, it is one of the effective methods of compensation losses. Insurance of information risks - is a method of information protection within the financial and economic system to ensure the protection of information, based on the issuance of the insurance company guarantees to subjects of information relationships to fill the financial and material damage in the event of the risks associated with information security threats. Developed countries have long appreciated the relevance of the information security risks for disclosure of data or malfunction of electronic systems entail huge losses. Accordingly, it is increasing and the number of customer calls to the insurance companies that operate in conjunction with software vendors, in order to increase the reliability of information systems. With the development of IT-technologies Services Insurance of information risks becoming popular in Uzbekistan, since the development of the ICT sector generates more new risks that are typical of this area. We have established a pattern: the growth rate of the number of the risks is directly proportional to the rate of development of the economy or a particular industry. The fact is that economic development contributes to the emergence of new types of uncertainties and risks are just the result of such uncertainties. In order to determine the dependence of the rate of growth in the number of risks and economic development, we carried out a sociological survey. As a result, we established the legitimacy of our conclusion about this relationship. At the same time the results of the survey showed that 73% of the subjects of the ICT sector believe that external

risk factors are the most dangerous, and the remaining 27% said that the most dangerous are the internal factors, particularly industrial and economic activities, the sphere of circulation of money and the scope of control. One of the important results of the poll of managers and specialists on risk management actors of the ICT sector of Uzbekistan was the conclusion that in a conceptually important is not to avoid risk at all, which is practically impossible, and through good monitoring system analytical work movement elements to business elimination of their deviation from the desired path. This requires the formation of a modern insurance system, capable of providing quality protection activity of ICT. And today in the field of ICT in Uzbekistan has already established such a system. First particular insurance program has become a product developed on the initiative of the Uzbek Agency for Communication and Information (now the Ministry for the development of information and communication technologies) Centre «UNICON.UZ» together with the insurance company «ALSKOM».

Innovative product "Insurance of information risks" allows to cover damage from exposure to the risks associated with loss, theft, destruction or alteration of information. Among them we can consider:

- Faults and failures of communication, hardware and software of computer technology;
- Unauthorized actions of staff or third parties;
- Interception of information in networks and data communication lines;
- Implementation of software viruses;
- Distortion of the information in the database;
- Illegal copying of data;
- Theft of information;
- The destruction or disruption of information processing, communication lines.

This insurance product is designed not only for the companies operating in the ICT sector, but also for all entities that use information technologies, such as billing and bank-client software and other types of information systems. The benefits of insurance as a method of protection against information risks are

obvious. This is not only a way of pecuniary damage. The use of insurance involves the analysis of the object of insurance, as well as a complete and thorough audit of information security systems of the enterprise prior to the conclusion of an insurance contract. In this interest as a policyholder, that it is important not to overpay premiums and the insurer who does not want to take insurance "unfinished" system. This insurance carries a stimulating function, ie enterprise, improving their information security system, is able to lower their insurance costs. In general insurance information risk allows covering the risks associated with virtually any hardware and software systems for the collection, transmission, storage and processing.

A number of organizations of communication and information have already realized the economic benefits of information security risks and are active users of the insurance services. In a relatively short period of implementation of this innovative insurance product has already taken place more than one insured event for which the Company promptly and fully compensated the damage from the impact of information risks. To date, the largest single amount of insurance indemnity amounted to about 35 million sum.

Conclusion for Chapter 2. With the rapid development of informatization in Uzbekistan must not forget that the losses from the impact of information risks can be enormous, and as a result, may suffer not only the owners, but also users of information systems. That is why the question of the widespread introduction of the insurance product is important. The most optimal solution of the widespread introduction of information security risks is the use of a binding mechanism for the use of this service by all entities providing services in the field of ICT.

We believe that the development and successful implementation of the program of development of information security risks will contribute to the widespread use of insurance products in Uzbekistan. This in turn will strengthen the system of information security and minimize damage from the impact of information risks in the conditions of the introduction of advanced information technologies.

