ინფორმაციული უსაფრთხოების აუდიტორული რისკების ანალიზი

გულნარა ჯანელიძე[1], ბექა ქაფიანიძე[1], ნინო მეფარიშვილი[2]
1. საქართველოს ტექნიკური უნივერსიტეტი,
2. „ხალიკ“-ბანკი საქართველო

რეზიუმე

საწარმოს ინფორმაციული უსაფრთხოებისადმი მოთხოვნის მიხედვით აუდიტს შეიძლება ჰქონდეს სხვადასხვა მიმართულება და მოიცვას ინფორმაციული უსაფრთხოების ცალკეული სფერო. აუდიტი რეკომენდებულია ინფორმაციული რესურსების მთლიანობისა და კონფიდენციალობისადმი მაღალი მოთხოვნების, ინფორმაციულ ტექნოლოგიებზე მკაცრად დამოკიდებული, აქტიურად განვითარებადი ინფორმაციული ტექნოლოგიების მქონე კომპანიებისათვის. კომპლექსური აუდიტი საინფორმაციო სისტემების დაცულობის სრული და ობიექტური შეფასების, არსებული პრობლემების ლოკალიზების, ინფორმაციული უსაფრთხოების სისტემის აგების ეფექტური პროგრამის შემუშავების საშუალებას იძლევა. სტატიაში წარმოდგენილია კომპლექსური აუდიტის ამოცანები და ჩატარების ძირითადი ეტაპები. ასევე, მოცემულია აუდიტორული საქმიანობის დროს წარმოშვებული რისკების ანალიზი.

საკვანძო სიტყვები: რისკების მართვა. აუდიტორული რისკები.

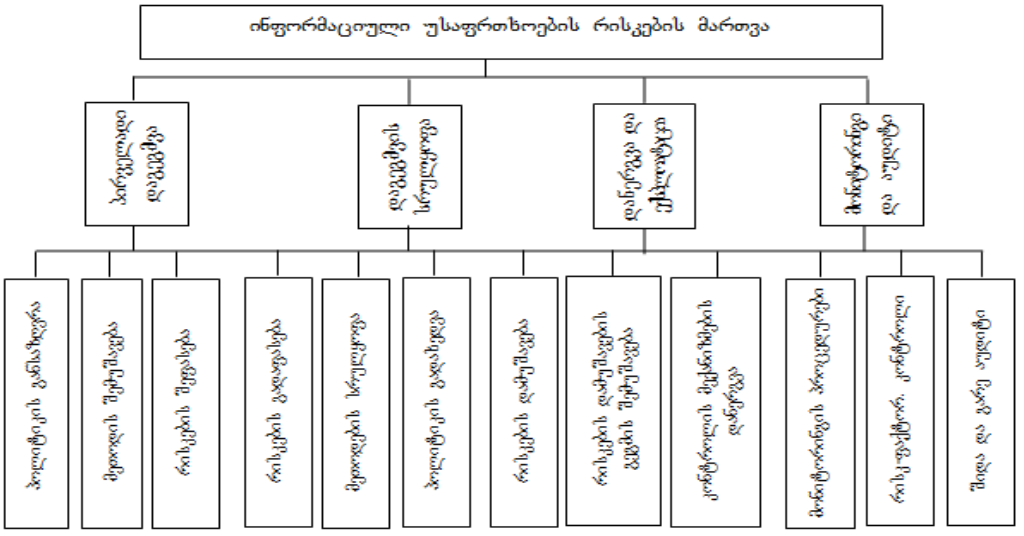
1. შესავალი

თანამედროვე პირობებში საწარმოს ინფორმაციული უსაფრთხოების უზრუნველყოფის პრობლემა მეტად მწვავე ხასიათს იღებს. გახშირდა მონაცემებისა და საწარმოს ავტომატიზებული სისტემების არასაკმარისი დაცვით გამოწვეული ინციდენტები, რაც შესაბამისად უარყოფითად აისახება ბიზნესის წარმატებაზე [1].

