ინფორმაციის დაცვის ადაპტური მოდელი

ოთარ შონია, გიორგი ჯაფარიძე, ია ირემაძე
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

ინფორმაციის დაცვა პრაქტიკაში სხვადასხვა სახის ფაქტორების შემთხვევითი ზემოქმედების პირობებში მიმდინარეობს. ზოგიერთი მათგანი სისტემატიზებულია სტანდარტების მიხედვით, ზოგიერთი წინასწარ უცნობია, შეუძლია იმოქმედოს გათვალისწინებულ ღონისძიებებზე და შეამციროს ეფექტურობის დონე. დაცვის ეფექტურობის შეფასება უნდა ითვალისწინებდეს ობიექტურ გარემოებებს და ალბათურ ფაქტორებს. დღეს ექსპერტები, ცოდნის სხვადასხვა სფეროებში, მუშაობენ საინფორმაციო უსაფრთხოების საკითხებზე. ეს განპირობებულია იმით, რომ შემდეგი ასი წლის განმავლობაში ჩვენ ვიცხოვრებთ საინფორმაციო ტექნოლოგიების საზოგადოებაში, სადაც მნიშვნელოვანი იქნება უსაფრთხოების საკითხები.

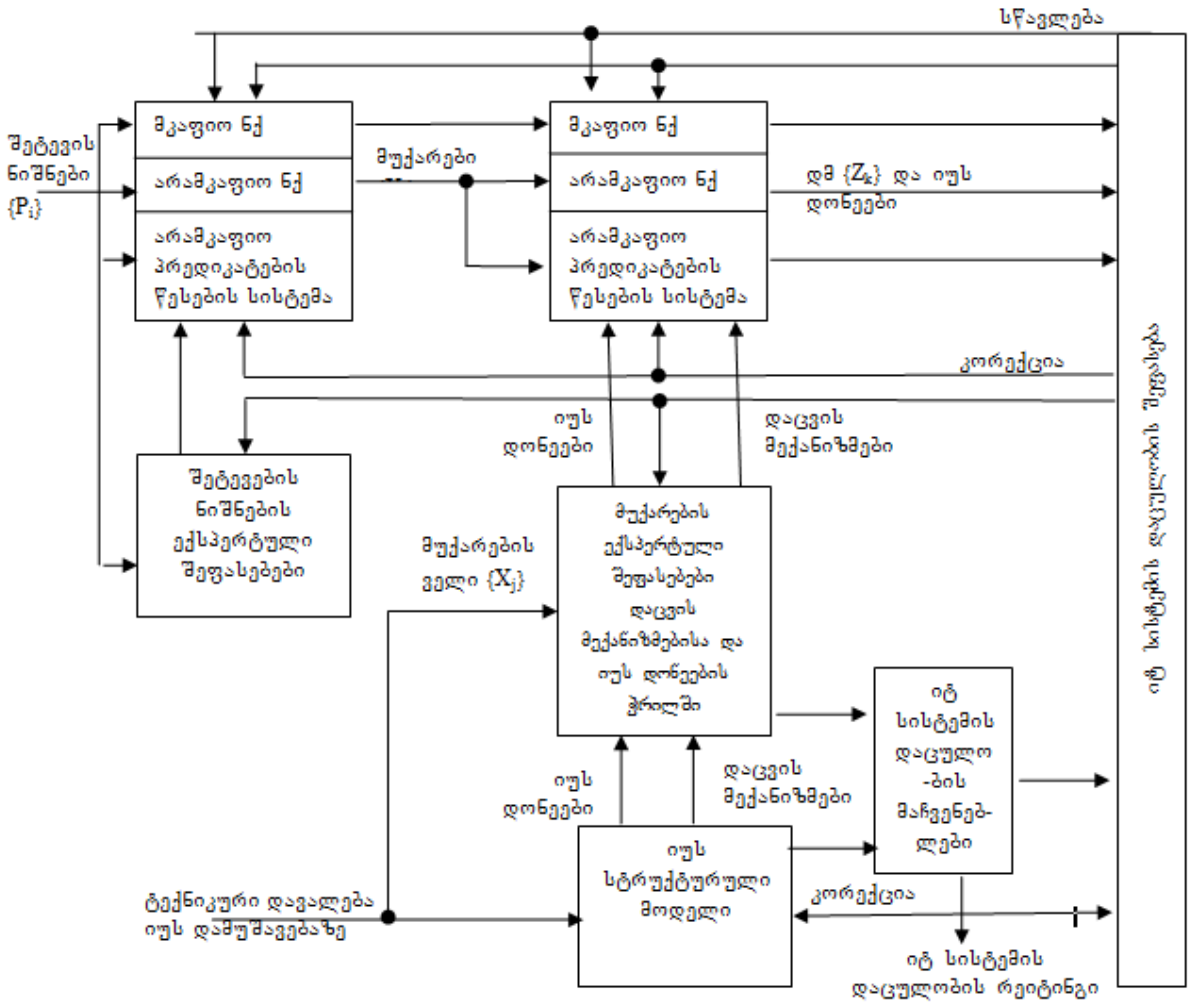
საკვანძო სიტყვები: ფაქტორი. ობიექტური გარემოებები. ეფექტურობის შეფასება. საზოგადოება.

