საქართველოს ტექნიკური უნივერსიტეტი

თამარ ქიტიაშვილი

ინფორმაცია-უსაფრთხოების სახელმწიფო სამსახურში

წარმოდგენილია დოქტორის აკადემიური ხარისხის
მოსაპოვებლად

სადოქტორო პროგრამა „ინფორმატიკა“, შიფრი - 0401

საქართველოს ტექნიკური უნივერსიტეტი
თბილისი, 0175, საქართველო
2016

სამუშაო შესრულებულია საქართველოს ტექნიკური უნივერსიტეტში
ინფორმატიკისა და მართვის სისტემების ფაკულტეტი
გამოთვლით მათემატიკის დეპარტამენტი

ხელმძღვანელი: პროფესორი დავით ბურჭულაძე

რეცენზენტები _____
_____

დაცვა შედგება 2016 წლის ——— თებერვალს ——— საათზე
საქართველოს ტექნიკური უნივერისტეტის ინფორმატიკისა და მართვის სისტემების ფაკულტეტის სადისერტაციო საბჭოს კოლეგიის სხდომაზე
კორპუსი ——— აუდიტორია ———
მისამართი: 0175, თბილისი, კოსტავას 77

დისერტაციის გაცნობა შეიძლება სტუ-ს ბიბლიოთეკაში,
ხოლო ავტორეფერატისა - ფაკულტეტის ვებ-გვერდზე

სადისერტაციო საბჭოს მდივანი, პროფესორი: თინათინ კაიშაური

საქართველოს ტექნიკური უნივერსიტეტი

ინფორმატიკისა და მართვის სისტემების ფაკულტეტი

ჩვენ, ქვემოთ ხელისმომწერნი ვადასტურებთ, რომ გავეცანით თამარ ქიტიაშვილის მიერ შესრულებულ სადისერტაციო ნაშრომს დასახელებით **„ინფორმაცია-უსაფრთხოების სახელმწიფო სამსახურში“** და ვაძლევთ რეკომენდაციას საქართველოს ტექნიკური უნივერსიტეტის ინფორმატიკისა და მართვის სისტემების სადისერტაციო საბჭოში მის განხილვას დოქტორის აკადემიური ხარისხის მოსაპოვებლად.

2016 წელი

ხელმძღვანელი: პროფ.დავით ბურჭულაძე

რეცენზენტი: _____

რეცენზენტი: _____

საქართველოს ტექნიკური უნივერსიტეტი
2016 წელი

ავტორი: თამარ ქიტიაშვილი
დასახელება: ,,ინფორმაცია-უსაფრთხოების სახელმწიფო სამსახურში‘‘
ფაკულტეტი: ინფორმატიკისა და მართვის სისტემების ფაკულტეტი
ხარისხი: დოქტორი
სხდომა ჩატარდა:

ავტორის ხელმოწერა

რეზიუმე

თანამედროვე საქმიანობა წარმოუდგენელია საინფორმაციო სისტემების გამოყენების გარეშე. ასეთი სისტემების ინფორმაციული უსაფრთხოება ორგანიზაციის საქმეთა წარმოების ერთ-ერთ გადამწყვეტ ფაქტორს წარმოადგენს. საინფორმაციო სისტემების სწრაფმა განვითარებამ გამოიწვია მათი ფართო გავრცელება ყოველდღიურ ცხოვრებაში, რამაც სულ უფრო მნიშვნელოვანი გახადა საიმედობის და უსაფრთხოების გარანტია. ნაშრომში გაანალიზებულია თანამერდროვე ორგანიზაციის ძირითადი თავისებურებები და წარმოდგენილია ამ თავისებურებებიდან გამომდინარე საინფორმაციო სისტემების დაცვის პრობლემები და ამოცანები.

საქართველოში, ამ ეტაპზე, ინფორმაციული უსაფრთხოება, როგორც პროფესია, ჩამოყალიბების პროცესშია. ბანკებისა თუ სხვა ორგანიზაციებში ამ სფეროს სპეციალისტებს ექმნებათ დიდი პრობლემები, რადგანაც მათ არ გააჩნიათ შესაბამისი ბერკეტები და გამოცდილება. ჩვენი აზრით, დღესდღეისობით ეს არის ყველაზე მოთხოვნადი და აქტუალური საკითხი, განსაკუთრებით საბანკო სექტორისთვის, რადგანაც მათ აქვთ მთელი რიგი ინფორმაციები, რომლის კონფედენციალურობაც არავითარ შემთხვევაში არ უნდა დაირღვეს.

ინფორმაცია წარმოადგენს ცნობებს, რომლებიც მიიღება გამოკვლევების, შესწავლის ან განსწავლის შედეგად: სიახლეს, ფაქტებს, მონაცემებს; ბრძანებებს ან მონაცემთა წარმოდგენის სიმბოლოებს (კავშირის საშუალებებში ან კომპიუტერზე); ცოდნას (შეტყობინება, ექსპერიმენტული მონაცემები, გამოსახულებები), რომლებიც ცვლიან ფიზიკურ ან გონებრივი გამოცდილების შედეგად მიღებულ კონცეფციას. უსაფრთხოება განისაზღვრება, როგორც თავისუფლება საფრთხეთაგან, დაცულობა. თუ გავაერთიანებთ ამ ორ ცნებას, მივიღებთ ინფორმაციული უსაფრთხოების განსაზღვრას, რომელიც წარმოადგენს არასანქცირებული გამოყენების, ბოროტად გამოყენების, ცნობების, ფაქტების, მონაცემების ან აპარატურული საშუალებების შეცვლის ან მათ წვდომაზე მტყუნების აღმოფხვრის მიზნით მიღებულ ზომებს.

ზემოთქმულიდან გამომდინარე, ინფორმაციული უსაფრთხოება არ უზრუნველყოფს აბსოლუტურ დაცვას. ის არის გამაფრთხილებელ მოქმედებათა ერთობლიობა, რომელიც საშუალებას იძლევა დაცულ იქნას

ინფორმაცია და მოწყობილობები საფრთხეთაგან, რომელიც მოსალოდნელია მათი სუსტი ადგილების გამოყენებით.

„უკანასკნელ ათწლეულში მნიშვნელოვნად გაფართოვდა ინფორმაციული უსაფრთხოების უზურნველყოფის საშუალებები. მრავალი სხვადასხვა ორგანიზაცია ჩაერთო დაცვის უზურნველყოფის ამოცანების გადაწყვეტაში. კომპიუტერებისა და კომპიუტერული ქსელების რიცხვის ზრდამ და ტექნოლოგიების ფართოდ გამოყენებამ მნიშვნელოვნად გააფართოვა არა მხოლოდ მომხმარებლები და მათი ერთმანეთთან ურთიერთობათა საშუალებები, არამედ გაზარდა ქსელური ბიზნეს-პროცესების რეალიზაციის შესაძლებლობები. ამასთან ერთად იზრდება მონაცემების დაკარგვის რისკი. სტატისტიკა უჩვენებს, რომ ყოველწლიურად იზრდება კომპიუტერული დამნაშავეების მიერ მიყენებული ფინანსური ზარალი“.[9]

აქედან გამომდინარე, ორგანიზაციებს, კომპანიებს და რიგით მომხმარებლებს უხდებათ გამოყონ დრო და საშუალებები ინფორმაციისა და ქსელური რესურსების უსაფრთხოების დაცვის უზრუნველსაყოფად.

ინფორმაციული უსაფრთხოება მოიცავს უსაფრთხოების მრავალ ასპექტს. საიმედო დაცვის ყველა საშუალების და მეთოდის გაერთიანებას. საიმედო ფიზიკური დაცვაა საჭირო მატერიალური აქტივების – სისტემების დაცულობის უზრუნველსაყოფად. კომუნიკაციის დაცვა (COMSEC) უზრუნველყოფს ინფორმაციის გადაცემის უსაფრთხოებას. გამოსხივების დაცვას (EMSEC) საჭიროა, თუ მოწინააღმდეგეს აქვს მძლავრი აპარატურა კომპიუტერული უსაფრთხოება (COMPUSEC) საჭიროა კომპიუტერულ სისტემებში წვდომის მართვისათვის, ხოლო ქსელის უსაფრთხოება (NETSEC) – ლოკალური ქსელის დაცვისათვის. დაცვის ყველა სახეობა ერთობლივად უზურნველყოფს ინფორმაციულ უსაფრთხოებას (INFOSEC).

შეიძლება ითქვას, რომ XXI საუკუნე არის ინფორმაციული საუკუნე. ამავე დროს იზრდება ინფორმაციაზე ბოროტმოქმედება და წარმოიშვა ინფორმაციის დაცვის აუცილებლობაც. გამოცდილება გვიჩვენებს, რომ ამ ტენდენციასთან საბრძოლველად საჭიროა ინფორმაციული რესურსების დაცვის პროცესის მიზანმიმართული ორგანიზაცია, რაშიც უნდა მონაწილეობდნენ პროფესიონალი სპეციალისტები, ადმინისტრაცია, თანამშრომლები და მომხმარებელი, რაც აამაღლებს საკითხის ორგანიზაციულ მხარეს.

ბოლო ხანებში, როგორც ჩვენს ქვეყანაში, ასევე საზღვარგარეთ, მნიშვნელოვანი სამუშაოები ტარდება კიბერუსაფრთხოების გაზრდის თვალსაზრისით, თუმცა პრობლემის სრულად გადაჭრამდე ჯერ კიდევ დიდი მანძილია გასავლელი, რადგანაც რთულდება სისტემები, იხვეწება შეტევების მეთოდები და მექანიზმები.

Resume

Contemporary activities are impossible without using information systems. Information security of such systems is one of the crucial factors of organization proceedings. Rapid development of information systems caused the fact that they are widespread in our daily lives that made it more important to ensure reliability and security. Main features of modern organization are analyzed and according to these features problems and objectives of protection of information systems are presented in this paper.

At this stage, information security as a profession in the progress of establishment in Georgia. Specialist of the field face a number of problems in banks or other organizations as they do not have corresponding leverage and experience. To our point of view, nowadays this is the most demanded and actual issue, especially for bank sector as they have a great number of information the confidentiality of which shall not be violated.

Information is the details which are obtained as a result of researches, observation or examination; it is news, facts, data; orders or data symbols (in connection means or computers); knowledge (notification, experimental data, images) which change the concept received from physical or mental experience. Security is defined as freedom from threat, safety. If we combine these two concepts we will get the definition of information security which is the measures taken for the purpose of preventing non-sanction usage, abuse, and change of notifications, facts or data.

Therefore, information security does not provide absolute protection. It is the combination of preventive actions which enables to protect information and devices from the threat which is expected from the usage of their weaknesses.

For the last decade the means of providing information security have been significantly extended. A lot of different organizations are involved in solving the objectives of providing protection. Increasing number of computers and computer networks and wide use of technologies greatly expanded not only customers and the means of their communication but also increased the opportunities of realizing network business processes. In addition, the risk of losing data is increasing. Statistics shows that financial damage caused by computer criminals are increased annually.

Accordingly, organizations, companies and ordinary customers have to allocate time and means to provide protection of information and security of network resources.

Information security includes multiple aspects of security; combination of all the means and methods of reliable protection. Reliable physical protection is needed to provide the security of material assets. Communication security (COMSEC) ensures the security of transferring information. Emission security (EMSEC) is needed if the opposite party has powerful equipment. Computer security (COMPSEC) is necessary to manage access, and Network security – for protection of local network. All the types of protection jointly provide information security (INFOSEC).

It may be said that XXI century in an information century. At the same time, crimes related to information are increasing and the necessity of protecting information has been created. Experience shows us that to fight against this tendency it is necessary to organize the process of protection of information resources where professional specialists, administration, staff and customers shall participate that will raise the organizational side of the issue.

Considering the threats and challenges of the international system planning and implementation of Georgia's security policy discusses the following threats and challenges in the field of cyber security:

Recently, both in our country and abroad important works are performed in terms of increasing cyber security, however, a long distance has to be gone till the problems are solved as systems are complex, attack methods and mechanisms are improved.

The dissertation thesis consists of introduction, three chapters, summary, list of literature used and annex.

შინაარსი

ნახაზების ნუსხა

დისერტაციაში გამოყენებული აბრევიატურები

იუკუ - ინფორმაციული უსაფრთხოების კომპლექსური უზრუნველყოფის სისტემა.

იდ - ინფორმაციის დაცვა.

ENISA - European Union Agency for Network and Information Security

COMSEC – Communications security - კომუნიკაციის დაცვა

EMSEC – Emission security - გამოსხივების დაცვა

COMPUSEC – Computer security - კომპიუტერული უსაფრთხოება

NETSEC - ლოკალური ქსელის უსაფრთხოება

INFOSEC – Information security - ინფორმაციული უსაფრთხოება

იდს - იფორმაციული დაცვის სისტემა

WLAN – Wireless local area network - უგამტარო ლოკალური ქსელები

იტ - ინფორმაციული ტექნოლოგიები

DNS – Domain name system - დომენური სახელის სისტემა

SMTP – Simple mail transfer protocol - უბრალო ფოსტის გადაცემის პროტოკოლი

HTTP – Hypertext transfer protocol - ჰიპერტექსტის გადაცემის პროტოკოლი

EPIC – Electronic Privacy Information Center - ელექტრონულ სისტემებში კონფიდენციალური ინფორმაციის დაცვის ცენტრი

ნქ - ნეირონული ქსელები

გა - გენეტიკური ალგორითმები

იუს - ინფორმაციული უსაფრთხოების სისტემები

დმ - დაცვის მექანიზმები

გკქ - გლობალური კომპიუტერული ქსელი

გმპ - გადაწყვეტილების მიმღები პირი

სტს - სოციოტექნიკური სისტემა

აკმ - არამკაფიო კოგნიტური მოდელი

შესავალი

თემის აქტუალურობა. ინფორმაციული უსაფრფთხოება არის ინფორმაციისა და ინფორმაციული სისტემების დაცვა, დაზიანებისა და განადგურებისაგან. დღეისათვის, როდესაც ინფორმაციულ სისტემებს მნიშვნელოვანი როლი აქვს ჩვენს ცხოვრებაში, ისმის მასში შემავალი ინფორმაციის უსაფრთხოების საკითხი.

თანამედროვე სამყაროს წარმოდგენა კომუნიკაციისა და გამოთვლითი ტექნიკის საშუალებების გარეშე შეუძლებელია. ინფორმაციული ტექნოლოგიური ვითარება ძალზედ სწრაფად და ისინი მოიცავენ ადამიანური შემოქმედების კიდევ უფროს ფართო არეალს. ამდენად, ინფორმაციული ტექნოლოგიების უსაფრთხოება მათი ფუნქციონირების უზრუნველყოფის უმნიშვნელოვანეს საკითხს წარმოადგენს.

მსოფლიოს მასშტაბით კომპიუტერები თითქმის სრულად მოიცავს ყველა მნიშვნელოვან ლეგალურ ოპერაციას. მათ შორის საქართველოში იგი უკვე გამოიყენება არამხოლოდ სოციალური კომუნიკაციებისათვის, არამედ კონტრაქტების გასაფორმებლად, შესყიდვების საწარმოებლად.

ნაშრომში წარმოდგენილია ის ფაქტორები, რომლებიც რეალურ საფრთხეს წარმოადგენენ, ასევე მოცემულია მეთოდები და პრინციპები, რომლის შესრულება აუცილებელია, რათა შეიქმნას დაცული ქსელური ინფრასტუქტურა.

კვლევის მიზანი და ამოცანები. ინფორმაციის ცნება დღესდღეობით გამოიყენება საკმაოდ ფართოდ და მრავალმხრივად. უზარმაზარი ინფორმაციული ნაკადი მოედინება ადამიანების გარშემო. შეიძლება ითქვას, რომ 21-ე საუკუნე ინფორმაციული საუკუნეა. ამავე დროს იზრდება ინფორმაციაზე ბოროტმოქმედება, და წაროიშვება ინფორმაციის დაცვის აუცილებლობაც.

გამოცდილება გვიჩვენებს, რომ:

- ინფორმაციული უსაფრთხოების უზრუნველყოფა არ შეიძლება იყოს ერთჯერადი აქტი. ეს უწყვეტი პროცესია, რომელიც მდგომარეობს დაცვის სისტემის სრულყოფისა და განვითარებისათვის უფრო რაციონალური მეთოდების, ხერხებისა და გზების დაფუძნებასა და რეალიზაციაში, დაცვის სისტემის მდგომარეობის განუწყვეტელ კონტროლში, სისტემის სუსტი ადგილების გამოვლენაში.

- ინფორმაციის უსაფრთხოება იყოს უზრუნველყოფილი სისტემის ყველა სტრუქტურულ ელემენტზე და ინფორმაციის დამუშავების ტექნოლოგიური ციკლის ყველა ეტაპზე.
- მნიშვნელოვანი ეფექტი მიიღწევა მაშინ, როცა გამოყენებული მეთოდი, საშუალება და მიღებული ზომები ერთიანდება მთლიან ორგანიზმად – ინფორმაციის დაცვის სისტემად (იდს). ამავე დროს სისტემის ფუნქციონირება უნდა იყოს კონტროლირებადი, განახლებადი და შევსებადი, გარე და შიდა პირობების ცვლილების მიხედვით.
- იდს უნდა აკმაყოფილებდეს ინფორმაციის უსაფრთხოების მოთხოვნილ დონეს, რისთვისაც საჭიროა მომხმარებელთა მომზადება და მათ მიერ ინფორმაციის დაცვისათვის გამიზნული ყველა წესის დაცვა.

საქართველოში, ამ ეტაპზე, ინფორმაციული უსაფრთხოება, როგორც პროფესია, ჩამოყალიბების პროცესშია. ბანკებისა თუ სხვა ორგანიზაციებში ამ სფეროს სპეციალისტებს ექმნებათ დიდი პრობლემები, რადგანაც მათ არ გააჩნიათ შესაბამისი ბერკეტები და გამოცდილება. ჩვენი აზრით, დღესდღეისობით ეს არის ყველაზე მოთხოვნადი და აქტუალური საკითხი, განსაკუთრებით საბანკო სექტორისთვის, და არა მარტო, რადგანაც მათ აქვთ მთელი რიგი ინფორმაციები, რომლის კონფედენციალურობაც არავითარ შემთხვევაში არ უნდა დაირღვეს.

ნაშრომის მოცულობა და სტრუქტურა. სადისერტაციო ნაშრომი შედგება შესავალის, სამი თავისაგან, დასკვნისა და გამოყენებული ლიტერატურის სიისაგან.

შესავალ ნაწილში ზოგადად დახასიათებულია სადისრტაციო ნაშრომის პრობლემატიკა.

პირველ თავში აღწერილია საინფორმაციო ტექნოლოგიების და სისტემების როლი თანამედროვე სახელმწიფოების მდგრად განვითარებაში და მათთან დაკავშირებული მუქარები, საფრთხეები და საშიშროებები.

მეორე თავში განხილულია მსოფლიოს განვითარებული ქვეყნების კიბერუსაფრთხოების სტრატეგიები, საერთო პრინციპები, რეკომენდაციები და ამ მიმართულებით საქართველოში არსებული მდგომარეობა.

მესამე თავში განხილულია სახელმწიფოში კრიტიკული ინფრასტრუქტურის კიბერუსაფრთხოების ინოვაციური მეთოდები და საშუალებები.

I. ლიტერატურის მიმოხილვა

1.1. საინფორმაციო ტექნოლოგიების და სისტემების როლი თანამედროვე სახელმწიფოების მდგრად განვითარებაში და მათთან დაკავშირებული მუქარები, ზოგადი საფრთხეები და საშიშროებები.

ოცდამეერთე საუკუნეში მნიშვნელოვნად გაიზარდა კომპიუტერული ტექნოლოგიის როლი. მსოფლიო ორგანიზაციები ცდილობენ მათი საქმიანობის ძირითადი ნაწილის ავტომატიზებას ელექტრონული სისტემების და ტექნოლოგიების დანერგვით. ამ ფაქტმა განაპირობა კონფედენციალური ინფორმაციის დაცვის აუცილებლობა. შეიქმნა სპეციალური სისტემები, რომლებიც განსაზღვრავენ ინფორმაციასთან წვდომის საფეხურებს. ამ ყველაფრის გათვალისწინებით მთელ რიგ ორგანიზაციებში შეიქმნა მონიტორინგისა და ინფორმაციული უსაფრთხოების დეპარტამენტები, რომლებიც იცავენ ორგანიზაციას არასასურველი მომხმარებლისგან.

”მსოფლიოს წამყვან მეცნიერთა აზრით ინფორმაციული ტექნოლოგიების თავბრუდამხვევმა განვითარებამ საფუძველი დაუდო მთელს მსოფლიოში ახალი ფასეულებების სისტემის ფორმირებას, სადაც გლობალური ეკონომიკა და გლობალური სოციუმი იკავებს ადგილს. ცნობილი ესპანელი მკვლევარი მანუელ კასტელი კი 21-ე საუკუნის ეკონომიკის ქსელურს უწოდებს. მისი აზრით უშუალოდ ქსელების განვითარებაზე იქმნება დამოკიდებული ამა თუ იმ ქვეყნის და საერთოდ მსოფლიოს ეკონომიკის განვითარება. ამერიკელი ეკონომისტი ლ.ტუროუ კი მიიჩნევს, რომ ინფორმაციული ეკონომიკის პირობებში იზრდება კომპანიების დასაქმებული პერსონალის თავისუფლების ხარისხი და მათი გადაწყვეტილების უფრო თავისუფლად მიღების საშუალება ეძლევათ“.[21]

ჩვენ პირველ რიგში ყურადღება უნდა გავამახვილოთ იმ უარყოფით ფაქტორებზე, რომლებიც ხელს უშლიან ინფორმაციული ტექნოლოგიების დანერგვა-განვითარებას, სერიოზულ საფრთხეს უქმნიან ცალკეულ სახელმწიფოებს და მთელს მსოფლიოს პროგრესულ საზოგადოებასაც კი ამ ტექნოლოგიათა შესაძლებლობების არამართლზომიერი გამოყენებით. ე. ი. მხედველობაში გვაქვს ორი ძირითიდი ფაქტორი: ერთი, რომელიც

ცნობილია კომპიუტერული დანაშაულობათა სახელით და მიმართულია ინფორმაციული რესურსების არაკანონიერ გამოყენება-მითვისებაზე, მათ დაზიანებაზე და მეორე, როდესაც დანაშაულებრივი ჯგუფები, მაგალითად სხვადასხვა ტერორისტული დაჯგუფებები გლობალურ ინფორმაციულ ტექნოლოგიებს იყენებენ თავიანთი მიზნების განსახორციელებლად.

მას შემდეგ, რაც ტექნოლოგიურმა პროგრესმა შეაღწია ყველა სფეროში და მათ შორის ბიზნესში, აქტიურად ხდება ინფორმაციის გაცვლა და გადაცემა. ეს ყველაფერი კი ხელს უწყობს იმ საკმაოდ ძვირფასი და ღირებული ინფორმაციის გადინებას, რასაც კომპანიისთვის სასიცოცხლო მნიშვნელობა აქვს.

მეოცე საუკუნის დასასრულს ტექნიკურმა პროგესმა თავის დადებით შედეგებთან ერთად ნათლად დაგვანახა ის საშიშროებები, რომლებიც წარმოიშობიან ბუნებრივი რესურსების ინტენსიური მოხმარებისას, მნიშვნელოვნად გაიზარდა ანთროპოგენული ხასიათის კატასტროფების დადგომის შესაძლებლობები. ამავდროულად ინფორმაციული ტექნოლოგიების საოცარმა პროგრესმა მეცნიერებაში წარმოშვა აზრი, რომ კაცობრიობის გადარჩენის და შემდგომი პროგრესის აუცილებელი პირობაა საზოგადოების ინფორმატიზაცია – ინფორმაციული სივრცეების, მისი ინფრასტრუქტურის ყოველმხრივი განვითარება და უსაფთხო ფუნქციონირება.

თანამედროვე საზოგადოება გადადის თავისი განვითარების პოსტინდუსტრიულ პერიოდში, რომელსაც საყოველთაო აზრით შეიძლება ვუწოდოთ ინფორმაციული.

ფაქტია, რომ ინფორმაციული საზოგადოების განვითრებას, გარდა შემოქმედებითი შესაძლებლობების გაფართოებისა, მივყავართ ეროვნული უსაფრთხოების მუქარების გაზრდამდე, რომლებიც დაკავშირებული არიან ინფორმაციული და საკომუნიკაციო სისტემების დადგენილი რეჟიმების დარღვევასთან, ასევე მოქალაქეთა კონსტიტუციური უფლებების დარღვევასთან, მავნე პროგრამების გავრცელებასთან, აგრეთვე თანამედროვე ინფორმაციული ტექნოლოგიების (იტ) შესაძლებლობების გამოყენებასთან მტრულ, ტერორისტულ და სხვა დანაშაულებრივ მოქმედებებთან.

ამასთან დაკავშირებით განსაკუთრებულ აქტუალურობას იძენს ინფორმაციის საიმედოდ დაცვის პრობლემა (ინფორმაციის დამახინჯება ან

განდაგურება, არასანქცირებული მოდიფიკაცია, ბოროტზრახულად მიღება და გამოყენება).

აღნიშნული, შეიძლება ითქვას, ერთ-ერთი ურთულესი და უმნიშვნელოვანესი პრობლემის გადაწყვეტაში ჩართული არიან მსოფლიოში იტ წამყვანი კომპანიები, ექსპეტრები, მეცნიერები, მიმდინარეობს ინტესიური და მსხვილმასშტაბიანი კვლევები და პროექტების დამუშავება, რომელთა ძირითად მეთოდოლოგიურ ინსტრუმენტს წარმოადგენს აპარატი სისტემური ანალიზისა და გადაწყვეტილებათა მირების თეორიისა.

მეთოდები და მეთოდოლოგიები, რომლებიც მუშავდებიან ამ მიმართულების ფარგლებში შეიძლება გამოყენებულ იქნას როგორც ანალიზის ეტაპზე პრობლემაშემცველი ინფორმაციული სისტემის (ის), ასევე სინთეზის ეტაპზე პრობლემაგადამწყვეტი ინფორმაციული უსაფრთხოების კომპლექსური უზურუნველყოფის სისტემისა (იუკუ) ინფორმაციის დაცვის (იდ) მიზნების დასასმელად, დასამუშავებლად სამართლებრივი, ორგანიზაციული და პროგრამულ-ტექნიკური ზომების და საშუალებებისა, რომლებიც უზურნველყოფენ დასახული მიზნების რეალიზებას, ასევე არჩეული ტექნიკური გადაწყვეტების დასაბუთებულობისათვის.

ამ დროს უმთავრესია და განსაკუთრებული მნიშვნელობა აქვს უსაფრთხოების შესაბამისი მუქარების სისტემურ ანალიზს. ასეთი ანალიზის საფუძველი უნდა იყოს მუქარების კლასიფიკაცია გარკვეული ბაზური პარამეტრების მიხედვით, რომლებიც საშუალებას აძლევენ მკვლევარს ერთიანობაში წარმოადგინონ დესტრუქციული ზემოქმედებები და მათი შედეგები.

ამრიგად, მთავარი ამოცანაა განხორციელდეს სისტემური ანალიზი იუ მუქარებისა და დამუშავდეს მეთოდიკა მათი წარმოშობის აპრიორული ალბათობის დონის შეფასებისა.

1.2. ინფორმაციული ტექნოლოგიები - მათი როლი და ადგილი თანამედროვე მსოფლიოს განვითარებაში.

ინფორმაციული ტექნოლოგიების (იტ) ქვეშ ვგულისხმობთ ყველაფერს იმას, რაც საშუალებას იძლევა განხორციელდეს ინფორმაციის მოპოვება, მიღება, გადამუშავება, შენახვა და გადაცემა - ის ყველაფერი, რაც ინფორმაციას აქცევს უმნიშვნელოვანეს საწარმოო რესურსად მატერიალური და ენერგეტიკული რესურსების მსგავსად. იტ ესაა, პირველ რიგში, საკომუნიკაციო სისტემები, საშუალებები და მეთოდები. გასული საუკუნის მიწურულს და მიმდინარე საუკუნის დასაწყისში გამოთვლით ტექნიკაში რევოლუციური მიღწევენის - ნანო ტექნოლოგიის განვითარების შედეგად ნათელი გახდა 21-ე საუკუნისთვის ინფორმაციის საუკუნის სახელწოდების მინიჭების არსი.

ინფორმაციული უსაფრთხოება არის ინფორმაციის დაცვა მთელი რიგი საფრთხეებისაგან, რათა უზრუნველყოფილი იყოს ბიზნეს-პროცესების უწყვეტობა, რისკების შემცირება და ინვესტიციებიდან და ბიზნესის შესაძლებლობებიდან მოგების გაზრდა.

„ინფორმაციის უსაფრთხოება, ისევე როგორც ინფორმაციის დაცვა, კომპლექსური და რთული ამოცანაა, რაც მიმართულია უსაფრთხოების უზრუნველყოფისკენ და სპეციალური სისტემების დანერგვისკენ. ინფორმაციის დაცვა მთელი რიგი კომპანიებისთვის საკმაოდ პრობლემატური საკითხია და მოიცავს არაერთ ამოცანას. ინფორმაციის დაცვა უნდა მოხდეს ყველა იმ შემოტევებისაგან, რომელსაც ე.წ. „Adversaries“ გვიწყობენ, ესენი შეიძლება იყოს შემდეგი ჯგუფის წარმომდაგენლები: Terrorist; Criminals; Hackers; Government და ა.შ“.[11]

არსებობს უსაფრთხოების 6 კლასი: C1,C2,B1,B2,B3,A1. იმისათვის რომ, სისტემა სერტიფიკაციის პროცედურების შედეგად რომელიმე კლასს მივაკუთვნოთ, მისი უსაფრთხოების პოლიტიკა და გარანტირების დონე უნდა აკმაყოფილებდეს განსაზღვრულ მოთხოვნებს.

იმისათვის, რომ შესაძლებელი იყოს ორგანიზაციის ინფორმაციული უსაფრთხოების დაცვა აუცილებელია შემდეგი პროგრამული და აპარატურული პროდუქტების დანერგვა:

Antivirus – ანტივირუსი საშუალებას იძლევა მოვახდინოთ კომპიუტერში არსებული „ვირუსული“ ფაილების დეტექტირება,

ლოკალიზება და იმ შემთხვევაში თუ გექნებათ შესაბამისი მონიტორინგის სისტემები, შესაძლებელი იქნება აკონტროლოთ ცენტრალიზებულად თქვენ ქსელში არსებული კომპიუტერების მდგომარეობა.

Anti spy – ანტი ჯაშუში. სამწუხაროდ ანტივირუსებს არ აქვთ იმის შესაძლებლობა, რომ აღმოაჩინონ სისტემაში დამალული პროგრამები. იმასთვის, რომ ავიმაღლოთ სისტემის უსაფრთხოება და თავიდან ავიცილოთ ინფორმაციის გაჟონვა, საჭიროა გვქონდეს პროგრამული უზრუნველყოფა, რომელიც მოახდენს ჯაშუში პროგრამების დეტექტირებას და ნეიტრალირებას.

ადგილი	ვირუსი	პროცენტი საერთოდ დარეგისტრირებულ ინციდენტებში
1.	I-worm.klez	84,28%
2.	I-worm. Lentin	9,24%
3.	Win.95 CIH	0,93%
4.	I-worm. Frethen	0,90%
5.	I-worm. Desos	0,28%
6.	Win.32 Fun love	0,15%
7.	I-worm. Hybris	0,12%

Firewall – ყველაზე საჭირო და აუცილებელი ხელსაწყო გახლავთ IT სპეციალისტის ხელში, ჩვენი აზრით ორგანიზაციას, რომელიც ჯერ კიდევ არ აქვს ჩამოყალიბებული ინფორმაციული უსაფრთხოებიბს ინფრასტრუქტურა, მან უნდა დაიწყოს სწორედ ამ მექანიზმის დანერგვით.

რა არის Firewall? ეს არის აპარატურული ან პროგრამული უზრუნველყოფა, რომელიც ახორციელებს მასში შემავალი პაკეტების კონტროლს და ფილტრაციას. მის ძირითად დავალებას წარმოადგენს ლოკალური ქსელის ან ცალეკული კვანძების დაცვა არასანქცირებული წვდომისაგან, რომელიც კრძალავს არაავტორიზებულ წვდომას და ნებას რთავს მხოლოდ ავტორიზებულ კავშირს, როგორც ქსელიდან გამავალ პაკეტებზე, ასევე ქსელში შემავალ პაკეტებზე.

როგორც დაცვითი საშუალება, Firewall–ი პირველად გამოყენებულ იქნა 1988 წელს, როდესაც Digital Equipment Corporation კორპორაციის თანამშრომლებმა განაცხადეს პაკეტების ფილტრაციის სისტემის შექმნაზე

სახელწოდებით Firewall. Bill Cheswick და Steve Bellovin განაგრძობდნენ კვლევას პირველი ფილტრაციის სისტემაზე ამავე კომპანიაში.

კიდევ ერთი და ყველაზე აუცილებელი მექანიზმი, რომელიც აუცილებელია ინფრასტრუქტური მართვისთვის ე.წ. Firewall–ის შემდეგ, სასურველია დანერგილი იყოს Active Airectory. Active Directory (AD) არის კომპანია Microsoft–ის მიერ შემუშავებული ტექნოლოგია, რომელიც შეიქმნა ისეთი ქსელური მოწყობილობების მონიტორინგისა და მართვისათვის, როგორიცაა: LDAP directory services, Kerberos based authentication, DNS naming, უსაფრთხო კავშირი რესურსებთან და მრავალი სხვა. Active Directory იყენებს ერთ საერთო მონაცემთა ბაზას, რომელზე წვდომა და ინფორმაციის შენახვა მრავალ სხვადასხვა პროგრამას და სერვისს შეუძლია.

AD გამოიყენება სისტემის ადმინისტრატორების მიერ, რათა შეინახონ ინფორმაცია მომხმარებლის შესახებ, უსაფრთხოების პოლიტიკის შესახებ და დანერგოს სხვადასხვა პროგრამული პროდუქტი. განვიხილოთ Active Directory–ის ძირითადი სტრუქტურა, მუშაობის პრინციპები და შემდგენელი კომპონენტები.

Active Directory არის ადგილი, სადაც ინახება ინფორმაცია ხალხის, საგნების (კომპიუტერები, პრინტერები და ა.შ.), პროგრამების, სერვისების და უსაფრთხოების წესების შესახებ, ხოლო პროგრამები და სერვისები შემდეგ იყენებს ამ ინფორმაციას. მაგალითად: Microsoft Windows იყენებს Active Directory–ში არსებულ ინფორმაცია, რათა მომხმარებელს მისცეს სისტემაში შესვლის ნება (login) და მიენიჭოს ის უფლებები, რაც უსაფრთხოების პოლიტიკაშია გაწერილი [1,2]. თუ მომხმარებლის ანგარიში Active Directory–ში გაუქმებულია, მაშინ Windows არ აძლევს მას სისტემაში შესვლის უფლებას.

აღსანიშნავია, რომ AD საშუალებით ხდება პროგრამების დანერგვა. ქსელის ადმინისტრატორს შეუძლია შეიტანოს წესების პოლიტიკაში ცვლილებები იმის შესახებ, რომ კონკრეტული პროგრამა დაინერგოს კონკრეტული მომხმარებლისათვის. შემდეგ ამ ინფორმაციის საფუძვლეზე თავად მომხმარებლის ოპერაციული სისტემა Windows ახორციელებს აღნიშნული პროგრამის ინსტალაციას.

Active Directory შესაძლებლობას გვაძლევს შევქმნათ მოქნილი იერარქია ჩვენი გარმოსათვის. შესაძლებელია აიგოს იერარქია ნებისმიერი სასურველი გზით – გეოგრაფიული ადგილების, ქვეგანყოფილებების, ზოდიაქოს

ნიშნების და ა.შ. AD–ის სტრუქტურა იწყება forest და domain-ით და მთავრდება ორგანიზაციული ერთეულებითა და ობიექტებით. მოქნილი იერარქიული დიზაინი არის უპირატესობა ქსელური არქიტექტურისათვის, მაგრამ დასაწყისში არასწორად დაგეგმილი სტრუქტურა მომავალში შეიძლება საფრთხედ გადაიქცეს. აქედან გამომდინარე, აუცილებელია ხანგრძლივი ანალიზი, ვიდრე მის აგებას შევუდგებით.

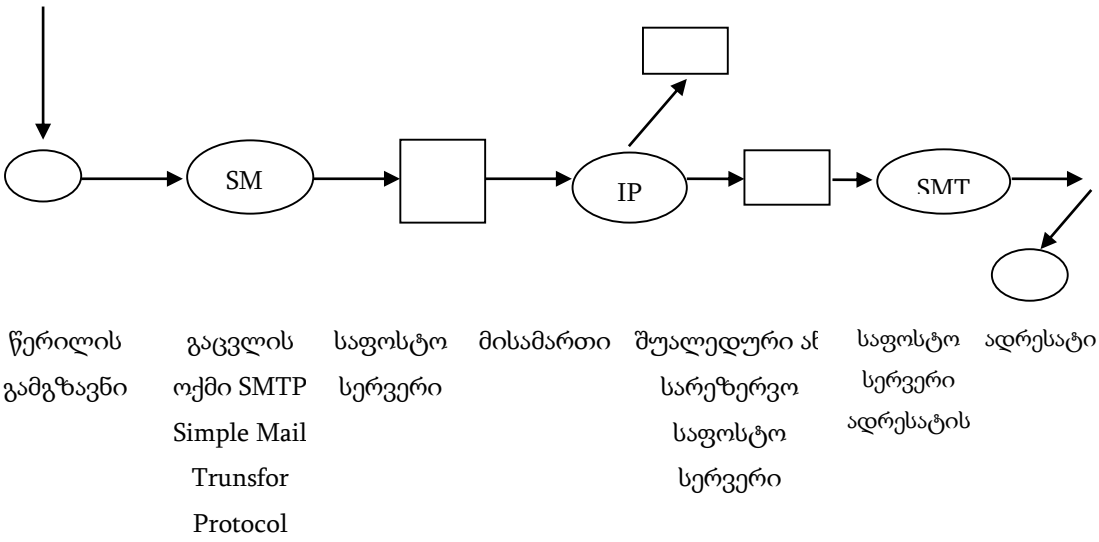
თანამედროვე ორგანიზაცია წარმოადგენს რთულ სისტემას, რომლის ჩარჩოებშიც ხორციელდება ინფორმაციის დაცვა. განვიხილოთ მისი ძირითადი თავისებურებანი:

- რთული საორგანიზაციო სიტუაციები;
- ფუნქციონირების მრავალი ასპექტი;
- მაღალი ტექნიკური აღჭურვილობა;
- ინფორმაციის ხელმისაწვდომობის გაფართოების აუცილებლობა;
- ტექნიკურ მატარებლებზე დიდი მოცულობის ინფორმაციის დაგროვება;
- სხვადასხვა დანიშნულების ინფორმაციის ინტეგრაცია ცალკეულ ბაზებში;
- ავტომატიზებული სისტემების რესურსებისადმი უშუალო და დროული ხელმისაწვდომობა;
- სხვადასხვა კატეგორიის დიდი რაოდენობის მომხმარებლების უშუალო და დროული ხელმისაწვდომობა ავტომატიზებული რესურსების სისტემებისადმი;
- განხილული თავისებურებებიდან გამომდინარეობს საინფორმაციო სისტემების დაცვის ძირითადი ამოცანები:
- საინფორმაციო სისტემაში მყოფი ინფორმაციის საიმედო დაცვა, გამიზნული და შემთხვევითი ინფორმაციის უცხო პირებზე მიღების კონტროლი, ადმინისტრაციისა და მომსახურე პერსონალის გამიჯვნა;
- მიუწვდომლობა დასაცავი სისტემის რესურსებისა და მოწყობილობებისადმი;
- დაცვა არ უნდა ქმნიდეს უხერხულობას იმ პირების მიმართ, რომლებიც ჩართულები არიან რესურსების დაცვის სისტემაში.

1.3. კომპიუტერული დანაშაულებათა მასშტაბები და მათგან მომდინარე საფრთხეები - კიბერუსაფრთხოება.

ფაქტია, რომ ინტერნეტი ყალიბდება როგორც სერიოზული პროფესიული გარემო, ასევე ფაქტია ისიც, რომ ე.წ. კომპიუტერული დამნაშავეები, მათ შორის ხაკერები, სხვადასხვა სახის ვირუსების შემქმნელები უფრო ხშირად ცდილობენ თავიანთი ჩვევებიდან მიიღონ მატერიალური სარგებელი. ისინი სხვდასხვა მეთოდებით, მათ შორის ე.წ. „ტროას ცხენის“ სახლეწოდებით ცნობილი მავნე პროგრამების გამოყენებით, ცდილობენ კომპიტერებიდან მოიპარონ ღირებული კონფიდენციალური ინფორმაცია, ასეთ რიცხვს მიეკუთვნება, მაგალითად, ინტერნეტში შეღწევის პირადი პაროლები, საკრედიტო ბარათების ნომრები, საბანკო ანგარიშებთან და კომერციულ დოკუმენტებთან შეღწევის კოდები და სხვა მრავალი.

კომპიტერულ დამნაშავეებს გააჩნიათ მთელი „არსენალი მეთოდებისა“, რათა შეტევები განახორციელონ ინტერნეტის (არა მარტო) ერთ-ერთ უმნიშვნელოვანეს მომსახურების სფეროზე, როგორიცაა ელექტრონული ფოსტა (ნახაზი 1.)



ამ შემთხევავში, უმეტეს წილად, გადასაცემი ინფორმაციის კოდირება არ ხდება და მისი გადაცემა ხდება ჩვეულებრივი ტექსტით.

საფოსტო სერვერი აანალიზებს წერილის მისამართის იმ ნაწილს, რომელიც მოიყვანება საფოსტო სერვერისა, რომელიც ემსახურება ადრესატს, მეორე ეტაპზე მყარდება კავშირი ამ სერვერთან და ხდება წერილის გადაცემა.

ამ შემთხვევაში იგულისხმება, რომ არ გამოიყენება წერილის ხელში ჩაგდებისათვის სპეციალური ტექნიკა. წერილი შეიძლება ხელში ჩაგდებული იქნას მხოლოდ გამგზავნისა და ადრესატის სერვერებზე.

გავრცელებულია გამგზავნის ან მიმღების კომპიუტერში შეღწევის გამოყენება კონკრეტული შეტყობინების ხელში ჩასაგდებად. ამ შემთხვევაში, ლოკალურ კომპიუტერში ხდება ფარული პროგრამის ჩაყენება (მაგალითად პროგრამა „ტროას ცხენი“) ბოროტგანმზრახველის საფოსტო მისამართზე შემავალი და გამომავალი ფოსტის გადამისამართებისათვის. ეს მეთოდი მხოლოდ კონკრეტული პირის ელექტრონული ფოსტის ხელში ჩასაგდებადაა კარგი, მაგრამ გამოუსადეგარია პირთა ჯგუფის წინააღმდეგ სამოქმედოდ, ვინაიდან იზრდება მსხვერპლის კომპიუტერზე გარეშე პირის ყოფნის აღმოჩენის რისკი.

e-mail-ზე ყურადღებას იმიტომ ვამახვილებთ, რომ ამ სერვისს გააჩნია მთელი რიგი უპირატესობანი, რაც განაპირობებს მის ფართოდ გავრცელებას. ეს უპირატესობებია:

ა) შეტყობინებათა მიწოდების უდიდესი სიჩქარე;

ბ) ადრესატისათვის შეტყობინების გარანტირებული მიწოდება;

გ) კონფედენციალობა.

როგორც პრაქტიკამ გვიჩვენა, ძალზე მწვავედ დგას ინტერნეტ მომსახურების ინფორმაციის კონფიდენციალობის უზრუნველყოფა. გარდა ამისა პრობლემას წარმოადგენს ის, რომ სტანდარტული ფოსტის ოქმებით გადაცილებული ინფორმაცია ღიაა, თანაც არცერთი სტანდარტული ოქმი ელექტრონული ფოსტისა (SMTP, POP3, IMA P4) არ შეიცავს დაშიფვრის მექანიზმს, რომელიც უზრუნველყოფდა მიმოწერის კონფიდენციალობას. ფაილები შეიძლება წაკითხული იქნას ბოროტგანმზრახველის მიერ. უფრო მეტიც, ადამიანთა უმეტესობას ავიწყდება, რომ ინტერნეტი ესაა საზოგადოებრივი ადგილი და რომ ელექტრონული ფოსტა, სანამ ის მიაღწევს დანიშნულ ადგილს გაივლის რამოდენიმე კომპიტერს და „მოგზაურობისას“ შეიძლება მოხდეს მისი პერლუსტრაცია.

„მსგავსი შეტევისაგან თავდასაცავად ექსპერტები გვთავაზობენ შემდეგი სახის მეთოდებს:

1. თუ თქვენს ქსელის მარშრუტიზატორებზე და ქსელურ ეკრანებზე სწორადა ორგანიზებული აუტენტიფიკაციის ფუნქცია. ეს უნდა მოიცავდეს მინიმუმ RES 2827 ფილტრაციას. თუ ბოროტგანმზრახველი ვერ შეძლებს მოახდინოს თავისი პიროვნების მარკირება, მაშინ ძნელი წარმოსადგენია, რომ მან გაბედოს შეტევის განხორციელება.

2. არსებობს ანტი ფუნქცია, რომლის სწორი გამოყენებაც, ასევე საშუალებას იძლევა შემცირდეს მსგავსი შეტევების რისკი. ამ ფუნქციის მეშვეობით ხდება დროის ნებისმიერ მომენტში ნახევრად ღია არხების რაოდენობის შეზღუდვა.

3. ტრაფიკის მოცულობის შეზღუდვა (traffic rate limiting) - ორგანიზაციამ შეიძლება პროვაიდერს თხოვოს ტრაფიკის შეზღუდვა. ამ ტიპის ფილტრაციით შესაძლებელია შემცირდეს ქსელზე გამავალი არაკრიტიკული ტრაფიკის მოცულობა.

როგორც აღვნიშნეთ, ბოროტგანმზრახველი ცდილობს იპოვოს თავისი ქმედებებით ქსელში სარგებელი და ხშირად მიმართავს პაროლებზე შეტევას, რომლისთვისაც იყენებს მთელ რიგ მეთოდებს: უბრალო გადარჩევა (brute force attack), „ტროას ცხენი“, IP - სპუფინგი და პაკეტების სნიფინგი.

IP - სპუფინგი გაყალბებასთანაა დაკავშირებული - ბოროტგანმზრახველი, რომელიც იმყოფება კორპორაციის შიგნით ან მის გარეთ, თავს ასაღებს ნებადართულ მომხმარებლად.

აღნიშნული სახის შეტევის შესუსტება (და არა თავიდან აცილება) შესაძლებელია შემდეგი მეთოდების გამოყენებით:

1. დაშვების კონტროლი - ექსპერტთა აზრით, უმარტივეს მეთოდად IP-სპუფინგის ასაცილებლად ითვლება დაშვების კონტროლის სისტემის სწორად ორგანიზება.

2. REC 2827 ფილტრაციის გამოყენება.

3. დამატებითი აუტენტიფიკაციის საუკეთესო საშუალებად ითვლება კრიპტოგრაფია, მაგრამ თუ ეს შეუძლებელია, მაშინ კარგი შედეგის მიღება შესაძლებელია ე.წ. ორფაქტორიანიი აუტენტიფიკაციის ერთჯერადი პაროლების გამოყენებით“.[17]

რაც შეეხება პაკეტების სნიფერს - ესაა გამოყენებითი პროგრამა, რომელიც იყენებს ქსელურ რუქას და მუშაობს promiscuous mode რეჟიმში (ამ რეჟიმში ყველა პაკეტს, რომლებიც მიიღება ფიზიკური არხებით, ქსელური ადაპტერი აგზავნის გამოყენებით პროგრამასთან). ამ დროს სნიფერი

მოიტაცებს ყველა ქსელურ პაკეტს, რომელიც გადაიცემა გარკვეული დომენის გავლით. დღეისათვის სნიფერები ქსელში მუშაობენ სავსებით კანონიერად. მათი მეშვეობით შეიძლება გავიგოთ სასარგებლო ინფორმაცია, ზოგჯერ - კონფიდენციალურიც.

ექსპერტები პაკეტების სნიფინგისგან მომდინარე საფრთხის შესამცირებლად გვთავაზობენ შემდეგ საშუალებებს:

1. აუტენტიფიკაცია - აუტენტიფიკაციის საშუალებები პაკეტების სნიფინგისგან დაცვის ერთ-ერთ ძლიერ საშუალებადაა აღიარებული;

2. კომუტირებადი ინფრასტრუქტურა - იგულისხმება ქსელში კომუტირებადი ინფრასტრუქტურის შექმნა;

3. ანტი-სნიფერები - ესაა სპეციალური პროგრამები ან აპარატურული საშუალებები, რომელთაც შეუძლიათ ქსელში მომუშავე სნიფების ამოცნობა;

4. კრიპტოგრაფია - ამ შემთხვევაში ინფორმაცია სრულადაა დაცული გამჟღავნებისაგან.

