საფინანსო-საბანკო ორგანიზაციაში ინფორმაციული უსაფრთხოების უზრუნველყოფისა და რისკების მართვის მეთოდები

ლევან ქუთათელაძე
სტუ დოქტორანტი
ალეკო ქუთათელაძე
ემდ,სტუ პროფესორი

ინფორმაციული უსაფრთხოების უზრუნველყოფის მეთოდები იყოფა საკანონმდებლო, ორგანიზაციულ-ტექნიკურ და ეკონომიკურ მეთოდებად.

საკანონმდებლო მეთოდები გულისხმობს საკანონმდებლო სფეროსთან დამოკიდებულებაში რეგლამენტირებულ ნორმატიულ-საკანონმდებლო აქტების და ასევე, საქართველოს რესპუბლიკაში ინფორმაციული უსაფრთხოების უზრუნველყოფის საკითხებზე ნორმატიული დოკუმენტების შემუშავებას.

საქართველოს სისხლის სამართლის კოდექსის XXXV თავის 284, 285, 286 და XXXVIII თავის 324[1] მუხლები ეძღვნება კომპიუტერულ დანაშაულობებს. მათში გათვალისწინებულია ბიზნეს პროცესებში ინფორმაციის მნიშვნელოვანი როლი, ასევე ასახულია კომპიუტერული ტექნიკის გამოყენებასთან დაკავშირებული სასჯელი სხვადასხვა დანაშაულისათვის – ინფორმაციულ რესურსებში არაკანონიერი შეღწევა, განადგურება, ინფორმაციის მოდიფიკაცია, ბლოკირება, კომპიუტერებისა და ქსელების ექსპლუატაციის მოშლა და სხვა.

ინფორმაციული უსაფრთხოების უზრუნველყოფის ორგანიზაციულ-ტექნიკურ მეთოდებად შეიძლება ჩაითვალოს ინფორმაციული უსაფრთხოების უზრუნველყოფის სისტემის შექმნა და მისი სრულყოფა, სახელმწიფოს ფედერალური ორგანოების მიერ საკანონმდებლო მოქმედებების გაძლიერება, დამცავი ტელეკომუნიკაციური სისტემების განვითარება, არასანქცირებული შეღწევისგან დამცავი სისტემებისა და საშუალებების შექმნა და ა.შ.

ქვეყნის ინფორმაციული უსაფრთხოების უზრუნველყოფის ეკონომიკური მეთოდები შეიცავენ: ინფორმაციული უსაფრთხოების უზრუნველყოფისთვის პროგრამების შემუშავების და მათი ფინანსირების განსაზღვრას, ინფორმაციის დაცვის საკანონმდებლო და ორგანიზაციულ-ტექნიკური მეთოდების რეალიზაციასთან დაკავშირებული სამუშაოების დაფინანსების მექანიზმის სრულყოფას, ფიზიკური და იურიდიული პირების ინფორმაციული რისკების დაზღვევის სისტემის შექმნას.

დაზღვევა – ეს არის სოციალური მექანიზმი, რომელიც საშუალებას აძლევს სუბიექტებს საკუთარი სადაზღვევო დანაზოგებიდან კომპენსაცია გაუკეთონ გაწეული რისკის შესაძლო დანაკარგების გარკვეულ წილს. დანაკარგები შეიძლება გამოწვეული იყოს ამა თუ იმ არასასურველი გარემოებებით.

ინფორმაციული რისკების დაზღვევა – დაზღვევის ერთ-ერთი უახლესი სახეობაა მსოფლიოში. ინფორმაციული რისკების დაზღვევის წარმოშობისა და განვითარების წინაპირობებია: კომპიუტერული ტექნიკის და კომპიუტერული ქსელების ფართო გავრცელება და გამოყენება; შემთხვევითი მოვლენების რიცხვის ზრდა, რომლებსაც ინფორმაციული სისტემების დაზიანებისა და ინფორმაციის მოპარვის შედეგად მოაქვს მნიშვნელოვანი მატერიალური და მორალური ზარალი; კომპიუტერული დანაშაულის წარმოშობის საშიშროება, მისი დაუშვებლობა, ზარალის მინიმიზაცია და კომპენსაცია.

