საინფორმაციო სისტემებში რისკების შეფასების მეთოდები და პროგრამული საშუალებები

ოთარ შონია, ნინო თოფურია
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია საინფორმაციო უსაფრთხოებასთან დაკავშირებული რისკების ანალიზის მეთოდიკები: CRAMM, FRAP, OCTAVE, RISK WATCH, Microsoft-ის მეთოდიკა. კონკრეტულ მაგალითზეა განხილული რისკების შეფასების პროგრამული უზრუნველყოფა – Microsoft Security Assessment Tool (MSAT) და კომპანიის ინფორმაციული უსაფრთხოების პოლიტიკის მართვის პროგრამული კომპლექსი "КОНДОР+".

საკვანძო სიტყვები: საინფორმაციო სისტემები. ინფორმაციული უსაფრთხოება. რისკების ანალიზის მეთოდები. რისკების შეფასების პროგრამული პროდუქტები.

1. შესავალი

რისკი ინფორმაციული უსაფრთხოების სფეროში არის ზარალის პოტენციური შესაძლებლობა, რომელიც საინფორმაცი სისტემებში უსაფრთხოების დარღვევის გამო წარმოიქმნება. ნებისმიერი პროექტისათვის, რომლის რეალიზაციისათვის საჭიროა ფინანსური დანახარჯები, სასურველია საწყის ეტაპზე განისაზღვროს, თუ როგორ იქნება შეფასებული პროექტის შედეგები. ეს საკითხი კიდევ უფრო აქტუალურია საინფორმაციული სისტემებში ინფორმაციის უსაფრთხოების დაცვის თვალსაზრისით.

პრაქტიკაში გავრცელებულია ორი მიდგომა უსაფრთხოების დაცვის ქვესისტემის პროექტის დასამტკიცებლად. პირველი დაფუძნებულია იმის შემოწმებაზე, თუ რამდენად შეესაბამება ინფორმაციული სისტემების დაცვის დონე ინფორმაციული უსაფრთხოების სფერში დაწესებულ სტანდარტების (ISO17799) მოთხოვნებს. მეორე მიდგომა ითვალისწინებს ინფორმაციული უსაფრთხოების უზრუნველყოფასთან დაკავშირებული რისკების შეფასებასა და მართვას. სტატიაში განხილულია საინფორმაციო უსაფრთხოებასთან დაკავშირებული რისკების ანალიზის მეთოდიკები: CRAMM, FRAP, OCTAVE, RISK WATCH, Microsoft-ის მეთოდიკა. კონკრეტულ მაგალითზე განხილულია რისკების შეფასების პროგრამული უზრუნველყოფა – Microsoft Security Assessment Tool (MSAT) და კომპანიის ინფორმაციული უსაფრთხოების პოლიტიკის მართვის პროგრამული კომპლექსი "КОНДОР+".

2. ძირითადი ნაწილი

ყველაზე მეტად გავრცელებული რისკების ანალიზისა და მართვის მეთოდიკები, რომლებიც დაკავშირებულია საინფორმაციო უსაფრთხოებასთან, იყოფა სამ ჯგუფად:

1. მეთოდიკები, რომლებიც იყენებენ რისკების შეფასებას ხარისხობრივ დონეზე (მაგალითად, სკალაზე „მაღალი", „საშუალო", „დაბალი"). ასეთს მიეკუთვნება, კერძოდ, FRAP მეთოდიკა (Facilitated Risk Analysis Process), შექმნილი Peltier and Associates კომპანიის მიერ. მეთოდიკის სრული აღწერა მოცემულია ინტერნეტში [7]. იგი საშუალებას აძლევს კომპანიებს იპოვონ ბალანსი დაცვის საშუალებებზე გაწეულ ხარჯებსა და მიღებულ ეფექტს შორის. რისკების მართვა იწყება ამ რისკების შეფასებით, შემდეგ ხდება ანალიზი დახარჯვა/მიღების ანალიზი (cost/benefit analysis), რომელიც საშუალებას იძლევა განისაზღვროს დაცვის ის საშუალებები, რომელიც საჭიროა რისკების შესამცირებლად მისაღებ დონემდე;