გამოყენებითი პროცესების დონეზე შეტევებიც მრავალნაირია. ყველაზე უფრო გავრცელებულია უზრუნველყოფის (sendmail, HTTP, FTP) სუსტი მხარეების გამოყენება, რომელთა მეშვეობითაც ბოროტგანმზრახველებს შეუძლიათ შეაღწიონ კომპიტერებში, იმ მომხმარებლის სახელით, რომლებიც უშუალოდ მუშაობენ ამ გამოყენებით პროგრამებთან (ეს მომხმარებელი პრივილეგირებულია, სისტემური დაშვების მქონე ადმინისტრატორი). ამ დონეზე შეტევების სრულად აცილება შეუძლებელია. ხაკერები ძალზე ხშირად აქვეყნებენ ინტერნეტში მონაცემებს სხვადასხვა პროგრამების სუსტი მხარეების შესახებ. ამ შემთხვევაში მთავარია სისტემური ადმინისტრირების სწორად წარმართვა.

ქსელური შეტევების სახეებს განეკუთვნება ქსელური დაზვერვა, რომელიც გულისხმობს ქსელზე საყოველთაოდ ხელმისაწვდომი მონაცემების და გამოყენებითი პროცესების მეშვეობით. რომელიმე ქსელის წინააღმდეგ შეტევის განხორციელებისას ბოროტგანმზრახველი, როგორც წესი, ცდილობს მასზე მიიღოს რაც შეიძლება მეტი ინფორმაცია. ქსელური დაზვერვა ხორციელდება DNS შეკითხვათა ფორმით, ექო-ტესტირებით (ping sweep) და პორტების სკანირებით. DNS შეკითხვები საშუალებას იძლევიან გაგებული იქნას თუ ვინ ფლობს ამა თუ იმ დომენს და ამ დომენებს რა მისამართები აქვთ მიკუთვნებული. ექო-ტესტირება DNS-ის მეშვეობით გაგებული მისამართებისა საშუალებას იძლება დავინახოთ თუ მოცემულ

მომენტში რეალურად რომელი ჰოსტები მუშაობენ. ხშირ შემთხვევებში ადგილი აქვს ქსელში არსებული ნდობის ბოროტად გამოყენებას. ასეთი ნდობის ბოროტად გამოყენების კლასიკურ მაგალითს წარმოადგენს სიტუაციები კორპორაციული ქსელების პერიფერიულ ნაწილში. ქსელების ამ ნაწილში ხშირად განთავსებულია DNS, SMTP და HTTP სერვერები. ვინაიდან ისინი ეკუთვნიან ქსელის ერთიდაიგივე სეგმენტს და ენდობიან ერთმანეთს, ამიტომ ერთ-ერთი მათგანის გატეხვა იწვევს სხვების გატეხვასაც.

არ შეიძლება არ შევეხოთ ისეთ მავნე პროგრამებს, რომლებიც ავრცელებენ კომპიუტერულ ვირუსებს და ზიანს აყენებენ, როგორც ცალკეულ მომხმარებლებს, აგრეთვე მთლიანად იმ საქმიან სამყაროს, რომელიც ინტესიურად სარგებლობს ინტერნეტით. საინტერესოა ბრიტანული ფირმის Netcraft-ის საკმაოდ პარადოქსული მოსაზრება, რომ ვირუსები მიუხედავად ყველაფრისა თამაშობენ დადებით როლს WWW უსაფრთხოებისათვის. ვირუსები დამანგრეველია, მაგრამ მათ სააშკარაოზე გამოაქვთ ბოროტგანმზრახველების საქმიანობა.

1.4. ჰაკერების მძვარცველობითი საქმიანობა კიბერსივრცეში და მათი კავშირები სახელმწიფოს სპეცსამსახურებთან

ინფორმაციული და კომპიუტერული ტექნოლოგიების განვითარების თანამედროვე ეტაპზე, ენერგეტიკულ და გარემოს დაცვის პრობლემებთან ერთად, ერთ-ერთ მნიშვნელოვან პრობლემას ინფორმაციული უსაფრთხოება წარმოადგენს. ეს განპირობებულია კომპიუტერული და ქსელური ტექნოლოგიების ადამიანის საქმიანობის ყველა სფეროში შეჭრით და აგრეთვე დაგროვილი და გენერირებული ციფრული ინფორმაციის მოცულობის ექსპონენციალური ზრდით. უფროს მეტიც, ჩვენს სამყაროს შეიძლება ვუწოდოთ „გაფართოებადი ციფრული სამყარო“. კერძოდ, 2007 წელს შეიქმნა 2828 ექსბაიტი ინფორმაცია (1 ექსბაიტი $=10^{18}$ ბაიტს). ანუ 10%-ით მეტი წინა წლის პროგნოზთან შედარებით. ახალი პროგნოზებით, 2012 წელს შეიქმნება 4,000-მდე ექსბაიტის მოცულობის ინფორმაცია - ეს ასტრონომიული რიცხვია.

თანამედროვე მსოფლიოს კიბერსივრცეში არსებული და პოტენციური რისკები/საფრთხეები საზოგადოებრივი ცხოვრების რეალობად იქცა.

ტექნოლოგიების განვითარებასთან ერთად უფრო რთული ხდება აღნიშნული საფრთხეების პრევენცია და დაძლევა. საერთაშორისო სტატისტიკის მიხედვით, წარმატებული კიბერინციდენტების რიცხვი ყოველწლიურად მატულობს და შესაბამისად იზრდება კიბერინციდენტებით გამოწვეული ზარალი.

გლობალური ინტერნეტ სივრცის მუდმივი განვითარება და მასთან დაკავშირებული არსებული საფრთხეები, საქართველოს კიბერსივრცესა და შესაბამისად კრიტიკული ინფორმაციული ინფრასტრუქტურის სისტემის გამართულ ფუნქციონირებას მუდმივად ახალი გამოწვევების წინაშე აყენებს. სტრატეგიის თანახმად, ინფორმაციული სისტემის კრიტიკულობა და კიბერუსაფრთხოების მდგრადობა განისაზღვრება ისეთი კრიტერიუმებით, როგორიცაა მოსალოდნელი მატერიალური ზარალის სიმძიმე და მასშტაბები, ინფორმაციული სისტემის აუცილებლობა სახელმწიფოსა და საზოგადოების ნორმალური ფუნქციონირება, სისტემის მომხმარებელთა რაოდენობა და კიბერუსაფრთხოების სათანადო დონის უზრუნველყოფა საჭირო რესურსებით.

ჰაკერების მიერ დაინფიცირდა ქართული საინფორმაციო საიტების მხოლოდ ის გვერდები, სადაც განთავსებული იყო ინფორმაცია ნატო-ს დელეგაციის ვიზიტების, სამხედრო სიახლეების, პრეზიდენტის განცხადებების, ამერიკასთან ურთიერთობის შესახებ. ამრიგად კიბერ შეტევის ორგანიზატორების მიერ წინასწარ იყო შერჩული სამიზნე აუდიტორია. აღნიშნული ვებ-გვერდების გახნისას ინტერნეტ მომხმარებლის კომპიუტერი ავტომატურად ინფიცირდებოდა უცნობი ვირუსული პროგრამით. ვირუსი ამოწმებდა კომპიუტერის გეოგრაფიულ მდგომარეობას დროითი სარტყელის მიხედვით.

მთავარი ფუნქცია - კომპიუტერში არსებულ ფაილებში, დოკუმენტებში წინასწარ განსაზღვრული სიტყვების ძიება (სამხედრო, საიდუმლო, სადაზვერვო თემაზე). აღმოჩენის შემთხვევაში აღნიშნული ფაილების გადაწერა ხდეობდა ვირუსის ავტორის სამართავ სერვერზე.

დაინფიცირდა მრავალი სახელმწიფო უწყება და რამდენიმე კრიტიკული ინფრასტრუქტურის ობიექტი.

„Flame/Gauss - 2012 წელს გამოვლენილი მაღალი დონის კიბერ შეტევა არაბულ სახელმწიფოებზე. სპეციალურად შექმნილი კომპიუტერული ვირუსები აინფიცირებდნენ სამიზნე ქვეყნების უწყებებს. შემდგომ ეტაპზე

ვირუსული ფაილი კომპიუტერულ სისტემებში ეძებდა და იპარავდა სენსიტიურ, საიდუმლო ინფორმაციას (დოკუმენტები, ელ-ფოსტა და ა.შ.). ვირუსს ჰქონდა ვიდეო და აუდიო ჩანაწერის განხორციელების ფუნქცია კომპიუტერის შესაბამისი მოწყობილობების გამოყენებით. აღნიშნული ვირუსი იყენებს კომუნიკაციის დაშიფრულ არხებს და ტექნიკური დახვეწილობიდან გამომდინარე რთულია მისი აღმოჩენა.

Stuxnet - კიბერშეტევა ირანის ბირთვული პროგრამის წინააღმდეგ. არსებობს სხვადასხვა ინფრასტრუქტურის სამართავი „ICS - ინდუსტრიული კონტროლის სისტემები“. ერთ-ერთ ასეთ სისტემაში აღმოჩენილი სისუსტის გამოყენებით, ვირუსი Stuxnet ახერხებდა დაინფიცირებული სისტემიდან - ატომური რეაქტორების ცენტრი ფუგების მუშაობაში ჩარევას, მცდარი პარამეტრების გადაცემას და შედეგად მათ დაზიანებას. როგორც მოგვიანებით გაირკვა ვირუსი მაღალ პროფესიონალურ დონეზე იყო შესრულებული, გავრცელდა USB ფლეშ მოწყობილობების საშუალებით და სისტემების დასაინფიცირებლად იყენებდა ჯერ კიდევ უცნობ, და არადოკუმენტირებულ შეტევის მეთოდებს და ვექტორებს.

Acad/Medre - 2011-2012 წლები. კიბერშეტევის დროს ვირუსის მთავარი ფუნქცია სამხრეთ ამერიკული სახელმწიფოებიდან არქიტექტურული პროექტების ხელში ჩაგდება იყო. მისი მოქმედება მხოლოდ მაშინ ვლინდება, თუკი დაინფიცირებულ კომპიუტერზე აღმოჩნდება, ვირუსის შემქმნელებისთვის საინტერესო CAD არქიტექტურული პროგრამის ფაილები, ნახაზები და პროექტები. მოძიებული ფაილები გადაეცემოდა ვირუსის ავტორებს სხვადასხვა ქვეყნებში განთავსებულ შემგროვებელ სერვერებზე (მოგვიანებით დაინფიცირებულ ქვეყნებს დაემატა აშშ, ჩინეთი, ტაივანი, ესპანეთი).

Ghostnet - ჩინური კიბერშპიონაჟი ტიბეტის მთავრობის წინააღმდეგ. 2009 წელს 10 თვიანი გამოძიების შედეგად დადგინდა, რომ არსებობდა 1295 კომპიუტერისგან შემდგარი ქსელი, 103 ქვეყანაში. მათი უმეტესობა განთავსებული იყო საგარეო ურთიერთობის სამინისტროებსა და უწყებებში, საელჩოებში, საერთაშორისო ორგანიზაციებში, ახალი ამბების სააგენტოებში, არასამთავრობო ორგანიზაციებში. მრავალი დიპლომატის, სამხედრო წარმომადგენლის, მინისტრის თანაშემწეების, ჟურნალისტის და სახელმწიფო მოხელის კომპიუტერებიდან მოპოვებული და გადაწერილი იქნა პოლიტიკური, ეკონომიკური, საიდუმლო შინაარსის დოკუმენტაცია.

Operation Shady RAT - 2007-2012 წლების განმავლობაში 70-ზე მეტ გლობალურ კომპანიაში, ორგანიზაციებში და რამდენიმე სახელმწიფოს სხვადასხვა სტრუქტურაში გამიზნული კიბერ შეღწევა, სენსიტიური დოკუმენტაციის ხელში ჩაგდების მიზნით (ფინანსურ-ეკონომიკური კიბერ შპიონაჟი). დაინფიცირებული უწყებები: 14 ქვეყნის სამთავრობო უწყებები, ინდუსტირული ცენტრები, ქარხნები (მძიმე ლითონები, მზის ენერგია), ელექტრონიკა-სატელიტური კომუნიკაციები (შესაბამის თემაზე მომუშავე ინსტიტუტები, ორგანიზაციები, ქარხნები), სამხედრო უწყებები, უძრავი ქონების და საფინანსო-საბანკო დაწესებულებები.

Night Dragon - გოლბალურ ნავთობ, ენერგო და ფეტოქიმიურ კორპორაციებში კიბერშპიონაჟი ვირუსული პროგრამების გამოყენებით (ინდუსტრიული შპიონაჟი).

Red October 2007-2012 წლები მასშტაბური კიბერშპიონაჟი ათეულობით სახელმწიფოს სხვადასხვა სტრუქტურებში (სამინისტროები, საელჩოები, დაწესებულებები, ინსტიტუტები)“.[52]

სახელმწიფოსა და კერძო სექტორს შორის თანამშრომლობა აუცილებელი პირობაა კიბერ სივრცის დაცვის უზრუნველყოფისთვის. ერთის მხრივ სახელმწიფო ეროვნული უსაფრთხოების უზრუნველყოფიდან გამომდინარე, ვალდებულია დაიცვას ქვეყნის მთლიანი ინფრასტრუქტურა არასანქცირებული შეღწევისგან, მაგრამ არ ფლობს ყველა საჭირო რესურსს, ვინაიდან რესურსის დიდი ნაწილი არის კერძო სექტორის მფლობელობაში. ეს საბაზრო ეკონომიკის პირობებში ნორმალური და აუცილებელი მოვლენაა. მეორეს მხრივ, კერძო სექტორს არ გააჩნია არავითარი სამართლებრივი ვალდებულებები ითანამშრომლოს სახელმწიფოსთან და გამოაყენებინოს მის ხელთ არსებული რესურსი. აქ ძირითადად საუბარია ინტერნეტ პროვაიდერებზე, რომელთა მფლობელობაშიც არის ქსელები, რომლებიც თავის მხრივ ინტერნეტით უზრუნველყოფენ სამთავრობო სტრუქტურებს, სტრატეგიული დანიშნულების ობიექტებს, კერძო მომხმარებლებს, სამრეწველო ობიექტებსა და მსხვილ კომპანიებს, მათ შორის მსხვილ ბანკებს, დიპლომატიურ და სხვა უცხოურ მისიებსა თუ წარმომადგენლობებს. მსოფლიო საზოგადოება დადგა ახალი კიბერ საფრთხის წინაშე, რაც მომდინარეობს ისლამური ჰაკერული ჯგუფებიდან და დაჯგუფებებიდან. უახლოეს მომავალში იგივე საფრთხის წინაშე აღმოჩნდება საქართველოც, რომლის საგარეო პოლიტიკა მიმართულია ევროპულ ინსტიტუტებში

ინტეგრაციისკენ, ქვეყანა უნდა გახდეს ევროკავშირისა და ჩრდილოეთ ატლანტიკური ალიანსის წევრი, საქართველომ ხელი მოაწერა ევროპასთან ასოცირების ხელშეკრულებას, სადაც ერთერთ პუნქტად ჩადებულია უსაფრთხოების საკითხების უზრუნველყოფა. ყოველივე ეს გამოიწვევს, ქვეყანაში დასავლური კომპანიების, ახალი მისიებისა და წარმომადგენლობითი ოფისების გახსნას. ეს პროცესი სულ უფრო გაიზრდება, რაც თავის მხრივ, ჩვენი ქვეყნის მიმართ კიდევ უფრო ზრდის საფრთხეებს ისლამური ფუნდამენტალიზმის მხრიდან, რის პარალელურადაც იზრდება კიბერ საფრთხეებიც. მაგალითისთვის, 2015 წლის იანვარიდან დღემდე განხორციელდა რამოდენიმე კიბერშეტევა, რომელიც მოდიოდა ისლამური ჰაკერული დაჯგუფებებისგან. აქ აღსანიშნავია მიმდინარე წლის 10 იანვარს ფრანგულ კომპანია "კარფურის" საქართველოს ფილიალის ვებგვერდზე განხორციელებულ კიბერ შეტევაც, რომელიც განახორციელა "ახლო აღმოსავლეთის კიბერ არმიამ". სხვათა შორის, იმ პერიოდში განხორციელდა საკმაოდ მასიური კიბერ შეტევა ფრანგულ კომპანიებსა და მათ წარმომადგენლობით ოფისებზე მთელს მსოფლიოში, სადაც ასევე ფიგურირებდა "კარფურის" საქართველოს ფილიალი. ეს ფაქტი ყურადღებას იმსახურებს და ის უნდა განვიხილოთ, როგორც პრეცედენტი ჩვენი ქვეყნისთვის, რომელსაც მომავალშიც ექნება ადგილი, და ეს არ შემცირდება, პირიქით უფრო გაიზრდება. ასევე ამა წლის 16 აპრილს ისლამური ჰაკერული დაჯგუფება "ელ მოჰაჯირის" მიერ განხორციელდა თავდასხმა "საქართველოს მოსამართლეთა ერთობის" ვებ გვერდზე.

კიბერ შეტევის მთავარი მიზანი - დაინფიცირებული უწყებიდან ყველა შესაძლო მექანიზმით და ტექნიკური საშუალებით სხვადასხვა სახის ინფორმაციის მოპარვა, გადაწერა. ვირუსულ ფაილს აქვს შემდეგი ფუნქციები: კომპიუტერის დეტალური ინფორმაციის გადაგზავნა ვირუსის ავტორთან, ნატო-ს შიფრაციის სტანდარტით დაშიფრული ფაილების, დოკუმენტაციის ძებნა და გადაწერა, კომპიუტერთან მიერთებული მობილური ტელეფონების ან პლანშეტური კომპიუტერების დაინფიცირება და მათგან ინფორმაციის მოპოვება, მაღალ დონეზე დაშიფრული, და დაფარული მართვის მექანიზმი (რთულდება ვირუსის სამართავი წყაროს აღმოჩენა).

სავარაუდოდ აღნიშნული კიბერ შეტევის დროს გამოყენებულია სხვადასხვა დროს რუსი და ჩინელი ჰაკერების მიერ შექმნილი ვირუსული ელემენტები (კომპანია Kaspersky-ის დასკვნის მიხედვით).

High Roller - კიბერ-შეტევის მიზანია მასობრივი გლობალური ფინანსური მანიპულაციები, მაქინაციები. შექმნილი ვირუსების Zeus / SpyEye-ს მეშვეობით დაინფიცირებული ინტერნეტ მომხმარებლების კომპიუტერებში მიმდინარეობს საბანკო ბარათების პაროლების, საკრედიტო ნომრების და გადარიცხვების მონიტორინგი. შესაბამისად ვირუსის ავტორებმა დააგროვეს კონფიდენციალური საბანკო ინფორმაცია ათიათასობით მომხმარებლის შესახებ.

კომპანია McAfee-ს და რამდენიმე საფინანსო ორგანიზაციის დასკვნის მიხედვით კიბერ კრიმინალებმა მოახერხეს 60 მილიონი ევროს უკანონო ტრანზაქციის განხორციელება, 60-ზე მეტი საფინანსო ინსტიტუტის ანგარიშებიდან. დასკვნის მიხედვით იმ შემთხვევაში, თუ ყველა დაინფიცირებული კომპიუტერიდან განოხციელებული მაქინაცია და ტრანზაქციები წარმატებით დასრულდებოდა, კიბერ კრიმინალები გამოიწვევდნენ 2 მლრდ. ევროს ზარალს. Shamoon - საუდის არაბეთი სახელმწიფო ნავთობ კომპანის ARAMCO-ს კომპიუტერული ქსელის დაინფიცირება. შედეგად კომპანიის კუთვნილი უამრავი კომპიუტერის ოპერაციული სისტემა დაზიანდა და დროებით შეწყვიტა ფუნქციონირება. მუშაობის სრულად აღსადგენად კომპანიას სერიოზული ადამიანური რესურსი და დრო დასჭირდა, რამაც გარკვეული ზარალი მიაყენა მსოფლიოს ყველაზე მდიდარ ნავთობ-კომპანიას. CREECH USB - ამერიკული უპილოტო საფრენი აპარატების ოპერატორების კომპიუტერების დაინფიცირება USB მოწყობილობებიდან. ვირუსის მთავარი ფუნქცია, საფრენი აპარატების სამართავი კოდების მოპარვა და გადაცემა, ავღანეთის მისიის დროს.

II. შედეგები და მათი განსჯა

2.1. კვლევის მიზანი.

აღსანიშნავია, რომ სპეციფიკა, რაც დამახასიათებელია ინტერნეტისათვის მდგომარეობს იმაში, რომ იგი არ ეკუთვნის არავის, არცერთ მთავრობას არ ძალუძს მასზე განახორციელოს მონოპოლია, თუ არ გავითვალისწინებთ, იმას, რომ მთავრობა იტოვებს უფლებას მიაწოდოს ესა თუ ის ინფორმაცია მომხმარებელს.

ინფორმაცია ყოველთვის უნდა იყოს შესაბამისად დაცული. ინფორმაციული უსაფრთხოება მიიღწევა შესაბამისი კონტროლის მექანიზმების, მათ შორის პოლიტიკის, პროცესების, პროცედურების, ორგანიზაციული სტრუქტურისა და პროგრამული უზრუნველყოფისა, აგრეთვე კომპიტერული ტექნიკის დანერგვით. აქედან გამომდინარე, უნდა მოხდეს აღნიშნული კონტროლის მექანიზმების ჩამოყალიბება, დანერგვა, მონიტორინგი, გადახედვა და საჭიროების შემთხვევაში, გაუმჯობესება. ინფორმაციული უსაფრთხოების სისტემა უნდა დაინერგოს და ფუნქციონირებდეს საქმიანობის მართვის სხვა პროცესებთან ერთად.

ორგანიზაციები, მათი ინფორმაციული სისტემები და ქსელები უშუალოდ დგანან ისეთი საფრთხეების პირისპირ, როგორებიცაა კომპიუტერული თაღლითობა, შპიონაში, საბოტაჟი, ვანდალიზმი, მავნე კოდის შემცველი პროგრამები, კოპიუტერული ჰაკეროზა, კომპიუტერულ პროგრამებზე თავდასხმა მომხმარებლისთვის სერვისი შეფერხებით მიწოდების მიზნით უფრო და უფრო დახვეწილი ხერხებით ხორციელდება.

ინფორმაციული უსაფრთხოების სფეროში სხვადასხვა სტანდარტები შემუშავდა, რომლებშიც ნაწილობრივ სხვადასხვა მიზნობრივი ჯგუფები ან თემატური სფეროები არის წინა პლანზე წამოწეული. უსაფრთხოების სტანდარტების გამოყენება ხელისუფლებაში არა მხოლოდ აუმჯობესებს უსაფრთხოების დონეს, ასევე ხელს უწყობს სხვადასხვა დაწესებულებებს შორის კოორდინაციას, რომლებშიც უსაფრთხოების ზომები უნდა განხორციელდეს ნებისმიერი ფორმით.

ყოველი სტადიისთვის საჭიროა ინფორმაციული უსაფრთხოების შესაფერისი ზომების შერჩევა:

1. პრევენციული – უსაფრთხოების ზომები, რომლებიც გამორიცხავს წინასწარ ინფორმაციული უსაფრთხოების ინციდენტის გამოვლენას. მაგალითად, წვდომის ნებართვების განაწილება;

2. აღდგენა – უსაფრთხოების ზომები, მიმართული პოტენციური ზარალის შესამცირებლად ინციდენტის შემთხვევაში. მაგალითად, სარეზერვო დუბლირება;

3. აღმომჩენი – უსაფრთხოების ზომები, მიმართული ინციდენტების აღმოსაჩენად. მაგალითად, ანტივირუსული დაცვა ან შემოჭრის აღმოჩენის სისტემა;

4. ჩამხშობი (აღმკვეთი) – უსაფრთხოების ზომები, რომლებიც ეწინააღმდეგება საფრთხის რეალიზაციის მცდელობას, ანუ ინციდენტებს. მაგალითად, ბანკომატი ართმევს კლიენტს ელექტრონულ ბარათს მის მიერ რამდენჯერმე PIN-კოდის არასწორად შეტანის შემთხვევაში;

5. მაკორექტირებელი – უსაფრთხოების ზომები, მიმართული აღდგენისათვის ინციდენტის შემდეგ. მაგალითად, სარეზერვო დუბლების აღდგენა, წინა სამუშაო მდგომარეობაში დაბრუნება და ა.შ.

2.2. კვლევის ეტაპები.

თანამედროვე ორგანიზაცია წარმოადგენს დიდი რაოდენობის კომპონენტების ნაირსახეობას გაერთიანებულს ერთ სივრცეში, რათა უზრუნველყოს დასახული მიზნების შესრულება, რომლებმაც შეიძლება განიცადონ მოდიფიკაცია მისი ფუნქციონირების პროცესში. ამავდროულად გაჩნდა ინფორმაციის გადანაწილების აუცილებლობა, რამაც ლოკალურ, გლობალურ ქსელებში გაამძაფრა სიტუაცია ინფორმაციის დაცვის კუთხით. ზუსტად ეს ფაქტორები განაპირობებენ ინფორმაციის მოპოვებისა და მიღების მაღალეფექტური სისტემის შექმნის აუცილებლობას.

უსაფრთხოება არ არის უცვლელი მდგომარეობა, რომელიც მიიღწევა ერთხელ და შემდეგ არასდროს იცვლება, და ყოველი დაწესებულება ექვემდებარება მუდმივ დინამიკურ ცვლილებებს.

ხელმძღვანელობის დონე აქტიურად უნდა მართავდეს და აკონტროლებდეს უსაფრთხოების პროცესს. ამისთვის განიხილება შემდეგი ეტაპები:

- მიღებულ უნდა იქნას ინფორმაციული უსაფრთხოების სტრატეგია და უსაფრთხოების მიზნები;

- უსაფრთხოების რისკების გავლენა ბიზნესზე ან ამოცანების შესრულებაზე უნდა იქნას გამოკვლეული;

- უნდა შეიქმნას ორგანიზაციული ჩარჩოს პირობები ინფორმაციული უსაფრთხოებითვის;

- ინფორმაციული უსაფრთხოებითვის უნდა გამოიყოს საკმარისი რესურსები;

- უსაფრთხოების სტრატეგია სისტემატურად უნდა მოწმდებოდეს და ტარდებოდეს მიზნის მიღწევის მონიტორინგი.

- გამოვლენილი ნაკლოვანებანი და შეცდომები უნდა გასწორდეს. ამისათვის უნდა შეიქმნას ,,ნოვატორული'' სამუშაო კლიმატი და ორგანიზაციის შიგნით მუდმივი სრულყოფის ნების დემონსტრირება;

- თანამშრომლები მოტივირებული უნდა იყვნენ უსაფრთხოების საკითხებზე და ინფორმაციული უსაფრთხოება განიხილონ როგორც თავიანთი ამოცანების მნიშვნელოვანი ასპექტი. ამისათვის საჭიროა, სხვებთან ერთად, საკმარისი საინფორმაციო-საგანმანათლებლო ღონისძიებების შეთავაზება.

გამოცდილებამ აჩვენა, რომ ქვემოთ ჩამოთვლილი ფაქტორები მნიშვნელოვანწილად განსაზღვრავენ ორგანიზაციაში ინფორმაციული უსაფრთხოების წარმატებულ დანერგვას:

1. ინფორმაციული უსაფრთხოების პოლიტიკა, მიზნები და ქმედებები, რომლებიც ასახავს ბიზნესის (საქმისწარმოების) მიზნებს;

2. ინფორმაციული უსაფრთხოების დანერგვის, მხარდაჭერის, მონიტორინგისა და გაუმჯობესებისადმი მიდგომა და ჩარჩო, რომელიც თავსებადობაშია ორგანიზაციულ კულტურასთან;

3. ყველა რანგის მენეჯმენტის მხრიდან მხარდაჭერა;

4. ინფორმაციული უსაფრთხოების მოთხოვნების, რისკების შეფასების და რისკების მართვის სიღრმისეული გაცნობიერება;

5. ყველა რანგის მენეჯერების, თანამშრომლების და სხვა მხარეების მიერ ცნობიერების ამაღლების მიზნით ინფორმაციული უსაფრთხოების ეფექტიანი მარკეტინგი;

6. ინფორმაციული უსაფრთხოების პოლიტიკის და სტანდარტების სახელმძღვანელო მითითებების განაწილება და მიწოდება ყველა რანგის მენეჯერის, თანამშრომლისა და სხვა მხარეებისთვის;

7. ინფორმაციული უსაფრთხოების მართვის დაფინანსების უზრუნველყოფა;

8. ცნობიერების ამაღლების, ტრენინგისა და სწავლების შესაბამისი უზრუნველყოფა;

9. ინფორმაციული უსაფრთხოების ინციდენტების მართვის ეფექტიანი პროცესის ჩამოყალიბება;

10. შეფასების სისტემის დანერგვა, რომელიც გამოიყენება ინფორმაციული უსაფრთხოების მართვის წარმატების შესაფასებლად და მისი გაუმჯობესების შესახებ უკუკავშირის უზრუნველსაყოფად.

2.3.მსოფლიოს განვითარებული ქვეყნების კიბერუსაფრთხოების სტრატეგიები, საერთო პრინციპები, რეკომენდაციები და ამ მიმართულებით საქართველოში არსებული მდგომარეობა

თანამედროვე მსოფლიოში კიბერსივრცეში არსებული და პოტენციური რისკები/ საფრთხეები საზოგადოებრივი ცხოვრების აშკარა რეალობად იქცა. ტექნოლოგიების განვითარებასთან ერთად რთულდება აღნიშნული საფრთხეების დაძლევა და პრევენცია. ყველა ქვეყანამ აღიარა კიბერუსაფრთხოების მნიშვნელობა და აუცილებლობა, როგორც სახელმწიფო, ასევე გლობალურ უსაფრთხოებაში. თითოეული ქვეყანა,

როომელსაც ტექნოლოგიურად განვითარების სურვილი აქვს, საზოგადოების წინაძე ვალდებულია, დაიცვას საკუთარი კიბერსივრცე, უზრუნველყოს მისი უსაფრთხოება და დინამიკური განვითარება. საქართველო მზად არის, გადადგას გარკვეული ნაბიჯები ელექტორნული ინფორმაციის დაცვის ისეთი სისტემის შესაქმნელად, რომელიც უპასუხებს მსოფლიო გამოწვევებს და ხელს შეუწყობს ინფრომაციული და კომუნიკაციებისს ტექნოლოგიების უსაფრთხოებას. ამ ნაბიჯით საქართველო კიდევ უფრო დაუახლოვდება ევროკავშირსა და ნატოს, რომელთა ერთ–ერთი მოთხოვნა ინფორმაციული უსაფრთხოების დაცვაა.

კაცობრიობა ვითარდება და ომის წარმოების მეთოდები სულ უფრო და უფრო დახვეწილი ხდება. ჩნდება ახალი სფეროები, პარადოქსულია, მაგრამ ინტერნეტის შესაქმნელად და განსავითარებლად უზარმაზარი ფული დაიხარჯა, რომ აღარაფერი ვთქვათ უამრავი მეცნიერის დაუღალავ შრომაზე, და რა მივიღეთ ბოლოს, ინტერნეტი, სხვა ყველაფერთან ერთად, დღეს სრული სერიოზულობით ერთ-ერთ ბრძოლის ველად მოიაზრება. ბევრ განვითარებულ ქვეყანაში იქმნება სპეციალური ქვედანაყოფები ინტერნეტში ომის საწარმოებლად, მუშავდება კიბერ ომების ტაქტიკა და სტრატეგია.

როგორც ვხედავთ, „საინფორმაციო არმია“ საკმაოდ მოწესრიგებული მექანიზმია; უფრო მეტიც ეს არმია აგვისტოს ომის მერე საჭიროებს დახვეწას და ახალი კადრების მოძიებას, რადგან რუსეთი საინფორმაციო ომს განიხილავს როგორც გეოპოლტიკური ამოცანების გასახორციელებელ რეალურ ფაქტორს.

„გამოთქმა „საინფორმაციო ომი“ პირველად გამოიყენა ამერიკელმა თომას რონმა 1976 წელს. ის ტერმინში გულისხმობდა „საკუთარი საინფორმაციო სისტემის დაცვასა და მოწინააღმდეგე მხარისადმი კომპლექსურ, მიზანმიმართულ და დამანგრეველ ინფორმაციულ ზეგავლენას.“

თანამედროვე მსოფლიოში „საინფორმაციო ომმა“ პრაქტიკულად შეცვალა შეიარაღებული ომები; საინფორმაციო ომში საბრძოლო იარაღია სამეცნიერო დებულებები; პატარა, მაგრამ გეოპოლიტიკურად სტრატეგიული ქვეყნისათვის - არსებითი მნიშვნელობა აქვს ზუსტად სამეცნიერო დასკვნებსა და აკადემიური ინფორმაციების ფართოდ გავრცელებას“.[37]

იქვე, ამის პარალელურად არის ახალი ტექნოლოგიები, რომლებიც უზრუნველყოფენ კიბერუსაფრთხოებას და მიუხედავად ამისა, კიბერ სივრცეში გაიზრდება გამალებული შეიარაღების პროცესი. კიბერდანაშაულებები კვლავ იქნება გამოწვევა საზოგადოებისთვის და ეკონომიკური დანაკარგები სულ უფრო გაიზრდება, რაც სხვა მხრივ ხელს შეუწყობს სახელმწიფოსა და კერძო სექტორს შორის თანამშრომლობის განვითარებას. კიბერ შესაძლებლობების კონცეფციას გავლენა ექნება საერთაშორისო პოლიტიკაზე და ძალაუფლებისთვის გლობალურ ბრძოლაზე, რაც ასევე შეუწყობს ხელს კიბერ სივრცეში გამალებული შეიარაღების პროცესის გაზრდის ტენდენციას. სავსებით შესაძლებელია, რომ ახლო მომავალში მოხდება გლობალური კიბერ კატასტროფა, რაც მთლიანად შეცვლის ჩვენს მიდგომას არამარტო კიბერუსაფრთხოების, არამედ მთლიანად კიბერსივრცეში საერთაშორისო თანამშრომლობის მიმართ. კიბერის ახალ ეპოქაში გამარჯვებული იქნება ის, ვინც შეძლებს საბაზრო ეკონომიკის გათვალისწინებით უსაფრთხოების საკითხების კომპლექსურ გადაწყვეტას; გააჩნიათ საუკეთესო ტალანტების მობილიზების შესაძლებლობა; და შესწევთ ადაპტაციის უნარი და ყოველგვარი ძალისხმევის გარეშე იმუშაონ მრავალეროვან გარემოში.

2.4.მსოფლიოს ინფორმაციული ინფრასტრუქტურის განვითარების ძირითადი მოთხოვნები.

გასული საუკუნის მიწურულს საინფორმაციო და საკომუნიკაციო სფეროში განხორციელებულმა სამეცნიერო-ტექნიკურმა რევოლუციამ კომპიუტერები, საკომუნიკაციო და გლობალური საინფორმაციო ქსელები გახადა განვითარებული (და არა მარტო) ქვეყნების, საზოგადოებების აუცილებელ და განუყოფელ ნაწილად. უფრო მეტიც, ინფორმაციული ტექნოლოგიების მეშვეობითაც ადამიანების ინტელექტუალური დონის ამაღლება მეცნიერებს კაცობრიობის გადარჩენის აუცილებელ პირობად

მიაჩნიათ და ალბათ ამიტომაცაა, რომ 21-ე საუკუნეს ინფორმაციის საუკუნეს უწოდებენ.

საქმე ისაა, რომ არცერთი სახელმწიფო არ წარმოადგენს ჩაკეტილ სისტემას და მას უნდა თუ არა საკუთარი უსაფრთხოებისა და მდგრადი განვითარების მიზნებისათვის იძულებულია ჩაერთოს ინფორმაციული ტექნოლოგიების განვითარებისა და გამოყენების პროცესში, ასევე ვერცერთი ქვეყანა, უკვე დღეს, გვერდს ვერ აუვლის გლობალურ საინფორმაციო ქსელში ჩართვისა და ამ ქსელის რესურსების გამოყენების საკითხს.

გაითვალისწინა რა, ინფორმაციული ტექნოლოგიების გამოყენების გლობალიზაციის უდიდესი მნიშვნელობა კაცობრიობისათვის „დიდმა შვიდეულმა“ თავისი ქვეყნების წარმომადგენლებთან ერთად გამოიმუშავეს ერთობლივი კატალოგი ძირითადი წესებისა, რომელშიც განსაზღვრულია ექვსი ძირითადი მოთხოვნა, რომელიც წაეყენება მსოფლიოს ინფორმაციული ინფრასტრუქტურის განვითარებას. შეთანხმებული საკითხების ჩამონათვალში შედიან:

1. მოთხოვნები ინფორმაციული სისტემების ინტეგრაციაზე, რაც უზრუნველყოფს მათ ერთობლივ გამოყენებას;

2. ინფორმაციული ქსელების და მომსახურების გლობალური ბაზრის განვითარება;

3. კერძო ინტერეების და ინფორმაციის დაცვა;

4. საავტორო უფლებების დაცვა;

5. თანამშრომლობა საკომუნიკაციო ტექნოლოგიების კვლევებისა და განვითარების სფეროში;

6. დაკვირვება ინფორმაციული საზოგადოების განვითარების სოციალურ და საზოგადოებრივ გამოვლინებებზე.

გლობალურ საინფორმაციო ქსელებში ჯერჯერობით გადაულახავ პრობლემად იქცა ბრძოლა კომპიუტერულ დანაშულებათა წინაარმდეგ და მომხმარებელთა უფლებების დაცვა. საქმე იმაშია, რომ კომპიუტერული დანაშაულებათა წინააღმდეგ ბრძოლა ითხოვს საინფორმაციო ქსელში მკაცრი კონტროლის დაწესებას, რაც თავის მხრივ, ხშირად, მიზეზი ხდება მომხმარებლების თავისუფლებათა შელახვისა.

წინამდებარე ანგარიშში გავაანალიზებთ:

- ინტერნეტით მომსახურების სფეროში არსებულ მდგომარეობას;

- კონფიდენციალური ინფორმაციის დაცვისა და სახელმწიფოს ინფორმაციული უსაფრთხოების უზრუნველყოფის ზოგიერთ ასპექტებს;

- საავტორო უფლებების დაცვის საკითხებს;

- აღნიშნული პროცესების სამართლებრივი რეგულირების საკითხებს.

ექსპერტთა შეფასებით არ გადის მეოთხედი საათიც კი ჩვენი კომპიუტერის ინტერნეტში ჩართვიდან, რომ პირველი ჯერი ავტომატურად ახორციელებს პროგრამულად მართვად შეღწევას ჩვენს სისტემაში. ასეთი ჰაკერის მცდელობა შევიდეს სისტემაში ხორციელდება თითქმის ყოველ ათ წუთში. ამავე დროს არ უნდა დაგვავიწყდეს ათასობით სხვადასხვა ვირუსის არსებობა, რომლებსაც შეუძლიათ დააზიანონ ნებისმიერი მომხმარებლის სისტემა ელექტრონული დოკუმენტების ელექტრონული ფოსტით გაცვლისა და ინტერნეტით მონაცემების გადაცემისას.

ინტერნეტის მნიშვნელობაზე მიუთითებს ის ფაქტიც, რომ მასში მიმდინარე დანაშაულობებს ვერ აღუდგა ისეთი მონსტრიც კი როგორიცაა აშშ-ის გამოძიების ფედერალური ბიურო (გფბ). ამ სპეც. სამსახურმა შექმნა სპეციალური კომპიუტერული პროგრამა Infra Gard, რომლის მიზანია ინტერნეტში დანაშაულობათა წინააღმდეგ საბრძოლველად ჩართოს სხვადასხვა ორგანიზაციები და ბიზნეს-სტრუქტურები, მათ შორიც უცხოურიც. Infra Gard-ის პროგრამა კიბერბრძოლებში მონაწილეების საშუალებას აძლევს უსაფრთხოდ და სწრაფად დაუკავშირდნენ გფბ-ს სერვერს და გადასცენ ინფორმაცია საეჭვო ინტერნეტ-მოქმედებებზე.

ვინ და რატომ ქმნის მრავალრიცხოვან ვირუსებს? ყველა - ვისაც არ ეზარება. თუ დღემდე ასეთი ვირუსების შექმნა საჭიროებდა სერიოზულ კვალიფიკაციას, ამჟამად არსებობს საკმაო რაოდენობის პროგრამები, რომელთა მეშვეობითაც შესაძლებელია არსებული ვირუსების მაგალითზე შეიქმნას ახალი ვირუსები.

როგორც აღვნიშნეთ, ინფორმაციის კონფიდენციალურობის უზრუნველსაყოფად კრიპტოგრაფიული საშუალებების გამოყენებისას მსოფლიო პრაქტიკა წააწყდა წინააღმდეგობებს, რომლებიც დაკავშირებულია ამ პროცესის სამართლებრივ უზრუნველყოფასთან.

დილემა სავსებით ნათელია: კოდირებას შეუძლია დაიცვას როგორც კანონმორჩილი მოქალაქე, ასევე დამრღვევები. ერთის მხრივ მონაცემთა უკონტროლო დაშიფვრამ, გადაცემამ და შენახვამ შეიძლება მნიშვნელოვნად

შეამციროს სახელმწიფოს შესაძლებლობები წინ აღუდგეს არასამართლებრივ ქმედებებს სხვადასხვა სფეროებში.

ელექტრონულ სისტემებში კონფიდენციალური ინფორმაციის დაცვის ცენტრის მიერ (EPIC – Electronic Privacy Information Center) შედგენილი იქნა მიმოხილვა, რომელიც წარმოდგენას იძლევა სხვადასხვა ქვეყნების პოლიტიკაზე და ინფორმაციის კრიპტოგრაფიული დაცვის გამოყენებასთან დაკავშირებით. პირობითად, ამ დამოკიდებულების მიხედვით ეს ქვეყნები დაყოფილია სამ ჯგუფად, რომელთაც მინიჭებული აქვთ შემდეგი აღნიშვნები:

მწვანე - ქვეყნები, სადაც ფაქტიურად კრიპტოგრაფიაზე რაიმე შეზღუდვები არ ვრცელდება.

ყვითელი - ქვეყნები, რომელტაც განზრახული აქვთ შემოიღონ გარკვეული კონტროლი კრიპტოგრაფიაზე, მათი ქვეყანაში გამოყენებისა და ორმაგი დანიშნულების პროგრამების ექსპორტის ჩათვლით.

წითელი - ქვეყნები, რომლებიც ახორციელებენ ქვეყნის შიგნით კრიპტოგრაფიის კონტროლს.

როგორც აღვნიშნეთ, მსოფლიოს განვითარებული ქვეყნები ცდილობენ თავიანთი მოწინავე ინფორმაციული ტექნოლოგიების გამოყენებით დაამყარონ „ახალი ინფორმაციული წესრიგი“, რათა სრულად განახორციელონ ნაციონალური მიზნები, რისთვისაც ფართოდ იყენებენ როგორც საკუთარი, ისე სხვა ქვეყნის ინფორმაციულ რესურსებს. ნიშანდობლივია, რომ ეს ქვეყნები ყოველმხრივ ხელს უწყობენ სადაზვერვო სამსახურების მოდერნიზაცია-სრულყოფას, ანვითარებენ ტექნიკური დაზვერვის შესაძლებლობებს. იქმნება ინფორმაციის მოპოვების სრულყოფილი გლობალური სადაზვერვო სისტემები მძლავრი ავტომატიზებული საშუალებებით და მაღვალკვალიფიცირებული სადაზვერვო და ანალიტიკური კადრებით.

აუცილებლად მიგვაჩნია მიღებული იქნას სასწრაფო ღონისძიებები კომპიუტერული სისტემების უსაფრთხოების უზრუნველყოფის სახელმწიფო სტანდარტების დამუშავებისა და მიღების მიზნით. ასეთი პირველი რიგის სტანდარტებად მიგვაჩნია შემდეგი დოკუმენტები:

1. „დირექტივა დაშიფვრის სტანდარტის გამოყენებაზე“;
2. ”მონაცემთა დაშიფვრის სტანდარტი“;
3. ‘შიფრის ორგანიზაცია“;

4. „საიდომლოების უზურნველყოფის ძირითადი მოთხოვნები იმ მოწყობილობებისათვის, რომლებშიც გამოყენებული მონაცემთა დაშიფვრის სტანდარტი“;

5. „ავტონომიური კომპიუტერების დაცულობის კრიტერიუმები“;

6. „მონაცემთა დამუშავების ავტომატიზებული სისტემების დაცულობის კრიტერიუმები“;

7. „მონაცემთა გადაცემის დახურული ქსელური სისტემები“

8. სხვა ქვეყნების ტექნიკური დაზვერვისაგან დაცვის მოთხოვნათა შინაარსი და მათი ჩართვის წესი სამეცნიერო-კვლევით და საცდელ-საკონსტრუქტორო სამუშაოების სამეცნიერო-ტექნიკურ დოკუმენტაციაში“ და ა.შ.

2.5. ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების სტრატეგიები, საერთო პრინციპები და რეკომენდაციები.

საერთო მოხმარების ინფორმაციული სისტემების ფუნქციონირებაზე დიდი გავლენა აქვს ისეთ ფაქტორებს, როგორებიც არის ინტერნეტზე შეტევა (attack), ფიზიკური ზემოქმედების შედეგად მიყენებული დარღვევები, პროგრამული და აპარატული უზრუნველყოფის მწყობრიდან გამოსვლა, ადამიანის როგორც მომხმარებლის მიერ მუშაობის პროცესში დაშვებული შეცდომები. ჩამოთვლილი ფაქტორები ნათლად აჩვენებს იმ გარემოებას, თუ რამდენად არის დამოკიდებული თანამედროვე საზოგადოება ინფორმაციული სისტემების სტაბილურ მუშაობაზე. მოცემულს ნათლად ასახავს კიბერუსაფრთხოების გერმანული სტრატეგია, კერძოდ: „კიბერსივრცეზე დაშვების უზრუნველყოფა, ასევე ინფორმაციის კონფიდენციალობა და სანდოობა კიბერსივრცეში გახდა ერთერთი მნიშვნელოვანი პრობლემა 21 - ე საუკუნეში. ამიტომ კიბერსივრცის დაცვა ხდება მთავარი ამოცანა სახელმწიფოს, ეკონომიკისა და საზოგადოების, როგორც ქვეყნის, ისე საერთაშორისო დონეზე“.[51]

კიბერუსაფრთხოება ხშირად განიხილება, როგორც სახელმწიფო მნიშვნელობის სტრატეგიული პრობლემა, რომელიც ეხება საზოგადოების ყველა ფენას. კიბერუსაფრთხოების სახელმწიფო პოლიტიკა (NCSS - National Cyber Security Strategy) არის საშუალება, რომელიც ემსახურება სახელმწიფოს

ინფორმაციული სისტემებისა და მთლიანად ინფრასტრუქტურის უსაფრთხოებისა და სანდოობის გაზრდის შესაძლებლობას, რომელიც ამავდროულად მაქსიმალურად ამცირებს რისკებს. კიბერუსაფრთხოების სტრატეგიაში გამოიყენება პრობლემისადმი მაღალი დონის მიდგომა, კერძოდ: გამოიყოფა სახელმწიფოს მთელი რიგი მიზნები, ამოცანები და პრიორიტეტები, რომლებიც აუცილებელია მოცემული დროის მონაკვეთში მისაღწევად. ფაქტიურად, სტრატეგია ეს არის მოდელი, რომელიც საშუალებას იძლევა კიბერუსაფრთხოების საკითხების მოგვარებას ქვეყნის შიგნით. ევროკავშირის წევრ - ქვეყნებში კიბერუსაფრთხოების უზრუნველყოფის გაუმჯობესებისა და კოორდინირებული მუშაობის, ასევე, საერთო პოლიტიკის შემუშავების მიზნით, შექმნილია სპეციალური სააგენტო European Union Agency for Network and Information Security – ENISA. ENISA ამუშავებს სპეციალურ სახელმძღვანელოს Good Practice Guide, რომელიც წარმოადგენს ევროკავშირის წევრი ქვეყნების მხარდამჭერ დოკუმენტს მათი მხრიდან კიბერუსაფრთხოების სახელმწიფო პოლიტიკის შემუშავების მთავარ მისიაში.

„ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების სტრატეგიები კიბერუსაფრთხოების პირველი სტრატეგია შემუშავებულ იქნა ამერიკის შეერთებულ შტატებში 2000 წლების დასაწყისში. შეერთებული შტატები გახდა ის ქვეყანა, რომელმაც დაიწყო კიბერუსაფრთხოების აღქმა, როგორც სახელმწიფო მნიშვნელობის საკითხი. 2003 წელს შეერთებულ შტატებში გამოქვეყნდა კიბერსივრცის უსაფრთხოების ეროვნული სტრატეგია (National Strategy to Secure Cyberspace). მოცემული დოკუმენტი წარმოადგენს უფრო ფართო ეროვნული უსაფრთხოების უზრუნველყოფის სტრატეგიის ნაწილს (National Strategy for Homeland Security), რომელიც შეიქმნა 2001 წლის 11 სექტემბრის ტერორისტული შეტევის პასუხად.

