საქართველოს ტექნიკური უნივერსიტეტი

ხელნაწერის უფლებით

თამარ ქიტიაშვილი

ინფორმაცია- უსაფრთხოების სახელმწიფო სამსახურში

დოქტორის აკადემიური ხარისხის მოსაპოვებლად

წარდგენილი დისერტაციის

ა ვ ტ ო რ ე ფ ე რ ა ტ ი

სადოქტორო პროგრამა

სადოქოტორო პროგრამა „ინფორმატიკა“ - შიფრი 0401

თბილისი

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

სადისერტაციო ნაშრომის ძირითადი მიზანი

უკანასკნელ ათწლეულში მნიშვნელოვნად გაფართოვდა ინფორმაციული უსაფრთხოების უზურნველყოფის საშუალებები. მრავალი სხვადასხვა ორგანიზაცია ჩაერთო ინფორმაციის 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.

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

ძირითადი ამოცანები. ინფორმაციული უსაფრთხოება მოიცავს უსაფრთხოების მრავალ ასპექტს. საიმედო დაცვის ყველა საშუალების და მეთოდის გაერთიანებას. საიმედო ფიზიკური დაცვა საჭიროა მატერიალური აქტივების – სისტემების დაცულობის უზრუნველსაყოფად. კომუნიკაციის დაცვა (COMSEC) საჭიროა ინფორმაციის გადაცემის უსაფრთხოებისათვის. გამოსხივების დაცვა (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.

სადოქტორო ნაშრომის შინაარსი

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.

შესავალი. ინფორმაციული უსაფრთხოება არის ინფორმაციისა და ინფორმაციული სისტემების დაცვა, დაზიანებისა და განადგურებისაგან. დღეისათვის, როდესაც ინფორმაციულ სისტემებს მნიშვნელოვანი როლი აქვს ჩვენს ცხოვრებაში, ისმის მისი და 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 წარმოიშვა ინფორმაციის დაცვის აუცილებლობაც. 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 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.
- ინფორმაციის დაცვის სისტემა (იდს) უნდა აკმაყოფილებდეს ინფორმაციის უსაფრთხოების მოთხოვნილ დონეს, რისთვისაც საჭიროა მომხმარებელთა მომზადება და მათ მიერ ინფორმაციის დაცვისათვის გამიზნული ყველა წესის დაცვა.

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

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. ე. ი. მხედველობაში გვაქვს ორი ძირითადი 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.

აღნიშნული, შეიძლება ითქვას, ერთ-ერთი ურთულესი და უმნიშვნელოვანესი პრობლემის გადაწყვეტაში ჩართული არიან მსოფლიოში ინფორმაციული ტექნოლოგიების (იტ) წამყვანი კომპანიები, ექსპერტები, მეცნიერები, მიმდინარეობს ინტესიური და მსხვილმასშტაბიანი კვლევები და პროექტების დამუშავება, რომელთა ძირითად მეთოდოლოგიურ ინსტრუმენტს წარმოადგენს აპარატი სისტემური ანალიზისა და გადაწყვეტილებათა მიღების 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 დასაბუთებულობას.

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.

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

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 შემუშავებული კიბერუსაფრთხოების პოლიტიკა 2014–2016 წლებისათვის.

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.

ეს 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 სტანდარტებთან 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 დაკავშირებულ 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 შემთხვევაში, ძალიან რთული ხდება, განისაზღვროს რომელი სამართლებრივი ნორმა არეგულირებს კიბერინციდენტის კონკრეტულ შემთხვევას.

მესამე თავში განხილულია სახელმწიფოში კრიტიკული ინფრასტრუქტურის კიბერუსაფრთხოების უზრუნველყოფის ინოვაციური მეთოდები და საშუალებები, სარეჟიმო ობიექტის დაცვის სისტემის ფუნქციონირების ზოგადი მოდელი, სიტუაციური მიდგომის გამოყენება თანამედროვე სახელმწიფოს ინფრასტრუქტურის იუ-ს უზრუნველყოფასა და მდგრად განვითარებაში, ინფორმაციის ადაპტური დაცვის მოდელი, ინფორმაციული ტექნოლოგიების ინფრასტრუქტურა და ელექტრონული სერვერები.

