საქართველოს ტექნიკური უნივერსიტეტი

ივანე ალფაიძე

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

წარდგენილია დოქტორის აკდემიური ხარისხის მოსაპოვებლად

სადოქტორო პროგრამა: ინფორმატიკა

შიფრი - 0401

საქართველოს ტექნიკური უნივერსიტეტი

თბილისი, 0175, საქართველო

2019 წ

**საქართველოს ტექნიკური უნივერსიტეტი**

ინფორმატიკის და მართვის სისტემების ფაკულტეტი

ჩვენ, ხელისმომწერნი ვადასტურებთ, რომ გავეცანით **ივანე ალფაიძის** მიერ შესრულებულ სადისერტაციო ნაშრომს დასახელებით: **„სახელმწიფოში კრიტიკული ინფრასტრუქტურის ინფორმაციული უსაფრთხოების უზრუნველყოფის პრობლემების, მათი გადაწყვეტის მეთოდების დასაშუალებების კვლევა“** და ვაძლევთ რეკომენდაციას საქართველოს ტექნიკური უნივერსიტეტის ინფორმატიკის და მართვის სისტემების ფაკულტეტის საუნივერსიტეტო სადისერტაციო საბჭოში მის განხილვას დოქტორის აკადემიური ხარისხის მოსაპოვებლად.

„----“ „----------“, 2019 წელი

თანახელმძღვანელი: ასოც. პროფესორი კ. ოდიშრია

რეცენზენტი: _____

რეცენზენტი: _____

საქართველოს ტექნიკური უნივერსიტეტი

2019 წ

ავტორი: ივანე ალფაიძე

დასახელება: „სახელმწიფოშიკრიტიკულიინფრასტრუქტურის ინფორმაციულიუსაფრთხოებისუზრუნველყოფისპრობლემებ ის, მათიგადაწყვეტისმეთოდებისდასაშუალებებისკვლევა“

ფაკულტეტი: იფორმატიკა და მართვის სისტემები

სადოქტორო პროგრამა: ინფორმატიკა

ხარისხი: საძიებო დოქტორის აკადემიური ხარისხი

სხდომა ჩატარდა: _____

ინდივიდუალური პიროვნებების ანინსტიტუტებისმიერ ზემოთმოყვანილი დასახელებისდისერტაციისგაცნობისმიზნით მოთხოვნის შემთხვევაში, მისი არაკომერციულიმიზნებით კოპირებისადა გავრცელებისუფლებამინიჭებულიაქვს საქართველოსტექნიკურ უნივერსიტეტს.

_____

ავტორის ხელმოწერა

ავტორი ინარჩუნებს დანარჩენ საგამომცემლო უფლებებს და არც მთლიანინაშრომის და არც მისიცალკეულიკომპონენტებისგადაბეჭდვა, ან რაიმე მეთოდითრეპროდუქციადაუშვებელიაავტორის წერილობითი ნებართვისგარეშე.

ავტორიირწმუნება,რომ ნაშრომშიგამოყენებული საავტორო უფლებებით დაცულ მასალებზე მიღებულია შესაბამისი ნებართვა(გარდაიმ მცირეზომისციტირებებისა,რომლებიცმოითხოვენ მხოლოდ სპეციფიურმითითებებს ლიტერატურისციტირებაში, როგორც ეს მიღებულიასამეცნიერონაშრომების შესრულებისას)დაყველამათგანზე იღებსპასუხისმგებლობას.

# რეზიუმე

სახელმწიფო მართვის პროცესში ინფორმაციული და საკომუნიკაციო ტექნოლოგიების ფართო დანერგვის შედეგად ხდება ფუნდამენტალური ცვლილებები სახელმწიფოს ბუნებაში.

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,

საქართველოსათვის, დასაერთოდ, ნებისმიერიგანვითარებადიქვეყნისთვის, რომლებშიცინფორმაციულიტექნოლოგიებისდანერგვა-გავრცელებისდონებევრადჩამორჩებააშშ, ევროპის, იაპონიისდასხვაგანვითარებულიქვეყნებისას, მაგრამკიბერთაღლითობებისიგნორირებამ, შემოთავაზებულისაერთოკონცეფციისდაგამოცდილებისგაუთვალისწინებლობამ, გადაუჭარბებლადშეიძლებაითქვას, რომძალზეშეიძლებაშეაფერხოსმათიშემდგომიგანვითარებადამოიტანოსდა მანგრეველიშედეგები.

თანამედროვე ინფორმაციული სისტემები, როგორც წესი, შეიცავენ დიდ რაოდენობას უსაფრთხოების მართვის ერთმანეთთან დაკავშირებულ მოწყობილობებს და საშუალებებს, რომლებიც აფორმირებენ უზარმაზარი რაოდენობის ინფორმაციას და ინფორმაციის შემთხვევებს. ეს ინფორმაცია უნდა იქნას დამუშავებული იმ მიზნით, რომ გამოკვლეული იქნას დაცვაში შესაძლო მოწყვლადობები – სუსტი ადგილები, მოხდეს იდენტიფიკაცია კომპიუტერული შეტევებისა და მიღებულ-გატარებულ იქნას კონტრზომები.

სამწუხაროდ, თანამედროვეინფორმაციულსაზოგადოებაშითაღლითობასინფორმაციული ტექნოლოგიებისგამოყენებითაქვსსაყოველთაოხასიათი. კომუნიკაციისქსელებიდასაშუალებები, ინფორმაციულისისტემებიიქცნენადამიანისმუდმივთანამგზავრებად, რომლებსაცისანდობსთავისპერსონალურმონაცემებს, ფინანსუროპერაციებს, ბიზნესს. პიროვნება “მავთულისმეორებოლოში” უკვეაღარწარმოადგენსცალსახადსანდომხარეს, როგორცესშეიძლებაყოფილიყოუშუალოპირისპირურთიერთმოქმედებისას, რომშეიძლება “წარდგე” როგორცმხარე, რომელიციმსახურებსნდობას,

ადვილადიპოვამიმდევრებითანამედროვეინფორმაციულსამყაროში.

დისერტაცია „სახელმწიფოშიკრიტიკულიინფრასტრუქტურისინფორმაციულიუსაფრთხოებისუზრუნველყოფისპრობლემების, მათიგადაწყვეტისმეთოდებისდასაშუალებებისკვლევა“შედგება შესავლის, ლიტერატურის მიმოხილვის, 3 თავის, 11 ქვეთავის, დასკვნისა და გამოყენებული ლიტერატურისაგან.

სადისერტაციონაშრომიეძღვნებაინფორმაციულიუსაფრთხოებისთანამედროვემეთოდებისკვლევას, მიზანდასახულსისტემაში (კომპანია) ინფორმაციისუსაფრთხოებისთანამედროვემეთოდებისდანერგვისდაინფორმაციულიუსაფთხოებისდონისამაღლებისმიზნით.

სადისერტაციო ნაშრომში ინფორმაციის უსაფრთხოების თანამედროვე მეთოდები განიხილება დეტალურად, დაწყებული არსებული ინფორმაციული უსაფრთხოების კლასიფიკაციით, ინფორმაციის გაჟონვის რისკების გამოვლენის, შეფასების, თავიდან აცილების,მათზე რეაგირების მეთოდების ჩამოყალიბებით და დამთავრებული მიზანდასახული სისტემისთვის (კომპანია) ინფორმაციული უსაფრთხოების თანამედროვე მეთოდების დანერგვის მექანიზმის აწყობით.

**შესავალში** დასაბუთებულია სადისერტაციო თემის აქტუალობა, კვლევის მიზნები და ამოცანები, ნაჩვენებია საკითხის შესწავლის დონე, ნაშრომის სიახლე და ძირითადი შედეგები, მისი პრაქტიკული მნიშვნელობა.

**ნაშრომის პირველ თავში**: „სახელმწიფოშიკრიტიკულიინფრასტრუქტურისინფორმაციულიუსაფრთხოებისუზრუნველყოფისპრობლემების, მათიგადაწყვეტისმეთოდებისდასაშუალებებისკვლევა“გაანალიზებულია ელექტრონული ხელისუფლების ინფორმაციული უსაფრთხოების სტრატეგიული მართვის კოგნიტიური მოდელი. შესწავლილია არამკაფიო კოგნიტიური რუკები, ელ.ხელისუფლების იუ მართვის ფაქტორები, ფაქტორების ურთიერთგავლენის მატრიცის აგება, აკმ დინამიკის მოდელირება და გამოთვლითი ექსპერიმენტების შედეგები.

**ნაშრომის მეორე თავში**: „სახელმწიფოშიკრიტიკულიინფრასტრუქტურისინფორმაციულიუსაფრთხოებისუზრუნველყოფისპრობლემების, მათიგადაწყვეტისმეთოდებისდასაშუალებებისკვლევა“აღწერილია: განაწილებული ქსელის მუშაობა დაცვის ქვეშ, კრიტიკულადმნიშვნელოვანინფრასტრუქტურებშიინფორმაციისდაცვისინტელექტუალურისერვისებისარქიტექტურა, კონფიდენციალური ინფორმაციის გაჟონვა მსოფლიოში და მეზობელსახელმწიფოებში (რუსეთის მაგალითზე)2016 წლის კვლევის შედეგები, კმო იუ – ის უზრუნველყოფა ტპმას – ის სპეციფიკისგათვალისწინებით.

**ნაშრომის მესამე თავში:**„სახელმწიფოშიკრიტიკულიინფრასტრუქტურისინფორმაციულიუსაფრთხოებისუზრუნველყოფისპრობლემების,

მათიგადაწყვეტისმეთოდებისდასაშუალებებისკვლევა“ წარმოდგენილია ანალიზი განუსაზღვრელობებისა დარღვევების და მისი იზ – ის ეფექტურობის შეფასების მოდელირების პროცესების, იუ – ის დამრღვევის მოდელირებაზე რეკომენდაციები და იუ – ის დარღვევის პროცესების სემანტიკური კვლევების ასპექტები სტოპარტული ინდიკაციის თეორიის პოზიციიდან

ნაშრომის დასკვნით ნაწილში შეჯამებული და განზოგადებულია ჩატარებული კვლევის შედეგები.


## ABSTRACT

### Research of critical security information security solutions in the state, their solution methods and means

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.

## შინაარსი

# ნახაზების ნუსხა

# ცხრილების ნუსხა

# გამოყენებული აბრევიატურა

იუ - ინფორმაციული უსაფრთხოება
იტ – ინფორმაციული ტექნოლოგიები
კრ – კოგნიტიური რუკები
აკრ – არამკაფიო კოგნიტიური რუკები
აკმ – არამკაფიო კოგნიტიური მატრიცა
SIEM – SECUITY INFORMATION AND EVETS MANAGEMENT
CC– Countermeasure Cost
SDNS – Software-Defined Network Security
იდისს – ინფორმაციისდაცვისინტელექტუალურისერვისებისსისტემა
SI – Security Information
სოა – სერვისულად-ორიენტირებულიარქიტექტურა
მის – მასობრივი ინფორმაციის საშუალებები
კიი – კრიტიკული ინფორმაციული ინფრასტრუქტურა
ას – ავტომატიზებულ სისტემები
ტპ მას – ტექნოლოგიური პროცესების მართვის ავტომატიზებული სისტემა
იზ – ინფორმაციული ზემოქმედება
ფპმ – ფუნქციონირების პირობების მახასიათებლები
ტპ – ტექნოლოგიური პროცესი
კმო – კრიტიკულად მნიშვნელოვანი ობიექტი
კმი – კრიტიკულად მნიშვნელოვანი ინფორმაცია

# შესავალი

სახელმწიფომართვის თეორიულიპრობლემები, მისი ფუნქციები, მეთოდებიდარეალიზაციისმექანიზმები, საჯაროდასახელმწიფო პოლიტიკისა დასახელმწიფო მართვისთანაფარდობა და ურთიერთქმედება, სახელმწიფო მართვაში სისტემური მიდგომის გამოყენებასაზოგადოებრივიცხოვრებისადა სახელმწიფომართვის რეფორმებისდღევანდელეტაპზე უაღრესად მნიშვნელოვანია. 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“.

კომუნიკაციისქსელებიდასაშუალებები, ინფორმაციულისისტემებიიქცნენადამიანისმუდმივთანამგზავრებად, რომლებსაცისანდობსთავისპერსონალურმონაცემებს, ფინანსუროპერაციებს, ბიზნესს. პიროვნება “მავთულისმეორებოლოში” უკვეაღარწარმოადგენსცალსახადსანდომხარეს, როგორცესშეიძლებაყოფილიყოუშუალოპირისპირურთიერთმოქმედებისას, რომშეიძლება “წარდგე” როგორცმხარე, რომელიციმსახურებსნდობას, ადვილადიპოვამიმდევრებითანამედროვეინფორმაციულსამყაროში.

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.

ელ. ხელისუფლების იუ–ს მართვა წარმოადგენს სუსტად სტრუქტურირებულ ამოცანას: მართვის ობიექტი წარმოადგენს რთულ სოციოტექნიკურ სისტემას, რომელიც შედგება ავტონომიური კომპონენტებისაგან, თითოეული მათგანი მოქმედებს მიზანდასახულად.

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 და ინფორმაციის შემთხვევებს. ეს ინფორმაცია უნდა იქნას დამუშავებული იმ მიზნით, რომ გამოკვლეული იქნას დაცვაში შესაძლო მოწყვლადობები – სუსტი ადგილები, მოხდეს იდენტიფიკაცია კომპიუტერული შეტევებისა და მიღებულ-გატარებულ იქნას კონტრზომები.

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.

სახელმწიფოშიუსაფრთხოებისუზრუნველყოფისპრობლემების და მათიგადაწყვეტისმეთოდების შემუშავება კრიტიკულიინფრასტრუქტურისინფორმაციულისაშუალებებით.

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 სახელმწიფოშიკრიტიკულიინფრასტრუქტურისინფორმაციულიუსაფრთხოებისპრობლემების, მათიგადაწყვეტისმეთოდებისდასაშუალებებისკვლევა, 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.

სახელმწიფოშიკრიტიკულიინფრასტრუქტურისინფორმაციულიუსაფრთხოებისუზრუნველყოფისპრობლემების, მათიგადაწყვეტისმეთოდებისდასაშუალებებისკვლევა, 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; კრიტიკური ინფორასტრუქტურის ფუნქციონირების, მისი „კიბისებრი“ სისტემური კანონზომიერების კრიტერიუმებით განვითარებისას, მართვის ავტომატიზაციის და მთელი სისტემის ეფექტური ფუნქციონირების, ამ დროს რისკების ეფექტური და ხარისხიანი მართვის, მათ შორის ინფორმაციული უსაფრთხოების უზრუნველოფის ჩათვლით, კონცეპტუალური მოდელის ჩამოყალიბება; ინფორმაციული უსაფრთხოების უზრუნველყოფის თვალსაზრისით საქართველოში

არსებული მდგომარეობის მოკლე ანალიზი კორპორაციული ქსელის მაგალითზე და ამ სფეროში სახელმწიფო პოლიტიკის ძირითადი მიმართულების დადგენა.

სადისერტაციო თემა ძალზე აქტუალურია არა მარტო ცალკეული ორგანიზაციების და სახელმწიფოებისათვის, არამედ მთელი კაცობრიობისათვის, ამიტომ მის გადაწყვეტაში შეტანილ ნებისმიერ, თუნდაც ძალიან მოკრძალებულ წვლილს აქვს მნიშვნელობა, ვინაიდან ხატოვნად, რომ ვთქვათ: „დღევანდელ სამყაროში ნებისმიერი მიზანდასახული სისტემის ფუნქციონირების ხარისხი განსაზღვრავს მისი ხელმძღვანელის ცხოვრების ხარისხს“ -წარმოადგენს მნიშვნელოვან სტიმულს თვით სისტემის მენეჯმენტისათვის – ადამიანისათვის, როგორც თვითმმართველისათვის და დირექტორისათვის როგორც ორგანიზაციის ხელმძღვანელისათვის.

ინფორმაციის დაცვის პრობლემა არასასურველი გარეშე ზემოქმედებებისადმი გაჩნდა იმ მომენტიდან, როგორც კი ადამიანს გაუჩნდა იმის მოთხოვნილება, რომ არ გაეზიარებინა ის სხვა ადამიანებისათვის, ინფორმაციის პრიმიტიული მატარებლების არსებობის პერიოდში მისი დაცვა ხორციელდებოდა ორგანიზაციული ღონისძიებებით, რომლებიც მოიცავდნენ მასთან დაშვების შეზღუდვასა და გამიჯვნას, დასჯის გარკვეულ ზომებს საიდუმლოს გამჟღავნებისას. ჰეროდოტეს თანახმად, ჯერ კიდევ V საუკუნეში ჩ.წ. გამოიყენებოდა ინფორმაციის გარდასახვა კოდირების მეთოდით. თავისი საიდუმლო ანბანი გააჩნდა იულიუს ცეზარს. შუა საუკუნეებში და აღორძინების ეპოქაში ინფორმაციის დასაცავად საიდუმლო შიფრების შექმნაზე შრომობდნენ ცნობილი ადამიანები, მათ შორის ცნობილი ფილოსოფი ფრენსის ბეკონი, მათემატიკოსები ფრანსუა ვიეტი, ჯეროლამო კარდანო, ჯონ ვალისი.

მე-20 საუკუნის 70-80-იან წლებში უდიდესმა მიღწევებმა ინფორმაციული ტექნოლოგიების (იტ) განვითარების მიმართულებით არა

მარტო შესაძლებელი, აუცილებელიც კი გახადა ტექნოლოგიური პროცესების ავტომატიზებასთან ერთად საწარმოების, ორგანიზაციების, კომპანიების, ორგანიზაციული მართვის ავტომატიზებაც, რამაც დიდ პროგრესთან ერთად წარმოშვა უდიდესი საფრთხე, რომელიც დაკავშირებულია ინფორმაციის, როგორც უკვე სისტემაწარმომქმნელი დომინანტის, მთლიანობის, ხელმისაწვდომობის და კონფიდენციალობის დარღვევით გამოწვეულ კატასტროფულ შედეგებთან. ხოლო 1993 წელს ინტერნეტის ოფიციალურმა დაბადებამ და მისმა თავბრუდამხვევმა გავრცელება-ხელმისაწვდომობამ წარმოშვა იტ-ში დამნაშავეობის სრულიად ახალი სახეობა: ხაკერები, კრეკერები, კომპიუტერული ხულიგნები, სპამერები, გაჩნდა კიბერტერორიზმის ცნება. დღეს მეცნიერები აღიარებენ, რომ ფაქტიურად ინფორმაცია იქცა ძალიან საშიშ იარაღად.

მსოფლიოს წამყვანი სახელმწიფოები (აშშ, დიდი ბრიტანეთი, იაპონია და ა.შ.) სტანდარტიზაციის საერთაშორისო ორგანიზაციები (ISO, IEEE და ა.შ.) უდიდეს ძალისხმევას იჩენენ ინფორმაციული ინფრასტრუქტურის უსაფრთხოების უზრუნველსაყოფად. ასევე სახეზეა სამეცნიერო წრეების დიდი ინტერესი და მონდომება აღნიშნული პრობლემის გადაწყვეტისადმი, რაზეც მეტყველებს უამრავი სამეცნიერო სტატიები, მონოგრაფიები. აქვე უნდა აღვნიშნოთ, რომ პოსტსაბჭოთა სივრცის ქვეყნებში იტ დანერგვისა და წარმოშობილი იუ-ს უზრუნველყოფის პრობლემები ყურადღების მიღმა იყო დარჩენილი, დღეისათვის ეს სიტუაცია დიამეტრალურადაა შეცვლილი, ამ მხრივ კარგ მაგალითს იძლევა საქართველო, თუმცა იუ-ს უზრუნველყოფის მიმართულებით მაინც საკმაოდ მძიმე მდგომარეობაა და ეს ეხება განვითარებულ სახელწმიფოებსაც, რაზეც მიგვანიშნებს ის დიდი ზარალი (წელიწადში ათეულობით მილიარდი დოლარი), რასაც განიცდიან ამ ქვეყნებში მოღვაწე კომპანიები, მთავარ მიზეზად აღიარებული კომპანიების მხრიდან იუ-ს უზრუნველყოფისას არსებული რისკების შეუფასებლობა-

გაუთვალისწინებლობაა და რის შედეგადაც კომპანიებს არ გააჩნიათ ინფორმაციის დაცვის საჭირო მეთოდები.

მთავარ საყრდენად კომპანიების, სახელმწიფოშიკრიტიკულიინფრასტრუქტურისინფორმაციულიუსაფრთხოებისუზრუნველყოფისპრობლემების, იუ-ს უზრუნველყოფაში, ჩვენი აზრით, უნდა იქცეს საერთაშორისო საკანონმდებლო მოთხოვნების დაწესება-გაკონტროლება ინტერნეტ სივრცეში მოღვაწე სუბიექტებისათვის, აქ ჩადენილი დანაშაულობების დასჯადობა, სახელმწიფოთა ინფორმაციულ საზღვრების და დამოუკიდებლობის დაწესება-უზრუნველყოფა, სახელმწიფოებმა უნდა იზრუნონ საკუთარი მოქალაქეების, ორგანიზაციების ინფორმაციულ უსაფრთხოებაზე, ხელი შეუწყონ ინფორმაციის დაცვის, რისკების მართვის თანამედროვე კომპიუტერული ცენტრების შექმნას, რომლებიც იზრუნებენ ნებისმიერი მასშტაბის მიზანდასახული სისტემების უსაფრთხოდ, ეფექტურად ფუნქციონირებაზე, რითაც ხელს შეუწყობენ თვით სახელმწიფოების მდგარდ განვითარებას. ამ დროს მხედველობაში გვაქვს ის გარემოება, რომ მსოფლიოს გიგანტი იტ კომპანიები (IBM, Microsoft, Cisco,HP,Oracle და ა.შ.) უდიდეს ინტელექტუალურ და ფინანსურ რესურსებს ხარჯავენ მსგავსი პროგრამული სისტემების შექმნაზე, მაგრამ ისიც ფაქტია რომ ეს საკმაოდ ძვირადღირებული პროდუქტებია, რის გამოც მათი გამოყენება მცირე ბიზნეს კომპანიებისათვის ხელმიუწვდომელია. მდგომარეობას ართულებს ნებისმიერი მიზანდასახული სისტემის ორგანიზაციული უნიკალურობა, ამიტომ საჭიროა ინფორმაციულ სივრცეში, პირველ რიგში, იუ-ს უზრუნველყოფის თვალსაზრისით, ურთიერთთანამშრომლობა და საკუთარი წვლილის შეტანა.

მოცემულ ნაშრომს მეთოდოლოგიურ საფუძვლად უდევს: კონკრეტული შემთხვევების კვლევა, რომლებიც საშუალებას იძლევიან შესწავლილი იქნას სახელმწიფოშიკრიტიკულიინფრასტრუქტურისინფორმაციულიუსაფრთხო

ებისუზრუნველყოფისპრობლემები,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.

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 მოვლენებისა იქნება იმ, 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 მეცნიერული სიახლე მდგომარეობს იმაში, რომ იუ-ში დამატებითი ფაქტორი (ხარჯების გათვალისწინებით) კომპანიის იუ-ის დამატებით ხელსაწყოს წარმოადგენს, კერძოთ ბიომეტრიული პარამეტრის გამოყენება როგორც ინფორმაციაზე დაშვების ახალი პროტოკოლი წარმოადგენს ბოროტგანმზრახველებისთვის ინფორმაციაზე წვდომის დაშვების დამატებით ბარიერს, ასევე თანამედროვე იუ- მეთოდების

გამოყენებით და ლოგების მონიტორინგით შესაძლოა დროული რეაგირების მოხდენა ინფორმაციის გაჟონვის, დამახინჯება, დაკარგივის რისკის მინიმიზაციისთვის, შესაბამისად ქართულენოვანი ლოგების მონიტორინგის სისტემის დანერგვით მეტწილად გამარტივდება ყოველდღიური ლოგების ანალიტიკის საკითხი საქართველოში არსებულ კორპორაციულ ქსელებში, რადგან პრობლემის დაფიქსირებისას (და არა პრობლემის აღმოფხვრისას) საჭირო აღარ იქნება მაღალკვალიფიციური სპეციალისტის ჩარევა და უცხო ენის ცოდნა. იუ – ის დამრღვევის მოდელირებაზე რეკომენდაციები, იუ – ის დარღვევის პროცესების სემანტიკური კვლევების ასპექტები სტოპარტული ინდიკაციის თეორიის პოზიციიდან

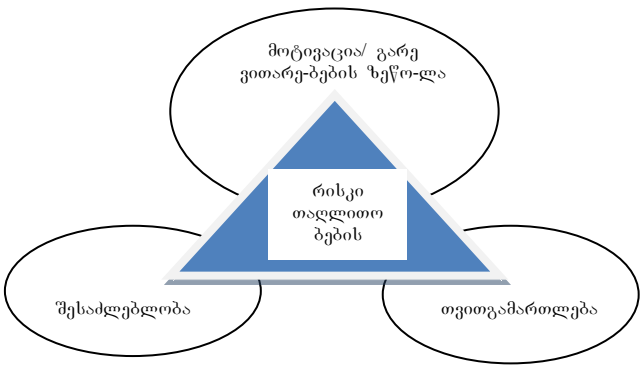
ნაშრომისპრაქტიკულმნიშვნელობასგანაპირობებსმიღებულიშედეგებ ი: ელექტრონული ხელისუფლების ინფორმაციული უსაფრთხოების სტრატეგიული მართვის კოგნიტიური მოდელი: არამკაფიო კოგნიტიური რუკები, ელ.ხელისუფლების იუ მართვის ფაქტორები, ფაქტორების ურთიერთგავლენის მატრიცის აგება, აკმ დინამიკის მოდელირება, გამოთვლითი ექსპერიმენტების შედეგები, ინფორმაციის და უსაფრთხოების შემთხვევების მართვის სისტემებში კონტრზომების შერჩევის მეთოდიკა: განაწილებული ქსელი დაცვის ქვეშ, კრიტიკულადმნიშვნელოვანინფრასტრუქტურებშიინფორმაციისდაცვისინ ტელექტუალურისერვისებისარქიტექტურა, კონფიდენციალური ინფორმაციის გაჟონვა მსოფლიოში და მეზობელ სახელმწიფოებში კვლევის შედეგები:კმო იუ – ის უზრუნველყოფა ტპმას – ის სპეციფიკის გათვალისწინებით, ანალიზი განუსაზღვრელობებისა დარღვევების და მისი იზ – ის ეფექტურობის შეფასების მოდელირების პროცესების, იუ – ის დამრღვევის მოდელირებაზე რეკომენდაციები, იუ – ის დარღვევის პროცესების სემანტიკური კვლევების ასპექტები სტოპარტული ინდიკაციის თეორიის პოზიციიდან.

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.

# ლიტერატურის მიმოხილვა

ბრძოლაკიბერთაღლითობებისწინააღმდეგ პრობლემებიდაპერსპექტივები.სამწუხაროდ, თანამედროვეინფორმაციულსაზოგადოებაშითაღლითობასინფორმაციული ტექნოლოგიებისგამოყენებითაქვსსაყოველთაოხასიათი. კომუნიკაციისქსელებიდასაშუალებები, ინფორმაციულისისტემებიიქცნენადამიანისმუდმივთანამგზავრებად, რომლებსაცისანდობსთავისპერსონალურმონაცემებს, ფინანსუროპერაციებს, ბიზნესს. პიროვნება “მავთულისმეორებოლოში” უკვეაღარწარმოადგენსცალსახადსანდომხარეს, როგორცესშეიძლებაყოფილიყოუშუალოპირისპირურთიერთმოქმედებისას, რომშეიძლება “წარდგე” როგორცმხარე, რომელიციმსახურებსნდობას, ადვილადიპოვამიმდევრებითანამედროვეინფორმაციულსამყაროში. ერთ-ერთიუძველესიკონცეფციათაღლითობებისშეკავებისადააღმოჩენისა – სამკუთხედითაღლითობებისკრიმინოლოგი დონალდკრესის (ნახ.1.) – იდეალურადჯდებაკიბერგარემოში. შესაძლებლობათასიმრავლერომელსაციძლევაიტ-ტექნოლოგია, თაღლითზემოქმედებს, როგორცწითელიმატერიისნაჭერიხარზე, ხოლოხერხებისაკუთარიპერსონისდამალვისაბადებენსაფუძველსდაუსჯელ ობისრწმენისა.

ველაზემთავარიმოტივაციაცხადიაესააფინანსურიმოთხოვნილებები (საჭიროებები).

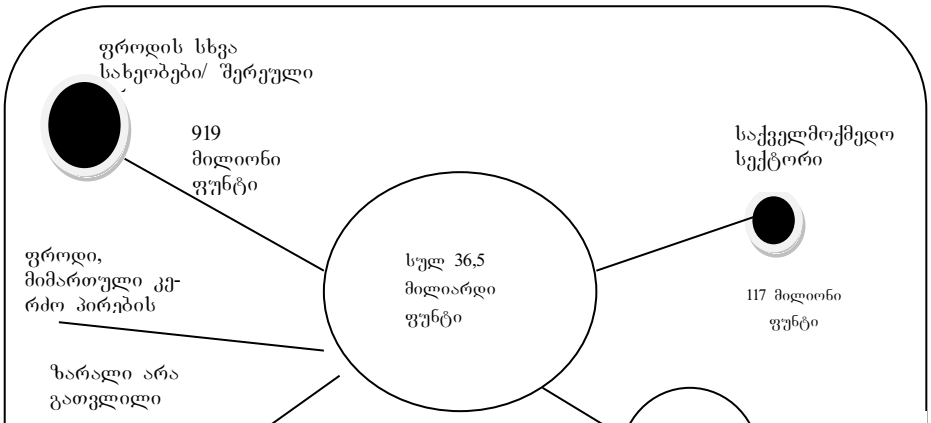


ნახაზი 1. დ. კრესისსამკუთხედი

თაღლითურიოპერაციებისბაზარიძალზეშთამბეჭდავია, თუმცააქრაიმეკონკრეტულრიცხვებზეარაასაუბარი – “ზარალიაჭარბებსასეულობითმილიარდდოლლარს”. სამწუხაროდარარსებობსამსფეროშირაიმეფროდ-მონიტორინგისცენტრი, რომელიცშეძლებდაამსფეროშიკონკრეტიკისშემოტანას – ინფორმაციამთლიანობაშიდაცალკეულიჭრილებისმიხედვით. მეორესმხრივ, არხდებაყველათაღლითობისრეგისტრაცია.

სტატისტიკურიმაგალითისსახითშეიძლებადავასახელოთდიდიბრიტანეთისფროდისწინააღმდეგბრძოლისინსტიტუტის(National Fraud Authority)ყოველწლიურიბიულეტენი, რომლისთანახმადაც 2012 წელისმარტი - 2013 წლისაპრილიპერიოდშიდარეგისტრირებულიქნაკიბერთაღლითობათა (კიბერფროდის) 38 662 შემთხვევა, ხოლოდანაკარგებისსაშუალომაჩვენებელმაშეადგინა 3 629 ფუნტი. იქმნებაშთაბეჭდილება, რომთაღლითობებიაღრიცხულიაერთეულისსიზუსტით, მაგრამწყარომიუთითებს, რომარარსებობსმოყვანილიციფრებისზუსტიშეფასებები, ვინაიდანარარსებობსსაპრობლემოთემასთანდაკავშირებითდაინტერესებულისტრუქტურებისურთიერთმოქმედება.

ანუამონარჩევიარისნაწილობრივიხასიათისდაარასახავსრეალურზუსტსურათს. მისგარდა, ჩარეულიაისეთიცნება, როგორიცააჰიდდენფრაუდ (ნახ.2.) – ფროდი (თაღლითობა), რომელსაცჰქონდაადგილი, მაგრამარიყოიდენტიფიცირებული.



ნახაზი.2. არაცხადიფროდი

რათვისებებითხასიათდებაისეთიმოვლენა, როგორიცააკიბერთაღლითობა? რასაწყდებიანორგანიზაციებიდამომხმარებლებისერვისებისდასისტემებისგ ამოყენებისას? ნირველი – ისფაქტი, რომფროდ-აქტიურობაშესამჩნევიანებისმიერსფერიში, რომელიცდაკავშირებულიაელექტრონულტრანზაქციებთან, სადაცშეიძლებაგამოიყოსზევითმითითებულისამისაწყისიწერტილი – მოტივაცია, ტექნიკურიშესაძლებლობადანაშაულისჩასადენას, კვალისდაფარვისშესაძლებლობა.

ლექტრონულიფროდისყოველისახეობისათვისშეიძლებამოვიპოვოთამომწ ურავიინფორმაციაღიაწყაროებში. ინსაიდერისმხრიდან - თაღლითობები, ფიშინგიფროდიSS– სიაშეიძლებაგავაგრძელოთ. იმისათვის, რომმივიღოთძალიანდიდისიმრავლეყველაშესაძლოსცენარებისა, ღირსშევეცადოთთაღლითობებისმეთოდებიმოვარგოთიმსფეროებს, სადაცმათშეიძლებაგამოყენებაჰპოვონ.

რსებობენეგზოტიკურიდაძნელადხელშიჩასაგდებისცენარები. მაგალითისათვის, პრაქტიკიდანცნობილიაშემთხვევა, როდესაცფროგ-მონიტორინგისსისტემისფიჭურიკავშირისმსხვილოპერატორშიდანერგვისმ იზეზიგახდაშიდათაღლითობებისიდენტიფიკაციისაუცილებლობა, თაღლითობისა, რომელიცდაკავშირებულიიყოთანამშრომლებისმიერსაკუთარილეგალური უჰლებებისბოროტადგამოყენებასთან.

ონუსურიდასალატარეოპროგრამებისფარგლებშიპრიზებიერიცხებოდათარ
არიგითაბონენტებს, არამედოპერატორისთანამშრომლების,
რომლებიცბოროტადიყენებდნენთავიანთმდგომარეობას,
ნაცნობებსდანათესავებს.

კიბერუსაფრთხოებისათვისდამახასიათებელიაცვალებადობა –
დაწყებულითაღლითურიმოქმედებებისსქემებიდანდალოგიკიდანტექნიკუ
რინსტრუმენტამდე, მაგალითად,
მავნებლობისმატარებელპროგრამულიუზრუნველყოფისკოდისა.
შეიძლებაგავავლოთანალოგიათაღლითობისევოლუციასადამუტირებადივი
რუსისვერაგობასშორია, რომელიც "ასნებოვნებს"
ახალსერვისებსდაახერხებსმორგებასდაცვისსისტემებთან,
რომლებიცგადიანსრულყოფისპროცესს.
ფროდთანბრძოლისტექნოლოგიებისდასაშუალებებისპრევენციულიშესაძლ
ებლობებიხშირადაღმოჩნდებიანმოუმზადებლებიახალისცენარებისათვის,
ხოლოგამოძიებების (გამოკვლევების) ჩატარებაგაძნელებულია,
ვინაიდანთაღლითობისფაქტისგანხორციელებამდემომავალმსხვერპლებსარ
ცჰქონიათიმისიფიქრიცკიდაეყენებინათსაჭირო "სენსორები"
ზუსტადიმადგილას,
საიდანაცინფორმაციისმოხსნაიქნებოდამაქსიმალურადსასარგებლო.

სიტუაციასკიდევუფროამძაფრებსთაღლითებისკვალიფიკაციისმაღა
ლიდონე. თანაცსაუბარიაარამარტოტექნიკურკვალიფიკაციაზე.
ტექნიკურიკვალიფიკაციაუმეტესობასცენარებისრელიზებისათვისაუცილებ
ელია, მაგრამარასაკმარისიპირობაა.
კვალიფიკაციისქვეშუნდავიგულისხმოთსაგნობრივსფეროშიმიმდინარეპრ
ოცესებისგაგება, სადაციგეგმებათაღლითურიმოქმედებებისორგანიზაცია.
მოძიება "პარატექნიკურიმოწყვლადობებისა",
არაუსაფრთხოდაგებულიბიზნეს – დატექნოლოგიურიპროცესები,
შესაძლებლობამათშიჩაშენებულიქნასსაკუთარირგოლებისა,
საკანონმდებლოხვრელებისგამოყენება,

რომლებიცბევრშემთხვევაშიქმნიანდაუსჯელობისგანწყობას (შეგრძნებას) – პირველრიგში, აქიტკენაამიმართულითაღლითებისმთელიძალისხმევა. შემდეგინაბიჯი – ესაატექნიკურიინსტრუმენტებისგამოყენება.

რასწარმოადგენსდღეისათვისანტიფროდ-საზოგადოება, დამუქარებისსაპასუხოდრამცდელობებიასაპასუხოღონისძიებებისგატარებისა? საზოგადოება, ბიზნესის, კანონშემქმნელიორგანოების, კომერციულიანსახელმწიფოდანაყოფებისსახით, ბრძოლაშიელექტრონულთაღლითობებთანდაკომპანიები – მომწოდებლებითაღლითობებისწინააღმდეგბრძოლისსაშუალებებისა, გადისევოლუციასპრობლემისაღიარებიდანძალისხმევისკონსოლიდაციისმცდელობამდე.

სხვილდასაშუალოკომპანიებშიდიდიხანიაგამოჩნდადამოუკიდებელიდანაყოფებითაღლითობებთანსაბრძოლველად, ან, როგორცმინიმუმი, პრობლემისაღიარებახდებახელმძღვანელობისდონეზედამისიდამუშავებისათვისგამოიყოფარაღაცრესურსი.

საუბარისაჭიროკვალიფიკაციაზეთაღლითობისათვისადეკვატურიპასუხისგაცემისათვის, ცხადადჩანს, მაგრამგანვითარებასაჭიროტექნიკურიკომპეტენციისადამოუკიდებლადბევრკომპანიასსაამისოდძალაარშესწევს. თუმცა, ისიცფაქტია, რომმსხვილიკომპანიებიცხშირადარარიანმზადცალკე – მარტომუპასუხონმუქარებს.

შწორიიქნებოდასაუბარიკომპანიისშესახებრისკებისშეფასებისასტექნოლოგიურიდაბიზნეს-პროცესებისფუნქციონირებისას, დამათდასამუშავებლადადეკვატურიზომებისმიღებისას.

უმნიშვნელოცვლილებებმაბიზნეს-პროცესებშიშეიძლებათაღლითებსგაუზნელონ “ჩაშენება” სცენარებში, ასევეიყვნენსაფუძველიეფექტურიწერტილებისშესაქმნელადინფორმაციისმოსახსნელადდაამინფორმაციითტექნიკურისისტემებისშემდგომიგამდიდრებისათვის.

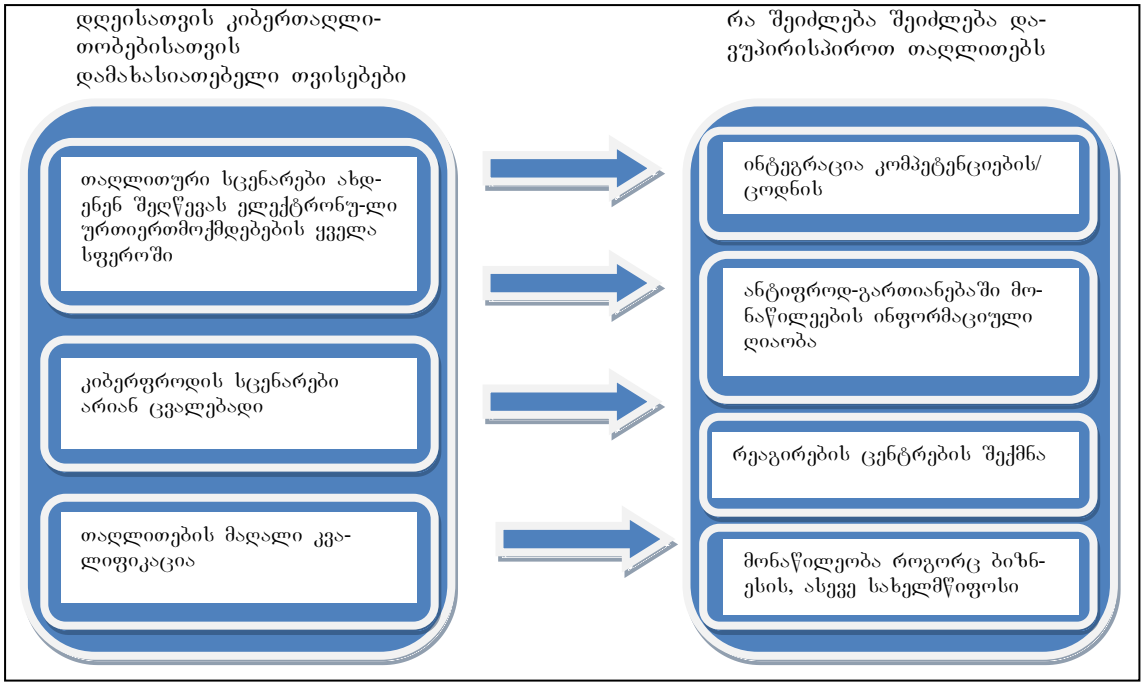
ძალიანსავარაუდოა,
რომრისკებისიდენტიფიკაციადამუქარებისგამოვლენაგამოიწვევსფროდ-მონიტორინგისტექნიკურისაშუალებებისდანერგვას.
აქგადაწყვეტილებათაბაზარიმუდმივადვითარდება,
შემოთავაზებულიროგორცუნივერსალური,
ასევევიწროპროფილიანიგადაწყვეტები. ბიზნესსეხმარებიან - გადაწყვეტები, სპეციალიზებულიგადაწყვეტები – ქცევითიანალიზისსისტემებიფროდ-კეისებისგამოსავლენად.
ჩალსახამსჯელობაბაზარზეამათუიმკლასისგადაწყვეტებისძირითადროლზეიქნებოდაარცისეკორექტული.
მათიძლიერიდასუსტიმხარეებისგამოვლენაშესაძლებელიამხოლოდმუქარტათასპექტრისჭრილში, რომელთანეიტრალიზებასაცემსახურებაგადაწყვეტა.

