საფინანსო-საბანკო ორგანიზაციაში ინფორმაციის დაცვის საშუალებების ოპტიმიზაცია

ზურაბ ჩხაიძე –
სტუ-ს სრული პროფესორი
ლევან ჟუთათელაძე –
სტუ-ს დოქტორანტი

პრაქტიკაში ინფორმაციული უსაფრთხოების დაცვის სისტემის აგება ხდება ორგანიზაციის ბიუჯეტით გამოყოფილი შეზღუდული ფინანსური რესურსების პირობებში. მსგავს სიტუაციებში ლაპარაკი არ არის იმაზე, რომ აიგოს უსაფრთხოების ოპტიმალური სისტემა, არამედ იმაზე, რომ აიგოს უსაფრთხოების სისტემა, რომელიც იქნება უფრო ეფექტიანი ძირითადი საფრთხეებისგან დასაცავად. ამასთან, დაცული უნდა იყოს ინფორმაციული უსაფრთხოების ხარჯვით ნაწილზე მკაცრი შეზღუდვები.

კომპანიის ინფორმაციული უსაფრთხოების სისტემის (სხვადასხვა ინფორმაციული საფრთხისგან დასაცავად) ეფექტიანი ფუნქციონირებისათვის იგი უნდა აღიჭურვოს აპარატული, პროგრამული, ადმინისტრაციულ-ორგანიზაციული და სხვა საშუალებების კომპლექსით ისე, რომ ინფორმაციული უსაფრთხოების სისტემის აგებისას მოვახდინოთ მისი ოპტიმიზაცია ოპტიმალობის რომელიმე კრიტერიუმით.

დღეისათვის ინფორმაციული ტექნოლოგიების უსაფრთხოების უზრუნველსაყოფად სხვადასხვა საშუალება არსებობს. მათ სახვადასხვა დანიშნულება, ფუნქციონირების ეფექტიანობა და შესაბამისად, საჭირო რესურსების მოცულობა აქვთ. მათი შერჩევისათვის საჭიროა ადექვატური ინსტრუმენტების შერჩევის ამოცანის გადაწყვეტა.

ფაქტობრივად, კომპიუტერულ სისტემებში ინფორმაციის დაცვის საშუალებების ეკონომიკურად ხელსაყრელ ფასად შეძენისათვის აუცილებელია გადაწყდეს რამდენიმე ამოცანა:

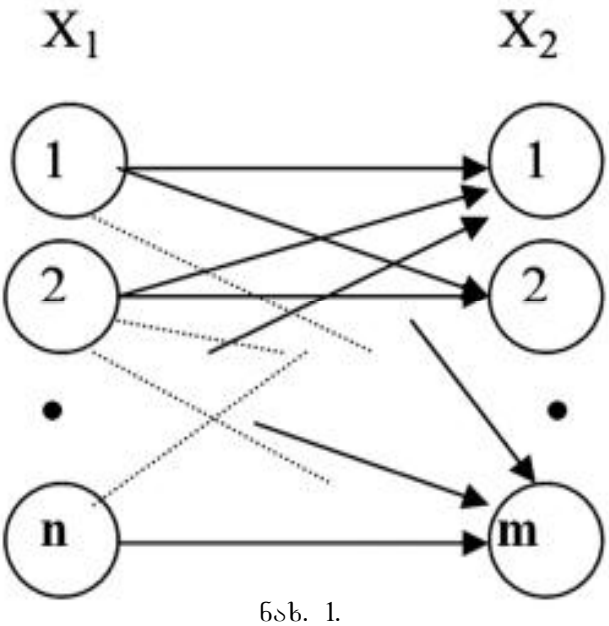
1. შესაძლო ინფორმაციული საფრთხეების განხილვისას ამოირჩეს ისეთები, რომლებსაც შესაძლოა ექნებათ ადგილი კონკრეტულ შემთხვევაში. განისაზღვროს თითოეული ამ საფრთხის რეალიზაციისას ზარალის ოდენობა;
2. საფრთხეების აღმოჩენისას მივიღოთ სტატისტიკური მონაცემების საკმარისი რაოდენობა. საქართველოში ასეთი სტატისტიკა ფაქტობრივად არ არსებობს, თუ არ ჩავთვლით ორგანიზაციებს ინფორმაციული ტექნოლოგიების განვითარებული ინფრასტრუქტურით. აშშ-ში ასეთი მასალის შეკრებასა და დამუშავებას დიდი ყურადღება ეთმობა;
3. ინფორმაციის დაცულობის დარღვევისას შეფასდეს მოსალოდნელი ზარალი. პრინციპში ეს შესაძლებელია მაშინ, როცა საქმე ეხება ისეთი ინფორმაციის დაცვას, რომელიც შეიძლება შეფასდეს. ძირითადად ესენია: ეკონომიკური, სამრეწველო, კომერციული და მათი მსგავსი.
4. შეფასდეს დაცვის სისტემის ელემენტთა საიმედოობა. წარმოიშვება მეთოდიკის შემუშავების პრობლემა, რომლის საშუალებითაც საკმარისად ზუსტად შეიძლება შეფასდეს, როგორც დაცვის სისტემის ელემენტების, ასევე მთელი დაცვის სისტემის საიმედოობა.

