## 0619 ინფორმაციისა და კომუნიკაციის ტექნოლოგიები
## INFORMATION AND COMMUNICATION TECHNOLOGIES (ICTS)

# საინფორმაციო ქსელში შეღწევის გამოვლენის თანამედროვე სისტემები

დათა დათაშვილი
სამცხე-ჯავახეთის სახელმწიფო უნივერსიტეტი
E-mail: datadatashvili99@gmail.com

**რეფერატი**

თანამედროვე ქსელური ტექნოლოგიების, განსაკუთრებით IoT (Internet of Things - ნივთების ინტერნეტი) სისტემების ფართო გამოყენებამ კიბერუსაფრთხოების მიმართულებით მნიშვნელოვანი საფრთხეები შექმნა. ერთ-ერთი გავრცელებული პრობლემა ანომალიებია - სიტუაციები, როდესაც არსებული მონაცემები არ ემთხვევა ნორმალურ შაბლონს, რაც შესაძლოა გამოწვეული იყოს თაღლითური ქმედებებით. ნაშრომში გაანალიზებულია საინფორმაციო ქსელში ანომალიის აღმომჩენი სისტემები. განხილულია მათი მუშაობის პრინციპები. განსაკუთრებული ყურადღება გამახვილებულია თანამედროვე კიბერშეტევების პროგნოზირების სირთულეებზე, რამაც გამოიწვია დაცვის სისტემებში ხელოვნური ინტელექტის მეთოდების გამოყენების აუცილებლობა. ამ თვალსაზრისით, აღწერილია ცოდნაზე და გამოთვლით პროგნოზებზე დაფუძნებული სისტემები; აღნიშნულია მათი დადებითი მხარეები და გამოწვევები. აქცენტები გაკეთებულია სისტემებში მოვლენათა კორელაციაზე, რომელიც მოიცავს კომპლექსურ ამოცანებს, როგორიცაა აღმოჩენა, პრევენცია და რეაგირება უსაფრთხოების მონაცემთა გაერთიანების მეშვეობით. ნაშრომში დამუშავებულია ცოდნაზე დაფუძნებული მანქანური სწავლების ალგორითმი, რომელიც შეიძლება გამოყენებულ იქნას დიდ მონაცემთა ნაკადების შემოდინებისას რეალურ დროში. ალგორითმში ახალი წესის ფორმირებისთვის შემოთავაზებულია გენეტიკური პროგრამირების და შემთხვევითი ტყის მეთოდების გამოყენება.

**საკვანძო სიტყვები:** ანომალიის აღმომჩენი სისტემები, ცოდნაზე დაფუძნებული მანქანური სწავლების ალგორითმი.

### შესავალი

თანამედროვე ინტერნეტქსელების სწრაფი განვითარებისა და IoT მოწყობილობების გავრცელების ფონზე, ქსელური ინფრასტრუქტურის უსაფრთხოება სულ უფრო მნიშვნელოვან გამოწვევად იქცა. კიბერშეტევების გართულებული ბუნება მოითხოვს იმგვარი სისტემების დანერგვას, რომლებიც არამარტო აღიქვამენ მიმდინარე საფრთხეს, არამედ ანალიზის საფუძველზე პროგნოზირებენ შესაძლო შეღწევებსაც. ამ კონტექსტში, განსაკუთრებული როლი ენიჭება შეღწევის აღმოჩენის სისტემებს (Intrusion Detection Systems, IDS), რომლებიც უზრუნველყოფენ ქსელის ტრაფიკისა და სისტემური აქტივობების უწყვეტ მონიტორინგსა და ანომალიების იდენტიფიცირებას. IDS-ები იყოფა სხვადასხვა ტიპად და იყენებს როგორც ხელწერის, ასევე ანომალიაზე დაფუძნებულ მეთოდებს. ანომალიაზე დაფუძნებული სისტემების ეფექტიანობის გაზრდის მიზნით, ფართოდ გამოიყენება მანქანური სწავლებისა და ხელოვნური ინტელექტის თანამედროვე მეთოდები, რაც უზრუნველყოფს შეღწევების დროულ და ზუსტ გამოვლენას.