2. რაოდენობრივი მეთოდიკა (რისკი ფასდება, როგორც რიცხვითი მნიშვნელობა, მაგალითად მოსალოდნელი წლიური დანაკარგები). ამ კლასს მიეკუთვნება RiskWatch კომპანიის მეთოდიკა. ესაა რისკების ანალიზის საკუთარი მეთოდიკა, რომლის სრული აღწერა მოცემულია ინტერნეტში [9]. RiskWatch-ის ოჯახში შედის შემდეგი პროგრამული პროდუქტები: RiskWatch for Physical Security – ინფორმაციული სისტემების ანალიზისა და დაცვისათვის; RiskWatch for Information Systems – ინფორმაციული რისკებისათვის; HIPAA-WATCH for Healthcare Industry – HIPAA (US Healthcare Insurance Portability and Accountability Act) სტანდარტის მოთხოვნებთან შესაბამისობის შესაფასებლად (აქტუალურია მედიცინის მუშაკებისათვის); RiskWatch RW17799 for ISO 17799 – საერთაშორისო ISO 17799.სტანდარტის მოთხოვნებთან შესაბამისობის შესაფასებლად. RiskWatch-ის მეთოდიკა რისკების შეფასებისა და მართვის კრიტერიუმად იყენებს მოსალოდნელ წლიურ დანახარჯებს (Annual Loss Expectancy, ALE) და ინვესტიციის დაბრუნების შეფასებას (Return on Investment, ROI).

3. მეთოდიკები, რომლებიც იყენებენ შერეულ შეფასებებს. ამ მიდგომას გამოიყენებს CRAMM, Microsoft და ა.შ. CRAMM მეთოდიკა ერთ-ერთი პირველი რისკების ანალიზის მეთოდიკაა. იგი 80-იან წლებში შემუშავდა დიდი ბრიტანეთის ტელეკომუნიკაციებისა და კომპიუტერების ცენტრალური სააგენტოს მიერ. ამ მეთოდიკას ახასიათებს რისკების შეფასესების კომპლექსური მიდგომა, რომელიც მოიცავს რაოდენობრივ და ხარისხობრივ ანალიზის მეთოდიკებს. მეთოდიკა უნივერსალურია და გამოიყენება, როგორც დიდ, ისე პატარა სამთავრობო და კომერციულ ორგანიზაციებში. კომერციული ორგანიზაციებისათვის არსებობს კომერციული ცოდნის ბაზები (Commercial Profile), სამთავრობო ორგანიზაციებისათვის – სამთავრობო პროფილი (Government profile) [2];

4. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – მეთოდიკა შემუშავებულია Software Engineering Institute (SEI) ინსტიტუტის მიერ. მისი სრული აღწერა მოცემულია ინტერნეტში [8]. იგი განსაკუთრებულია იმით, რომ ანალიზის მთელ პროცესს აწარმოებენ ორგანიზაციის თანამშრომლები, გარეშე კონსულტანტების მოწვევის გარეშე. ამისათვის კომპლექტდება შერეული ჯგუფი, შემდგარი ტექნიკური სპეციალისტებისა და სხვადასხვა დონის ხელმძღვანელებისაგან. ასეთი მიდგომა საშუალებას იძლევა ყოველმხრივ შეფასდეს ბიზნესისათვის შესაძლო ინციდენტების რეზულტატები და შემუშავდეს კონტრზომები;

5. Microsoft-ის მეთოდიკის მიხედვით უსაფრთხოების რისკების მართვის პროცესი იყოფა სამ ეტაპად: - დაგეგმვა: საფუძველის მომზადება რისკების წარმატებულად შესაფასებლად; - მონაცემების კოორდინირებული შეგროვება; - რისკების პრიორიტეტის განსაზღვრა.

შემდეგ განისაზღვრება სამი ხარისხობრივი სახის აქტივი:

1. მაღალი გავლენა ბიზნესზე – მნიშვნელოვანი გავლენა კონფიდენციალობაზე. თუ ეს აქტივები გახდა ხელმისაწვდომი ორგანიზაციას შესაძლოა მიადგეს მნიშვნელოვანი ზიანი. მაგალითად, კონფიდენციალური საქმიანი მონაცემები;

2. საშუალო გავლენა ბიზნესზე – საშუალო ზიანი, როდესაც არ ხდება კატასტროფული ცვლილებები, მაგრამ ირღვევა ორგანიზაციის ნორმალური მუშაობის წესი. მაგალითად, კომერციული მონაცემები, თანამშრომლების გვარები, მონაცემები საწარმოს შეკვეთების შესახებ;

3. დაბალი გავლენა ბიზნესზე – ასეთ აქტივებს არ ჭირდება დამატებითი კონტროლი. მაგალითად, მონაცემები ორგანიზაციის სტრუქტურის შესახებ.

