ინფორმაციული უსაფრთხოების ეფექტური მართვის ამოცანები

შოთა ქვაჩაკიძე
სტუ-ს დოქტორანტი

რეზიუმე

ნაშრომის მიზანია ინფორმაციული უსაფრთხოების ეფექტური მართვის ორგანიზაციული მექანიზმების შემუშავება, კვლევა და დანერგვა.

დასახული მიზნის მიღწევა შემდეგი ამოცანების თანმიმდევრულ გადაწყვეტას მოითხოვს:

1. კორპორაციის ინფორმაციული უსაფრთხოების სპეციფიკის როგორც მართვის ობიექტის კვლევა.

ინფორმაციული უსაფრთხოების მართვის სისტემის თავისებურებების შესწავლა კორპორაციის ორგანიზაციულ სტრუქტურასთან დამოკიდებულებით. კორპორაციის ინფორმაციული უსაფრთხოების ორგანიზაციული მართვის ამოცანების კლასიფიკაციის სისტემის შემუშავება.

2. ინფორმაციული უსაფრთხოების მართვის ორგანიზაციული მექანიზმების მოდელების, ანალიზის მეთოდებისა და სინთეზის შემუშავება და კვლევა კორპორაციის ორგანიზაციულ სტრუქტურაზე დამოკიდებულებით, შემდეგი ტიპიური სტრუქტურისა და მათი შესაბამისი მოდელების ჩათვლით: ბიუროკრატიული („ძლიერი ცენტრი-სუსტი აგენტები"), გარდამავალი („საშუალო ცენტრი - საშუალო აგენტები"), და ორგანული („სუსტი ცენტრი-ძლიერი აგენტები").

3. კორპორაციის ინფორმაციული უსაფრთხოების ეფექტური კომპლექსური სისტემის აგების მეთოდების შემუშავება.

4. კორპორაციის საქმიანობაში შეთავაზებული ინფორმაციული მართვის ორგანიზაციული მექანიზმების დანერგვა. კვლევის ძირითადი მეთოდი მათემატიკური მოდელირებაა, რომელიც იყენებს სისტემური ანალიზის მიდგომებსა და ანალიზს, გადაწყვეტილებების მიღების თეორიებს, იმიტაციურ მოდელირებას, თამაშების თეორიებს და აქტიური სისტემების თეორიებს.

დღეისათვის, ბაზრის ძირითადი მოთხოვნა საწარმოებისა და ორგანიზაციების ეფექტურად მართვაა. მოდმივად მიმდინარე ცვლილებები (უპირველეს ყოვლის ეკონომიკურ სფეროში) ბიზნესის წარმოების სტრატეგიებისა და ტაქტიკის უწყვეტად სრულყოფასა და ძიებას მოითხოვენ. მეორეს მხრივ, თანამედროვე პირობებში ბიზნესის მართვა შეუძლებელია ინფორმაციული ტექნოლოგიების (იტ) გამოყენების გარეშე, რომლებიც თავის მხრივ ინტენსიურად ვითარდება ბიზნესის წინაშე მდგარი სტრატეგიული და ტაქტიკური ამოცანების ზემოქმედებით.

უკანასკნელ ათწლეულში იტ გამოყენების სფეროში ძირეული ცვლილებები მოხდა. ამ ცვლილებებმა მნიშვნელოვნად დადებითად იმოქმედა ბიზნესზე, მაგრამ სამაგიეროდ უსაფრთხოების სფეროსადმი მთავრობის, კომერციული საწარმოების, სხვა ორგანიზაციების, მომხმარებლების, ინფორმაციულ სისტემებისა და ქსელის შემმუშავებლებისაგან, მათდამი სერიოზული დამოკიდებულება მოითხოვეს. მოცემული პრობლემისადმი დაბალანსებული მიდგომის ძირითად ფაქტორებს შეიძლება მივაკუთნოთ, პირველ რიგში ინფორმაციული საფრთხეებისა და რისკების მოდმივად მზარდი რაოდენობა, ასევე არსებულ ინფორმაციულ სისტემებში (იტ) ინფორმაციული უსაფრთხოების არა დამაკმაყოფილებელი დონე.

ნებისმიერ ეკონომიკურ საქმიანობა თან ახლავს რისკი და ზარალის მიღების საფრთხე. დღეისათვის რისკების მრავალფეროვნებიდან შეიძლება განსაკუთრებით ინფორმაციული რისკები გამოიყოფა, რომელიც თანამედროვე იტ არსებული დაუცველობით წარმოიქმნება, ეკონომიკური სუბიექტის სხვადასხვა დონის საქმიანობის (მართველური, საწარმოო, გასაღების, ინვესტიციური, სავაჭრო, საკრედიტო) პროცესში.

თავის მხრივ ინფორმაციული რისკების არსებობა მართვას მოითხოვს. ინფორმაციული რისკების მართვა, სხვა სიტყვებით, ინფორმაციული უსაფრთხოების მართვა (რაც ISOjIEC 17799 საერთაშორისო სტანდარტების - „ინფორმაცი-

ული უსაფრთხოების მართვა" - მიხედვით ინფორმაციის ისეთ დაცვას გულისხმობს, როგორიცაა კონფიდენციალურობა, მთლიანობა და ხელმისაწვდომობა), გულისხმობს ეკონომიკური ობიექტის სტაბილურობის უზრუნველყოფის შესაძლებლობას, არასასურველი სიტუაციებისადმი წინააღმდეგობის გაწევის უნარს. ინფორმაციული რისკების შემცირების მეთოდოლოგიის შემუშავება ზოგადად ამაღლებს საწარმოს უსაფრთხოებას.