შემდგომ წლებში ევროპაში მთელი მასშტაბით დაიწყო ღონისძიებებისა და სტრატეგიების შემუშავება, რომელიც ემსახურებოდა კიბერუსივრცის დაცვის საკითხს. 2005 წელს გერმანია იღებს ინფორმაციული ინფრასტრუქტურის დაცვის სახელმწიფო გეგმას (National Plan for Information Infrastructure Protection - NPSI). მომავალ წელს შვედეთის მთავრობა ამუშავებს შვედეთში ინტერნეტის უსაფრთხოების გაძლიერების სტრატეგიას (Strategy to improve Internet Security in Sweden). ესტონეთმა თავისი კიბერუსაფრთხოების სტრატეგიის შემუშავება დაიწყო 2007 წელს

რუსეთის მხრიდან ქვეყანაზე განხორციელებული მასიური კიბერშეტევის შემდეგ და 2008 წელს ევროკავშირის წევრ - ქვეყნებს შორის გახდა პირველი, რომელმაც გამოაქვეყნა კიბერუსაფრთხოების სახელმწიფო სტრატეგია. ამის შემდეგ ევროკავშირის და უშუალოდ წევრი ქვეყნების მიერ გატარებულ იქნა მთელი რიგი ღონისძიებები და ჩატარდა დიდი სამუშაოები კიბერსივრცის უსაფრთხოების უზრუნველყოფის მიმართულებით".[7]

2011 წლის მაისში შეერთებულმა შტატებმა გამოაქვეყნა თავისი სტრატეგია კიბერსივრცის დაცვაზე. სტრატეგიას საფუძვლად უდევს მთავრობის, საერთაშორისო პარტნიორებისა და კერძო სექტორს შორის თანამშრომლობის მოდელი, სადაც აღწერილია მთელი რიგი ღონისძიებები, რომლებიც აუცილებელია გატარდეს შემდეგი შვიდი მიმართულებით: • ეკონომიკა - საერთაშორისო სტანდარტებისა და ინოვაციების მოზიდვა, ღია და ლიბერალური ბაზარი; • ეროვნული ქსელის დაცვა - უსაფრთხოების ამაღლება, სანდოობა და მდგრადობა; • სამართალებრივი მხარე - თანამშრომლობისა და სამართლებრივი ნორმების გაფართოება; • სამხედრო სფერო - უსაფრთხოების თანამედროვე გამოწვევებზე მზადყოფნა; • სამთავრობო ინტერნეტის ქსელი - სამთავრობო სტრუქტურების ეფექტურობისა და მრავალმომცველობის გაფართოება; • საერთაშორისო განვითარება - უსაფრთხოების ორგანიზება, საერთაშორისო კომპეტენციების განვითარება და ეკონომიკური აყვავება; • თავისუფლება ინტერნეტში - მოქალაქეთა კერძო ცხოვრების ხელშეუხებლობისა და თავისუფლების მხარდაჭერა.

„ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების სტრატეგიების საერთო პრინციპები და რეკომენდაციები კიბერუსაფრთხოების განსაზღვრების შესახებ შეთანხმება საერთაშორისო დონეზე არ არსებობს. ყოველ ქვეყანაში კიბერუსაფრთხოების, კიბერსივრცის, კიბერდანაშაულისა და მასთან დაკავშირებული მთავარი ტერმინების განსაზღვრება შეიძლება მკვეთრად განსხვავდებოდეს ერთმანეთისგან. ასევე განსხვავდება თითოეული ქვეყნის მიდგომა კიბერუსაფრთხოების სტრატეგიის შედგენის მიმართ. მიუხედავად იმისა, რომ საერთაშორისო თანამშრომლობის მნიშვნელობას აღიარებს ყველა ქვეყანა, მაინც საერთო მთავარი ტერმინებისა და ერთიანი ე. წ. „ენის" არარსებობა ძალზედ ართულებს თანამშრომლობას საერთაშორისო დონეზე. საერთო პრინციპები როგორც წესი, ყოველი ქვეყნის კიბერუსაფრთხოების სტრატეგიებს მაინც გააჩნიათ საერთო პრინციპები,

რომელიც შეიძლება შემდეგნაირად ჩამოყალიბდეს: ⎪ სახელმწიფო მოდელისა და პოლიტიკის შემუშავება, რომელიც მიმართულია კიბერუსაფრთხოების უზრუნველყოფაზე; ⎪ სახელმწიფო პარტნიორობაზე დაფუძნებული შესაბამისი მექანიზმის განსაზღვრა, რომელიც კერძო და სახელმწიფო სექტორის დაინტერესებულ მხარეებს საშუალებას აძლევს განიხილონ და დაამტკიცონ პოლიტიკა დაკავშირებული კიბერუსაფრთხოების პრობლემებთან; ⎪ აუცილებელი პოლიტიკისა და მექანიზმების რეგულაციების დაგეგმვა და განსაზღვრა, როლების, უფლებებისა და პასუხისმგებლობის მკვეთრი გამიჯვნა კერძო და სახელმწიფო სექტორისთვის".[38]

„კიბერდანაშაულის ტრანსსასაზღვრო ხასიათი წევრ - ქვეყნებს იძულებულს ხდის მჭიდროდ ითანამშრომლონ ერთმანეთთან და ზოგადად საერთაშორისო დონეზე. მსგავსი თანამშრომლობა აუცილებელია არამარტო კიბერშეტევისთვის ეფექტური მომზადებისთვის, არამედ მათზე დროული რეაგირებისთვის. ამიტომ კიბერუსაფრთხოების მიმართ სახელმწიფო სტრატეგიის მიდგომა უნდა იყოს კომპლექსური. ამ მიზნით, ევროკავშირი, მასში შემავალი წევრი ქვეყნების მიმართ იძლევა ზოგად რეკომენდაციებს, კერძოდ: მოკლევადიანი პერიოდისთვის ⎪ დაპროექტდეს, შეფასდეს და მხარი დაეჭიროს კიბერუსაფრთხოების სახელმწიფო სტრატეგიას. ასევე ის ღონისძიებები, რომლებიც აუცილებელია გატარდეს სტრატეგიის ჩარჩოში; ⎪ მკვეთრად უნდა განისაზღვროს მოქმედების არეალი, სტრატეგიის მიზნები და თავად ტერმინი „კიბერუსაფრთხოება"; ⎪ უნდა დარწმუნდნენ, რომ კიბერუსაფრთხოებაზე პასუხისმგებელი სახელმწიფო ორგანოს მიერ შემუშავებული წინადადებები და რეგულაციები, იქნება განხილული და მიღებული; ⎪ სტრატეგიაში უნდა იქნას გათვალისწინებული სამეცნიერო საზოგადოების, სამრეწველო და ეკონომიკური წარმომადგენლებისა და სამოქალაქო ინტერესები; ⎪ კიბერუსაფრთხოების კოორდინირებული და შეთანხმებული ხასიათის გარანტირებული თანამშრომლობის მიზნით, წევრმა ქვეყნებმა უნდა ითანამშრომლონ ერთმანეთთან, აგრეთვე მათ მჭიდრო ურთიერთობა უნდა გააჩნდეს ევროკავშირის კომისიასთან; ⎪ აუცილებელია აღიარებული იქნას ის გარემოება, რომ კიბერსივრცე და კიბერუსაფრთხოება მუდმივად განიცდის განვითარებას, და ამიტომ სტრატეგია მუდმივად მოითხოვს რედაქტირებასა და გადახედვას, რათა ის შესაბამისობაში იქნას მოყვანილი ახალ გამოწვევებთან".[8]

აუცილებელია გავითვალისწინოთ ის ფაქტი, რომ მუდმივად არსებული რისკები და ახალი საფრთხეები საშუალებას იძლევა განვითარდეს და გაუმჯობესდეს ინფორმაციული სისტემები სახელმწიფო, კერძო და სამოქალაქო სექტორებისთვის; ⎪ აუცილებელია თავიდან იქნას არიდებული გატარებული ღონისძიებების დუბლირება და ფოკუსირება გაკეთდეს ახალ პრობლემებსა და გამოწვევებზე; ⎪ აუცილებელია, რომ სტრატეგია შესაბამისად იქნას გამოყენებული და მოქმედებდეს ეროვნული და ევროპული უსაფრთხოების დონის ამაღლებაზე; ⎪ მხარი უნდა დაეჭიროს ევროკავშირის კომისიას ინტერნეტის უსაფრთხოების სტრატეგიაზე მუშაობის, შექმნისა და იმპლიმენტაციის საკითხში. გრძელვადიანი პერიოდისთვის ⎪ მომავალში მთლიანად ევროკავშირისთვის საერთო მიზნების მიღწევისა და ფორმულირების მიზნით, აუცილებელია შემუშავდეს და შეთანხმდეს „კიბერუსაფრთხოების“ საერთო განსაზღვრება და მასთან დაკავშირებული ტერმინოლოგია; ⎪ აუცილებელია გათვალისწინებული იქნას ის გარემოება, რომ ევროკავშირისა და მისი წევრი ქვეყნების კიბერუსაფრთხოების სტრატეგიები არ უნდა ეწინააღმდეგებოდეს საერთაშორისო საზოგადოების მიზნებს და ადამიანის უფლებებს, თუმცა ამავდროულად, გლობალურ დონეზე მხარს უნდა უჭერდეს კიბერუსაფრთხოების პრობლემებთან ბრძოლას.

2.6. საქართველოში კიბერუსაფრთხოების უზრუნველყოფის მიმართულებით არსებული მდგომარეობა და რეკომენდაციები

2008-2011 წლებში საქართველოს წინააღმდეგ განხორციელებულმა ფართომასშტაბიანმა კიბერშეტევებმა ნათლად დაგვანახა კიბერუსაფრთხოების პოლიტიკის შემუშავების აუცილებლობა, რათა უზრუნველყოფილ იქნეს კრიტიკული ინფორმაციული სისტემების გამართული და უსაფრთხო ფუნქციონირება. აღნიშნულმა გარემოებამ განაპირობა თავდაცვის სამინისტროს მიერ შემუშავებულიყო კიბერუსაფრთხოების პოლიტიკა 2014-2016 წლებისათვის.

სახელმწიფოს ინიციატივა-უზრუნველყოს და განავითაროს კიბერუსაფრთხოება, გახლავთ მისი მხრიდან გადადგმული ერთ-ერთი მნიშვნელოვანი ნაბიჯი, რაც უზრუნველყოფს საქართველოს თავდაცვის სფეროსა და მასში შემავალი კრიტიკული ინფორმაციული სისტემების დაცვასა და გაძლიერებას.

კიბერსივრცე ქმნის ერთიან კომპლექსურ გარემოს მასში შემავალი ინფორმაციული და კომუნიკაციების ტექნოლოგიების მოწყობილობებითა და ქსელებით, რაც საშუალებას აძლევს საქართველოს თავდაცვის სამინისტროს სამოქალაქო ოფისს, შეიარაღებული ძალების გენერალური შტაბის სტრუქტურულ ქვედანაყოფებსა და სამინისტროში შემავალ საჯარო სამართლის იურიდიულ პირებს განახორციელონ სხვადასხვა ტიპის კომუნიკაცია, ძალებისა და საშუალებების მართვა.

მომავალში კიბერსივრცე კიდევ უფრო მასშტაბური გახდება, გაიზრდება სახელმწიფო სტრუქტურების დამოკიდებულება ინფორმაციულ ტექნოლოგიებზე, რაც განაპირობებს ახალი რისკებისა და საფრთხეების წარმოქმნას. სწორედ აქედან გამომდინარე, აუცილებელია კიბერუსაფრთხოების ისეთი მოქნილი მექანიზმების შექმნა, რომლებიც ეფექტურად უპასუხებენ ახლად წარმოქმნილ გამოწვევებს. კიბერუსაფრთხოების უზრუნველყოფის მნიშვნელოვან ნაწილს, აგრეთვე წარმოადგენს ახალი კიბერშეტევებისადმი ინფორმაციული სისტემების მდგრადობის ამაღლება, პრევენციული ღონისძიებების შემუშავება და გატარება.

კიბერუსაფრთხოება მოიცავს საქართველოს თავდაცვის სამინისტროს საქმიანობის ყველა იმ სფეროს, სადაც გამოიყენება ინფორმაციული ტექნოლოგიები, იქნება ეს სამხედრო/თავდაცვითი ოპერაციების დაგეგმვა, სამხედრო წვრთნების წარმოება, ლოგისტიკური მხარდაჭერა თუ სხვა, რათა უზრუნველყოფილი იქნეს ინფორმაციის მთლიანობა, ხელმისაწვდომობა და დროული გაზიარება.

კიბერსივრცეში ადგილი აქვს მიზანმიმართული, შემთხვევითი, ბუნებრივი ხასიათის ინციდენტებს. ინფორმაციული ტექნოლოგიები შესაძლებელია გამოყენებული იქნეს არამართებული მიზნებისათვის სხვადასხვა წყაროს მიერ. მიზანმიმართულმა კიბერშეტევამ შესაძლოა მნიშვნელოვნად შეაფერხოს კრიტიკული ინფორმაციული სისტემების

გამართული ფუნქციონირება, საფრთხე შეუქმნას ქვეყნის თავდაცვისუნარიანობას და უსაფრთხოებას.

კიბერუსაფრთხოება ხშირად განიხილება, როგორც სახელმწიფო მნიშვნელობის სტრატეგიული პრობლემა, რომელიც ეხება საზოგადოების ყველა ფენას. კიბერუსაფრთხოების სახელმწიფო პოლიტიკა (NCSS - National Cyber Security Strategy) არის საშუალება, რომელიც ემსახურება სახელმწიფოს ინფორმაციული სისტემებისა და მთლიანად ინფრასტრუქტურის უსაფრთხოებისა და სანდოობის გაზრდის შესაძლებლობას, რომელიც ამავდროულად მაქსიმალურად ამცირებს რისკებს. კიბერუსაფრთხოების სტრატეგიაში გამოიყენება პრობლემისადმი მაღალი დონის მიდგომა, კერძოდ: გამოიყოფა სახელმწიფოს მთელი რიგი მიზნები, ამოცანები და პრიორიტეტები, რომლებიც აუცილებელია მოცემული დროის მონაკვეთში მისაღწევად. ფაქტიურად, სტრატეგია ეს არის მოდელი, რომელიც საშუალებას იძლევა კიბერუსაფრთხოების საკითხების მოგვარებას ქვეყნის შიგნით.

როგორც წესი, ყოველი ქვეყნის კიბერუსაფრთხოების სტრატეგიებს გააჩნიათ საერთო პრინციპები, რომელიც შიძლება შემდეგნაირად ჩამოყალიბდეს:

- ✓ სახელმწიფო მოდელისა და პოლიტიკის შემუშავება, რომელიც მიმართულია კიბერუსაფრთხოების უზრუნველყოფაზე;
- ✓ სახელმწიფო პარტნიორობაზე დაფუძნებული შესაბამისი მექანიზმის განსაზღვრა, რომელიც კერძო და სახელმწიფო სექტორის დაინტერესებულ მხარეებს საშუალებას აძლევს განიხილონ და დაამტკიცონ პოლიტიკა დაკავშირებული კიბერუსაფრთხოების პრობლემებთან;
- ✓ აუცილებელი პოლიტიკისა და მექანიზმების რეგულაციების დაგეგმვა და განსაზღვრა, როლების, უფლებებისა და პასუხისმგებლობის მკვეთრი გამიჯვნა კერძო და სახელმწიფო სექტორისთვის;
- ✓ რისკების სახელმწიფო მართვის მიმართ სისტემური და ინტეგრირებული მიდგომის შემუშავება;
- ✓ ინფორმაციული პროგრამების მიზნების განსაზღვრა და აღნიშვნა, რომელიც მიმართულია შესთავაზოს მომხმარებელს ქცევისა და მუშაობის ახალი მოდელები;
- ✓ საერთაშორისო თანამშრომლობა არამარტო ევროკავშირის წევრ - ქვეყნებს შორის, არამედ იმ ქვეყნებთანაც, რომლებიც არ შედიან ევროკავშირში;

✓ კომპლექსური კვლევების ჩატარება და პროგრამების განვითარებაზე მუშაობა, რომელიც მიმართულია კიბერსივრცის უსაფრთხოების პრობლემების გადაჭრაზე. ინტელექტუალური რესურსების განვითარება;

საქართველოს ეროვნული უსაფრთხოების კონცეფცია კიბერსივრცის დაცვის უზრუნველყოფასა და ზოგადად კიბერუსაფრთხოებას განიხილავს, როგორც ქვეყნის უსაფრთხოების ერთ - ერთ ძირითად შემადგენელ ნაწილსა და მის მნიშვნელოვან მიმართულებას. კიბერსივრცის დაცვასა და კიბერუსაფრთხოების უზრუნველყოფაზე ბევრად არის დამოკიდებული ქვეყნის შემდგომი ეკონომიკური სტაბილურობა და სოციალური განვითარება. მოცემული მიზნის მისაღწევად, სტრატეგია განიხილავს შემდეგი თანამშრომლობის მნიშვნელოვან პრინციპებს:

- საქართველოს მთავრობის ერთიანი მიდგომა;
- თანამშრომლობა სახელმწიფო და კერძო სექტორებს შორის;
- აქტიური საერთაშორისო თანამშრომლობა;
- ინდივიდუალური პასუხისმგებლობა;
- ადეკვატური ზომები.

საქართველო აქტიურად მიისწრაფვის ევროინტეგრაციისკენ, ქვეყანა ცდილობს გახდეს ევროკავშირისა და ჩრდილოეთ ალიანსის სრულუფლებიანი წევრი, ხელი მოეწერა ასოცირების ხელშეკრულებას. ყოველივე ეს ნიშნავს, რომ ქვეყანა თავის თავზე იღებს ყველა იმ ვალდებულებას, რაც უზრუნველყოფს არამარტო საქართველოს უსაფრთხოებას, არამედ ევროკავშირის როგორც ცალკეული წევრი ქვეყნებისა ისე მთლიანად ევროკავშირის უსაფრთხოების შესაბამისი ნორმების დაცვას, სადაც ასევე იგულისხმება კიბერსივრცის მაქსიმალური დაცვის უზრუნველყოფა. ეს არის ქვეყნისთვის სერიოზული გამოწვევა, რადგან საქართველომ წესრიგში უნდა მოიყვანოს და საერთაშორისო სტანდარტებს შეუსაბამოს ქვეყნის კრიტიკული ინფორმაციული ინფრასტრუქტურის სისტემისა და ცალკეული სუბიექტების დაცვა, გაზარდოს საერთაშორისო თანამშრომლობა და რისკების შემცირების მიზნით, უნდა მოახდინოს საზოგადოების ცნობიერების ამაღლება და საგანმანათლებლო სისტემის შემუშავება.

მიმართულებების მიხედვით და ერთიანი საწარმოების, ორგანიზაციების, სახელმწიფო დაწესებულებების, მთავრობის ხელისუფლების სხვადასხვა ორგანოების ხელმძღვანელები და საერთოდ

ნებისმიერი მიზანდასახული სისტემის ხელმძღვანელი - ესაა ადამიანი, რომელსაც უხდება მთელი რიგი პრობლემების მრავალჯერად გადაწყვეტა სხვადასხვა პირობებში. მიმდინარე გადაწყვეტილებების გარდა, არსებობენ უნიკალური გადაწყვეტილებები. ისინი ხასიათდებიან იმით, რომ ასეთი გადაწყვეტილების მიღების აუცილებლობა წარმოიშობა ერთჯერ ან ძალიან იშვიათად, მაგრამ ასეთი არჩევანის გაკეთებამ მომავალში შესაძლებელია ძალზე სერიოზული გავლენა მოახდინოს სისტემის ფუნქციონირებაზე.

2008 წელსაც, რუსეთ-საქართველოს დაპირისპირებისას, საქართველოს მთავრობის ინტერნეტ რესურსებიც ფაქტობრივად დაბლოკილი აღმოჩნდა. მაშინაც ომმა ინტერნეტ სივრცეშიც გადაინაცვლა. 2009 წელს რუსეთ-საქართველოს ომის წლისთავზე, ინტერნეტში ნამდვილი ბრძოლა გაჩაღდა. დაპირისპირება იმდენად მასშტაბური იყო, რომ მსოფლიოს სხვადასხვა კუთხეში მცხოვრებ უამრავ ადამიანს შეეხო. ამის შესახებ წამყვანი უცხოური მედია საშუალებებიც წერდნენ – New York Times, CNET, The Register და ა.შ. ცდილობდნენ გაერკვიათ რაში იყო საქმე, რატომ დაიბლოკა ინტერნეტ სერვისები, რომლებსაც მილიონობით ადამიანი იყენებს.

სწორეს 2008 წლის რუსეთ-საქართველოს ომის შემდეგ რუსულ ინტერნეტსივრცეში გაჩნდა პირველი ინფორმაცია იმის შესახებ, რომ რუსეთში ახალი გასამხედროებული სტრუქტურა შეიქმნა - „საინფორმაციო არმია“, ეს არის კარგად გაწერილი ცენტრალიზირიებული მექანიზმი, რომლის მთავარ მიზანს წარმოადგენს რუსეთისათვის საჭირო ინფორმაციის შექმნა და მსოფლიოში გავრცელება.

ინფორმაცია სხვადასხვა გზებით, საშუალებებით და ფორმით ვრცელდება; ახლად შექმნილი სტრუქტურის მიზანი სხვადასხვა პროფესიის ადამიანური რესურსისა და თანამდეროვე ტექნიკური საშუალებების გაერთიანებაა, რომ უფრო კოორდინირებულად მოხდეს საინფორმაციო ომის წარმოება. „საინფორმაციო არმია“ აერთიანებს: ისტორიკოსებს, ეთნოლოგებს, რელიგიის სპეციალსიტებს, ანალიტიკოსებს, სოციოლოგებს, ფსიქოლოგებს, სცენარისტებს და სხვ. „საინფორმაციო პროდუქცია: წიგნი, ბროშურა, პლაკატი, დოკუმენტური თუ ნახატი ფილმი და სხვ.

უფრო საგულისხმოა ის სამი ამოცანა, რომლის დეტალურად აღწერს „საინფორმაციო არმიის“ არსს და მიზანს:

1. სტრატეგიული ანალიზი;

2. ინფორმაციული ზეგავლენა;

3. საინფორმაციო უკუქმედება.

მათი აზრით, ყოველივე ეს უნდა მუშაობდეს კოორდინირებულად; იმისთვის, რომ პირველი განხორციელდეს, აუცილებელია ის ფუნქციონირებდეს კონტრდაზვერვაში, რომელიც მოახდენს ინფორმაციის მართვას და უზრუნველყოფს მის დაცვას; მეორე - უნდა შეიქმნას ანტიკრიზისული ცენტრი, რაც გულისხმობს სახელმწიფოს მხრიდან ჰოლდინგის შექმნას, რაშიც შედის ტელეარხი და საინფორმაციო სააგენტო. მესამე ამოცანის შესასრულებლად საჭიროა ისეთი ცენტრების შექმნა, რომლებიც აღმოაჩენენ მოწინააღმდეგის ინფორმაციის გავრცელების სტრუქტურას და მოახდენენ მის ფიზიკურ ლიკვიდაციას; რადიოელექტრონული ბრძოლისთვის, ფსიქოლოგიური და ქსელური ოპერაციებისთვის, „საჭიროა ხაკერების მომზადებაც“.

2007-2014 წლის განმავლობაში დაფიქსირდა მრავალი შემთვევა, როდესაც ინტერნეტის და კომპიუტერული ვირუსების გამოყენებით მიზანმიმართულად დაზიანდა სხვადასხვა ქვეყნის და კომპანიის კრიტიკული, მნიშვნელოვანი ინფრასტრუქტურა. 2008 წლის რუსეთ-საქართველოს საომარი მოქმედებების დროს, საქართველოს ინტერნეტ სივრცე სერიოზული კიბერ შეტევების წინაშე აღმოჩნდა.

- მიზანმიმართულად გატყდა და დაზიანდა მრავალი სახელმწიფო საიტი, ასევე საინფორმაციო სააგენტოების კუთვნილი ინტერნეტ გვერდები. ზოგიერთი სახელმწიფო საიტის ფუნქციონირების აღდგენის მიზნით მოხდა მათი დროებითი ასლების შექმნა ამერიკულ და ევროპულ ინტერნეტ სივრცეში.

- ქართული ინტერნეტ სივრცის მიმართულებით იგზავნებოდა დიდი რაოდენობის ქსელური პაკეტები, რამაც გამოიწვია ინტერნეტ არხების გადავსება და ქართული ინტერნეტ სივრცის დროებითი დაზიანებები.

GeorBot – 2011-2012 წლების განმავლობაში მიზანმიმართული კიბერშპიონაჟი ქართული სახელმწიფო რესურსების წინააღმდეგ.

კიბერუსაფრთხოების სფეროში არსებულ რთულ გამოწვევებთან გამკლავებას უდიდესი მნიშვნელობა აქვს როგორც საერთაშორისო და რეგიონალურ, ისე ეროვნულ დონეზე.

მომავალში თანამედროვე საზოგადოება გახდება სულ უფრო მოწყვლადი, რადგან, რთულია ერთმანეთთან დაკავშირებული და დამოკიდებული სისტემების სრულად აღქმა და დაცვა. გაიზრდება

გლობალური და შიდა საზოგადოებრივი დამოკიდებულებები, რაც კიბერუსაფრთხოების გამოწვევებს სულ უფრო გლობალურ ხასიათს აძლევს და ამდენად, არსებობს კიბერ საფრთხეებზე საერთაშორისო რეაგირების აუცილებლობა. ახალი ტექნოლოგიური ინოვაციები ძირითადად მოდის კერძო სექტორიდან და ეს პროცესი სულ უფრო მზარდი იქნება, რაც ერთი – ორად ზრდის ასევე უსაფრთხოების უზრუნველყოფის საჭიროებას.

კიბერდანაშაულებები კვლავ იქნება გამოწვევა საზოგადოებისთვის და ეკონომიკური დანაკარგები სულ უფრო გაიზრდება, რაც სხვა მხრივ ხელს შეუწყობს სახელმწიფოსა და კერძო სექტორს შორის თანამშრომლობის განვითარებას. კიბერ შესაძლებლობების კონცეფციას გავლენა ექნება საერთაშორისო პოლიტიკაზე და ძალაუფლებისთვის გლობალურ ბრძოლაზე, რაც ასევე შეუწყობს ხელს კიბერ სივრცეში გამალებული შეიარაღების პროცესის გაზრდის ტენდენციას. კიბერის ახალ ეპოქაში გამარჯვებული იქნება ის, ვინც შეძლებს საბაზრო ეკონომიკის გათვალისწინებით უსაფრთხოების საკითხების კომპლექსურ გადაწყვეტას; გააჩნიათ საუკეთესო ტალანტების მობილიზების შესაძლებლობა; და შესწევთ ადაპტაციის უნარი და ყოველგვარი ძალისხმევის გარეშე იმუშაონ მრავალეროვან გარემოში.

ფაქტიურად, კიბერუსაფრთხოება გახდა საგარეო პოლიტიკის შემადგენელი ნაწილი და ის სულ უფრო აქტიურ როლს თამაშობს საერთაშორისო ურთიერთობების საკითხში. საინტერესოა ამ მხრივ რა მდგომარეობაა საქართველოში? უკვე 2008 წლის აგვისტოს ომის შემდეგ, როცა რუსეთის მხრიდან მოხდა მასირებული კიბერ შეტევა ქვეყნის ინფრასტრუქტურაზე, სამთავრობო ვებ გვერდებზე. ქვეყანა დადგა სერიოზული პრობლემის წინაშე, იყო საფრთხე, რომ საქართველო მოქცეულიყო ინფორმაციულ ვაკუუმში. მიღებული ცუდი გამოცდილების გათვალისწინებით, ხელისუფლებამ დაიწყო კიბერუსაფრთხოების სფეროს განვითარებაზე ფიქრი. კერძოდ, იუსტიციის სამინისტროში შეიქმნა სსიპ – მონაცემთა დაცვის სააგენტო, განისაზღვრა კრიტიკული ინფორმაციული ინფრასტრუქტურის სუბიექტები, რომელთა დაცვა დაევალა მონაცემთა გაცვლის სააგენტოს, ასევე თავდაცვის სამინისტროში შექმნილია სსიპ – კიბერუსაფრთხოების ბიურო, რომელიც პასუხისმგებელია თავდაცვის სფეროში კიბერუსაფრთხოებითი ღონისძიებების გატარებაზე. ასევე შინაგან საქმეთა სამინისტროს ცენტრალური კრიმინალური პოლიციის

დეპარტამენტში არსებობს კიბერდანაშაულთან ბრძოლის სამმართველო, და ბოლოს რაც ასევე მნიშვნელოვანია შეიქმნა კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელი მთავარი დოკუმენტი – საქართველოს კიბერუსაფრთხოების 2013-2015 წლების სტრატეგია. კიბერუსაფრთხოების სტრატეგიის რეალიზაციისთვის აუცილებელია კერძო და სახელმწიფო სექტორების ერთმანეთთან მჭიდრო თანამშრომლობა, რომელიც სახელმწიფო და ზოგადად ევროკავშირის დონეზე, უნდა განხორციელდეს ინფორმაციის გაცვლის საშუალებებით, მოწინავე ტექნოლოგიებისა და პრაქტიკული ცოდნის გაზიარებით, აგრეთვე სამეცნიერო წრეების ერთმანეთთან დაახლოებითა და პრობლემაზე ერთობლივი მუშაობით.

3.1. სახელმწიფოში კრიტიკული ინფრასტრუქტურის კიბერუსაფრთხოების უზრუნველყოფის ინოვაციური მეთოდები და საშუალებები

დღეს არსებული მდგომარეობით თითოეული სამინისტრო და სახელმწიფო უწყება თავისი არსებული რესურსების გამოყენებით ზრუნავს კიბერ უსაფრთხოების დაცვაზე. რესურსებიდან გამომდინარე დაცვის დონე განსხვავებულია უწყებებს შორის. ხშირად ეს დონე არ შეესაბამება დაცვის მინიმალურ დონესაც. რაც შეეხება სამოქალაქო სექტორს ან მოქალაქეებს, ამ მიმართულებით თითქმის არავითარი ნაბიჯები არ არის გადადგმული.“ იგივე დასკვნის გაკეთების საშუალებას გვაძლევს კრიტიკული ინფრასტრუქტურის განსაზღვრებაც: „კრიტიკული ინფრასტრუქტურა – ნორმატიული აქტის საფუძველზე გამოცემული სხვა განსაზღვრული იურიდიული პირების, სახელმწიფო ორგანოებისა და საქმიანობის სფეროების ერთობლიობა, რომლის ინფორმაციული სისტემების უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალური ფუნქციონირებისათვის. აქედან გამომდინარე, ჩვენ მიგვაჩნია, რომ დებულებები მიმართული უნდა იყოს ინფორმაციული სისტემებისა და ამ სისტემების უსაფრთხოდ ფუნქციონირების უზრუნველსაყოფად.

სისტემის უსაფრთხოების გეგმები წარმოადგენენ რეალურ დოკუმენტაციას, რომლებიც მოითხოვენ პერიოდულ გადახედვას, განახლებას და ასევე ქმედებებს და ეტაპებს უსაფრთხოების კონტროლის მექანიზმების დასანერგად. ადგილზე უნდა არსებობდეს ასევე პროცედურები, რომლებიც აფიქსირებენ, თუ ვის მიერ განხორციელდა გეგმის გადახედვა, მოცემული მომენტისათვის ვინ არის გეგმაზე პასუხისმგებელი და ასევე ვინ მეთვალყურეობს პერიოდულად უსაფრთხოების კონტროლის დაგეგმილ მექანიზმებს. ამას გარდა, პროცედურები უნდა ავალდებულებდნენ იმასაც, რომ სისტემის უსაფრთხების გეგმები შექმნილი და გადახედილ იქნას მათთვის უსაფრთოების სერტიფიკატის მინიჭებამდე და ასევე სისტემისათვის აკრედიტაციის პროცესის დასრულებამდე.

უსაფრთხოების სერტიფიცირებისა და აკრედიტაციის დროს ხდება სისტემის უსაფრთხოების გეგმის ანალიზი, განახლება და დამტკიცება.

სერტიფიცირების აგენტი ადასტურებს, რომ უსაფრთხოების კონტროლის მექანიზმები, რომლებიც აღწერილია სისტემის უსაფრთოხების გეგმაში, უსაფრთოხების იმ კატეგორიასთან, რომელიც საინფორმაციო სისტემებისათვის არის დადგენილი და რომ საფრთხის იდენტიფიცირება და საწყისი რისკების დადგენა იდენტიფიცირებული და დოკუმენტირებულია სისტემის უსაფრთხოების გეგმაში, რისკის შეფასების ან სხვა ექვივალენტურ დოკუმენტში. უსაფრთოხების სერტიფიცირების შედეგები გამოიყენება რისკების ხელმეორედ შესაფასებლად და ასევე საქმიანობის ეტაპების გეგმის შესადგენად, რომელთა არსებობაც აუცილებელია გამოსასწორებელი სამუშაობის ზედამხედველობისათვის და ასევე სისტემის უსაფრთხების გეგმის განსაახლებლად, რაც ფაქტიური საფუძველია უფლებამოსილი ოფიციალური პირისათვის უსაფრთხოების აკრედიტაციის შესახებ გადაწყვეტილების მისაღებად.

კერძოდ, იქიდან გამომდინარე, რომ საერთაშორისო პრაქტიკის გათვალისწინებით, ვფიქრობთ, რომ კრიტიკული ინფრასტრუქტურის სუბიექტებში იგულისხმება: საფინანსო სექტორი;¬ კომუნიკაციების სექტორი;¬ ინფორმაციული ტექნოლოგიების სექტორი;¬ ენერგეტიკისა და წყალმომარაგების სექტორი;¬ სატრანსპორტო სისტემების სექტორი;¬ ჯანმრთელობის დაცვისა სექტორი;¬ ინდუსტრიული, მათ შორის სამშენებლო და ქიმიური მრეწველობის სექტორი;¬ თავდაცვისა და უსაფრთხოების სექტორი და ა.შ.¬ თავისთავად, აღნიშნული სექტორები მოიცავენ საკმაოდ ფართო სპექტრს მიმართულებებისა, რომელიც შესაძლებელია მიჩნეულ იქნეს კრიტიკული ინფრასტრუქტურის სუბიექტებად. მაგალითად, ამერიკის შეერთებული შტატებში კრიტიკულ ინფრასტრუქტურად ითვლება მასობრივი საზოგადოებრივი თავშეყრის ადგილები.

უნდა დადგინდეს და დაცული იქნას ინფორმაციული უსაფრთხოების რისკების მართვის პროცესისთვის საჭირო ორგანიზაციული სტრუქტურა და პასუხისმგებლობები. ძირითადი როლები და პასუხისმგებლობები გახლავთ:

- ორგანიზაციაზე მორგებული ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის შემუშავება;
- დაინტერესებული პირების გამოვლენა და ანალიზი;
- ყველა მხარის (როგორც შიდა ასევე გარე) როლებისა და პასუხისმგებლობების განსაზღვრა ორგანიზაციისათვის;

- ორგანიზაციასა და დაინტერესებულ პირებს შორის საჭირო ურთიერთობის დამტკიცება, ასევე ორგანიზაციის მაღალი დონის რისკების მართვის ფუნქციებისთვის ინტერფეისების დადგენა (მაგალითად: ოპერაციული რისკების მართვა), ასევე სხვა პროექტების და ქმედებებისთვის საჭირო ინტერფეისები;

- გადაწყვეტილების მიღების წესის განსაზღვრა;

- აღრიცხვიანობის (რეგისტრირების, ჩანაწერების) მახასიათებლები.

ამგვარი ორგანიზაციული სტრუქტურა დამტკიცებული უნდა იქნას მენეჯერების მიერ.

იზრდება რა კომპიუტერის როლი და მისი გამოყენების არეალი სახელმწიფოში, პირდაპირპროპორციულად მატულობს კიბერდანაშაულებების საფრთხეც. სწორედ ამიტომ, მნიშვნელოვანია, რომ ამ საკითხის ირგვლივ სრულფასოვნად და მაქსიმალურად ინფორმირებულნი იყვნენ, როგორც კონკრეტული კომპეტენციის წრეები, ისე სამოქალაქო საზოგადოება.

საინფორმაციო და საკომუნიკაციო-ტექნოლოგიურმა რევოლუციამ ბიძგი მისცა არა მხოლოდ საზოგადოების პროგრესს, არამედ გახდა მანამდე უცნობი ნეგატიური პროცესების წარმოშობისა და განვითარების სტიმულატორი. კომპიუტერული ტექნპლოგიები უზარმაზარ პოტენციალს ატარებს როგორც პროგრესისათვის, ისე ბოროტად გამოყენებისათვის - კომპიუტერული მონაცემის ან სისტემის ხელყოფა, გამოყენება და სხვა.

3.2. სარეჟიმო ობიექტის დაცვის სისტემისფუნქციონირების ზოგადო მოდელი

სარეჟიმო ობიექტის ქვეშ მოვიაზრებთ ინფორმაციას, რომელიც ცირკულირებს ნებისმიერი სახის მიზანდასახულ სისტემაში დაწყებული ადამიანით და სახელმწიფო და საერთაშორისო ორგანიზაციებით დამთავრებული, და წარმოადგენს სისტემას წარმოქმნილ მთავარ დომინანტს. დაცვას საჭიროებს სუბიექტი, როგორც ღირებული ინფორმაციის მატარებელი. სარეჟიმო ობიექტის ცნება მოიცავს ყველა იმ მატერიალურ მატარებელს, რომელშიც ინახება ან ცირკულირებს ღირებული ინფორმაცია.

აქვე ხაზი უნდა გავუსვათ იმ გარეომოებას, რომ ჩვენი საგნის სპეციფიკიდან გამომდინარე მთავარ აქცენტს ვაკეთებთ მაინც მონაცემთა დამუშავების ავტომატიზებულ სისტემაზე, ასს-ზე, რომელიც წარმოადგენს ნებისმიერი ორგანიზაცული მართვის ავტომატიზებული სისტემის (მას) უმთავრეს მაორგანიზებელ საშუალებას.

ერთ-ერთი უმნიშვნელოვანესი დასკვა, რომელიც მიღებულია თეორიული გამოკვლევებისა და დაცვის პრობლემების პრაქტიკული გადაწყვეტების გამოცდილების ანალიზის შედეგად, ესაა დასკვნა იმის შესახებ, რომ ინფორმაციის დაცვის თანამედროვე მოთხოვნილებებისა და პირობების ადეკვატური შეიძლება იყოს მხოლოდ კომპლექსური მიდგომა მოცემული პრობლემების გადაწყვეტისადმი. ამ დროს უნდა გვახსოვდეს, რომ თვით კომპლექსურობის ცნება არის რთული და მოიცავს თავის თავში შემდეგ ასპექტებს მაინც:

- მიზნობრივ კომპლექსურობას, ანუ დაცვა ინფორმაციისა დაცულობის ყველა მაჩვენებლის მიხედვით და ყველა იმ ფაქტორების ერთობლიობის გათვალისწინებით, რომლებიც გავლენას ახდენენ დაცულობაზე;

- დროით კომპლექსურობას, ანუ ინფორმაციის უწყვეტად დაცვას დროში და ყველა ეტაპზე ინფორმაციის, მისი მატერიალური მატარებლების, ასს სასიცოცხლო ციკლისა;

- კონცეპტუალურ კომპლესურობას, ანუ დაცვის პრობლემის შესწავლა და რეალიზაციას, მას-ის განვითარების, აგების და გამოყენების ყველა პრობლემასთან ერთად.

აღნიშნული მიდგომის არსი ძალიან ზოგადი სახით შეიძლება წარმოდგენილ იქნას შემდეგი სამი თითქმის ძალზე ცხადი, მაგრამ პრაქტიკულად არა ყოველთვის რეალიზებადი სახით:

- სისტემური გათვალისწინება იმ ფაქტორების მთელი ერთობლიობისა, რომლებსაც აქვთ არსებითი მნიშვნელობა გადასაწყვეტი პრობლემის თვასაზრისით;

- დამუშავება უბრალოდ არა მხოლოდ აუცილებელი გადაწყვეტებისა , არამედ სრული და საკმარისი საერთო კონცეფციისა, რომლის ფარგლებშიც ნებისმიერი კონკრეტული გადაწყვეტა განისაზღვრებოდეს იქმნება როგორც კერძო შემთხვევა;

- გამოყენება რთული დიდი სისტემების და მათი ფუნქციონირების პროცესების მოდელირების უახლესი საშუალებების და მეთოდების.

აღნიშნული პრინციპების ინტერპრეტაცია ასს-ში და ორგანიზაციული მართვის ავტომატიზებული სისტემებში ინფორმაციის დაცვის პრობლემების გადაწყვეტასთან დაკავშირებით მოცემულია ნახაზი 2.

<table>
<tr><td></td><td>მიდგომის სისტემურობა</td><td></td><td>მიდგომის კონცეპტუალურობა</td></tr>
<tr><td rowspan="2">მიზნობრივი</td><td rowspan="2">1. ინფორმაციის ფიზიკური მთლიანობის უზრუნველყოფა;
2. ინფორმაციის ლოგიკური მთლიანობის უზრუნველყოფა;
3. ინფორმაციის არასანქცირებული მოდიფიკაციის თავიდან აცილება;
4. ინფორმაციის არასანქცირებული მიღების თავიდან აცილება;
5. ინფორმაციის არასანქცირებული გამრავლების თავიდან აცილება.</td><td rowspan="3">დაცვის უნიფიცირებული კონცეფციის დამუშავება</td><td>1. სისტემურობის ყველა ასპექტი გათვალისწინება</td></tr>
<tr><td>2. საჭირო დაცვის უზრუნველსაყოფად პირობების შექმნა</td></tr>
<tr><td>მასშტაბური</td><td>1. ინფორმაციის დაცვა ნებისმიერ მატერიალურ მატარებელში;
2. ინფორმაციის დაცვა ცალკე აღებულ მონაცემთა დამუშავების ავტომატიზებულ სისტემაში(მდას)
3. ინფორმაციის დაცვა რეგიონალურ, სახელმწიფო მდას-ებში.</td><td>3. რეალიზაციის შესაძლებლობების გათვალისწინება</td></tr>
<tr><td>3.მეთოდოლოგიური</td><td>1. საინფორმაციო ტექნოლოგიების, ასს-ების განვ-ის და გამოყენების კონცეფციების კომპლექსური გათვალისიწინება;
2. ინფორმაციის დაცვაზე გავლენის მქონე ყველა ფაქტორის კომპლექსური გათვალისწინება;
3. კომპლექსური დაცვის შესაძლებლობების კომპლექსური გათვალისი</td><td></td><td></td></tr>
<tr><td>4.დროითი</td><td>1. მიმდინარე დაცვის უზრუნველყოფა;
2. დაცვის უზრუნველყოფა დროის მოცემულ ინტერვალში;
3. ბაზისის ფორმირება პერსპექტივისათვის</td><td></td><td></td></tr>
</table>

ნახაზი 2. ინფორმაციის დაცვისადმი სისტემურ-კონცეფტუალური მიდგომის არსი.

უნდა გვახსოვდეს, რომ თანამედროვე ასს-ები მოქცეული არიან დიდი რაოდენობის მუქარების - რეალური საფრთხეების ზემოქმედების ქვეშ, აქ მხედველობაში გვაქვს ზოგადად ასს-ის წინააღმდეგ მიმართული ყველა სახის მუქარების სისტემური კლასიფიკაცია შეიძლება განხორციელდეს შემდეგი კრიტერიუმის მიხედვით:

- ინფორმაციის მდებარეობა ავტომატიზებული დამუშავების პროცესთან მიმართებაში: არის მუქარები, რომლებიც შეიძლება გამოჩნდნენ დამოუკიდებლად იმისა ხდება თუ არა მისი დამუშავება ასს-ში და არის ისეთი მუქარები, რომლებიც შეიძლება გამოჩნდნენ მხოლოდ უშუალოდ ინფორმაციის დამუშავების პროცესში;

- ინფორმაციაზე მადესტაბილიზებელი ზემოქმედების წყაროს პოზიცია ასს კომპონენტებთან მიმართებაში და მისი ურთიერთმოქმედება ამ კომპონენტებთან: წყარო შეიძლება იმყოფებოდეს ასს-ის კონტური (საზღვრებს) მიღმა ან მის ფარგლებში, თანაც ამ ბოლო შემთხვევაში მან შეიძლება არაფერი შეცვალოს ასს-ში, ან შემთხვევით ან ბოროტგანზრახულად შეიტანოს ესა თუ ის ცვლილებები ტექნიკურ საშუალებებში, დოკუმენტებში და ა.შ.

სარეჟიმო ობიექტების დაცვის სისტემის ფუნქციათა შესრულებისას (ფუნქციონირებისას) პოტენციურად შესაძლებელ სიტუაციათა თანმიმდევრობა და ანალიზი ნაჩვენებია ნახ.3 -ზე. თითოეული ჩამოთვლილი მოვლენის დასასრულზე დამოკიდებულებით შეიძლება მივიღოთ სხვადსხვა ჯამური მოვლენები. მოვლენა N1 შეიძლება ინტერპრეტირებულ იქნას როგორც ინფორმაციის მოთხოვნილი დონის დაცვის უზურუნველყოფა, N2 - როგორც დაცვის გარღვევა, ხოლო N3 მოვლენა აღნიშნავს საბოლოო შედეგს - დაცვის სისტემა მოშლილია.

სარეჟიმო ობიექტების (ინფორმაციის) დაცვის სისტემის ექსპერტისათვის მოსახერხებელია დაცვის ფუნქციათა შესრულების საერთო მოდელი წარმოვადგინოთ ნახ.4 -ზე ნაჩვენები სახით. 4, 6 და 7 ნომრით აღნიშნულ დაცვის უზურნველყოფის ფუნქციებს გააჩნიათ ორი მოდიფიკაცია, რომლებიც დაკავშირებული აღმოჩენილი და აღმოუჩენელი მუქარების ზემოქმედებათა აცილებისა და მათი ზემოქმედების შედეგების ლიკვიდაციასთან. დიაგრამის მარჯვენა ნაწილში მოყვანილია ფუნქციათა შესრულების შესაძლო ათი საბოლოო შედეგი, რომლებიც ქმნიან

არათავსებად ხდომილებათა ჯგუფს. თუ i -ური საბოლოო შედეგის ალბათობა იქნება P_i , მაშინ

$$\sum_{i=1}^{10} \mathrm{Pi} = 1$$

ხოლო პირველიდან მეექვსის ჩათვლით საბოლოო შედეგების ალბათობათა ჯამი გამოსახავს ინფორმაციის დაცულობას

$P_{\text{დაც}} = \sum_{i=1}^{6} \mathrm{Pi} = 1$

თავის მხრივ, ალბათობები შეიძლება შეფასდეს შემდეგი გამოსახულების მეშვეობით

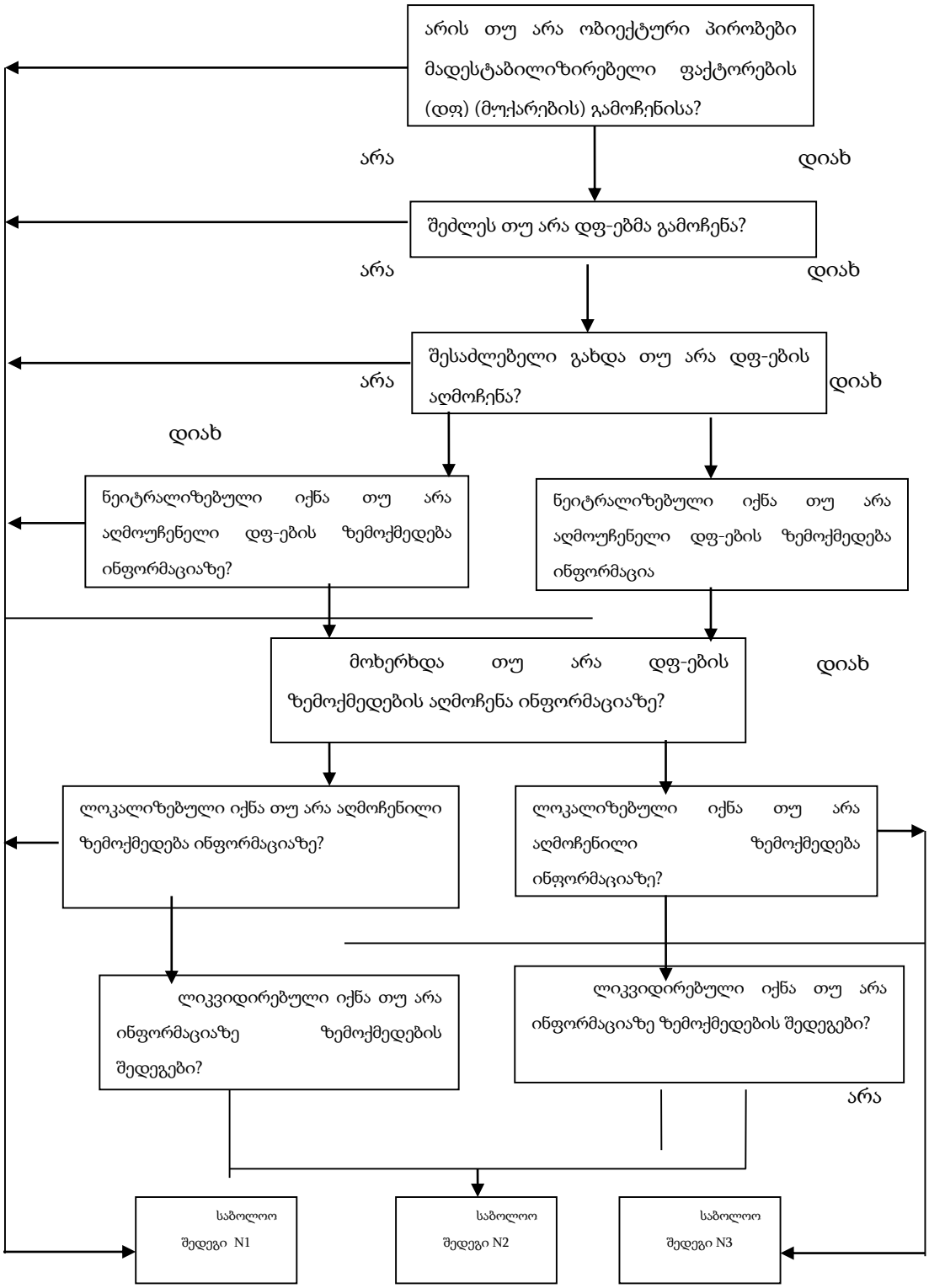
$\mathrm{Pi} = \mathrm{F}\left(\left\{P_r^f\right\}\right), \mathrm{r} = \overline{1,7}$

სადაც, P_r^f - არის მე- r დაცვის ფუნქციის წარმატებით განხორციელების ალბათობა.

