# ევოლუციური ალგორითმები ინფორმაციის დაცვის ამოცანებში

გულნარა ჯანელიძე, ბადრი მეფარიშვილი
საქართველოს ტექნიკური უნივერსიტეტი

## რეზუმე

ქსელური თავდასხმების მუდმივად ცვალებადი ხასიათი მოითხოვს მოქნილი დაცვის სისტემის შექმნას, რომელსაც ექნება ქსელური ტრაფიკის დიდი მოცულობის გაანალიზების უნარი. ინფორმაციის დაცვის ინტელექტუალური სისტემების ორგანიზებისთვის საბაზოა ნეირონული ქსელები. მსგავსმა სისტემებმა უნდა უზრუნველყოს ავტომატური და ოპერატიული რეაქცია დასაცავი სისტემის მოწყვლადობის ხასიათის ან საფრთხეთა სივრცის ცვლილებებისას, რასაც მივყავართ ინფორმაციის დაცვის სისტემებში ევოლუციური მეთოდების გამოყენებასთან. შემოთავაზებულია გენეტიკური ალგორითმის გამოყენებით ნეირონული ქსელის კავშირების წონების ოპტიმიზაციის ამოცანის გადაწყვეტა, ქსელის როგორც უცვლელი ტოპოლოგიის, ასევე შესაბამისობის ფუნქციის მიხედვით ცვალებადი ტოპოლოგიის შემთხვევებისთვის.

**საკვანძო სიტყვები:** გენეტიკური ალორითმი. ნეირონული ქსელი. წონების ოპტიმიზაცია.

## 1. შესავალი

ქსელური რესურსების უსაფრთხოების ამოცანების გადასაწყვეტად საკმაოდ ეფექტურად გამოიყენება ნეირონული ქსელების მეთოდი. ნეირონული ქსელები სახეთა შეცნობისა და კლასიფიკაციის სხვადასხვა პრაქტიკული ამოცანის ამოხსნის საშუალებას იძლევა. ამ მეთოდის უპირატესობაა, რომ მათ შეუძლიათ ავტომატურად მოიპოვონ ცოდნა განსწავლის პროცესში და აქვთ განზოგადების უნარი. ქსელის ძირითადი ელემენტია ხელოვნური ნეირონი – ბიოლოგიური ნერვული უჯრედის მათემატიკური მოდელი[1].

ნეიროქსელების განსწავლის მოდულის ძირითადი ამოცანაა ხარისხიანად განსწავლული ქსელის მომზადება თავდასხმის ამოსაცნობად. ოპერატორი, რომელიც მუშაობს მოცემულ მოდულთან განიწავლის ნეირონულ ქსელს და აანალიზებს ქსელის პარამეტრებს განსწავლის შემდეგ, რის საფუძველზეც აკეთებს მისი მიმდინარე მდგომარეობის შეფასებას. ნეიროქსელების განსწავლის პროგრამასთან მუშაობის დამთავრების შემდეგ, ოპერატორი ინახავს ქსელის მიმდინარე მაჩვენებლებს, რომლებიც შემდგომ გამოყენებული იქნება მოცემული ქსელის განსაახლებლად ქსელური ტრაფიკის ანალიზატორში.

თანამედროვე პერიოდში მრავალ ანტივირუსულ უტილიტაში, ქსელური დაცულობის ანალიზის პროგრამებში, შეიმჩნევა ხელოვნური ინტელექტის ტექნოლოგიების გამოყენების მასშტაბების ზრდის ტენდენცია. ამას ხელს უწყობს მასში განსწავლის შესაძლებლობების არსებობა, ხელოვნური ინტელექტის მეთოდების აქტიური განვითარება, ქსელური საფრთხეების რიცხვისა და სირთულის ზრდა.