### ძირითადი ნაწილი

ანომალიის გამოვლენა მონაცემთა ანალიზის რთული ამოცანაა, რომლის ფარგლებში მნიშვნელოვან როლს თამაშობს შეღწევის აღმოჩენის საკითხები, რაც გულისხმობს ისეთ ქმედებებს, რომლებიც მიზნად ისახავს IoT სისტემების და ქსელის უსაფრთხოების, კონფიდენციალურობისა და ხელმისაწვდომობის დაცვას. აღნიშნული სრულდება შიდა ან გარე აგენტის მიერ, რათა შესაძლებელი გახდეს კონტროლის მოპოვება უსაფრთხოების მექანიზმზე. შეტევების მრავალფეროვანი რისკების გამო იქმნება სისტემები, რომლებიც ინტერნეტით განხორციელებულ თავდასხმებს ეწინააღმდეგებიან. მათ შორის, შეღწევის აღმოჩენის სისტემები (IDS) ეხმარება ქსელს, გაუმკლავდეს გარე საფრთხეებს.

შეღწევის გამოვლენის სისტემები წარმოადგენს უსაფრთხოების ინსტრუმენტებს, რომლებიც, სისტემის უსაფრთხოების გასაძლიერებლად, ავტომატურად ახდენენ მონიტორინგსა და ანალიზს ქსელის ტრაფიკსა და მომხმარებლის აქტივობაზე. აღნიშნული სისტემები მოიცავს ორ მთავარ პროცესს,

როგორიცაა სისტემის ძირითადი აქტივობების მონიტორინგი და შედეგად მიღებული ჟურნალის მონაცემების ანალიზი [1].

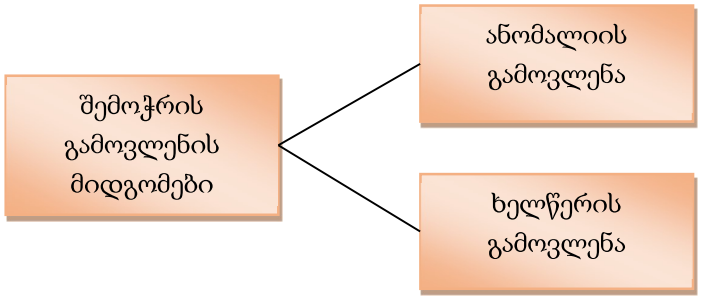
ზოგადად, IDS-ები შეიძლება დავყოთ ორ ძირითად ტიპად: ჰოსტზე დაფუძნებული შეღწევის აღმოჩენის სისტემები (HIDS) და ქსელზე დაფუძნებული შეღწევის აღმოჩენის სისტემები (NIDS) [2]. აღსანიშნავია, რომ NIDS-ს გააჩნია მექანიზმები, რომლებიც აგროვებენ და აანალიზებენ მონაცემებს ჰოსტისა თუ ქსელის სხვადასხვა ნაწილიდან უსაფრთხოების დარღვევების გამოვლენისთვის. აღსანიშნავია, რომ განირჩევა შეღწევის აღმოჩენასთან დაკავშირებული შემდეგი ფუნქციები:

1. მომხმარებლის, სისტემის და ქსელის აქტივობების მონიტორინგი და ანალიზი;
2. შესაძლო დაუცველობის შესახებ ანგარიშების მიხედვით სისტემების კონფიგურაცია;
3. სისტემისა და ფაილის მთლიანობის შეფასება;
4. ტიპიური შეტევების ნიმუშების ამოცნობა;
5. ანომალური აქტივობის ანალიზი;
6. მომხმარებლის მიერ პოლიტიკის დარღვევების თვალყურის დევნება.

IDS იყენებს დაუცველობის შეფასებას ჰოსტის ან ქსელის უსაფრთხოების შესაფასებლად. შეღწევის გამოვლენის სისტემის მუშაობა განპირობებულია იმ ვარაუდით, რომ შეღწევის აქტივობები შესამჩნევად განსხვავდება სისტემის ნორმალური აქტივობებისგან, ხოლო თავდამსხმელთა ქცევა განსხვავდება კანონიერი მომხმარებლისგან.

