УДК 654.07.012.12

V.S. Kanev, Dr. Sci (Tech.), Cand. Sci. (Phys.-Math.), Associate Professor

Siberian State University of Telecommunications and Information Sciences, Novosibirsk, RF,
e-mail: shevcova_yuliya@mail.ru, kanev@sibsutis.ru

SYSTEM RISK MANAGEMENT METHODS, MODELS AND THEIR IMPLEMENTATION IN TELECOMMUNICATIONS

В.С. Канів, д-р техн. наук, канд. фіз.-мат. наук, доц.

Сибірський державний університет телекомунікацій та інформатики, м.Новосибірськ, Росія, e-mail: kanev@ngs.ru

МЕТОДИ, МОДЕЛІ ТА ЇХ РЕАЛІЗАЦІЇ ПРИ СИСТЕМНОМУ УПРАВЛІННІ РИЗИКАМИ В ТЕЛЕКОМУНІКАЦІЯХ

Purpose. To investigate the problems of system risk management in telecommunications in the Siberian region of the Russian Federation, specifics of the industry, its risk profile and risk management opportunities.

Methodology. Qualitative and quantitative risk management, risk factors diagnostics and modeling of operational losses, Bayesian networks.

Findings. Highlighted features of communication and Infocomm for risk management, their risk profile and risk management capabilities evaluated in a systematic manner. Determined when and how the possible qualitative and quantitative risk management, what the methods of management and gauges risk modeling capabilities perspective of risk situations are. In analyzing the Russian and foreign risk management practices in telecommunications, Cawthra shows the trend in the integration of risk management functions and automation of these functions in a single model the monitoring of the measuring complex to the nucleus in the center - Bayesian decision support technologies**.**

Distinct specifics of the telecommunication sector risk profile are identified based on qualitative and quantitative risk management. Prospective for using Bayesian technologies at continuous risk management are determined. Available experience of telecom companies in risk management is analyzed.

Originality. Adequate description of efficient procedures for integrated risk management systems in the rapidly developing sector that would make a pronounced impact to the overall economy growth rate.

Practical value. Methods and components of the risk management methodology will establish the basis for development of automated integrated risk management systems in the telecommunications sector. Such computing architecture will effectively organize preventive risk-Management at Telecom.

Keywords: *risk, risk map, risk profile, modeling, simulation, diagnostics, Bayesian networks*

Problem statement. Market success of a telecommunication company, its capacity to create competitive advantages, improve operational efficiency and, ultimately, increase its capitalization depends first of all on how successfully, fast and timely the company manages the complex of adverse threats and risks.

Today executives of telecommunication companies understand better that risk management is quite a considerable part of strategic management aimed at creation of preventive conditions for execution of enterprise management strategy being pursued at the given period of time.

The top telecommunication companies of a country that continuously improve the quality of corporate management lately began paying more attention to the enterprise risk control issues and already have achieved pronounced results in this area.

At the present time Russian telecommunication enterprises are ahead of other companies of non-financial sector in implementation of risk management. Mobile communications operators are the most active in this area, more than half of them have already been implementing elements of risk management while others, about the third of all, are ready to commence this process in the next years.

Risk management cannot be viewed as one-time decision or activity, even if it has been worked out in detail and seems to be justified. Risk management is dynamic process. This process is controllable if and only if the organization, simulation, measurement and methodology are in place.

Identification of unsolved problem. Simulation / measurement and methodology provisions for risk management systems directly depend on the nature of groups of risks the company faces, on skills possessed by the personnel in using appropriate tools and on risk management culture.

All risks encountered by telecommunication companies can be classified in the most aggregated version by the following types:

- operational risks related to the operational activity, business process functions performed by the personnel;
- financial risks associated with the financial activity: credit risks, market risks, liquidity, etc.;
- strategic risks that arise in the course of the company strategy definition, development and execution.

We suggest that system risk management in information and telecommunication companies shall be based

on a toolset engineered as a specially developed simulation / methodological measurement complex that would enable the companies to solve primary risk management problems [1].

Formulation of the objective of the study. This paper is aimed at studies of capabilities and specifics of system risk management in telecommunication companies in terms of development of an automated simulation / measurement complex for integrated risk management.

To do so it was necessary to learn and answer a number of questions and solve the following theoretical and practical problems:

- identify specifics of the industry, highlight its risk profile and evaluate capabilities for systematic risk management;
- stipulate when and how qualitative and quantitative risk management can be arranged;
- what the management methods and potential simulation are?