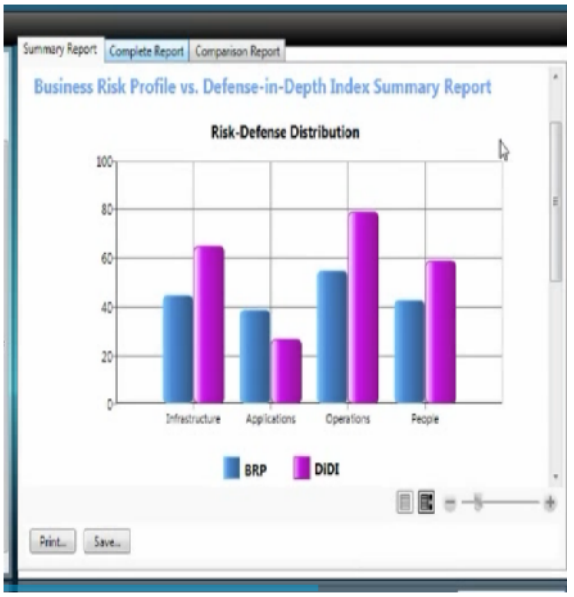
შემდეგ ხდება საფრთხეების ჩამოთვლა და შეფასება სპეციალურ სკალაზე. ბოლოს გამოითვლება მოსალოდნელი ერთჯერადი ზიანის (SLE) რაოდენობრივი შეფასება და მისი წარმოქმნის სიხშირე (ARO), ხოლო მოსალოდნელი წლიური ზიანი (ALE) გამოითვლება ფორმულით:

$$ALE = SLE \times ARO$$

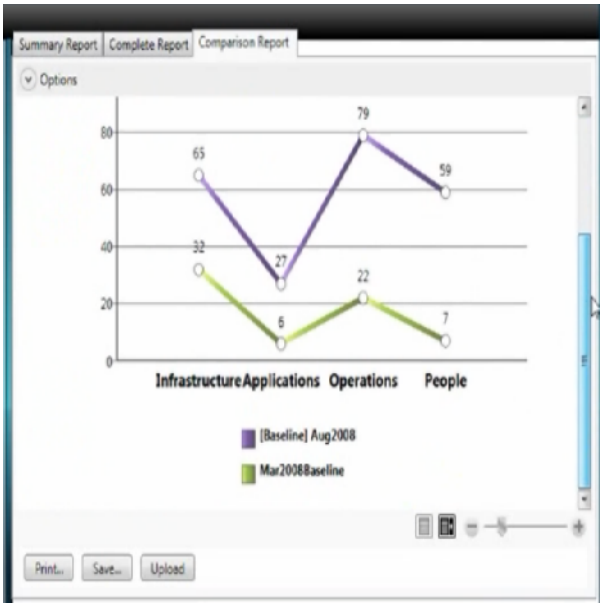
კერძო ფირმის მაგალითზე განვიხილოთ პროგრამა – Microsoft Security Assessment Tool (MSAT). იგი შეიმუშავა ფირმა მაიკროსოფთმა და საშალებას აძლევს კომპანიებს დამოუკიდებლად შეაფასონ უსაფრთხოების რისკები. პროგრამა უფასოდ შეიძლება ჩამოტვირთოთ http://technet.microsoft.com/en-us/security/cc185712 საიტიდან.

MSAT განკუთვნილია ისეთი კომპანიებისათვის, რომელთა თანამშრომლების რაოდენობა არ აღემატება ათასს. მუშაობის პროცესში მომხმარებელი, რომელიც გამოდის ანალიტიკოსის როლში, პასუხობს 200-ზე მეტ შეკითხვაზე. ეს შეკითხვები გამომდინარეობს პრაქტიკული რეკომენდაციებიდან და საერთაშორისო ISO 17799 და NIST-800.x სტანდარტებიდან.

MSAT შეკითხვები იყოფა ორ ჯგუფად: პირველი მიმართულია კომპანიის ბიზნეს-მოდელის შესაქმნელად და ვღებულობთ ე.წ. ბიზნესის რისკის პროფილს (BRP). შეკითხვების მეორე ჯგუფი განკუთვნილია უსაფრთხოების ზომების სიის შესადგენად. ეს უსაფრთხოების ზომები ერთად აღებული ქმნიან დაცვის დონეს ე.წ. ღრმა დაცვის ინდექსს (DiDI). შემდეგ ხდება BRP-ისა და DiDI-ს შედარება, რათა მოხდეს საფრთხის შეფასება და ანალიზი სხვადასხვა არეებისათვის – ინფრასტრუქტურა, აპლიკაციები, ოპერაციები და თანამშრომლები.