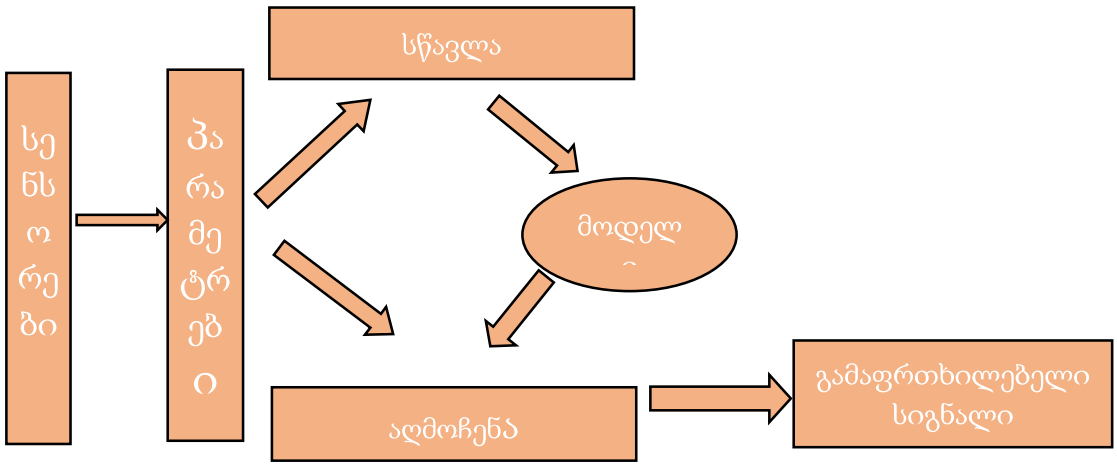
ზოგადად, ანომალიების აღმოჩენის მიდგომების მიხედვით IDS იყოფა ორ კატეგორიად: ანომალიისა და არასწორი გამოყენების (ხელწერის ანუ Signature) გამოვლენა. შეყვანის მონაცემები მოითხოვს დამუშავებას, რადგან ისინი განსხვავებული ტიპისაა - მაგალითად: IP მისამართები იერარქიულია, პროტოკოლები კატეგორიული, ხოლო პორტები რიცხობრივი. დამუშავების პროცესი ეფუძნება კონკრეტულ ანომალიის გამოვლენის ტექნიკას, რომელიც შეიძლება იყოს ზედამხედველობითი ან ზედამხედველობის გარეშე. მუშაობის შედეგის შესაფასებლად კი გამოიყენება ქულები ან ეტიკეტები.

ქსელში შეღწევის აღმოჩენის სისტემები (NIDS) მოიცავს ერთ ან მეტ სენსორს, რომლებიც ქსელის ინტერფეისის ბარათებთანაა დაკავშირებული და აგროვებს მონაცემებს ტრაფიკის მოცულობაზე, პროტოკოლებზე, წყაროსა და დანიშნულების IP მისამართებზე, სერვისის პორტებზე და სხვ. IDS-ის ეს ტიპი ჩვეულებრივ იკვლევს ქსელის ტრაფიკს. მოცემული ანალიზის ტიპი არის ყველაზე მნიშვნელოვანი ასპექტი, რომელიც გამოიყენება NIDS-ების კატეგორიზაციისთვის. შესაბამისობის მიხედვით შეიძლება იდენტიფიცირება ანომალიის გამოვლენისა და ხელწერის გამოვლენის საფუძველზე (ნახ. 1).



