საწარმოს ინფორმაციული უსაფრთხოება, როგორც მისი ეკონომიკური უსაფრთხოების უზრუნველყოფის ერთ-ერთი უმთავრესი მდგენელი

კორნელი ოდიშარია, სალომე ოდიშარია, ნანა მაღლაკელიძე
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია თუ რამდენად მნიშვნელოვანია თანამედროვე საწარმოს ეკონომიკური უსაფრთხოების (ეკუ) უზრუნველყოფისას ინფორმაციის დაცვის პრობლემების გათვალისწინება. ეკონომიკა დღეს განვითარების ინოვაციურ სტადიაზეა და საწარმოს ეფექტური ფუნქციონირებისათვის აუცილებელი ინსტრუმენტია ავტომატიზებული საინფორმაციო სისტემის გამოყენება, რომელიც სერიოზულ საშუალებას წარმოადგენს ეკუ უზრუნველსაყოფად ინფორმაციული უსაფრთხოების სისტემის გამოყენებით.

საკვანძო სიტყვები: საწარმო. ეკონომიკური უსაფრთხოება. ავტომატიზაცია. საინ-ფრმაციო სისტემა. ინფორმაციული უსაფრთხოება. საფრთხე. სიტუაციური მართვა.

1. შესავალი

უნდა აღინიშნოს, რომ ეკონომიკურ თემათიკასთან დაკავშირებულ სამეცნიერო ნაშრომებში საერთოდ არაა მსჯელობა საწარმოს ინფორმაციულ უსაფრთხოებაზე (იუ). ჩვენი აზრით, თანამედროვე ავტომატიზებული მართვის საინფორმაციო სისტემების ტოტალური განვითარება – დანერგვის პირობებში, საწარმოს იუ უნდა განვიხილოთ როგორც საწარმოს ეკუ უზრუნველყოფის ერთ-ერთი უმთავრესი მდგენელი.

ჩატარებული ანალიზის საფუძველზე, სისტემური მიდგომის პრინციპებიდან გამომდინარე, საწარმოს ეკონომიკურ უსაფრთხოებას ასე განვმარტავთ: საწარმოს ეკონომიკური უსაფრთხოება არის კორპორატიული რესურსების ყველაზე ეფექტური გამოყენების მდგომარეობა, გარემოს ფაქტორების – პარამეტრების გათვალისწინებით, საწარმოს სტაბილურად ფუნქციონირების უზრუნველსაყოფად მიმდინარე პერიოდში და მომავალში. საწარმოს ეკონომიკური უსაფრთხოება (სეუ) – კი არის პროცესი, რომელიც ხასიათდება ხარისხობრივი და რაოდენობრივი მაჩვენებლების ერთობლიობით, რომელთა შორისაც უმთავრესია ეკონომიკური უსაფრთხოების დონე.

ეკონომიკის განვითარების თანამედროვე ეტაპის თავისებურებაა ინდუსტრიული ტექნოლოგიების შეხამება საინფორმაციო-კომუნიკაციურ ტექნოლოგიებთან. უფრო მეტიც, დღეისათვის საწარმოები არსებობასაც კი ვერ შეძლებს თუ ისინი არ გამოიყენებს მართვის საინფორმაციო სისტემებს. აშკარაა, რომ საწარმოს ეკონომიკური უსაფრთხოების უზრუნველყოფა გულისხმობს მისი სტრატეგიული და მიმდინარე მიზნების რეალიზა-ციისათვის დანერგილი ყველა სახის ფუნქციების შესაბამისი ხარისხით რეალიზებას, რაც ასევე გულისხმობს საწარმოო პროცესების და მთლიანობაში საწარმოს სტაბულურ, სერიოზული ზარალის გარეშე მოღვაწეობას გარეშე და შიგა ხელშემშლელი ფაქტორების, მუქარების არსებობისას. ფაქტია, საწარმოს ხელმძღვანელობას მკაფიოდ უნდა ქონდეს წარმოდგენილი საწარმო, როგორც რთული სისტემა და სისტემურ მართვასთან ერთად შეეძლოს ეფექტური რეაგირება წარმოქნილ, პროგნოზირებულ მუქარებზე. ეს კი მოითხოვს მართვის ურთულესი მეთოდის – სიტუაციური მართვის გამოყენებას [1].

თანამედროვე განვითარების ინოვაციურ ეტაპზე სიტუაციური მართვა შეუძლებელია ავტომატიზებული საინფორამციო-საკომუნიკაციო სისტემების გამოყენების გარეშე. საწარმოს კორპორაციული ქსელი მძლავრი ინსტრუმენტია საწარმოს ეფექტური სიტუაციური მართვისათვის საჭირო მონაცემების, ინფორმაციის შესაგროვებლად. გარდა ამისა ის საშუალებას იძლევა მოხდეს ცალკეული სამართავი პროცესების მოდელირება, სხვადასხვა მავნე ფაქტორების მათზე ზემოქმედების გათამაშება, სტატისტიკური მონცემების შეგროვება, და რაც მთავარია, მიღებული გამოცდილების საფუძველზე შეიქმნას სხვადასვა სიტუაციის მართვის ცოდნის ბაზა, რაც მნიშვნელოვანი საყრდენი იქნება მომავალში მსგავსი სიტუაციების ეფეტური მართვისათვის, რა თქმა უნდა, ადაპტირების ჩათვლით. ამგვარი მსჯელობის საფუძველზე აშკარაა თუ რამდენად სასიცოცხლო მნიშნელობა აქვს საწარმოს მართვის ავტომატიზებული სისტემის შექმნა-დანერგვა-გამოყენებას თანამედროვე საინფორმაციო ტეაქნოლოგიების ბაზაზე და მათი ინფორმაციული უსაფრთხოების უზრუნველყოფას.