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:

- 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 სასიცოცხლო ციკლისა;

- კონცეპტუალურ კომპლესურობას, ანუ დაცვის პრობლემის შესწავლას და რეალიზაციას, მისი განვითარების, აგების და გამოყენების ყველა პრობლემას.

ქვეყანაში ფართომასშტაბიანი ერთიანი ინფორმაციული სივრცის შექმნა აუცილებელია იმისათვის, რომ დაინერგოს სახელმწიფოს სიტუაციური მართვის სისტემა. ამის აუცილებლობაზე მიგვანიშნებს მსოფლიოში დღეს არსებული პირობები, 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 კანონზომიერებები, ვინაიდან მათმა იგნორირებამ შეიძლება გამოიწვიოს სახელმწიფოს არამდგრადობა, კატასტროფები, დაშლა ან დანერგვა. აღნიშნულის ერთ-ერთ სერიოზულ დამადასტურებელ მაგალითად შეიძლება დავასახელოთ „კანონზომიერება სისტემის პოტენციალის დამოკიდებულება მისი სტრუქტურული ელემენტების ურთიერთქმედების ხასიათზე ან სისტემის ორგანიზებულობის ხარისხზე“, რომლის თანახმადაც, თუ ორგანიზებულ სისტემაში A პოტენციალი P მრავალჯერ აღემატება ყველა შემადგენელი ელემენტების (ქვესისტემების, სახელმწიფოს შემდგენელი ელემენტების) პოტენციალების ჯამს

