საქართველოს ტექნიკური უნივერსიტეტი

ხელნაწერის უფლებით

ივანე ალფაიძე

# სახელმწიფოში კრიტიკული ინფრასტრუქტურის ინფორმაციული უსაფრთხოების უზრუნველყოფის პრობლემების, მათი გადაწყვეტის მეთოდების და საშუალებების კვლევა

სადოქტორო პროგრამა: ინფორმატიკა შიფრი - 0401

დოქტორის აკადემიური ხარისხის მოსაპოვებლად
წარდგენილი დისერტაციის

**ავტორეფერატი**

თბილისი

2019

სამუშაო შესრულებულია საქართველოს ტექნიკური უნივერსიტეტში
ინფორმატიკის და მართვის სისტემებისფაკულტეტი
მართვის ავტომატიზებული სისტემების დეპარტამენტი

ხელმძღვანელი: ასოც. პროფესორი კორნელი ოდიშარია

რეცენზენტები: ----------
----------

დაცვა შედგება ---------- წლის ”------” ----------, --------- საათზე, საქართველოს ტექნიკური უნივერსიტეტის ინფორმატიკის და მართვის სისტემების ფაკულტეტის საუნივერსიტეტო სადისერტაციო საბჭოს სხდომაზე, კორპუსი ----------, აუდიტორია ----------

მისამართი: 0175, თბილისი, კოსტავას 77.

დისერტაციის გაცნობა შეიძლება სტუ-ს ბიბლიოთეკაში,
ხოლო ავტორეფერატის - ფაკულტეტის ვებგვერდზე

საუნივერსიტეტო სადისერტაციო საბჭოს მდივანი პროფ. თ.კაიშაური

## ნაშრომის ზოგადი დახასიათება

**თემის აქტუალობა.** სადისერტაციო ნაშრომის აქტუალობა განპირობებულია, იმით რომ სახელმწიფო მართვის თეორიული პრობლემები, მისი ფუნქციები, მეთოდები და რეალიზაციის მექანიზმები, საჯარო და სახელმწიფო პოლიტიკისა და სახელმწიფო მართვის თანაფარდობა და ურთიერთქმედება, სახელმწიფო მართვაში სისტემური მიდგომის გამოყენება საზოგადოებრივი ცხოვრებისა და სახელმწიფო მართვის რეფორმების დღევანდელ ეტაპზე უაღრესად მნიშვნელოვანია.

კომუნიკაციის ქსელები და საშუალებები, ინფორმაციული სისტემები იქცნენ ადამიანის მუდმივ თანამგზავრებად, რომლებსაც ის ანდობს თავის პერსონალურ მონაცემებს, ფინანსურ ოპერაციებს, ბიზნესს. პიროვნება "მავთულის მეორე ბოლოში" უკვე აღარწარმოადგენს ცალსახად სანდომხარეს, როგორც ეს შეიძლება ყოფილიყო უშუალო პირისპირ ურთიერთმოქმედებისას, რომ შეიძლება "წარდგე" როგორც მხარე, რომელიც იმსახურებს ნდობას, ადვილად იპოვა მიმდევრები თანამედროვე ინფორმაციულ სამყაროში.

ყოველმხრივი გლობალიზაციის, მზარდი რისკების და საზოგადოებრივი პროცესების განუსაზღვრელობის პირობებში ინფორმაციული უსაფრთხოება (იუ) ხდება ერთ–ერთ ძირითად ფუნქციად ელექტრონული ხელისუფლების თვითშენარჩუნებისა.

სახელმწიფოს ძირითადი მიზანი ინფორმაციის უსარფთხოების პრობლემების გადაწყვეტის მეთოდების და საშუალებების კვლევაა. თანამედროვე ინფორმაციული სისტემები, როგორც წესი, შეიცავენ დიდ რაოდენობას უსაფრთხოების მართვის ერთმანეთთან დაკავშირებულ მოწყობილობებს და საშუალებებს, რომლებიც აფორმირებენ უზარმაზარი რაოდენობის ინფორმაციას. ეს ინფორმაცია უნდა იქნას დამუშავებული იმ მიზნით, რომ გამოკვლეული იქნას დაცვაში შესაძლო მოწყვლადობები – სუსტი ადგილები, მოხდეს იდენტიფიკაცია კომპიუტერული შეტევებისა და

მიღებულ-გატარებულ იქნას კონტრზომები.

**კვლევის მიზანი:** საკვლევი თემის მიზანს წარმოადგენს მოცემულ სფეროში მსოფლიოს განვითარებული ქვეყნების გამოცდილების, არსებული მდგომარეობის ანალიზი, და იმის დადგენა ინფორმაციული ტექნოლოგიების დანერგვა-განვითარების რა პოლიტიკა და სტრატეგია უნდა განახორციელონ ისეთმა განვითარებადმა ქვეყნებმა, როგორიცაა საქართველო, რომელსაც სერიოზული მიღწევები აქვს ელექტრონული ხელისუფლების, ხალხის ელექტრონული მომსახურების ხაზით, რომ არ მოხდეს მოსახლეობის ინფორმაციულ ტექნოლოგიებში მაქსიმალურად გათვითცნობიერება ჩართვის პერიოდში კატასტროფული საფრთხეების გაზრდა-რეალიზება.

**კვლევის ობიექტი და საგანი:**სახელმწიფოში უსაფრთხოების უზრუნველყოფის პრობლემების და მათი გადაწყვეტის მეთოდების შემუშავება კრიტიკული ინფრასტრუქტურის ინფორმაციული საშუალებებით. კვლევის ობიექტს წარმოადგენს მიზანდასახული სისტემები, რომელთა შექმნა განვითარება, არსებობა დამოკიდებულია თანამედროვე ინფორმაციული ტექნოლოგიების, საერთო სისტემური კანონზომიერებების გათვალისწინებით, დანერგვასა და ფუნქციონირების პროცესებში წარმოქმნილი ან შესაძლო რისკების მართვა, ესაა სახელმწიფოს როგორც ურთულესი სისტემის, ის შემადგენელი ძირითადი საყრდენი ელემენტები, რომელთა ეფექტური ფუნქციონირება თვით სახელმწიფოს მდგრადი განვითარების აუცილებელი პირობაა.

**კვლევის საგანია** სახელმწიფოში კრიტიკული ინფრასტრუქტურის ინფორმაციული უსაფრთხოების პრობლემების, მათი გადაწყვეტის მეთოდების და საშუალებების კვლევა, დასმული საწყისი მიზნის რეალურობის დასაბუთების, შექმნა-გაშვების და ფუნქციონირების, ამ დროს არსებული, მოსალოდნელი რისკების შეფასების, მართვისა და კონტროლის, ავტომატიზაციისა და ინფორმაციული უსაფრთხოების

უზრუნველყოფის პროცესები, მათი წარმატებით გადაწყვეტის სამეცნიერო-პრაქტიკული პირობები.

**კვლევის ამოცანა:** სახელმწიფოში კრიტიკული ინფრასტრუქტურის ინფორმაციული უსაფრთხოების უზრუნველყოფის პრობლემების, მათი გადაწყვეტის მეთოდების და საშუალებების კვლევა, გარემოს პირდაპირი ზემოქმედების ფაქტორების მოკლევადიანი პროგნოზირების და შესაძლო რისკების შეფასების საფუძველზე; კრიტიკული ინფრასტრუქტურის ინფორმაციული უსაფრთხოების შექმნა-გაშვების პროცესის ანალიზი, შესაძლო რისკების გამოვლენა და პროცესის ავტომატიზების კონცეფციის ჩამოყალიბება; შრომითი რესურსების შეგროვების და შერჩევისას რისკების ანალიზი და ინფორმაციის უსაფრთხოების დონის ამაღლება.

**კვლევის მეთოდები:** მოცემულ ნაშრომს მეთოდოლოგიურ საფუძვლად უდევს: კონკრეტული შემთხვევების კვლევა, რომლებიც საშუალებას იძლევიან შესწავლილი იქნას სახელმწიფოში კრიტიკული ინფრასტრუქტურის ინფორმაციული უსაფრთხოების უზრუნველყოფის პრობლემები, დასმული მიზნის მიღწევის შესაძლებლობა შრომის, ინტელექტის, სხვა ადამიანების ქცევის მოტივების გამოყენებით; სისტემური მიდგომები და საერთოსისტემური კანონზომიერები, რომლებსაც ექვემდებარებიან უმეტესობა ბუნებრივი და საზოგადოებრივი სისტემების ფუნქციონირება, კრიტიკულად მნიშვნელოვანი ინფრასტრუქტურებში ინფორმაციის დაცვის ინტელექტუალური სერვისების არქიტექტურა. სტატისტიკური შესწავლა კონფიდენციალური ინფომაციის გაჟონვის, კონფიდენციალური ინფორმაციის გაჟონვა მსოფლიოში და მეზობელსახელმწიფოებში (რუსეთის მაგალითზე), კრიტიკული ინფრასტურუქტურის ინფორმაციული უსაფრთხოების დარღვევის პროცესების მოდელირება.

**ნაშრომის ძირითადი შედეგი და მეცნიერული სიახლე:**იუ – ის შესაძლო დარღვევის პროცესების ცნობა უსასრულოა და შესაბამისად დროის ნებისმიერ პერიოდში მკვლევარის ცოდნა შეიცავს გაურკვევლობის

ელემენტს, ხოლო რიცხვი საფეხურებისა (დონისა) ამ ანალიზისა შეიძლება შეუზღუდავად იზრდებოდეს. მართლაც ყველა ალბათური მოდელები შემთხვევითი მოვლენების ანალიზი იქნება იმიტომ, რომ ექსპერიმენტის ძირითადი პირობები ცნობილია. მაშ ასე, ალბათობის ელემენტარულ თეორიაში – ესაა „ექსპერიმენტის“ პირობების $\chi$ კომპლექსი, აქსიომატურ თეორიაში – ესაა სივრცე U ელემენტარული მოვლენებისა, მათემატიკურ სტატისტიკაში – ესაა გენერალური ერთობლიობა.

ეს დაშვება დაედო საფუძვლად დღეისათვის არსებულ შემთხვევითი მოვლენების ალბათურ მოდელებს, რომლებიც დამახასიათებელია იუ – ის ცნებისთვის.