ფაქტია, რომ ცოდნაზე დამყარებული ეკონომიკის, ანუ უკანასკნელ წლებში მსოფლიო ეკონომიკურ ლიტერატურაში გავრცელებული ინტელექტუალური ეკონომიკის ცნება, რომელიც, პირველ რიგში, დაფუძნებულია ეკონომიკის ინფორმატიზაციაზე, იმ გარემოების აღიარებას ასახავს, რომ მეცნიერული ცოდნა ეკონომიკური ზრდის პარამეტრებს უშუალოდ განსაზღვრავს და ინოვაციებისა და კვალიფიციური მუშახელის შექმნის საფუძველს ქმნის. ფაქტია ის, რომ ამჟამად, გადამამუშავებელი მრეწველობისა და მომსახურების სფეროს მეცნიერებატევადი დარგების წილად საშუალოდ წამყვანი ინდუსტრიული ქვეყნების მშპ–ის დაახლოებით ნახევარი მოდის [2].

ამრიგად, თანამედროვე საწარმოს ეფექტური ფუნქციონირების, მისი ეკონომიკური უსაფრთხოების მთავარი საყრდენი ინსრუმენტი კორპორაციული ქსელია. აქვე უნდა აღვნიშნოთ, რომ ბიზნესში საინფომაციო ტექნოლოგიების გამოყენებამ, უდიდეს პროგრესთან ერთად, დაბადა ურთულესი პრობლემა, რომელიც დაკავშირებულია ავტომატიზებულ საინფორმაციო სისტემაში ცირკულირებული მონაცემების, ინფორმაციის, ცოდნის ბაზის და სხვა რესურსების უსაფრთხოების უზრუნველყოფასთან. თანამედროვე ეტაპზე ფაქტია, რომ თუ საწარმოში არ იქნება სრულად გათვალისწინებული მართვის საინფორმაციო სისტემის, და ზოგადად, თვით საწარმოს მთლიანობაში, ინფორმაციული უსაფრთხოების მაღალ დონეზე უზრუნველყოფის აუცილებლობა, მაშინ ის არესებობასაც კი ვერ შეძლებს [3-5].

2. ძირითადი ნაწილი

როგორც ჩატარებულმა გამოკვლევებმა გვიჩვენა, სამეცნიერო ნაჩრომებში, რომლებიც ეძღვნება ნებისმიერი დონის მეურნე სუბიექტების *ეკონომიკური უსაფრთხოების* საკითხებს, ნაკლები ყურადღება ექცევა მათი *ინფორმაციული უსაფრთხოების უზრუნველყოფის* აუცილებლობას.

თანამედროვე ინტელექტუალურ ეკონომიკურ სფეროში ინფორმაციის დაცვის პრობლემას შეუძლებელია ეწოდოს გამოგონილი. ყველგან გვესმის ბიზნეს სივრცეში გამოყენებული ინფორმაციული სისტემების „გატეხვების“ შესახებ, ზიანის მომტან პროგრამულ-ტექნიკურ უზრუნველყოფებზე, მუქარებზე და მათი განხორციელებით მთელი ქვეყნის მასშტაბით მიყენებულ ზარალზე და სხვ.

რეალობაა ის, რომ სახელმწიფო, საწარმოები და სხვა სუბიექტები სერიოზულ ყურადღებას უნდა აქცევდეს თავიანთი საქმიანობის ინფორმაციული უსაფრთხოების უზრუნველყოფას. ამ საკითხის უდიდესი პრობლემურობიდან გამომდინარე, ჩვენ ნაშრომში ყურადღებას დავუთმობთ იმის დადგენას, თუ რა უნდა გააკეთოს პირველ რიგში მეურნე სუბიექტმა-საწამომ საკუთარი საქმიანობის ინფორმაციული უსაფრთხოების უზრუნველსაყოფად.

ინფორმაციული უსაფრთხოება - ესაა ღონისძიებათა კომპლექსი, რომელთა შორისაც შეუძლებელია გამოიყოს მეტად ან ნაკლებად მნიშვნელოვანი. აქ ყველფერი მნიშვნელოვანია ! დაცვის ზომები უნდა იყოს გათვალისწინებული საწარმოს მიერ გამოყენებული მართვის კომპიუტერული ქსელის ყველა წერტილში, ნებისმიერი სუბიექტის ინფორმაციასთან მუშაობისას (ამ შემთხვევაში სუბიექტი – ეს სისტემის მომხმარებელი, პროცესი, კომპიუტერი ან პროგრამული უზრუნველყოფაა ინფორმაციის დამუშავებისათვის). ყოველი ინფორმაციული რესურსი, იქნება ეს მომხმარებლის კომპიუტერი, საწარმოს სერვერი ან ქსელური მოწყობილობა, უნდა იყოს დაცული ყველა შესაძლო მუქარისაგან. დაცული უნდა იყოს ფაილური სისტემები, მონაცემთა ბაზები, ქსელი და სხვ.

საერთო აღიარებით, 100%-იანი დაცვის უზრუნველყოფა შეუძლებელია. ამასთან ერთად უნდა გვახსოვდეს, რომ რაც უფრო მაღალია დაცულობის დონე, მით უფრო ძვირია სისტემა და მით უფრო მოუხერხებელი ხდება გამოსაყენებლად მომხმარებლისათვის, რაც, ცხადია, ხდება მიზეზი დაცვის გაუარესებისა ადამიანის ფაქტორის გავლენის შედეგად.