CHAPTER 3. CHALLENGES AND RECOMMENDATIONS ON ASSESSMENT COST OF INFORMATION SYSTEMS AND RISKS, THEIR IMPLEMENTATION OF MODERN CONDITIONS

3.1. Problems on assessment cost of information systems and risks, the development of the information risk insurance

Every organization today which are use information technology have problem with information system security. The first step in process of protection of an information system is identification and classification of information resources or assets, which need protection, because they are vulnerabilities to threats. The major purpose of the classification is to prioritize further investigation and identify appropriate protection. The typical assets associated with information and information technology includes: information, hardware, software, people, services and documents. Risk assessment is process of assessing security-related from internal and external threats to an entity, its assets, or personnel. Also, we can say that the risk assessment is process of identifying vulnerabilities and threats to an organization's information resources (difference in terminology between the risk analysis and the risk assessment brings a new vague in the risk management process). Generally, risk can be transferred, rejected, reduced or accepted, but risk never eliminated, and they can be describing in the follow mathematical equation: Total risk = threats x vulnerability x asset value. When we develop risk management and assessment program, we must follow next steps: 1. understand the organization and identify the people and assets at risk, 2. Specify loss risk events and/or vulnerabilities, 3. establish the probability of loss risk and frequency of events, 4. Determine the impact of events, 5. Develop options to mitigate risk, 6. Study the feasibility of implementation of options and 7. Perform a cost benefit analysis. For developing a risk management and assessment program we must use some of the various methods and techniques for risk assessment, which can be complete or incomplete. Differences between these two approaches in process of risk assessment determine which approach will be implemented in particular

organization. The risk assessment process is about creation decisions. The impact of a successful attack and the level of suitable risk for any given situation is a basic strategy decision. A primary problem of risk management is to accomplish a cost-effective balance between design characteristic and the related countermeasures to threats and impact. This paper describes an analysis and comparison of complete methods for risk assessment major representative like British Standard (BS); CCTA[10]Risk Analysis and Management Method (CRAMM); Consultative, Objective and Bi-functional Risk Analysis (COBRA); RuSecure; Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) and Failure Mode and Effects Analysis (FMEA), which is the first step in process of develop a new method for risk assessment for the particular organization.

With the development of information and communication technologies (ICT), any business activity is closely linked to the receipt, storage, processing and use of various information. Uncertainties and risks associated with entrepreneurship are one of its characterizing features. Today the level of competitiveness of the economy largely depends on the ability to protect information from theft, unauthorized use, alteration, destruction and other IT-inherent risks. Operating experience of information systems and resources in various areas conclusively shows that there are different and very real threats (risks) loss of information, leading to a specific expressible material damage. To protect and store data on the impact of information risks are different automated systems, which are designed to prevent unauthorized intrusion. However, to completely eliminate the risk of leakage or loss of information is impossible. This is due to the vulnerability of networks and errors provoked by human factor, as well as the rapid development of new technologies. In world practice of risk management used such methods to reduce risks such as diversification or risk allocation, reservation of funds to cover unexpected losses, insurance risks, and others. Among them insurance as international practice shows, it is one of the effective methods of compensation losses.

[10] Central Computer and Telecomunications Agency

Insurance of information risks - is a method of information protection within the financial and economic system to ensure the protection of information, based on the issuance of the insurance company guarantees to subjects of information relationships to fill the financial and material damage in the event of the risks associated with information security threats.

Developed countries have long appreciated the relevance of the information security risks for disclosure of data or malfunction of electronic systems entail huge losses. Accordingly, it is increasing and the number of customer calls to the insurance companies that operate in conjunction with software vendors, in order to increase the reliability of information systems.

With the development of IT-technologies Services Insurance of information risks becoming popular in Uzbekistan, since the development of the ICT sector generates more new risks that are typical of this area. We have established a pattern: the growth rate of the number of the risks is directly proportional to the rate of development of the economy or a particular industry. The fact is that economic development contributes to the emergence of new types of uncertainties and risks are just the result of such uncertainties.