**ნაშრომის შედეგების გამოყენების სფერო:** ნაშრომის პრაქტიკულ მნიშვნელობას განაპირობებს მიღებული შედეგები: ელექტრონული ხელისუფლების ინფორმაციული უსაფრთხოების სტრატეგიული მართვის კოგნიტიური მოდელი: არამკაფიო კოგნიტიური რუკები, ელ.ხელისუფლების იუ მართვის ფაქტორები, ფაქტორების ურთიერთგავლენის მატრიცის აგება, აკმ დინამიკის მოდელირება, გამოთვლითი ექსპერიმენტების შედეგები, ინფორმაციის და უსაფრთხოების შემთხვევების მართვის სისტემებში კონტრზომების შერჩევის მეთოდიკა: განაწილებული ქსელი დაცვის ქვეშ, კრიტიკულად მნიშვნელოვან ინფრასტრუქტურებში ინფორმაციის დაცვის ინტელექტუალური სერვისების არქიტექტურა, კონფიდენციალური ინფორმაციის გაჟონვა მსოფლიოში და მეზობელ სახელმწიფოებში კვლევის შედეგები: კმო (კრიტიკულად მნიშვნელოვანი ობიექტი) იუ (ინფორმაციული უსაფრთხოება) – ის უზრუნველყოფა ტპმას (ტექნოლოგიური პროცესების მართვის ავტომატიზირებული სისტემა) – ის სპეციფიკის გათვალისწინებით, ანალიზი განუსაზღვრელობებისა დარღვევების და მისი იზ (ინფორმაციული ზემოქმედება) – ის ეფექტურობის შეფასების მოდელირების პროცესების, იუ–ის დამრღვევის

მოდელირებაზე რეკომენდაციები, იუ–ის დარღვევის პროცესების სემანტიკური კვლევების ასპექტები.

კონცეპტუალური მოდელების – მიზანდასახული სისტემის საწყისი მიზნის რეალურობის შემოწმების, შექმნა-გაშვების, შრომით რესურსებთან მუშაობისას რისკების მართვის სიტემის, ორგანიზაციის მართვის ავტომატიზების მასშტაბების მართვის და იუ-ს უზრუნველყოფის კომპლექსური სისტემის, რომელთა გამოყენებაც შესაძლებელია, როგორც ცალკეულ ორგანიზაციებში ასევე სახელმწიფო ორგანოების მიერ. დისერტაციის მასალები შეიძლება გამოყენებულ იქნას უმაღლეს სასწავლებლებში სპეციალური კურსების მოსამზადებლად, აგრეთვე აღნიშნული თემატიკის საკითხებზე სამეცნირო პროექტების და კვლევების განხორციელების სფეროში.

**სადისერტაციო ნაშრომის სტრუქტურა და მოცულობა:** სადისერტაციო ნაშრომი შედგება შესავლის, სამი თავის, 11ქვეთავის დასკვნისა და გამოყენებული ლიტერატურის სიისგან. საერთო მოცულობა შეადგენს 151 გვერდს.

## თავი I. ელექტრონული ხელისუფლების ინფორმაციული უსაფრთხოების სტრატეგიული მართვის კოგნიტიური მოდელი

სახელმწიფო მართვის პროცესში ინფორმაციული და საკომუნიკაციო ტექნოლოგიების ფართო დანერგვის შედეგად ხდება ფუნდამენტალური ცვლილებები სახელმწიფოს ბუნებაში. მოქალაქეები ფართოდ მონაწილეობენ პოლიტიკის ფორმირებასა და რეალიზაციაში. ხდება ფორმირება სახელმწიფოს, კერძო სექტორსა და სამოქალაქო საზოგადოებას შორის ურთიერთმოქმედებისა და თანამშრომლობის ეფექტური სისტემისა. ეს ფენომენი აღინიშნება ტერმინით „ელექტრონული ხელისუფლება“.

ყოველმხრივი გლობალიზაციის, მზარდი რისკების და საზოგადოებრივი პროცესების განუსაზღვრელობის პირობებში ინფორმაციული უსაფრთხოება (იუ) ხდება ერთ–ერთ ძირითად ფუნქციად ელექტრონული ხელისუფლების თვითშენარჩუნებისა. ამიტომ ძალზე

აქტუალურია ელექტრონული ხელისუფლების იუ–ს უზრუნველყოფის სისტემის მართვა.

თანამედროვე პირობებში ასეთი სახის სისტემის ანალიზისა და მართვისათვის ფართოდ გამოიყენება კოგნიტიური მიდგომა, რომელიც საშუალებას იძლევა დანახულ და გააზრებულ იქნას მოვლენათა განვითარების ლოგიკა ურთიერთმოქმედი ფაქტორების დიდი რიცხვისას,

აქ შემოთავაზებულია, არამკაფიო კოგნიტიური რუკების საფუძველზე, კოგნიტიური მოდელი ელ. ხელისუფლების იუ–ს სტრატეგიული მართვისა. კოგნიტიური მოდელირების შემოთავაზებული მიდგომა პერსპექტიულია გადაწყვეტილებათა მიღების მხარდამჭერი ინტელექტუალური სისტემსბის შექმნის კონტექსტში, და მისმა გამოყენებამ შეიძლება არსებითად აამაღლოს ელ. ხელისუფლების იუ–ს უზრუნველყოფის სფეროში სტრატეგიული მართვის ეფექტურობა და მიღებული გადაწყვეტილებების ხარისხი

### 1.1. არამკაფიო კოგნიტიური რუკები

კოგნიტიური რუკები (კრ) პირველად წარმოდგენილი იქნა ამერიკელი ფსიქოლოგის ე. ტოლმენის (E. Tolman) მიერ თაგვებში ელემენტალური კოგნიტიური პროცესების შესწავლისას. ე. ტოლმენი თაგვების სხვადასხვა ტიპის ლაბირინთებში სწავლებისას მივიდა დასკვნამდე, რომ გარემომცველ გარემოსთან ურთიერთმოქმედების პროცესში ცხოველში ფორმირდება რაღაც „კოგნიტიური რუკა“, ან „აზრობრივი გეგმა“, ლაბირინთის ყველა მახასიათებლებისა, რომლის სრულყოფაც ხდება ყოველი შემდგომი ურთიერთმოქმედებებისას გარემოსთან.

კოგნიტიური რუკები წარმოადგენენ რობასტიულ სისტემებს, რომლებსაც შეუძლიათ დაამოდელირონ ძალიან რთული საქციელები (ყოფაქცევები). თავის ნაშრომში რ. აქსელროდმა გამოიყენა კოგნიტიური რუკები პოლიტიკური ელიტების გადაწყვეტილებების სტრუქტურის შესწაქვლისას. მან შემოიტანა ცნებები აწონ–დაწონილი კრ და

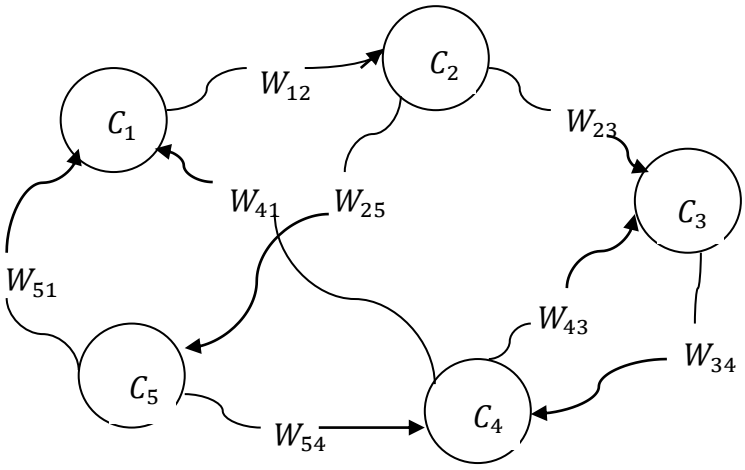
ფუნქციონალური კრ. აწონ–დაწონილ კრ–ებში ნიშანი შეცვლილია დადებითი ან უარყოფითი რიცხვით, რომელიც აჩვენებს მიმართულებას, ასევე მის მნიშვნელობას. ფუნქციონალურ კრ–ებში კავშირის ყოველ მიზეზთან ასოცირდება ფუნქცია, რომელიც უფრო ზუსტად უჩვენებს ეფექტის მიმართულებას და მნიშვნელობას. ეს ორი ტიპი კოგნიტიური რუკებისა იძლევიან უფრო მეტ მოქნილობას, რამდენადაც მათ შეუძლიათ დაამუშაონ და წარ4მოადგინონ უფრო დაწვრილებითი (ვრცელი) ინფორმაცია.

არამკაფიო კოგნიტიური რუკები (აკრ) წარმოდგენილი იქნა ბ. კოსკოს (B. Kosko) მიერ როგორც არამკაფიო გაფართოება კოგნიტიური რუკებისა. ფაქტიურად აკრ–ები წარმოადგენენ კოგნიტიურ რუკებს, აწონილებს არამკაფიო წონებით. ჩვეულებრივ კრ იგება ექსპერტებისაგან ინფორმაციის შეგროვებით, და ექსპერტები, უფრო მიდრეკილი არიან გამოაჩინონ საკუთარი თავი ხარისხობრივ, და არა რაოდენობრივ ტერმინებში. ამ თვალსაზრისით უფრო მიზანშეწონილია აკრ გამოყენება, რომლებშიც კონცეფციები (წარმოიდგინებიან) წარმოდგენილი არიან ლინგვისტურად, შესაბამისი არამკაფიო სიმრავლით.

აკრ ახდენს კომბინირებას გარკვეული ასპექტებისა არამკაფიო ლოგიკისა და ნეირონული ქსელებისა სქემაში წარმოდგენისა ევრისტიკების და არამკაფიო ლოგიკის საღი აზრის წესებისა ევრისტიკით ნეირონული ქდელების სწავლებისა. ეს სტრუქტურა წარმოიდგინება როგორც აწონილი ორიენტირებული გრაფი, რომელშიც წვეროები ურთიერთ ცალსახად შეესაბამებიან ფაქტორებს და რომელთა ტერმინებშიც აღიწერება საგნობრივი არე, ხოლო რკალები ასახავენ ფაქტორებს შორის (ურთიერთდამოკიდებულებას) ურთიერთგავლენას.

წონა რკალისა $C_i$ და$C_j$ ფაქტორებს შორის შეიძლება იყოს დადებითი, რომელიც აღნიშნავს, რომ$C_i$ფაქტორის მნიშვნელობის გაზრდა იწვევს$C_j$ფაქტორის მნიშვნელობის ზრდას,ამავდროულად$C_i$ ფაქტორის მნიშვნელობის შემცირება იწვევს $C_j$ ფაქტორის მნიშვნელობის შემცირებას.

თუ $C_i$ და$C_j$ ფაქტორებს შორის რკალის წონა უარყოფითია, მაშინ$C_i$ მნიშვნელობის ზრდა იწვევს$C_j$ მნიშვნელობის შემცირებას, ხოლო $C_i$




ნახაზი 4.არამკაფიო კოგნიტიური რუკის მაგალითი

ფაქტორის მნიშვნელობის შემცირებას მივყავართ $C_j$ ფაქტორის მნიშვნელობის გაზრდამდე.

