ინფორმაციული სისტემის რისკების ანალიზისა და კონტროლის თანამედროვე მეთოდები და საშუალებები

დავით კაპანაძე, თალიკო ჟვანია
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

სტატიაში განხილულია ბიზნესის ინფორმაციულ უსაფრთხოებაში აუცილებელი დონის დაბანდებების შეფასება ამ სფეროში მაქსიმალური ეფექტიანობის ინვესტირების მისაღწევად. აღწერილია თანამედროვე რისკების ანალიზის სისტემები, რომლებიც საშუალებას იძლევა შეფასდეს არსებული რისკები და შეირჩეს ეფექტურობის მიხედვით ოპტიმალური დაცვის ვარიანტი.

საკვანძო სიტყვები: ბიზნესი. რისკები. ანალიზი. კონტროლი. ინფორმაციული უსაფრთხოება.

1. შესავალი

თანამედროვე ბიზნესის ინფორმაციული უსაფრთხოების უზრუნველსაყოფად ინვესტიციის ჩადების აუცილებლობა დღეისათვის ეჭვს არ იწვევს. ამ კუთხით ბიზნესის მთავარი ამოცანაა – როგორ შეფასდეს ინფორმაციულ უსაფრთხოებაში დაბანდებების საჭირო დონე, აღნიშნულ სფეროში ინვესტიციების მაქსიმალური ეფექტურობის მისაღწევად. ამ ამოცანის გადაწყვეტის საუკეთესო გზაა თანამედროვე რისკების ანალიზის სისტემის გამოყენება, რომელიც საშუალებას იძლევა შეფასდეს არსებული რისკები და შეირჩეს ეფექტურობის მიხედვით ოპტიმალური დაცვის ვარიანტი [1]. ოპტიმალობის კრიტერიუმად, როგორც წესი, გამოიყენება კომპანიის ინფორმაციულ სისტემაში არსებული რისკების შეფარდება ინფორმაციულ უსაფრთხოებაზე გაწეულ დანახარჯებზე.

2. ძირითადი ნაწილი

2003 წელს აშშ-ში FBI-ს მიერ ჩატარებული კვლევის შედეგად, სადაც გამოკითხული იქნა 530 მსხვილი და საშუალო ბიზნეს-კომპანია, ანგარიშში გამოქვეყნებული სტატისტიკის მიხედვით, კომპანიაში ინფორმაციული უსაფრთხოების უზრუნველყოფისათვის გასატარებელი ღონისძიებების ყველაზე დიდ დაბრკოლებად დასახელებულ იქნა ორი მიზეზი:

- ბიუჯეტის შეზღუდვები;
- ხელმძღვანელობის მხრიდან მხარდაჭერის არარსებობა.

ორივე მიზეზი გამოწვეულია ხელმძღვანელობის მხრიდან საკითხის სერიოზულობის გაუთვალისწინებლობით და ინფორმაციული ტექნოლოგიების (IT) მენეჯერის მხრიდან გადასწყვეტი ამოცანის სირთულით, დაასაბუთოს რატომ არის საჭირო (და რა რაოდენობით) ფულის ჩადება ინფორმაციულ უსაფრთხოებაში. ამ შემთხვევაში ძირითადი პრობლემა მდგომარეობს იმაში, რომ IT-მენეჯერები და კომპანიის ხელმძღვანელები ლაპარაკობენ სხვადასხვა - ტექნიკურ და ფინანსურ - ენებზე. ხშირად, IT-სპეციალისტებისთვის ძნელია შეაფასონ, რაში უნდა დაიხარჯოს ფული და რამდენია საჭირო კომპანიის ინფორმაციული სისტემის უკეთ დაცვის უზრუნველსაყოფად, რათა ეს დანახარჯები არ აღმოჩნდეს ფუჭი, ან უზომოდ დიდი.

