UDC 004.422

D.O. Lysytsia, S.S. Bulba

National Technical University "Kharkiv Polytechnic Institute", Kharkiv

CLASSIFICATION OF METHODS ASSESSMENT AND MANAGEMENT RISK DEVELOPMENT SOFTWARE

The paper deals with methods for assessing the risks of software development (Software). Revealed their strengths and weaknesses. The ways to improve the methods of qualitative risk assessment. The classification management of software development that will minimize the level of vulnerability in the software, in consequence of which enhance the quality of the product. Identified strengths and weaknesses of existing methods of risk management software development. The ways of further development of security software development.

Keywords: *risk assessment, methods for the safe design, method of "security team", method of "clean rooms", method of structural correctness, method «decision tree», scenario method.*

Introduction and problem statement

In the modern sphere of software development we can see trends for: improvement in methodology of development software, setting up clear goals, restrictions, pluses and minuses. The most perspective in this direction are flexible methodologies of software development in which we can point out next stages and processes:

- analysis, requirements formation, drawing up specifications and designing process;
- implementation process;
- testing, commissioning and support of already developed software.

Considering overall structure of flexible methodologies, we can see the relevance of risk assessment. This is especially important now with the raise occurrence of cyber-attacks and search for vulnerabilities in software.

Unfortunately, it is hard to take in account all of this factors, because of a number of subjective and objective reasons. Partially this happens due to lack of structured knowledge in this area.

The purpose of this article is analysis of the current methods of risk assessment in development of software, which will allow minimizing amount of vulnerabilities in software by taking into account a lot of social and economical factors in the process of risk assessment in life cycle of software.

Literature analysis [1 – 10] howed that there is several studies which describe qualitative and quantitative methods of risk assessment. These methods include:

- «Interview»;
- «Method of interest rate»;
- «Sensitivity analysis»;
- «Solutions analysis»;
- «Script method»;
- «The method of decision tree »;
- «Simulation»;
- «Assessment of risk trends»;
- «Estimation of the potential risks and risk impact».

In [1, 3 – 6] considered the question of risk control and their size. In [5, 7 – 9] main attention is brought to the question of existing methods of risk assessment and their description

However, due to neglect consideration of informational security factors, presented methods can't fully estimate risks of software development. We will review possible solutions and risk management methods of software development, while also taking in consideration factor of cyber-vulnerabilities. By doing all of this we will create classification of assessment methods and risk management.

Research methods for assessing risk

Quantitative Methods**.** Quantitative risk assessment (fig. 1) determines the likelihood of risk and it impact on project.

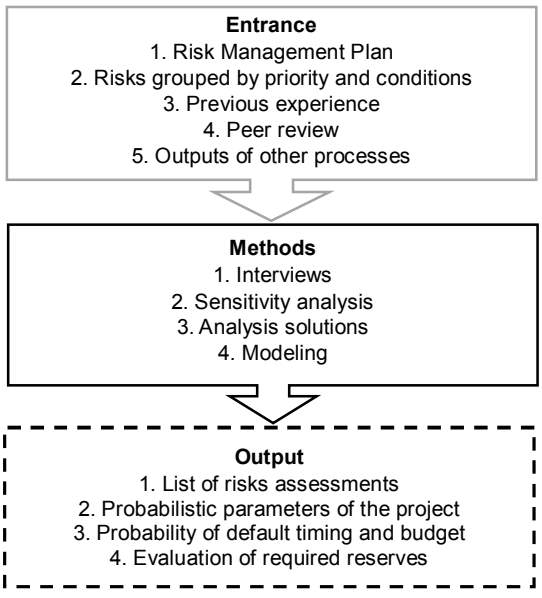

Fig. 1. Methods of quantitative risk assessment

This helps project management group in making correct decisions and avoid uncertainties. Quantitative risk assessment usually accompanied by qualitative assessment and also requires risk identification. Quantitative and qualitative risk assessment can be used separately or together depending on amount of time, budget and their necessity.

Qualitative methods is a process of risk identification analysis (fig. 2) and finding risks that require immediate solving. Such risk assessment method determines importance of each hazard and picks way to respond. Accessibility of supporting information makes it easier to put priorities for different categories of risks. This assessment estimates reasons behind hazards and determines their impact on the project with standart methods and tools. Usage of this tools helps to partially avoid uncertainty, which are often found in projects. During the lifetime of the project, there must be constant re-evaluation of risks.