### 1.2. ელ.ხელისუფლების იუ მართვის ფაქტორები

აკრ არის ერთ–ერთი მეთოდთაგანი ცოდნის წარმოდგენისა. აკრ–ის ასაგებად გამოყენებულ უნდა იქნას საგნობრივ არეში ექსპერტების ცოდნა და გამოცდილება. ექსპერტები განსაზღვრავენ იმ ფაქტორებს, რომლებიც უკეთესად აღწერენ საგნობრივ არეს. ფაქტორები შეიძლება იყოს ნიშან–თვისებები, მდგომარეობები ან სისტემური ცვლადები. ექსპერტები ახდენენ იდენტიფიკაციას იმისა თუ რომელი ფაქტორებია ცენტრალურები სისტემის მოდელირებისათვის, და ავლენენ, რომელი ფაქტორები ახდენენ ზეგავლენას ერთმანეთზე, და შესაბამისი აქტორებისათვის განსაზღვრავენ პოზიტიურ ან ნეგატიურ გავლენას ერთი ფაქტორისა მეორეზე.

ცხრილი 2.

| ფაქტორები | ფაქტორის სახელწოდება | აღნიშვნა |
|---|---|---|
| $C_1$ | სამართლებრივი ზომები | Legal |
| $C_2$ | ორგანიზაციული ზომები | Org |
| $C_3$ | ტექნიკური ზომები | Tech |
| $C_4$ | პოტენციალის განვითარება | HR |
| $C_5$ | დაინტერესებული მხარეების თანამშრომლობა | Coop |

| | | |
|---|---|---|
| $C_6$ | იუ–ს მუქარების განვითარება | |
| $C_7$ | ელ. ხელისუფლების იუ–ს დონე | NewT Isee |

განვიხილოთ ამ ფაქტორების მოკლე დახასიათება (აღწერები).

**1.სამართებლივი ზომები** – იუ უზრუნველსაყოფად უნდა ჩამოყალიბდეს ადექვატური ნორმატიულ–სამართებლივი ბაზა.

$C_{11}$.სისხლის სამართლის კანონმდებლობა.

$C_{12}$. რეგულირება და შესატყვისობა სტანდარტების მოთხოვნებთან.

**2.ორგანიზაციული ზომები** – კიბერუსაფრთხოების სტრატეგიებში გათვალისწინებულია აგება მართვის მოქნილი ორგანიზაციული სტრუქტურისა, რომელიც მიმართულია იუ–ს უზრუნველყოფაზე.

$C_{21}$. პოლიტიკა - ოფიციალურად აღიარებული ეროვნული ან კონკრეტული სექტორების მიხედვით იუ–ს სტრატეგიები.

$C_{22}$.საგზაო რუკა მართვისათვის – ოფიციალურად აღიარებული ეროვნული ან კონკრეტული სექტორების მიხედვით იუ–ს მართვისათვის გეგმები.

$C_{23}$. პასუხსმგებელი ორგანო – ოფიციალურად აღიარებული ეროვნული ან კონკრეტული სექტორების მიხედვით იუ სააგენტოები.

$C_{24}$. ნაციონალური ბენჩმარკინგი – ოფიციალურად აღიარებული ნაციონალური ან კონკრეტული სექტორების მიხედვით წვრთნები (ვარჯიშები) ბენჩმარკინგში, რომლებიც გამოიყენებიან იუ–ს დონის გასაზომად.

**3.ტექნიკური ზომები** – ტექნოლოგია წარმოადგენს კიბერმუქარების და მავნებლობის მატარებელი ინტერნეტ აგენტების წინააღმდეგ თავდაცვის პირველ ხაზსს.

$C_{31}$. ადრეული გაფრთხილების სისტემა – ხდება გათვალისწინება ინციდენტებისადმი მზადყოფნის ამაღლების, რეაგირების დროის შემცირების, დამუშავება აღდგენის გეგმისა კრიტიკული ინფორმაციული ინფრასტრუქტურისა ავარიების შემდეგ და დაცვის მექანიზმების.

$C_{32}$. სტანდარტები – ეს მაჩვენებელი განსაზღვრავს მთავრობის მიერ უფლებამოსილი სტრუქტურების (სტრუქტურის) არსებობას საერთაშორისო აღიარებული იუ სტანდარტების რეალიზებისათვის სახელმწიფო სექტორში და კრიტიკულ ინფრასტრუქტურებში.

$C_{33}$. სერტიფიკაცია – ეს მაჩვენებელი განსაზღვრავს არსებობას მთავრობის მიერ დამტკიცებული სტრუქტურებისა (სტრუქტურისა), რომლებიც ახდენენ სერტიფიკაციას და აკრედიტაციას სახელმწიფო დაწესებულებების და სპეციალისტებისა სახელმწიფო სტრუქტურისა იუ–ს სფეროში საერთაშორისო დონეზე აღიარებული სტანდარტებით.

**4.პოტენციალის განვითარება** – განვითარება ადამიანური და ინტელექტუალური პოტენციალისა არსებითია პირველი სამი ფაქტორისათვის (სამართლებრივის, ტექნიკურის და ორგანიზაციულის).

ქვეჯგუფი შედგება შემდეგი მაჩვენებლებისაგან:

$C_{41}$. კადრების მომზადება – მიუთითებს აუცილებლობაზე ახალი საგანმანათლებლო პროგრამებისა, რომლებიც ყურადღებას ამახვილებენ იტ–სპეციალისტების განათლებაზე და პროფესიონალებზე კიბერუსაფრთხოებაში.

$C_{42}$. მოსახლეობის საქმეში ჩახედულობა – საქმეში ჩახედულობის პროგრამები, რომლებიც ითვალისწინებენ მომხმარებლების სწავლებას კიბერსივრცეში ქცევის და და მუშაობის ახალ მოდელებში.

$C_{43}$.სამეცნიერო კვლევები და ინოვაციები - აუცილებელია ჩატარება კომპლექსური სამეცნიერო–პრაქტიკული კვლევებისა, რომლებიც მიმართული არიან პრობლემების გადაწყვეტაზე კიბერუსაფრთხოების და მდგომარეობის როგორც არსებულის, ასევე მომავალი სისტემების და სერვისების.

$C_{44}$. სტანდარტების დამუშავება – ნებისმიერი ოფიციალურად აღიარებული ეროვნული ან კონკრეტული სექტორებით პროგრამები/პროექტები იუ–ში სტანდარტების კვლევების და დამუშავების,

საუკეთესო პრაქტიკები და წესებიგამოყენებისა სახელმწიფო და კერძო სექტორებში.

$C_{45}$. სახელმწიფო ორგანოების სერტიფიკაცია – ეს მაჩვენებელი შეიძლება შეფასდეს რიცხვით იმ სახელმწიფო ორგანოებისა, რომლებიც სერტიფიცირებულები არიან საერთაშორისო აღიარებული სტანდარტებით.

**5.დაინტერესებული მხარეების თანამშრომლობა** – იუ–ს მართვისათვის აუცილებელია ყველა დაინტერესებული მხარის მონაწილეობა, ამიტომ სახელმწიფო სტრუქტურები და კერძო სექტორი უნდა მუშაობდნენ მჭიდრო თანამშრომლობით.

$C_{51}$. შიდასახელმწიფოებრივი თანამშრომლობა – ოფიციალურად აღიარებულა ეროვნული ან კონკრეტული სექტორების მიხედვით პარტნიორობა იუ აქტივების ტრანსაზღვრო ერთობლივი გამოყენებისათვის სხვა სახელმწიფოებთან ერთად.

$C_{52}$. უწყებათაშორისი თანამშრომლობა – ნებისმიერი ოფიციალურად აღიარებული ნაციონალური ან კონკრეტული სექტორების მიხედვით პროგრამები იუ აქტივების გაცვლისა (ადამიანები, პროცესები, ინსტრუმენტები) სახელმწიფო სექტორში.

$C_{53}$. პარტნიორობა სახელმწიფო და კერძო სექტორებს შორის – ოფიციალურად აღიარებული ეროვნული ან კონკრეტული სექტორების მიხედვით პროგრამები იუ–ს აქტივების გაცვლისა სახელმწიფო და კერძო სექტორს შორის.

$C_{54}$. საერთაშორისო თანამშრომლობა – საერთაშორისო თანამშრომლობა შეიძლება მოიცავდეს საკანონმდებლო ზომებს, ინციდენტებზე რეაგირებას, სამეცნიერო კვლევებს, სერტიფიკაციას აპარატურული და პროგრამული უზრუნველყოფებისა.

**6,იუ–ს მუქარების განვითარება** – აქ ჩვენ განვიხილავთ შემდეგ მაჩვენებლებს:

$C_{61}$. მუქარების აქტორების განვითარება – დინამიკა ცვლილებებისა მუქარების აქტორებში (ინსაიდერები, აქტივისტები/ხაკტივისტები, კრიმინალები, სტრატეგიული კონკურენტები, მტრული სახელმწიფოები).

$C_{62}$. ახალი ტიპის შეტევების გამოჩენა – დამუშავება და განხორციელება კარგად კოორდინირებული, მიზანმიმართული შეტევების, სრულყოფა არსებული შეტევების მეთოდებისა, მრავალბიჯიანი, მრავალვექტორიანი შეტევები, ნულოვან დღის შეტევები, დინამიური, პოლიმორფული მავნე პროგრამები და ა.შ.

$C_{53}$. შეტევების მიზნების განვითარება – განვითარება ახალი ინფორმაციული ტექნოლოგიების (კრიტიკული ინფრასტრუქტურები, მობილური, „ღრუბლოვანი“ გამოთვლები, ინტერნეტი და ა.შ.) და ელექტრონული მომსახურებები.

<u>7.ელ. ხელისუფლების იუ–ს დონე</u> – ელ. ხელისუფლების იუ–ს დონის ინტეგრებული შეფასება, განისაზღვრება ელ. ხელისუფლების იუ–ს რისკების ძირითადი მაჩვენებლების საფუძველზე. განიხილება იუ შემდეგი სამი დონე შესაბამისი რისკების დონეების მიხედვით:

– იუ მაღალი დონე – შეესაბამება რისკის დაბალ დონეს;

– იუ დამაკმაყოფილებელი დონე – შეესაბამება რისკის მისაღებ დონეს;

– იუ დაბალი დონე – შეესაბამება რისკის მაღალ დონეს.

