საქართველოს ტექნიკური უნივერსიტეტი

ხელნაწერის უფლებით

ქეთევან ყიფიანი

ინფორმაციის დაცვის მეთოდების კვლევა სატელეკომუნიკაციო ქსელებისა და სისტემების სტრუქტურისა და ფუნქციონირების ალგორითმის გათვალისწინებით

დოქტორის აკადემიური ხარისხის მოსაპოვებლად

წარდგენილი დისერტაციის

ა ვ ტ ო რ ე ფ ე რ ა ტ ი

სადოქტორო პროგრამა: ”ტელეკომუნიკაცია“

შიფრი: 0402

თბილისი

2019

სამუშაო შესრულებულია საქართველოს ტექნიკურ უნივერსიტეტში
ენერგეტიკისა და ტელეკომუნიკაციის ფაკულტეტი
ტელეკომუნიკაციის დეპარტამენტი

ხელმძღვანელი: პროფესორი თ. კუპატაძე

რეცენზენტები:

დაცვა შედგება 2019 წლის ”-------” ”---------- ”-------” საათზე საქართველოს ტექნიკური უნივერსიტეტის ენერგეტიკისა და ტელეკომუნიკაციის ფაკულტეტის სადისერტაციო კოლეგიის სხდომაზე, კორპუსი VIII, აუდიტორია
მისამართი: 0175, თბილისი, კოსტავას 77.

დისერტაციის გაცნობა შეიძლება სტუ-ის ბიბლიოთეკაში,
ხოლო ავტორეფერატისა - ფაკულტეტის ვებგვერდზე

სადისერტაციო საბჭოს მდივანი, გ. გიგინეიშვილი
ასოცირებელი პროფესორი

ნაშრომის ზოგადი დახასიათება

ინფორმაციული სისტემების ფუნქციონირების ეფექტურობისა და ინფორმაციული სისტემების ქმედითუნარიანობის დარღვევა, შეიძლება ხდებოდეს ინფორმაციის დამახინჯების ან ბლოკირების გამო, რაც განსაკუთრებულად აქტუალური პრობლემაა რეალური დროის ინფორმაციის დაცვის ინტეგრირებული სისტემებისათვის. აქ გამოყენებული მათემატიკური მოდელები ეფუძნება გამოსაკვლევი პროცესების მიმდინარე და მოთხოვნილი მახასიათებლების ფარდობით ალბათურ წარმოდგენას, რაც დაკავშირებულია მათემატიკური აპარატის და პროგრამული მეტრიკის დიდ სიღრმეებთან. სადისერტაციო კვლევებში კი დგას სხვა ამოცანა, კერძოდ, დაწესებულების ან კომპანიის ინფორმაციული უსაფრთხოების უზრუნველყოფა უკვე არსებული, კონკრეტული პრობლემების შესაბამისი, საშუალებების გამოყენებით.

სამომავლოდ, ნივთების ინტერნეტი გარდაქმნის ჩვენს ცხოვრებას. მსოფლიოს ტექნოლოგიურად განვითარებული ქვეყნებისათვის ეს არის აწმყო და მათ დაინახეს, რომ ამ პროცესს მოყვა ახალი ხიფათები, ვინაიდან ძალზე ბევრი პირადი და კომერციული ინფორმაცია გაიშალა ეგრეთწოდებულ „ღრუბლებში“, ანუ ყველგან, ეს კი იმას ნიშნავს, რომ ინფორმაციის უსაფრთხოებას გაუჩნდება მრავალი ხიფათები, შემოტევების ახალი საშუალებები. ნივთების ინტერნეტი უბიძგებს დაწესებულებებსა და კომპანიებს, რომ განახორციელონ ყველგან ჩართულობა, რაც საინჟინრო სპეციალისტებს ავალებს უზრუნველყონ ასეთი ქსელების უსაფრთხოება.

თემის აქტუალობა: დღეისათვის, როდესაც მილიარდობით მომხმარებელი სარგებლობს სატელეკომუნიკაციო ქსელებით და იყენებენ საბანკო ანგარიშებს, ავსებენ საგადასახადო დეკლარაციებს, სარგებლობენ ინტერნეტ მაღაზიებით, ცხადია, ქსელში ინფორმაციის უსაფრთხოების პრობლემა ძალზე აქტუალურია.

ინფორმაციის დაცვის საშუალებების ტექნოლოგიურმა განვითარებამ დღეისათვის მიაღწია იმ დონეს, როდესაც პირველ პოზიციებზე უკვე წამოწეულია მათი გამოყენების მოხერხებულობა. იზრდება მოთხოვნილება, ქსელში არსებული ვითარების ვიზუალიზაციაზე – რეალურ დროში, მოხერხებული ფორმატით ვუთვალთვალოთ არსებულ მდგომარეობას. დაცვის საშუალებების ინტერფეისის განვითარება მნიშვნელოვნად შეამცირებს დროის ხანგრძლიობას ინფორმაციული უსაფრთხოების ინციდენტებზე ზემოქმედებისათვისაც.

სამუშაოს მიზანი: იმის შესაბამისად, თუ რა კატეგორიის დაცვა ესაჭიროება ობიექტს, ინფორმაციის უსაფრთხოების უზრუნველსაყოფად, უნდა განისაზღვროს შესაბამისი კონკრეტული მოთხოვნები. განსხვავებული კიბერშეტევები მოითხოვს განსხვავებულ ტექნოლოგიურ გადაწყვეტილებებს. სამუშაოს მიზანია, ჩასატარებელი ღონისძიებებისათვის ინფორმაციის დაცვის საშუალებების სწორად შერჩევის უზრუნველყოფის ხელშეწყობა.

ცნობილია, ობიექტების ინფორმაციული უსაფრთხოების უზრუნველყოფის შემდეგი ზომები და საშუალებები:
(ინფორმაციის წყარო: ელექტრონული ჟურნალი „ Network journal. Theory and Practike". http://network–journal mpei.ac.ru/cgi-bin/main.P.)

- საკანონმდებლო (სამართლებრივი) ზომები;
- ორგანიზაციული (ადმინისტრაციული) დაცვის ზომები;
- პროგრამულ - ტექნიკური ზომები;
- არასანქცირებული ჩართვებისა და მიერთებებისაგან დაცვის საშუალებები;
- იდენტიფიცირებისა და აუტენტიფიცირების საშუალებები;
- შეღწევების გამიჯვნის საშუალებები;
- საინფორმაციო და პროგრამული რესურსების მთლიანობის უზრუნველყოფისა და კონტროლის საშუალებები;

- მოვლენების ოპერატიული კონტროლისა და რეგისტრაციის საშუალებები;
- ინფორმაციის დაცვის კრიპტოგრაფიული საშუალებები;
- ინფორმაციის უსაფრთხოების უზრუნველყოფის სისტემის მართვა;
- დაცვის სისტემის ეფექტურობის კონტროლი;
- საინფორმაციო - სატელეკომუნიკაციო სისტემებისა და ქსელების დაცვის ფიზიკური ზომები და საშუალებები.

იმის შესაბამისად, თუ ინფორმაციის უსაფრთხოების უზრუნველსაყოფად რა კატეგორიის დაცვა გააჩნია ობიექტს, განისაზღვრება შესაბამისი კონკრეტული მოთხოვნები. აქ მნიშვნელოვანია ობიექტზე არსებული ინფორმაციის კონფიდენციალურობის ხარისხი (დონე) და მისი განთავსების პირობები.

