საქართველოს ტექნიკური უნივერსიტეტი

ქეთევან ყიფიანი

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

წარდგენილია დოქტორის აკადემიური ხარისხის მოსაპოვებლად

სადოქტორო პროგრამა: ტელეკომუნიკაცია

შიფრი: 0402

საქართველოს ტექნიკური უნივერსიტეტი

თბილისი, 0175, საქართველო

ივლისი, 2019 წ.

თბილისი

2019 წელი

საქართველოს ტექნიკური უნივერსიტეტი

ენერგეტიკისა და ტელეკომუნიკაციის ფაკულტეტი

ჩვენ, ქვემორე ხელისმომწერნი ვადასტურებთ, რომ გავეცანით ქეთევან ყიფიანის მიერ შესრულებულ სადისერტაციო ნაშრომს დასახელებით: „ინფორმაციის დაცვის მეთოდების კვლევა სატელეკომუნიკაციო ქსელებისა და სისტემების სტრუქტურისა და ფუნქციონირების ალგორითმის გათვალისწინებით“ და ვაძლევთ რეკომენდაციას საქართველოს ტექნიკური უნივერსიტეტის ენერგეტიკისა და ტელეკომუნიკაციის ფაკულტეტის სადისერტაციო საბჭოში მის განხილვას დოქტორის აკადემიური ხარისხის მოსაპოვებლად.

ივლისი, 2019 წელი

ხელმძღვანელი: _____ პროფესორი თ. კუპატაძე

რეცენზენტი: _____

რეცენზენტი: _____

საქართველოს ტექნიკური უნივერსიტეტი

2019

ავტორი: ქეთევან ყიფიანი

თემის დასახელება: „ინფორმაციის დაცვის მეთოდების კვლევა სატელეკომუნიკაციო ქსელებისა და სისტემების სტრუქტურისა და ფუნქციონირების ალგორითმის გათვალისწინებით“

ფაკულტეტი: ენერგეტიკისა და ტელეკომუნიკაციის

ხარისხი: აკადემიური დოქტორი

სხდომა ჩატარდა: ივლისი, 2019 წ.

რეზიუმე

სადისერტაციო ნაშრომში შემოთავაზებულია ინფორმაციის დაცვის საშუალებების ნაკრების ოპტიმალურობის კრიტერიუმი, რომელმაც უნდა უზრუნველყოს, ნორმატიული დოკუმენტების მოთხოვნების შესაბამისად, ინფორმაციის დაცვის კომპლექსური სისტემის შექმნა.

სადისერტაციო ნაშრომის პრაქტიკული ღირებულებაა ინფორმაციის უსაფრთხოების უზრუნველყოფის სხვადასხვა საშუალებების ინტეგრაციის დროს, გარანტირებული, აუცილებელი ან დასაშვები დონეების შეფასების შესაძლებლობების პირობების ჩამოყალიბება, ინფორმაციის დაცვის მოთხოვნების შესაბამისი საშუალებების სერტიფიცირებული სისტემის საფუძველზე.

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.

სამუშაოს მიზანია ინფორმაციის დაცვის სერტიფიცირებული საშუალებების შერჩევის პროცესის გამარტივებული ამოცანის ამოხსნა, რათა შეიქმნას დაწესებულებისათვის (კომპანიისათვის) ინფორმაციის დაცვის კომპლექსური სისტემა. ასეთი სამუშაოს განხორციელებას ემსახურება თეორიული ანალიზისა და მათემატიკური მეთოდების გამოყენება.

სადისაერტაციო ნაშრომში წარმოდგენილია სატელეკომუნიკაციო ქსელის ინფორმაციული უსაფრთხოების პრინციპების კვლევის ლიტერატურული მიმოხილვა, გაანალიზებულია 35 სამეცნიერო კვლევის შედეგები.

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.

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

ტექნოლოგიური თვალსაზრისით პრობლემა, რომ არ მოხდეს ინფორმაციის გაჟონვა, შედარებით გასაგებია: საჭიროა ორგანიზაციული და ტექნიკური ღონისძიებების გატარება, აუცილებელია მომხმარებელთა აუტენტიფიკაცია და ავტორიზაცია სათანადო დონეზე, კავშირგაბმულობის არხებში შიფრაციის გათვალისწინება, პერსონალურ მონაცემებთან ხელმისაწვდომობის შეფასება და სატელეკომუნიკაციო არხებში მონაცემების გადაცემის სისრულის დაცვა და აგრეთვე საინფორმაციო სატელეკომუნიკაციო სისტემები, რომლითაც ხდება ამ მონაცემების დამუშავება. ამასთანავე, გასათვალისწინებელია, რომ დაცული ინფორმაცია ლოკალურ ქსელში შეიძლება მომხმარებლებისათვის პრაქტიკულად მიუწვდომელი გავხადოთ. მაგრამ, ინტერნეტის ქსელში ეს შეუძლებელია, ვინაიდან ინფორმაციული საზოგადოებისათვის ასეთი ღონისძიება შეუთავსებელია. ჩვენ ვცხოვრობთ ღია ინფორმაციულ სამყაროში, სადაც სახელმწიფო ორგანოების მოღვაწეობის შესახებაც კი მონაცემები უნდა იყოს მაქსიმალურად ღია.

როდესაც დასრულდება ინფორმაციული საზოგადოების კონცეფციის რეალიზება, ელექტრონული მთავრობის, 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.

დისერტაციის პირველ თავში შეფასებულია ინფორმაციული უსაფრთხოების დარღვევის მიზეზები, გაჟონვის წყაროები, გაჟონვის არხები, გაჟონვის გეოგრაფია, გაჟონვის შედეგები, ინფორმაციის გაჟონვათა დარგობრივი სპეციფიკა, ინფორმაციის გაჟონვის მიზეზები.

დისერტაციის მეორე თავი ეძღვნება სატელეკომუნიკაციო ქსელში პერსონალური მონაცემების დაცვის პრობლემებს. გაანალიზებულია სამეტყველო ინფორმაციის დაცვის პრობლემები, ინფოსაკომუნიკაციო სისტემების კიბერუსაფრთხოება, ინტეგრირებული ინფოსაკომუნიკაციო სისტემის ფუნქციონირების უსაფრთხოება. განხილულია კიბერსივრცის საინფორმაციო ტექნოლოგიების კომპონენტები.

მესამე თავში განსაზღვრულია ინფორმაციის დაცვის საშუალებები, შერჩევის პრინციპები და შეფასებულია ინფორმაციაზე შეტევებისაგან ობიექტის დაცულობა. შემოთავაზებულია ინფორმაციის დაცვის საშუალებების ნაკრების ოპტიმალურობის კრიტერიუმი.

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, ეს შედეგი შეიძლება გამოვიყენოთ ქსელის ფუნქციონირებაში არასანქციონირებული ჩართვის აღმოსაჩენად.

სადისერტაციო ნაშრომის ძირითად მეცნიერულ სიახლეს წარმოადგენს ინფორმაციის დაცვის საშუალებების ნაკრების შემოთავაზებული ოპტიმალურობის კრიტერიუმი, რომელიც უზრუნველყოფს ნორმატიული დოკუმენტების მოთხოვნების შესაბამისად ინფორმაციის დაცვის კომპლექსური სისტემის შექმნას.

დაცვის საშუალებებისადმი წაყენებული მოთხოვნების შესაბამისად შერჩეულია დაცვის ფუნქციების რაოდენობა, განსაზღვრულია ამოცანის მიზნობრივი ფუნქცია და მათემატიკური მოდელი ზოგადი სახით, რომელიც იძლევა კონკრეტული მოდელის განსაზღვრის საშუალებას.

სადისერტაციო ნაშრომში შემოთავაზებული ოპტიმალურობის კრიტერიუმი, დაცვის საშუალებებისათვის დადგენილ ფასს, მიუხედავად მისი დიდი მნიშვნელობისა, არ ითვალისწინებს, ვინაიდან უმეტეს შემთხვევებში აუცილებელია მწარმოებელი ფირმის მენეჯერთან მოლაპარაკება. გასათვალისწინებელია ის ფაქტიც, რომ ელექტრონულ საშუალებებზე ფასები დროში მნიშვნელოვნად მცირდება - მურის კანონის შესაბამისად, ყოველ ორ წელიწადში, როგორც მინიმუმ ნახევრდება.

აქედან გამომდინარე, დისერტაციაში შემოთავაზებული, ინფორმაციის დაცვის საშუალებების ნაკრების ოპტიმალურობის კრიტერიუმი ემყარება ინფორმაციის დაცვის საშუალებების ურთიერთგადაფარვის შესაძლებლობების არსებობას.

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.

შინაარსი

გვ.

ცხრილების ნუსხა

გვ.

ნახაზების ნუსხა

გვ.

მადლიერება

მოკრძალებითა და დიდი მადლიერებით მინდა აღვნიშნო, პერსონალურ მონაცემთა დაცვის სახელმწიფო ინსპექტორის სამსახურის თანამშრომელთა და პირადად მარიამ ელყანაშვილის წვლილი, სადისერტაციო ნაშრომის შედეგების შეფასების, მათი წლიური ანგარიშების მოწოდებისა და დისერტაციის დაცვის წინ სერთიფიკატის გადმოცემის საფუძველზე ჩემი რწმენის გამყარებისათვის.

მადლობას ვუხდი საქართველოს ტექნიკური უნივერსიტეტის ტელეკომუნიკაციის დეპარტამენტის პროფესორებს: ჯემალ ბერიძეს, ჯანიკო ხუნწარიას, ელვირა ბჟინავას, ომარ შამანაძეს, ვახტანგ აბულაძეს და მარინა ქურდაძეს, სემინარებსა და კოლოქვიუმებზე სასარგებლო შენიშვნების, მითითებებისა და დისერტაციაზე, საუკეთესო სამუშაო პირობების შექმნისათვის.

მადლობას ვუხდი საქართველოს ტექნიკური უნივერსიტეტის ინფორმატიკისა და მართვის სისტემების ფაკულტეტის პროფესორებს: ვლადიმერ ადამიას, დავით კაპანაძეს, ოთარ შონიას, გოგი მაისურაძეს, კორნელი ოდიშარიას და თეიმურაზ შარაშენიძეს, დისერტაციის შედეგების მოსმენის საფუძველზე სასარგებლო შენიშვნებისა და რჩევებისათვის.

მადლობას ვუხდი ჩემს ხელმძღვანელს, პროფესორ თამაზ კუპატაძეს ღირსეული სამეცნიერო ხელმძღვანელობისათვის.

მადლობას ვუხდი ჩემს მეუღლეს ალექსანდრე ნადირაძეს, რომელმაც დისერტაციაზე მუშაობისა და კონფერენციებში მონაწილეობის პერიოდებში სრულად აიღო თავის თავზე მცირეწლოვანი შვილების მოვლა–პატრონობაზე პასუხისმგებლობა.

ბატონებო, ყველას გისურვებთ დიდ წარმატებებს საქვეყნო საქმიანობასა და პირად ცხოვრებაში.

ღრმა პატივისცემით, ქეთევან ყიფიანი 25.05.2019 წ.

შესავალი

ინფორმაციული სისტემების ფუნქციონირების ეფექტურობის დარღვევა, ანუ 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. ჩემს წინაშე კი დგას სხვა ამოცანა, კერძოდ, დაწესებულების ან კომპანიის ინფორმაციული უსაფრთხოების უზრუნველყოფა უკვე არსებული, კონკრეტული პრობლემების შესაბამისი, საშუალებების გამოყენებით.

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.

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.

სამეცნიერო სიახლე: სადისერტაციო ნაშრომში წარმოდგენილია სატელეკომუნიკაციო ქსელის ინფორმაციული უსაფრთხოების პრინციპების კვლევის ლიტერატურული მიმოხილვა.

[1]-ში აღნიშნულია ინფორმაციის უსაფრთხოების კონტროლის შერჩევითი ხასიათის გამოყენების შესაძლებლობა, შეზღუდული რესურსებისა და საკონტროლო ღონისძიებისათვის გამოყოფილი დროის ხანგრძლიობით. განხილულია შერჩევითი კონტროლის მეთოდი ერთჯერადი ამორჩევით. შემოთავაზებულია შერჩევითი კონტროლის მახასიათებლები და მათი გამოთვლებისათვის საჭირო ანალიზური გამოსახულებები.

[2-11]-ში განხილულია ხიფათების ანალიზის მეთოდები, რომლებიც დაკავშირებულია შორეული ელექტრონული აუტენტიფიკაციის პროცესთან. განხილულია განსაკუთრებულად განვითარებული მეთოდები, დაკავშირებული აუტენტიფიკაციის პროცესის ხიფათებთან. ნაჩვენებია, რომ ხიფათების ანალიზის მეთოდების უდიდესი უმეტესობა შეიძლება გამოყენებული იქნას აუტენტიფიკაციის ხიფათების შესაფასებლადაც.

[12-14]-ში განხილულია მოდელირების კლასიკური სქემების გამოყენების შესაძლებლობა ინფორმაციული პროცესების კვლევისათვის, სისტემაში ინფორმაციის მთლიანობის და მიღწევადობის დარღვევისადმი ხიფათის არსებობის პირობებში და ინფორმაციის დაცვის მექანიზმების გამოყენება დამახინჯებებისა და ბლოკირებისაგან. კვლევის ობიექტად გამოყენებულია უსაფრთხოების ინტეგრირებადი სისტემა.

[15-17]-ში წარმოდგენილია ინფორმაციის მიტაცების სპეციალური ელექტრონული მოწყობილობის სიგნალების მახასიათებლების იმიტაციის შედეგი. შემოთავაზებულია ასეთი მოწყობილობების მოდელირების შედეგების გამოყენება ინფორმაციის დაცვის სფეროს მომსახურე პერსონალის სწავლებისა და კვალიფიკაციის ამაღლებისათვის.

[18]-ში შემოთავაზებულია სამეცნიერო-ტექნიკური გადაწყვეტილება, რომელიც მიეკუთვნება ტელეკომუნიკაციის სფეროს და შეიძლება გამოყენებული იქნას ქსელების დაცვისათვის გარე დესტრუქციული ზემოქმედებისაგან. წარმოდგენილი მეთოდის გამოყენების შემთხვევაში უზრუნველყოფილი იქნება ქსელისა და მისი სტრუქტურული ელემენტების დაცულობა ბოროტმზრახველის შესაძლებლობების შეფასების საფუძველზე. ხდება შეფასება, ბოროტმზრახველისაგან რესურსების გამოყენების ეფექტურობის თვალსაზრისით, აგრეთვე ქსელის დროულად რეკონფიგურირების შესაძლებლობის უზრუნველყოფით.

[19-21]-ში 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. შემოთავაზებული კონცეფციის ფარგლებში დასაბუთებულია კონტროლის პროცესის სტრუქტურირებული წარმოდგენა, კერძოდ, საკონტროლო აპარატურის მუშაობის რეჟიმი, თანმხლები ელექტრომაგნიტური გამოსხივების გაზომვის მეთოდიკა და კომპლექსური ტექნიკური კონტროლის რეალიზაციის ავტომატიზებული მეთოდები. შემოთავაზებულია ასეთი ოპტიმიზირებული ამოცანის ამოხსნის მეთოდი, ურთიერთდაკავშირებული, კერძო ამოცანების რესურსების ოპტიმალურად განაწილებული სამეტაპიანი მიმდევრობის სახით. შემოთავაზებულია მიზნობრივი ფუნქციების გამოყენებითი განმატრება.

[22-25]-ის მიზანია ინფორმაციის დაცვის სერტიფიცირებული საშუალებების შერჩევის პროცესის გამარტივებული ამოცანის ამოხსნა, რათა შეიქმნას დაწესებულებისათვის (კომპანიისათვის) ინფორმაციის დაცვის კომპლექსური სისტემა. ასეთი სამუშაოს განხორციელებას ემსახურება თეორიული ანალიზისა და მათემატიკური მეთოდების გამოყენება.

[26]–ში განხილულია სატელეკომუნიკაციო ქსელის შესასვლელსა და გამოსასვლელზე ტრაფიკების კორელაციაზე შეტევის შემთხვევა, აგრეთვე ტრაფიკის მარკირების გამოყენება შეტევის შედეგიანობის გაზრდის მიზნით. წარმოდგენილია ანონიმური ქსელების მონაცემთა ნაკადების მოდელები და შემოთავაზებულია მიზნობრივი ქსელის შესასვლელსა და გამოსასვლელზე ტრაფიკების კორელაციის შემცირების მეთოდები.

[27-31]-ში დამუშავებულია კავშირგაბმულობის ქსელების აპარატურის ინფორმაციული უსაფრთხოების მოთხოვნებთან შესაბამისობის შეფასება, რომელიც დაფუძნებულია ISO 15408 მეტასტანდარტის მეთოდოლოგიაზე. წარმოდგენილია უსაფრთხოების ფუნქციონალური მოთხოვნების სინთეზის შედეგები, რომლებიც უნდა პასუხობდნენ კავშირგაბმულობის სისტემების აპარატურისადმი წაყენებულ პირობებს. დასაბუთებულია სინთეზის შედეგების გამოყენება, როგორც კავშირგაბმულობის აპარატურის დაცვის

სახეობების პერსპექტიული პაკეტი. შემოთავაზებულია აპარატურის კომპლექსური დაცვის კონცეპტუალური მოდელი, რომელიც ხორციელდება სასერთიფიკაციო გამოცდების ჩარჩოებში. ნაჩვენებია, რომ შემოთავაზებული მოდელები უზრუნველყოფენ გამოცდის პროცესის დეტერმინირებულობას. სასერტიფიკაციო გამოცდების ჩატარებისათვის დროის მინიმიზაციის საკითხების კვლევამ დაასაბუთა, რომ ამ დროის მონაკვეთის შემცირება შეიძლება განხორციელდეს გამოსაცდელი ტესტების კრებულების ურთიერთგადაფარვების გამოყენებით.

[32-35]-ში შემოთავაზებულია ინტეგრირებული სტრუქტურის დაწესებულების, ინფორმაციის უსაფრთხოების პროგნოზირების ხარისხის მენეჯმენტის ავტომატიზებული სისტემის მართვის მეთოდი. მეთოდი, რომელიც დამუშავებულია პროგნოზირებადი მოდელების მართვის (Model Predictive Control) გამოყენებით და უზრუნველყოფს ინფორმაციის დაცვასთან დაკავშირებული გადაწყვეტილების მიღების ხელშეწყობას.