ნებისმიერშემთხვევაშისაკუთარიკომპეტენციისგაზრდისშესაძლებლობისარარსებობაარუნდაგახდესსაბაბიმუქარისწინაშემელისჩამოჩვებისა.
პირიქით,
ესუნდაიყოსმამოძრავებელიძალაჯვარედინიკავშირებისდასამყარებლადდაინტერესებულორგანიზაციებსშორის,
სახელისუფლებოორგანოებთანდამოტივაციაანტიფროდ-გადაწყვეტებისბაზრისგანვითარებისათვის.
შწორედძალისხმევააკონსოლიდაცია,
უნდაჩავთვალოთძირითადგარანტიადიმისა,
რომრაცშეიძლებაეფექტურადვებრძოლოთთაღლითობებს.

როცავსაუბრობთძალისხმევისინტეგრაციაზე,
შეიძლებამოვიყვანოთროგორცმაგალითი, ევროპულიკავშირის იგიტალ გენდამიერგახმოვანებულისტრატეგია.
ამინციატივისფარგლებშიშემოთავაზებულიადავალდებულება 46 ათასამდედაწესებულებისა (ენერგეტიკულიკომპლექსისდაწესებულებები, ბანკების, სამედიცინოდაწესებულებებისჩათვლით) მოახსენონკიბერფროდისმომხდარისიტუაციებისშესახებკომპიუტერულიდ

ანაშაულებებისსფეროშიგარესიტუაციებზერეაგირებისცენტრს. ასეთიდანაყოფიუნდაშეიქმნასევროკავშირისყველაქვეყანაშიდაიყოსპასუხის მგებელითაღლითობებისშემთხვევებისშესახებინფორმაციისმირებაზე, აგრეგაციაზე, დამუშავებაზე, ასევემინიჭებულიაქვსუფლებადაუწესოსსაჯარიმოსანქციებიკომპანიებს, რომლებმაცდაუშვესგაჟონვა.

მართალიაინციატივამთლიანობაშიმიღებულიქნაროგორცაუცილებელი, მაგრამსაკითხისაჯარიმოსანქციებისდაწესებისკრიტერიუმებისადღემდერჩე ბადისკუსიებისსაგნად.




ნახაზი 3

სამწუხაროდდღემდეუცნობიათურამდგომარეობააამმიმართულებით საქართველოში.

კიბერსაფრთხეთააღიარებასახელმწიფოსდონეზედასპეციალიზებულიცენტრებისშექმნასამართალდამცავორგანოებშიშეიძლებაჩაითვალოსგარდამტეხდააუცილებელმომენტადკიბერდანაშაულებათაპრევენციისადამათწინააღმდეგბრძოლაში.

საკანონმდებლომოთხოვნებიორგანიზაციებისადმიშექმნიანწინაპირობასფროდისთავიდანაცილებისგადაწყვეტებისსაყოველთაოდანერგვისათვის, რაცმნიშვნელოვნადშეზღუდავსთაღლითებისმოღვაწეობისარეალს.

ხოლოძალისხმევათაგაერთიანებისპერსპექტივაორგანიზაციებისა, რომლებიცაღჭურვილიარიანფროდისწინააღმდეგმიმართულიტექნიკურისა შუალებებით, დასამართალდამცავიორგანოებისშესაძლებლობებისა, უეჭველად,

შეარყევსკიბერსამყაროშიდღესარსებულიდაუსჯელობისდაყველაფრისკეთებისუფლებისქონისგანწყობას.

საქართველოსათვის, დასაერთოდ, ნებისმიერიგანვითარებადიქვეყნისთვის, რომლებშიცინფორმაციულიტექნოლოგიებისდანერგვა-გავრცელებისდონებევრადჩამორჩებააშშ, ევროპის, იაპონიისდასხვაგანვითარებულიქვეყნებისას, მაგრამკიბერთაღლითობებისიგნორირებამ, ზევითშემოთავაზებულისაერთოკონცეფციისდაგამოცდილებისგაუთვალისწინებლობამ, გადაუჭარბებლადშეიძლებაითქვას, რომძალზეშეიძლებაშეაფერხოსმათიშემდგომიგანვითარებადამოიტანოსდამანგრეველიშედეგები.

ამისდასტურადგამოდგებაკორპორაციაშყმენტეცმიერწარმოდგენილიანგარიში ორტონღეპორტ 2013, ძალზესაყურადღებოაSYMENTECტექნიკურიდირექტორისსტივენტრილინგის (STEPHEN TRILLING) ანგარიშშიმოყვანილიმონაცემებიდადასკვნები. ისმიუთითებს,

რომდღესკიბერდამნაშავეებიიყენებენსულუფროდადახვეწილმეთოდებსშე

ტევებისა, როგორებიცაა (პროგრამა-გამომძალველი) დაSPEARPHISHING (მიმართულიფიშინგი),
დასაშუალოზარალიყოველიცალკეაღებულიშეტევისაგანროგორცარასდროს მაღალია. ორტონღეპორტ გამოკვლევებისშედეგებიმიუთითებენიმაზე, რომმომხმარებლების 49% თავისიპერსონალურმობილურმოწყობილობებსიჯენებენერთდროულადრო გორცთამაშებისათვის, ასევესამუშაოსათვის, რაციწვევსწარმოსობასსრულიადახალიმუქარებისაკომპანიებისუსაფრთხოე ბისათვის,
ვინაიდანუკვეკიბერდამნაშავეებსშეუძლიათმიიღონდაშვებაკიდევუფროღი რებულინფორმაციასთან.

ანგარიშშიასევესაუბარიაიმისშესახებ, რომმიუხედავადიმისა, რომსმარტფონებისმომხმარებლებისთითქმისნახევრისათვისიმდენადმნიშვ ნელოვანიამათთვისესმოწყობილობა, რომმათმათთანერთადსძინავთ, მაგრამმომხმარებლებიარუზრუნველყოფენამმოწყობილობებისათვისსაიმე დოდაცვისდონეს.სმარტფონებისდაპლანსეტებისმომხმარებლების 48% არმიმართავენსიფრთხილისისეთბაზურზომებსაცკი, როგორიცააპაროლისდაყენება, ანტივირუსულიპუ-სდაყენებადამობილურმოწყობილობაშიარსებულიფაილებისსარეზერვიკოპ იოებისშექმნა.

ანგარიშშიმითითებულია, "ესრომყოფილიყოგამოცდაიმისა, რომმომხმარებლებიღებულობენზომებსთავისიპერსონალურიკომპიუტერებ ისდასაცავად,
მათარგააჩნიათგაგებასაკუთარისმარტფონებისდაპლანშეტებისდაცვისაუცი ლებლობისა. ესძალიანგავსიმშემთხვევას, როცაადამიანსსახლშიგააჩნიასაკმაოდსაიმედოდაცვისსიგნალიზაციისსისტ ემადაღიადტოვებსსანუთარიავტომობილისდაკარებსდაფანჯრებს."

ამთვალსაზრისითჭკუისსასწავლადშეიძლებამივიჩნიოთრუსეთშიარს ებულიმდგომარეობისშემდეგისტატისტიკურიმონაცემები:

- 85% რუსეთისმოქალაქეებისაწააწყდნენკიბერდანაშაულობებს;
- 59% სმარტფონებისმომხმარებლებისაბოლოწელსწააწყდნენმობილურკიბერდანა შაულობებს;
- 56% მობილურიმოწყობილობებისმომხმარებლებმარუსეთშიარიციანმათთვისსაჭ იროუსაფრთხოებისარსებულიგადაწყვეტებისშესახებ;
- 56% მომუშავემომხმარებლებისა (18 წელზეზევითასაკის) საკუთარმობილურმოწყობილობებსიყენებენროგორცგასართობად, ასევესამუშაოდ;
- 60% მომხმარებლებისა (18 წელზეზევითასაკის) იყენებენსაზოგადოანჭი- იდაუცველ – ქსელებს.

აქვეუნდააღვნიშნოთ, რომანგარიში Norton Report – ესაამსოფლიოშიერთ-ერთიუდიდესიგამოკვლევაკიბერდანაშაულობებისასამომხმარებლოსეგმენ ტში.

ისსერიოზულობასადამასშტაბურობაზემიუთითებსთუნდაცისფაქტიც, რომგამოკვლევებშიმონაწილეობამიიღო 13 ათასზემეტმაადამიანმა 24 ქვეყნიდან, დამისიმიზანია – გაგებაიმისა, თუროგორიაგავლენაკიბერდანაშაულობების, ასევეახალიტექნოლოგიებისგანვითარებისდადანერგვისამომხმარებლებზე დამისუსაფრთხოებაზე. მოზრდილთა (NR=13 022) საერთოშერჩევისცდომილებამსანდოობის 95% ალბათობითშეადგინა 0,9%, გამოკითხულიქნაათას-ათასირესპოდენტიაშშ-სადაინდოეთში, დანარჩენქვეყნებში – ხუთას-ხუთასირესპოდენტი.

ცხ.1.-შიმოგვყავსანგარიშშიNorton Reportმოცემულიძირითადიმონაცემები, ცალკეგამოვყოფთპოსტსაბჭოთასივრცის, იტ-ისდანერგვა-განვითარებისთვალსაზრისითროგორცგანვითარებადიქვეყნის, რუსეთისსტატისტიკურმონაცემებს.

ცხრილშიმოყვანილიმსოფლიომონაცემებიარისსაშუალოდაწონილი, რათაუზრუნველყოფილიიყოსყველასახელმწიფოსათვისრეპრეზენტაციულ იამონარჩევი – ნ500 მომხმარებლები.

ცხ.1.-შიმოყვანილმონაცემებს, უდიდესიმნიშვნელობააქვსნებისმიერიმასშტაბისადაკატეგორიისორგანიზაციისიუ-სუზრუნველყოფისათვის, ისსაშუალებასიზლევაგამოიყოსისმუქარები, რომლებიცდაკავშირებულიაორგანიზაციისთანამშრომლებისგავითცნობიერებულობაზეთანამედროვეიტ-სგამოყენებისასმოსალოდნელმუქარებზე, აგრეთვეორგანიზაციისუნარზეუზრუნველყონთანამშრომელთამართვა, მოტივაცია, ისე, რომმაქსიმალურადთავიდანიქნასაცილებულიორგანიზაციისიუ-სშესაძლომუქარები.

ცხრილი.1.

| Norton Report 2013 | | |
|---|---|---|
| | რუსეთში | მსოფლიოში (24 |
| კიბერდანაშაულობათა შემთხვევები | | |
| 18 წ.-ზე მეტი ხნის მომხმარებლები, რომლებიცოდესმე წაწყდო-მიან კიბერდანაშაულობებს | 85% | 61% |
| 18 წ.-ზე მეტი ხნის მომხმარებლები, რომლებიც წაწყდომიან კიბ-ერდანაშაულობებს ბოლო 12 თვის განმავლობაში | 61% | 41% |
| 18 წ.-ზე მეტი ხნის მომხმარებლები, რომლებიც გახდნენ კიბერ-დანაშაულობათა მსხვერპლი ან წინდაუხედავი ქცევისა | 74% | 50% |
| კიბერდანაშაულობათა მსხვერპლის რაოდენობა 12 თვის განმავ-ლობაში | 17მილ. | 178მილ |
| ჭილი მამაკაცებისა, რომლებიც ოდესმე გამხდარან კიბერდანაშა-ულობათა მსხვერპლი | 88% | 64% |
| 18-34 წლის ადამიანების წილი, რომლებიც ოდესმე გამხდარან კიბერდანაშაულებათა მსხვერპლი | 85% | 66% |
| კიბერდანაშაულობები აყენებენ დიდ ზარალს | | |
| საერთო ზარალი კიბერდანაშაულობებისაგან ბოლო 12 თვის განმავლობაში | $1მილიარდი | $113მილიარდი |
| საერთო ზარალი კიბერდანაშაულობებისა ერთ მსხვერპლზე გა-დაანგარიშებით ბოლო 12 თვის | $87 | $298 |

| | | |
|---|---|---|
| განმავლობაში | | |

| მობილური კიბერდანაშაულობები მომხმარებლებს აგდებენ მოულოდნელობაში | | |
|---|---|---|
| სმარტფონების მომხმარებლები, რომლებიც იყენებენ უფასო ბა-ზურ ინფორმაციული უსაფრთხოების (იუ) გადაწყვეტებს | 40% | 33% |
| პლანშეტების მომხმარებლები, რომლებიც იყენებენ უფასო ბა-ზურ იუ-ს გადაწყვეტებს | 52% | 42% |
| 18 წ.-ზე მეტი ხნის მომხმარებლები, რომლებიც კარგავდნენ მო-ბილურ მოწყობილობებს ან ხდებოდნენ მათი მოპერვის მსხვერ-პლი | 39% | 27% |
| ობილური მოწყობილობების მომხმარებლები, რომლებსაც წარ-მოდგენა არა აქვთ მობილური ინფორმაციული უსაფრთხოების გადაწყვეტების არსებობაზე | 56% | 57% |

# 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“.

ხაზი უნდა გაესვას იმას, რომ ტერმინი „electronic government“ (e-government) ხშიად ითარგმნება როგორც „ელექტრონული ხელოსუფლება“. ასეთი თარგმანი ავიწროვებს (ზღუდავს) და საკითხი დაყავს მხოლოდ სახელმწიფოს მართვაზე, რომელიც ხორციელდება აღმასრულებელი ხელისუფლების ორგანოების მიერ. მაგრამ ტერმინი გულისხმობს მხარდაჭერას ხელისუფლების სამივე შტოსი – საკანონმდებლოსი, აღმასრულებელი და სასამართლოსი, საინფორმაციო და საკომუნიკაციო ტექნოლოგიების დახმარებით. მეცნიერულ ნაშრომებში განიხილება სხვადასხვა მიდგომა ტერმინების „„ელექტრონული ხელოსუფლება“ და „ელექტრონული სახელმწიფო“ განმარტებისადმი და ხაზგასმულია, რომ უფრო სწორია გამოყენებულ იქნას ტერმინი „ელექტრონული სახელმწიფო“, ამავდროულად ბევრი წყარო უშვებს ამ ტერინების გამოყენებას როგორც სინონიმებისა. იმის გათვალისწინებით, რომ ოფიციალურ დოკუმენტებში ფართოდ გამოიყენება ტერმინი „ელექტრონული ხელისუფლება“, ჩვენც გამოვიყენებთ სწორედ ამ ტერმინს.

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.

ელ. ხელისუფლების იუ–ს მართვა წარმოადგენს სუსტად სტრუქტურირებულ ამოცანას: მართვის ობიექტი წარმოადგენს რთულ სოციოტექნიკურ სისტემას, რომელიც შედგება ავტონომიური კომპონენტებისაგან, თითოეული მათგანი მოქმედებს მიზანდასახულად. სისტემაში მიმდინარეობს – ხდება მრავალრიცხოვანი პროცესები

(სოციალური, პოლიტიკური, ტექნოლოგიური), რომლებიც მნიშვნელოვნად ურთიერთმოქმედებენ ერთმანეთთან. ეს პროცესები იცვლაბიან დროში, მათში მონაწილეობს სხვადასხვა სახის განუსაზღვრელობა, მაგრამ რაოდენობრივი ინფორმაცია პროცესების დინამიკის შესახებ რჩება ხელმიუწვდომელი. გარე გარემო, რომელიც გარემომცველია ელექტრონული ხელისუფლებისა წარმოადგენს პოტენციურად „მტრულ“ გარემოს. როგორც თვით ელ ხელისუფლების ელემენტები, ასევე გარე გარემო წარმოადგენენ მრავალრიცხოვანი მუქარების წყაროებს, რომლებიც მიმართული არიან ელ.ხელისუფლების იუ–ს დარღვევაზე.

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

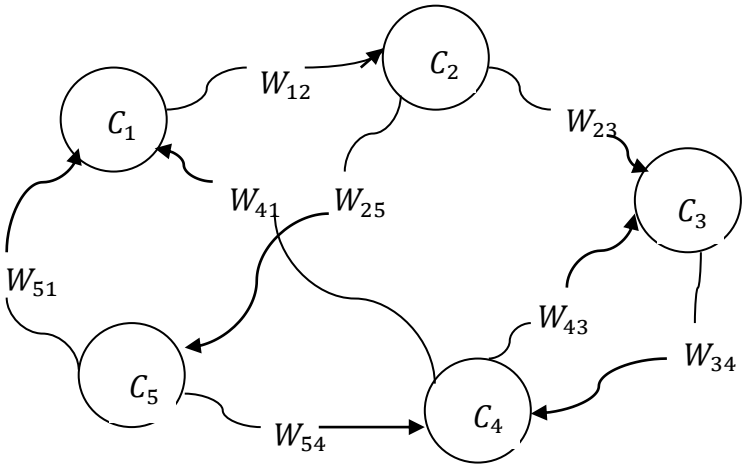
პროცესში ცხოველში ფორმირდება რაღაც „კოგნიტიური რუკა“, ან „აზრობრივი გეგმა“, ლაბირინთის ყველა მახასიათებლებისა, რომლის სრულყოფაც ხდება ყოველი შემდგომი ურთიერთმოქმედებებისას გარემოსთან.

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 წარმოადგინონ 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 (ნახ. 1.)




ნახაზი 4.არამკაფიო კოგნიტიური რუკის მაგალითი

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 $C_i$ ფაქტორის მნიშვნელობის შემცირებას მივყავართ $C_j$ ფაქტორის მნიშვნელობის გაზრდამდე.

ბოლო ათწლეული განმავლობაშიშეინიშნება გაზრდილი ინტერესი მკვლევარებისა მრავალ სფეროში არამკაფიო კოგნიტიური მოდელების აგების მიმართულებით. აკრ მეთოდოლოგია წარმატებით იქნა გამოყენებული ცოდნის წარმოდგენაში, პოლიტიკურ, სოციალურ და სოციალურ–ეკონომიკურ გამოკვლევებში, სტრატეგიულ დაგეგმვაში და სტრატეგიული გადაწყვეტილებების მიღებაში არამკაფიო სიტუაციებში

ბიზნეს–ანალიტიკაში, ეკონომიკურ პროგნოზირებაში, სადისპეტჩერო კონტროლის სისტემებში, ინფორმაციული ტექნოლოგიების პროექტების მართვაში, პროგრამული უზრუნველყოფების ხარისხის რისკების შეფასებისას, გადაწყვეტილებათა მიღების სისტემებში სამედიცინო ინფორმატიკაში, ეკოლოგიაში, მონაცემების ინტელექტუალურ ანალიზში და ა.შ. უნდა აღინიშნოს, რომ არის ნაშრომი [27], სადაც კოგნიტიური მოდელი გამოყენებულია ორგანიზაციის იუ–ს მდგომარეობის მოდელირებისა და ანალიზისათვის.

ელ. ხელისუფლების იუ–ს მართვის კოგნიტიური მოდელირებისათვის აუცილებელია:

– განისაზღვროს ფაქტორები, რომლებიც გავლენას ახდენენ იუ მდგომარეობაზე;

– აიგოს ფაქტორების ურთიერთ გავლენის მატრიცა;

– აიგოს იუ–ს მართვის კოგნიტიური მოდელი;

– დამუშავებულ მოდელზე გამომუშავდეს ელ. ხელისუფლების იუ–ს მართვის შესაძლო სტრატეგიები.

## 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.

იმ ფაქტორების გამოსავლენად, რომლებიც გავლენას ახდენენ ელ. ხელისუფლების იუ–ზე, გაანალიზებულ იქნა მთელი რიგი ქვეყნების ნაციონალური სტრატეგიები კიბერუსაფრთხოებაში, ასევე მოდელური სტრატეგიები ორგანიზაციების. ამ სტრატეგიების დამუშავება ხდებოდა იუ–ს ექსპერტების უშუალო ჩართულობა–მონაწილეობით და შეიძლება ისინი განხილულ იქნას როგორც კარგი წყაროები ექსპერტების ცოდნის აკუმულირებისა. კიბერუსაფრთხოების სტრატეგიების ანალიზისას გამოყენებულ იქნა რიგი ფაქტორებისა, რომლებიც გავლენას ახდენენ ელ. ხელისუფლების იუ–ს მართვაზე, და მათი სრული სია წარმოდგენილია ცხ.1.–ში.

ცხრილი 2.

| ფაქტორები | ფაქტორის სახელწოდება | აღნიშვნა |
|---|---|---|
| $C_1$ | სამართლებრივი ზომები | Legal |
| $C_2$ | ორგანიზაციული ზომები | Org |
| $C_3$ | ტექნიკური ზომები | Tech |
| $C_4$ | პოტენციელის განვითარებს | HR |
| $C_5$ | დაინტერესებული მხარეების თანამშრომლობა | Coop |
| $C_6$ | იუ–ს მუქარების განვითარება | |
| $C_7$ | ელ. ხელისუფლების იუ–ს დონე | NewT<br>Isee |

განვიხილოთ ამ ფაქტორების მოკლე დახასიათება (აღწერები).

1.<u>სამართებლივი ზომები</u> – იუ უზრუნველსაყოფად უნდა ჩამოყალიბდეს ადექვატური ნორმატიულ–სამართებლივი ბაზა. ნორმატიულ–სამართებლივ ბაზას განეკუთვნებიან დაგეგმვა და დამუშავება მექანიზმებისა საჭირო პოლიტიკების და რეგულირებისა, ზუსტი განსაზღვრა როლების, უფლებების და ვალდებულებებისა დაინტერესებული მხარეების, ბაზური ღონისზიებები და ინსტრუქციები მოქმედებებისა იუ უზრუნველყოფისა და ა.შ. გათვალისწინებულია ასევედამუშავება დარღვევებზე რეაგირების ძირითადი მექანიზმებისა დანაშაულებების გამოძიებისა და სამართლებრივი დევნის მეშვეობით და სანქციების დაწესებით კანონის დაუცველობის ან დარღვევაზე.

ნორმატიულ–სამართლებრივი ზომები შეიძლება შემუშავებულ იქნას არსებული სამართლებრივი ინსტიტუტების და სტრუქტურების ბაზაზე, რომლებიც დაკავებულები არიან კიბერუსაფრთხოებით და კიბერდანაშაულებებით. ეს ჯგუფი შედგება შემდეგი მაჩვენებლებისაგან.

$C_{11}$.სისხლის სამართლის კანონმდებლობა – კიბერდანაშაულებათა გაფრთხილებისათვის და დასაკავშირებლად საერთაშორისო ბრძოლასთან კიბერდანაშაულებათა წინააღმდეგ აუცილებელია განვითარება შესაბამისი სამართლებრივი ბაზისა. კანონმდებლობა კიბერდანაშაულობებისა შეიძლება შეფასებულ იქნას შემდეგი დონეების მიხედვით: არ არსებობს; დამუშავებულია ნაწილობრივ; არის ამომწურავი.

$C_{12}$. რეგულირება და შესატყვისობა სტანდარტების მოთხოვნებთან – იუ–ს რეგულირება აღნიშნავს კანონებს, რომლებიც ეხება დაცვას მონაცემების, შეტყობინებების დარღვევაზე და მოთხოვნები სერტიფიკაციის/სტანდარტიზაციის. კანონები ასევე შეიძლება კლასიფიცირებულ იქნას დონეების მიხედვით: არ არსებობს; დამუშავებულია ნაწილობრივ; არის ამომწურავი.

<u>2.ორგანიზაციული ზომები</u> – კიბერუსაფრთხოების სტრატეგიებში გათვალისწინებულია აგება მართვის მოქნილი ორგანიზაციული სტრუქტურისა, რომელიც მიმართულია იუ–ს უზრუნველყოფაზე. ეფექტური ორგანიზაციული სტრუქტურების შესაქმნელად აუცილებელია იუ–ს წინწაწევისათვის, კიბერდანაშაულებათა წინააღმდეგ საბრძოლველად და მონიტორინგის, გაფრთხილებების და რეაგირებების როლის ასამაღლებლად ინციდენტებზე უწყებათაშორისი, კროს–სექტორული და ტრანსსასაზღვრო კოორდინაციის უზრუნველსაყოფად ახალ და არსებულ ინციატივებისათვის. ორგანიზაციული ზომები შეიძლება შეფასებულ იქნას არსებული დაწესებულებების რიცხვის და სტრუქტურების საფუძველზე, რომლებიც ორგანიზებას უკეთებენ იუ განვითარებას ეროვნულ დონეზე. ქვეჯგუფი შედგება შემდეგი მაჩვენებლებისაგან:

$C_{21}$. 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. კიბერშეტევების გამონლენისათვის ადექვატური ზომების და პოტენციალის გარეშე ელ. ხელისუფლება და მისი სუბიექტები რჩებიან მოწყვლადებად კიბერმუქარებისათვის. ამიტომ ელ. ხელისუფლებას უნდა შეეძლოს განავითაროს სტრატეგიები დადგენილების უსაფრთხოების მინიმალური კრიტერიუმების და აკრედიტაციის სქემების მიხედვით პროგრამული უზრუნველყოფებისა და ინფორმაციული სისტემებისათვის.

$C_{31}$. ადრეული გაფრთხილების სისტემა – ხდება გათვალისწინება ინციდენტებისადმი მზადყოფნის ამაღლების, რეაგირების დროის შემცირების, დამუშავება აღდგენის გეგმისა კრიტიკული ინფორმაციული ინფრასტრუქტურისა ავარიების შემდეგ და დაცვის მექანიზმების (მაგალითად, ეროვნული გეგმა მოქმედებებისა განსაკუთრებულ პირობებში, კიბერსივრცეში მოქმედებების წესები, სიტუაციებზე ინფორმირება).

$C_{32}$. 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). გაგებას ტექნოლოგიების, რისკებისა შეუძლია სერიოზული დახმარება უფრო სრულყოფილი კანონმდებლობის, უფრო ეფექტური პოლიტიკების და სტრატეგიების დამუშავება–შექმნაში, ასევე უფრო უკეთესი ორგანიზაციისათვის ცალკეული როლებისა და პასუხისმგებლობებისა.

ქვეჯგუფი შედგება შემდეგი მაჩვენებლებისაგან:

$C_{41}$. კადრების მომზადება – მიუთითებს აუცილებლობაზე ახალი საგანმანათლებლო პროგრამებისა, რომლებიც ყურადღებას ამახვილებენ იტ–სპეციალისტების განათლებაზე და პროფესიონალებზე კიბერუსაფრთხოებაში. ზოგიერთ ნაციონალურ სტრატეგიებში კიბერუსაფრთხოებისა ისახავს მიზანს კიბერუსაფრთხოებაში სპეციალისტების საგანმანათლებლო პროგრამების სრულყოფისა, რათა საიმედოდ უზრუნველყოფილ იქნას კიბერუსაფრთხოება, ასევე იუ–ს სპეციალისტების სერტიფიკაციისა.

$C_{42}$. 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. მთელ რიგ სტრატეგიებში გათვალისწინებულია განსაზღვრა წამყვანი ცენტრებისა კიბერუსაფრთხოების სფეროში კვლევებისა და უზრუნველყოფა ინვესტიციებით.

$C_{44}$. 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.<u>დაინტერესებული მხარეების თანამშრომლობა</u>** – იუ–ს მართვისათვის აუცილებელია ყველა დაინტერესებული მხარის მონაწილეობა, ამიტომ სახელმწიფო სტრუქტურები და კერძო სექტორი უნდა მუშაობდნენ მჭიდრო თანამშრომლობით. საერთაშორისო თანამშრომლობა სასიცოცხლო მნიშვნელობისაა, ვინაიდან ყველანი დამოკიდებული არიან ერთ კიბერსივრცეზე. თანამშრომლობა უნდა ხორციელდებოდეს გაცვლით ინფორმაციის და მოწინავე გამოცდილებით, ცოდნით ცალკეულ დონეებზე.

ეროვნული და საერთაშორისო თანამშრომლობა შეიძლება შეფასებულ იქნას პარტნიორობის არსებონის რიცხვის, ინფორმაციის გაცვლის ერთობლივი სტრუქტურების და ქსელების საფუძველზე.

ქვეჯგუფი შედგება შემდეგი მაჩვენებლებისაგან:

$C_{51}$. 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,<u>იუ–ს მუქარების განვითარება</u>** – 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.

**7.<u>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.

## 1.3. ფაქტორების ურთიერთგავლენის მატრიცის აგება

აკრ–ის აგებისას ყველაზე უფრო რთულ ამოცანას წარმოადგენს ფაქტორების ურთიერთგავლენებისათვის წონების მიკუთვნება. სამეცნიერო ნაშრომებში მოცემულია ორი ალგორითმი ფატორების ურთიერთგავლენის მატრიცის გამოსათვლელად.

პირველ ალგორითმში ყოველი ექსპერტი აფასებს ურთიერთგავლენის წონებს როგორც რიცხვს ინტერვალიდან [–1.1]. შემდეგ ურთირთგავლენების წონების ეს მატრიცა აგრეგირდება როგორც გასაშუალებული მნიშვნელობა წონების ჯამისა ან გამოიყენება ზღურბლური ფუნქცია. იმდენად რამდენადაც ექსპერტების ცოდნა და გამოცდილება შეფასების ობიექტებისა შეიძლება იყოს სახვადასხვანაირი, ამიტომ ყოველ ექსპერტს შეიძლება მიენიჭოს ნდობის არაუარყოფითი რიცხვითი წონა. ექსპერტების ნდობის წონების გათვალისწინებით ინტეგრებული წონები ურთიერთ გავლენებისა შეიძლება გამოთვლილ იქნას შემდეგი ფორმულით (გათვალისწინება ხდება მხოლოდ ერთნაირი ნიშნის წონებისა):

$$W_{ij} = \frac{\sum_{k=1}^{m} b_k W_{ij}^k}{m} \quad (1)$$

სადაც$W_{ij}^k$ – არის შეფასება$C_i$ და $C_j$შორის ურთიერთგავლენის წონისა k–ური ექსპერტის მიერ; – $b_k$არის k–ური ექსპერტის ნდობის წონა; m– არის ექსპერტების რაოდენობა – რიცხვი. თუ ექსპერტის შეფასება განსხვავდება უმეტესობა ექსპერტების შეფასებებისაგან, მაშინ ხდება მისი დაჯარიმება –

მას ენიჭება ნდობის ძალზე დაბალი ან ნულოვანი წონა. უფრო დეტალურად ამ ალგორითმს შეიძლება გავეცნოთ ნაშრომში [20].

აკმ ფაქტორების ურთიერთგავლენის მატრიცის აგების მეორე ალგორითმი იყენებს არამკაფიო ლოგიკას. ექსპერტები აღწერენ ფაქტორებს შორის კაუზალურობას ლინგვისტური ცვლადების მეშვეობით. ყოველი ექსპერტი განსაზღვრავს ერთი ფაქტორის გავლენას მეორე ფაქტორზე როგორც „ნეგატიურს“ ან „პოზიტიურს“ და ამის შემდეგ აღწერს გავლენის ხარისხს შემდეგი ტიპის ლინგვისტური ცვლადების მეშვეობით: „ძლიერი“, „სუსტი“ და ა. შ. ამ მეთოდოლოგიის უპირატესობას წარმოადგენს ის, რომ ექსპერტებს არ სჭირდებათ კაუზალური კავშირებისათვის რიცხვითი წონების მინიჭება, ისინი აღწერენ კაუზალური კავშირის ხარისხს ფაქტორებს შორის მიჩვეული ტერმინებით.

ამ მეთოდოლოგიიის თანახმად, ერთი ფაქტორის გავლენა მეორეზე შეიძლება ინტერპრეტირებულ იქნას როგორც ლინგვისტური ცვლადი, რომელიც ღებულობს მნიშვნელობებს უნივერსალურ სიმრავლეში [–1, 1]. მისი თერმების სიმრავლე შეიძლება იყოს შემდეგი:

T(გავლენა) = {ნეგატიურად ძალიან ძლიერი, ნეგატიურად ძლიერი, ნეგატიურადსაშუალო, ნეგატიურად სუსტი, ნეგატიურად ნულოვანი, პოზიტიურად სუსტი, პოზიტიურად საშუალო, პოზიტიურად ძლიერი, პოზიტიურად ძალიან ძლიერი}.

ქვემოთ განსაზღვრულია სემანტიკური წესი, და ეს თერმები ხასიათდებიან არამკაფიო სიმრავლეებით, რომელთა მიკუთვნების ფუნქციები ნაჩვენებია ნახ.5.–ზე

– T(ნეგატიურად ძალიან ძლიერი) = არამკაფიო სიმრავლე „გავლენა – 75% ქვევით“–თვის მიკუთვნების ფუნქციით $\mu_{nvs}$;

– T(ნეგატიურად ძლიერი) = არამკაფიო სიმრავლე „გავლენა ახლოსაა – 75%–თან“–თვის მიკუთვნების ფუნქციით $\mu_{ns}$;

– T(ნეგატიურად საშუალო) = არამკაფიო სიმრავლე „გავლენა ახლოსაა – 50%–თან“–თვის მიკუთვნების ფუნქციით $\mu_{nm}$;

– T(ნეგატიურად სუსტი) = არამკაფიო სიმრავლე „გავლენა ახლოსაა – 25%–თან“–თვის მიკუთვნების ფუნქციით $\mu_{nw}$;

– T(ნეგატიურად ნულოვანი) = არამკაფიო სიმრავლე „გავლენა ახლოსაა – 0–თან“–თვის მიკუთვნების ფუნქციით $\mu_z$;

– T(პოზიტიურად სუსტი) = არამკაფიო სიმრავლე „გავლენა ახლოსაა – 25%–თან“–თვის მიკუთვნების ფუნქციით $\mu_{pw}$;

– T(პოზიტიურად საშუალო) = არამკაფიო სიმრავლე „გავლენა ახლოსაა – 50%–თან“–თვის მიკუთვნების ფუნქციით $\mu_{pm}$;

– T(პოზიტიურად ძლიერი) = არამკაფიო სიმრავლე „გავლენა ახლოსაა – 75%–თან“–თვის მიკუთვნების ფუნქციით $\mu_{ps}$;

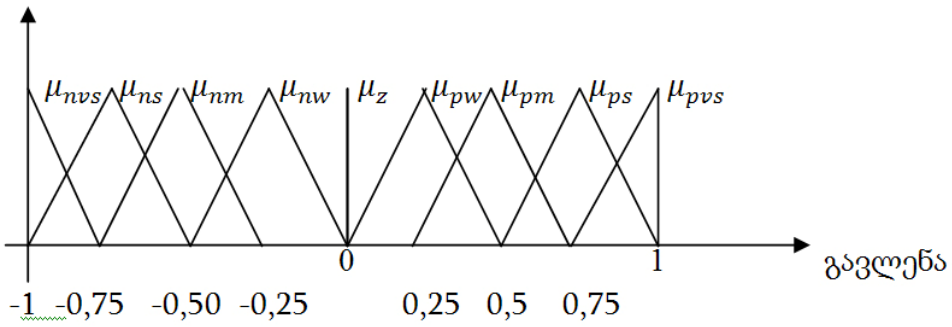
– T(პოზიტიურად ძალიან ძლიერი) = არამკაფიო სიმრავლე „გავლენა მეტია – 75%–“–თვის მიკუთვნების ფუნქციით $\mu_{pvs}$;

ლინგვისტური ცვლადები, რომლებიც აღწერენ ფაქტორების ყველა ურთიერთმოქმედებებს, აგრეგირდებიან, და საერთო ლინგვისტური ცვლადი გარდაისახება ინტერვალში [–1. 1] დეფაზიფიკაციის მეშვეობით. აქ გამოვიყენებთ სიმძიმის ცენტრის მეთოდს დეფაზიფიკაციისათვის.

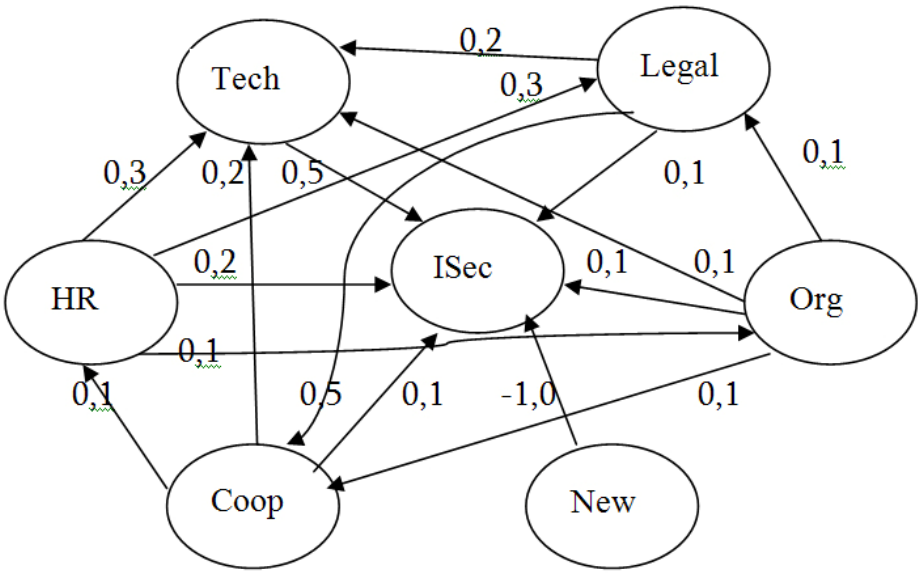
აკმ–ებს გააჩნიათ ის ძირითადი ნაკლოვანებები, რომლებიც დამახასიათებელია სხვა არამკაფიო სისტემებისათვის: მათ არ შეუძლიათ სწავლება დამოუკიდებლად. შესაბამისი მონაცემების ხელმისაწვდომობის შემთხვევაში ფაქტორების ურთიერთგავლენების წონები შეიძლება გაუმჯობესებულ იქნას, ნეირონული ქსელების სწავლების მექანიზმების გამოყენებით. უმეტესობა ასეთი მიდგომებისა დაფუძნებულია ჰების სწავლების მეთოდიკაზე [38, 39], მაგრამ არსებობს სხვა მეთოდებიც, რომლებშიც გამოყენებულია ევოლუციური გამოთვლების მეთოდები [40].

აკმ–ის მოდელში ელ. ხელისუფლების სტრატეგიული მართვისათვის ფაქტორების ურთიერთგავლენის მატრიცის გამოსათვლელად მოწვეულ იქნა ხუთი ექსპერტი იუ–ს მართვაში. ექსპერტებმა შეაფასეს ფაქტორების ერთმანეთზე ზეგავლენა ზემოთ განსაზღვრული ლინგვისტური

ცვლადებისა, და მიღებული შედეგი აგრეგაციისა და დეფაკიფიკაციის შემდეგ მოცემულია ნახ.5.–ზე




ნახაზი5. ლინგვისტური ცვლადის „გავლენა“ თერმებზე




ნახაზი 6. „ელ. ხელისუფლების“ იუ–ს მართვის აკმ მოდელი გრაფის სახით

## 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:

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

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 [41]. 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) [10].

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.

განვიხილოთ იუ მართვის შემდეგი სცენარები:

**სცენარი**A: სისტემის თვით განვითარება

A(0) = (1.0, 1.0, 1.0, 1.0, 1.0, 1.0, 0.0).

**სცენარი**B: გამოყენება მხოლოდ ტექნიკური ზომების

A(0) = (0.0, 0.0, 1.0, 0.0, 0.0, 0.0, 0.0).

**სცენარი**C: ძლიერი აქტივაცია ფაქტორისა, იუ მუქარების განვითარება

A(0) = (0.0, 0.0, 0.0, 0.0, 0.0, 1.0, 0.0).

**სცენარიD:** ძლიერი აქტივაცია ფაქტორისა, „განვითარება პოტენციალის“ და „განვითარება იუ–ს მუქარების“ A(0) = (0.0, 0.0, 0.0, 1.0, 0.0, 1.0, 0.0).

გამოთვლით ექსპერიმენტში გამოყენებული იყო სიგმოიდური ფუნქცია პარამეტრით $\lambda$=1. როგორც წესი, გამოთვლები ფორმულით (2) იკრიბებოდნენ მოდელირების ხუთი დროითი ბიჯზე ნაკლებ დროში. ყველა მოდელი დასრულდა სტაბილურ მდგომარეობაში, მაგრამ თეორიულად ისინი შეიძლება გადასულიყვნენ ასევე ზღვრულ ციკლში ან ქაოსურ ატრაქტორში [6]. ფაქტორების შუალედური მნიშვნელობები A სცენარით გამოთვლისას მოცემულია ცხ.3.–ში.

როგორც ჩანს ცხ.3–დან,შენარჩუნება ფაქტორების არსებული ტენდენციებისა მიგვიყვანს იუ დონის გაუარესებასთან.

ცხ.3.–ის მიხედვითშეიძლება გაკეთდეს დასკვნა, რომ მხოლოდ ტაქნიკური ზომების გამოყენება არ იძლევა იუ მდგომარეობის არსებითი გაუმჯობესების საშუალებას (სხვაობა A და B სცენარების სტაბილურ მდგომარეობებს შორის შეადგენს 0,0424).