სადისერტაციო ნაშრომში წარმოდგენილია სატელეკომუნიკაციო ქსელის ინფორმაციული უსაფრთხოების პრინციპების კვლევის ლიტერატურული მიმოხილვა, გაანალიზებულია 50 სამეცნიერო კვლევის შედეგები, რომლებშიც:

აღნიშნულია ინფორმაციის უსაფრთხოების კონტროლის შერჩევითი ხასიათის გამოყენების შესაძლებლობა, შეზღუდული რესურსებისა და საკონტროლო ღონისძიებისათვის გამოყოფილი დროის ხანგრძლიობით. განხილულია ხიფათების ანალიზის მეთოდები, რომლებიც დაკავშირებულია შორეული ელექტრონული აუტენტიფიკაციის პროცესთან, განხილულია მოდელირების კლასიკური სქემების გამოყენების შესაძლებლობა ინფორმაციული პროცესების კვლევისათვის, სისტემაში ინფორმაციის მთლიანობის და მიღწევადობის დარღვევისადმი ხიფათის არსებობის პირობებში. წარმოდგენილია ინფორმაციის მიტაცების სპეციალური ელექტრონული მოწყობილობის სიგნალების მახასიათებლების იმიტაციის შედეგი. შემოთავაზებულია სამეცნიერო-ტექნიკური გადაწყვეტილება, რომელიც მიეკუთვნება ტელეკომუნიკაციის სფეროს და შეიძლება გამოყენებული იქნას ქსელების დაცვისათვის გარე

დესტრუქციული ზემოქმედებებისაგან. წარმოდგენილია იმ დროითი რესურსის ოპტიმალურად გამოყენების კონცეფცია, რომელიც საჭიროა ინფორმაციის დაცულობის კომპლექსური ტექნიკური კონტროლისათვის, კერძოდ, ინფორმაციის გაჟონვის შესაძლებლობის კონტროლისათვის, თანმხლები ელექტრომაგნიტური გამოსხივებისა და ზედდების შედეგად. განხილულია სატელეკომუნიკაციო ქსელის შესასვლელსა და გამოსასვლელზე ტრაფიკების კორელაციაზე შეტევის შემთხვევა, აგრეთვე ტრაფიკის მარკირების გამოყენება შეტევის შედეგიანობის გაზრდის მიზნით.

კვლევის ობიექტი და მეთოდები: დაწესებულების ან კომპანიის ინფორმაციული უსაფრთხოების უზრუნველსაყოფად, დისერტაციის შედეგები ეფუძნება ინჟინრულ ხედვასა და მიდგომას, რომლის მიზანია, ერთის მხრივ დაწესებულებას ან კომპანიას გაუმარტივოს ინფორმაციის, მათთვის აუცილებელი დაცვის საშუალების შერჩევა, ინფორმაციის დაცვის კომპლექსური სისტემის შექმნისათვის და მეორეს მხრივ დაცვის კომპლექსური სისტემა გახადოს კონკრეტული ობიექტისათვის ოპტიმალური, კომპლექსში გამოყენებული დაცვის საშუალებების მინიმალური რაოდენობის შერჩევის საფუძველზე, რაც ხარჯების შესაბამისად, ოპტიმიზაციის პროცესის განხორციელების ექვივალენტურია.

ნაშრომის ძირითადი შედეგები და სიახლე: სადისერტაციო ნაშრომში შემოთავაზებულია ინფორმაციის დაცვის საშუალებების ნაკრების ოპტიმალურობის კრიტერიუმი, რომელმაც უნდა უზრუნველყოს, ნორმატიული დოკუმენტების მოთხოვნების შესაბამისად, ინფორმაციის დაცვის კომპლექსური სისტემის შექმნა.

შედეგების გამოყენების სფერო: ინფორმაციის უსაფრთხოების უზრუნველყოფის სხვადასხვა საშუალებების ინტეგრაციის დროს, გარანტირებული, აუცილებელი ან დასაშვები დონეების შეფასების შესაძლებლობების პირობების ჩამოყალიბება, ინფორმაციის დაცვის

მოთხოვნების შესაბამისი საშუალებების სერტიფიცირებული სისტემის საფუძველზე.

ნაშრომის აპრობაცია. სადისერტაციო ნაშრომის ძირითადი შედეგები მოხსენებული და განხილულია სხვადასხვა დროს გამართულ სემინარებსა და კონფერენციებზე:

1. მე-2 საერთაშორისო სამეცნიერო კონფერენცია. „ენერგეტიკა: რეგიონული პრობლემები და განვითარების პერსპექტივები“ მაისი, 2013 წ; 327 – 331 გვ.
2. მე-3 საერთაშორისო სამეცნიერო კონფერენცია. „ენერგეტიკა: რეგიონული პრობლემები და განვითარების პერსპექტივები“ ოქტომბერი, 2015 წ; 136 – 138 გვ.
3. საერთაშორისო სამეცნიერო კონფერენცია. „მდგრადი ენერგეტიკა: გამოწვევები და განვითარების პერსპექტივები.“ ივნისი, 2015 წ; 141 – 145 გვ.
4. მე-4 საერთაშორისო სამეცნიერო კონფერენცია. „ენერგეტიკა: რეგიონული პრობლემები და განვითარების პერსპექტივები.“ ოქტომბერი, 2016 წ; 147 – 151 გვ.
5. პირველ, მეორე და მესამე კოლოქვიუმებზე (სტუ, 2013 – 2018წ);
6. წინასწარ დაცვაზე (სტუ, 03.05.2019 წ.);
7. პერსონალურ მონაცემთა დაცვის სახელმწიფო ინსპექტორის სამსახურის სერთიფიკატი, ტრენინგში: „პერსონალური მონაცემების დაცვა“ – მონაწილეობისათვის.

ცნობები დისერტაციის მოცულობისა და სტრუქტურის შესახებ: ნაშრომი შედგება შესავალის, ოთხი თავისაგან, დასკვნისა და გამოყენებული ლიტერატურის 50 ჩამონათვალისაგან. ნაშრომის სრული მოცულობა შეადგენს 103 გვერდს, მათ შორის 6 ცხრილი და 4 ნახაზი.

ნაშრომის მოკლე შინაარსი

პირველი თავი - ინფორმაციული უსაფრთხოების დარღვევის მიზეზების შეფასება. გამოყენებულია კომპანია Zecurion-ის ანალიტიკური განყოფილების ანგარიშში თავმოყრილი ინფორმაცია კომპანიების შინაგანი უსაფრთხოების შემთხვევებთან დაკავშირებით, სახელმწიფო დაწესებულებებში, კომერციულ ორგანიზაციებში და იძლევა დარგებში არსებული ვითარებების სრულ სურათს, რაც განსაკუთრებულად საიმედო მონაცემებს შეიცავს, სრულყოფილი ანალიზის ჩასატარებლად.