In order to determine the dependence of the rate of growth in the number of risks and economic development, we carried out a sociological survey. As a result, we established the legitimacy of our conclusion about this relationship. At the same time the results of the survey showed that 73% of the subjects of the ICT sector believe that external risk factors are the most dangerous, and the remaining 27% said that the most dangerous are the internal factors, particularly industrial and economic activities, the sphere of circulation of money and the scope of control.

One of the important results of the poll of managers and specialists on risk management actors of the ICT sector of Uzbekistan was the conclusion that in a conceptually important is not to avoid risk at all, which is practically impossible, and through good monitoring system analytical work movement elements to business elimination of their deviation from the desired path. This requires the

formation of a modern insurance system, capable of providing quality protection activity of ICT. And today in the field of ICT in Uzbekistan has already established such a system. First particular insurance program has become a product developed on the initiative of the Uzbek Agency for Communication and Information (now the Ministry for the development of information and communication technologies) Centre «UNICON.UZ» together with the insurance company «ALSKOM».

Innovative product "Insurance of information risks" allows to cover damage from exposure to the risks associated with loss, theft, destruction or alteration of information. Among them we can consider:

- Faults and failures of communication, hardware and software of computer technology;
- Unauthorized actions of staff or third parties;
- Interception of information in networks and data communication lines;
- Implementation of software viruses;
- Distortion of the information in the database;
- Illegal copying of data;
- Theft of information;
- The destruction or disruption of information processing, communication lines.

This insurance product is designed not only for the companies operating in the ICT sector, but also for all entities that use information technologies, such as billing and bank-client software and other types of information systems. The benefits of insurance as a method of protection against information risks are obvious. This is not only a way of pecuniary damage. The use of insurance involves the analysis of the object of insurance, as well as a complete and thorough audit of information security systems of the enterprise prior to the conclusion of an insurance contract. In this interest as a policyholder, that it is important not to overpay premiums and the insurer who does not want to take insurance "unfinished" system. This insurance carries a stimulating function, ie enterprise, improving their information security system, is able to lower their insurance costs.

In general insurance information risk allows covering the risks associated with virtually any hardware and software systems for the collection, transmission, storage and processing.

A number of organizations of communication and information have already realized the economic benefits of information security risks and are active users of the insurance services. In a relatively short period of implementation of this innovative insurance product has already taken place more than one insured event for which the Company promptly and fully compensated the damage from the impact of information risks. To date, the largest single amount of insurance indemnity amounted to about 35 mln. UZS. One of the main issues in the insurance of information risks is to determine the sum insured, ie monetary values within which the insurer is liable for the fulfillment of its obligations under the insurance contract. It is determined by agreement of the parties and shall not exceed the cost of information systems.

The problems for the development the assessment the cost of information systems and risks, the development of information risk insurance:

1. There is the implementation of the mechanism of insurance of information risks only for the legal entities in the field of information security.
2. There is no development and approval of the draft decision on compulsory insurance information and communication systems and resources, including Electronic databases of public authorities, economic entities and banks.
3. Still there is no the inclusion in a licensing agreement entered into with entities providing services in the field of ICT, of the requirement of information security risks as the financial and economic method of ensuring the information security of their activities.
4. There is no the development of the legal framework for assessing the value of the information systems of individuals.
5. The possibility of incorporating this type of insurance qualifier insurance activities in Uzbekistan hasn’t considered.

6. To provide in a statement to the expert organization, the audit information security business entity to implement the recommendations of insurance of information risks, as a method of information security, in cases where the level of information security would be below a certain standard.

3.2. Recommendations on assessment cost of information systems and risks, their implementation of modern conditions

It should be noted that the above method is used to determine the value of information systems entities. The question of determining the value of the information systems of individuals today is difficult due to the individuality of their information systems. In simple words, the information owner can cost a lot of money, but for the other person does not have a value.