Presentation of the key material. The information and telecommunication industry in its contemporary interpretation as a sector of production and social infrastructure that consolidates telecommunication and information technologies and generates a considerable range of services for the telecommunications market.

The term "telecommunication market" is understood as the market of services such as: telephone services – local, long-distance, international phone communications, mobile communications, document communications, including data exchange, satellite communications and other continuously expanding communication services (e.g., telecommunication channels leasing, etc.).

Today the situation in the global telecom industry is driven by such key factors as: rapid growth of the mobile telecommunications segment, explosive expansion of the Internet, nearly discontinued growth of income of operators of conventional telecommunication services and fast development of liberalization, privatization and convergence of wide range of services.

Real boom is observed in the telecom sector: last years the overall growth of the telecom services providers' revenues was about twice as high as the world economy growth.

Traditionally the information and telecom industry grows faster than national economies. Information and revenues of the telecommunication companies have grown 7.6 times in the last 8 years; telecommunication services contributed 8.84 times and IT services grew 6.4 times while, at the same period, GDP grew 5.5 times. Comparing the annual average increments of GDP (6.5%) and information/telecom services (25.8%) indicates that the rate of economic growth of the information and telecommunications industry is almost 4 times greater than that of the national economy [3–4].

The causes of such fast growth rate can be explained, among other reasons, by the fact that contemporary environment business activities depend on more and more up-to-date information received in a timely manner and on development of supporting telecommunication technologies. Transformation of the telecom industry is growing fast. From the era of dominance of powerful state monopolies the industry is approaching formation of the large, most competitive and dynamic market, penetrating new business processes in different enterprises. The industry is changing rapidly and, merging with other industries, is heading to formation of the global information/telecommunication sector.

Telecom companies face a variety of risks in their business activities, ranging from those related to deficiencies in business processes to those strategic risks. Credit risks, market risks and liquidity risks are also in this risk range [5–6].

The integrated system for management of the entire range of company risks allows for minimization of losses and damages and, also, serves as one of the critical components of the attractiveness of company for investors. Besides, it creates favorable conditions for access to the international capital markets and, in case of the U.S. securities markets after the Sarbanes-Oxley Act was enacted, it becomes one of mandatory requirements to issuers [6].

To implement efficient tactical and strategic control stimuli modern telecom market agents must implement technological innovations, they should act boldly and beyond the conventional thinking, which increases the risks.

In the recent years risk management has become common practice for major telecommunication companies worldwide. British Telecom, France Telecom, Telenor and other companies pay more attention to integrated risk management systems that cover the entire enterprise (Enterprise Risk Management). Such systems provide for management and minimization of not only financial, currency and investment risks, but also enable their customers to control non-financial or operational risks.

As investors pay more attention than ever to this aspect, telecom companies have to search actively for new ways for stable generation of income, new ways for achievement of sound financial results.

It is unlikely to observe income growth resulting from technology advances or drastic increase of customers' activity in foreseeable future. Income growth can be achieved only through advances in such fundamental venues of risk-adjusted cost-efficiency improvement as:

- improvement of clients loyalty and retaining of enterprise efficiency;
- generation of maximum profit based on relations with each customer;
- development of more efficient and dynamic business processes with minimization of operational risks;
- determination of business profile potentials based on assessment of capital under risk using results based on adequate and correct indicators of the business operation;
- framing the entire activities of the company in the common strategic vectors based on the integrated risk management system.

If the modern business environment does not give telecom companies any reason to hope for significant growth of profit on the account of conventional technological advances or for a rapid growth of customer's activity, it should be achieved in different way. For instance, implementation of efficient schemes for retaining the existing subscribers and attraction of new ones, getting maximum benefits from relations with each clients,

optimizing of advanced business processes, running highly efficient marketing campaigns.

As we have noted above, all risks of telecom companies can be differentiated under the following categories:

- operational risks related to the operational activity, performance of business processes functions;
- financial risks associated with the financial activity;
- strategic risks that arise in the course of the company strategy defining, developing and implementing.

In our preliminary discussion at this point we will elaborate to some extent the issue of diagnostics and analysis of operational and strategic risks. These are most difficult for quantitative determination since they have been poorly supported by data and lack of scientifically developed methodology.

Operational risks are variances, off-nominal situations arising in the course of performance of different functions – business processes. The bigger is the company and the broader is the list of business processes performed in it, the more urgent becomes the problem of risk management system creation, the need for complex that would provide diagnostics, risk evaluation and measures employed for their mitigation.