გაანალიზებულია გაჟონვის წყაროები. რიგი ორგანიზაციებისათვის აუცილებლობას წარმოადგენს ინფორმაციის დაცულობის მდგომარეობის შეფასება, რათა მინიმუმამდე იქნას დაყვანილი ის სახიფათო მოვლენები, რომლებიც დაკავშირებულია თაღლითურ ქმედებებთან ელექტრონული ურთიერთქმედებების პროცესში. სახიფათო მოვლენის შედეგი შეფასებულია ფორმულით:

$$R = \sum_{i=1}^{M} [P(U_i) \cdot L(U_i)],$$

აქ U_i არის i – ური სახიფათო მოვლენა;

$P(U_i)$ - i- ური სახიფათო მოვლენის მოსალოდნელი ალბათობა;

$L(U_i)$ - i - ური სახიფათო მოვლენისგან შესაძლო ზარალის ოდენობა;

M- მოსალოდნელი სახიფათო მოვლენების რაოდენობა.

ინციდენტების რაოდენობა უმნიშვნელოდ იცვლება წლების განმავლობაში. წლიდან - წლამდე ინციდენტების რაოდენობის გათანაბრების ტენდენცია აღინიშნება Zecurion-ის ანალიტიკური განყოფილების ანგარიშებშიც. ამის ძირითადი მიზეზია - მასობრივი ინფორმაციის საშუალებების გაჯერება შეტყობინებებით გაჟონვების შესახებ.

სადისერტაციო ნაშრომში წარმოდგენილია მსოფლიოში გაჟონვების გეოგრაფიული განაწილება, გაჟონვების დარგობრივი სახეცვლილება,

გაჟონვების არხები, გაჟონვების შედეგები და გაჟონვების მიზეზები. მოყვანილია მაგალითი იმის შესახებ, რომ არსებობს ინფორმაციის გაჟონვები, რომელთა თავიდან აცილება ტექნიკური საშუალებებით შეუძლებელია და ტექნიკური საშუალებების დონეზე აუცილებლად უნდა იქნას განხილული ორგანიზაციული საკითხები.

მეორე თავი – სატელეკომუნიკაციო ქსელში პერსონალური მონაცემების დაცვის პრობლემები. რა ითვლება პერსონალურ მონაცემებად? განსაზღვრის შესაბამისად – ეს არის ნებისმიერი ინფორმაცია, რომელიც პირდაპირ ან ირიბად ეხება გარკვეულ ან გასარკვევ ფიზიკურ პირს (პერსონალური მონაცემების სუბიექტს). მაგალითად, თუ მითითებულია სუბიექტის მისამართი, მაგრამ ამ მონაცემებს არ ახლავს სახელი და გვარი, ესეც აგრეთვე არის პერსონალური მონაცემები, მაგრამ უსახური, რადგანაც პერსონალური მონაცემების სუბიექტის დადგენა შეუძლებელია დამატებითი მონაცემების გარეშე (პერსონალური დაცვის ასეთი კლასიფიკაცია წარმოდგენილია: // Вестник связи, №9, 2015, გვ.6.).

როდესაც დასრულდება ინფორმაციული საზოგადოების კონცეფციის რეალიზება (ელექტრონული მთავრობა, სახელმწიფო მომსახურების უზრუნველყოფა ინტერნეტით და ა. შ) შეიქმნება „ღია გასაღებების“ ინფრაქტრუქტურა. მაგრამ, ამ შემთხვევაშიც წარმოიქმნება ქსელური უსაფრთხოების პრობლემა. ღია გასაღებების ინფრასტრუქტურაც დაუცველი აღმოჩნდება შემოტევებისაგან, ვინაიდან მისი საქსელო კომპონენტები გაფანტულია ღია ქსელებში. გასათვალისწინებელია, რომ ინფორმაციის მისაღებად, ნებისმიერ შემთხვევაში აუცილებელია მიერთების ქსელის არსებობა, შესაბამისად ინფორმაციული უსაფრთხოების საკითხის გადასაწყვეტად, საჭიროა შესაბამისი რესურსებით სატელეკომუნიკაციო სივრცის უზრუნველყოფა სახელმწიფო დონეზე. უნდა არსებობდეს ინფორმაციის უსაფრთხოების უზრუნველყოფის ნაციონალური ცენტრი, სადაც შეისწავლიან ყველა არსებულ საკითხს და შეიმუშავებენ მათთან გამკლავების ღონისძიებებს. რა შეიძლება

ზემოქმედებდეს პერსონალური მონაცემების გაჟონვის ალბათობაზე - ძირითადია, დასამუშავებელ პერსონალურ მონაცემებში ცნობების მოცულობა.

ცხრილი 1. პერსონალური მონაცემების შესახებ ჩანაწერების რაოდენობა

პერსონალური მონაცემების შესახებ ჩანაწერების რაოდენობა	რესპოდენტების რაოდენობა პროცენტებში,რომლებიც ამუშავებენ პერსონალურ მონაცემებს
მილიონზე მეტი	16%
500 ათასიდან მილიონამდე	6%
100 ათასიდან 500 ათასამდე	5%
50 ათასიდან 100 ათასამდე	4%
10 ათასიდან 50 ათასამდე	20%
1000-დან 10 ათასამდე	20%
1000-ზე ნაკლები	19%
ანალიზს არ ექვემდებარება	10%

აქედან ჩანს, რომ ნახევარზე მეტი რესპოდენტი ამუშავებს არანაკლებ 10 ათასი პიროვნების პერსონალურ მონაცემებს და შესაბამისად, ასეთი ინფორმაციიდან გაჟონვების რაოდენობა იქნება ძალზე დამაფიქრებელი.