აღნიშნულიდან გამომდინარე საწარმომ აუცილებლად უნდა განახორციელოს ინფორმაციული უსაფრთხოების სფეროში თანამშრომლების ცოდნის შემოწმება და სწავლების განხორციელება. მიღებულია, რომ თანამშრომლებმა ხელმოწერით უნდა დაადასტურონ თავიანთი ვალდებულებები საკანონმდებლო მოთხოვნების შესაბამისად. ამასთან ერთად, აუცილებლად მიგვაჩნია საწარმომ მაქსიმალურად გააცნობიეროს და გაითვალისწინოს მსოფლიოში აღიარებული Toyota-ს ფენომენი – ყოველთვის იზრუნოს თავისი თანამშრომლების პოზიტიური განწყობისათვის. ამით იმის დასაბუთება გვსურს, რომ თანამშრომლები ყოველ სწავლებას, სიახლეების დანერგვა–ათვისება–გამოყენებას პოზიტიურად შეხედავენ თუ ეს იქნება საწარმოს მიერ წახალისებული. საწარმომ პერსონალის მართვისას მუდმივად უნდა იზრუნოს საკუთარი ემოციური კომპეტენტურობის განვითარებასა და თანამშრომლებისადმი სწორი მიდგომის უნარის ჩამოყალიბებაზე [6].

პერსონალის მართვა იწყება ახალი თანამშრომლის მიღებისას და უფრო ადრეც – თანამდებობის აღწერით და მისი მაქსიმალურად ეფექტურად განმახორციელებლი მომავალი თანამშრომლის მოდელის შექმნით. უკვე ამ ეტაპზევეა სასურველი როგორც ეკონომიკური, ასევე ინფორმაციული უსაფრთხოების სპეციალისტების ჩართვა, რათა გაირკვეს ის კომპიუტერული და სხვა პრივილეგიები, რომლებიც ასოცირდება მოცემულ თანამდებობასთან [7].

არსებობს ორი საერთო პრინციპი, რომლებიც მხედველობაში უნდა იქნას მიღებული: 1) მოვალეობების გამიჯვნა; 2) პრივილეგიების მინიმიზება.

მოვალეობების გამიჯვნის პრინციპი აწესებს ისე განაწილდეს როლები და პასუხისმგებლობები, რომ ერთმა ადამიანმა ვერ შეძლოს საწარმოსათვის კრიტიკულად

მნიშვნელოვანი პროცესის მოშლა. მაგალითად, არასასურველია სიტუაცია, როდესაც საწარმოს მსხვილი გადასახადების შესრულება ხდება ერთი ადამიანის მიერ. უფრო საიმედოა ერთ ადამიანს დაევალოს გაფორმება განაცხადისა მსგავს გადასახადზე, ხოლო სხვას დაევალოს ამ განაცხადის დადასტურება. ასეთ შემთხვევაში კრტიკულად მნიშვნელოვანი მოქმედებები მსს ადმინისტრირების ხაზით შესაძლებელია შესრულდეს მხოლოდ ორივე პირის ერთდროული თანხმობით, რაც ამცირებს შეცდომების და ბოროტმოქმედების ალბათობას.

პრივილეგიების მინიმიზირების პრინციპი აწესებს მომხმარებლებს გამოეყოთ დაშვების მხოლოდ ის უფლებები, რომლებიც აუცილებელია მათ მიერ სამსახურებრივი მოვალეობების შესასრულებლად. ამ პრინციპის დანიშნულება ცხადია – შემცირდეს ზარალი შემთხვევითი ან წინასწარგანზრახული არაკორექტული მოქმედებებით.

როგორც აღვნიშნეთ, თანამდებობის აღწერის წინასწარი შედგენა საშუალებას იძლევა შეფასდეს მისი კრიტიკულობა და ფორმირებულ იქნას კანდიდატების შემოწმების და შერჩევის პროცედურები. რაც უფრო საპასუხისმგებლოა თანამდებობა, მით უფრო გულდასმით უნდა შემოწმდეს კანდიდატები: მოგროვდეს მათზე ცნობები, შესაძლოა ჩატარდეს გასაუბრებები ყოფილ თანამშრომლებთან და სხვ. მსგავსი პროცედურა შეიძლება იყოს ხანგრძლივი და ძვირი, ამიტომ არა აქვს აზრი ზედმეტად გართულებას. ერთდროულად არაა გამართლებული სულ უარი ითქვას შემოწმების ჩატარებაზე, რათა არ მოხდეს შემთხვევითი მიღება სამუშაოზე ადამიანისა კრიმინალური წარსულით ან ფსიქიკური გადახრებით.

როდესაც კანდიდატი განსაზღვრულია, მან, უნდა გაიაროს სწავლება; უკიდურეს შემთხვევაში მას დეტალურად უნდა განემარტოს სამსახურებრივი მოვალეობები, ასევე ინფორმაციული უსაფრთხოების ნორმები და მისი სისტემური ანგარიშის შესასვლელის სახელი, პაროლი და პრივილეგიები შეტანამდე.

მისი სისტემური ანგარიშის შეტანისთანავე იწყება საწარმოს მსს–ში მისი ადმინისტრირება, აგრეთვე მომხმარებლის მოქმედებების პროტოკოლირება (ოქმის შედგენა) და ანალიზი. თანდათან ხდება გარემოცვის შეცვლა, რომელშიც მუშაობს მომხმარებელი, ასევე მისი სამსახურებრივი მოვალეობების და ა.შ. ყოველივე ეს კი მოითხოვს პრივილეგიების თანდათანობით შეცვლას. ტექნიკურ სირთულეს ქმნის მომხმარებლის დროებითი გადაადგილება, მის მიერ დროებით სხვა მოვალეობების შესრულება, საქმე ეხება უფლებამოსილებათა მინიჭებას, ხოლო გარკვეული დროის შემდეგ მის ჩამორთმევას. ასეთ პერიოდში მომხმარებლის აქტიურობის პროფილი მკვეთრად იცვლება, რაც ქმნის სირთულეებს საეჭვო სიტუაციების გამოვლენისას, არ უნდა იქნას დავიწყებყლი მსს–ში ძველი დაშვების უფლებების ლიკვიდაცია.