Taking this into account, as well as to improve and wide application of information security risks in the practice should consider the development and approval of the Ministry for the development of information technologies and communications of a clear program of information security risks, taking into account the decision of the following important tasks in this direction:

1. The introduction of the mechanism of insurance of information risks for the individuals in the field of information security. With the rapid development of information technologies and information society issues of information security has become an urgent problem today. Insurance of information risks is the most alternative financial and economic method of information security. For this reason, the widespread introduction of information security risks in the Republic will offset the costs resulting from the impact of information risks. This service normally provides for Internet users in the event of a leak are mainly due to the use of the Internet. The insurance company cannot determine the value of information for individuals, so that information can be valuable only for the subject. Therefore, the sum insured and the premium can be installed fixed (amount set for all constant) amount.

2. Development and approval of the draft decision on compulsory insurance information and communication systems and resources, including Electronic databases of public authorities, economic entities and banks. Losses from the impact of information risks can be enormous, and as a result, may suffer not only the owners, but also users of information systems. That is why the question of the widespread introduction of the insurance product is important. The most optimal solution of the widespread introduction of information security risks is the use of a binding mechanism for the use of this service by all entities providing services in the field of ICT. It will introduce a monitoring mechanism in this regard by the state regulator in the field of ICT.

3. The inclusion in a licensing agreement entered into with entities providing services in the field of ICT, of the requirement of information security risks as the financial and economic method of ensuring the information security of their activities. Uzbekistan already has experience in the use of such a mechanism. To date, 19 types of compulsory insurance services are widely used because of its established system of state control.

4. Development of the legal framework for assessing the value of the information systems of individuals. The current method of assessment is to determine the value of information systems entities. The question of determining the value of the information systems of individuals today is difficult due to the individuality of their information systems. In simple words, the information owner can cost a lot of money, but for the other person does not have a value. This development should be carried out by studying the international experience of the valuation of information systems, taking into account the peculiarities of information society in Uzbekistan.

5. Consider the possibility of incorporating this type of insurance qualifier insurance activities in Uzbekistan. Today the product is insurance of information risks is implemented as a property insurance within the framework of the relevant class of insurance. Taking into account the distinctive features of an insurance product from a traditional property insurance, as well as to its

widespread introduction in the domestic insurance market by engaging in the process of other insurance organizations considered appropriate, develop and implement a separate class of licensed insurance of information risks.

6. To provide in a statement to the expert organization, the audit information security business entity to implement the recommendations of insurance of information risks, as a method of information security, in cases where the level of information security would be below a certain standard. This will implement reasonable insurance information risk in subjects with low levels of information security.

Conclusion for Chapter 3. One of the important results of the poll of managers and specialists on risk management actors of the ICT sector of Uzbekistan was the conclusion that in a conceptually important is not to avoid risk at all, which is practically impossible, and through good monitoring system analytical work movement elements to business elimination of their deviation from the desired path. This requires the formation of a modern insurance system, capable of providing quality protection activity of ICT. We believe that the development and successful implementation of the program of development of information security risks will contribute to the widespread use of insurance products in Uzbekistan. This in turn will strengthen the system of information security and minimize damage from the impact of information risks in the conditions of the introduction of advanced information technologies.

CONCLUSION

Today the private and public sectors face financial and reputational damage, competitive inroads, and significant regulatory sanctions when confidential information is inadequately protected. Clearly enough reasons as to why cyber security must be prioritized regardless of what sector one conducts their organization.

Besides the weekly round, or of late what seems to be becoming more of a daily occurrence of cyber attacks just as much continues to happen offline as well. “Unencrypted” mobile devices continue to get lost which in turn increases the number of data breaches that we all read about in the media headlines on what seems like a weekly basis.

In today's world, where technology is a key element in the structure of any company, increasingly raises the question of protection of digital data. Despite the large number of antivirus software, passwords and system access restriction information stored on electronic media, it is still exposed to various risks, whether it is a server failure or accidental destruction of the necessary data.

The benefits of insurance as a method of protection against information risks are obvious. This is not only a way of pecuniary damage. The use of insurance involves the analysis of the object of insurance, as well as a complete and thorough audit of information security systems of the enterprise prior to the conclusion of an insurance contract. In this interest as a policyholder, that it is important not to overpay premiums and the insurer who does not want to take insurance "unfinished" system. This insurance carries a stimulating function, ie enterprise, improving their information security system, is able to lower their insurance costs.