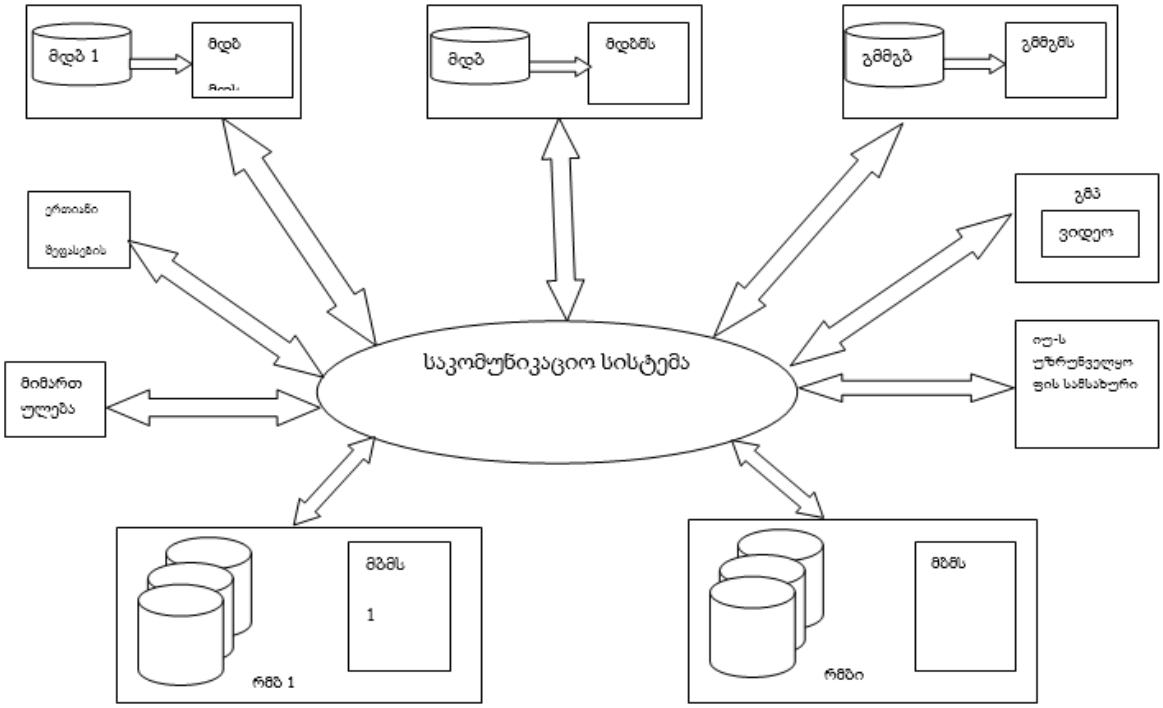
$$P(A)>[P(a_1)+P(a)+...+P(a_n)],$$

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

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

ძალზე გამარტივებული სქემატური მოდელი ქვეყნის სიტუაციური მართვის სისტემისა (ნახ.1.) 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 უზრუნველყოფის სამსახური, იზრუნებს ინფორმაციის წყაროებთან სანდო კავშირების დამყარებაზე და მთელი სისტემის უსაფრთხოებაზე.



ნახაზი. 1 სიტუაციური მართვის სისტემა

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.

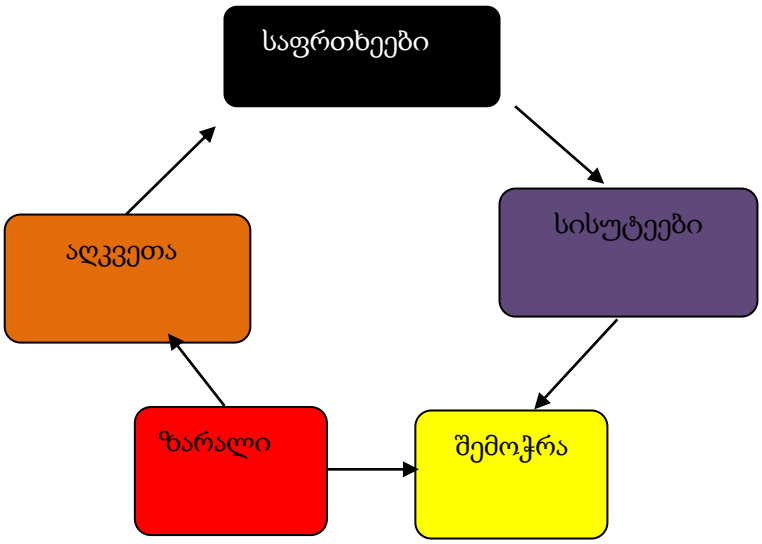
ინფორმაციული უსაფრთხოების რისკების მართვა უნდა იყოს უწყვეტი პროცესი. პროცესმა უნდა დაადგინოს ორგანიზაციული გარემო, შეაფასოს რისკები და გადაჭრას რისკები რისკებთან მოპყრობის გეგმის მიხედვით რეკომენდაციების და გადაწყვეტილებების დასანერგად. რისკების დასაშვებ დონეზე დაყვანისათვის რისკების მართვა აანალიზებს 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 პირების 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 სისტემების უსაფრთხოების უზრუნველყოფა პირველ რიგში მოიცავს სისუსტეების გამოვლენის და აღმოფხვრის ღონისძიებებს,

შეტევების აღმოჩენის და აღკვეთის სამუშაოებს, რომლის ციკლურ პროცესს წარმოადგენს ნახაზი 2.



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, რომლიც ასეთ საქმიანობას გააადვილებდა იმისთვის, რომ განხორციელებულიყო ინფორმაციული სისტემების უსაფრთხოების უზრუნველყოფის პროცესის სრულყოფა, საჭიროა მისი ადეკვატური და ეფექტური მოდელის შექმნა. წარმოდგენილი პროცესი ძნელად ფორმალიზებადია, რადგანაც მასში გასათვალისწინებელია როგორც აპარატურულ-პროგრამული ასპექტები, ასევე ადამიანური ფაქტორები.

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 მონიტორისფუნქციებში 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.
ინფორმაციის დაცვის უზრუნველყოფისათვის აუცილებელი საშუალებების მართვის მოდელირებისას უნდა განისაზრვროს სახარჯი რესურსების შემადგენლობა 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 ღირებულებები;
- დაცვის ყველა მეთოდის გადატეხვით მიყენებული ზარალის სიდიდე.

