საფინანსო-საბანკო ორგანიზაციაში ინფორმაციული უსაფრთხოების პრინციპები და დაცვის ოპტიმალური მართვის მეთოდიკა

ლევან ქუთათელაძე
სტუ დოქტორანტი

საფინანსო-საბანკო ორგანიზაციის ინფორმაციული უსაფრთხოების სისტემაზე ფინანსური ხარჯების გათვლის ორი ძირითადი მიდგომა არსებობს. **პირველი** მდგომარეობს სისტემის უსაფრთხოებაზე გამოყოფილი ხარჯების ათვისებაში და შემდეგ ინფორმაციის უსაფრთხოების დონის ინსტრუმენტალურ გაზომვაში და კონტროლში. ამისათვის აუცილებელია ორგანიზაციის ხელმძღვანელობამ ყურადღება მიაქციოს ინფორმაციული რესურსების ღირებულების შეფასებას, ინფორმაციული უსაფრთხოების სფეროში დარღვევების გამო პოტენციური დანაკარგების შეფასებას და განსაზღვრას. ამ შედეგებზეა დამყარებული ინფორმაციის უსაფრთხოების სფეროში ხელმძღვანელთა შემდგომი მოქმედება.

თუ ინფორმაცია არაა მნიშვნელოვანი, კომპანიის ინფორმაციული აქტივებისათვის არსებითი საფრთხეები არ არის, ხოლო პოტენციური დანაკარგი მინიმალურია და ინფორმაციული უსაფრთხოების უზრუნველყოფის პრობლემაც არ არსებობს.

თუ ინფორმაცია შეიცავს გარკვეულ ღირებულებას, საფრთხეები და პოტენციური დანაკარგი აუცილებლად მოსალოდნელია, მაშინ დგება საკითხი ორგანიზაციის ბიუჯეტში ინფორმაციის უაფრთხოებაზე ხარჯვითი ნაწილის გამოყოფის შესახებ. ამ შემთხვევაში აუცილებელია ინფორმაციული უსაფრთხოების პრობლემების მოგვარებასა და ინფორმაციის დაცვის კორპორატიული სისტემის აგებაში ორგანიზაციის ხელმძღვანელობის მხარდაჭერა.

მეორე მიდგომა – ვუწოდოთ პრაქტიკული – მდგომარეობს შემდეგში: უნდა მოიძებნოს ინფორმაციის დაცვის კორპორატიული სისტემის გონივრული ღირებულების ინვარიანტი(არსებობენ ანა-

ლოგიური ინვარიანტები სხვა სფეროებში, სადაც ბიზნესისათვის მნიშვნელოვან მოვლენებს სავარაუდო ხასიათი აქვთ). არ არის გამორიცხული, რომ დაცვის კორპორატიულ სისტემაზე დაიხარჯოს დიდი თანხა და ამასთან აღმოჩნდეს სუსტი ადგილი, სადაც ადრე თუ გვიან მოხდება კონფიდენციალური ინფორმაციის გაჟონვა.

ინფორმაციის დაცვის სფეროში ექსპერტ-პრაქტიკოსებმა იპოვეს ოპტიმალური გადაწყვეტა – უსაფრთხოების კონკრეტული მოთხოვნების გათვალისწინებით ინფორმაციული უსაფრთხოების სისტემის ღირებულება უნდა შეადგენდეს ინფორმაციულ სისტემაზე დანახარჯების დაახლოებით 10-20%-ს. პრაქტიკული ცდების საფუძველზე სწორედ ეს არის შეფასება, რასაც შეიძლება დავეყრდნოთ (თუ არ ჩავატარებთ დეტალურ გამოთვლებს). პრაქტიკაში ინფორმაციული უსაფრთხოების სისტემის შეფასებისათვის კონკრეტული მეთოდების გამოყენება დამოკიდებულია მთელ რიგ ფაქტორებზე. მათ შორის მთავარია ორგანიზაციის სიმწიფის (ხანგრძლივი არსებობის) ხარისხი და მისი მოღვაწეობის სპეციპიკა.

ინფორმაციულ უსაფრთხოებაზე სახსრების დაბანდების აუცილებლობა, რომელიც მიიღება სტატისტიკური მოდელირების მეთოდიკის საფუძველზე ასევე შეიძლება სასარგებლო აღმოჩნდეს ქსელური დაცვის უზრუნველყოფისათვის. კომპანიის მენეჯმენტს, რომელსაც გააჩნია ინფორმაციის გაცვლის უსაფრთხო სისტემა, შეუძლია გაზარდოს შემოსავალი ელექტრონული ბიზნესის გამოყენებით და მიიღოს მოგება.