Rather high risks in telecom companies are specific feature of operational risks management with heavy operational losses caused by such factors as:

- wrong directing of messages;
- internal and external frauds;
- billing errors;
- introduction of new rates and products;
- imperfections in business processes;
- incomplete or erroneous call detail records (CDR).

Analysis of recent researches. According to Analytics Research assessment 104 telecom operators worldwide have the losses due to operational risks that alone make up to 11.6% of the annual turnover.

Deeper analysis shows that the operational risk includes four main risk subcategories grouped by the source of losses.

Business processes risk is the risk of losses related to deficiencies of business operations or failures to observe the adopted technology for these operations, including sales of services, billing and payments, control and reporting, management, etc.

System risk is the risk of losses related to deficiencies or faults in computer exploiting or telecommunication systems, software or potential inadequacy of these systems and software.

Personnel risk is the risk of losses related to intentional or inadvertent errors made by the personnel and caused by lack of integrity or negligence, poor skills, insufficient or unstable manpower or criminal behavior.

External risk is the risk of losses caused by external events: frauds, unauthorized activities, changes in state administration, changes in legislation, tax regulations, social factors, natural disasters, etc.

Trying to move further in the analysis we will select the entire multitude or operational risk events such ones, for example, as external operational risks related to fraud and unauthorized activities and discuss them in detail.

Deeper analysis in this direction shows rather complex network of potential threats for stable operation of telecom companies. By acting in such a manner it is interesting to track down the financial and economic component of the problem. The following statistics help to understand the scale of the problem. It turns out that 20 billion dollars are the damage made to the telecom operators by fraudulent activities. Expensive international calls make up to 80% of all fraudulent calls while 20% of such calls are made locally [7].

More often the operators face frauds done by individuals or even companies. According to experts' assessments fraudulent calls take from 10 to 30% of the operators' traffic. For the last two-three years the number of fraud related crimes in phone networks dramatically increased. According to "C" Administration of the Russian Ministry of Interior Affairs only for 9 months of 2004 more than 10.200 crimes were committed in the area of telecommunications while in the 2003 their number were 10.900 [7].

Cases of fraud affect both operators and subscribers of telecommunication services. Rapid development of the Internet, implementation of new interfaces into the shared telephone networks equipment has created new sources of potential threat for telecommunication systems. In this case special role shall be assigned to security of the Common Channel Signaling CCS7 that connects most built networks which use different technologies, but do not have embedded security functions. What can be done to fight against such a serious threat?

The growing number of access weak points among networks increases potential safety breaches and networks become more vulnerable to external attacks. For example, if a connection route has at least one IP segment, all networks involved in the connection, including CCS7, are at danger of hacking.

From the CCS7 safety assurance standpoint the threats can be caused by both inadvertent and intentional offences. Inadvertent offences can result in overload or spontaneous propagation of errors. Intentional activities: masking, data integrity damages or important data monitoring and disclosure.

Three types of threats are identified: unauthorized access to resources, overloads and spontaneous propagation of errors throughout the network. Hackers often mix attacks of different types with consideration of object specifics under attacked and the goal of the attack, which may result in rather unpleasant and very diverse consequences: interruption of service, refusal in service providing, service quality deterioration, equipment overload, fraud, traffic disorder and theft. Still there are number of chances to interception into subscriber data integrity, billing data, content or chats. Besides the evident financial losses and damages they are far from being equal in terms of liability for financial damages.

The largest Siberian operator of Rostelecom reported [8] that it had equipped its network with multi-tier protection system that protects the company's servers and its subscribers from viruses and hackers. This equipment is designed for integrated protection of data processing centers, in particular – for protection of billing data and personal information of the company's subscribers.

The system is based on StoneGate solutions and employs Symantec products and software tools ArcSight; it provides integrated protection of data during its transmission and backup recording at the rate of up to 20Gb/s. The solution includes: protection against external threats, subsystems for network anomalies detection, preclusion of intrusions on the level of individual units, vulnerability analysis and multi-stage antivirus protection with centralized control.

These subsystems, in turn, are closely linked to the monitoring system developed by ArcSight and "capacitates a prompt respond to safety-related issues".

The Siberian operator does not disclose the cost of outfitting its entire system with this multi-tier protection, but it admits that its employees have to deal with attempts to crack company services all the time and these illegal activities include both direct breach attempts and virus attacks.

Every week the general directorate safety systems alone prevent from 300 to 600 thousand attempts to make unauthorized connections. The company has recorded all kinds of possible attacks, from chain letters to DDoS attacks, i.e. distributed attacks that destroy servers. However, according to the operator, so far hackers have been unable to hack the key systems such as billing. Nonetheless, the biggest Siberian operators admit, the share of costs for data security is growing.