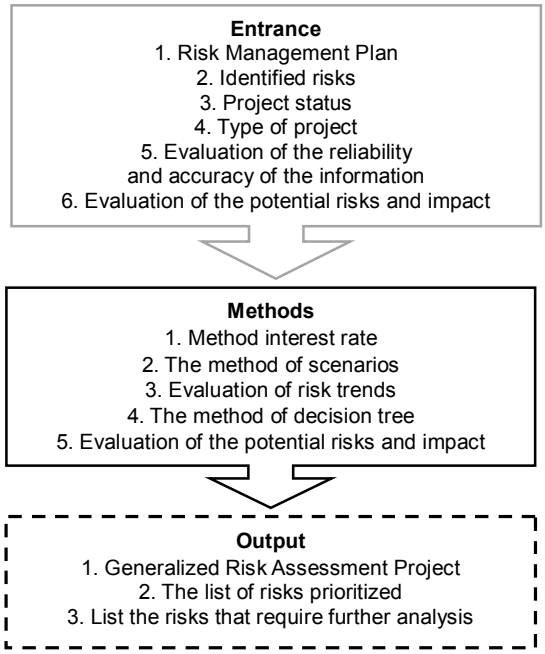

Fig. 2. Methods of qualitative risk assessment

By using the method of decision trees we can resolve classification and prognostication tasks in three possible options: optimistic, pessimistic and normal. Decision tree represents network diagrams, which show time when event happened and probability of getting necessary result. Each branch of the tree represents different ways of how things will happen. More variations in the projected criteria's means more risks for project. Script method allows to move from detailed description of strategic and operational risk, which are same for all kinds of corporative activities, to processing of two likely to happen scenarios: pessimistic (worst-case) and optimistic (best-case). At the final stage of strategic planning such risk assessment needs to implemented in performance of planned tasks: intense- the optimistic scenario, most real and lowered. Beside that, during development of software, risk of strategic risks of the enterprise as whole and certain activities of operational risk such as management software, production and marketing are also taken into the account.

Among these methods, represented on (pic. 2) were pointed out «decision tree method» and «script method». In [11, 12] noted that this method provide better software development experience because of their high accuracy and quick process of learning and through evaluation of possible scenarios they allow to take single right decision. By lining scenarios and analyzing them we can see a rational strategy of influencing the situation for making right decision.

Classification of assessment methods and risk management of software development

Now days a lot of users face vulnerabilities when using software. In order to reduce the number of vulnerabilities, there are many methods of risk assessment. Among the methods used in the management of software development, are:

- method "security team";
- method "sterile room";
- method of structural correctness;
- CMMI process improvement model.

"Security team" method is to allocate the structure of the organization or department, called security team, which is responsible for development and improvement of informational security, also acts as an expert on information security for the entire organization as a whole and for each project in particular.

Security Division appoint compliance officer or group of employees for the role of the Security Engineer for specific development.

Security Engineer helps development team by analyzing all of their actions, documents, created during development process, such as list of safety requirements and project documentation and gives recommendations based on produced analysis.

This way Security Engineer is responsible for development methodology and for the safety of the product as a whole.

As for this method it should be noted that using such approach doesn't guarantee safety of developed software. However using such approach can lower overall amount of vulnerabilities in developed software.

The main social and economic factors, which are taken into account in this method, are:

- cultural issues and problems of environment;
- not detecting vulnerabilities in software security;
- unforeseen technical issue.

Software development using "sterile room" method is theoretically grounded, focused on team development process, verification and certification of correct soft-

ware systems with statistical quality control. "Sterile room" method covers whole life-cycle of the development including project management, definition of functions and architecture specifications, functional validation, as well as statistical testing for the program certification. Main idea of this method is preventing errors and defects in the software, rather than their elimination. Main principals of the metod are:

- incremental development based on statistical quality control;
- using the principle of structured design concepts;
- testing based on statistical methods;
- iterative development;
- reallocation of time between the stages of life cycle;
- software development should be based on formal methods.

The advantages of the "sterile room" method include – wide capabilities for verification of software systems through the use of formal specifications, method involves a detailed formal description of all possible execution scenarios of developed programs, which greatly reduces the likelihood of incorrect program operation and reduces the likelihood of errors in specifications and requirements for the software.

Method allows detection and elimination of errors and vulnerabilities on early stages of development, starting from the stage of forming specifications and thus prevents such critical errors at the stage of design and implementation. Among the shortcomings should be noted that the method focuses on the correct development of the individual components of the system, but at the same time does not provide sufficiently effective tools for analysis and verification of system as a whole.

The method of "sterile room" does not provide the means to analyze system behavior in dynamics, requires a complicated auxiliary tools for automated verification of various representation systems and their compliance and compliance specifications, design documents and code.

The main social and economic factors that are taken into account in this method are:

- inadequate choice of strategy for software development;
- instability of suppliers;
- not detecting software vulnerability;
- inefficient interaction between stakeholders.

The method of structural correctness includes definitions of formal notations for system specifications and architecture components based on their consistency and correctness. It allows, by using formal methods, to check software for defects and promptly remove them during its life cycle.

This method includes definitions of formal notations for system specifications and architecture components based on their consistency and correctness.

For safe systems allocate categories of system states and operations, which are determined on the basis of their impact on the overall safety The end goal is to create an architecture that minimizes the number of functions critical for the protection and to isolate them. This helps to further reduce the cost and amount of work involved with correctness validation of all elements.

The main social and economic factors that are taken into account in this method are:

- inadequate choice of strategy for software development;
- ineffective project management;
- discrepancy of organizational structure.