ცხ.4. აჩვენებს, რომ ფაქტორის „იუ მუქარების განვითარება“ აქტივაციისას იუ მდგომარეობა უარესდება მნიშვნელოვნად, ასევე

შეიძლება აღინიშნოს ფაქტორის „ტექნიკური ზომები“ საწყისი მდგომარეობის გაუარესება.

ცხ.5. აჩვენებს, რომ იუ–ს მუქარების განვითარებისას ვერ ხერხდება უზრუნველყოფილ იქნას იუ–ს მისაღები დონე მხოლოდ პოტენციალის გაზრდით; შესაბამისი პოტენციალის გაზრდასთან ერთად საჭიროა მოიძებნოს ოპტიმალური თანაფარდობა ინფორმაციულ უსაფრთხოებაში სამართლებრივი, ტექნიკური, ორგანიზაციული ზომებისა ყველა დაინტერესებული მხარეების ეფექტური თანამშრომლობისას.

აკმ–თვის სტაბილური მდგომარეობის გამოთვლა სცენარი (A)

ცხრილი.3.

| იტერაციის ფაქტორები | Legal | Org | Tech | HR | Coop | NewT | ISec |
|---|---|---|---|---|---|---|---|
| O | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 |
| 1 | 0,5498 | 0,5250 | 0,6457 | 0,5987 | 0,5498 | 0,5000 | 0,5987 |
| 2 | 0,5281 | 0,5150 | 0,5871 | 0,5619 | 0.5292 | 0,5000 | 0,5721 |
| 3 | 0,5269 | 0,5140 | 0,5821 | 0,5570 | 0,5275 | 0,5000 | 0,5633 |
| 4 | 0,5268 | 0,5139 | 0,5816 | 0,5566 | 0,5274 | 0,5000 | 0,5624 |
| 5 | 0,5267 | 0,5139 | 0,5816 | 0,5566 | 0,5274 | 0,5000 | 0,5624 |
| 6 | 0,5267 | 0,5139 | 0,5816 | 0,5566 | 0,5274 | 0,5000 | 0,5624 |

B სცენარის მიხედვით გამოთვლების საბოლოო შედეგები

ცხრილი.4.

| ფაქტორები | B სცენარის – საწყისი მნიშვნელობები | სცენარი B – საბო–ლოო მნიშვნელობები | A და B სცენარების სტაბილურ მდგო-მარეობებს შორის სხვაობა |
|---|---|---|---|
| სამართლებრივი ზომები | 0,00 | 0,5275 | 0.0008 |
| ორგანიზაციული ზომები | 0,00 | 0,5147 | 0.0008 |
| ტექნიკური ზომები | 1,0 | 1,00 | 0,4184 |
| პოტენციალის გან–ვითარება | 0,00 | 0,5875 | 0,0309 |
| დაიტერესებული მხარეების თანამშრომლობა | 0,00 | .0,5378 | 0,0104 |

| | | | |
|---|---|---|---|
| იუ მუქარების განვი–თარება | 0,00 | 0,5000 | 0 |
| იუ დონე | 0,00 | 0,0048 | 0,0424 |

C სცენარის მიხედვით გამოთვლების საბოლოო შედეგები

ცხრილი.5.

| ფაქტორები | C სცენარის – საწყისი მნიშვნელობები | სცენარი C – საბო–ლოო მნიშვნელობები | A და C სცენარების სტაბილურ მდგომა–რეობებს შორის სხვაობა |
|---|---|---|---|
| სამართლებრივი ზო–მები | 0,00 | 0,5267 | 0.00 |
| ორგანიზაციული ზომები | 0,00 | 0,5139 | 0.00 |
| ტექნიკური ზომები | 0,00 | 0,5569 | -0,0247 |
| პოტენციალის გან–ვითარება | 0,00 | 0,5547 | -0,0019 |
| დაიტერესებული მხარეების თანამშრომლობა | 0,00 | 0,5267 | -0,0007 |
| იუ მუქარების განვი–თარება | 1,00 | 1,0 | 0,5 |
| იუ დონე | 0,00 | 0,4076 | -0,0648 |

D სცენარის მიხედვით გამოთვლების საბოლოო შედეგები

ცხრილი 6.

| ფაქტორები | D სცენარის – საწყისი მნიშვნელობები | სცენარი D – საბო–ლოო მნიშვნელობები | A და D სცენარების სტაბილურ მდგომა–რეობებს შორის სხვაობა |
|---|---|---|---|
| სამართლებრივი ზო–მები | 0,00 | 0,5381 | 0.0114 |
| ორგანიზაციული ზომები | 0,00 | 0,5250 | 0.0111 |
| ტექნიკური ზომები | 0,00 | 0,5904 | 0,0088 |
| პოტენციალის გან–ვითარება | 0,00 | 1,0000 | 0,4434 |
| დაიტერესებული | 0,00 | .0,5279 | 0,0005 |

| | | | |
|---|---|---|---|
| მხარეების თანამშრომლობა | | | |
| იუ მუქარების განვი–თარება | 1,00 | 1,00 | 0,5 |
| იუ დონე | 0,00 | 0,5238 | -0,0386 |

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

თანამედროვე ინფორმაციული სისტემები, როგორც წესი, შეიცავენ დიდ რაოდენობას უსაფრთხოების მართვის ერთმანეთთან დაკავშირებულ მოწყობილობებს და საშუალებებს, რომლებიც აფორმირებენ უზარმაზარი რაოდენობის ინფორმაციას და ინფორმაციის შემთხვევებს. ეს ინფორმაცია

უნდა იქნას დამუშავებული იმ მიზნით, რომ გამოკვლეული იქნას დაცვაში შესაძლო მოწყვლადობები – სუსტი ადგილები, მოხდეს იდენტიფიკაცია კომპიუტერული შეტევებისა და მიღებულ-გატარებულ იქნას კონტრზომები.

მოცემული ინფორმაციის ხელით დამუშავება არაეფექტურია მთელი რიგი მიზეზებით: დამუშავების შეზღუდული დრო, რის გამოც შეიძლება ვერ მოესწროს კომპიუტერული შეტევებისათვის წინააღმდეგობის გაწევა. დამოკიდებულება ექსპერტის ცოდნაზე, რომელმაც შეიძლება ხელიდან გაუშვას მნიშვნელოვანი შეტყობინება ან არ დააკავშიროს ერთმანეთთან შემთხვევები, რომლებიც მიუთითებენ შეტევაზე; შესაძლებლობა სისტემისათვის კიდევ უფრო მეტი ზიანის მიყენების – არაეფექტური კონტრზომების გამოყენებით ან არასწორი შეფასებით შეტევის დამანგრევლობის და მასზე არა დროული რეაგირებით სისტემის მოწყობილობებსა და სერვისებს შორის რთული ურთიერთკავშირების გამო.

უსაფრთხოების ინფორმაციის და შემთხვევების მართვის სისტემები (SECUITY INFORMATION AND EVETS MANAGEMENT-SIEM) იქმნებიან ამ პრობლემების გადასაწყვეტად და მოხდეს უსაფრთხოების ინფორმაციის და შემთხვევების პროცესების დამუშავება. SIEM – სისტემების ფუნქციები მოიცავენ ჩანაწერების მოგროვებას შემთხვევების შესახებ სხვადასხვას წყაროებიდან, მათ ნორმალიზაციას, აგრეგაციას, ანალიზურ დამუშავებას და ანგარიშების შედგენას.

კომპიუტერულ შეტევებზე რეაგირების ეფექტურობის ასამაღლებლად შემოთავაზებულია დამატება SIEM–სისტემაში დაცულობის ანალიზისა შეტევათა და სერვისების დამოკიდებულების გრაფების საფუძველზე. აღნიშნული კომპონენტი საშუალებას იძლევა უსაფრთხოების ინფორმაციის და შემთხვევების ანალიზის შედეგად გაკეთდეს დასკვნები სისტემის დაცულობის დონეზე და არჩეულ იქნას ყველაზე უფრო ეფექტური ნაკრები კონტრზომებისა სისტემის დაცულობის საერთო დონის

ასამაღლებლად, ასევე რეაგირებისათვის ცალკეულ შეტევებზე, რომლებიც სრულდება რეალურ დროში.

აღნიშნული მიდგომის დამუშავებისას გათვალისწინებულ იქნა SIEM –სისტემის არქიტექტურა და თავისებურებები კომპიუტერულ ქსელზე შეტევების მოდელირებისას შეტევების გრაფების სახით.

შემოთავაზებული მიდგომის ძირითად თავისებურებებს წარმოადგენენ შეტევების და სერვისების დამოკიდებულებების გრაფების გამოყენება; გამოყენება შემოთავაზებულ მოდელში კონტრზომებისა, რომლებიც ბაზირებული არიან სტანდარტებზე “დაცვითი ზომების საერთო ჩამონათვალი” () და “გაფართოებული ინფორმაცია გაფართოებულ დაცვით ზომებზე” (); გამოყენება შემოთავაზებული მაჩვენებლებისა ეფექტურობის, ღირებულების და კონტრზომების თანმდევი ზარალის, ასევე შესაძლებლობა გადაწყვეტების შემოთავაზებისა კონტრზომების შერჩევისა დროის ნებისმიერ მომენტში გამოკიდებულებით მიმდინარე ინფორმაციაზე დაცულობის მდგომარეობაზე და უსაფრთხოების შემთხვევებზე ფუნქციონირების სტატიკურ და დინამიურ რეჟიმებში. აღნიშნული მიდგომა საშუალებას იძლევა ამაღლდეს ინფორმაციული სისტემების დაცულობა დასაბუთებული დაცვის ზომების შერჩევის ავტომატიზაციით.

რელევანტური შრომები.დაცვის ზომების შერჩევის ავტომატიზებას ბევრი სამეცნიერო ნაშრომია მიძღვნილი. მთელ რიგ ნაშრომებში რისკის დონის შეფასების ასპექტი შეტევათა გრაფების და სერვისების დამოკიდებულებების გრაფების საფუძველზე [6-8]. ზოგიერთი ავტორი იყენებს ეკონომიკურ ინდექსს შესაძლო დანაკარგების და კონტრზომების ეფექტურობის შესაფასებლად [10,11]. ასე, მაგალითად, ნაშრომში [11] კონტრზომების შეფასება ხდება სამი პარამეტრით, რომელთა საფუძველზეც განისაზღვრება საერთო მოგება k–ური კონტრზომის გამოყენებისას:

$\text{Net\_Benefit}_k = \text{Benefit}_k - \text{Added\_}Cost_k + \text{Added\_}Profit_k$, $\forall k$={1,2,3,….l},

სადაცL – კონტრზომებისრაოდენობაა;ENEFT–(k )-კონტრზომისგატარებითმიღებულიმოგება; DDED–〖COST〗–k-დანახარჯებიkკონტრზომაზე; DDED–〖 ROFIT〗–k-დამატებითისარგებელიk–კონტრზომისგატარებითმიღებული.

ნაშრომში[7] შემოთავაზებულიაშეტევებზერეაგირებისკონტრზომებისშერჩევისმაჩვენებელისერვისებისდამოკიდებულებებისგრაფისსაფუძველზე – რეაგირებაშიჩადებულიინვესტიციისდაბრუნებისმაჩვენებელი (RRETURN-N-RETURN-N-RESPONSE-INVESTMENT-RORI):

$$\text{RORI} = \frac{RG-(CD+OC)}{CD+OC},$$

სადაცR – რეაგირებისეფექტურობაა; C - გვერდითიდანაკარგებირეაგირებისას; C - დანახარჯებიკონტრზომებზე.

ნაშრომში [12] წარმოდგენილიამოდიფიცირებულიმაჩვენებელიRORI, რომელიცითვალისწინებსვარიანტსკონტრზომებისარარსებობისა, ასევესისტემისინფრასტრუქტურისზომას:

$$\text{RORI} = \frac{(ALE\times RM)- ARC}{ARC+AIV} \times 100$$

სადაცR – მოსალოდნელიწლიურიდანაკარგები (შეესაბამებანეგატიურიშემთხვევისშედეგს, კონტრზომისარარსებობისშემთხვევაში), რომლებიცდამოკიდებულიარიანშეტევებისკრიტკულობასადარეალიზაციისალბათობაზე; R - რისკისდაწევისდონეკონტრზომისრეალიზებისას; RC - მოსალოდნელიწლიურიდანახარჯებიკონტრზომებზე; IV - წლიურიდანახარჯებიინფრასტრუქტურაზე (მოწყობილობა, მხარდაჭერა) დაცვითიზომებისრეალიზაციისშემთხვევაში.

ამასთანერთად, აუცილებელია, გათვალისწინებულიქნასსაერთაშორისოდასახელმწიფოსტანდარტებიკონტრზომებისშერჩევისსფეროში.

ჩვენორიენტირებულივართგამოკვლევებზეუსაფრთხოებისინფორმაციისდაშემთხვევებისმართვისსისტემებზე.

ამსფეროშიარსებობსსერიოზულისამეცნიერონაშრომები [7, 12]. ჩვენსმიზანსწარმოადგენსგანვითარებაარსებულიმიდგომებისამაჩვენებლებისგაფართოებულინაკრებისგამოყენებითდამრავალდონიანიმიდგომით, რომელშიცგამოყენებულია, მათშორის, ოჯახისტანდარტებისა, რომლებიცგამოიყენებიანპროტოკოლშიSC[13].

3) მიდგომისაღწერა

ა) კონტრზომისმოდელი

რამდენადაცმოცემულგამოკვლევებშიგამოიყენებასტანდარტიპროტოკოლისSC დაცულობისშეფასებისავტომატიზებისათვის, განვიხილოთშესაბამისისტანდარტებიკონტრზომებისაღწერისა: სტანდარტებიSR [4] და RI [5]. თუმცასტანდარტებიჯერკიდევიმყოფებიანდამუშავებისპროცესშიდაარააფორმირებულიმონაცემთასრულიბაზა, რომლებიციყენებენმითითებულსტანდარტებს, ისინიხელსაყრელიაკონტრზომებისმოდელებისშესაქმნელად.

სტანდარტიCRწარმოადგენსსქემასკონტრზომებისგანსაზღვტისდააღწერისაფორმატში X[4]. ხოლოსტანდარტი RIშეიცავსდამატებითინფორმაციასCR –თვის [5].

ჩვენსმიერშემოთავაზებულიაკონტრზომებისმოდელში (ნახ.1.) ჩართულიიქნას:

CR სტანდარტისველები: ელემენტისტექსტურიაღწერა (კონტრზომისმეთოდიდამოქმედება), პლათფორმასენისCR PPLICABILITY ANGUAGE 2.3 გამოყენებით, რომლისთვისაცგამოყენებადიამოცემულიკონტრზომა.

RIსტანდარტისველები: ინდიკატორები (მითითებებიCC –ზე [14] ანCV –ზე [15]); გავლენამუშაობაზე – უარყოფითიგავლენააქტივებისუსაფრთხოებისთვისებებზე,

რომელიცგამოისახებამაჩვენებლითგვერდითიზრალისდონე(CollateralDamage - CD)სამგანზომილებიანივექტორისსახით( 〖CD〗_c 〖CD〗_i 〖CD〗_a), სადაც 〖CD〗_(c,) 〖C〗_i 〖,CD〗_a – შესაბამისადზარალიათვისებებისათვისკონფიდენციალობის/მთლიანობისუ რღვევობის/ხელმისაწვდომობისაკონტრზომებისრეალიზაციისშედეგად; ესპარამეტრებიღებულობენმნიშვნელობას 0-დან 1-მდე;

დამატებითიველები: კონტრღონისძიებისსახელწოდება; შეტევათაგრაფზეგავლენისტიპი (ველიღებულობსმნიშვნელობებს{REMOVE[CVE1-CVE2], ADD[CVE1-CVE2], MODIFY[CVE1-CVE2]});

მაჩვენებლები: კონტრზომისეფექტურობა (ჩოუნტერმეასურე ფფეცტივენესს - C ) – უსაფრთხოებისთვისებისშეცვლისხარისხისამგანზომილებიანივექტორისსა ხით [〖C 〗–c〖C 〗–I〖C 〗–A], სადაც 〖C 〗–(c,) 〖C 〗–I, 〖C 〗–A – შესაბამისადეფექტურობისმნიშვნელობებიათვისებებისმიმართულებებისკო ნფიდენციალობის/მთლიანობისურღვევობის/ხელმისაწვდომობისშეცვლისა კონტრზომებისშესრულებისშედეგად; ესპარამეტრებიღებულობენმნიშვნელობებს 0-დან 1-მდე; კონტრღონისძიებისღირებულება(Countermeasure Cost - CC) – კონტრღონისძიებისრეალიზებისღონისძიება, იზომებაფულადერტეულებში.

სადემონსტრაციომაგალითადგანვიხილოთკონტრზომებისშემდეგივა რიანტები: პატჩი (მარშუტი) მოწყვლადობისათვის (ინფორმაციისაღებაშეიძლება, მაგალითად, ბაზიდანXORC [16, 17], რომელიცშეიცავსდროითშეფასებებსCVSSმათშორისგამოსწორებისდონის, რომელიცგანსაზღვრავსპატჩისარსებობასმოწყვლადობისათვის); მოშორებამოწყვლადიპროგრამულიუზრუნველყოფისა; პორტისდაკეტვა; დამატებადამატებითიდაცვითისაშუალებების (მაგალითად, ფაირვოლისანანტივირუსის).

ცხრილი 7. კონტრზომებისმოდელი

| სახელწოდება | აღწერა | CCE ან CVE | პლათფორმა | გავლენა შეტევათა გრაფზე | გავლენა მუშაობაზე | ეფექტურობა | ღირებულება |
|---|---|---|---|---|---|---|---|

ველების მნიშვნელობების მაგალითები

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| მოთხოვნების აკრძალვა ან გადამისამართება | urlმოთხოვნების აკრძალვაანგადამისამართებასაეჭვო სააღრიცხვო ჩანაწერებისაგან | CVE-2010-1870 | cpe:/a:apache:struts:2.0.0 | კავშირის მოშორება | CD ==[000.5] | CE==[0.50.50.5] | 500€ |

ა) კონტრზომებისმოდელისდაშეტევებისგრაფისკავშირი

გადაწყვეტილებათამიღებისმეთოდიკასსაფუძვლადუდევსშეტევების გრაფი. შეტევათაგრაფიწარმოადგენსმდგომარეობათაგადასვლისგრაფს, რომელშიცყოველიკვანძიშეესაბამებამოწყვლადობისწარმატებულ/წარუმატებელექსპლუატაციას, ხოლორკალი – შესაძლებლობასგადასვლისაერთიშემტევიმდგომარეობისამეორეზე [19]. კონტრზომისრეალიზაციაგავლენასახდენსმდგომარეობებისგადასვლებზედა, შესაბამისად, ცვლისშეტევებუსგრაფს (კვანძებისმოშორებით/დამატებით) დაშეტევებისალბათობებს. ჩხადია, რომკონტრზომასშეუძლიაგავლენამოახდინოსყოველამელემენტზესამიხერხით: მოშორებით, დამატებით, შეცვლით (მაგალითად, შეტევისალბათობის) (ნახ.7.). წყვეტლიდაუწყვეტიისრებითგამოყოფილიაგზები, რომლებიცშეესაბამებიანგარკვეულკონტრზომებს, მაგალითად, პორტისგახსნაგანაპირობებსრკალისდამატებას, დაარაკვანძისა.

გ) მაჩვენებლებისტაქსონომიისგაფართოება

არსებულიმეცნიერულინაშრომებისთანახმად [3, 19] მაჩვენებლებისტაქსონომისსასაგებადგამოიყენებამაჩვენებლებისკომპლექსუ

რიიერარქიულისისტემა,

რომლებიცსაშუალებასიძლევიანსხვადასხვადონეებზე (ტოპოლოგიურ, შეტევეცისგრაფის, შემტევის, შემთხვევებისდასისტემის) დასხვადასხვაასპექტებისგათვალისწინებით (ძირითადიმაჩვენებლების, ნულოვანიდღისმაჩვენებლებიდაღირებულებითიმაჩვენებლების).

ისახოსმიმდინარედაცულობისა.

ტოპოლოგიურიდონისმაჩვენებლებიგანისაზღვრებაადმინისტრატორ ისმიერსისტემის (ქსელის) ტოპოლოგიისსაფუძველზე.

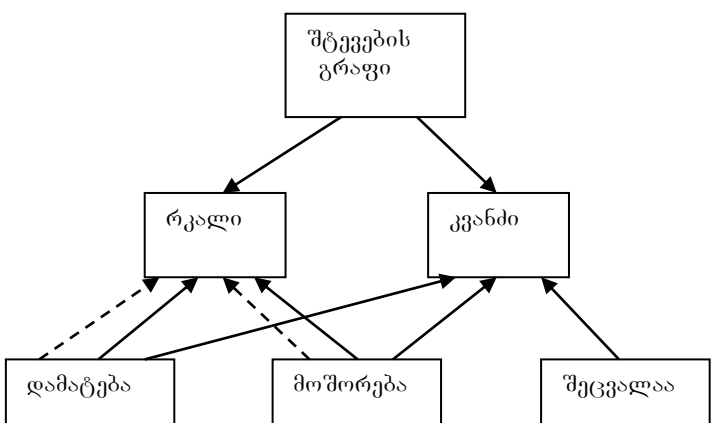
შეტევათაგრაფისდონრზედაცულობისდონისგამოსათვლელადგამოი ყენებაინფორმაცია, რომელიცმიღებულიაშეტევათაგრაფისსაფუძველზე.

ოცემულიდონესაშუალებასიძლევაგანისაზღვროსშეტევისალბათობადაშეს აძლოზარალიშეტევათაყველაგზებისგათვალისწინებით.

შეტევისდონეზეხდებაშემოტანაშეტევისდამოკიდებულებისაშემტევი სპროფილისაგან (ანუმისიმდგომერეობა (მდებარეობა) ქსელშიდაჩვევების). ესსაშუალებასიძლევაფორმირებულიქნასე.წ. შეტევათაპროფილურიგრაფი, რომელიცმოიცავსშეტევებს, რომელიცშეიძლებარეალიზებულიქნასმოცემულიშემტევისმიერ.

სისტემისდონეზეგანსაზღვრებასისტემისდაცულობისდონედასისტემ ისშეტევისზედაპირი.

ყოველიდონისძირითადიმაჩვენებლებიწარმოდგენილიანახ.3.-ზე, სადაცწყვეტილიისრებითაღნიშნულიაარააუცილებელიკავშირ



ნახაზი 7. დამოკიდებულებაკონტრზომებსადაშეტევათაგრაფის ობიექტებსშორის

ონტრზომებისგარკვეულიმოდელისშესაბამისადაუცილებელიადაცუ ლობისმაჩვენებლებისტაქსონომიისგაფართოებადამატებითიმაჩვენებლების შემოტანითკონტრზომისმოდელში: კონტრზომებისღირებულება, კონტრზომებისეფექტურობადაგვერდითიზარალისდონე

დ)

კავშირიგადაწყვეტილებისმიღებისადატაქსონომიისდანარჩენიდონეე ბისა

განვიხილოთკავშირიგადაწყვეტილებისმიღებისდონისასხვაოთხსონე ებთანმიმართებაში: ტოპოლოგიურის, შეტევებისგრაფის, შემტევისდაშემთხვევების.

ტოპოლოგიურიდონე.

ამმოცემულდონეზეარგანიხილებიანმრავალბიჯიანიშეტევები, რომლებიციყენებენმოწყვლადობებისსიმრავლეს. ღოგორცშედეგი,

არხდებაგათვალისწინებაკონტრზომებისგავლენისაშეტევებისგრაფზე. ამიტომგადაწყვეტილებისმიღებადაფუძნებულიარისკისდონისგამოყენებაზ ეცალკეულიაქტივებისათვის, რომელიცგანისაზღვრებაკონტექსტურიშეფასებისCVSS (0-დან 10-მდე) დახმარებით [18].

$$Risk = round\_to\_1\_dicimal\ (AdjustedBase),$$

სადაცAdjustedBase, რომელშიცBaseScore Impact შეცვლილია AdjustedImpact;

$$AdjustedBase = round\_to\_1\_dicimal\times$$

$$\times((0{,}6AdjustedImpact + 0{,}4Exploitability - 1{,}5 )\times$$

$$\times f(Adjustedimpact));$$

$$AdjustedImpact =$$

$$= \min(10;10{,}41\times(1 - (1 - ConfImpact\times ConfReq)\times$$

$$\times(1 - IntegImpact\times IntegReq)\times$$

$$\times(1 - AvailImpact\times AvailReq)))$$

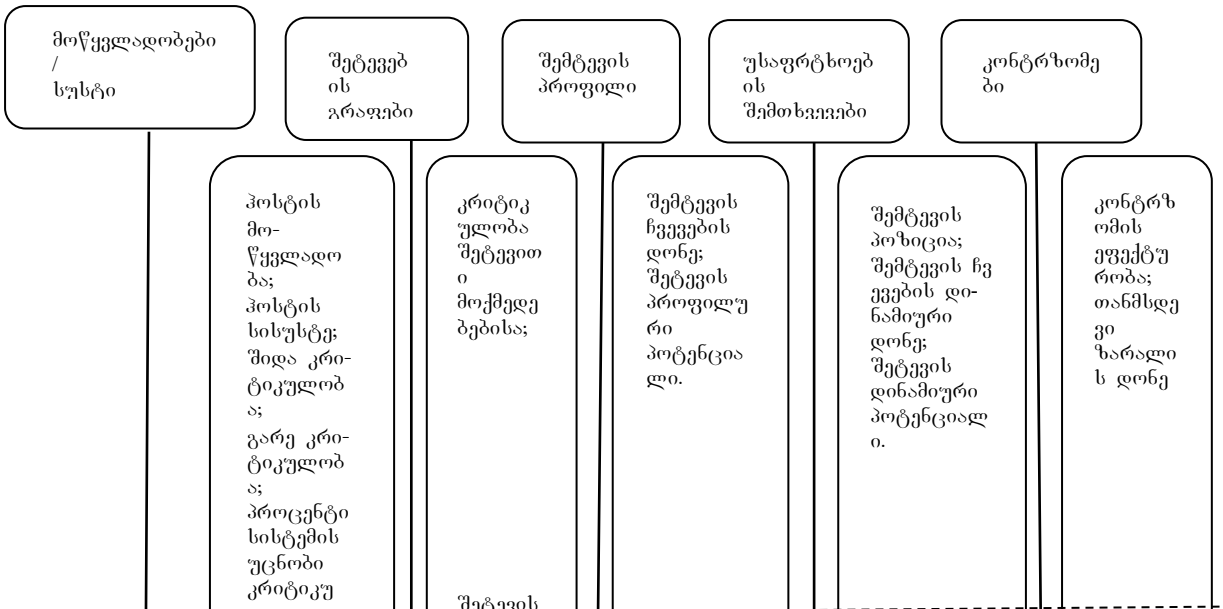
სადაცConfImpact,IntegImpact,AvailImpact – გავლენაკონფიდენციალობაზე, მთლიანობაზე და ხელმისაწვდომობაზე; ConfReq,IntegReq,AvailReq - მოთხოვნები უსაფრთხოებისა, რომლებიც მოცემიულ კონტექსქტექსტში განიხილებიან როგორც აქტივების კრიტიკულობა, ამიტომ

$$AdjustedImpact =$$

$$= \min(10;\ 10{,}41\times(1 - (1 - ConfImpact\times$$

$$\times Criticality(c))(1 - IntegImpact\times Criticality(i)\times$$

$$\times(1 - AvailImpact\times Criticality(a))))$$



0-დღე

ღირებულ
ებითი

ნახაზი8. დაცულობის მაჩვენებლების გაფართოებული ტაქსონომია

სადაცCriticality(c), Criticality(i) და Criticality(a) – კრიტიკულობაკონფიდენციალობის მთლიანობის და ხელმისაწვდომობის. შესაძლო მნიშვნელობები კრიტიკულობის მაჩვენებლებია[0; 1,51];

$$Exploitability = 20 \times AccessVector \times$$

$$\times AccessComplexity \times Authentication,$$

სადაცAccessVector – დაშვების ვექტორია; AccessComplexity - დაშვების სირთულე; Authentication - აუტენტიფიკაცია;

f(AdjustedImpact) =

$$= \begin{cases} 0, & \text{თუ Authentication} = 0 \\ 1{,}176 & \text{თუ Authentication} \neq 0 \end{cases}$$

კონტრზომებისშერჩევისმეთოდიკამოცემულდონეზერეალიზდებარა მოდენიმეეტაპში.

გამოვლენააქტივებისარისკისმიუღებელიდონით, ანუ "მაღალი" კონტექსტური (ENVIROMENTAL) CVSS – შეფასებითCVSSსისტემისთანახმად (7,0-დან 10,0-მდე).

განსაზღვრადროითი (TEMPORAL) CVSS – შეფასებისაიმისთაობაზე, შემცირდებათუარარისკიპატჩისრეალიზაციით. შეფასებაგანისაზღვრებაCVSSდროითიგანტოლებისსაფუძველზე, რომელიციყენებსმხოლოდერთდამატებითმაჩვენებელს – გასწორებისდონე (REMEDIATION EVEL), რომელიცგანსაზღვრავსპატჩისარსებობასმოწყვლადობისათვის [18].

TemporalScore = round_to_1_decimal (aseScore × RemediationLevel), სადაცფუნქციაround_to_1_decimal ასრულებსარგუმენტისდამრგვალებასერთნიშნამდემძიმისშემდეგ. დროითიCVSS – შეფასებასაქვსმნიშვნელობა 0-დან 10-მდე. თუთურისკისდონეაქტივისათვისრჩება 7,0-ზედაბალი, მაშინსისტემაიძლევარეკომენდაციასგამოყენებულიქნასპატჩებიშესაბამისიმ ოწყვლადობებისათვის.

აქტივებისათვისრისკისმაღალიდონისშეფასებითგანისაზღვრებაოთხ იასპექტი:

რისკიდარღვევისაკონფიდებციალობის/მთლიანობის/ხელმისაწვდომობისდ აპრივილეგიებისმირებისაარალეგიტიმურიმომხმარებლისმიერ(CVSS - მონაცემებისმიხედვითმოწყვლადობისა,

რომელიცგანსაზღვრავსრისკისშეფასებას).

ამისათვისგამოიყენებამაჩვენებლებიround_to_1_decimal დაConfReq, IntegReq, AvailReq შემდეგნაირად: კონტრზომისრეალიზაციააუცილებელიაუსაფრთხოებისშესაბამისითვისებე ბისუზრუნველსაყოფად, თუჩონფIმპაცტ, IntegImpactან vailImpact≥0,275(ანუზარალიარსებობს), დათუმოთხოვნებიამთვისებებისათვისConfReq, IntegReq, AvailReq >1,0 (ანუკრიტიკულობამაღალია).

აუცილებელიაგადარჩევაყველამოწყვლადობებისარისკების "მაღალი" შეფასებით, რომლებიცგანეკუთვნებიანმოცემულაქტივს. იმშემთხვევაშითუმოწყვლადობასაშუალებასიძლევაპრივილეგიისმირებისა, აუცილებელიაკონტრზომისმირება.

იმისგანდამოკიდებულებით, თუუსაფრთხოებისრაასპექტებიშეიძლებაიქნასდარღვეული, აირჩევიანკონტრზომებიუსაფრთხოებისშესაბამისითვისებებისუზრუნველს აყოფად (მაგალითად, დამატებითიაუტენტიფიკაციაკონფიდენციალობისდარღვევისრისკისშემთხ ვევაში)

კონტრზომისმოდელშიესჩადებულიაეფექტურობისმაჩვენებლებისშეფასება ში[〖CE〗_c 〖CE〗_i 〖CE〗_a]:თუ〖CE〗_c 0, მაშინშესაბამისიკონტრზომაშეიძლებაგამოყენებულიქნასკონფიდენციალობ ისდარღვევისწინააღმდეგ; თუ〖CE〗_i 0 – მაშინმთლიანობისდარღვევისწინააღმდეგ, თუ〖CE〗_a 0 – მაშინხელმისაწვდომობისდარღვევისწინააღმდეგ.

კონტრზომისასარჩევადგამოიყენებაშემდეგიმიდგომა. ინტუიციურადგასაგებია, რომაუცილებელიაგაიზარდოსმოგებადაცვითიზომებისრეალიზაციისაგანდ ანახარჯებისშემცირებისას. მოგებაგანისაზღვრებათანაფარდობითრისკისა, დამცავიზომებისრეალიზაციამდე,

რისკთანდამცავიზომებისრეალიზაციისშემდეგ.

ღაცუფრომცირეიქნებარისკიდამცავიზომებისრეალიზაციისშემდეგ, მითუფროდიდიიქნებამოცემულისიდიდე. ანახარჯები, რომლებიცნორმალიზებულიაკრიტიკულობისსკალისმიხედვით, თავსდებამნიშვნელში. ამრიგად, დანახარჯებისგაზრდითმოცემულიმაჩვენებელიმცირდება, დაპირიქით, მაჩვენებელიგადაწყვეტილებისმიღებისინდექსი (Countermeasure Index-CI), რომელიცგამოიყენებადამცავიზომებისშესარჩევად, განისაზღვრებაშემდეგიგამოსახულებით:

$$\text{Ci} = \frac{R_b}{R_a \times CC},$$

სადაც $R_b$– რისკია, როცა დაცვითი ზომები არაა რეალიზებული, Ra - რისკია იმ შემთხვევაში, თუ დაცვითი ზომები რეალიზებულია.

დონე შეტევების გრაფის, დონე შემტევის და დონე შემთხვევების შეტევების გრაფის დონეზე განიხილებიან შეტევათა გრაფის კვანძები რისკების დონით, რომლებიც აღემატებიან დასაშვებს. ასეთი კვანძებისათვის განიხილებიან შესაძლებლობა დაცვითი ზომების განხორციელებისა ნახ.8.-ზე მოცემული კლასიფიკაციის მიხედვით. მოცემულ დონეზე გამოიყენება მეთოდებირისკის დონის გაანგარისებისა, შეტევათა გრაფისათვის განსაზღვრული [3, 19, 20]. შემტევის დონეზე დამატებით ხდება დამრღვევის შესაძლებლობების გათვალისწინება.

შემთხვევების დონეზე კონტრზომების რეალიზაცია ხდება დამრღვევის მიმდინარე და მომავალ ნაბიჯებზე (პროგნოზირებულების) დამოკიდებულებით. ამ დროს ხდება გათვალისწინება გრაფის სიღრმე კრიტიკულ რესურსამდე“, რომელიც განისაზღვრება როგორც რაოდენობა გრაფის კვანძებისა აქტივამდე კრიტიკულობის მაღალი დონით. თუ მოცემული სიღრმე აღემატება გარკვეულ მნიშვნელობას, მაშინ სისტემა ელოდება ახალ შემთხვევას თავისი შეფასებების დასაზუსტებლად; თუ სიღრმე ნაკლებია გარკვეულ მნიშვნელობაზე, სისტემა გვთავაზობს კონტრზომას არსებული მონაცემების საფუძველზე სიზუსტის ხარისხით,

რომელიც შეესაბამება უკვე გამოვლენილი რელევანტური შემთხვევების რაოდენობას.

case study აღწერა

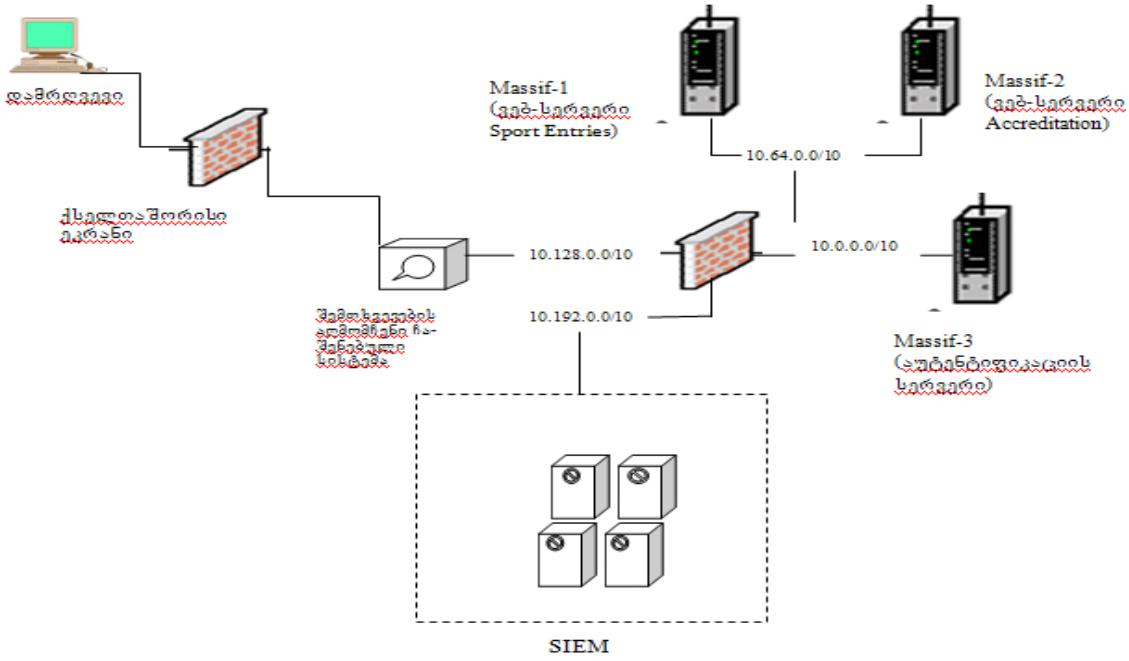
ტესტური ქსელის და შესაძლო კონტრზომების აღწერა

ტესტური ქსელის ფრაგმენტი წარმოდგენილია ნახ.9.-ზე

pu აღწერა

| ჰოსტი | პროგრამული უზრუნველყოფა |
|---|---|
| ვებ-სერვერი Accreditation (Massif-2) | Widows Server 2008 R2 (64 bits); Jboss AS 5.0.1; Snare agent;<br>ApacheStruts2 framework |
| ვებ-სერვერი Sport Entries (Massif-1) | Widows Server 2008 R2 (64 bits); Jboss AS 5.0.1; Snare agent;<br>ApacheStruts2 framework<br>(cpe:/a:apache:struts:2.0.0) |
| აუტენტიფიკაციის სერვერ Authentication (Massif-3) | SUSE Enterprise Linux 11 SP1 (32bits)<br>(cpe:/o:novell:suse_linux:<br>11:sp1:server)<br>NetIQ eDirect server 8.8.7.1<br>(cpe:/a:netiq:edirectory:8.8.7.1) |

ცხრილში [1] აღწერილიატესტურიქსელისპროგრამულიმუზრუნვე4ლყოფა. ტესტურიქსელისსერვისებისსტრუქტურაგანვსაზღვროთშემდეგნაირად: აუტენტიფიკაციისათვისგამოიყენება ETI EIRECT, დაშვებამონაცემებთანeDirect ხორციელდებაპროტოკოლით, რომელიცინკაფსულირებულიაSS –ში (პორტი 363) ვებ-დანართებიCCREDITATIONდაSPORT NTRIESაამოქმედებენPACHESTRUTS2 FRAMEWORK (იყენებსპორტს 8080 ვებ-გვერდებთანდასაშვებად, რომელსაცმხარსუჭერსJboss AS (იყენებსპორტს 443).



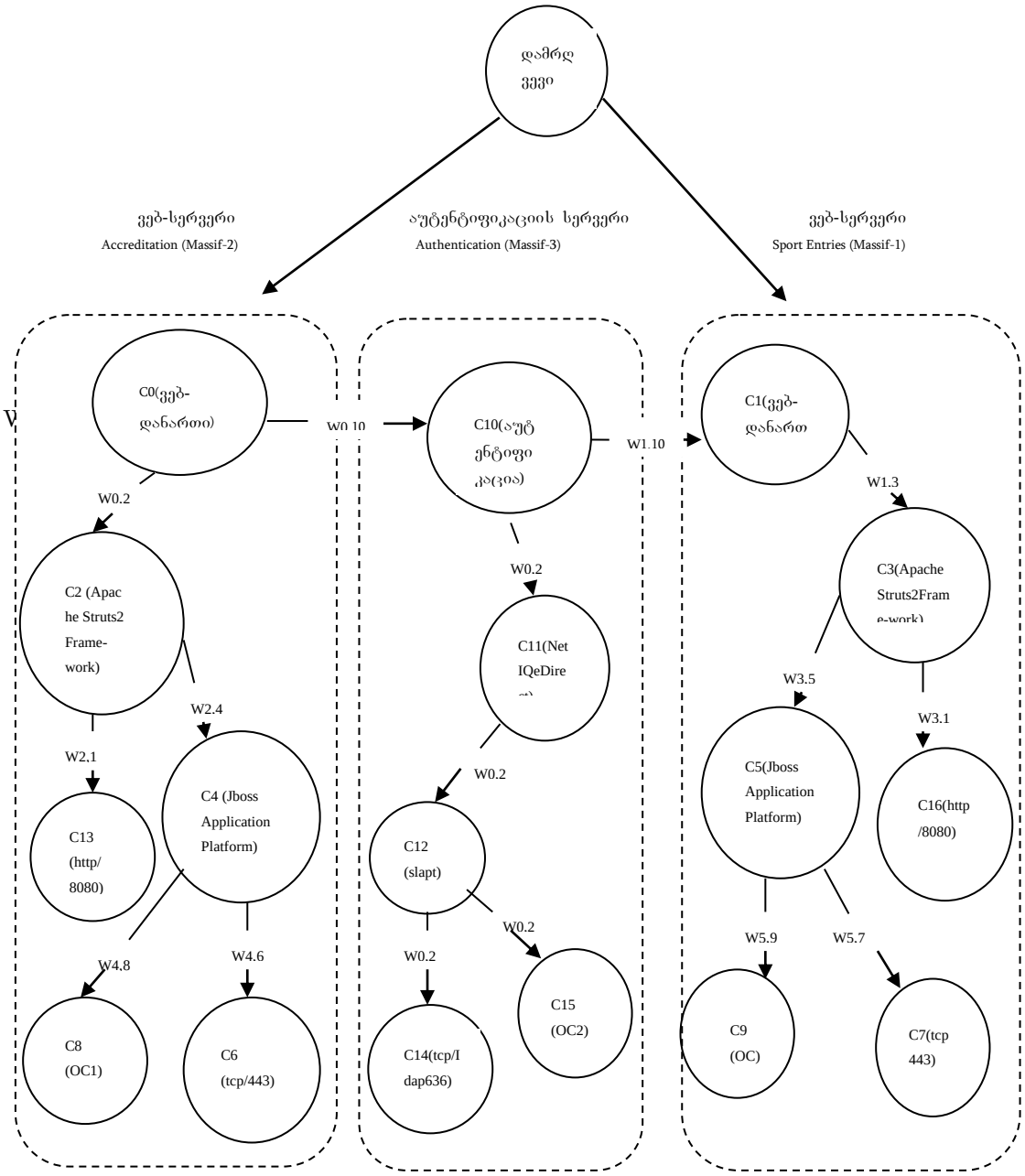

ნახაზი.9. ტესტურიქსელისფრაგმენტისსქემა

სერვისებისდამოკიდებულებებისგრაფი.