დისერტაციის შედეგების შესაბამისად, ძირითადი **სამეცნიერო სიახლე** მდგომარეობს შემდეგში: შემოთავაზებულია ინფორმაციის დაცვის საშუალებების ნაკრების „ოპტიმალურობის კრიტერიუმი“, რომელმაც უნდა უზრუნველყოს, ნორმატიული დოკუმენტების მოთხოვნების შესაბამისად, ინფორმაციის დაცვის კომპლექსური სისტემის შექმნა.

პრაქტიკული ღირებულება: ინფორმაციის უსაფრთხოების უზრუნველყოფის სხვადასხვა საშუალებების ინტეგრაციის დროს, გარანტირებული, აუცილებელი ან დასაშვები დონეების შეფასების შესაძლებლობების პირობების ჩამოყალიბება, ინფორმაციის დაცვის მოთხოვნების შსაბამისი საშუალებების სერტიფიცირებული სისტემის საფუძველზე.

თავი 1. ინფორმაციული უსაფრთხოების დარღვევის მიზეზების შეფასება[36]

ედვარდ სნოუდენისა და მის მიერ გასაჯაროებული ინფორმაციის წყალობით, 2013 წელი მეხსიერებაში დარჩება, როგორც ინფორმაციის გაჟონვებისა და მათი გამოვლენების წელი. კონფიდენციალური მონაცემების გაჟონვის თემა იმდენად აქტიურად იხილებოდა მასობრივი ინფორმაციის საშუალებებით, რომ ამ საკითხით ძალზე სერიოზულად დაინტერესდა საზოგადოების ყველა ფენა. კომპანია Zecurion-ის ანალიტიკური განყოფილების ანგარიშში თავმოყრილია ინფორმაცია კომპანიების შინაგანი უსაფრთხოების შემთხვევებთან დაკავშირებით, რომლებიც აღირიცხა 2013 წლის განმავლობაში სახელმწიფო დაწესებულებებში, კომერციულ ორგანიზაციებში და იძლევა დარგებში არსებული ვითარებების სრულ სურათს, რაც განსაკუთრებულად საიმედო მონაცემებს შეიცავს, სრულყოფილი ანალიზის ჩასატარებლად.

უნდა აღინიშნოს, რო ედვარდ სნოუდენთან დაკავშირებულ ჯაშუშურ აყალმაყალს გააჩნია „მედლის მეორე მხარეც“ - ამერიკის მთავრობის საიდუმლო დოკუმენტების ირგვლივ ატეხილი ხმაურის ფონზე, კომერციული ორგანიზაციებიდან გაჟონილი მონაცემები, რომლებიც რეალურად ეხებოდა ადამიანთა დიდი რაოდენობის ინტერესებს, სრულიად უყურადღებოდ დარჩა. გარდა ამისა, გასულ 2013 წელს ერთდროულად მოხდა რამოდენიმე ინციდენტი, რომლებიც მიეკუთვნება განსაკუთრებულ ინცინდენტთა რიცხვს.

1.1 გაჟონვის წყაროები

დღეისათვის რიგი ორგანიზაციებისათვის აუცილებლობას წარმოადგენს ინფორმაციის დაცულობის მდგომარეობის შეფასება, რათა მინიმუმამდე იქნას დაყვანილი ის სახიფათო მოვლენები, რომლებიც დაკავშირებულია თაღლითურ ქმედებებთან ელექტრონული

ურთიერთქმედებების პროცესში. მომხმარებლების იდენტიფიკაციის მეთოდების შეფასებასა და ანალიზს ეძღვნება [37], სადაც სახიფათო მოვლენის შედეგი შეფასებულია ფორმულით:

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

აქ U_i არის i 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 რაოდენობაა.

[38] ნაშრომში დასაბუთებულია შესაძლო სახიფათო მოვლენების რანჟირების აუცილებლობა, წლის განმავლობაში გარკვეული მოვლენის წარმოჩენის ალბათობისა და მოსალოდნელი ხიფათის (რისკის) ფარდობით $\overline{R}$ მნიშვნელობის შესაბამისად, სადაც ნორმირების პირობას წარმოადგენს:

$$\bar{R} = \frac{\sum_{i=1}^{M} R_i}{\sum_{i=1}^{M} L(U_i)}$$

სადისერტაციო ნაშრომში გამოყენებულია, სატელეკომუნიკაციო ქსელში სახიფათო მოვლენების რანჟირებისათვის ინფორმაციის გაჟონვის შესაძლო წყაროების, გაჟონვის გეოგრაფიის, ინფორმაციის გაჟონვების დარგობრივი სპეციფიკის, გაჟონვის მიზეზებისა და შედეგების ანალიზი. ინფორმაციის წყარო [39].

2013 წელს, დაწესებულების შინაგანი უსაფრთხოების მნიშვნელოვანი ინციდენტების რაოდენობა უმნიშვნელოდ შეიცვალა ორ გასულ წელთან შედარებით და მიგვაჩნია, რომ ეს ტენდენცია დღემდეა შენარჩუნებული. წლიდან - წლამდე ინციდენტების რაოდენობის გათანაბრების ტენდენცია აღინიშნება Zecurion-ის წინა ანგარიშებშიც. ამის ძირითადი მიზეზია - მასობრივი ინფორმაციის საშუალებების გაჯერება შეტყობინებებით

გაჟონვების შესახებ. გაჟონვების დაფიქსირებულ რაოდენობაზე შეიძლება ითქვას, რომ ინციდენტების რეალური რაოდენობა ცალკეულ ქვეყნებში და მთლიანად მსოფლიოში, რამდენიმე თანრიგით უფრო მაღალია. მაგრამ მათი დიდი ნაწილი არასდროს არ ხდება საჯარო, ხოლო რიგ შემთხვევებში გაჟონვის შესახებ ინფორმაცია რჩება დაფარული შესაბამისი მონაცემების მფლობელთათვისაც კი.

გაჟონვების გეოგრაფიული განაწილებაც უნდა ვივარაუდოთ, რომ შენარჩუნებულია გასული წლების სახით - დაახლოებით, ინციდენტების ორი მესამედი მოდის ამერიკის შეერთებულ შტატებზე. სხვა ქვეყნებიდან, ყველაზე მეტად დაზარალდნენ ბრიტანელები და კანადელები. გარდა ამისა, ათეულობით ინციდენტს ჰქონდა ადგილი ინდოეთში, ავსტრალიაში, გერმანიასა და ახალ ზელანდიაში. აღინიშნა რომ რუსეთში გაიზარდა არა მარტო ინციდენტების რაოდენობა(2013 წელს - 48 ერთეული), არამედ მათი სიმძიმეც. ინფორმაციული უსაფრთხოების სამსახურების ხელმძღვანელების გამოცდილებით DLP (Data Leak Prevention - მონაცემთა გაჟონვის პრევენცია)-გადაწყვეტილების გამოყენების ჩარჩოებში, რომელიც განხორციელდა 2013 წელს, მაინც აღინიშნებოდა მილიონობით ზარალი დოლარებში.

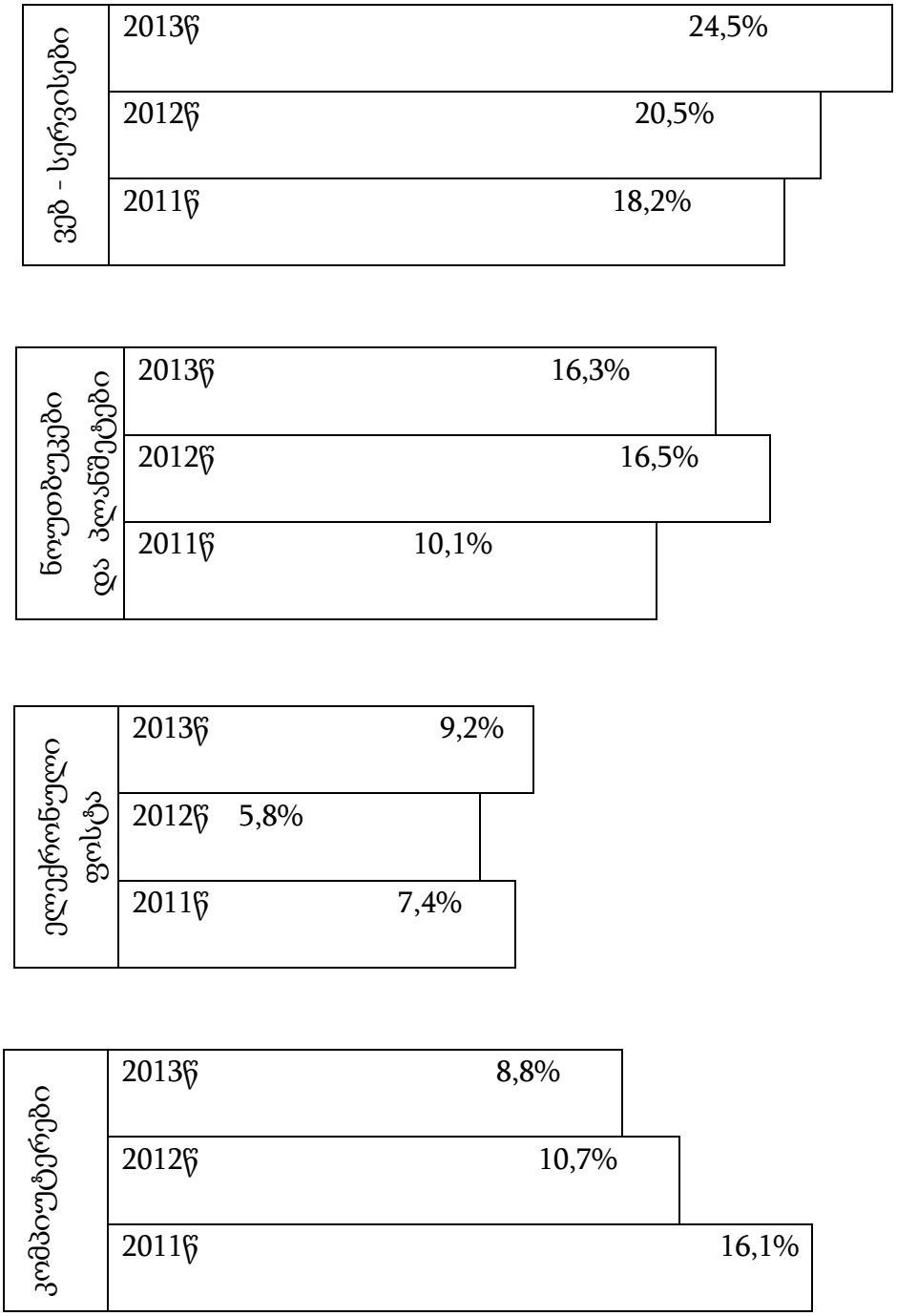
2013 წელს შესამჩნევი გახდა ინციდენტების დარგობრივი სახეცვლილება. თუ 2012 წელს შინაგანი ინციდენტების რაოდენობის უდიდესი ნაწილი მოდიოდა განათლების სფეროზე, 2013 წელს საგანმანათლებლო დაწესებულებები არ მოხვდნენ პირველ სამეულშიც კი. მათი წილი შემცირდა 20,1 % - დან, 11,6 % - მდე.

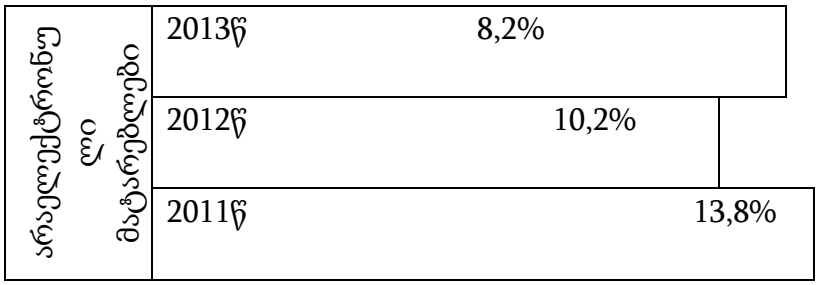
2013 წელს, ერთდროულად სამი დარგი წარმოჩინდა ლიდერობის პრეცენდენტებად გაჟონვების რაოდენობის მიხედვით. ესენი იყო საცალო ვაჭრობა (16,2 %), ჯანდაცვის ორგანიზაციები (16%) და სახელმწიფო დაწესებულებები (15,5). უნდა აღინიშნოს, რომ კონფიდენციალური ინფორმაციის დაცვის თვალსაზრისით, სახელმწიფო სექტორი

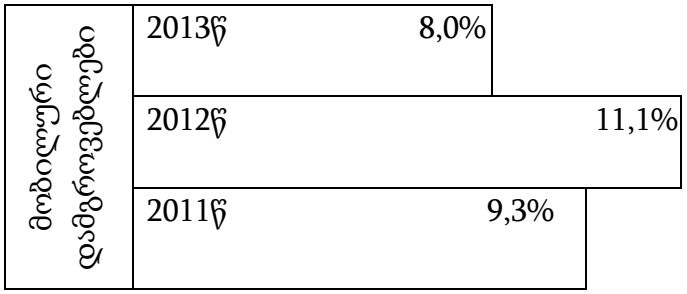
გამოირჩეოდა მაღალი სტაბილურობით. ამ სფეროში გაჟონვების ცვლილების წილი მინიმალური იყო.

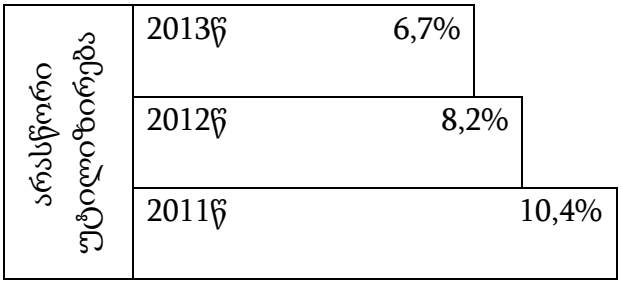
1.2. გაჟონვის არხები

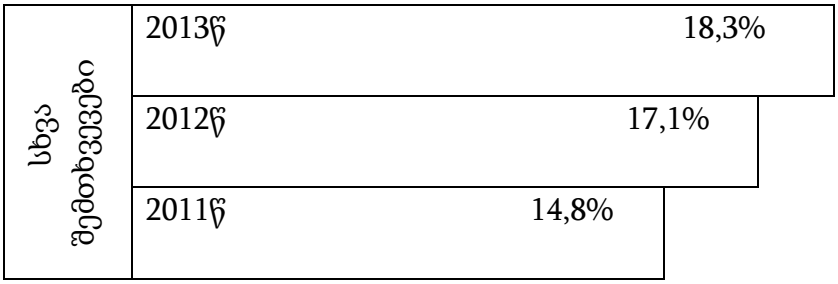
(ინფორმაციის წყარო: Zecurion 2014)




არაელექტრონული მასტარებლები
2013წ
8,2%
2012წ
10,2%
2011წ
13,8%

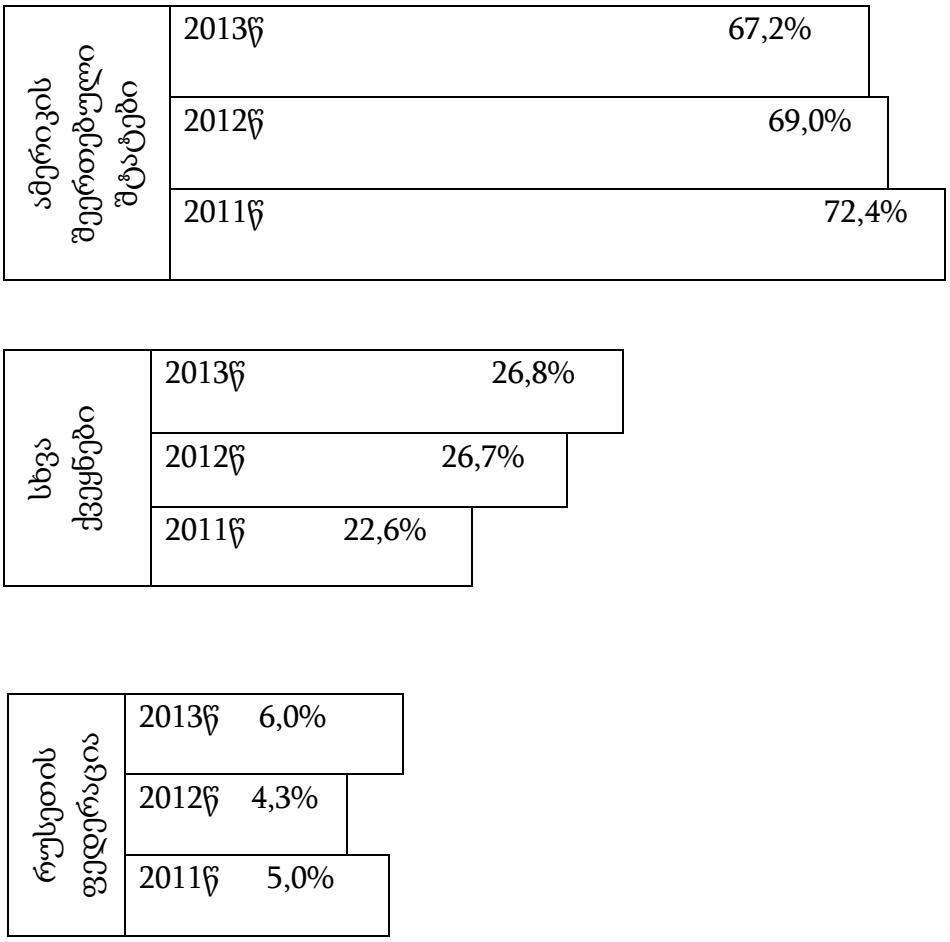

მობილური დამგრძელებლები
2013წ
8,0%
2012წ
11,1%
2011წ
9,3%


არასწორი ჭეშმარიტება
2013წ
6,7%
2012წ
8,2%
2011წ
10,4%


სხვა მემთხვევები
2013წ
18,3%
2012წ
17,1%
2011წ
14,8%

1.3. გაჟონვის გეოგრაფია

(ინფორმაციის წყარო: Zecurion, 2014)



მაგრამ სავალალოა ისიც, რომ არავითარი ძვრა არ იგრძნობა. ამასთანავე, სახელმწიფო ორგანიზაციებში იქმნება მოცულობითი რეესტრები და მოქალაქეთა პერსონალური მონაცემების ბაზები, რომლებიც ხელმისაწვდომია თანამშრომელთა დიდი რაოდენობისათვის. ამიტომ იზრდება ამ მონაცემთა შემთხვევითი კომპრომენტაციის ან მიზანდასახული გადაქაჩვის რისკები.