1. შესავალი

თანამედროვე ინფორმაციული ტექნოლოგიების ერთ-ერთი უმნიშვნელოვანესი თავისებურება არა მარტო გავრცელება და განვითარების ძალზე მაღალი ტემპია, არამედ მათთვის დამახასიათებელია ინფრასტრუქტურის გართულება, ფუნქციური შესაძლებლობების გაფართოება და გამოთვლითი საშუალებების ინტელექტუალიზაცია. საინტერესოა ის ფაქტი, რომ შეიმჩნევა გარკვეული პარალელი ბიოსისტემების სხვადასხვა სახეობების ეკოლოგიასა და ინფორმაციული ტექნოლოგიების (იტ) ევოლუციას შორის [1]. ბიოსისტემების განვითარება მიმდინარეობს ინფორმაციული პროცესების დაცვის სრულყოფის წყალობით, ხოლო ინფორმაციული ტექნოლოგიების შემდგომი განვითარება შესაძლებელია იტ-სისტემების შესაფერისი დაცვის დონის უზრუნველყოფით, რომელიც იტ-ის სირთულის ზრდის ადექვატური იქნება. შეიძლება იმის ვარაუდი, რომ ინფორმაციული უსაფრთხოების სისტემების (იუს) დამუშავების პერსპექტიულ მეთოდს წარმოადგენს ხელოვნურ სისტემებში ბიოსისტემების ინფორმაციული პროცესების დაცვის მექანიზმების (დმ) ანალოგიების გამოყენება. შევეცდებით აღნიშნული ანალოგიების გამოყენებას ადაპტური იუს-ის ასაგებად:

- ინფორმაციის დაცვის მექანიზმებში;
- იტ-ს არქიტექტურაში;
- მემკვიდრეობის, განვითარების, ადაპტაციის და შერჩევის ევოლუციურ პროცესებში;
- ინფორმაციის განაწილებული ჭარბი ინფორმაციული ველის ფორმით წარმოდგენისას;
- პროგრამირებაში ინფორმაციული პროცესების იტ-სისტემებში ინფორმაციული ველების ფორმირების მეშვეობით, ნეირონული ქსელების (ნქ) ინტელექტუალური მექანიზმების, არამკაფიო ლოგიკის და გენეტიკური ალგორითმების (გა) გამოყენებით.

მოდელირების შესაძლებლობა ესაა დამუშავებისა და ვერიფიკაციის ძირითადი ბაზა, რომელიც საშუალებას იძლევა თავიდან ავიცილოთ შეცდომები ნებისმიერი კიბერნეტიკული სისტემების (და არა მარტო) დაპროექტებისას. ცხადია აქ პირველ რიგში ვგულისხმობთ ინფორმაციული უსაფრთხოების სისტემასაც. იუს-ში ადგილი აქვს ურთიერთდაკავშირებულ მოვლენებს: მუქარის წყარო – ფაქტორი (მოწყვლადობა) – მუქარა (მოქმედება) – შედეგები (შეტევა). შეტევათა ველისა და დასაცავი იტ-სისტემების ექსპლუატაციის პირობების შეცვლისას შესაძლებელია სრულიად ახალი მოწყვლადობების (სუსტი ადგილების) წარმოშობა, რომლებიც არ იყო ასახული საწყის მოდელში. ინფორმაციული უსაფრთხოების ადაპტური სისტემის დაპროექტებისას გათვალისწინებული უნდა იყოს გადასაწყვეტი ამოცანის კომპლექსური ხასიათი. ადაპტური იუს მოდელის დამაკავშირებელ რგოლს წარმოადგენს იტ-სისტემების დაცულობის შეფასების მეთოდიკა, რომელიც მუქარების კლასიფიკატორების და დაცვის მექანიზმების (ნეირონული ქსელების, არამკაფიო ნეირონული ქსელების, არამკაფიო პრედიკატების წესების სისტემის სახით), სისტემის ინფორმაციული უსაფრთხოების სტრუქტურული მოდელის, დაცულობის მაჩვენებლების და იტ-სისტემის რეიტინგის გაანგარიშების ინსტრუმენტული საშუალებების ურთიერთკავშირის კოორდინაციას ახდენს. (ნახ. 1).



ნახ.1. ინფორმაციული უსაფრთხოების ადაპტური სისტემის მოდელი

ნეირონული ქსელების ადაპტურობა საშუალებას იძლევა შეზღუდული დანახარჯებით მოხდეს იტ-სისტემის უსაფრთხოების სათანადო დონის უზრუნველყოფა, რომელიც მუქარათა ველის ცვლილებაზე ოპერატიულად რეაგირების მეშვეობით განხორციელდება. ნეირონული ქსელების მნიშვნელოვან უპირატესობას წარმოადგენს, აგრეთვე გამოცდილების დაგროვების შესაძლებლობა, რომელიც დაცვის იერარქიაში ნეირონული ქსელების ინფორმაციული ველების სახით ხორციელდება.