სერვისებისდამოკიდებულებებისგრაფი (ნახ.10.) აგებულიამეთოდიკით, რომელიცშემოთავაზებულისნაშრომში [7]: დამოკიდებულებაგანისაზღვრებასერვისებისდაშვებადობის, მთლიანობისდაკონფიდენციალობისაუცილებლობითსხვასერვისისხელმის აწვდომობის, მთლიანობისდაკონფიდენციალობისუზრუნველსაყოფად. სერვისებისშემოთავაზებახდებასისტემისჰოსტებისსხვადასხვადანართებით ანქსელურიმოწყობილობებით.მაჩვენებლებისგამოსათვლელადაუცილებელ იამოცემულიქნასდამოკიდებულებებისწონითიმატრიცები (მოიცემიანექსპერტებისმიერ).

ნაპოვნი იქნას რისკის დონე კონტრზომის გატარებამდე და გატარების შემდეგ. გამოთვლების გასამარტივებლად ავირჩიოთ ტოპოლოგიური დონე.

ტოპოლოგიურ დონეზე ვებ-სერვერზე Massif-2 შეტევის რისკი კონტრზომების დანერგვამდე განისაზღვრება შემდეგნაირად. თავიდან გამოვთვალოთ აქტივების კრიტიკულობა (მოცემულ შემთხვევაში, ესაა




ნახაზი10. სერვისების დამოკიდებულებები

ინფორმაცია ვებ-სერვისებზე): Ctiticality(c) = 0,8, Ctiticality(i) = 0,8 da Ctiticality(a) = 0,8.

შემდეგ უნდა შეფასდეს რისკი კონტრზომის დანერგვამდე ტოპოლოგიური დონის ფორმულის შესაბამისად, რომელიც განსაზღვრულია ზემოთ. მაგალითად, კვანძისათვის Massif-2 ის იქნება განსაზღვრული მაქსიმალური CVSS - შეფასებით მოწყვლადობებისა

ჰოსტის – მოწყვლადობით ApacheStruts2 Framework CVE-2013-4316 (10,0 H; AV:L/AC:L/Au:N/C:C/I:C/A:C).

უნდა აღვნიშნოთ, რომ თუმცა თვით სერვისი ApacheStruts2 Framework არაა აღნიშნული როგორც კრიტიკული სისტემისათვის, მით უმეტეს შენარჩუნება მისი უსაფრთხოების თვისებებისა აუცილებელია ვებ-დანართის უსაფრთხოების თვისებების შენარჩუნებისათვის წონითი კოეფიციენტების შესაბამისად:

$$W_{0,2} = \begin{bmatrix} 0,7 & 0,7 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

კრიტიკულობაApacheStruts2 Frameworkგანისაზღვრება როგორცCtiticality(c) = 0,56, Ctiticality(i) = 0,8 და Ctiticality(a) = 0,8.

მოწყვლადობა წარმოდგენილია იდენტიფიკატორით CVE [15] მეშვეობით, ბაზური შეფასებისCVSS სკალით 1-დან 10-მდე დაშესაბამისი ხარისხობრივი მნივშნელობით (H-მაღალი, M-საშუალო, L-დაბალიშეფასებამოწყვლადობისკრიტიკულობისა), დაბაზურივექტორებისCVSS:

AV[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C],

სადაც AV – დაშვებისვექტორიამოწყვლადობასთან (L-ლოკალური, A-მოსაზღვრე (მომიჯნავე) ქსელი, N-მოშორებული); AC - მოწყვლადობასთანდაშვებისსირთულე (H-მაღალი, M-საშუალო, L-დაბალი); AU - მაჩვენებელიიმისა, საჭიროათუარადამატებითიაუტენტიფიკაცია (M-საჭიროააუტენტიფიკაციისრამოდენიმეპროცედურისგავლა, შ-საჭიროააუტენტიფიკაციისერთიპროცედურისგავლა, N-არარისსაჭირო); C, I და A - ზარალი, მიყენებულიკონფიდენციალობის, მთლიანობისდახელმისაწვდომობისამოწყვლადობისწარმატებულიექსპლუატაციისასშესაბამისად ( -არა, -ნაწილობრივი, C-სრული) [15].

რამდენადაცზარალიარისსრული, ამიტომშეფასებითისისტემისCVSSშესაბამისადConfImpact(C), IntegImpact(I) და vailImpact(A)გააჩნიათმნიშვნელობები 0,660. მაშინ

$$\text{AdjustedImpact} =$$

$$= \min(10;10{,}41\times(1-(1-0{,}660\times0{,}56)\times$$

$$\times(1-0{,}660\times0{,}8)\times(1-0{,}660\times0{,}8))) = 8.948$$

დაშვებისვექტორიგანისაზღვრებაროგორცლოკალური, რაცშეფასებისსისტემისთანახმადშეესაბამებამნიშვნელობას 1,0; დაშვებისსირთულეგანისაზღვრებაროგორცდაბალი, რაცშეესაბამებამნიშვნელობას 0,71; აუტენტიფიკაციაარაასაჭირო, რაცშეესაბამებამნიშვნელობას 0,704. ამრიგად:

$$\text{Exploittability} = 20\times1{,}0\times\text{o},71\times\text{p},704 = 9{,}9968,$$

$$\text{f(AdjustedImpact)} = 1{,}1176;$$

$$\text{AdjustedBase} =$$

$$= \text{round\_to\_1\_dicimal}(((0{,}6\times8{,}948) +$$

$$+ (0{,}4\times9{,}9968) - 1{,}5)\times1{,}176) = 9{,}3;$$

$$\text{Risk} = \text{AdjustedBase} = 9{,}8.$$

განვსაზღვროთრისკიკონტრზომებისდანერგვისშემდეგ. მაგალითისათვისავიღოთკონტრზომა 1 “ბლოკირებასაეჭვოსაღრიცხვოჩანაწერებისა” (რომლისშემთხვევაშიცეფექტურობა[C]−C1= 0,75 დაღირებულება 〖CC〗 −1 = 0,0001) დაკონტრზომა 2 “მრავალფაქტორიანიაუტენყიფიკაციისაქტივაცია” ( 〖CE〗_c2 = 0,85 და 〖CC〗 −2 = 0,0001):

$\text{AdjustedImpact}_1 = 8{,}948,$

$\text{AdjustedImpact}_2 = 8{,}948;$

$\text{Exploitability}_1 =$

$$= 20\times1{,}0\times0{,}71\times0{,}704\times0{,}75 = 7{,}4976,$$

$\text{Exploitability}_2 = 8{,}4973;$

$$f(AdjustedImpact_1) = 1{,}176,$$

$$f(AdjustedImpact_2) = 1{,}176;$$

$AdjustedBase_1$ =

$$= round\_to\_1\_dicimal(((0{,}6\times 8{,}948) +$$

$$+ (0{,}4\times 7{,}4976) - 1{,}5)\times 1{,}176) = 8{,}1,$$

$AdjustedBase_2$ =

$$= round\_to\_1\_dicimal(((0{,}6\times 8{,}948) +$$

$$+ (0{,}4\times 8{,}4973) - 1{,}5)\times 1{,}176) = 8{,}5;$$

$Risk_1 = AdjustedBase_1 = 8{,}1,$

$Risk_2 = AdjustedBase_2 = 8{,}5$

შესაბამისად, კონტრზომების შერჩევის კოეფიციენტები

$CI_1 = \frac{R_b}{R_{a1}\times CC_1} = \frac{9{,}3}{8{,}1\times 0{,}0001} = 11\ 481{,}5;$

$CI_2 = \frac{9{,}3}{8{,}5\times 0{,}0001} = 10\ 941{,}2.$

მაქსიმალურიკოეფიციენტიგამოიყენებადამცავიზომებისშესარჩევად. მრიგად, შერჩეულიქნებაკონტრზომა "საეჭვოსააღრიცხვოჩანაწერებისბლოკირება."

ექსპერიმენტებმადაადასტურეს, რომყოველახალდონეზედამატებითიინფორმაციისმესვეობითშესაძლებელი აარჩეულიქნასუფროეფექტურიდაცვითიზომები (ნაკლებიღირებულებისდასასუალებასიძლევამინიმიზებულიქნასზარალი).

მიუხედავადამისაგადაწყვეტილებისმიღებისინდექსსგააჩნიარიგიშეზღუდვებისა, ასემაგალითად, ისგამოუყენებადიდამცავიზომებისნულოვანიღირებულებისასდანულოვანი რისკისშემთხვევაშიდამცავიზომებისდანერგვისშემდეგ.

## 2.1. განაწილებული ქსელი დაცვის ქვეშ

თანამედროვეინფორმაციულისისტემებიდიდიუმეტესობაგანაწილებულიხასიათისაადაშეუძლიათფუნქციონირებამხოლოდმაღალიწარმადობის

მონაცემთაგადაცემისკორპორატიულიქსელისარსებობისას, რომლისგარეშეცძნელიწარმოსადგენიამუშაობაკომერციულიკომპანიებისდა სახელმწიფოორგანიზაციებისა.

Zk Research გამოკვლევებისმონაცემებით, საწარმოებისთანამშრომლების 75%-ზემეტიმუშაობსსათაოოფისისგარეთ – ფილიალებისტერიტორიაზე.

ველამათგანსჭირდებადაშვებაკორპორატიულდანართებთანდამონაცემებთან, მათშორისისეთკრიტიკულადმნისვნელოვანსისტემებთან, როგორიცაა racle E-Busieness Suite, NetSuite, Sage ERP Microsoft Dynamics. რცისეიშვიათადისინიმუშაობენღრუბლოვანდანართებთან – მაგალითად, Salesforce.com, Google Apps da Microsoft Office 365.

საწარმოსყველაოფისებისდაქვედანაყოფების, რომლებიცგამლაგებულიარიანცენტრალურიოფისიდან (შტაბ-ბინიდან) საკმაოდმოსორებულად, გაერთიანებაერთიანსისტემაშიკორპორატიულიქსელიასაშუალებასიძლევაპერსონალსშესთავაზოსშესაძლებლობებიაეთდროულადმუშაობისაგანაწილებულანცენტრალიზებულდანართებთან, მონაცემთაბაზებთანდასხვასერვისებთან.

ამდროსტერიტორიულადგანაწილებულმაქსელებმაუნდაუზრუნველყონუსაფრთხოებაგადასაცემიინფორმაციისა, გააჩნდესსაჭირომწარმოებლურობა, მოხერხებულიიყოსადმინისტრირებისათვისდა “გამჭვირვალე” მომხმარებლებისადადანართებისათვის.

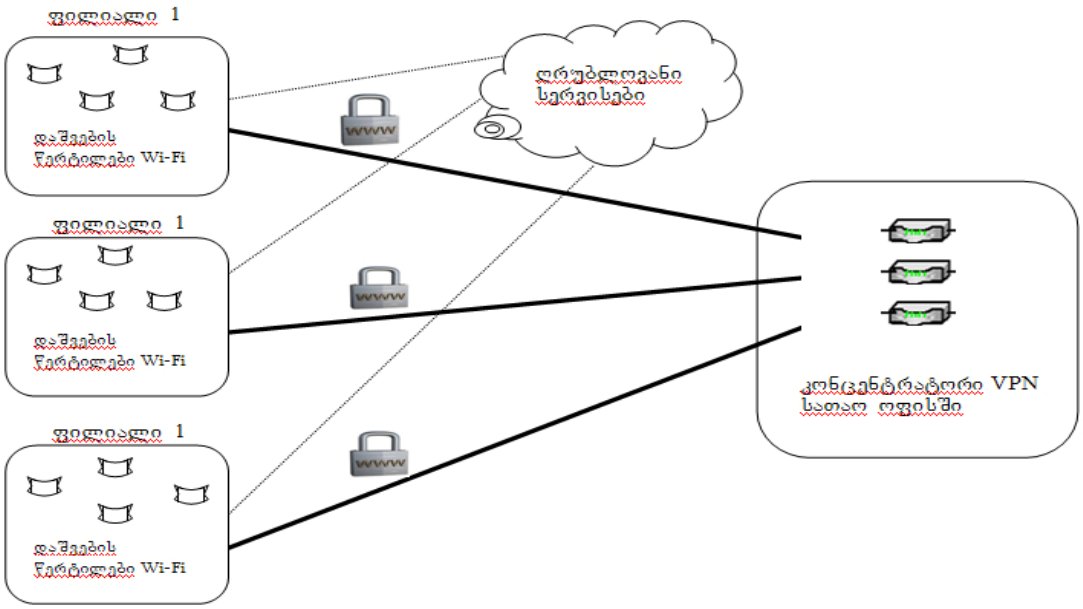
ესგულისხმობსმოსორებულიოფისებისდაფილიალებისგაერთიანებასერთიანინფორმაციულსტრუქტურ5აშიდამათბაზაზეფორმირებასდაცულიკორპორატიულისამუშაოგარემოსი.

რცისეიშვიათადინფრასტრუქტურულიდონემოიცავსასევესგმენტებსუმავთულოჭი- იქსელებისა,

რომლებიცუზრუნველყოფენთანამშრომლებისმობილურობაკომპანიისოფის
ში (ნახ.11.).

სპეციალისტებითვლიან, რომიმისათვის, რომუზრუნველყოფილიქნასდაცულიმოშორებულიდაშვებაკორპორაციულქ
სელთანაუცილებელია,
რათამიერთებაგანხორციელდესმხოლოდპროტოკოლებისSSL VPN/IPSec
გამოყენებითაუცილებელიორფაქტორიანიაუტენტიფიკაციისას.
შასურველიაასევემოშორებულიმომხმარებლებისავტომატურიუზრუნველყ
ოფადაცულისამუშაოსივრცით,
რათასამუშაოადგილზემიერთებისდასრულებისასარდარჩესარანაირიკვალი
(დროითიანგადმოტვირთულიფაილები,
გვერდებისმიკითხვისისტორიადაა.შ. უნდაიყოსმოშორებული).

IP
VPNტერიტორიულადგანაწილებულკომპანიაშიდანაყოფებისგასაერთიანებ
ლადერთიანკორპორატიულქსელშიგამოყენებულუნდაიქნასგამოყოფილიკა
ვშირგაბმულობისარხებიანსაერთოხელმისა-
წვდომიმონაცემთაგადაცემიაქსელი.
თუმონაცემებისხმოვანიდავიდეოტრაფიკისგადასაცემადგამოიყენებიანგამო
ყოფილიარხები,
მათიმეშვეობითგადაცემულიინფორმაციადაცულიაგარეშეზემოქმედებების
აგან, მაგრამასეთიგადაწყვეტა, ჯერერთი, საკმაოდძვირია, დამეორე,
საწარმოსარაყოველთვისდაარაყვე;განგააჩნიატექნიკურიშესაძლებლობამიი
ღოსთავისგანკარგულებაშიგამოყოფილიარხი.




ნახაზი 11.

განაწილებულიკორპორაციულიქსელიუმავთულოსეგმენტებითფილიალებ ში

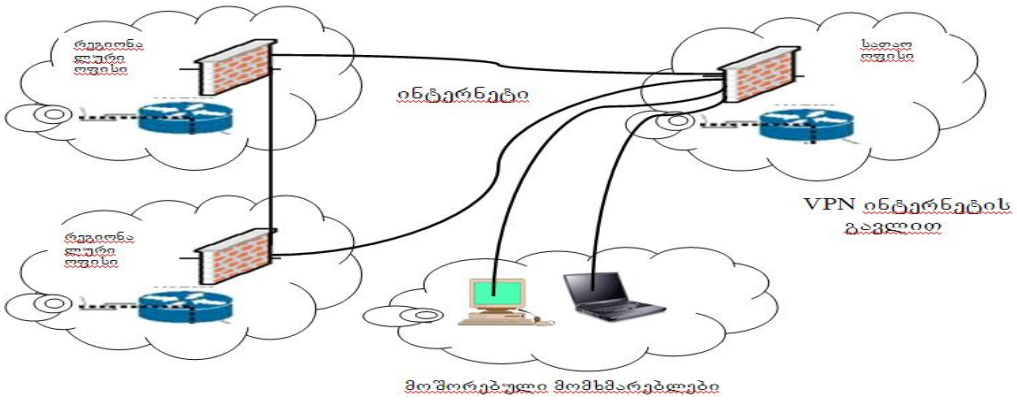
ასეთორგანიზაციებშიერტიანიკორპორაციულიქსელისშესაქმნელადხ შირადგამოიყენებაVPNშეერთებაინტერნეტისგამოყენებითIPSecმიხედვით, ზოგჯეროპერატორულიქსელებითMPLS (იხ. ნახ.12.). მსგავსი ქსელური ინფრასტრუქტურის დაცვა ხდება აუტენტიფიკაციის, დაშვების მართვის, გვირაბების გაყვანით დანაყოფებს შორია და დაშიფვრის გამოყენებით.

ვირტუალურიკერძოქსელებისტექნოლოგია(Virtual Private Network, VPN)უზრუნველყოფსსიმრავლესუპირატესობებისაშედარებითარცისემაღა ლიღირებულებისას. VPN– ლოგიკურიკერძოქსელი, რომლისორგანიზებაცხდებასაყოველთაოქსელისზემოთ.

ამოყოფილიარხებისმსგავსად, ისსაშუალებასიძლევაშექმნასდაცულიშეერთებამოშორებულპლათფორმებს ანლოკალურქსელებსშორის.

L2VPN რეალიზაცის ხდება Ethernet სერვისების გამოყენებით ან MOLS –ის საფუძველზე. ამ შემთხვევაში კომუტატორები ახდენენ კლიენტის

მოწყობილობებიდან მიღებული კადრების MOLS ან IP MPLS“შეფუთვას” და გადასცემენ მას დანიშნულების ადგილზე “ვიტუალური არხით”. ასეთი ტექნოლოგიით იგება საქალაქო ქსელები Metro Ethernet ან შესაბამისად საოლქო ქსელები IP MPLS.




ნახაზი 12. ტერიტორიულად განაწილებულ კომპანიას შეუძლია გამოიყენოს მონაცემთა გადაცემის საერთო ქსელი

L3 VPN (IP VPN)-ის შემთხვევაში კერძო ვირტუალური ქსელის ორგანიზებას ახდენს პროვაიდერი (MPLშ VPN) ან მომხმარებელი (IPშეც VPN). თუ საწარმოს გააჩნია სიმრავლე ფილიალებისა, მაშინ ტექნოლოგიის DYNAMIC MULTIPOINT VPN (DM VPN) მეშვეობით შეუძლია იოლად გასვლა ორი VPN კონცენტრატორით.

სერვისების ინტეგრაცია. VPN ორგანიზაციისას კორპორატიული ქსელი ლოგიკურად გამიჯნულია საყოველთაოდ ხელმისაწვდომი ქსელისაგან, ანუ ტრაფიკი დაცულია არასანქცირებული დაშვებისაგან. ამ დროს კომპანია ღებულობს სრულ კონტროლს მის ფუნქციონირებაზე. ასეთი ქსელით შესაძლებელია გადაცემულ იქნას სხვადასხვა სახის ტრაფიკები განიჯნული მომსახურების სხვადასხვა კლასებით.

მონაცემების გადაცემასთან ერთად ვიტუალური კერძო ქსელები გამოყენებულ უნდა იქნას IP-ტელეფონების და ვიდეო-კონფერენც-კავშირების სერვისებისათვის, მოქნილად შეიცვალოს გამტარუნარიანობა არხებისა ბიზნესის მოთხოვნილებებისაგან დამოკიდებულებით, მოხდეს მასშტაბირება ქსელური ინფრასტრუქტურისა, ახალი ობიექტების ერთიან დაცულ კერძო ქსელში ჩართვით. ამიტომ ტერიტორიულად განაწილებული

ქსელები VPN საფუძველზე წარმოადგენენ საფუძველს სხვადასხვა სერვისებისა, როგორიცაა VOIP, ВКН, ბიზნეს-დანართები, დასანერგად.

კერძო ვირტუალური ქსელების მესვეობით შესაძლებელია გაბნეული ოფისების გაერთიანება საერთო ქსელში, შექმნა ერთიანი სამისამართო სივრცის ლოკალური ქსელისა და ერთიანი ნუმერაციისა კორპორატიული ტელეფონისა, ანუ ფორმირებულ იქნას საერთო ინფორმაციული სივრცე, რომელიც ხელმისაწვდომია კორპორატიული ქსელის ნებისმიერი წერტილიდან.

IPSEC VPN – საკმაოდ მარტივი და გავრცელებული მეთოდია დაცული ქსელური ინფრასტრუქტურის შექმნისა ტერიტორიულად განაწილებული კომპანიებისა. მოწყობილობებს შორის იქმნებიან ვირტუალური გვირაბები, და მთელი ტრაფიკის დაშიფვრა ხდება დამკვეთის მოწყობილობებზე. ამრიგად ხდება უზრუნველყოფა სრული დამოუკიდებლობისა კავშირის ოპერატორისაგან. მართალია გადაწყვეტა გამოირჩევა უფრო დაბალი ღირებულებით არხების იჯარით აღებასთან შედარებით, მაგრამ მას გააჩნია თავისი ნაკლოვანებები: ხშირად საჭიროა დამატებითი მოწყობილობა (ან პროგრამული უზრუნველყოფა), ყოველთვის ვერ ხერხდება სერვისის ხარისხის გარანტირება.

დაცვის სტრატეგიები. ტექნოლოგიების და მიერთების ვარიანტების არჩევა დამოკიდებულია გადასაცემი ტრაფიკის სახეზე, ორგანიზაციის სტრუქტურასა დამის ბიზნეს-პროცესებზე, ინფორმაციული უსაფრთხოების მოთხოვნებზე, ოპერატორის ტარიფებზე, რომლის მომსახურებითაც კომპანია ფიქრობს ისარგებლოს, და სხვა ფაქტორებზე. აუცილებლია შეფასდეს საჭირო გამტარუნარიანობა და მოცულობა ტრაფიკისა, მოთხოვნები კავშირის არხის პარამეტრებზე (საიმედოობისა და დაცვის ხარისხის ჩათვლით) სხვადასხვა სახის ტრაფიკისათვის. ანალიზი ბიზნეს-პროცესებისა საშუალებას იძლევა გამოვლენილ იქნას, რამდენად კრიტიკულია საწარმოს მოღვაწეობისათვის გამოყენებული სერვისები.

ოღონდ ინფორმაცვიული უსაფრთხოება (იუ) უნდა დამუშავდეს არა მარტო კავშირის არხებისათვის, არამედ მთლიანად კომპანიისათვის.

უსაფრთხოების სისტემა დაფუძნებულია ტექნოლოგიების სიმრავლეზე, რომელთა შორისაა – ტრაფიკის დაშიფვრა, იუ-ს მართვის ერთიანი სისტემა, ქსელის უმავთულო ნაწილის დაცვის საშუალებები. არჩევა, ტექნოლოგიური, პროგრამული და ორგანიზაციული გადაწყვეტებისატერიტორიულად განაწილებულ სისტემებში კომუნიკაციების დასაცავად განისაზღვრება ქსელის არქიტექტურით, მისი მასშტაბით, დასამუშავებელი ინფორმაციის ხასიათით, ბალანსით ტექნიკური და ფინანსური შესაზლებლობებისა. კონკრეტული რეალიზაცია დაცული შეერთებებისა მოედნებს შორის აირჩევა გადასაცემი მონაცემების კატეგორიზაციის სფუძველზე მათი კრიტიკულობის გათვალისწინებით კომპანიის ბიზნეს-პროცესებისათვის და ტექნოლოგიური თავისებურებებით, მაგალითად აუცილებლობით DOS მხადაჭერისა.

ქსელური უსაფრთხოების ძირითად მიმართულებებს განეკუთვნებიან კორპორაციული ინფორმაციული სისტემის რესურსებთან დაშვების მართვა, მისი პერიმეტრის დაცვა, ტრანზაქციების აუტენტიფიკაცია, უსაფრთხოების შემთხვევების მონიტორინგ და სხვა. ღაციონალური დაცვა უნდა მოიცავდეს მონაცემების დაშიფვრას, ტერიტორიულად გაბნეული დანაყოფების დაკავშირებისას გარეშე ქსელის მესვეობით, გამოყენება ქსელთაშორისი ეკრანებისა და სემოჭრების აღმომჩენი საშუალებებისა ქსელის პერიმეტრის დასაცავად, ოპერატიული კონტროლი იუ-ს შემთხვევებისა. ის იგება გათვალისწინებით მახასიათებლებისა ინფორმაციის, პარამეტრებისა ინფორმაციული სისტემისა, რისკების და სხვადასხვა მუქარების დონის შეფასებით.

დღეისათვის ხელმისაწვდომი ქსელთაშორისი ეკრანების და VPN გადაწყვეტების სპექტრი საკმაოდ ვრცელია და შეუძია დააკმაყოფილოს მრავალფეროვანი მოთხოვნები ფუნქციონირებისა, მწარმოებლურობისა და ღირებულებისა. არც ისე იშვიათად ვენდორები გვთავაზობენ ინტეგრებულ

სისტემებს, რომლებიც აერთიანებენ უსაფრთხოების რამოდენიმე ფუნქციას, მაგალითად, ფუნქციები ქსელთაშორისი ეკრანირებისა VPN და IPS ერთად.

როგორც სპეციალისტები მიუთითებენ, კონკრეტული დაცვის სტრატეგიის რეალიზაცია დამოკიდებულია თვით ორგანიზაციაშიუსაფრთხოების პროცესების მოწიფულობაზე. შერვისების კრიტიკულობიდან გამომდინარე უსაფრთხოების საშუალებებს შეუძკიათ გაითვალისწინონ დაშვების კონტროლი, მონაცემების, არხების და მოწყობილობების დაცვა, ასევე ვერიფიკაცია უკანასკნელებისა. ჩვეულებრივგამოიყენებიან შემდეგი ტექნოლოგიები: მრავალფაქტორიანი აუტენტიფიკაცია დაშვების ორგანიზებისას (არა აუცილებლად ხდება არხის დაცვა), არხის დაშიფვრა (VPN), მოწყობილობების პროფილირება, ყოველი შეერთების რისკის ანალიზი, შექმნა/კონტროლი სანდო გარემოსი ბოლო მოწყობილობაზე.

როგორც სპეციალისტები აღნიშნავენ, როდესაც კიბერდამნაშავეების მიზან წარმოადგენს მსხვილი ორგანიზაცია დიდი ინვესტიციებით იუ-ში, გატეხვა ქსელის მოშორებული (და შედარებით ნაკლებად დაცული) სეგმენტისა წარმოადგენს ყველაზე უფრო მარტივ ხერხს  შეღწევისა. პრევენციული ტექნოლოგიები დაცვისა მოსორებული სეგმენტების მხარეს – მათთვის სრულად დაძლევადი ბარიერია. მათ შეუძლიათ გაიმეორონ შეტევების მცდელობები ისევ და ისევ ვიდრე არ იქნება მიღწეული წარმატება, მიიღებენ რა დაშვებას მოშორებულ სეგმენტთან, შეტევები უკვე განხორციელდება მთავარ ოფისზე/ძირითად პროცესებზემიღებული ლეგიტიმური უფლებების გამოყენებით, - ამიტომ კომპანიებს, რომლებსაც გააჩნიათ ფილიალების განვითარებული ქსელები, უნდა იყვნენ მზად არა მარტო წინ აღუდგნენ მუქარებსმოსორებულ სეგმენტებზე, არამედ გააჩნდეთ საშუალებები მათი აღმოჩენისა შეტევების რეალიზაციის სხვადასხვა ეტაპებზე როგორც რეაქტიული (მაგალითად, ხაფანგები კლასის ჰონეყპოტ), ასევე პროაქტიური ხასიათის (შემოჭრების აღმომჩენი სისტემები, ტარგეტირებული შეტევებისაგან დაცვის სისტემები).

კორპორაციულ ქსელში შორიდან დაცული დაშვებასთან ერთად სულ უფრო ხშირად საჭირო ხდება უზრუნველყოფილ იქნას უსაფრთხოება ღრუბლოვან სერვისებთან მუშაობისას, როდესაც კომპანია ღებულობს გადაწყვეტილებას გამოიყენოს ასეთი სერვისები, ის ორიენტირებულია პროვაიდერის კომპეტენციაზე. ოღონ გათვალისწინებული დაცვის ტექნოლოგიები ვერ წყვეტენ პრობლემებს, რომლებიც დაკავშირებულია დროული შეწყვეტით ან სწორი მართვის რესურსებთან დაშვების უფლებებთან, თუ საუბარია დაცვის ბაზურ ელემენტებზე ღრუბლოვანი სერვისების გამოყენებისას, მაშინ IT-ადმინისტრატორმა უნდა ააგოს პროცესი დაშვების მართვის (IDETITY MANAGEMENT), რომელიც შესაძლებელს გახდის მოხდეს ბლოკირება თანამშრომლის მიმართვის გარე სერვისებთან მისი სტატუსის შეცვლის შემთხვევაში (გადასვლა სხვა განყოფილებაში, მოსალოდნელი დათხოვნა). ამის გარდა, ასეთმა პროცესებმა უნდა გაითვალისწინონ IT-ადმინისტრატორის შეცვლაც.

სპეციალისტების აზრით, ტერიტორიულად განაწილებული კორპორაციული ქსელის პირობებში თანამედროვე მუქარებისადმი ეფექტური წინააღმდეგობისათვის გათვალისწინებულ უნდა იქნას შემდეგი მოთხოვნები:

- ცენტრალიზებული მართვა უსაფრთხოების პოლიტიკისა დაცვის სისტემის ყველა ელემენტებისა;

- კორექცია მონაცემებისა შემომავალი შემთხვევების საფუძველზე და მოქნილი შეცვლა წესებისა მოწყობილობებზე შეცვლილი მუქარების შესაბამისად;

- უწყვეტი განახლება მდგომარეობებისა სერვისული მოდულებისა უსაფრთხოების მოწყობილობებზე, ისეთების როგორებიცაა ვებ-ფილტრაცია, შემოჭრების აღმოჩენის სისტემები, დანართების ტრაფიკების კონტროლი, ანტისპამი, ბაზა IP-რეპუტაციისა და სხვების;

- უზრუნველყოფა მტყუნება მედეგობისა იუ-ს უზრუნველყოფის მთავარი ელემენტებისა;

- რეალიზაცია პოლიტიკებისა (SINGLE SIGN ON და IDENTITY BASED POLICY) ქსელის ყველა მომხმარებლების კონტროლისათვის.

ცხადია, რომ კორპორაციულ ქსელში უსაფრთხო მუშაობის ორგანიზებისათვის აუცილებელია კომპლექსური მიდგომა. სხვადასხვას ტექნიკური გადაწყვეტები – ქსელთაშორისი ეკრანები, ანტივირუსული და ანტისპამ-სისტემები, VPN და სხვა – აუცილებელია შევსებულ იქნას ორგანიზაციული ზომებით, ეს განსაკუთრებით აქტუალურია, როდესაც ორგანიზაციას გააჩნია ტერიტორიულად დაშორიშორებული ფილიალები ან მოითხოვს შეიქმნას პირობები მობილური თანამშრომლების უსაფრთხო მუშაობისათვის, მაგალითად იმ თანამშრომლებისა, რომლებიც იმყოფებიან მივლინებაში.

ამ შემთხვევაში ძალზე მნიშვნელოვანია არა მარტო არსებობა საიმედო და დაცული კავშირის არხისა თანამშრომელსა და კორპორაციულ ქსელს შორის, არამედ შესაძლებლობა ცალსახად იდენტიფიცირებულ იქნას მომხმარებელი, რათა მიეცეს მას კუთვნილი უფლება დაშვებისა ინფორმაციასთან. აუცილებელია ხაზი გაესვას დიდ მნიშვნელობას სწორედ მომხმარებლების აუტენტიფიკაციისა, და არა მოწყობილობებისა (ნოუთბუკების, სმარტფონების), რომლებიც მიუერთდებიან კორპორაციულ ქსელს, ვინაიდან მოწყობილობების დაკარგვისას ან მოპარვისას ბოროტგანმზრახველს შეუძლია მიიღოს დაშვება საწარმოს ქსელთან.

ანალოგიური ამოცანები წარმოიქმნებიან ურთიერთმოქმედებების უზრუნველყოფისას ტერიტორიულად განაწილებულ ფილიალებს შორისაც. ძალზე მნიშვნელოვანია გამოყენება აუტენტიფიკაციის საიმედო მექანიზმებისა როგორც კორპორაციულ ქსელთან მიერთებისას, ასევე დაშვებისას სხვადასხვა ინფორმაციულ სისტემებთან, პორტალებთან და სერვისებთან, რომლებიც მასში მუშაობენ. ერთ-ერთ ასეთ მექანიზმს წარმოადგენს გამოყენება ღია გასაღებების სერტიფიკატებისა, რომელიც გამოშვებულია კორპორაციული მადასტურებელი ცენტრის მიერ. ჩენტრალიზებული სისტემა მართვისა აუტენტიფიკაციის საშუალებების და

თვით დაშვების კორპორაციულ რესურსებთან და სისტემებთან საშუალებას იძლევა მოხდეს ოპერატიული რეაგირება მუქარების აღმოჩენის შემთხვევებისას ან ინციდენტების წარმოქმნისას.

ცენტრალიზებული მონიტორინგი და მართვა

რამდენად მნიშვნე;ოვანია ამ კონტექსტშიცენტრალიზებული მართვის ფუნქციები რეალურ დროში? მონიტორინგ და აღმოჩენა IT-უსაფრთხოების მუქარებისა რეალურ დროში მოითხოვენ სისტემატიურ შეგროვებას ინფორმაციისა შემთხვევებზე, რომლებიც ხდებიან ქსელის განაწილებულ სეგმენტში. მაგრამ მოშორებულ დანაყოფებში ყოველთვის როდი ყავთ სპეციალისტები მხარდაჭერის სამსახურისა, მით უმეტეს თანამშრომლები, რომლებიც პასუხს აგებენ დაცვის საშუალებების ადმინისტრირებაზე. ამ შემთხვევაში საჭიროა რა მარტო ცენტრალიზაცია, არამედ შესაძლებლობა იერარქიული მართვისა, მაგალითად, გავრცელება გლობალური კრიტიკული პოლიტიკებისა, რომლებიც ფორმირებულია სათაო ოფისში, ერთდროულად ლოკალური ადმინისტრირებისას უნიკალური წესებისა განაწილებული სეგმენტებისათვის.

შექმნა ერთიანი მართვის ცენტრებისა, რა თქმა უნდა, აუცილებელია, ვინაიდან გვეხმარება გამოვლენილ იქნას რისკები და, შესაბამისად, მინიმიზებულ იქნას შედეგი. მაგრამ ასეთი ცენტრების ადმინისტრირება რეალურ დროში მოითხოვს დამატებითი ფინანსების გამოყოფას. ყველაფერი უნდა იყოს თანაზომადი, და თუ რისკების შეფასებისას დგინდება მაღალი ალბათობა იმისა, რომ სავარაუდო შეტევამ საწარმოზე შეიძლება გამოიწვიოს მასშტაბური ზარალი, მაშინ ცენტრალიზებული მართვის სისტემები აუცილებლად უნდა ფუნქციონირებდნენ რეალური დროის რეჟიმში.

მონიტორინგის საშუალებების ჯგუფში შეიძლება გამოიყოს გადაწყვეტები უსაფრთხოების შემთხვევების და მონაცემების მართვისათვის (Security Information & EventManagement, SEIM) მოვლენების კორელაციით, რომლებიც საშუალებას იძლევიან გაკონტროლდეს როგორც

თვით უსაფრთხოების შემთხვევები, ასევე მათი ურთიერთკავშირი. შემთხვევების ჟურნალები ანალიზდებიან გამოყენებით მეთოდებისა, ანალოგიურების დიდი მონაცემების ანალიზისა. სწრაფად ვითარდებიან აგრეთვე შიდა მუქარების თვალთვალის და ინფორმაციის გაჟონვისაგან დაცვის საშუალებები (DLP). ევოლუციას განიცდიან აუტენტიფიკაციის მეთოდები და PKI გადაწყვეტები.

ცენტრალიზებული მართვის გარეშე შეუძლებელია აიგოს ეფექტური სისტემა დაცვისა განაწილებული ქსელის პირობებში. მართვის თანამედროვე საშუალებები საშუალებას იძლევიან კოორდინირებულ იქნას გადაწყვეტები სხვადასხვა მწარმოებლებისა, საერთო კორპორაციული უსაფრთხოების პოლიტიკის პრინციპების გათვალისწინებით. მაგალითს წარმოადგენს ტექნოლოგია SDN. ვენდორებიაქტიურად მუშაობენ მოცემული მიმართულებით: მაგალითად, კომპანიამ FORTINET წარმოადგინა ახალი სისტემა უსაფრთხოებისა პროგრამულად განსაზღვრებადი ქხელებისა (Software-Defined Network Security, SDNS).

IU-ში ეფექტური ინვესტიციებიმოითხოვენ კომპლექსურ შეფასებას რისკებისა და მუქარებისა. მხედველობაში უნდა იქნას მიღებული, მომავალი განვითარება დაცული ტელესაკომუნიკაციო ინფრასტრუქტურისა, სხვანაირად გარდაუვალია დამატებითი დანახარჯები სისტემის მოდერნიზაციაზე.

## 2.2.

## კრიტიკულადმნიშვნელოვანინფრასტრუქტურებშიინფორმაციისდაცვისინტელექტუალურისერვისებისარქიტექტურა

ინფორმაციისდაცვაგანაწილებულკომპიუტერულქსელებსადასისტემებში,

რომლებიცდამახასიათებელიაკრიტიკულადმნიშვნელოვანიინფრასტრუქტურებისათვის (კმი),

რომელთარიცხვსაცგანეკუთვნებიანკავშირისადამართვისსისტემებიარამარ

ტოპოლიტიკურიდასახელმწიფო – ადმინისტრაციული, ასევესაწარმოო-ეკონომიკური, ძალოვანი, სამეცნიერო-ტექნიკური, საგანმანათლებლოდასხვასტრუქტურებისადაორგანიზაციებისათვის, უნდაიყოსდაფუძნებულიდაცვისინტელექტუალურისერვისებისგამოყენებაზე. მი-შიინფორმაციისდაცვისინტელექტუალიზაციისპროცესების, მეთოდების, მოდელებისდაალგორითმებისრეალიზაციახორციელდებაინფორმაციისდაცვისინტელექტუალურისერვისებისსისტემის (იდისს) აგებითდაფუნქციონირებითროგორცახალიდაუნიშვნელოვანესიკომპონენტისაკრიტიკულინფრასტრუქტურაშიინფორმაციისდაცვისსისტემისა.

იდისსშეიძლებაგანვიხილოთროგორცტრადიციულიდაცვისსისტემის ზედნაშენი, რომელიცკიარცვლის, არამედავსებსამუკანასკნელისფუნქციონალურშესაძლებლობებს. იდისს-შიმმართველობითიგადაწყვეტილებებისგამომუშავებახორციელდებაუსაფრთხოებისშემთხვევებისშესახებინფორმაციისდამუშავებით, ხოლოიდისსფუნქციონირებისსაფუძველსმიზანშეწონილიაწარმოადგენდეს “უსაფრთხოებისინფორმაციისდაშემთხვევებისმართვა” (Security Information and Event Management System, (SII).ინფორმაციას, რომელიცახასიათებსუსაფრთხოებისშემთხვევებს, განეკუთვნებიანყველამონაცემებიდასაცავიინფრასტრუქტურისელემენტებისცვლილებებისშესახებ, რომლებიცუნდაიქნასშენახულიელექტრონულისახითსპეციალურჟურნალებშიანშემოდიანუშუალოდსისტემაSIკავშირისხაზებით.