### 1.4. აკმ დინამიკის მოდელირება

აკმ გამოყვანის პროცესები მოიცავენ მდგომარეობის ვექტორს $A_{1xn}$, რომელიც შედგება ფაქტორების n მნიშვნელობებისაგან, და წონით მატრიცას $W_{nxn}$, რომელიც ასახავს წონებს$w_{ij}$ ურთიერთ გავლენისა n–ფაქტორებს შორის. ყოველი ფაქტორის მნიშვნელიბაზე გავლენას ახდენენ მათთან დაკავშირებული ფაქტორების მნიშვნელობები და მათი წინანდელი მნიშვნელობა. აქტივაციის მნიშვნელობა ყოველი ფაქტორისათვის გამოითვლება იტერაციულად შემდეგი წესით:

$$A_i^{(t+1)} = \mathrm{f}(\sum_{j=1}^{n} w_{ij}\, A_j^{(t)}).\ \ \mathrm{i} \neq \mathrm{j} \quad (2)$$

სადაც t – მიმდინარე დროა; A – ფაქტორის აქტივაციის დონე; $A_j$– $C_j$ ფაქტორის აქტივაციის დონეა;$W_{ij}$ – $C_i$ და $C_j$ შორის ურთიერთგავლენის წონაა; f – ზღურბლური ფუნქციაა.

ზღურბლური ფუნქციის სახით გამოიყენება ბინარული, ტრივალენტური და სიგმოიდური ფუნქციები. აქ ჩვენ ზღურბლური ფუნქციის სახით აკმ–თვის გამოვიყენებთ სიგმოიდურ ფუნქციას

$$f(x) = \frac{1}{1+e^{-\lambda x}} \quad (3)$$

სადაც $\lambda$>0, და ფუნქცია უწყვეტია, და მისი მნიშვნელობების უბანს წარმოადგენენ მონაკვეთი {0, 1}.

აქ იგულისხმება, რომ ფაქტორების მდგომარეობა შეიძლება განსაზღვრულ იქნას როგორც არამკაფიო ცვლადები, რომელიც შედგება სამი არამკაფიო სიმრავლისაგან: მაღალი (high), საშუალო (medium) და დაბალი (low).

### 1.5. გამოთვლითი ექსპერიმენტების შედეგები

უნდა აღვნიშნოთ, რომ ყოველ კონცეფციას$C_j$–დან შეუძლია მიიღოს მნიშვნელობები ინტერვალში [0, 1], რომელსაც ასევე ეწოდება „აქტივაციის დონე“. აქტივაციის დონე შეიძლება ინტერპრეტირებულ იქნას როგორც ფარდობითი რიცხვი {25}. უფრო მკაცრად აქტივაციის დონე შეიძლება წარმოადგენდეს წევრობას არმაკაფიო სიმრავლეში, რომელიც აღწერს ლინგვისტურ ზომებს ფარდობითი რაოდენობისა (მაგალითად, დაბალი, საშუალო, მაღალი).

აკმ მოდელირების პროცესი ინციალიზირდება მნიშვნელობების მინიჭებით ინტერვალიდან [0.1] აკმ თითოეული კვანძის აქტივაციის დონისათვის სპეციალისტების/დაინტერესებული მხარეების მიმდინარე მდგომარეობაზე. მნიშვნელობა 0 მიგვანიშნებს იმაზე, რომ მოცემული ფაქტორი არ არსებობს სისტემაში გარკვეული იტერაციით, მაშინ როცა 1 მიუთითებს, რომ მოცემული ფაქტორი ფიგურირებს (არსებობს) მაქსიმალური ხარისხით. სხვა მნიშვნელობები შეესაბამებიან აქტივაციის შუალედურ დონეებს.

# თავი II. ინფორმაციის და უსაფრთხოების შემთხვევების მართვის სისტემებში კონტრზომების შერჩევის მეთოდიკა

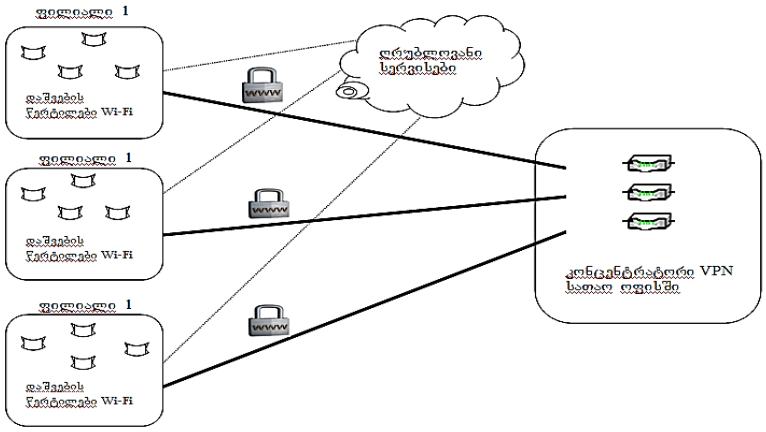
## 2.1. განაწილებული ქსელი დაცვის ქვეშ

თანამედროვე ინფორმაციული სისტემების დიდი უმეტესობა განაწილებული ხასიათისაა და შეუძლიათ ფუნქციონირება მხოლოდ მაღალი წარმადობის მონაცემთა გადაცემის კორპორატიული ქსელის არსებობისას, რომლის გარეშეც ძნელი წარმოსადგენია მუშაობა კომერციული კომპანიების და სახელმწიფო ორგანიზაციებისა.

Zk Research გამოკვლევების მონაცემებით, საწარმოების თანამშრომლების 75%-ზე მეტი მუშაობს სათაო ოფისის გარეთ – ფილიალების ტერიტორიაზე. ყველა მათგანს სჭირდება დაშვება კორპორატიულ დანართებთან და მონაცემებთან, მათ შორის ისეთ რიტიკულად მნისვნელოვან სისტემებთან, როგორიცაა racle E-Busieness Suite, NetSuite, Sage ERP Microsoft Dynamics. რაც ისე იშვიათად ისინი მუშაობენ ღრუბლოვან დანართებთან – მაგალითად, Salesforce.com, Google Apps da Microsoft Office 365.

ორგანიზაციებში ერთიანი კორპორაციული ქსელის შესაქმნელად ხშირად გამოიყენება VPN შეერთება ინტერნეტის გამოყენებით IPSec მიხედვით, ზოგჯერ ოპერატორული ქსელებით MPLS (იხ. ნახ.12.). მსგავსი ქსელური ინფრასტრუქტურის დაცვა ხდება აუტენტიფიკაციის, დაშვების მართვის, გვირაბების გაყვანით დანაყოფებს შორის და დაშიფვრის გამოყენებით.

ვირტუალური კერძო ქსელების ტექნოლოგია (Virtual Private Network, VPN) უზრუნველყოფს სიმრავლეს უპირატესობებისა შედარებით არც ისე მაღალი ღირებულებისას. VPN– ლოგიკურიკერძოქსელი, რომლის ორგანიზებაც ხდება საყოველთაო ქსელის ზემოთ. გამოყოფილი არხების მსგავსად, ის საშუალებას იძლევა შეიქმნას დაცული შეერთება მოშორებულ პლათფორმებს ან ლოკალურ ქსელებს შორის.

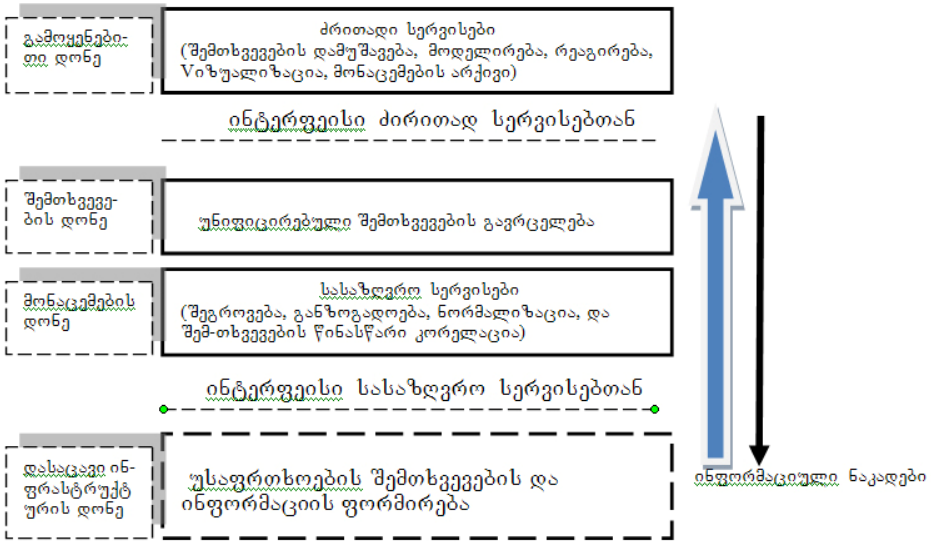



ნახაზი 11. განაწილებული კორპორაციული ქსელი უმავთულო სეგმენტებით ფილიალებში

ქსელური უსაფრთხოების ძირითად მიმართულებებს განეკუთვნებიან კორპორაციული ინფორმაციული სისტემის რესურსებთან დაშვების მართვა, მისი პერიმეტრის დაცვა, ტრანზაქციების აუტენტიფიკაცია, უსაფრთხოების შემთხვევების მონიტორინგს და სხვა.

## 2.2. კრიტიკულად მნიშვნელოვანი ნფრასტრუქტურებში ინფორმაციის დაცვის ინტელექტუალური სერვისების არქიტექტურა

იდისს-ში (ინფორმაციის დაცვის ინტელექტუალური სერვისების სისტემა) SI ტექნოლოგიის პრინციპების შესაბამისად უნდა გამოიყოს უსაფრთხოების შემთხვევების დამუშავების სამი ჯგუფი: 1) საწყისი ინფორმაციის წარდგენის ფორმატისშ ეგროვებისა და გარდასახვის მექანიზმები; 2) მოთხოვნით ინფორმაციის შენახვის, ძებნისა და გაცემის მექანიზმები; 3) ინფორმაციის ანალიზისა და გადაწყვეტილებათა გამომუშავების მექანიზმები. იდისს პრაქტიკული რეალიზაცია კმი-თან (კრიტიკულად მნიშვნელოვანი ინფორმაცია) მიმართებაში მოითხოვს გამომუშავებას გადაწყვეტილებებისა, რომლებიც დაკავშირებული არიან როგორც თვით იდისს არქიტექტურის გამომუშავებასთან, ასევე მის შემადგენლობაში შემავალი კომპონენტებისა.




ნახ.13 იდისსსაერთო (ზოგადი) არქიტექტურა.