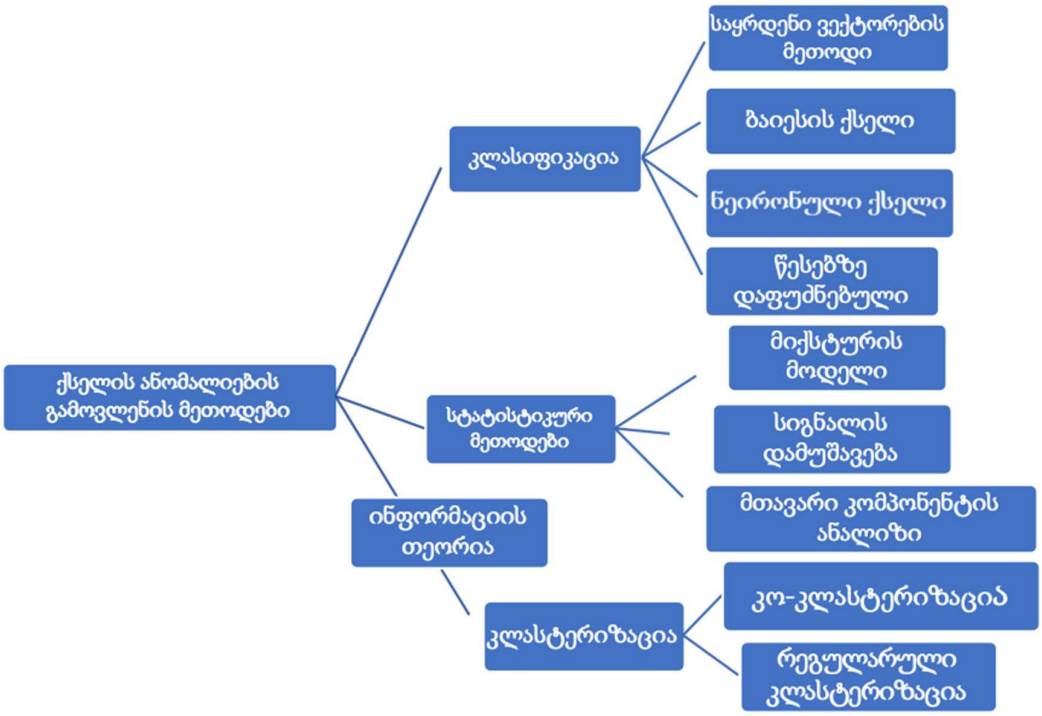

ნახ. 1. IDS-ების კატეგორიზაცია გამოყენებითი ანალიზის საფუძველზე

მიუხედავად არსებული გარკვეული განსხვავებისა ანომალიის გამოვლენაზე დაფუძნებულ IDS-ებს ანუ ქცევაზე დაფუძნებულ IDS-ებს (Behavioral BIDS) ქვეტიპებს შორის, ზოგადად ანომალიის გამოვლენაზე დაფუძნებულ IDS-ებს შეუძლიათ ფუნქციონირება ორ განსხვავებულ რეჟიმში (ნახ. 2).




ნახ. 2. BIDS ფუნქციონალური არქიტექტურა

წვრთნის რეჟიმში სისტემა იყენებს სენსორულ მონაცემებს, რომლებიც აღწერს ნორმალურ ქსელურ და მომხმარებლის ქცევას. ეს მონაცემები ფორმალიზდება ნორმალური ქცევის პროფილებად პარამეტრიზაციის მოდულით. ამ პროფილებზე დაყრდნობით სასწავლო მოდული ქმნის ქსელის ქცევის მოდელს - ავტომატურად, ხელით ან შერეული მეთოდით. შემდეგ BIDS გადადის გამოვლენის რეჟიმში: სენსორის ფაქტობრივი მონაცემები გარდაიქმნება ფაქტობრივ პროფილად, აღმოჩენის მოდული ადარებს მას ადრე შექმნილ მოდელს. მიღებული ცოდნის საფუძველზე სისტემა განსაზღვრავს, არის თუ არა აქტივობა საზიანო.