იდისს-შიSI ტექნოლოგიისპრინციპებისშესაბამისადუნდაგამოიყოსუსაფრთხოებისშემთხვევებისდამუშავებისსამიჯგუფი: 1) საწყისიინფორმაციისწარდგენისფორმატისშეგროვებისადაგარდასახვისმექანიზმები; 2) მოთხოვნითინფორმაციისშენახვის, ძებნისადაგაცემისმექანიზმები; 3)

ინფორმაციისანალიზისადაგადაწყვეტილებათაგამომუსავებისმექანიზმები. იდისსპრაქტიკულირეალიზაციაკმი-

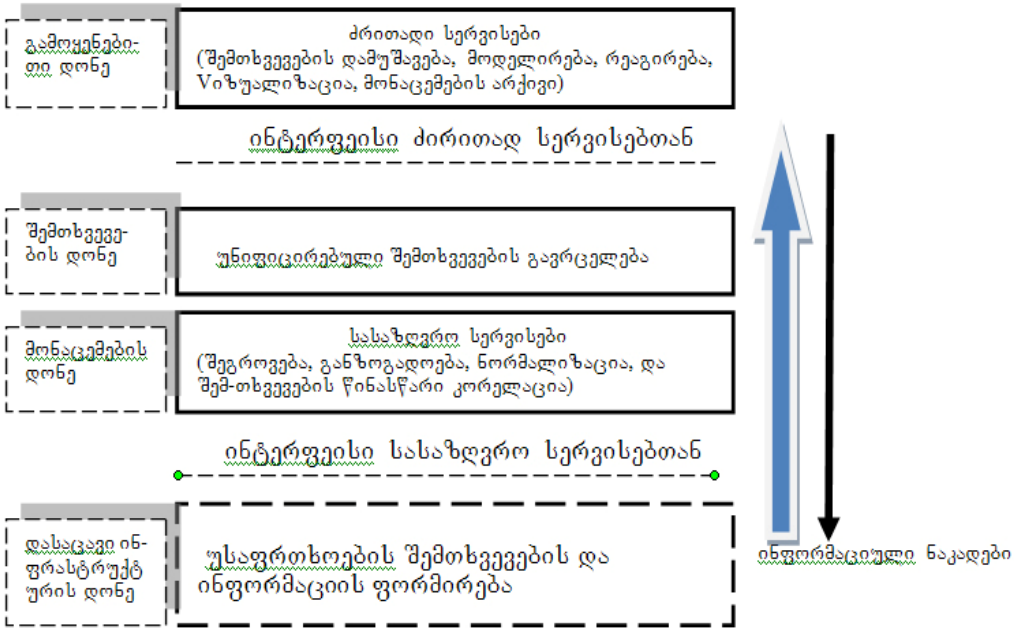
თანმიმართებაშიმოითხოვსგამომუშავებასგადაწყვეტილებებისა, რომლებიცდაკავშირებულიარიანროგორცთვითიდისსარქიტექტურისგამომ უშავებასთან, ასევემისშემადგენლობაშიშემავალიკომპონენტებისა. აქნაჩვენებიიქნებასწორედ, იდისსსაერთოარქიტექტურიდანგამომდინარე, მისიყველაკომპონენტებისარქიტექტურულიაღწერა.

2) იდისსსაერთოარქიტექტურა

ვინაიდანიდისსკმი-

სათვისფუნქციონირებსჰეტეროგენულდამსხვილმასშტაბიანგარემოშისხვად ასხვადონისკომპიუტერულიშეტევებისპირობებში, ისსაჭიროებსკორექტულდამდგრადგამოთვლითმოდელებს, რომლებიცადექვატურადასახავენმისმახასიათებლებს. ამიტომიდისსკმი-სათვისუნდამოიცავდესკვანძებსდამოწყობილობებსგანაპირაკვანზებისდაქს ელებისშესაძლოშეერთებითუწყებათაშორისიქსელებითდასაერთოგამოყენე ბისქსელებით. ამდროსგათვალისწინებულიუნდაიყოს, რომგანაპირაკვანძები, რომლებიცგანკუთვნილიარიანმონაცემებისშესაგროვებლად, დაცულებიარიანნაკლებიხარისხით, ვინაიდანძირითადიკვანძები, რომლებზეცხდებამონაცემებისდამუშავება, ხოლოტელესაკომუნიკაციოგარემოშეიძლებაიყოსარასაიმედო. ძირითადიკვანზებიდაცულებიუნდაიყვნენუფრომაღალიხარისხით.

ზოგადადიდისსარქიტექტურასგააჩნიარამოდენიმედონე: მონაცემებისდონე, შემთხვევებისდონე, გამოყენებითიდონე. ესდონეებიზედედებიანდასაცავიინფრასტრუქტურისდონეს, როგორცესნაჩვენებიანახ.13.-ზე.




ნახ.13 იდისსსაერთო (ზოგადი) არქიტექტურა.

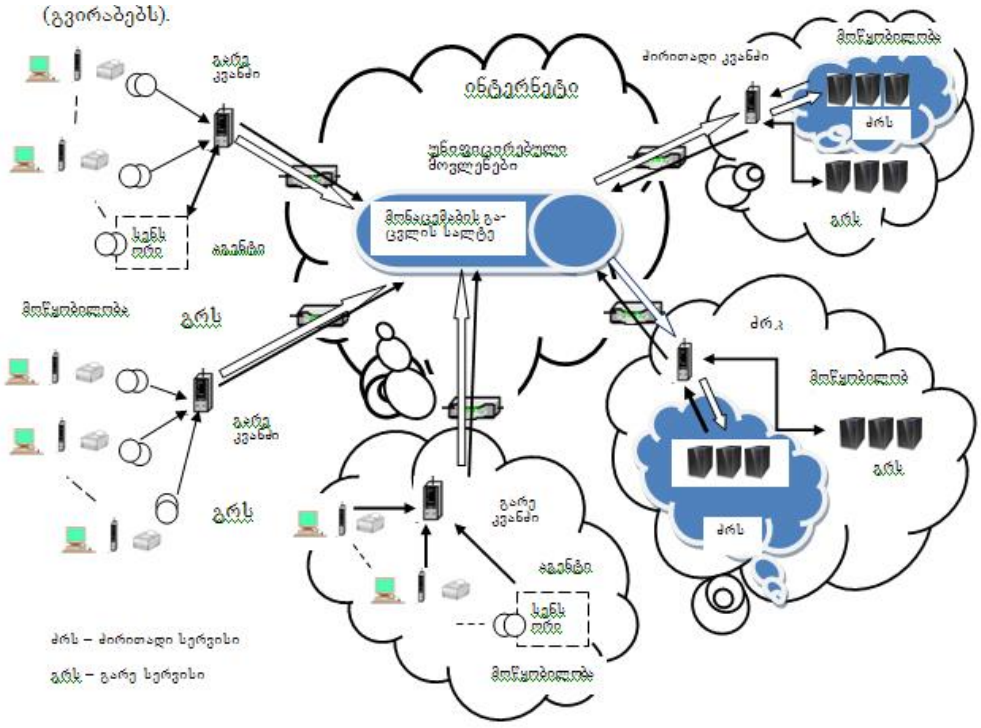
მონაცემებისდონეზეხორციელდებამონაცემებისშეგროვებაუსაფრთხოებისშემთხვევებისშესახებ, მათიდამუშავებადაწინასწარიკორელაცია. შემთხვევებისდონეპასუხსაგებსუსაფრთხოებისშემთხვევებისშესახებინფორმაციისნაკადებისგავრცელებაზემომხმარებლებსშორისრეალურდროში.

ამდროსუნდააღინიშნოს, რომამომავალინაკადიინფორმაციისამონაცემთადონიდანგამოყენებისთდონეზე, არისუფროინტენსიური, ვიდრესაპირისპირო. გამოყენებითიდონეახდენსუსაფრთხოებისშემთხვევებისდამუშავებას, მოდელირებას, გადაწყვეტილებათამიღებისადარეაგირებისმხარდაჭერას, ვიზუალიზაციას, შემთხვევებისშენახვას.

უსაფრთხოებისშემთხვევებისშესახებმონაცდემებისფორმირებახდება დასაცავიინფრასტრუქტურისდონეზედასაჭიროებსწინასწარდამუშავებასმონაცემებისდონეზე, შემდეგვრცელდებიანშემთხვევებისდონისმეშვეობითგამოყენებითიდონისს აჭიროელემენტებსშორისდა, საბოლოოჯამში, საბოლოოდამუშავებახდებაბოლოელემენტებისმიერ.

იდისსზოგადიარქიტექტურისსტრუქტურულიმოდელიწარმოდგენი ლიანახ.14-ზე. როგორცჩანსნახ.14.- დანიდისსსტრუქტურაშიგამოყოფილიაელემენტებისსამიჯგუფი: მოშორებული (საზღვრისპირა) სერვისებიდააგენტები, მონაცემთაგაცვლისსალტედაძირითადისერვისებიდააგენტები.

ტელესაკომუნიკაციოსისტემა, რომელიცთამაშობსმონაცემებისგაცვლისსალტისროლს, შეესაბამებამოდელს "გლობალურიქსელისა, რომელიცშედგებალოკალურიქსელებისაგან" (WAN-of-LANs),რომელიცაღწერსსუსტადდაკავშირებულგამოთვლითინფრასტრუქტურებს, რომლებიცმოიცავენერთიდაიგივეანსხვადასხვაგვარადმინისტრაციულდომენებს. ესმოდელიუმეტესწილადდამახასიათებელიაკმი-სათვის, ვინაიდანკმი-სობიექტებიმნიშვნელოვნადარიანგანმხოლოებულებიგეოგრაფიულად. მათიადგილობრივიინტერესებიერტმანეთთანარიანდაკავშირებულებისაერთომოხმარებისქსელის (ინტერნეტის) მეშვეობით. ერთ-ერთმეთოდსმათიგაერთიანებისაწარმოადგენსვირტუალურიკერძოქსელები, რომლებიცქმნიანდაცულკავშირებისარხებს (გვირაბებს).




ნახ.14. იდისსზოგადი (საერთო) არქიტექტურისსტრუქტურულიმოდელი

იდისსზოგადიარქიტექტურისფუნქციონალურიმოდელიწარმოდგენილიანახ.3.-ზე, რომელზეცნაჩვენებიაინფორმაციისნაკადებისგავრცელებაარქიტექტურისდონეებისდამისიელემენტებისგავლით. ინფორმაციისშეგროვებახდებაგანაპირაკვანძებშიდაგავრცელებახდებაგამოყენებითსერვისებთან.

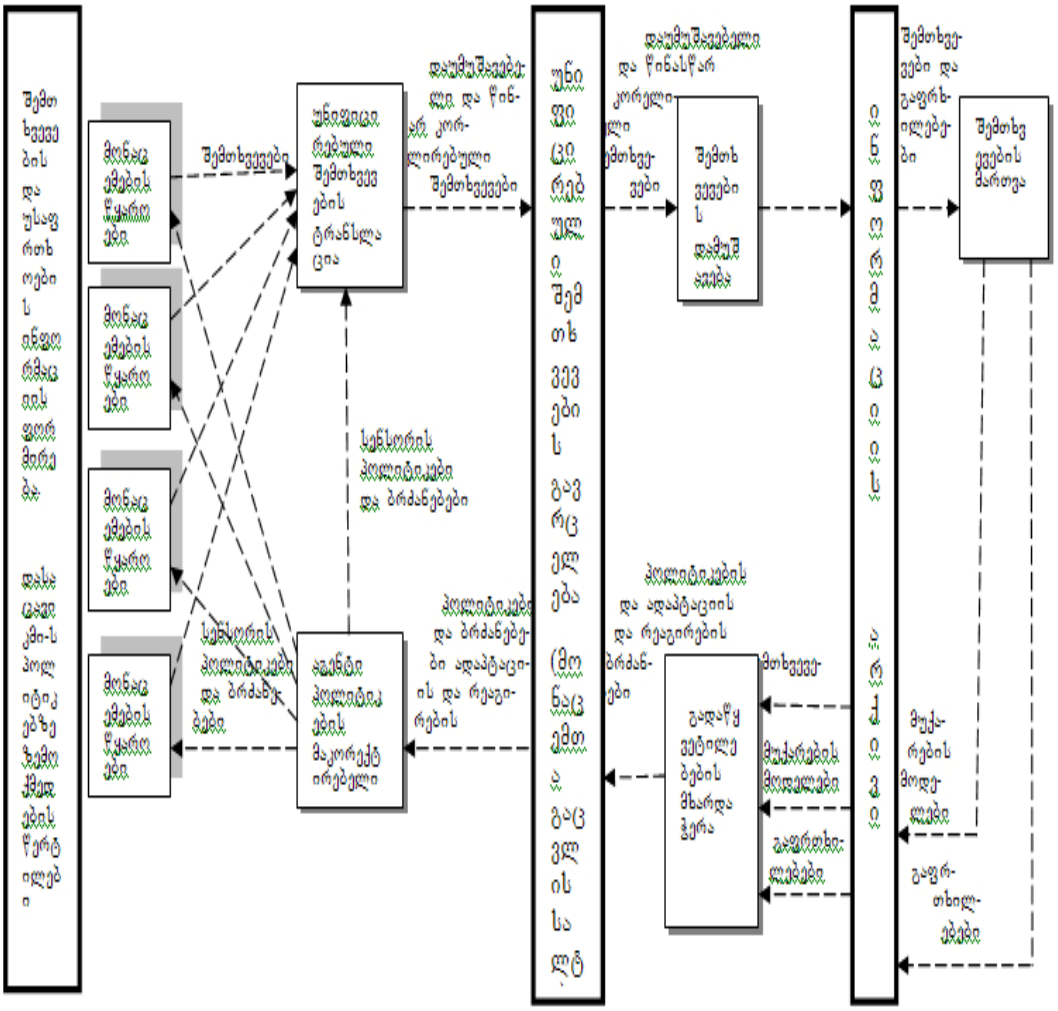
დავახასიათოთისძირითადიმექანიზმები, რომლებიცნაჩვენებიანახ.14.-ზე.

შემთხვევებისდამუშავებისმექანიზმიახორციელებსრელევანტურიშემთხვევებისკორელაციას, რომლებიცგამოიყოფაინფორმაციისნაკადიდანშემთხვევითანწინასწარიდამუშავებით, დაათავსებსმათშესანახადინფორმაციულარქივში. ინფორმაციისარქივიახდენსუშუალოურთიერთმოქმედებებსსხვაგამოყენებითმოდულებთან.

მოდულებისმართვისსერვისებიახორციელებენსისტემისქცევისმოდელირებასდაგამოიმუშავებენდამატებითმოდელრბს:

მუქარებისდაუსაფრთხოებისგაფრთხილებისმოდელები,

რომლებიცბრუნდებიანუკანინფორმაციისარქივში.



ნახ.15 იდისსსაერთოარქიტექტურისფუნქციონალურიმოდელი.

ამბოლოს,

გადაწყვეტილებებისდარეაგირებისმხარდამჭერისერვისებიაანალიზებენშემომავალშემთხვევებს,

მოდელებსმუქარებისდაუსაფრთხოებისგაფრთხილებებისადაგამოიმუშავებენრეაქციასდაკონტრზომებს,

რომლებიცახდენენუსაფრთხოებისპოლიტიკებისმოდიფიკაციას,

რომლებიცგადაეგზავნებათუკანგანაპირაკვანძებსდაზემოქმედებენმოშორებულმონაცემებისწყაროებზე,

აგენტებზედაუსაფრთხოებისშემთხვევებისწინასწარიდამუშავებისმოდულებზე.

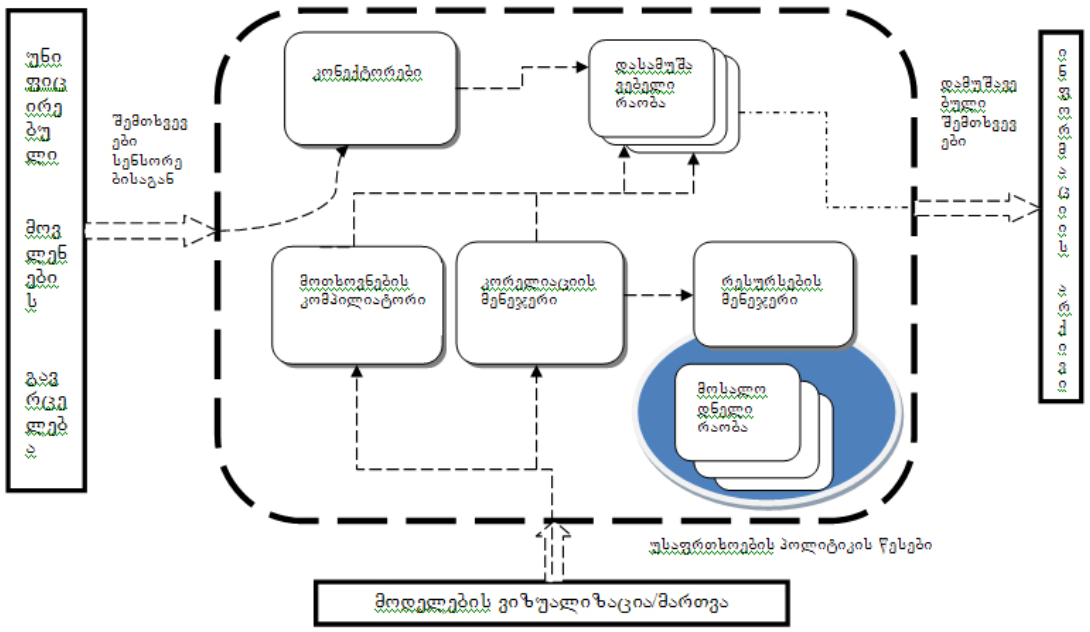
განვიხილოთუფროდეტალირადმოდულებისარქიტექტურები, რომლებიცახდენენაღნიშნულიმექანიზმებისრეალიზებას.

**შემთხვევებისდამუშავება**

შემთხვევებისდამუშავებახდებაკორელაციისმართვისმასშტაბირებად დაადაპტიურმოდულში, რომელიცორიენტირებულიართულიშემთხვევებისპარალელურიდამუშავებისსისტემაზე, რომელსაცშეუძლიაგააერთიანოსგამოთვლითისიმძლავრეებირათადაამუშაოსდიდირაოდენობისშემთხვევებიწამშიდამოახდინოსრეაგირებარაოდენობრივადგამოყოფილირესურსებითმოცემულიკმი-სათვის.

ამმოდულისქცევაშესაძლებელიაექსტენსიურადმომართულიიქნასმოთხოვნებისმეშვეობით, რომლებიციქმნებიანმომხმარებლებისმიერგანსაზღვრულისტანდარტულიდირექტივებიდან. მოთხოვნებიგანსაზღვრავენროგორუნდამოხდესშემომავალიშემთხვევებისაბსტრაქცია, განზოგადოებადაკორელაცია. მოთხოვნაშედგებაოპერატორებისაგან.

კორელაციისმარტვისმოდელისშიდაარქიტექტურადამისიკავშირისხვაკომპონენტებთანნაჩვენებიანახ.16.-ზე.




ნახ.16. კორელაციისმართვისმოდულისარქიტექტურა

მოცემულიმოდულისათვისდამახასიათებელიადიდირაოდენობადასა მუშავებელირაობებისა,
რომლებიცორგანიზებულიარიანქვეკლასტერებისთანმიმდევრობაში. ყველარასამუშავებელირაობაქვეკლასტერისაგამოიმუშავებენეართნაირპორ ციასმოთხოვნებისა, რომლებსაცეწოდებათქვემოთხოვნები, ღებულობენრაშემომავალიინფორმაციასწინაქვეკლასტერისაგანდაგადასცემე ნგამომავალშემთხვევებსმომდევნოქვეკლასტერზე.

კორელაციისმენეჯერიაკონტროლებსყოველიდასამუშავებელირაობისმდგ ომარეობასდაგანსაზღვრავსქვეკლასტერისზომასგამომდინარემისიმიმდინა რეშემავალიდატვირტვისმიხედვით.

ამატებაანმოშორებადასამუშავებელირაობისაკორელაციისმენეჯერისაგანმ ოითხოვსმისურთიერთმოქმედებასრესურსებისმენეჯერთან, რომელიცშეიცავსგარკვეულრაოდენობასმოსალოდნელირაობებისა, რომლებიცხელმისაწვდომიაშემდგომიდამუშავებისათვის.

ამდროსკორელაციისმენეჯერსშეუძლიაგადაანაწილოსდატვირთვადასამუ შავებელრაობებსშორის, რომლებიცუშუალოდდაკავშირებულიარიანქვეკლასტერთან.

ამბოლოს,

მოთხოვნებისკომპილატორიღებულობსსტენდარტულდირექტივებსშემავა

ლიინტერფეისისგავლითანმოდულებისმართვისკომპონენტისმეშვეობით,

შემდეგახდენსმათტრანსლირებასმოთხოვნებში,

ახდენსმათრეალიზაციასქვემოთხოვნებშიდააგზავნისყოველმოთხოვნასქვეკ

ლასტერში.

4.მოდელებისმართვა

მოდელებისმართვისმექანიზმისრეალიზებახდებაორიმოდულით:

უსაფრთხოებისმაპროგნოზირებადიანალიზატორით (უმა)

დაშეტევებისდაცვისსისტემისქცევისმოდელირებისკომპონენტით (შდსქმკ).

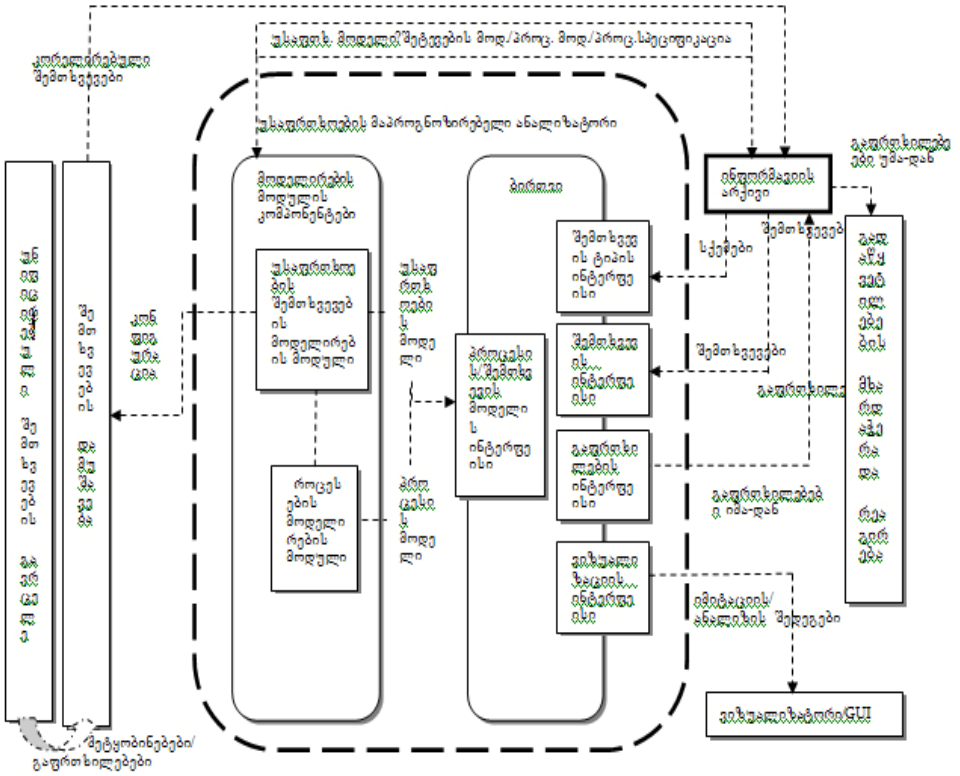
ამმოდელიუზრუნველყოფსიდისს-

შიუსაფრთხოებისმონიტორინგისშესაძლებლობებისგაფართოებას. კერძოდ,

ისმხარსუჭერსუახლესპერსპექტივაშიკმი-

სსაქციელისმოდელირებასდაწინასწარმეტყველებასუსაფრთხოებისშესაძლო

დარღვევებზე. ამმოდულისარქიტექტურამოცემულიანახ. 17.-ზე.




ნახ.17. უსაფრთხოებისპროგნოსტიკურიანალიზატორისარქიტექტურა.

ვინაიდანჩასატარებელიანალიზისხარისხიარსებითადდამოკიდებულ
იაპროცესებისაღწერისხარისხსადაგულმოდგინებაზე,
ასევეუსაფრთხოებისშემთხვევებისშესაბამისაღწერაზე, ამიტომუმა-
სმუშაობისდაწყებამდეყველაპროცესების,
მიზნებისდაუსაფრთხოებისშემთხვევებისაღწერებიუნდაიყოსგარდასახულ
იგასაგებმოდელებად,
რომლებიცშემდეგშიინტენსიურადგამოყენებულიიქნებარეალურდროშიუწყ
ვეტიანალიზისსაწარმოებლადდაუახლესიპერსპექტივისმოდელირებისათვ
ის.

ესხორციელდებაუსაფრთხოებისშემთხვევებისმოდელირებისმოდულშიდა
პროცესებისმოდელირებისმოდულში,
რომლებიცწარმოადგენენმოდელირებისმოდულისკომპონენტებს.
მოცემულიმოდულებიურთიერთმოქმედებენინფორმაციისარქივთან,
რომელიცშეიცავსშეტევებისმოდელებს, რომლებიცშექმნილიაშდსქმკ-ში,
დამოდელებს, რომლებიცადრეიყოშექმნილიმოდელირებისმოდულში.
ინტერფეისებიუსაფრთხოებისშემთხვევებისმოდელებისდაპროცესებისმოდ
ელებისუზრუნველყოფენმათთანდაშვებასუმა-სმხრიდან.

ოდელებირომლებმაც, მიიღესინტერპრეტაცია, იმპორტირდებიანუმა-
შიინციალიზაციისფაზაზე.

უმა-
სმოდელირებისმოდულიმხარსუჭერსუსაფრთხოებისგამოვლენილმოთხოვნ
ებს,
სპეციფიკაციასინიტაციურიმოდელისადამონიტორინგისწესებისგანვითარე
ბას.
იდისსინფორმაციისარქივშიუნდაინახებოდესდაცვისმაღალდონიანიმიზნებ
ი, უსაფრთხოებისმოთხოვნები, მონიტორინგისწესები,
დამუშავებულისპეციფიკაციებიდამათშორისკავშირები.

ესკავშირებიაუცილებელიაგაფრთხილებებისკორელაციისუზრუნველსაყო

ფად, რომლებიცგამომუშავდებიანუმა-ში, დაცვისდაუსაფრთხოებისმოთხოვნებისმიზნებიდანგამომდინარე.

ფრომეტიც, კმირესურსებისაღწერადაშემთხვევებისფორმატირება, რომლებიცინახებიანინფორმაციისარქივში, აუცილებელიააუცილებელიაკორელაციისათვისინფორმაციისრესურსებისშესახებმიღებულიშემთხვევებითდაგაფრთხილებებით, რომლებიცგადაიგზავნებიანუმა-შიინფორმაციისარქივისმეშვეობით (გავლით).

კომპონენტიშდსქმკუზუნველყოფსდამატებითანალიტიკურშესაძლებლობებსიდისშეტევათამოდელირებისადადაცულობისანალიზისფუნქციებისრეალიზებისმეშვეობით. ისშემავალმონაცემებშიშედიან:

1) კომპიუტერულიქსელის (სისტემის) კონფიგურაცია;

2) უსაფრთხოებისპოლიტიკებიკომპიუტერულიქსელისაღვის (სისტემისათვის), რომლებიცგანისაზღვრებიანუფლებამოსილებათაანდაშვებისწესებისსიმრავლით;

3) ფორმირებადიგაფრთხილებები;

4) გარემონაცემთაბაზებიმოწყვლადობების, შეტევების, პლათფორმებისდაა.შ.;

5) შესაძლოდამრღვევებისპროფილები (დამრღვევებისმახასიათებლებისსიმრავლისსახით);

6) უსაფრთხოებისმატრიცისმოთხოვნილი (საჭირო) მნიშვნელობა (უსაფრთხოებისმოთხოვნათასიმრავლისსახით);

მდსქმკმუშაობისძირითადშედეგებსწარმოადგენენ:

1) მოწყვლადობებისგამოვლენა-აღმოჩენა;

2) შესაძლომარშუტები (გრაფები) შეტევებისდაშეტევებისმოზნები;

3) ამოკიდებულებებისერვისებსშორის;

4) ‘‘ვიწროადგილები’’ კომპიუტერულუსაფრთხოებაში’

5) შეტევებისკორექტირებულიხეები, რომლებიცდაფუძნებულიარიანცვლილებებზე, რომლებიცმოხდაქსელებში;

6) წინასწარმეტყველებადამრღვევისშემდეგინაბიჯებისა, რასაცადგილიაქვსმიმდინარესიტუაციებში;

7) უსაფრთხოებისმეტრიკები, რომლებიცშეიძლებაგამოყენებულიქნასკომპიუტერულიქსელის (სისტემის) დამისიკომპონენტებისუსაფრთხოებისსაერთოდონისშესაფასებლად;

8) შეტევებისდაკონტრზომებისშედეგები;

9) წინადადებებიუსაფრთხოებისდონისასამაღლებლად;

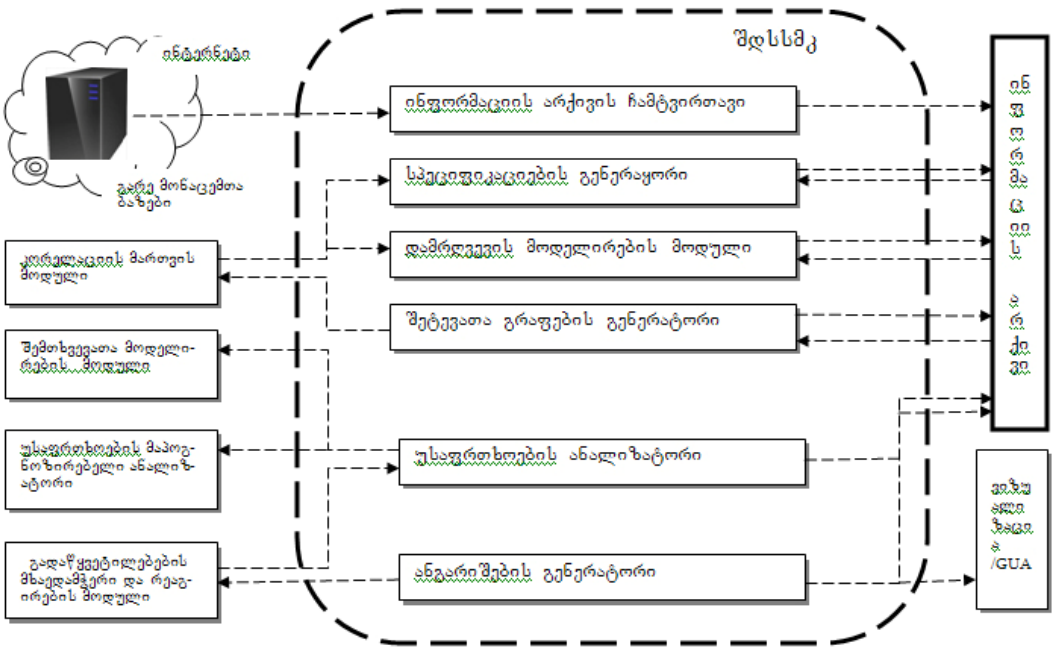
10) გადაწყვეტილებები, რომლებიცდაფუძნებულიარიანუსაფრთხოებისღონისძიებებზე, პოლიტიკებსადაინსტრუმენტებზე.

შდსქმკმუშაობსორრეჟიმში:

1) პროექტირების (კონფიგურირება), როდესაცხორციელდებაპროექტირებადაშიდაანალიზისაკვლევიქსელის (სისტემის). ესრეჟიმიარაარეალურიდროისრეჟიმი;

2) ექსპლუატაციის, როდესაცკომპონენტისგამოყენებახდებარეალურიდროისანმასთანახლორეჟიმში.

შდსქმკზოგადი (საერთო) არქიტექტურანაჩვენებიანახ.18.-ზე.




ნახ.18. შეტევების და დაცვის სისტემის ქცევის მოდელირების კომპონენტის არქიტექტურა.

დავახასიათოთ შდსქმკ ელემენტები.ინფორმაციის არქივის ჩამტვირთავი ახდენს გარე წყაროებიდან მოწყვლადობების, შეტევების, კონფიგურაციის, “ვიწრო ადგილების”, პლათფორმების და კონტრზომების მონაცემთა ბაზების ჩატვირთვას, აგზავნის რა მოთხოვნებს გარე მონაცემთა ბაზებში განხლებისა და ურთიერთმოქმედებისათვის მონაცემთა წყაროებთან.

სპეციფიკაციების გენერატორი გარდასახავს ინფორმაციას ქსელური მოვლენების, კონფიგურაციის და უსაფრთხოების პოლიტიკების შესახებ, რომლებსაც ღებულობს სხვა კომპონენტებისაგან შიდა წარდგენისათვის.

დამრღვევის მოდელირების მოდული განსაზღვრავს დამრღვევის ინდივიდუალურ მახასიათებლებს, მათი კვალიფიკაციის დონეს, საწყის ადგილმდებარეობას (შიდა ან გარედან შესვლის შესაძლო წერტილი და ა.შ.), უფლებამოსილებათა სიმრავლეს, უკვე განხორციელებული შესაძლო მოქმედებები (შეტევები), რომლებიც შეიძლება წინასწარ იქნას ამოცნობილი

მოვლენების და გაფრთხილებების და გასაანალიზებელი ქსელის ცოდნის საფუძველზე.

შეტევათა გრაფების გენერატორი აგებს შეტევათა გრაფებს დამრღვევის შემტევი მოქმედებების თანმიმდევრობების მოდელირებით გასაანალიზებელ კომპიუტერულ ქსელში, იყენებს ინფორმაციას სხვადასხვა ტიპის შესაძლო შეტევების შესახებ, სერვისების დამოკიდებულებებზე , ქსელის კონფიგურაციაზე და უსაფრთხოების გამოყენებულ პოლიტიკებზე. შეტევათა გრაფების გენერატორს შეუძლია ასევე ააგოს შეტევათა ტრასები, მოწყვლადობების, უცნობი მოწყვლადობების გათვალისწინებით, რომლებიც გამოიყენებიან სისტემის რესურსების კომპრომეტაციისათვის.

უსფრთხოების ანალიზატორი გვეხმარება გადაწყვეტილებების მიღებაში (შემოწმებული შემთხვევების და გაფრთხილებების, უსაფრთხოების შესაძლო მომავალი მოვლენების, კონტრზომების შესახებ), როლებიც აუცილებელია სხვა კომპონენტებისათვის. ის ახდენს ალბათური სახით იმიტირებას მრავალბიჯიანი შეტევებისა და ანგარიშობს სხვადასხვა კონტრზომების ღირებულებას და ეფექტურობას. მაგალითად, ის გენერირებს რთულ ობიექტებს და ანგარიშობს მათი უსაფრთხპების მეტრიკებს, რათა შეფასებულ იქნას უსაფრთხოების საერთო დონე და, შეძლებისდამიხედვით, გამოიმუშაოს რეკომენდაციები მათ მოსაშორებლად.

ანგარიშების გენერატორი აჩვენებს მოწყვლადობებს, აღმოჩენილს შდსქმკ მიერ, წარმოადგენს “ვიწრო ადგილებს”, გენერირებს რეკომენდაციებს დონის ამაღლებაზე და გამოყოფს სხვა რელევანტურ ინფორმაციას უსაფრთხოებისა.

5) გადაწყვეტილებების მხარდაჭერა და რეაგირება

კომპონენტი გადაწყვეტილებების მხარდაჭერა და რეარეაგირება (კგმრ) განკუთვნილია ადმინისტრატორის ინსტრუმენტარიების დამუშავებისა და რეალიზაციისათვის, რომელიც დაფუძნებულია ორგანიზაციის მოდელზე ORBAC. მოდელი ORBAC დღეისათვის

წარმოადგენს ყველაზე უფრო გავრცელებულ საშუალებას უსაფრთხოების პოლიტიკების აღწერისა. ასეთი მიდგომა კგმრ აგებისას საშუალებას იძლევა გაერთიანებულ იქნას უსაფრთხოების პოლიტიკები ორგანიზაციის სხვადასხვა სტრუქტურული კომპონენტების მესვეობით და ავტომატურად მოხდეს მათი კონფიგურაცია.

KKGRM შემოთავაზებული არქიტექტურა ორიენტირებულია Pყტჰონ ენაზე მის რეალიზაციაზე. ამ კომპონენტის ფუნქციონირების მიზანს წარმოადგენს ცემტრალიზებული ინფრასტრუქტურა უსაფრთხოების პოლიტიკების მართვისა, რომელიც დაფუძნებულია მოთხოვნებზე.

KKGRM საშუალებას იზლევა მოხდეს კონფიგურირება უსაფრთხოების პოლიტიკებისა გარე სისტემების, რომლებიც მოითხოვებიან შესაბამისი კომპონენტების (მაგალითად, APACHE, MYSQL, LDAP და ა.შ.) მიერ. ამ დროს ივარაუდება, რომ ადმინისტრატორს არ ჭირდება სხვა კომპონენტების რეკონფიგურაციის წესების ცოდნა, მას მოეთხოვება კგმრ მართვის ცოდნა.

KGMR-ის მეშვეობით ადმინისტრატორს ადვილად შეუძლია მოახდინოს წესებს შორის კონფლიქტების არსებობის იდენტიფიცირება. მაგალითად, ადმინისტრატორს არ შეუზლია აღმოაჩინოს ერთი და იგივე უსაფრთხოების პოლიტიკის ზემოქმედება გარე კომპონენტებზე, თუ ის ახდენს მათ კონფიგურაციას ხელით. მეორეს მხრივ, ამ კომპონენტების კონფიგურირებისას კგმს-ის დახმარებით სისტემა ავტომატურად აღმოაჩენს ამ კონფლიქტების არსებობას და ინფორმაციას აწვდის მათ შესახებ მანამ სანამ მოხდება უსაფრთხოების პოლიტიკის წესების გამოყენება.

უსაფრთხოების პოლიტიკების გაწყობა ხდება დინამიურად კონტექსტის მესვეობით, რაც საშუალებას აძლევს სისტემას უფრო სწრაფად მოახდინოს რეაგირება ნებისმიერ ცვლილებებზე (მაგალითად, SETWEVIS ან თავდასხმის მცდელობებზე). ამ დროს მკაფიოდ უნდა იყოს განსაზღვრული კონტექსტი და მონიტორინგის სისტემა, რათა სწორად მოგდეს კონტექსტში ცვლილებების გამოვლენა.

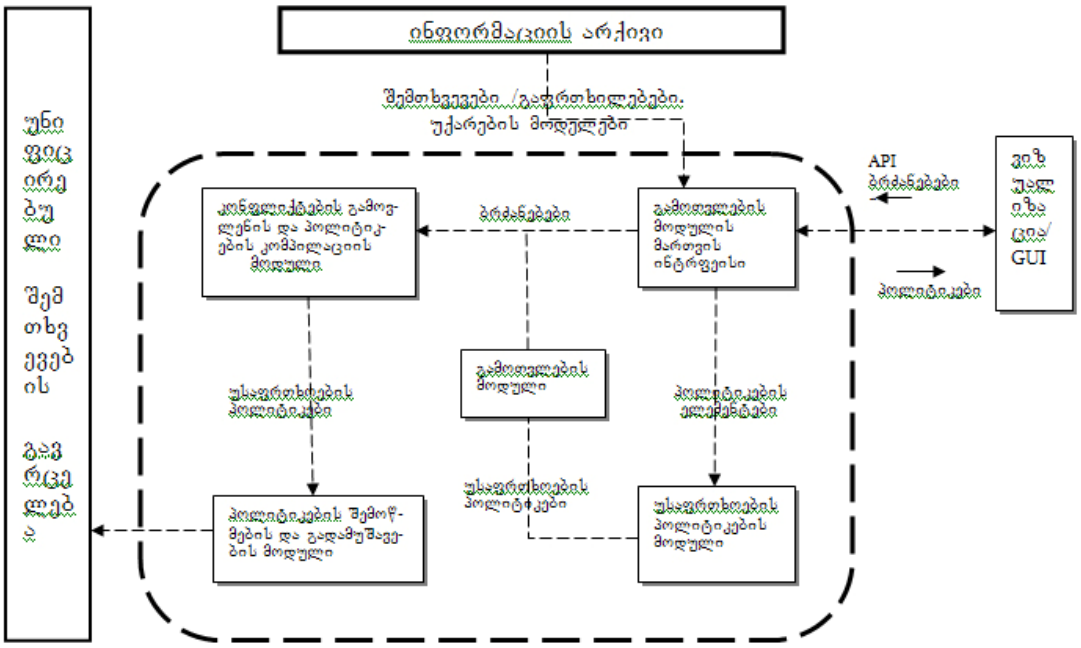
ყველა თავიდან გენერირებული უსაფრთხოების წესები შეიძლება ერთდროულად გამოყენებულ იქნას ყველა კომპონენტების მიმართ, რომლებიც დაკავშირებული არიან ორგანიზაციასთან. ამისათვის ახალი წესები ვრცელდებისნ კგმრ სისტემაში, ხოლო სხვა კომპონენტები ცვლიან თავიანთ კონფიგურაციას ამ წესებიდან გამომდინარე (ამ წესების შესაბამისად-მიხედვით).