# თავი III. ანალიზი განუსაზღვრელობებისა დარღვევების და მისი იზ – ის ეფექტურობის შეფასების მოდელირების პროცესების

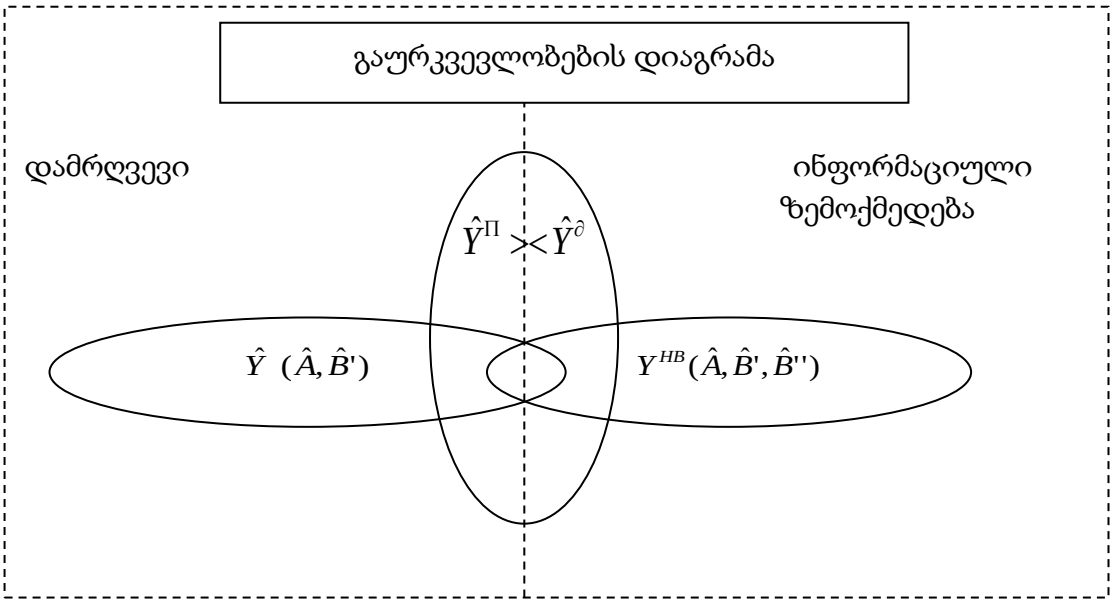
დამრღვევის მოდელირების პროცესი მოიცავს განუზღვრელობებს:

ტიპი 1. დამრღვევის მათემატიკური სტრუქტურის – დამრღვევის პოტენციალის განუსაზღვრელობა – $\hat{Y}^{n}(\hat{A},\hat{B}')$

ტიპი 2. დამრღვევის მიერ იზ (ინფორმაციული ზემოქმედება) – ის სცენარის არჩევის კრიტერიუმის – $\hat{Y}^{\Pi}\underset{<}{\geq}\hat{Y}^{\partial}$,

ტიპი 3. იზ – ის შედეგების ხარისხის მაჩვენებლები $\hat{Y}^{NB}_{<3>}=\hat{Y}^{NB}_{<3>}(\hat{A}_{<K>},\hat{B}_{<I>})$.

პირველი და მეორე ტიპის გაურკვევლობების გადაწყვეტა საშუალებას იძლევა აგებულ იქნას მოდელი დამრღვევის, ხოლო მოიხსნა მეორე და მესამე ტიპის გაურკვევლობების – მოდელი B" – ის იუ – ს დარღვევის პროცესის მოდელი. ნახ. 32 – ზე მოყვანილია სქემატური დიაგრამა, რომელზეც ილუსტრირებულია ჩამოთვლილი გაურკვევლობების დამოკიდებულებები.




ნახ. 32 სქემატური დიაგრამა, რომელზეც ილუსტრირებულია დამოკიდებულებები გაურკვევლობების დარღვევის და მისი ზემოქმედებები მოდელირების პროცესზე

უფრო დეტალურად განვიხილოთ გაურკვევლობები, რომლებსაც აწყდებიან მკვლევარები დარღვევების მოქმედებების მოდელირებისას.

ჯერ – ერთი შეტანა გაურკვევლობებისა დამრღვევის მათემატიკურ სტრუქტურაში, რომელიც აღიწერება ვექტორით $\hat{Y}^{\Pi}_{<3>}$ საშუალებას იძლევა მოდელირებისა აისახოს რეალური პირობები დარღვევის შესახებ ცნობების არა სრულობისა უკიდურეს შემთხვევაში გაურკვევლობისა არასტრუქტურულობა, ანუ შესაბამისი მოდელის აგების შეუძლებლობა დარღვევის დროს, რომელიც განეკუთვნება ამა თუ იმ ტიპის მათემატიკურ სტრუქტურას. იმისათვის რომ მოიხსნას ესსტრუქტურულიგანუსაზღვრელობა შეიძლება შემოთავაზებულ იქნას მასკირება ტპ (ტექნოლოგიური პროცესი) მას – ის ინფორმაციული რესურსების მასკირების ტექნოლოგია, რომელიც შემოთავაზებულია ნაშრომში. მოცემული ტექნოლოგია საშუალებას იძლევა:

– აღმოჩენილი იქნას ინფორმაციულ რესურსებზე დამრღვევის იზ – ის ფარული არსება,

ფორმირებული იქნას დარღვევის რეფლექსური მართვა მატყუარა საინფორმაციო – გამოთვლითი გარემოს მეშვეობით, რომლის პარამტრები აღიწერება ვექტორით $\hat{B}^{''}_{<I>}$)

მასკირების მიზანია დარღვევის იდენტიფიკაცია (მოდელის აგება), ანუ განსაზღვრა პარამეტრების $\hat{A}^{'}_{<k'>}, \hat{A}^{''}_{<k''>}$ მნიშვნელობების და ფორმირება ვექტორის $\hat{Y}^{\Pi}_{<3>}$ ეს მიიღწევა დარღვევისათვის შეტევის ობიექტზე (შო) მცდარი შეხედულების შექმნა $\hat{B}^{'}_{<3'>}$ შეცვლთ $\hat{B}^{'}_{<I'>}$ როგორც შედეგი, ხდება რეალიზება შესაძლებლობისა. ყოველმხრივი შესწავლისა სტრუქტურის პოტენციალის $\hat{Y}^{\Pi}_{<3>}$ შეფასების: განსაზღვრა საკუთარი დამცავი ზომების $\hat{B}^{'}_{<3'>}$ ჩამონათვალისა.

იდეა მდგომარეობს იმაში, რომ გამოკვლეულიქნას განუსაზღვრელობა დარღვევისთვის იზ რეალიზაციის ამა თუ იმ სცენარის შერჩევისას. მოცემული მიდგომისას არ ისმება ამოცანა პოტენციალის $\hat{Y}^{\Pi}_{<3>}$ განსაზღვრისა, ვინაიდან უცნობია პარამეტრების $\hat{A}^{'}_{<k'>}, \hat{A}^{''}_{<k'>}$ მნიშვნელობები. შემოთავაზებულია შეფასებულ იქნას დამრღვევი იზ – ის შესაძლო მუქარების შესატყვისი ტიპები $U = \{U_i\}_{i=1}^{N}$ და „მექანიზმში შერჩევა“ $\lg(\eta_j^i)$ სცენარისა კონკრეტული მუქარის $\eta_j^i \in U_i$ რეალიზაციისა ანუ დამრღვევის მოდელის სახით განიხილება მისი პროფილი <U,G> ცენტრის არჩევის წინ დამრღვევი აწყდება:

– ტპ მას – ის სპეციფიკის შესწავლის პროცესში და იდენტიფიკაციის ვექტორების $\hat{B}^{'}_{<I'>}$ და $\hat{B}^{''}_{<I''>}$

– შედარებისა $\hat{Y}^{\Pi} \underset{<}{\geq} \hat{Y}^{\partial}$ და განსაზღვრისას დასაშვები მნიშვნელობებისა $\hat{Y}^{\Pi}_{<3>}(B^{''}_{<I'>})$ ვექტორისა $\hat{Y}^{\Pi}_{<3>}$ თავისი პოტენციური შესაძლებლობებისა.

ცხადია, რომ გამოთვლაზე საუბარი იზ – ის სტოქასტილურ ბუნებისა არარაციონალურია, ვინაიდან დარღვევისთვის არჩევენ არა შემთხვევით

პროცესს. მისი არჩევანი მიზანშეწონილია, რაც განპირობებულია არჩევის გარკვეული კრიტერიუმებით.

მაშინ შეიძლება ითქვას, რომ "შერჩევის მექანიზმი" $\lg(\eta_j^i)$ ხასიათდება ამა თუ იმ უცნობი (შემთხვევითი) ფაქტორების არსებობით. ამ შემთხვევაში აუცილებელია შემოტანა დაშვებისა – იუ – ის აუდიტორისათვის ცნობილია სიმრავლე U იუ – ის ტიპიური მუქარების და მათი რეალიზაციის სცენარები. ეს დაშვება სავსებით დასაბუთებულია, ვინაიდანსწორედ იყო ტიპიური მუქარები ცნობილი.

განვასხვავებთ შემდეგი სამი ტიპის სიტუაციას:

<u>პირველ ტიპს</u> მივაკუთვნებთ სიტუაციას, როდესაც სიმრავლე მუქარების U და შერჩევის კრიტერიუმები lg ცნობილია. მოცემულ სიტუაციაში დარღვევის პრიფილი ცნობილია, რჩება მხოლოდ ოპერატიულად მოხდეს შესაბამისი დაცვის ორგანიზება.

<u>მეორე ტიპი</u> მოიცავს სიტუაციას, რომლის დროსაც სიმრავლე მუქარებისა ცნობილია, ხოლო შერჩევის lg კრიტერიუმები უცნობია. მოცემულ შემთხვევაში დაცვის მართვის პროცესი ჰგავს თამაშის პროცესს. ასეთი ამოცანის ამოხსნით დაკავებულია მათემატიკის ნაწილი, რომლის სახელიცაა „თამაშთა თეორია". თამაშების თეორიის ქვეშ ხშირად ესმით თეორია მათემატიკური მოდელებისა ოპტიმალური გადაწყვეტილებების მიღების გაურკვევლობების და კონფლიქტების პირობებში. მაგრამ თამაშთა თეორია როგორც მათემატიკური აპარატი, ხასიათდება კონცეპტუალური არასისრულით. ასე მაგალითად. რეალურ კონფლიქტში შესაძლო მუქარების U ჩამონათვალი მათირეალიზაციის სცენარები უცნობია, და დამრღვევისათვის ყველაზე უკეთესი გადაწყვეტილება კონფლიქტურ სიტუაციაში იქნება გამოსავალი იზ – ის ცნობილი სცენარების ფარგლებიდან.