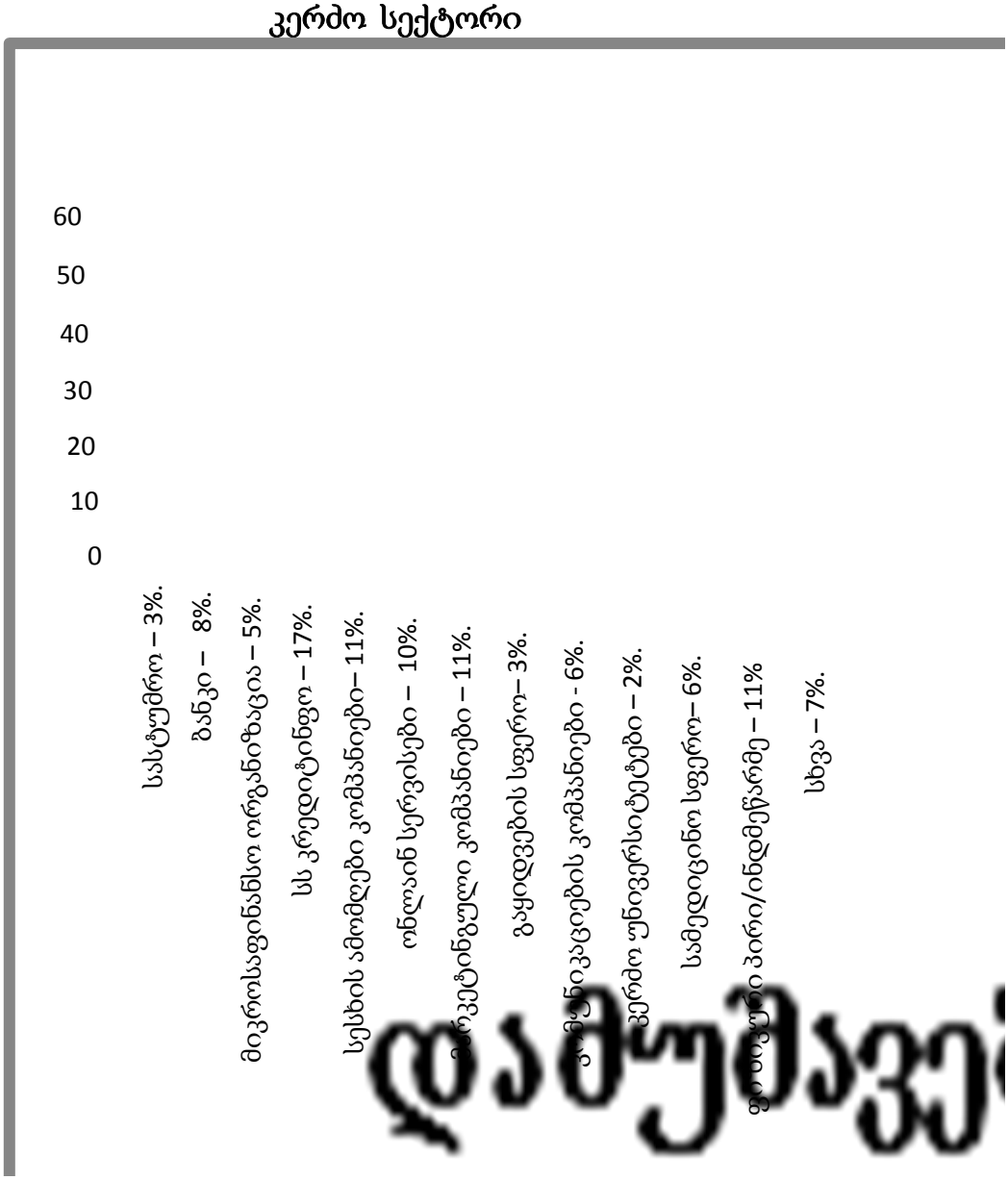
შემდეგი მნიშვნელოვანი საკითხია, თუ ვის და რა რაოდენობის პირებს აქვთ წვდომა პერსონალურ მონაცემებზე:

ცხრილი 2. პერსონალურ მონაცემებზე წვდომის შესაძლო მაჩვენებლები

ინფორმაციული ტექნოლოგიების სამსახურის თანამშრომლები	41%
მენეჯერები და ძირითადი ქვედანაყოფების ხელმძღვანელები	13%
ქვედანაყოფების თანამშრომლები	12%
ანალიტიკური სამსახურის თანამშრომლები	10%
ტექნიკური უზრუნველყოფის სამსახურების თანამშრომლები	10%
უსაფრთხოების სამსახურების თანამშრომლები	4%
არ ექვემდებარება აღწერას	10%

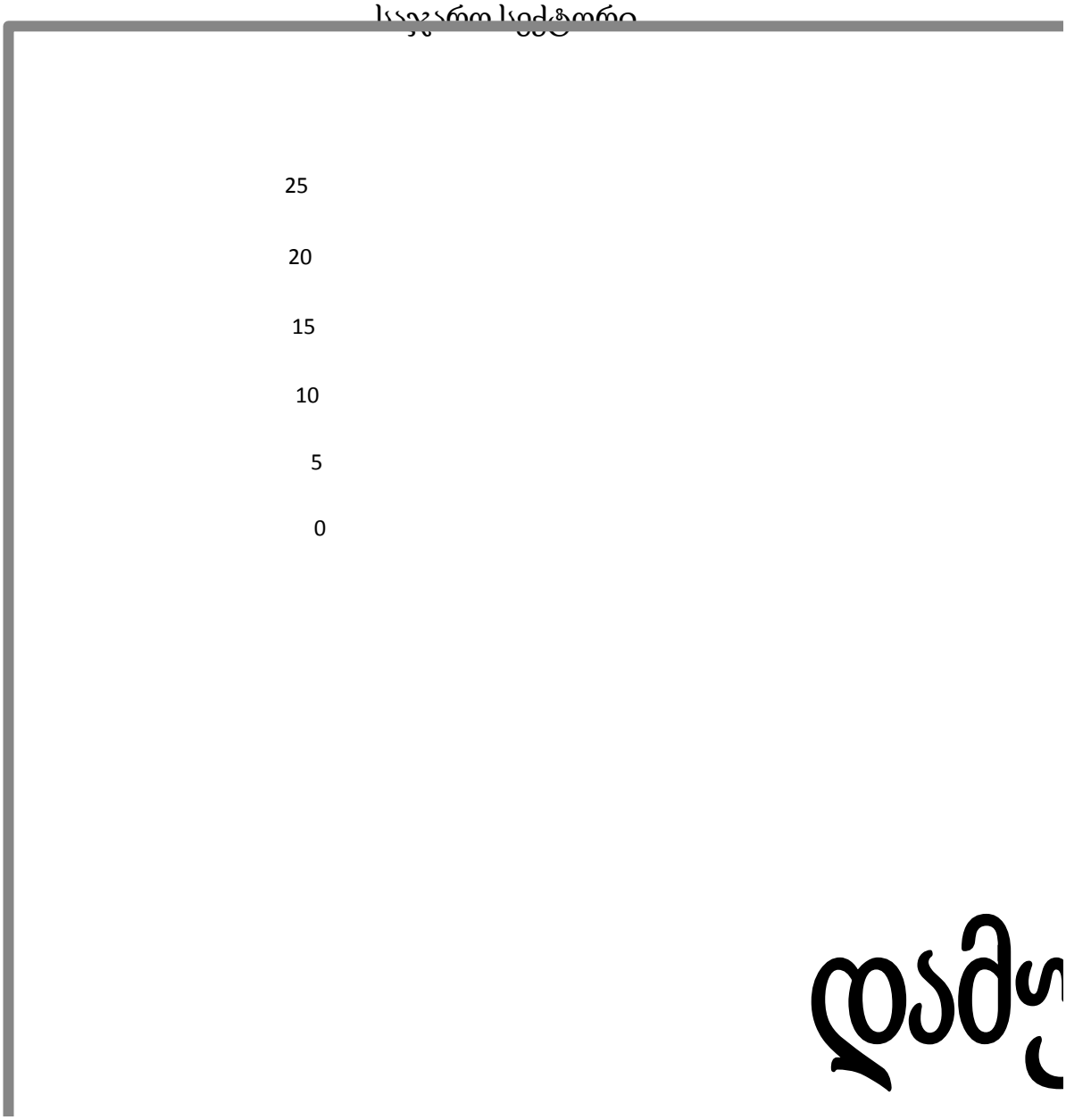
პრაქტიკულად, მხოლოდ უსაფრთხოების სამსახურის თანამშრომლების დაშვება პერსონალურ მონაცემებთან შეესაბამება 4%–ს, რაც ძალზე დამაფიქრებელია.

საქართველოსათვის, პერსონალური მონაცემთა დაცვის სახელმწიფო ინსპექტორის სამსახურის, პერსონალურ მონაცემთა დაცის მდგომარეობის და ინსპექტორის საქმიანობის შესახებ 2018 წლის ანგარიშების შესაბამისად, კერძო სექტორში შესწავლილია მონაცემთა დამუშავების 355, ხოლო საჯარო სექტორში 115 შემთხვევა. შესწავლის შედეგები მოცემულია ნახაზ 1–ზე და ნახაზ 2-ზე.