## 2. ძირითადი ნაწილი

განვიხილოთ ინფორმაციული უსაფრთხოების პრაქტიკულ ამოცანაში ნეირონული ქსელის გამოყენების მაგალითი, სადაც ნეირონული ქსელის საშუალებით საჭიროა მონაცემთა ბაზაზე წვდომის დეტექტირება რომელიმე პროგრამული უზრუნველყოფიდან ან ანომალიის განსაზღვრა მომხმარებლის მუშაობაში. ნეირონულ ქსელს აქვს ოთხი შესასვლელი, რომელთაგანია:

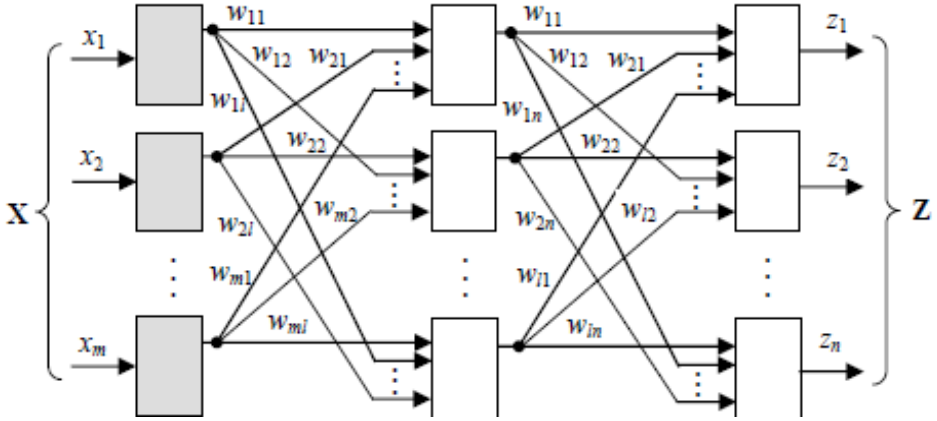
- ინფორმაციის მოცულობა, რომელიც ჩაიტვირთება მონაცემთა ბაზიდან საკონტროლო პერიოდის განმავლობაში. მიღებული მნიშვნელობა უნდა იქნას ნორმალიზებული, რამდენადაც მონაცემთა ბაზიდან წაკითხული მოცულობა წინასწარ არ არის ცნობილი და ინდივიდუალურია

ცალკეული ამოცანისათვის და ცალკეული მომხმარებლისათვის. ნორმალიზაციის სახით შეიძლება გამოყენებულ იქნას ტრაფიკის შეფასება ათქულიანი სკალით, ანუ 0 აღნიშნავს, რომ მოცულობა ნულის ტოლია, 10 აღნიშნავს ტრაფიკის მაქსიმალურ მოცულობას;

- წუთში ტრანზაქციის რაოდენობა;

- წუთში მონაცემთა მოდიფიკაციის ოპერაციის რაოდენობა. ამ მაგალითში ავტომატიზებული მუშა ადგილი იყენებს მოკლე ტრანზაქციებს, ანუ ერთი ტრანზაქციის ჩარჩოში ჩვეულებრივ შეიძლება იყოს მონაცემების მოდიფიკაციის 1-2 ოპერაცია;

- მონაცემთა ბაზების ლექსიკონზე მიმართვის ნიშნები. უმეტესობა კლიენტის ავტომატიზებული მუშა ადგილი ლექსიკონს არ მიმართავს. რაც განასხვავებს მათ დამუშავებების საშუალებებისა და ადმინისტრირებისაგან. ნიშნები იქნება დისკრეტული 0 – არ არის მიმართვა, 1- არის მიმართვა, და მათ ექნებათ რამდენიმე - ცალკეულ ცხრილს თითო, ბაზის ლექსიკონი. მოცემულ მაგალითში გამოიყენება პირდაპირი განვრცობის ორფენიანი ნეირონული ქსელი, რომელიც შეიცავს ორი ნეირონისაგან შემდგარ ერთ ფარულ ფენას და გამომავალ ფენას ერთი ნეირონით (ნახ.1).