In general insurance information risk allows covering the risks associated with virtually any hardware and software systems for the collection, transmission, storage and processing. A number of organizations of communication and information have already realized the economic benefits of information security risks and are active users of the insurance services.

Information security has increasingly become an important topic for small and big organizations alike. Although awareness and efforts towards security have increased, unfortunately, this increase does not appear to be mitigating the number or cost of incidents from either internal or external sources. One reason for the problem is that the technology is changing faster than what financially-strapped businesses and information technology (IT) departments can handle. Most organizations are not only increasing the size of their networks but also adding new types of connectivity and complexity. For example, acquisition and implementation of different types of systems because of back-end business process integration with suppliers and other partners and front-end process integration with clients and customers. In some cases, this kind of integration is forced due to mergers and acquisitions. In several instances, market's competitive pressures on hardware and software vendors forces them to implement security features and test products prior to product release in a shortened time span and compromise security. A lot of times security is an afterthought and it turns out to be an add-in into existing systems and applications which is difficult, expensive, and, in some cases, impossible without serious operational impact. Even if security mechanisms exist, there is another fundamental problem involving the implementation of controls. With the development of information and communication technologies (ICT), any business activity is closely linked to the receipt, storage, processing and use of various information. Uncertainties and risks associated with entrepreneurship are one of its characterizing features. Today the level of competitiveness of the economy largely depends on the ability to protect information from theft, unauthorized use, alteration, destruction and other IT-inherent risks. Operating experience of information systems and resources in various areas conclusively shows that there is different and very real threats (risks) loss of information, leading to a specific expressible material damage. To protect and store data on the impact of information risks are different automated systems, which are designed to prevent unauthorized intrusion. However, to completely eliminate the risk of leakage or loss of information is impossible. This is due to the

vulnerability of networks and errors provoked by human factor, as well as the rapid development of new technologies. In world practice of risk management used such methods to reduce risks such as diversification or risk allocation, reservation of funds to cover unexpected losses, insurance risks, and others. Among them insurance as international practice shows, it is one of the effective methods of compensation losses.

Insurance of information risks - is a method of information protection within the financial and economic system to ensure the protection of information, based on the issuance of the insurance company guarantees to subjects of information relationships to fill the financial and material damage in the event of the risks associated with information security threats.

Developed countries have long appreciated the relevance of the information security risks for disclosure of data or malfunction of electronic systems entail huge losses. Accordingly, it is increasing and the number of customer calls to the insurance companies that operate in conjunction with software vendors, in order to increase the reliability of information systems.

With the development of IT-technologies Services Insurance of information risks becoming popular in Uzbekistan, since the development of the ICT sector generates more new risks that are typical of this area. We have established a pattern: the growth rate of the number of the risks is directly proportional to the rate of development of the economy or a particular industry. The fact is that economic development contributes to the emergence of new types of uncertainties and risks are just the result of such uncertainties.

In general, we can say that now in Uzbekistan, favorable conditions for the development of this type of insurance. However, it is clear that as the formation of a civilized culture of risk management the demand for insurance of information risks will grow.

LIST OF REFERENCES

I. Legislation of the Republic of Uzbekistan

1. Law “On communication” of the Republic of Uzbekistan, dated 13.01.1992 №512-XII (with amendments and additions).

2. Law “On telecommunications” of the Republic of Uzbekistan, dated 20.08.1999 №822-I (with amendments and additions).

3. Law of the Republic of Uzbekistan "About principles and guarantees of freedom of information"

4. Law “On informatization” of the Republic of Uzbekistan, dated 11.12.2003 №560-II.

5. Law “On digital signature” of the Republic of Uzbekistan, dated 11.12.2003 №562-II.

5. Law “On electronic document management” of the Republic of Uzbekistan, dated 29.04.2004 №611-II.

II. Decrees of the President of the Republic of Uzbekistan and resolutions of the Cabinet of the Ministers

6. The Decree of the President of the republic of Uzbekistan“On measures of further implementation and development of modern information and communication technologies” dated 4.02.2012.№PD-1730.