მომხმარებლის სისტემური ანგარიშის ლიკვიდაცია, განსაკუთრებით კონფლიქტისას (მომხმარებელს) თანამშრომელსა და საწარმოს შორის, უნდა ჩატარდეს მაქსიმალურად ოპერატიულად (ფაქტობრივად, ერთდროულად დასჯის ან განთავისუფლების შეტყობინების მიწოდებასთან ერთად). შესაძლებელია ფიზიკური შეზღუდვაც სამუშაო ადგილთან მისვლაზე. ცხადია, თუ ხდება თანამშრომლის დათხოვნა, მისგან უნდა იქნას მიღებული მისი მთელი კომპიუტერული მეურნეობა.

თანამშრომლების მართვას ესაზღვრება ადმინისტრირება პირებისა, რომლებიც მუშაობენ კონტრაქტით. მაგალითად: ა) აუდიტორი ან აუდიტორული ფირმის წარმომადგენლები, რომლებიც ახორციელებენ საწარმოში აუდიტორულ კვლევას და შესაბამისი დასკვნის მომზადებას, საამისოდ მათ სჭირდებათ საწარმოს მსს-ში შესაბამის ელექტრონულ მონაცემებთან, დოკუმენტებთან დაშვება; ბ) საწარმოს მსს-თვის საჭირო პროგრამული, ტექნიკური და სხვა საშულებების მომწოდებელი ფირმის სპეციალისტები, რომლებიც ახორციელებენ მათ დანერგვა–გაშვებას და სხვ.

პრივილეგიათა მინიმიზების პრინციპით საწარმოს მსს-თან მუშაობისას მათ უნდა მიენიჭოთ ის მინიმალური უფლებები, რომლებიც საჭიროა მათი მოვალეობების შესასრულებლად და მოხდეს მათი დაუყოვნებლივ გაუქმება კონტრაქტის დასრულებასთან ერთად. ოღონდ პრობლემა მდგომარეობს იმაში, რომ ამ დროს „გარეშე“ თანამშრომლები ადმინისტრირებდნენ იქნება „ადგილობრივებს“, და არა პირიქით. აქ პირველ პლანზე გამოდის საწარმოს ამ პროცესებში ჩართული თანამშრომლების კვალიფიკაცია, მათი უნარი (საკუთარი ცოდნა–გამოცდილებით) სწრაფად გაერკვნენ აუდიტით გამოვლენილ პრობლემურ საკითხებში, სწრაფად დაეუფლონ შემოტანილ სიახლეებს, ასევე სასწავლო კურსების ოპერატიული ჩატარება. ძალზე მნიშვნელოვანია საქმიანი პარტნიორების შერჩევის პრინციპებიც.

განსაკუთრებული ყურადღება გვინდა მივაქციოთ იმ გარემოებას, რომ თანამედროვე საწარმოს კორპორაციული ქსელების უსაფრთხოების კომპლექსურ სისტემაში დანერგილია და ფართოდ გამოიყენება *ოქმის შედგენის აუდიტის რეალიზაციის* ქვესისტემა, რომელიც წარმატებით შეიძლება გამოყენებულ იქნას საწარმოს ეკუ-ის უზრუნველყოფის სამსახურის მიერ. ოქმის შედგენა ინფორმაციულ სისტემაში მიმდინარე მოვლენების შესახებ ინფორმაციის შეგროვება და დაგროვებაა. აქ იგულისხმება მოქმედებები, რომლებიც დაკავშირებულია ნებისმიერ მონაცემებთან, ინფორმაციულ მასივებთან, ცოდნის ბაზებთან, სხვადასხვა სერვის–პროგრამის გამოყენებასთან და ა.შ., სისტემაში მომუშავე საწარმოს თანამშრომლების, შიგა და გარე მომხმარებლის ადმინისტრატორების მხრიდან.

აუდიტი ესაა ოქმის მეშვეობით დაგროვილი ინფორმაციის ანალიზი, რომელიც სრულდება ოპერატიულად, რეალურ დროში ან პერიოდულად (მაგალითად, ერთხელ დღეში და ა.შ.). აუდიტი აუცილებლად უნდა იყოს აქტიური. რაც იმას ნიშნავს, რომ ავტომატური რეჟიმით ხდებოდეს საშიში, არასწორი, ზიანის მომტან სიტუაციაზე რეაქცია.

ოქმის შედგენა და აუდიტი წყვეტს შემდეგ ამოცანებს:

– მომხმარებლის და ადმინისტრატორის ანგარიშვალდებულობის უზრუნველყოფა;

– მოვლენათა თანმიმდევრობის რეკონსტრუქციის შესაძლებლობის უზრუნველყოფა;

– ინფორმაციული უსაფრთხოების დარღვევის მცდელობის აღმოჩენა და მისი ეკუ–სთან კავშირის მითითება;