"We have to use the most advanced solutions," explains [9] the Head of Information Security and Technical Protection Unit of the Siberian branch of Open Joint Stock Company MTS. He says, however, that it is not often that someone would try to hack the MTS system directly. "The last time such a situation was detected and defeated half a year ago." It is not that the attack intensity is growing, but hackers keep inventing new ways to penetrate closed networks. IT security unit experts, on the other hand, when developing network protection take account of all potential loopholes in the system and fix them. Smaller operators sometimes use non-conventional ways to protect their servers.

Procedures employing control of these risks may involve organizational/economical and engineering/ technology measures. Engineering/technology measures often come to development of custom devices to fight the threats.

When developing defense measures, attention must be paid to special systems for fraud monitoring that would be able to detect frauds in the networks and prevent thefts and other illegal activities. One of such systems is monitoring system Spider, this system designed in by LONIIS Russia and its anti-fraud component Spider FMS .

Here it shall be noted that recognition of the importance of operational risk management led Rostelecom holding to thorough attention to execution of pilot projects aimed at risk management [7].

Rostelecom became the first company in the industry that had implemented the pilot project for creation of operational risk management system in the regional branches of the company. As we have already noted (see Section 3), implementation of this system resulted in reduction of risk losses by up to 30%, improvement of manageability and creation of adequate information environment for efficient decision-making.

Deployment of such systems in telecom companies encounters a lot of difficulties due to a lack or shortage of risk management economy analysts who would possess professional skills for work in conditions of risk profiles immanent to telecom companies.

Qualitative analysis capabilities for risk management and, especially, the possibility of modeling different functions of the risk management are to a large extent driven by the type of the risk to be controlled and the method selected to control it.

Generally, this is a point of special consideration, but we do not pursue this goal here, even though we do not think it is insignificant. We only note here that operational risk and, actually, strategic risk as well are the least susceptible to modeling and obtaining reliable qualitative estimates – and it is exactly due to the lack of specially arranged statistics. Yet, even realizing these facts, telecom companies are forced to evaluate operational risks due to urgent business reasons, among which the following ones can be named:

- for organizations participating in security markets the very fact of having a department that control risks and facilitates their capitalization;
- damages from competition losses (customers loyalty issues);
- impossibility to meet customers' needs;
- risks related to development of networks;
- contractors missing the deadlines;
- financial deficiency to deal with peak loads.

Risk diagnostics can be run in the following steps:

- analysis of consequences of risk event occurrence;
- cause and effect links analysis for various business threats and hazards;
- analysis of independent risk factors (potential threats);
- analysis of potential interdependences between the risk factors.

In the course of diagnostics data on risk incidents occurrence is acquired and analyzed and list of key risks of the company that may considerably affect its business is compiled. Preliminary qualitative evaluation of risks can be achieved based on surveys of experts' opinions and questionnaire surveys (point-based or rank-based estimate, development of company risk maps).

Risk map is graphical and textual description of a limited number of company's risks placed in a rectangular table where one "axis" denotes the magnitude of impact or significance of the risk while the other axis marks the probability or frequency of the risk occurrence. Fig. 1 shows the example of a risk map.

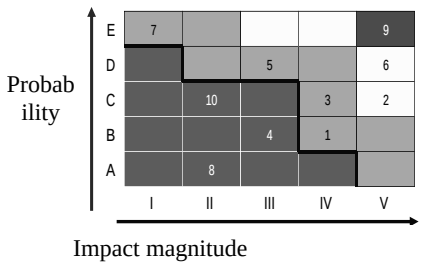

Fig. 1. Risk map

ISSN 2071-2227, Науковий вісник НГУ, 2014, № 4

On this risk map the probability or frequency is mapped on the vertical axis while the impact magnitude or significance is marked on the horizontal axis. In this case the probability of risk occurrence increases from bottom up when moving along the vertical axis and risk impact increases from left to right along the horizontal axis.

Arabic numbers on the map denote risks that were classified by four significance categories and six probability categories in such a way that one type of risk is related to each combination of probability and significance. This classification that places each risk in a separate rectangle simplifies the priority setting process by showing the position of each risk relative to other risks (it improves the efficiency of this method).

The heavy broken line marks the critical boundary of risk tolerance. When identifying critical risks the cases (cause and effect chain in processes, events and accumulation of risk factors) that are above this line are the cases assumed to be intolerable. When developing a strategy, for instance, before this strategy is adopted, it has to be understood how to mitigate or transfer the intolerable risks, while the risks below this boundary are controllable in the course of routine operation. Risk significance shall be evaluated through empirical rule as the product of criticality and probability.

