საწარმოს ინფორმაციული რისკების ანალიზი

გულნარა ჯანელიძე, ნინო მეფარიშვილი
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

ნაშრომი ეძღვნება საწარმოს ინფორმაციული უსაფრთხოების უზრუნველყოფის პრობლემებს, კერძოდ ინფორმაციული რისკების გამოვლენისა და შეფასების ალგორითმის დამუშავებას. კონკრეტულ საწარმოს, თავისი სპეციფიკიდან გამომდინარე, გააჩნია განსხვავებული შიდა გარემო. გარდა ამისა, იგი მუშაობს სპეციფიკურ კონკურენტულ გარემოში. ამდენად ცალკეულ საწარმოში წარმოიშობა საინფორმაციო რისკები, რომლის დროული გამოვლენა ან მისი წარმოშობის ალბათობის განსაზღვრა მნიშვნელოვნად შეამცირებს შესაძლო ზარალს. საწარმოს ინფორმაციული რისკების ანალიზისადმი წარმოდგენილი მიდგომა, რომელიც ძირითადად რისკების ხასიათისა და მისი რეალიზების შემთხვევაში შესაძლო დანაკარგების განსაზღვრაში მდგომარეობს, ხელს შეუწყობს ობიექტის მდგრად განვითარებას და კლიენტების ინტერესების დაცვას.

საკვანძო სიტყვები: ინფორმაციული უსაფრთხეობის სისტემა, რისკ-ფაქტორები, ინფორმაციული რისკები, მოწყვლადობათა შეფასება.

1. შესავალი

საწარმოს უსაფრთხოების უზრუნველყოფისადმი კომპლექსური მიდგომა მისი ფუნქციონირების აუცილებელ პირობას წარმოადგენს. კომპლექსურობაში მოიაზრება წინასწარ გაანალიზებული, დაბალანსებული დაცვა, მკაფიოდ გამოკვეთილი ორგანიზაციულ-ტექნიკური ზომების მიღება და დაცვის ყველა ღონისძიების შესრულებაზე მკაცრი კონტროლის უზრუნველყოფა.

საწყის ეტაპზე საჭიროა საწარმოს საინფორმაციო პროცესებზე აუდიტის ჩატარება კრიტიკულად მნიშვნელოვანი ინფორმაციის გამოვლენის მიზნით. აუდიტის დასრულების შემდეგ ცხადი ხდება რა, სად და ვისგან არის დასაცავი.

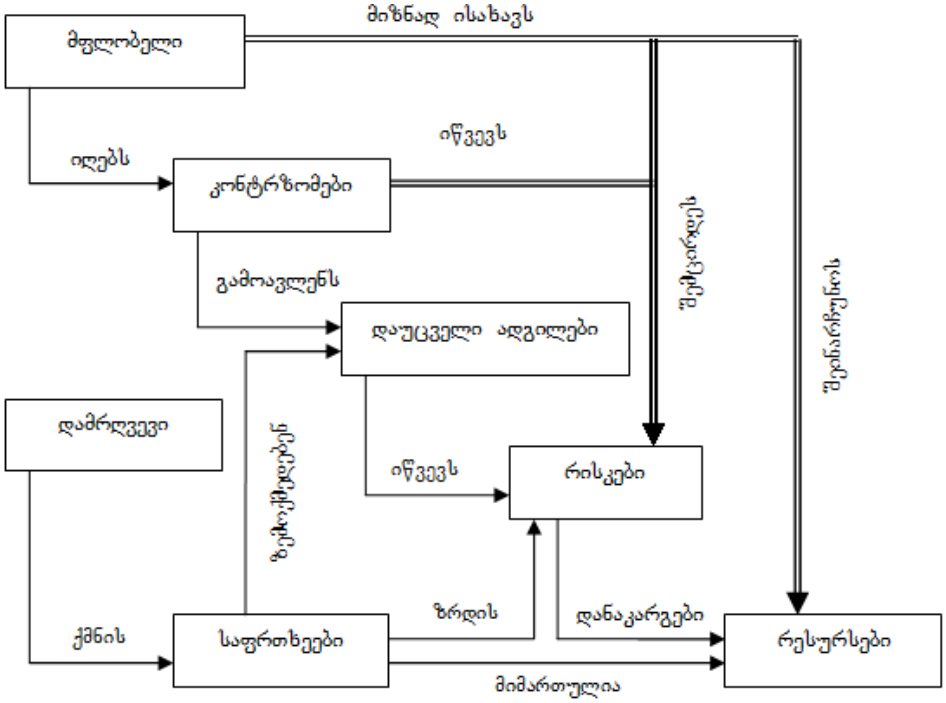
საწარმოს ინფორმაციული უსაფრთხოების სისტემის მთავარ მიზანს წარმოადგენს ობიექტის მდგრადი ფუნქციონირების და მომსახურე პერსონალის ნორმალური მწარმოებლური საქმიანობის უზრუნველყოფა, დამკვეთის კანონიერი უფლებების დაცვა, შემოთავაზებული მომსახურეობის ხარისხის ამაღლება და კლიენტების ინტერესებისა და ქონებრივი უფლებების უსაფრთხოებაზე გარანტიების უზრუნველყოფა.