განვიხილოთ მოდელი, რომელიც გამოიყენება ორგანიზაციის ინფორმაციული უსაფრთხოების სისტემის შესაქმნელად. ჩავთვალოთ, რომ მოცემულია ინფორმაციული საფრთხეების (ის) სიმრავლე, რომლებიც შეიძლება წარმოიშვას ორგანიზაციის ინფორმაციული უსაფრთხოების სისტემაში, და აპარატული და პროგრამული დაცვის საშუალებების (დს) სიმრავლე, რომელთა საშუალებითაც ხდება ამ საფრთხეების ნეიტრალიზება. ამასთანავე, ყოველი შერჩეული ის-დს-ს წყვილისათვის განსაზღვრულია რიცხვი $r_1(i,j)$ – i-ური დაცვის საშუალებით j-ური ინფორმაციული საფრთხის ნეიტრალიზაციის ეფექტიანობა. მათემატიკური მოდელის ასაგებად შემოვიტანოთ ცვლადი y(i,j), რომელიც უდრის 1-ს, თუ j-ური ინფორმაციული საფრთხის ნეიტრალიზება ხდება i-ური დაცვის საშუალებით, და უდრის 0-ს. წინააღმდეგ შემთხ-

ვევაში. ამასთან, იგულისხმება, რომ ინფორმაციული საფრთხეები ერთმანეთთან არაა დაკავშირებული.

მოდელის უკეთესად გასაგებად გრაფების თეორიის დახმარებით დავსვათ ინფორმაციული უსაფრთხოების სისტემის შერჩევის ამოცანა. ამისათვის ავაგოთ გრაფი G(X,U), ($X=\cup X_i$, i=1,2), რომელშიც X_1 სიმრავლის წვეროები წარმოადგენენ აპარატული და პროგრამული დაცვის საშუალებებს, ხოლო X_2–ის, შესაბამის ინფორმაციულ საფრთხეებს (ნახ.1). X_1 სიმრავლის თითოეული ელემენტი (წვერო) ხასიათდება ინფორმაციული საფრთხეების ნეიტრალიზაციის წონითა და ეფექტიანობით. $X_1 \backslash X_2$ სიმრავლის ყოველ წვეროს ენიჭება წონა, რომელიც შეესაბამება უსაფრთხოების სისტემის ღირებულებას, ხოლო ყოველ წყვილს $(i,j) \in U$ – წონა, $z(i,j)=1,0$.