ინფორმაციული უსაფრთხოების სისტემის დაპროექტების მოთხოვნების შესაბამისად აირჩევა იუს-ის სტრუქტურული მოდელი დაცვის დონეების მექანიზმების იერარქიის სახით, ხოლო ექსპერტების გამოცდილება გამოისახება ექსპერტული შეფასების მატრიცებით, რომელთა ბაზაზეც ფორმირდება არამკაფიო პრედიკატული წესების სისტემები შემდეგი კლასიფიკაციისათვის:

1) მუქარების შეტევათა ნიშნების მიხედვით და
2) დაცვის მექანიზმები მუქარათა ველზე.

პირველ შემთხვევაში (დაცვის იმუნური დონის კლასიფიკატორი) არამკაფიო პრედიკატული წესების სისტემები, შემდგომი ადაპტაციისა და ანალიზისათვის, გამოისახება არამკაფიო ნეირონული ქსელების სახით, რომელსაც „ასწავლიან“ შეტევების ნიშნების შემომავალი ვექტორების გარკვეულ ქვესიმრავლეზე. ამავე დროს ასწავლიან კლასიფიკატორებს მკაფიო ნეირონული ქსელების სახით ისეთნაირად, რომ თვით სწავლებისას წარმოშობილი კლასტერების რიცხვი ტოლი იყოს არამკაფიო პრედიკატული წესების რიცხვისა. მეორე შემთხვევაში ანალოგიურად ფორმირდება და ისწავლება დაცვის რეცეპტორული დონის ნეირონული კლასიფიკატორი ცნობილი მუქარების ვექტორების მოცემულ ქვესიმრავლეზე.

ინფორმაცია ადაპტურ იუს-ში შეიძლება ინახებოდეს და გადაეცემოდეს შთამომავლობებზე ნეირონული ქსელების განაწილებული ინფორმაციული ველების სახით:

1) დაცვის იმუნური კლასიფიკატორების ცნობილი მუქარების ველები და

2) დაცვის რეცეპტორული დონის კლასიფიკატორების სასიცოცხლო გამოცდილების ველები.

პირველ შემთხვევაში ადაპტაციის პროცესი დაკავშირებულია კლასიფიკაციის ამოცანების გადაწყვეტასთან, მუქარების კლასტერიზაციასთან შეტევების ნიშნების მიხედვით, რომლებსაც მივყავართ ცნობილი მუქარების ინფორმაციული ველების ცვლილებასთან იდს-ის ქვედა დონეზე. მუქარათა ჩამონათვალის ცვლილება აისახება იდს-ის იერარქიის ზედა დონეზე სასიცოცხლო გამოცდილების ინფორმაციული ველების შესაბამის მოდიფიკაციებში.

მეორე შემთხვევაში ადაპტაციის პროცესი დაკავშირებულია კლასიფიკაციის ამოცანების გადაწყვეტასთან, დაცვის მექანიზმების კლასტერიზაციასთან მუქარათა ნიშნების მიხედვით, რომლებსაც მივყავართ იდს-ის იერარქიის ზედა დონეზე ინფორმაციული ველის გაფართოებასთან. კლასიფიკატორების სწავლების პროცესში იცვლება იმუნური და რეცეპტორული დონეების ინფორმაციული ველები, ადექვატურად სახეცვლილებას განიცდის არამკაფიო პრედიკატული წესების სისტემები და ადპტირებადი ექსპერტული შეფასების მატრიცები.

თუ იდს-ის ადაპტური მოდელისათვის ბაზისად ავირჩევთ მრავალდონიანი მოდელირებიდან ერთ-ერთს, მაშინ დასაწყისში იდს-ის ადაპტურ მოდელში მოთავსებული იქნება დაცვის მექანიზმების მინიმალური რაოდენობა, რომელიც საკმარისია იტ-სისტემებში გამოვლენილი მოწყვადობების დასაცავად. მათი ჩამონათვალი შეივსება მუქარათა ველის ყოველი ცვლილებისას და ცალკეული პოტენციური მოწყვლადობები გამოვლენილის სტატუსით შეიცვლება.

დაცვის მექანიზმების საწყისი დანაწილება იუს მოდელის დონეების მიხედვით განსაზღვრავს ექსპერტულ შეფასებათა მატრიცის განზომილებას, ხოლო ცვლილებები იუს-ის მოდელში აისახება ექსპერტული შეფასების მატრიცის სტრიქონებისა და სვეტების ელემენტების რაოდენობასა და მნიშვნელობებზე.

ექსპერტული შეფასების მატრიცისათვის აწარმოებენ დაცულობის მაჩვენებლების და იტ-სისტემის რეიტინგის გაანგარიშებას, რომლებიც გამოიყენება იტ-სისტემის დაცულობის შეფასების მეთოდიკაში ანალიზისა და კორექციისათვის, როგორც მნიშვნელობების შეფასებათა მატრიცაში, ასევე იმუნური და რეცეპტორული დონეების ფუნქციონალური პარამეტრების ნეიროქსელური კლასიფიკატორებისათვის, და ასევე შესაბამისი არამკაფიო პრედიკატული წესების სისტემებისათვის.