როდესაც IT-მენეჯერს ცხადად აქვს ჩამოყალიბებული, რამდენს დაკარგავს კომპანია საფრთხის რეალიზების შემთხვევაში, რომელი ადგილებია სისტემაში სუსტი, რა ღონისძიებები უნდა გატარდეს დაცულობის დონის ასამაღლებლად, ამასთან ისე, რომ არ მოხდეს ზედმეტი თანხების ხარჯვა და ყველაფერ ამას დოკუმენტალურად ასაბუთებს, მაშინ ხელმძღვანელობის დარწმუნების ამოცანა, ყურადღება მიექცეს ინფორმაციული უსაფრთხოებისათვის თანხების გამოყოფას, ხდება გაცილებით უფრო რეალური.

ამ ამოცანის გადასაწყვეტად დამუშავებულია ინფორმაციული რისკების ანალიზისა და კონტროლის პროგრამული კომპლექსები: ბრიტანული CRAMM (კომპანია Insight Consulting, www.insight.co.uk), ამერიკული RiskWatch (კომპანია RiskWatch, www.riskwatch.com). განვიხილოთ გამოყენებული რისკების ანალიზისა და კონტროლის მეთოდები და მათ ბაზაზე აგებული პროგრამული სისტემები.

სისტემა CRAMM. მეთოდი CRAMM (the UK Government Risk Analysis and Management Method) [2] დამუშავებული იქნა დიდი ბრიტანეთის უსაფრთხოების სამსახურის (UK Security Service) მიერ, ბრიტანეთის მთავრობის დავალებით და ის სახელმწიფოს სტანდარტად იქნა აღიარებული. იგი გამოიყენება სახელმწიფო და კომერციული ორგანიზაციებში როგორც დიდ ბრიტანეთში, ისე მთელი მსოფლიოს მასშტაბით. დღეისათვის CRAMM წარმოადგენს საკმაოდ მძლავრ ინსტრუმენტს, რომელიც რისკების ანალიზის გარდა, საშუალებას იძლევა გადაიჭრას სხვა აუდიტორიული ამოცანებიც:

- **ინფორმაციული სისტემის გამოკვლევის ჩატარება და თანმხლები დოკუმენტაციის მომზადება ყველა ეტაპისათვის;**
- **აუდიტის ჩატარება BS 7799:1995 - Code of Practice for Information Security Management BS7799 სტანდარტის მიხედვით;**
- **უსაფრთხოების პოლიტიკისა და ბიზნესის უწყვეტობის უზრუნველყოფის გეგმის დამუშავება.**

CRAMM მეთოდს საფუძვლად უდევს რისკების შეფასების კომპლექსური მიდგომა ანალიზის რაოდენობრივი და ხარისხობრივი მეთოდების გათვალიწინებით. მეთოდი უნეევრსალურია და ის ერგება, როგორც მსხვილ, ისე მცირე ორგანიზაციებს, როგორც სახელმწიფო, ისე კერძო სექტორს. CRAMM-ის პროგრამული უზრუნველყოფის ვერსიები ორიენტირებულია სხვადასხვა ტიპის ორგანიზაციებზე და ერთმანეთისგან განსხვავდებიან ცოდნის ბაზების მიხედვით (profiles). სისტემას კომერციული საწარმოებისათვის აქვს Commercial Profile, ხოლო სახელმწიფო ორგანიზაციებისათვის - Government profile. სახელმწიფო პროფილის ვარიანტი საშუალებას იძლევა აუდიტი ჩატარდეს ამერიკული სტანდარტის ITSEC–ის (“ნარინჯისფერი წიგნის”) მოთხოვნების შესაბამისობაზეც.

CRAMM მეთოდის გონივრული გამოყენება კარგი შედეგების მიღების საშულებას იძლევა. განსაკუთრებით აღსანიშნავია ინფორმაციულ უსაფრთხოებაზე და ბიზნესის უწყვეტობაზე ორგანიზაციის ხარჯების ეკონომიკურად დასაბუთების შესაძლებლობა. რისკების მართვის ეკონომიკურად დასაბუთებული სტრატეგია საბოლოო ჯამში იწვევს სახსრების ეკონომიას და გაუმართლებელი დანახარჯებისგან თავის არიდებას.