ოპტიმალური ინფორმაციული უსაფრთხოების სისტემის არჩევის ამოცანა მდგომარეობს შემდეგში: მოცემული შეზღუდული დანახარჯების (Q) პირობებში სხვადასხვა დაცვითი საშუალებების გამოყენებით მოვახდინოთ ინფორმაციული საფრთხეების სიმრავლის ნეიტრალიზაციის მაქსიმიზაცია. ფორმალურად ამოცანა შეიძლება დაისვას შემდეგი სახით:



ნახ. 1.

$$\sum_{j=1}^{m}\sum_{i=1}^{n} r_1(i,j)\, y(i,j) \rightarrow \max,$$

$$\sum_{i=1}^{n} r_2(i) * sign \sum_{x_j \epsilon X_2} y(i,j) \le Q,$$

$$\forall (i,j) \epsilon X_2, \quad \sum_{x_i \epsilon X_1} y(i,j) = 1;$$

$$\forall (i,j) \epsilon U, \quad y(i,j) = \{1,0\}.$$

სადაც $r_2(i)$ არის i-ური დაცვის სისტემის შესაძენად დახარჯული თანხები.

თუ აუცილებელია ეფექტიანობის (P) მოცემული დონის შეზღუდვისას კომპანიის ინფორმაციული სისტემის ინფორმაციული საფრთხეებისგან დაცვის საშუალებებზე დანახარჯების მინიმიზაცია, მაშინ ამოცანა შეიძლება ასეთი სახით დაისვას:

$$\sum_{i=1}^{n} r_2(i) * sign \sum_{j=1}^{m} y(i,j) \rightarrow min.$$

$$\frac{\sum_{j=1}^{m}\sum_{i=1}^{n} r_1(i,j) * y(i,j)}{\sum_{i=1}^{n}(\underbrace{max}_{j} r_1(i,j)} \le P;$$

$$\forall x_j \epsilon U, X_2 \ , \quad \sum_{x_i \epsilon X_1} y(i,j) = 1;$$

$$\forall (i,j) \epsilon U, \quad y(i,j) = \{1,0\}.$$

მოცემულ მოდელში გათვალისწინებულია, რომ ინფორმაციული უსაფრთხოების სისტემის ეფექტიანობის მაღალი დონე მიიღწევა მაშინ, როცა ყოველი საფრთხის ნეიტრალიზება მოხდება მაქსიმალური ეფექტიანობის დაცვის საშუალებების შერჩევის შედეგად.

ინფორმაციული უსაფრთხოების სისტემის ეფექტიანობის მაღალი დონე შეესაბამება $r_1(i,j)$ მატრიცის თითოეული სვეტის მაქსიმალური ელემენტების ჯამს.

დაცვის განსაკუთრებით საერთო კამონზომიერებას მიეკუთვნება თვისება, რომელიც ადასტურებს, რომ სისტემის უსაფრთხოების ხარისხი განისაზღვრება მისი ყველაზე "სუსტი" ელემენტის დაცულობის ხარისხით. მოცემული შემთხვევისათვის ინფორმაციული უსაფრთხოების დონე განისაზღვრება ყველაზე ნაკლები ეფექტიანობის დაცვის საშუალებით, რომელსაც ვირჩევთ დაცვის საშუალებების სიმრავლიდან. ასეთ შემთხვევაში ამოცანა დაისმება შემდენაირად:

$$\underbrace{min}_{j}\sum_{j=1}^{n} r_1\,(i,j)\,y(i,j)\ \rightarrow \max\ ,$$

$$\sum_{i=1}^{n} r_2\,(i) * sign \sum_{x_i \epsilon X_2} y(i,j) \le Q\ ,$$

$$\forall x_j \epsilon X_2\ ,\quad \sum_{x_i \epsilon X_1} y(i,j) = 1\ ;$$

$$\forall (i,j)\epsilon U,\quad y(i,j) = \{1,0\}.$$

იმ შემთხვევაში, თუ ინფორმაციული საფრთხეები(ის) არ არიან დამოუკიდებლები, ერთი ის წარმოადგენს მეორის წარმოშობის წყაროს, მაშინ აღნიშვნით – "მარცხენა" ნაწილის წვეროების ქვესიმრავლე, რომელიც პასუხს აგებს j-ური ინფორმაციული საფრთხის წარმოშობისას სისტემის დაცვაზე და მოცემული მოდელი გარდაიქმნება ასე:

$$\sum_{x_k \epsilon X_2^1} \sum_{(i,j)\epsilon L(s,t_k)} r_1(i,j)\,y(i,j)\ \rightarrow \max\ ,$$

$$\sum_{i=1}^{n} r_2\,(i) * sign \sum_{x_j \epsilon X_2} y(i,j) \le Q\ ,$$

$$\forall x_j \epsilon X_2\ ,\quad \sum_{x_i \epsilon X_1} y(i,j) = 1\ ;$$

$$\forall (i,j)\epsilon U,\quad y(i,j) = \{1,0\}.$$

აღნიშნულ მოდელში იგულისხმება, რომ j-ური ინფორმაციული საფრთხის შესრულებისას ინფორმაციის მისაღებად საკმარისია ერთი ის-ს (X^i) წარმოშობაც კი. $L(s,t_k)$ – გზა ფიქტიური წვერო-სათავიდან ქვესიმრავლის ყველა X_2 წვერო-სათავეებთან.

ზემოთ შემოთავაზებული ფიქტიური მოდელები მიეკუთვნება ბულის ცვლადებიანი დისკრეტული პროგრამირების ამოცანების კლასს. მათი ამოხსნისათვის შეიძლება გამოყენებული იქნეს გადარჩევის ალგორითმის სხვადასხვა ტიპი.

გამოყენებული ლიტერატურა

1. ქუთათელაძე ლ., საფინანსო-საბანკო ორგანიზაციაში ინფორმაციული უსაფრთხოების პრინციპები და დაცვის ოპტიმალური × მეთოდები. ყოველთვიური საერთაშორისო რეცენზირებადი და რეფერირებადი სამეცნიერო ჟურნალი "ეკონომიკა", №1-2, 2012წ. გვ. 144-148.
2. Курило и др. Обеспечение информационной безопасности бизнеса. Издотелская группа «БДЦ-пресс», Москва, 2008.

ОПТИМИЗАЦИЯ ПРОГРАММНО-ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ В ФИНАНСОГО-БАНКОВСКОМ УЧРЕЖДЕНИИ

ЗУРАБ ЧХАИДЗЕ
профессор ГТУ
ЛЕВАН КУТАТЕЛАДЗЕ
докторант ГТУ

На практике работникам службы информационной безопасности (ИБ) компании приходится строить систему защиты в рамках достаточно ограниченного количества финансовых ресурсов, выделяемых экономическим департаментом компании. В подобной ситуации речь не идет о том, чтобы построить оптимальную систему безопасности, вопрос ставится так — построить систему безопасности, которая оказалась бы наиболее эффективной при противодействии основным угрозам информационной системе компании при условии наличия жесткого ограничения на стоимость входящих в систему ИБ средств.

Для эффективного функционирования системы информационной безопасности предприятия её необходимо оснастить комплексом аппаратных и программных средств защиты от различных информационных угроз таким образом, чтобы оптимизировать некоторый критерий оптимальности создания СИБ.

OPTIMIZATION OF PROGRAM-TECHNICAL FACILITIES FOR INFORMATION PROTECTION IN FINANCE AND BANKING ORGANIZATION

ZURAB CHKHAIDZE
professor of GTU
LEVAN QUTATELADZE
PhD student of GTU

In practice, staff of the information security service has to construct security system in limited financial sources allocated by the economy department of the organization. In such cases, the goal is not to construct optimal security system, but to construct security system that will be more effective against basic dangers. At the same time, strict limitations on information security expenditures have to be followed.

With the aim of effective operation of the company information security system, it must be equipped with (to protect from different information dangers) complex of hardware and program facilities in the way that when constructing information security system, its optimization has to be realized by one of the optimality criteria.