მაღალტექნოლოგიური კომპანიებიდან გაჟონვის რაოდენობრივი წილი იქნებოდა მნიშვნელოვნად მაღალი, თუ დარგების მიხედვით გადავითვლიდით ინფორმაციის გაჟონვების რაოდენობას, გაჟონვებთან შეხებაში არსებული პირების რაოდენობაზე. მაგალითად, ინციდენტების ისტორიაში უმსხვილესად ითვლება კორპორაცია Adobe Systems-თან დაკავშირებული ინციდენტი. 2013 წელს ინტერნეტით გამომჟღავნდა

Adobe-ს სხვადასხვა სერვისების მომხმარებელთა მონაცემების ბაზა. პირველადი შეფასებით, ბაზაში იყო 3 მილიონამდე ანგარიში. მაგრამ აღმოჩენილი ნაგავსაყრელის დაწვრილებითმა შესწავლამ დაგვანახა, რომ ბაზა შეიცავს 150 მილიონზე მეტ ჩანაწერს. როგორც ვხედავთ გაჟონვის მასშტაბები შთამბეჭდავია.

აღსანიშნავია, რომ მოცემულ შემთხვევაში ერთ-ერთი მთავარი პრობლემა დაკავშირებულია არა იმასთან, რომ ბოროტგანმზრახველებს შეუძლიათ სხვისი სახელით Adobe-ს საიტზე ავტორიზება, არამედ იმაში, რომ მომხმარებლები ხშირად იყენებენ შესასვლელისა და პაროლის ერთი და იგივე კომბინაციას (ან ელექტრონული ფოსტის მისამართის) სხვადასხვა სისტემებთან სერვისებთან მისაერთებლად. აქ კი იშლება თაღლითობისათვის ხელსაყრელი გარემო. მომხმარებლისათვის შესაძლო შედეგები ვარირებს პირდაპირი ფულადი დანაკარგებიდან, როდესაც ხდება ქსელის საფინანსო სერვისების პირდაპირი გამოყენება, ბანალურ გამოძალვამდე ანგარიშის დაბრუნებისათვის სოციალურ ქსელებში და სხვა სერვისებისათვის. ამავდროულად, ელექტრონული მისამართების მიყიდვა სპამერებისათვის გამოიყურება, როგორც ერთ-ერთი ყველაზე უცოდველი ვარიანტი.

1.4. გაჟონვის შედეგები

საინფორმაციო უსაფრთხოების შინაგანი ინციდენტების შედეგების ფინანსური შეფასება სპეციალისტებისათვის წარმოადგენს აქტუალურ და ამავდროულად არატრივიალურ საკითხს. ძირფესვიანი გამოძიება და ინციდენტის გულმოდგინედ დამუშავება ყოველთვის არ იძლევა სასურველ შედეგს და აქ განსაკუთრებულ სირთულეს ქმნის ხელიდან გაშვებული სარგებლის შეფასება. მიუხედავად ამისა ზარალის კონკრეტული ციფრი, თუნდაც საორიენტაციო, აუცილებელია ყოველდღიურ საქმიანობაში

რისკების ანალიზისათვის და ინფორმაციის დაცვისათვის შესაბამისი ზომების მისაღებად.

2013 წელს, ინფორმაციის გაჟონვის გამო მსოფლიო საერთო ზარალმა მიაღწია რეკორდულ მაჩვენებელს და შეადგინა 25,11 მილიარდი დოლარი. ეს ყველაზე მაღალი ნიშნულია შესაბამისი სტატისტიკის წარმოების მანძილზე. რიგი მსხვილი გაჟონვის გამო, რამაც გამოიწვია პიროვნებათა დიდი რაოდენობის დაზარალება, ერთი წლის განმავლობაში (2013) ზარალი გაიზარდა და შეადგინა 31,23 მილიონი დოლარი.

ყველაზე ძვირადღირებულ ინციდენტებში უმეტეს შემთხვევებში ჩათრეულია კომპანიების ტოპ-მენეჯერები. მაგალითად, 2013 წლის ზაფხულში ტაივანის პოლიციამ დააკავა კორპორაცია HTC-ს სამი ტოპ-მენეჯერი, რომლებიც დაკავშირებულები იყვნენ პროგრამული პროდუქტების დამუშავების საქმესთან. მათ მიმართ წაყენებული იქნა ბრალდება კონკურენტ ფირმებისათვის პერსპექტიული დამუშავების შედეგების შესახებ კონფიდენციალური ინფორმაციის მიწოდება. სამსახურებრივი მდგომარეობის გამოყენება არის ერთ-ერთი ტიპიური საშუალება მიზანდასახული გაჟონვებისათვის.

ფინანსური ზარალის შეფასებაში არ არის გათვალისწინებული სნოუდენისური მხილებების შედეგები. სხვადასხვა შეფასებებით, ამერიკის შეერთებული შტატების ზარალი ინფორმაციის გაჟონვის გამო სპეცხამსახურების ყოფილი თანამშრომლების მხრიდან, შეადგენს რამოდენიმე ათეულ მილიარდ დოლარს.

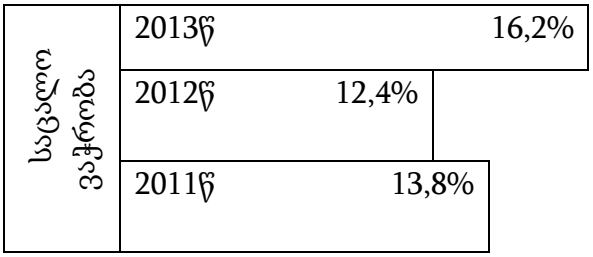
ინფორმაციის გაჟონვის შედეგები დამოკიდებულია იმაზე, თუ რა ტიპის მონაცემების გაჟონვა მოხდა. სხვადასხვა მომხმარებლებს შორის მიმოცვლის მონაცემებიდან, ყველაზე ხშირად კომპრომეტირებულია სხვადასხვა Web- სერვისებისა და საინფორმაციო სისტემების მომხმარებლების სააღრიცხო ჩანაწერები. ყველაზე იშვიათია ინფორმაციის გაჟონვა დაკავშირებული სახელმწიფო ან კომერციულ საიდუმლოებებთან, ინტელექტალურ საკუთრებასთან. თუმცა ასეთი შემთხვევებიც

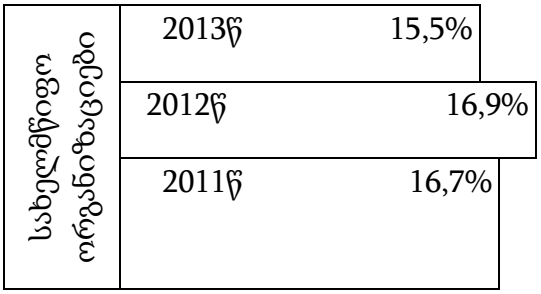
რეგულარულია, მაგრამ ინფორმაცია ამის შესახებ იშვიათად ხვდება ჟურნალისტებთან. ედვარდ სნოუდენის მაგალითი, მისი მილიონშვიდასიათასი საიდუმლო დოკუმენტების შესახებ - გამონაკლისს წარმოადგენს.

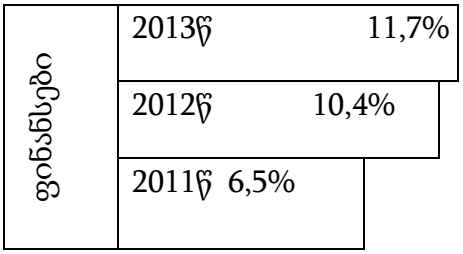
დროთა განმავლობაში, ინფორმაცია მსგავსი არასტანდარტული ინციდენტების შესახებ, აღწევს პრესას. ერთ-ერთ მაგალითს წარმოადგენს საფეხბურთო კლუბის „ბავარიის“ ტაქტიკური სქემების გაჟონვა, პრინციპული მატჩის წინ დორტმუნდის „ბორუსიასთან“. მომავალი შეხვედრის წინ, რამოდენიმე დღით ადრე დაწვრილებითი გეგმა გამოაქვეყნა ჟურნალმა Bild-მა. აღსანიშნავია, რომ ეს ინფორმაცია „ბორუსიის“ ფეხბურთელებს არ გამოადგათ, ისინი დამარცხდნენ გამანადგურებელი ანგარიშით. ისმის კითხვა, შეიძლება თუ არა, ნორმალურად აღიქვა კოლექტივში „გამცემის“ არსებობა - ეს მნიშვნელოვანი კითხვაა, თუმცა ბავარიელების სპორტულ მიღწევაზე ამ ინციდენტს არავითარი გავლენა არ მოუხდენია.

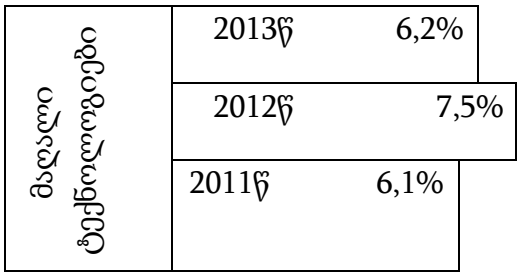
ზემოთ მოყვანილი მაგალითი, იმის მაჩვენებელია, რომ არსებობს ინფორმაციის გაჟონვები, რომელთა თავიდან აცილება ჩვეულებრივი ტექნიკური საშუალებებით შეუძლებელია. როგორი სრულყოფილიც არ უნდა იყოს ინფორმაციის კონტროლის საშუალებები, ყოველთვის არსებობს იმის შესაძლებლობა, რომ ინფორმაციიდან გარკვეული ცნობები დაინტერესებულმა პირმა დაიმახსოვროს, ამიტომ, ტექნიკური საშუალებების დონეზე აუცილებლად უნდა იქნას განხილული ორგანიზაციული საკითხები.

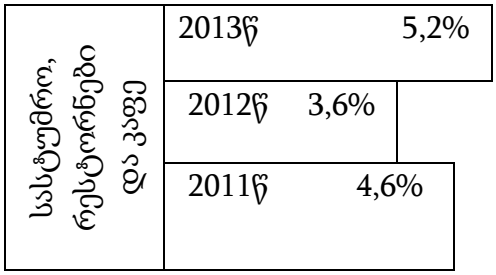
1.5. ინფორმაციის გაჟონვათა დარგობრივი სპეციფიკა

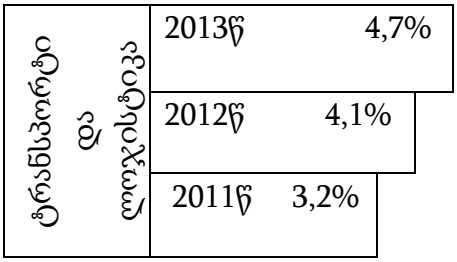


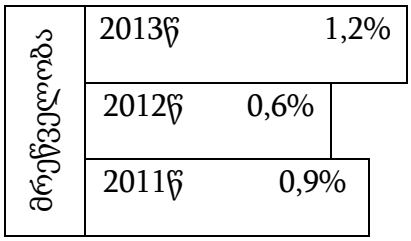


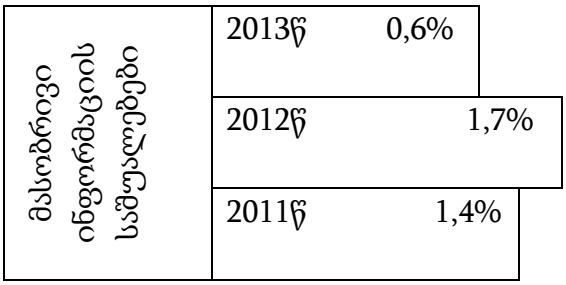


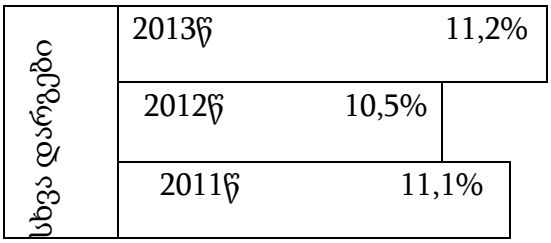

მაღალი ტექნოლოგიები
2013წ 6,2%
2012წ 7,5%
2011წ 6,1%


სასტუმრო, რესტორნები და კვება
2013წ 5,2%
2012წ 3,6%
2011წ 4,6%


ტრანსპორტი და ლოჯისტიკა
2013წ 4,7%
2012წ 4,1%
2011წ 3,2%


მრეწველობა
2013წ 1,2%
2012წ 0,6%
2011წ 0,9%


მასობრივი ინფორმაციის საშუალებები
2013წ 0,6%
2012წ 1,7%
2011წ 1,4%



1.6. ინფორმაციის გაჟონვის მიზეზები

მიუხედავად იმისა, რომ კონფიდენციალური ინფორმაციის მოპოვებაში ყოველთვის არის ვინმე დაინტერესებული, Zecurion-ის ბაზებში არსებული სტატისტიკური მასალების საფუძველზე, შეიძლება ითქვას, რომ ინციდენტების უმეტესი ნაწილი არ არის დაკავშირებული თაღლითობასთან და გამოწვეულია შემთხვევითობებით ან პიროვნებების გულგრილობით. ეს ტენდენცია არსებობს, გრძელდება და დაკავშირებულია იმ მეთოდოლოგიასთან, რომ ბაზებიდან ინფორმაციის გაჟონვების შესახებ ბაზებში საქმე გვაქვს ისეთ შემთხვევებთან, რომლების ხდება საჯაროდ ცნობილი. ხოლო, როდესაც საქმე გვაქვს ინფორმაციის მიზანდასახულ გატანასთან, მონაცემთა ქურდობასთან შემოგზავნილი ან მოსყიდული პირის მიერ, ისინი ყოველთვის დაინტერესებულები არიან კონფიდენციალურობის შენარჩუნებაში და გაჟონვის ფაქტი შეიძლება გაამჟღავნოს მხოლოდ ინფორმაციის მეპატრონემ, თუ ის ვითარებას დროულად შეაფასებს.

მიუხედავად ამისა, 2013 წელს ინფორმაციის შემთხვევითი და წინასწარგანზრახული გაჟონვების წილობრივი რაოდენობები გათანაბრდა. არსებობს ისეთი ინციდენტებიც, რომელთათვისაც მიზნების შინაარსის დადგენა რთულია. იმ შემთხვევებში, როდესაც ინფორმაციის გაჟონვა ერთდროულად უზრუნველყოფილია გარეშე პირთა წინასწარგანზრახული ქმედებითა და საკუთარი თანამშრომლების გულგრილობით, ინციდენტი კლასიფიცირდება, როგორც წინასწარგანზრახული ქმედება. მიზანდასახული გაჟონვების უმრავლესობა იმის დამადასტურებელი

აღმოჩნდა, რომ კომპანიები არასაკმარის მზრუნველობას იჩენენ ინფორმაციის დაცვის მიმართ და მაშინაც კი, როდესაც ეს დაკავშირებულია მნიშვნელოვან ფინანსურ ზარალთან.

სხვადასხვა არხებით ინფორმაციის გაჟონვის სტატისტიკა წინა წლის სტატისტიკის მსგავსია. ერთადერთი შესამჩნევი განსხვავებით, თითქმის გაჟონვების ერთნახევარჯერ ზრდით გამოირჩევა ელექტრონული ფოსტა. გასულ წლებში ინფორმაციის გაჟონვათა შესახებ წარმოებულ ანგარიშებში აღნიშნულია, რომ ელექტრონული ფოსტა კარგად კონტროლდება ავტომატიზებული ტექნიკური საშუალებებით, მათ შორის DLP (Data loss prevention - მონაცემთა დაკარგვის პრევენცია) სისტემებით. მაგრამ, სისტემების გავრცელება, ჯერ-ჯეროობით დაბალ დონეზეა, მაგალითად რუსეთში, საშუალო და მსხვილი ბიზნესის ორგანიზაციებში, 2012 წლის მონაცემებით, DLP–ს გავრცელებამ შეადგინა მხოლოდ 20%.

გამოიკვეთა აგრეთვე, რომ უმეტეს შემთხვევებში ერთ-ერთი მთავარი პრობლემა დაკავშირებულია არა იმასთან, რომ ბოროტგანმზრახველებს შეუძლიათ სხვისი სახელით შესაბამის საიტზე ავტორიზება, არამედ იმაში, რომ მომხმარებლები ხშირად იყენებენ ელექტრონული ფოსტის მისამართის და პაროლის ერთი და იგივე შეხამებას სხვადასხვა სისტემის სერვისებთან მისაერთებლად. აქ კი იშლება თაღლითობისათვის ხელსაყრელი გარემო. მომხმარებლისათვის შესაძლო შედეგები ვარირებს პირდაპირი ფულადი დანაკარგებიდან, როდესაც ხდება ქსელის საფინანსო სერვისების პირდაპირი გამოყენება, ბანალურ გამოძალვამდე სოციალურ ქსელებში გამოგონილი სერვისებისათვის.

ეს მაგალითიც, იმის მაჩვენებელია, რომ ტექნიკური საშუალებების დონეზე აუცილებლად უნდა იქნას განხილული, აგრეთვე ორგანიზაციული საკითხებიც.

დასკვნა

1. ინფორმაციის გაჟონვის შედეგები დამოკიდებულია იმაზე, თუ რა ტიპის მონაცემების გაჟონვა მოხდა. სხვადასხვა მომხმარებლებს შორის მიმოცვლის მონაცემებიდან, ყველაზე ხშირად კომპრომეტირებულია სხვადასხვა Web- სერვისებისა და საინფორმაციო სისტემების მომხმარებლების სააღრიცხო ჩანაწერები. ყველაზე იშვიათია ინფორმაციის გაჟონვა დაკავშირებული სახელმწიფო ან კომერციულ საიდუმლოებებთან, ინტელექტალურ საკუთრებასთან.
2. სხვადასხვა არხებით ინფორმაციის გაჟონვის სტატისტიკაში, ერთნახევარჯერ ზრდით გამოირჩევა ელექტრონული ფოსტა. ელექტრონული ფოსტა კარგად კონტროლდება ავტომატიზებული ტექნიკური საშუალებებით, მათ შორის DLP- სისტემებით. მაგრამ, რიგ ქვეყნებში DLP–ს გავრცელებამ შეადგინა მხოლოდ 20%.
3. არსებობს ინფორმაციის გაჟონვები, რომელთა თავიდან აცილება ჩვეულებრივი ტექნიკური საშუალებებით შეუძლებელია. როგორი სრულყოფილიც არ უნდა იყოს ინფორმაციის კონტროლის საშუალებები, ყოველთვის არსებობს იმის შესაძლებლობა, რომ ინფორმაციიდან გარკვეული ცნობები დაინტერესებულმა პირმა დაიმახსოვროს, ამიტომ, ტექნიკური საშუალებების დონეზე აუცილებლად უნდა იქნას განხილული ორგანიზაციული საკითხები.