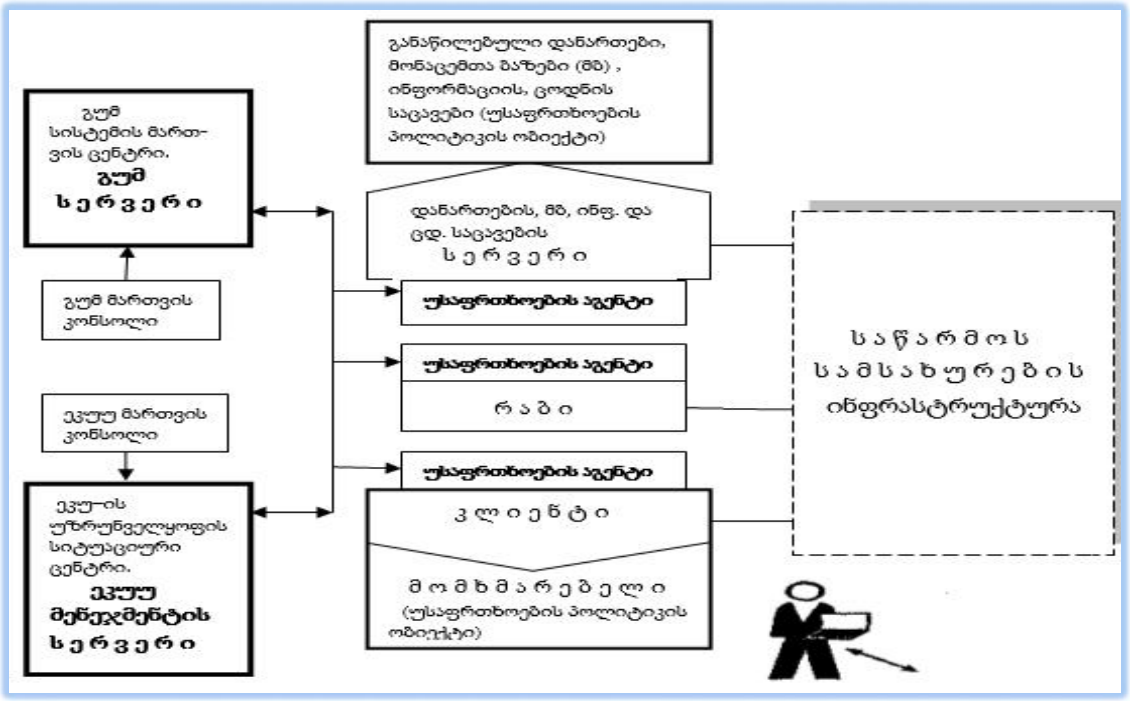
– პრობლემების გამოვლენისა და ანალიზისათვის ინფორმაციის მიწოდება იუ-ის და ეკუ-ის სისტემების მენეჯერებისათვის.

ოქმის შედგენა თავისი რეალიზაციისათვის მოითხოვს საკმაოდ დაკვირვებულ და აზრიან მიდგომას. რა მოვლენები უნდა იქნას დარეგისტრირებული? დეტალიზაციის რა ხარისხით? მსგავს შეკითხვებზე არ არსებობს ცალსახა პასუხი. აუცილებელია თვალყური მიედევნოს იმას, რომ ერთი მხრივ, მიღწეულ იქნას ზევით ჩამოთვლილი მიზნები, ხოლო

მეორე მხრივ, ამ დროს რესურსების ხარჯვა იყოს დასაშვებ ფარგლებში. ზედმეტად ფართო და დეტალური ოქმის შედგენა არა მარტო აქვეითებს სერვისების წარმადობას, რაც უარყოფითად მოქმედებს ხელმისაწვდომობაზე, ანუ საწარმოს სხვადასხვა დონის მენეჯერებისათვის ქმნის სირთულეებს, ასევე ართულებს აუდიტსაც, ე.ი. კი არ ზრდის არამედ აქვეითებს ინფორმაციულ უსაფრთხოებას, რაც სერიოზულ პრობლემად იქცევა საწარმოს ეკუ–ის უზრუნველყოფის სისტემისათვის.

აქვე უნდა ავღნიშნოთ, რომ საწარმოს მსს-ში ნებისმიერი აქტიურობა, რომელიც არ შეესაბამება უსაფრთხოების პოლიტიკას, მიზანშეწონილია დაიყოს შეტევებად, რომლებიც მიმართულია უკანონოდ უფლებამოსილების მისაღებად და მოქმედებებად, რომლებიც სრულდება არსებული უფლებამოსილების ფარგლებში, მაგრამ არღვევენ უსაფრთხოების პოლიტიკას. არატიპური ქცევის გამოვლენა შესაძლებელია სტატისტიკური მეთოდებით. მარტივ შემთხვევაში შეიძლება გამოყენებულ იქნას ზღურბლების სისტემა, რომელთა გადამეტებაც ითვლება შეტევად.

აქტიური აუდიტის საშუალებები შეიძლება განლაგებული იყოს მსს დაცვის ყველა ხაზზე. საკონტროლო ზონის საზღვარზე მათ შეუძლია აღმოაჩინოს საეჭვო აქტივობები გარეშე ქსელებთან მიერთების წერტილებში. მსს-ში, ანუ შიგა ქსელში აუდიტს შეუძლია აღმოაჩინოს და აღკვეთოს გარეშე და შიგა მომხმარებლების საეჭვო აქტივობები, გამოავლინოს პრობლემები სერვისების მუშაობაში, გამოწვეული როგორც უსაფრთხოების დარღვევით, ასევე აპარატურულ-პროგრამული შეცდომებით. მნიშვნელოვანია იმის აღნიშვნა, რომ აქტიურ აუდიტს, პრინციპში, შეუძლია უზრუნველყოს დაცვა დაშვებადობაზე შეტევებისაგან. საწარმოს სიტუაციურ ცენტრს პირდაპირი კავშირი უნდა ჰქონდეს მსს-თან და მისი ინფორმაციული უსაფრთხოების საშუალებების მართვის ცენტრთან (ნახ.1).