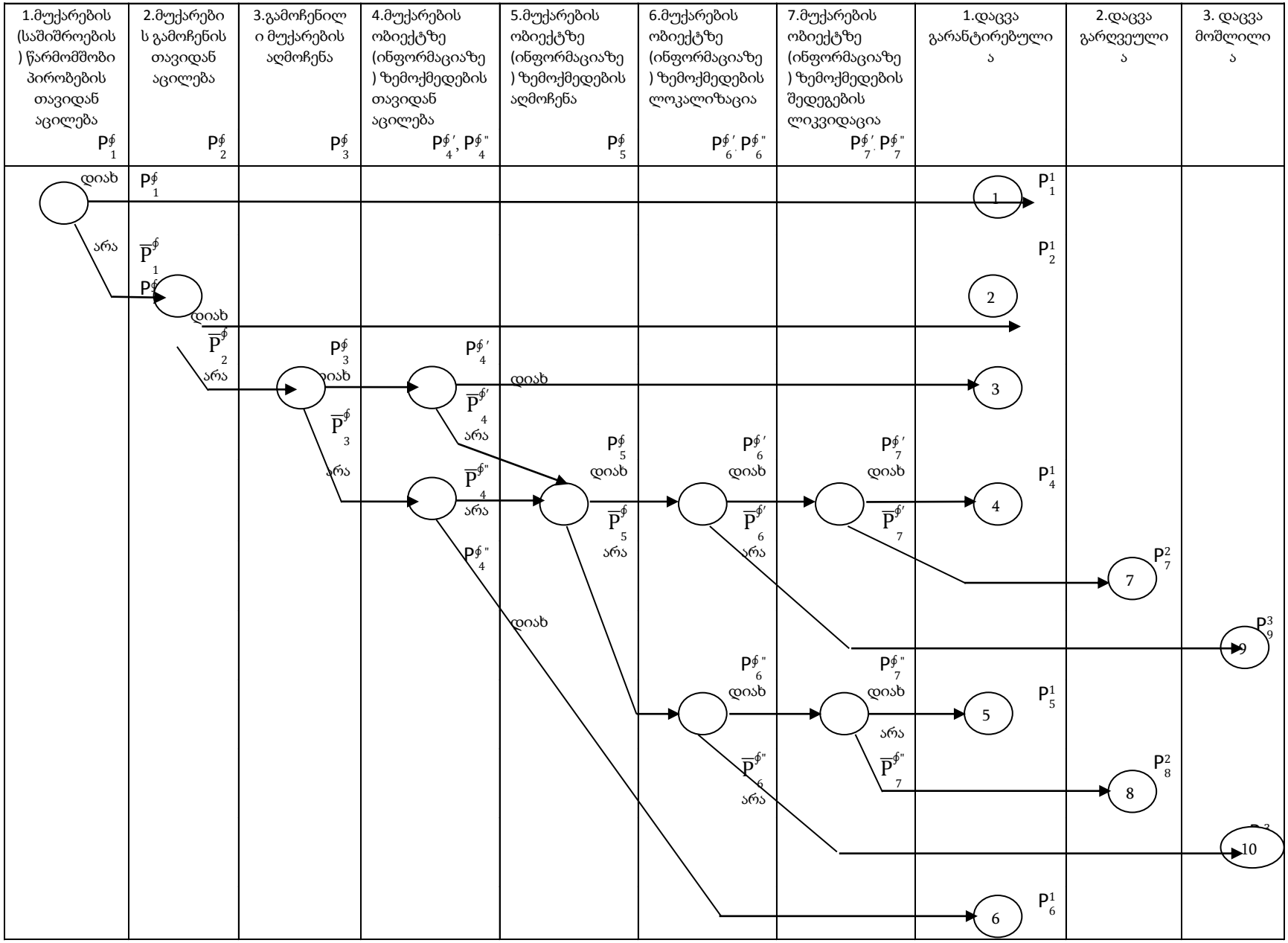
თუ მოცემულია ინფორმაციის დაცულობის უზურნველყოფის ალბათობების მნიშვნელობა $P_{\text{მოც}}$, მაშინ გარანტირებული დაცვის სტრატეგიას ექნება სახე:

$P_{\text{დაც}} = \sum_{i=1}^{6} \mathrm{Pi} > P_{\text{მოც}}$

ამრიგად, სარეჟიმო დაცვის ობიექტის რეალური დაცულობა, დაცვის სისტემის დანერგვის შემდეგ მეტი ან ტოლი უნდა იყოს დაცულობის მოცემულ $P_{\text{მოც}}$ მნიშვნელობაზე.



ნახაზი 3.. ინფორმაციის დაცვის პროცესში პოტენციურად შესაძლო სიტუაციების თანმიმდევრობა და ანალიზის შინაარსი.



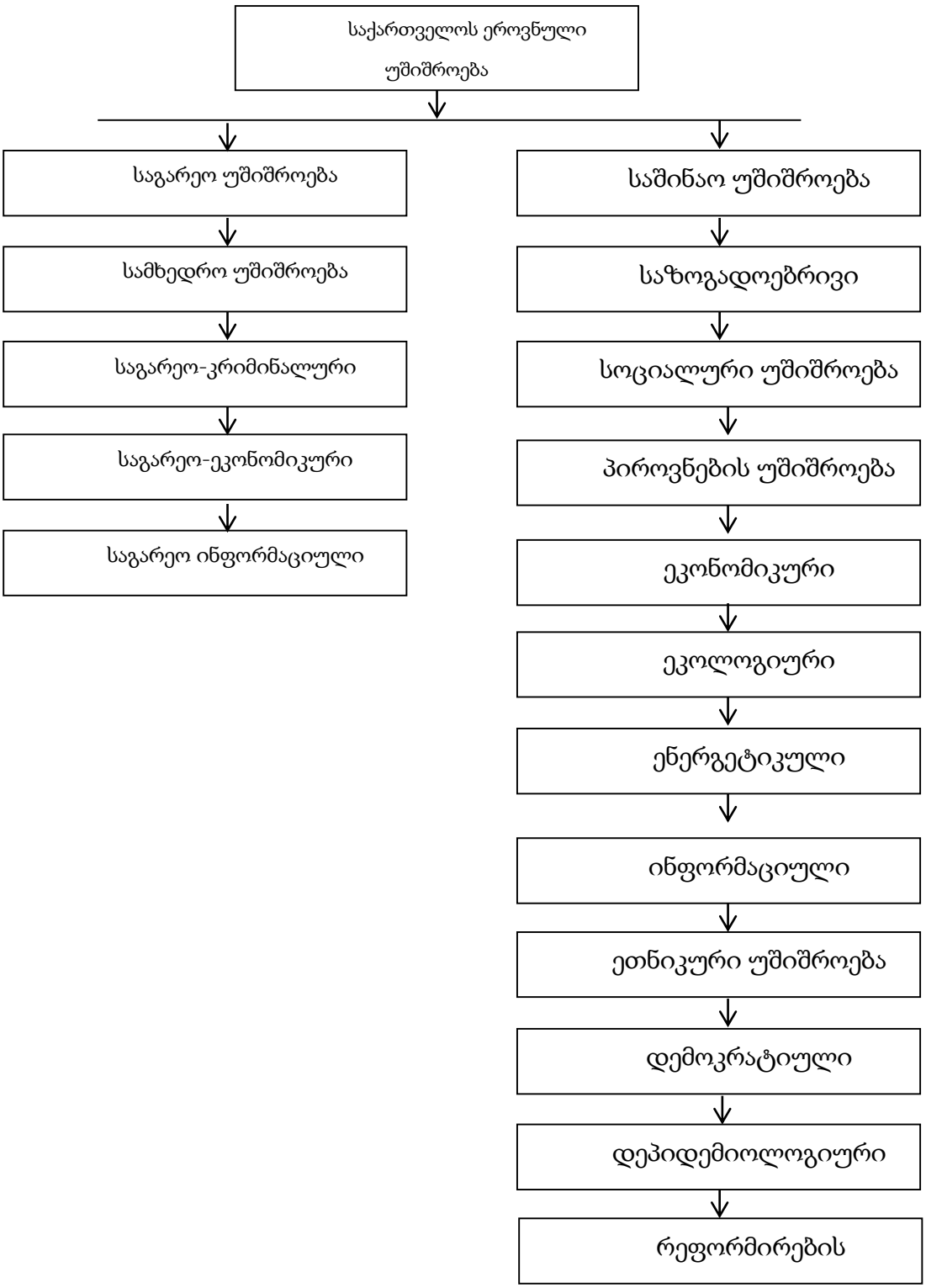
ნახ. 4.5. ინფორმაციის დაცვის უზრუნველყოფის ფუნქციების განხორციელებისას საბოლოო შედეგების ზოგადი მოდელი

3.3. სიტუაციური მიდგომის გამოყენება თანამედროვე სახელმწიფოს ინფრასტრუქტურის იუ-ს უზრუნველყოფასა და მდგრად განვითარებაში.

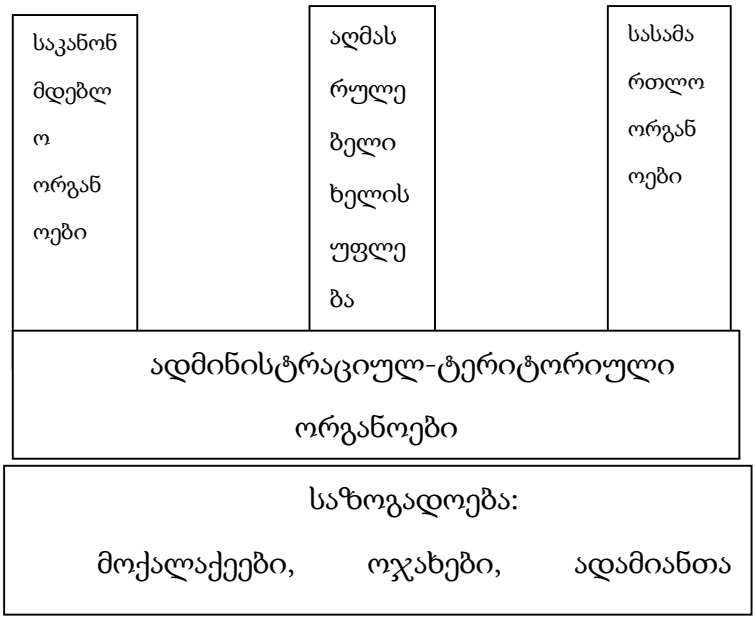
ქვეყანაში არსებული მდგომარეობის სიტუაციური ანალიზისთვის აუცილებელია ერთიანი ინფორმაციული სივრცის არსებობა, რომელმაც უნდა უზრუნველყოს წინასწარ განსაზღვრული პარამეტრების მიხედვით მონაცემების დაგროვება შემდეგი მიმართულებით: 1)დემოგრაფიული; 2)სოციალური; 3)პოლიტიკური; 4)ეკონომიკური; 5)სამეცნიერო–ტექნიკური; 6)ენერგეტიკული; 7)ეკოლოგიური; 8)კულტურა; 9)საინფორმაციო უზრუნველყოფის; 10)სამართალი. ცალკე უნდა იყოს გამოყოფილი ქვეყანაში განსაკუთრებით მნიშვნელოვანი ობიექტების მდგომარეობის კონტროლისა და უსაფრთხოების უზრუნველყოფის სისტემა, რომელსაც ექნება დადგენილი ინფორმაციული კავშირი ქვეყნის ერთიანი ინფორმაციულ სივრცესთან.

საერთო ინფორმაციული სივრცის (სის) შექმნისას, პირველ რიგში მკაფიოდ უნდა იქნას განსაზღვრული აღნიშნული ყოველი სფეროსთვის ინფორმაციის წყარო ან წყაროები. ყოველი წყარო უნდა იყოს შეფასებული საიმედოობის შემდეგი სკალის გამოყენებით: ა) სრული საიმედო; ბ)ჩვეულებრივ საიმედო; გ)საკამაოდ საიმედო; დ) არაყოველთვის საიმედო; ე) არასაიმედო; ვ)საიმედოობის შეფასება შეუძლებელია. ამასთან ერთად აუცილებელია სის ფასობდეს ის თუ რამდენად შეესაბამება შინაარსობრივად წყაროდან მიღებული ინფორმაცია წინასწარ დადგენილ მოთხოვნებს, მისი უტყუარობა, საამისოდ კი შემოგვაქვს შემდეგი სკალა წყაროდან მიღებული ინფორმაციის შინაარსის შეფასებისა: ა) დადასტურებულია სხვა საშუალებებითაც; ბ) სავსებით შესაძლებელია, რომ შეესაბამება სინამდვილეს; გ) შეიძლება , რომ შეესაბამება სინამდვილეს; დ) საეჭვოა; ე) შეფასება შეუძლებელია; ვ) უტყუარობის შემოწმება შეუძლებელია.

იმისათვის, რომ წარმოვადგინოთ ქვეყნის ერთიანი ინფორმაციული სივრცის ზოგადი მოდელი ვისარგებლებთ ქვეყნის, როგორც ურთულესი თვითგანვითარებადი სისტემის გამარტივებული სტრუქტურული სქემებით: 1) სახელმწიფო ღია სისტემა, ერთობა ხელისუფლების, მოქალაქეების, ადამიანთა ერთობების და ბუნების; 2) სახელმწიფოს კონსტრუქციულად განსაზღვრული ზოგადი სტრუქტურა.



ნახაზი. 5. სახელმწიფოს კონსტიტუციურად განსაზღვრული სტრუქტურა.



ნახაზი 6. ქვეყანა

ქვეყანაში ფართომასშტაბიანი ერთიანი ინფორმაციული სივრცის შექმნა აუცილებელია იმისათვის, რომ დაინერგოს სახელმწიფოს სიტუაციური მართვის სისტემა. ამის აუცილებლობაზე მიგვანიშნებს მსოფლიოში დღეს არსებული პირობები, გარეშე შემშფოთი ზემოქმედებები, რომელთა გავრცელებაც საყოველთაოდ ხელმისაწვდომი გლობალური საინფორმაციო ინტერნეტ სისტემის მეშვეობით, ფაქტიურად არავითარ პრობლემას არ წარმოადგენს. სახელმწიფომ რომ შეძლოს არსებობა და მდგრადი განვითარება მან ძალიან კარგად უნდა იცოდეს საერთო სისტემური კანონები და კანონზომიერებები, ვინაიდან მათმა იგნორირებამ შეიძლება გამოიწვიოს სახელმწიფოს არამდგრადობა, კატასტროფები, დაშლა ან დანგრევა. პირიქით, გეგმაზომიერი და სისტემური გათვალისწინება კანონზომიერებების საშუალებას იძლევა უზრუნველყოფილ იქნას, ზოგადად, ტექნიკური, ეკონომიკური, სოციალური და ორგანიზაციული სისტემების მაქსიმალური მდგრადობა. აღნიშნულის ერთ–ერთ დამადასტურებელ მაგალითად შეიძლება დავასახელოთ „კანონზომიერება სისტემის პოტენციალის დამოკიდებულება მისი სტრუქტურული ელემენტების ურთიერთქმედების ხასიათზე ან სისტემის ორგანიზებულობის ხარისხზე“(1) რომლის თანახმადაც, თუ ორგანიზებულ სისტემაში A პოტენციალი P მრავალჯერ აღემატება ყველა

შემდგენელი ელემენტების (ქვესისსტემების, სახლემწიფოს შემდგენელი ელემენტების) პოტენციალების ჯამს.

$P(A) > [P(a_1)+P(a)+\ldots+P(a_n)]$,

ცუდად ორგანიზებულ სისტემაში, როდესაც ელემენტების ურთიერთქმედებას აქვს ანტაგონისტური ხასიათი და როდესაც სისტემის თითოეული ელემენტი მოქმედებს წინააღმდეგობრივად ყველა დანარჩენისა, მაშინ სისტემის პოტენციალი ნაკლებია ნებისმიერი ყველაზე სუსტი ელემენტის პოტენციალისა

$P(A) < \min [P(al); P(a2);\ldots; P(an)]$.

აღნიშნულიდან გამომდინარეობს ის, რომ დამოუკიდებელ სახელმწიფოში, როგორც სისტემაში, თუ ეკონომიკის, მეცნიერების, განათლების და .შ. ორგანიზაციის დონე.

სახელმწიფო ორგანოების პირველმა პირებმა შეუძლებელია შეძლონ გადაწყვეტილებათა მიღებისას გაითვალისწინონ როგორც სისტემური კანონზომიერებები, ასევე არსებული სიტუაციები სახელმწიფოს საარსებო სფეროებში იქნება ეს ეკონომიკა, პოლიტიკური მდგომარეობა, თუ ეკოლოგიური მდგომარეობა, შიდა და გარე საფრთხეები, მიმართული სახელმწიფოს მდგრადი განვითარების და მისი არსებობის წინააღმდეგაც კი.

განვითარებულ ქვეყნებში აღიარებულია სიტუაციური მიდგომის აუცილებლობა და შექმნილია სიტუაციური ცენტრები, რომელთა მთავარი დანიშნულებაა სახელმწიფოს ცალკეულ სფეროებში სიტუაციების გაანალიზება, მოვლენების პროგნოზირება და შესაძლო გადაწყვეტილებების ან გადაწყვეტილებათა ვარიანტების წარდგენა გადაწყვეტილების მიმღები პირისათვის (გმპ).

ისეთმა განვითარებულმა ქვეყნებმა, როგორიც საქართველოა, განსაკუთრებული ყურადღება უნდა დაუთმოთ სახელმწიფოს მართვაში მსოფლიო გამოცდილების შესწავლას და ინოვაციური მიდგომების გამოყენებას. საამისოდ კი აუცილებელია სახელმწიფომ შექმნას ხელსაყრელი კლიმატი შემდეგი სამი ძირითადი ამოცანის გადაწყვეტის მეშვეობით:

- სტიმულების და პირობების შექმნის ინოვაციური პროექტების მხარდასაჭერად;

- აღმოფხვრა ბიუროკრატიული, კონკრეტული და სხვა დაბრკოლებებისა ინოვაციათა განვითარებისათვის;

- ინოვაციური ბაზის და მათი გამოყენების მეთოდების სრულყოფა თანამედროვე ტექნოლოგიების და სამეცნიერო–კვლევითი და საცდელ საკონსტრუქციო სამუშაოების სფეროებში სწავლების განსავითარებლად.

სახელმწიფოს მართვაში სიტუაციური მიდგომის დანერგვა მოითხოვს მძლავრი სამეცნიერო–ინტელექტუალურ, ტელესაკომუნიკაციო და ეკონომიკურ რესურსებს. ამაზე მიგვითითებს თუნადაც ის, რომ სიტუაციური ცენტრის კომპლექსში, რომელიც წარმოადგენს გმპ ნდობით არჭურვილ მხარდამჭერ სისტემას, უნდა იყოს შემდეგი შესაძლებლობები:

- ერთიანი ინფორმაციული სივრცის მაორგანიზებელი კომუნიკაციების თანამედროვე საშუალებების ინტეგრაცია, რომლის მეშვეობითაც მიიღება ყველა ინფორმაცია გადაწყვეტილების მიღებისათვის;

- რეგიონალური სიტუაციათა მონაცემთა ბაზრების სიმრავლე, (რმბი) – მიმდინარე და გაზომილი მონაცემები და მათი მართვის სისტემები (მბმსი);

- სიტუაციათა შეფასების მოდელების ბაზა (მდმჯ) და მათი მართვის სისტემები (მდბმსჯ);

- იმიტაციური მოდელირების შედეგების ბაზა(იმბჯ) და მათი მართვის სისტემები (იმბმსჯ);

- ანალიტიკური სიტუაციური სისტემები, გადაწყვეტილებათა მიღების და მმართველობითი გადაწყვეტილებების ალგორითმების ბაზა (გმმგბჯ) და მათი მართვის სისტემები (გმმგმსჯ);

- ინტერფეისი ჩამოთვლილი სისტემებსა და ექსპერტ–ანალიტიკოსებს, გმპ შორის;

- კოლექტიური მოხმარების ინფორმაციის წარმოდგენა ნებისმიერ ფორმატში;

- ვიდეოკონფერენციების უზურნველყოფა, რომლის საშუალებითაც შესაძლებელი იქნება სახელმწიფოს მართვის ნებისმიერი დონის ხელმძღვანელების და ხელმძღვანელთა ჯგუფების კონფიდენციალური თათბირების გამართვა;

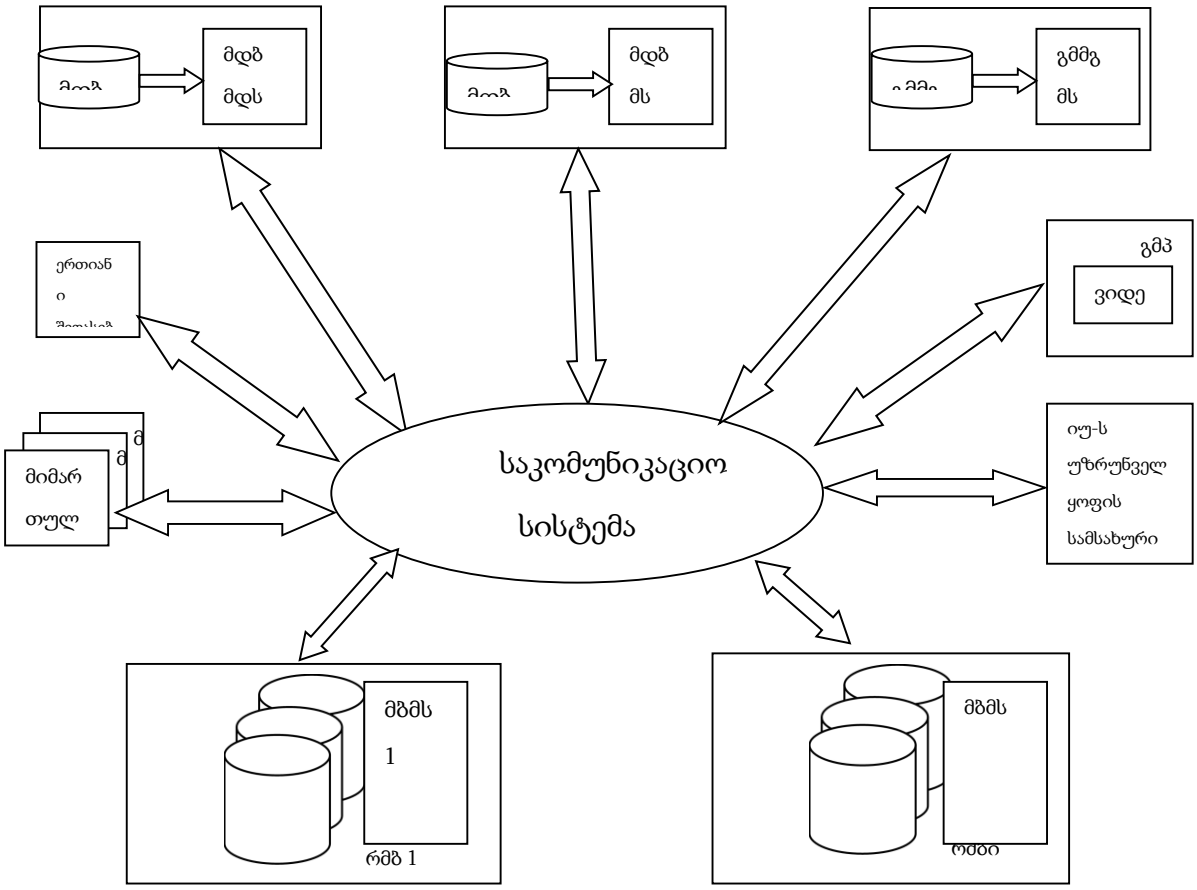
- სიტუაციური მართვის სისტემის ინფორმაციული უსაფრთხოების (იუ) უმაღლეს დონეზე უზრუნველყოფა.

ძალზე გამარტივებული სქემატური მოდელი ქვეყნის სიტუაციური მართვის სისტემისა (ნახ.6.) წარმოადგენს ერთობლიობას ერთიანი ინფორმაციული სივრცის და სიტუაციური ცენტრისა, რომელშიც ჩართული არიან ექსპერტ-ანალიტიკოსთა ჯგუფები მიმართულებების მიხედვით და

ერთიანი შეფასების ცენტრი, აქვე ნაჩვენებია გმპ ჯგუფების დიალოგი სისტემაში.

წარმოდგენილი სისტემის ფუნქციონირებისას დიდი მნიშვნელობა ენიჭება მისი ინფორმაციული უსაფრთხოების უზრუნველყოფას, გარანტირებული უნდა იყოს საჭირო

მონაცემების უტყუარობა, ხელმისაწვდომობა და კონფიდენციალობა. ამიტომ, სახელმწიფომ, ვინაიდან მსგავსი სისტემის სწორად, დაუმახინჯებლად და ოპერატიულად ფუნქციონირებას სასიცოცხლო მნიშვნელობა ეკისრება ქვეყნის მდგრადი განვითარების უზრუნველყოფის თვალსაზრისით, უნდა მოახერხოს მთელი საკომუნიკაციო სისტემა ააგოს ინტერნეტ ტექნოლოგიაზე, იყოს ის მთლიანად სახელმწიფოს განკარგულებაში და მისი უსაფრთხოების უზრუნველსაყოფის სამსახური, რომელიც იზრუნებს ინფორმაციის წყაროებთან სანდო კავშირების დამყარებაზე და მთელი სისტემის უსაფრთხოებაზე.



ნახაზი. 7 სიტუაციური მართვის სისტემა - ერთიანი ინფორმაციული სივრცე

დღეისთვის ქვეყნის ერთ–ერთ მნიშვნელოვან პრიორიტეტულ მიმართულებას წარმოადგენს სახელმწიფო ხელისუფლების განხორციელებისას ელექტრონული მმართველობის პრინციპებზე დაფუძნებული ერთიანი სისტემის შექმნა, ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავება და მისი განხორციელების ხელშეწყობა. ელექტრონული სერვისები წარმოადგენს სახელმწიფოს მიერ განხორციელებული მომსახურების ყველაზე უფრო იაფ, მოსახერხებელ და სწრაფ მომსახურებას. ელექტრონული მომსახურების განვითარებასთან ერთად კრიტიკულ მნიშვნელობას იძენს ინფორმაციული უსაფრთხოების საკითხები, რაც სახელმწიფო უშიშროების საკითხებს განეკუთვნება.

ეროვნული უშიშროება კონკრეტული გამოხატულებაა ეროვნული მიზნებისა და გულისხმობს სახელმწიფოს განვითარების უზრუნველყოფას, როგორც გარეშე, ისე შიდა საფრთხეების პირობებში.

ტერმინი „ეროვნული უსაფრთხოების სისტემა“ გულისხმობს ნებისმიერ საინფორმაციო სისტემას (მათ შორის სატელეკომუნკაციო სისტემებსაც), რომლებიც გამოიყენება ან ოპერირებს სააგენტოს მიერ ან სააგენტოს ნებისმიერი კონტრაქტორის მიერ ან სხვა ორგანიზაციის მიერ, რომელიც მოქმედებს სააგენტოს სახელით; რომლის ფუნქცია, ოპერირება ან გამოყენება:

- მოიცავს დაზვერვის საქმიანობას;

- მოიცავს ეროვნულ უსაფრთხოებასთან დაკავშირებულ კრიპტოლოგიურ საქმიანობებს;

- მოიცავს სამშვიდობო ძალების კონტროლს და მართვას;

- მოიცავს იმ აღჭურვილობას, რომელიც იარაღის ან შეიარაღებული სისტემის შემადგენელი ნაწილია ან ქვეპარაგრაფში წარმოდგენილი საკითხი მნიშვნელოვანია სამშვიდობო და სადაზვერვო მისიების პირდაპირ დასაკმაყოფილებლად; ან

დაცულია ნებისმიერ დროს იმ პროცედურების საფუძველზე, რომლებიც დაწესებულია იმ ინფორმაციისათვის, რომლებიც სპეციალურად იქნა ავტორიზირებული აღმასრულებელი ბრძანების ან კონგრესის აქტის საფუძველზე დადგენილი კრიტერიუმის საფუძველზე, რათა კლასიფიცირებულად იქნას შენარჩუნებული ეროვნული თავდაცვის ან საგარეო პოლიტიკის ინტერესებში.

ქვეპარაგრაფი (A)(i)(V) არ მოიცავს ისეთ სისტემებს, რომლებიც უნდა იქნას გამოყენებული რუტინული ადმინისტრაციული და ბიზნეს საქმიანობებისათვის (მათ შორის დაქირავებული პერსონალის ხარჯები, ფინანსები, ლოჯისტიკა და პერსონალის მართვის აპლიკაციები).“

სისტემები, რომლებიც ყველა ჩამოთვლილი კრიტერიუმიდან თუნდაც ერთს არ აკმაყოფილებენ არ წარმოადგენენ ეროვნული უსაფრთხოების სისტემებს.

როგორც წარმომადგენლობითი კომიტეტის ანგარიშში არის განმარტებული ეროვნული უსაფრთხოების სისტემის FISMA-სეული განმარტება „ერგება სამშვიდობო და სადაზვერვო მისიების საკმაოდ სტაჟიან დაკანონებულ მიდგომას - დაკავშირებული სისტემები და კლასიფიცირებული სისტემები“. პალატის ანგარიში აერთიანებს ეროვნული უსაფრთხოების სისტემის განმარტების „ვარნერის ცვლილებას“. უშიშროების უზრუნველყოფის ძირითად პრინციპებად უნდა მივიჩნიოთ: პიროვნების და სახელმწიფოს სასიცოცხლოდ მნიშვნელოვანი ინტერესების ბალანსის დაცვა; უშიშროების უზრუნველყოფაში პიროვნების, საზოგადოების და სახელმწიფოს ურთიერთპასუხისმგებლობა; საერთაშორისო უსაფრთხოების სისტემებთან ინტეგრაცია.

იდეალურ შემთხვევაში ეროვნული უსაფრთხოების სისტემის კლასიფიცირება მისი სიცოცხლის, რაც შეიძლება ადრეულ სტადიაზე უნდა მოხდეს. სერტიფიცირების, სტანდარტების აკრედიტაციის, რეგულირების, პროცედურების, გაიდლაინების და ინსტრუქციების მთელი სისტემა, რომლებიც ვრცელდება თითოეულ სისტემაზე დამოკიდებულია იმაზე, არის თუ არა სისტემა ეროვნული უსაფრთხოების სისტემის სტატუსის მქონე. იმ სისტემებისათვის, რომლებიც მოცემული მომენტისათვის აქტიურ მდოგმარეობაში არიან, და რომლებსაც არ აქვთ მინიჭებული ეროვნული უსაფრთხოების სისტემის სტატუსი, სავალდებულოა მათთვის ამ სტატუსის მინიჭება მოხდეს რაც შეიძლება მალე.

ქვეყანაში ეროვნული უშიშროების სისტემის შექმნის მიზანია უზრუნველყოფილი იქნას ყველა სახის საფრთხეებისაგან, მუქარებისაგან თავდაცვა, რაც მიიღწევა ეროვნული უშიშროების სტრატეგიისადმი ინტეგრალური მიდგომით:

1. ქვეყნის ეროვნული ინტერესების წინააღმდეგ მიმართული საფრთხეების, მუქარების ნეიტრალიზების გარკვეული ხელშეწყობი საერთაშორისო ვითარების ფორმირება;

2. საფრთხეების, მუქარების წინააღმდეგ ბრძოლის, მოსპობის ან ნეიტრალიზების შესაძლებლობის მხარდაჭერა;

3. დროული მომზადება მომავალში გაუთვალისწინებელ მოვლენებთან შესახვედრად.

სახელმწიფოს ეროვნული უშიშროების სისტემის მთავარ ელემენტებს უნდა წარმოადგენდეს სხვადასხვა დონის სიტუაციური (ანალიტიკური) ცენტრები, რომლის ძირითადი ამოცანებია ოპერატიული და სხვა ინფორმაციის სიღრმისეულის ანალიტიკური დანუშავების საფუძველზე ხელი შეუწყონ სახელმწიფოს მართვის, მათ შორის ქვეყნის უშიშროების უზრუნველყოფისას სტრატეგიულ და ოპერატიული გადწყვეტილებების მიღებისას.

ეროვნული უსაფრთხოების სისტემის იდენტიფიცირებისათვის საჭირო საკონტროლო კითხვარის შევსების მიზნით „კრიპტოლოგიური ქმედებები“ მოიცავს სიგნალების სადაზვერვო ქმედებებს, რომელიც შედის სადაზვერვო ქმედებების ფარგლებში და გადაწყვეტილებებს, პროდუქციას და სერვისებს, რომლებიც უზრუნველყოფენ ეროვნული უსაფრთხოების ტელეკომუნიკაციებისა და საინფორმაციო სისტემების ხელმისაწვდომობას, მთლიანობას, იდენტიფიკაციას, კონფიდენციალურობას და არა უწყვეტობას.

ინფორმაციული უსაფრთხოება მნიშვნელოვანია როგორც საჯარო, ასევე კერძო სექტორის საქმიანობისთის, აგრეთვე კრიტიკული ინფრასტრუქტურის დაცვისათვის. ინფორმაციული უსაფრთხოება ორივე სექტორში შუამავლის ფუნქციას ასრულებს, მაგალითად, ის გამოიყენება ელექტრონული მმართველობის, ან ელექტრონული ბიზნესის (საქამისწარმოების) მიზნების მისაღწევად, ასევე ამ პროცესებთან დაკავშირებული რისკების შესამცირებლად ან თავიდან ასარიდებლად. საჯარო და კერძო ქსელების ურთიერთდაკავშირება და ინფორმაციული რესურსების გაზიარება ართულებს წვდომის კონტროლის მექანიზმების დანერგვასა და მისი მიზნების მიღწევას. მონაცემების განაწილებულმა დამუშავებამ ასევე შეასუსტა კონტროლის ძირითადი მექანიზმები.

მნიშვნელოვანია, რომ ორგანიზაციამ გამოავლინოს უსაფრთხოების საკუთარი მოთხოვნები. არსებობს უსაფრთხოების მოთხოვნების სამი ძირითადი წყარო:

1. პირველი წყარო არის ორგანიზაციისთვის რისკების შეფასება, რაც ასევე ითვალისწინებს ორგანიზაციის ბიზნესის სტრატეგიას და მიზნებს. რისკების შეფასების მეშვეობით გამოვლენილია საფრთხეები, რომლებიც ემუქრება აქტივებს, შეფასებულია სისუსტეები, მათი ხდომილების ალბათობა და მათი პოტენციური გავლენა.

2. მეორე წყარო არის იურიდიულად დადგენილი, მარეგულირებელი და სახელშეკრულებო მოთხოვნები, რომლებიც ორგანიზაციამ, მისმა სავაჭრო პარტნიორმა, კონტრაქტორებმა და მომსახურების მომწოდებლებმა უნდა დააკმაყოფილონ, აგრეთვე გასათვალისწინებელია სოციალურ-კულტურული გარემო.

3. მესამე წყარო წარმოადგენს პრინციპების, მიზნებისა და ბიზნესის (საქმისწარმოების) მოთხოვნების ნაკრებს, რომელიც შემუშავებულია ორგანიზაციაში ოპერაციების მხარდამჭერი ინფორმაციის დამუშავებისთვის.

ქვეყნის ინფორმაციული ინფრასტრუქტურის მუდმივი და სწრაფი განვითარების პირობებში, სახელმწიფო მმართველობის პროცესები სულ უფრო მეტად ხდება დამოკიდებული საინფორმაციო სისტემებზე.

რუსეთ - საქართველოს ომის დროს, რუსეთის ფედერაციამ საქართველოს წინააღმდეგ სახმელეთო, საჰაერო და საზღვაო შეტევების პარალელურად, განახორციელა მიზანმიმართული და მასირებული კიბერშეტევები. აღნიშნულმა კიბერშეტევებმა აჩვენა, რომ კიბერსივრცის დაცვა ეროვნული უსაფრთხოებისთვის ისევე მნიშვნელოვანია, როგორც სახმელეთო, საზღვაო და საჰაერო სივრცეების დაცვა". ეს კიბერშეტევა ბევრი საერთაშორისო ექსპერტის მიერ შეფასდა როგორც „ინფორმაციული/კიბერ ომი" საქართველოს წინააღმდეგ, რასაც ქვეყანა მოუმზადებელი შეხვდა, არ არსებობდა საჭირო რესურსები, გამოცდილება და შესაბამისად საქართველომ კიბერშეტევის მოგერიება ვერ შეძლო. შედეგად ქვეყანა აღმოჩნდა სერიოზული საერთაშორისო ინფორმაციული ვაკუუმის წინაშე. პრობლემა გადაიჭრა ქვეყნის უცხოელი სტრატეგიული პარტნიორების, ჩარევის შემდეგ, რის შედეგადაც შეჩერებული და თავიდან აცილებული იქნა მთლიანი ინფრასტრუქტურის განადგურება.

„საქართველოს საკონსტიტუციო სასამართლომ 2008 წლის 30 ოქტომბრის გადაწყვეტილებით მოახდინა საჯარო ინფორმაციის რამდენიმე კატეგორიად დაყოფა: ა) ინფორმაცია, რომელიც საჯარო ინფორმაციის მიღების მსურველ პირს შეეხება; ბ) ინფორმაცია, რომელის შეიცავს სახელმწიფო, კომერციულ ან პროფესიულ საიდუმლოებას; გ) ინფორმაცია, რომელიც საჯარო ინფორმაციის მიღების მსურველს არ შეეხება, დ) ინფორმაცია, რომელიც კერძო პირის კერძო საკითხებს შეეხება. ზემოთ ჩამოთვლილ განსაზღვრებათა რიცხვს ემატება კიდევ ოთხი: კონფიდენციალური, შეზღუდული, არაკლასიფიცირებული და ღია ინფორმაცია“.[27]

ძირითადად ინფორმაცია მიიღება, ინახება, მუშავდება და გადაიცემა ინტენსიურ-ტექნოლოგიური საინფორმაციო სისტემების საშუალებით, როგორებიცაა: პერსონალური და სუპერ კომპიუტერები, მობილური მოწყობილობები, სატელეკომუნიკაციო სისტემები და სხვა. ორგანიზაციები პირდაპირ დამოკიდებულნი არიან აღნიშნულ ტექნოლოგიებზე, რომლებიც უზრუნველყოფენ ბიზნეს ფუნქციისა და მისიის წარმატებით განხორციელებას.

ინფორმაციულ სისტემებზე ზეგავლენას ახდენს სხვადასხვა ტიპის სერიოზული საფრთხე, რომლებმაც შეიძლება უარყოფითი ზეგავლენა მოახდინონ ორგანიზაციის საოპერაციო გარემოზე, ორგანიზაციის აქტივებსა თუ ინდივიდებზე სხვადასხვა ფართოდ გავრცელებული სისუსტეების გამოყენებით, რომლებიც არღვევენ აღნიშნულ ინფორმაციულ სისტემებში მიღებული, შენახული, დამუშავებული თუ გადაცემული ინფორმაციის კონფიდენციალურობას, მთლიანობასა თუ ხელმისაწვდომობას. ინფორმაციული სისტემების საფრთხეებს მიეკუთვნება: მიზანმიმართული შეტევები, გარემოსდაცვითი ხასიათის დარღვევები, ადამიანური / მანქანური შეცდომები და სხვა, რომლებიც საბოლოოდ დიდ ან საერთოდ გამოუსწორებელ ზიანს აყენებენ ორგანიზაციას.

რისკების მართვა წარმოადგენს პროცესს, რომლის დროსაც ერთად სხდებიან ორგანიზაციის მთავარი წევრები და აანალიზებენ ყველა იმ რისკს, რომელიც არსებობს ორგანიზაციაში. აღნიშნულ რისკებში განიხილება როგორც კრიტიკული, ასევე უმნიშვნელო რისკები: დაწყებული ხანძრიდან, დამთავრებული ბუნებრივ კატასტროფამდე.

იმისათვის, რომ წარმატებულად მოხერხდეს ორგანიზაციაში არსებული უსაფრთხოების რისკების მართვა, აუცილებელია ორგანიზაციის ლიდერებმა / აღმასრულებლებმა გაითავისონ და გახადონ რისკების მართვის პროცესი ორგანიზაციის მისიის / ბიზნეს გარემოს შემადგენელი ნაწილი. სწორედ ეს ზედა დონის მმართველობითი ორგანოები / აღმასრულებლები უზრუნველყოფენ რისკების მმართველობის პროცესისთვის საჭირო რესურსების გამოყოფას.

ინფორმაციული უსაფრთხოების რისკების მართვა უნდა იყოს უწყვეტი პროცესი. პროცესმა უნდა დაადგინოს ორგანიზაციული გარემო, შეაფასოს რისკები და გადაჭრას რისკები რისკებთან მოპყრობის გეგმის მიხედვით რეკომენდაციების და გადაწყვეტილებების დასანერგად. რისკების დასაშვებ დონეზე დაყვანისათვის რისკების მართვა აანალიზებს რეაგირების არქონის შემთხვევაში შესაძლო უარყოფით მოვლენებს და განსაზღვრავს სამოქმედო გეგმას.

ინფორმაციული უსაფრთხოების რისკების მართვამ ხელი უნდა შეუწყოს:

1. რისკების იდენტიფიცირებას;
2. ამ რისკების დადგომის ალბათობას და მათ შესაძლო შედეგებს, მათ შესახებ ინფორმირებულობის არსებობას;
3. რისკებთან მოპყრობის პრიორიტეტულობის დადგენას;
4. რისკების შემცირების შესახებ ქმედებების პრიორიტეტულობას;
5. რისკების მართვასთან დაკავშირებული გადაწყვეტილებების მიღებაში ჩართული დაინტერესებული პირები და მათი ინფორმირებულობა რისკების მართვის სტატუსის შესახებ;
6. რისკებისა და რისკების მართვის პროცესის რეგულარულ მონიტორინგსა და განხილვას;
7. რისკების მართვისადმი მიდგომის გაუმჯობესების მიზნით საჭირო ინფორმაციის შეგროვებას;
8. მენეჯერებისა და თანამშრომლების ინფორმირებულობას რისკებისა და მათი შემცირების შესახებ.

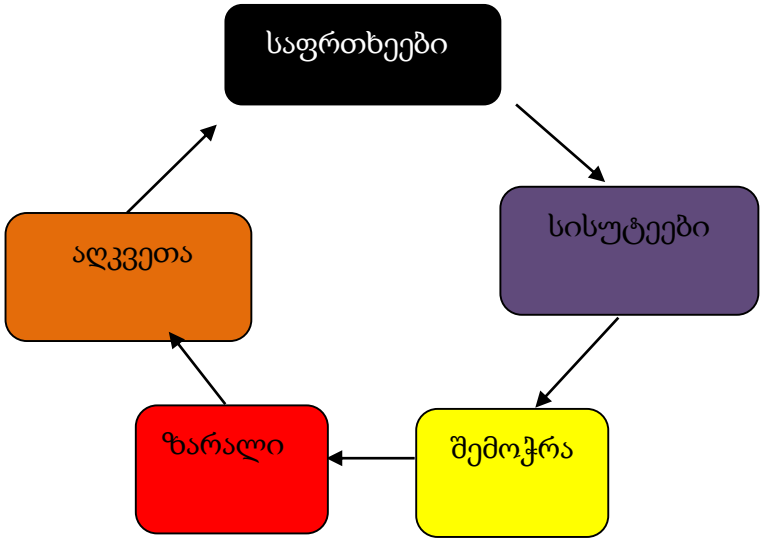
ინფორმაციული უსაფრთხოების რისკების მართვის პროცესი შესაძლოა მიესადაგოს მთლიან ორგანიზაციას, ან მის ცალკეულ ნაწილს (მაგალითად: დეპარატმენტს, ფიზიკურ მდებარეობას, სერვისს), ნებისმიერ ინფორმაციულ

სისტემას, კონტროლის მექანიზმების არსებულ ან დაგეგმილ ან სპეციფიკურ ასპექტებს (მაგალითად: ბიზნესის უწყვეტობის დაგეგმვა).

ადამიანის საქმიანობა სულ უფრო დამოკიდებული ხდება ციფრულ გარემოზე და ამ სფეროში ნებისმიერმა შეფერხებამ შეიძლება მნიშვნელოვანი ზარალი მიაყენოს მას. ციფრული ინფორმაციის მოცულობის ზრდასთან ერთად იზრდება ინფორმაციის დატაცების, არასანქცირებულ წვდომის, გამიზნული შეცვლის რისკები და მათი დანშაულებრივი მიზნებით გამოყენების ცდუნებები. ეს პრობლემები კიდევ უფრო აქტუალური ხდება გლობალური ქსელების და ტექნოლოგიების არსებობის პირობებში. საფრთხეები მოსალოდნელია როგორც ქვეყნის შიგნით, ასევე გარედან. საქართველოში ინტერნეტში ჩართული მომხმარებლების რიცხვი 2015 წელს მილიონებს აჭარბებს. აქედან გამომდინარე, კიდევ უფრო აქტუალურია მოქალაქეების საკუთრების ახალი ფორმის დასაცავად სახელმწიფოს მიერ მნიშვნელოვანი ღონიძიებების ჩატარების ამოცანის ანალიზი და გადაწყვეტა.

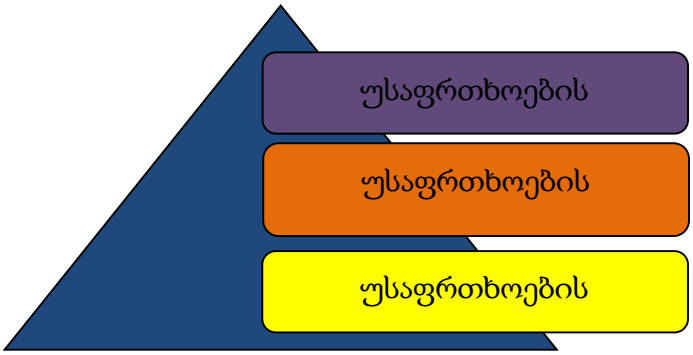
ბოლო ხანებში, როგორც ჩვენს ქვეყანაში, ასევე საზღვარგარეთ, მნიშვნელოვანი სამუშაოები ტარდება კიბერუსაფრთხოების გაზრდის თვასაზრისით, თუმცა პრობლემის სრულად გადაჭრამდე ჯერ კიდევ დიდი მანძილია გასავლელი, რადგანაც რთულდება სისტემები, იხვეწება შეტევების მეთოდები და მექანიზმები.

ინფორმაციული სისტემების უსაფრთხოების უზრუნველყოფა პირველ რიგში მოიცავს სისუსტეების გამოვლენის და აღმოფხვრის ღონისძიებებს, შეტევების აღმოჩენის და აღკვეთის სამუშაოებს, რომლის ციკლურ პროცესს წარმოადგენს (ნახაზი 7).



ნაზაზზე წარმოდგენილი პროცესი რთული და დინამიურია. ინფორმაციული სისტემების სისუსტეებზე და საფრთხეებზე ანალიზი კვალიფიციურ სპეციალისტებს და დიდ რესურსებს მოითხოვს. ამასთან სასურველია თუ აიგებოდა მოდელი და ავტომატიზირებული სისტემა, რომლის ასეთ საქმიანობას გააადვილებდა იმისთვის, რომ განხორციელდეს ინფორმაციული სისტემების უსაფრთხოების უზრუნველყოფის პროცესის სრულყოფა, საჭიროა მისი ადექვატური და ეფექტური მოდელის შექმნა. წარმოდგენილი პროცესი ძნელად ფორმალიზებადია, რადგანაც მასში გასათვალისწინებელია როგორც აპარატურულ- პროგრამული ასპექტები, ასევე ადამიანური ფაქტორები.

სიახლეს წარმოდგენს ინფორმაციული სისტემის უსაფრთხოების უზრუნველყოფის ერთიანი პროცესის წარმოდგენა მოდელების იერარქიის სახით (ნახაზი 8).