თავი 2. სატელეკომუნიკაციო ქსელში პერსონალური მონაცემების დაცვის პრობლემები [40]

პერსონალური მონაცემების დაცვა არის სახელმწიფოებრივ დონეზე, ერთ-ერთი უმნიშვნელოვანესი მიმართულება ინფორმაციული უსაფრთხოების უზრუნველყოფის ერთიან სისტემაში.

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.).

ტექნოლოგიური თვალსაზრისით პრობლემა, რომ არ მოხდეს ინფორმაციის გაჟონვა, შედარებით გასაგებია: საჭიროა ორგანიზაციული და ტექნიკური ღონისძიებების გატარება, აუცილებელია მომხმარებელთა აუტენტიფიკაცია და ავტორიზაცია სათანადო დონეზე, კავშირგაბმულობის არხებში შიფრაციის გათვალისწინება, პერსონალურ მონაცემებთან ხელმისაწვდომობის შეფასება და სატელეკომუნიკაციო არხებში მონაცემების გადაცემის სისრულის დაცვა და აგრეთვე საინფორმაციო სისტემები, რომლითაც ხდება ამ მონაცემების დამუშავება. ამასთანავე, გასათვალისწინებელია, რომ დაცული ინფორმაცია ლოკალურ ქსელში შეიძლება მომხმარებლებისათვის პრაქტიკულად მიუწვდომელი გავხადოთ. მაგრამ, ინტერნეტის ქსელში ამის დაშვება შეუძლებელია, ვინაიდან ინფორმაციული საზოგადოებისათვის ასეთი ღონისძიება შეუთავსებელია. ჩვენ ვცხოვრობთ ღია ინფორმაციულ სამყაროში, სადაც სახელმწიფო ორგანოების მოღვაწეობის შესახებაც კი მონაცემები უნდა იყოს მაქსიმალურად ღია.

როდესაც დასრულდება ინფორმაციული საზოგადოების კონცეფციის რეალიზება (ელექტრონული მთავრობა, სახელმწიფო მომსახურების უზრუნველყოფა ინტერნეტით და ა. შ) შეიქმნება „ღია გასაღებების“ ინფრაქტრუქტურა [41]. 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. პერსონალური მონაცემების დაცვასთან დაკავშირებით არსებობს მნიშვნელოვანი შედეგები, თუ 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%

(ინფორმაციის წყარო [42])

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

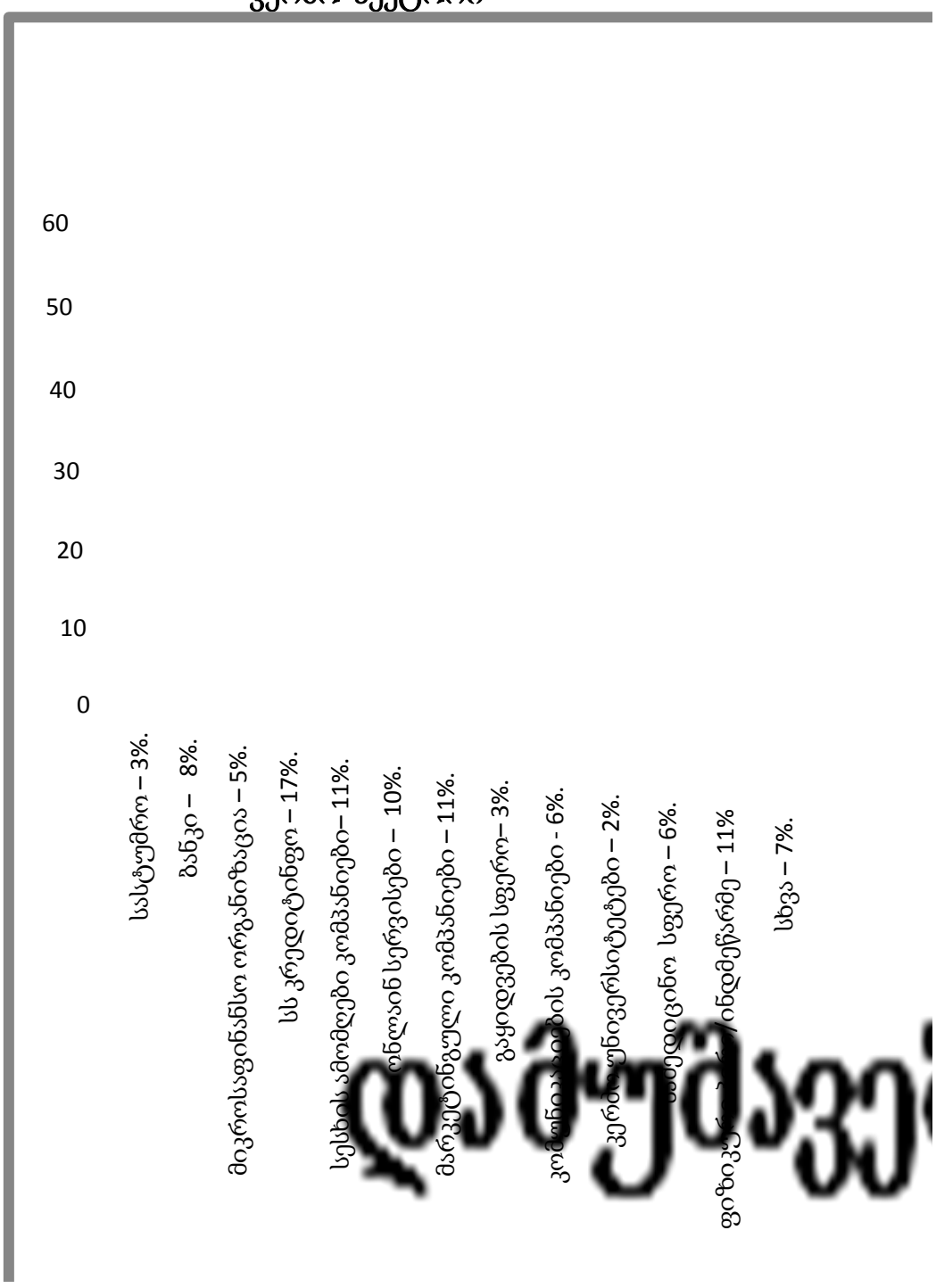
შემდეგი მნიშვნელოვანი საკითხი, რომელიც გაანალიზებულია სამეცნიერო კვლევებში და შეეხება, თუ ვის და რა რაოდენობის პირებს აქვთ წვდომა პერსონალურ მონაცემებზე:

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%

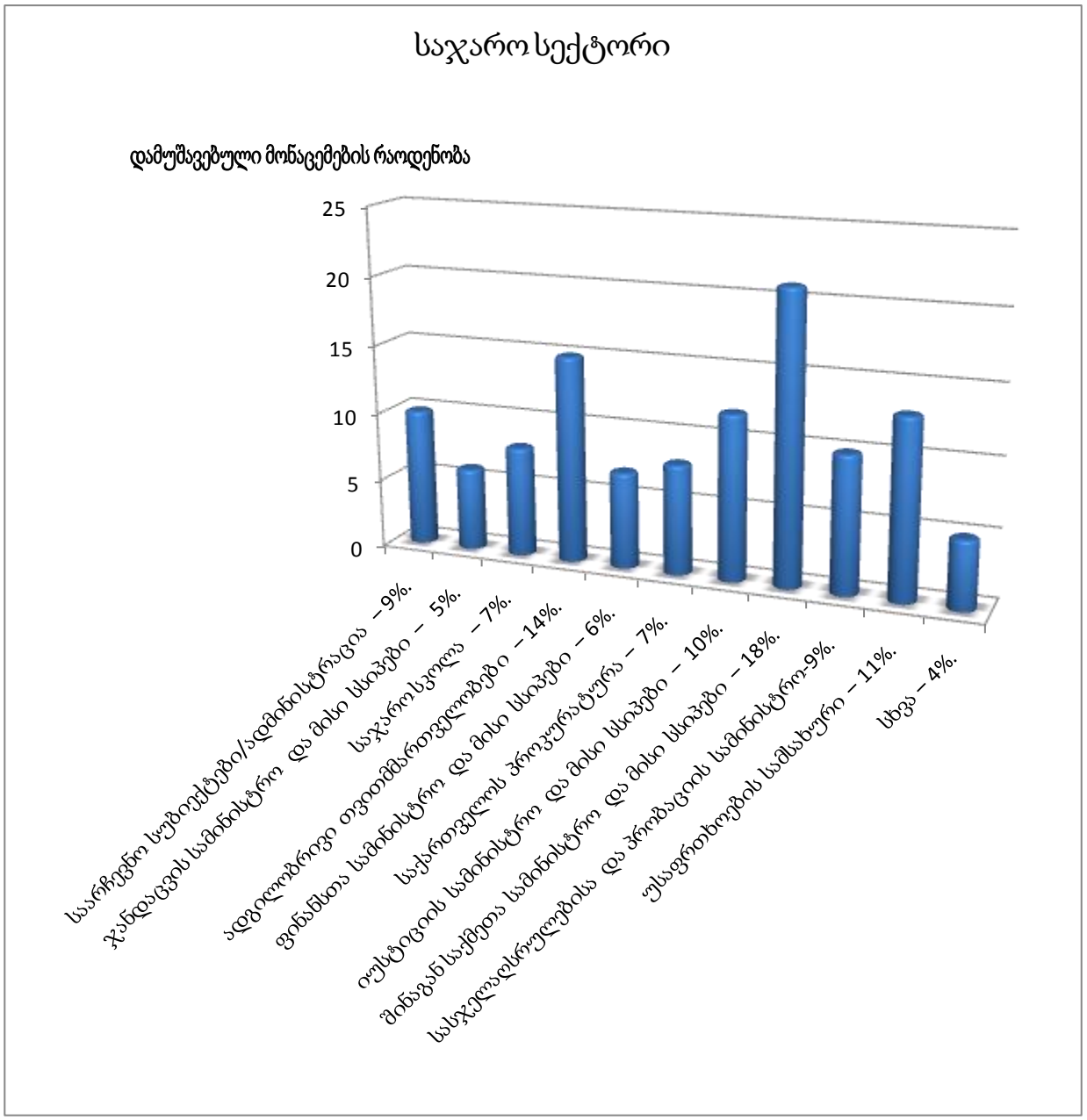
(ინფორმაციის წყარო [42])

პრაქტიკულად, მხოლოდ უსაფრთხოების სამსახურის თანამშრომლების დაშვება პერსონალურ მონაცემებთან შეესაბამება 4%, ხოლო ინფორმაციული ტექნოლოგიების სამსახურის თანამშრომლები ყველაზე ხშირად (41%) არიან პერსონალურ მონაცემებთან, რაც ძალზე დამაფიქრებელია.



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)

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.

სამეცნიერო კვლევებში გაანალიზებულია აგრეთვე დაბრკოლებები, რომლებიც დაკავშირებულია პერსონალური მონაცემების დაცვისათვის გათვალისწინებული ღონისძიებების გატარებასთან:

ცხრილი 3. დაბრკოლებები დაცვის გათვალისწინებული ღონისძიებებისათვის

კვალიფიცირებული კადრების ნაკლებობა	31%
ფინანსური შეზღუდვები	30%
პრაქტიკულად როგორ განხორციელდეს არ არის ცხადი	24%
არავითარი დაბრკოლება და სიძნელეები არ არსებობს დაცვის განსახორციელებლად	7%
გვაქვს განსხვავებული პრიორიტეტული პროექტები	3%
ხელმძღვანელობის მხარდაჭერა არ გაგვაჩნია	3%
პასუხი არ გვაქვს	2%

საერთაშორისო გამოცდილებით მიზანშეწონილია შეირჩეს უმისამართო, ანუ ღრუბლებში არსებული პერსონალური მონაცემების საინფორმაციო სისტემა, რაც იდეალურად ითვლება მომსახურების სახეობების დამმუშავებელთათვის; მსხვილი ორგანიზაციებისა და კომპანიების განაწილებადი (Shared Services) სერვისების განსათავსებლად; ინტერნეტ–მაღაზიებისათვის; სოციალური ქსელებისათვის.

ასეთი მიდგომის უპირატესობებია:

- მომსახურე პერსონალზე დანახარჯების შემცირება;
- კაპიტალური ხარჯების ეკონომია;
- გამოთვლითი ტექნიკის სიმძლავრეების მასშტაბირება;
- ინფრასტრუქტურის მაღალმიღწევადობა;
- მოწყობილობების მოდერნიზაციაზე და მოვლაზე ხარჯების შემცირება;
- კომპანიის სერვისების სტანდარტიზაცია.

ამისათვის, უნდა გადაიდგას შემდეგი ნაბიჯები: პირველი– შეირჩეს მონაცემთა დამუშავების ცენტრი აუცილებლად საქართველოს ტერიტორიაზე. აუცილებელია მონაცემთა დაცვის ცენტრის შემოწმება შეფერხებამდგრადობაზე, საერთაშორისო სტანდარტის შესაბამისად (კლასიფიკაციის სისტემა Tier). უნდა გააჩნდეს ინფორმაციის დაცვის ლიცენზირებული საშუალებები (ინფორმაციის დაცვის ტექნიკური საშუალებები და იყენებდეს დაცვის კრიპტოგრაფიულ საშუალებებს).

მეორე ნაბიჯი: განსათავსებელი სისტემის არქიტექტურის შერჩევა. აქ მნიშვნელოვანია, რომ პერსონალური მონაცემების სისტემის ყველა კომპონენტი იყოს დაცული. მაგალითად, სტატისტიკური მონაცემებისათვის პერსონალური მონაცემები უნდა იყოს უსახური. ამრიგად ხორციელდება მსხვილი სისტემის დანაწილება, იმის მიხედვით თუ როგორ მოითხოვება პერსონალური მონაცემების დამუშავება. შესაბამისად, მცირდება ინფორმაციის გარკვეული ნაწილის დაცულობის დონე, რომელიც დოკუმენტალურად და დასაბუთებულად გახდება პერსონალური მონაცემების დამოუკიდებელი ინფორმაციული სისტემა. ეს დასაშვებია მსხვილი კორპორატიული, სამედიცინო, საბანკო და სხვა სისტემებისათვის.

მესამე ნაბიჯი: ინფორმაციის დაცვის საშუალებების შერჩევა, რაც გარკვეულ სირთულეებთან არის დაკავშირებული, ვინაიდან დაცვის სისტემების გამოყენება მნიშვნელოვან ზეგავლენას ახდენს მომსახურებისათვის წვდომის მაჩვენებელზე და ქმედითუნარიანობაზე.

ჩვენს მიერ შემოთავაზებული დაცვის სისტემის შერჩევისა და ოპტიმიზაციის პრინციპი მნიშვნელოვნად ამარტივებს და მაქსიმალურად ამყარებს დაცულობის უზრუნველყოფის პროცესს.

მეოთხე ნაბიჯი: ტესტური კონტურის შექმნა, რომელშიც შემოწმდება სისტემის ძირითადი თვისებები და დადგენილი იქნება, რამდენად შეესაბამება სატელეკომუნიკაციო ქსელის ინფრასტრუქტურა დაკისრებული ამოცანების გადაწყვეტას, ანუ განხორციელდება ტესტირება ინფორმაციის დამუშავების ცენტრის დატვირთვაზე და მის გამტარუნარიანობაზე.

მეხუთე ნაბიჯი: როდესაც პერსონალურ მონაცემთა სისტემა მიგრირებული და ტესტირებულია მონაცემთა დამუშავების ცენტრში (რომელიც განთავსებულია „ღრუბლებში“) ის შედის ექსპლუატაციაში. საჭიროა მონიტორინგის გამართლებული სისტემისა და ყველა ქმედებაზე სარეზერვო ასლების შექმნა.

2.1. 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.

ამასთანავე, აღსანიშნავია, რომ ორგანიზაციებსა და კომპანიებში სამეტყველო ინფორმაციის დაცვა ტექნიკური არხებით მათი გაჟონვისაგან, უნდა პასუხობდეს თანამედროვე მოთხოვნებს დაზვერვის არსებული ტექნიკური საშუალებების შესაძლებლობებიდან გამომდინარე. შეუსაბამობის ძირითად მიზეზს შეიძლება წარმოადგენს დაცვის უზრუნველყოფისადმი ტრადიციული მიდგომა, კერძოდ იმ ტექნიკური არხების აღმოჩენა, რომლებითაც შეიძლება გაჟონოს სამეტყველო ინფორმაციამ. ამისათვის საჭიროა შესწავლილ იქნას ბოროტმზრახველის შესაძლო ქმედებები დაკავშირებული სამეტყველო ინფორმაციის მიტაცების შესაძლებლობებთან, ანუ უნდა დამუშავდეს ბოროტმზრახველის შესაძლო მოქმედებების განსაზღვრის ალგორითმი, რაც საშუალებას მოგვცემს არა მარტო მოვახდინოთ გაჟონვის საშიშროების წყაროს იდენტიფიცირება, არამედ ავამაღლოთ ასეთი სახის საშიშროებებისაგან დაცვის ღონისძიებების ეფექტურობა.

იმისათვის, რომ განისაზღვროს სამეტყველო ინფორმაციის გაჟონვის შესაძლო ტექნიკური არხები, აუცილებელია ინფორმაციის ფიზიკური ველების შესწავლის უწყვეტი პროცესი, საშიშროებათა ნიშნების სისტემეტიზაციის მიზნით, რაც მოგვცემს საშუალებას სწორად შევარჩიოთ ორგანიზაციისა თუ დაწესებულებისათვის. ინფორმაციის ფიზიკური ველების მდგომარეობის განსაზღვრის მეთოდები და ტექნიკური საშუალებები.

სამეტყველო ინფორმაციის გაჟონვის საშიშროებათა განსაზღვრის ხარისხის მაჩვენებლის შეფასებისათვის გამოვიყენოთ მოვლენის P ალბათობა, რომელიც ცალკეული მინიშნებებიდან საზღვრავს სამეტყველო ინფორმაციის გაჟონვის საშიშროების არსებობის ხარისხს. შეფასება ჩაითვლება განხორციელებულად თუ P ალბათობა $\{x_i\}$ სიმრავლიდან, $i=1,2,\ldots X$ საშიშროებათა ცალკეული მინიშნებების განსაზღვრებებიდან, ახდენს საშიშროების წარმოშობის ხარისხის ფორმირებას.