განვსაზღვროთ საინფორმაციო რისკების დაზღვევის ორი ძირითადი სახეობა: დაზღვევის ობიექტი (რა შეიძლება დაეზღვიოს) და დასაზღვევი რისკები (რისგან შეიძლება წარმოიშვას დაზღვევა).

დაზღვევის ობიექტი. დღეს რეალურად შეიძლება დაზღვეული იყოს:

1. ინფორმაციული რესურსები. მათ ეკუთვნის:

- მონაცემთა ბაზები, ბიბლიოთეკები, ინფორმაციის ნებისმიერ მატარებელზე მქონე ელექტრონული არქივები;

- დამუშავების პროცესში ან ექსპოატაციაში მქონე პროგრამული საშუალებები და კომპლექსები.

2. ფინანსური აქტივები:

- ელექტრონული ფორმის სახით ფულადი საშუალებების ანგარიშების ჩანაწერები (სისტემა კლიენტი-ბანკი);

- ელექტრონული სახის მქონე ფასიანი ქაღალდები.

3. დაზღვეული შემთხვევისთვის კომერციული საქმიანობის დროები-

თი შეწყვეტით გამოწვეული ზარალი:

- იძულებითი შეჩერების პერიოდში მოგების ნაწილის დაკარგვა;

- შეწყვეტილი საქმიანობის გამო გამოწვეული მიმდინარე ხარჯები.

4. ბიზნესის აღდგენისათვის დამატებითი ხარჯები:

- დანადგარებისთვის და პროცესების მომსახურებისთვის დროებითი არენდა;

- პროგრამული უზრუნველყოფისა და მოწყობილობების სასწრაფო შეცვლის გამო გამოწვეული ხარჯები;

- სადაზღვევო შემთხვევის გამოძიების ხარჯები;

- კომპანიის რეპუტაციის დაცვისთვის საჭირო ხარჯები.

დასაზღვევი რისკები. დღეისათვის ელექტრონული ფინანსური აქტივების და ინფორმაციული რესურსების განკარგვასთან დაკავშირებით დამზღვევლებმა ზარალის ანაზღაურების საკითხი შეიძლება განიხილონ შემდეგი მიზეზების გამო:

- ინფორმაციული სისტემის მტყუნება (მწყობრიდან გამოსვლა), რომელიც გამოწვეულია მისი პროექტირების, დამუშავების, შექმნის, ინსტალაციის და ექსპუატაციისას დაშვებული შეცდომებით;

- საბანკო-საფინანსო დაწესებულების თანამშრომელთა შეგნებული უკანონო ქმედება;

- მესამე პირის მიერ დაწესებულების მიმართ კომპიუტერული შეტევა;

- კომპიუტერული ვირუსების მოქმედებისას;

- კომპიუტერული ქსელების საშუალებით ფულადი საშუალებებისა და ფასიანი ქაღალდების ძარცვა.

რისკი რომ ექვემდებარებოდეს დაზღვევას, ის უნდა აკმაყოფილებდეს შემდეგ მოთხოვნებს:

- უნდა არსებობდეს ე. წ. ''ერთგვაროვანი'' დასაზღვევების საკმარისად დიდი ჯგუფი, რომლთა დახასიათებები სამართლიანია წარსულში;

- დანაკარგების მიზეზები და სერიოზულობა არ უნდა განისაზღვრებოდეს დასაზღვევების მოქმედებებით. ეს მიზეზები უნდა იყოს შემთხვევითი;

- განხილულ საფრთხეებს უნდა მივყავდეთ დანაკარგებამდე, რომელთა იდენტიფიკაცია ადვილია;

- დანაკარგების ალბათობების გამოთვლისთვის რეალური მონაცემების სტატისტიკა (მონაცემთა ბაზა) უნდა იყოს ხელმისაწვდომი;

- დაზღვევის ფასი რომ ეკონომიკურად მისაღები გახდეს, ამისათვის დანაკარგების ალბათობა უნდა იყოს საკმარისად მცირე.