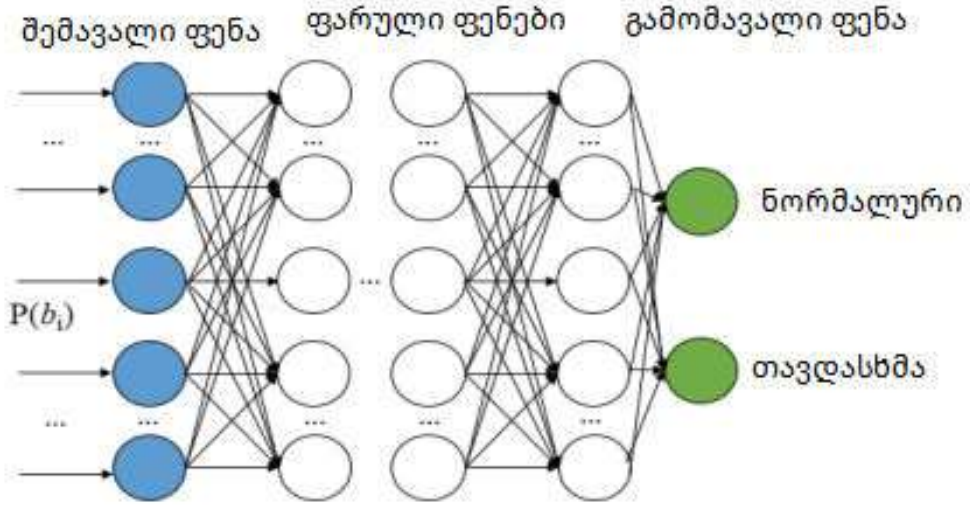



ნახ.3. ქსელის ანომალიების გამოვლენის ზოგადი ჩარჩოს სქემა

თანამედროვე კიბერშეტევების, განსაკუთრებით NIDS-ის წინააღმდეგ მიმართულ თავდასხმების პროგნოზირების სირთულემ გამოიწვია IDS-ში თანამედროვე მეთოდების, როგორიცაა ღრმა (DNN), რეკურენტული (RNN) და გრძელვადიანი მეხსიერების (LSTM) ნეირონული ქსელების გამოყენების აუცილებლობა. მექანიკურ სწავლებაზე (ML) დაფუძნებული IDS-ები ხშირად იყენებენ K-means-ს, ფარულ მარკოვის მოდელს, თვითორგანიზების რუკებს (SOM), ასევე ნეირონულ ქსელებს (ნახ 4), გადაწყვეტილების ხეებს, მიამიტ ბაიესის მოდელსა და საყრდენი ვექტორების მეთოდს.

წესებზე დაფუძნებული ხეების მიდგომით, BIDS შეიძლება პირობითად დაიყოს სამ კატეგორიად მონაცემთა დამუშავების რეჟიმის მიხედვით: სტატისტიკურ, ცოდნაზე და გამოთვლით პროგნოზირებაზე დაფუძნებულ მიდგომებად.

სტატისტიკურ BIDS აკონტროლებს ქსელის ტრაფიკს, ამოწმებს კომუნიკაციის სიჩქარეს, პროტოკოლებსა და IP მისამართებს, და იკვლევს მიმდინარე პროფილს ნორმალურ პროფილთან შედარებით. ანომალიის აღმოჩენისას ითვლება მისი ზომა და თუ იგი აღემატება ზღვარს - გენერირდება სიგნალი. სისტემა იყენებს სტატისტიკურ მეთოდებს მავნე ქმედებების დასადგენად და ანგარიშების შესაქმნელად.




ნახ.4. ნეირონული ქსელის ზოგადი სქემა უსაფრთხოების ამოცანებისთვის

ცოდნაზე დაფუძნებული BIDS მუშაობს მონაცემთა ბაზაზე, რომელიც მოიცავს ინფორმაციას წინა თავდასხმების ნიმუშების შესახებ. ამ ინფორმაციის საფუძველზე ხდება მონიტორინგის ქვეშ მყოფი აქტივობის შეფასება - ეკუთვნის თუ არა ის ანომალურ ქცევას. ეს მოდელი ხშირად გამოიყენება, რადგან იძლევა ნაკლებ ცდომილებას და იყენებს სტანდარტულ სიგნალებს, რომლებიც ადვილად აღსაქმელია ადმინისტრატორებისთვის.

გამოთვლით პროგნოზირებაზე (CI) დაფუძნებული BIDS ამოიცნობს წესებსა და კანონზომიერებებს ნიმუშებზე დაყრდნობით - დამოუკიდებლად ან ადამიანის დახმარებით. შეუძლია თვითონ მიიღოს გადაწყვეტილება ახლად წარმოქმნილ, უცნობ მონაცემებზე. CI-ზე დაფუძნებული BIDS ასევე იყენებს სტატისტიკური ანალიზის ტექნიკას მათი მუშაობის გასაუმჯობესებლად. თუმცა, როგორც წესი, დასამუშავებელი მონაცემთა უზარმაზარი რაოდენობის გამო, საჭიროებენ დიდ გამოთვლით რესურსებს [3].