CRAMM-ში მთელი პროცედურა დაყოფილია სამ ეტაპად. პირველი ეტაპის ამოცანაა პასუხი გაეცეს კითხვას: "ინფორმაციული სისტემის დაცვისათვის საკმარისია ბაზისური დონის საშუალებების გამოყენება, თუ საჭიროა უფრო დეტალური ანალიზის ჩატარება?" მეორე ეტაპზე ტარდება რისკების იდენტიფიკაცია და ფასდება მათი ზომა. მესამე ეტაპზე ხდება ადეკვატური კონტრ-ღონისძიებების შერჩევა.

CRAMM მეთოდიკა ყოველი ეტაპისათვის განსაზღვრავს საწყისი მონაცემების ერთობლიობას, ღონისძიებების ერთობლიობას, ინტერვიუების ჩატარების ანკეტის განსაზღვრას, საკონტროლო სიებს და ანგარიშის დოკუმენტების ერთობლიობას.

თუ **პირველი ეტაპის** ჩატარების შედეგად დადგინდა, რომ რესურსების კრიტიკულობის დონე ძალიან დაბალია და არსებული რისკები არ გადააჭარბებენ რაიმე ბაზისურ დონეს, მაშინ სისტემას წაეყენება უსაფრთხოების მინიმალური მოთხოვნები. ამ შემთხვევაში მეორე ეტაპის ღონისძიების ჩატარება აუცილებელი არა არის და ხდება მესამე ეტაპზე გადასვლა, სადაც გენერირდება კონტრ-ღონისძიებების სტანდარტული ჩამონათვალი, უსაფრთხოების ბაზისურ მოთხოვნებთან შესაბამისობის უზრუნველსაყოფად.

მეორე ეტაპზე ხდება საფრთხეების და სუსტი ადგილების ანალიზი. საფრთხეების და სუსტი ადგილების შესაფასებლად საწყის მონაცემებს აუდიტორი იღებს ორგანიზაციის უფლებამოსილი წარმომადგენლებისგან ინტერვიუების შედეგად. ინტერვიუების ჩასატარებლად გამოიყენება სპეციალური კითხვარები.

მესამე ეტაპზე წყდება რისკების მართვის ამოცანა, რომელიც შედგება ადეკვატური კონტრ-ღონისძიებების შერჩევისაგან.

ინფორმაციულ სისტემაში უსაფრთხოების ახალი მექანიზმების დანერგვისა და ძველების მოდიფიკაციის გადაწყვეტილებას ღებულობს ორგანიზაციის ხელმძღვანელობა, რომელიც ითვალისწინებს ამ გადაწყვეტილებასთან დაკავშირებულ ხარჯებს, მათ აუცილებლობას და ბიზნესისთვის საბოლოო სარგებელს. აუდიტორის ამოცანაა რეკომენდირებული კონტრ-ღონისძიებების დასაბუთება ხელმძღვანელობისათვის.

ახალი კონტრ-ღონისძიებების და ძველების მოდიფიკაციის დანერგვის გადაწყვეტილების მიღების შემთხვევაში, აუდიტორს შესაძლოა დაევალოს ახალი კონტრ-ღონისძიებების დანერგვის გეგმის მომზადება და მათი გამოყენების ეფექტურობის შეფასება. ამ ამოცანების გადაწყვეტა CRAMM- ის მეთოდების ფარგლებიდან გადის.

CRAMM- ის მეთოდების ნაკლოვანებად შეიძლება ჩაითვალოს:

- **CRAMM-ის მეთოდის გამოყენებას ჭირდება სპეციალური მომზადება და აუდიტორის მაღალი კვალიფიკაცია;**
- **CRAMM გაცილებით უფრო კარგად ერგება უკვე არსებულ ინფორმაციულ სისტემებს, რომლებიც იმყოფებიან ექსპლუატაციის სტადიაში, ვიდრე იმ ინფორმაციულ სისტემებს, რომლებიც დაპროექტების სტადიაში არიან;**