<u>მესამე ტიპში</u> შედიან სიტუაციები, როდესაც მუქარების სიმრავლე U უფრო ზუსტად მათი რეალიზაციის სცენარები, უცნობია. მოცემულ სიტუაციაში დაცვის სისტემას უნდა შეეძლოს ოპერატიულად გადაჭრას უცნობი იზ დაცვის მექანიზმების დროული მიმართვით და / ან

კონტრმოქმედებებით საამისოდ დაცვის სისტემა აღჭურვილი უნდა იყოს პრინციპულად ახალი თვისებით, რომელიც საშუალებას მისცემს მას ოპერატიულად გაითვალისწინოს რეალიზაცია უცნობი მუქარისა U და თავის დროზე მოემზადოს მისთვის. ასეთ თვისებას ეწოდება „ანტიციპაცია“, რომელიც უფრო დეტალურად განხილულია ნაშრომში მესამე (გაურკვევლობის (შემთხვევითობის) დონე იზ – ის შედეგების ხარისხის მაჩვენებლების $\hat{Y}^{NB}_{<3>} = \hat{Y}^{NB}_{<3>}(\hat{A}_{<k>}, \hat{B}_{<I>})$, რომელიც იყენებს პროფილს $<U, \lg>$, ხასიათდება ალბათობით $P^{NB}_{DL}$ ოპერაციის მიზნის მიღწევისა და წარმოადგენს იზ – ის ეფექტურობის მაჩვენებელს . მართლაც ვექტორები $\hat{A}_{<k>}, \hat{B}^{'}_{<I>}$ ხოლო მაშასადამე $\hat{Y}^{\Pi}_{<3>}$ აღმოჩნდებიან შემთხვევითები უფრო მეტიც აპრიორულად შემთხვევითებია და დასაშვებია მნიშვნელობები $\hat{Y}^{\partial}_{<3>}$ ვექტორისა $\hat{Y}^{\Pi}_{<3>}$ რამდენადაც დამრღვევის მიერ იზ – ის ჩატარებამდე ჩვენთვის უცნობია თუ როგორი უნდა იყოს ამ ზემოქმედების შედეგები, რათა მიღწეულ იქნას დამრღვევის მიერ დასახული მიზანი ანუ

$$\begin{cases} \hat{Y}^{\Pi}_{<3>} = \hat{Y}^{\Pi}_{<3>}(\hat{A}_{<k>}, \hat{B}^{'}_{<I'>}) \\ \hat{Y}^{\partial}_{<3>} = \hat{Y}^{\partial}_{<3>}(\hat{B}^{''}_{<I'>}) \end{cases}$$

ვინაიდან რეალურ პირობებში იზ – ის ვარგისიანობის კრიტერიუმები ღებულობს სახეს $G_L : \hat{Y}^{\Pi}_{<3>} \in \{\hat{Y}^{\partial}_{<3>}\}$, მაშინ $G^{NB}_{DL} = P(\hat{Y}^{\Pi}_{<3>} \in \{\hat{Y}^{\partial}_{<3>}\})$ როგორც ჩანს ვარგისიანობის ფაქტი ოპერაციის შედეგებისა არის შემთხვევითი (მოვლენა) ხდომილება. ამიტომ დამრღვევის მიერ ოპერაციის მიზნის მიღწევის ზომა წარმოადგენს ალბათურ მახასიათებელს $P^{NB}_{DH}$ გამოსათვლელად საკმარისია (მაგრამ არაა აუცილებელი) განსაზღვრული იქნას დამრღვევისათვის პროფილით <U,lg> ხელწშემწყობი პირობები U მუქარების რეალიზაციისათვის. იზ – ის რეალიზაციის პირობების ქვეშ მოიაზრება ცოდნა (ქონა)ინფორმაციის დარღვევებისა:

– ITCS (Information Technology Cet Security)სტრუქტურებისა და მახასიათებლების

– მოწყვლადობებისა პროგრამულ აპარატურაში უზრუნველყოფისა და დაცვის სისტემის.

### 3.1.იუ – ის დამრღვევის მოდელირებაზე რეკომენდაციები

ზემოთ წარმოდგენილი დამრღვევის პოტენციალის და მისი ზემოქმედებების ეფექტურობის შეფასების ხერხები კონცეპტუალურია და საჭიროებენ შემდგომ გამოკვლევებს. შემდგომი გამოკვლევების მიმართულება – გამომდინარეობს დამრღვევის გამოვლენის მეთოდის სტრუქტურის გაურკვევლობით. ვინაიდან მოცემული მიდგომების რეალიზაცია იუ – ის აუდიტის ჩარჩოებში ყოველთვის როდია შესაძლებელი, რადგან მოითხოვს დამატებითი ტექნიკური საშუალებებს და დროის ხარჯს. ამიტომ აუდიტის ჩატარების მსვლელობისას ფართოდ გამოიყენება დამრღვევის ექსპერტული შეფასებები იუ – ის შესაძლო U მუქარების ტიპები, რომელთა გამოყენებაც მას შეუძლია. შესაბამისად, დარღვევის მოდელი უნდა განსაზღვრავდეს თუ რომელ შესაძლო შემტევ მოქმედებებს ანიჭებს უპირატესობას დამრღვევი, იგულისხმება ელემენტარული მოვლენები იუ – ის დარღვევისა, რომელთაგან ხდება ფორმირება იზ – ის მუქარების რეალიზაციის სხვადასხვა სცენარების. ანუ აუდიტორის წინაშე დგას ამოცანა დასაბუთებული შემცირების U სიმრავლის სიმძლავრის მოცემული ამოცანის ფორმულირებისას, შეიძლება მიღებულ იქნას შემდეგი დაშვებები არსებულ მონაცემებზე

– დამრღვევის ცოდნის დონესა და კომპეტენტურობაზე.

– დამრღვევის საწყის პოზიციაზე ITCS – ში, რომელიც განსაზღვრავს მისთვის ხელმისაწვდომი პოსტების სიის გარკვეული ფორმალური მოდელისM საფუძველზე,

– დამრღვევის საწყის უფლებებზე, რომლებიც ზღუდავენ სიმრავლის იზ–ის რეალიზაციისათვის საჭირო პირობების საფუძველზე.

ერთმანეთისაგან განსხვავებით დამრღვევის აპრიორულ $N^A$ და აპოსტერიორულ $N^P$ მოქმედებას. პირველ ტიპს მივაკუთვნებთ მოდელს, ჩამონათვალი პარამეტრების და მათი მნიშვნელობების, რომელიც

განსაზღვრულია კონკრეტულ საკვლევ ავტომატიზებულ სისტემის სტრუქტურასთან დაკავშირების გარეშე. მის სტრუქტურას განსაზღვრავენ ჰიპოთეზები, რომლებსაც წარმოადგენენ აუდიტორები მათთვის ცნობილი აპროირული მონაცემების და საკუთარი კომპეტენციის საფუძველზე. შედეგად აპრიორული მოდელი დამრღვევის, რომელიც ითვალისწინებს მისთვის სასურველ შესაძლო შემტევი მოქმედებების არჩევას გამოიყენება შემდეგნაირად: პოტენციურად

$$N^A =< Z, H, K, G >$$

სადაც Z – საწყისი ცოდნაა დამრღვევის ყოველი შეტევის სამიზნე პოსტის და დაშვების უფლებების, რომელსაცეს დამრღვევი ფლობს, H – პოსტები, რომლებთანაც დამრღვევს გააჩნია ფიზიკური ან დაშვებული წვდოვა შეტევების განხორციელების დაწყებამდე, K – დამრღვევის კომპეტენტურობის დონე, ანუ კლასების სია –დაფუძნებული მისთვის მოწყვლადი, ხელმისაწვდომი შემტევი მოქმედებების, რომლებიც ხასიათდებიან განსხვავებული კრიტიკულობით, ასევე ინფორმაციის შეგროვების სხვადასხვა მეთოდებით, G – დამრღვესის ძირითადი მიზნები, მაგალითად, ტექნოლოგიური პროცესის (ტპ) მართვადობის კონტროლიზებადობის ან იდენტიფიცირებადობის მოშლა.

დამრღვევის მოქმედებების მოდელირებისათვის, მისი სტრუქტურის ადეკვატური ასახვისათვის, აუცილებელი იქნება დამუშავებული იქნას ონტოლოგიური მოდელი დამრღვევის შესახებ ცოდნის წარმოსადგენად. შემდეგ, მაგალითად, აუდიტის ჩატარების მსვლელობისას „გაჯერდეს“ ის ექსპურტული მონაცემებით (ჰიპოთეზებით) დამრღვევის შესახებ კონკრეტული ტპ მას – თან მიმართებაში და ასეთნაირად ჩამოყალიბებულ იქნას დამრღვევის შესახებ ცოდნის ბაზა $BZ^N$.

დამრღვევის აპრიორული მოდელის $N^P$ დამუშავება მდგომარეობს ნაპოვნი იქნას შესაბამისობა q მოწესრიგებულ $N^A$ სიმრავლეებს და $V^{ПАО}$ სიმრავლეებს შორის ან $q = (N^A, N^{ПАО}, Q)$ სადაც $N^{ПАО}$ არის სიმრავლე ავტომატიზებული სისტემის პროგრამული – აპარატურული

უზრუნველყოფის მოწყვლადობებისა. სიმრავლე $Q \subseteq N^A \times V^{ПАО}$ განსაზღვრავს წესს, რომლის საშუალებითაც ხორციელდება შესატყვისობა სიმრავლეების $N^A$ და $V^{ПАО}$ ელემენტებს შორის და როგორც შემდეგი, მოძიება მოწყვლადობების სიმრავლისა $V^A \subseteq V^{ПАО}$, რომლებითაც შეიძლება ისარგებლოს დამრღვევმა $N^A$. სიმრავლე $V^N$ ეწოდება q შესატყვისობის ცოდნის არე. შედეგად აპოსტერიორული მოდელი დამრღვევისა. $N^P$ ღებულობს სახეს $N^A =< Z, H, K, G, V^N >$.

სხვა გადაწყვეტა $V^N$ სიმრავლის პოვნისა მდგომარეობს დამრღვევის ონტოლოგიური მოდელის სტრუქტურის შეცვლა გათვალისწინებით, იმ ცნობებისა, რომლებიც მიიღება მოწყვლადობათა ცოდნის ბაზებთან $BZ^V$.

## 3.2. იუ – ის დარღვევის პროცესების სემანტიკური კვლევების ასპექტები სტრუქტურული ინდიკაციის თეორიის პოზიციიდან

როგორც უკვე ავღნიშნეთ, იზ – ის შედეგების ხარისხის მაჩვენებლების $\hat{Y}^{NB}$ განუსაზღვრელობა ფასდება ალბათობით ოპერაციის $P_{OL}^{NB}$ მიზნის მიღწევისა, რაც სწორედ წარმოადგენს მაჩვენებლის იზ – ის ეფექტურობას. საკუთრივ დამრღვევის იზ – ის ეფექტურობის $P_{OL}^{NB}$ შეფასებისა განსახორციელებლად საჭიროა განსაზღვრულ იქნას საჭირო მნიშვნელობა $P_{DL}^{TP}$ იზ – ის ეფექტურობის მაჩვენებლისა $P_{DL}^{TP}$ ფორმულირებულ და რეალიზებულ იქნას გამოსადეგობის კრიტერიუმები $G_{L\ni} : P_{DL}^{NB} \geq P_{DL}^{TP}$

ზემოთ მოყვანილი სიტუაციების რაოდენობრივი ანალიზისათვის ავაგოთ მისი მათემატიკური მოდელი. საამისოდ გამოვიყენებთ სტრუქტურული ინდიკაციის თეორიის მეთოდებს.