თანამედროვე IDS სისტემები და ინტელექტუალური აგენტები განიხილავენ ფართო შეტევების შედეგებს, ინციდენტებსა და მენეჯმენტის რეაგირებას. ამ კონტექსტში განსაკუთრებით მნიშვნელოვანია მოვლენათა კორელაცია, რომელიც აერთიანებს აღმოჩენის, პრევენციისა და რეაგირების ამოცანებს უსაფრთხოების მონაცემების კონსოლიდაციის გზით. ასევე მნიშვნელოვანი მოთხოვნაა უცნობი

განაწილებული შეტევებისადმი ადაპტაცია და მათი ავტომატური იდენტიფიკაცია. მოვლენა ქსელის მენეჯმენტში განისაზღვრება როგორც ინფორმაციის ნაწილი, რომელიც ასახავს ქსელში მომხდარ ხდომილობებს და ხშირად უკავშირდება პრობლემებს.

მოვლენათა კორელაციის მიზანია ერთი ძირეული პრობლემის გამოვლენა, რამაც შეიძლება გამოიწვიოს მრავალი განსხვავებული სიმპტომის გაჩენა. ეს მეთოდი ცდილობს გამოავლინოს მიზეზ-შედეგობრივი კავშირი (მაგ. A იწვევს B-ს). მოვლენის კორელაციის ტრადიციული მიდგომა კი წარმოადგენს წესებზე დაფუძნებულ ანალიზს. საინტერესოა, რომ თანამედროვე კორელაცია იყენებს AI ტექნიკებს, როგორიცაა ბაიესის ქსელები, ექსპერტთა სისტემები, სავარაუდო და უახლოესი მეზობლის მიდგომები. ასევე გამოიყენება შემთხვევებზე, წესებზე და მოდელებზე დაფუძნებული მსჯელობის კომბინაციები, ბაიესისა და ნეირონულ ქსელებთან ერთად - ხარვეზის იდენტიფიკაციის, გამოსწორებისა და განახლების მიზნით [4].

მოვლენათა კორელაციის სისტემების უმეტესობა ეფუძნება საწყისი წესების შექმნას, რაც კრიტიკულად მნიშვნელოვანია, რადგან არასწორი წესები იწვევს არასწორ შედეგებს. თანამედროვე ქსელების დინამიური ბუნება ართულებს ტოპოლოგიის ცოდნას, რომელიც კი აუცილებელია კორელაციისთვის, რათა ქსელის მართვის სისტემამ შეძლოს პრობლემების იდენტიფიკაცია და მიზეზების დადგენა.

ცოდნაზე დაფუძნებული BIDS ფუნქციონირებს სტატისტიკური Big Dataset-ების საფუძველზე შექმნილი ცოდნის ბაზით. ეს ბაზა წარმოადგენს ბინარული ხისებრი სტრუქტურის მქონე ონტოლოგიების კრებულს. თითოეული წესი გამოხატულია ხე-გრაფის სახით, სადაც მწვერვალები აღნიშნავს მოვლენებს, ხოლო რკალები - მათ შორის არსებულ პრედიკატებს.

ცოდნის ბაზაზე დაფუძნებული მანქანური სწავლების პროცესი მოიცავს შემდეგ ბიჯებს:

1. პროტოკოლის შესაბამისად, სისტემაში მოვლენათა სტატისტიკური Big Dataset-ების შემოდინება.
2. Naive Bayes-ის, Nearest Neighbors-ის, K-means-ისა და რეგრესიული ანალიზის შერჩევითი გამოყენებით ყალიბდება კორელაციური სისტემის წესები - ბინარული, აციკლური ხისებრი სტრუქტურების სახით.
3. Big Dataset-ების ყოველი მოვლენისთვის ყალიბდება მისი ხისებრი მოდელი.
4. მიმდინარე მოვლენის მოდელი შედარდება ცოდნის ბაზაში არსებულ წესებთან და კლასიფიცირდება როგორც ნორმალური ან ანომალური.
5. თუ შესაბამისი წესი არ მოიძებნა, იწყება ცოდნის ბაზის განახლება - იქმნება და დაემატება ახალი წესი. აღსანიშნავია, რომ ახალი წესის ფორმირების თვალსაზრისით, მიზანშეწონილია მანქანური სწავლების ორი მეთოდის: გენეტიკური პროგრამირებისა (Genetic Programming) და შემთხვევითი ტყის (Random Forest) გამოყენება.