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.

2.2. ინფოსაკომუნიკაციო სისტემების კიბერუსაფრთხოება

ინფორმაციული უსაფრთხოებისათვის ახალი ხიფათები დაკავშირებულია საინფორმაციო ტექნოლოგიების მასიურ გამოყენებასთან, იმ ელემენტების მრავალრიცხოვნობასთან, რომლებისაგანაც შედგება საინფორმაციო სივრცე, მათ შორის ურთიერთკავშირების მრავალფეროვნებასა და ურთიერთქმედებების დიდ რაოდენობასთან, მაშინ როდესაც ინფორმაციული უსაფრთხოების უზრუნველყოფის პროცესებზე კონტროლი სუსტია. ცხადია, კიბერუსაფრთხოების პრობლემები გადაწყვეტილი უნდა იქნას სისტემურ დონეზე, ზემოთაღნიშნული ფაქტორების გათვალისწინებით. პრობლემის სირთულე დაკავშირებულია აგრეთვე იმასთან, რომ ძირითადი ცნებებისა და განსაზღვრებების სისტემა არ არის განვითარებული, ამასთანავე, საინფორმაციო ტექნოლოგიების გარკვეული კონსერვატულობა, რომელიც დაკავშირებულია მოწყობილობებისა და ინფორმაციული პროცესების თავსებადობის

უზრუნველყოფის აუცილებლობასთან, მნიშვნელოვნად ზღუდავენ ინფოსაკომუნიკაციო სისტემების ინფორმაციული უსაფრთხოების სათანადო დონემდე აყვანას.

ჩვენ ვცდილობთ, წარმოვადგინოთ სისტემური ხედვა ინფორმაციული პროცესების იმ ძირითად შემადგენელ ელემენტებზე, რომლებიც დღეისათვის ერთმანეთთან შეუკავშირებელია კობერუსაფრთხოების უზრუნველყოფის თვალსაზრისით.

ინფოკომუნიკაციის ტერმინის ქვეშ იგულისხმება ინფორმაციით–მართული სისტემების, აგრეთვე საინფორმაციო ტექნოლოგიების არაერთგვაროვანი კომპონენტების, მაგალითად დისტანციურად მართული ობიექტების, ტელემეტრიული, ინფორმაციის შეკრებისა და დამუშავების სისტემები და სხვა რთული გაერთიანება სხვადასხვაგვარი არხებითა და ინფორმაციის გადაცემის სხვადასხვა ტიპის ქსელებით.

ინფოსაკომუნიკაციო სისტემების სტრუქტურა და შემადგენლობა განისაზღვრება მათი მიზნობრივი დანიშნულების მიხედვით, მაგრამ უსაფრთხოებისა და ინფოსაკომუნიკაციო სისტემის ფუნქციონირების საიმედობის პრობლემებს აქვთ საერთო საწყისები და მდგენელები.

ინფოსაკომუნიკაციო სისტემების უსაფრთხოების ყველა პრობლემების საწყის პირობას წარმოადგენს, ერთის მხრივ მნიშვნელოვანი სამომხმარებლო საინფორმაციო რესურსი და მეორეს მხრივ კი ბოროტმომქმედის არსებობა, რომლის მიზანია მიიღოს, დაამახინჯოს ან გაანადგუროს ეს რესურსი.

ინფოსაკომუნიკაციო სისტემების უსაფრთხოდ ფუნქციონირების უზრუნველყოფის სირთულე, პროექტირების ზოგად პრობლემატიკასთან შეფარდებით, დაკავშირებულია იმ გარემოებასთან, რომ საინფორმაციო ტექნოლოგიების ძირითად მაჩვენებელს წარმოადგენს მისი ფუნქციონირების ეფექტურობა და არა მისი დაცულობის დონე, რაც იწვევს სისტემური პროექტირების ფუნდამენტურ პრობლემაზე მოთხოვნას, რომ გათვალისწინებული იქნას სისტემის ეფექტურობის გაზომვადი

მეჩვენებელი, გათვალისწინება, რომელიც უშუალოდ იქნება დამოკიდებული მისი უსაფრთხოდ ფუნქციონირების დონეზე. მაგალითად, ინფოსაკომუნიკაციო სისტემისაგან ინფორმაციული მომსახურების ხარისხიანი (ოპერატიულად, სრულად) მიღება, უნდა განისაზღვრებოდეს მისი უკუქმედების უნარით DoS (Denial of Service –უარი მომსახურებაზე) ტიპის ბოროტმომქმედის შემოტევებზე (ცხადია, ეს მხოლოდ მაგალითია), ხოლო საინფორმაციო–მმართულ სისტემებში უსაფრთხოების ცნების ძირითადი შინაარსია დაუცველობა, საფრთხეები და შემოტევები.

დაუცველობა განისაზღვრება, როგორც ნაკლოვანება, რომლის გამოყენებით ბოროტმომქმედს შეუძლია დაარღვიოს სისტემის ფუნქციონირების სისრულე და გამოიწვიოს სისტემის არაკორექტული მოქმედება. გასათვალისწინებელია, რომ სისტემის ნაკლოვანება, ანუ დაუცველობა ხასიათდება არა რაოდენობრივად, არამედ დაუცველობის გამო მოსალოდნელი საფრთხის ხარისხით. იმისათვის, რომ ეს მსჯელობა ხაზგასმით გამოჩნდეს, იყენებენ ტერმინს „ დაუცველობის წყაროები“ [43].

რომელიმე ნაკლოვანების (დაუცველობის) არსებობისაგან საშიშროება უმეტესად განისაზღვრება მისი მნიშვნელობით (სისტემის ძირითადი მახასიათებლების დამოკიდებულებით ნაკლოვანებაზე, მათ შორის სისრულის მახასიათებელზე), სიცხადის ხარისხით ბოროტმომქმედისათვის და მასზე შეტევის შედეგად , თუ რამდენად შესრულებადია ზემოქმედება. აქ სიცხადის ქვეშ ვგულისხმობთ ბოროტმომქმედისათვის, რამდენად ხელმისაწვდომია დაუცველობის შესახებ რეალური ინფორმაცია. ცალკეული დაუცველობის მნიშვნელობა და სიცხადე ერთიანდება ცნებაში – საშიშროება, ხოლო შეტევა განიხილება, როგორც საშიშროების რეალიზება.

2.3. ინტეგრირებული ინფოსაკომუნიკაციო სისტემის ფუნქციონირების უსაფრთხოება

დღეისათვის არსებობს რიგი შედეგები, რომლებიც უზრუნველყოფენ სატელეკომუნიკაციო ქსელებისა და სისტემების ინფორმაციულ უსაფრთხოებას, თუ შევძლებთ, რომ მათგან გამოვყოთ ყველაზე აქტუალურები, რომელთა დანერგვაც საშუალებას მოგვცემს, მაქსიმალურად დავიცვათ ორგანიზაციებისა და კომპანიების ინფორმაცია.

სადისერტაციო ნაშრომში გამოყოფილია ის ოთხი ძირითადი მიმართულება ინფორმაციის უსაფრთხოების უზრუნველყოფისათვის, რომლებიც იკვეთება მსოფლიოს ინფოსატელეკომუნიკაციო სისტემებისა და ქსელების ექსპლუატაციის შედეგად მიღებული გამოცდილების საფუძველზე:

1. დაცვა DDOS (Distributed Denial of Service - დანაწილებული უარი მომსახურებაზე) – შემოტევებისაგან;
2. უსადენო სატელეკომუნიკაციო ქსელების დაცვა;
3. NGFW (Next Generation Firewall - შემდეგი თაობის საქსელთაშორისო ეკრანი) და UTM parameters (Urchin Tracking Module) ნიშნულები;
4. SIEM (Security information and event management) ინფორმაციის უსაფრთხოებისა და ინფორმაციული მოვლენების მართვა.

DDOS – შემოტევებისაგან დაცვა აქტუალური პრობლემაა შემდეგი ფაქტორების გამო:

- DDOS – შეტევების სიმარტივე და რეალიზებისათვის მცირე ხარჯები;
- ბოტნეტ–ქსელების ფართოდ გავრცელება (პროგრამული უზრუნველყოფის კომპლექტი რომელიც შედგება ვირუსებისაგან, ეკრანებისაგან და ოპერაციული სისტემის დამალული ინსტრუმენტებისაგან);
- შემოტევების ახალი სახეობების გამოჩენა და კომპლექსური სირთულის ამაღლება შესაბამისი უკუქმედების მისაღწევად.

როგორც ცნობილია, არსებობს DDOS – შემოტევების შემდეგი ტიპები:

- შემოტევები სატელეკომუნიკაციო არხის გადავსების მიზნით;
- შემოტევები სესიის (დამყარებული კავშირის) გადავსენის მიზნით;
- შემოტევები მომსახურების სახეობებზე.

ცნობილი ანალიტიკური კომპანიების ანგარიშებიდან იკვეთება, რომ DDOS – შემოტევების რაოდენობა იზრდება ყოველდღიურად, ამასთანავე შეიმჩნევა რომ შემოტევების ზრდა მოდის ძირითადად სესიებისა და მომსახურების სახეობების გადავსებაზე. აღსანიშნავია, რომ IPS (In plane switching) ქსელთაშორისი ეკრანები აღმოჩნდნენ არაეფექტურები, ვინაიდან არ გააჩნიათ ძირითადი ამოცანის გადაწყვეტის უნარი, კერძოდ მომსახურების სახეობების შეუფერხებელი ამოქმედება DDOS – შეტევის გამოჩენისას.

კომპანია Space IT (იტალია, 28 წლიანი გამოცდილებით კოსმოსური სისტემების სივრცეში) ანგარიშიდან ჩანს რომ: Infonetics DDOS Report 2013: Arbor Pravail APS დაამუშავა საშუალება, რომელიც იცავს მომხმარებლის მხარეს, ანუ განკუთვნილია ორგანიზაციის (კომპანიის) დასაცავად. ეს სისტემა თავსებადია ქსელში არსებული, მათ შორის ღრუბლების ანუ (მისამართი უცნობია) DDOS არსებულ სისტემებთან. აგრეთვე უსადენო სატელეკომუნიკაციო ქსელების: WIPS (Wireless Intrusion Prevention System) და MDM (Master Data Manegment) დაცვა.

მობილური მოწყობილობების ფართოდ გავრცელებამ და WiFi-ს საშუალებით მონაცეთა გადაცემის სიჩქარის გაზრდამ დააჩქარა კორპორატიული უსადენო ქსელების რაოდენობრივი აღმავლობა. კორპორატიულ ქსელებში WiFi დანერგვა მოითხოვს ინფორმაციის დაცვის საშუალებების გამოყენებას. მაშინაც, კი როდესაც კომპანია კორპორატიული სტანდარტებით არ ითვალისწინებს უსადენო ქსელის გამოყენებას, რითაც ისინი ხელს უწყობენ (უნებურად) მონაცემთა გაჟონვას.

ამრიგად, შესაძლებელია ასეთ ვითარებაზე სრული კონტროლის დამყარება და ინფორმაციის გაჟონვის არხების ჩახშობა, შესაძლებელია რადიოეთერის სკანირება და WiFi–სათვის ხელშეშლების წყაროს

ადგილმდებარეობის აღმოჩენა და მისი აღმოფხვრა. უსადენო სატელეკომუნიკაციო ქსელების დაცვის კიდევ ერთ მიმართულებას წარმოადგენს BYOD (Bring Your Own Device - მოიტანე საკუთარი მოწყობილობა) ტენდენციის არსებობა. თანამშრომელთა მობილურობის გაზრდამ წარმოქმნა კიდევ ერთი დაუცველობა ინფორმაციის დაცვის სისტემაში. მომხმარებლები საკუთარ მოწყობილობებს იყენებენ, როგორც კორპორატიული, ასევე პირადი ინტერესებისათვისაც. კომპანია Aruba Networks–ს გააჩნია მოწყობილობების სრული კომპლექსი BYOD დაცვის შესაქმნელად.

ტრადიციული ქსელთაშორისი ეკრანები ტრაფიკის კლასიფიცირებას ახდენენ პორტებისა და პროტოკოლების შესაბამისად, რაც საშუალებას აძლევს მომხმარებლებს (მომსახურების სახეობებს) გვერდი აუარონ დაცვის სისტემას და გამოიყენეონ არასტანდარტული პორტები, რამოდენიმე პორტი ან ნებისმიერი პორტი. ამის შედეგად სისტემური ადმინისტრატორი კარგავს ქსელის ინფრასტრუქტურაზე კონტროლს, რაც იწვევს ქსელში საშიშროების მატარებელი პროგრამული უზრუნველყოფის შემოჭრას, მნიშვნელოვანი ინფორმაციის დაკარგვას და ქსელის მდგრადი მუშაობის დარღვევას. ყველა ეს პრობლემები შეიძლება გადაიჭრას ახალი თაობის ქსელთაშორისი ეკრანის NGFW–ს გამოყენებით. ასეთი ქსელთაშორისი ეკრანები მუშაობენ არა იმ პორტებთან, რომლებთანაც დაკავშირებულია მომსახურების სახეობები, არამედ მუშაობენ უშუალოდ მომსახურების სახეობებთან. NGFW–არის დღეისათვის ქსელთაშორისი ეკრანების განვითარების უმაღლესი ეტაპი, რომელიც ითვალისწინებს მომხმარებელთა ბაზებთან ინტეგრაციას, პორტებისა და პროტოკოლებისაგან დამოუკიდებლად მომხმარებლებისა და საქსელო მომსახურების სახეობების განსაზღვრას.

NGFW უზრუნველყოფს კორპორატიული ქსელის ელემენტებისა და მომხმარებლების დაცვას საფრთხისშემცველი კონტენტისა და მომსახურების სახეობებისაგან და ამ დროს ის იყენებს მომხმარებელთა

პროფილებს და არა მათ მისამართებს. გარდა ამისა ყველა NGFW წარმოადგენს UTM (Unifled Threat Managment) - ერთიან მოწყობილობას, რომელიც იმართება საერთო ოპერაციული სისტემიდან და შეიცავს დაცვის ელემენტების კომპლექსს.

თანამედროვე კორპორატიული ქსელების გამოყენებას თან ახლავს თაღლითობებისა და ინტერნეტსაფრთხეების, ღირებული კორპორატიული ინფორმაციის ქურდობა გარე სამყაროდან. აქ მნიშვნელოვანია, რომ დროულად იქნას გამოვლენილი ასეთი საფრთხეების არსებობა და მათი წყაროები. ამ ამოცანის გადაწყვეტას ემსახურება SIEM სისტემა, რომელიც აანალიზებს ქსელში არსებული ინფორმაციიდან ნაკადებს და იძლევა საშუალებას, მოვლენათა დიდი რაოდენობიდან მოახდინოს უსაფრთხოების ინციდენტებისა და ანომალიების (network behavior) იდენტიფიცირება, რის საფუძველზეც აღმოაჩენს საფრთხეებს. ამ სისტემაში ხდება ინფორმაციის ნორმირება და კორელირება საფრთხეების ეფექტურად აღმოჩენის, შეტყობინებების და მათგან დაცვაზე დროულად რეაგირების მიზნით. შედარებისათვის შეიძლება ითქვას, რომ სხვა მიდგომები არის შეზღუდული უნარების მქონე. მაგალითად მონიტორინგის საშუალება QRadar SIEM საშუალებას აძლევს ორგანიზაციებსა და კომპანიებს აღმოაჩინონ და აღმოფხვრან ისეთი საფრთხეები, როგორებიცაა მომსახურებათა სახეობების არამოზნობრივი გამოყენება, გარე სამყაროდან განხორციელებული თაღლითობები, საშიშროებები რომლებიც შეიძლება, სხვა მილიონობით მოვლენას შორის,შეუმჩნევლად დარჩენილიყო.

შეგვიძლია დავასკვნათ, რომ ამჟამად არსებობს მსოფლიოს ლიდერი მწარმოებლების (PaloAlfo, WatchGuard, Cisco, CheckPoint, juniper Networks და სეგმენტის ლიდერის IBM – გადაწყვეტილებები) შემოთავაზებები, რომლებსაც შეუძლიათ მაქსიმალურად უზრუნველყონ ორგანიზაციებისა და კომპანიების სატელეკომუნიკაციო ქსელებსა და სისტემებში ინფორმაციის დაცვა, სატელეკომუნიკაციო ქსელებისა და სისტემების სტრუქტურისა და ფუნქციონირების ალგორითმის გათვალისწინებით. ეს

უკანასკნელი მოითხოვს, რომ სატელეკომუნიკაციო ქსელები და სისტემები განხილული იქნას, როგორც კიბერსივრცე.

ინფორმაციული უსაფრთხოების შესახებ Cisco–ს ანგარიში, რომელიც გამოქვეყნდა 2014 წელს Black Hot („შავი ცხელება“) – კონფერენციაზე შეიცავს, ეგრეთწოდებული საინფორმაციო სისტემების სუსტი რგოლების ანალიზს. საინფორმაციო სისტემების სუსტ რგოლებს შეიძლება წარმოადგენდეს მოძველებული პროგრამული უზრუნველყოფა, ცუდად შედგენილი (დაწერილი) კოდი, მომხმარებელთა შეცდომები ან უყურადღებოდ მიტოვებული ინფორმაციული აქტივები, რაც ავისმზრახველებს უადვილებს არსებული დაუცველობების გამოყენებას, მაგალითად DNS შეკითხვების საშუალებით, გაძლიერებული შეტევებით, POS-სისტემების კომპრომეტაციით, საფრთხისშემცველი რეკლამებით, გამომძალველთა პროგრამებით, შიფრირების პროგრამებით, სოციალური ინჟინერიითა და რეალურ მოვლენებთან ადაპტირებული სპამით. Cisco–ს ანგარიშში ნაჩვენებია, რომ ის ორგანიზაციები, რომლებიც განსაკუთრებულ ყურადღებას უთმობენ მხოლოდ პოპულარულ დაუცველობებს, დიდი რისკის ქვეშ აყენებენ ობიექტებსა და კომპანიებს. ბოროტმზრახველები, რომლებიც უტევენ უყურადღებოდ მიტოვებულ, მოძველებული მომსახურებების სახეობებსა და ინფრასტრუქტურას ცნობილი დაუცველობებით, არ იქნებიან აღმოჩენილები, რადგანაც ინფორმაციული უსაფრთხოების სპეციალისტები ძირითადად დაკავებულები არიან უფრო თვალსაჩინო დაუცველობებით, მაგალითად ისეთით, როგორიცაა Heartbleed (უსაფრთხოების შეცდომა კრიპტოგრაფიულ პროგრამულ უზრუნველყოფაში, რომელიც სერვერის, კლიენტის მეხსიერების და მომხმარებელთა პაროლების არასანქციონირებულად კითხვის საშუალებას იძლევა).