**ნახ.1. ორფენიანი ნეირონული ქსელი**

ნეირონული ქსელის გამოსასვლელი შეიძლება იქნას ინტერპრეტირებული როგორც მიმდინარე ქმედებების ხაკერის მოქმედებებთან პროცენტული შესაბამისობა. ასეთივე ხერხით შეიძლება იქნას ორგანიზებული სხვადასხვა თავდასხმის განსაზღვრა და ახალი ტიპის საფრთხეთა მიმართ ადაპტაცია.

ინფორმაციის დაცვის ინტელექტუალური სისტემების ორგანიზებისთვის საბაზოა ნეირონული ქსელები. არსებულ ექსპერტულ სისტემებში ნეირონული ქსელი გამოიყენება შემოსული შეტყობინებების ფილტრაციისათვის, ექსპერტული სისტემებისათვის დამახასიათებელი მცდარი შედეგების რაოდენობის შემცირების მიზნით. მხოლოდ, თუ განსწავლის შემდეგ ნეირონულმა ქსელმა დაიწყო ახალი თავდასხმების იდენტიფიცირება, მაშინ ექსპერტული სისტემის ცოდნის ბაზა უნდა განახლდეს. წინააღმდეგ შემთხვევაში ახალი შემოტევები მის მიერ იქნება იგნორირებული, ვინაიდან ახალი საფრთხეების შეცნობა შეუძლებელი იქნება ძველი წესების მიერ [1,2].

ნეირონული ქსელის ბაზაზე ორგანიზებულ ინფორმაციის დაცვის სისტემას აქვს ტრაფიკის დამუშავების და გაანალიზების უნარი შემოსული ინფორმაციის ბოროტად გამოყენების არსებობის შემთხვევაში. თუმცა ნეირონული ქსელების ძირითადი ნაკლი არის ანალიზის შედეგების ფორმირების გაუმჭვირვალობა. მხოლოდ ჰიბრიდული, როგორიცაა ნეირო-ექსპერტული ან ნეირო-არამკაფიო სისტემების გამოყენება იძლევა საშუალებას ნეირონული ქსელის სტრუქტურაში ცხადად გამოისახოს If (პირობა) – Then (ქმედება) წესების სისტემა. აღნიშნული წესები ავტომატურად კორექტირდება ნეირონული ქსელის განსწავლის პროცესში. ნეირონული ქსელების ადაპტურობის თვისებას უნარი აქვს არამარტო ამოხსნას საფრთხის იდენტიფიკაციის და მომხმარებლის ქცევის სისტემაში არსებულ

შაბლონებთან შესაბამისობის ამოცანა, არამედ ავტომატურად გაუკეთოს ფორმირება ახალ წესებს საფრთხის ველის შეცვლისას.

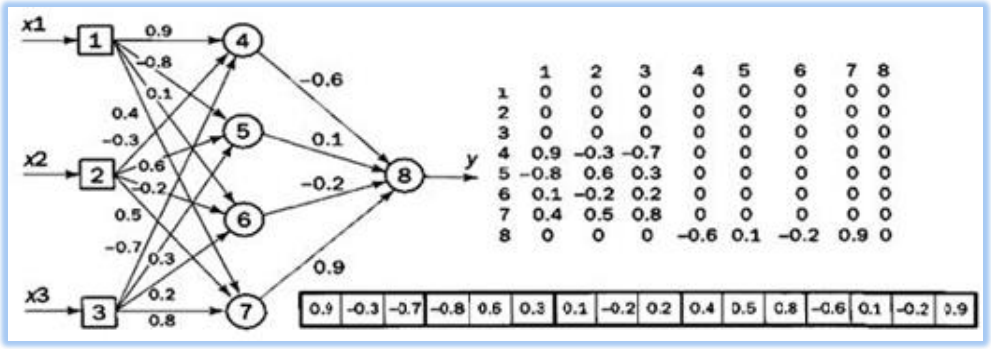
ევოლუციური მეთოდები გამოიყენება მრავალპარამეტრიანი ოპტიმიზაციის ამოცანების გადასაწყვეტად. როგორც წესი მსგავს შემთხვევებში ფუნქცია შეიძლება გამოვსახოთ შემდეგი სახით: $f(x_1, x_2, \dots \dots x_n)$, სადაც n პარამეტრების რაოდენობაა. ნაპოვნი უნდა იქნას მოცემული ფუნქციის გლობალური მაქსიმუმი ან მინიმუმი. ინფორმაციის დაცვის ინტელექტუალურმა სისტემამ უნდა უზრუნველყოს ავტომატური და ოპერატიული რეაქცია დასაცავი სისტემის მოწყვლადობის ხასიათის ცვლილებისას ან საფრთხის ველის ცვლილებისას, რასაც მივყავართ ცოდნის ბაზის დინამიკურობიდან გამომდინარე ინფორმაციის დაცვის სისტემის ადაპტაციის ამოცანის გადაწყვეტასთან.