ნახ.1. საწარმოს იუ და ეკუ მართვის სისტემის საერთო სქემა

ძირითადი დაცვის საშუალებების დანიშნულებაა:

– უსაფრთხოების აგენტი, რომელიც დაყენებულია მომხმარებლის პერსონალურ კომპიუტერზე, ორიენტირებულია ინდივიდუალური მომხმარებლის დაცვაზე, მისი მოქმედებების კონტროლზე და დარღვევების და სხვა საგანგაშო მოვლენების, მდგომარეობების შესახებ შეტყობინების მიწოდებაზე მართვის ცენტრებისათვის. როგორც წესი, მომხმარებელი გვევლინება კლიენტის-სერვერ დანართებში;

– უსაფრთხოების აგენტი, რომელიც დაყენებულია დანართების, მონაცემთა ბაზების, ინფორმაცის და ცოდნის ბაზის სერვერზე, ორიენტირებულია განაწილებული დანართების სერვერული კომპონენტების დაცვაზე;

– უსაფრთხოების აგენტი, რომელიც დაყენებულია რაბ–კომპიუტერზე, უზრუნველყოფს საწარმოს შიგნით ან საწარმოებს შორის ქსელის სეგმენტების განმხოლოებას.

მართვის ცენტრი უზრუნველყოფს ქსელის მასშტაბში უსაფრთხოების პოლიტიკის აღწერას ეკუ-ის მენეჯმენტთან ერთად, მის შენახვას და გლობალური პოლიტიკის ტრანსლირებას დაცვის მოწყობილობების ლოკალურ პოლიტიკებში, დაცვის მოწყობილობების ჩატვირთვას და სისტემის ყველა აგენტის მდგომარეობის კონტროლს. საწარმოს უსაფრთხოების მართვის განაწილებული სქემის ორგანიზებისათვის გლობალური უსაფრთხოების მენეჯმენტის სისტემაში (გუმ) შესაძლებელია რამდენიმე გუმ-სერვერის დაყენება. გუმ შემადგენლობაში ცალკე უნდა იყოს ეკუუ-მენეჯმენტის სერვერი.

მართვის კონსოლი განკუთვნილია სისტემის ადმინისტრატორის სამუშაო ადგილის ორგანიზებისათვის. ყოველი გუმ-სერვერისათვის შესაძლებელია დაყენებულ იქნას რამდენიმე კონსოლი, რომლებიც მომართულია გუმ-სისტემის ადმინისტრატორთა როლების შესაბამისად.

უსაფრთხოების ლოკალური აგენტი პროგრამაა, რომელიც ყენდება ბოლო მოწყობილობებზე (კლიენტზე, რაბზე, სერვერზე) და ასრულებს იუ და ეკუ უზრუნველყოფისათვის შემდეგ აუცილებელ ფუნქციებს:

– უსაფრთხოების პოლიტიკის ობიექტების აუთენტიფიკაცია, აუთენტიფიკაციის სხვადასხვა სერვისის ინტეგრაციის ჩათვლით;

– მომხმარებლების განსაზღვრა სისტემასა და მოვლენებში, რომლებიც დაკავშირებულია მოცემულ მომხმარებლებთან;

– უსაფრთხოებისა და დაშვების კონტროლის საშუალებების ცენტრალიზებული მართვის უზრუნველყოფა;

– რესურსების მართვა დანართების ინტერესის მიხედვით, გამოყენებითი დონის რესურსებთან დაშვების მართვის მხარდაჭერა;

– ტრაფიკის დაცვა და აუთენტიფიკაცია;

– ტრაფიკის გაფილტვრა;

– მოვლენების ოქმის შედგენა, აუდიტი, საგანგაშო სიგნალიზაცია.

ლოკალური აგენტის ცენტრალური ელემენტია უსაფრთხოების ლოკალური პოლიტიკის პროცესორი, რომელიც ახდენს უსაფრთხოების ლოკალური პოლიტიკის ინტერპრეტაციას და გამოძახებათა განაწილებას დანარჩენ კომპონენტებს შორის.

აუცილებელია, რომ იუ-ის და ეკუ-ის მენეჯმენტის სამსახურები სრული შეთანხმებულობით მუშაობდეს და ქმნიდეს საწარმოს გლობალური უსაფრთხოების პოლიტიკას.

საწარმოს ეკუ-ის მენეჯმენტის სამსახურმა, სიტუაციურ ცენტრთან ერთად, მკაფიოდ უნდა განსაზღვროს საწარმოს მსს-ში განთავსებული, დამუშავების პროცესში გამოყენებული მონაცემების, ცოდნის მოდელების, დოკუმენტების, საინფორმაციო ფაილების და სხვა დაცვის ობიექტების კატეგორირება ხელმისაწვდომობის, კონფიდენციალობის, ურღვევობის მაჩვენებლებით და გამოყოს განსაკუთრებით კრიტიკულები, რომელთათვისაც აღნიშნული მაჩვენებლების დარღვევა გამოიწვევს საწარმოს ეკონომიკურ ზარალს. აუცილებელია თითოეული დაცვის i-ური ობიექტისათვის განისაზღვროს ზარალის მაქსიმალური მნიშვნელობა Δq_{ii} და ჯამური ზარალი

$$W = \sum_{i=1}^{n} \Delta q_{ii} \quad (1)$$

რომელიც შეიძლება დამანგრეველი იყოს საწარმოსათვის.