Cisco–ს ანგარიში შედგენილი იყო 16 მსხვილი საერთაშორისო ორგანიზაციების კორპორატიული ქსელების ყურადღებით შესწავლის

საფუძველზე. ანალიზის საფუძველზე გამოვლენილი იქნა კორპორატიული ქსელისათვის სამი, ზიანისშემცველი ტრაფიკი:

- შეტევები (MITM - Man in the middle) „ადამიანის როლი ბრაუზერში“ ტიპის, მომხმარებლების ქსელების 94%–ში , 2014 წელს, ვებ–საიტებზე დაფიქსირებული იქნა ზიანისშემცველი კოდი. კერძოდ, ქსელებიდან იგზავნებოდა DNS შეკითხვები ხოსტის სახელებით, რომლებიც გარდაიქმნებოდა მოწყობილობის IP–მისამართად, რომელიც ცნობილი იყო, როგორც ზიანისშემცველი Palevo, SpyEye და Zeus (ვირუსების სახელწოდებებია) ტიპის პროგრამული უზრუნველყოფის გამავრცელებელი (MITM - Man in the middle) „ადამიანის როლი ბრაუზერში“ შეტევის ტიპის შესაძლებლობებით.
- „დამალობანას მოთამაშე“ ბოტნეტი. Cisco–ს ანგარიშში აღნიშნულია, რომ ქსელების 70% აგზავნის DNS შეკითხვებს DNS–ის დინამიურ დომენებში. ეს კი მიანიშნებს, რომ ამ ქსელების ექსპლუატაციას, ან კომპრომენტაციას ეწევიან ბოტნეტები, რომლებიც განუწყვეტლივ იცვლიან IP–მისამართებს დინამიური DNS–ის საშუალებით, რათა არ იქნან აღმოჩენილები. კორპორატიული ქსელიდან სანქციონირებული გამავალი შეერთებები არ იყენებს დინამიურ DNS დომენს. დინამიურ DNS დომენს იყენებს ბოტნეტის მიერ მართული სერვერი უკუშეკითხვების პროცესში, ბოტნეტის ადგილმდებარეობის მასკირების მიზნით.
- მოპარული მონაცემების შიფრირება. Cisco–ს ანგარიშის მიხედვით, ქსელების 44% დაფიქსირდა გამავალი DNS მოთხოვნები საიტებისა და დომენების მიმართ, რომლებსაც გააჩნიათ არხების შიფრირების მოწყობილობები, რითაც ავისმზრახველები ცდილობენ წაშალონ მონაცემების მიმთვისებელთა კვალი, რომლებსაც გადასცემენ დაშიფრული არხებით (VPN, SSH, SFTP, FTP და FTPS).

დასკვნისათვის გამოვიყენებ Cisco–ს ინფორმაციული უსაფრთხოების დირექტორის (John Stewart) მოსაზრებას: „კომპანიების უმეტესობა

თავიანთ განვითარებაში ეყრდნობიან ინტერნეტს. იმისათვის, რომ წარმატებულები იყვნენამ სწრაფად ცვლად გარემოში, აღმასრულებელმა ხელმძღვანელობამ უნდა გაითვალისწინოს და ორგანიზაციული თვალსაზრისით უნდა აიყვანონ კონტროლზე თანამდევი კიბერსაფრთხეები. ინფორმაციული უსაფრთხოების სისტემის დაუცველობის ანალიზი და ცოდნა, ძირითადად ეფუძნება ცალკეული ორგანიზაციებისა და მთელი დარგის უნარებს მოიპოვონ ცნობები კიბერსაფრთხეებზე არა მარტივად ტექნოლოგიებით, არამედ ორგანიზაციული შესაძლებლობითაც. დღეისათვის, რომ შევძლოთ შეტევის მოგერიება, მისი მთელი სიცოცხლისუნარიანობის განმავლობაში, ორგანიოზაციებმა უნდა გამოიყენონ ინფორმაციული უფასრთხოების ის საშუალებები, რომლებსაც შეუძლიათ მოქმედება იქ, სადაც შეიძლება საშიშროების არსებობა.

2.4. კიბერუსაფრთხოება – ინფორმაციული უსაფრთხოების ტექნიკური და ტექნოლოგიური ასპექტები

ტერმინი კიბერუსაფრთხოების განმარტება სრულად არ არის მდგრადი [44], თუმცა, კიბერუსაფრთხოების ძირითადი დებულებები შესულია საერთაშორისო სტანდარტში ISO / IEC 27032:2012 Information technology - Security techniques – Guiolelines for cybersecurity [2].

ამ ტერმინში უმეტესად განცხადებულია საინფორმაციო ობიექტების ფუნქციონირების (გამოყენების) უსაფრთხოების ცნება, ანუ შინაარსით კიბერუსაფრთხოება იგივეა, რაც ინფორმაციით მართული სისტემების ინფორმაციული უსაფრთხოება. სამეცნიერო კვლევებში ინფოსაკომუნიკაციო სისტემების სპეციფიკის გათვალისწინებით, კიბერუსაფრთხოება განმარტებულია, როგორც ინტეგრირებული ინფოსაკომუნიკაციო სისტემის ფუნქციონირების უსაფრთხოება, რომლის შემადგენელ ნაწილსაც წარმოადგენს ინფორმაციით მართული სისტემებიც.

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, ჭიები და სხვა.

კომპიუტერული სისტემების პროგრამული უზრუნველყოფაც, მათ მიერ შენახული და განახლებული ინფორმაციაც შედის კიბერსივრცეში, მოწყობილობებიც და ნაგებობებიც, რომლებშიც განთავსებულია ისინი და აგრეთვე ისინიც კიბერსივრცის ნაწილს წარმოადგენენ.

კიბერუსაფრთხოების მიზანია უსაფრთხო კიბერსივრცის ორგანიზება. ამის შესაბამისად კიბერუსაფრთხოება შეიძლება განხილული იქნას 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 მოსალოდხიფათების მართვა. ეს პროცესი მოიცავს იმ კომპონენტების იდენტიფიკაციას, რომლებიც უნდა იქნან დაცული. იმისათვის, რომ გავამარტივოთ რისკის ანალიზი, აუცილებელია, რომ განხილული იქნას დაცვის დარღვევების მცდელობები, რომლებიც მიეკუთვნებიან შმდეგ 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), 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.

2.5. კიბერსივრცის საინფორმაციო ტექნოლოგიების კომპონენტები

კიბერსივრცის შემადგენელ ელემენტებს მიეკუთვნებიან ქსელის მოწყობილობები, პერიფერიული (პრინტერები, სკანერები და ა.შ.) და ინტერფეისის მოწყობილობები, რომლებიც უმეტეს შემთხვევებში წარმოადგენენ ქსელის მოწყობილობებს.

კიბერსივრცის საინფორმაციო ტექნოლოგიების ნებისმიერი კომპონენტები შეიძლება განხილული იქნან, როგორც საფრთხის პოტენციალური ობიექტები, უსაფრთხოებისათვის რისკის შესაბამისი შეფასებით. საფრთხის ანალიზი მოიცავს შესაძლო შემოჭრების, პოტენციალური შემოტევების, ინფორმაციის დაცვის საშუალებების ქმედითუნარიანობის დარღვევის, წარმატებული შემოტევის შედეგად მიღებული ზარალის შესაბამისი ამოცანების აღწერას.

ინფორმაციის დაცვის სისტემის დარღვევა შეიძლება მიმდინარეობდეს უშუალოდ კიბერსივრციდან. ეს შეიძლება იყოს შემოჭრები დამაზიანებელი პროგრამების გამოყენებით, ინფრასტრუქტურის მნიშვნელოვანი ელემენტების დაცვის პროცესის დარღვევით, მაგალითად მონაცემთა გადაცემის საკაბელო სისტემებისათვის.

კიბერუსაფრთხოება დაკავშირებულია აგრეთვე რისკების მართვასთანაც, ცხადია, დაცვის სტრატეგიის განხორციელების საფუძველზე, რომელიც განსაზღვრავს უკუქმედების ზომებს, რომლებიც უნდა იქნას გათვალისწინებული დაცვის დარღვევის მცდელობის დროს. დაცვის სტრატეგია უნდა ითვალისწინებდეს:

– შემოტევის აღმოჩენას, მცდელობის დაწყების მომენტში;

- შემოტევის მცდელობაზე შესაბამისი ქმედების ფორმულირებას, რომელშიც განსაზღვრული იქნება შემოტევაზე უკუქმედების ღონისძიებათა ერთობლიობა, შემოტევის მოსაგერიებლად ან შემოტევის ეფექტურობის მნიშვნელობის შესამცირებლად;
- ქმედებების ფორმულირებას, რომელიც საჭიროა სატელეკომუნიკაციო ქსელის ქმედითუნარიანობის აღსადგენად, მისი არსებული მდგომარეობის გათვალისწინებით.

ITU – T X. 800 რეკომენდაციების შესაბამისად [45], მონაცემთა გადაცემის სისტემებისათვის საშიშროებათა (მუქარები) ჩამონათვალი მოიცავს ინფორმაციის ან სხვა რესურსების დარღვევას, დაზიანებას ან ინფორმაციის შეცვლას, მოპარვას, ინფორმაციის ან სხვა რესურსების დაკარგვას, ინფორმაციის გახსნას, მომსახურების სახეობების მიწოდების პროცესის წყვეტას.

ITU – T X. 800 –ის შესაბამისად საფრთხეები კლასიფიცირებულია, როგორც შემთხვევითი და როგორც განზრახული, ასევე კლასიფიცირებაში შედის აქტიური და პასიური საფრთხეები. შემთხვევითი საფრთხეები წარმოიქმნებიან წინასწარგანზრახვის გარეშე, მაგალითად არასასურველი (დაზიანებული) მოწყობილობის გამოყენების შემთხვევაში, ან საინფორმაციო ტექნოლოგიების ნებისმიერი კომპონენტის დისტანციური მართვის დროს არაკვალიფიციური ქმედება, სისტემის შეცდომით ამოქმედება, უხეში (სისტემური) შეცდომები პროგრამულ უზრუნველყოფაში.

წინასწარგანზრახული საფრთხე, განხორციელების შემთხვევაში აღიქმება, როგორც ინფორმაციის დაცვის მოშლა, ხოლო პასიური საფრთხე, კი არ იწვევს ინფორმაციის, რაიმე ცვლილებას, არც სისტემის მოქმედების რეჟიმის ან მდგომარეობის ცვლილებას. ამის მაგალითს წარმოადგენს, ინფორმაციაზე დაკვირვებისათვის მიყურადების მოწყობილობების გამოყენება.

სატელეკომუნიკაციო სისტემისათვის აქტიური საფრთხეები შეიცავენ ინფორმაციის შეცვლის, მოქმედების რეჟიმის ან მდგომარეობის შეცვლის შესაძლებლობებს. აქტიური საფრთხის მაგალითს წარმოადგენს ქსელის მოწყობილობების მარშრუტიზაციის ცხრილების წინასწარგანზრახული შეცვლა არასანქციონირებული მომხმარებლის მიერ.

ინფორმაციით მართული სისტემებისათვის, ზემოთჩამოთვლილი თავისებურებების გარდა, როგორიცაა გარემოში შეღწევადობა, რაც წარმოადგენს გარემოს დაუცველობას, აუცილებელია იმის გათვალისწინებაც, რომ ასეთ სისტემებში ინფორმაციული რესურსი უშუალოდ, ფიზიკურ დონეზე არის საფრთხისშემცველი, მაგალითად რადიოარხის შემთხვევაში. მართლაც, რადიოარხში აქტიური რადიოელექტრონული შემტევი ზემოქმედების არსებობა რეტრანსლიაციური ან სხვა ინტელექტუალური ტიპის რადიოხელშეშლების სახით, იწვევს ინფორმაციული რესურსის ნაწილობრივ შეცვლას ან დამახინჯებას.

ინფორმაციით მართული სისტემების მიზნობრივი დანიშნულების მიუხედავად, მისი ფუნქციონირება განისაზღვრება ინფორმაციული ინფრასტრუქტურით. მაგალითად, სანავიგაციო სისტემებში ინფორმაციულ ინფრასტრუქტურას წარმოადგენს სანავიგაციო ველი ან მომხმარებელთა ინტერფეისი. აქ შეტევის მიზნებს წარმოადგენს ინფორმაციული ინფრასტრუქტურის სრულფასოვნად ფუნქციონირების დარღვევა, ხოლო დაცვისათვის, კი ინფორმაციული ინფრასტრუქტურის სრულფასოვნების შენარჩუნება.

ინფორმაციით მართული სისტემების უსაფრთხოების პრობლემატიკის თავისებურება იმაში მდგომარეობს, რომ უსაფრთხოების საშიშროებებს აქ წარმოადგენს კიბერსაფრთხეები საინფორმაციო სისტემის შესასვლელზე, ხოლო დაცვა უნდა ითვალისწინებდეს სისტემის მთელ პერიმეტრზე (საზღვრებზე) კიბერდაცვას. ამასთანავე, შეტევითი ზემოქმედება (საფრთხისშემცველი) უნდა განვიხილოთ ინფორმაციით მართული

სისტემის შესასვლელზე , ანუ ფიზიკურ (სიგნალის) დონეზე. ამ თვალსაზრისით დაცვის ცალკეული ღონისძიებები შიფრირების, კოდირების, და სხვა სახით, გვესახება არამაღალეფექტურად. აქ დაცვის პრობლემის გადაწყვეტის ქვაკუთხედი, OSI (Open Systems Interconnection) - ის მოდელის უმაღლესი დონეებიდან, ინაცვლებს ფიზიკურ დონეზე.

აქედან გამომდინარე შესაბამის ძირითად დასკვნას წარმოადგენს: ის, რომ კიბერუსაფრთხოების უმნიშვნელოვანესი ამოცანების ფექტურად გადაწყვეტა შესაძლებელია OSI მოდელის მხოლოდ ფიზიკურ დონეზე, რაც უზრუნველყოფს ინფოსაკომუნიკაციო სისტემის მთელ პერიმეტრზე (საზღვრებზე) ინფორმაციის უსაფრთხოების უზრუნველყოფას.

დასკვნა

1. საჭიროა ორგანიზაციული და ტექნიკური ღონისძიებების გატარება, მომხმარებელთა აუტენთიფიკაცია და ავტორიზაცია დადგენილი მოთხოვნების დონეზე, სატელეკომუნიკაციო არხებში შიფრაციის გატვალისწინება, პერსონალურ მონაცემებთან ხელმისაწვდომობის შეფასება და მონაცემთა გადაცემის სისრულის დაცვა.
2. აუცილებელია ინფორმაციის უსაფრთხოების უზრუნველყოფის ნაციონალური ცენტრის არსებობა, რომელიც შეისწავლის ყველა არსებულ პრობლემას და შეიმუშავებს მათთან გამკლავების ღონისძიებებს.
3. ორგანიზაციებსა და კომპანიებში სამეტყველო ინფორმაციის დაცვა ტექნიკური არხებით მათი გაჟონვისაგან, უნდა პასუხობდეს თანამედროვე მოთხოვნებს დაზვერვის არსებული ტექნიკური საშუალებების შესაძლებლობებიდან გამომდინარე. საჭიროა შესწავლილ იქნას ბოროტმზრახველის შესაძლო ქმედებები დაკავშირებული სამეტყველო ინფორმაციის მიტაცების

შესაძლებლობებთან, რაც საშუალებას მოგვცემს ავამაღლოთ ასეთი სახის საშიშროებებისაგან დაცვის ღონისძიებების ეფექტურობა.

4. ინფორმაციული უსაფრთხოებისათვის ახალი ხიფათები დაკავშირებულია საინფორმაციო ტექნოლოგიების მასიურ გამოყენებასთან, იმ ელემენტების მრავალრიცხოვნობასთან, რომლებისაგანაც შედგება საინფორმაციო სივრცე, მათ შორის ურთიერთკავშირების მრავალფეროვნებასა და ურთიერთქმედებების დიდ რაოდენობასთან, რაც ართულებს მაშინ ინფორმაციული უსაფრთხოების უზრუნველყოფის პროცესებზე კონტროლს.
5. ინფოსაკომუნიკაციო სისტემების უსაფრთხოდ ფუნქციონირების უზრუნველყოფის სირთულე, პროექტირების ზოგად პრობლემატიკასთან შეფარდებით, დაკავშირებულია იმ გარემოებასთან, რომ საინფორმაციო ტექნოლოგიების ძირითად მაჩვენებელს წარმოადგენს მისი ფუნქციონირების ეფექტურობა და არა მისი დაცულობის დონე, რაც იწვევს სისტემური პროექტირების ფუნდამენტურ პრობლემაზე მოთხოვნას, რომ გათვალისწინებული იქნას სისტემის ეფექტურობის გაზომვადი მეჩვენებელი.
6. ინფორმაციის უსაფრთხოება უნდა განიხილებოდეს როგორც ახალი მეთოდების, საინფორმაციო სისტემებისა და მომსახურების სახეობების დაცვის ეფექტური საშუალებების ფორმირების პროცესი და მეთოდები.
7. კიბერუსაფრთხოების უმნიშვნელოვანესი ამოცანების ფექტურად გადაწყვეტა შესაძლებელია OSI (Open Systems Interconnection) მოდელის მხოლოდ ფიზიკურ დონეზე, რაც უზრუნველყოფს ინფოსაკომუნიკაციო სისტემის მთელ პერიმეტრზე (საზღვრებზე) ინფორმაციის უსაფრთხოების უზრუნველყოფას.

თავი 3. ინფორმაციის დაცვის საშუალებების განსაზღვრა

როგორც დისერტაციის შესავალ ნაწილში აღვნიშნეთ, 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.

ინფორმაციის დაცვის საშუალებების შერჩევა წარმოადგენს რთულ ამოცანას, რადგანაც ინფორმაციის დაცვის უკვე არსებულ სისტემაზე ნებისმიერი დამატება, ზემოქმედებს სისტემის ქმედითუნარიანობასა და მომსახურების სახეობების წვდომაზე.