ინფორმაციული უსაფრთხოების ექსპერტების გამოცდილება, რომელიც წარმოდგენილია მატრიცულ ფორმაში, გარდაისახება არამკაფიო წესების სისტემებში, რომლებიც აღწერს შესაბამის გზავნილებს და დასკვნებს, მაგალითად:

Π_1: თუ $\tilde{x}_1$ არის A_{11} და ... $\tilde{x}_{n1}$ არის A_{1n}, მაშინ $\tilde{y} = B_1$,

Π_2: თუ $\tilde{x}_1$ არის A_{21} და ... $\tilde{x}_{n1}$ არის A_{2n}, მაშინ $\tilde{y} = B_2$,

$\vdots$

Π_k: თუ $\tilde{x}_1$ არის A_{k1} და ... $\tilde{x}_n$ არის A_{kn}, მაშინ $\tilde{y} = B_k$,

სადაც $\tilde{x}$ და $\tilde{y}$ – არის არამკაფიო შემავალი ცვლადი და გამოტანის ცვლადი, ხოლო A_{ij} და B_i, $i = \overline{1,k}$, $j = \overline{1,n}$ – გაწევრიანების ფუნქციებია.

განსახილველ მოდელში (ნახ.3) ასახულია იუს-ის იმუნური და რეცეპტული დონეები. იმუნური დონე წყვეტს მუქარების $x_j, j = \overline{1,N}$ (დასკვნები) კლასიფიკაციის ამოცანას შეტევათა ნიშნების $P_i, i = \overline{1,P}$ (გზავნილები) მიხედვით, ხოლო რეცეპტული დონე წყვეტს დაცვის მექანიზმების კლასიფიკაციის მსგავს ამოცანას $Z_k, k = \overline{1,K}$ (დასკვნები) მუქარათა ველის $x_j, j = \overline{1,N}$ (გზავნილი) მიხედვით. არამკაფი პრედიკატული წესების სისტემები, თავის მხრივ, ასახავს არამკაფიო ნეირონულ ქსელებს „გამჭვირვალე“ სტრუქტურაში, რომელიც განკუთვნილია ადაპტაციის პროცესის შედეგების, შემდგომი სწავლებისა და ანალიზისათვის.

იუს-ის ყოველი დონის კლასიფიკატორები ორგანიზებულია შემდეგი სქემით:

ექსპერტული შეფასებების მატრიცა → არამკაფიო პრედიკატული წესების სისტემა → არამკაფიო ნეირონული ქსელები → თვითშემსწავლელი ნეირონული ქსელები

თვითშემსწავლელი ნეირონული ქსელები აუცილებელია კლასიფიკაციის ამოცანის გადასაწყვეტად. თვითშესწავლის პროცესში ნქ აღწევეს ვექტორების ისეთ დაყოფას ჯგუფებად, რომ ჯგუფების რიცხვი მკაფიო კლასიფიკატორში დაემთხვეს წესების რიცხვს არამკაფიო პრედიკატული წესების სისტემაში.

უკანასკნელი პირობა აუცილებელია ადაპტური კლასიფიკატორის შესაქმნელად, რომელიც გზავნილების ვექტორის ცვლილებისას შეცვლის (აუცილებლობის შემთხვევაში) დასკვნების ვექტორის განზომილებას. ე.ი. წყვეტს რა კლასიტერიზაციის ამოცანას, მკაფიო ნქ ცვლის დასკვნების ვექტორის განზომილებას, რაც იწვევს ახალი წესების დამატებას არამკაფიო პრედიკატული წესების სისტემაში და შესაბამისი ფორმალური ნეირონების დამატებას არამკაფიო ნქ-ში. არამკაფიო ნქ-ის სწავლება და ახლად შემოტანილი ფორმალური ნეირონების კავშირების წონების ანალიზი, საშუალებას იძლევა ფორმალიზებულ იქნეს სპეციფიკაცია იუს-ში დაცვის მექანიზმების არ არსებობის შესახებ.

იუს მუშაობის პროცესში ხდება იტ-სისტემის გამოცდილების დაგროვება არამკაფიო პრედიკატული წესების სისტემის ადაპტაციის მეშვეობით, ასევე არამკაფიო ნქ პარამეტრების და ექსპერტული შეფასებების მატრიცის მეშვეობით. ექსპერტული შეფასების მატრიცის კორექცია ცვლის იტ-სისტემის დაცულობის მაჩვენებლების სისტემას, რომელიც საშუალებას იძლევა თვალყური მიედევნოს (იტ-სისტემის დაცულობის შეფასების მეთოდიკის მეშვეობით) ინფორმაციის დაცვის დინამიკას და მიღებულ იქნას გადაწყვეტილებები დმ-ის სტრუქტურასა და შემადგენლობასთან დაკავშირებით.