ამის შემდეგ გუმ სამსახურმა უნდა განსაზღვროს: ყოველი i-ური ობიექტის შესაძლო მუქარები, რომლებსაც, ზოგადად რომ ვთქვათ, ბოროტგანმზრახველი (სუბიექტი, რომელიც დაიტერესებულია საწარმოს მსს-ში თავისი მოქმდებებით მიიღოს სარგებელი, ზიანი მიაყენოს მთელ საწარმოს და სხვ.) შესაბამისი წყაროების მეშვეობით აგენერირებს მუქარებს მსს-ის წინააღმდეგ (ვთქვათ, ყოველი i-ური დაცვის ობიექტისათვის მუქარების ერთობლიობა არის სასრული და თვლადი, m = $\overline{1,M}$); ყოველი m-ური მუქარის გამოჩენის $P_{ii\ \ მუქ}$ ალბათობა და მის მიერ მიყენებული შესაძლო ზარალი $\Delta q_{ii}^{მუქ}$. I-ური დაცვის ობიექტის წინააღმდეგ მიმართული m-ური მუქარების რეალიზაციით გამოწვეული ჯამური ზარალი შეიძლება იყოს

$$\sum_{m=1}^{M} \Delta q_{ii}^{მუქ} \leq \Delta q_{ii} \quad (2)$$

საწარმოს მსს გლობალური დაცვის სისტემის მთავარი ფუნქციაა მოახდინოს ყოველი i-ური დაცვის ობიექტის m-ური მუქარის თავიდან აცილება, რაც აისახება თავიდან აცილებული ზარალის სახით $\overline{W_i}$:

$$\overline{W_i} = F_i(P_{ii\ \ მუქ}; \Delta q_{ii}^{მუქ}; P_{ii}^{აღმ}{}_{მუქ}; m=\overline{1,M}), \quad (3)$$

სადაც $P_{ii}^{აღმ}{}_{მუქ}$ – არის m-ური მუქარის აღმოფხვრის ალბათობა. ინფორმაციული უსაფრთხოების სფეროში აღიარებულია, რომ დაცვის სისტემას 100%-ით არ შეუძლია ნებისმიერი მუქარის აღმოჩენა და თავიდან აცილება, თუმცა აუცილებლად ხდება მისი მაქსიმალური მნიშვნელობის მისაღწევად შესაბამისი დაცვის ღონისძიებების გატარება და ხდება ამ დროს არსებული რისკის შეფასება. თავიდან აცილებული ზარალი m-ური მუქარის აღმოფხვრით განისაზღვრება შემდეგი გამოსახულებით:

$$\overline{\omega_m} = P_{ii\ \ მუქ} \cdot \Delta q_{ii}^{მუქ} \cdot P_{ii\ \ მუქ}^{აღმ} \quad (4)$$

i–ურ ობიექტზე m–ური მუქარების დამოუკიდებლობის შემთხვევაში და მათი მოქმედებების ადიტიურობისას

$$\overline{W_i} = \sum_{m=1}^{M} P_{ii\ \ მუქ} \cdot \Delta q_{ii}^{მუქ} \cdot P_{ii\ \ მუქ}^{აღმ} \quad (5)$$

წარმოდგენილ გამოსახულებაში m-ური მუქარის გამოჩენის ალბათობა $P_{ii\ \ მუქ}$ განისაზღვრება სტატისტიკურად და შეესაბამება მისი გამოჩენის ფარდობით სიხშირეს:

$$P_{ii\ \ მუქ} = \frac{\lambda_{ii}}{\sum_{m=1}^{M} \lambda_{ii}} = \overline{\lambda_{ii}} \quad (6)$$

სადაც λ_{ii} – არის i-ურ ობიექტზე m-ური მუქარის გამოჩენის სიხშირე.

საწარმოს მსს გლობალური უსაფრთხოების უმთავრესი ფუნქციაა უზრუნველყოს მთელი სისტემის, დასაცავი ობიექტების დაცულობა ისეთი დონით, რომ

$$W - \sum_{i=1}^{n} \overline{W_i} \leq W_{\text{დას}} \quad (7)$$

ეს კი იმას ნიშნავს, რომ ეკუ-ის მენეჯმენტის სამსახურმა უნდა განსაზღვროს ცალკეულ დასაცავ ობიექტებზე შესაძლო მუქარებით გამოწვეული დასაშვები ზარალი $W_{i\text{დას}}$, i = $\overline{1,n}$ და, ასევე მათი დასაშვები ჯამური მნიშვნელობა

$$W_{\text{დას}} = \sum_{i=1}^{n} \overline{W_{i\text{დას}}} \quad (8)$$

წარმოდგენილი ანალიზი გვიჩვენებს, რომ საწარმოს მსს გლობალური უსაფრთხოების სამსახურმა უდა გამოიკვლიოს ყოველი i-ური ობიექტის შესაძლო მუქარები, მათი წარმოშობის ალბათობები და ეკუ-ის სამსახურის მიერ წარმოდგენილი ცალკეული დაცვის ობიექტების დასაშვები ზარალების მიხედვით უზრუნველყოს შესაბამისი დაცვის მექანიზმების დანერგვა–გამოყენება. მათზე გაწეული ხარჯების მიზანშეწონილობა უნდა იყოს შეთანხმებული ეკუ-ის მენეჯმენტის სამსახურთან და საწარმოს სიტუაციურ ცენტრთან.