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, მთლიანობა მისი შენახვის და ღია კავშირის არხებით გადაცემას.

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 ფორმირება 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 გამთლიანებული ინფორმაცია გადაეცემა მომხარებელს.

თანამედროვე ინფორმაციული ტექნოლოგიების ერთადერთი უმნიშვნელოვანესი დამახასაითებელი თავისებურებებია 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. 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 პროცესების იტ–სისტემებში ინფორმაციული ველების ფორმირების მეშვეობით, ნეირონული ქსელების (ნქ) ინტელექტუალური მექანიზმები, არამკაფიო ლოგისტიკის და გენეტიკური ალგორითმების (გა) გამოყენებით.

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.

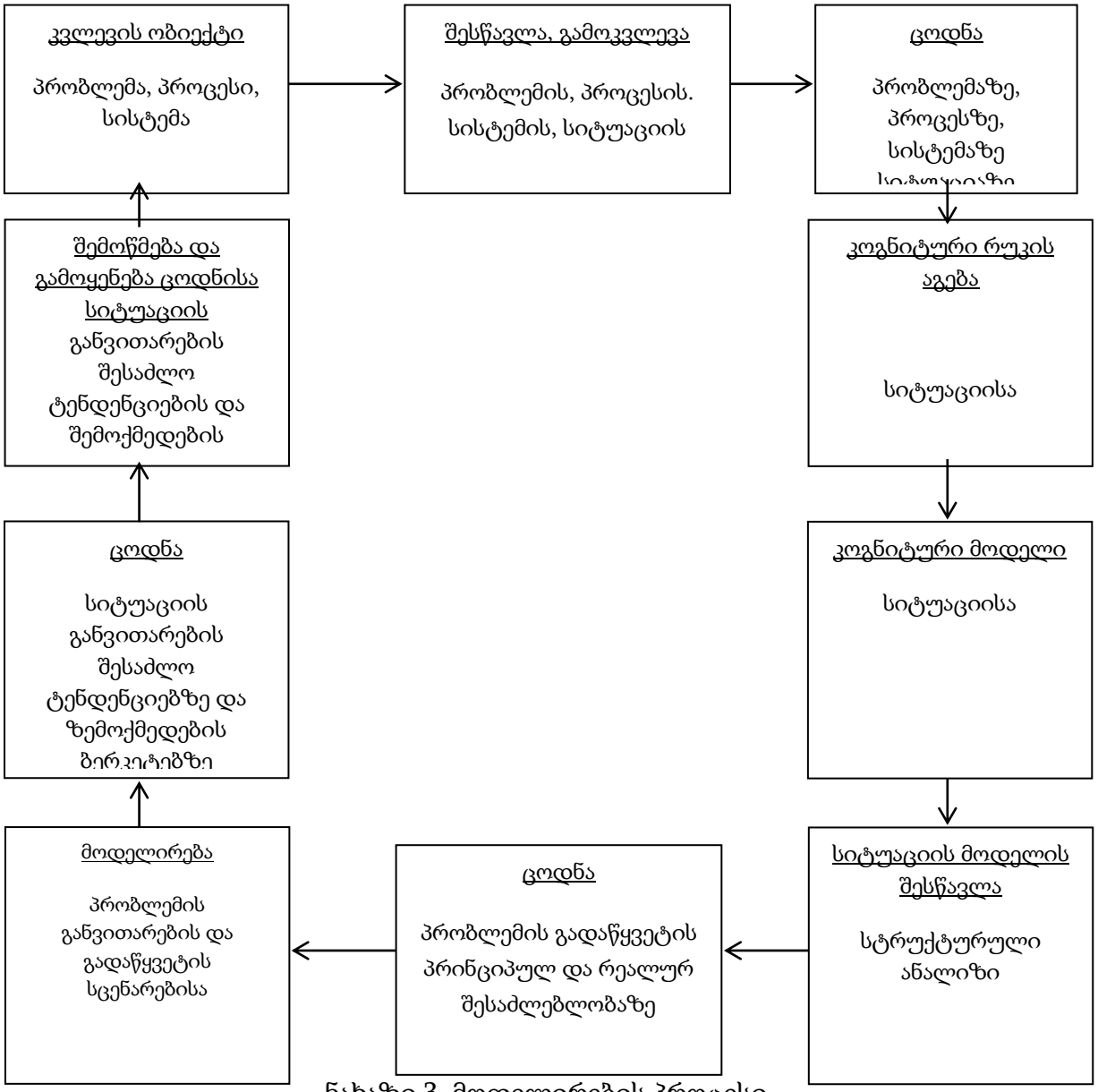
კაცობრიობამ მიაღწია თავისი განვითარების ისეთ ეტაპს, როცა მძლავრი ინფორმაციული ტექნოლოგიების - ავტომატიზებული სისტემების გამოყენებით შესაძლებელი ხდება წარმოდგენილი პრობლემების გადაწყვეტა და აღნიშნულ შეკითხვებზე წარმატებით პასუხის გაცემა.