პირველი საფეხურის წარმოება შესაძლებელია შემდეგი სახის ფორმალური მოდელით:

$IS_1 = \langle S_o, S, F, G \rangle$,

სადაც S - ინფორმაციული სისტემის მდგომარეობის სივრცეა $S=X*U*Y$, ამ გამოსახულებაში U - შემავალი ზემოქმედების სიმრავლეა, X - სისტემის შიდა მდგომარეობათა ამსახველი სიმრავლეა, Y - სისტემის რექაციის ამსახველი სიმრავლეა, S_o - სისტემის მდგომარეობათა სივრცის საწყისი

მდგომარეობაა, F წარმოადგენს ოპერატორთა სიმრავლეს, რომელიც სისტემის მდგომარეობათა სივრცის ცვლილებებს ასახავს F= X*U* Y−U* Y, ანუ F არის მოდელირების ოპერატორი. G - მიზნობრივ მდგომარეობათა სიმრავლეა და იგი შეიძლება წარმოდგინდეს G={sB(s, s, s€S} სადაც B - პრედიკატია, რომელიც აიგება შემავალი ზემოქმედებებიდან და ამოცანებიდან გამომდინარე.

მეორე საფეხური ასახავს ინფორმაციული უსაფრთხოების სფეროში ცოდნის სტრუქტურიზაციას (ცნებებს, ცნებებს შორის კავშირებს, ობიეტების აღწერას, ობიექტებს შორის კავშირებს, მიზეზ-შედეგობრივ დამოკიდებულებებს, გამოყვანის წესებს და კონკრეტულ ფაქტებს).

IS_2=<B, C, R, W>,

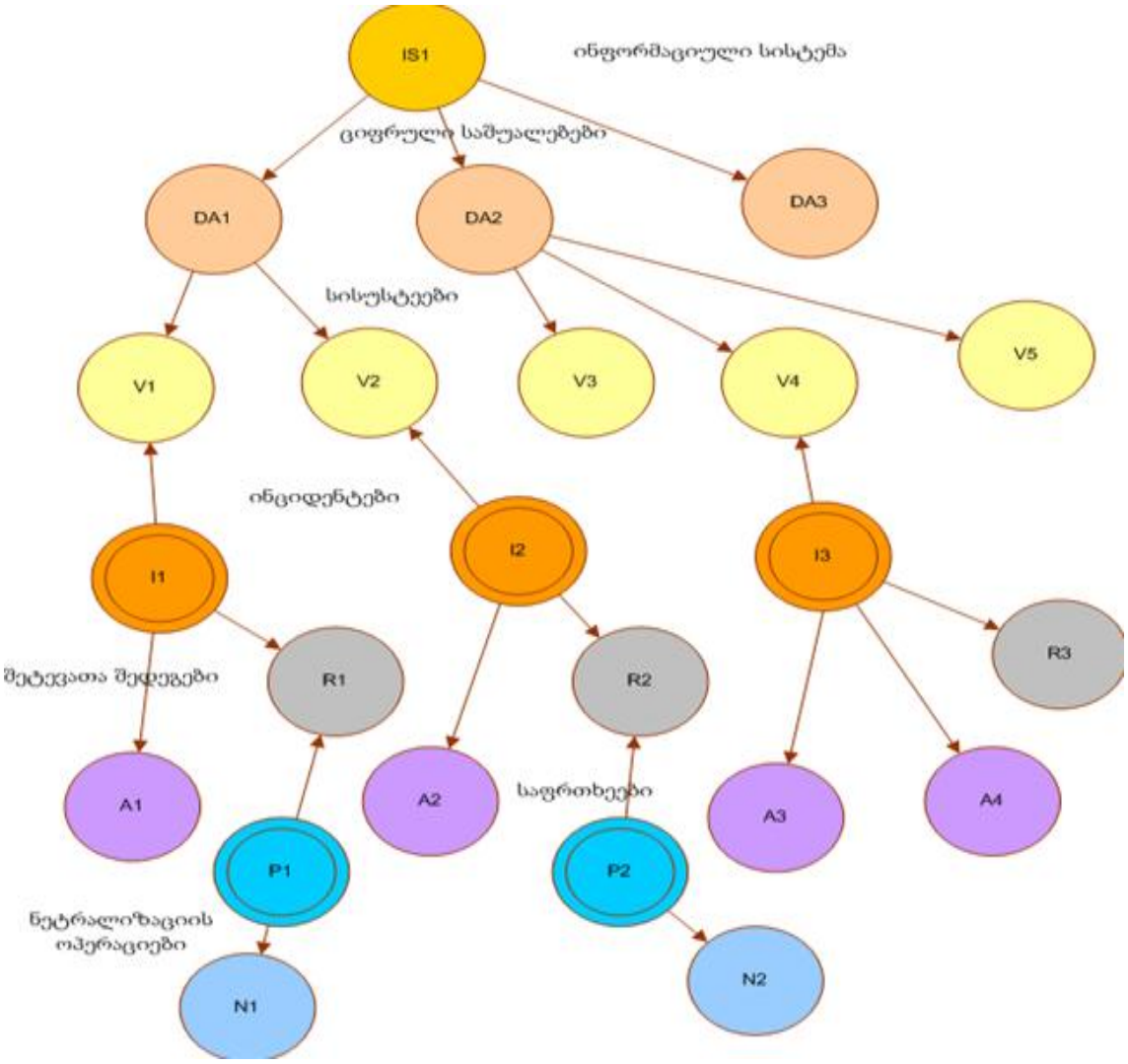
სადაც B=(O,A,V) ცნებების სიმრავლეა, რომლის წარმოდგინება „ობიექტი-ატრიბუტი მნიშვნელობა“ სამეულის სახით, ხოლო C=(B*B*B…*B) მიმართებების სიმრავლეა, R დასკვნების კეთების წესების სიმრავლეა, ხოლო W ფაქტების სიმრავლეა. ზოგადი ინფორმაცია წარმოდგება სემანტიკური ქსელების სახით, ხოლო ფაქტები ინახება მონაცემთა ბაზაში.

მესამე საფეხური ასახავს უსაფრთხოების პროცესის უზურნველყოფის ოპერაციულ სემანტიკას, რომლის საშუალებითაც რიცხობრივად აღიწერება სისტემის კომპონენტების ფუნქციონირება ლოგიკური ფუნქციების საშუალებით, რომელიც საშუალებას იძლევა განხორციელდეს სისტემის იმიტაციური მოდელირება და სისტემის მახასიათებლების რიცხობრივი დათვლა. შემოთავაზებულია აგებული მოდელების საფუძველზე შემუშავდეს პროგრამული ბაზა, ინფორმაციული სისტემების სისუსტეების ანალიზის პროცესების მოდელირებისათვის. კვლევის ობიექტებს წარმოდგენს ინფორმაციული სისტემების უსაფრთხოების უზურნველყოფის და მასში შემავალი სისუსტეების ანალიზის პროცესები, მათი ერთიანი იერარქიული მოდელების აგების მეთოდოლოგია, მეთოდები და ალგორითმები, რომლებიც გულისხმობს ფორმალური, ონთოლოგიური და ოპერაციული მოდელების შექმნას, სისტემის უსაფრთხოების ანალიზის პროგრამული ბაზის აგების პრინციპები და მეთოდები.

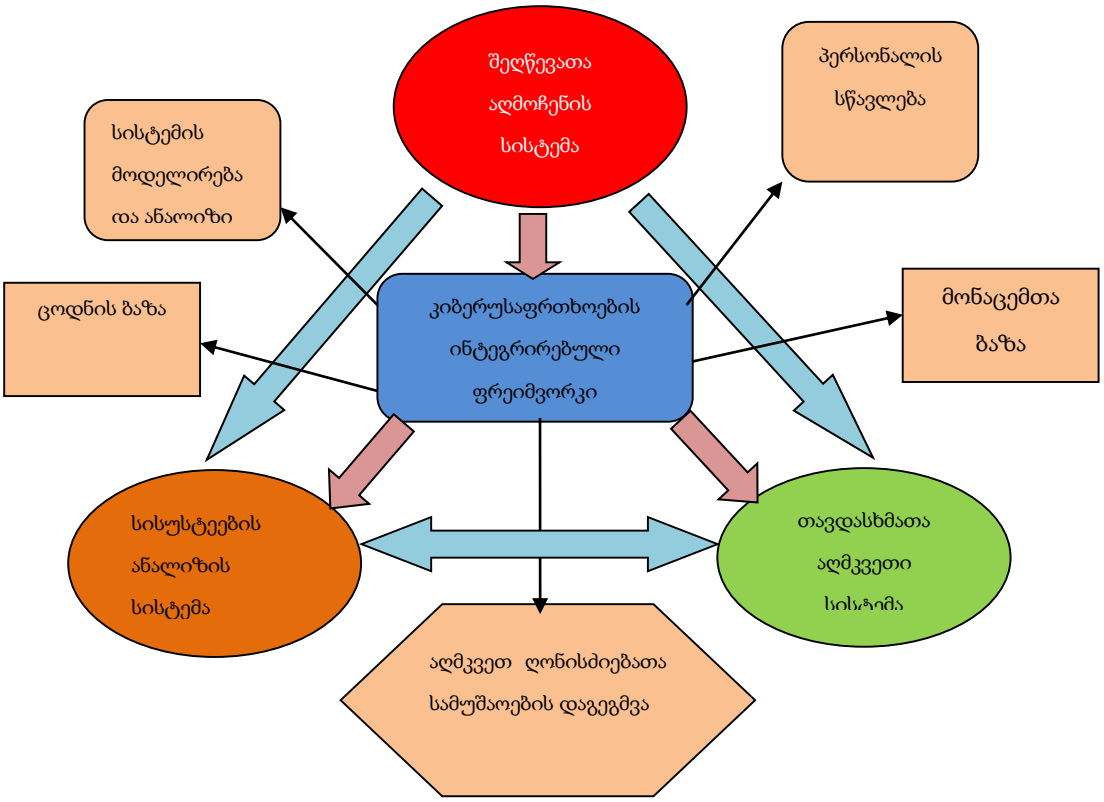
უსაფრთხოების ონთოლოგიური მოდელი გულისხმობს უსაფრთხოების უზურნველყოფის პროცესის სემანტიკური ქსელების საშუალებით წარმოადგენს მოდელის ასაგებად შემოთავაზებულია სემანტიკური ვების მრვალშრიანი არქიტექტურის გამოყენება:

XML → RDF → Ontology (OWL) → Logic → Proof.

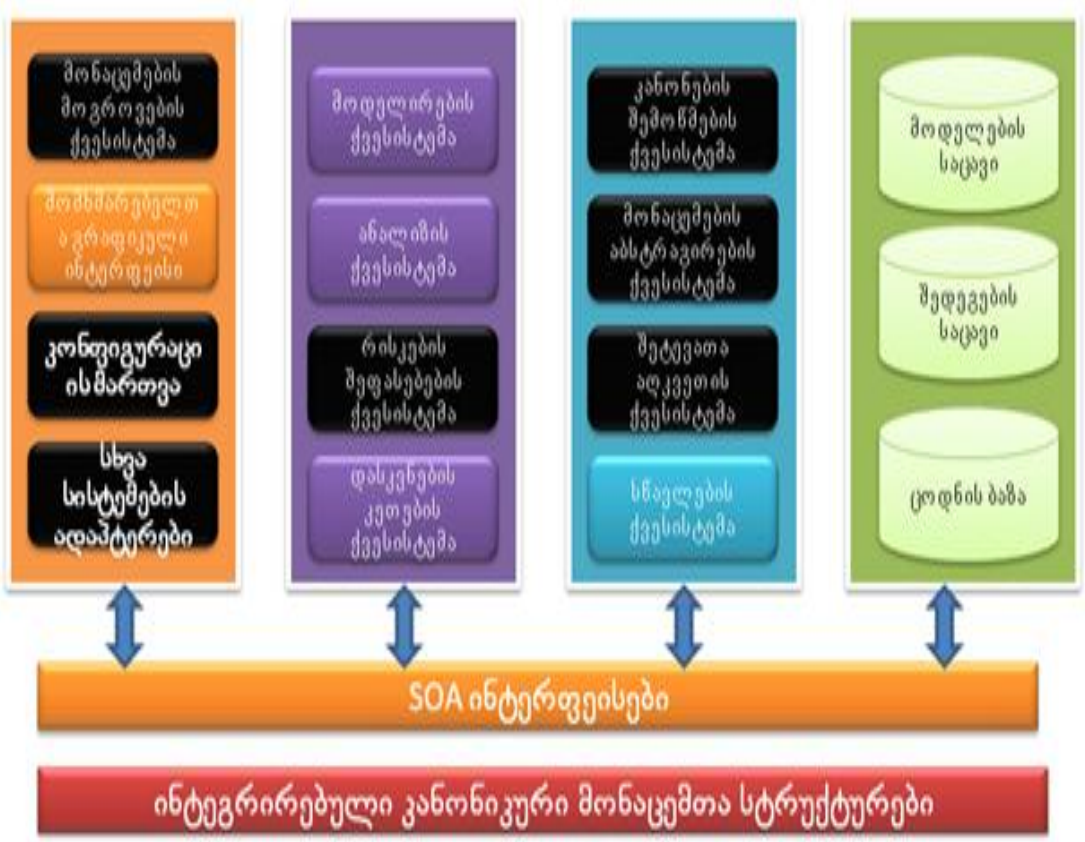
RDF წარმოადგენს რესურსების აღწერის ფორმატს Subject-Predicat-Object (არსი-პრედიკატი-ობიექტი) სამეულის სახით. ონთოლოგიის საშუალებით აღიწერება ცნობები და მათთან დაკავშირებული პროცესები. Logic და Proof უზრუნველყოფს ინფორმაციის ლოგიკურ წარმოდგენას და ლოგიკური დასკვნების კეთების მექანიზმებს. ეს ფორმალიზმი უნივერსალურია და შეიძლება გამოყენებული იყოს ნებისმიერი საგნობრივი სფეროს აღსაწერად.



არსებული უსაფრთხოების სისტემები ძირითადად ორიენტირებულია ერთ ფუნქციონალზე: შერწევათა აღმოჩენაზე, სისუსტეების ანალიზზე, ან საფრთხეების განეიტრალებაზე. რადგანაც ასეთ სისტემებს საერთო პრაგმატიკა, საერთო მონაცემთა ბაზები აქვთ, ამიტომ შემოთავაზებულია ინტეგრირებული პროგრამული ბაზის (ფრეიმვორკი) შეიქმნა, რომელიც დამატებით აღიჭურვება ნახაზზე ნაჩვენები ფუნქციონალობებით.



შემდეგ ნახაზზე 8. მოყვანილია შემოთავაზებული სისტემა აიგება საერთო სალტით დაკავშირებული ქვესისტემების სახით. საერთო სალტე რეალიზირდება ვებ სერვისების სახით და უზრუნველყოფს მონაცემების გაცვლას კანონიკურ, უნივერსალურ ფორმატში. მთლიანი სისტემის რეალიზაცია დიდ რესურსებს მოითხოვს და შეიცავს მისი განხორციელების დიდ რისკებს.



კვლევის მოსალოდნელი შედეგებია:

- დამუშავდება ინფორმაციული სისტემების უსაფრთხოების უზრუნველყოფის პროცესების მოდელირების საფუძვლები, რომელზედაც შეიძლება დაშენება შემდგომი კვლევების ამ მიმართულებით;

- შეიქმნება პროგრამული ბაზა სისუსტეების გამოვლენის და ანალიზის პროცესების მოდელირებისა;

- შექმნილი პროგრამული ფრეიმვორკი შეიძლება გამოყენებული იქნეს ინფორმაციულ ტექნოლოგიებში მომუშავე ნებისმიერი ორგანიზაციების მიერ, როგორც უსაფრთხოების პროცესების მოდელირებისათვის, ასევე პერსონალის სწავლებისათვის;

- შექმნილი პროგრამული ბაზით შესაძლებელი იქნება, როგორც ინფორმაციული სისტემების უსაფრთხოების უზრუნველყოფის სფეროში ცოდნის სტრუქტურიზაცია, ასევე ფაქტობრივი ცოდნის დაგროვება.

მიუხედავად იმისა, რომ არსებობს უდიდესი სიმრავლის მრავალფეროვანი პრობლემებისა, მათთან დაკავშირებით

გადაწყვეტილებების მიღების პროცესი შეიძლება გავაერთიანოთ გამარტივებულ სქემაში. ჯერ-ერთი გადაწყვეტილების მიმღებმა (გმპ) უნდა ჩამოაყალიბოს თავისი მოქმედებების ვარიანტები ე.წ. ალტერნატივები, მეორე - ამოირჩიოს მათში ყველაზე კარგი ვარიანტი ან მოახდინოს ალტერნატივების რანჟირება, დაალაგოს ისინი ხარისხის შემცირების მიხედვით. აქ პასუხი უნდა გაეცეს პირველ რიგში, შემდეგ კითხავს: რა არის საუკეთესო ალტერნატივა და რა აზრითაა ის საუკეთესო? საუკეთესო მიზნებიდან, ინტერესებიდან და გმპ მჯობინებიდან გამომდინარე, მაგრამ ცხადია, რომ ეს მიზნების, ინტერესები შეუძლებელია დახასიათდეს ერთი მაჩვენებლით.

გმპ ინტერესების მრავალფეროვნება გვაიძულებს ალტერნატივები შევაფასოთ ხარისხის მრავალი მაჩვენებლების ან კრიტერიუმების მიხედვით. თუმცა შეიძლება ერთი ალტერნატივა მეორეს სჯობდეს ერთი რომელიმე კრიტერიუმებით, მაგრამ უარესი იყოს სხვა კრიტერიუმის მიხედვით, ამიტომ გმპ უნდა მიანიჭოს ამორჩეული კრიტერიუმს „წინა“, განსაზღვროს მათი მნიშვნელობა. ამ ინფორმაციის საფუძველზე, აგრეთვე თითოეული ალტერნატივის ცალკეული კრიტერიუმების მიხედვით შეფასებათა გათვალისწინებით, შესაძლებელი ხდება ალტერნატივათა რანჟირება და უკეთესის ამორჩევა. თანამედროვე პირობებში, როგორც ვნახეთ, აუცილებელია აღნიშნულიპროცესის მოდელირება და ავტომატიზება, ანუ შეიქმნას კომპიუტერული სისტემა, რომელსაც შეეძლება ამ მიზნისთვის ინფორმაციის მიღება და დამუშავება და შესთავაზოს გმპ-ს გადაწყვეტილება, ანუ აღმოუჩინოს გადაწყვეტილების მიღებისას დახმარება გმპ - ესაა გადაწყვეტილებათა მიღების მხარდამჭერი სისტემა (გმმს). ფაქტია, რომ გადაწყვეტილების მიღების პირების მიერ უპირატესობების მინიჭება ამა თუ იმ გადაწყვეტილებისათვის, განსხვავდებიან ერთმანეთისაგან, ისევე როგორც ადამიანები. ამიტომ ალტერნატივათა ხარისხის შეფასებები, რომლებიც გამოითვლება ასეთი ობიექტური მეთოდებით, არის სუბიექტურები, რომლებიც ასახავენ გმპ მიერ უპირატესობის მინიჭებას. ერთი შეხედვით -ესაა აღნიშნული გადაწყვეტილების მიღების მხარდამჭერი მეთოდის უარყოფითი მხარე; რეალურად კი ეს წარმოადგენს მეთოდის ღირსებას, ვინაიდან საშუალებას იძლევა გათვალისწინებულ იქნას გმპ-ს ინდივიდუალურობის და მისი ინტერესები. მაგრამ იბადება კითხვა: თუ გმმს ეხმარება გმპ გათვალისწინებულ იქნას მისი მჯობინება, მაშინ ხომ არ ჯობია

გადაწყვეტილება მიღებული იქნას „ხელით“, ასეთი სისტემების დახმარების გარეშე?

ამ სისტემების გამოყენების აუცილებლობა მომდინარეობს გადაწყვეტილების მიმღები პირები და საერთოდ ადამიანების ფსიქოფიზიოლოგიური შესაძლებლობებიდან მიიღოს და დაამუშაოს დიდი მოცულობის ინფორმაცია.

ადამიანის მიერ ინფორმაციის აღქმის, მახსოვრობის, შესწავლის პროცესები და მექანიზმები ჯერ კიდევ არაა ბოლომდე გარკვეული, მაგრამ უკვე არსებული დასკვნებით ადამიანს შეუძლია დაიმახსოვროს და ერთდროულად დაამუშავოს არა უმეტეს 7-9 ობიექტისა [1].

როგორც უკვე დაგროვილი გამოცდილება გვიჩვენებს, გმმს უპირატესობები განსაკუთრებით ნათლად ვლინდება სტრატეგიული მნიშვნელობის საკითხებისას გადაწყვეტილებების მიღების უზურნველყოფის დროს.

გასათვალისწინებელია, ნებისმიერი კატეგორიის მიზანდასახული სისტემის მართვისას, რუტინული, ყოველდღიური, ე.წ. სტანდარტული მმართველობით პროცესების, რომელთაგან გმპ-ს განათავისუფლება ან მათში ჩარევის მაქსიმალურად გამარტივება და დროში მინიმიზება, მნიშვნელოვნად შეუწყობს ხელს სტრატეგიული, სასიცოცხლო მნიშვნელობის გადაწყვეტილებების მიღების ხარისხის გაუმჯობესებას და შესაბამისად, მიზანდასახული სისტემის ეფექტურად ფუნქციონირებას საკმაოდ ცვლად და დინამიურ, წინააღმდეგობებით გაჯერებულ თანამედროვე გარემოში. ე.წ. განმეორებადი გადაწყვეტილებების მიღების მხარდასაჭერად საკმარისია მარტივი გმმს-ები, რომლებიც გათვლილია ერთ მიმართულებაზე.

რაც მთავარია გმმს-მა უნდა უზრუნველყოს მიღებული გადაწყვეტილების ახსნა, რაც შესაძლებელია მასში ცოდნის ბაზების, მოდელების ბაზების და პრობლემათა ანალიზის ქვესისტემების არსებობისას. ასეთი სისტემის შექმნისას აუცილებელია, პირველ რიგში, პრობლემათა ანალიზისა და გადაწყვეტილებათა მიღების ქვესისტემებში ხდებოდა შემდეგი ძირითადი ამოცანების რეალიზაცია - გადაწყვეტა:

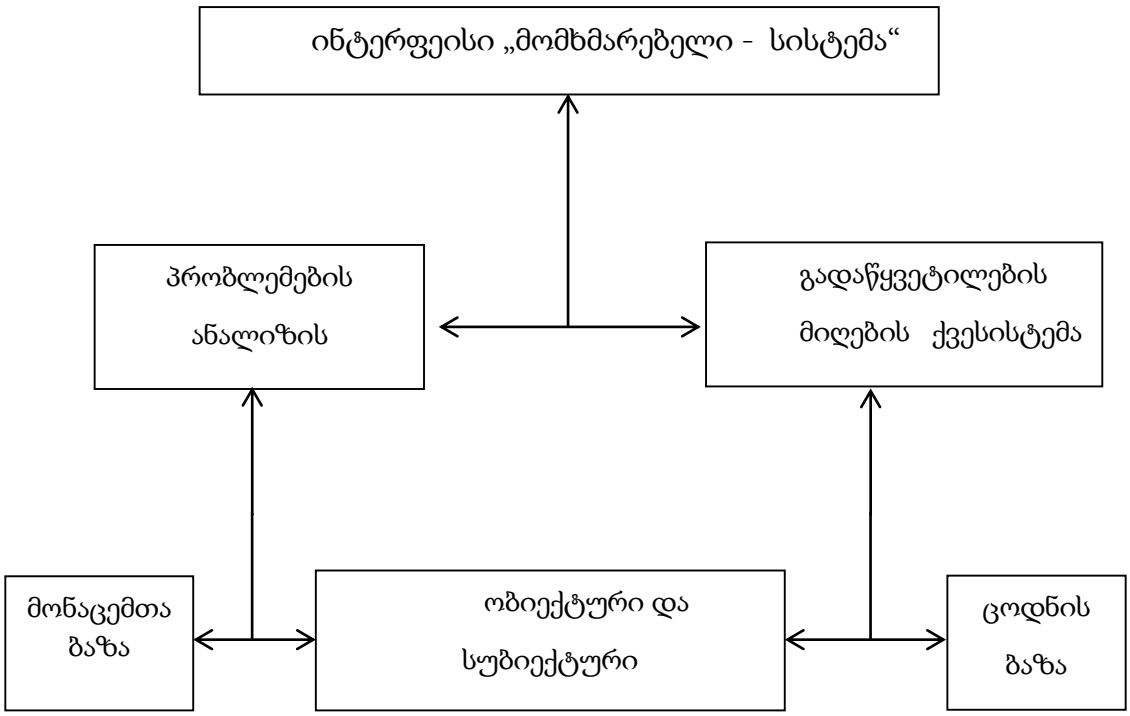
- მონაცემების ინტერპრეტაცია;
- დარღვევების ან უწესივრობის დიაგნოსტიკა;
- კონტროლი;

- პროგნოზირება;

- დაგეგმვა;

- დაპროექტება.

ამ ამოცანებიდან ერთ-ერთი უმთავრესია ორგანიზაციული სისტემაში დარღვევათა დიაგნოსტიკის ამოცანა, რომელიც უნდა გადაწყდეს პრობლემათა ანალიზის ქვესისტემაში, ხოლო საწყისი ინფორმაცია მოდელისათვის მონაცემთა ბაზაში და ცოდნის ბაზაში (ნახაზი 11).



ნახაზი 9. გმმს ზოგადი სქემა

გადაწყვეტილების მიღების პროცესი საკმაოდ რთულია და მოიცავს შემდეგ ძირითად პროცესებს (ეტაპებს):

- ინფორმაციის შეგროვება, შემოწმება და ანალიზი;

- შესაძლო გადაქწყვეტილებათა ვარიანტების მომზადება;

- გადაწყვეტილების არჩევა (ორგანიზაციის სტრატეგიის, მიღებული გადაწყვეტილების შესაძლო მოკლევადიან და გრძელვადიანი შედეგების გათვალისწინება);

- არჩეული გადაწყვეტილების დაგეგმვა და რეალიზაცია;

- აღრიცხვა;

- რეალიზაციის გეგმის შესრულების კონტროლი;

- შედეგების ანალიზი;

- დარღვევათა აღმოჩენა და მაკორექტირებელი ზემოქმედებების გამომუშავება და განხორციელება.

აღნიშნულიდან გამომდინარეობს, რომ დამოუკიდებელ სახელმწიფოში, როგორც სისტემაში, თუ ეკონომიკის, მეცნიერების, განათლების და ა.შ. ორგანიზაციის დონე ცუდია და ურთიერთქმედება სუბიექტებისა ატარებს ცუდად მართვად ან უმართავ ხასიათს, მაშინ ასეთი სახელმწიფოს პოტენციალი არაა მაღალი და შეიძლება ნაკლებიც იყოს ყველაზე სუსტი სუბიექტისა და ყველაზე მთავარი, ასეთი სისტემა ვერ შეძლებს შემდგომ მდგრად განვითარებას და მისი არსებობა შეიძლება კითხვის ნიშნის ქვეშ დადგეს.

ორგანიზებულობა, მიზნების სწორად განსაზღვრა, სისტემური კანონზომიერებების დაცვა, აუცილებლად მოითხოვს სახელმწიფოს მართვაში სიტუაციური მიდგდომის დანერგვას. სახელმწიფო ურთულესი მეგასისტემაა, დღეს არ არსებობს რაიმე ცალსახა მეთოდი მისი ეფექტურად მართვისა, ხოლო სიტუაციური მიდგომა, შეიძლება ითქვას ერთადერთი ინსტრუმენტია იმისათვის, რომ მართვის სხვადასხვა მეთოდების გამოყენება განისაზღვროს სიტუაციით. ვინაიდან არსებობს ისეთი სიმრავლე ფაქტორებისა, როგორც სახელმწიფოს შიგნით ასევე გარემომცველ გარემოში, რომ არ არსებობს ერთიანი „უნიკალური ხერხი“ მეთოდი, სახლემწიფოს და საერთოდ ნებისმიერი რთული ორგანიზაციის მართვისა,, მოკლედ რომ ვთქვათ, ყველაზე ეფექტურ მეთოდს კონკრეტული სიტუაციაში წარმოადგენს მეთოდი, რომელიც ყველაზე უფრო მეტად შეესაბამება მოცემულ სიტუაციას.

ამრიგად, ისეთი განვითარებადი ქვეყნისათვის (და არამარტო) როგორც საქართველოა სასიცოცხლო მნიშვნელობა აქვს იმას, რომ ქვეყნის მოქალაქეებს, პირველ რიგში კი პოლიტიკური ელიტას, რომელსაც აქვს სურვილი და პრეტენზია იყოს სახელმწიფოს მმართველი, კარგად უნდა ესმოდეს, რომ სახელმწიფო არის ურთულესი მეგასისტემა და მისი მდგრადი განვითარებისათვის საჭიროა ის კარგად ფლობდეს საერთო სისტემურ კანონზომიერებებს, სიტუაციური მართვის პრიციპებს და იზრუნოს ქვეყნის მეცნიერების, განათლების, კომუნიკაციების, ინოვაციების განსაკუთრებულად, რომ წარმატებით მოახერხოს სახელმწიფოს მართვაში უახლესი სამეცნიერო მიღწევების გამოყენება.

დღეს არსებული დაცვის მექანიზმები მიმართული არიან ინფორმაციული უსაფრთხოების (იუ) უზრუნველყოფის ცალკეული ასპექტების რეალიზაციაზე. რაც ვერ უზრუნველყოფს დაცვის სისტემის მართვის ანალიზისა და სინთეზის ამოცანების კომპლექსური გადაწყვეტილების მიღების დაცული ინფორმაციული სისტემების (ის) და მონაცემთა ბაზების (მბ) შექმნას.

სულ უფრო სერიოზულ ყურადღებას ითხოვს და ექცევა კიდევაც თვით ინფორმაციული ტექნოლოგიების დაცვის საკითხებს (1,2). ძირითადი მოთხოვნა დაცვის ტექნოლოგიისადმი არის შენარჩუნება მემკვიდრეობითობის და ოპერაციების თანმიმდევრობის ინტეგრირებული დაცვის სისტემის შექმნისა ინფორმაციული პროდუქტების, რომლებიც ორგანიზებული არიან მბ–ს სახით, ფორმირებისა და გამოყენებისას.

ჩვენი კონცეფცია გულისხმობს ინფორმაციული რესურსების დაცვის პროცესის ეტაპობრივ რეალიზაციას ურთიერთ დაკავშირებული მოდულების – ქვესისტემების სახით დაცვის თანამედროვე მეთოდების და მექანიზმების ბაზაზე დაწყებული სხვადასხვა ინფორმაციული პროდუქტების დაცული მბ სტრუქტურების პროექტირებით და სხვადსხვაგვარი მომხმარებლის ინფორმაციული მომსახურებით დასრულებული.

შემოთავაზებული მოდელები, მეთოდები, ინსტრუმენტალური საშუალებები, რომელთა დახმარებითაც მოხდება შემოთავაზებული კონცეფციის რეალიზება, მიმართული არიან მონაცემების კონფიდენციალობის და მთლიანობის ურღვევობის უზურუნველყოფაზე. ასევე შეიძლება გამოყენებული ერთგავროვანი თემატიკის მბ–სთვის რომლებშიც ერთდროულად ინახება სხვადასხვა ხარისხის კონფიდენციალობის მონაცემები.

ა) ამოცანის დასმა და მისი გადაწყვეტის მეთოდები.

პრაქტიკული გამოცდილებიდან გამომდინარე შეიძლება ითქვას, რომ მბ–ში ინახება მრავალფეროვანი ინფორმაცია არა მარტო წარმოდგენის ფორმის თვალსაზრისით, არამედ კონფიდენციალობის დონის მიხედვითაც. როგორც კორპორაციული ინფორმაციული საერთოდ შეზღუდული გამოყენების რესურსების მუქარების ანალიზმა გვიჩვენა, რომ ინფორმაციული დაცვის სისტემის ორგანიზაციისათვის აუცილებელია დამუშავდეს ინფორმაციული ტექნოლოგია, რომელშიც

გათვალისწინებული იქნება შეზღუდული მოხმარების დოკუმენტებთან მუშაობის მოთხოვნები როგორც წესი ეს მოთხოვნები სახელმწიფოში შესაბამისი ნორმატიული დოკუმენტებით უნდა იყოს განსაზღვრული. ჩვენს მიერ წარმოდგენილმა ტექნოლოგიამ უნდა უზრუნველყოს მრავალდონიანი კონტროლი დაშვებისა ინფორმაციასთან კრიპტოგრაფიული დაცვით, რომელმაც უნდა უზრუნველყოს მაღალი საიმედოობის დაცვა სხავდასხვა კონფიდენციალობის მქონე ინფორმაციისა, რომელის ინახება და გადაეცემა ღია საკომუნიკაციო არხებით. დაცვის წარმოდგენილი მოდელის ეფექტურობა უნდა ეფუძნებოდეს ოპტიმალურ, ინფორმაციული უსაფრთხოების თვალსაზრისით, პროექტირებას თემატური მბ (თმბ) სრუტრურისა. შესაძლებელია დაცვის პროცესის ტექნოლოგიის ფორმირების განსხვავებული მეთოდები და შესაბამისად მისი სხვადასხვანაირი აღწერა, დაწყებული დაცვის მეთოდოლოგიით, რომელიც განსაზღვრავს მეთოდებს და მექანიზმების დაცვისა და დასრულებული მიდგომებით, რომელიც ეფუძნებიან დასაცავი ობიექტების ტიპებისა გამოყოფას და დასაბუთებას. არსებულ ნაშრომზე დაყრდნობით შემოვიტანოთ ზოგიერთი განმარტებები:

ჩვენს შემთხვევაში ინფორმაციის დაცვის კონფიდენციალური მოდელის ქვეშ მოვიაზრებთ პროცესს, რომელიც შედგება დაცული ოპერაციებისაგან ინფორმაციული პროდუქტების (მბ, ელექტრონული დოკუმენტების, შეტყობინებებისა და ა.შ.) დაცულად დამუშავების, შენახვის და გადაცემის და ასეთი პროცესების და მეთოდების განხორციელების ხერხებისაგან, რომლებიც დამყარებული იქნებიან იუ–ს სფეროში თანამედროვე მიღწევებზე.

მრავალდონიანი დაცვა განისაზღვრება როგორც თვით ინფორმაციული სისტემის (ის) თვისება შეინახოს და დაამუშავოს მოხმარების სხვადასხვა დონისა და კატეგორიის მონაცემები, როდესაც არსებობს პერსონალი დაშვების სხვადასხვა უფლებამოსილებით, რათა გამოირიცხოს დაშვება ინფორმაციასთან ან მის მოდიფიკაციასთან პირებისა, რომელთა დაშვებაც არ პასუხობს საიდუმლოების დონეს და ნება დართოს შესრულება მხოლოდ ნებადართული ოპერაციებისა.

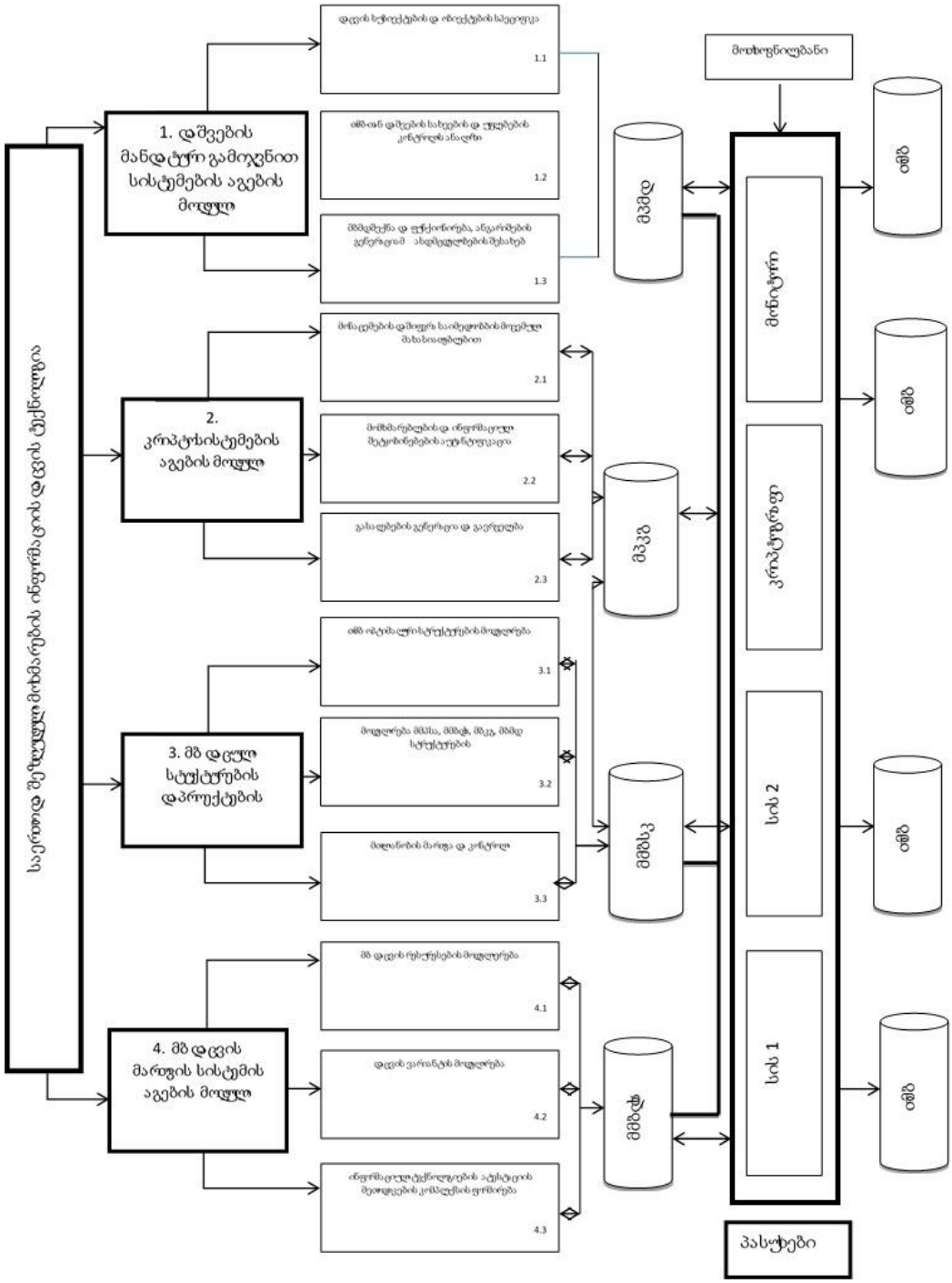
კვლევის ობიექტი – ინფორმაცია კონფიდენციალობის სხვადასხვა ხარისხით, რომელიც ინახება მბ–ში და გადეცემა კავშირის ღია არხებით. ჩვენი მიზანია გადაწყდეს ამოცანა კონფიდენციალობის შენარჩუნებისა შეზღუდული მოხმარების ინფორმაციისათვის და მთლიანობის

ურღვევობის ამოცანის მხარადაჭერა საერთო ხელმისაწვდომი ინფორმაციისათვის. შემოთავაზებულ კონცეფციას დაცვის უზრუნველყოფისა აქვს ინტეგრირებული მოდულის სისტემის სახე. ურთიერთკავშირი ძირითად მოდულებს შორის სხვადსხვა კონფიდენციალობის ხარისხის ინფორმაციული რესურსების დაცვის, წარმოდგენილია ნახ.12. მოდულებს შორის კავშირი მიიღწევა იუ –ს უზრუნველყოფის თითოეული ტექნოლოგიური ეტაპის ამოცანების გადაწყვეტების შედეგებისს ურთიერთ გამოყენებით, რომლებიც სტრუქტურირებული და ორგანიზებული არიან სპეციალურად დაპროექტებული მბ და მონაცემების ბაზების (მმბ) სახით;

- დაცვის მონაცემების ბაზების (მმბ) სახით;
- მრავალდონიანი (მმბდს) დაცვით;
- კრიპტოგრაფიული გარადასახვებით (მბკგ);

უზრუნველყოფს კონფიდენციალობის ინტეგრირებული ინფორმაციისათვის სხვადასხვა ხარისხის კრიტიკულობით, რომლებიც ინახებიან მბ–ში სხვადასხვა თემატური მიმართულებით და განკუთვნილი არიან სხვადასხვა მომხარებლების ჯგუფებისათვის, მიიღწევა ეტაპობრივი გადაწყვეტით ინფორმაციის დაცვის მართვის შემდეგი ამოცანის გადაწყვეტით:

დამუშავება მონაცემებთან, დაშვების გამიჯვნის მრავალდონიანი მოდელისა და ალგორითმებისა, რომლებიც ახდენენ რეალიზებას დაშვების მანდატური გამიჯვნისა შეზღუდული მოხმარების ინფორმაციასთან წონასწარ დადგენილი წესების მიხედვით (მოდული 1), მათ რიცხვში სპეციფიკაციის დაცვის სუბიექტების და ობიექტების (მოდული 1.1.), თმბ–თან დაშვების სახეების და წესების კონტროლი და ანალიზი (მოდული1.2.), შექმნა და ფუნქციონირება მბმდ, ანგარიშების გენერაცია არასანქცირებული დაშვების (ასდ) მცდელობის შესახებ (მოდული 1.3)



ნახაზი.10. სხვადასხვა კონფიდენციალობის ხარისხის ინფორაციული რესურსების დაცვის ტექნოლოგიის ძირითად მოდულებს შორის ურთიერთკავშირი

დამუშავება ინფორმაციის კრიპტოგრაფიული დაცვის ცალეკული კომპონენტებისა ამაღლებული საიმედოობით შეზღუდული მოხმარების ინფორმაციისათვის (მოდული 2.), მათ შორის მონაცემების დაშიფვრა საიმედოობის მოცემული მახასიათებლებით (მოდული 2.1), მომხმარებლების და ინფორმაციული შეტყობინების აუტენტიფიკაცია (მოდული 2,2), გასაღებების გენერაცია და გავრცეელება (მოდული 2,3);

თმბ მომხარებლის საგნობრივი ანალიზი არის, შეზღუდული და საერთო მოხმარების მონაცემების დამუშავებისა და შენახვის დაცვის სპეციფიკაციის აგება, თმბ ოპტიმალური სტრუქტურის მოდელირება სპეციალური ინსტრუმენტალური საშუალების გამოყენებით (მოდული 3).

მოდელირება მმბ სტრუქტურებისა, რომლებიც მხარს უჭერენ დაცვის ტექნოლოგიებს, და აგება თმბ დაცული სტრუქტურებისა, რომლებიც მხარს უჭერენ დაცვის ტექნოლოგიებს და აგება თმბ დაცული სტრუქტურებისა მონაცემების უტყუარობის და უსაფრთხოების კრიტერიუმების მიხედვით (3,2).

მოდელირება ამოცანათა კომპლექსისა ბმ–ს ასდ–გან დაცვის სისტემის მართვისა (მოდული 4), მათ შორის მოდელირება დაცვის რესურების (მოდული 4.1) და მისი ვარიანტების (მოდული 4.2) მაგალითად, ოპტიმალური მბმს შერჩევა მომხმარებლის ინფორმაციულ მოთხოვნებზე დაკმაყოფილების სისრულის კრიტერიუმებით და ინფორმაციულ–გამოთვლითი სისტემების (იგმ) დაცულობის კლასის მიხედვით, ფორმდება ინფორმაციული ტექნოლოგიების ადესტაციის მეთოდიკების კომპლექსისა (მოდული 4,3).

მონაცემთა მთლიანობის კონტურული (მოდული 3.3) ხორციელდება ხარისხის შემდეგი კრიტერიუმების მიხედვით:

1. სისრულე (კონტროლი მონაცემების მნიშვნელობების არა სისრულე და არასწორი აღწერისა, მონაცემთა სრუქტურის სრული აღწერის შემოწმება);

2. არაწინააღმდეგობრიობა (მონაცემებს შორის ლოგისტიკური კავშირების შემოწმება, გამოვლენა ჭარბი და წინააღმდეგობრივი აღწერების, კონტროლი მნიშვნელობათა დიაპაზონის საზღვრების და თვით მნიშვნელობების დამაჯერებლობის);

3. აქტუალურობა (კონკრეტული ერთდროული და დროული ცვლილებების შეტანისა თმბ და მმბ).

მთლიანობის კონტროლის მეთოდები და საშუალებები ეფუძნებიან შესატანი მონაცემების ანალიზს და მონაცემების მიმართ მოთხოვნის აღწერებს, რომლებიც მიღებულია მბმს სტანდარტებით და ფუნქციური მოთხოვნებით მომხმარებლებისა, რომლებიც დაფიქსირებულია მმბ და რეალიზებულია შესაბამის ინსტრუმენტულ საშუალებაში (სის2).

ცხადია, დასმული ამოცანების გადასაწყვეტად გამოყენებულ იქნა მონაცემთა ბაზების და ინფორმაციული სისტემების თეორიის, სისტემური ანალიზის. მათემატიკური ლოგიკის, სიმრავლეთა და ალგორითმების თეორიის, აგრეთვე პროგრამების ტექნოლოგიის მეთოდები და მიღწევები.

ბ) დაშვების კონტროლთან დაკავშირებული გადაწყვეტილებების მეთოდები.

მრავალდონიანი დაცვის სისტემის ბირთვს წარმოადგენს მოთხოვნების დამუშავების მონიტორი (მდმ), რომელიც ამოწმებს მომხმარებლის ყოველ მიმართვას მონაცემებთან ან პროგრამებთან თუ რამდენად შეესაბამებიან ისინი იმ მოქმედებების სიას, რომელიც დაშავებულია მომხმარებლისთვის. მდმ კონცეფციის გამოყენება ლოგიკური დაშვების კონტროლი მექანიზმების დამუშავების საშუალებას იძლევა თავიდან იქნას აცილებული გაურკვევლობის ელემენტები პირობების და შიდა შეზღუდვების მეშვეობით, როდესაც დარეგისტრირებულ პროცესება და ფიზიკურ პირებს შეუძლიათ იმის შესრულება, რისი უფლებაც აქვთ. დამუშავეულია გაფართოებული სია ძირითადი წესებისა მოთხოვნის ნებართვაზე, დაშვების უფლებამოსილების კონტროლზე და სისტემის მდგომარეობის შეცვლაზე. წარმოდგენილი მოდელი დაშვების მანდატური გამიჯვნისა მდმ–ში ახდენს. ფორმალურად დაცვის სუბიექტების და ობიექტების ხისებერ სტრუქტურაზე დაშვების გაფართოებული სიის რეალიზაციას.

დაცვის სუბიექტების და ობიექტებისათვის ხისებრი სტრუქტურის მინიჭება იძლევა ოპტიმალური სურსათს დაშვების მართვისა და უზრუნველყოფს კორექტული მართვის რეალიზებას დაშვების ისეთი წესებისა, როგორიცაა „ახალი ობიექტების შექმნის უფლება“, „დაშვების უფლების აღკვეთა“, „დაშვების უფლებების გადაცემა სუბიექტებს შორის“, „მოთხოვნის რეალიზაციის უფლება“(4). სუბიექტის მოთხოვნის რეალიზაციის უფლების შემოწმება აუცილებელმა შემთხვევაში, როდესაც დაშვების საკმარისი კატეგორიისას სუბიექტს შეიძლება არ ქონდეს

მინიჭებული უფლებამოსილება გაეცნოს კონკრეტული შემოსული დოკუმენტს საიდუმლოობის შედარებადი ხარისხით.

გათვალისწინებულია დაცვის სუბიექტების და ობიექტების ძირითადი პარამეტრების მინიჭება მათი ინფორმაციული ერთიანობის დონის და დაცულობის მაჩვენებლის მიხედვით კლასიფიკაციის და ტიპიზაციის გათვალისწინებით.

შემოთავაზებული მექანიზმი დაშვების უფლებათა მატრიცის შევსებია ითვალსიწინებს მატრიცის ანალიზის პროცედურებს, თუ რამდენად სრულად მოიცავს ის ინფორმაციულ რესურსებს და ინფორმაციული ნაკადების კორექტულობას დავების სახეების წინააღმდეგობრიობის თავიდან ასაცილებლად. კონფიდენციალური ინფორმაციის შენახვის საიმედოობის ასამაღლებლად შემოთავაზებულია მატრიცის ბირთვის კრიპტოგრაფიული დაცვა.

აღნიშნული მოდელი, რომელიც რეალიზებულია დაცვის სუბიქტების და ობიექტების ხისებურ სტრუქტურაზე, განკუთვნილია საიდუმლოობის რეჟიმის, რომელიც უნდა იყოს განსაზღვრული სახლემწიფო ნორმატიული დოკუმენტებით უზრუნველსაყოფად.

გ)კრიპტოდაცვის გადაწყვეტის მეთოდები.