- **CRAMM-ის მეთოდით აუდიტის პროცესი საკმაოდ შრომატევადია და შეიძლება დაჭირდეს აუდიტორის თვეობით უწყვეტი მუშაობა;**
- **CRAMM-ის პროგრამული ინსტრუმენტები ქმნიან დიდი რაოდენობის ქაღალდის დოკუმენტაციას, რომელიც პრაქტიკაში ყოველთვის არაა მოსახერხებელი;**
- **CRAMM არ იძლევა საშუალებას შეიქმნას საკუთარი ანგარიშების შაბლონები ან მოხდეს არსებულის მოდიფიცირება;**
- **CRAMM-ის ცოდნის ბაზაში ცვლილებების შეტანის შესაძლებლობა მომხმარებლისთვის გათვალისწინებული არაა, რამაც შეიძლება გამოიწვიოს გარკვეული სირთულეები ზოგიერთი ტიპის ორგანიზაციაში ადაპტაციისას;**
- **CRAMM- ის პროგრამული უზრუნველყოფა მხოლოდ ინგლისურენოვანია;**
- **ლიცენზიის მაღალი ღირებულება.**

სისტემა RiskWatch. პროგრამული უზრუნველყოფა RiskWatch, რომელიც დამუშავებულია ამერიკული კომპანიის RiskWatch_Inc მიერ, წარმოადგენს რისკების ანალიზისა და მართვის მძლავრ საშუალებას. RiskWatch პროგრამულ კომპლექსში შედის უსაფრთხოების აუდიტის ჩატარების სხვადასხვა სახის პროგრამული პროდუქტები. იგი მოიცავს რისკების ანალიზისა და აუდიტის შემდეგ საშუალებებს:

- **RiskWatch for Physical Security – ინფორმაციული სისტემების ფიზიკურად დაცვის მეთოდებისათვის;**
- **RiskWatch for Information Systems – ინფორმაციული რისკებისათვის;**
- **HIPAA-WATCH for Healthcare Industry – HIPAA სტანდარტის მოთხოვნებისადმი შესაბამისობის შეფასებას;**
- **RiskWatch RW17799 for ISO17799 – ISO17799 სტანდარტის მოთხოვნებისადმი შესაბამისობის შეფასებას.**

RiskWatch მეთოდში რისკების შეფასების და მართვის კრიტერიუმად გამოიყენება „წლიური დანაკარგების პროგნოზირება" (Annual Loss Expectancy – ALE) და „ინვესტიციიდან უკუგების" შეფასება (Return on Investment – ROI). RiskWatch ეხმარება ჩატარდეს რისკების ანალიზი და გაკეთდეს დაცვის ღონისძიებების და საშუალებების დასაბუთებული არჩევანი. პროგრამაში გამოყენებული მეთოდიკა მოიცავს 4 ფაზას:

პირველი ფაზა – კვლევის საგნის განსაზღვრა. ამ ეტაპზე ხდება ორგანიზაციის პარამეტრების აღწერა – ორგანიზაციის ტიპი, განსახილველი სისტემის შემადგენლობა, უსაფრთხოების კუთხით ბაზისური მოთხოვნები. ხდება აღწერების ფორმალიზება ქვეპუნქტებად. თითოეული პუნქტი აღიწერება დაწვრილებით. ანალიტიკოსის სამუშაოს შესამსუბუქებლად შაბლონებში სიებად მოიცემა დასაცავი კატეგორიები, რესურსები, დანაკარგები, საფრთხეები, სუსტი ადგილები და დაცვის ღონისძიებები. მათგან უნდა შეირჩეს ისინი, რომლებიც რეალურად არსებობენ ორგანიზაციაში.

მეორე ფაზა – მონაცემთა შეტანა, რომლებიც აღწერს სისტემის კონკრეტულ მახასიათებლებს. მონაცემები შეიძლება შეტანილი იქნას ხელით ან მოხდეს მათი ანგარიშებიდან იმპორტირება, რომლებიც შექმნილია კომპიუტერული ქსელის სუსტი ადგილების კვლევის ინსტრუმენტული საშუალებებით. დეტალურად აღიწერება რესურსები, დანაკარგები და ინციდენტების კლასები.

