



ბიზნესი, მენეჯმენტი, მარკეტინგი



ბიზნესის უსაფრთხოების სისტემური მართვის საფუძვლები

DOI:10.36962/ECS105/8-10/2023-157

რამაზ ოტინაშვილი

სტუ-ს პროფესორი,
r.otinashvili@gtu.ge

ალექსანდრე ელისაბედაშვილი

სტუ-ს დოქტორანტი,
a.elisabedashvili@gtu.ge

ვარაზ ბედინაშვილი

სტუ-ს დოქტორანტი,
v.bedinashvili@gtu.ge

რეზიუმე

უსაფრთხოება კომპლექსური მაჩვენებელია, რომელიც მოიცავს კომპანიის სხვადასხვა სფეროს - მენეჯმენტს, მარკეტინგს, პერსონალის მართვას, ფინანსურ ასპექტებს და ა.შ. რაც უფრო მდგრადია ბიზნესი მით უფრო ეფექტურია მისი ბიზნეს-პროცესები და ნაკლებადაა დამოკიდებული საბაზრო ვითარების მოულოდნელ ცვლილებებზე. უსაფრთხოების უზრუნველყოფაში განსაკუთრებული ადამიანური ფაქტორის როლი. პერსონალთან მუშაობა და მათი მხრიდან მავნე მცდელობის პრევენცია კომპანიის უსაფრთხოების სისტემის მნიშვნელოვანი ნაწილია. უსაფრთხოების სტრატეგიის კონტექსტში, გამოწვევების ბუნების მიხედვით, საჭიროა დაინერგოს პრევენციის შესაბამისი სისტემა. მნიშვნელოვანია მისი მუდმივი მონიტორინგი და უწყვეტი განვითარება. ბიზნესის უსაფრთხოების სისტე-

მის მიზანია გამოწვევების სწორი მართვა - კრიზისული სიტუაციების პროგნოზირება, შეფასება, გამოვლენა, გადანყვეტა და შესაძლო გამეორების საწინააღმდეგოთ პრევენციული ღონისძიებების დაგეგმვა. ბიზნესის უსაფრთხოების სისტემის ეფექტური მენეჯმენტი ქნის პირობებს კონკურენტუნარიანი ტექნოლოგიებისა და საქონლის/მომსახურების შესაქმნელად, რაც განაპირობებს ობიექტის წარმატებულ ფუნქციონირებას.

საკვანძო სიტყვები: ბიზნესი, მენეჯმენტი, უსაფრთხოება, სისტემა, სტრატეგია.

შესავალი

ბიზნესის უსაფრთხოების უზრუნველყოფა არის სისტემური პროცესი, რომლის მიზანია გამოწვევების სწორი მართვა - კრიზისული სიტუაციების პროგნოზირება, შეფასება, გამოვლენა, გადანყვეტა და შესაძლო გამეორების საწინააღმდეგოთ პრევენციული ღონისძიებების დაგეგმვა.

უსაფრთხოება არის კომპლექსური მაჩვენებელი და მოიცავს კომპანიის სხვადასხვა სფეროს - მენეჯმენტს, მარკეტინგს, პერსონალის მართვას, ფინანსურ ასპექტებს და ა.შ. რაც უფრო მდგრადია ბიზნესი მით უფრო ეფექტურია მისი ბიზნეს-პროცესები და ნაკლებადაა დამოკიდებული საბაზრო ვითარების მოულოდნელ ცვლილებებზე - მაკროეკონომიკურ დისპროპორციებზე, სავალუტო რყევებზე, ინფლაციურ პროცესებზე. ასევე უკეთ ხვდება კონკურენტებიდან მომდინარე გამოწვევებს.

ძირითადი ტექსტი

სტაბილური მაჩვენებლების მქონე ბიზნეს-ობიექტს გააჩნია უპირატესობა კონკურენტებთან შედარებით - ინვესტიციების მოზიდვაში, მომწოდებლების არჩევანსა და პროფესიონალი კადრების შერჩევაში. ყველას სურს დასაქმდეს პრესტიჟულ, მაღალანაზღაურებად კომპანიაში.