ინფორმაციული სისტემების მუშაობის პრაქტიკა გვიჩვენებს, რომ უსაფრთხოების დონის 100%-ანი მიღწევა ძალიან ძვირი ჯდება და ხშირად არც ამართლებს, რადგანაც:

- დღეისათვის ყველაზე სრულყოფილი ინფორმაციული დაცვის სისტემას არ შეუძლია დაუპირისპირდეს საფრთხეებს, რომელებიც შემდგომშია მოსალოდნელი;

- ინფორმაციული უსაფრთხოების სისტემის ეფექტიანობა და საიმედოობა მრავალ შემთხვევაში დამოკიდებულია მომსახურე პერსონალთან, რომელმაც შეიძლება დაუშვას უნებლიე ან შეგნებული შეცდომა;

- კომპლექსური დაცვის ღირებულება შეიძლება აღმოჩნდეს დასაცავი ინფორმაციული რესურების ღირებულებაზე გაცილებით მეტი.

უკანასკნელმა მოტივმა შექმნა ინფორმაციული ტექნოლოგიების სპეციალისტების ცნობილი პრინციპი "გონივრული საკმარისობა", რომელიც მდგომარეობს "აბსოლუტური დაცვის" შექმნის მცდელობის გარეშე უსაფრთხეობის მიღებული დონის შემუშავებაში. აქედან ნათელია, რომ, როგორც დამზღვევლებმა, ასევე დასაზღვევებმა სერიოზულად უნდა განიხილონ ინფორმაციული უსაფრთხოებისა და ინფორმაციული რისკების დაზღვევისათვის დანახარჯების მასშტაბები.

სამწუხაროდ, ინფორმაციული რისკების დაზღვევა ჩვენს ქვეყანაში რჩება დაზღვევის ექსკლუზიურ სახეობად. ამის ძირითადი მიზეზია მომსახურეობის ღირებულება. დაზღვევის პოლისის ღირებულება შეადგენს სადაზღვევო თანხის 3–8%-ს, ამასთან ოპტიმალურ სადაზღვევო თანხად ითვლება 1 მლნ აშშ დოლარი.

იმის გათვალისწინებით, რომ ინფორმაციული რისკების დაზღვევა დაზღვევის ახალი სახეობაა, ჯერ კიდევ არ არსებობს კლიენტებთან მკაცრი სტანდარტები და დამზღვევი იძულებულია პოტენციურ კლიენტებთან აწარმოოს ვაჭრობა დაზღვევის ღირებულებასთან დაკავშირებით. ამასთან, ეს ვაჭრობა უნდა მიმდინარეობდეს მათემატიკური ფორმულირების საფუძველზე, რომელიც არგუმენტირებულად დაასაბუთებს, რომ მუშაობა ინფორმაციული უსაფრთხოების უზრუნველყოფისათვის ხორციელდება სათანადო დონეზე.

დაზღვეულმა გარკვევით უნდა წარმოიდგინოს, რაც მეტს დახარჯავს თავისი ინფორმაციული სისტემის უსაფრთხოებისათვის, მით ნაკლებია

ალბათობა, რომ ბოროტმზრახველი შეძლებს შეაღწიოს და დაანგრიოს შენახული ინფორმაციის მთლიანობა, მით ნაკლები მოუწევს გადაუხადოს სადაზღვევო კომპანიას პოლისისათვის.

ინფორმაციულ სისტემებში დაცვის ეფექტიანობა მიიღწევა ინფორმაციის დაცვის საშუალებების გამოყენებით. ინფორმაციის დაცვის საშუალებების ქვეშ იგულისხმება ტექნიკური და პროგრამული საშუალებები, რომლებიც განკუთვნილია ინფორმაციის დასაცავად.

ქსელური ტექნოლოგიების განვითარებამ შექმნა ინფორმციის დაცვის საშუალებების ახალი ტიპი – ქსელთაშორისი ეკრანები (ფირეწალლს), რომელებიც უზრუნველყოფენ ისეთი ამოცანების ამოხსნას, როგორიცაა გარე ქსელებში ჩართვისგან დაცვა, კორპორატიული ქსელების სეგმენტებში შეღწევის გამოვლენა, ღია ქსელებით გადაცემული მონაცემთა კორპორატიული ნაკადების დაცვა.

სატელეკომუნიკაციო არხებით ინფორმაციის გადაცემისას მისი დაცვა ხორციელდება კრიპტოგრაფიული დაცვის საშუალებებით. ამ საშუალებების თავისებურებაა ის, რომ ისინი პოტენციურად უზრუნველყოფენ გადასაცემ ინფორმაციაში არასანქცირებული შეღწევისაგან დაცვის უმაღლეს ხარისხს.