KGMRსაშუალებას იძლევა მოხდეს წინასწარ დაყენებული კონფიგურაციების იდენტიფიკაცია და შენარჩუნებულ იქნას ინფორმაციის არქივში. Mოცემული ორგანიზაციის უსაფრთხოების ყველა პოლიტიკების ცოდნის საფუძველზე კგმრ შეუძლია ისინი შეამოწმოს და აღმოაჩინოს კონფლიქტები. ყოველთვის, როდესაც ადმინისტრატორი მოისურვებს ახალი პოლიტიკის კონფიგურირებას, კგმრ შეუძლია შეამოწმოს, ჯერ ერთი, რომ ეს პოლიტიკა ჯერ კიდევ არ არის შექმნილი, და, მეორე, რომ ახალი პოლიტიკა არ ქმნის რაიმე კონფლიქტებს სხვა არსებულ პოლიტიკებთან.

KGMR–ის შემოთავაზებული არქიტექტურა შეესაბამება კლიენტ-სერვერულ მოდელს, როგორც ეს ნაჩვენებია ნახ.19.-ზე. დავახასიათოთ მისი ელემენტები.

გამოთვლების მოდული კომპონენტისა მოქმედებს როგორც სერვერი, რომელიც უზრუნველყოფს დაშვების კონტროლის პოლიტიკების ცენტრალიზებულ ადმინისტრირებას. შიმრავლე აგენტებისა, რომლებიც შედიან გამოთვლების მოდულის შემადგენლობაში, ახორციელებენ კომპონენტების პოლიტიკების კონფიგურირებას, რომლებიც დაკავშირებული არიან KGMR-თან. პოლიტიკების ელემენტები შედიან KGMR-ში ინფორმაციის საცავიდან გამოთვლების მოდულის მართვის ინტერფეისის გავლით და შედიან უსაფრთხოების პოლიტიკების მოდულში. ბრძანებებით, რომლებიც გამომუშავდებიან გამოთვლების მოდულის მიერ და შემოდიან API და GUI ვიზულიზაციის მოდულებიდან, კონფლიქტების გამოვლენის და პოლიტიკების კომპილაციის მოდული ახორციელებს ვერიფიკაციას პოლიტიკისა და მათ გარდასახვას

(კომპილაციას) მოთხოვნილ (საჭირო) ფორმატში. პოლიტიკები, რომლებიც წარმოდგენილი არიან კომპილირებულ სახეში, პოლიტიკების შემოწმების და გადამუშავების მოდულის, რომლებიც მასში გადიან საბოლოო დამუშავებას, უნდა გადაეცეს მომხმარებლების მოწყობილობებს უნფიცირებული მოვლენების გავრცელების მექანიზმების მეშვეობით, რომელიც რეალიზებულია იდისს მონაცემთა გაცვლის სალტეში,




ნახ.19.

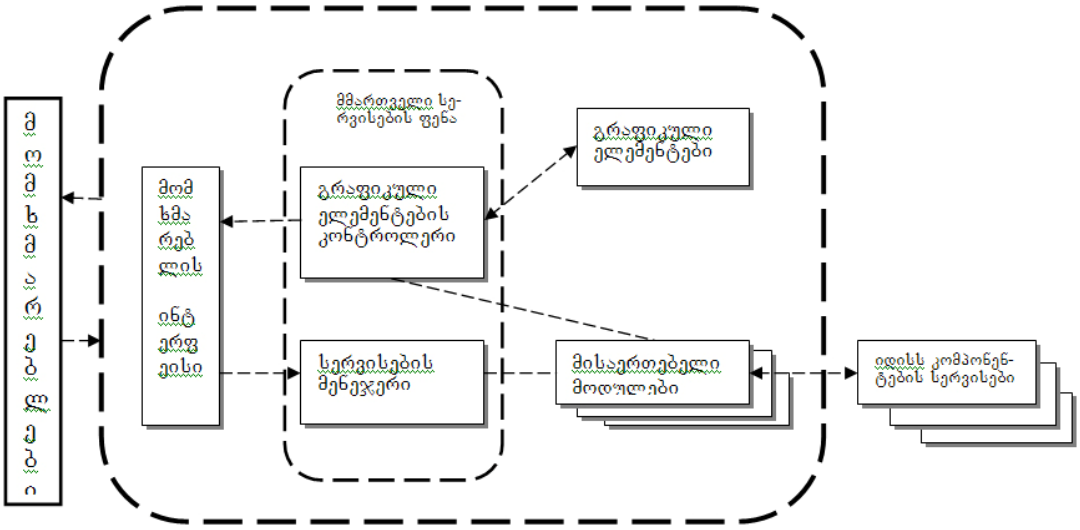
გადაწყვეტილებებისმხარდაჭერისდარეაგირებისკომპონენტისარქიტექტურა

6) ვიზუალიზაცია

ვიზუალიზაციამონაცემებისაუსაფრთხოებისმოვლენებისშესახებ, ასევემისიუზრუნველყოფისაწარმოადგენსსაკმაოდმნიშვნელოვანფუნქციასიდისს-საკმი-ში.

ამფუნქციისშესასრულებლადშემოთავაზებულიაგამოყენებულიქნასვიზუალიზაციისმოდული, რომლისარქიტექტურაცნაჩვენებიანახ. 8.-ზედამოიცავსამფენას: 1) მომხმარებლისინტერფეისს; 2) მართვისსისტემებისფენა; 3) გრაფიკულიელემენტებისფენა.

მომხმარებლისინტერფეისისგამოყოფაცალკედონედსაშუალებასიძლე
ვამხარდაჭერილსხვადასხვასახისგრაფიკულიინტერფეისისდამუშავებისმხა
რდაჭერა, დაწყებულიუბრალობრძანებისსტრიქონიდან,
დამთავრებულირთულიმრავალფანჯრიანიინტერფეისითმართვისსხვადასხ
ვაპანელებით.




ნახ.20. ვიზუალიზაციისმოდულისარქიტექტურა.

ივარაუდება, რომმონაცემები,
რომლებიცწარმოდგენილიუნდაიქნასგრაფიკულად,
გადაეცემიანშესაბამისსერვისს,
რომელიცაბრუნებსმზაშედეგსდანართისფორმაშიასახვისათვის.

ურთიერთმოქმედებისასეთიმექანიზმისაშუალებასიძლევადამალულ
იქნასდეტალები: ვინმოახდინავიზუალიზაციისპროცესისინიციირება –
მომხმარებელიანფუნქციურისერვისი,
რაცსაშუალებასიძლევაფენამმართველობითისევისებისაგანხილულიქნასრო
გორცმოდულივიზუალიზაციისკომპონენტისმართვისა.

სერვისებისმართვისფენაში,
გამომდინარემისმიერშესრულებულიფუნქციებიდან,
შეიძლებაგამოიყოსორიძირითადიკომპონენტი –
გრაფიკულიელემენტებისკონტროლერიდასერვისებისმენეჯერი.

გრაფიკულიელემენტებისკონტროლერირეალიზებასახდენსსტანდარ
ტულიინტერფეისისვიზუალიზაციისნაკრებთანსამუშაოდ,
რომელიცუზრუნველყოფსგრაფიკულინაკადისშექმნასდაშეჩერებას,
რომლებიცრეალიზდებაგრაფიკულიელემენტებისდონეზე.

სერვისებისმენეჯერიუზრუნველყოფსდაცვისინტელექტუალურისერ
ვისებისმიერტებას,
რომლებიცახდენენიდისსფუნქციონალურობისრეალიზაციას.
ასეთიგადაწყვეტასაშუალებასიზლევამოხდესიდისსკომპონენტებისდამუშა
ვება-შექმნაორგანიზაციებისმიერერტმანეთისაგანდამოუკიდებლად,
რაცწარმოადგენსცხად (უპირეტესობას)
ღირსებასერტობლივიკვლევითიპროექტისგანხორციელებისას.

გრაფიკულიელემენტებისდონემოიცავსბიბლიოთეკასაუცილებელი
გრაფიკულიპრიმიტივებისა – გრაფებს, ფურცლოვანდიაგრამებს,
ჰისტოგრამებს. ხეებისრუკებს, გრაფიკულრუკებსდაა.შ.
გრაფიკულიელემენტებიახდენენშემავალიმონაცემებისდამუშავებისრეალი
ზებას,
მათასახვასდამომხმარებლისურთიერთმოქმედებასუშუალოდშემომავალმო
ნაცემებთან.

აღნიშნულიმიდგომასაშუალებასიძლევაგრაფიკულიელემენტებისდა
სამუშავებლადგამოყენებულიქნასვიზუალიზაციისსხვადასხვატექნოლოგიე
ბი, მაგალითად, Java 3D, Flach, SVG დასხვა.

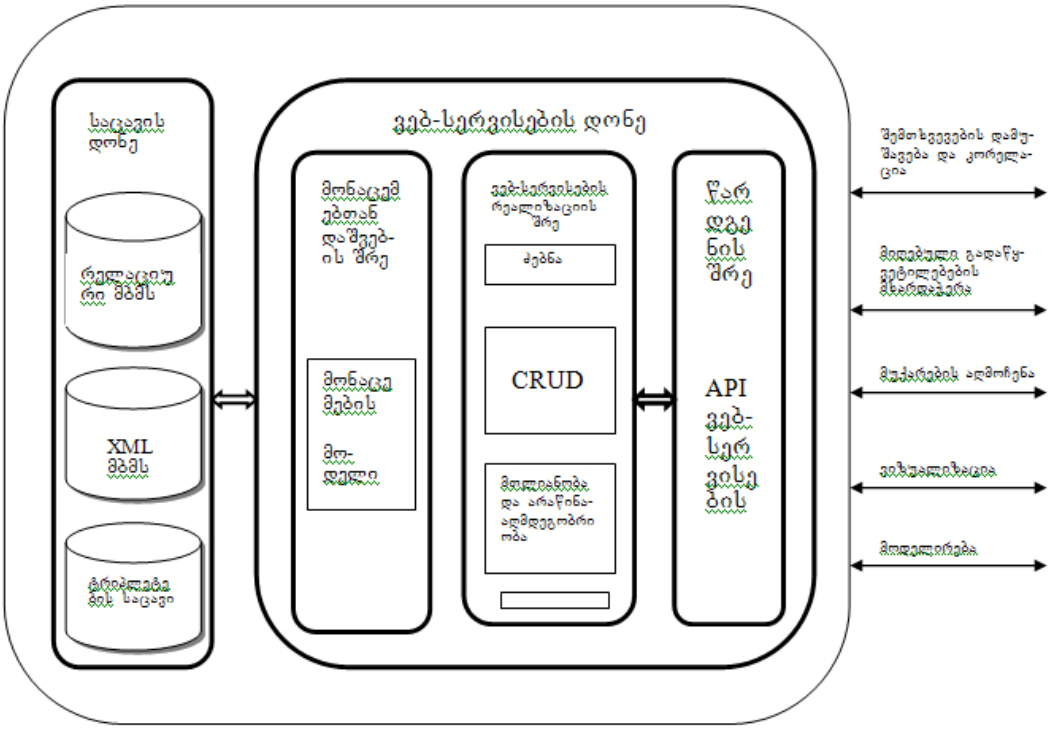
7) ინფორმაციულიარქივი

ინფორმაციულიარქივიწარმოადგენსიდისსსხვადასხვაკომპონენტები
სკროს-პლათფორმულიინტეგრაციისინსტრუმენტს.
მისირეალიზაციისსაფუძვლადშემოთავაზებულიასერვისულად-
ორიენტირებულიარქიტექტურა
(სოა),რომელიცწარმოადგენსგანაწილებულიინფორმაციულიგარემოსკონცე
ფციას,
რომელიცაერთიანებსმოდულებსპროგრამულიუზრუნველყოფისადადანარ

თების,

რომლებიცდაფუძნებულიარიანკარგადგანსაზღვრულინტერფეისებსადამათ შორისურთიერთმოქმედებებზე. ინფორმაციულიარქივისარქიტექტურა, რომელიცდაფუძნებულიასოა-ზე,

დამისიურთიერთმოქმედებაიდისსხვაკომპონენტებთან, ნაჩვენებიანახ.21-ზე.




ნახ.21. ინფორმაციულიარქივისარქიტექტურა.

ნახ.21.-ზეტერმინითCRUD

აღნიშნულიაერთობლიობაბაზურიოპერაციებისა: შექმნა (C), წაკითხვა (R),განახლება (U) დამოშორება (D).

ნახ.21.-დანჩანს,

რომინფორმაციულიარქივისარქიტექტურაგაყოფილიაორდონედ: საცავისდონედავებ-სერვისებისდონე.

საცავისდონემოიცავსრელაციურmbms, XML - mbmsდატრიპლერებისსცავს.

ამითმიიღწევაჰიბრიდულიმიდგომაუსაფრთხოებისშემთხვევებზემონაცემე

ბისშენახვისადმი, რომელიცთავისთავშიაერთიანებსყველაიმღონისძიებებს, რომლებიცდამახასიათებელიამონაცემებისწარმოდგენისბაზურიმოდელირე ბისათვისმონაცემთაბაზებშიდაუზრუნველყოფს, ერთისმხრივსაგნობრივიარისმოდელებისწარმოდგენასონტოლოგიისსახით, ხოლომეორესმხრივ – იდისს-შილოგიკურიდასკვნებისგამომუშავებასგადაწყვეტილებებისმიღებისათვის.

ვებ-სერვისებისრეალიზაციისდონეიყოფასამძირითადშრედ: დაშვებისშრე, ვებ-სერვისებისრეალიზაციისშრედაწარდგენისშრე.

მონაცემებთანდაშვებისშრეწარმოადგენსშუამავალსსაცავსადავებ-სერვისებისპროგრამულრეალიზაციებსშორის. ისახდენსინტერპრეტირებასუნივერსალურიმოთხოვნებისამონაცემებისამოს აღებად, მიღებასკლიენტებისდანართებისაგანენებისნოტაციებში, რომელიციყენებსmbms. მისგარდა, ამშრეზეგენერირებულიმოთხოვნებიინფორმაციულიარქივისადმიმოწმდებ იანცხრილებთანცხრილებისველებთანდაშვებისუფლებებისარსებობაზე. შაკმარისიუფლებებისარარსებობისასსისტემაახდენსმოთხოვნებისშეცვლასი სეთნაირად, რომმარეზულტირებელიარშეიცავდესაუცილებელმონაცემებს.

ვებ-სერვისებისრეალიზაციისშრესაშულებასიძლევამოხდესაბსტრაგირებაურთი ერთმოქმედებებისაერთანმრავალბიზნეს-ობიექტებსშორის, ნაკადებსადასერვისებსშორისშუალედურიინტერფეისის I მეშვეობით.

წარდგენისშრემოიცავსყველაელემენტებს, რომლებიცდაკავშირებულიარიანურთიერთმოქმედებითმომხმარებლისაიდ ისს-თან. ესმექანიზმიშეიძლებარეალიზებულიქნასბრძანებისსტრიქონისანტექსტური მენიუსსახით, მაგრამმისთვისუფრომისაღებიაგრაფიკულიინტერფეისი, რომელიცდამუშავებულიაროგორცთხელიკლიენტი (Windows, Swingდასხვა) ანდაფუძნებულიაHTML–ზე. წარდგენისშრისძირითადთავისებურებასწარმოადგენსასახვაინფორმაციისა

დაინტერპრეტაციაშემომავალისამომხმარებლობრძანებებისაიდისსმათიკონ
ვერტაციითშესაბამისოპერაციებშიდომენების (ბიზნეს-ლოგიკის)
დამონაცემებისმონაცემებისწყაროსკონტექსტში.
ესშრეუზრუნველყოფსმონაცემებისასახვას, შემთხვევებისდამუშავებას,
სამომხმარებლოინტერფეისს, სერვისუ თთ –მოთხოვნებს,
პაკეტურშესრულებასეს "ბრძანებისსტრიქონი" ტიპისდასხვაფუნქციების.

ამრიგად, აქწარმოდგენილიიდისსარქიტექტურაუზრუნველ-
ყოფსურთიერთკავშირსდაშეთანხმებულფუნქციონირებასინფორმაციისდაც
ვისძირითადიინტელექტუალურისერვისებისა,
რომლებიცაქტუალურიაკმი-თვის,
რომელთარიცხვსაცგანეკუთვნებიანსერვისებიმოდელებისმართვის,
გადაწყვეტილებათამხარდაჭერისდარეგისტრაციის,
უსაფრთხოებისსემთხვევებისშესახებმონაცემებისდამუშავების,
მათივიზუალიზაციისდაშენახვის.

იდისსრეალიზაციააქწარმოდგენილიარქიტექტურითწარმატებითიქნ
არეალიზებულიევროპულიკავშირისპროექტში MSSI,
რომლისმიზანიიყოდამუშავებაუსაფრთხოებისინფორმაციისდაშემთხვევებ
ისახალითაობისმართვისსისტემებისასერვისულიინფრასტრუქტურებისათვ
ის. თესტურდარგებს,
რომლებზეცხდებოდაიდისსაგებისასგამოყენებულიგადაწყვეტებისშეფასება
, წარმოადგენდნენკვიკლასსმიკუთვნებულისფეროები,
როგორებიცააკომპიუტერულიქსელიოლიმპიურითამაშებისუზრუნველყოფ
ისათვის, მობილურიკომპიუტერულიგადახდებისსისტემა,
განაწილებულიკომპიუტერულიქსელიმომსახურებებისტრანსნაციონალურ
იპროვაიდერისდაინფრასტრუქტურაჰიდროტექნიკურიაღჭურვილობებისა
(დამბები).

შედეგებმა,
რომლებიცმიღებულიიქნაიდისსარქიტექტურაშიგამოყენებულიგადაწყვეტი
ლებებისაპრობაციისას,

დაადასტურესმათიეფექტუროგადაშესაძლებლობამათიგამოყენებისაუფრო ფართოსიმრავლეშიკრიტიკულადმნიშვნელოვანიინფრასტრუქტურებისკლა სებისა.

## 2.3.კონფიდენციალური ინფორმაციის გაჟონვა მსოფლიოში და მეზობელ სახელმწიფოებში (რუსეთის მაგალითზე)

## 2016 წლის კვლევის შედეგები

წარმოდგენილი მონაცემები ეფუძნება კომპანიაSecurion Analytics-ის მიერ2016 წელს ჩატარებულ გამოკვლევებს.

კომპანიის აზრით 2015 წელს ინფორმაციის გაჟონვისაგან დაცვის ბაზარზე შექმნილი სურათი განაპირობა შემდეგმა ძირითადმა ფაქტორებმა: მობილური მუქარების გაზრდა, მიზანმიმართული შეტევები და ეკონომიკური კრიზისი. რაც შეეხება მობილურ მუქარებს, და შემდეგ მიზანმიმართულ შეტევებს, ამ ტრენდების ფორმირება ხდებოდა რამოდენიმე წლის განმავლობაში, და ყველაზე მკაფიოდ გამოჩნდნენ 2014, 2015 წლებში. ყველაზე უფრო გახმაურებულ ინციდენტების მაგალითად შეიძლება დავასახელოთ შეტევები Home Depot-ზე, რაც მსხვერპლს დაუჯდა სულ ცოტა 50 მილიონი დოლარი, უფრო მასშტაბური ხასიათი მიიღო Carbanak-მა, რომელიც შეეხო 100–ზე მეტ ბანკს ბევრ ქვეყანაში. დანაშაულებრივი დაჯგუფების Carbanak დანაშაულებრივი მოქმედებებით გამოწვეულმა ზარალმა შეადბინა 1 მილიარდ დოლარზე მეტი.

მობილური მოწყობილობებიდან მონაცემების კომპრომეტაციის რისკები არსებითად გაიზარდა ბოლო წლების განმავლობაში, თუმცა კომპანიები არა ერთი წელია უკვე ცდილობენ გადაწყვიტონ პრობლემები,

რომლებიც დაკავშირებულია ოფისის თანამშრომლების მობილიზაციასა და BYOD კონცეფციის გავრცელებასთან. გაჯეტები ანდროიდის პლათფორმაზე და iOS ხდებიან სულ უფრო პოპულარულები და საჭიროებენ კონტროლის ადეკვატურ ინსტრუმენტებს, მაგრამ მხოლოდ გამორჩეულ DLP-სისტემებს მობილური მოწყობილობებისა შეუძლიათ ამოიცნონ კონტენტი და თავიდან აიცილონ გაჟონვები, ისევე როგორც მაგიდის სისტემებში

კომპანიის აზრით 2015 წლის ყველაზე უფრო თვალისმომჭრელ ტრენდად შიგა მუქარების სფეროში შეიძლება აღიარებულ იქნას ყბადაღებული ეკონომიკური კრიზისი. მისი გავლენა აღმოჩნდა მართლა განმსაზღვრელი. რეალური შემოსავლების დაწევა, მასშტაბური შემცირებები, და მთლიანობაში არასტაბილური სიტუაცია შრომის ბაზარზე აისახა მრავალი კომპანიის თანამშრომლების განწყობილებასა და ქცევაში. საკუთარი მომავლის შიშიდან გამომდინარე, თანამშრომლებმა დაიწყეს მათთვის ხელმისაწვდომი კონფიდენციალური ინფორმაციის კოპირება. ძალიან ხშირად ეს ხდება ბოროტი განზრახვის გარეშე და იმის გაგების გარეშე თუ რისთვისაა ეს ინფორმაცია საჭირო. უბრალოდ ყოველი შემთხვევისათვის, მაგრამ არსებითად ზრდიან გაჟონვების რისკებს.

ეფექტი აღმოჩნდა იმდენად ძლიერი, რომ პროგნოზებისაგან განსხვავებით, DLP-სისტემების ბაზარი არა მარტო შეიკვეცა, არამედ გაიზარდა. კომპანიება, რომლებიც შეწუხებული იყვნენ კორპორაციული საიდულოებების გაჟონვით, დაიწყეს აქტიური ინვესტირება უსაფრთხოებაში, საკუთარი კონკურენტუნარიანობის ასამაღლებლად.

აქ ჩვენ წარმოვადგენთ კომპანიის მიერ2015 წელს ინფორმაციის გაჟონვასთან დაკავშირებით ჩატარებულ გამოკვლევებით მიღებულ შედეგებს, რომლებიც საინტერესოა როგორც კერძო კომპანიებისათვის, ასევე სახელმწიფო დაწესებულებებისათვის, რომლებიც ვალდებული არიან იზრუნონ მთელი ქვენის ინფორმაციული ინფრასტრუქტურის უსაფრთხოებაზე.

ჩატარებული გამოკვლევების მთავარი დასკვნების ასეთია:

– 2015 წელს დარეგისტრირებულია რეკორდული ზარალი ინფორმაციის გაჟონვისაგან – 29 მილიარდ დოლარზე მეტი.

– რუსეთი ინფორმაციის გაჟონვის მხრივ აღმოჩნდა მსოფლიოში მეოთხე ადგილზე (აშშ–ის, დიდი ბრიტანეთის და კანადის შემდეგ), აქ მხედველობაშია 2015 წელს მომხდარი 49 საქვეყნო–საჯარო ინციდენტი.

– ფზიკური პირების ფინანსური მონაცემები – ართ–ერთი ყველაზე მოთხოვნადი ტიპი ინფორმაციისა კიბერდამნაშავეების წრეში – სახეზეა 19,1% ინციდენტებისა.

– 2015 წელს ყველაზე უფრო ხშირად ხდებოდა ინფორმაციის გაჟონვა სახელმწიფო დაწესებულებებიდან, ბანკებიდან და საცალო ვაჭრობის საწარმოებიდან.

აქვე გვინდა მოკლედ წარმოვადგინოთ გამოკვლევების ის მეთოდოლოგია, რომლის მეშვეობითაც მიღებული იქნა ინფორმაციის გაჟონვებთან დაკავშირებული მონაცემები.

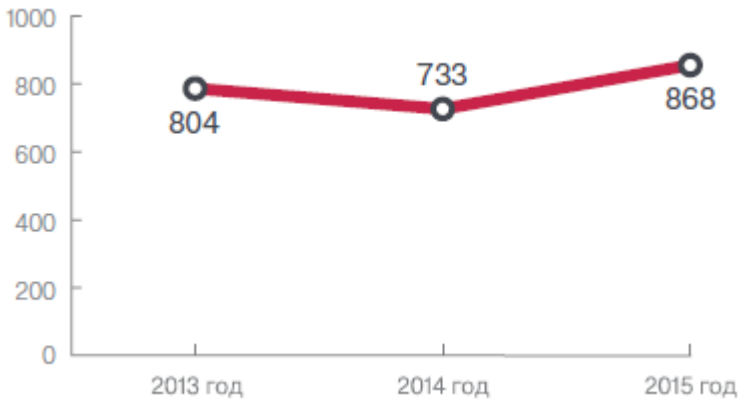
გამოკვლევების ძირითად საფუძველა წარმოადგენს ინფორმაციული უსაფრთხოების (იუ) ინცისენტების ბაზა, რომელთა მოძიება ხდება ღია წყაროებიდან (მასობრივი ინფორმაციის საშუალებები (მის)), აგრეთვე სერიოზული დახმარება მიიღება კომპანიის Securion იმ სპეციალისტებისაგან, რომლებიც ქმნიან პროექტებს კონფიდენციალური მონაცემების დაცვაზე/ინციდენტები ქრონოლოგიურად განაწილებული არიან კალენდარული წლების მიხედვით.

ინციდენტებით გამოწვეული პოტენციური ზარალის გაანგარიშება ხდება შიდა მეთოდიკით Securion Analytics, რომელიც ითვალისწინებს კომპრომეტირებული მონაცემების ტიპებსა და მოცულობას, დარგობრივ სპეციფიკას, ნაციონალური კანონმდებლობის თავისებურებებს, ასევე მარეგულირებელი ორგანოების მხრიდან რეაქციებს ინციდენტებზე, ასევე რეაქციებს მის–ის და საზპგადოების მხრიდან. ზარალის ექსპერტული შეფასება შეიძლება განსხვავდებოდეს მისი რეალური მნიშვნელობებისაგან როგორც ჯამის გაზრდის მიმართულებით, ასევე შემცირების

მიმართულებით. ინციდენტები, რომელთაგან მიღებული შეფასებითი ზარალი არ ღემატება 5 ათას დოლარს, არ განიხილებიან და ისინი სტატისტიკურ მონაცემებზე გავლენას არ ახდენენ.

2015 წელს კომპანიის ინციდენტების ბაზაში დაფიქსირდა 868 შემთხვევა, უფრო მეტი ვიდრე 2014 და 2013 წლებში (733 და 804 ინციდენტები შესაბამისად) (ნახ.22).

გამოყენებული მეთოდიკის ინციდენტების ბაზაში ხვდებისნ მხოლოდ ის შემთხვევები, რომლებიც საერთოდ ხდებიან ცნობილი. ეს განსაზღვრავს იმ ქვეყნების პროფილსაც, რომლებიც ყველაზე ხშირად ფიგურირებენ გაჟონვების შესახებ შეტყობინებებში. აშშ (71,9% დარეგისტრირებული ინციდენტებისა) ითვლება რეიტინგის უპირობო ლიდერად. შეერთებულ შტატებში ერთმანეთთან შეხამებულია მკაცრი კანონმდებლობა პრივატულობის დაცვის სფეროში და კეთილსინდისიერება თვით პერსონალური მონაცემების სუბიექტებისა. ამასთან ერთად, აშშ აქტიურად მოქმედებენ კიბერდამნაშავეების ჯგუფები, რომლებიც იყენებენ გაჟონილ მონაცემებს. ერთობლიობაში ეს იძლევა სინერგეტიკულ ეფექტს ინციდენტების საჯაროობისა და შესაბამის წილს საერთო სტატისტიკაში. (ნახ.2.).




ნახ.22.ინფორმაციული უსაფრთხოების დარეგისტრირებული შიგა ინციდენტების რაოდენობა

აშშ–ის შემდეგ აღნიშნულ სფეროში დომინირებენ თანმიმდევრობით დიდი ბრიტანეთი, კანადა, ავსტრალია, ახალი ზელანდია. რუსეთი, როგორც აღვნიშნეთ, გაჟონვათა რეიტინგში 49 დარეგისტრირებული ინციდენტების მიხედვით გადის მეოთხე ადგილზე (ასს–ის, დიდი ბრიტანეთის და კანადიშ შემდეგ). ცნობები გაჟონვების შესახებ სხვა ქვეყნებში დარგობრივ მის–ში ჩნდებიან ეპიზოდურად, ამიტომაც მათი წლი არ აღემატება ერთეულ პროცენტებს.

2015 წელს წინა წლებთან შედარებით (საუბარია 2013, 2014 წლებზე) სიტუაცია შეიცვალა. პირველად 2009 წლის შემდეგ სახელმწიფო დაწესებულებები გავიდნენ პირველ ადგილზე. ამ დროს, როგორც სტატისტიკამ აჩვენა, სახელმწიფო სექტორი სამეულიდან არც ერთხელ არ ამოვარდნილა.

საწარმოებმა საცალო ვაჭრობის სფეროდან თავიანთი წილი შეამცირეს 13,1%–მდე, მაგრამ მაინც წინანდებურად ჭანჭრობში იმყოფებიან. შეიძლება აღინიშნოს სემდეგი ტენდენცია: თუ ადრე კიბერდამნაშავეების შეტევათა უმეტესობა მიმართული იყო საფინანსო კომპანიების წინააღმდეგ, ამჟამად მათი ვექტორი შეიცვალა, რაც კატგად ჩანს მე–3 ნახაზზე.


ნახ.23. გაჟონვების გეოგრაფია

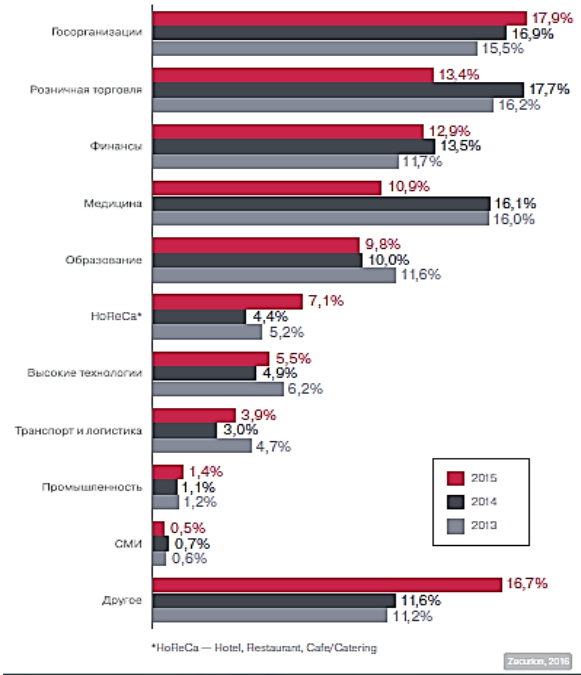
აქვე გვინდა წარმოვადგინოთ ის ზარალი, რად მოყვა 2015 წელს გაჟონვების ზრდას. კომპანიის მონაცემებით ამ ზარალმა გადააჭარბა 29

მილიარდ დოლარს. ადრეგაჟონვებისაგან მაქსიმალური წლიური ზარალი დაფიქსირდა 2013 წელს და შეადგინა 25,11 მილიარდი დოლარი.

კიბერდანაშაულობებით მიყენებული ზარალის ზრდაზე მიუთითებენ Ponemon Institute ანალიტიკოსებიც გამოკვლევებში „2015 Cost of Cyber Crime Study“. აშშ–ში კიბერდანაშაულობების საშუალო ზარალმა შეადგინა 15,42 მილიარდი დოლარი, რაც 20%–ით არემატება წინა წლების მაჩვენებლებს.

2015 წელს კომპრომეტირებულ მონაცემების ტიპებს შორის , ყველაზე უფრო (თითქმის ორჯერ) გაიზარდა ფიზიკური პირების საფინანსო ცნობების წილი. ძალიან ხშირად ასეთი ინფორმაციის გადინება ხდება მიზანმიმართული შეტევების შედეგად. ფიზიკური პირების ფინანსური ცნობები შავ ბაზარზე ადვილად მონერიზირდება და ყველაზე უფრო მოთხოვნადია. მონაცემები, რომელთა გაყიდვაც ძნელია, არ წარმოადგენენ მაღალი დონის კიბერდამნაშავეების ძირითად მიზანს და მათთან ხვდება, მაშინ თუ ადვილად ხელმისაწვდომია ან ინახება მთავარ სამიზნესთან ერთად.

ზევით უკვე მივუთითეთ, რომ მოხდა შეტევათა ვექტორის გადანაცვლება საფინანსო კომპანიებიდან საცალო ვაჭრობის კომპანიებზე. კიდევ ერთი ტენდენცია – ესაა ცალკეულ მომხმარებლებზე შეტევათა წილის შემცირება კორპორაციებზე შეტევებზე სასარგებლოდ. მიუხედავად იმისა, რომ კომპანიების დაცულობის დონე მთლიანობაში მაღალია,

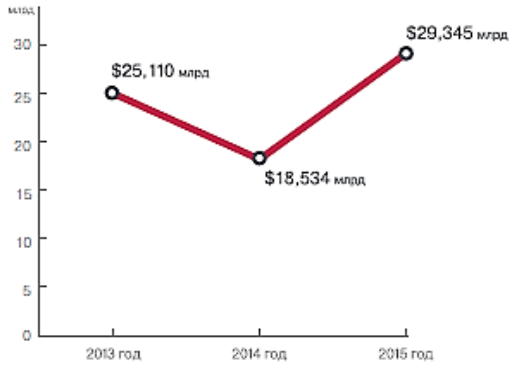


კიბერდამნაშავეების მიერ მირებული ინფორმაციის მოცულობა თურმე ბევრად მეტია, ხოლო ერთი ადამიანის მიერ მონაცემების მიღების შრომატევადობა შეუდარებლად დაბალია. უნდა აღინიშნოს, რომ სხვადასხვა მიზეზების გამო კიბერდამნაშავეები წინანდებურად ფართედ იყენებენ შეტევებს ინდივიდუალურ მომხმარებლებზე.

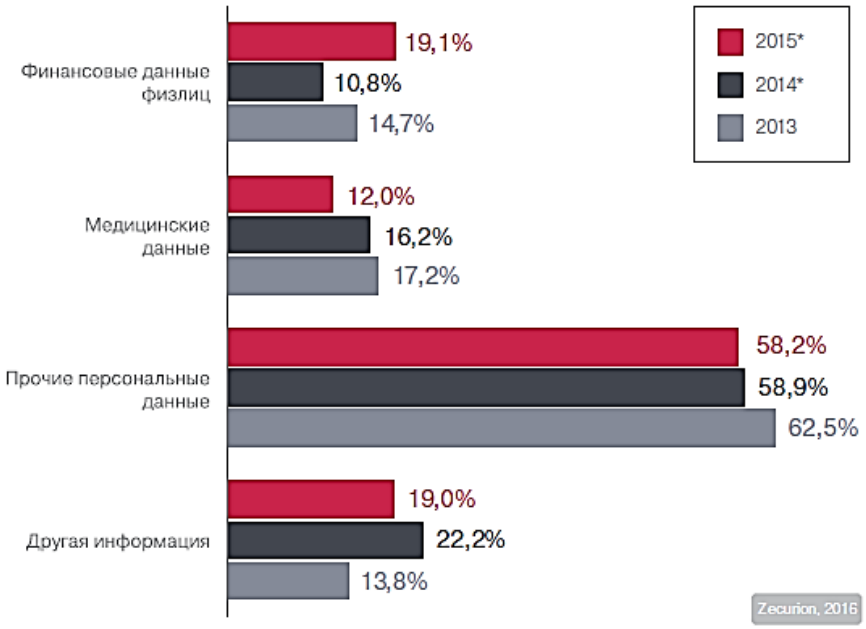
ნახ.24. გაჟონვების დარგობრივი სპეციფიკა

აქვე გვინდა წარმოვადგინოთ მონაცენების, ინფორმაციის გაჟონვების გამომწვევი მიზეზები.

უნდა აღინიშნოს, რომ სტატისტიკაში გამოიკვეთა საკმაოდ მოულოდნელი ციფრები ინსაიდერების განზრახვების არსებობასთან დაკაშირებით (ნახ.25.). მიუხედავად იმისა, რომ სახეზეა მიზანმიმართული შეტევების გაზრდის ტენდენცია, მათ შორის თანამშრომლების მონაწილეობით კომპანიის შიგნით, მთლიანობაში 2015 წელს წინასწარგანზეახული გაჟონვები ფაქტიურად არ შეცვლილა 2014 წელთან შედარებით.




ნახ.25. ინფორმაციის გაჟონვით გამოწვეული ზარალი

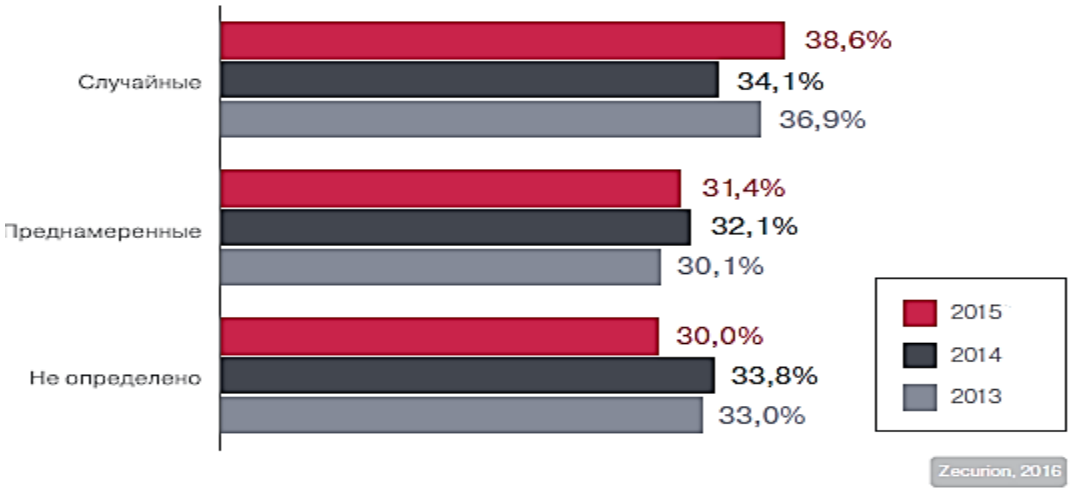



ნახ.26. როგორი მონაცემების გაჟონვა ხდება.

ამასთანავე, შემთხვევითი გაჟონვები მხოლოდ რამოდენიმე პროცენტით უსწრებენ წინ მიზანმიმართულებს. ხოლო ზარალი გაჟონვებისაგან, რომლებიც განხორციელდა წინასწარგანზრახულად, აშკარად მეტია. ანუ, ნაკლები რაოდენობის ბოროტგანზრახულმა ინსაიდერებმა მიაყენეს უფრო მეტი ზარალი კომპანიებს, ვიდრე მეტი რაოდენობის დაუდევარმა, გულგრილმა თანამშრომლებმა.

გაჟონვის არხებთან დაკავშირებით 2015 წელს ყველაზე უფრო შესამჩნევია შემდეგი ცვლილებები: გაჟონვების წილის გაზრდა მობილური დამგროვებლების მეშვეობით (6,4%–დან 11,6%–მდე) და დაქვეითება (ზუსტად ორჯერ) ქაღალდის დოკუმენტებთან დაკავშირებული ინციდენტებისა. გაჟონვათა წილი მობულური დამგროვებლებიდან 2012 წლიდან უცვლელად მცირდებოდა, და 2015 წელს ნახტომისებრი ცვლილება ამ სფეროში უფრო გამოსვლაა საერთო ტენდენციიდან. იმის გათვალიწინებით, რომ ამ სფეროში ინფორმაციული უსაფრთხოებაში გათვითცნობიერება და ფართომასშტაბიანი დანერგვა დაშიფვრის

საშუალებებისა, უნდა ვიფიქროთ, რომ შემდეგი ზრდა გაჟონვებისა ნაკლებად მოსალოდნელია.