ახლა შევეცდებით წარმოვადგინოთ იტ-სისტემების დაცულობის მაჩვენებლების კომპლექსი. ადაპტური დაცვის მოდელში ერთ-ერთ უმთავრეს კომპონენტს წარმოადგენს დაცულობის მაჩვენებლების გაანგარიშების ბლოკი, რომელიც იტ-სისტემის დაცულობის მეთოდიკასთან ერთად საშუალებას მოგვცემს:

- უზრუნველყოფილ იქნას იუს-ს ოპტიმალურთან მიახლოებული თანაფარდობა „ღირებულება /ეფექტურობა“ მხოლოდ აუცილებელი დაცვის მექანიზმებით შევსების ხარჯზე;
- დინამიკაში დავაკვირდეთ დაცვის მექანიზმების დატვირთვას მუქარათა ველის შეცვლისას;
- მოვახდინოთ მოთხოვნების სპეციფიკაციების ფორმირება არ არსებულ დაცვის მექანიზმებზე;
- შევაფასოთ იტ-სისტემის დაცულობა მოსალოდნელი ზარალის სიდიდისა და დმ-ის აქტიურობის ინტეგრალური მაჩვენებლების მიხედვით, რომელიც განაწილებულია იუს-ის იერარქიების მიხედვით.

გადაწყვეტილება შეტევატა კლასიფიკაციის და დაცვის მექანიზმების გაფართოებაზე ხორციელდება შეფასებათა იმ სისტემის მეშვეობით, რომელითაც ფასდება მუქარების ნეიტრალიზების უტყუარობა და მოსალოდნელი ზარალის ანალოგიური შეფასებები ცალკეული დმ-ის ჭრილში. ზარალს ჩვენ განვიხილავთ ფარდობით სიდიდეებში, მაგალითად, საწარმოს კორპორაციული სისტემის დასაშვები ზარალის სიდიდესთან მიმართებაში.

ექსპერტული შეფასებების შედეგები, ასევე არამკაფიო ნქ-ის შემდგომი სწავლება შეიძლება წარმოვადგინოთ უტყუარობის მატრიცის ME „მუქარები – დაცვის მექანიზმები“ სახით:

$$ME_{mxn} = \begin{bmatrix} m\ell_{11} & m\ell_{12} & \vdots & m\ell_{1n} \\ m\ell_{21} & m\ell_{22} & \vdots & m\ell_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ m\ell_{m1} & m\ell_{m2} & \vdots & m\ell_{mn} \end{bmatrix}$$

სადაც $i = 1, \cdots m$ – არის დაცვის მექანიზმების რიცხვი, $j = 1, \cdots n$ – არის იუს-ის ეშელონების რიცხვი. იუს-ის ელემენტების აქტიურობას მუქარების განეიტრალებაზე, რომელიც შედის სისტემაში პრედიკატული წესების გზავნილების სახით, განსაზღვრავენ ინტეგრალური მაჩვენებლების სტრიქონით. მაგალითად, ეშელონის მნიშვნელობის მაჩვენებლის სტრიქონით მრავალდონიან იუს-ში.

$$x_i = \sqrt[m]{\prod_{i=1}^{m} m\ell_{ij}}, \; j = 1,\ldots,n \qquad (1)$$

რომლებიც ნორმირებულია, მაგალითად x_{ij} -დან (j=1,...,n) მაქსიმალური მნიშვნელობის მიხედვით ან მნიშვნელოვნობის მაჩვენებლების სტრიქონის ელემენტების ჯამის $\sum_{j=1}^{h} x_j, j = 1,\ldots,n\,1$ მიხედვით. ინტეგრალური მაჩვენებლების შედარება სტრიქონის ფარგლებში ყველაზე უფრო აქტიური ეშელონის გამოვლენის საშუალებას იძლევა.

აქტიურობის უტყუარობის მატრიცის ანალოგიურად მუქარების ნეიტრალიზებისათვის შეიძლება მივიღოთ დაცვის ცალკეული მექანიზმების გამოყენების აქტიურობის ინტეგრალური მაჩვენებლების სვეტი მრავალდონიანი იუს-ის ყველა ეშელონებზე.

$$x_i = \sqrt[n]{\prod_{i=1}^{n} m\ell_{ij}}, i = 1,\ldots,m \qquad (2)$$

ინტეგრალური მაჩვენებლების შედარება სვეტის ფარგლებში საშუალებას იძლევა გამოვავლინოთ ყველაზე უფრო ამოქმედებული დაცვის მექანიზმები მრავალდონიანი იუს-ისათვის.

უტყუარობის მატრიცის ინტეგრალური მაჩვენებლების ანალიზი საშუალებას იძლევა დავასაბუთოთ დაცვის მექანიზმების გამოყენების მიზანშეწონილობა მრავალდონიანი იუს-ის შესაბამისი ეშელონისათვის.

ექსპერტული შეფასებების გამოყენება და მათი შემდგომი ასახვა ნეირო-არამკაფიო ქსელის სტრუქტურაში უნდა ხდებოდეს ექსპერტების გამოკითხვის შედეგების საფუძველზე. ექსპერტული შეფასებების არაწინააღმდეგობრიობის უზრუნველყოფა კი შესაძლებელია, მაგალითად, ექსპერტული შეფასების არამკაფიო დამოკიდებულების მატრიცის მეთოდით [6] ან მეთოდით, რომელიც დაფუძნებულია წყვილ-წყვილი შედარების მატრიცის მაქსიმალური საკუთარი მნიშვნელობების გაანგარიშებაზე [7].