ნახაზი 1. საქართველოს, პერსონალურ მონაცემთა დაცვის სახელმწიფო ინსპექტორის სამსახურის 2018 წლის ანგარიშიდან – მდგომარეობა კერძო სექტორში

(პერსონალურ მონაცემთა დაცვის სახელმწიფო ინსპექტორის სამსახურის ნებართვით. 17.05.2019)



ნახაზი 2. საქართველოს, პერსონალურ მონაცემთა დაცვის სახელმწიფო ინსპექტორის სამსახურის 2018 წლის ანგარიშიდან – მდგომარეობა საჯარო სექტორში

(პერსონალურ მონაცემთა დაცვის სახელმწიფო ინსპექტორის სამსახურის ნებართვით. 17.05.2019)

მეორე თავში განხილულია სამეტყველო ინფორმაციის დაცვის პრობლემები. რიგ ორგანიზაციებსა და დაწესებულებებში ინფორმაციის მნიშვნელოვან წილს წარმოადგენს სამეტყველო ინფორმაცია, რომელსაც იყენებენ თანამშრომლები, თავიანთი სამსახურებრივი მოვალეობის შესრულების დროს. ასეთი ინფორმაციის ფასეულობა და ინფორმატულობის დონე, რაც დამახასიათებელია სამეტყველო ინფორმაციისათვის, იწვევს მის გადაქცევას მიტაცების ობიექტად. ამასთანავე, ბოროტმზრახველები იყენებენ დაზვერვის ტექნიკური საშუალებების სრულ თანამედროვე არსენალს. ამის შესაბამისად შექმნილი, სამეტყველო ინფორმაციის გაჟონვის არხები ქმნიან, ორგანიზაციებისა და დაწესებულებების საქმიანობისათვის სერიოზულ საფრთხეს.

სამეტყველო, საზოგადოდ აკუსტიკური, ინფორმაციის გაჟონვის შესაძლებლობების არსებობა უნდა განისაზღვროს შემდეგი ამოცანების გადაწყვეტის საფუძველზე:

- დამუშავდეს აკუსტიკური ინფორმაციის გაჟონვის შესაძლო წყაროებისათვის გაჟონვის შესაბამისი მოდელების სინთეზის თეორიული საფუძვლები;
- განხორციელდეს აკუსტიკური ინფორმაციის მიტაცების შესაძლებლობათა ფუნქციონალური დეკომპოზიცია;
- აკუსტიკური ინფორმაციის შესაძლო გაჟონვის განსაზღვრის ეფექტურობის შეფასება;
- აუცილებელია, პრაქტიკული ცდებით შეფასდეს აკუსტიკური ინფორმაციის გაჟონვის მოდელების პარამეტრების სრული შესაბამისობა, ინფორმაციის უსაფრთხოებისათვის შერჩეული დაცვის ვიბროაკუსტიკური საშუალებების პარამეტრებთან.

მეორე თავში განხილულია ინფოსაკომუნიკაციო სისტემების კიბერუსაფრთხოება და ინტეგრირებული ინფოსაკომუნიკაციო სისტემის ფუნქციონირების უსაფრთხოება. უსადენო ტექნოლოგიების ქსელები, განაწილებული და აგრეთვე ღრუბლების ტექნოლოგიები, სოციალური

ქსელები აფართოებენ ინტერნეტის გლობალური ქსელის გავლენას ინფორმაციული პროცესების საიმედობასა და უსაფრთხოებაზე და საინფორმაციო მომსახურების მიწოდებაზე. ამრიდაგ, კიბერსივრცე აერთიანებს პერსონალურო კომპიუტერებისა და კომპიუტერული ქსელების მომხმარებლებს, რომლების ერთიანდებიან ლოკალურ ქსელებში და ინტერნეტში ისე, რომ გარკვეული ხარისხით გამჭირვალე და ხელმისაწვდომი ხდებიან მომსახურების სახეობები, რომლებიც შექმნილია და უშუალოდ, ან ირიბად განაწილებულია ინტერნეტში.

იზოლირებული მოწყობილობებიც კი შეიძლება აღმოჩნდნენ კიბერსივრცის ნაწილები, თუ ისინი დრო და დრო ერთმანეთში ცვლიან ინფორმაციას კომპიუტერულ მოწყობილობილობებთან და კომპიუტერულ სისტემებთან, მონაცვლებადი მატარებლების მეშვეობით. ამის კარგ მაგალითს წარმოადგენს ასეთი მოწყობილობების განახლება BIOS (firewall) - ით. შედეგად, ეს მოწყობილობები ხდებიან დაუცველი დაზიანებული პროგრამების ზემოქმედებით, როგორებიცაა ვირუსები და ჭიები.

სადისერტაციო ნაშრომში კიბერუსაფრთხოება განხილულია შემდეგნაირად:

– როგორც მოქმედებათა პოლიტიკის ერთობლიობა, რომლებიც გამიზნულია ინტეგრირებული ქსელების, მისი შემადგენელი მოწყობილობებისა და საინფორმაციო ტექნოლოგიების კომპონენტების დასაცავად არასანქციონირებული ჩართვების, ცვლილებების, ქურდობის და ღირებული რესურსის განადგურებისაგან დასაცავად;

– როგორც ღონისძიებათა ერთობლიობა, სისრულისა და მომსახურების გარანტირებული ხარისხის უზრუნველსაყოფად ხიფათების ცვლადი გარემოს არსებობის პირობებში.

აქედან გამომდინარე, უსაფრთხოების უზრუნველყოფა შესაბამისი პროგრამულ–აპარატურული საშუალებების მარტივი გაერთიანებით შეუძლებელი ხდება. ინფორმაციის უსაფრთხოება უნდა განიხილებოდეს როგორც ახალი მეთოდების, საინფორმაციო სისტემებისა და მომსახურების

სახეობების დაცვის ეფექტური საშუალებების ფორმირების პროცესი და მეთოდები.

კიბერსფეროსათვის საჭიროა აგრეთვე მოსალოდნელი ხიფათების მართვა. ეს პროცესი მოიცავს იმ კომპონენტების იდენტიფიკაციას, რომლებიც უნდა იქნან დაცული. იმისათვის, რომ გავამარტივოთ ხიფათის ანალიზი, აუცილებელია, რომ განხილული იქნას დაცვის დარღვევების მცდელობები, რომლებიც მიეკუთვნებიან შემდეგ კატეგორიებს:

1. დაცვის დარღვევა მომსახურების წყვეტის სახით. დარღვევის ეს ტიპი მომხმარებლებს უწყვიტავს მომსახურების სახეობებზე წვდომას დროებით ან მუდმივად, მომსახურების პროცესზე შეზღუდვა შეიძლება მიეკუთვნოს მომსახურების შეწყვეტას DoS–ით (Denial of Service –უარი მომსახურებაზე), მომსახურებაზე განაწილებული უარებით DDoS(Distributed Denial of Service – განაწილებული უარი მომსახურებაზე), შეიძლება დანგრეული იქნას მომსახურების უზრუნველმყოფელი ინფრასტრუქტურა.
2. რესურსზე არასანქცირებული მიერთება. შემოტევის ეს ტიპი მოიცავს ინფორმაციის მითვისებას ან ინფრასტრუქტურის არასწორ გამოყენებას. ასეთი შეტევები მნიშვნელოვნად ზემოქმედებენ კიბერუსაფრთხოებაზე, მაშინ, როდესაც შემოტევა არის დიდი მასშტაბის.
3. კიბერსივრცის ობიექტების მითვისება, ობიექტებზე კონტროლის მითვისება, შესაძლებელია ასეთი ობიექტების გამოყენებაც სხვა ობიექტებზე კიბერშეტევებისათვის.