Risk management quality can be naturally obtained and based on whether or not points marked with Arabic numerals 'migrated' from the top part of the map to the bottom part (fig. 2).

At the next stage to proceed to more developed and more reliable forms of quantitative analysis data on losses shall be stored in data banks of special structure and, hopefully, this data will be subjected to systematic mathematical/statistical processing.

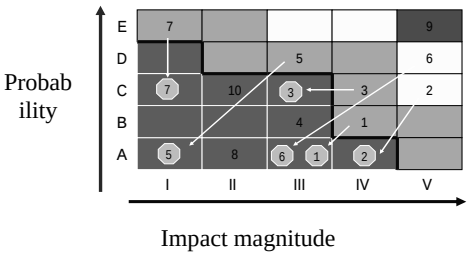

Fig. 2. Potential trajectories for the company risk background based on results of risk management

It would be reasonable to ask what toolset should be like for efficient management of operational risks. To answer this question it is necessary to clarify the economic nature of randomly occurring operational expenses. Expected and unexpected losses should be recorded through well-established procedures of statistical control; these losses are factors based on historical data on losses. Losses that are responsible for crises (excess losses) are amounts which are bigger than unexpected losses. A legitimate question can be raised on the size of capital required to cover the risks – the total amount of finance needed to cover unexpected losses. It should be noted that in this context it is an interesting purely mathematical problem and good approaches have already been found to solve it correctly.

Capital sufficiency to cover operational losses depends on the size of capital that can be safely withdrawn and it should be determined using both economic considerations and regulatory requirements. We do not know the main part of questions on capital sufficiency regulations for the RF telecom companies. Economic considerations lead to application of such methods [7] as:

- basic indicator (α-indicator) and
- standard approach (β-indicators by business processes elements), scenario-based approach.

The most advanced area in the quantitative operational risk management is the financial institutions sector, in particular – banking. For these companies simulation issues have been elaborated fairly well and in rather rich regulatory environment.

The nature of the operational risk profile generally is independent or, rather, not strongly dependent on what industry the enterprise belongs to, so the positive experience gained there should be applied in new or different disciplines.

The advanced approach [8] to computation of capital to be reserved for operational risks coverage requires banks to create databases that would reflect operational losses. And this is reasonable. The western banking communities have opportunities to approach external data providers who would supply information on risk events and who create operational losses data arrays; the banks can subscribe to these databases and obtain data in volumes required for reliable assessments.

This brings up the need to develop the model of operational losses with heterogeneous data and to incorporate them into integrated model through consolidated samples of operational losses, each containing data that exceeds different thresholds. No less important is to analyze model parameters susceptibility to thresholds variations.

In situations where the acquired statistics on operational losses is sufficient one can proceed to computation of more advanced risk measures.

One of the most popular simulations of risk measure is *VaR (Value-at-Risk).* This is how it can be defined. Let X be operational losses in N days. These losses are a random variable and depend on a number of different factors in the period of N days. The value $q = VaR_{\alpha}(X)$ is a quantile of level α of a random variable X distribution, i.e. the probability of X being no greater than q is 0.01α (here α is measured in percent). Once *VaR* is calculated, we can make statements like: "We are α % confident that we won't lose more than q in next N days" (fig. 3).

Quite a few works have been dedicated to *VaR* computation methodology [7–8]. Not only this method is used by traders and portfolio managers, but also by regulatory agencies. For example, in the USA regulatory agencies require the banks to have a surplus in the amount of 3 times the 10-day 99% *VaR* as an allowance for the market risks.

Despite its popularity *VaR* is not free from considerable shortcomings.

First, *VaR* does not take into account potential heavy losses that may take place at low probabilities (less than 1-0.01α).

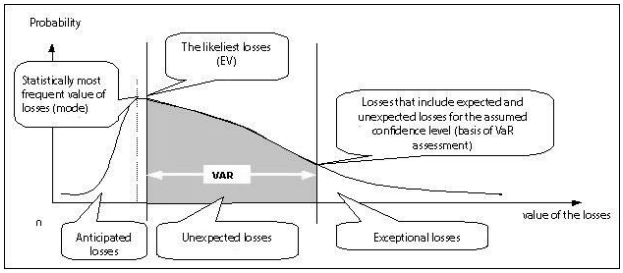

Fig. 3. Determination of VaR value

Second, *VaR* cannot distinguish between different types of loss distribution tails and, therefore, underestimates the risk in case the distribution has 'heavy tails' (i.e. its density drops slowly).