მაგრამ ხშირად იქმნება სიტუაცია, როცა ფინანსური, ან სხვა რესურსები არ არის საკმარისი ყველა პრობლემის მოსაგვარებლად და საჭირო ხდება ინფორმაციული რისკების პრობლემების ეტაპობრივი გადაჭრა, ან ცალკეული საფრთხეების წინააღმდეგ ბრძოლა. ამრიგად, ორგანიზაციის ხელმძღვანელი ინფორმაციული რისკების შემცირებისათვის რესურსების ოპტიმალურად განაწილების ამოცანის წინაშე დგება.

ინფორმაციული რისკების მართვის საკვანძო ელემენტი ამ რისკების შემცირების კონკრეტული კონტრქმედებების განხორციელების ეფექტური მეთოდოლოგიაა, რომელიც იტ საფრთხეებისა და დაუცველობის აღმოფხვრას ემსახურება. ასეთი მეთოდოლოგიის საფუძველი არსებული რესურსების (ფინანსური, ორგანიზაციული, ტექნოლოგიური და სხვ.) ეფექტურად გამოყენების მექანიზმი უნდა იყოს, რომლებიც, როგორც წესი, ყოველთვის დეფიციტს წარმოადგენენ.

ინფორმაციული რისკები ცალკე კატეგორიად ან ძალიან ვიწრო კუთხით არ განიხილება, იგი განიხილება ინფორმაციის კონფიდენციულურობის დარღვევის რისკად განიხილება.

ინფორმაციული უსაფრთხოების (Information Security Management) მართვა ის სფეროა, რომლის აუცილებლობა თეორიულად სულ ცოტა ხნის წინ გაცნობიერდა. ამ სფეროში პირველი კვლევები პირველად 1980 იანი წლების ბოლოს დაიწყო, 1990 იანი წლების ბოლოს კი პირველად გამოჩნდა ეროვნული და საერთაშორისო სტანდარტები ამ სფეროში (ISO/IEC 17799, BSI). მაგრამ სტანდარტების გაჩენის ფაქტი სულაც არ ნიშნავს, რომ ინფორმაციული უსაფრთხოების სფეროში ყველა პრობლემა გადაწყვეტილია. პირიქით, ინფორმაციული უსაფრთხოების მართვის ამოცანები ყოველდღიურად რთულდება ადამიანის საქმიანობის ყველა სფეროში იტ ინტენსიურ გამოყენებასთან დაკავშირებით.

როგორც წესი, ივარაუდება, რომ არსებობს ინფორმაციული უსაფრთხოების სისტემის აგებისათვის საჭირო რესურსები. ინფორმაციულ რისკებთან დაკავშირებული ზარალის შემცირების ამოცანა საერთო რაოდენობის რესურსების ოპტიმიზაციის ამოცანად განიხილება, რომელიც ინფორმაციული რისკების დასაშვებ დონემდე შემცირების კონტრქმედებებისათვის აუცილებელი რესურსების ოპტიმიზაციას სჭირდება.

ამრიგად, შეიძლება ითქვას, რომ დღეისათვის კორპორატიული რესურსების დეფიციტის პირობებში ინფორმაციული რისკების ორგანიზაციული მართვის პრობლემა არა საკმარისად არის შესწავლილი, რაც განაპირობებს ამ ნაშრომის აქტუალურობას, რამეთუ იგი ეძღვნება კორპორაციის ინფორმაციული უსაფრთხოების მართვის ორგანიზაციული მექანიზმების (ორგანიზაციაში მმართველური გადაწყვეტილებების მიღების პროცედურების) შემუშავებასა და კვლევას.

გამოყენებული ლიტერატურა

1. საქართველოს იუსტიციის სამინისტრო - „ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთხოების მართვის წესები და ნორმები". 2011 წ. თბილისი.

2. Анисимов, А.А. Менеджмент в сфере информационной безопасности Текст. : учеб. пособие / А.А. Анисимов; Интернет-университет информационных технологий ИНТУИТ.ру, БИНОМ. Лаборатория знаний. - М. - 2010. - 176 с.

ЭФФЕКТИВНЫЕ ЗАДАЧИ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ШОТА КВАЧАКИДЗЕ
Докторант ГТУ

Резюме

Цель данной работы разработка, исследование и внедрение эффективных организационных механизмов управления информационной безопасности.

Достижение намеченной цели требует последовательного решения следующих задач:

1. Исследование специфики информационной безопасности корпорации как объекта управления;

Изучение особенности систем информационной безопасности в зависимости от организационных структур корпорации. Разработка квалификаций систем для организационного управления информационной безопасности корпорации.

2. Разработка и исследование моделей организационных механизмов управления, методов анализа и синтеза в зависимости от организационной структуры корпорации включая следующих типичных структур и их соответствующих моделей: бюрократический («сильный центр- слабые агенты»), переходный («Средний центр - средние агенты»), органический («Слабый центр- сильные агенты»)

3. Разработка методов построения эффективных комплексных систем информационной безопасности корпорации.

4. Внедрение в корпорации предложенных организационных механизмов управления информацией. Основной метод исследования математическое моделирование, которое использует подходы системного анализа, теории принятия решении, имитационное моделирование, теорию игр и теории активных систем.