მესამე თავი – ინფორმაციის დაცვის საშუალებების განსაზღვრა. როდესაც ტექნიკური მოთხოვნები, რომლებიც დაცული უნდა იყოს, გარკვეულია სადისერტაციო ნაშრომში დგება ინფორმაციის დაცვის ურთიერთთავსებადი ტექნიკური საშუალებების შერჩევის ამოცანა. ამისათვის შემოთავაზებულია მოსალოდნელი საფრთხეების მოდელის შედგენა, შემდეგი სახით:

$$Aj = (Pj ; Xj),$$

სადაც, Pj - არის მოსალოდნელი საფრთხის ალბათობა;

Xj - ზიანის ხარისხი, რომელიც განისაზღვრება უსაფრთხოების დარღვევით გამოწვეული შედეგებით (კონფიდენციალურობა, ინფორმაციის სისრულე, მიღწევადობა).

ამასთანავე, მოსალოდნელი საფრთხის განხორციელება (რეალიზაცია) განისაზღვრება ინფორმაციის დაცულობის დონის საფუძველზე, ბოროტმოქმედის შესაძლებლობების გათვალისწინებით.

თუ ცნობილი იქნება ობიექტის დაცულობის ალბათობა და ბოროტმომქმედის შესაძლო პოტენციალი, ობიექტისათვის მოსალოდნელი საფრთხისა. ლოგიკურ–ალბათური ფუნქციის გამოსახულება ასე ჩაიწერება:

$$Pj = (P1 , P2);$$

სადაც P1 – არის მისაღწევი დაცულობის ალბათობა;

P2 – ბოროტმოქმედის შესაძლებლობების (პოტენციალის) ალბათობა;

თუ ვიმსჯელებთ ობიექტზე უკვე არსებული დაცვის სისტემის შესაძლებლობებიდან, მაშინ მოსალოდნელი საფრთხის ლოგიკურ–ალბათური ფუნქციის გამოსახულება იქნება:

$$Pj = (P1 \text{ საწყისი} , P2),$$

სადაც, P1 საწყისი – ინფორმაციის დაცვის კომპლექსური სისტემის შექმნამდე, პროექტით გათვალისწინებული დაცულობის ალბათობაა.

ინფორმაციაზე შეტევებისაგან დაცულობის შეფასება, ნებისმიერი სახის შემოტევის რისკის შესწავლისათვის, სადისერტაციო ნაშრომში შემოთავაზებულია ზოგადი მიდგომა, რომელიც დამუშავებულია და ცნობილია NGN (Next Generation Network - შემდეგი თაობის ქსელები) ობიექტებისათვის, ანუ მსოფლიოში დღეს არსებული სატელეკომუნიკაციო სისტემებისა და ქსელებისათვის, ლოგიკურ–ალბათურ ჩარჩოებში და შემოწმებულია სხვადასხვა პრაქტიკულ მაგალითებზე (შემთხვევებზე). აღმოჩენილია ბოტ–შეტევების რისკების თვისებები, გამოკვლეულია რისკების მოდელები და მიღებულია რისკების ექსტრემალური მნიშვნელობები. დისერტაციაში ცხრილების სახით მოცემულია მოთხოვნათა ის ერთობლიობები, რომლებიც განსაზღვრავენ

კონფიდენციალური ინფორმაციის კრიპტოგრაფიული დაცვის კლასებს, სატელეკომუნიკაციო ქსელის მნიშვნელობათა კატეგორიებს და სატელეკომუნიკაციო სისტემებისა და ქსელების მზადყოფნის კოეფიციენტებს, რაც საშუალებას იძლევა შევაფასოთ მოსალოდნელი საფრთხეების მოდელის პარამეტრები.

სადისერტაციო ნაშრომში დაჯგუფებულია ინფორმაციის დაცვის აპარატურულ–პროგრამული საშუალებები და ჩამოვთვლილია მათი შესაძლებლობები, რათა კონკრეტული ობიექტისათვის შესაძლებელი გახდეს ინფორმაციის დაცვის საშუალებების შერჩევა.

ინფორმაციის დაცვის საშუალებების ჯგუფები, მათი დანიშნულების შესაბამისად, შემდეგნაირად არის ჩამოყალიბებული დისერტაციაში:

1. ინფორმაციის დაცვის საინჟინრო (მექანიკური) საშუალებები;
2. ინფორმაციის დაცვის ვიბროაკუსტიკური საშუალებები;
3. დაცვა თანმხლები ელექტრომაგნიტური გამოსხივებისაგან და ზედდებებისაგან;
4. ინფორმაციის დაცვის საშუალებებზე არასანქცირებული მიერთებებისაგან დაცვა;
5. ინფორმაციის დაცვის მიზნით მოწყობილი საქსელთაშორისო ეკრანები;
6. ინფორმაციის ანტივირუსული დაცვის საშუალებები;
7. ინფორმაციის კრიპტოგრაფიული დაცვის საშუალებები.

ამ ჩამონათვალის საუძველზე შეიძლება შერჩეული იქნას ინფორმაციის დაცვის აპარატურულ–პროგრამული საშუალებები. ამისათვის უნდა არსებობდეს ინფორმაციის დაცვის სერტიფიცირებული საშუალებების ის გარკვეული ნაკრები, რომელიც გათვალისწინებულია ინფორმაციის დაცვის კომპლექსური სისტმის შესაქმნელად და რომელიც აკმაყოფილებს დამკვეთის მოთხოვნებს.

სადისერტაციო ნაშრომის ძირითადი მეცნიერული სიახლე მდგომარეობს შემდეგში: როგორც წესი კრიტერიუმად განიხილება

ინფორმაციის დაცვის საშუალებების ნაკრების „ოპტიმალურობის კრიტერიუმი“, რომელიც უზრუნველყოფს ნორმატიული დოკუმენტების მოთხოვნების შესაბამისად ინფორმაციის დაცვის კომპლექსური სისტემის შექმნას.

ინფორმაციის დაცვის M რაოდენობის საშუალებებიდან, დასაცავი ობიექტის მოთხოვნებიდან გამომდინარე, ვირჩევთ N რაოდენობის ინფორმაციის დაცვის საშუალებებს, ანუ N არის M სიმრავლის ქვესიმრავლე, N є M, სადაც $N \equiv \{n_j\}$, j=1,k, ცხადია k არის ინფორმაციის დაცვის კომპლექსურ სისტემაში გამოყენებული დაცვის საშუალებების რაოდენობა.

აღნიშნულის შესაბამისად $n_i = n_i(X_i)$, სადაც X_i არის i-იური დაცვის საშუალების ტექნიკური მახასიათებლების და ფუნქციების ამსახველი მაჩვენებელი.