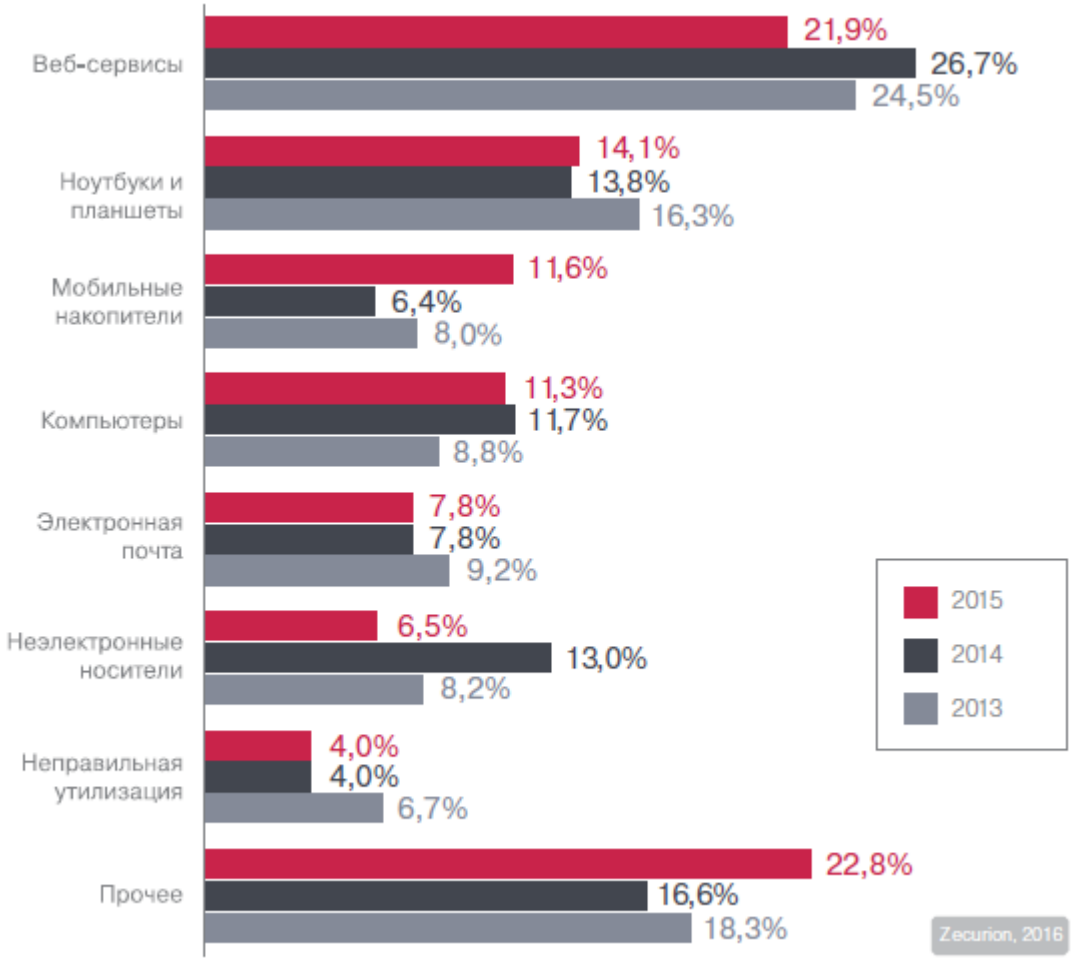

ნახ.27. განზრახვების არსებობა ინფორმაციის გაჟონვაში

მეორე ცვლილება შეიძლება ავხსნათ იმით, რომ კომპანიები ინფორმაციის დაცვაში გახდნენ უფრო ორგანიზებულები, და მნიშვნელოვნად შემცირდა კომპანიებში ქაღალდზე დოკუმენტბრუნვა. მიუხედავად ამისა, თუნდაც გადასვლა სრულად ელექტრონულ დოკუმენტბრუნვაზე ვერ გამორიცხავს მოცემული კლასის გაჟონვებს. აქ ბრალი მიუძღვის – წინა წლების უზარმაზარ არქივებს. ერთ–ერთი გავრცელებული კეისი – ესაა დოკუმენტების დაკარგვა, მათ შორის სათავსოების რემონტისას, ოფისის შეცვლისას, ან გაკოტრებისას. გასაგებია, ბოლო შემთხვევაში გაჟონვების შედეგები კომპანიისათვის არც ისე მნიშვნელოვანია, მაგრამ კომპრომეტირებული დოკუმენტების მფლობელებისათვის (კლიენტები, კომპანიის კონტრაგენტები) რისკი შეიძლება იყოს მაღალი.

ვებ–სევისი – ისევ და ისევ გაჟონვების ყველაზე პოპულარული არხია. მთელი ოთხი წლის განმავლობაში ინტერნეტის გავლით გაედინება ყველაზე მეტი კონფიდენციალური ინფორმაცია. მომხმარებლების მონაცემები და კლიენტების ბაზები – ტექნოლოგიის განვითარების გამო

ინსაიდერებს ვებ–ის მაშვეობით შეუძლიათ გააერთიანონ დიდი მოცულობის ინფორმაცია.

პრაქტიკულად არ შეცვლილა წილი გაჟონვებისა მობილური კომპიუტერებიდან და პლანსეტებიდან (14,1% 2015წელს), ელექტრონული ფოსტიდან (7,8%), მატარებლების არასწორი უტილიზაციის შედეგად (4%). ამ დროს 2012 წელს 8%–ზე მეტი ყველა გაჟონვებისა ხდებოდა ინფორმაციის განადგურების დაუმუშავებელი პროცედურების გამო. გამოდის, რომ სამი წლის შემდეგ წილი შემცირდა 2–ჯერ, რაც მიუთითებს ინფორმაციულ უსაფრთხოებაში მეტ გარკვეულობასა და ცოდნაზე. ნახ.30.–ზე მოცემულია გაჟონვების არხები და მათი სტატისტიკა 2013, 2014, 2015 წლებში.




ნახ.28. გაჟონვების არხები

წარმოდგენილი სტატისტიკური მონაცემებიდან გამომდინარე გვინდა წარმოვადგინოთ მოკლე შემაჯამებელი დასკვნები და პროგნოზი.

მიუხედავად იმისა, რომ 2013–2914 წლებში სახეზეა დარეგისტრირებული ინფორმაციის გაჟონვების რაოდენობა და თვით ზარალის შემცირებაც 25 მილიარდი დოლარიდან 18,5 მილიარდ დოლარამდე, 2015 წელს ჯამური შედეგები ცხადად მიგვანიშნებენ, რომ კორპორაციული ინფორმაციის გაჟონვების მოცულობა და კომპანიების დანაკარგები მომავალში იზრდებოდნენ იქნება. ამაზე მიუთითებენ სულ უფრო მეტი გახვეწილობა მეთოდებისა, რომლებსაც იყენებენ კობერდამნაშავეები, ასევე კომპანიების და მათი თანამშრომლების გულგრილობა ინფორმაციის დაცვის საკითხებში.

მაგრამ, ძნელია ცალსახად ვაღიაროთ მთავარ დასკვნად ის ფაქტი, რომ გაჟონვების რაოდენობამ და მათგან მიღებულმა ზარალმა მიაღწია ისტორიულ მაქსიმუმს. ბევრად უფრო მნიშვნელოვანია გაჟონვების ვექტორის გადანაცვლება ფიზიკური პირების საფინანსო მონაცემების მხარეს. ეს ინფორმაცია, რომელსაც გააჩნია მაღალი ღირებულება, მისი ცოცხალ ფულად გადაქცევა შედარებით ადვილად და სწრაფადაა შესაძლებელი. მაგრამ უფრო ხშირად მსგავსი მონაცემები კიბერდამნაშავეების ხელში ხვდება არა თვითონ მფლობელებისაგან, არამედ მსხვილი კომპანიებიდან, პიველ რიგში, საფინანსო ორგანიზაციებიდან და ცალობრივი ვაჭრობის საწარმოებიდან, მიზანმიმართული შეტევებით ან ინფორმაციის შემთხვევითი გაჟონვების შედეგად.

2015 წლის გაჟონვების ანტირეიტინგში მოხვდნენ გარდა საფინანსო კომპანიების და სცალო ვაწრობის მაღაზიებისა ასევე სახელმწიფო დაწესებულებები. თანაც ამ წელს სახელმწიფო სექტორი, პირველად მრავალი ხნის შემდეგ, გახდა ლიდერი. ბოლო წლების ტრენდების საშუალებას იძლევა იმის მტკიცებისა, რომ მომავალში სახელმწიფო დაწესებულებები დარჩებიან მოქალაქეების პერსონალური მონაცემების

მასობრივი გაჟონვებში მთავარი დამნაშავეების რიცხვში. ეს უბედურება დამახასიათებელია სახელმწიფოების უმეტესობისათვის, რომლებიც მოხვდნენ მოცემულ ანგარიშში. ინციატივები და ობიექტური მიზეზები, რომელთა გამოც ინციდენტების რიცხვი შეიზლება შემცირებულიყო, მოცემულ მომენტში უბრალოდ არ არსებობენ.

ამასთან ერთად, ინციდენტების სტატისტიკა მიუთითებს იმაზე, რომ გაიზარდა პროცენტი გაჟონვებისა რტული სქემების გამოყენებით, მათ შორის სოციალური ინჟინერიის ელემენტების, ჩანერგილი ინსაიდერების და ინფორმაციის გადაცემის სხვადასხვა არხებისა. ეს ნიშნავს, რომ კომპანიების უსაფრთხოების სამსახურებს მოუწევთ წინ აღუდგნენ ძალზე სერიოზულ გამოწვევებს, რომლებიც განსხვავდებიან ტიპიური სქემებისაგან, რომლებიც შექმნილი იყო ბოროტგანმზრახველების მიერ წინა წლებში. კიბერდამნაშავეები ერთად იყენებენ შეტევების რამოდენიმე ვექტორს, რაც საშუალებას იძლევა გამოვლენილ იქნას სუსტი ადგილები ყოველ ცალკეული მიმრთულებით, გამოიყენონ და შეუხამონ აღმოჩენილი ხვრელები, მაქსიმალური ზიანის მიყენებით. იმისათვის, რომ ეფექტურად წინ აღუდგნენ მსგავს სეტევებს, ინფორმაციული უსაფრთხოების სპეციალისტებს უწევთ იმოქმედონ ორგანიზაციასთან ერთად, დამოუკიდებლად აღმოაჩინონ და დახურონ არსებული ხვრელები (გარღვევები). მაგრამ ხშირად ასეთი რამ შეუზლებელია ფიზიკურად, ვინაიდან რესურსები (ადამიანური და მატერიალური) შეზღუდულია. ასეთ პირობებში მთავარი ძლისხმევა მიმართულია ყველაზე უფრო ღირებული რესურსების დაცვაზე. ეს კი ძალზე მნიშვნელოვნად აქცევს კორპორაციული ინფორმაციის კლასიფიკაციას; ამ ასპექტში თვით კლასიფიკაცია ითვლება უმნიშვნელოვანეს ეტაპად ინფორმაციული უსაფრთხოების უზრუნველყოფაში.შეიძლება იმედი ვიქონიოთ, რომ ცალკე პერსპექტივაში ტექნოლოგიის განვითარება საშუალებას მოგვცემს საკმარისად ეფექტურად იქნას დაცული კორპორაციული მონაცემების მთელი მოცულობა. მაგრამ ჯერ–ჯეროთ ყოველ წელს იზრდება კლასიფიკაციის როლი,, ხოლო

ინფორმაციული უსაფრთხოების დანაყოფების შესაძლებლობები მიმართულია ყველაზე მნიშვნელოვანი კორპორაციული რესურსების დაცვაზე.

გახმაურებული ინფორმაციის გაჟონვები რუსული კომპანიებიდან Securion Analytics-ის მონაცემებიდან გამოვყოფთ ცნობილ კომპანიებში დაფიქსირებულ ინციდენტებს.

### Mail.ru

როგორც ანგარიშშია აღნიშნული, Mail.ru უკვე პირველად როდი ხვდება გახმაურებული გაჟონვების სიაში. მაგრამ თუ ადრე ეჭვი ჰქონდათ მომხმარებლების მონაცემების გაჟონვებში, 2015 წელს, შესაძლებელია, კონკურენტებთან გაჟონა კონფიდენციალურმა ინფორმაციამ ახალი მომსახურებების შემოტანასთან დაკავშირებით. შედეგად Mail.ru–მ და იანდექსმა ერთ დღეს დაანონსეს ეკაუნტებთან ორფაქტორიანი აუტენტიფიკაციის გაშვება. თანაც იანდექსმა თავისი პრეს–რელისი დააგზავნა კონკურენტებზე რამოდენიმე საათით ადრე.

ოფიციალური პირების კომენტარებიდან გამომდინარე, Mail.ru გადინების შესახებ ზუსტ ინფორმაციას არ ფლობს, მაგრამ თვით დამთხვევის ფაქტი ბადებს ბევრ შეკითხვებს. Mail.ru–ს ვიცე–პრეზიდენტმა ანნა არტამონოვამ თავის ფეისბუკზე გამოაქვეყნა წერილი, სადაც აღნიშნავს, რომ „როგორ მოხდა ისე, რომ იმ დღეს როდესაც დანიშნული იყო რელიზი, ვიღაცამ დაგვასწრო სამი საათით ადრე – კარგი შეკითხვაა, მაგრამ არ მინდა ვინმეზე ეჭვის მიტანა“.

აღსანიშნავია, რომ ეს არაა ერთადერთი შემთხვევა . ჯერ კიდევ 2012 წელს, ორივე ინტერნეტ კომპანიამ ერთ დღეში გაუშვეს განახლებული სერვისი ტანსაცმლის არჩევისა მსგავსი ფუნქციონალით. უკვე მაშინ ბანალური თანხვედრა მიჩნეულ იქნა ძალზე გასაკვირ სცენარად.

### ბანკი „სანკტ–პეტერბურგი“

ყველაზე მასშტაბური გადინება საკრედიტო ორგანიზაციის კლიენტების შესახებ მონაცემებისა მოხდა 2015 წლის გაზაფხულზე, და

ყველაფერი ეს ცნობილი გახდა იმავე წლის ივლისში. ბანკი „სანკტ–პეტერბურგის“ წარმომადგენლების მონაცემებით ბოროტგანმზრახველების ხელში მოხვდა რამოდენიმე ათასი კლიენტის სახელები, ანგარიშების ნომრები, ბარათების ნომრები. ასევე ბანკი დაჟინებით მიუთითებს იმაზე, რომ არც საკრედიტო ორგანიზაციას, არც მის კლიენტებს შეტევების შედეგად რაიმე ზარალი არ მიყენებიათ, ხოლო თვით გადინებას უწოდებს „მართვადს“. სავარაუდოდ, დაუშვეს ინფორმაციის გადინება, რათა ადვილად მომხდარიყო გასვლა ბოროტგანმზრახველებზე. ამასთან ერთად, კლიენტებს შესთავაზეს უფასოდ მიეღოთ კომპრომეტირებული ბარათების შემცვლელი ახალი ბარათები.

თვითონ კიბერდამნაშავეები მოითხოვდნენ მათთვის 29 მილიონი რუბლის გადახდას, წინააღმდეგ შემთხვევაში იმუქრებოდნენ პრესაში გამჟღავნებით, საჩივრებით მარეგულირებელ ორგანოებში და საერთაშორისო საგადასახადო სისტემებში Visa და Mastercard. ბანკი არ დაემორჩილა გამომძალველების მუქარებს და თვითონ დაასწრო მათ მოვლენების შესახებ პუბლიკაციებით მასობრივი ინფორმაციის წყაროებში (მიწ). რეალური ზარალი ინციდენტებისაგან უცნობია, თუმცა შეიძლება ვივარაუდოთ, რომ ბანკისათვის სარეპუტაციო რისკები იყო საკმაოდ მაღალი. შეტყობინებები ბანკის უსაფრთხოების სისტემის მოწყვლადობებზე გაჩნდა დარგობრივ, რეგიონალურ და ფედერალურ მიწ–ებშიც კი, და, შესაძლებელია, გავლენა იქონიეს პოტენციური კლიენტების გადაწყვეტილებებზე, ასევე დაბლა დაეწია მიმდინარე კლიენტების ლოიალურობა.

### იჟევსკის ავტოქარხანა

გაჟონვა ახალი პროდუქტების ფოტოსურათების და მახასიათებლების მათი ოფიციალურად გამოჩენამდე არც ისე დიდი ხნით ადრე იქცა ნორმად საზღვარგარეთის ბაზარზე.. 2015 წელს ამ მხრივ გამოირჩეოდნენ რუსეთის ინსაიდერებიც. მათ გადაიღეს „საიდუმლო“

სურათები ახალი სერიული ავტომობილის – ლადა ვესტასი და მიყიდეს 200 რუბლად ინტერნეტ ბლოგერს.

აქვე უნდა აღინიშნოს, რომ საწარმოს უსაფრთხოების სამსახურს ეს ინვიდენტი არ დაუტოვებია უყურადღებოდ, ოპერატიულად ჩაატარა გამოძიება მომხდარი ინციდენტის, იპოვა და დასაჯა დამნაშავეები.ინციდენტთან დაკავშირებული აღმოჩნდა საწარმოს ორი თანამშრომელი და გარე მომწოდებლის წარმომადგენელი. შედეგად ერთი თანამშრომელი, რომელმაც გადასცა ფოტო, დათხოვნილი იქნა, მეორეს გამოეცხადა საყვედური, ხოლო გარე მომწოდებლის წარმომადგენელს შეეზღუდა დასვება ქარხანაში.

აღნიშნულმა ინციდენტმა მიიღო ფართო გახმაურება, თუმდა ქარხნის ზარალი არც ისე ცხადია. აქვე უნდა აღინიშნოს, რომ ფოტოგრაფიების მსგავსი გადინება მიზანშეწონილია შეიზღუდოს ორგანიზაციული ზომების გამოყენებით.

## Topface

2015 წლის იანვარში კიბერდამნაშავეებისათვის ერთ–ერთ ფორუმზე აღმოაჩინეს ბაზა მომხმარებლებისა რუსული სერვისის Topface–გაცნობა. თვით სერვისი საკმაოდ პოპულარულია რუსეთში და საზღვარგარეთაც. დაფიქსირდა ის ფაქტი, რომ 20 მილიონი აკაუნტიდან, მხოლოდ ნახევარი ეკუთვნის მომხმარებლებს რუსეთიდან.

მიუხედავად იმისა, რომ ბაზაში დაფიქსირებული იყო მხოლოდ ელექტრონული მისამართები და ფარული სახელები მომხმარებლების, კიბერდამნაშავეები ხალისიანად ყიდულობენ მსგავს ინფორმაციას არც ისე დიდ ფასად – სპამების, ფიშიგური წერილების დასაგზავნად ან აკაუნტების შესამოწმებლად სხვა სერვისებში.

გაჟონვების შესახებ კომპანიაში გაიგეს მიწ–დან, ოღონდ ოპერატიულმა რეაქციამ ინციდენტებზე და მისმა გამოძიებამ მოიტანა კატგი შედეგები. Topface–ის მფლობელებს შეეძლოთ დაკავშირება

ხაკერთან, რომელმაც გაყიდა მონაცემები, მაგრამ არ შეეცადნენ მის ჩაბარებას სამართალდამცავი ორგანოებისათვის, მაგრამ მოილაპარაკეს თანამშრომლობაზე. ხაკერმა უარი თქვა მიღებული მონაცემების გავრცელებაზე და მიიღო პრემია მოწყვლადობების აღმოჩენაზე. ამის გარდა, მხარეები შეთანხმდნენ ურთიერთთანამშრომლობაზე სერვისების უსაფრთხოების საკითხებში.

### მაღალი რანგის ჩინოვნიკების პირადი მონაცემების გაჟონვა

2015 წლის შემოდგომაზე სანქცირებული სიების გაფართოების მორიგი რაუნდისას გოსდუმის დეპუტატებმა დასვეს შეკითხვა, როგორ მიიღეს უკრაინელებმა რუსეთის მოქალაქეებმა (მათ შორის მაღალი თანამდებობის პირების), პასპორტების ნომრაბი, მისამართები, და ა.შ.სანქცირებული სიების ცალკეულმა მონაწილეებმა დაადასტურეს გამოქვეყნებული მონაცემების ნამდვილობა. ამ დროს სიებში აღმოჩნდა იმ ადამიანების მონაცემებიც, რომლებიც უკრაინის ტერიტორიაზე არასოდეს არ ყოფილან.

თუ რამოდენიმე წლის წინ რუსეთის მოქალაქეების საპასპორტო მონაცემების პოვნა  შედარებით ადვილად შეიძლებოდა, სახელმწიფო დაწესებულებების და უწყებების მრავალრიცხოვანი ბაზებიდან ერთ–ერთის შესყიდვით.მაგნიტური დისკები ბაზებით ფართოდ იყიდებოდა მიწისქვეშა გადასასვლელებსა და რადიობაზრობებზე. ამჟამად გართულებყკია ბაზების გაყიდვა, ასევე დაიწია მათი განახლებების სიხშირემ. ზოგიერთი არხები საერთოს დაიხურა. მიუხედავად ამისა, პერიოდული დაუდევარი გაჟონვები ფაქტიურად ხაზს უსვამენ ამ მიმართულებით გაწეულ მუშაობას.

2015 წლის მარტის ინციდენტი – სახელმწიფო შესყიდვების პორტალზე აღმოჩენილი იქნა ფედერაციის საბჭოს წევრების საპასპორტო მონაცემები. ინფორმაციის განთავსება პარლამენტის ზედა პალატის აპარატმა სენატორების უბედური შემთხვევებისაგან და ავადმყოფობის დაზღვევის სხვა საკონკურსო დოკუმენტებთან ერთად. თუმცა თვითონ

პოლიტიკოსები ინფორმაციის გახსნაში რაიმე საფრთხეს ვერ ხედავენ, დაშვება მონაცემებთან რჩება ღია.

### იანდექსი

კომპანია იანდექსმა კინაღამ დაკარგა თავისი ნოუ–ჰაუ თანამშრომლის არაკორექტული მოქმედებების გამო. მიუხედავად იმისა, რომ ისტორია დამთავრდა მშვიდობიანად, რისკები იყო ძალიან მაღალი. გაჟონვა ნამდვილად მოხდა; ინსაიდერმა შეძლო წამატებით მოეხდინა ფლეშზე კოპირება მაძიებლის ალგორითმის და სხვა მონაცემების.

ინსაიდერი შეეცადა გაეყიდა მოპარული მონაცემები 25 ათას დოლარად და 250 ათას რუბლად, მაგრამ ის დაკავებულ იქნა სპეც.სამსახურის თანამშრომლების მიერ. ამ დროს თვით იანდექსში საწყისი კოდის ღირებულება შეაფასეს რამოდენიმე მილიარდ რუბლად, სამაძიებლო პროგრამა ესაა ესაა კომპანიის ძირითადი სერვისი.

ინსაიდერი მიღებული თანხით გეგმავდა საკუთარი ბიზნეს–პროცესის გაშვებას. თუმცა წარმოიშვა პრობლემა მოპარული ინფორმაციის გაყიდვასთან დაკავშირებით. მყიდველებს იანდექსის ყოფილი თანამშრომელი ეძებდა ნაცნობების მეშვეობით და სპეციალიზირებულ ხაკერულ ფორუმებზე, სწორედ აქ ჩაუვარდა ის ხელში ოპერატიულ თანამშრომლებს.

### ადამიანური ფაქტორი

იუ–ის უზრუნველყოფის საქმეში ადამიანი წარმოადგენს ყველაზე უფრო მოწყვლად რგოლს. შეტევების უმეტესობა, მათ შორის მსხვილ კოპანიებსა დაწსებულებებზე არარეალიზებადია მათი თანამშრომლების მონაწილეობის გარეშე. ჩანერგილი ინსაიდერები და მოსყოდული თანამშრომლები მნიშვნელოვნად ამსუბუქებენ ბოროტგანმზრახველების ამოცანას, ოღონდ ინფორმაციების გაჟონვების უმეტესობა წარმოადგენს თანამშრომლების გულგრილობის და მათი ინფორმაციის დაცვაში გაუთვითცნობიერებლობის შედეგი. უფრო ხშირად და სულ უფრო წარმატებით გამოიყენება სოციალური ინჟინერიის მეთოდები.

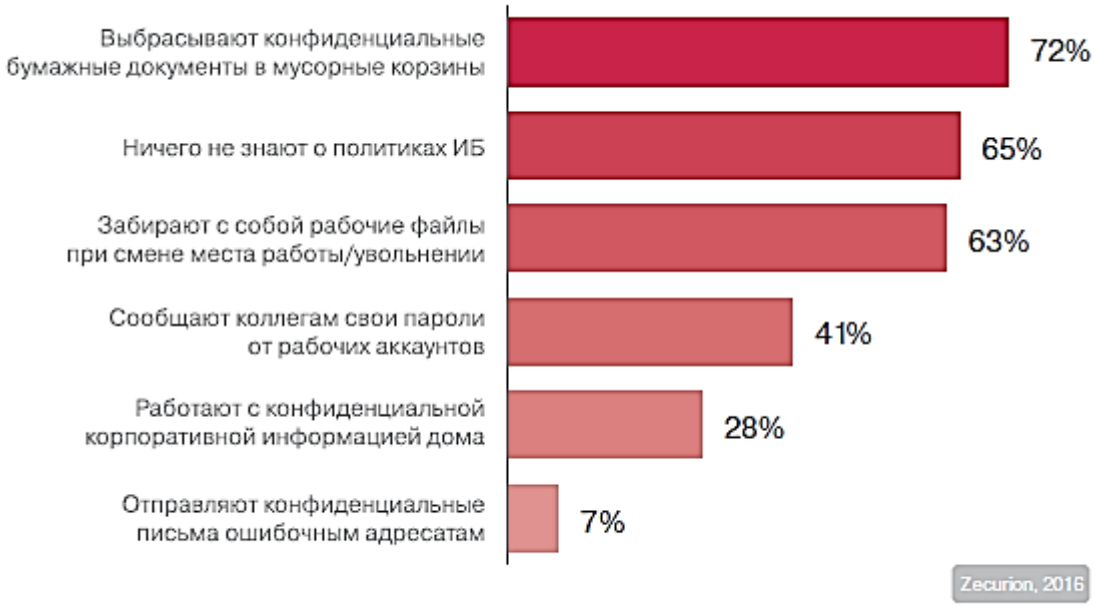
მაღალი კლასის ბოროტგანმზრახველებს გააჩნიათ უნარი გაიტანონ არა მარტო ინფორმაცია, არამედ პირდაპირ ფულიც.მართლაც, იმის ნაცვლად, რომ ინადირონ ინფორმაციაზე, რომლის გაყიდვისათვის საჭირო იქნება მყიდველის პოვნა , ბევრად ეფექტურია აიძულონ ადამიანი მაშინვე გადარიცხოს ფული. როგორც პრაქტიკა აჩვენებს, ეს მართლაც შესაძლებელია. ასე მაგალითად, კომპანია Ubiquiti-მა 2015 წლის ზაფხულში აღიარა რამოდენიმე მილონი დოლარის დაკარგვა თაღლითების მოქმედებების გამო.მხოლოდ ელექტრონული ფოსტის გამოყენებით, მათ აიძულეს კომპანიის ერთ–ერთი თანამშრომელი გაეკეთებინა რამოდენიმე საბანკო გადარიცხვა – ჯამში 46,7 მილიონი დოლარის, რომელთაგან მხოლოს 8,1 მილიონი დოლარის დაბრუნება ღა გახდა შესაძლებელი. ჩატარებულმა შიდა გამოძიებამ აჩვენა – გარედან ჩარევა ქსელის შიდა სერვისებსა და მუშაობაზე არ ყოფილა მსგავსი შეტევებისაგან დაცვის აგება ერთდროულად ადვილიცაა და რთულიც. ადვილია – იმიტომ რომ ღონისზიებები (იუ–ში ისტრუკტაჟი და ტრენინგები) არ მოითხოვენ დიდ ფინანსურ დანხარჯებს და ადვილად შეღანხმებადია ხელმძღვანელობასთან. რთულია – ფაქტია რომ შეცვლა ადანიანების ჩვევების, მათი დარწმუნება ინსრუქციების შესრულებაზე, რაღაც თვალსაზრისით შეცვლილი იქნას მსოფმხედველობა – ინტერნეტი არც ისე მეგობრულია, როგორც გვინდა ველოდოთ.

თუმცა ფორმალურად კორპორაციული ინფორმაციის შენარჩუნებაზე პასუხს აგებენ იუ–ის სპეციალისტები ან ბიზნეს–ქვედანაყოფების ხელმძღვანელები, უსაფრთხოება იწყება თვით მომხმარებლებიდან – ხაზური თანამშრომლებისაგან, რომლების მუშაობენ მონაცემებთან ყოველ დღე.

რუსეთში ოფისის თანამშრომლების ნახევარზე მეტი არ თვლის ამაზრზენად დათხოვნის მუქარისას ან სამუშაოს შეცვლისას გაიტანოს ინფორმაცია. თუნდაც ჩვეულებრივმა კოპირებამ მონაცემებისა ფლეშკაზე ან გაგზავნამ სახლის ფოსტაზე შიძლება გამოიწვიოს მონაცემების გაჟონვა. ეს

წარმოადგენს პირდაპირ დარღვევას შეთანხმებისა, რომ არ მოხდეს ინფორმაციის გათქმა, რომელსაც ბევრ კომპანიაში ხელს აწერენ თანამშრომლები.

გაჟონვები ასევე დაკავშირებული ინფორმაციასთან მუშაობის სხვა წესების დარღვევასთან. ყველაზე ადვილია მონაცემების შენახვა–შენარჩუნება მათი რეგლამენტირებული შენახვის ადგილებში. ჩვეულებრივ ესაა ქსელური დისკები ან შიდა საინფორმაციო სისტემები. მონაცემები ჩვეულებრივ ინახე დაშიფრულისახით, ხოლო იტ–სისტემები აადვილებენ მათთან დაშვების კონტროლს. კოპიოების შექმნა და და მონაცემების გადმოტვირთვა ლოკალურ დისკზე მნიშვნელოვნად ზრდიან რისკებს. ასევე ცუდია, როდესაც დოკუმენტები იქმნებიან და ინახებიან ლოკალურ კომპიუტერებზე. ამ შემთხვევაში გაჟონვის რისკს ემსტება მონაცემების დაკარგვის რისკი. მოწყობილობის შეფერხებისას ან კოპიუტერის ვირუსებით დაბიძურებისას ინფორმაცია შეიძლება აღმოჩნდეს ხელმიუწვდომელი. თუ ქსელურ სერვისებში მონაცემების რეზერვირება ხდება რეგულარულად, სამუშაო სადგურებში მომხმარებლები ასეთ რამეზე არც ფიქრობენ.



ნახ.29. თანამშრომლების შეცდომები, რომლებსაც მივყავართ ინფორმაციის გაჟონვენთან

ყველაფერი ეს ერთობლიობაში მნიშვნელოვნად ზრდის რისკებს კორპორაციული ინფორმაციის მიმართ. სწორედ ამიტომაც გაჟონვების თავიდან აცილების სისტემები ორიენტირებული არიან არა მარტო ბოროტგანზრახულ ინსაიდერებზე, არამედ ლოიალურებზეც, გულგრილ ან მანიპულატორებზე, ხოლო პროდუქტების ფუნქციონალი მოიცავს შესაძლებლობებს გამოსავლენად კონფიდენციალური ინფორმაციის შენახვის ადგილების, მონაცემების კლასიფიკაციას, გადაადგილებების დეტექტირებას და დარღვევების თავიდან აცილებას.

## კრიტიკული ინფრასტურუქტურის ინფორმაციული უსაფრთხოების დარღვევის პროცესების მოდელირება

ობიექტების (კმო) ინფორმატიზაციას IP ტექნოლოგიების ბაზაზე კრიტიკული ინფორმაციული ინფრასტრუქტურის (კიი) უსაფრთხოება ფაქტიურად ნებისმიერი სახელმწიფოსათვის აქცია თანამედროვეობის მწვავე პრობლემა. ინფორმაციზაციის პროცესი განაპირობებს ინფორმაციული უსაფრთხოების (იუ) ახალი სახის მუქარების გაჩენას, რომლებიც მიმართული არიან, პირველ რიგში, კმო –ის მართვის და სიცოცხლისუნარიანობის უზრუნველყოფის სისტემებზე, რომლებიც ყველაზე უფრ განიცდიან დესტრუქციულ ინფორმაციულ წემოქმედებას (დიზ) ტერორისტული მუქარების გაზრდილი დონე საზოგადოების სულ უფრო მეტ დამოკიდებულებას სამრეწველო სისტემებზე მოითხოვენ კოორდინირებულ გატარების ზომებისა, რომლებიც მიმართული არიან კმო – ის ფუნქციონირების დეზორგანიზაციის ან სრული შეწყვეტის რისკის გაწევაზე ინფორმაციული კონფლიქტისას. ერთ – ერთი შესაძლო მიმართულებას ამ პრობლემის დაძლევისა წარმოადგენს კმო – ის კიი – ის

აუდიტის ჩატარება, რომლის ძირითად ეტაპს წარმოადგენს იუ – ის არსებული მუქარების იდენტიფიკაცია.

იუ – ის მუქარების აქტუალური ჩამონათვალი უნდა განისაზღვროს კმო – ის იყოს დამრღვევის შესაძლო მოქმედებების მოდელირების შედეგების.

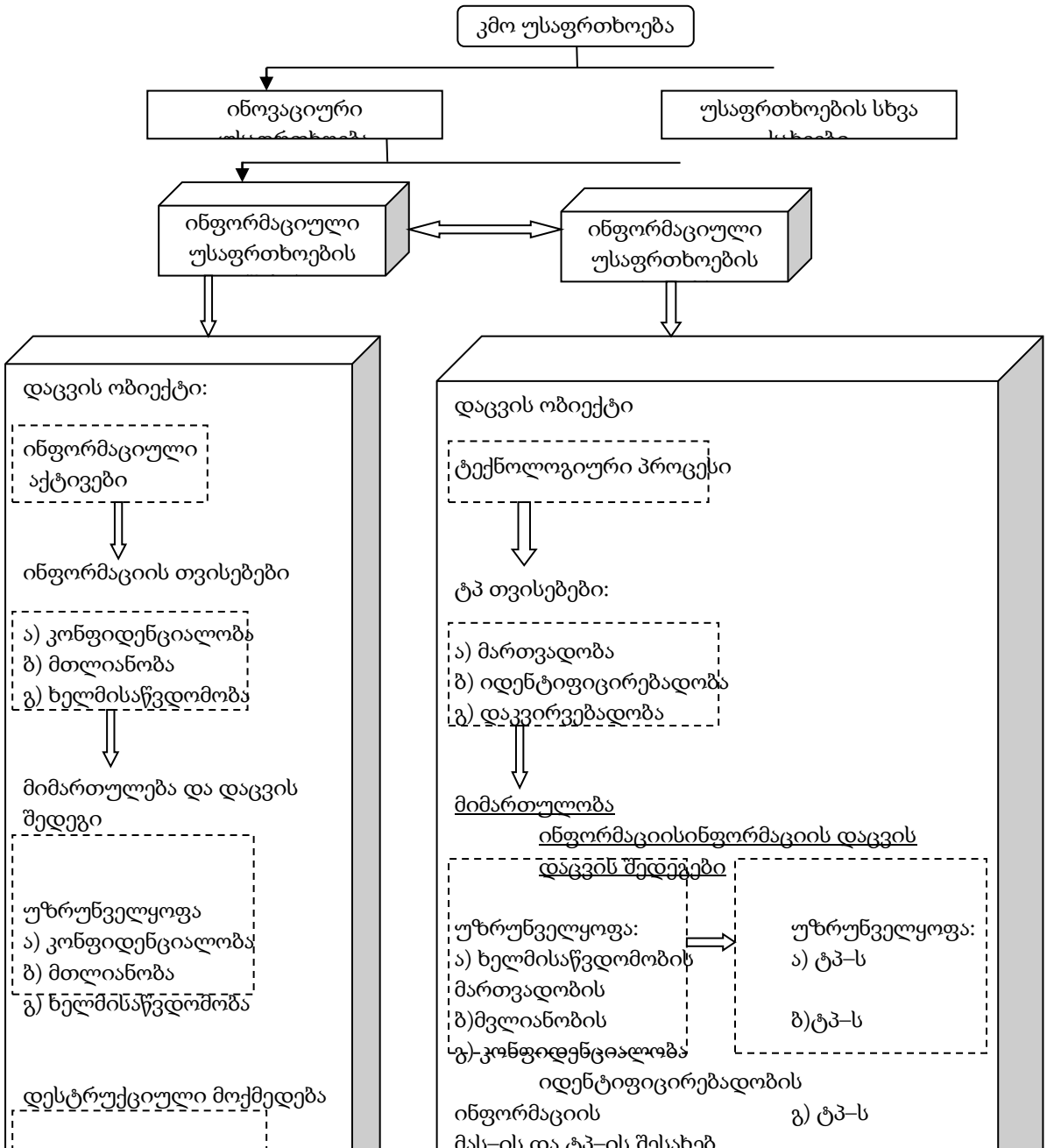
დღეისათვის არაა საკმარისად ფორმალიზებული დამრღვევის პოტენციალის დონის და მისი ინფორმაციული ზემოქმედების (იზ) ეფექტურობის შეფასების მეთოდოლოგია. ფაქტიურად დონე განისაზღვრება ექსპერტულად მხოლოდ მართვის ცნობილი კრიტერიუმების.

**ანალიზი ნორმატიულ – სამართლებრივი ბაზისა რესეთის ფედერაციის (რფ) მაგალითზე, რომელიც არეგლამენტირებს იც – ის დამრღვევის დონის შეფასების მიდგომებს.**

ტრადიციულ ავტომატიზებულ სისტემებში (ას) იუ – ის დამრღვევის მოქმედებების საფრთხეების დონის შეფასებისადმი მიდგომები მოყვანილია ნახ. 30 – ზე.

იუ – ის დამრღვევების კლასიფიკაცია (ნახ.30 პირველი მიდგომა) დღეისათვის უკვე მოძველებულია, ვინაიდან მისი შემუშავება ხდებოდა თანამედროვე ას – ების ქსელური არქიტექტურის გათვალისწინების გარეშე. მეორე მიდგომა (ნახ.30) საშუალებას იძლევა, მოხდეს იუ დამრღვევების კლასიფიკაცია არა მარტო დასაცავ ინფორმაციასთან დაშვების უფლებამოსილების დონის მიხედვით, არამედ საწარმოს კონტროლიზებად ზონაში თვით ფიზიკური დაშვების არსებობის ფაქტის გათვალისწინებით, მაგრამ მოცემული მიდგომა დამრღვევს აფასებს მხოლოდ ორი ასპექტით (რეალურად მათი რაოდენობა მეტია) და არ იძლევა საშუალებას კვალიმეტრის პოზიციიდან გაიზომოს დამრღვევის პოტენციალის დონე, ასევე შეფასდეს მისი მოქმედებების შედეგიანობა.

მესამე მიდგომის (ნახ.30) ჩარჩოებში შემოთავაზებულია არ მოხდეს განხილვა დამრღვევის შეტევის ობიექტთან ურთიერთმოქმედბისა და არ გაკეთდეს არავითარი ვარაუდი უსაფრთხოების ფუნქციის რეალიზაციის კორექტულობასთან დაკავშირებით, არამედ განხილული იქნას ინფორმაციული ზემოქმედება მხოლოდ და მხოლოდ ავტომატიზებული სისტემის მოწყვლადობების ანალიზის შედეგების კონტექსტში, ძირითადი მიზანი ამ ანალიზისა, რომელიც სრულდება აუდიტისას, – გაკეთდეს დასკვნა, რომ შეფასების ობიექტი არის მდგრადი მოწინააღმდეგის შეტევებისადმი, რომელსაც გააჩნია, საშუალო ან მაღალი პოტენციალი თავდასხმებისა. დამრღვევის პოტენციალი უნდა განისაზღვროს მისი შესაძლებლობების შეფასებისას, რომელიც ტარდება იუ აქტიური მუქარების განსაზღვრისას. იუ – ის ეს მუქარები უნდა განისაზღვროს



ნახ. 30

დამრღვევის შესაძლო მოქმედებების მოდელირების შედეგად, რაც მოითხოვს დამუშავებული იქნას მეთოდოლოგიური საფუძვლები დამრღვევის პოტენციალის შეფასებისა ტექნოლოგიური პროცესების მართვის ავტომატიზებული სისტემის (ტპ მას) სპეციფიკის გათვალისწინებით.

ტექნოლოგიური პროცესების უსაფრთხოების თვისებებზე ნახ. 30 გავლენას ახდენს ტპ ელემენტარული თვისებები და მათი მართვის სისტემები დაკვირებადობა, მართვადობა, იდენტიფიცირებადობა.

## 2.4. კმო იუ – ის უზრუნველყოფა ტპმას – ის სპეციფიკის გათვალისწინებით

მიმდინარე მომენტში კმო უსაფრთხოების გამოკვლევებთან დაკავშირებით კვლევითი მიმართულება ყოვნდება. ვინაიდან არ არსებობს ერთიანი შეხედულება  ცპ მას – ის იუ – ს არსთან დაკავშირებით. მოცემულ ტექნოლოგიურ სისტემებს გააჩნიათ უფრო მაღალი დონე რისკისა ტრადიციულ ას – ებთან შედარებით. სისტემის მუშაობისუნარიანობის

დარღვევა, მავნე ნივთიერების გამოყოფა, ტექნოლოგიური კატასტროფები და ადამიანების დაღუპვა. ამიტომ გარდა ინფორმაციის კონფიდენციალობის, ურღვეობის და ხელმისაწვდომობის უზრუნველყოფისა, დგება – ისმება საკითხი კმ – ში თვით ტექნოლოგიური პროცესების უსაფრთხოებისა.

ამიტომ ტპ – ს დაცვის მიზანს წარმოადგენს უზრუნველყოფილი იყოს ტექნოლოგიური პროცესების მართვადობის, დაკვირვებადობის და იდენტიფიცირნებადობის მოთხოვნები. ამ მოთხოვნების შეუსრულებლობის შემთხვევაში შესაძლებელია დესტრუქციული ზემოქმედებები ტ.პ. მას– ზე, რაც დაკავშირებულია დაკარგვასთან:

– ტექნოლოგიური პროცესების მართვადობის, რომელიც მოიცავს მართვის ბლოკირების და/ან არასანქცირებულ მართვას,

– ტპ – ს დაკვირვებადობის: ტპ – სს პარამეტრების მოდიფიკაცია და/ან განაწილების გაზომვების ფალსიფიკაცია,

– სისტემის მუშაობისნარიანობის ავარია (გაჩერება) ტპ – ის და /ან გამოთვლითი რესურსები დეგრადაცია..

ტპ მას – ზე ყველა დესტრუქციული ზემოქმედებები წარმოადგენენ ნაწარმოებს შემდეგი სამი მიზეზებით: დაშვებადობის დარღვევა (უარი მომსახურებაზე).