განვიხილოთ ორჯერ განუსაზღვრელი გამონათქვამი პრედიკატის სახით $\hat{Y} > \hat{Z},$, სადაც $\hat{Y}$ და $\hat{Z},$ არის ურთიერთდამოკიდებული შემთხვევითი ცვლადები. განვსაზღვროთ ალბათობა შემთხვევითი მოვლენისა:

$\hat{A} = (\hat{Y} > \hat{Z})$:

$$P(\hat{Z} < \hat{Y}) : \int_{-\infty}^{\infty} F_{\hat{z}}(y) dF_y(y); \tag{4}$$

$$P(\hat{Y} > \hat{Z}) : \int_{-\infty}^{\infty} R_{\hat{y}}(z) dF_{\hat{z}}(z); \tag{5}$$

სადაც $\left.\begin{matrix} F_{\hat{X}}(x)^d = P(\hat{X} < X) \\ R_{\hat{X}}(x)^d = P(\hat{X} \geq X) \end{matrix}\right\} - \hat{X}$ განაწილების ფუნქციაა

შემოვიტანოთ შემდეგი აღნიშვნები:

$$\hat{\omega}_1 = \omega_1(\hat{y}) = F_{\hat{Z}}(\hat{y}) \tag{6}$$

$$\hat{\omega}_2 = \omega_2(\hat{z}) = R_{\hat{y}}(\hat{z}) \tag{7}$$

მაშინ როგორც ჩანს გამოსახულებიდან (1) და (2)

$$\left.\begin{matrix} P(\hat{z} < \hat{y}) = M[\hat{\omega}_1] = \overline{\omega}_1 \\ P(\hat{y} \geq \hat{z}) = M[\hat{\omega}_2] = \overline{\omega}_2 \end{matrix}\right\} \Rightarrow \overline{\omega}_1 = \overline{\omega}_2 \tag{8}$$

შემთხვევითი სიდიდეებს $\overline{\omega}_1$ და $\overline{\omega}_2$ ეწოდებათ სტოქასტიკური სუპერინდიკატორები ]3 – 5[. ვინაიდან ყოველ ორადგილიან განუსაზღვრელ პრედიკატს შეესაბამება ორი სუპერინდიკატორი, მაშინ მათი ერთმანეთისგან განსხვავებისათვის ისინი აღინიშნებიან ინდექსების (ნომრები).

]5] თანაფარდობიდან გამომდინარეობს, რომ

$$P(\hat{z} < \hat{y}) = \overline{\omega}_1 = \int_0^1 \omega dF_{\hat{\omega}_1}(\omega) = P(\hat{y} \geq \hat{z}) = \overline{\omega}_2 = \int_0^1 \omega dF_{\hat{\omega}_2}(\omega)$$

სადაც $F_{\hat{\omega}_1}(\omega), F_{\hat{\omega}_2}$ შესაბამისად $\hat{\omega}_1$ და $\hat{\omega}_2$ განაწილების ფუნქციებია.

სუპერინდიკატორები $\hat{\omega}_1$ და $\hat{\omega}_2$ შეუძლიათ მიიღონ უსასრულო სიმრავლე მნიშვნელობებისა ინტერვალიდან [0,1]და გააჩნია აზრი აპოსტერიორული ალბათობის გამოთქმისა A გაურკვეველ (გამოურკვეველ სიტუაციისა $\hat{\aleph}$, მოცემულის $\hat{Y}$ და $\hat{Z}$ შესაბამისად.

ყველა ნათქვამიდან გამომდინარე შეიძლება გაკეთდეს დასკვნა, რომ უპირობო (აპრიორული) ალბათობა შემთხვევითი მოვლენის $A \approx (\hat{z} < \hat{y})$

ტოლია მათემატიკური მოლოდინის იმ პირობითი (აპოსტერიორული) ალბათობის ან სხვა სიტყვებით, ესაა მისი საშუალოდ აწონილი უტყუარობა. ამ დროს, უტყუარობა მოვლენისა $\hat{A}$ განაწილებულია ინტერვალში(0,1) სიმკვრივით $\varphi_{\hat{\omega}_1}(\omega)$ ან $\varphi_{\hat{\omega}_2}(\omega)$. ნათქვამიდან გამომდინარეობს, რომ არამარტო სიტუაციაა განსაზღვრული (ალბათობებია $\hat{z}$ და $\hat{y}$) და ხარისხულ შესაბამისი გამონათქვამის ნამდვილობის (სანდოობის ხარისხი მოვლენის $A=(\hat{z}<\hat{y})$ შემთხვევითია და შეიძლება მიიღოს მნიშვნელობები, რომლებიც განსხვავდებიან 0 და 1 – საგან ან $\overline{\omega}_1 \neq P(\hat{\omega}_1=1); \overline{\omega}_2 \neq P(\hat{\omega}_2=1)$

თუ ცნობილია განაწილების კანონი $F_{\hat{\omega}_2^{<3>}}(\omega)$, მაშინ შეიძლება განსაზღვრული იქნას ორი მნიშვნელოვანი მაჩვენებელიეფექტურობის უნიკალური იზ – ების, რომლებსაც ეწოდებათ გარანტირებადი ალბათობები მისი მიზნის მიღწევის.

$$\omega_{DL}^{\Gamma}(\gamma)\begin{cases}\omega_1^{\Gamma}(\gamma)\overset{d}{=}R_{\hat{\omega}_1^{<3>}}(\gamma)=F_{\hat{\omega}_1^{<3>}}(1-\gamma);\\ \omega_2^{\Gamma}(\gamma)\overset{d}{=}R_{\hat{\omega}_2^{<3>}}(\gamma)=F_{\hat{\omega}_2^{<3>}}(1-\gamma).\end{cases}$$

სადაც γ გარანტიის დონეა (გარანტიის ალბათობა).

რამდენადაც მაგარანტირებელი ალბათობის $\omega_{DL}^{\Gamma}(\gamma)$ განსაზღვრისას გამოიყენება კანონი სუპერ ინდიკატორის განაწილებისა $\hat{\omega}_2^{<3>}$, ამიტომ ეს მაჩვენებელი საშუალებას მოგვცემს შევაფასოდ მომავალი ეფექტურობა უნიკალური (ერთეულოვანი) ოპერაციებისა განსხვავებით ალბათობისაგან, რომელიც საკმარისად სრულად ახასიათებს ეფექტურობას მხოლოდ მასობრივი ოპერაციების. თავისი ბუნებით რეალიზაცია იზ – ის სცენარის უნიკალურია, რაც მიგვანიშნებს $\omega_{DL}^{\Gamma}(\gamma)$ მაჩვენებლისდიდ მნიშვნელობაზე. უნდა აღინიშნოს, რომ არამრავალჯერადი და განსაკუთრებით დამრღვევის მიერ იზ – ის საშუალებების ერთჯერადი გამოყენებისას (ერთეულოვანი იზ – ის რეალიზაციისათვის) გადახრები მაჩვენებლის $\hat{\omega}_2^{<3>}$ ეფექტურობისა იზ – ის მისი საშუალო მნიშვნელობებისაგან $\omega_{DL}^{\Gamma}(\gamma)$ შეიძლება აღმოჩნდეს

არსებითი და მაშინ უნდა გაეწიოს შესაძლებლობას მოუოდნელობების გამოჩენისა ყოველ ცალკეულ შემთხვევაში.

ოპერაციის ეფექტურობის მაჩვენებლის $\omega_{DL}^{\Gamma}(\gamma)$ განმარტებაში ფიგურირებს ორი ალბათობა: გარანტირებული – $\omega^{\Gamma}$ და საგარანტიო – $\gamma$. მათ შორის განსხვავების ასახსნელად წარმოვადგენთ მათ სიხშირულ განხილვას.

რამდენადაც – $\omega_{DL}^{\Gamma}(\gamma)$ – ესაა მინიმალური (ალბათობასთან $\gamma$) პირობითი ალბათობებიდან $\hat{\omega}^{<n>} = \Phi_{\hat{Y}<n>}(\hat{Z}_{<n>})$, რომელსაც ის ღებულობს დამრღვევის მიერ იზ – ის საშუალებების გამოყენების პირობების $B''_{<I''>}$ ფიქსაციისას, ანუ ვექტორის $\hat{Z}_{<n>}$ მნიშვნელობის $\hat{Z}_{<n>}$ ფიქსაციისას, მაშინ $\omega_{DL}^{\Gamma} < \gamma >$ აქვს აზრი მინიმალურად შესაძლო (ალბათობით $\gamma$) წილს დამრღვევის მიერ იზ – ის საშუალებების გამოყენების პირობების რეალიზაციისა, რომლებშიც ოპერაციის მიზანი მიიღწევა ალბათობით $\hat{\omega}^{<n>} \geq \omega_{DL}^{\Gamma}(\gamma)$. მაგალითად, შემდეგი ჩანაწერი $\omega_{DL}^{\Gamma}(0.8) = 0.1$ შეესაბამება $\omega_2^{\Gamma}(0.8) \overset{d}{=} R_{\hat{\omega}_2^{<3>}}(0.8) = P(\hat{\omega}_2^{<3>} \geq 0.8) = 0.1$ ეს ნიშნავს, რომ მოცემულ მომენტში ალბათობით $P_{DL}^{NB} \geq 0.8$ წარმატება უნიკალურია იზ – ის რეალიზაციისა შესაძლებელია შემთხვევების მხოლოდ 10% – ში.