ინტელექტუალური საშუალებების მანქანური განსწავლის ევოლუციური მიდგომა ეფუძნება ბუნებრივი გადარჩევის და გენეტიკის გამოთვლით მოდელებს. ევოლუციური გამოთვლების მეთოდები მოიცავენ: გენეტიკურ ალგორითმებს, ევოლუციურ სტრატეგიებს და გენეტიკურ პროგრამირებას. ყველა ამ მეთოდით შესაძლებელია ევოლუციის მოდელირება გადარჩევის, მუტაციის და მწარმოებლურობის გამოყენებით.

ინფორმაციის დაცვის ნეიროქსელური სისტემებისათვის ევოლუციური მეთოდები და კერძოდ, გენეტიკური ალგორითმები გამოიყენება ნეირონული ქსელის განსწავლისას შეცდომების მინიმიზებისათვის. გენეტიკური ალგორითმები როგორც რთული სისტემების ოპტიმიზაციის მეთოდი მნიშვნელოვან ინტერესს იწვევს ნეიროქსელურ თემატიკასთან მიმართებით. გენური ალგორითმების ცნობილი მეთოდები, რომლებიც გამოიყენება ნეირონული ქსელების განსწავლისათვის ნეირონთაშორის კავშირების წონების ოპტიმიზაციის გზით, შეიძლება დაიყოს: ქსელის უცვლელი ტოპოლოგიისას კავშირების წონების ოპტიმიზაციის მეთოდებად და მოცემული შესაბამისობის ფუნქციის მიხედვით ცვალებადი ტოპოლოგიისას კავშირების წონების ოპტიმიზაციის მეთოდებად.

ტიპიური გენეტიკური ალგორითმი ნეირონული ქსელის კავშირების წონების ოპტიმიზაციისათვის მოიცავს შემდეგ ეტაპებს: ქრომოსომას კოდირება; შესაბამისობის ფუნქციის განსაზღვრა, რომლის მიხედვითაც განხორციელდება ცალკეული ნეირონული ქსელის გადარჩევა მისი ევოლუციის პროცესში; ევოლუციის მოდელირებისათვის გენეტიკური ოპერატორების შერჩევა, როგორიცაა: თანაკვეთა, ინვერსია, მუტაცია [3]. დასაწყისში ვნომრავთ ნეირონული ქსელის კვანძებს, შემავალი ფენიდან დაწყებული და მის ტოპოლოგიას წარმოვადგენთ კავშირების კვადრატული მატრიცის სახით, რომლის სტრიქონების(სვეტების) რაოდენობა ნეირონული ქსელის კვანძების რაოდენობის ტოლია. ამასთან მატრიცის თითოეული ელემენტი შეესაბამება ცალკეულ ნეირონთაშორის კავშირს და კავშირის წონის მნიშვნელობის ტოლია. თუ ნეირონთა შორის კავშირი არ არის, მაშინ მატრიცის ელემენტის მნიშვნელობა ნულის ტოლია (ნახ.2).