კრიტიკულად მნიშვნელოვან ინფორმაციასთან, მისი მთლიანობის დარღვევა (მოდიფიკაცია) და კონფიდენციურობის დარღვევა (გაჟონვა).

კრიტიკულად მნიშვნელოვან ინფორმაციას წარმოადგენს ტპ მას – ის დოკუმენტაციაში დაფიქსირებული ტექნოლოგიური“ ინფორმაცია, რომლის განადგურებამ ბლოკირებამ ან დამახინჯებამ შეიძლება გამოიწვიოს ტპ მას ის ფუნქციონირების დარღვევა. ასევე ინფორმაციისა „ტპ მას –სის და ტპ – ის შესახებ“. რომელიც მისი მოპარვის შემთხვევაში შეიძლება გამოყენებული იქნას ტმ მას – ზე დესტრუქციული ზემოქმედებისათვის „ტექნოლოგიურ“ ინფორმაციას წარმოადგენს:

– ოპერატიული (დინამიური) ინფორმაცია (ტელემეტრია, ტელეგაზომვები, ტელემართვის) ტექნოლოგიური ტექნოლოგიური პროცეების მიმდინარეობის შესახაბ. საარქივო (სტატილური) ინფორმაცია (ნორმატიულ– ტექნიკური დოკუმენტაცია, ტპ – ს პარამეტრები და სხვა საარქივო ინფორმაცია.

ტპ იპს – ის ტნექნოლოგიური პროცესის შესახებ ინფორმაციის ქვეშ მოიაზრება ინფორმაცი შემადგენლობის სამართავი პროცესის მახასიათებლების პროგრამული და პროგრამულ – აპარატურული უზრუნველყოფის, განთავსების, კომუნიკაციების შესახებ.

ამიტომ ტპ მას – ისთვის დაცვის მთავარ მიმართულებას წარმოადგენს ტექნოლოგიური ინფორმაციის ხელმისაწვდომობის და ძალიანობის ურღვევობის უზრუნველყოფა,ხოლო მისი კონფიდენციალობის დაცვა არაა აქტუალური ოღონდ წარმოიშობა მომიჯნავე მუქარა „მპ მას – ის და ტექნოლოგიური პროცესების შესახებ“ ინფორმაციის კონფიდენციალურობის დარღვევისა.

4. ინფორმაციული უსაფრთხოების დარღვევის პროცესის მოდელირების ოპერატიული კომპლექსი

კვალიმეტრიის ძირითადი პრინციპებიდან ან მეთოდებიდან გამომდინარე, შემოთავაზებულია დარღვევის პოტენციალი დახასიათდეს ვექტორით:

$$Y_3^{\Pi} = Y_3^{\Pi}(A_{K'}^{'}; A_{K''}^{''}, B_{I'}^{'}),\ K = K'+K'',\ A_K < A_{(K)}^{'} + A_{<K'>}^{''} > [2,3,4]$$

მიზანმიმართული პროცესების ეფექტურობის თეორიის პოზიციიდან [5] ვექტორი $Y_3^{\Pi}$ არის მაჩვენებელი ინფორმაციალი ზემოქმედების შედეგების ვირტუალური ხარისხის. ის მოიცავს თავის თავში კომპონენეტების სამ ჯგუფს $Y_3^{\Pi} =< v, r, \tau >$, რომლებიც ახასიათებენ ვირტუალური (შესაძლე) მიზნობრივ ეფექტებს, სადაც V – არის მიზნობრივი ეფექტების (იზ – ის შედეგების) მაჩვნებელი, r – არის რესურსების ხარჯვის (იზ – ის რესურსების) მაჩვენებელი, τ – არის ოპერატიული დროის დანახარჯები (იზ – ის ოპერატიულობა). $Y_3^{\Pi}$

ვექტორის ყოველი კომპონენტი დამოკიდებულია ვექტორებზე $A'_{<k'>}, A''_{<k'>}, B'_{<I'>} =< v, r, \tau >$ – საექსპლუტაციო – ტექნიკური მახასიათებლები (სტმ) და პარამეტრები სისტემის იზ (სისზ) დარღვევისა, $B'_{<I'>}$ – სტმ და პარამეტრები იზ ორგანიზაციის პროცესისა (პრიზ) ან იზ ტექნოლოგიის, $B'_{<I'>}$ სიიზ ფუნქციონირების პირობების მახასიათებლები (ფპმ).

სიიზ ქვეშ მოვიაზრებთ ინფორმაციული ზემოქმედების (იზ) პროგრამულ – აპარატურული საშუალებების ერთობლიობას. იზ ფუნქციონირების პირობების მახასიათბელების (ფპმ) ქვეშ კი მოვიაზრებთ ერთობლიობას ფაქტორებისა, რომლებიც გავლენას ახდენენ სიოზ – ს სტმ – ზე (ვექტორი $A'_{<k'>}$) ასევე პრიზ – ს მახასიათებლებზე (ვექტორი $A''_{<3>}$) და მათი მეშვეობით განპირობება შესაძლო (ვირტუალური) იზ – ის $Y^{\Pi}_{<3>}$ შედეგებისა.

დაზღვევის მიერ იზ საშუალებების გამოყენება ხდება შეტევის ქვეშ მყოფი ტპ მას – ის დაცვის სისტემის აქტიური წინააღმდეგობების პირობებში. ამიტომ დამრღვევის მიერ სიიზ – ის გამოყენების პირობების $B''_{<I''>}$ ქვეშ მოვიაზრებთ შეტევის ქვეშ მყოფი ტპ მას – ის დაცვის მექანიზმების ერთობლიობას. დაცვის ეს მექანიზმები გავლენას ახდენენ სიტუაციაზე. რომელშიც მოუწევ სისზ ამოცანის შესრულება, და შესაბამისად განაპირობებენ მოთხოვნილ $Y^{3}_{<3>}(B''_{<I''>})$ დარღვევისათვის იზ შედეგებს ანუ $Y^{\Pi}_{<3>} \in \{Y^{3}_{<3>}\}$, სადაც $Y^{\Pi}_{<3>} =< V^{T}, r^{\Pi}, r^{D} >$ – არის მოთხოვნილი (მინიმალურად დასაშვები) მიზნობრივი ეფექტი $V, r^{\Pi}$ – არის ზღვრული (მაქსიმალურად დასაშვები) დანახარჯი რესურსების r, $\tau^{D}$ – არის დირექტიული (მაქსიმალურად დასაშვები) დრო τ.

თანაფარდობა $Y^{\Pi}_{<3>} \in \{Y^{3}_{<3>}\}$ წარმოადგენს ფორმალურ გამოსახულებას დამრღვევის იზ – ის მიზნებისა. შინაარსობრივად იზ – ის მიზანი განისაზღვრება დარღვევით ტექნოლოგიური პროცესების ფუნქციონირებისა, რომელთა დაცვის სპეციფიკა წარმოდგენილი იყო მე – 3 ნაწილში.

იზ – ის ეფექტურობის მაჩვენებელს აღვწერთ ვექტორით

$$Y^{nB}_{<3>} = Y^{nB}_{<3>}(A^{'}_{<k'>}, A^{"}_{<k">}, B^{'}_{<I'>}, B^{"}_{<I">})$$

სადაც

$$A^{'}_{<k'>} = A^{'}_{<k">}, B^{'}_{<I'>}, B^{"}_{<I">})$$

იუ – ის დარღვევის პროცესების მოდელირების ოპერატიული კომპლექსის (ოპკ) სტრუქტურული სქემა ნაჩვენებია ნახ. 3 – ზე.

გავხსნათ დარღვევის ტმ მას ინფორმაციალი ზემოქმედების ოპკ – ის ძირითადი ელემენტების შინაარსი.

– სას – სახელმძღვანელო დარღვევის.

– პმო – იზ პროცესის მართვის ორგანო,

– სიიზ – სისიტემა იზ – ძალები და საშუალებები იზ – ის,

– პროზ – პროცესი იზ – ტექნოლოგია (ორგანიზაციის პროცესი) იზ – ის,

– ფპმ – სიიზ – ის ფუნქციონირების პირობები,

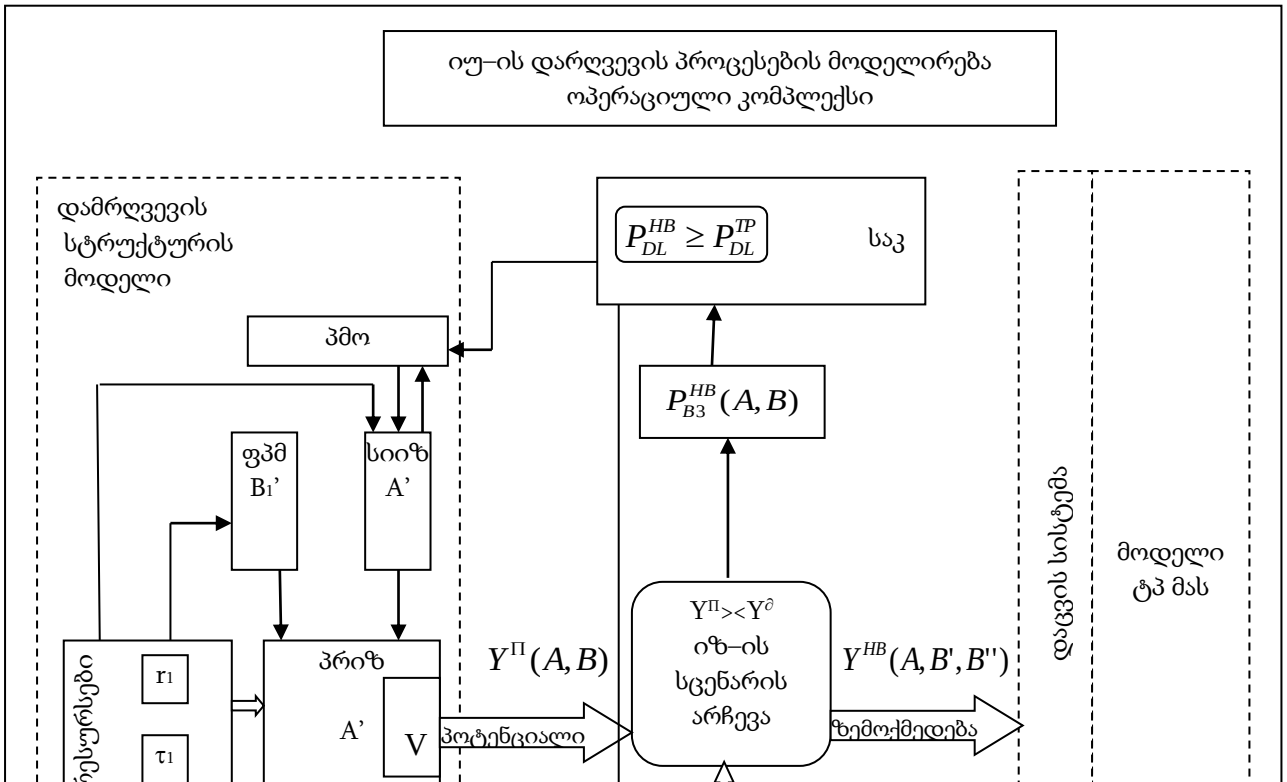
– გპს – დარღვევის მიერ სიიზ – ის გაომყენების პირობები.

– v – მიზნობრივი ეფექტების მაჩვენებლების (იზ – ის შედეგიანობა),

– r – რესურსების ხარჯვის მაჩვენებლები (იზ – ის რესურსტევადობა),

– τ – იზ – ზე დახარჯული დრო (იზ – ის ოპერატიულობა).

იუ – ის დარღვევის პროცესების მოდელირების ოპერატიული კომპლექსი



ნაზ. 31 იუ – ის დარღვევის პროცესების მოდელირების ოპერატიული კომპლექსის სტრუქტურული სქემა $Y^{\partial}(B^{11})$

უნდა აღინიშნოს, რომ დამრღვევი (და მის მიერ რეალიზებული იზ) ინფოტელური კომუნიკაციურ სივრცეში დაცვის ქვეშ მყოფი მხარისთვის წარმოდგენილია საშიში პროცესების – იუ – ის დარღვევის პროცესები სახით. ეს დექტრუქციული პროცესები დაცვის პროცესებთან ერთად ქმნიან ე.წ. კონფლიქტში მყოფ პროცესები (მაკონფლიქტებელ), ხოლო გამოკვლევა მათ ერთმანეთს მიმართ წინააღმდეგობებისა – აქტუალური ამოცანაა.

ფაქტიურად პოტენციალი $Y_3^{\Pi}$ ახასიათებს დარღვევის შიდა სტრუქტურას და შესაძლებელის ანალიტიკურად წარმოდგენილ იქნას სხვანაირად. წყვილის სახით $< St_r, P_{ar} >$, სადაც $St_r$ – არის დამრღვევის სტრუქტურა, $P_{ar}$ მისი პარამეტრების $A'_{<r>}, A''_{<k">}, B'_{<i'>}$ მნიშვნელობები. $St_r$ სტრუქტურის ცოდნა და პარამეტრების $P_{ar}$ საშუალებას იძლევა კლასიფიცირებულ იქნას მოწინააღმდეგე სხვადასხვა კრიტერიუმების. ამიტომ დამრღვევის მახასიათებლებს აღვწერთ ფაქტორით $< St_r, P_{ar}, KI_{as} >$,. სადაც $KI_{as}$ – დარღვევის კლასიფიკაციის კრიტერიუმებია. გამოვიყენებთ რა პარამეტრებს $A'_{<k'>}, A''_{<k">}, B'_{<i'>}$ სხვადასხვა თანაფარდობებს შეიძლება კლასიფიცირება დამრღვევისა. ასპექტების სიმრავლით. მაგალითად პარამეტრის $A''_{<k">}$ მიხედვით – დარღვევის მიერ რეალიზებული იზ – ის ტიპი პარამეტრის $B'_{<i'>}$ მიხედვით – ტპ მას – თან შორიდან მიერთების სახე.

ამიტომ იუ – ის აუდიტის ჩატარებისას აუცილებელია, პირველ რიგში განისაზღვროს დამრღვევის კლასი, ხოლო შემდეგ უკვე შეფასდე ს მისი პოტენციალი. განვსაზღვროთ ფიზიკური არსი ცვლადებისა $A'_{<k'>}, A''_{<k">}, B'_{<i'>}, B''_{<i">}$

$A'_{<k'>}$ – – პარები და სტმ სიიზ – ესი დამრღვევის:

- სიიზ შემადგენლობა და სტრუქტურა,
- დარღვევის ტექნიკური კომპეტენტურობის დონე,
- შორიდან იდენტიფიკაციის საშუალებების მახასიათებლები (აგალითად მოშორებული პოსტების სკანირებისათვის გამოყენებული სესხები, სკანირების დროითი პარამეტრების მიმართვები, T⊂P/UD პროვოკაციების მდგომარეობის იდენტიფიკაცია და სხვა).
- ინფორმაცილი ზემოქმედების იზე, საშუალებების მახასიათებლები, მაგალითად რეალიზებადი ქსელური შედეგების კლასები და მათი რეალიზაციის ხერხები – მეთოდები, შესაძლებლობა მოდელის სხვადასხვა დონეებზე ზემოქმედების რეალიზაციის, მიმართულობა ინფორმაციული ზემოქმედების: დარღვევა კონფიდენციალობის მთლიანობის ან ინფორმაციასთან დაშვებადობის. და ა. შ. )
- გადაწყვეტილების მიღების სისტემების მახასიათებლები და ა.შ.

$A''_{<k">}$ – სტმ და პრ იზ პარამეტრები.

- იზ– ის მიზნების მათემატიკური აღწერა.
- იზ – ის დაწყების დროის მომენტი და განხორციელების პერიოდი,
- რეალიზებადი იზ – ის ტიპი,
- იზ – ის დაწყების პირობები (რეალიზებადი შეტევის ობიექტიდან მოთხოვნით (შეტევის ობიექტი –ში) ან შო – ზე მოსალოდნელი – სასურველი ოვლენის დადგენით უპირობა ზემოქმედებები),
- შო – თან უკუკავშირის არსებობა: უკუკავშირით უკუკავშირის გარეშე (ცალმხრივი მიმართულები იზ.).

– ეტალონური მოდელის OSI დონე, რომელზეც ხდება იზ – ის რეალიზება,

– იზ – ის განხორციელების ცენტრი,

– იზ – ის განხორციელების დაფარულობა და სხვა.

მახასიათებლები $B'_{<I'>}$ იზ ფუნქციონირების პირობები,

– ტპ მასთან დაშვების წერტილის არსებობა.

– ქსელი ინტერნეტს მეშვეობის შორიდან მიერთების სახე (აგალითად, კომუტირებადი მიერთება PSTN – ის საფუძველზე, მიერთება ISDN გამოყენების ლოკალური მიერთება DSL ტექნოლოგიით; გამოყენება თანამგზავრული კავშირების სიმეტრიული სისტემებისა, გამოყენება თანამგზავრული კავშირების ასიმეტრიული სისტემების, გამოყენებს მონაცემთა გადაცემის ფიჭური კავშირების და სხვა),

– ბო – ის შესახებ ცოდნის დონე: პოსტების რაოდენობა და მახასიათებლები, პოსტები და სერვისები, პროგრამული უზრუნველყოფა (პუ), აპარატურული უზრუნველყოფა, ქსელის ტიპოლოგია და სხვა.

– მოწყვლადობების არსებობა: სისტემური პუ – ს მოწყვლადობები (მათ შორის ქსელური ურთიერთქმედების პროტოკოლების) გამოყენებითი პუ – მოწყვლადობები (ათ შორის ინფორმაციის დაცვის საშუალებების) და სხვა.

# 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 – $\hat{Y}^{n}(\hat{A},\hat{B}'$

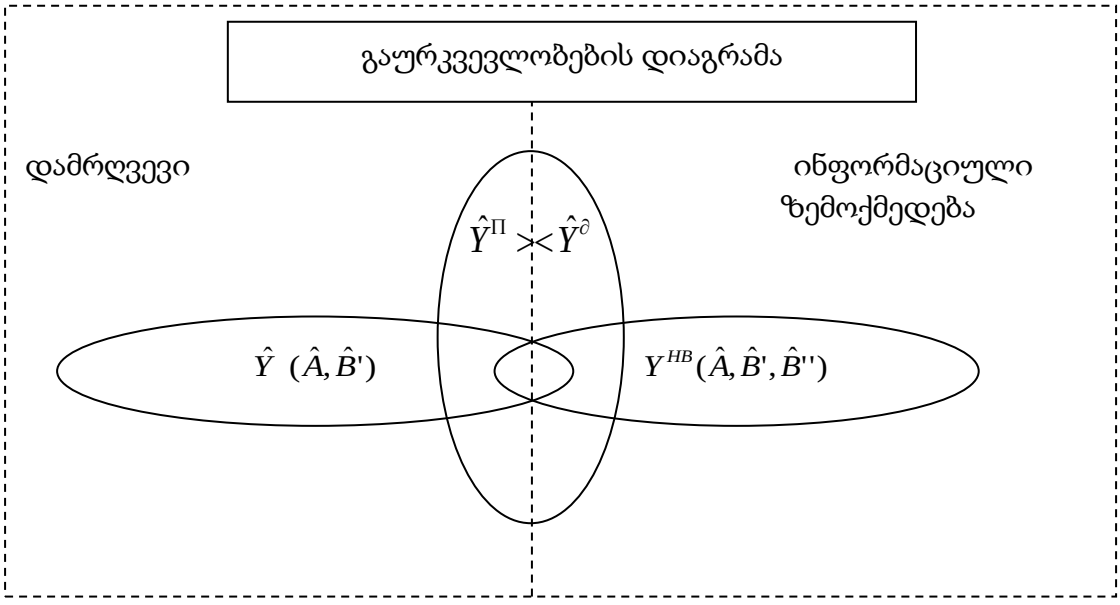
ტიპი 2. დამრღვევის მიერ იზ – ის სცენარის არჩევის კრიტერიუმის – $\hat{Y}^{\Pi}\underset{<}{\geq}\hat{Y}^{\partial}$,

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

იმის გამო, რომ როგორც დამრღვევს, ასევე მისგან დაცვის სისტემას უწევთ იმოქმედონ გაურკვევლობის პირობებში, პარამეტრების ვექტორების $\hat{A}_{<K>}$ და ,$\hat{B}_{<I>}$ მნიშვნელობები არიან შემთხვევითი (Λ – არის შემთხვევითი სიდიდის სიმბოლო), ხოლო შესაბამისად $\hat{Y}^{\Pi}$ ვექტორიც და $\hat{Y}^{NB}$ ვექტორიც ასევე იქნებიან შემთხვევითები, უფრო მეტიც, აპრიორში შემთხვევითები არიან დასაშვები მნიშვნელობები $\hat{Y}^{NB}_{<3>}$ ვექტორისა $\hat{Y}^{\Pi}$ რომლებიც დამოკიდებული ანიან შეტევის ქვეშ მყოფი სისტემის არ დაცვის სისტემაზე,

ვინაიდან დამრღვევის მიერ იზ – ის განხორციელებამდე თვითონ დამრღვევი და მის მიერ დასახული, ოპერაციის ჩატარების მიზანი უცნობია.

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




ნახ. 32 სქემატური დიაგრამა, რომელზეც ილუსტრირებულია დამოკიდებულებები გაურკვევლობებისა დარღვევის და მისი ზემოქმედებები მოდელირების პროცესისა

უფრო დეტალურად განვიხილოთ გაურკვევლობები, რომლებსაც აწყდებიან მკვლევარები დარღვევის მოქმედებები 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 შეუძლებლობა დარღვევის შესაბამისი მოდელის აგებისა, რომელიც განეკუთვნება ამა თუ იმ ტიპის მათემატიკური სტრუქტურისა. იმისათვის რომ მოიხსნას ეს სტრუქტურულიგანუსაზღვრელობა შეიძლება შემოთავაზებულ იქნას მასკირება ტპ მას – ის ინფორმაციული რესურსების მასკირების ტექნოლოგია, რომელიც შემოთავაზებულია ნაშრომში [6]. 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.

მეორეც, არსებობს განუსაზღვრელობა ბაზისური სიმრავლეების და თანაფარდობების მონაცემებში, რომელთა საფუძველზეც იგება დამრღვევის მოდელი. ასეთი გაურკვევლობის რაოდენობრივი შეფასებისათვის შეიძლება გამოყენებულ იქნას სტოქასტილური მიდგომა. (სტოქასტილური სტატიქტიკის ფუნდამენტალურ დებულებებს, ან მოდგომა არამკაფიო სიმრავლეთა თეორიის (რამკაფიო სტრუქტურები) პოზიციიდან.

იდეა მდგომარეობს იმაში, რომ გამოკვლეულიქნას განუსაზღვრელობა დარღვევის მიერ იზ რეალიზაციის ამა თუ იმ სცენარის შერჩევის. 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.

ცხადად ითვლება, რომ საუბარი იზ – ის სტოქასტილურ ბუნებაზე არარაციონალურია, ვინაიდან დარღვევისათვის არჩევენ ((არ აკეთებს) არ ახორციელებს შემთხვევით. მისი არჩევანი მიზანშეწონილია და 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 იყოს ტიპიური მუქარები მართლაც ცნობილია.

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 „თამაშების თეორია“. თამაშების თეორიის ქვეშ ხშირად ესმით თეორია მათემატიკური მოდელებისა ოპტიმალური გადაწყვეტილებების მიღების გაურკვევლობების და კონფლიქტების პირობებში. მაგრამ თამაშების თეორია როგორც მათემატიკური აპარატი, ხასიათდება კონცეპტუალური არასისრულით. ამე 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 [7]

<u>მასამე</u> (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 ღებულობა 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 (ოვლენა) ხდომილება. ამიტომ დარღვევის 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) დარღვევების ინფორმაციისა:

– ИТКС 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 – გამოიშვება დამრღვევის სტრუქტურული გაურკვევლობის მოხსნის მეთოდებით. ოღონდ მოცემული მიდგომების რეალიზაცია იუ – ის აუდიტის ჩარჩოებში ყოველთვის როდია შესაძლებელი, ვინაიდან მოითხოვს დამატებითი ტექნიკური საშუალებები და დროის მოზიდვას.

ამიტომ აუდიტის ჩატარების მსვლელობისას ფართოდ გამოიყენებს დამრღვევის ექსპერტული შეფასებები იუ – ის შესაძლო U მუქარების ტიპები, რომელთა გამოყენებაც მას შეუძლია. შესაბამისად, დარღვევის მოდელი უნდა განსაზღვრავდეს დამრღვევი თუ რომელს შესაძლო შემტევი მოქმედებებიდან ანიჭებს უპირატესობას, იგულისხმება ელემენტარული მოვლენები იუ – ის დარღვევისა, რომელთაგან ხდება ფორმირება იზ – ის მუქარების რეალიზაციის სხვადასხვა სცენარებისა. ანუ აუდიტორის წინაშე დგას ამოცანა დასაბუთებული შემცირებისა U სიმრავლის სიმძლავრისა მოცემული ამოცანის ფორმულირებისას შეიძლება მიღებულ იქნას შემდეგი დაშვებები მონაცემების არსებობაზე. [8]

– დამრღვევის ცოდნის დონისა და კომპეტენტურობაზე

– დამრღვევის საწყის პოზიციაზე NTKC – ში, რომელიც განსაზღვრავს მისთვის ხელმისაწვდომი პოსტების სიის გარკვეული ფორმალური მოდელის M საფუძველზე,

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

ერთმანეთისაგან განსხვავებით დამრღვევის აპრიორულ $N^A$ და აპოსტერიორულ $N^P$ მოქმედებას. პირველ ტიპს მივაკუთვნებთ მოდელ, ჩამონათვალი პარამეტრების და მათი მნიშვნელობების, რომელიც განსაზღვრული კონკრეტული საკვლევ ავტომატიზებული სისტემის სტრუქტურასთან დაკავშირების გარეშე. მის სტრუქტურას განსაზღვრავენ ჰიპოთეზები, რომლებსაც წარმოადგენენ აუდიტორები მათთვის ცნობილი აპროირული მონაცემების და საკუთარი კომპეტენციის საფუძველზე. შედეგად აპრიორული მოდელი დამრღვევისა, რომელიც ითვალისწინებს მისთვის სასურველი შესაძლო შემტევი მოქმედებების არჩევას გამოიყენება შემდეგნაირად: პოტენციურად

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

სადაც Z – საწყისი ცოდნა დამრღვევისა ყოველი შეტევის სამიზნე პოსტისა და დაშვების უფლებების, რომელსაცეს დამრღვევი ფლობს, H –

პოსტები, რომლებთანაც დამრღვევს გააჩნია ფიზიკური ან შორიდან დაშვებული შეტევების დაწყებამდე განხორციელებამდე, K – კომპეტენტურობის დონე დამრღვევისა, ანუ კლასები ან სიები მისთვის ხელმისაწვდომი შემტევი მოქმედებებისა როგორც დაფუძნებული მოწყვლადობებზე, რომლებიც ხასიათდებიან განსხვავებული კრიტიკულობით, ასევე ინფორმაციის შეგროვების სხვადასხვა მეთოდებზე, 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 $BZ^V$.

დამრღვევის პოტენციალის მაჩვენებლის ცოდნის რაოდენობრივი შეფასებისათვის შემოთავაზებულია გამოყენებულ იქნას იდეა, რომელიც შემოთავაზებულია ნაშრომში [9], ზომოთ წარმოდგენიოლი ოპკ – ს გათვალისწინებით (იხ. ნახ. 3). დამრღვევის პოტენციალის დონე განიხილება კონტექსტში მათ მიერ განხორციელებული მოწყვლადობების ანალიზის შედეგებისა და კეთდება ვარაუდი იმის შესახებ, რომ შეუძლიათ მოწყვლადობები, რომლებიც იდენტიფიცირებულ იქნა აუდილის პროცესში გამოყენუბელ იქნან სხვადასხვა პოტენციალის დონის დამრღვევის მიერ. იზ – ის პოტენციალის ანალიზისას, პოტენციალისა რომელსაც უნდა ფლობდეს დამრღვევი მოწყვლადობის რეალიზაციისათვის, აუცილებელია ექსპერიმენტულად შეფასდეს ცოდნამოწყვლადობების იდენტიფიკაციისა და რეალიზაციის პარამეტრებისა:

– დამრღვევის ტექნიკური კომპეტენტურობის დონე ( $A^{'}_{<K'>}$ )

– შორიდან იდენტიფიკაციის და იზ – ის საშუალებების ხარისხი $A^{'}_{<K'>}$.

– დროითი დანახარჯები მოწყვლადობების იდენტიფიკაციისა და რეალიზაციაზე ( $A^{''}_{<K''>}$ ).

– შეტევის ობიექტზე (შო) ცოდნის მოცულობა ( $B^{'}_{<I'>}$ )

## 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. [3.4.]

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 მოვლენისა $A \approx (\hat{z} < \hat{y})$ ტოლია მათემატიკური მოლოდინისა მიმსი 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 (ალბათურებია $\hat{z}$ და $\hat{y}$) და ხარისხულ შესაბამისი გამონათქვამის ნამდვილობისა (სანდოობის ხარისხი მოვლენის $A = (\hat{z} < \hat{y})$ შემთხვევითია და შეიძლება მიიღოს მნიშვნელობები, რომლებიც განსხვავდებიან 0 და 1 – საგან ან $\overline{\omega}_1 \neq P(\hat{\omega}_1 = 1); \overline{\omega}_2 \neq P(\hat{\omega}_2 = 1)$

ამრიგად ჩამოყალიბებული მოსაზრებების თანახმად სიტუაციის გაურკვევლობა $\hat{\aleph}$ რომელშიც დამრღვევს მოუწევს იმოქმედოს, ხასიათდება სუპერინტელექტორის $\hat{\omega}$ შესაძლო მნიშვნელობებით, ხოლო შემთხვევითობა გამონათქვამისა $\hat{A}$ ხასიათდება ალბათობით P მისი უტყუარობის.

სუპერინდიკატორები $\hat{\omega}_1$ და $\hat{\omega}_2$ ითავსებენ თვისებებს და ფუნქციებს $\omega(\hat{y})$ (6) შემთხვევითი არგუმენტისა და შემთხვევითი ფუნქციის $\hat{\omega}(y)$ (7) ანუ წარმოადგენენ შემთხვევით ფუნქციებს შემთხვევითი არგემუნტებისა.

ფიზიკური არსი ასეთი თვისებებისა სოქასტური ინდიკატორებისა მდგომაროებს შემდეგში. პრაქტიკაში $\hat{z} < \hat{y}$ ცვლადი $\hat{y}$ განსაზღვრავს საზღვარს „გაურკვეველი“ („შემთხვევითი“) სიმრავლისა $\hat{A} = (-\infty, \hat{Y})$ რომელშიც მოხვედრისას შემთხვევითი სიდიდის $\hat{Z}$ ინდიკატორების $\hat{\omega}_1$ შეუძლია მიიღონ ნებისმიერი მნიშვნელობა ინტერვალიდან (0,1] სტოქასტური სუპერინდიკატორების მათემატიკური აპარატის პრაქტიკული გამოყენებისათვის აუცილებელია ცოდნა მათი განაწილების კანონებისა. შემოვიტანოთ აღნიშვნები

$$\hat{\omega}_2 \stackrel{d}{=} R_{\hat{y}}(\hat{z}); \omega = \omega(y) = R_{\hat{y}}(z); z = z(\omega) = R_{\hat{y}}^{-1}(\omega).$$

მაშინ, თუ განაწილების ფუნქციები $R_{\hat{y}}(y)$ და $R_{\hat{z}}(z)$ შემთხვევითი სიდიდეებისა $\hat{S}$ და $\hat{Z}$ ცნობილია , მაშინ

$$F_{\hat{\omega}_2}(\omega) \stackrel{d}{=} P(\hat{\omega}_2 < \omega) = P\{R_{\hat{Y}}(\hat{z}) < P_{\hat{Y}}[z(\omega)]\} = P[\hat{z} > z(\omega)] =$$
$$= R_{\hat{z}}[z(\omega)] = R_{\hat{z}}[R_{\hat{Y}}^{-1}(\omega)]. \ \omega \in (0,1].$$

შედეგად $F_{\omega_2}(\omega) = R_{\hat{z}}[R_{\hat{Y}}^{-1}(\omega)].$

როგორც უკვე ვაჩვენეთ, თანაფარდობა. $Y_{<3>}^{\Pi} \in \{Y_{<3>}^{\partial}\}$ წარმოადგენს დარღვევის იზ – ის მიზნის ფორმატურ გამოსახულებას. შემოვიტანოთ შემდეგი აღნიშვნები: $V^T \stackrel{d}{=} \hat{Z}; \ r^n \stackrel{d}{=} \hat{Z}_z; \tau^D \stackrel{d}{=} \hat{Z}_3$

მაშინ კრიტერიუმები იზ – ის რომელიც ხორციელდება დამრღვევის მიერ, შედეგების ვარგისიანობისა მიიღებს სახეს:

$$G_{LP} : (\hat{Y}_{<3>} \in \{\hat{Y}_{<3>}^{\partial}\} \simeq (\hat{Y}_{<3>} \stackrel{\geq}{<} \hat{Z}_{<3>}) \simeq [(\hat{Y}_1 \geq \hat{Z}) \cap (\hat{Y}_2 \leq \hat{Z}_2) \cap (\hat{Y}_3 \leq \hat{Z}_3)]$$

შედეგად, დამრღვევის მიერ მიზნის მიღწევის ოპერაციის ალბათობა განისაზღვრება გამოსახულებით

$$P_{DL}^{NB} = P(\hat{Y}_{<3>} \in \{\hat{Y}_{<3>}^{\partial}\}) = P(\hat{Y}_{<3>} \stackrel{\geq}{<} \hat{Z}_{<3>}) = \begin{cases} \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \Phi_{\hat{Z}_{<3>}}(Z_{<3>}) dF_{\hat{Z}<3>}(Z_{<3>}) \\ \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \overline{\Phi}_{\hat{Z}_{<3>}}(Y_{<3>}) dF_{\hat{Y}<3>}(Y_{<3>}) \end{cases} \quad (9)$$

(9) გამოსახულების სტრუქტურიდან ჩანს, რომ $P_{DL}^{NB}$ წარმოადგენს მათემატიკურ მოლოდინს ერთ – ერთი შემთხვევითი სიდიდისა:

$$\hat{\omega}_1^{<3>} \overset{d}{=} \Phi_{\hat{Y}_{<3>}}(\hat{Z}_{<3>}) \text{ ან } \hat{\omega}_2^{<3>} \overset{d}{=} \Phi_{\hat{Z}_{<3>}}(\hat{Y}_{<3>})$$

რომლებსაც ეწოდებათ პირველი და მეორე სტოქარტიკური სუპერინდიკატორები მესამე რანგის. შესაბამისად:

$$P_{DL}^{NB} = \overline{\omega}_i^{<3>} = M_{\hat{\omega}_i^{<3>}} = M[\hat{\omega}_i^{<3>}] = \int_0^1 \omega dF_{\hat{\omega}_i^{<3>}}(\omega), \ [i = 1,2].$$

ამასთან დაკავშირებით ალბათობა $P_{DL}^{NB}$ აქვს აზრი განვიხილოთ, როგორც საშუალო პირობითი (აპოსტერიორული) ალბათობა ოპერაციის მიზნის მიღწევისა. ყურადღება უნდა მივაქციოთ იმას, რომ მათემატიკური მოლოდინი $M[\hat{\omega}_i^{<3>}]$ შემთხვევითი სიდიდისა $\hat{\omega}_2^{<3>}$ (ტოქასტიკური მესამე რანგის სუპერინტიალური) იძლევა პროგნოზს მხოლოდ საშუალო შედეგებისა მომავალი მასობრისი ცდებისა, მაშინ როცა კანონი განაწილებისა $F_{\hat{\omega}_2^{<3>}}(\omega)$ სუპერინდიკატორისა $\hat{\omega}_2^{<3>}$ საშუალებას იძლევა გაკეთდეს პროგნოზირება ერთეულოვანი ცდებისა.

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

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

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 (რთეულოვანი) ოპერაციებისა განსხვავებით ალბათობისაგან, რომელიც საკმარისად სრულად ახასიათებს ეფექტურობას მხოლოდ

მასობრივი ოპერაციების. თავისი ბუნებით რეალიზაცია იზ – ის სცენარისა უნიკალურია, რაც მიგვანიშნებს დიდ მნიშვნელობაზე მაჩვენებლის $\omega_{DL}^{\Gamma}(\gamma)$. 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 ვეტორის $\hat{Z}_{<n>}$ 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 უნიკალუროი 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 მოვლენებისა იქნება იმ, 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 მახასიათებლებისა 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 სუპერინდიკატორებისა, 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.

## გამოყენებული ლიტერატურა


1.Massif FP7 Project. Management of Security information and events in Service Infrastructures. http://www.massif-progect.eu.

2.Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Тр. СПИИРАН. 2012.Вып. 1(20).С. 27-56.

3.Kotenko I. And DoynikovaE. Security Assessment of Compiuter Networks based on Attack Graphs and Security Events //Proc.of the 2014 Asian Conf. On Availability, Reliability, and Security, LNCS, 2014. P.462-471.

4.McGuire G.T., Waltermire D., Baker J> O. Common Remediation Enumeration (DRE) Version 1.0 (Draft)// NIST Interagecy Report 7831 (Draft). – National Institute of Standards and Technology, Dec. 2011. – 33p.

5.Johnson C. Enterprise Remediation Automation // Proc. Of the IT Security Automation Conf., Sept. 27-29, 2010. NIST. http//csap.nist.gov/events/2010/itsac/presentations/day1/ Automation_Specifications-Eterprise_Remedation_Automation.pdf.

6. Kotenko I., Stepashkin M. Attack Gdaph based Evaluation of Network Security // Proc/ of the 10th IFIP Conf. On Communication and Multimedia Security (CMS"2006), Heraklion, Greece, 2006. P. 216-227.

7.Kheir N. Response Policies and Counter-Measures: Management Ofservice Dependencies and Intrusion and Reaction Impacts: PhD thesis. – Ecole Nationale Superieture des Telecommunication de Bretagne, 2010. – 229p.

8.Poolsappasit N., Dewri R., Eay I. Dynamic Security Risk Management Using Bayesian Attack Graphs // IEEE Transactions on Dependable and Security Computing. 2012. Vol. 9. N1 P. 61-74.

9.Balepin I., Maltasev S., Rowe J., Levitt K. Using Specification-Based Intrusion Detection for Automated Response // Proc. Of 6th Intern. Symp., RAID 2003. Lecture Notes in Computer Science, 2003. P. 136-154.

10.Cremonini M. And Martini P. Evaluating Information Security Investments from Attackers Perspecktive: the Return-On-Attack (ROA) // Workshop on the Economics of Information Security (WEIS'05), 2005. http://infosecon.net/workshoo/pdf/23.pdf

11.Hoo K. J. S. How Much is Enough? A Risk-Management Approach to Compiuter Security: PhD thesis . – Stanford University, June 2000. – 99p.

12.Grenadillo G. G., Debar H., Jacob G., Achemlal C. G. M. Individual Countermeasure Selection Based on the Return on Response Investment Index // Lectire Notes in Compiuter Science. 2012. Vol. 7531. P. 156-170.

13.Waltermire D., Quinn S., Scarfone K., Halbardier A. The Technical Specification for the Security Content Automation Protocol (SCAP):SCAP Version 1.2. Sept.2011. http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf.

14.Common Configuration Enumeration (CCE): http://cce.mitre.org/

15.Common Vulnerabilities and Exposures (CVE):http://cce.mitre.org/.

16.X-Force:http://xforce.iss.net/

17.Федорченко А. В., Чечулин А. А., Котенко И. В. Исследование открытыж баз уязвимостей и оценка возможности их применения в системах анализа зашишенности компьютерных систем и сетей // Информациооно-управляющие состемы.2014. №5.С. 72-79.

18.Mell P., Scarfone K. A Complete Guide to the Common Vulnerability Secoring SysremVersion 2.0, 2007. – 23p.

19. Котенко И. В., Степашкин М. В., Дойникова Е. В. Анализ зашишенности автоматизированных систем с учетом социо-инженерных атак // Проблемы информационной безопасности. Компьютерные системы. 2011. №3. С. 40-57.

20. Котенко И. В., Новикова Е. С. Визуальный анализ для оценки зашишенности компьютерных сетей // Информационно-управляющие системы. 2013. №3. С. 55-61.

21. კუპრაშვილი ჰ., ოდიშარია კ., ალფაიძე ი. სახელმწიფოს პრობლემები და სისტემური მიდგომა მათ დასაძლევად. საისტორიო ვერტიკალები. 37-38. 2017. გვ. 332

22. კუპრაშვილი ჰ., ოდიშარია კ., ალფაიძე ი. თანამედროვე ინფორმაციული ტექნოლოგიების როლი საქართველოს სახელმწიფო სისტემის სრულყოფაში. საისტორიო ვერტიკალები. 39. 2018. გვ. 39

23. ივანე ალფაიძე. ელექტრონული ხელისუფლების ინფორამაციული უსაფრთხოების სტრატეგიული მართვის კოგნიტური მოდელი. სტუ. „განათლება“. №1(24). 2019. გვ. 201.

24. ალფაიძე ი. ბრძოლა კიბერთაღლითობის წინააღმდეგ, პრობლემები და პერსპექტივები. სტუდენტთა 86–ე ღია საერთაშორისო კონფერენცია. სტუ. 2019წ