ინფორმაციული რისკების, როგორც საწარმოო პროცესის განუყოფელი ნაწილის, არსებობას მივყავართ მათი გამოვლენისა და შეფასების კონკრეტული ალგორითმის დამუშავების აუცილებლობამდე. საწარმო, აქვს რა სპეციფიკური შიდა გარემო, საწარმოო პოტენციალის დონე, საკადრო შემადგენლობა და სხვა მახასიათებლები, მუშაობს კონკურენტული გარემოს განსხვავებულ პირობებში. ამდენად, ცალკეულ საწარმოში წარმოიშობა საინფორმაციო რისკი, რომელიც დაკავშირებულია კონკრეტულად ამ ობიექტის სპეციფიკიდან გამომდინარე საწარმოო, ტექნოლოგიურ, კომერციულ, ფინანსურ და სხვა სახის საქმიანობასთან. მნიშვნელოვანია რისკის როგორც დროული გამოვლენა, ასევე მისი წარმოშობის ალბათობის, დროის და შესაძლო დანაკარგების განსაზღვრა.

2. ძირითადი ნაწილი

ობიექტის ინფორმაციული უსაფრთხოების სისტემის აგების პროცესის საწყის ეტაპს წარმოადგენს ობიექტისათვის უსაფრთხოების პოლიტიკის დამუშავება. კერძოდ, საწარმოს უსაფრთხოების საორგანიზაციო პოლიტიკა აღწერს მომხმარებლებზე წვდომის უფლებების წარდგენისა და მათ მიერ ამ უფლებების გამოყენების წესებს. ასევე, აღნიშნული პოლიტიკა მომხმარებლებიდან მოითხოვს ანგარიშგებას უსაფრთხოების მიმართულებით შესრულებული ყველა მოქმედების შესახებ[1].

საწარმოს ინფორმაციული უსაფრთხოების სისტემის ზოგადი მოდელი წარმოდგენილია 1-ელ ნახაზზე.



ნახ.1. საწარმოს ინფორმაციული უსაფრთხოების სისტემის ზოგადი მოდელი

წარმოდგენილი მოდელი არის ობიექტური შიგა და გარე ფაქტორების ერთობლიობა და მათი ზეგავლენა როგორც დასაცავი ობიექტის ინფორმაციული უსაფრთხოების მდგომარეობაზე, ასევე მატერიალური რესურსების დაცულობაზე.