საწარმოს თანამედროვე საინფორმაციო სისტემებს, გააჩნია რა დიდი რაოდენობის პროგრამული და აპარატურული საშუალებები, აქვს რთული ჰეტეროგენული სტრუქტურა. ბუნებრივია, რომ ასეთ პირობებში ძალზედ რთულია მოსალოდნელი საფრთხის ან განხორციელებული თავდასხმის, როგორც ოპერატიული აღმოჩენა, ასევე მათი სალიკვიდაციო ღონისძიებების დროული ჩატარება. დიდია იმის ალბათობა, რომ ზოგიერთი თავდასხმა ხდომილების შემდგომ იქნეს აღმოჩენილი ან საერთოდ იგნორირებული დარჩეს. აღნიშნული პრობლემის გადასაწყვეტად საჭიროა ინფორმაციული უსაფრთხოების რისკების მართვის კარგად ორგანიზებული სისტემის შექმნა, სადაც მნიშვნელოვანი ადგილი უჭირავს როგორც საინფორმაციო სისტემების მუდმივ მონიტორინგს და კომპლექსური აუდიტის წარმოებას, ასევე აუდიტორული რისკების შეფასებას.

2. ძირითადი ნაწილი

ინფორმაციული უსაფრთხოების რისკების მართვის პროცესი შეიძლება დავყოთ ოთხ ეტაპად (ნახ.1):



ნახ.1. ინფორმაციული უსაფრთხოების რისკების მართვის სისტემა

დაგეგმვის ეტაპზე უნდა განისაზღვროს რისკების მართვის პოლიტიკა და მეთოდოლოგია, ასევე მოხდეს რისკების შეფასება, რომელიც მოიცავს აქტივების ინვენტარიზაციას, საფრთხეებისა და დაუცველი ადგილების პროფილების შედგენას, კონტრზომების ეფექტურობისა და პოტენციური ზარალის შეფასებას, დარჩენილი რისკების დასაშვები დონის განსაზღვრას.

რეალიზაციის ეტაპზე რისკები უნდა დამუშავდეს და დაინერგოს მართვის მექანიზმები, რომელიც გათვლილია რისკების მინიმიზებაზე.

შემოწმების ეტაპზე თვალყური უნდა მიედევნოს მართვის მექანიზმების ფუნქციონირებას, გაკონტროლდეს რისკ-ფაქტორების (როგორიცაა აქტივები, საფრთხეები, დაუცველი ადგილები) ცვლილება, ჩატარდეს აუდიტი და სხვადასხვა მაკონტროლებელი პროცედურები.

უსაფრთხოების განყოფილება ორგანიზაციის პოლიტიკის შესაბამისად შეიმუშავებს აუდიტის ჩატარების გეგმებს. ასეთი აუდიტი შეიძლება ფოკუსირებული იყოს სისტემის კონფიგურაციაზე, სარეზერვო ასლების პოლიტიკის შესაბამისად, ან ფიზიკურ ფორმაში ინფორმაციის დაცვაზე. ცალკეული აუდიტი გამიზნულია ორგანიზაციის რომელიმე ნაწილისათვის, რამდენადაც იგი მოითხოვს დიდ ძალისხმევას პერსონალის მხრიდან. მნიშვნელოვანი შეუსაბამობის აღმოჩენისას შესაბამის ქვედანაყოფში ტარდება უფრო მასშტაბური აუდიტი. ორგანიზაციის აუდიტის განყოფილებას უნდა ჰქონდეს თავისი განრიგი და აუდიტების გეგმები. აუდიტი განსაზღვრავს თუ რამდენად კარგად სრულდება უსაფრთხოების პოლიტიკა და პროცედურები, შემდგომში ნაკლოვანებების და შეუსაბამობების აღმოფხვრის მიზით [2].

ინფორმაციული უსაფრთხოების აუდიტი შეიძლება დავყოთ შემდეგ ეტაპებად: პირველადი გამოკვლევა; წინასაპროექტო გამოკვლევა; ობიექტის ატესტაცია; რისკების დაზღვევა; საკონტროლო გამოკვლევა.

პირველადი გამოკვლევის ეტაპზე დამკვეთმა უნდა დაადგინოს თუ რას სთავაზობენ მას რეალურად, რამდენად შეესაბამება იგი განსაზღვრულ მოთხოვნებს და კრიტერიუმებს, რის შედეგადაც იგი მიიღებს პრობლემის საერთო ხედვას და მისი გადაწყვეტის მიმართულებას. ამ ეტაპზე ყალიბდება საწარმოს ინფორმაციული უსაფრთხოების კონცეფცია. ამ შედეგების საფუძველზე შეიძლება შეიქმნას ინფორმაციის დაცვის გონივრული პოლიტიკა.