მოცემულ შემთხვევაში გენების რანგში შეირჩევა კავშირების წონების მნიშვნელობები, რომლებიც ასოცირდებიან ფორმალური ნეირონების შესასვლელებთან. ქრომოსომა წარმოადგენს წონების ჯგუფს, რომლებიც მიიღება წონების მატრიცის ცალკეული სტრიქონის მნიშვნელობებიდან. გენეტიკური ოპერაციების რანგში გამოიყენება: თანაკვეთა და მუტაცია. თანაკვეთის შედეგად მიიღება შვილი ქრომოსომას წყვილი ორი მშობლიდან შემთხვევით არჩეული ერთსახელიანი გენის გაცვლის გზით. მუტაციის ოპერატორი ახდენს ქრომოსომას გენის(წონის) ჩანაცვლებას მოცემული დიაპაზონიდან შემთხვევით აღებული წონით.




| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0.9 | -0.3 | -0.7 | 0 | 0 | 0 | 0 | 0 |
| 5 | -0.8 | 0.6 | 0.3 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0.1 | -0.2 | 0.2 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0.4 | 0.5 | 0.8 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | -0.6 | 0.1 | -0.2 | 0.9 | 0 |

**ნახ.2. გენეტიკური ალგორითმი ნეირონული ქსელის კავშირების წონების ოპტიმიზაციისათვის**

ცალკეულ ევოლუციურ ციკლში გამოითვლება ნეირონული ქსელის გამოსასვლელების მნიშვნელობები და შესაბამისობის ფუნქციები. ქრომოსომას გადარჩევა შემდგომ პოპულაციაში ხდება შესაბამისობის ფუნქციის მიხედვით. შემდგომ ხორციელდება მომდევნო ევოლუციური მცდელობა მანამ, სანამ თუნდაც ერთი ქრომოსომა არ დააკმაყოფილებს ნეირონული ქსელის განსწავლაში დასაშვები შეცდომების მოთხოვნებს.

ანალოგიურად გენეტიკური ალგორითმების გამოყენებით შესაძლებელია ნეირონული ქსელის ტოპოლოგიის ოპტიმიზაცია, ანუ ქსელში ნეირონების და ნეირონთაშორისი კავშირების ოპტიმალური რიცხვის შერჩევა. შევადგინოთ ქსელის კავშირების მატრიცა, რომლის ცალკეული ელემენტი აღვნიშნოთ 0-ით თუ ნეირონულ ქსელში კავშირი არ არის, ხოლო 1-ით - წინააღმდეგ შემთხვევაში. ქრომოსომა წარმოიქმნება კავშირების მატრიცის სტრიქონების მიმდევრობითი გაერთიანების გზით. ევოლუციური პროცესი მოიცავს შემდეგ ეტაპებს:

1. საწყისი პოპულაციის ფორმირება, ანუ მოცემული ინტერვალიდან აირჩევა საწყისი გენოტიპების წინასწარ განსაზღვრული რაოდენობის შემთხვევითი მნიშვნელობები;

2. საწყისი ამონახსნების შეფასება. იგი განსაზღვრავს სახეობის სიცოცხლისუნარიანობას მომდევნო იტერაციაში;

3. სახეობათა რანჟირება. რაც ითვალისწინებს სორტირების შედეგების შესაბამისად ყოველი სახეობისათვის რანგის მინიჭებას;

4. კროსოვერი. ამ ეტაპზე ხდება ლიდერთა ჯგუფის სახეობათა დაწყვილება რანგის შესაბამისად. ყოველი წყვილისათვის საუკეთესო წყვეტის წერტილის პოვნის თვალსაზრისით ხდება შიდაწყვილური გადარჩევის ციკლი, რომლის დროსაც წყვილთა ნაწილები ჯვარედინად შეიცვლება ანუ მიიღება შთამომავლობის შესაძლო ვარიანტები, რომლებიც შეფასდება მიზნობრივი ფუნქციის მიხედვით. შიდა ციკლის შედეგად განისაზღვრება საუკეთესო შეჯვარება და ორი შთამომავალი. თუმცა, თუ შთამომავალთა ფუნქციური შეფასება მშობელთა შეფასებაზე უარესი აღმოჩნდა, მაშინ მათ მიენიჭებათ მშობელთა შეფასება;