მოყვანილი მაჩვენებლები უფრო ინფორმაციული იქნება, თუ გავითვალისწინებთ არამარტო დმ-ის გამოყენების უტყუარობას იუს-ის სტრუქტურაში, არამედ მოსალოდნელი ზარალის მაჩვენებლებსაც, რომელიც წარმოიშობა იტ-სისტემაზე შეტევის დროს და რომელიც შესაძლებელია ავიცილოთ თავიდან ინფორმაციული უსაფრთხოების სისტემის წყალობით. ამ მიზნით [6]-ის გათვალისწინებით, დაცულობის შეფასება ირიბად შეიძლება დავაკავშიროთ იტ-სისტემაში ზარალის თავიდან აცილებასთან და ექსპერტული შეფასებები გამოვიყენოთ იუ-ს მუქარების ველის მათი რეალიზაციის პოტენციურ ზარალთან შესადარებლად.

ა) იტ-სისტემის დაცულობის შეფასების მეთოდიკა

მრავალდონიანი იუს-ის ყოველი ეშელონისათვის ფორმირდება ექსპერტული შეფასებები – ველის ნეიტრალიზების უტყუარობა და მოსალოდნელი ზარალი, გამომდინარე საგნობრივი არის სპეციალისტების გამოცდილებიდან. მოსალოდნელი ზარალის გაანგარიშება ხდება დროის გარკვეულ მონაკვეთში მუქარათა აქტიურობის სიხშირის გათვალისწინებით. იტ-სისტემის დაცულობის მაჩვენებლების კომპლექსი (რომლის პროგრამული რეალიზაცია სავსებით შესაძლებელია) მოიცავს შემდეგ ძირითად ელემენტებს.

1. საწყისი მონაცემები – ექსპერტული მონაცემების წარმოდგენა ხდება მატრიცული ფორმით. იუს-ს ყოველი ეშელონისათვის ფასდება დაცვის მექანიზმებით მუქარების ნეიტრალიზების უტყუარობა და ფორმირდება უტყუარობის მატრიცა „დაცვის მექანიზმები-მუქარა“ MT:

$$MT_{mxp} = \begin{pmatrix} mt_{11} & mt_{12} & \vdots & mt_{1p} \\ mt_{21} & mt_{22} & \vdots & mt_{2p} \\ \ldots & \ldots & \ldots & \ldots \\ mt_{m1} & mt_{m2} & \vdots & mt_{mp} \end{pmatrix},$$

სადაც $i = 1,\ldots,m$ – არის დაცვის მექანიზმების რაოდენობა (რიცხვი), $j = 1,\ldots,p$ – არის ცნობილი მუქარების რიცხვი, და „მუქარები-ეშელონები“ უტყუარობის მატრიცა TE.

$$TE_{pxn} = \begin{pmatrix} te_{11} & te_{12} & \vdots & te_{1n} \\ te_{21} & te_{22} & \vdots & te_{2n} \\ \dots & \dots & \dots & \dots \\ te_{p1} & te_{p2} & \vdots & te_{pn} \end{pmatrix}$$

$i = 1,\dots,n-$ არის ცნობილი მუქარების რიცხვი, $j = 1,\dots,n-$ არის იუს-ის ეშელონების რიცხვი.

მრავალდონიანი იუს-ის ყოველი ეშელონისათვის ცალკე ფასდება მოსალოდნელი ზარალის დონე და ფორმირდება მატრიცები „ეშელონი-ზარალი“ ET.

$$ET_{nxp} = \begin{pmatrix} et_{11} & et_{12} & \vdots & et_{1p} \\ et_{21} & et_{22} & \vdots & et_{2p} \\ \dots & \dots & \dots & \dots \\ et_{m1} & et_{m2} & \vdots & et_{np} \end{pmatrix}$$

$i = 1,\dots,n-$ არის იუს-ის ეშელონების რიცხვი, $j = 1,\dots,p-$ არის ცნობილი მუქარების რიცხვი.

$$TM_{pxm} = \begin{pmatrix} tm_{11} & tm_{12} & \vdots & tm_{1m} \\ tm_{21} & tm_{22} & \vdots & tm_{2m} \\ \dots & \dots & \dots & \dots \\ tm_{p1} & tm_{p2} & \vdots & tm_{pm} \end{pmatrix}$$

$i = 1,\dots,p-$ არის ცნობილი მუქარების რიცხვი, $j = 1,\dots,m-$ არის დაცვის მექანიზმების რიცხვი.