CMMI process improvement model used to assess the overall effectiveness of the organization, according to the criteria specified in the model and find ways to improve it. CMMI model includes the main directions of development processes in the organization, sets of practices and methods of development, adaptation and optimization of which are specific to a particular organization is pretty effective tool to improve the entire development process. The main social and economic factors that are taken into account in this method are:

- changes in the law;
- inadequate financial management;
- discrepancy of organizational structure.

As seen from the results of the above analysis, the main drawbacks of these methods of assessment and risk management are lack of vulnerability detection in software security. This can lead to significant problems during software operation. The decision of this contradiction is the analysis of software vulnerabilities and conducting PEN-testing.

Conclusions

In general, it can be noted that the proper and correct application of assessment methods and risk management during software development can significantly improve the quality and safety of the product, developed at relatively moderate costs. Thus, given the effectiveness of different methods and differences in their use it seems that the most effective way of using them is together, for safe development at different stages

List of references

1. Fenton N. Decision Support Software for Probabilistic Risk Assessment Using Bayesian Networks / N. Fenton, M. Neil // IEEE Software. – 2014. – № 31 (2). – P. 21-26.

2. Fenton N. Risk Assessment and Decision Analysis with Bayesian Networks / N. Fenton, M. Neil // CRC Press. – 2012. – P. 33-38.

3. Soumya Krishnan M. Software Development Risk Aspects and Success Frequency on Spiral and Agile Model / M. Soumya Krishnan // Int. Journal of Innovative Research in Computer and Comm. Eng. – 2015. - Vol. 3. – P. 122-129.

4. Hijazi H. A Review of Risk Management in Different Software Development Methodologies / H. Hijazi // Int. Journal of Comp. Appl. – 2012. – Vol. 45, № 7. – P. 1311-1318.

5. Abdullahi M. A Study on SME Software Development Background and Risk Assessment Implementation in Malaysia / M. Abdullahi, Sh. Basri, H. Osman Ali // World Applied Sciences Journal. – 2013. – Vol. 26. - № 12. – P. 55-61.

6. Abdullahi M. Strength and Weakness of Software Risk Assessment Tools / M. Abdullahi, Sh. Basri, H. Osman Ali // International Journal of Software Engineering and Its Applications. – 2014. – Vol. 8. – № 3. - P. 389-398.

7. Woody C. Supply-Chain Risk Management: Incorporating Security into Software Development / C. Woody, R. Ellison // Software Engineering Institute Carnegie Mellon University. – 2010. – P. 166-178.

8. Britkin A.I. Model estimate the duration of the iterative software development process / A.I. Britkin // Open education, 2009. – №4. – P. 75.

9. Seacord R. Secure Coding in C and C++ / R. Seacord // 2nd Edition by Addison-Wesley Professional. Part of the SEI Series in Software Engineering series Published. – 2013.

10. William R. Project Management Body of Knowledge/ R. William. – PMI Standard Committee. – 2006. – 182 p.

11. Sommerville I. Software Engineering / I. Sommerville. – Addison-Wesley Publ. Company. – 2011. – 866 p.

12. Hijazi H. A Review of Risk Management in Different Software Development Methodologies / H. Hijazi // Int. Journal of Computer Appl. – 2013. – Vol. 48, № 3. – P.1441-1453.

Надійшла до редколегії 5.01.2016

Рецензент: д-р техн. наук с.н.с. С.Г. Семенов, Національний технічний університет «ХПІ», Харків.

КЛАСИФІКАЦІЯ МЕТОДІВ ОЦІНКИ ТА УПРАВЛІННЯ РИЗИКАМИ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Д.О. Лисиця, С.С. Бульба

У роботі розглядаються методи оцінки ризиків розробки програмного забезпечення. Виявлено їх переваги і недоліки. Визначено шляхи удосконалення методів якісної оцінки ризиків. Представлена класифікація методів управління розробки програмного забезпечення, які дозволять максимально знизити рівень уразливостей в програмному забезпеченні, в слідстві чого підвищують якість програмного продукту. Визначено переваги і недоліки існуючих методів управління ризиками розробки програмного забезпечення. Виявлено шляхи подальшого розвитку безпеки розробки програмного забезпечення.

Ключові слова: *оцінка ризиків, методи безпечної розробки, метод «команди безпеки», метод «стерильної кімнати», метод структурної коректності, метод «дерево рішень», метод сценаріїв.*

КЛАССИФИКАЦИЯ МЕТОДОВ ОЦЕНКИ И УПРАВЛЕНИЯ РИСКАМИ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Д.А. Лисица, С.С. Бульба

В работе рассматриваются методы оценки рисков разработки программного обеспечения. Выявлены их достоинства и недостатки. Определены пути усовершенствования методов качественной оценки рисков. Представлена классификация методов управления разработки программного обеспечения, которые позволят максимально снизить уровень уязвимостей в программном обеспечении, в следствии чего повышают качество программного продукта. Определены достоинства и недостатки существующих методов управления рисками разработки программного обеспечения. Выявлены пути дальнейшего развития безопасности разработки программного обеспечения.

Ключевые слова: *оценка рисков, методы безопасной разработки, метод «команды безопасности», метод «стерильной комнаты», метод структурной корректности, метод «дерево решений», метод сценариев.*