Third, *VaR* is not coherent measure; in particular, it does not possess the *subadditive* property. Examples can be shown where portfolio *VaR* is greater than sum of two *VaR*s of two subportfolios it consists of. This does not make sense. In fact, if the risk measure is viewed as a size of capital reserved to cover the market risk, then to cover the risk of the entire portfolio there is no need to reserve more than a sum of reserves of sub-portfolios the whole portfolio is composed of.

Identification of the unsolved part of the overall problem. As it was noted above (see section 3) a great deal of interest to operational risks measurement and control has been observed lately in the telecommunication services sector. This concern is related to introduction of a few regulatory recommendations in the area of corporate management and evaluation of capital sufficiency to cover operational risks.

Apart from market, credit or insurance risks, which are covered with usually assigned finances in most cases companies suffer financially from operational risk that is usually not backed up with reserve capital.

Development of models arouses for more adequate definition of operational risk that would be based not on sources of losses (see section 2), but rather on the profiles of business activities of the company. Then the operational risk can be defined as the risk of direct or indirect losses caused by errors or imperfections of processes, systems in the organization, personnel mistakes or insufficient skills or by unfavorable external events of non-financial nature, such as frauds or natural disasters.

Operational risks have their unique features and specifics of dealing with them in development of models. The features of operational risks in this context can be presented as follows.

1. Operational risks are internal by their nature, so they are different in each company. They also depend on technologies, processes, organization, personnel and company culture, in contrast with the market, credit and insurance risks that are the result mostly from external factors.

Evaluation of the operational risk requires to collect data that is specific for the company. It should be noted that most companies do not have long histories or relevant data. In the banking sector industry data is often used but it may turn out that the data is not quite applicable.

2. Operational risks change dynamically and continuously, driven by strategy, business processes, technologies in place and competitive environment. Even the internal historical data of any company may not provide precise indicators of the current and future risks.

3. The most cost-efficient risk mitigation strategies include changes in business processes, technology, organization and personnel. It is necessary to work out the approach to simulation that would allow measuring the impact on operational decision. For instance, "how operating risks would change if the company starts selling its products through the Internet?"

As it has been noted above the operational risks are the most difficult ones for quantitative analysis since relevant statistical data has been quite poor. Western telecommunication service providers are capable of full implementation of quantitative risk management only due to systematic collection of databases on operational losses and opportunities for accessing such databases maintained by other firms working in the same industry.

Russian companies only begin creating such databases, at best. It should be noted though that a great deal of information on threats and dangers to information and telecommunication business is kept by the top management who are experts in these companies and one should figure out how to painlessly extract that data from there for the benefit of the task on hand.

Operational risks can be simulated using Bayesian neural networks that use causal network developed on the bases of conditional probabilities.

A Bayesian network is the statistical method for description of patterns in data. Based on initial information that databases contain, a model is built as a network where the set of vertices describes events while the edges are interpreted as causal links between the events.

Bayesian probabilistic methods employed in machine learning are significant steps forward in comparison with popular "black box" models. These networks provide clear explanations of their conclusions, they allow logical interpretation and modification of the problem variables of structural relations and open ways for explicit inclusion of prior experience of experts.

Due to smart representation in the form of graphs Bayesian networks are very useful in applications.

Bayesian networks are based on fundamental points and results of the probability theory that have been under development for a few centuries, which is the cornerstone of their practical success.

Reduction of joint distribution of probabilities in the form of product of conditional probabilities that depend on a small number of variables allow avoiding "combinatorial explosions" in modeling.

Bayesian networks are based on the Bayes probability theory for determination of posterior probabilities of

pairs of mutually exclusive events Y_i through their prior probabilities.

$$P(Y_i \mid X) = \frac{P(Y_i)P(X \mid Y_i)}{P(X)} \quad .$$

Cause-and-effect models help to explain the origins of losses and evaluate losses that take place in the course of business processes. The primary advantages of Bayesian networks in financial analysis are the capability to take into account both qualitative and quantitative market indicators, dynamic input of new data and explicit dependencies between important factors that affect financial results.

Detailed analysis of possibilities for modeling Bayesian networks as a tool for evaluation of operational risks can be efficient for obtaining not only qualitative but also quantitative results of assessment of the risk component of telecommunication business.

Development and implementation of risk management systems has become standard procedure and not only for global leaders in telecommunication who have been using risk management systems, such as British Telecom, France Telecom, Deutsche Telekom, Telecom Italia, AT&T, NTT, Vodafone, Sprint, but also for a number of domestic telecommunication companies.