ვითარების დინამიკიდან გამომდინარე მოთხოვნები $P_{DL}^{TP}$ ეფექტურობის მაჩვენებლისადმი $P_{DL}^{NP}$ ასევე თვით $P_{DL}^{NP}$ იცვლებოდნენ იქნება, და როგორც შედეგი, ისინი იქნებიან შემთხვევითი სიდიდეები. შედეგად დამრღვევის მოქმედებების ეფექტურობის მაჩვენებელი ღებულობს სახეს $P_H^*(\hat{P}_{DL}^{ng} \geq P_{DL}^{TP})$. ეს სიტუაცია შეესაბამება ამოცანას, რომელიც მოითხოვს განხილვას შემდეგი სახის მოტივაციის $\hat{\omega}_i \geq \hat{\omega}_j$ (სადაც $\hat{\omega}_i, \hat{\omega}_j$ – ინდექსური სუპერინდიკატორების) გამოთვლა ალბათობის $P(\hat{\omega}_i < \hat{\omega}_j)$ და ანალიზი მისი სტოქასტური თვისებების, ანალოგიურის ზემოთ მოყვანილის ალბათობასთან $P(\hat{y} > \hat{z})$ გამოყენებით. ასეთი

ამოცანების გადასაწყვეტად საჭირო იქნება ტრანსფორმატები განაწილებისა სუპერინდიკატორების $\hat{\omega}_i, \hat{\omega}_j$, რომლებშიც ამ შემთხვევაში შეიძლება ვუწოდოთ პირველირიგის ინდიკატორები, ინდიკატორებში $\hat{\omega}_{ij}^{[2]}, \hat{\omega}_{ji}^{[2]}$) მეორე რიგისა და რეალიზებულ იქნას შემდეგი პროცედურა:

$$P(\hat{\omega}_j > \hat{\omega}_i) = \int_0^1 R_{\hat{\omega}_j} dF_{\hat{\omega}_i}(\omega) = \int_0^1 \omega dF_{\hat{\omega}_{ji}^{[2]}}(\omega) = \overline{\omega_{ji}^{[2]}}$$

## დასკვნა

იუ – ის შესაძლო დარღვევის პროცესების ცნობა უსასრულოა და შესაბამისად დროის ნებისმიერ პერიოდში მკვლევარის ცოდნა შეიცავს გაურკვევლობის ელემენტს, ხოლო რიცხვი საფეხურებისა (დონისა) ამ ანალიზისა შეიძლება შეუზღუდავად იზრდებოდეს. მართლაც ყველა ალბათური მოდელები შემთხვევითი მოვლენების ანალიზი იქნება იმიტომ, რომ ექსპერიმენტის ძირითადი პირობები ცნობილია. მაშ ასე, ალბათობის ელემენტარულ თეორიაში – ესაა „ექსპერიმენტის“ პირობების $\chi$ კომპლექსი, აქსიომატურ თეორიაში – ესაა სივრცე U ელემენტარული მოვლენებისა, მათემატიკურ სტატისტიკაში – ესაა გენერალური ერთობლიობა.

ეს დაშვება დაედო საფუძვლად დღეისათვის არსებულ შემთხვევითი მოვლენების ალბათურ მოდელებს, რომლებიც დამახასიათებელია იუ – ის ცნებისთვის. ეს მოდელები იგება იმ ვარაუდებში, რომ ცნობილია:

– პირობები ოპერაციის განხორციელებისა, მაგალითად, პირობები იზ – ის სცენარების ჩატარებისა,

– განაწილების კანონები და მნიშვნელობები რიცხვითი მახასიათბელბებისა საკვლევი შემთხვევითი სიდიდეების (ვექტორები $\hat{A}'_{<k'>}, \hat{A}''_{<k'>}, \hat{B}'_{<k'>}$)

ოღონდ ამჟამად გამოყენებული ალბათური მოდელები იძლევიან მხოლოდ საშუალო შედეგებს მომავალი მასობრივი ცდებისა, ამიტომ ალბათობა $P_{DL}^{NB}$ იზ – ის წარმატებისა, რომელიც გამოითვლება მოცემულ პირობებში საკმაოდ სრულად დაახასიათებს ეფექტურობას მხოლოდ მასობრივი ზემოქმედებისა, რაც კონცეპტუალურად არაა სწორი.

თავისი ბუნებით იზ – ის ცნების რეალიზაცია უნიკალურია, ვინაიდან დარღვევისათვის ყველაზე უკეთეს გადაწყვეტილებად კონფლიქტურ სიტუაციაში იქნება სწორედ გამოსვლა იზ – ის ცნობილი სცენარების ფარგლებიდან. მეორეს მხრივ, თუ პირობები χ დამრღვევის მიერ იზ – ის განხორციელებისა (ვექტორები $B'_{<I'>}, B''_{<I''>}$) მის განხორციელებამდე უცნობია (საკმარისი სისრულით), მაშინ ამოცანა იზ – ის შედეგების ალბათობების $P_{DL}^{NB}$ განსაზღვრისა ხდება განუსაზღვრელი. მოცემული პრობლემის გადასაწყვეტად – პროგნოზირება ერთეულოვანი ცდების შედეგებისა, ეფექტურია მათემატიკური აპარატი სტოქასტური ინდიკაციის თეორიისა. ის წარმოადგენს საფუძველს უნიკალური ოპერაციების ეფექტურობის შეფასების მეთოდებისა, რომელთა გამოკვლევისათვის ცნობილია ალბათური მეთოდები ნაკლებად გამოსადეგია.

საშტატო ფუნქციონირება ტექნოლოგიური პროცესისა დამოკიდებულია სხვა საწარმოო პროცესების სიმრავლის მუშაობის ხარისხზე, რომელთა დარღვევაც წარმოადგენს დამრღვევის იზ – ის მიზანს. მაშინ შეიძლება ითქვას, რომ გამოსავალს დამუშავებული ოპერაციული კომპლექსისა წარმოადგენს სიმრავლე სტოქასტური სუპერინდიკატ– ორებისა, რომლებიც შეესაბამებიან დამრღვევის იზ – ის მიზნების სიმრავლეს. კომპლექსში ეს სუპერინდიკატორები იძლევიან რაღაც ინტეგრებულ შეფასებას – ინდიკატორის. ამ ინდიკატორის ფიზიკური აზრი ამ ინდიკატორის ხასიათდება ხარისხით ქცევის სისტემისა დამრღვევის წინააღმდეგობის გასაწევად, ტპ მას – ის დაცულობის ფარდობით შეფასების და სიტუაციის გამოურკვევლობის ზომისა, რომელშიც მოქმედებს დამრღვევი.

გამოკვლევა დინამიკაში ინდიკატორის მნიშვნელობებისა, რომლებიც მიიღებიან ოპერაციული კომპლექსის ფუნქციონირების მსვლელობისას საშუალებას იძლევა მომავალში გამოვლენილ იქნას თვით ფაქტი დამრღვევის ყოფნისატმ მას – ში, ასევე მისთვის ხალმისაწვდომი იზ – ის სცენარებისა. უნდა აღინიშნოს პროგნოსტიკური შესაძლებლობები ოპერაციული კომპლექსისა, რომლებიც საშუალებას იძლევიან გამოკვლეულ იქნას დამრღვევი დროის მიმდინარე მომენტში, ასევე მოხდეს წინსწრებად გენერირება დამრღვევის ახალი მოდელებისა, გამოკვლეულ

იქნას მათი შესაძლებლობები და შემოთავაზებულ იქნას დაცვის სხვადასხვა ვარიანტები.

# ABSTRACT


**Critic modeling of information security strategic management of the electronic government is analyzed**

The fundamental changes in the state's nature are resulted in a wide arrangement of information and communication technologies in the state management process.
Information security (IS) is one of the main functions of the self-preservation of the electronic government in terms of globalization, increasing risks and uncertainties of public processes. Therefore it is very important to manage the system of the IS-Government security system.
Cognitive approach is widely used for analysis and management of such a system in modern conditions, which allows for the development of the logic of events in a large number of interaction factors.
Georgia, and in general, any developing country, in which information technology-distribution level is far behind the US, Europe, Japan and other developed countries, but kibertaghlitobebis Ignoring, proposed the overall concept and experience gautvalistsineblobam, without exaggeration, that too can be A hinder their further development and bring devastating consequences.
Modern informative systems, as a rule, contain a large number of security related interconnecting devices and means, which provide a large number of information and information. This information should be worked out to investigate possible vulnerabilities in the protection - weaker areas, identify identification of computer attacks and counter-moneys.
Unfortunately, fraudulent use of information technologies has a universal character in modern information society. Communication networks and means, information systems are the permanent satellites of humans, who trusts his personal data, financial transactions, business. Personality "at the other end of the wire" is no longer a reliable side, as it could have been directly in the face of interaction that could "stand" as a party that deserves the trust, easily finds followers in the modern information world.
Dissertation "Research of information security solutions to critical infrastructure in the state, their solution methods and means" consists of the introduction, literature review, 3 chapters, 11 subjects, conclusions and used literature.
The dissertation work is dedicated to researching modern methods of information security, introducing modern methods of information security in the targeted system and increasing the level of information security.
The dissertation work in information security technologies are discussed in detail, starting with the classification of information security, information leakage risk detection, assessment, prevention, response and methods for establishing a precise finishing system (company) information security method BIS implementation mechanism assembling.

The introduction of the dissertation topic, the objectives and objectives of the research, the study level of the subject, the novelty of the thesis and the main findings, its practical significance.
In the first chapter of the work: "Critic modeling of information security strategic management of the electronic government is analyzed" to analyze the problems of information security, their decision methods and means of critical infrastructure in the state. Fuzzy cognitive maps have been studied, el-management factors, mitigation of factors interacting factors, modeling act dynamics and results of computational experiments.
The second chapter: "Critic modeling of information security strategic management of the electronic government is analyzed" are described: a distributed network of clients, critical information infrastructure protection of intellectual services architecture, leakage of confidential information WORLD Io and the neighboring countries (Russia, for example) of the 2016 survey of bi, kmo IS - tpmas's software - the specifics.
The third chapter: "Critic modeling of information security strategic management of the electronic government is analyzed" the analysis of the uncertainties and violations of the IS - the efficiency of the modeling process, IS - an offender's recommendations on modeling and IS - a violation of the processes semantical stopart semantical studies aspects of the theory of indication from the position.
The results of the survey are summarized in the final part of the work.

## გამოქვეყნებული ნაშრომები


1. კუპრაშვილი ჰ., ოდიშარია კ., ალფაიძე ი. სახელმწიფოს პრობლემები და სისტემური მიდგომა მათ დასაძლევად. საისტორიო ვერტიკალები. 37-38. 2017. გვ. 332
2. კუპრაშვილი ჰ., ოდიშარია კ., ალფაიძე ი.თანამედროვე ინფორმაციული ტექნოლოგიების როლი საქართველოს სახელმწიფო სისტუმის სრულყოფაში. საისტორიო ვერტიკალები. 39. 2018. გვ. 39
3. ივანე ალფაიძე. „ელექტრონული ხელისუფლების ინფორამაციული უსაფრთხოების სტრატეგიული მართვის კოგნიტური მოდელი. სტუ. „განათლება“. №1(24). 2019. გვ. 201.
4. ალფაიძე ი. ბრძოლა კიბერთაღლითობის წინააღმდეგ, პრობლემები და პერსპექტივები. სტუდენტთა 86–ე ღია საერთაშორისო კონფერენცია. სტუ. 2019წ