2. იუს-ს ყოველი ეშელონისთვის არამკაფიო პრედიკატული წესების ექსპერტულ შეფასებებს ასახეავენ ნეირონულ-არამკაფიო ქსელების სტრუქტურაში. არამკაფიო ნქ-ის შემდგომი ადაპტაციის პროცესში იდს-ის შემადგენლობაში სწავლების ამონარჩევში, რომელიც შეესაბამება ცნობილი მუქარების ველის რაღაც ქვესიმრავლეს, ხდება არამკაფიო პრედიკატული წესების სისტემის, ასევე მოსალოდნელი ზარალის მაჩვენებლების ავტომატური კორექცია. საწყისი ექსპერტული შეფასებების კორექტულობა შეიძლება შემოწმდეს ზევით ჩამოთვლილი მატრიცების ელემენტების დაპირისპირებით ან დაცულობის იმ ინტეგრალური შეფასებების დაპირისპირებით, რომლებიც მიღებულია იდს-ის ნეირო-არამკაფიო სწავლების პროცესის დაწყებამდე და დაწყების შემდეგ.

დაცულობის ინტეგრალური შეფასებები შეიძლება მივიღოთ მატრიცებზე ოპერაციების შედეგად. კერძოდ, გამრავლება უტყუარობის მატრიცის „დაცვის საშუალებები – მუქარები“ MT და „მუქარები – ეშელონები“ TE მატრიცის გადამრავლების შედეგად მიიღება „დაცვის მექანიზმები – ეშელონები“ MT – დაცვის მექანიზმების აქტივიზაციის უტყუარობის მატრიცა, რომელიც განაწილებულია მრავალდონიანი იუს-ის ეშელონების მიხედვით, ცნობილი მუქარების ნეიტრალიზებისათვის.

$$ME_{mxn} = \begin{pmatrix} me_{11} & me_{12} & \vdots & me_{1n} \\ me_{21} & me_{22} & \vdots & me_{2n} \\ \dots & \dots & \dots & \dots \\ me_{m1} & me_{m2} & \vdots & me_{mn} \end{pmatrix}$$

არის $i = 1,\dots,n-$ არის დაცვის მექანიზმების რიცხვი, $j = 1,\dots,m-$ არის იუს-ის ეშელონების რიცხვი, ხოლო მოსალოდნელი ზარალის მატრიცის „ეშელონი-ზარალი“ ET და „ზარალი–დმ“ TM მატრიცის გამრავლება – იძლევა მოსალოდნელი ზარალის „ეშელონები – დმ“ EM მატრიცას, რომელიც ასახავს მოსალოდნელ ზარალს.

$$EM_{mxn} = \begin{pmatrix} em_{11} & em_{12} & \vdots & em_{1m} \\ em_{21} & em_{22} & \vdots & em_{2m} \\ \dots & \dots & \dots & \dots \\ em_{n1} & em_{n2} & \vdots & em_{nm} \end{pmatrix}$$

$i=1,...,n-$ არის იუს-ის ეშელონების რიცხვი, $j=1,...,m-$ არის დაცვის მექანიზმების რიცხვი. ინტეგრალური მახასიათებლების შუალედური შეფასებები სტრიქონების (1) და სვეტების (2) სახით ახასიათებს მრავალდონიანი იუს-ის ფარგლებში დაცვის ცალკეული მექანიზმებისა ან ეშელონების გამოყენების აქტუალურობას. ასევე საშუალებას იძლევა შეფასდეს პოტენციური ზარალი იუს-ის დაცვის მექანიზმებისა და ეშელონების ჭრილში.

4. შემდგომი ოპერაციები მატრიცებზე *ME* და *EM* საშუალებას იძლევა ჯამური მატრიცის დიაგონალურ ელემენტებში განვაზოგადოთ, როგორც შეტევის შედეგად დაცვის მექანიზმების აქტივაციის უტყუარობის მაჩვენებელი. უტყუარობის მატრიცის *ME* და მოსალოდნელი ზარალის მატრიცის *EM* გამრავლებით ვღებულობთ უტყუარობისა მოსალოდნელი ზარალის „დმ – დმ“ *MM* კვადრატულ მატრიცას.

$$EM_{mxn}=\begin{pmatrix} mm_{11} & mm_{12} & \vdots & mm_{1m} \\ mm_{21} & mm_{22} & \vdots & mm_{2m} \\ \dots & \dots & \dots & \dots \\ mm_{m1} & mm_{m2} & \vdots & mm_{mm} \end{pmatrix}$$

$i=1,...,m-$ არის დმ რიცხვი, ხოლო *EM* მატრიცის და *ME* მატრიცის გამრავლებით ვღებულობთ, მოსალოდნელი ზარალის „ეშელონი–ეშელონი“ *EE* უტყუარობის კვადრატულ მატრიცას.

$$EE_{nxn}=\begin{pmatrix} ee_{11} & ee_{12} & \vdots & ee_{1n} \\ ee_{21} & ee_{22} & \vdots & ee_{2n} \\ \dots & \dots & \dots & \dots \\ ee_{n1} & ee_{n2} & \vdots & ee_{nn} \end{pmatrix}$$

$i=j=1,...,n-$ არის იუს-ის ეშელონების რიცხვი.