However, looking at these solutions it can be noted that their functionality is aimed either at automation of the Sarbanes-Oxley Act requirements (which is important for our operators, especially those who participate in securities markets) or at assessment of specific risks (mostly in the financial sector).

Executives on Russian companies, such as System Telecom, VympelCom, MegaFon, Comstar-ORS and some others already see both tangible and intangible benefits from implementation of risk management:

- stronger market position;
- company image improvement;
- better customer loyalty;
- operator income growth;
- OPEX reduction;
- improvement of liquidity and credit capacity.

Some companies of Svyasinvest holding already started implementing certain elements of their risk management system.

For example, Telecom companies operating in Siberia and the Southern region perform identification, evaluation and ranking of operational risks and have plans to run measures for risk mitigation and to arrange control over this process. Pilot projects commenced in two interregional companies of Rostelecom have been predominantly oriented at operational risks management in the enterprises.

When creating the risk management system the companies conducted diagnostics that covered 14 functional areas of business activities and described their business processes (about 400 in each of the two companies). Then a three-ties risk management system was shaped out. Out of 1.500 risks diagnosed in the course of the project 200 were recognized as significant [3–6].

First procedures and regulations for risk management have been developed and risk management teams have been formed; the risk losses (related to the parameters under evaluation) have been cut by 30% in average, while the corporate management rating jumped up to two points. Furthermore, Rostelecom implemented the financial reporting risk management system based on the requirements imposed by the Sarbanes-Oxley Act.

A specialized department has been created in MTS. It is responsible for large-scale income management system and this system is designed to achieve maximum profitability of the business with detailed consideration of growth priorities, minimization and prevention of financial losses from errors in the areas of technology and business processes, reduction of losses caused by fraudulent offences of subscribers and partners.

Pochta Rossii (Russian Postal Service) has complex multi-tier structure that includes 40.000 offices in all parts of the country. Its risk and insurance management department describes operational activities, gives their evaluation, controls insurance, monitors events, provides analysis of assets operation, risks to counterparties and losses from frauds.

Conclusions and outlook of the development in this area. The results of the study suggest the following. Specifics of information and telecommunication sector are focused on risk management, the risk profile and opportunities to manage risks in systematic mode. It has been determined when and how qualitative and quantitative risk management is possible, what methods and measures of risk are, what prospective opportunities for simulation of risk situations are available. The review of risk management practice in telecommunications both in Russia and abroad reveals trend toward integration of risk management functions and automation of these functions in order to build single monitoring simulation and metering complex with the core consisting of Bayesian technologies that support decision-making. This computational architecture will provide preventive risk management in telecommunication companies.

References / Список літератури

1. Kanev, V.S. (2008), Risk Management in Telecommunications. // Russian Scientific-Technical Conference *Informatics and Telecommunication Problems*. Novosibirsk, pp. 16–17.

Канев В.С. Управление рисками в телекоммуникациях: российская научно-техническая конференция „Информатика и проблемы телекоммуникаций“ / В.С. Канев – Новосибирск, 2008. – С. 16–17.

2. Corporate Management. Available at: www.avacco.ru/ page.asp?code=korporativnoe_upravlenie

Корпоративное управление [Электронный ресурс] – Режим доступа: www.avacco.ru/ page.asp?code= korporativnoe_upravlenie

3. Round table: Learning to Control Risks. Available at: www.connect.ru/article.asp?id=5706 (Accessed on: 02/25/2009.)

Круглый стол: Учимся управлять рисками [Электронный ресурс] – Режим доступа: www.connect.ru/ article.asp?id=5706

4. Kuzovkova, T.A. and Kuzovkov, D.V. (2008), "Analysis of Development of the Russian Information and Telecommunications Market", *Electrosvyaz*, no. 2, pp. 8–11.

Кузовкова Т.А. Анализ развития российского рынка инфокоммуникаций / Т.А. Кузовкова, Д.В. Кузовков // Электросвязь. – 2008. – №2. – С. 8–11.

5. Kanev, V.S. (2006), "Risks in the Telecommunication Services Market", *IX International Conference Data Networks Operation Problems* (PFIS-2006), Novosibirsk, pp. 120–123.

Канев В.С. Риски рынка телекоммуникационных услуг: IX международная конференция „Проблемы функционирования информационных сетей" / В.С. Канев – Новосибирск, 2006. – С. 120–123.