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 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 ეკონომიკური, 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. ცოდნა საკვლევ პრობლემაზე ფართოვდება და ზუსტდება, ხოლო საწყისი მოდელი განიცდის სისტემატურ სრულყოფას.



ნახაზი 3. მოდელირების პროცესი.

რთული სიტუაციის მიმდინარე მდგომარეობის ანალიზისას აუცილებლად დგება შემდეგი საკითხები:

მართვის რომელი მეთოდები უნდა შეირჩეს მიზნობრივი ფაქტორების სასურველი ქცევის უზრუნველსაყოფად?

სიტუაციის როგორი ცვლილებებია შესაძლებელი (უახლოეს) მომავალში?

რა პირობები შეიძლება ამ დროს წარმოიშვას?

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:

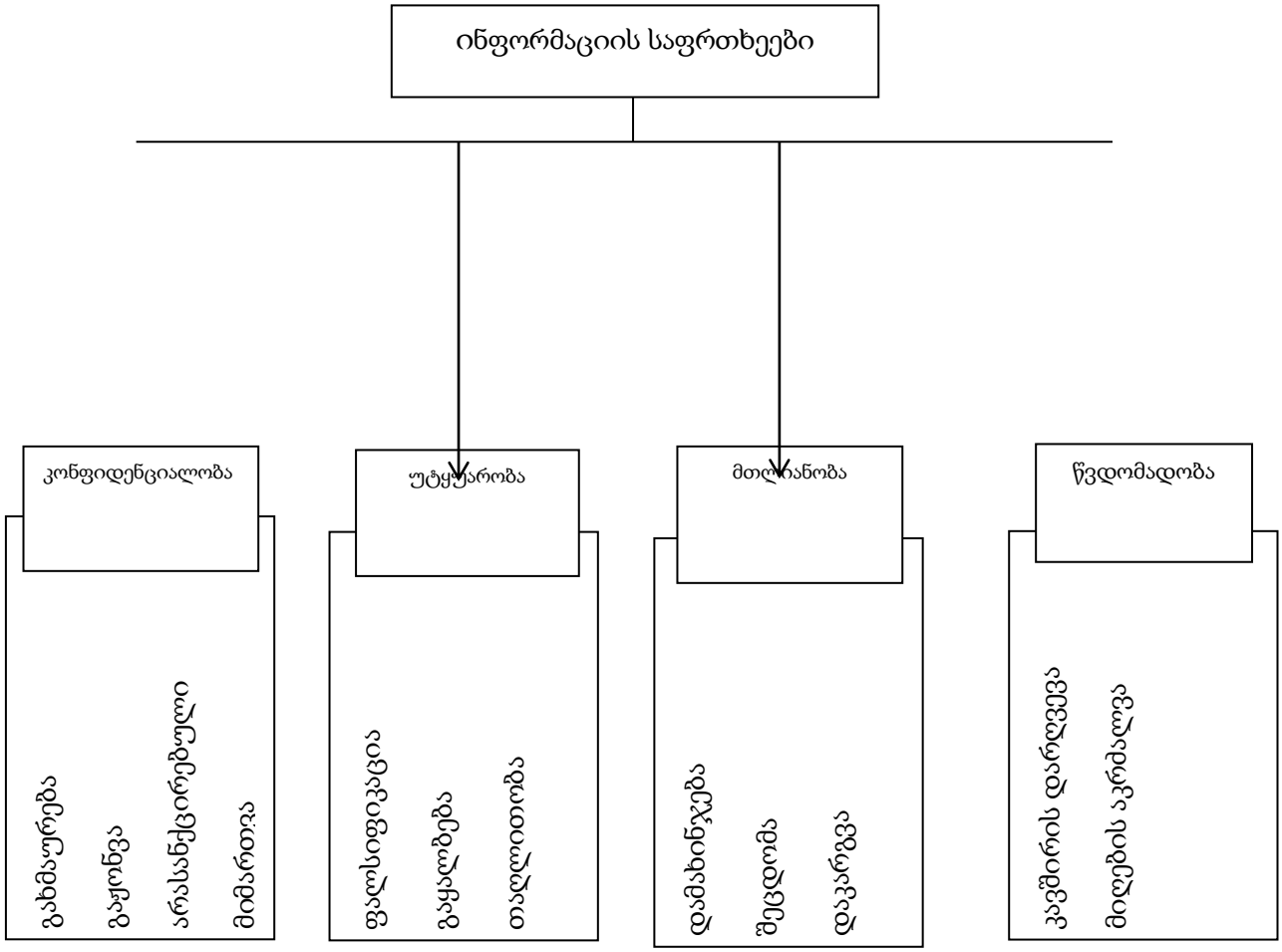
- მართვის შედეგების სიახლოვით დასახულ მიზანთან (ვარიანტების ეფექტურობის მაჩვენებლების მიხედვით);
- დანახარჯებით (ფინანსური, ფიზიკური, მორალური და ა.შ.), რომლებიც დაკავშირებული არიან ცალკეული ვარიანტების რეალიზაციასთან;
- შედეგების ხასიათის (შექცევადი, შეუქცევადი) მიხედვით, რეალურ სიტუაციაში შესაბამისი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