ნახ.1. MSAT-ის ფანჯარა: BRP-ისა და DiDI-ს შედარება



ნახ.2. MSAT-ის ფანჯარა: შეფასების ანალიზი

3. დასკვნა

ამგვარად, ჩამოვთვალოთ ის უპირატესობები, რომელიც მოგვცა რისკების ანალიზის ჩატარებამ:

- უსაფრთხოების სფეროში არსებული პრობლემების გამოვლენა;
- რისკების ანალიზი საშუალებას აძლევს არატექნიკურ სპეციალისტებს შეაფასონ დაცვის საშუალებებისა და მექანიზმების დანერგვის შედეგად მიღებული სარგებელი;
- რისკების რანჟირება პრიორიტეტების მიხედვით საშუალებას იძლევა გამოვყოთ შედარებით პრიორიტეტული მიმართულებები, სადაც დაინერგება ინფორმაციული უსაფრთხოების დაცვის ახალი პროცედურები.

უნდა აღინიშნოს, რომ რისკების შეფასება ხარისხობრივ დონეზე არ იძლევა საშუალებას ერთმნიშვნელოვნად შევადაროთ ინფორმაციული უსაფრთხოების უზრუნველყოფაზე გაღებული დანახარჯები და მიღებული სარგებელი. ამ მხრივ უმჯობესია რაოდენობრივი მეთოდიკები, მაგრამ ამ შემთხვევაში საჭიროა თითოეული საფრთხის წარმოშობის ალბათობის შეფასება. ამას გარდა, ინტეგრალური მაჩვენებელი (ALE) სახიფათოა იმით, რომ ძალიან ძვირად ღირებული აქტივის შემთხვევაში შეიძლება კარდინალურად შეცვალოს რისკების ჯამური ღირებულების მნიშვნელობის შეფასება.

ლიტერატურა:

1. შონია ო., თოფურია ნ., მაისურაძე გ. ინფორმაციული უსაფრთხოების სისტემის აგება კორპორაცია Microsoft-ის ტექნოლოგიების გამოყენებით. სტუ, თბილისი 2009
2. Нестеров С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft. http://www.intuit.ru/department/itmngt/riskanms/lit.html
3. The logic behind CRAMM's assessment of measures of risk and determination of appropriate countermeasures
4. Peltier, Thomas R, Information security risk analysis, Auerbach 2001. ISBN 0-8493-0880-1
5. Alberts C., Dorofee A, OCTAVE threat profiles
6. Симонов С., “Современные технологии анализа рисков в информационных системах”, PCWEEK. 2001. №
7. http://www.peltierassociates.com/
8. www.cert.org/octave
9. http://www.riskwatch.com/

TECHNIQUES AND SOFTWARE PRODUCTS FOR AN ESTIMATION OF RISKS IN INFORMATION SYSTEMS

Shonia O, Topuria N

Georgian Technical University

Summary

Short descriptions of some widespread techniques of the analysis of risks and software products of an estimation of risks in information systems are resulted. Techniques of the analysis of risks in information security sphere are analyzed: CRAMM, FRAP, OCTAVE, Risk Watch and Microsoft. On a concrete example the software for an estimation of risks of information security - Microsoft Security Assessment Tool (MSAT) and a program complex of management by a policy of information security of the company «КОНДОР +» is considered.

МЕТОДЫ И ПРОГРАММНЫЕ ПРОДУКТЫ ДЛЯ ОЦЕНКИ РИСКОВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Шония О.,Топурия Н.

Грузинский Технический Университет

Резюме

Приводятся краткие описания ряда распространенных методик анализа рисков и программных продуктов оценки рисков в информационных системах. Анализируются методики анализа рисков в сфере информационной безопасности: CRAMM, FRAP, OCTAVE, Risk Watch и Microsoft. На конкретном примере рассматривается программное обеспечение для оценки рисков информационной безопасности - Microsoft Security Assessment Tool (MSAT) и программный комплекс управления политикой информационной безопасности компании «КОНДОР+».