შეიძლება გამოვყოთ შემდეგი ობიექტური ფაქტორები:

- საფრთხეები, რომლებიც ხასიათდება როგორც აღძრის, ასევე რეალიზების ალბათობით;
- საინფორმაციო სისტემის სუსტი ადგილები, რომლებიც ზეგავლენას ახდენენ საფრთხის რეალიზების ალბათობაზე;
- რისკ-ფაქტორები, რომლებიც ასახავენ საწარმოს შესაძლო ზარალს საფრთხის რეალიზების შედეგად. საბოლოოდ რისკი ასახავს შესაძლო ფინანსურ დანაკარგებს.

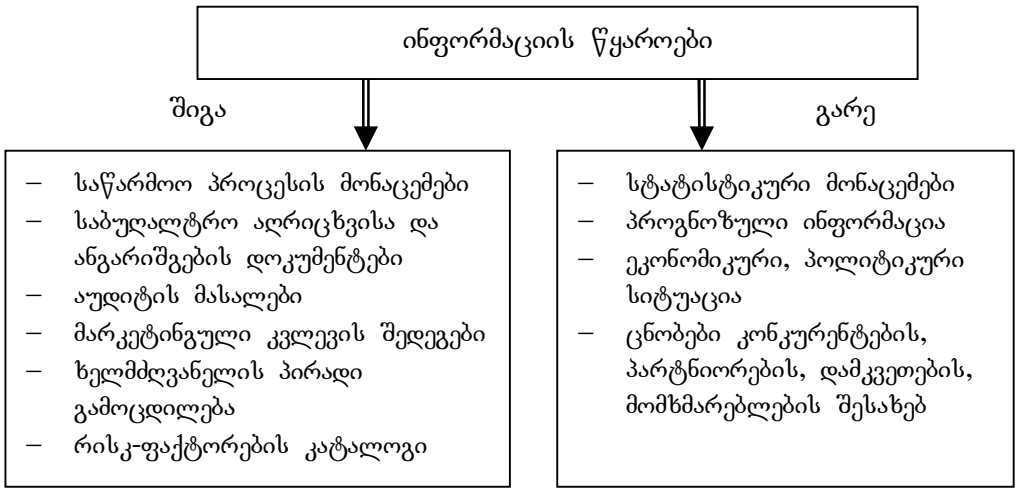
საწარმოს ინფორმაციული უსაფრთხოების სისტემის ასაგებად მიზანშეწონილია რისკების ანალიზის ჩატარება. შემდგომ უნდა განისაზღვროს კონკრეტული საწარმოსათვის რისკების ოპტიმალური დონე, მოცემული კრიტერიუმების საფუძველზე.

ანალიტიკური სამუშაოების ჩატარების მეთოდიკა მოითხოვს:

- სრულად იქნას გაანალიზებული და დოკუმენტურად გაფორმებული ინფორმაციული უსაფრთხოების უზრუნველყოფასთან დაკავშირებული მოთხოვნები;
- თავიდან იქნას აცილებული დანახარჯები უსაფრთხოების გადამეტებული ღონისძიებებისათვის;
- უზრუნველყოფილ იქნას სამუშაოების ჩატარება მინიმალურ ვადებში;
- ჩატარდეს კონტრზომების შესაძლო ვარიანტების გადარჩევა;
- განხორციელდეს არჩეული კონტრზომების ეფექტურობის შეფასება.