5. დახარისხება. ჩატარებული გენეტიკური ოპერაციების შემდეგ კვლავ ხდება სახეობათა სორტირება კლების მიხედვით, რომლის დროსაც გამოიკვეთება ლიდერი მაქსიმალური შემგუებლობის უნარით;

6. ალგორითმის დასრულება. მოცემულ ეტაპზე მოწმდება ლიდერის ფუნქციური მნიშვნელობა. თუ მომდევნო იტერაციაზე ლიდერის ფუნქციური მნიშვნელობა იზრდება, მაშინ გადავდივართ მომდევნო ეტაპზე. თუ ლიდერის ფუნქციური მნიშვნელობა აღარ განიცდის ზრდას ან პირიქით იწყებს კლებას, მაშინ გადავდივართ მოცემული სახეობის მუტაციაზე. თუ მუტაციის მეშვეობით მიზნობრივი ფუნქციის მნიშვნელობა არ გაიზარდა, მაშინ ალგორითმი ამთავრებს მუშაობას. რაც ნიშნავს რომ ოპტიმალური ამონახსნი მიღებულია. უნდა აღინიშნოს, რომ რამოდენიმე იტერაციის

შემდეგ პოპულაციის წევრები მნიშვნელობათა ერთ არეში განთავსდებიან, ეს არის ოპტიმუმის არე, საიდანაც მოხდება ოპტიმალური ამონახსნის ამორჩევა.

### 3. დასკვნა

ყოველივე ზემოაღნიშნულიდან გამომდინარე ხელოვნური ინტელექტის მეთოდების გამოყენება ქსელური სისტემების დაცვისათვის მეტად აქტუალურია. გენეტიკური ალგორითმები წარმოადგენენ ინტელექტუალური საშუალებების, კერძოდ ნეირონული ქსელების წონითი კავშირების ადაპტირებადი პარამეტრების ოპტიმიზაციის ეფექტურ საშუალებას. ზოგიერთი განხილული მეთოდი შეიძლება ჯერჯერობით ნაკლებად არის გამოყენებული, მაგრამ ცხადია, რომ მათ აქვთ დიდი პერსპექტივები ქსელური უსაფრთხოების სფეროში.

### ლიტერატურა - References - Литература:


1. Портал искусственного интеллекта. http://neuronus.com/nn/38-theory
2. http://cgm.computergraphics.ru
3. Андрианов В.И., Андронов А.В. «Эволюционные методы в задачах обеспечения безопасности автоматизированных систем», Журнал научных публикации аспирантов и докторантов, ISSN 1991-3087, http://jurnal.org/articles/2010/inf22.html


## EVOLUTIONARY ALGORITHMS OF INFORMATION PROTECTION PROBLEMS


Janelidze Gulnara, Meparishvili Badri

Georgian Technical University


**Summary**


Constantly changing nature of network attacks requires a flexible protection system, which will have the ability to analyse large volumes of network traffic. Neuronal networks are the basis for organizingsystems of protection of intellectual information. Such systems must ensureautomatic and operative reaction in case of changes of vulnerability of protective system or space of threats, which leads tothe use of evolutionary methods in protection of information systems. The thesis presentssolution of neuronal network connections weights optimization problem by using genetic algorithm, in the case of a constant network topology and in the case of changeable topology of compatibility functions.


## ЭВОЛЮЦИОННЫЕ АЛГОРИТМЫ В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ


Джанелидзе Г., Мепаришвили Б.

Грузинский Технический Университет


**Резюме**


Постоянно изменчивый характер сетевых атак требует создание систем защиты, которые будут способны анализировать большой объем сетевого трафика. Базисом для организации интеллектуальных систем по защите информации являются нейронные сети. Подобные системы должны обеспечить автоматическую и оперативную реакцию при изменении характера уязвимости или пространства угрозы защитной системы, что приводит к использованию эволюционных методов в системах защиты информации. В работе представлено решение задач по оптимизации веса связей нейронных сетей с использованием генетических алгоритмов для сети как с постоянной топологией, а также для сети с изменчивой топологией по функции совместимости.