თუ დავუშვებთ, რომ ინფორმაციის დაცვის i-იური საშუალება უზრუნველყოფს დაცვის Ni რაოდენობის ფუნქციებს, მაშინ

$$\sum_{i=1}^{K} \mathrm{Ni} = \mathrm{N}_{\text{დაცვის}}$$

სადაც $\mathrm{N}_{\text{დაცვის}}$ -არის ინფორმაციის დაცვის კომპლექსური სისტემის დაცვის ფუნქციების რაოდენობა. იმის გათვალისწინებით, რომ ინფორმაციის დაცვის საშუალებებისათვის შერჩეულ კრიტერიუმებს უზრუნველყოფს განსხვავებული დანიშნულებების სისტემები, მაგალითად, ინფორმაციული დაცვის ანტივირუსული საშუალებების Outpost (Agnitum) და „კასპერსკის ლაბორატორია“ (Kaspersky) უზრუნველყოფენ არასანქცირებული შეერთებების ბლოკირებასაც, ხოლო დაცვის ანტივირუსული საშუალება Panda Security, ბრანდმაუერს ანუ ქმნის საქსელთაშორისო ეკრანს და ა.შ. ცხადია:

$$\sum_{i=1}^{K} \mathrm{Ni} < \mathrm{N}_{\text{დაცვის}}$$

რადგანაც

$$X_i \cong X_{i\text{მოთხვონლი}}$$

სადაც $X_{i\text{მოთხვონლი}}$ - არის i-ური დაცვის საშუალებისადმი წაყენებული მოთხოვნების შესაბამისად შერჩეული დაცვის ფუნქციების რაოდენობა, მაშინ ჩვენი ამოცანის მიზნობრივ ფუნქციას ექნება შემდეგი სახე:

$$\begin{cases} \sum_{i=1}^{K} \mathrm{Ni} < \mathrm{N}_{\text{დაცვის}} \\ X_i \cong X_{i\text{მოთხვონლი}}, \quad i=1,K \end{cases}$$

ეს არის ჩვენი ამოცანის მათემატიკური მოდელი ზოგადი სახით, რომელიც იძლევა კონკრეტული მოდელის განსაზღვრის საშუალებას.

ამრიგად, ჩვენს მიერ შემოთავაზებული ოპტიმალურობის კრიტერიუმი, დაცვის საშუალებისათვის დადგენილ ფასს, მიუხედავად მისი დიდი მნიშვნელობისა, ვერ ითვალისწინებს, ვინაიდან უმეტეს შემთხვევებში ფასი არ არის მითითებული და საჭიროებს მწარმოებელი ფირმის მენეჯერთან მოლაპარაკებას. გასათვალისწინებელია ის ფაქტიც, რომ ელექტრონულ საშუალებებზე ფასები დროში მნიშვნელოვნად მცირდება - მურის კანონის შესაბამისად, ყოველ ორ წელიწადში, როგორც მინიმუმ ნახევრდება.

აქედან გამომდინარე, ინფორმაციის დაცვის საშუალებების ნაკრების ოპტიმალურობის კრიტერიუმი, ემყარება ინფორმაციის დაცვის საშუალებების ურთიერთგადაფარვის შესაძლებლობების არსებობას. ამისათვის, დისერტაციაში წარმოდგენილია ინფორმაციის დაცვის საშუალებების დანიშნულების ფუნქციების მიმოხილვა.

მეოთხე თავში განხილულია მულტისერვისული ქსელის ფრაგმენტი დროში დაყოვნების შესწავლისათვის და მიღებულია შედეგი, რომ განშტოებული ქსელი შეიძლება ჩანაცვლდეს ქსელის ექვივალენტური უბნით, რომელიც ხასიათდება სიგნალის გავრცელების იგივე დაყოვნებით, როგორც ქსელის კვანძებშია განსაზღვრული, რაც შეიძლება გამოვიყენოთ ქსელის ფუნქციონირებაში არასანქციონირებული ჩართვის აღმოსაჩენად.

დასკვნები

1. ინფორმაციის დაცვის საშუალებების შერჩევა ხორციელდება ექსპერტების მიერ ინფორმაციის დაცვის არსებული სერტიფიცირებული საშუალებების ჩამონათვალის საფუძველზე. ეს მიდგომა არის საყოველთაოდ გავრცელებული, მაგრამ ხასიათდება შემდეგი ნაკლოვანებებით:

– არ არსებობს ინფორმაციის დაცვის არსებული საშუალებების შერჩევისათვის სისტემური მიდგომა;
– საქმე გვაქვს ეკლექტიკური შერჩევის მოვლენასთან;
– შერჩევის ხარისხი მნიშვნელოვნად არის დამოკიდებული ექსპერტის კვალიფიკაციაზე.

2. ინფორმაციის დაცვის სერტიფიცირებული საშუალებების ავტომატიზებული მეთოდით შერჩევა იქნება ოპტიმალური და ტექნიკურად დაბალანსებული დაცვის კომპლექსური სისტემის აგების განხორციელების საშუალება. ეს მიდგომა არის სისტემური, რომელიც ამცირებს ინფორმაციის დაცვის საშუალებების აგებისათვის დროის ხანგრძლიობას და ადამიანური ფაქტორის ზეგავლენას გადაწყვეტილებების მიღებაზე.

3. შემოთავაზებული მათემატიკური მოდელი, რომელიც იძლევა კონკრეტული მოდელის განსაზღვრის საშუალებას, საფუძვლად უნდა დაედოს ინფორმაციის დაცვის სერტიფიცირებული სისტემების ანალიზის პროცესის ავტომატიზაციას და უნდა დამუშავდეს პროგრამული უზრუნველყოფა შემდეგი ფუნქციებით:

– მოთხოვნების შესაბამისი ინფორმაციის დაცვის სერტიფიცირებული სისტემის შესახებ ცნობების ავტომატიზებულად მოპოვება და ამის საფუძველზე მონაცემთა განახლებული ბაზის გენერირება;
– მოთხოვნების შესაბამისად ინფორმაციის დაცვის საშუალებების ოპტიმალური ნაკრების გენერირება;

– ინფორმაციის დაცვის სისტემის ტექნიკურ-ეკონომიკური დასაბუთების ფორმირება, ხარჯების სიდიდისა და სისტემის ფუნქციონალური შესაძლებლობების საფუძველზე.

4. პროგრამის დამუშავება უზრუნველყოფს: მოთხოვნების შესაბამისი ინფორმაციის დაცვის სისტემისათვის აუცილებელი საშუალებების შერჩევის დროის ხანგრძლიობისა და წინასაპროექტო მოკვლევასთან დაკავშირებული ხარჯების შემცირებას.

5. იმისათვის, რომ გაგვაჩნდეს უნარი წინაღვუდგეთ ინფორმაციაზე შემოტევებს მთელი მათი ქმედითუნარიანობის განმავლობაში, ორგანიზაციებმა და კომპანიებმა უნდა გამოიყენონ ინფორმაციული უსაფრთხოების უზრუნველყოფის საშუალებები ყველგან, სადაც კი მოსალოდნელია, რაიმე საშიშროება. რაც შეეხება საქართველოსათვის არსებულ განსაკუთრებულ ვითარებას, აქ ყველაზე მაღალი ალბათობა გააჩნია სახელმწიფო საინფორმაციო რესურსებზე შემოტევებს. აუცილებლად უნდა არსებობდეს შესაბამისი 3 – 5 წლიანი სახელმწიფო პროგრამა, დაცული ბიუჯეტით, რომელშიც, გარდა სახელმწიფო ორგანოებისა, ჩართული იქნება საგანმანათლებლო სისტემა, ვინაიდან ამ პროგრამის შედეგებს ესაჭიროება დანერგვა და კომპეტენტური ექსპლუატაცია.