მომდევნო ეტაპი არის ტექნიკური აუდიტი. ამ ეტაპზე დასაპროექტებელი საინფორმაციო სისტემის და მოცემული ობიექტის საფრთხეთა მოდელის შედარების შედეგად განისაზღვრება რომელი ფაქტორებია მეტნაკლებად კრიტიკული. ტექნიკური აუდიტის შედეგად მიიღება ინფორმაციული უსაფრთხოების სისტემის მიმართ მოთხოვნათა ნაკრები, რაც ფაქტობრივად წარმოადგენს დაცვის პროფილს. გარდა ამისა, აღნიშნულ ეტაპზე განისაზღვრება საორგანიზაციო ღონისძიებების კომპლექსი, დაცვის დონე და სხვა საკითხები.

შემდგომი ეტაპი არის ატესტაციის სტადია, იმის დასადგენად თუ რამდენად აკმაყოფილებს დამუშავებული სისტემა დამკვეთის მიერ წაყენებულ მოთხოვნებს. აღნიშნულ ეტაპზე მზადდება ექსპერტის დასკვნა.

ინფორმაციის მფლობელი აცნობიერებს თავისი ინფორმაციის ღირებულებას. ინფორმაციის დაკარგვამ შეიძლება გამოიწვიოს მნიშვნელოვანი ფინანსური დანაკარგები. ამდენად, წარმოიშვება დანაკარგის შესაძლო კომპენსაციის აუცილებლობა, რაც შეიძლება განხორციელდეს ინფორმაციული რისკების დაზღვევით. აღნიშნულ ეტაპზე კვლევის შედეგები გადაეცემა მესამე პირს – სადაზღვევო კომპანიას, სადაზღვევო გადასახადის განსაზღვრისათვის. ეტაპის დასრულებისას მზადდება სადაზღვევო ანგარიში.

აუდიტის დამამთავრებელი ეტაპია საკონტროლო გამოკვლევა, რომელიც ტარდება ორ კრიტიკულ სიტუაციაში. ერთი იმ შემთხვევაში, თუ ადგილი ჰქონდა ხდომილებას, რომელმაც გამოიწვია ინფორმაციის დაკარგვა და საჭიროა მიზეზების გამოკვლევა, მეორე – დაგეგმილი საკონტროლო გამოკვლევის შემთხვევაში, ინფორმაციის უსაფრთხოების წესების დაცვის შემოწმების მიზნით [3].

აუდიტის სამსახური უსაფრთხოების პოლიტიკის შესაბამისად წყვეტს შემდეგ ამოცანებს:

– რეალური დროის რეჟიმში ჰაკერების თავდასხმის და ინფორმაციული უსაფრთხოების სხვა საფრთხეების აღმოჩენა;

– სხვადასხვა წყაროებიდან შეგროვებული ინფორმაციის ანალიზის საფუძველზე ინციდენტების ამოცნობა;

– წინასწარ დაპროგრამებული მოქმედებების ავტომატური შესრულება, რომელიც მიმართულია თავდასხმის აღმოჩენის შემთხვევაში საფრთხის შეჩერებაზე.

აუდიტორული რისკები ძირითადად არასწორი შეხედულებების ან რეალური მონაცემებიდან გადახრის, აუდიტის პროცესში დაშვებული უზუსტობების შედეგად წარმოიშვება. აღნიშნული რისკის უგულვებელყოფის შედეგი იქნება ყალბი დასკვნის გაკეთება, რაც უარყოფითად აისახება ორგანიზაციის მომავალ საქმიანობაზე. თუმცა არსებობს რისკის დასაშვები დონე, რომელსაც აუდიტორი იღებს თავის თავზე და წარმოადგენს დასკვნაში. რისკის აბსოლუტური აღმოფხვრა შეუძლებელია. აუდიტორულ პრაქტიკაში დადგენილია რისკების მისაღები დონე, რაც დაახლოებით 5%-ს წარმოადგენს[4].