დაცვის სუბიექტებისათვის, რომელსაც გააჩნია მაღალი კატეგორიის დაშვება, ინფორმაციის ნაწილი საიმედოდ უნდა იყოს დაშიფრული. მაღალეფექტური და საიმედო გამოთვლითი სისტემების პროექტირების სიმეტრიული კრიპტოსისტემების გამოყენება შესაძლებელია შიფრაციისადმი არა ტრადიციული მიდგომის გამოყენებით. მაღალი დონის საიდუმლო ელექტრონული დოკუმენტის კრიპტოგარასახვის პროცედურები უნდა იყოს ისეთი, რომ მან უზრუნველყოს კრიპტომდგრადობა, რომელიც დადგენილია მსგავსი დონის კონფიდენციალური ინფორმაციის დასაცავად.

მომხმარებლის მოთხოვნების დამუშავების, კონტროლისა და ანალიზის მონიტორის ფუნქციებში დამატებითი სისტემის სახით ჩართულია ინფორმაციის შიფრაციის და დეშიფრაციის პროცედურები არატრადიციული მიდგომის ბაზაზე, რომელიც საშუალებას იძლევა კრიპტოალგორითმის საიმედოობის კარირების დაცვის დონისაგან დამოკიდებულებით ნებისმიერი კლასის საიდუმლო ინფორმაციისათვის საიდუმლოობის დონეს. ტექნოლოგიურად უმჯობესდება ვარიანტი,

რომლის დროსაც დაშიფვრის სხავასხვა ალგორითმის რაოდენობის არჩევა დამოკიდებულია დაცვის ობიექტის საიდუმლოს დონეზე და ინფორმაციის დამუშავების მეთოდებზე.

შემოთავაზებული არატრადიციული მეთოდი დაშიფვრისა არაპოზიციურ პოლინომიალურ სისტემაში საშუალებას იძლევა მიღწეულ იქნეს კრიპტომდგრადობა, რომელიც დამოკიდებულია არა მარტო გასაღების სიგრძეზე, არამედ შერჩეული პოლინომილაური საფუძვლის სისტემაზე, ასევე მათ განაწილებაზე (მიმდევრობის წესზე) (5).

დ) თმბ და მმბ სტრუქტურების დაპროექტების გაწყვეტის მეთოდი.

ინფორმაციული ტექნოლოგიების ბაზარზე დღეს არსებული საშუალებები და სისტემები მბ და პროექტებისა და თანხლებისა სრულად ვერ აკმაყოფილებენ კორპორაციული მბ დამპროექტებლის მოთხოვნებს, განსაკუთრებით ეს ეხება განსხვავებული კონფიდენციალობის მქონე მბ შექმნას. საჭირო დონე უტყუარობისა და დაცვისა მბ, რომლებიც ინახავენ ინფორმაციულ თემატურ პროდუქტებს, ემსახურებიან განხილულ დაცვის ტექნოლოგიას, მიიღწევა სტრუქტურული მეთოდებით, რომლებიც უზრუნველყოფენ მბ ოპტიმალური სტურქტურის ანალიზისა და სინთეზსს, ერთდროულად იყენებენ მოდიფიცირებულ მექანიზმებს და სისტემებს მბ დაცვის უტყუარობის ასამაღლებლად.

ყველა მმბ ექსპლუატაციისას აქტუალურ მდგომარეობაში შენარჩუნების პროცესის ავტომატიზებისათვის გამოყენებულია მონაცემების ზოგადი აღწერის მეთოდი (საიდენტიფიკაციო სახელები, ტიპები, ზომები, და ა.შ.). თმბ ოპტიმალური სტრუქტურების მოდელირებისას აუცილებელია გათვალისწინებულ იქნას შენახული მონაცემების დაცულობის დონე, მომხმარებლის თმბ სტრუქტურაში მოთხოვნების და საჭიროებების უტყუარობა და სისრულე. ამიტომ თმბ–ში შენახვა დიდი მოცულობის სხვადასხვაგვარი ინფორმაციისა იწვევს შენახვის სტრუქტურის გართულებას, ძნელდება დაშვება მონაცემებთან და საჭიროებს ეფექტურ ზომებს მთლიანობის და უტყუარობის უზრუნველსაყოფად, როგორც საკუთრივ მონაცემებისა (საგნობრივი არის ინფორმაციული ელემენტებისა), ასევე მათ შორის კავშირებისა (ურთიერთობისა).

შეზღუდული მოხმარების ინფორმაციის დამუშავების, შენახვის ან გადაცემისას გამოიყენება ისეთი მექნიზმები და საშუალებები, რომლებიც ერთდროულად უზრუნველყოფენ დაცულობის საჭირო დონეს და

აკმაყოფილებენ შეზღუდვებს. ამ საშუალებების დაპროექტების და ექსპლუატაციის ღირებულებაზე. ამ მაჩვენებლების ოპტიმალური მნიშვნელობები, რომლებიც მიიღწევა დაცვის საშუალებების გარკვეული ნაკრებისას, წარმოადგენენ დასაბუთებას, ამ ნაკრების გამოსაყენებლად ინფორმაციის დასაცავად სისტემაში ან ქსელებში.

მმბსა და მმბდ–ს აგებისას დამუშავებულია სპეციფიკაციების ფორმები, რომლებიც მოიცავენ უსაფრთხოების პოლიტიკის დამუშავების პროცესს, ასევე ყველა მმბ სტრუქტურის და შემადგენლობის დამუშავების პროცესებსაც ინფორმაციის ერთჯერადი შეტანისა და მონაცემთა მეტად აღწერის მრავალჯერადი გამოყენების პრინციპებზე. მომხმარებლის ყველა მოთხოვნები კრიტიკული მონაცემების დამუშავებაზე და მოთხოვნები სისტემისადმი, რომელმაც უნდა უზრუნველყოს ინფორმაციის მთლიანობა, კონფიდენციალობა, ხელმისაწვდომობა სპეციფიცირებულია და შეტანილია როგორც დაცვის სამი ტიპის ფუნქციონალურ ფაილებში: კლასიფიკატორები; ლექსიკონები; ცნობარები.

ამრიგად, შექმნილმა მბ უნდა უზრუნველყონ დაცვის ტექნოლოგიის საიმედო ფუნქციონირება, მაგრამ უნდა გავითვალისწინოთ, რომ ისინი თვითონაც შეიძლება გახდნენ ბოროტგანმზრახველთა შეტევების ობიექტები. ყოველი მბ გამოყენების სპეციფიკიდან გამომდინარე ჩამოყალიბებულია მოთხოვნები მექანიზმებისადმი არასანქცირებული დაშვებისაგან დასაცავად მათი მოდელირებისას:

მბკგ–თვის მხარდაჭერილი უნდა იყოს ინფორმაციის ხელმისაწვდომობა, ვინაიდან მასში ინახება ყველა ის მონაცემები, რომლებიც საჭიროა კრიპტოგარდასახვის ამოცანის გადასაწყვეტად.

მბმდ–თვის აუცილებელია შენარჩუნებულ იქნას კონფიდენციალური მონაცემები სანქცირებული დაშვების შესაძლებლობების შესახებ (საიდენტიფიკაციო სახელები, სუბიექტების და ობიექტების, ობიექტების მომხმარებლების კატეგორიები და მათი უფლებამოსილებათა პროფილები, დაშიფვრის გასარებები მომხმარებლის აუდენტიფიკაციისათვის და ა.შ.)

ე) დაცვის მართვის გადაწყვეტის მეთოდი.

ინფორმაციის დაცვის უზრუნველყოფისათვის აუცილებელი საშუალებების მართვის მოდელირებისას უნდა განისაზრვროს სახარჯი რესურსების შემდგენლობა და სტრუქტურა და მთავარი, შემდგომი ოპტიმალური (მიზანშეწონილი და რაციონალური) გამოიყენება

გამოყოფილი რესურებისა. მოდელი მოიცავს პარამეტრების ერთობლიობას, რომლებიც განსაზღვრავენ ინფორმაციის დაცულობის მაჩვენებლების მნიშვნელობას, და ნავარაუდევია, რომ მონაცემთა დაცვის სისტემის მართვისათვის აუცილებელია ოპტიმიზირებულ იქნას:

- დაცვის უზრუნველყოფის ღირებულება;

- დაცვის სისტემის ეფექტურობა;

- დაცვისათვის გამოყენებული ყველა მეთოდების გატეხვის (დაძლევი) ალბათობები და ღირებულება;

- დაცვის ყველა მეთოდის გატეხვით მიყენებული ზარალის სიდიდე.

არასანქცირებული დაშვებისაგან დაცვის ვარიანტების მოდელირება გულისხმობს განსაზღვრას დაცვის მეთოდების ოპტიმალური შერჩევისა ყოველი კონკრეტული ობიექტისა და სისტემისათვის მთლიანობაში. ოპტიმალურობა მიიღწევა ყოველი კონკრეტული ობიექტებისათვის დაცვის მეთოდების ღირებულებით მახასიათებლების თანაფარდობებით დაცვის ყოველი მექნიზიმის გატეხვის ალბათობასთან.

ვ) შემოთავაზებული მეთოდების განსხვავება და უპირატესობები.

წარმოდგენილი დაცვის მრავალდონიან მოდელში, რომელიც ახორციელებს სხვადასხვა ხარისხის კონფიდენციალურობას ინფორმაციასთან დაშვების სამანდატო კონტროლს, რეალიზებულია დაშვების უფლებათა გაფართოების სია და დაშვების უფლების მართვა მომხმარებლის შემოსული მოთხოვნის უფლების რეალიზაციით, არსებული ნორმატიული დოკუმენტების და ორგანიზაციული ტიპის განაწილებულ მბ–ებში კრიტიკული ინფორმაციის დამუშავების წესების დაცვით. დამუშავებულია დაცვის სუბიექტების და ობიექტების იერარქიების გამოყოფის პროცედურები, აგრეთვე (ობიექტების) – ობიექტების მფლობელების ქვესიმრავლისა, დანაწილების ინტერფეისის ნდობით აღჭურვილი და სისტემის მოშორებულ აბონენტებს შორის.

კრიპტოგრაფიული დაცვის სისტემა, რომელიც ინტეგრირებულია დაშვების მანდატურ გამიჯვნასთან, საშუალებას იძლევა მიცემულ იქნას საიმედოობის მახასიათებლები კრიპტოგარდასახვისა შენახული ან გადასაცემი ინფორმაციის საიდუმლოობის ხარისხის მიხედვით.

შემოთავაზებული ალგორითმების მაღალი კრიპტომდგრადობა საშუალებას იძლევა უზრუნველყოფილი იქნას შეზღუდული მოხმარების

ინფორმაციის კონფიდენციალობა და მთლიანობა მისი შენახვის და ღია კავშირის არხებით გადაცემას.

მბ ოპტიმალური სტრუქტურების მოდელების მეთოდოლოგიების და ამ სფეროში მომუშავე წამყვანი სპეციალისტების ნაშრომების ანალიზმა გვიჩვენა, რომ თანამედროვე საპროექტო გადაწყვეტები მხარს არ უჭერს დაცვის ბევრ მნიშვნელოვცან ფუნქციებს, მაგალითად მომხმარებლების აუდენტიფიკაციას.

დაპროექტებული ოპტიმალური სისტემები მბ დაცვის არასანქცირებული დაშვებებისაგან საშუალებას იძლევა ფორმალიზებულ იქნას, ალგორითმიზებულ უნდა იქნას და უმეტეს შემთხვევაში ავტომატიზებულ იქნას მბ დაცვის ოპტიმალური მექნიზმების და სისტემების პროექტირება. დამუშავებული მოდელები და მეთოდები ითვალისწინებენ მბ მომხმარებლების საგნობრივი არის თავისებურებებს და აპარატურულ–პროგრამული პლატფორმების მახასიათებლებს, ინფორმაციული რესურსების საიდუმლობის დონის მიმართ მოთხოვნებს და კონფიდენციალურ ინფორმაციასთან მომხმარებლის დაშვების უფლებებს. თმბ სტრუქტურების ოპტიმიზაცია საიმედოობისა და უტყუარობის კრიტერიუმების მიხედვით იძლევა დამატებით დაცვას არასანქცირებული დაშვებებისაგან.

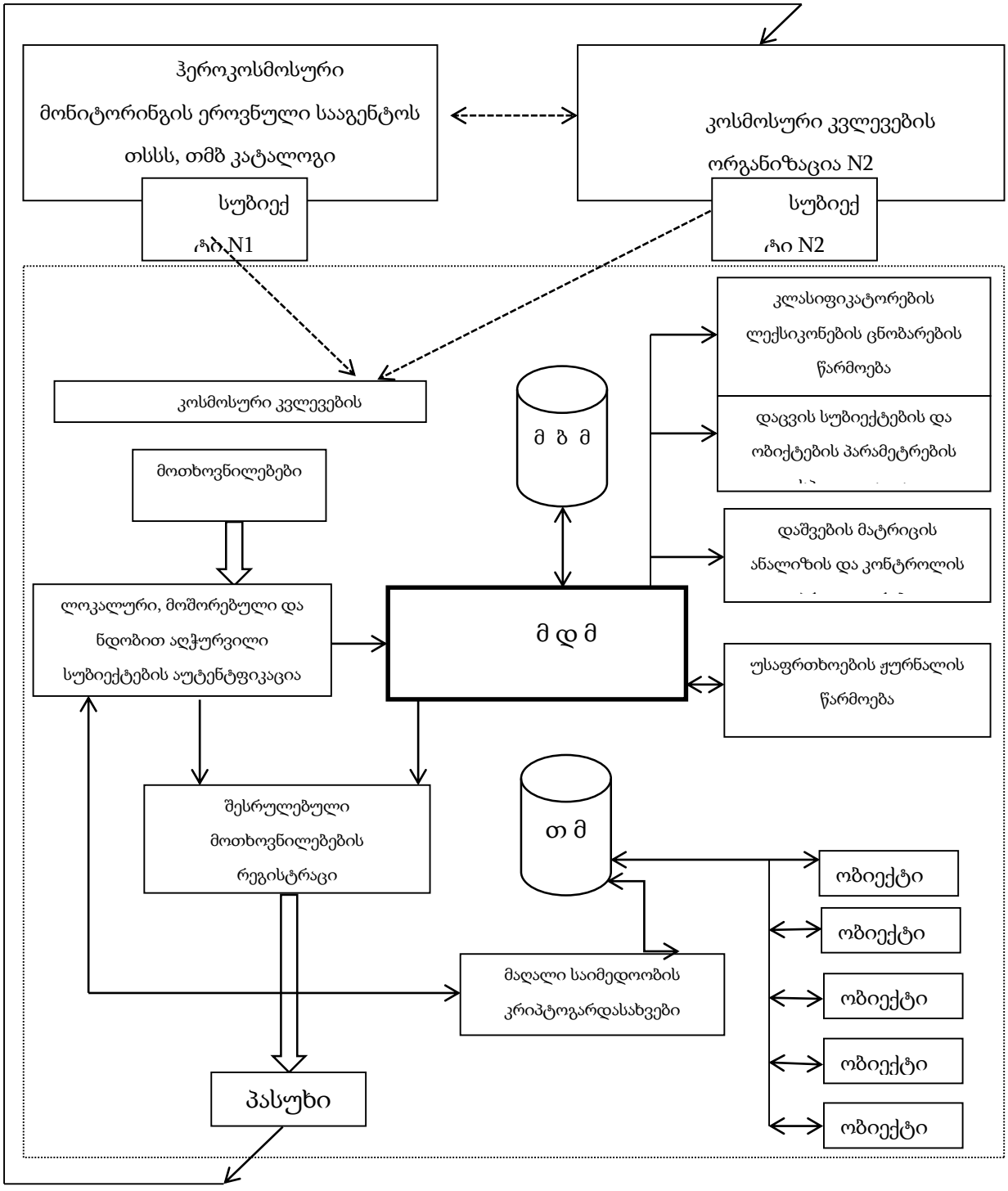
ზ) გამოყენების სფეროები და დანერგვის პერსპექტივები.

განვიხილოთ სახელმწიფო ტერიტორიის მონიტორინგის თანამგზავრული საინფორმაციო-საკომუნიკაციო სისტემის (თსსს) შექმნისა და მისი უსაფრთხოების უზრუნველყოფის საკითხი. თსსს შექმნა, ზოგადად, ითვალისწინებს სახელმწიფოს ტერიტორიის ზედაპირის მონიტორინგისას თანამგზავრებიდან დისტანციური ზონდერების მონაცემების მიღებას და დამუშავებას. მიღებული თემატური პროდუქტები გროვდება, ინახება და გადაეცემათ დაინტერესებულ ორგანიზაციებს ქსელის მეშვეობით და ოპტიკურ მატარებლებზე.

სავსებით შესაძლებელია აეროკოსმოსური მონიტორინგის ეროვნულ სააგენტოში ან კომიტეტში (ასეთი სააგენტო დღეს მრავალ სახელმწიფოშია შექმნილი, მათ შორის საქართველოშიც) ორგანიზებულ იქნას მმეტამონაცემების ბაზები (მმბ), რომელიც შეიცავს კატალოგიზირებული ინფორმაციის აღწერას ყველა თმბ-ზე, რომლებიც ტერიტორიულად

განთავსებული იქნება ორგანიზაციებში, რომლებიც დაკავებული არიან კოსმოსური კვლევებით სახელმწიფო პროგრამის ფარგლებში.

ინფორმაციული უსაფრთხოების შემოთავაზებული ორგანიზაცია ითვალისწინებს ინფორმაციის დაცვას თმბ-თან დაშვების მრავალდონიანი კონტროლის რეალიზაციით კოსმოსური ინფრასტრუქტურის კორპორაციულ ქსელში, კონფიდენციალური ინფორმაციის კრიპტოგრაფიული დახურვით, გადასაცემი მონაცემების მთლიანობის შემოწმებით და თსსს აბონენტების ავტორიზაციის უზრუნველყოფით, კოსმიური ინფრასტრუქტური კორპორაციულ ქსელში დაშვების გამიჯვნის მრავალდონიანი სისტემა წარმოდგენილი ნახ. 13. თემატური მონაცემთა ბაზები აგროვებენ საკმაოდ დიდ მოცულობას.



ნახაზი 11.კოსმოსური ინფრასტრუქტურის კორპორაციულ ქსელში დაშვების გამიჯვნის მრავალდონიანი სისტემა.

ინტეგრირებული ინფორმაციისა (ტოპოგრაფიული რუკები, გრაფიკი, ანალიზური ცნობარები, დიაგრამები, დოკუმენტები), რომლებიც ეხება სხვადასხვა თემატურ მიმართულებებს და გააჩნია კონფიდენციალობის სხვადასხვა დონე. აღნიშნული ინფორმაცია განკუთვნილია სხვადასხვა მომხმარებლისათვის და გადანაწილებულია ქსელის სხვადასხვა მოწყობილობებში ან კვანძებში. გათვალისწინებულია ორი ტიპის მოთხოვნილებების ფორმირებისა სახელმწიფოს ტერიტორიის მონიტორინგის თემატურ პროდუქტებთან:

მომხმარებელი - მოსარგებლე აფორმირებს მოთხოვნილებას თმბ კატალოგთან ინფორმაციული რესურსების მართვის ცენტრში (ირმც), სადაც სუბიექტის მოთხოვნილების პროფილის შესაბამისად ხორციელდება მოთხოვნილი თმბ მისამართის ძებნა. თუ ეს ირმც საკუთრებაა, მაშინ მოცემული თმბ ელექტრონულ ან ნაბეჭდი სახით გადაეცემა მომხმარებელს (რეკლამისათვის, სარეალიზაციოდ და ა.შ.).

მოსარგებლე აფორმირებს მოთხოვნას პირდაპირ თმბ-თან და მისი უფლებამოსილებით დონის ვერიფიკაციისაგან დამოკიდებულებით, მოთხოვნილებების დამუშავების შედეგებს მდმ თავიდან გადასცეს თსსს, სადაც ხდება მათი აწყობა, გაერთიანება და ვერიფიკაცია, ხოლო შემდეგ გაერთმთლიანებული ინფორმაცია გადაეცემა მომხარებელს.

აქ სავსებით შესაძლებელია დამუშავდეს კონკრეტული პროგრამების კომპლექსური უსაფრთხო დაშვების მონიტორის სახით, რომელიც უზრუნველყოფს უსაფრთხო დასვების სხვადასხვა კატეგორიის ინფორმაციასთან, რომელიც განსაზღვრავს გაიცეს თუ არა ნებართვა სუბიეტის მიერ წარმოდგენილი მოთხოვნილი სახის დაშვებაზე ობიექტთან და არსებობას უფლებისა მოთხოვნილი სახის დაშვების რეალიზაციაზე. თუ ეს პირობები სრულდება, მაშინ ეს დაშვება განხორციელდება სხვანაირად, უნდა აიკრძალოს და უნდა დაფიქსირდეს წარმოდგენილი სახის მოთხოვნილება როგორც მცდელობა არასანქცირებული დაშვებისა.

მდმ მოიცავს შემდეგი ქვესისტემების ერთობლიობას:

- ყველა ტიპის მომხმარებლების (დაცვის სუბიექტების) ინტერფეისების და აუტენტიფიკაციის ორგანიზაცია;
- სპეციფიკაცია დაცვის ობიეტების და სუბიექტების და მართთვის შესაბამისი საიდუმლოობის დონის და ნდობის ხარისხის მინიჭება;

- ფორმირება დაშვების გამიჯვნის წესებისა ქვეყანაში მიღებული შეზღუდულის გამოყენების ინფორმაციასთან მუშაობის პროცედურების შესაბამისად;
- მართვა დაშვების უფლებების და ფლობა დაცვის ობიექტების და მოთხოვნილებათა რეალიზაციის უფლების;
- დაშვების მატრიცის ფორმირება წყვილის „სუბიეტი-ობიექტი“ ნებადართული დაშვების სახით მოდიფიკაციის და კორექტირების ფუნქციებით;
- ინფორმაციის მაღალი ხარისხის საიმედოობით კრიპტოგრაფიული გარდასახვა ღია კავშირის არხებით გადასაცემად;
- მდმ კლასიფიკატორების და ცნობარების წარმოება;

რეგისტრაცია შესრულებული მოთხოვნილებების და ინფორაციულ რესურსებთან არასანქცირებული მომართვების მცდელობების.

ლოკალური, მოშორებული და ნდობით აღჭურვილი აბონენტების აუტენტიფიკაცია ხორციელდება ნამდვილობის დამადასტურებელი ფუნქციით პაროლის საფუძველზე, რომელიც ინახება დაშიფრული სახით, რაც მნიშვნელოვნად ამცირებს მის გახსნის რისკს. ფაილები, რომლებიც ინახება პაროლი და ობიექტის საიდუმლოობის გრიფის და სისტემის სუბიექტების დაშვების შესახებ ინფორმაცია, ასევე დაცული არასანქცირებული დაშვების მცდელობისაგან.

ამრიგად, შემოთავაზებული კონცეფცია გულისხმობს დაცვის ინტეგრირებული სისტემის შექმნას, დაწყებული თმბ პროექტირებით, რომლებიც შეიცავენ სხვადასხვა ხარისხის კონფიდენციალობის ინფორმაციას და დამთავრებულ მსგავს ინფორმაციულ რესურსებთან სხვადასხვა უფლებამოსილების დონის მქონე მომხმარებლების დაშვების ორგანიზაციით. დაშვების მანდატური გამიჯვნა საშუალებას იძლევა ავტომატიზებულ იქნას დამუშავება მოთხოვნებისა, რომლებიც განსაზრვრულია სახელმწიფოს შესაბამისი დოკუმენტებით (ან დოკუმენტით) საიდუმლოების რეჟიმის უზრუნველყოფაზე. თმბ ოპტიმალური სტრუქტურების პროექტირება, არასანქცირებული დაშვებებისაგან დაცვის თვალსაზრისით, მიმართულის რეაქციის დროს შესამცირებლად ინფორმაციის დამუშავებისას მომხმარებლების მოტხოვნილებებზე პასუხების ფორმირებისას თმბ-დან ამორჩევის დროის შემცირების ხარჯზე.

დღეს არსებული სამეცნიერო ნაშრომებში წარმოდგენილია უსაფრთხოების მუქარების მთელი რიგი კლასიფიკაციებისა, რომლებიც ასახავენ განსახილველი პრობლემის ამა თუ იმ ასპექტებს [1-5]. აღნიშნული ნაშრომების საფუძველზე განხორციელებული ინფორმაციული რესურების მუქარების განზოგადოებული კლასიფიკაციის სქემა წარმოდგენილია ნახ.14-ზე. წარმოდგენილ სქემაში წყაროების დაყოფა სუბიეტურებად და ობიექტურებად გამართლებულია გამომდინარე მოსაზრებიდან ბრალის განსაზღვრისა ინფორმაციისათვის ზარალის მიყენების გამო. ხოლო დაყოფა შიდა და გარეშე წყაროებად გამართლებულია იმით, რომ ერთი და იგივე მუქარისათვის მოგერიების მეთოდები შიდა და გარეშე წყაროებისათვის შეიძლება იყოს სხვადსხვა.

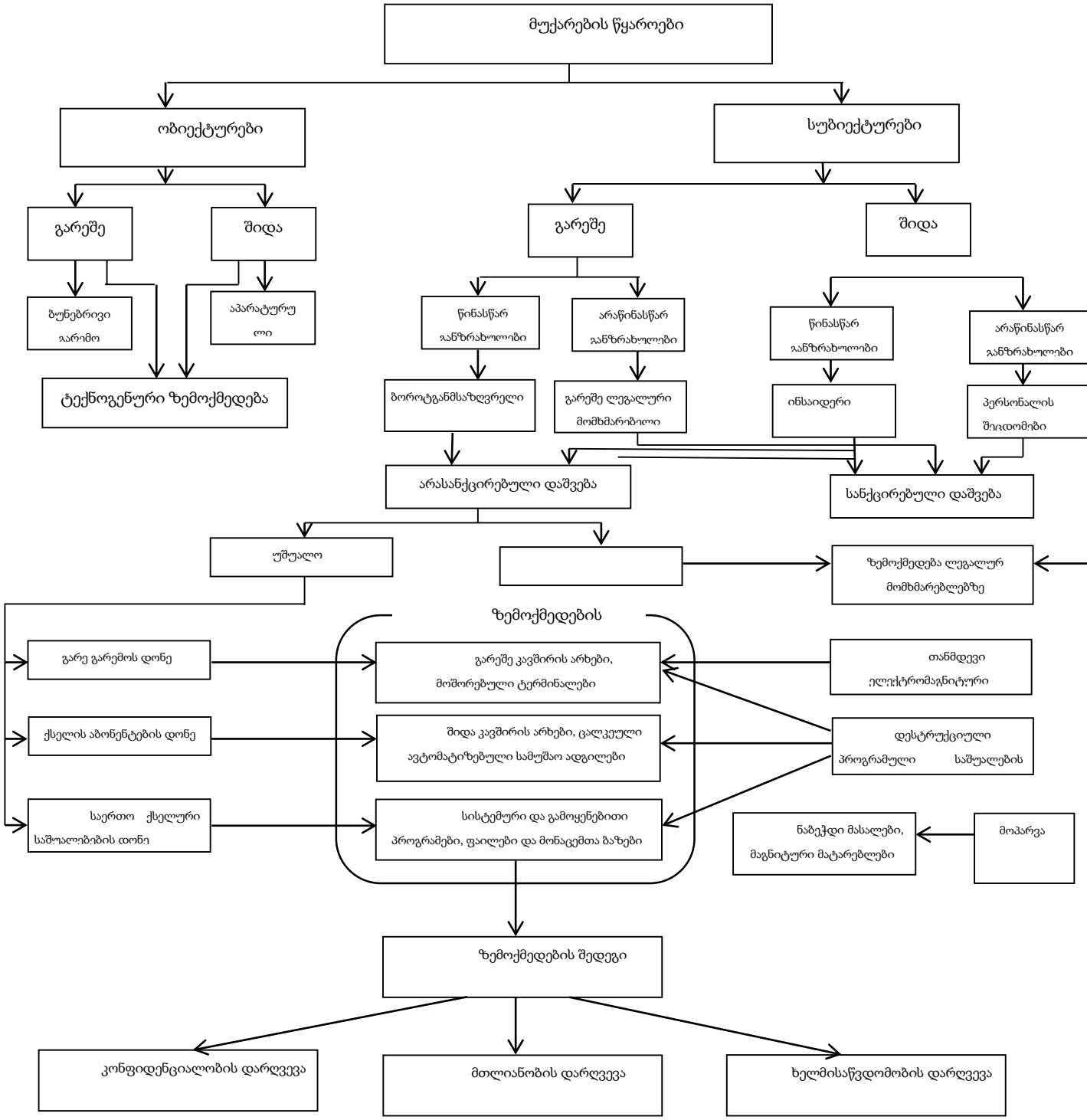
ნახაზი 14. ინფორმაციული რესურსების მუქარების კლასიფიკაცია

Eecutive Information Network განხორციელებული გამოკვლევების მოანცემებით [5] შემთხვევების 80%-ში მუქარების მატარებელია ადამიანი. შემთხვევითი მუქარების (ოპერატორის შეცდომები) შეადგენენ 55% საერთო რაოდენობიდან, წინასწარ განზრახულ მუქარებზე მოდის 25% და სტიქიურ მოვლენებზე მოდის 20%.

მოყვანილი მონაცემები მიგვანიშნებს იმაზე, რომ ძირითადია მუქარები, რომლებიც განპირობებული არიან სუბიექტების მოქმედებებით (ანტროპოგენული წყაროები მუქარების), შემდეგ მოდის მუქარები, რომლებიც განპირობებული არიან ტექნიკური საშუალებებით (მუქარების ტექნოლოგიური წყაროები) და მუქარები, რომლებიც მომდინარეობენ სტიქიური წყაროებიდან (მუქარების ბუნებრივი წყაროები)

სუბიექტები (წყაროები), რომელთა მოქმედებებმა შეიძლება გამოიწვიონ ინფორმაციის უსაფრთხოების დარღვევა, შეიძლება იყვნენ როგორც გარეშეები, ასევე შიდა.

მუქარის გარეშე სუბიექტი-წყაროები, თავის მხრივ შეიძლება იყვნენ არაწინასწარგანზრახულები (შემთხვევითები) ან წინასწარგანზრახულები და გააჩნდეთ კვალიფიკაციის სხვადსხვა დონე. მათ განეკუთვნებიან: კრიმინალური სტრუქტურები, პოტენციური დამნაშავეები და ხაკერები, არაკეთილსინდისიერი პარტნიორები, ტექნიკური პერსონალი ტელესაკომუნიკაციო მომსახურების მომწოდებლებისა, წარმომადგენლები საზედამხედველო ორგანიზაციების და ავარიული სამსახურების, ძალოვანი სტრუქტურების წარმომადგენლები.



ნახაზი 12. ინფორმაციული რესურსების მუქარების კლასიფიკაცია.

შიდა წყაროები, როგორც წესი, არიან მაღალი კვალიფიკაციის სპეციალისტები პროგრამული უზრუნველყოფის და აპარატურული საშუალებების დამუშავებისა და ექსპლუატაციის სფეროში იცნობენ

ინფორმაციის დაცვის პროგრამულ-აპარატურული საშუალებების გადასაწყვეტი ამოცანების სპეციფიკას, სტრუქტურას, ძირითად ფუქციებს და მუშაობის პრინციპებს, გააჩნიათ შესაძლებლობა გამოიყენონ საშტატო მოწყობილობები. მათ განეკუთვნებიან: ძირითადი პერსონალი (მომხმარებლები, პროგამისტები, დამპროექტებლები); ინფორმაციის დაცვის სამსახურის წარმომადგენლები, დამხმარე პერსონალი (ყარაულები, დამლაგებლები); ტექნიკური პერსონალი (საინჟინრო ქსელების ექსპლუატაცია).

ნაშრომში [6] მოყვანილია სამაგალითო სია პერსონალის და შესაბამისი საფრთხის ხარისიხი მისი მოქმედებებისა:

- ყველაზე მეტი საშიშროება; უსაფრთხოების ადმინისტრატორი;

- გაზრდილი დონე საშიშროებისა; სისტემის ოპერატორი, მონაცემთა შეტანისა და მომზადების ოპერატორი, სისტემური პროგრამისტი;

- საშუალო დონე საშიშროებისა: სისტემის წამყავნი ინჟინერი, წამყვანი ინჟინერი, პროგრამულ უზრუნველყოფაში;

- შეზღუდული დონე საშიშროებისა: გამოყენებითი პროგრამისტი, კაბშირგაბმულობის ინჟინერი ან ოპერატორი, მონაცემთა ბაზების ადმინისტრატორი, მოწყობილობების ინჟინერი,პერიფერიული მოწყობილობების ოპერატორი, მომხმარებელ-პროგრამისტი;

- დაბალი დონე საშიშროების: პერიფერიული მოწყობილობების ინჟინერი, გამოყენებითი პროგრამების ბიბლიოთეკარი.

ამრიგად, მომხამრებლები ინფორმაციული სისტემის და მისი მომსახურე პერსონალი, ერთის მხრივ წარმოადგენენ შემდგენელ ნააწილს, აუცილებელ ელემენტს ის, მეორეს მხრივ - ძირითად მიზეზს და მამოძრავებელ ძალას დარღვევებისა უსაფრთხოების სფეროში. ამ დროს მუქარების ანტროპოგენული წყაროების კვალიფიკაცია თამაშობს მნიშვნელოვან როლს უსაფრთხოებაზე მათი გავლენის შეფასებაში.

განსაკუთრებულ ჯგუფს, შიდა ანტროპოგენური წყაროებს ქმნიან პიროვნებები მოშლილი ფსიქიკით და სპეციალურად ჩანერგილი და გადაბირებული აგენტები, რომლებიც შეიძლება იყვნენ ძირითადი, დამხმარე და ტექნიკური პერსონალიდან, ასევე ინფორმაციის დაცვის სამსახურის წარმომადგენლები. მოცემული ჯგუფი განიხილება ზემოთ ჩამოთვლილი მუქარით წყაროების შემდგენლობაში, მაგრამ შეტევათა

აცილების მეთოდებისა, რომლებიც მომდინარეობენ ამ ჯგუფებიდან, შეიძლება გააჩნდეთ საკუთარი განსხვავებები.

ანტროპოგენული ფაქტორების არსებობას მივყავართ იმასთან, რომ ინფორმაციის დაცვის სისტემის (იდს) მახასიათებლები ხდებიან არა მკაცრად განსაზღვრულები: კავშირები ქვესისტემებს შორის აღიწერებიან არამკაფიოდ, ღიად რჩება საკითხი საწყისი მონაცემების რაოდენობასა და შემდგენლობაზე, რამდენადაც არაა ცნობილი, რამ შეიძლება მოახდინოს გავლენა ადამიანის როგორც, სისტემის ელემენტების ქცევაზე და ა.შ. მნიშვნელობების უმეტესობა შემავალი და გამომავალი ფაქტორებისა სოციოტექნიკურ სისტემაში (სტს), რომლის მკაფიო მაგალითს წარმოადგენს სისტემა ინფორმაციული უსაფრთხოების კომპლექსური უზურნველყოფისა (იუკუ), რიცხობრივად არაა გაზომილი. ამ დროს ადამიანი გვევლინება არა მარტო პიროვნების სახით, რომელიც იღებს გადაწყვეტილებას (გვპ), არამედ თვითოვე წარმოადგენს მართვის ობიექტს. მმართველი ზემოქმედების დონე (ძალა) ასევე განისაზღვრება არა მაკაფიოდ. ძნელად ამოსაცნობია წინასწარ მმართველობითი ზემოქმედების ეფექტური სისტემის ანტროპოგენურ ელემენტებზე. ამის გარდა, რამდენადაც სისტემის მიზანი გმპ მიერ ფორმირება ხარისხობრივად ან არამკაფიოდ, ამას მივყავართ მის „გაბუნდოვანებამდე“ გაურკვევლობამდე, „დასაშვები დიაპაზონის“ გაჩენამდე, მის მიღწევამდე. და თუ გაურკვევლობის გახსნისათვის სტს ტექნიკური ქვესისტემის გამოკვლევისა გამოყენებადია მათემატიკური სტატისტიკის კლასიკური მეთოდები, მაგრამ ანტროპოგენული შემადგენლისათვის ისინი გამოუსადეგარია, ვინაიდან ამ შემთხვევაში გაურკვევლობა ატარებს სუბიექტურ ხასიათს.

განსხვავებით ობიექტური ალბათობისაგან, რომელიც ასახავს ფარდობით სიხშირეს, რაც მოვლენებისა დაკვირვებათა საერთო მოცულობაში, სუბიექტური ალბათობის ქვეშ მოიაზრება რომელიღაც ადამიანის ან ადამიანთა ჯგუფის (ექსპერტები) დარწმუნებულობის ზომაში. იმაში, რომ მოცემულ მოვლენას ნამდვილად ექნება ადგილი. სუბიექტური ალბათობა შეიძლება ფორმალურად წარმოდგენილ იქნა სხვადასხვა ხერხებით. უფრო ხშირად მისი წარმოდგენა ხდება როგორც ალბათური საზომი მოვლენათა სიმრავლეში, მიღებულია ექსპერტული გზით [7].

სუბიექტური ალბათობა სისტემური ანალიზის სფეროში მეცნიერულ ნაშრომებში არა უბრალოდ წარმოდგენილია როგორც, ზომა

დარწმუნებულობისა მოვლენათა სიმრავლეზე, არამედ მიბმულია გმპ მჯობინების სისტემასთან და საბოლოო ჯამში სარგებლიანობის ფუნქციასთან, რომელიც ასახავს მის მჯობინებას ალტერნატივათა სიმრავლეზე.

იუ-ს კომპლექსური უზურნველყოფის შემთხვევაში ეს ნიშნავს, რომ ალგორითმი ინფორმაციული აქტივის IAM წინააღმდეგ UG_n მუქარის აპრიორული ალბათობის მნიშვნელობის UG^m საპოვნელად დამოკიდებულია იმაზე, თუ რომელ მუქარათა ტიპს განეკუთვნება UG_n.

ობიექტური მუქარების, რომლებიც გამოწვეულია ტექნოლოგიური ან სტიქიური (ბუნებრივი) წყაროებით, შემთხვევაში შეიძლება გამოყენებულ იქნას სტატისტიკური ანალიზის ან სკალირების მეთოდები, რომლის გამოყენების შემთხვევაში ყოველი სიხშირეს გარკვეული მუქარის წარმოშობისა შეიძლება შესატყვისობაში დაესვას რაღაც მნიშვნელობა სიმრავლიდან ლინგვისტური ცვლადისა „მუქარის წარმოშობის ალბათობა“. მაგალითად თუ სიხშირე მუქარებისა „წყალდიდობა“ არის სამ წელიწადში ერთხელ, მაშინ ლინგვისტური ცვლადის „ალბათობა წყალდიდობის წარმოშობისა“ მნიშვნელობა შეიძლება მიღებულ იქნას ტოლად „საშუალოზე დაბალი“. ამავე დროს, ინფორმატიზაციის ობიექტებზე იმავე სიხშირით ხანძრის წარმოშობა შეიძლება შეფასებულ იქნას როგორც „საშუალოზე მაღალი“.

იმ შემთხვევაში, როცა მუქარები განეკუთვნებიან სუბიექტები მუქარების კატეგორიას (ესაა მუქარები, რომლებიც დაკავშირებული არიან ანტროპოგენურ წყაროებთან), მაშინ UG_{nm} მნიშვნელობის განსაზღვრისათვის შეიძლება აიგოს არამკაფიო კოგნიტური მოდელი (აკმ) უფროს დაბალი დონის ვიდრე ობიექტის ინფორმაციული უსაფრთხოების დონის კომპლექსური შეფასება, როგორც ეს მოცემულია [8]. ასეთი იერარქიული მიდგომა საშუალებას იძლევა გამარტივდეს აკმ აგება მაღალი სირთულის სისტემებისათვის. ფაქტიურად ამ შემთხვევაში აუცილებელია აიგოს ე.წ. „დამრღვევის მოდელი“.

სწორად აგებული (რეალობის ადეკვატური) მოდელი დამრღვევისა, რომელშიც აისახონ მისი პრაქტიკული და თეორიული შესაძლებლობები, აპრიორული ცოდნა, მოტივირებულობა და ა.შ. მახასიათებლები - უმნიშვნელოვანესი, დადგენელია რისკების წარმატებული ანალიზისა და

დაცვის სისტემის შემდგენლობის და მახასიათებლებისადმი მოთხოვნის დასადგენად.

რაც შეიძლება სრულმა განხილვამ ანტროპოგენული მუქარების სიმრავლისა უნდა გაითვალისწინოს აგება ისეთი მოდელისა, ყოველი სუბიექტებისათვის, რომელსაც გააჩნია პოტენციური შესაძლებლობა ინფორმაციულ აქტივებთან დაშვებისა.

ამ დროს შეიძლება გამოიყოს დარღვევათა რამოდენიმე ძირითადი მოტივი: ვანდალიზმი; იძულება; შურისძიება; ანგარებითი ინტერესი, იდეური მოსაზრებები.

დარღვევისა, რომლებიც გამოწვეული არიან უპასუხისმგებლობით, მომხმარებელი ახორციელებს რაღაც დამანგრეველ მოქმედებას, რომელიც არაა დაკავშირებული რაიმე ბოროტ განზრახვასთან. ზოგიერთი მომხმარებლები მონაცემებთან დაშვებას თვლიან სერიოზულ დიდ წარმატებად, ახორციელებენ რა თავისებურ თამაშს „მომხმარებელი - სისტემის წინააღმდეგ“ საკუთარი პოზიციების გამყარებით საკუთარ თვალში, ან კოლეგების თვალში. უსაფრთხოების დარღვევა შეიძლება ასევე დაკავშირებული იყოს, როგორც უკვე აღვნიშნეთ, იძულებასთან (შანტაჟურ), შურისძიებასთან, იდეურ შეხედულებებთან ან ანგარებით ინტერესებთან სისტემის მომხმარებლისა. ამ შემთხვევაში ასეთი მომხმარებელი შეცდეს მიზანდასახულად გადალახოს სისტემის დაცვა რათა მიიღოს დაშვება შენახულ, გადაცემულ და დამუშავების პროცესში მყოფ ინფორმაციასთან ან სხვა ინფორმაციულ აქტივებთან. ცოდნის დონის მიხედვით დამრღვევების კლასიფიკცია შეიძლება შემდეგნაირად:

- იცის ის-ის ფუნქციური თავისებურებები, ძირითადი კანონზომიერებები მასში მონაცემთა მასივების და მიკითხვის ნაკადების ფორმირებისა, შეუძლია ისარგებლოს (გამოიყოს) საშტატო საშუალებები;
- გააჩნია ცოდნის მაღალი და გამოცდილება მუშაობისა სისტემის ტექნიკური საშუალებებთან და მათ მომსახურებაში;
- გააჩნია ცოდნის მაღალი დონე პროგრამირებისა და გამოთვლითი ტექნიკის პროექტირების და ავტომატიზირებული ის ექსპლუატაციის სფეროში;
- იცის სტრუქტურა, ფუნქციები და მოქმედების მექანიზმები დაცვის საშუალებებისა მათი ძლიერი და სუსტი მხარეები;

- შესაძლებლობათა (გამოყენებული მეთოდების და საშუალებებისა) დონის მიხედვით დამრღვევებს შეუძლიათ:
- გამოიყენონ მხოლოდ ცნობების მიღების აგენტურული მეთოდები;
- გამოიყენონ პასიური საშუალებები (ტექნიკური საშუალებები ხელში ჩაგდებისა სისტემის კომპონენტების მოდიფიკაციის გარეშე);
- გამოიყენონ მხოლოდ საშტატო საშუალებები და დაცვის სიტემის ნაკლოვანებები მის გადასახავად (არასანქცირებული მოქმედებები ნებადართული საშუალებების გამოყენებით), ასევე კომპაქტური ინფორმაციის მაგნიტური მატარებლები, რომელთა გადატანის შესაძლებელია მალულად დაცვის პოსტის გავლით;
- გამოიყენონ ზემოქმედების აქტიური მეთოდები და საშუალებები (მოდიფიკაცია და მიმართება დამატებით ტექნიკური საშუალებების, მიერთება მონაცემთა გადაცემის არხებთან, პროგრამების ჩასმა და გამოყენება სპეციალური ინსტრუმენტალური და ტექნოლოგიური პროგრამების).

შესაძლო დამრღვევების მოდელების აგებისას მახასიათებლების კონკრეტული მნიშვნელობების განსაზღვრა უმეტესწილად სუბიექტურია.

სუბიექტური დონის შესამცირებლად აკმ კონცეპტების მნიშვნელობების განსაზღვრისას, რომლებიც ასახავენ დაშვების უფლებათა დონეს, ტექნიკურ აღჭურვილობას, ფსიქოფიზიოლოგიურ შესაძლებლობებს, შეიძლება გამოყენებულ იქნას სკალირება, ექსპერტული შეფასების მეთოდით მიენიჭოს შესატყვისობაში თითოეულს თვისებათა შესაძლო ნაკრებიდან, რომელიღაც მნიშვნელობა ლინგვისტიკური ცვლადისა მისი თერმოსიმრავლიდან [9]. მაგალითად, თუ დამრღვევი იყენებს მხოლოდ შტატურ საშუალებებს და დაცვის სისტემის ნაკლოვანებებს მის დასაძლევად (ანუ ახორციელებს არასანქცირებულ მოქმედებებს ნებადართული საშუალებების გამოყენებით, მაშინ მისი აღჭურვილობის დონე შეიძლება შეაფასებულ იქნას როგორც „საშუალოზე დაბალი“, ხოლო იმ შემთხვევაში როდესაც ადგილი აქვს გამოიყენება აქტიური ზემოქმედების საშუალებების და მეთოდების (მოდიფიკაცია და მიერთება დამატებითი ტექნიკური საშუალებების, მიერთება მონაცემთა გადაცემის არხებთან, პროგრამების ჩანერგვა და გამოყენება სპეციალური ინსტრუმენტალური და ტექნოლოგიური პროგრამებისა), მაშინ დამრღვევის აღჭურვილობის დონე

ფასდება როგორც „მაღალი“. ანალოგიურად შეიძლება შეფასდეს სხვა ზემოთ ჩამოთვლილი კომპონენტების მნიშვნელობები.

შიდა პოტენციური დამრღვევების (ინსაიდერების) კომპეტენტურობის ამსახველი ფაქტორის მნიშვნელობის მისაღებად, მიზანშეწონილად მიგვაჩნია გამოყენებულ იქნას მეთოდიკა, რომელიც გამოიყენება იუ-ს სფეროში კადრების შერჩევისა და მომზადების ამოცანის გადასაწყვეტად და მოცემულია ნაშრომებში[10,11].

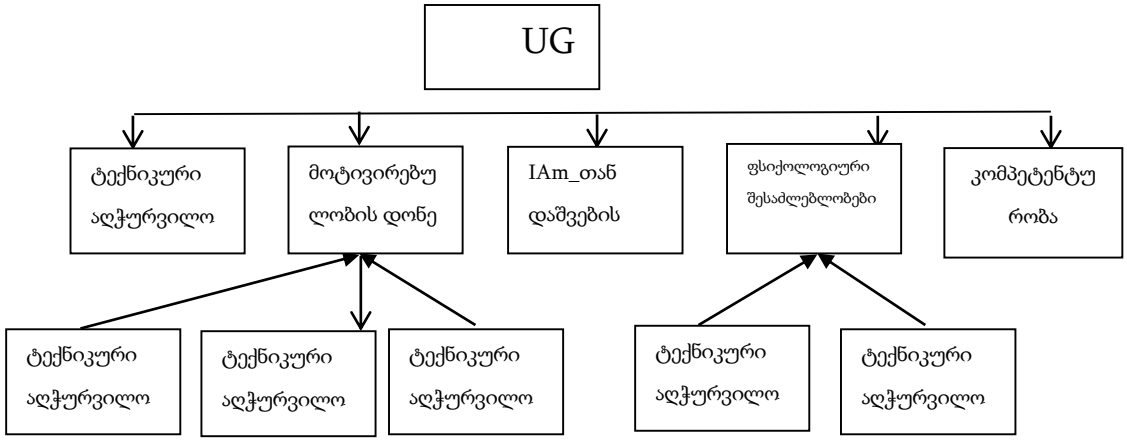
ფორმალიზებას ყველაზე უფრო ძნელად ექვემდებარება დამრღვევის მოქმედების მოტივირებულობის (მოტივაციის) ხარისხის შეფასება. ამ შემთხვევაში საჭირო ინფორმაციის მისაღებად შესაძლო მეთოდები შეიძლება იყოს ფსიქოლოგიური ტესტირება (საკუთარი თანამშრომლების) ქცევათა ანალიზის საშუალებები, აგენტურული მეთოდები, ფარული დაკვირვებები და ა.შ. [12]

გარეშე დამრღვევებისათვის ცალსახა შეფასება შეიძლება გაკეთდეს მათი ინფორმაციულ აქტივებთან დაშვების უფლებების დონის მიხედვით (დაბალი). სხვა პარამეტრებთან მიმართებაში, რომლის გამოყენებაც ხდება დამრღვევის მოდელის ფორმირებისას, აუცილებელია გაკეთდეს ვარაუდი, რომელიც ეფუძნება ცნობებს, რომლებიც მიღებულია დახმარებით აგენტურული და ანალიტიკური დაზვერვის, ანალიზისა და შეფასებით „მტრული“ გარემოცვის ხარისხისა და ა.შ.