მაგალითად, ეპლში (Apple), რომელიც ლიდერია მსოფლიოში ყველაზე ინოვაციური კომპანიების სიაში. ასევე ტრადიციუ-

ლად აქვს ძლიერი პოზიციები განათლების, გამომცემლობის, მუსიკისა და დიზაინის ინდუსტრიებში. დასაქმებული პერსონალის პირობები აქ საუკეთესოა. იმდენად მაღალია ანაზღაურებაა, რომ ოფიციალურად ყველაზე მეტი მილიონერი ამ კომპანიაშია დასაქმებული. 1985 წელს აშშ-ს პრეზიდენტმა რონალდ რეიგანმა მისი დამფუძნებლები ვოზნიაკი და ჯობსი მედლებით დააჯილდოვა ტექნოლოგიური პროგრესის განვითარებაში შეტანილი წვლილისთვის.

ეკლის წარმატების ერთ-ერთი მიზეზი სისტემურ მართვაშია, რომლის მიზანია კომპანიის დაცვა სხვადასხვა შიდა თუ გარე გამოწვევებისაგან და არაპროგნოზირებადი გარემოებებისგან.

პოტენციური საფრთხეების დროულად გამოვლენისთვის საჭიროა კონკურენტების და პარტნიორების ქმედებების მონიტორინგი, კონფიდენციალურ მონაცემებთან მომუშავე პერსონალისთვის სპეციალური ტრენინგების ჩატარება, სიახლეებზე მუდმივად თვალყურის დევნება და ა.შ.

ხშირად მენეჯმენტი გამოწვევებთან გამკლავებას გარკვეული ზიანის მიღების შემდეგ იწყებს. პრევენცია ბევრად ეფექტურია, ვიდრე პოსტფაქტუმ მათი შედეგების აღმოფხვრა.

უმჯობესია ავაგოთ ბიზნესის უსაფრთხოების სისტემა კომერციული ობიექტის შექმნისთანავე და მაქსიმალურად გავითვალისწინოთ ყველა ნიუანსი. მაგალითად, რაიმე ცვლილება ბიზნეს ტექნოლოგიებში ავტომატურად უნდა აისახოს უსაფრთხოების უზრუნველყოფის სისტემაში.

დაცვის უზრუნველყოფის ობიექტებია:

- ბიზნეს პროცესები;
- მენეჯმენტი და პერსონალი;
- აქტივები, ფინანსური და მატერიალური ფასეულობები;
- ტექნოლოგიები და საინფორმაციო რესურსები;
- კომპანიის იმიჯი და რეპუტაცია და ა.შ.
- დაცვის სისტემის ძირითადი კომპონენტებია:
- ინფორმაციული უსაფრთხოება - მთავარი კომპონენტია;
- - ბიზნეს-პროცესების მართვის უსაფრთხოება გულისხმობს საინვესტიციო თუ სხვა მნიშვნელოვანი პროექტის

დანყებამდე გამოწვევების შეფასებას, რაც დამატებით ხარჯებთან შეიძლება იყოს დაკავშირებული;

- სამართლებრივი უსაფრთხოება გულისხმობს მოქმედი კანონმდებლობის დარღვევის პრევენციას. კერძოდ, მონაცემების ფალსიფიკაციას, საბუთების გაყალბებებს, თაღლითობებს და ა.შ.

- ეკონომიკური უსაფრთხოების ამოცანაა თავიდან ავიცილოთ აქტივების გაფლანგვა, მათი დეფიციტი, გადასახადების გადაუხდელობა, მარკეტინგული ღონისძიებები და ა.შ.

- უსაფრთხოების კომპონენტების საჭირო დონეზე შენარჩუნება მნიშვნელოვანადაა დამოკიდებული პერსონალის პროფესიონალიზმზე, არანაკლებ მნიშვნელოვანია მათი წესიერება და საიმედოობა.

- პერსონალის უსაფრთხოება კომპანიის მენეჯმენტის მნიშვნელოვანი ასპექტია. იგი მოიცავს ღონისძიებებს ობიექტის ტერიტორიის დასაცავად მესამე მხარის შეღწევისგან, რამაც შეიძლება საფრთხე შეუქმნას, როგორც კომპანიას ისე თანამშრომლებს. პერსონალის უსაფრთხოება ასევე გულისხმობს ადამიანური ფაქტორიდან გამომდინარე შესაძლო საფრთხეებისგან კომპანიის დაცვაში.