როდესაც ის ტექნიკური მოთხოვნები, რომლებიც დაცული უნდა იყოს, გახდება ნათელი, ამის შემდგომ დღის წესრიგში დგება ინფორმაციის დაცვის ურთიერთთავსებადი ტექნიკური საშუალებების შერჩევის ამოცანა. ამისათვის მიზანშეწონილია მოსალოდნელი საფრთხეების მოდელის შედგენა, მაგალითად:

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

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.

ცხადია, 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 ალბათობა.

3.1. ინფორმაციაზე შეტევებისაგან დაცულობის შეფასება

ნებისმიერი სახის შემოტევის რისკის შესწავლისათვის ზოგადი მიდგომები 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.

ამასთანავე, განსაკუთრებულად არის ხაზგასმული ინფორმაციის უსაფრთხოების გარანტირებული, აუცილებელი ან დასაშვები დონეები სატელეკომუნიკაციო ქსელების მომხმარებლების კლასებისათვის, მითუმეტეს, როდესაც სისტემაში ინტეგრირებულია ინფორმაციის დაცვის განსხვავებული საშუალებები და პროტოკოლები. აქვე გასათვალისწინებელია, რომ დღეისათვის არ არის შესადარებელი ბაზა, მაგალითად მარეგულირებელი ორგანოს მოთხოვნებთან, ან უსაფრთხოების რეგლამენტირებულ პოლიტიკასთან.

ცხრილი 4. კრიპტოგრაფიული დაცვის მოთხოვნები და მათი ცვლილების ხასიათი

№	მოთხოვნები	კონფიდენციალური ინფორმაციის კრიპტოგრაფიული დაცვის კლასები					
		I	II	III	IV	V	VI
1.	ინფორმაციის კრიპტოგრაფიული დაცვის ვადები	*	+	=	+	=	+
2.	ინფორმაციის კრიპტოგრაფიული დაცვის სისტემის უსაფრთხოდ ექსპლუატაციის ვადები	*	=	=	+	=	+
3.	ინფორმაციის კრიპტოგრაფიული დაცვის სისტემის საინჟინრო–კრიპტოგრაფიული დაცვა	*	=	=	+	=	=
4.	ინფორმაციის კრიპტოგრაფიული დაცვის სისტემისა და ელექტრონულ მოწყობილობებში თანმხლები ელექტრომაგნიტური გამოსხივებისა და ზედდებების სახაზო სიგნალების ინფორმაციულობა	–	=	=	*	+	+
5.	ინფორმაციის კრიპტოგრაფიული დაცვის სისტემის მიზნობრივი ფუნქციის შემოწმება	*	=	=	+	=	+
6.	ინფორმაციის კრიპტოგრაფიული დაცვის სისტემისა და მისი ქვესისტემისადმი წაყენებული მოთხოვნების პროგრამული კომპონენტების ანალიზი	*	+	=	=	+	+
7.	ინფორმაციის კრიპტოგრაფიული დაცვის სისტემისა და მისი ქვესისტემისადმი წაყენებული მოთხოვნების შესაბამისი აპარატურული კომპონენტების ანალიზი	*	=	+	+	=	+
8.	ინფორმაციის კრიპტოგრაფიული დაცვის სისტემის მომხმარებელთა აუტენტიფიკაცია	*	=	=	+	=	+
9.	ინფორმაციის კრიპტოგრაფიული დაცვის სისტემისა და მისი ქვესისტემისადმი წაყენებული მოთხოვნების სრულყოფილება	*	=	=	+	=	+
10.	მომსახურებაზე მიღწევადობის (წვდომის) მართვა	–	–	*	=	+	=
11.	მოვლენათა რეგისტრირება	–	–	*	+	=	+
12.	დამატებითი მოთხოვნები	*	+	+	+	+	=

აღნიშვნები:

- მოთხოვნები არ არის წაყენებული;

* მოთხოვნები წაყენებულია;

= წაყენებულია წინა საფეხურზე არსებული კლასის შესაბამისი მოთხოვნები;

+ წინა საფეხურზე არსებული მოთხოვნები გამკაცრებულია.

ამრიგად, საკითხის სიმწვავე, პირველ რიგში დაკავშირებულია ინფორმაციის უსაფრთხოების დასაშვები დონის შეფასებისათვის მეთოდური მასალის უქონლობასთან. როგორც ამის მაგალითი, შეიძლება განვიხილოთ ინფორმაციის დაცვის ზოგიერთი კლასიფიკატორები, იმ მიზნით, რომ ჩვენს მიერ შემოთავაზებულ ლოგიკურ–ალბათურ ფუნქციებს მივანიჭოთ გამოყენებითი მნიშვნელობა.

კონფიდენციალური ინფორმაციის დაცვის კრიპტოგრაფიული სისტემა განსხვავებულებია კრიპტოგრაფიული დაცვით უზრუნველყოფის დონეებით. განასხვავებენ კონფიდენციალური ინფორმაციის კრიპტოგრაფიული დაცვის ექვს დონეს, სადაც დონეების შესაბამისად იზრდება მოთხოვნების რაოდენობა და სიმკაცრე. ცხრილი 4–ში მოცემულია მოთხოვნათა ის ერთობლიობა, რომლებიც განსაზღვრავენ კრიპტოგრაფიული დაცვის ექვსივე დონის მოთხოვნებს და ამ მოთხოვნების ცვლილების ხასიათს.

ცხრილი 5–ში წარმოდგენილია ინფორმაციის უსაფრთხოების უზრუნველყოფაზე მოთხოვნათა ერთობლიობა განსაკუთრებული (კრიტიკული) მოთხოვნების შესაბამისი ობიექტებისათვის.

ცხრილი 5. განსაკუთრებული მოთხოვნების ობიექტისათვის ინფორმაციის უსაფრთხოების უზრუნველყოფის მაჩვენებლები

№	განსაკუთრებული მოთხოვნების შესაბამისი ობიექტების, სატელეკომუნიკაციო სისტემებსა და ქსელებში ინფორმაციის დაცულობაზე მოთხოვნების მაჩვენებლები	სატელეკომუნიკაციო ქსელის მნიშვნელობათა კატეგორიები		
		I (უმაღლესი)	**II (საშუალო)**	**III (დაბალი)**
1.	ინფორმაციის დაცულობის მართვა	+	+	+
2.	მიღწევადობის (წვდომის) განცალკევება და მისი მართვის შესაძლებლობები	+	+	+
3.	პროგრამული უზრუნველყოფის დაცვა საფრთხის შემცველი პროგრამებისა და სპამებისაგან	+	+	+
4.	სამუშაო ადგილებიდან და კავშირგაბმულობის არხებიდან ინფორმაციის გაჟონვისაგან დაცვა	+		
5.	შემოტევებისა და არასანქციონირებული ჩართვებისაგან სატელეკომუნიკაციო სისტემებისა და ქსელების დაცვა	+	+	
6.	ინფორმაციის დაცვისადმი არსებული მოვლენების პროტოკოლირება	+	+	
7.	ინფორმაციის კრიპტოგრაფიული დაცვა	+	+	
8.	სატელეკომუნიკაციო ქსელებისა და სისტემების რესურსების ფიზიკური უსაფრთხოება	+	+	+
9.	სატელეკომუნიკაციო ქსელებისა და სისტემების დაცულობის ანალიზი	+	+	
10.	სატელეკომუნიკაციო ქსელებსა და სისტემებში ინფორმაციის დაცულობის დარღვევის შემთხვევებზე ელექტრონული რეაგირების არსებობა	+		
11.	ინფორმაციის სარეზერვო ასლების შექმნა (კოპირება)	+	+	+
12.	კვების წყაროების რეზერვირება	+	+	+
13.	სატელეკომუნიკაციო ქსელებისა და სისტემების კრიტიკული ელემენტების რეზერვირება	+		
14.	წარმატების ალბათობა	+	+	+

განსაკუთრებული (კრიტიკული) მოთხოვნების შესაბამისი ობიექტებისათვის სატელეკომუნიკაციო ქსელებსა და სისტემებს უნდა გააჩნდეთ მზადყოფნის კოეფიციენტები კრიტიკულობის კოეფიციენტების შესაბამისად, რომელიც წარმოდგენილია ცხრილი 6–ში, სადაც მზადყოფნის კოეფიციენტების მნიშვნელობები განსაზღვრულია მათი მდგრადობის (სიცოცხლისუნარიანობის) შესაბამისად (იხილეთ თავი 3.4. გვ 88).

ცხრილი 6. სატელეკომუნიკაციო სისტემებისა და ქსელების მზადყოფნის კოეფიციენტები კატეგორიების შესაბამისად

ზემოქმედება	სატელეკომუნიკაციო სისტემებისა და ქსელის დაზიანების ხარისხი პოტენციალურად შესაძლო ზემოქმედებისგან	სატელეკომუნიკაციო სისტემებისა და ქსელების მზადყოფნის კოეფიციენტი		
		კრიტიკულობის კოეფიციენტი		
		I კატეგორია	**II კატეგორია**	**III კატეგორია**
არ არსებობს	0	0,999	0,99	0,9
დაბალი	შეფერხდა ყველა ელემენტების 15% რაოდენობის მოქმედება	0,95	0,95	0,95
საშუალო	შეფერხდა ყველა ელემენტების (16–49)% რაოდენობის მოქმედება	0,9	0,85	0,8
მნიშვნელოვანი	შეფერხდა ყველა ელემენტებიდან 50%–ზე მეტის მოქმედება	0,8	0,75	0,7
მოწყობილობების რაოდენობის აღდგენის პროცენტი		6 საათში–75%, 24საათში-სრულად	6 საათში–10%, 24საათში-30%	24 საათში - 15%

წარმოდგენილი ცხრილები საშუალებას იძლევა ვიმსჯელოთ ობიექტზე არსებული ინფორმაციის უსაფრთხოების უზრუნველყოფის

უნარიანობაზე, ლოგიკურ–ალბათური ფუნქციების გამოყენების საფუძველზე. უნდა აღინიშნოს, რომ აქ არ არის გამოკვლეული სხვადასხვა მადესტაბილიზირებელი ფაქტორების ურთიერთზემოქმედება. ცხრილებში მოცემულია ერთმანეთთან დაკავშირებული მოთხოვნები, რაც განსაკუთრებულ მნიშვნელობას ანიჭებს ექსპერტის ცოდნასა და გამოცდილებას, რას ასეთი მიდგომის ნაკლოვანებაზე მიუთითებს.

აქედან გამომდინარე, უნდა დავასკვნათ, რომ აუცილებელია ახალი, ფუნდამენტალური შედეგი, როგორც ინფორმაციაზე შემოტევებისაგან დაცვის პრობლემების მეცნიერულად ფორმულირებისათვის, ასევე მადესტაბილიზირებელი ინფორმაციის ზემოქმედებების აცილების მეთოდებისა და საშუალებების ანალიზისა და სინთეზისათვის, იმის გათვალისწინებით, რომ შემოტევების მეთოდები და მექანიზმები აგრეთვე, განიცდიან სრულყოფას. ბოროტმზრახველები გამოძებნიან დღეისათვის აღმოუჩენელ მადესტაბილიზირებელ ფაქტორებს. შესაბამისად, უნდა გავითვალისწინოთ, რომ დაცვის ფუნქციებიც მოძველების გამო, ვერ გაითვალისწინებენ ახალი მადესტაბილიზირებელი ფაქტორების შესაძლებლობებს. ამიტომ ინფორმაციული ზემოქმედებების აცილების მეთოდებისა და საშუალებების სრულყოფის პროცესიც უწყვეტად გვესახება.

3.2 ინფორმაციის დაცვის საშუალებების შერჩევა

რა კრიტერიუმებით განვსაზღვროთ ინფორმაციის დაცვის საშუალებები.

ამისათვის დავაჯგუფეთ ინფორმაციის დაცვის აპარატურულ–პროგრამული საშუალებები და ჩამოვთვალეთ მათი შესაძლებლობები, რათა კონკრეტული ობიექტისათვის შესაძლებელი გახდეს ინფორმაციის დაცვის საშუალებების შერჩევა.

ინფორმაციის დაცვის საშუალებების ჯგუფები, მათი დანიშნულების შესაბამისად, შემდეგნაირად ჩამოვაყალიბეთ:

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.

3.3. ინფორმაციის დაცვის საშუალებების ნაკრების ოპტიმალურობის კრიტერიუმი

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 ϵ 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

$$X_i \cong X_{i\text{მოთხოვნილი}}$$

სადაც $X_{i\text{მოთხოვნილი}}$ - არის i-ური დაცვის საშუალებისადმი წაყენებული მოთხოვნების შესაბამისად შერჩეული დაცვის ფუნქციების

რაოდენობა, მაშინ ჩვენი ამოცანის მიზნობრივ ფუნქციას ექნება შემდეგი სახე:

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

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, ჩავატაროთ ინფორმაციის დაცვის საშუალებების დანიშნულების ფუნქციების მიმოხილვა. ფუნქციების ჩამონათვალი გვაძლევს საშუალებას აღმოვაჩინოთ ურთიერთგადაფარვები და მათი სიღრმე.

3.3.1. ინფორმაციის დაცვის საინჟინრო (მექანიკური) საშუალებები

ინფორმაციის დაცვის საინჟინრო (მექანიკური) საშუალებების დანიშნულებაა ინფორმაციის ობიექტამდე მიღწევისათვის ბოროტმზრახველისათვის მექანიკურად ხელშეშლა. ინფორმაციის დაცვის

საინჟინრო (მექანიკური) დაცვის საშუალება წარმოადგენს საინჟინრო კონსტრუქციას, რომელიც ბოროტმზრახველს უქმნის მექანიკურ ბარიერს. მიუხედავად დაცვის ელექტრონული საშუალებების განვითარებისა, საინჟინრო კონსტრუქციები გამოირჩევიან მნიშვნელოვანი ეფექტურობით, განსაკუთრებით აღსანიშნავია მათი მნიშვნელობა ნივთების (IoT – Internet of Things) ინტერნეტის განვითარებისათვის.

დაცული უნდა იქნას ყველა ის წესი, რომელიც უზრუნველყოფს სატელეკომუნიკაციო ქსელისა და სისტემების ფიზიკურ უსაფრთხოებას: საკაბელო კომუნიკაციის დაცვა ფიზიკური ზემოქმედებებისაგან, რისთვისაც გამოყენებული უნდა იქნას საკომუნიკაციო შახტები, საკომუნიკაციო მოწყობილობებზე დაუშვებელია მარტივი ფიზიკური წვდომა. გათვალისწინებული უნდა იქნას დაცვა ელექტრომაგნიტური ველის ზემოქმედებისაგან, საკაბელო კომუნიკაციადაცული უნდა იქნას ფოლადის მილებით ან სპეციალური კაბელების გამოყენებით. აუცილებელია სატელეკომუნიკაციო სისტემების დაცვა გარემოს ზემოქმედებისაგან, აუცილებელია შესაბამისი კლიმატური პირობების უზრუნველყოფა.

დაწესებულებებისა და კომპანიების კორპორატიული ქსელები მუდმივ რეჟიმში უნდა ექვემდებარებოდეს მონიტორინგს, რაც საშუალებას მოგვცემს ვიმოქმედოთ დროულად და ეფექტურად.

3.3.2. ინფორმაციის დაცვის ვიბროაკუსტიკური სისტემები

ინფორმაციის დაცვის ვიბროაკუსტიკურ სისტემებს იყენებენ, იმ შენობების დასაცავად, რომლებიც განკუთვნილია კონფიდენციალური ღონისძიებების ჩასატარებლად. ის იცავს შენობას სარკმლის მინებიდან, კედლებიდან, კარებებიდან, ვენტილაციის სისტემებიდან და გათბობის მილებიდან ინფორმაციის მოხსნისაგან (აღებისაგან).

ვიბროაკუსტიკური დაცვის სისტემა იცავს შენობას, ტრადიციული მიკროფონებით, ხმისჩამწერი აპარატურით, რადიომიკროფონებით, ელექტრონული სტეტოსკოპებით, სარკმლის მინებიდან აკუსტიკური ინფორმაციის ლაზერული მოხსნისაგან.

შენობის ვიბროაკუსტიკური დაცვისათვის გამოყენებულია თეთრი ხმაურის გენერატორები და ვიბრაციული გახმაურების სისტემები, რომლებიც დაკომპლექტებულია ელექტრომაგნიტური და პიეზოელექტრული ვიბროგარდამსახებით.

მასკირებისათვის განკუთვნილი ზემოქმედების წყაროები სრულად უნდა ფარავდნენ სამეტყველო სიგნალის სიხშირული სპექტრის (200-5000ჰერცი) სიხშირულ დიაპაზონს.

ხმაურის აკუსტიკური გენერატორი უზრუნველყოფს დაცვას, მიყურადების ნებისმიერი სისტემისგან.

- ვიბროაკუსტიკური დაცვის სისტემა “Камертон - 3”;
- ვიბროაკუსტიკური და აკუსტიკური ხელშეშლების განხორციელების სისტემა ЛГШ – 304;
- ტექნიკური არხებიდან სამეტყველო ინფორმაციის გაჟონვისაგან დაცვის სისტემა Соната – АВ, Модель 4Б;
- ინფორმაციის დაცვის აკუსტიკური და ვიბრაციული დაცვის სისტემა “Шорох-5Л”;
- აკუსტიკური და ვიბროაკუსტიკური ხელშეშლების სისტემა “Буран”;
- აკუსტიკური და ვიბროაკუსტიკური ხელშეშლების სისტემა “Кедр”;
- სამეტყველო აკუსტიკური ინფორმაციის აქტიური დაცვის სისტემა SEL -157 “Шагрень”;
- ხმაურის შექმნის სისტემა “Шорох-3”;
- სიგნალების ციფრული გენერატორი “ЛГШ - 402”;
- ვიბროგენერატორი “ЛГШ - 404”;
- ვიბროაკუსტიკური კომპლექტი “ВВ 301”;
- ვიბროაკუსტიკური ხმაურის გენერატორი “ГНШ -3С ”;

- ვიბროაკუსტიკური ხმაურის გენერატორი ANG – 2000;
- ვიბროაკუსტიკური ხმაურის გენერატორი VNG - 006DM;
- ვიბროგენერატორი “БАРОН”;
- ვიბროაკუსტიკური დაცვის სისტემა “Равнина - 3”.