ნაშრომში [13] წარმოდგენილი იუკუ ამოცანების გადაწყვეტისას აკმ აგების ზოგად მეთოდიკის გამოყენებით, მუქარის, რომელიც გამოწვეულია ანტროპოგენული წყაროებით აპრიორული ალბათობის განსაზღვრის მოდელი, შეიძლება წარმოდგენილი იქნას შემდეგი G გრაფის სახით (ნახ.2).

მიღებულ G გრაფს აუცილებლად უნდა დაედოს წონების S სისტემა გრაფის თითოეული რკალისთვის. ასეთი სისტემა შეიძლება მივიღოთ ექსპერტული გზით, მაგალითად, არამკაცრი რანჟირების მეთოდის დახმარებით როდესაც გრაფს დაედება ფარდობები არამკაცრი მჯობინებისა ერთი ფაქტორებისა მეორეს მიმართ იმისდა მიხედვით თუ როგორია მათი გავლენა იერარქიის შემდეგი (მომდევნო) დონის მოცემულ ელემენტზე [8].

აღნიშნული მეთოდით მიღებული შეფასებები წარმოადგენს განზოგადოებას წონების სისტემისა მჯობინებათა შერეული განაწილების შემთხვევისათვის, როდესაც სისტემაში შემოდიან მჯობინებებთან ერთად დამოკიდებულებათა განურჩევლობაც[14].



ნახაზი 13. აკმ ანტროპოგენული მუქარების აპრიორული ალბათობის განსაზღვრისათვის.

წონები ფიშბერნისა ასახავენ იმ ფაქტს, რომ სისტემას კლებადი მჯობინებით N ალტერნატიკებისა ყველაზე უკეთესად პასუხობს სისტემა არითმეტიკული პროგრესიის წესით კლებადი წონებისა. ამიტომ ეს წონები წარმოადგენენ რაციონალური წილადები, რომელთა მნიშვნელია ჯამი N ნატურალური რიგის პირველი წევრებისა (არითმეტიკული პროგრესიის ბიჯით 1), მრიცხველთა -ერთეული კლებადი ელემენტები ნატურალური რიგისა, N-დან 1-მდე (მაგალითად, 3/6,2/6,1/6), ანუ ფიშბერნის მიხედვით მჯობინება გამოიხატება კლებაში ერთიანით წონითი კოეფიციენტის რაციონალური წილადის მრიცხველის უფრო სუსტი ალტერნატივისა..

ამრიგად, სუბიექტური (ანტროპოგენული) მუქარის დონის შეფასების მოდელად შეიძლება მიღებულ იქნას კორტეჟი:

UGS= < G, QL, S, R, SL >

სადაც G - ორიენტირებული გრაფია, რომელსაც გააჩნია ერთი ძირეული მწვერვალი და არ შეიცავს ჰორიზონტალურ რკალებს იერარქიის ერთ დონეზე;

QL - ნაკრები ხარისიხობრივი შეფასებებისა თითოეული ფაქტორის იერარქიაში (ლინგვისტური ცვლადი);

S - სიმრავლე წონებისა G გრაფის რკალიების, რომლებიც ასახავენ კონცეპტების გავლენას ხარისხსს მოცემულ ელემენტზე იერარქიის მომდევნო დონისა;

R - ნაკრები წესებისა კონცეპტების მნიშვნელობების გამოსათვლელად G იერარქიის ყოველ დონეზე;

SL - ინდექს მსგავსებისა, რომელიც საშუალებას იძლევა ამოცნობილ იქნას კონცეპტების ლინგვისტური მნ იშვნელობები.

თავის მხრივ G ასევე წარმოადგენს კორტეჟს:

$$G =< \{GFij\}:\{GDij\}>$$

სადაც {GFij} - სიმრავლეა გრაფის მწვერვალებისა (ფაქტორების ან კონცეპტების S კმ ტერმინოლოგიაში);

{GDij} - სიმრავლე რკალებისა, რომლებიც აერთიანებენ i-ურ და j-ურ მწვერვალებს (სიმრავლე მიზეზ -შედეგობრივი კავშირებისა კონცეპტებს შორის).

იერარქიის მომდევნო დონეზე მნიშვნელობების გამოსათვლელად, როცა ცნობილია უფრო დაბალი კონცეპტების მნიშვნელობა განსაზღვრულობის ტერმინებში ლინგვისტური ცვლადებისა D2 = {დაბალი(დ), საშუალოზე დაბალი (სდ), საშუალო (ს), საშუალოზე მარალი (სმ), მაღალი (მ)}, და რკალების წონების მოცემული მნიშვნელობებისას S საჭიროა აგრეგირებულ იქნას გავლენა ქვემოთ მდგომი კონცეპტებისა მიხედვით წესებისა Ri სიმრავლიდან R. სიმრავლის R ელემენტებს შეიძლება წარმოადგენენ მულტიპლიკაციური ადიტიური, მინიმაქსური და სხვა სახე ნახვევებისა, რომლებიც განისაზღვრებიან კონცეპტრების ერთმანეთზე ზეგავლენის სპეციფიკთ.

უნდა შევნიშნოთ, რომ ზოგიერთი მაჩვენებლის მნიშვნელობების ხვეულებისა აუცილებელია წინასწარ ინვერტირებულ იქნას, რამდენადაც მოცემული კონცეპტების გავლენა ფაქტორებზე უფრო მაღალი დონისა შეიძლება იყოს უარყოფითი.

ზოგად შემთხვევაში F ფაქტორის მნიშვნელობის ინვერსიის საპოვნელად შეიძლება გამოვიყენოთ სტანდარტული ფორმულა:

Inv (F) = 1-M(F)

სადაც M(F) -ესაა ფუნქცია კუთვნილებისა არამკაფიო რიცხვის, რომელივ შეესაბამება F ფაქტორის მნიშვნელობას.

თერმ-სიმრავლისათვის Q2 კუთვნილების ფუნქციის ოჯახის სახით შეიძლება გამოიყენოთ სტანდარტული ხუთდონიანი 01 -კლასიფიკატორი [IS];

{დ (0;0;0,15;0,25); სდ (0,15;0,25;0,35;0,45); ს(0,35;0,45;0,55;0,65);

სმ (0,55;0,65;0,75;0,85); მ (0,75;0,85;1;1)},

სადაც არამკაფიო რიცხვში X (a_1 a_2 a_3 a_4) a_1 და a_4 - აბცისებია ტრაპეციის ქვედა საფუძვლისა, ხოლო a_2 და a_3 - აბცისებია ზედა საფუძვლისა.

ლინგვისტური ცვლადების შემთხვევაში ნახევის პოვნისას ორი ფაქტორის ჯამის ან ნამრავლის ქვეშ იგულისხმება ჯამი ან ნამრავლი მათი შესატყვისი არამკაფიო რიცხვებისა (4). ამ შემთხვევაში შედეგიც ასევე წარმოადგენს არამკაფიო რიცხვს, რომელიც შემდეგში ლინგვისტურად უნდა იქნას ამოცნობილი, რათა გამომუშავებულ იქნას გამსჯა მაჩვენებელთა ხარისხობრივ დონეზე. ამისათვის აუცილებელია გამოთვლით იქნას მსგავსების ინდექსი , რომელიც ახასიათებს ხარისხს შესატყვისობისა ფაქტორის მნიშვნელობისა ამა თუ იმ ხარისხობრივ შეფასებასთან ლინგვისტური ცვლადის QL თერმოსიმრავლიდან.

მსგავსების ინდექსი შეიძლება ნაპოვნი იქნას შემდეგნაირად:

$$\Omega = \frac{(1+s)}{2},$$

$$\tilde{s} = \frac{\text{Sin} - Sout}{\text{Sin+Sout}}$$

სადაც Sout - ველია არამკაფიო ტრაპეციისმაგვარი რიცხვისა, რომელიც ახასიათებს შედეგს, რომელიც დევს სტალონური რიცხვის გარეთ, ხოლო Sin - ველია, რომელიც დევს ამავე სტალონური რიცხვის შიგნით.

ასეთნაირად განსაზღვრული მსგავსების ინდექსი იცვლება რა დიაპაზონში 0-დან 1-მდე, ახასიათებდეს იქნება სიახლოვეს ნაპოვნი ნახევისა ამა თუ იმ არამკაფიო რიცხვთან, რომელიც თავის მხრივ შეესაბამება ელემენტს ეტალონური თერმასიმრავლის.

ამ დროს უზრუნველყოფილია სემანტიკური შესატყვისობა; რაც უფრო მაღალია მსგავსების ინდექსი, მით უფრო მაღალია გამოთვლილი მნიშვნელობის შესაბამისობა ერთ-ერთ ელემენტთან თერმასიმრავლისა QL.

ამრიგად, წარმოდგენილი მოდელი დამრღვევისა ითვალსწინებს სუბიექტის ის-თან დაშვების უფლებების დონეს; დამრღვევის მოქმედებების ლოიალურობის ხარისხზე, მის ფსიქოლოგიურ პორტრეტზე, დასახულ მიზნებზე, გარეშე ფიზიკური და/ან ფსიქოლოგიური ზემოქმედების (მისი ცოდნის დონე); ტექნიკური აღჭურვილობა (დამრღვევის მიერ გამოყენებულ მეთოდები და საშუალებები) და საშუალებას იძლევა შეფასდეს ინფორმაციული აქტივებისადმი სუბიექტური მუქარების დონე.

ჩატარებულმა სისტემურმა ანალიზმა საშუალება მოგვცა განგვეხორციელებინა ინფორმაციული უსაფრთხოების მუქარითა წყაროების

კლასიფიკაცია, გამოკვევლინებინა დამრღვევის მოდელის აგების პროცესის თავისებურებები. მოვეხდინა ფორმულირება მიდგომებისა ობიექტური და სუბიექტური მუქარების აპრიორული ალბათობებეის განსაზღვრისათვის. მიღებული შედეგები შეიძლება გამოყენებულ იქნას სოციოტექნიკური სისტემის იუ-ს კომპლექსური უზრუნველყოფის საერთო მოდელის ასაგებად.

3.4. ინფორმაციის ადაპტური დაცვის მოდელი

თანამედროვე ინფორმაციული ტექნოლოგიების ერთადერთი უმნიშვნელოვანესი დამახასაითებელი თავისებურებებისა არა მარტო გავრცელება–განვითარების ძალზე მაღალი ტემპი, არამედ ინფრასტუქტურული გართულება და ფუნქციური შესაძლებლობების გაფართოება, გამოთვლითი საშუალებების ინტელექტუალიზაციის ჩათვლით. საინტერესოა ის ფაქტი, რომ შეიმჩნევა გარკვეული პარალელის არსებობა ბიოსისტემების სახეობების ევოლუციას და ინფრომაციული ტექნოლოგიების (იტ) ევოლუციას შორის [1]. ბიოსისტემების განვითარება ხდება ინფორმაციული პროცესების დაცვის სრულყოფილის წყალობით, ხოლო იტ შემდგომი განვითრება შესაძლებელია იტ–სისტემების დაცვის დონის უზრუნველყოფის შემთხვევაში, რომელიც ადეკვატური იქნება ინფორმაციული ტექნოლოგიების სირთულის ზრდისა. შეიძლება არის ვარაუდი, რომ ინფორმაციული უსაფრთხოების სისტემების (იუს) დამუშავების პერსპექტიულ მეთოდს წარმოადგენს ხელოვნურ სისტემებში ბიოსისტემების ინფორმაციული პროცესის დაცვის მექანიზმები (დმ) ანალოგიების გამოყენება. შევეცდებით აღნიშნული ანალოგიების გამოყენების ადაპტური იუს ასაგებად:

- ინფორმაციული დაცვის მექანიზმებში;
- იტ–ს არქიტექტურაში;
- მემკვიდრეობის, განვითარების, ადაპტაციის და შერჩევის ევოლუციურ პროცესებში;
- ინფორმაციის განაწილებული ჭარბი ინფორმაციული ველის ფორმაში წარმოდგენისას;

პროგრამირების ინფორმაციული პროცესებისა იტ–სისტემებში ინფორმაციული ველების ფორმირების მეშვეობით, ნეირონული ქსელების (ნქ) ინტელექტუალური მექანიზმები, არამკაფიო ლოგისტიკის და გენეტიკური ალგორითმების (გა) გამოყენებით.

ლოკალური და კორპორაციული ქსელების ცნობილი იუს–ები ორიენტირებული არიან ეკონომიკურ მიზანშეწონილ ინფორმაციული უსაფრთხოების (იუ) დონეზე მიმდინარე მომენტში, მაგრამ დინამიკა მოთხოვნებისა სისტემების სიცოცხლისუნარიანობის მართვისადმი, გლობალური კომპიუტერული ქსელების (გკქ) სირთულის ზრდა წინა პლანზე სწევენ ამოცანას ინფორმაციის პერსპექტიული (ხვალიდელი დღის) უსაფრთხოების უზრუნველყოფისა გკქ –ში, რომლებიც გამოიყენებიან კრიტიკულ დანართებში და პირველ რიგში, ხელისუფლების ორგანოებში, ფინანსური სტრუქტურებში, ენერგეტიკულ საწარმოებში. იტ შემდგომი ევოლუცია შეუძლებელია გკქ–ში ინფორმაციის დაცვის ამოცანის კომპლექსური გადაწყვეტის გარეშე. [2].

იტ– სისტემების ევოლუცია მიმდინარეობს ინტელექტუალური სისტემების შექმნის მიმართულებით, რომლებშიც ადგილი აქვს მემკვიდრეობის, განვითარების, ადაპტაციის და შერჩევის პროცესებს [3]. ტექნიკურ სისტემებში ეს პროცესები ახდენენ რეალიზაციას, ბიოსისტემების ანალოგიის გამოყენებით, რომლებისთვისაც დამახასიათებელია მაღალი ფუნქციური მდგრადობა და დაცვის მუქარათა ველის ცვლილებათა პირობებში.

ახლა განვიხილოთ ის თუ რა გვაქვს მხედველობაში ბიოსისტემური ანალოგიასთან დაკავშირებით.

ის–ს მოდელირების ამოცანის დასმა ატარებს კომპლექსურ ხასიათს იყენებს ბიოსოსტემურ ანალოგიას, დაწყებული ინფორმაციის წარდგენის ფორმით, ინფორმაციული ველების პროგრამებით და დასრულებული იტ–სისტემების არქიტექტურით აშენებული იუ–ს უზრუნველყოფის მექანიზმებით და პროცესების ევოლუციური მიმდინარეობით (ნახ.1).

დაცული ინფორმაციული პროცესების მოდელირება ეფუძნება ინფორმაციის წარმოდგენის ერთიანობას ბიოსისტემების იერარქიაში, რომელშიც შეტყობინებები გადაიცემიან უნივერსალური კონტეინერით, რომელიც განისაზღვრება დნკ სტურქტურირებული ინფორმაციული ველით. ამ ხასიათისაა განაწილებული ინფორმაციული ველები ნეირონული

კომპლექსებისა ნერვული სისტემის, რისი წყალობითაც ბიოსისტემებში არსებობენ მახსოვრობის ადაპტური მექანიზმები, რომლებიც აგროვებენ ცხოვრებისეულ გამოცდილებას [4]. მახსოვრობის ადაპტური მექანიზმების რეალიზაციის შესაძლებლობა ხელოვნური ნეირონული ქსელებიბს (ნქ) ინფორმაციულ ველებში –ესაა ძირითადი წინამძღვარი იტ– სისტემების ევოლუციისა.

პროგრამირებას ბიოსისტემებში აქვს ჭარბი განაწილებული ხასიათი, რაც უზრუნველყოფს ინფორმაციული პროცესების მაღალ ფუნქციურ მდგრადობას. ინფორმაციის ცალეკული დამახინჯებები, ერთის მმხრივ, კომპენსირდებიან სიჭარბით ინფორმაციული ველებისა, ხოლო მეორეს მხრივ, საშუალებას იძლევიან რეალიზებულ იქნას მუტაციის მექანიზმი და განვითარებისა და გადარჩევის ევოლუციური პროცესები.

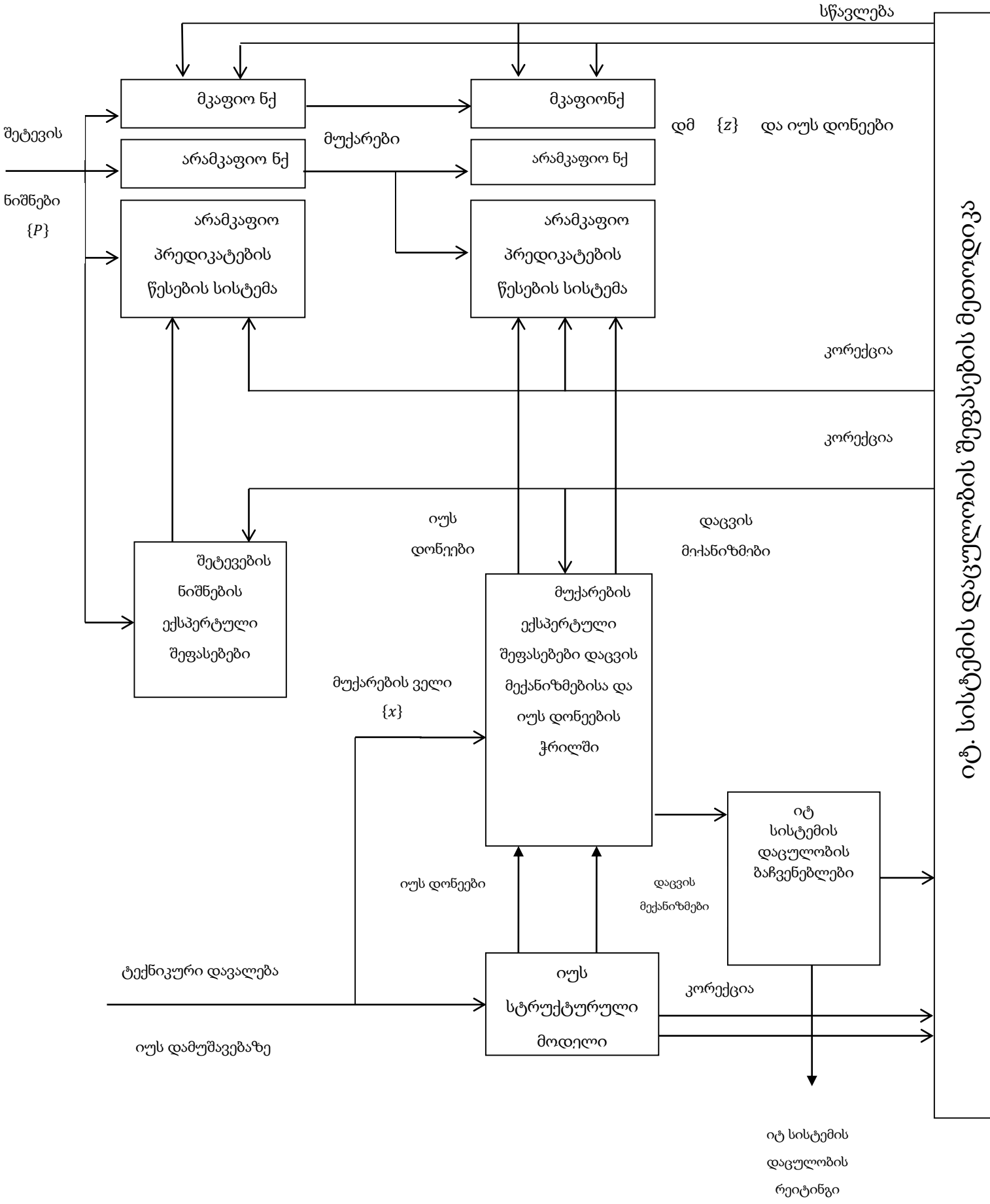
ანალოგიურად იტ–სისტემებში ინფორმაციული პროცესების მოდელირება უნდა შესრულდეს სტრუქტურირებული პროგრამების გამოყენებით,, რომელიც საშუალებას იძლევა ნქ ჭარბი განაწილებული იფორმაციული ველები აღიწეროს პაკეტური ნეიროქსელური პროგრამების სახეში (პმპ) [5]. პნპ საშუალებას იძლევა ნქ პროგრამულ რეალიზაციებს მიენიჭოს ფუნქციური მდგრადობა, რომელიც დამახასიათებელია აპარატულრული ნეიროქსელური საშუალებებისათვის, სრულად იქნას გამოყენებული ევოლუციური პროცესების შესაძლებლობები იუს–ში, კერძოდ, ადაპტური პროცესები ნქ ინფორმაციულ ველებში იტ–სისტემის საშუალებას აძლევენ განვითარდეს და დააგროვოს გამოცდიელბა მუქარათა ველის გაფართოების პირობებში, ხოლო გამოცდილების მემკვიდრეობა სისტემის შემდგომ რეალიზაციებში დაიყვანება შესაბამისი ინფორმაციული ველების გადაცემაზე. იუ ადაპტური სისტემის იერარქია ასახავს დაცვის ფუნქციის დაყოფას იმუნურებად; რომლებიც ამოწმებენ ინფორმაციის წარმოდგენის ფორმას და რეცეპტორულად, რომლებიც ახდენენ რეალიზაციას სისტემის გარემოსთან ურთიერთქმედებას და ცხოვრებისეული გამოცდილების დაგროვებას (ნახ.2).

ბიოსისტემების არქიტექტურულ თავისებურებას წარმოადგენს დაცვის მექანიზმმების შიდასისტემური ხასიათი, რომელიც რეალიიზებულია იტ–სისტემის იერარქიაში. ხელოვნული სისტემების მოდელირებისას უნდა იქნას გათვალსიწინებული, რომ იმუნური სისტემის და ნერნვული სისტემის ინფორმაციული ველების ადაპტური მექანიზმების რეალიზაციისას

ინფორმაციი დაცვის ფუნქციები უნდა იყვენენ პროექტირებადი იტ–სისტემის შიდა ფუნქციები.

მოდელირების შესაძლებლობა ესაა ძირითადი საშუალება დამუშავების და ვერიფიკაციის, რაც საშუალებას იძლევა თავიდან ავიცილოთ შეცდომები ნებისმიერი კიბერნეტიკული სისტემების (და არა მარტო) პროექტირებისას, ცხადია აქ პირველ რიგში ვგულისხმობთ ინფორმაციული უსაფრთხოების სისტემასაც. იუს–ში ადგილი აქვს ურთიერთკავშირს მოვლენებისა: მუქარის წყარო – ფაქტორი (მოწყვლადობა) – მუქარა (მოქმედება) – შედეგი (შეტევა). შეტევათა ველისა და დასაცავი იტ–სისტემის ექსპლუატაციის პირობების შეცვლისას შესაძლებელია წარმოშობა სრულად ახალი მოწყვლადობების (სუსტი ადგილების), რომლებიც არ იყო ასახული საწყის მოდულში და შესაბამისად, პოტენციური შესაძლებლობა ახალი მუქარების რეალიზაციისა ინფორმაციული სისტემის პროექტირების უსაფრთხხოებისა.

ინფორმაციული უსაფრთხოების ადაპტური სიტემის პროექტირებისას გათვალისწინებული უნდა იყოს გადასაწყვეტი ამოცანის კომპლექსური ხასიათი. დამაკავშირებელ რგოლს ადაპტური იუს მოდელისა წარმოადგენს იტ–სისტემის დაცულობის შეფასების მეთოდიკა, რომელიც ახასაითებს ურთიერთკავშირს კლასიფიცირებული მუქარისა და ცვის მექანიზმებისა (ნქ სახით, არამკაფიო ნქ, არამკაფიო პრედიკატების წესებსი სისტემის) იუს სტრუქტურული მოდელის, დაცულობის მაჩვენებლების და იტ–სისტემის რეიტინგის გაანგარიშების ინსტრუმენტული საშუალებები (ნახ.13).


სწავლება
მკაფიო ნქ
მკაფიონქ
დმ {z} და იუს დონეები
შეტევის
მუქარები
არამკაფიო ნქ
არამკაფიო ნქ
ნიშნები
{P}
არამკაფიო
პრედიკატების
წესების სისტემა
არამკაფიო
პრედიკატების
წესების სისტემა
კორექცია
კორექცია
იუს
დონეები
დაცვის
მიქანიზმები
შეტევების
ნიშნების
ექსპერტული
შეფასებები
მუქარების
ექსპერტული
შეფასებები დაცვის
მექანიზმებისა და
იუს დონეების
ჭრილში
მუქარების ველი
{x}
იტ
სისტემის
დაცულობის
ბაჩვენებლები
იუს დონეები
დაცვის
მექანიზმები
ტექნიკური დავალება
იუს
სტრუქტურული
მოდელი
კორექცია
იუს დამუშავებაზე
იტ. სისტემის დაცულობის შეფასების მეთოდიკა
იტ სისტემის
დაცულობის
რეიტინგი

ნახაზი 14. ინფორმაციული უსაფრთხოების ადაპტური სისტემის მოდელი

ნქ ადაპტურობა საშუალებას იძლევა შეზღუდული დანახარჯებისას უზურუნველყოფილ იქნას იტ–ს სისტემის უსფრთხოების მოცემული დონე მუქარათა ველის ცვლილებებზე ოპერატიულად რეაგირების მეშვეობით. მნიშვნელოვან ხარისხს ნქ წარმოადგენს აგრეთვე გამოცდილების დაგროვების შესაძლებლობა, რომელიც ხორციელდება დაცვის იერარქიაში ნქ ინფორმაციული ველების სახით.

ინფორმაციუოლი უსაფრთხოების სიტემის პროექტირების დავალების შესაბამისად აირჩევა იუს სტრუქტურული მოდელი დაცვის დონეების მექანიზმების იერარქიის სახით, ხოლო იუს– ექსპერტების გამოცდილება წარმოიდგინება ადაპტირებული ექსპერტული შეფასების მატრიცებით, რომელთა ბაზაზეც ფორმირდება სისტემა არამკაფიო პრედიკატული წესებისა კლაისიფიკაციისათვის:

1. მუქარების შეტევათა ნიშნის მიხედვით და

2. დმ მუქარათა ველზე.

პირველ შემთხვევაში (დაცვის იმუნური კლაისიფიკატორი) სისტემები არამკაფიო პრედიკატული წესებისა შემდგომი ადაპტაციისა და ანალიზისათვის წარმოდგინდებიან არა მკაფიო ნქ სახით, რომლებიც სწავლობენ შეტევების ნიშნის შემავალი ვექტორი რაღაც სიმრავლეზე. ერთდროულად ასწავლიან კლასიფიატორებს მკაფიო ნქ სახით ისეთნაირად, რომ თვითსწავლებისას წარმოშობილი კლასტერების რაოდენობა ტოლი იყოს წესების რიცხვისა არამკაფიო პრედიკატული წესების სისტემაში. მეორე შემთხვევაში ანალოგიურად ფორმირდებიან და ისწავლებიან დაცვის რეცეპტორული დონის ნერონული კლასიფიკატორი ცნობილი მუქარების ვექტორების მოცემულ ქვესიმრავლეზე.

ინფორმაცია ადაპტურ იუს–ში შეიძლება ინახებოდეს და გადაეცემოდეს შთამომავლობებში ნქ განაწილებული ინფორმაციული ველების სახით:

დაცვის იმუნური კლასიფიკატორების ცნობილი მუქარების ველები და

დაცვის რეცეპტორული დონის კლასიფიკატორების სასიცოცხლო გამოცდილების ველები.

პირველ შემთხვევაში ადაპტაციის პროცესი დაკავშირებულია კლასიფიკაციის ამოცანების გადაწყვეტასთან, მუქარების კლასტერიზაციასთან შეტევების ნიშნებით, რომლებსაც მივყავართ ცნობილი მუქარები ინფორმაციული ველების ცვლილებასთან იდს იერარქიის ზედა დონეზე სასიცოცხლო გამოცდილების ინფორმაციული ველების შესაბამის მოდიფიკაციებში.

მეორე შემთხვევაში ადაპტაციის პროცესი დაკავშირებულია კლასიფიკაციის ამოცანების გადაწყვეტასთან, დმ კლასერიზაციასთან მუქარათა ნიშნების მიხედვით, რომლებასც მივყავართ იდს იერარქიის ზედა დონეზე ინფორმაციული ველის გაფართოებასთან. კლასიფიკატორების სწავლების პროცესში იცვლებიან იმუნური და რეცეპტორული დონეების ინფორმაციულ ველები, ადეკვატურად სახეცვლილებას განიცდიან არამკაფიო პრედიკატული წესების სისტემები და ადაპტირებადი ექსპერტული შეფასების მატრიცები.

თუ იდს ადაპტური მოდელისათვის ბაზისად ავირჩევთ ერთ–ერთს იდს მრავალდონიანი მოდელებიდან, მაშინ დასაწყისში იდს ადაპტური მოდელი შეიცავდეს იქნება მდ–ის მინიმალურ რაოდენობას, რომელიც საკმარისია მუქარათაველის ყოველი ცვლილებისას და ცალკეული პოტენციური მოწყვლადობების გამოვლენათა სტატუსში გადასაყვანისას.

დმ საწყისი განაწილება იუს მოდელის დონეების მიხედვით განსაზღვრავს ექსპერტულ შეფასებათა მატრიცის განზომილებას, ხოლო ცვლილებები იუს მოდელში აისახებიან ექსპერტული შეფასების მატრიცის სტრიქონებისა და სვეტების რაოდენობასა და მნიშვნელობებზე.

ექსპერტული შეფასებების მატრიცისათვის აწარმოებენ დაცულობის მაჩვენებლების და იტ–სისტემის რეიტინგის გაანგარიშებას, რომლებიც გამოიყენებიან იტ–სისტემის დაცულობის შეფასების მეთოდიკის მიერ ანალიზისა და კორექციისათვის, როგორც მნიშვნელობების ექსპერტულ შეფასებათა მატრიცაში,, ასევე ფუნქციური პარამეტრებისა ნეიროქსელური კლასიფიკატორებისა იმუნურ და რეცეპტორულ დონეზე, ასევე შესაბამის არამკაფიო პრედიკატული წესების სისტემების.

ინფორმაციული უსაფრთხოების ექსპერტების გამოცდილება, რომელიც წარმოდგენილია მატრიცულ ფორმაში, გარდაისახებიან არამკაფიო პრედიკატული წესების სისტემებში, რომლებიც აღწერენ შესაბამის გზავნილებს და დასკვნებს, მაგალითად:

$П_1$: თუ x_1 არის A_{11} და ... x_n არის A_{1n}, მაშინ $Ỳ=B_1$,

$П_2$ თუ x_1 არის A_{21} და ... x_n არის A_{2n}, მაშინ $Ỳ=B_2$,

$П_k$ თუ x_1 არის A_{k1} და ... x_n არის A_{kn}, მაშინ $Ỳ=B_k$,

სადაც x_1 და $Ỳ$ - არის არამკაფიო შემავალი ცვლადი და ცვლადი გამოყვანის, ხოლო A_{11} და

B_1, ¿=1,k, j=1, n - საკუთნო ფუნქციები.

განსახილველ მოდელში ასახულია იუს იმუნური და რეცეპტორული დონეები. იმუნური დონე წყვეტს მუქარების **X**1 =, , j=1, n (დასკვნები) კლასიფიკაციის ამოცანას შეტევათა ნიშნების კლასიფიკაციისა დაცვის მექანიზმების (დმ) მუქარებისა Ź$_k$, K=1,K (დასკვნები) მუქარათა ველის **X**1, , j=1, N (გზავნილი) მიხედვით. სისტემები არამკაფიო პრედიკატული წესებისა, თავის მხრივ ასახავენ არამკაფიო ნქ „გამჭირვალე“ სტრუქტურაში, რომლებიც განკუთვნილი არიან ადაპტაციის პროცესის შედეგების შემდგომი სწავლებისა და ანალიზისათვის.

იუს ყოველი დონის კლასიფიატორები ორგანიზებულია შემდეგი სქემით:

ექსპერტული შეფასებების მატრიცა - სისტემა არამკაფიო პრედიკატული წესების - არამკაფიო ნქ - თვითშემსწავლელი ნქ. - თვითშემსწავლელი ნქ აუცილებელია კლასიფიკაციის ამოცანის გადასაწყვეტად. თვითშესწავლის პროცესში ნქ აღწევენ ისეთ დაყოფას დამსწავლი ამონაკრების ვექტორების ჯგუფებად, რათა ჯგუფების რიცხვი მკაფიო კლასიფიკატორში დაემთხავეს წესების რიცხვს არამკაფიო პრედიკატული წესების სისტემაში.

უკანასკნელი პირობა აუცილებელია შესაქმნელად ადაპტური კლასიფიკატორისა, რომელიც გზავნილების ვექტორის ცვლილებისას ცვლის (აუცილებლობისას) განზომილებას დასკვნების ვექტორისა, ანუ წყვეტს რა კლასტერიზაციის ამოცანის, მკაფიო ნქ ცვლის დასკვნების ვექტორი განზომილებას, რაც იწვევს ახალი წესების დამატებას სისტემაში არამკაფიო პრედიკატული წესებისა და შესაბამისი ფორმალური ნეირონების დამატებას არამკაფიო ნქ-ში. არამკაფიო ნქ სწავლება და ანალიზი კავშირების წონებისა ახლად შემოტანილი ფორმალური ნეირონებისა საშუალებას იძლევა ფორულირებულ იქნეს სპეციფიკაცია იუს-ში დაცვის მექანიზმების არ არსებობაზე.

იუს მუშაობის პროცესში ხდება იტ-სისტემის გამოცდილების დაგროვება არამკაფიო პრედიკატული წესების სისტემების ადაპტაციის მეშვეობით, ასევე არამკაფიო ნქ პარამეტრების, ექსპერტული შეფასების მატრიცის მეშვეობით. ექსპერტული შეფასების მატრიცის კორექცია ცვლის იტ-სისტემის დაცულობის მაჩვენებლების სისტემას, რომელიც საშუალებას იძლევა თვალყური მიადევნოს (იტ-სისტემის დაცულობის შეფასების მეთოდიკის მეშვეობით) დინამიკას ინფორმაციული დაცვისა და მიღებულ იქნას გადაწყვეტილებები დმ სტრუქტურის და შემადგენლობის მრავალდონიან იუს-ში ცვლილებებთან დაკავშირებით.

ადაპტური დაცვის მოდელში ერთ-ერთ უმთავრეს კომპონენტს წარმოადგენს დაცულობის მაჩვენებლების გაანგარიშების ბლოკი, რომელიც იტ-სისტემის დაცულობის მეთოდიკასთან ერთად საშუალებას მოგვცემს:

უზრუნველყოფილ იქნას ოპტიმალურთან მიახლოებული თანაფარდობა „ღირებულება/ეფექტურობა“ იუს მისი მოდელი მხოლოდ აუცილებელი დმ შეცსებით;

დინამიკაში თვალყური მივადევნოთ დმ დატვირთულობას მუქარათა ველის შეცვლისას;

დავაფორმიროთ სპეციფიკაცია მოთხოვნებისა არ არსებულ დაცვის მექანიზმებზე;

შევაფასოთ იტ-სისტემის დაცულობას მოსალოდნელი ზარალის სიდიდის და დმ აქტიურობის ინტერალური მაჩვენებლების მიხედვით, რომლებიც განაწილებული არიან იუს იერარქიების მიხედვით.

გადაწყვეტილება შეტევათა კლასიფიკაციის და დაცვის მექანიზმების გაფართოებაზე ხორციელდება შეფასებათა იმ სისტემის მეშვეობით, რომლითაც ფასდება მუქარების ნეიტრალიზების უტყუარობა ცალკეული მდ ჭრილში ან იუს ცალკეული ეშელონებისა და ანალოგიური შეფასებებისა მოსალოდნელი ზარალის, რომლებიც ასევე (გაანგარიშებადია) შეფასებადია ცალკეული დმ ან იუს ეშელონებისათვის.

ინფორმაცია წარმოადგენს ცნობებს, რომლებიც მიიღება გამოკვლევების, შესწავლის ან განსწავლის შედეგად: სიახლეს, ფაქტებს, მონაცემებს; ბრძანებებს ან მონაცემთა წარმოდგენის სიმბოლოებს (კავშირის საშუალებებში ან კომპიუტერზე); ცოდნას (შეტყობინება, ექსპერიმენტული მონაცემები, გამოსახულებები), რომლებიც ცვლიან ფიზიკურ ან გონებრივი გამოცდილების შედეგად მიღებულ კონცეფციას. უსაფრთხოება

განისაზღვრება, როგორც თავისუფლება საფრთხეთაგან, დაცულობა. თუ გავაერთიანებთ ამ ორ ცნებას, მივიღებთ ინფორმაციული უსაფრთხოების განსაზღვრას, რომელიც წარმოადგენს არასანქცირებული გამოყენების, ბოროტად გამოყენების, ცნობების, ფაქტების, მონაცემების ან აპარატურული საშუალებების შეცვლის ან მათ წვდომაზე მტყუნების აღმოფხვრის მიზნით მიღებულ ზომებს.

ინფორმაციული უსაფრთხოება არ უზრუნველყოფს აბსოლუტურ დაცვას. ის არის გამაფრთხილებელ მოქმედებათა ერთობლიობა, რომელიც საშუალებას იძლევა დაცულ იქნას ინფორმაცია და მოწყობილობები საფრთხეთაგან, რომელიც მოსალოდნელია მათი სუსტი ადგილების გამოყენებით.

უკანასკნელ ათწლეულში მნიშვნელოვნად გაფართოვდა ინფორმაციული უსაფრთხოების უზურნველყოფის საშუალებები. მრავალი სხვადასხვა ორგანიზაცია ჩაერთო დაცვის უზურნველყოფის ამოცანების გადაწყვეტაში.

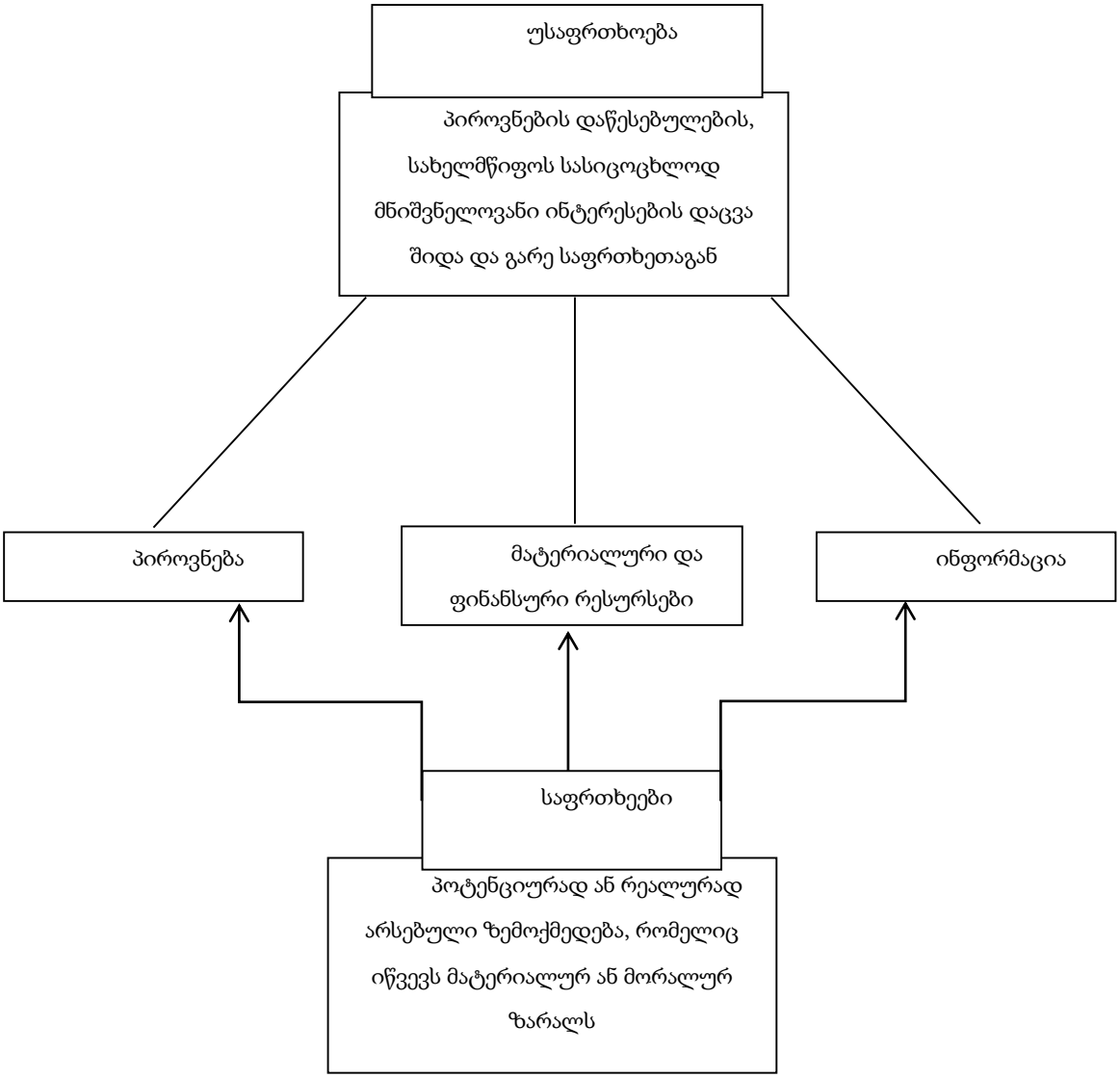
ინფორმაციული უსაფრთხოება მოიცავს უსაფრთხოების მრავალ ასპექტს. საიმედო დაცვის ყველა საშუალების და მეთოდის გაერთიანებას. საიმედო ფიზიკური დაცვა საჭიროა მატერიალური აქტივების – ქაღალდის მატარებლების და სისტემების დაცულობის უზრუნველსაყოფად. კომუნიკაციის დაცვა (COMSEC) უზრუნველყოფს ინფორმაციის გადაცემის უსაფრთხოებას. გამოსხივების დაცვას (EMSEC) საჭიროა, თუ მოწინააღმდეგეს აქვს მძლავრი აპარატურა კომპიუტერული უსაფრთხოება (COMPUSEC) საჭიროა კომპიუტერულ სისტემებში წვდომის მართვისათვის, ხოლო ქსელის უსაფრთხოება (NETSEC) – ლოკალური ქსელის დაცვისათვის. დაცვის ყველა სახეობა ერთობლივად უზურნველყოფს ინფორმაციულ უსაფრთხოებას (INFOSEC).

შეიძლება ითქვას, რომ XXI საუკუნე არის ინფორმაციული საუკუნე. ამავე დროს იზრდება ინფორმაციაზე ბოროტმოქმედება და წარმოიშვა ინფორმაციის დაცვის აუცილებლობაც. გამოცდილება გვიჩვენებს, რომ ამ ტენდენციასთან საბრძოლველად საჭიროა ინფორმაციული რესურსების დაცვის პროცესის მიზანმიმართული ორგანიზაცია, რაშიც უნდა მონაწილეობდნენ პროფესიონალი სპეციალისტები, ადმინისტრაცია, თანამშრომლები და მომხმარებელი, რაც აამაღლებს საკითხის ორგანიზაციულ მხარეს.

გამოცდილება გვიჩვენებს, რომ:

- ინფორმაციული უსაფრთხოების უზურუნველყოფა არ შეიძლება იყოს ერთჯერადი აქტი. ეს უწყვეტი პროცესია, რომელიც მდგომარეობს დაცვის სისტემის სრულყოფისა და განვითარებისათვის უფრო რაციონალური მეთოდების, ხერხებისა და გზების დაფუძნებასა და რეალიზაციაში, დაცვის სისტემისს მდგომარეობის განუწყვეტელ კონტროლში, სისტემის სუსტი ადგილების გამოვლენაში.
- ინფორმაციის უსაფრთხოება იყოს უზრუნველყოფილი სისტემის ყველა სტრუქტურულ ელემენტზე და ინფორმაციის დამუშავების ტექნოლოგიური ციკლის ყველა ეტაპზე.
- მნიშვნელოვანი ეფექტი მიიღწევა მაშინ, როცა გამოყენებული მეთოდი, საშუალება და მიღებული ზომები ერთიანდება მთლიან ორგანიზმად – ინფორმაციის დაცვის სისტემად (იდს). ამავე დროს სისტემის ფუნქციონირება უნდა იყოს კონტროლირებადი, განახლებადი და შევსებადი, გარე და შიდა პირობების ცვლილების მიხედვით.
- იდს უნდა აკმაყოფილებდეს ინფორმაციის უსაფრთხოების მოთხოვნილ დონეს, რისთვისაც საჭიროა მომხმარებელთა მომზადება და მათ მიერ ინფორმაციის დაცვისათვის გამიზნული ყველა წესის დაცვა.

დაგროვილი გამოცდილების გათვალისწინებით იდს შეიძლება განისაზღვროს როგორც სპეციალური ორგანოების, საშუალებების, მეთოდების და მიღებული ზომების ერთობლიობა, რომელიც უზრუნველყოფს ინფორმაციის დაცვას შიდა და გარე საფრთხეთაგან. ინფორმაციული უსაფრთხოების ზოგადი სქემა წარმოდგენილია ნახ.14.-ზე.



ნახაზი 15. ინფორმაციული უსაფრთხოების ზოგადი სქემა.

ინფორმაციის დაცვას სისტემური მიდგომის თვალსაზრისით წაეყენება გარკვეული მოთხოვნები. ინფორმაციის დაცვა უნდა იყოს:

- უწყვეტი.
- გეგმიური.
- მიზანმიმართული.
- კონკრეტული.
- აქტიური, გარკვეული ხარისხით.
- საიმედო.
- უნივერსალური.
- კომპლექსური.

გამოცდილება უჩვენებს, რომ ინფორმაციის დაცვის სისტემა (იდს) უნდა აკმაყოფილებდეს შემდეგ მოთხოვნებს:

- მოიცავდეს ინფორმაციული ქმედების მთელ ტექნოლოგიურ კომპლექსს;

- იყოს გათვალისწინებული ცვლილებებისა და დამატებების შეტანა;

- იყოს არასტანდარტული, განსხვავებული. დაცვის საშუალებების არჩევა არ უნდა იყოს გათვლილი ბოროტმოქმედის მცირე შესაძლებლობებზე;

- იყოს მარტივი ტექნიკური მომსახურების თვალსაზისით და მოხერხებული მომხმარებელთა მიერ ექსპუატაციის თვალსაზრისით;

- იყოს საიმედო. ტექნიკური საშუალებების ნებისმიერი გატეხვა არის ინფორმაციის გაჟონვის არაკონტროლირებადი არხების გაჩენის მიზეზი;

- იყოს კომპლექსური, მთლიანი.

- იდს-ს მიმართ განსაზღვრულია გარკვეული მოთხოვნები:

- ცხადად იყოს განსაზღვრული მომხმარებლის უფლებები გარკვეული სახის ინფორმაციის წვდომაზე;

- წაუყენოს მომხმარებელს მინიმალური უფლება, რომელიც სჭირდება დაკისრებული სამუშაოს შესასრულებლად;

- აღრიცხოს კონფედენციალური ინფორმაციის ხარისხის შეფასება;

დაცვის საშუალებების მთლიანობის კონტროლის უზრუნველყოფა და მომენტალური რეაგირება დაცვის საშუალბების მწყობრიდან გამოსვლისას.

უსაფრთხოების სისტემა წარმოადგენს სპეციალური ორგანოების, სამსახურების, საშუალებების, მეთოდების და ღონიშძიებების ერთობლიობას, რომელიც უზრუნველყოფს პიროვნების, დაწესებუელების, სახელმწიფოს სასიცოცხლოდ მნიშვნელოვანი ინტერესების დაცვას შიდა და გარე საფრთხეთაგან.

დამოუკიდებელი მნიშვნელობა აქვს ინფორმაციული რესურსების კლასიფიკაციას მისი გამოყენება სფეროების მიხედვით, რომელსაც საფუძვლად უდევს მომხმარებლის ინტერესები, როგორიცაა: განათლების მიღება, ფიფზიკური პირის პროფესიული მომზადება.როგორც წესი, მიმდინარეობს ინფორმაციული რესურსების ფორმირება იმ სუბიექტების მოთხოვნათა გათვალისწინებით, რომლებიც გამოიყენებენ უკვე დაგროვილ რესურსებს. ფორმირდება საერთო, სპეციალიზებული ბიბლიოთეკები, არქივები, ინფორმაციის სხვადასხვა ფონდი, ინფორმატიზაციის პირობებში

ეს წყაროები, ინფორმაციული რესურსების საცავები გადაჰყავთ ელექტრონულ ფორმაში, იქმნება ელექტრონული საინფორმაციო სისტემები.

ინფორმაცია შეიძლება იყოს სრულად განსხვავებული სუბიექტების რესურსი: ცალკეული პირის (მოქალაქის), იურიდიული პირის, სახელმწიფო ორგანოს, ადგილობრივი თვითმმართველობის ორგანოების, საზოგადოებრივი ორგანიზაციების. ეს სუბიექტები აწარმოებენ, ქმნიან გარკვეულ ინფორმაციულ პროდუქტს და იყენებენ მათ სხვადასხვა სახით.

კაცობრიობამ მიაღწია თავისი განვითარების ისეთ ეტაპს, როცა მძლავრი ინფორმაციული ტექნოლოგიების - ავტომატიზებული სისტემების გამოყენებით შესაძლებელი ხდება წარმოდგენილი პრობლემების გადაწყვეტა და აღნიშნულ შეკითხვებზე წარმატებით პასუხის გაცემა.