კიბერუსაფრთხოება დღეს საკმაოდ აქტუალური პრობლემაა. ბუნებრივია რაც უფრო მაღალია ობიექტის სტატუსი, მით უფრო საპასუხისმგებლოა მსგავსი ღონისძიებები. ამისათვის აქტიურად გამოიყენება ვიდეო სამეთვალყურეო კამერები, ციფრული მონაცემების დაცვის თანამედროვე პროგრამები. ფიზიკურის დროს - გამშვები პუნქტები, საშვთა სისტემა და ა.შ.

- ადამიანური რესურსების უსაფრთხოება გულისხმობს დაცვას პერსონალის „გაფონვისგან“. თუ ბიზნეს-ობიექტს უკავია კარგი პოზიციები ბაზარზე, კონკურენტები შეეცდებიან „ღირებული“ თანამშრომლის გადაბირებას. პერსონალის უსაფრთხოების მიზანია დაცული ვიყოთ ასეთი სიურპრიზებისაგან. მნიშვნელოვანია პერსონალის მომზადება უსაფრთხო კომუნიკაციისთვის გარე სტრუქტურების წარმომადგენელთან. მაგალითად, ტრენინგებზე, კონფერენციებზე, შეხვედრებზე, ინტე-

რეიუების დროს და ა.შ. განსაკუთრებული ყურადღება უნდა მიექცეს მომავალ კონტაქტებს კონკურენტებთან;

● ბიზნეს იმიჯის და რეპუტაციის დაცვა. თანამედროვე ბიზნეს-ურთიერთობები მიმდინარეობს უსწრაფესი საინფორმაციო ტექნოლოგიების ფონზე. არასასურველ, ღირსებაშემლახველ ინფორმაციას, იქნება ეს სოციალურ ქსელში არასასურველი პოსტი თუ სატელევიზიო გადაცემა შეუძლია მკვეთრად შელახოს კომპანიის იმიჯი. ასევე კომერციული მონაცემების გაჟონვა, არასწორი სამიზნე აუდიტორიის შერჩევა - ზიანს აყენებს რეპუტაციას.

ბიზნესის უსაფრთხოების სისტემის ეფექტურმა მენეჯმენტმა უნდა შექმნას პირობები კონკურენტუნარიანი ტექნოლოგიებისა და საქონლის/მომსახურების შესაქმნელად, რაც უზრუნველყოფს ობიექტის წარმატებულ ფუნქციონირებას.

საჭიროა მოგერიდოთ შემთხვევით და არაკეთილსინდისიერ პარტნიორებს, რომ ბიზნეს-პროცესები არანაირად არ იყოს მათზე დამოკიდებული. აუცილებელია საინფორმაციო პროცესების მუდმივი ანალიზი და დასაცავი მონაცემების მონიტორინგი. საჭიროა შედგეს ჩამონათვალი პირებისა, რომლებსაც აქვთ კონფიდენციალურ ინფორმაციასთან წვდომა. უნდა ვიცოდეთ რა სახის ზარალი შეიძლება მოჰყვეს ღირებული ინფორმაციის გაჟონვას.

უსაფრთხოების სტრატეგიის კონტექსტში, გამონევენების ბუნების მიხედვით, საჭიროა დაინერგოს პრევენციის შესაბამისი სისტემა, სადაც ეტაპობრივად გაიწერება:

1. უსაფრთხოების კუთხით კომპანიაში არსებული მდგომარეობა: რეალური და პოტენციური საფრთხეების იდენტიფიცირება, მათი საშიშროების ხარისხის, შესაძლო გააქტიურების ვადებისა და სავარაუდო ზიანის მითითებით. პირობების იდენტიფიცირება, რამაც შეიძლება გამოიწვიოს პრობლემები. შესაძლო საფრთხეების პროგნოზირება, არსებული პრობლემების შეფასება და ა.შ.

2. მიზნები ბიზნესის დაცვის უზრუნველსაყოფად, რისთვისაც საჭირო იქნება: უსაფრთხოების შესაბამისი პოლიტიკის შე-

მუშავენ. ჩამონათვალის შედგენა შესაბამისი სტრატეგიის და მისი რეალიზების მეთოდების შერჩევით.