საწარმოს სიტუაციურ ცენტრში ჩართულ შიგა ადიტის სამსახურს, მსს გლობალური უსაფრთხოების სამსახურის მხარდაჭერით, ოპერატიულად და ეფექტურად შეუძლია განახორციოლოს თავისი ფუნქციები. მაგალითად, ის მსს დახმარებით ადვილად შეძლებს ბუღალტერიაში საქმეების მდგომარეობის გაანალიზებას და დასკვნის მომზადებას საწარმოს ეკონომიკური უსაფრთხოების უზრუნველყოფის (სეუ) დონის შესახებ. ასეთი მოსაზრების სისწორეზე მიგვითითებს ის გარემოება, რომ რაც უფრო მეტია ნეგატიური მოვლენები საწარმოს ფსმ-ში, მით უფრო მეტია მასთან დაკავშირებული შესაბამისი მოვლენები ბუღალტერიაში. ასეთი ანალიზი არ საჭიროებს შესწავლას ბუღალტერიის დოკუმენტების მასივების შესაბამისი სპეციალისტების მიერ ხანგრძლივი პერიოდის განმავლობაში. ამის გარდა, თუ ნეგატიური მოვლენები საწარმოს ფსმ-ში ხორციელდება რომელიმე თანამშრომლების მიერ განზრახ, მაშინ იმ განყოფილებაში, სადაც მუშაობენ ისინი, გარეგნულად ყველაფერი კარგადაა, საქმეები სრულ წესრიგშია. იმისათვის, რომ შეფასებულ იქნას საწარმოს ეკუუ-ის დონე, უნდა დამუშავდეს ტესტი, რომელიც დაფუძნებულ იქნება ზემოთ მოყვანილ განსჯებზე და აგებული იქნება ისეთნაირად, რომ გამოყოფილ იქნას გარკვეული მოვლენები ბუღალტერიაში და მიღებულ იქნას, თუნდაც ირიბი, ინფორაცია სეუ–ის მუქარების შესახებ.

ყველა მოკვლეული და აღწერილი მუქარები, პროცესები, შეფასებები, პირობები დაფიქსირებული უნდა იყოს საწარმოს გლობალური უსაფრთხოების პოლიტიკაში (გუპ), რომელიც უნდა შთანხმდეს და დამტკიცდეს საწარმოს ხელმძღვანელობის მიერ. აღნიშნულ გუპ–ში აუცილებლად უნდა იყოს გათვალისწინებული და დაცული სახელმწიფო კანონმდებლობის მოთხოვნები, საერთაშორისო და სახელმწიფო სტანდარტები, საწარმოს ადმინისტრაციული დონის ნორმატიული დოკუმენტები.

3. დასკვნა

ჩვენს მიერ ჩატარებული გამოკვლევა გვაძლევს იმის უფლებას ვამტკიცოთ, რომ თანამედროვე პირობებში ვერანაირი საწარმო კი არა, სახელმწიფოც კი ვერ შეძლებს არსებობასაც კი, თუ ის არ ზრუნავს და არ ნერგავს თნამედროვე ინოვაციურ

ტექნოლოგიებს, არ უწყობს ხელს მოსახლეობის, თანამშრომლების ინტელექტუალური დონის ამაღლებას. ასევე სასიცოცლო მნიშვნელობა აქვს ნებისმიერი სახელმწიფოსა და საწარმოსათვის მეცნიერული კვლევების გააქტიურებას, და ზოგადად მეცნიერული მოღვაწეობის, კვლევების ამღლება-გააქტიურებას. საწარმოს ეკუ–ის სისტემა სრულყოფილად უნდა იყენებდეს მსს-ის გლობალურ–კომპლექსური დაცვის სისტემის შესაძლებლობებს, რათა დროულად და ეფექტურად იქნას შეფასებული საწარმოს მიმდინარე მომენტში სიტუაციური მდგომარეობა და ამ შეფასების საფუძველზე მიღებულ იქნას ადექვატური გადაწყვეტილებები.

ლიტერატურა – References – Литература:

1. ოდიშარია კ., ხოშტარია ს., ებანოიძე ჟ. (2011). სისტემების და პროცესების მოდელირება. საქართველოს საავიაციო უნივერსიტეტი. თბილისი
2. ჩოგოვაძე გ. (2003). ინფორნაცია: ინფორმაცია, საზოგადოება, ადამიანი. სტუ, თბილისი
3. Мескон М.Х., Альберт М., Хедоури Ф. (1999). Основы менеджмента. –М.: „Дело“
4. Шангин В.Ф. (2017). Информационная безопасность и защита информации. –М.: ДМК Пресс
5. Сазыкин Б.В. (2008). Управление операционным риском в коммерческом банке. –М.: Вершина
6. Liker J.K., Hoseus M. (2008). Toyota Culture: The Heart and Soul of the Toyota Way. – McGraw-Hill
7. ოდიშარია კ., ზირაქაშვილი გ., ცომაია ნ. (2012). კადრები, როგორც თანამედროვე ორგანიზაციის ეფექტურად ფუნქციონირების მთავარი გარანტი. სტუ, „ბიზნეს-ნჟინერინგი“, №3.

INFORMATION SAQURITY OF THE ENTERPRISE AS ONE OF THE KEY CONTRIBUTORS TO ITS ECONOMIC SECURITY

Odisharia Korneli, Odisharia Salome, Maghlakelidze Nana

Georgian Teqnical UniversiTy

Summary

It is important to consider how important the security of the modern enterprise is to ensure the security of information security. The economy is today in an innovative stage of development and is an instrument for effective functioning of an automated information system that is a serious means of securing ecumen using information security systems.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ КАК ОДИН ИЗ КЛЮЧЕВЫХ ФАКТОРОВ ЕГО ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Корнели Одишария, Саломе Одишария, Нана Маглакелидзе

Грузинский Технический Университет

Резюме

Рассматриваются насколько важна при обеспечении экономической безопасности современного предприятия учитывать сушествующие проблеми защити информации. Экономика сегодня находится на инновационной стадии развития и для эффективного функционирования предприятия обезателним инструментом является применение автоматизированной информационной системы, которая является серьезным средством обеспечения экономической безопасности при использовании систем информационной безопасности.