ინფორმაციული უსაფრთხოება ყოველთვის იყო და რჩება კომპანიის ბიუჯეტის ხარჯვით ნაწილად. ბიუჯეტის დაგეგმვისას კომპანიის ხელმძღვანელობამ უნდა მიიღოს ინფორმაცია ინფორმაციული ტექნოლოგიების განყოფილების უფროსისგან ახალი ტექნოლოგიების და დაცვის სისტემების დანერგვის შესახებ. ასევე პასუხი კითხვებზე – რამდენად გაიზრდება კომპანიის რესურსების საერთო დაცულობა? როგორ შეფასდეს იგი? ინფორმაციული განყოფილების ხელმძღვანელობას ყოველთვის არ შეუძლია შეარჩიოს შესაბამისი

არგუმენტები და ბიუჯეტში დაარეზერვოს თანხები ინფორმაციულ უსაფრთხოებაზე. ასე რომ, ინფორმაციული უსაფრთხოების უზრუნველყოფის სისტემის შექმნა და მოდერნიზაცია ხდება პრობლემა, რომელიც განიხილება ფინანსურ სიბრტყეში. ინფორმაციულ უსაფრთხოებაზე დანახარჯების დასაბუთებისას უნდა გავითვალისწინოთ, რომ უსაფრთხოების რაღაც დონე უზრუნველყოფილია იმის მიუხედავად, იფიქრა თუ არა ამაზე ვინმემ.

კომპანიის რეალობაში ინფორმაციული უსაფრთხოებების სამსახურის თანამშრომლები იძულებულნი არიან ეკონომიკური დეპარტამენტის მიერ გამოყოფილი შეზღუდული ფინანსური რესურსების პირობებში ააგონ ინფორმაციული დაცვის სისტემები. მსგავს სიტუაციებში საუბარი არ არის უსაფრთხოების ოპტიმალური სისტემის აგებაზე. საკითხი დგას ასე – აიგოს უსაფრთხოების სისტემა, რომელიც შეზღუდული ფინანსური რესურსების პირობებში ინფორმაციული საფრთხეების წინააღმდეგ აღმოჩნდება უფრო ეფექტიანი.

ინფორმაციული უსაფრთხოების სისტემის ეფექტიანი ფუნქციონირებისათვის აუცილებელია დაცვის აპარატული და პროგრამული საშუალებების ისე აღჭურვა, რომ რომელიმე ოპტიმალობის კრიტერიუმით მოხდეს ამ სისტემის შექმნა. ფაქტიურად, კომპიუტერულ სისტემებში ინფორმაციის დაცვის საშუალებების შეძენა ეკონომიკურად სასარგებლო რომ გახდეს, აუცილებელია გადაწყდეს შემდეგი ამოცანები:

1. შესაძლო ინფორმაციული საფრთხეების განხილვისას შევარჩიოთ ისინი, რომლებსაც აუცილებლად ექნებათ ადგილი კონკრეტულ შემთხვევაში და განვსაზღვროთ ზარალის დონე თითოეული საფრთხის რეალიზაციისას.

2. გამოვლენილ საფრთხეებსა და მათ შედეგებზე დავაგროვოთ სტატისტიკური მონაცემების საკმარისი რაოდენობა, რათა განვსაზღვროთ თითოეული საფრთხის რეალიზაციიდან მიღებული ზარალის დონე. საქართველოში ასეთი სტატისტიკა პრაქტიკულად არ არსებობს, როცა აშშ-ში ამ ინფორმაციების მოპოვებას და დამუშავებას ეთმობა დიდი ყურადღება. ამის შედეგად რიგი საფრთხეებისთვის მი-

იღება მონაცემთა დიდი რაოდენობა, რომელიც შეიძლება საფუძვლად დაედოს მოცემულ გაანგარიშებებს.

3. ინფორმაციის დაცვის დარღვევისას შეფასდეს მოსალოდნელი დანაკარგები. ეს შესაძლებელია მხოლოდ მაშინ, როცა საქმე გვაქვს ისეთ ინფორმაციის დაცვასთან, რომელიც შეიძლება შეფასდეს(ეკონომიკური, სამრეწველო, კომერციული).

4. შეფასდეს დაცვის სისტემის ელემენტების საიმედოობა. მიმდინარე მომენტში არ არსებობს კომპიუტერული სისტემების დაცულობის შეფასების საყოველთაოდ მიღებული მეთოდიკა. ამიტომ წარმოიშვა ისეთი მეთოდიკის დამუშავების პრობლემა, რომლის საშუალებითაც შესაძლებელი იქნება საკმარისი სიზუსტით შეფასდეს როგორც დაცვის სისტემის ცალკეული ელემენტების, ასევე მთლიანად დაცვის სისტემის საიმედოობა.