3. უსაფრთხოების უზრუნველყოფის მართვის სტრუქტურის ფორმირება;

4. კრიტერიუმებისა და ინდიკატორების შერჩევა, რომლის მიხედვითაც შეფასებული იქნება დაცვის დონე და შეირჩევა აღმოფხვრის მეთოდები;

5. შესაბამისი ღონისძიებების მომზადება, რესურსების მოძიება და თანხების გამოყოფა;

აღნიშნული ეტაპები დაცულია არსებული ტექნიკურ-ორგანიზაციული და სამართლებრივი ნორმებით. ბიზნესის უსაფრთხოების სტრატეგია უნდა იყოს ადეკვატური და რაციონალური. ასევე საჭიროა შექმნილი დაცვის სისტემის მუდმივი მონიტორინგი და მისი უწყვეტი განვითარება.

ბიზნესის უსაფრთხოების მენეჯმენტში ითვალისწინებენ შემდეგ წესებს:

- გამოყენებული მეთოდები არ უნდა ეწინააღმდეგებოდეს არსებულ კანონმდებლობას.

- რესურსების კომპლექსური გამოყენება, ნიშნავს ყველა თანამშრომლის, კომპანიაში არსებული ყველა საშუალების ჩართვას.

- ეფექტური კოორდინაცია კომპანიის დანაყოფებს შორის.

- საჯაროობისა და საიდუმლოების ოპტიმალური შეხამება. კომერციული საიდუმლოებას ესაჭიროება დაცვა და პირიქით სარეკლამო და მარკეტინგულ ინფორმაციას - გაზიარება.

- პროფესიონალიზმი. ბიზნესის დაცვაში კვალიფიცირებული სპეციალისტების ჩართვა;

- ეკონომიკური მიზანშეწონილობა. უსაფრთხოების სისტემის ხარჯები არ უნდა აღემატებოდეს კომპანიის მოგებას.

- განვითარების ძირითადი მაჩვენებლების გეგმები შესაბამისობაში მოდიოდეს კომპანიის მიზანთან და ამოცანებთან.

ინფორმაციული რისკები სულ უფრო აქტუალურია. მაგალითად, თანამშრომელმა დატოვა კომპანია, მაგრამ გათავისუფლებამდე სამსახურებრივი მოვალეობის ფარგლებში საიდუმლო ინფორმაციასთან ჰქონდა წვდომა. თუ პირი წავიდა

სამსახურიდან უკმაყოფილო, მაღალია ალბათობა, რომ მან ჩაიდინოს ინფორმაციული დივერსია. მოხდეს მის ხელთ არსებული კომერციული მონაცემების გასაჯაროება ან კონკურენტებისთვის მიწოდება.

ასევე შესაძლებელია რისკი მომდინარეობდეს ე.წ. „მესამე პირისგან“, რომელსაც შეიძლება არ ჰქონდეს საერთო კომპანიასთან მაგრამ შეეცადის დაცული ინფორმაციის მოპოვებას. ეს შეიძლება იყოს ჰაკერი სარგებლის მოლოდინში, ან „ჭკვიანი“ მოზარდი, რომელიც აფასებს საკუთარ შესაძლებლობებს IT სფეროში.

თუ საინფორმაციო სისტემებში ხარვეზებია კონფიდენციალური მონაცემების გაჟონვის ალბათობა მატულობს. მაგალითად, არასაკმარისად სანდო პროგრამული და აპარატურული ბაზები, სუსტი კოდები, დაგვიანებული განახლებები და ა.შ.

ინფორმაციის გაჟონვის ძირითადი მეთოდებია:

- ფიშინგი. წერილების გაგზავნას იმ ადამიანების ფოსტიდან, რომლებსაც მიმღები ენდობა. ეს შეიძლება იყოს უშუალო მენეჯერი. შედეგად, ჰაკერები უბიძგებენ ადამიანს ჩამოტვირთოს დავირუსებული დანართი, გახსნას მანვე ბმული და ა.შ. ანუ ადრესატი „ყლაპავს“ სატყუარას ფიქტიური გზავნილის სახით და ერთგვარად თავად ეხმარება თავდამსხმელს.