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“ მოვემზადოთ მათ დასაძლევად.

თითოეული საფრთხე, რომელიც ვლინდება ნახ.4-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 3. ინფორმაციის საფრთხეთა გამოვლენა

დასკვნა. დღეს იუ-ს უზურნველყოფა მოიცავს ისეთ ცნებებს, როგორებიცაა მთლიანობა, ინფორმაციის კონფიდენციალობა და დაცულობა არასანქცირებული დაშვებისაგან, და უზრუნველყოფა სისტემის ფუნქციონირების საიმედოობაა. როგორც პრაქტიკამ აჩვენა, ეს ამოცანა ყველაზე უფრო ეფექტურად წყდება კრიპტოგრაფიის მეთოდების გასინჯული და ლიცენზირებული პროგრამული უზურნველყოფასთან ერთად, 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 უნდა 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 სხვადასხვა 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 ადმინისტრირების 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 სისტემების დაცვა;
- მონაცემთა ბაზების უსაფრთხოება;
- სახიფათო და დავირუსებული პროგრამების დაცვა;
- გარე ინფორმაციული მოწყობილობების დაცვა;
- ინციდენტების მართვა;
- პროცედურების და პროცესების სტანდარტებთან შესაბამისობაში მოყვანა.

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 უზრუნველყოფით, 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 ჰაკერობა, კომპიუტერულ პროგრამებზე თავდასხმა მომხმარებლისთვის სერვისის 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.

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 შესაფასებლად და მისი გაუმჯობესების შესახებ უკუკავშირის უზრუნველსაყოფად.

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 პროფესი, 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.

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 დაცვა საჭიროა მატერიალური აქტივების – სისტემების დაცულობის უზრუნველსაყოფად. კომუნიკაციის დაცვა (COMSEC) საჭიროა ინფორმაციის გადაცემის უსაფრთხოებისათვის. გამოსხივების დაცვა (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.