აუდიტორული რისკების შეფასებისათვის საჭიროა შემდეგი მოქმედებების შესრულება:

– შიდა აუდიტორების თანამდებობრივი მოვალეობების გაცნობა;

– შიდა აუდიტის სამსახურის საქმიანობის კონკრეტული პროგრამისა და გეგმის დეტალების გაცნობა;

– მუშა დოკუმენტების შემოწმების პროგრამების შედეგებისა და შიდა აუდიტორების ანგარიშების სისრულისა და შესაბამისობის ხარისხის დადგენა;

– ცალკეული ობიექტის შიდა აუდიტისათვის გამოყენებული მეთოდიკის საფუძვლიანობის ხარისხის კონტროლი;

– არსებული შიდა საკონტროლო ინფორმაციის საფუძველზე შიდა კონტროლის მთელი სისტემის ფუნქციონირების ხარისხის შეფასება;

– შიდა აუდიტის შედეგების მიხედვით მაკორექტირებელი ზემოქმედებების და ღონისძიებების განსაზღვრა;

– საკონტროლო ხდომილებების ტესტირება, შიდა კონტროლის სისტემის ხარისხის შემოწმების მიზნით;

– შიდა აუდიტის სამსახურის ხელმძღვანელის მხრიდან შიდა აუდიტორების მუშაობის ხარისხის კონტროლის მდგომარეობის განსაზღვრა;

– შიდა აუდიტორებისათვის საკადრო პოლიტიკის გაცნობა, საკვალიფიკაციო გამოცდების ჩატარება, პროფესიული მომზადების პროგრამების დანერგვა.

3. დასკვნა

კომპლექსური აუდიტის ძირითადი მიზანია დამკვეთის ინფორმაციული უსაფრთხოების დონის მიმდინარე მდგომარეობის რეალური და დამოუკიდებელი შეფასების მიღება. აუდიტის პროცესში მიმდინარეობს დამკვეთის ინფორმაციული რესურსების, ინფორმაციის დამუშავების საშუალებების და მეთოდების, დაცვის სამართლებრივი ნორმების კვლევა. მოქმედების ეტაპზე უწყვეტი მონიტორინგისა და ჩატარებული შემოწმებების შედეგების მიხედვით სრულდება აუცილებელი მაკორექტირებელი მოქმედებები, რომელიც შეიძლება მოიცავდეს რისკების სიდიდის გადაფასებას, პოლიტიკის კორექტირებას და რისკების მართვის მეთოდოლოგიას, აგრეთვე რისკების დამუშავების გეგმას.

ამდენად, აუდიტის მასალები შეიძლება გამოყენებულ იქნეს ინფორმაციული უსაფრთხოების პოლიტიკის და კონცეფციის დამუშავების ინფორმაციულ-ანალიტიკურ ბაზად.

ყოველივე ზემოთქმულიდან გამომდინარე, აუდიტორული რისკების ანალიზი ინფორმაციული უსაფრთხოების ერთ-ერთ მნიშვნელოვან ამოცანას წარმოადგენს.

ლიტერატურა:

1. Layton T.P. Information Security: Design, Implementation, Measurement, and Compliance. Boca Raton, FL: Auerbach publications. 2007

2. შონია ო., ჯანელიძე გ., მეფარიშვილი ბ. ინფორმაციული და ქსელური რესურსების უსაფრთხოების ურუნველყოფა, თბ., სტუ, 2009

3. Курило А. П. Аудит информационной безопасности. -БДЦ-пресс. 2006

4. Peltier T.R. Information Security Risk Analysis. Boca Raton, FL: Auerbach publications. 2001.

INFORMATION SAFETY AUDIT RISK ANALYSIS

Janelidze Gulnara, Qafianidze Beqa, Meparishvili Nino
Georgian Technical University

Summary

Depending on the demand for the Information Safety in the business-organization, the audit may have different directions and include different spheres of information Safety. Audit is recommended for businesses with high demand on information completeness and confidentiality, for highly dependent businesses on Information Technologies and companies possessing rapidly developing information technologies. Complex Audit gives the possibilities of complete and objective assessment of the information system's safety, localization of existing problems and creation of effective program for construction of Informational Safety System. The article presents objectives of the complex audit and main stages of execution. The risks occurring during the auditor work are also specified.

АНАЛИЗ АУДИТОРНЫХ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Джанелидзе Г., Капианидзе Б., Мепаришвили Н.
Грузинский Технический Университет

Резюме

В зависимости от требовании к информационной безопасности предприятия аудит может иметь разные направления и охватывать отдельные сферы информационной безопасности. Аудит может быть рекомендован для компаний с высокими требованиями к целостности информационных ресурсов и конфиденциальности, строго зависимым от информационных технологий, а также для компаний с активно развивающими информационными технологиями. Комплексный аудит дает возможность полной защиты и объектной оценки информационных систем, локализации существующих проблем, разработки эффективной программы построения системы информационной безопасности. В статье представлены задачи комплексного аудита и основные этапы его проведения, а также проведен анализ рисков, имеющих место во время аудиторной деятельности.