- კომპანიის ანგარიშებზე წვდომა. თანამშრომელი, რომელიც ფიშინგის მსხვერპლია, ხშირად ხსნის საბანკო ანგარიშს თავდამსხმელისთვის. საკმარისია ჰაკერმა მას გაუგზავნოს წერილი, ერთი შეხედვით კორპორატიული ფოსტიდან, რომელიც შეიცავს ბმულს. მასზე დაწკაპუნებით, მიმღები აღმოჩნდება ავტორიზაციის გვერდზე, სადაც საჭიროა მომხმარებლის ID-ის და პაროლის შეყვანა, აღნიშნული კი მყისიერად ხელმისაწვდომი ხდება ჰაკერისთვის.

- სუსტი პაროლები, მათი განმეორებითი გამოყენება. პაროლის მონაცემთა ბაზები შეიძლება გაერთიანდეს, მაგალითად, ფორუმების ან ძველი გატეხილი ფოსტის მეშვეობით და ა.შ. შემდეგ კი რწმუნებათა სიგელების აღება და საჭირო ანგარიშში შესვლა ჰაკერისთვის მარტივდება.

ბიზნეს ინფორმაციის უსაფრთხოების უზრუნველსაყოფად ყველაზე გავრცელებული ღონისძიებებია: ქსელის სტრუქტურის ოპტიმიზაცია, ვირუსის პროგრამული უზრუნველყოფის კონტროლი, აპლიკაციების მართვა, განახლებები, გარე სერვისების და მობილური ტელეფონების გამოყენების მონიტორინგი. განსაკუთრებული ყურადღება უნდა მიექცეს ფულადი გზავნილების დაცულობას და ა.შ.

კონტრაქტორი კომპანიის საქმიანობის კონტროლის კონტექსტში მომავალი პარტნიორის შემოწმების ვალდებულება არ არის გათვალისწინებული საკანონმდებლო დონეზე. თუმცა, ამ საკითხში სიფხიზლე არაა ზედმეტი. საეჭვო გარიგებებით შეიძლება შეექმნათ პრობლემები შეუსრულებელი ვალდებულებების გამო, რასაც შესაძლოა მოჰყვეს ინვესტიციების უნდობლობა.

რა მოწმდება კონტრაგენტთან საქმიანი ურთიერთობის დაწყებამდე:

- იურიდიული პირის ან ინდივიდუალური მენარმის რეგისტრაციის ნომერი, ზუსტი დასახელება. რა სახის ინფორმაციაა მის შესახებ ერთიან სახელმწიფო რეესტრში. მეპატრონის სახელი, გვარი რამდენად სტაბილურია კომპანიის პოზიცია ბაზარზე. არის თუ არა რეალურად რეგისტრირებული მითითებულ მისამართზე. აწარმოებს თუ არა ბუღალტრულ აღრიცხვას, წარადგენს ანგარიშებს და ა.შ.

ბიზნესის სამართლებრივი უსაფრთხოების უზრუნველყოფა ღონისძიებების ერთობლიობაა იურიდიული საკითხების გადასაჭრელად, კონსულტაციისა და მსგავსი დახმარების დროული მიწოდებისთვის. რა უნდა გაკეთდეს ბიზნესის სამართლებრივი უსაფრთხოების შენარჩუნებისათვის:

- ყველა დოკუმენტაციის პროფესიონალურად შედგენა და ექსპერტიზის ჩატარება;

- კომპანიის წარმომადგენელი ადვოკატის მიერ სასამართლოში წარდგენა;

- ტრანზაქციის სრული მართვა ყველა წარმოშობილი სამართლებრივი საკითხის კომპეტენტური გადანყვითა;

- მომავალი ტრანზაქციების, საინვესტიციო ან კომერციულ საქმიანობასთან დაკავშირებული ნებისმიერი პროექტის ექსპერტიზის შეფასება;

- გარკვეული სამთავრობო უწყებების მოთხოვნების დროული გადანაცვება;

- აუდიტისთვის მზადყოფნა;

- ბიზნეს-ობიექტის ინტერესების დაცვა სხვადასხვა უწყებებში;

- საჩივრების და სარჩელების კომპეტენტური მომზადება მარეგულირებელი ან სამართალდამცავი ორგანოების წინააღმდეგ, თუ მათი ქმედებები სცილდება მოქმედ კანონმდებლობას;

ბიზნესის უსაფრთხოების უზრუნველყოფაში განსაკუთრებულია ადამიანური ფაქტორის როლი. შედეგად, პერსონალთან მუშაობა და მათი მხრიდან მავნე მცდელობის პრევენცია კომპანიის უსაფრთხოების სისტემის მნიშვნელოვანი ნაწილია.