ევოლუციური გამოთვლა (EC) არის AI-ის დარგი, რომელიც ეფუძნება სახეობების ევოლუციის თეორიას. ევოლუციური ალგორითმის თითოეული გენერაცია მოიცავს გადაწყვეტილებების ნაკრებს, რომლიდანაც შერჩევით და გენეტიკური ოპერატორების გამოყენებით იქმნება ახალი თაობები. ეს წარმოადგენს ზედამხედველობის ძიების ტექნიკას. გენეტიკური პროგრამირება (GP) - EC-ზე დაფუძნებული მეთოდია, სადაც ინდივიდები წარმოდგენილნი არიან როგორც კომპიუტერული პროგრამები, რაც მათ აღწერას მეტად მოქნილს ხდის. მისი ვარიანტი, გენის გამოხატვის პროგრამირება (GEP), ითვალისწინებს თაობათა რაოდენობისა და პოპულაციის ზომის კრიტიკულ მნიშვნელობას, რაც ზრდის რესურსის ხარჯებს [5]. GEP, Linear GP და MEP გამოიყენება IDS-ის წესების გენერირებისთვის, თუმცა GP პირდაპირ მოვლენის კორელაციაზე ჯერ არ გამოყენებულა. გენეტიკური პროგრამირება მსგავსი ამოცანებისთვის განსაკუთრებით შესაფერია, რადგან კორელაციის წესები ცვლადი სიგრძისაა და შეიძლება გამოთვლით სირთულეებთან იყოს დაკავშირებული.

**დასკვნა**

შეღწევის აღმოჩენის სისტემები წარმოადგენს უსაფრთხოების არსებით კომპონენტს, რომელიც ადაპტირდება ცვალებად კიბერსაფრთხეებთან და აუმჯობესებს ქსელურ ინფრასტრუქტურაზე ზედამხედველობას.

ანომალიაზე დაფუძნებული IDS-ები გამოირჩევა მაღალი სიზუსტით და მოქნილობით, რაც განსაკუთრებით მნიშვნელოვანი ხდება თანამედროვე, დინამიური ქსელების პირობებში. სტატისტიკური, ცოდნაზე და გამოთვლით პროგნოზირებაზე დაფუძნებული მიდგომები ქმნის ძლიერ ჩარჩოს ანომალიების აღმოჩენისთვის, ხოლო მანქანური სწავლებისა და ევოლუციური ალგორითმების

გამოყენება უზრუნველყოფს სისტემის თვითგანახლებისა და ადაპტაციის უნარს. მოვლენათა კორელაციის მექანიზმების ინტეგრაცია კი შესაძლებელს ხდის ერთიანი უსაფრთხოების პოლიტიკის ფორმირებას, რაც ზრდის რეაგირების ეფექტიანობას და უზრუნველყოფს მთლიან სისტემურ უსაფრთხოებას.

**ლიტერატურა**

1. Katsaumire, c. (2023). Intrusion detection systems: categories, attack detection and response.
2. Sonawane, a., & jaiswal, r. C. (2023). Network based intrusion detection system.
3. Thapa, s., & dissanayaka, a. M. (2025). The role of intrusion detection/prevention systems in modern computer networks: a review.
4. Yeo, l. H., che, x., & lakkaraju, s. (2024). Understanding modern intrusion detection systems: a survey.
5. Raj jain, carlos m. Travieso, sanjeev kumar, cybersecurity and evolutionary data engineering: select proceedings of the 2nd international conference, iccede 2022, springer nature singapore, 2023 m09 20 - 369 pages

## Modern systems for detecting intrusion into the information network

**Data Datashvili**

**Abstract**

The widespread use of modern network technologies, especially IoT (Internet of Things) systems, has created significant threats to cybersecurity. One of the common problems is anomalies - situations when the available data does not match the normal pattern, which may be caused by fraudulent actions. The paper analyzes anomaly detection systems in the information network. The principles of their operation are discussed. Special attention is paid to the difficulties of predicting modern cyberattacks, which led to the need to use artificial intelligence methods in protection systems. In this regard, systems based on knowledge and computational predictions are described. Their advantages and challenges are noted. Emphasis is placed on the correlation of events in systems, which includes complex tasks such as detection, prevention and response through the integration of security data. The paper develops a knowledge-based machine learning algorithm that can be used to process large data streams in real time. The algorithm proposes the use of genetic programming and random forest methods to form a new rule.

**Keywords:** anomaly detection systems, knowledge-based machine learning algorithm