7. The 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” dated 21.03.2012. № PD1730.

8. The Decree of the President of the republic of Uzbekistan “On creation of the State Committee for communication, informatization and telecommunication technologies of the Republic of Uzbekistan” dated 16.10.2012 №PD-4475.

9.The Decree of the Cabinet of Ministers of the Republic of Uzbekistan "On measures for further improvement of interaction of public and economic governance, the local authorities with legal entities and individuals using information and communication technologies" dated 23.08.2007. №181.

10. The Decree of the Cabinet of Ministers of the Republic of Uzbekistan “On measures for further improvement of the governmental portal with the provision of online public services” dated 30.12.2012, №378.
11. The Decree of the Cabinet of Ministers of the Republic of Uzbekistan ”On measures to organize the activities of the e-Government center and the Information security center” dated 16.09.2013. №250.
12. The law "On Commercial Secrets" was signed on September 11, 2014 by the President of the Republic of Uzbekistan Islam Karimov.
13. The Law "On electronic payments" and "On protection of information in automated banking systems." were signed in 2005 by the President of the Republic of Uzbekistan Islam Karimov.

III. Publications of the President of the Republic of Uzbekistan

14. Karimov I.A. Our main task – the country’s development and welfare of the people. – Tashkent.: Uzbekistan, 2010., P.54.
15. Karimov I. A.The Speech of the President of Uzbekistan at the meeting of the Cabinet of Ministers on January 18, 2013, dedicated to the summary of social and economic development in 2012 and main priorities of economic program for 2013.
16. Karimov I.A. Development of the country rapidly mobilizes all the possibilities of the continuation of proven strategies reform. Uzbekistan. 2014. P.64.
17. I.A. Karimov, the magazine “Xalq So’zi” dated January 19, 2013.

IV. Main references

18. Арипов А.Н. ва бошқ. Ўзбекистонахборот коммуникация технологиялари соҳас именежменти масалалари. – Т.: «Fan va texnologiya», 2005.
19. Joon Song H. E-government in developing countries: Lessons learned from Republic of Korea. UNESCO: Communication and Information in Asia, 2006.-87p
20. Information Risk Management. Economically viable safety / Petrenko SA, Simonov SV - M .: IT Co., DMK Press, 2004. - 384 p .: ill. - (IT engineers).
21. The INSURANCE FOR CYBER-RISK MANAGEMENT By Lawrence A. Gordon, Martin P. Loeb, and Tashfeen Sohail

22. The Risk Management in the Insurance Business Sector, Claudio Fernandez Published by MFC Artes Graficas, S.L.

V. Periodical and statistical publications and reports

23. National Seminar: "Information security in communications and informatization sphere. Problems and solutions”

24. The User Challenge. Benchmarking the Supply of Online Public Services, European Commission, Directorate General for Information Society and Media. Brussels, 2007. – 122 p.

25. Yearbook. International telecommunication union.Measuring the Information Society 2012.ITU, 2012. – 71 p.

26. Measuring information society. International Telecommunication Union GenevaSwitzerland,2013. – 157 p.

VI. Internet sites

http://gov.uz/uz- The Governmental portal of the Republic of Uzbekistan

https://my.gov.uz/en - The single interactive state services portal

http://en.wikipedia.org - The free encyclopedia

http://www.uz.undp.org - United Nations Development Programme

http://stat.uz/en/index.php - The State Committee of the Republic of Uzbekistan on Statistics

http://www.ziyonet.uz/ - Scientific Portal

http://ccitt.uz/uz/ - The State Committee for Communication, Informatization and Telecommunication Technologies of the Republic of Uzbekistan

http://press-service.uz/en/ - Press Service of the President of the Republic of Uzbekistan

http://parliament.gov.uz/en/ - Official website of Legislative Chamber of OliyMajlis of Uzbekistan

http://www1.worldbank.org/publicsector/ egov/egostudies.htm - World Bank