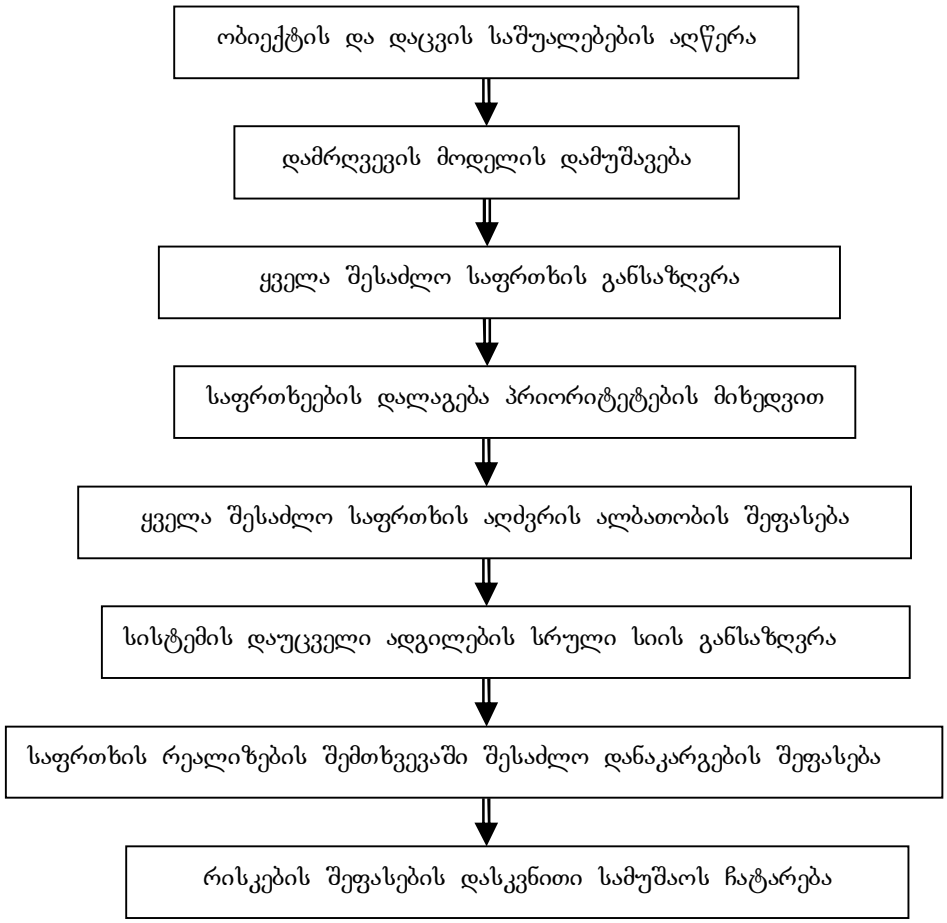
რისკის სახეების და წყაროების განსაზღვრისათვის აუცილებელია არსებობდეს საიმედო ინფორმაციული უზრუნველყოფა. ყველა ინფორმაცია ცალკეული რისკის ხასიათის შესახებ შეიძლება მიღებულ იქნას სხვადასხვა წყაროდან, როგორიცაა: ერთჯერადი და მუდმივი, ოფიციალური და არაოფიციალური, მიღებული და მოკვლეული, სანდო და საეჭვო. რისკების მართვისას გამოყენებული ინფორმაცია უნდა იყოს სანდო, სრულყოფილი და დროული[2,3].

ინფორმაციული რისკების მართვის სისტემა გამოიყენებს ინფორმაციის წყაროებს, რომელიც შეიძლება კლასიფიცირდეს, როგორც ინფორმაციის შიდა და გარე წყარო. მე-2 ნახაზზე წარმოდგენილია ინფორმაციის წყაროების კლასიფიკაცია.



ნახ.2. რისკების მართვის სისტემის მიერ გამოყენებული ინფორმაციის წყაროები

საწარმოს ინფორმაციული რისკების შეფასებისას საფუძვლიანად უნდა იქნას მოკვლეული ინფორმაციის შიდა და გარე წყაროები[4]. შეფასების პროცესი, რომელიც ძირითადად რისკების ხასიათის განსაზღვრაში მდგომარეობს, შეიძლება წარმოვადგინოთ მე-3 ნახაზზე გამოსახულ მოქმედებათა მიმდევრობის სახით:



ნახ.3. საწარმოს ინფორმაციული რისკების შეფასების ალგორითმი

რისკების შეფასების დასკვნით ეტაპზე უნდა შემუშავდეს რეკომენდაციები, რომელსაც შეასრულებს საწარმოს უსაფრთხოების განყოფილება. ამათგან მნიშვნელოვანია რისკების