დასკვნა

მასასადამე, უსაფრთხოების უზრუნველყოფა მოითხოვს ცვალებად საბაზრო გარემოში კომპანიის მენეჯმენტის მხრიდან **სისტემურ მიდგომას**. არ არსებობს უსაფრთხოების პრობლემის უნივერსალური გადაჭრა, ის კონკრეტული ბიზნესისთვის სპეციფიკურია ისევე, როგორც თავად ბიზნეს-ობიექტების საქმიანობაა განსხვავებული.

გამოყენებული ლიტერატურა:

1. ელისაბედაშვილი ა., ბედინაშვილი ვ., ოთინაშვილი რ., უსაფრთხო ბიზნეს გარემოს ფორმირების მნიშვნელოვანი ასპექტები, სტუ, „გლობალიზაცია და ბიზნესის თანამედროვე გამოწვევები“, VII საერთაშორისო სამეცნიერო კონფერენციის შრომების კრებული, 2023, გვ.271-275;

2. ოთინაშვილი რ., ეკონომიკური უსაფრთხოება, ანალიზის ანტიკრიმინალური ასპექტები, თბილისი: სტუ, 2005.-440გვ.;

3. Apple, “About Apple Corporation,” 2022. [Online]. Available:

Error! Hyperlink reference not valid.

4. Bedinashvili V., Contemporary Business Challenges in a Globalized World (Volume 4) // Collective Monograph. Saarbrücken, Saarland, Germany; May 2023.

5. Handbook of e-business security / editors, Joao Manuel, R.S. Tavares [and three others], Description: Boca Raton, FL : CRC Press, 2018.

6. <https://simplisafe.com/blog/business-security-system-basics>

7. <https://www.businessnewsdaily.com/3329-best-business-alarm-system.html>

8. <https://www.scimagojr.com/journalsearch.php?q=4100151524&tip=sid&clean=0>

REFERENCES:

1. Elisabedashvili A., Bedinashvili V., Otinashvili R., Important aspects of the formation of a safe business environment, Stu, "Globalization and modern business challenges", Proceedings of the VII International Scientific Conference, 2023, pp. 271-275;

2. Otinashvili R., Economic security, anti-criminal aspects of analysis, Tb.: Stu, 2005.-440 p.;

3. Apple, "About Apple Corporation," 2022. [Online]. Available: Error! Hyperlink reference not valid.

4. Bedinashvili V., Contemporary Business Challenges in a Globalized World (Volume 4) // Collective Monograph. Saarbrücken, Saarland, Germany; May 2023.

5. Handbook of e-business security / editors, Joao Manuel, R.S. Tavares [and three others], Description: Boca Raton, FL : CRC Press, 2018.

6. <https://simplisafe.com/blog/business-security-system-basics>

7. <https://www.businessnewsdaily.com/3329-best-business-alarm-system.html>

8. <https://www.scimagojr.com/journalsearch.php?q=4100151524&tip=sid&clean=0>

FUNDAMENTALS OF SYSTEMATIC MANAGEMENT OF BUSINESS SECURITY

Ramaz Otinashvili,

GTU Professor, r.otinashvili@gtu.ge

Aleksandre Elisabedashvili,

Doctoral of GTU a. elisabedashvili@gtu.ge

Varaz Bedinashvili,

Doctoral of GTU, v.bedinashvili@gtu.ge

RESUME

Safety is a complex indicator that includes various areas of the company - management, marketing, personnel management, financial aspects, etc. The more sustainable the business is, the more efficient its business processes are and the less dependent it is on unexpected changes in the market situation. The human factor plays a special role in ensuring business security. As a result, working with staff and preventing malicious attempts on their part is an important part of the company's security system. In the context of a security strategy, depending on the nature of the challenges, an appropriate system of prevention needs to be introduced. It is important to constantly monitor its continuous development. The purpose of the business security system is the correct management of challenges - forecasting, assessment, detection, resolution of crisis situations and planning of preventive measures against possible recurrence. Effective management of the business security system should create conditions for the creation of competitive technologies and goods/services that ensure the successful operation of the facility.

Keywords: business, management, security, system, strategy.