6. ინფორმაციის მიმოცვლის პროცესში, სატელეკომუნიკაციო ქსელში შესაძლო ხიფათის წარმოქმნის გათვალისწინება და მისი მართვის უნარის არსებობა წარმოადგენს ინფორმაციული დაცულობის უზრუნველყოფის საფუძველს. ნაშრომში დასაბუთებულია, რომ აუტენტიფიკაციის მიზნებისათვის არსებული იდენტიფიკატორების ნამდვილობის დამოწმებისათვის აუცილებელია შესაძლო სახიფათო მოვლენების ანალიზი და ინფორმაციის გაცვლის სისტემით მათი მოგერიების უზრუნველყოფის პირობების გათვალისწინება. ასევე საერთო სარგებლობის სატელეკომუნიკაციო ქსელში ინფორმაციული უსაფრთხოებისათვის კომპლექსური სისტემის შექმნის საკითხები, რაც

დაცული ინფორმაციული საზოგადოების ჩამოყალიბებისათვის აუცილებელ მოთხოვნას წარმოადგენს.

7. აუცილებელია ინფორმაციის დაცვის კომპლექსური სისტემის გათვალისწინება საერთო სარგებლობის ქსელებში. მაშინ, ტექნიკურ სრულყოფასთან ერთად შეიძლება შეიქმნას დაცული ინფორმაციული საზოგადოება. ამისათვის ტექნიკური საშუალებები არსებობს, მაგრამ არ არსებობს ნორმატიული ბაზა.

დისერტაციის თემაზე გამოქვეყნებული შრომები

1. ყიფიანი ქ., გვალია თ., კუპატაძე თ. მომსახურების ხარისხის შეფასება საერთო სარგებლობის სატელეფონო ქსელში. მე-2 საერთაშორისო სამეცნიერო კონფერენციის - „ენერგეტიკა: რეგიონული პრობლემები და განვითარების პერსპექტივები“ - მოხსენებების კრებული. ქ. ქუთაისი, 25 მაისი, 2013 წ. გვ. 327 – 331.
2. ყიფიანი ქ., კოპლატაძე მ., კუპატაძე თ. სატელეკომუნიკაციო ქსელში პერსონალური მონაცემების დარღვევის პრობლემები. მე-3 საერთაშორისო სამეცნიერო კონფერენციის – „ენერგეტიკა: რეგიონული პრობლემები და განვითარების პერსპექტივები“ - მოხსენებების კრებული. ქ. ქუთაისი, 24 ოქტომბერი, 2015წ. გვ.136 – 138.
3. ყიფიანი ქ., გვალია თ., კუპატაძე თ. ინფორმაციული უსაფრთხოების დარღვევის მიზეზების შეფასება. საერთაშორისო სამეცნიერო კონფერენციის – „მდგრადი ენერგეტიკა: გამოწვევები და განვითარების პერსპექტივები.“ - მოხსენებების კრებული. ქ. ქუთაისი, 18 ივნისი, 2015წ. გვ. 141 – 145.
4. ბჟინავა ე., ყიფიანი ქ., გვალია თ. მულტისერვისულ ქსელში მოთხოვნებზე დაყოვნებების წარმოქმნის დამოკიდებულება ქსელში არსებულ მარშრუტებზე. მე-4 საერთაშორისო სამეცნიერო კონფერენციის – „ენერგეტიკა: რეგიონული პრობლემები და განვითარების პერსპექტივები“ – მოხსენებების კრებული. ქ. ქუთაისი, 29 ოქტომბერი, 2016წ. გვ. 147 – 151.

Summary

The dissertation thesis offers optimization criteria of the set of information protection tools, which should ensure creation of the complex system of information protection, in accordance with the requirements of the normative documents.

The practical value of the dissertation thesis is the establishment of the conditions for the assessment of guaranteed, necessary or acceptable levels, within the integration of various means of information protection, on the basis of certification system of appropriate means of information protection.

In order to provide information protection for the institution or company, the results of dissertation are based on engineer vision and approach, which aims on the one hand simplify the information to the institution or company in order to create a complex system of information protection, and on the other hand, to make optimal protection system for specific object, on the basis of the use of the minimum number of protection tools in the complex, which according to the costs is equivalent to the implementation of the optimization process.

The purpose of the thesis is to solve the problem of simplifying the process of selecting the certified means of information protection, in order to establish a complex system of information protection for the institution (company). Theoretical analysis and mathematical methods are used to carry out such work.

Dissertation thesis presents literary review of the research of information protection principles of telecommunication network, by analyzing the results of 35 scientific research.

In accordance with what category of object protection is required to secure information security, specific requirements should be determined. Different cyber attacks require different technological solutions. The aim of the dissertation thesis is to promote the proper selection of information protection tools.

In terms of technology, in order to avoid leakage of information it must be clarified: the organizational and technical measures that are required, the user authentication and authorization that is necessary for the proper level, also should be taken into account the encryption in communications channels, the evaluation of access to personal data and protection of the completion of data transfer in telecommunication channels and moreover information telecommunication systems that process this data.

When the realization of the concept of information society is completed, the electronic government, the provision of state services via internet and so on, the "open keys" infrastructure will be created. But, in this case, the network security problem will arise. The "open keys" infrastructure is also vulnerable to attacks, as its instrumental components are scattered in open networks. However, it should be taken into consideration that in any event, it is necessary to have access to the network in order to resolve the information security issue, it is necessary to provide telecommunication space with relevant resources.

The first chapter of the dissertation thesis assesses the reasons for information security violations, leakage sources, leakage channels, leakage geography, leakage results, specificity of information leakage, and reasons for information leaking.

The second chapter of the dissertation thesis reviews personal data protection problems in the telecommunication network. It analyzes problems of oral information security, cyber security of the info-communication systems and functioning security of integrated info-communication system. The components of information technologies of cyberspace are discussed.

The third chapter defines the means of protection of information, selection principles, and assesses the protection of object from attacks on information. The criterion of optimality of the set of information protection tools is offered.

The fourth chapter discusses the fragment of multiservice network in the timelapse to study delays. It has been shown that broad network can be substituted with the equivalent network segment, which is characterized by the same delay in the distribution of signal as defined in network nodes.

The main scientific innovation of the dissertation thesis is the criterion of proposed optimality of the set of information protection tools, which provides the creation of a complex system of information protection according to the requirements of the normative documents.

The number of protection functions is selected in accordance with the requirements set out to information protection, also the target function of the task and mathematical model in general form is defined, that allow us to define a specific model.

The criterion of optimality offered in the dissertation thesis, despite its great importance, does not include the price fixed for the means of protection, since in most cases it is necessary to negotiate with the manager of the firm's manufacturer. Also it should be taken into consideration that prices on electronic means are significantly reduced in time -- according to the Moor Law, every two years, at least half of it.

Hence, the criterion of optimality of the set of information protection tools proposed in the sessions is based on the existence of mutual surveillance of information protection means.