კომპანიის ინფორმაციულ უსაფრთხოებაზე ხარჯების გათვლის მეთოდიკა

ლევან ქუთათელაძე,
სტუ, დოქტორანტი

ინფორმაციის დაცვის სფეროში ექსპერტ-პრაქტიკოსებმა უსაფრთხოების კონკრეტული მოთხოვნების გათვალისწინებით იპოვეს ოპტიმალური გადაწყვეტა –ინფორმაციული უსაფრთხოების სისტემის ღირებულება უნდა შეადგენდეს ინფორმაციული 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[1].

ინფორმაციული უსაფრთხოება ყოველთვის იყო და რჩება კომპანიის ბიუჯეტის ხარჯვით ნაწილად. ძნელია და ხშირად შეუძლებელიც შეფასდეს უსაფრთხოებაში ჩადებული ინვესტიციების დაბრუნება. ბიუჯეტის დაგეგმვისას კომპანიის ხელმძღვანელობამ უნდა მიიღოს ინფორმაცია ინფორმაციული განყოფილების უფროსებისგან ახალი ტექნოლოგიების და დაცვის სისტემების დანერგვის შესახებ. ასევე პასუხი კითხვაზე – რამდენად გაიზრდება კომპანიის რესურსების საერთო დაცულობა? როგორ შეფასდეს იგი? ინფორმაციული განყოფილების ხელმძღვანელობას ყოველთვის არ შეუძლია შეარჩიოს შესაბამისი არგუმენტები და ბიუჯეტში დაარეზერვოს თანხები ინფორ-

1 ქუთათელაძე ლ., ქუთათელაძე ა., საფინანსო-საბანკო ორგანიზაციაში ინფორმაციული უსაფრთხოების უზრუნველყოფისა და რისკების მართვის მეთოდები. თბილისი, ყოველთვიური საერთაშორისო რეცენზირებადი და რეფერირებადი სამეცნიერო ჟურნალი 'ეკონომიკა', #1-2, 2012. გვ. 57-61.

მაციულ 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. როგორც უკვე ცნობილია, ბიზნესში შეტანილი ცვლილებების ეკონომიკური შეფასებისთვის აქტიურად იყენებენ ფინანსურ მაჩვენებელს (ROI), რომლიც განისაზღვრება შემდეგი ფორმულით:

$$ROI = \frac{\text{შემოსავალი} - \text{ხარჯი}}{\text{ინვესტიციები}};$$

სადაც,

შემოსავალი - საანგარიშო წელში (1 წელი) კომპანიის შემოსავალია;

ხარჯი - საანგარიშო წელში (1 წელი) კომპანიის გასავალია;

ინვესტიციები – კომპანიაში ჩადებული ინვესტიციებია.

როგორც წესი ROI–ს გამოთვალა ხელმიუწვდომელია იმ ქვედანაყოფისთვის, რომელიც პასუხს აგებს ინფორმაციული ტექნოლოგიების გამართულობაზე. იმისათვის რომ გავიგოთ, როგორ აისახება ROI-ში ინვესტიციები ინფორმაციულ უსაფრთხოებაზე, უნდა განვსაზღვროთ დამხმარე roi, რომელიც გამოწვეულია ინფორმაციულ უსაფრთხოებაზე მიღებული ცვლილებებით:

$$roi = \frac{\Delta\text{შემოსავალი} - \Delta\text{ხარჯი}}{\Delta\text{ინვესტიციები}};$$

სადაც,

roi - ინფორმაციულ უსაფრთხოებაზე ინვესტიცირებისას ROI–ს ცვლილების მაჩვენებელი;

ΔШემოსავალი- ინფორმაციულ უსაფრთხოებაზე ინვესტიცირებისას შემოსავლის ცვლილება;

Δხარჯი - ინფორმაციულ უსაფრთხოებაზე ინვესტიცირებისას ხარჯის ცვლილება;

Δინვესტიციები - ინფორმაციულ უსაფრთხოებაზე ჩადებული ინვესტიციები.