MM მატრიცისათვის განზოგადოებულ მაჩვენებლად შეიძლება ჩავთვალოთ ვექტორი, რომელიც წარმოიშობა $mm_{ij}==p_i, i=j=1,...,m$, მატრიცის დიაგონალური ელემენტებისაგან – არის მოსალოდნელი ზარალის განაწილებისა უტყუარობის ვექტორი იუს-ის დაცვის მექანიზმების მიხედვით:

$$P_{1xm}=(P_1,P_2,...,P_m).$$

ხოლო *EE* მატრიცისათვის – ვექტორი შედგენილი მისი დიაგონალური ელემენტებისაგან; $ee_{ij}=d_i, i=j=1,...,n$ – იუს-ის ეშელონების მიხედვით მოსალოდნელი ზარალის განაწილების უტყუარობის ვექტორი.

$$D_{1xn}=(d_1,d_2,...,d_n)$$

5. იტ-სისტემის დაცულობის ინტეგრალურ შეფასებად დაცვის მექანიზმების ჭრილში შეიძლება ჩავთვალოთ რეიტინგული მაჩვენებელი R_m-P_{1xm} ვექტორის $m-$ განზომილების სიგრძე

$$R_m=\left|P_{1xm}\right|=\sqrt{\sum_{i=1}^{m}p_i^2},\ \ i=1,...,m$$

ხოლო ეშელონის ჭრილში – რეიტინგული მაჩვენებელი R_E-D_{1xn} ვექტორის $n-$ განზომილების სიგრძე

$$R_E=\left|D_{1xn}\right|=\sqrt{\sum_{i=1}^{m}d_i^2},\ \ i=1,...,m$$

იუს-ის მიმდინარე ეფექტურობა შეიძლება შევაფასოთ ფარდობით სიდიდეებში, ზღვრული მნიშვნელობების სახით გამოვიყენოთ $R_{m\,max}$ და $R_{E\,max}$ მაჩვენებლების რეიტინგული მაქსიმალური მნიშვნელობები, რომელიც ითვალისწინებს იუს-ის სანდოობას ყველა ეშელონებში.

$$\eta_m = \frac{R_m}{R_{m_{max}}}; \quad \eta_E = \frac{R_E}{R_{E_{max}}}$$

მაჩვენებლების გამოყენება შესაძლებელია სისტემების ცნობილი მუქარების ველებისა და მუქარათა ველის ქვესიმრავლეების (ინფორმაციის მთლიანობის, კონფიდენციალობის, ხელმისაწვდომობის დარღვევის) დაცულობის შესაფასებლად.

ლიტერატურა:

1. Осовенский Л.Г. Научно-технические предпосылки роста роли защиты информации в современных информационных технологиях. Изв. ВУЗов. Приборостроение, 2003, т. 46, №7.
2. Минаев В.А., Перспективы развития IT-security в России. Межотраслевой тематический каталог „Системы безопасности – 2003“, 2003.
3. Кузнецов В.А., Раков М.А. Самоорганизация в технических системах. Киев. наук думка. 1987.
4. Мелик-Гайназян И.В. Информационные процессы и реальность. – М.: Наука, 1998.
5. Нестерук Г.Ф., Купрянов М.С., Нестерук Ф.Г. О разработке языковых средств для программирования нейросетевых структур. Сб. докл. V Междун.конф. по мягким вычислениям и измерениям SCM 2002. СПб: СПГЭТУ, 2002, т. 2.
6. Жижелев А.В., Панфилов А.П., Язов Ю.К. Батищев Р.В. К оценке эффективности защиты информации в телекоммуникационных системах посредством нечетких множеств. Изв. ВУЗов. Приборостроение, 2003, т. 46, №7.
7. Корнев В.В., Гарев А.Ф., Васютин С.В. Базы данных. Интеллектуальная обработка информации. – М.: Нолидж, 2001.

THE ADAPTIVE MODEL OF INFORMATION PROTECTION

Shonia Otar, Japaridze Giorgi, Iremadze Ia

Georgian Technical University

Summary

The guarantee of information protection occurs under the conditions of the random action of the most different factors. Some of them are systematized according the standards, whereas others are unpredictable and capable of decreasing effectiveness or compromising the provided measures. The estimation of the effectiveness of protection must compulsorily consider both the objective circumstances and probabilistic factors. Today specialists from the most different fields of knowledge are occupied by questions of providing information security. This is because of the fact that in the nearest future we will live in the society (environment) of information technology, where problems of information security is of key importance.

АДАПТИВНАЯ МОДЕЛЬ ЗАЩИТЫ ИНФОРМАЦИИ

Шония О.Б., Джапаридзе Г.Т. Иремадзе И.З.

Грузинский Технический Университет

Резюме

Обеспечение защиты информации на практике происходит в условиях случайного воздействия самых разных факторов. Некоторые из них систематизированы в стандартах, некоторые заранее неизвестны и способны снизить эффективность или даже скомпрометировать предусмотренные меры. Оценка эффективности защиты должна обязательно учитывать как объективные обстоятельства, так и вероятностные факторы. Сегодня специалисты из самых разных областей знаний, так или иначе, вынуждены заниматься вопросами обеспечения информационной безопасности. Это обусловлено тем, что в ближайшие лет сто нам придется жить в обществе (среде) информационных технологий, куда перекочуют все социальные проблемы человечества, в том числе и вопросы безопасности.