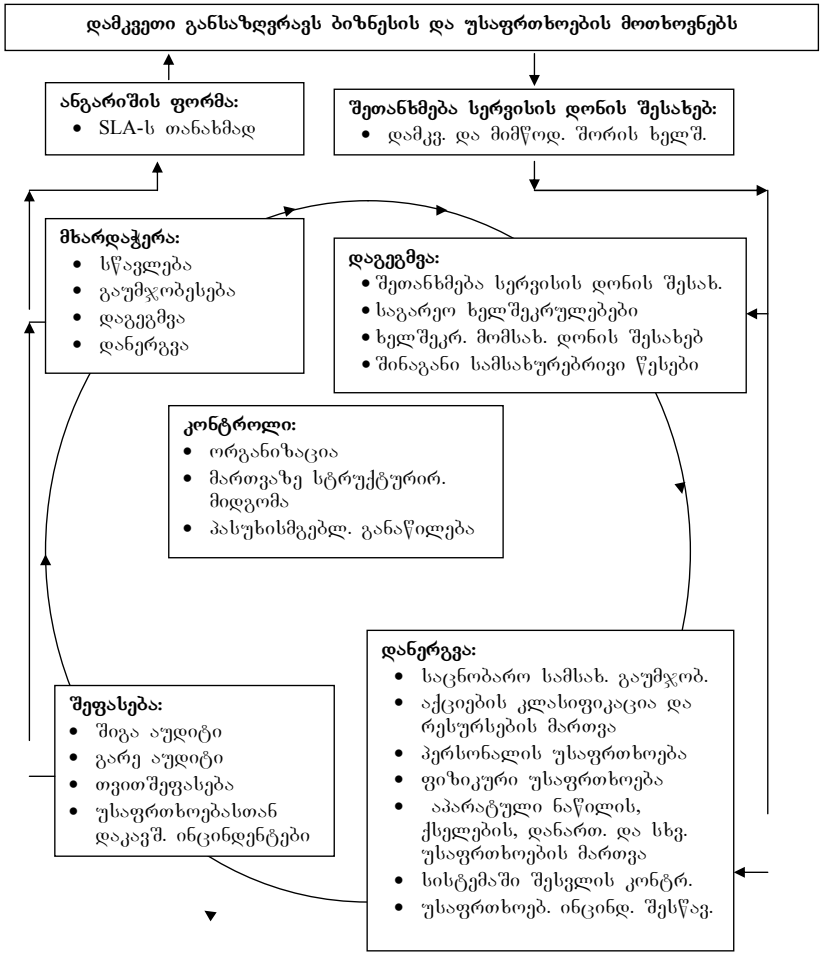
ბევრი ბიზნეს-პროცესის არსებობა შეუძლებელია ინფორმაციული უსაფრთხოების უზრუნველყოფის გარეშე. ფაქტიურად, სულ ეფრო მეტი ბიზნეს-პროცესები შედგებიან ერთი ან რამდენიმე ინფორმაციული სისტემისგან. ინფორმაციული უსაფრთხოების მართვა ორგანიზაციის საქმიანიბის მნიშვნელოვანი სახეა, რომლის მიზანსაც წამოადგენს ინფორმაციული უზრუნველყოფის პროცესების კონტროლი და მისი არასანქცირებული მოხმარების თავიდან აცილება.

ინფორმაციული უსაფრთხოების მართვის პროცესს აქვს ორი მიზანი:

1. უსაფრთხოების მოთხოვნების შესრულება, დადასტურებული SLA-სა და სხვა შიდა მოლაპარაკებების შედეგად, საკანონმდებლო აქტებით და დადგენილი წესებით;

2. შიდა მოთხოვნებისგან დამოუკიდებელი უსაფრთხოების დონის ბაზური უზრუნველყოფა.

ინფორმაციული უსაფრთხოების მართვის პროცესი აუცილებელია ინფორმაციული ტექნოლოგიების დეპარტამენტის უწყვეტი ფუნქციონირებისათვის (ნახ.1). პროცესისათვის შემავალი მონაცემები ემსახურება SLA-ს შეთანხმებას, რაც განსაზღვრავს უსაფრთხოების მოთხოვნებს.


დამკვეთი განსაზღვრავს ბიზნესის და უსაფრთხოების მოთხოვნებს
ანგარიშის ფორმა:
• SLA-ს თანახმად
შეთანხმება სერვისის დონის შესახებ:
• დამკვ. და მიმწოდ. შორის ხელშ.
მხარდაჭერა:
• სწავლება
• გაუმჯობესება
• დაგეგმვა
• დანერგვა
დაგეგმვა:
• შეთანხმება სერვისის დონის შესახ.
• საგარეო ხელშეკრულებები
• ხელშეკრ. მომსახ. დონის შესახებ
• შინაგანი სამსახურებრივი წესები
კონტროლი:
• ორგანიზაცია
• მართვაზე სტრუქტურირ. მიდგომა
• პასუხისმგებლ. განაწილება
დანერგვა:
• საცნობარო სამსახ. გაუმჯობ.
• აქციების კლასიფიკაცია და რესურსების მართვა
• პერსონალის უსაფრთხოება
• ფიზიკური უსაფრთხოება
• აპარატული ნაწილის, ქსელების, დანართ. და სხვ. უსაფრთხოების მართვა
• სისტემაში შესვლის კონტრ.
• უსაფრთხოებ. ინცინდ. შესწავ.
შეფასება:
• შიგა აუდიტი
• გარე აუდიტი
• თვითშეფასება
• უსაფრთხოებასთან დაკავშ. ინცინდენტები