შეფასების ყოველწლიური გეგმის შედგენა. დაგეგმვაზე, შესრულებაზე და ანალიზზე ზოგიერთ საწარმოს შეიძლება დასჭირდეს რამდენიმე თვე, რომლის შედეგადაც ცვლილებების გასატარებლად დარჩება ძალზედ მცირე დრო. ამიტომ მიზანშეწონილია ჩატარდეს უფრო ხშირი, მაგრამ ნაკლებმასშტაბური შეფასება, ხოლო სრული შეფასება განხორციელდეს პერიოდულად, არსებული პირობების თანახმად.

უსაფრთხოების განყოფილებამ რეგულარულად უნდა ჩაატაროს საწარმოს სისტემების მოწყვლადობათა შეფასება (სკანირება). თუ ძალიან ბევრი კომპიუტერია, მაშინ საჭიროა მათი დაჯგუფება და ნაწილ-ნაწილ სკანირება დროის მოკლე მონაკვეთებში, მაგალითად, ყოველი კვირის დასასრულს.

3. დასკვნა

რისკების შეფასების ზემოგანხილული მიდგომა საწარმოს ინფორმაციული უსაფრთხოების მიმდინარე მდგომარეობის დონის შეფასებას ან გადაფასებას უზრუნველყოფს. ამავდროულად იგი საშუალებას იძლევა შემუშავებულ იქნას რეკომენდაციები საწარმოს ინფორმაციული უსაფრთხოების ასამაღლებლად, შემცირდეს საწარმოს პოტენციური დანაკარგები, შემოთავაზებულ იქნას კავშირის ღია არხებით გადასაცემი კონფიდენციალური ინფორმაციის დაცვის გეგმები, დაცულ იქნას საწარმოს ინფორმაცია მიზანმიმართული განადგურებისაგან, არასანქცირებული წვდომისა და არაუფლებრივი გამოყენებისაგან.

ლიტერატურა

1. შონია ო., ჯანელიძე გ., მეფარიშვილი ბ. ინფორმაციული და ქსელური რესურსების უსაფრთხოების ურუნველყოფა, თბ., სტუ, 2009
2. Александрович Г. Я., Нестеров С. Н., Петренко С. А. Автоматизация оценки информационных рисков компании. “Конфидент” №2, М., 2006
3. Астахов А. М. Аудит безопасности информационных систем. Конфидент №6, М., 2007
4. Lam J. Enterprise Risk Management: From Incentives to Controls. John Wiley. ISBN 978-0-471-43000-1. 2003.

THE ENTERPRISE INFORMATION RISKS ANALYSE

Janelidze Gulnara, Meparishvili Nino
Georgian Technical University

Summary

The present paper is concentrated on the problems related to information security of enterprise, particularly of information risks detection and estimation algorithms. In every particular enterprise, the information risks can occur due to different and competitive environment. The timely detection or determination of the probability can reduce the possible damages. The proposed approach of analyses and information risks occurrence probability determination is based on the forecasting and computing all damages, provoked due to occurrence of the information risks thus ultimately leading to the sustainable development of enterprise and protection consumer rights and interests.

АНАЛИЗ ИНФОРМАЦИОННЫХ РИСКОВ ПРЕДПРИЯТИЯ

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

Резюме

Данная статья посвящается проблемам обеспечения информационной безопасности предприятия, в частности, выявления информационных рисков и разработки алгоритмов их оценки. Исходя из специфики деятельности, конкретное предприятие имеет свою отличительную среду. Кроме этого, из-за функционирования в конкурируюших условиях возникают некоторые информационные риски, своевременное выявление или определение их вероятностей в значительной мере может уменьшить всевозможные убытки. Представленный подход анализа характера и вероятностей возникновения информационных рисков в предприятии заключается в определении убытков в случае реализации информационных рисков, что, в свою очередь, может отразиться на устойчивом развитии объекта и на защите интересов клиентов.