ინციდენტების კლასები მიიღება დანაკარგების კატეგორიების შედარებით რესურსების კატეგორიებთან. შესაძლო სუსტი ადგილების გამოსავლენად გამოიყენება კითხვარები, რომლის ბაზა შეიცავს 600-ზე მეტ კითხვას. დასაშვებია კითხვების კორექტირება, ამოგდება ან ახლის დამატება. შესაძლებელია თითოეული საფრთხის ხდომილების სიხშირის, სუსტი ადგილების ხარისხის და რესურსების ღირებულების მითითება. ყველაფერი ეს შემდგომში გამოიყენება დაცვის საშუალებების დანერგვის ეფექტურობის გამოსათვლელად.

მესამე ფაზა – რისკების შეფასება. თავიდან დგინდება დამოკიდებულებები რესურსებს, დანაკარგებს, საფრთხეებს და სუსტ ადგილებს შორის, რომლებიც წინა ეტაპებზე გამოიკვეთა. რისკებისათვის გამოითვლება წლიური დანაკარგების მათემატიკური მოლოდინი ფორმულით: $m=p*v$, სადაც p- წელიწადში საფრთხის წარმოქმნის სიხშირეა, v – იმ რესურსის ღირებულებაა, რომელსაც

საფრთხე ემუქრება. დანერგილი დაცვის ღონისძიებების და მის გარეშე მოსალოდნელი დანაკარგების შედარებით შეიძლება შეფასდეს ამ ღონისძიებების ეფექტურობა.

მეოთხე ფაზა – ანგარიშების გენერირება. ანგარიშების ტიპებია: მოკლე შედეგები; სრული და მოკლე ანგარიშები იმ ელემენტების შესახებ, რომლების აღწერაც მოხდა 1 და 2 სტადიაზე; საფრთხის რეალიზაციის შემთხვევაში დასაცავი რესურსების ღირებულებისა და შესაძლო დანაკარგების ანგარიში; საფრთხეებისა და კონტრ-ღონისძიებების ანგარიში; უსაფრთხოების აუდიტის ანგარიში.

RiskWatch-ის ნაკლოვანებად შეიძლება ჩაითვალოს:

- **ასეთი მეთოდი გამოდგება, როდესაც მოითხოვება პროგრამულ-ტექნიკურ დონეზე რისკების ანალიზის ჩატარება, ამ დროს არაა გათვალისწინებული ადმინისტრაციული და ორგანიზაციული ფაქტორები;**
- **RiskWatch პროგრამული უზრუნველყოფა მხოლოდ ინგლისურენოვანია;**
- **ლიცენზიის მაღალი ღირებულება (მცირე ორგანიზაციისათვის ერთი სამუშაო ადგილი -15000$; კორპორატიული ლიცენზიისათვის - 125000$).**

3. დასკვნა

თანამედროვე რისკების ანალიზის სისტემის გამოყენებით შესაძლებელია ორგანიზაციაში შეფასდეს ინფორმაციული უსაფრთხოების კუთხით არსებული რისკები და შეირჩეს ეფექტურობის მიხედვით ოპტიმალური დაცვის ვარიანტები.

ლიტერატურა:

1. Симонов С. Современные технологии анализа рисков в информационных системах. PCWEEK N37'2001
2. www.insight.co.uk
3. www.riskwatch.com

СОВРЕМЕННЫЕ МЕТОДЫ И СРЕДСТВА АНАЛИЗА И КОНТРОЛЯ РИСКОВ ИНФОРМАЦИОННЫХ СИСТЕМ

Капанадзе Д.Ш., Жвания Т.Г.
Грузинский Технический Университет

Резюме

Рассмотрена оценка необходимого уровня вложений в информационной безопасности бизнеса для обеспечения максимальной эффективности инвестиций в данную сферу. Описаны современные системы анализа рисков позволяющие оценить существующие в системе риски и выбрать оптимальный по эффективности вариант защиты.

MODERN METHODS AND MEANS OF ANALYSIS OF RISKS AND MONITORING OF INFORMATION SYSTEMS

Kapanadze D., Zhvania T.
Georgian Technical University

Summary

The estimation of a necessary level of investments in information safety of business for effective investment in this sphere are discussed in article. Modern systems of the analysis of risks are described, which allow to make an estimation of existing risks and choose an optimum variant of protection over efficiency.