6. Chachin, P. (2007), "Telecommunication Companies Learn Risk Management", *PCWeek/RE*, no.3, pp. 17.

Чачин П. Предприятия связи осваивают риск-менеджмент / Чачин П. // PC Week/RE – 2007. – № 3. – 17 с.

7. Likhvantsev, N., Genne, O. and Maznyak, A. (2005), "FMS SYSTEMS: A Road Block Against Fraudsters", *Svyazinvest*, no.1, pp. 25.

Лихванцев Н. FMS СИСТЕМЫ: Барьер на пути мошенников / Лихванцев Н., Генне О., Мазняк А. // Связьинвест. – 2005. – № 1. – 25 с.

8. Malkov, P. Hack Me if You Can. Available at: http://news.ngs.ru/more/42413/ (Accessed on: 02/25/2009).

Малков П. Взломай меня, если сможешь [Электронный ресурс] / Малков П. – Режим доступа: http://news.ngs.ru/more/ 42413.

Мета. Дослідити питання системного управління ризиками в телекомунікаціях Сибіру РФ: особливості галузі, її ризиковий профіль і можливості управління ризиками.

Методика. Якісний та кількісний ризик-менеджмент, діагностика ризик-факторів і моделювання операційних втрат, байєсовські мережі.

Результати. Висвітлені особливості галузі зв'язку та інфокомунікацій на предмет управління ризиками, їх ризиковий профіль та оцінені можливості управління ризиками на систематичній основі. Визначено, коли і як можливий якісний і кількісний ризик-менеджмент, які методи управління та виміри ризику, перспективні можливості моделювання ризикових ситуацій. Проаналізована російська та зарубіжна практика управління ризиками в телекомунікаціях, що показує тренд на інтеграцію функцій управління ризиками та автоматизацію цих функцій в єдиному моніторинговому модельному вимірювальному комплексі з ядром у центрі – байєсівських технологій підтримки прийняття рішень. Розкриті особливості ризикового профілю галузі телекомунікацій, особливості управління ризиками на основі якісного та кількісного ризик-менеджменту. Визначено перспективи використання байєсівських технологій при перманентному управлінні ризиками. Проаналізований доступний досвід компаній „Телеком" у справі управління ризиками.

Наукова новизна. Адекватний опис ефективних процедур комплексного управління ризиками в секторі, що швидко розвивається, значно впливає на темпи розвитку всього господарського комплексу.

Практична значимість. Методи та елементи методології управління ризиками складають основу розробки автоматизованих інтегрованих систем управління ризиками в телекомунікаційному секторі. Така обчислювальна архітектура дозволить ефективно організовувати превентивний ризик-менеджмент у компаніях „Телеком".

Ключові слова: *ризик, карта ризику, ризиковий профіль, моделювання, діагностика, байєсовські мережі*

Цель. Исследовать вопросы системного управления рисками в телекоммуникациях Сибири РФ: особенности отрасли, её рисковый профиль и возможности управления рисками.

Методика. Качественный и количественный риск-менеджмент, диагностика риск-факторов и моделирование операционных потерь, байесовские сети.

Результаты. Высвечены особенности отрасли связи и инфокоммуникаций на предмет управления рисками, их рисковый профиль и оценены возможности управления рисками на систематической основе. Определено, когда и как возможен качественный и количественный риск-менеджмент, каковы методы управления и измерители риска, перспективные возможности моделирования рисковых ситуаций. Проанализирована российская и зарубежная практика управления рисками в телекоммуникациях, которая показывает тренд на интеграцию функций управления рисками и автоматизацию этих функций в едином мониторинговом модельном измерительном комплексе с ядром в центре – байесовских технологий поддержки принятия решений. Вскрыты особенности рискового профиля отрасли телекоммуникаций, особенности управления рисками на основе качественного и количественного риск-менеджмента. Определены перспективы использования байесовских технологий при перманентом управлении рисками. Проанализирован доступный опыт компаний „Телеком" в деле управления рисками.

Научная новизна. Адекватное описание эффективных процедур комплексного управления рисками в бурно развивающемся секторе, значительно влияющем на темпы развития всего хозяйственного комплекса

Практическая значимость. Методы и элементы методологии управления рисками составят основу разработки автоматизированных интегрированных систем управления рисками в телеком-муникационном секторе. Такая вычислительная архитектура позволит эффективно организовывать превентивный риск-менеджмент в компаниях „Телеком".

Ключевые слова: *риск, карта риска, рисковый профиль, моделирование, диагностика, байесовские сети*

Рекомендовано до публікації докт. техн. наук Є.В. Кочурою. Дата надходження рукопису 15.06.14.