აქ მხედველობაში გვაქვს არა მარტო უახლესი კომპიუტერული ტექნიკის ტელეკომუნიკაციების შესაძლებობები, არამედ სისტემოლოგების მიღწევები, რომელთა მტკიცებითაც ნებისმიერი რთული სისტემა მიუხედავად თავისი ბუნებისა მოდელირებადია, ე.ი. რთული სისტემა შეიძლება წარმოვიდგინოთ მოდელების სრული სიმრავლით, რომელშიც თითოეული მოდელი ასახავს რთული სისტემის რომელიმე გარკვეულ არსს. ამ სიმრავლეს უნდა მივაკუთნოთ სიტუაციური შემეცნებითი (კოგნიტური) მოდელირების კომპიუტერული საშუალებები, რომლებიც უკვე ათეულობით წელია გამოიყენება ეკონომიკურად განვითარებულ ქვეყნებში, რომლებიც ეხმარებიან საწარმოებს გადარჩნენ და განავითარონ ბიზნესი, ხოლო ხელისუფლების ორგანოებს მოამზადონ კარგი ნორმატიული დოკუმენტები.

კოგნიტური მოდელირიების საშუალებებს გააჩნიათ ისეთი თავისებურებები, რაც გამორიცხავს მათ მექანიკურ გადმოტანას არა მარტო სხვა ქვეყანაში, არამედ თუნდაც ერთი საწარმოდან მეორე საწარმოში. ეს სპეციფიკაა - მათი ორიენტირებულობა სიტუაციების განვითარების კონკრეტულ პირობებზე, რომლებიც არსებობენ ამა თუ იმ ქვეყანაში, რეგიონში, ქალაქში, დასახლებულ პუნქტში, სოფელში (პოლიტიკური და ეკონომიკური მდგომარეობა, მოსახლეობის და ხელისუფლების მენტალობა, საინფორმაციო სფეროს ქაოტურობა, ბაზრის გახსნილობა და სხვა).

მოდელირება - ესაა საშუალება ნეგატიური ტენდეციების დასწრების და თავიდან აცილების ეკონოკური, პოლიტიკური და სოციალური კანონზომიერების გამოვლენის, პრობლემაზე თეორიული და პრაქტიკული

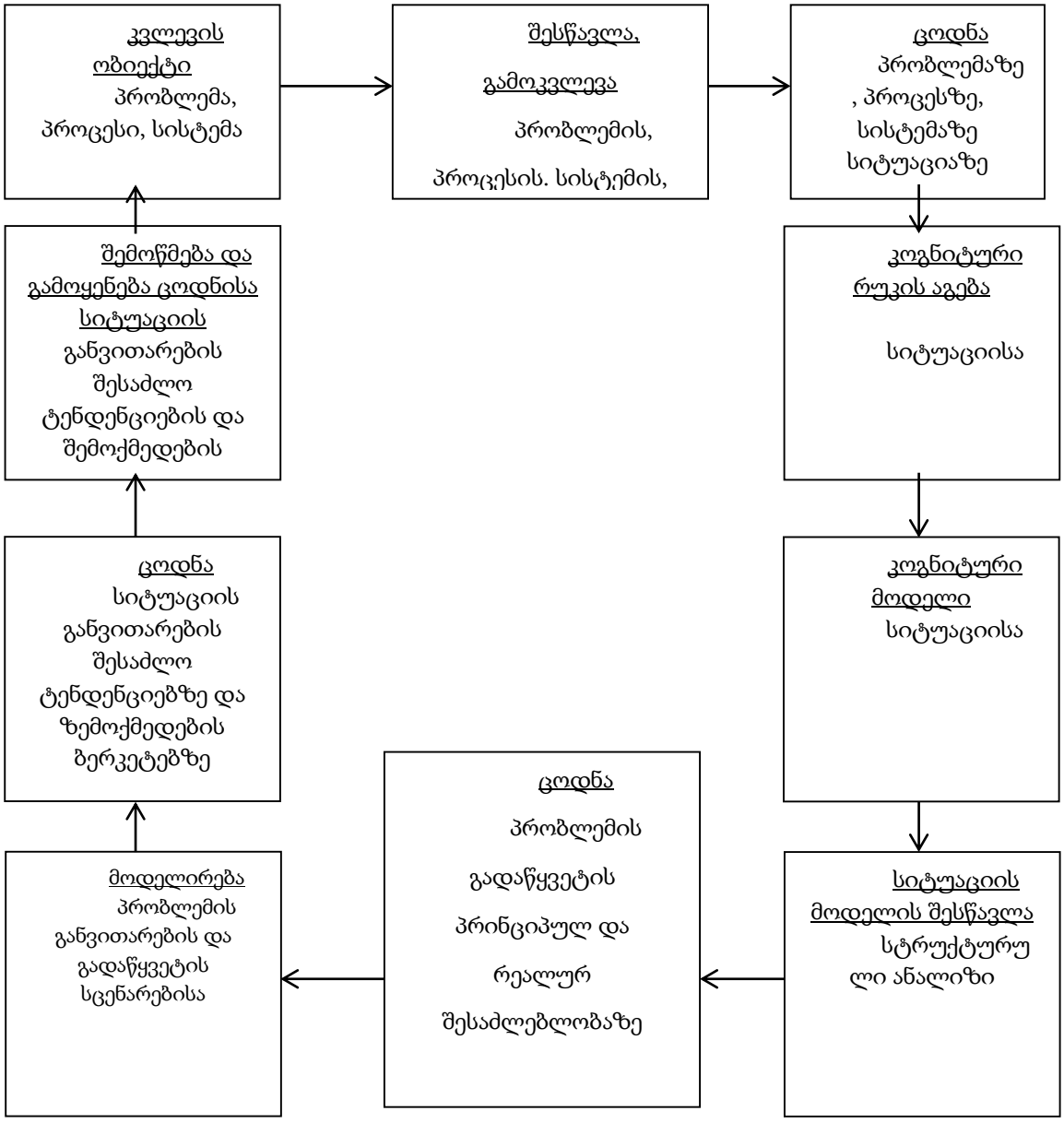
ცოდნის მიღების და ამის საფუძველზე პრაქტიკული დასკვნების ფორმულირებისა.

მოდელირება, როგორც მართვის მთავარი ინსტრუმენტი, წარმოადგენს ციკლურ პროცესს (ნაზ.15) ცოდნა საკვლევ პრობლემაზე ფართოვდება და ზუსტდება, ხოლო საწყისი მოდელი განიცდის სისტემატურ სრულყოფას.

რთული სიტუაციის მიმდინარე მდგომარეობის ანალიზისას აუცილებლად დგება შემდეგი საკითხები:

მართვის რომელი მეთოდი უნდა შეირჩეს მიზნობრივი ფაქტორების სასურველი ქცევის უზრუნველსაყოფად?

სიტუაციის როგორი ცვლილებებია შესაძლებელი (უახლოეს) მომავალში?



ნახაზი 16. მოდელირების პროცესი.

„პირველი ჯგუფის შეკითხვები - ესაა დასახული მიზნის მისაღწევად სიტუაციის მიმდინარე (ოპერატიული) მართვის საკითხები. ამ ამოცანის ამოხსნა შეიძლება იყოს მართვის რამოდენიმე „ვარგისი“ ვარიანტი. ნაპოვნი მართვის თითოეული ვარიანტის რეალიზაცია გულისხმობს შესაბამისი კონკრეტული ღონისძიებების გატარებას. ამ დროს უნდა გადაიჭრას ვარიანტების შედარებითი შეფასების ამოცანა შემდეგი მაჩვენებლების მიხედვით:

- მართვის შედეგების სიახლოვით დასახულ მიზანთან (ვარიანტების ეფექტურობის მაჩვენებლების მიხედვით);
- დანახარჯებით (ფინანსური, ფიზიკური, მორალური და ა.შ.), რომლებიც დაკავშირებული არიან ცალკეული ვარიანტების რეალიზაციასთან;
- შედეგების ხასიათის (შექცევადი, შეუქცევადი) მიხედვით, რეალურ სიტუაციაში შესაბამისი ვარიანტების რეალიზაციისას და ა.შ.

მეორე ჯგუფის შეკითხვები დაკავშირებული არიან მიმდინარე სიტუაციაში შესაძლო ცვლილებების სტრატეგიების პროგნოზირებასთან. ეს ცვლილებები შეიძლება გამოწვეული იყოს შიდა მიზეზებით (მაგალითად, გარკვეული მართვის რეალიზაცია შეიძლება დაკავშირებული იყოს რეალურ სიტუაციაში ფაქტორების ურთიერთმოქმედების ცვლილებასთან და ამ ცვლილებამ შეიძლება წარმოშვას ახალი პრობლემები) და გარეშე მიზეზებით, რაც განპირობებულია იმ გარემოებით, რომ რეალურ სიტუაციაზე უწყვეტად მოქმედებენ გარე შეშფოთებები, რომელთა წყაროები არ არიან ჩართულნი გასაანალიზებელი სიტუაციის კოგნიტურ მოდელში. მიზეზების ხასიათისაგან დამოუკიდებლად, რომლებიც ცვლიან სიტუაციას, მათი გათვალისწინება მოითხოვს სიტუაციის საწყისი კოგნიტური მოდელი შეცვას.

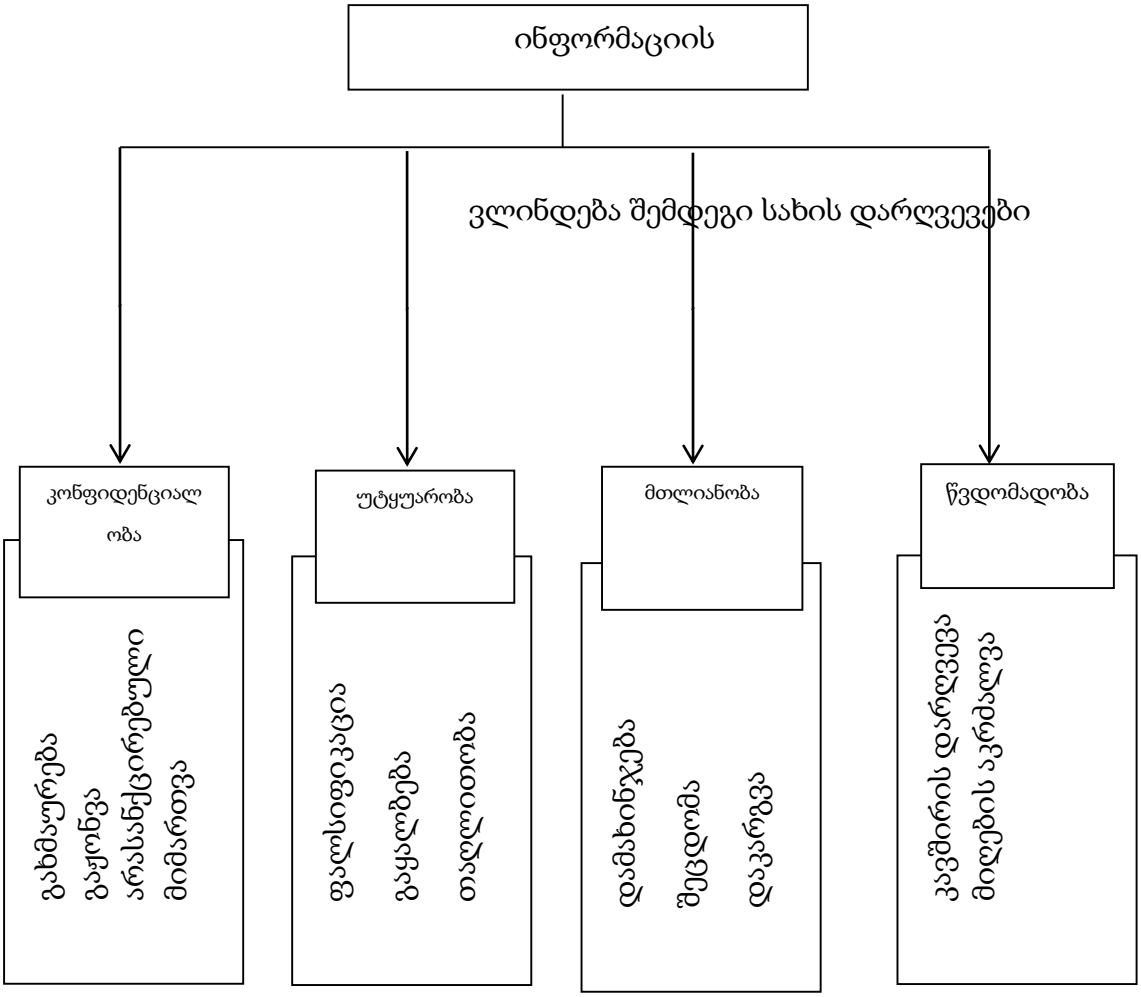
მესამე ჯგუფის შეკითხვები დაკავშირებული არიან შეცვლილი სიტუაციის ანალიზსა და ამ დროს წარმოქმნილი პრობლემების (კერძოდ, კრიზისული სიტუაციების შესაძლო წარმოქმნით) აღწერასთან. გასათვალისწინებელია ისიც, რომ შეიძლება ანალიზის მიზნებიც შეიცვალოს, ამიტომ ახალი პრობლემები დაკავშირებული არიან შეცვლილ სიტუაციაში შეცვლილი მიზნობრივი ფაქტორების სასურველი ქცევის

უზრუნველყოფასთან. ამ დროს წინასწარ განჭვრეტადი მიზნებისათვის ანალიზი და გადაწყვეტა პრობლემებისა, რომლებიც დაკავშირებული არიან კრიზისული სიტუაციების წარმოქმნასთან, ხორციელდება ასეთი სიტუაციების რეალურ დადგომამდე, რაც საშუალებას იძლევა მიღებული იქნას წინასწარი ზომები კრიზისული სიტუაციების თავიდან ასაცილებლად, ან „კარგად“ მვემზადოთ მათ დასაძლევად“.[33]

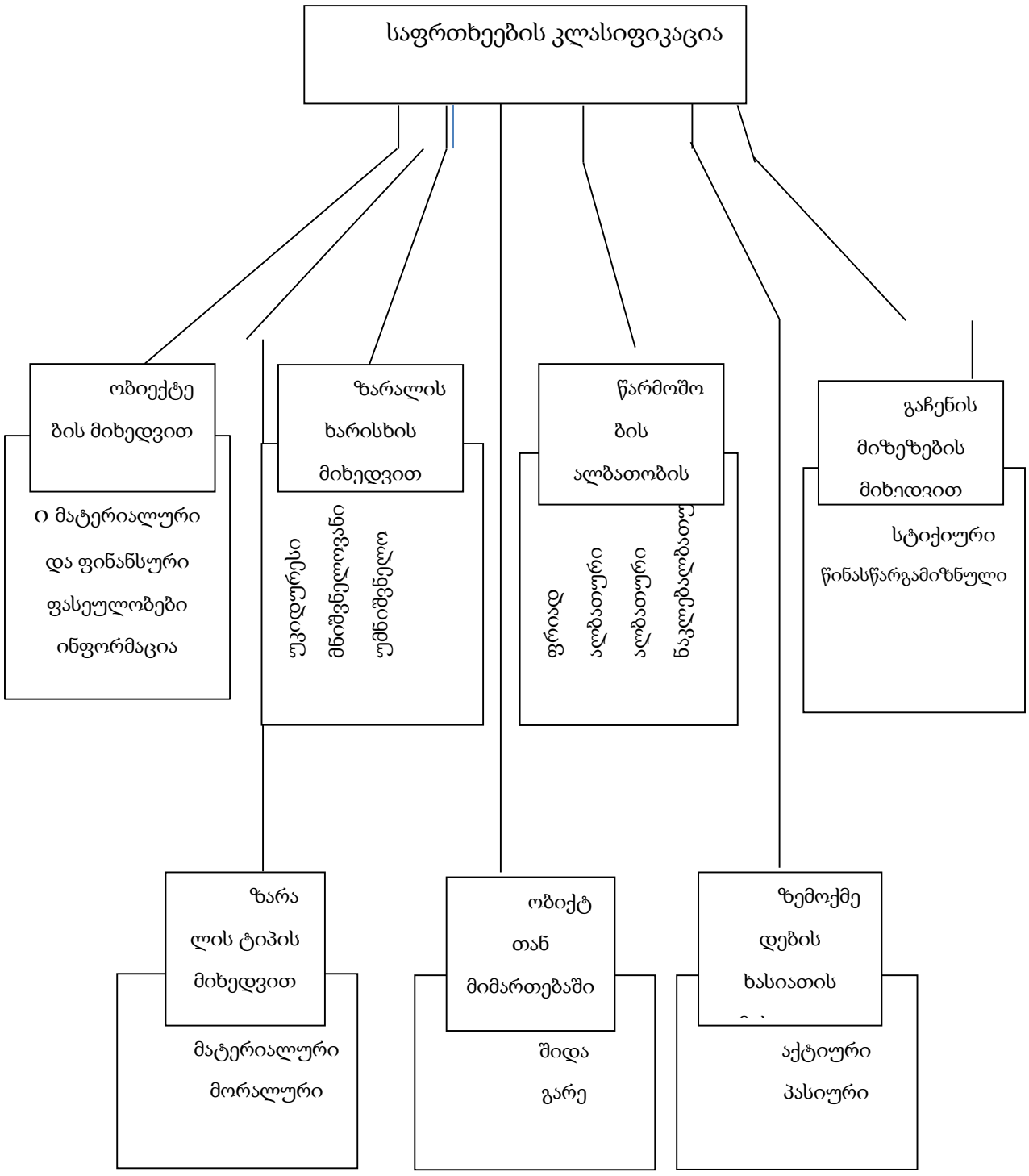
სახელმწიფოს მართვის ერთიანი ავტომატიზებული სისტემის შექმნა, რაც თავისთავად ურთულესი პრობლემაა, იძლევა იმის საშუალებას, რომ სახელმწიფოსა და საზოგადოებას შორის დამყარდეს თვისობრივად სრულიად ახალი ურთიერთობები. დღეს მსოფლიოს ბევრი ქვეყანა - განვითარებულიც და განვითარებადიც, სახელწიფოში მიმდინარე პროცესების, შექმნილი სიტუაციების მართვის ავტომატიზებით უფრო დაუახლოვდა თავიანთ მოქალაქეებს, საზოგადოებას, მეწარმეებს, გაიგოს მათი შეხედულებები ამა თუ იმ პრობლემების და საერთოდ, ქვეყანაში არსებული მდგომარეობის შესახებ და ამის მიხედვით განახორციელოს სიტუაციის მართვა, სწორედ ასეთი მიდგომა შეიძლება იქცეს მძლავრ ხელწემწყობ ფაქტორად ქვეყანაში სტაბილურობისა და შემდგომი განვითარებისათვის.

დღევანდელმა ადამიანმა კარგად უნდა გააცნობიეროს, თუ რამდენად მნიშვნელოვანია საიდუმლოება მის ცხოვრებაში და ეს უფლება განსაზღვრულია კონსტიტუციით. ორგანიზაციები, რომლებიც აგროვებენ პერსონალურ მონაცემებს, უნდა იყოს დარეგისტრირებული მთავრობაში და უზრუნველყონ ზომები მათი ბოროტად გამოყენების წინააღმდეგ.

თითოეული საფრთხე, რომელიც ვლინდება ნახ.17-ზე მოცემულ დარღვევებში, მოიცავს განსაზღვრულ ზარალს - მორალურს ან მატერიალურს, ხოლო დაცვა და საწინააღმდეგო ქმედებები ამცირებს მას მნიშვნელოვნად ან ნაწილობრივ. თუმცა ეს ყოველთვის არ ხერხდება. ამის გათვალისწინებით საფრთხეები შეიძლება კლასიფიცირდეს კლასტერების სახით, რომელიც მოცემულია ნახაზზე.



ნახაზი 17. ინფორმაციის საფრთხეთა გამოვლენა



ნახ. 18 საფრთხეთა კლასიფიკაცია.

3.5. ინფორმაციული ტექნოლოგიების ინფრასტრუქტურა და ელექტრონული სერვერები

სერვისები განხორციელდა ბიუროს თანამშრომლებისთვის აუცილებელი კომპიუტერული პარკის აპარატურული და პროგრამული უზრუნველყოფის შერჩევა და გამართვა, შედეგად, ბიუროს ყველა თანამშრომელი უზრუნველყოფილია სამუშაო კომპიტერითა და საჭირო პროგრამული უზრუნველყოფით.

შეიქმნა ბიუროს ლოკალური ინფორმაციული ქსელი და განხორციელდა მისი ფუნქციონირებისათვის საჭირო ქსელის აქტიური მოწყობილობების, სასერვერო აპარატურული და პროგრამული უზრუნველყოფის შერჩევა/გამართვა' ლოკალური ქსელის ბიუროს თანამშრომლებს საშუალებას აძლევს, ისარგებლონ გლობალური ქსელით, ბიუროს ელ–ფოსტით, ციფრული სატელეფონო კავშირით (VolP) და სხვა ქსელური სერვისებით, ხოლო IT სპეციალისტებს – ცენტრალიზებულად მართონ მომხმარებლის ანგარიშები და სერვისები;

ბიუროს ლოკალური ქსელის უსაფრთხოების უზრუნველსაყოფად, განხორციელდა ქსელური დაცვის ეკრანის (Fire Wall) კონფიგურირება და ბიუროს ქსელში ჩართვა; ქსელური დაცვის ეკრანის დანიშნულებაა, ლიკალური ქსელის არასანქცირებული წვდომისაგან დაცვის და ქსელურ მონაცემტა ნაკადის ფილტრაციის უზრუნველყოფა;

ბიუროს ინფორმაციული სისტემის და ელექტრონული ინფორმაციის დაცვის მიზნით, შერჩეული და გამართული იქნა ანტივირუსული პროგრამული უზრუნველყოფა;

შემუშავდა და ფუნქციონირება დაიწყო ბიუროს ინფორმაციულმა სისტემამ და ელექტრონულმა სერვისებმა;

ბიუროს ელექტრონული კომუნიკაციების საშუალებებით უზრუნველსაყოფად მოხდა შიდა ციფრული (VolP) სატელეფონო კავშირის და ელ–ფოსტის სერვერის გამართვა;

„განხორციელდა ბიუროს ლოკალური ქსელის ინტეგრაცია საქართველოს თავდაცვის სამინისტროს შიდა (დახურულ) ქსელთან, რამაც საშუალება მისცა ბიუროს ისარგებლოს ისეთი ელექტრონული სერვისებით, როგორიცაა "eflow". თავდაცვის სამინისტროს სატელეფოონო ცნობარი და შიდა ციფრული (VolP) სატელეფონო კავშირი;"[4]

განხორციელდა საკომუნიკაციო მომსახურების განყოფილების გამართული ფუნქციონირებისათვის საჭირო აპარატულ/პროგრამული უზურუნველყოფის შერჩევა და გამართვა;

საქართველოს თავდაცვის სამინისტროს ინფორმაციული ტექნოლოგიების ინფრასტრუქტურაში განხორციელდა ქსელური სენსორის განთავსება და მისი ფუნქციონირებისთვის საჭირო ყველა ღონისძიებების გატარება;

შესწავლილ იქნა საქართველოს თავდაცვის სამინისტროს დანაყოფებში მონაცემთა ელექტრონული შიფრაციის პროგრამული უზურუნველყოფის სატეტსო ვერსია, რომლის საიმედოობის შესახებ ინფორმაცია წარედგინა დაინტერესებულ სტრუქტურულ დანაყოფს;

„ამჟამად, კიბერუსაფრთხოების ბიურო ფუნქციონირების საწყის ეტაპზეა და შესაბამისად, ეტაპობრივად იწყებს დაკისრებული ვალდებულებებისა და ამოცანების განხორციელებას. ბიურო ჩართულია კიბერდანაშაულთან ბრძოლის ერთიანი სახელმწიფო პოლიტიკის განხორციელებაში, შეიმუშავებს ინფორმაციული უსაფრთხოების პოლიტიკას ტავდაცვის სფეროში, განსაზღვრავს კიბერსივრცეში არსებულ რისკებსა და გამოწვევებს და მათი დროულად აღმოფხვრისა და პრევენციის მეთოდებს. კომპიუტერულ ინციდენტებზე რეაგირების საკომუნიკაციო მომსახურების განყოფილება წინასწარ განსაზღვრული კავშირის საშუალებით (ელ–ფოსტა, ქსელური სენსორი) იღებს შეტყობინებას კომპიუტერული ინციდენტის შესახებ, ახდენს მის რეგისტრაციას ინციდენტების მართვის სისტემში და დახარისხებას, რაც თავის მხრივ, რამდენიმე ეტაპისაგან შედგება – ვერიფიკაცია, პირველადი კლასიფიცირება, განაწილება.“[6]

ინციდენტის რეგისტრაციის შემდეგ ხდება მისი ვერიფიკაცია და პირველადი კლასიფიცირება. ინციდენტის ვერიფიკაციის მიზანია, განისაზღვროს, რამდენად არის ეს შემთხვევა კომპიუტერული ინციდენტი. ხორციელდება ინციდენტის პირველადი კლასიფიცირება ინციდენტის კრიტიკულობის დონის განსაზღვრის მიზნით. დახარისხების ბოლო ეტაპზე ხორციელდება ინფორმაციის გადაცემა ინციდენტების მართვაზე პასუხისმგებელ პირზე (ჯგუფზე), შემდგომი რეაგირებისათვის.

2008-2011 წლებში საქართველოს წინააღმდეგ განხორციელებულმა ფართომასშტაბიანმა კიბერშეტევებმა ნათლად დაგვანახა კიბერუსაფრთხოების პოლიტიკის შემუშავების აუცილებლობა, რათა

უზრუნველყოფილ იქნეს კრიტიკული ინფორმაციული სისტემების გამართული და უსაფრთხო ფუნქციონირება.

ქვეყანაში კიბერუსაფრთხოების დანერგვა და განვითარება ნატოსთან ნაკისირი ვალდებულებების ერთ–ერთი შემადგენელი ნაწილია. საქართველოს თავდაცვის სამინისტროს მიერ დასახული მიზნები და გატარებული ღონისძიებები კიბერუსაფრთხოების სფეროში ხელს შეუწყობს საქართველოს ინტეგრაციის პროცესს ევროპულ და ჩრდილო–ატლანტიკურ ორგანიზაციებში.

კიბერსივრცე ქმნის ერთიან კომპლექსურ გარემოს მასში შემავალი ინფორმაციული და კომუნიკაციების ტექნოლოგიების მოწყობილობებითა და ქსელებით, რაც საშუალებას აძლევს საქართველოს თავდაცვის სამინისტროს სამოქალაქო ოფისს, შეიარაღებული ძალების გენერალური შტაბის სტრუქტურულ ქვედანაყოფებსა და სამინისტროში შემავალ საჯარო სამართლის იურიდიულ პირებს განახორციელონ სხვადასხვა ტიპის კომუნიკაცია, ძალებისა და საშუალებების მართვა.

კიბერუსაფრთხოების პოლიტიკის პირველი პრიორიტეტული ამოცანაა, განსაზღვროს კიბერსივრცის უსაფრთხოების უზრუნველყოფასთან დაკავშირებული სტრატეგია. პოლიტიკა აღწერს იმ პრინციპებს, რომლებიც განაპირობებენ ინფრასტრუქტურის უსაფრთხოების უზრუვენლყოფას და იმ სტანდარტების დანერგვას, რომელთა გამოყენება მყარ საფუძველს შეუქმნის ინფორმაციული სისტემებისა და ქსელების ეფექტურ დაცვას თავდაცვის სფეროში. პოლიტიკა ხაზს უსვამს კიბერუსაფრთხოების წარმატებული და ოპერატიული დაცვის მიზნით ადგილობრივი სტრუქტურების მჭიდრო და აქტიურ კოორდინაციასა და მათი ჩართულობის აუცილებლობას.

პოლიტიკის მეორე პრიორიტეტული ამოცანაა საქართველოს შეიარაღებული ძალების ინფორმაციული სისტემების დაცვა პოტენციური კიბერშეტევებისგან, დაზვერვის და რადიო–ელექტრონული ბრძოლის ხერხების და საშუალებების, ფსიქოლოგიური ოპერაციების აქტიური წინააღმდეგობის საშუალებებისა და მეთოდების განვითარება.

სხვა ამოცანებია:

– შეიქმნას უსაფრთხო კიბერსისტემა თავდაცვის სფეროში, მოხდეს ნდობის გენერირება ინფორმაციული ტექნოლოგიების სფეროში, შესაბამისად, გაძლიერდეს ინფრასტრუქტურული შესაძლებლობები

თავდაცვის სფეროსა და მასში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტებისთვის;

- ჩამოყალიბდეს ისეთი სისტემა, რომელიც უზრუნველყოფს უსაფრთხოების განხორციელებისათვის საჭირო კონცეპტუალური დოკუმენტების შემუშავებას. აღნიშნული სისტემა შემდგომში ხელს შეუწყობს ამ დოკუმენტების გლობალური უსაფრთხოების სტანდარტებთაან და საუკეთესო პრაქტიკასთან შესაბამისობაში მოყვანას;

- დაინერგოს და განვითარდეს ინფორმაციული ტექნოლოგიების უსაფრთხოების ინციდენტებზე რეაგირების 24/7 მექანიზმი, რომლებიც უზრუნველყოფენ ინფორმაციული და კომუნიკაციების ტექნოლოგიების ინფრასტრუქტურის დაცვას, მოახდენენ საფრთხეებისა და რისკების სწრაფ იდენტიფიცირებას, მათზე რეაგირებას, პრევენციული ზომების გატარებას და საჭიროების შემთხვევაში, კრიზისების მართვას პროგნოზირებადი, პრევენციული, დაცვითი, აღდგენითი მექანიზმების საშუალებებით;

- გაძლიერდეს თავდაცვის სფეროსა და მასში შემავალი კრიტიკული ინფორმაციული სისტემის სუბიექტების კრიტიკული ინფრასტრუქტურის დაცვა და გამართული ფუნქციონირების უზრუნველყოფა 24/7 მოქმედი მექანიზმების მიერ ინფორმაციული რესურების შექმნის, დაუფლების, განვითარების, ოპერირების საუკეთესო პრაქტიკის გამოყენებით;

- რეგულარულად განხორციელდეს კიბერსივრცეში არსებული და პოტენციური საფრთხეების, რისკების და გამოწვევების კვლევა და ანალიზი. საფრთხეების გაცნობიერება და მათი პოტენციური ზემოქმედების შეფასება ხელს შეუწყობს უსაფრთხოების ზომების გაძლიერებას. საფრთხეების ანალიზისა და რისკების კვლევის შედეგების საფუძველზე მოხდეს პრევენციული ზომების შემუშავება და გატარება თანამდროვე გამოწვევების დაძლევის მიზნით;

- პროფესიული უნარ–ჩვევების განვითარების მიზნით საგანმანათლებლო პროგრამებისა და ტრენინგების საშუალებით შეიქმნას კიბერუსაფრთხოების სფეროში სპეციალიზებული ჯგუფი;

- შეიქმნას და დამკვიდრდეს კიბერუსაფრთხოებისა და კონფიდენციალობის კულტურა, რაც საშუალებას მისცემს მომხმარებელს, იმოქმედოს ეფექტურად წინასწარ განსაზღვრული წესებით;

- ხელი შეუწყოს თანამშრომლებს, მონაწილეობა მიიღონ კიბერუსაფრთხოების სფეროსთან დაკავშიირებულ სხვადასხვა საგანმანათლებლო ტრენინგებსა და პროგრამებში;

- დამყარდეს მჭიდრო თანამშრომლობა ადგილობრივ და საერთაშორისო ორგანიზაციებთან, ხელი შეეწყოს ორმხრივი და მრავალმხრივი ურთიერთობების განვითარებას;

შეუძლებელია კიბერუსაფრთხოების უზრუნველყოფა და განვითარება იზოლირებულად განხორციელდეს. ამ ამოცანის ეფექტურად შესრულება შესაძლებელია მხოლოდ იმ შემთხვევაში, თუკი უზრუნველყოფილი იქნება მჭიდრო კოლაბორაცია საერთაშორისო და ადგილობრივ დონეზე. აქედან გამომდინარე, სახელმწიფომ უნდა განავითაროს ორმხრივი და მრავალმხრივი ურთიერთობები და აქტიურად დაუჭიროს მხარი ევროპული და ჩრდილო–ატლანტიკური ხელშეკრულების ორგანიზაციების რეკომენდაციებს, რაც ხელს შეუწყობს კიბერუსაფრთხოების უზრუნველყოფისათვის საჭირო ამოცანების შესრულებას. კიბერუსაფრთხოება დინამიკური სფეროა, იცვლება შეტევების ტიპი, თავდამსხმელთა მიზნები და მოტივები და ხშირ შემთხვევაშ, ძალიან რთული ხდება, განისაზღვროს რომელი სამართლებრივი ნორმა არეგულირებს კიბერინციდენტის კონკრეტულ შემთხვევას.

გასული წლების, ასევე უცხოეთის ქვეყნების გამოცდილებამ და განსაკუთრებით 2008 წლის რუსეთ-საქართველოს ომმა ცხადჰყო თუ რამდენად მნიშვნელოვანია კიბერ-სივრცის დაცულობის უზრუნველყოფა, კიბერდანაშაულთან ბრძოლის ერთიანი სახელმწიფო პოლიტიკის შემუშავება და ინფორმაციული უსაფრთხოების პოლიტიკის რეალურად გატარება. სწორედ ამ მიზნით 2014 წელს საქართველოს თავდაცვის სამინისტროს სისტემაში ჩამოყალიბდა სსიპ „კიბერუსაფრთხოების ბიურო“, რომელსაც დაევალა:

- ინფორმაციული სისტემების უსაფრთხოების აუდიტი, აპლიკაციებისა და ინფრასტრუქტურის უსაფრთხოების მექანიზმების შექმნა/დანერგვა;
- კომპიუტერული უსაფრთხოების ინციდენტების, სისუსტეებისა და მტკიცებულების დამუშავება, ანალიზი, რეაგირების მხარდაჭერა და კოორდინაცია;

- ინფორმაციული ტექნოლოგიების (სისტემების) უსაფრთხოების სფეროში მოქმედ ადგილობრივ, საერთაშორისო და უცხო ქვეყნების ორგანიზაციებთან, სახელმწიფო დაწესებულებებთან და კერძო სამართლის სუბიექტებთან ურთიერთობის დამყარება

დასკვნა

დღეს იუ-ს უზურნველყოფა მოიცავს ისეთ ცნებებს, როგორებიცაა მთლიანობა, ინფორმაციის კონფიდენციალობა და დაცულობა არასანქცირებული დაშვებისაგან და უზრუნველყოფა სისტემის ფუნქციონირების საიმედოობის. როგორც პრაქტიკამ აჩვენა, ეს ამოცანა ყველაზე უფრო ეფექტურად წყდება კრიპტოგრაფიის მეთოდების გასინჯული და ლიცენზირებული პროგრამული უზურნველყოფასთან ერთად გამოყენებით, ასევე გასაღებების ინფორმაციის საიმედო ინტელექტუალური მატარებლების გამოყენებით. ამ დროს ტექნიკური საიმედოობა, რომელიც ვლინდება როგორც სისტემის უნარი იმუშაოს დროის მოცემულ მონაკვეთში საშტატო სიტუაციაში მტყუნებათა გარეშე განსაზღვრავს სისტემის მდგრადობის მინიმალურ ზღრუბლს, რომლის გარეთაც დაკარგული ელემენტების და ფუნქციების აღდგენის სისტემის არ არსებობისას შეიძლება დადგეს კატასტროფა, შესაბამისად, სიცოცხლისუნარიანობას ინფორმაციული სისტემების გააჩნიათ განმსაზღვრელი მნიშვნელობა იუ-სთვის მთლიანობაში.

დაცვის ასეთი კონცეფციის ეფექტურობა სახელმწიფო და კომერციული ინფორმაციული სისტემებისათვის განსაზღვრავს უსაფრთხოების სახელმწიფო ინფრასტრუქტურას მთლიანობაში, ხოლო სიცოცხლისუნარიანობა ასეთი სისტემებისა - სამობილიზაციო მზადყოფნას შეიარაღებული ძალების, მრეწველობის, ეკონომიკის, სახალხო მეურნეობის და საზოგადოებისა მთლიანობაში როგორც ომის წარმოებისათვის, ასევე ტერიტორიული აქტების, სტიქიური უბედურებების და ტექნიკური კატასტროფების შედეგების ლიკვიდაციისათვის.

ამრიგად, მომავლის ინფორმაციული უსაფრთხოების სისტემებმა არა მარტო და არა იმდენად შეზღუდონ მომხმარებლების დაშვება პროგრამებთან და მონაცემებთან, არამედ განსაზღვრონ და მოახდინონ მათი უფლებამოსილების დელეგირება.

კიბერტექნიკური სივრცის ყველა ძირითადი ელემენტი (ადამიანები, ორგანიზაციები, პროგრამები და მოწყობილობები) სისტემურად განიცდიან იმის აუცილებლობას, რომ დამყარდეს ესა თუ ის ურთიერთობები დინამიურ საფუძველზე უფლებამოსილებათა და ცენტრის გარანტიის გარეშე ან ადრე დადგენილი შუამავლის გარანტიის გარეშე. აუცილებელია ახალი

ორგანიზაციულ-ტექნიკური გადაწყვეტილება ამ უმწვავესი პრობლემისა, რომლებიც გაითვალისწინებენ ავტონომიურობას ცალეკული წარმონაქმნებისა, რომლებიც ტერიტორიულად არიან გაბნეული და გააჩნიათ სხვადსხვა საუწყებო კუთვნილება, მასშტაბი, სირთულე და დინამიკა კრიტიკული ინფრასტრუქტურისა მთლიანობაში.

გამოკვლევები, რომლებიც ტარდება ამჟამად, სრულად როდი ითვალისწინებენ სხვადასხვა უწყებების ურთიერთმოქმედების მასშტაბს და კოორდინაციას რესურსების განვითარებისა და ადმინსიტრირების პოლიტიკაში, რაც ნეგატიურად აისახება ეროვნული ინფორმაციის სტრუქტურის დაცვის ხარისხზე. მომავალში კვლევები უნდა ტარდებოდეს აღმოჩენის სისტემების შექმნის მიმართულებით ინციდენტების პროგნოზირებისა და აღმოჩენის ელემენტებით, აგრეთვე სისტემის აღდგენისა და რეკონფიგურაციისათვის.

გადაწყვეტილებები, რომლებიც გავლენას ახდენენ ინფორმაციული ინფრასტრუქტურის მდგომარეობაზე, მიიღებიან როგორც წესი, ეკონომიკური, სამართლებრივი, ადმინისტრაციული და პოლიტიკური ფაქტორების გათვალისწინების გარეშე. აუცილებელი გამოკვლევების ჩატარება მთლიანობაში კიბერნეტიკული უსაფრთხოების პრობლემების გასაგებად და ურთიერთკავშირების დასადგენად ფაქტორებისა, რომლებიც აფორმებენ ინფორმაციული ინფრასტრუქტურის დაცვის სისტემას (კანონები, პოლიტიკა, ბაზრის სტრუქტურა, ეკონომიკური პირობები, ტექნოლოგიები).

აქედან გამომდინარე, შესაძლოა ჩამოვაყალიბოთ მიმართულებები, რომელსაც აუცილებლად ხაზი უნდა გაესვას ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავებისას:

- ინფორმაციის და ინფორმაციული სისტემების ინვენტარიზაცია;
- რისკების შეფასება და ჯგუფებად დაყოფა;
- ინფორმაციაზე წვდომის დაშვება-აკრძალვის პოლიტიკა;
- პაროლების და გასაღებების მართვა;
- კრიპტოგრაფია;
- მომხმარებლის მართვა;
- ლოგირება, მონიტორინგი და კონტროლი;
- ინფორმაციული სისტემების ფიზიკური უსაფრთხოება;
- ოპერატიული სისტმების დაცვა;

- მონაცემთა ბაზების უსაფრთხოება;

- სახიფათო და დავირუსებული პროგრამების დაცვა;

- გარე ინფორმაციული მოწყობილობების დაცვა;

- ინციდენტების მართვა;

- პროცედურების და პროცესების სტანდარტებთან შესაბამისობაში მოყვანა.

გამოყენებული ლიტერატურა:

1. კიბერუსაფრთხოების პოლიტიკა „საქართველოს თავდაცვის სამინისტრო“ 2014-1016.

2. საქართველოს თავდაცვის სამინისტროს სსიპ - კიბერუსაფრთხოების ბიუროს გენდერული თანასწორობის სტრატეგია.

3. „ინფორმაციული უსაფრთხოება“ - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთხოების მართვის წესები და ნორმები, გვ. 10 2011 წელი, 8 ნოემბერი.

4. საქართველოს თავდაცვის მინისტრის ბრძანება №26 2014 წლის 7 აპრილი ქ. თბილისი. „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“

5. „საჯარო სამართლის იურიდიული პირის“ - კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შესახებ“.

6. საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“.

7. ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოების სტრატეგიები, საერთო პრინციპები და რეკომენდაციები. საქართველოს კიბერუსაფრთხოების სტრატეგია

ვლადიმერ სვანაძე.

9. „ინფორმაციული უსაფრთხოების შესახებ“ (კანონპროექტის ანალიზი)

10. Осовенкий А.Г. Научно-технические предпосылки роста роли защиты информации в совремерныч информационныч технологияч./Изв. Вузовю Приборостроение, 2003. Т.46, №7.

11.Мелик-Гайназов И.В. Информациониые процессы и реальность – М., наука, 1998г.

12. Кузнецов В.А.,Раков М.А. Самоорганизация в технических системах – Киев, Наук, думка 1987г.

13. Корнеев В.В.,Гарев А.Ф., Васютин С.В., Раих В.В., База данных, Интелектуальая обработка информации – 2001г.

14. ჩოგოვაძე გ. ინფორმაცია: ინფორმაცია, საზოგადოება, ადამიანი, - საქართველო, თბილისი, 2003წ.

15. Bosikashvili Z., Kapanadze D., Zhvania T. “About Unified Model of Safety of Information Systems”.Reacent Advances in Computational Intelligance Proceedings of the 4yh WSEAS International Conference oCOMPUTATIONAL

INTELLIGENCE (CI'10). Universitataea Politehnica, Bucharest, Romania, April 20-22, 2010. Pg. 35-38;

16. Bosikashvili Z , The blocking meta-heuristics for combinatorial problems solving, The ACM Digital Library, World Scientific and Engineering Academy and Society (WSEAS) Stevens Point, Wisconsin, USA ©2010 ISBN: 978-960-474-179-3,

17. Bosikashvili Z , Lominadze.T,Factorization of combinatorial problems with blocking meta-heuristics, The ACM Digital Library, World Scientific and Engineering Academy and Society (WSEAS) Stevens Point, Wisconsin, USA ©2009 ISBN: 978-960-474-088-8,

18. Bosikashvili Z., Kapanadze D., Zhvania T., About formalization of the problem of the test control, Transactions Automated Control Systems #1(2), GTU, Tbilisi, 2007.

19.Karibskiy V.V., Etc., Technical diagnostics of objects of the control, M.: Energya, 1967;

20.Peter. R. Stephenson, A Formal Model for Information Risk Analysis Using Colored Petri Nets, http://www.daimi.au.dk/CPnets/workshop04/cpn/papers/stephenson.pdf;

21. ინფორმაციული უსაფრთხოების კონცეფცია ორგანიზაციებსა და დაწესებულებებში —— ბ.კახელი,იო. ქართველიშვილი

22. http://ka.wikipedia.org/ ტერმინთა განმარტება.

23. საქართველოს იუსტიციის სამინისტრო, მონაცემთა გაცლის სააგენტო მგს 27002:2011 8 ნოემბერი 2011 წელი ვერსია 1.0. „ინფორმაციული უსაფრთხოება - უსაფრთხოების მექანიზმები - ინფორმაციული უსაფრთხოების მართვის წესები და ნორმები - გვ.11

25. „საქართველო და ახალი გამოწვევები კიბერსივრცეში - ვლადიმერ სვანიძე

26. Содеринов А.А. и др. Информацционная безопосностъ предприятия – М. „Дашков и к", 2004.

27. Расторгчев С.П. Философия информацционной войны – М. Вуз – книга, 2001.

28.საქართველოს საკონსტიტუციო სასამართლოს 2008 წლის 30 ოქტომბრის #2/3/406.408 გადაწყვეტილება საქმეზე „საქართველოს სახალხო დამცველი და საქართველოს ახალგაზრდა იურისტთა ასოციაცია საქართველოს პარლამენტის წინააღმდეგ.

29.პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ ევროპის საბჭოს N108 კონვენცია; ასევე პერსონალური მონაცემების დამუშავებისა და გადაცემის დროს ფიზიკური პირების დაცვის შესახებ ევროპის პარლამენტისა და ევროპის საბჭოს დირექტივა (95/46/EC) და ევროპის ქვეყნების საუკეთესო გამოცდილება.

30. საქართველოს თავდაცვის მინისტრის ბრძანება №26 2014 წლის 7 აპრილი ქ. თბილისი, „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“

32. Прангишвили И.В. системный подход и обшественные закономерности. Серия Системыи проблемы управления – М.СИНТЕГ, 2000.)

33.Осовенкий А.Г. Научно-технические предпосылки роста роли защиты информации в совремерныч информационныч технологияч./Изв. Вузовю Приборостроение, 2003. Т.46, №7

34. Мелик-Гайназов И.В. Информациониые процессы и реальность – М., наука, 1998г.

35.Кузнецов В.А.,Раков М.А. Самоорганизация в технических системах – Киев, Наук, думка 1987г.

36. Корнеев В.В.,Гарев А.Ф., Васютин С.В., Раих В.В., База данных, Интелектуальая обработка информации – 2001г

37. „საინფორმაციო ომი“ - თამარ ბელქანია

38. „ჟენევის კონვენცია“ კიბერ ომების დასარეგულირებლად. - სანდრო ასათიანი

40. http://georgianreview.ge/2015/06/axaligamowvevebkibersivrce/?lang=ge 4/23

41.http://www3.weforum.org/docs/Global_IT_Report_2012.pdf

Кибербезопасность. Краеугольный камень безопасности современного общества,

http://aka.ms/TwC_Cyber_Paper

42. ჟურნალი „სოციალური ეკონომიკა“ - თ.ქიტიაშვილი უსადენო ქსელების კრიპტოგრაფიული დაცვის ზოგიერთი საკითხი გვ.72, თბილისი 2014წ.

43. საქართველოს ტექნიკური უნივერსიტეტი „შრომები მართვის ავტომატიზებული სისტემები“ - დავით ბურჭულაძე, თამარ ქიტიაშვილი - საინფორმაციო საზოგადოება და კიბერუსაფრთხოება გვ.168

44. საქართველოს ტექნიკური უნივერსიტეტი „შრომები მართვის ავტომატიზებული სისტემები“ - დავით ბურჭულაძე, გიორგი მაისურაძე, თამარ ქიტიაშვილი - ინფორმაცია და კიბერუსაფრთხოების სტრატეგია გვ. 173

45. ყოველწლიური საერთაშორისო სამეცნიერო კონფერენცია - „ხელისუფლება და საზოგადოება“- თამარ ქიტიაშვილი - სახელმწიფო სამსახურში ინფორმაციული უსაფრთხოების უზრუნველყოფის მექანიზმები თანამედროვე ეტაპზე.

46. საქართველოს ტექნიკური უნივერსიტეტის ბიზნეს-ინჟინერინგის ფაკულტეტი, ლიბერალურ მეცნიერებათა დეპარტამენტი, ევროინტეგრაციული პროცესების შემსწავლელი კვლევითი ცენტრი, IV საერთაშორისო სამეცნიერო სიმპოზიუმი „მეორე მსოფლიო ომი და სამხრეთ კავკასია“ - თამარ ქიტიაშვილი საქართველოს კანონმდებლობა ინფორმაციის უსაფრთხოების შესახებ და კიბერუსაფრთხოების საკითხი.

47. http://www.foreignaffairs.com/articles/66552/william-lynniii/defending-a-new domain.

48. საქართველოს თავდაცვის სამინისტრო, სსიპ - კიბერუსაფრთხოების ბიური - წლიური ანგარიში 2014 წ.

49. კიბერუსაფრთხოების პოლიტიკა თბილისი 2014-2015წწ.

50.«Международно-правовые стандарты обеспечения кибербезопасности.Первоочередныезадачи»
М.А.Кочубей, руководитель Научно-консультативного совета, Антитеррористический центр СНГ

51. Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов / Отв. ред. М.Б. Касенова; сост. О.В. Демидов и М.Б. Касенова. – М.: Статут, 2013. – с.]

52. Кибербезопасностъ – подходы к определению понатия - Безкоровайный М.М., кандидат технических наук, доцент Татузов А. Л., доктор технических наук, доцент

53.Взатмосвязъполитики и еффективности обиспечения кибербезопасности - Арон Кляйнер (Aaron Kleiner), Пол Николас (Paul Nicholas), Кевин **Салливан (Kevin Sullivan),** группа Microsoft Trustworthy Computing

54. საქართველოს თავდაცვის მინისტრის ბრძანება №27 2014 წლის 7 აპრილი ქ. თბილისი.