დაუშვათ, რომ ინფორმაციული უსაფრთხოების სისტემაზე ცვლილებების შეტანამდე კომპანიის ROI იყო - ROIold, ჩადებული ინვესტიციები – Iold, დაგეგმილი ინვესტიციები - ΔI. მაშინ კომპანიის ROI პროექტის დანერგვის შემდეგ ასე განისაზღვრება:

$$ROI = ROIold\frac{Iold}{Iold + \Delta I} + roi\frac{\Delta I}{Iold + \Delta I};$$

ინფორმაციული უსაფრთხოების ეფექტიანობა დამოკიდებულია საერთო ინვესტიციებიდან გამოყოფილ ნაწილზე. ამის საფუძველზე იცვლება კომპანიის საერთო ეფექტიანობა: ROI შეიძლება გაიზარდოს(roi>ROI), შემცირდეს (roi<ROI) ან დარჩეს ძველ რეჟიმში (roi=ROI).

ინფორმაციული უსაფრთხოების სისტემას შემოსავლების ზრდაზე პირდაპირი გავლენა არა აქვს, ამიტომ ინფორმაციულ უსაფრთხოებაზე ჩადებული ინვესტიციებიდან კომპანიაში ხელფასების ზრდა არ არის მოსალოდნელი. მაგრამ Δშემოსავალი-ს ნულთან გათანაბრება მაინც არ შეიძლება, რადგან არსებობს ისეთი სტანდარტული ინფორმაციული სისტემები, რომლებშიც გონივრულად აგებული ინფორმაციის დაცვის სისტემა აისახება კომპანიის შემოსავლების ზრდაზე. მაგალითად, კომპანია PriceWaterhouseCoopers-ის კვლევების თანახმად, პირადად ელექტრონული გადარიცხვებისას არასრულყოფილი უსაფრთხოება გახდა კლიენტების ნდობის დაკარგვის მიზეზი, რამაც გამოიწვია შემოსავლების ნაკადის შემცირება[1].

ინფორმაციული უსაფრთხოების სისტემის აგებისას გვერდს ვერ ავუვლით ხარჯვით ნაწილს: ოპერაციული დანახარჯები არის ყველგან – ესაა პროექტის შემუშავება, პერსონალის სწავლება თუ ინფორმაციის დაცვის საშუალებების ღირებულება. მაგრამ არის შემად-

1 Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. Москва, Горячая линия-Телеком, 2009.

გენლები, რომლებსაც შეუძლიათ ამის კომპენსაცია და პროექტის რეალიზაციის შემდეგ ხარჯების შემცირებაც.

ხარჯების შემცირების მთავარი მიზეზი (რის გამოც ინფორმაციული უსაფრთხოების სისტემა იგება და ხდება მისი მოდერნიზაცია) არის რისკებისგან დაცვის გაძლიერება. გამოთვლილი roi აუცილებელია შედარდეს შემდეგ ზღვრულ სიდიდეებს:

- roi<0, ე.ი. პროექტის ეფექტიანობა უარყოფითია. ეს ბუნებრივია არის უარესი ვარიანტი (არის უფრო უარესი ვარიანტი, როცა roi იმდენად უარყოფითია, რომ უარყოფითი შეიძლება გახდეს მთელი კომპანიის ROI);
- ROI>roi>0, ე.ი. პროექტის დანერგვას მოყვება კომპანიის საერთო ROI-ს შემცირება;
- roi>ROI ე.ი. პროექტის დანერგვას მოყვება კომპანიის საერთო ROI-ს გაზრდა.

ნებისმიერი ეკონომისტი უარს იტყოდა 1) პროექტზე (პროექტი წამგებიანია), დაფიქრდებოდა, აელო თუ არა 2) პროექტი (პროექტი ამცირებს საერთო ეფექტიანობას, მაგრამ იგი მაინც შემოსავლიანია) და რეკომენდაციას გაუწევდა 3) პროექტის დანერგვას (პროექტი შემოსავლიანია და ხელს უწყობს ეფექტიანობის ზრდას).

ინფორმაციული უსაფრთხოების რისკების შეფასებისთვის საჭიროა გათვალისწინებული იქნეს არა მარტო ზარალი მათი წარმოშობის ალბათობის გათვალისწინებით, ასევე ზარალის აბსოლუტური მნიშვნელობა. თუ დანაკარგების ღირებულება თავსებადია კომპანიის საერთო ღირებულებასთან, მაშინ ინფორმაციული უსაფრთხოების სისტემის პროექტირებისას ზარალის წარმოშობის დაბალი (არა ნულთან ε მახლობლობაში) ალბათობისთვისაც, ეს დანაკარგები უნდა იქნეს გათვალისწინებული.