3.3.3. ინფორმაციის დაცვა გაჟონვისაგან, ელექტრონულ მოწყობილობებში თანმხლები ელექტრომაგნიტური გამოსხივებისა და ზედდებების გამო

ელექტრონული საშუალებების (კომპიუტერების) ფუნქციონირებისას წარმოიშვება ინფორმაციის შემცველი ელექტრომაგნიტური გამოსხივება, ხოლო ახლომახლო არსებულ ნებისმიერი დანიშნულების სადენებში ინფორმაციის შემცველი ზედდებები. ამიტომ ინფორმაციის შესაძლო გაჟონვის ტექნიკური არხები იყოფა ელექტრომაგნიტურ და ელექტრულ არხებად:

- ელექტრომაგნიტური გამოსხივების ველი;
- თანმხლები ელექტრომაგნიტური გამოსხივების ველი წარმოიქმნება: ინფორმაციის მატარებელ წრედებში ვიდეოიმპულსებისა და საინფორმაციო საშუალებების ნებისმიერ ელექტრულ წრედებში რადიოიმპულსების მეშვეობით;
- საინფორმაციო საშუალებების ფუნქციონირების ობიექტიდან გამავალ სადენებში ელექტრომაგნიტური ზედდებით, ინფორმაციის გაჟონვა;
- ზედდება ელექტრონული საშუალებების ელექტროკვებისა და დამიწების წრედებზე.

თანმხლები ელექტრომაგნიტური გამოსხივება წარმოიქმნება ინფორმაციის დამუშავების შემდეგ პროცესებში:

- ინფორმაციის მონიტორის ეკრანზე გამოტანის დროს;
- კლავიატურიდან მონაცემების შეტანის დროს;
- ინფორმაციის ჩაწერა-წაკითხვის დროს მეხსიერებაში;

- მონაცემების კავშირგაბმულობის არხებით გადაცემის დროს;
- მონაცემების გამოტანა პერიფერიულ მოწყობილობებში (პრინტერზე და სხვა);
- სკანერიდან მონაცემების გადაწერისას მეხსიერებაში.

თანმხლები ელექტრომაგნიტური გამოსხივების მიტაცება შესაძლებელია ჩვეულებრივი რადიო და რადიოტექნიკური დაზვერვის საშუალებებით და მითუმეტეს დაზვერვის სპეციალური საშუალებებით.

აღნიშნულიდან გამომდინარე, გამოთვლითი ტექნიკის მიმართ წაყენებულ ინფორმაციის დაცულობის მოთხოვნებში მითითებულია, რომ სერტიფიცირებული საშუალებები გადიან სპეციალურ შემოწმებას, რათა ხელოვნურად უზრუნველყოფილი ხმაურის ფონის გარეშეც, სერტიფიკატში აღნიშნულ საკონტროლო რადიუსში ინფორმაციის დამუშავების პროცესი იქნას დაცული. საკონტროლო–გამზომი ხელსაწყოებით შეიძლება გამოკვლეულ იქნას ინფორმაციის დაცულობის უზრუნველყოფა მოთხონების შესაბამისად.

3.3.4. ინფორმაციის დაცვა არასანქციონირებული მიერთებებისაგან

არასანქციონირებული მიერთებებისაგან დაცვის საშუალებები შეიძლება იყოს პროგრამული, ტექნიკური ან პროგრამულ - ტექნიკური, რომელთა დანიშნულებაა ინფორმაციაზე, არასანქციონირებული წვდომის აღკვეთა ან მნიშვნელოვნად გართულება.

არასანქციონირებული მიერთებებისაგან დაცვის საშუალებები ასრულებენ შემდეგ ფუნქციებს:

- ქსელის მომხმარებელთა და მოწყობილობათა იდენტიფიკაციასა და აუტენტიფიკაციას;
- პროგრამებისა და პროცესების ამოქმედების/დასრულების რეგისტრაციას;

- მიერთების/წვდომის გამიჯვნის წესების, ტიპების და მეთოდების განხორციელებას;
- მოწყობილობებს შორის ინფორმაციის ნაკადების მართვას;
- ინფორმაციის მატარებლების აღრიცხვასა და სხვა ფუნქციებს.

ინფორმაციის დაცვის საშუალება " Secret Net " წყვეტს შემდეგი ტიპის ამოცანებს:

ინფორმაციის დაცვა მოქმედ სადგურებში და სერვერებში მოთხოვნების შესაბამისად;

- დასაცავი ინფორმაციის გაჟონვის შესაძლებლობების კონტროლი.

ძირითადი შესაძლებლობებია:

- მიერთებების გამიჯვნა;
- გაჟონვათა კონტროლი;
- ვირტუალური სამუშაო მაგიდების (VDI) ინფრასტრუქტურის დაცვა;
- ცენტრალიზებული მართვა;
- ანგარიშგების სისტემა;
- მასშტაბირების მაღალუნარიანობა.

ინფორმაციის დაცვის საშუალება Dallas Lock 8.0-K უზრუნველყოფს:

- ინფორმაციის დაცვას არასანქციონირებული მიერთებებისაგან;
- ვირტუალური სივრცეების არსებობის გათვალისწინებას;

საინფორმაციო რესურსებთან მიერთებების გამიჯვნისა და სხვა მოწყობილობებთან, მიერთების მატრიცის შესაბამისად, დისკრეციული პრინციპის გამოყენებას;

- მომხმარებელთა ქმედებების აუდიტის;
- სისტემის ფაილების, პროგრამულ–აპარატურული გარემოსა და რეესტრის მთლიანობის / სისრულის კონტროლს;
- დასაცავი პერსონალური კომპიუტერების გაერთიანებას, დაცვის მექანიზმებით, ცენტრალიზებული მართვის გამოყენების მიზნით.

ინფორმაციის დაცვის საშუალება Secret Net Card – წარმოადგენს დამოუკიდებელ პლატას კომპიუტერის შესაძლებლობების გასაფართოვებლად, რომელიც ჩაისმება PCI და PCI-E სტანდარტის შინაში და განახორციელებს მომხმარებელთა იდენტიფიცირებასა და აუტენტიფიცირებას iButton ელექტრონული იდენტიფიკატორების საშუალებით და კრძალავს სხვა მისაერთებელი მატარებლებიდან ოპერაციული სისტემის არასანქციონირებულ ჩატვირთვას.

პროდუქტს გააჩნია შემდეგი შესაძლებლობები:

- მომხმარებელთა იდენტიფიცირება და აუთენტიფიცირება;
- ინფორმაციის გარემატარებლებიდან ჩატვირთვისაგან დაცვის მექანიზმები;
- მოთვალთვალე ტაიმერის ამოქმედების მომენტის ავტომატური განმსაზღვრელი;
- იყენებს/ხელს უწყობს კომპიუტერული სისტემის დეფაქტო პროგრამის Basic Input Output System –BIOS არსებობას.

3.3.5. ინფორმაციის დაცვის საქსელთაშორისო ეკრანები

საქსელთაშორისო ეკრანი (ხშირად ხმარებაშია გამოთქმა „ბრანდმაუერი“ ან ინგლისური firewall - ფაირვოლი) არის დაცვის საშუალება, რომელსაც ვიყენებთ საერთო სარგებლობის ქსელსა (მაგალითად ინტერნეტი) და შიდა (კორპორატიულ) ქსელს შორის, რომელიც ზღუდავს საერთო სარგებლობის ქსელიდან შიდა ქსელში შეღწევას ფილტრების და აუტენტიფიკაციის საშუალებების გამოყენებით, რათა გამოირიცხოს არასანქცირებული შეღწევა და შიდასაქსელო ინფრასტრუქტურის ნორმალური ქმედითუნარიანობის დარღვევა. მეორეს მხრივ, საქსელთაშორისო ეკრანი არეგულირებს შიდა ქსელის მომხმარებლების მიერთებას (შეღწევას) საერთო სარგებლობის ქსელის რესურსებთან, როდესაც უსაფრთხოების თვალსაზრისით (ან სხვა

მიზეზებით) უნდა იქნან იზოლირებულები. საქსელთაშორისო ეკრანებს იყენებენ უშუალოდ კორპორატიულ ქსელშიც, როდესაც შეზღუდულია განსაკუთრებული მნიშვნელობის ინფორმაციაზე წვდომა. არსებობს, აგრეთვე პერსონალური საქსელთაშორისო ეკრანები ცალკეული კომპიუტერებისათვის, რომლებიც არეგულირებენ მათზე წვდომას.

საქსელთაშორისო ეკრანები, რომლებსაც იყენებენ TCP/IP ქსელებისათვის, ღია სისტემების ურთიერთქმედების ეტალონური მოდელის OSI (Open Systems Interconection) - ის შესაბამისად, იყოფიან შემდეგ ტიპებად (პირობითი კლასიფიცირება):

1. მართვადი კომუტატორები (საარხო დონე);
2. პაკეტური ან საქსელო ფილტრები (ქსელის დონე);
3. სეანსის დონის რაბი (გადასასვლელი) – circuit-level proxy;
4. გამოყენებითი დონის შუამავლები;
5. მდგომარეობის ინსპექტორები (stateful inspection), რომელიც წარმოადგენს გაფართოებული შესაძლებლობების მქონე სეანსის დონის საქსელთაშორისო ეკრანს.

3.3.6. ინფორმაციის დაცვის ანტივირუსული საშუალებები

ანტივირუსული დაცვა (ანტივირუსი), არის პროგრამა კომპიუტერული ვირუსებისა და საერთოდ არასასურველი პროგრამების აღმოსაჩენად, არასასურველი პროგრამებით დაზიანებული ფაილების აღსადგენად და, ფაილების მოდიფიცირების თავიდან ასაცილებლად.

ანტივირუსული პროგრამების კლასიფიცირება:

1. Dr.Web

ფუნქციები:

- დაცვა ვირუსებისაგან, რუტკიტებისაგან, ტროას პროგრამებისაგან, საჯაშუშო და სარეკლამო პროგრამული უზრუნველყოფა, ჰაკერული საქმიანობის აღმოჩენა;

- შემომავალი და გამავალი ტრაფიკების შემოწმება;
- ინტერნეტ-რეკლამისაგან დაცვა;
- „სპამ“ -გზავნილების ფილტრაცია;
- შემომავალი და გამავალი http – ტრაფიკის შემოწმება;
- არასასურველი კონტენტისაგან დაცვა;
- არასანქცირებული შეერთებების ბლოკირება;
- ინფორმაციის შიფრირება;
- შიფრირების ცნობილი ალგორითმების გამოყენების შესაძლებლობების უზრუნველყოფა;
- არასაჭირო ფაილებისა და მონაცემების მოცილება.

2. Symantec

ფუნქციები:

- დაცვა ვირუსებისაგან, რუტკიტებისაგან, ტროას პროგრამებისაგან, საჯაშუშო და სარეკლამო პროგრამული უზრუნველყოფა, ჰაკერული საქმიანობის აღმოჩენა;
- შემომავალი და გამავალი ტრაფიკების შემოწმება;
- „სპამ“ -გზავნილების ფილტრაცია;
- შემომავალი და გამავალი http – ტრაფიკის შემოწმება;
- არასასურველი კონტენტისაგან დაცვა;
- არასანქცირებული შეერთებების ბლოკირება;
- ინფორმაციის შიფრირება;
- შიფრირების ცნობილი ალგორითმების გამოყენების შესაძლებლობების უზრუნველყოფა;
- არასაჭირო ფაილებისა და მონაცემების მოცილება;
- ინფორმაციის სარეზერვო სათადარიგო კოპირება და აღდგენა;
- ბრანდმაუერი (საქსელთაშორისო ეკრანი);
- კომპიუტერის მუშაობის ოპტიმიზირება.

3. Bit Defender SRL

ფუნქციები:

- დაცვა ვირუსებისაგან, რუტკიტებისაგან, ტროას პროგრამებისაგან, საჯაშუშო და სარეკლამო პროგრამული უზრუნველყოფა, ჰაკერული საქმიანობის აღმოჩენა;
- შემომავალი და გამავალი ტრაფიკების შემოწმება;
- „სპამ“- გზავნილების ფილტრაცია;
- შემომავალი და გამავალი http – ტრაფიკის შემოწმება;
- არასასურველი კონტენტისაგან დაცვა;
- არასანქცირებული შეერთებების ბლოკირება;
- ინფორმაციის შიფრირება;
- შიფრირების ცნობილი ალგორითმების გამოყენების შესაძლებლობების უზრუნველყოფა;
- არასაჭირო ფაილებისა და მონაცემების მოცილება;
- ინფორმაციის სარეზერვო სათადარიგო კოპირება და აღდგენა;
- ბრანდმაუერი (საქსელთაშორისო ეკრანი);
- კომპიუტერის მუშაობის ოპტიმიზირება.

4. „ კასპერსკის ლაბორატორია“ (Kaspersky)

ფუნქციები:

- დაცვა ვირუსებისაგან, რუტკიტებისაგან, ტროას პროგრამებისაგან, საჯაშუშო და სარეკლამო პროგრამული უზრუნველყოფა, ჰაკერული საქმიანობის აღმოჩენა;
- შემომავალი და გამავალი ტრაფიკების შემოწმება;
- შემომავალი და გამავალი http – ტრაფიკის შემოწმება;
- არასასურველი კონტენტისაგან დაცვა;
- არასანქცირებული შეერთებების ბლოკირება;
- ინფორმაციის შიფრირება;
- თანამშრომელთა მხრიდან ინტერნეტზე და მომსახურების სახეობებზე წვდომის შეზღუდვა;
- არასაჭირო ფაილებისა და მონაცემების მოცილება;
- ინფორმაციის სარეზერვო სათადარიგო კოპირება და აღდგენა;

- ბრაუზერებისა და მომსახურებათა სახეობების (დანართების) გამოყენება.

5. Outpost (Agnitum)

ფუნქციები:

- დაცვა ვირუსებისაგან, რუტკიტებისაგან, ტროას პროგრამებისაგან, საჯაშუშო და სარეკლამო პროგრამული უზრუნველყოფა, ჰაკერული საქმიანობის აღმოჩენა;
- შემომავალი და გამავალი ტრაფიკების შემოწმება;
- შემომავალი და გამავალი http – ტრაფიკის შემოწმება;
- არასანქცირებული შეერთებების ბლოკირება;

6. Panda Security

ფუნქციები:

- დაცვა ვირუსებისაგან, რუტკიტებისაგან, ტროას პროგრამებისაგან, საჯაშუშო და სარეკლამო პროგრამული უზრუნველყოფა, ჰაკერული საქმიანობის აღმოჩენა;
- შემომავალი და გამავალი ტრაფიკების შემოწმება;
- „სპამ“- გზავნილების ფილტრაცია;
- შემომავალი და გამავალი http – ტრაფიკის შემოწმება;
- არასასურველი კონტენტისაგან დაცვა;
- არასანქცირებული შეერთებების ბლოკირება;
- ინფორმაციის შიფრირება;
- არასაჭირო ფაილებისა და მონაცემების მოცილება;
- თანამშრომელთა მხრიდან ინტერნეტზე და მომსახურების სახეობებზე წვდომის შეზღუდვა;
- ინფორმაციის სარეზერვო სათადარიგო კოპირება და აღდგენა;
- ბრანდმაუერი (საქსელთაშორისო ეკრანი);
- კომპიუტერის მუშაობის ოპტიმიზირება;
- კონფიდენციალური ინფორმაციის დაცვის ფილტრი;
- ვირტუალურ კლავიატურაზე პაროლების შეყვანის ფუნქცია.

7. McAfee Labs

ფუნქციები:

- დაცვა ვირუსებისაგან, რუტკიტებისაგან, ტროას პროგრამებისაგან, საჯაშუშო და სარეკლამო პროგრამული უზრუნველყოფა, ჰაკერული საქმიანობის აღმოჩენა;
- შემომავალი და გამავალი ტრაფიკების შემოწმება;
- „სპამ“- გზავნილების ფილტრაცია;
- შემომავალი და გამავალი http – ტრაფიკის შემოწმება;
- არასასურველი კონტენტისაგან დაცვა;
- არასაჭირო ფაილებისა და მონაცემების მოცილება;
- ბრანდმაუერი (საქსელთაშორისო ეკრანი);
- პერსონალური კომპიუტერის ოპტიმიზაცია;
- კონფიდენციალური ინფორმაციის დაცვის ფილტრი.

3.3.7. ინფორმაციის კრიპტოგრაფიული დაცვის საშუალებები

კრიპტოგრაფიული დაცვის მეთოდები კონკრეტულობასთან ახლოს არ არის, ვინაიდან გასაიდუმლოებულია. ალბათ შევძლებ, რომ ჩამოვთვალო (შევთავაზო) კრიპტოგრაფიული დაცვის მექანიზმები, მაგალითად შენახვის ან გადაცემის პროცესში ინფორმაციის დაცვა შიფრაციის ალგორითმებით – კონკრეტიზაციის გარეშე; ან კავშირის დამყარების დროს იდენტიფიკაციისათვის ელექტრონული ხელმოწერის გამოყენება და ა.შ.

3.4. ინფორმაციულად დაცული მონაცემთა გადაცემის არხის შექმნის პრობლემები [46]

საზოგადოების განვითარების შეფასების ერთ-ერთ ძირითად კრიტერიუმს წარმოადგენს კომპიუტერული საინფორმაციო-სატელეკომუნიკაციო ტექნოლოგიების დანერგვის დონე. ამასთანავე,

საინფორმაციო-სატელეკომუნიკაციო განვითარების უმნიშვნელოვანესი კომპონენტია - ინფორმაციული უსაფრთხოება.

ინფორმაციული - უსაფრთხოების პრობლემის მნიშვნელობის მიმართ, ყურადღების განსაკუთრებულად გამახვილება განპირობებულია იმ ფაქტით, რომ საინფორმაციო-სატელეკომუნიკაციო ტექნოლოგიების განვითარებისა და მსოფლიო, გლობალურ, კიბერ-სივრცედ ჩამოყალიბების პარალელურად, აქტიურად ვითარდება არასანქცირებული მიერთებების, ინფორმაციის დამახინჯებისა და მცდარი ინფორმაციის თავსმოხვევის მეთოდები და საშუალებები, რაც ანგრევს საინფორმაციო-სატელეკომუნიკაციო სისტემის ნორმალური ფუნქციონირების პირობებს.

დღეისათვის, როდესაც მილიონობით მომხმარებელი სარგებლობს სატელეკომუნიკაციო ქსელებით, იყენებენ საბანკო ანგარიშებსა და საგადასახადო დეკლარაციებს, ავსებენ საგადასახადო დეკლარაციებს და სარგებლობენ ინტერნეტ მაღაზიებით, ცხადია, ასეთ პირობებში ქსელში ინფორმაციის უსაფრთხოების პრობლემა ძალზე აქტუალურია.

უსაფრთხოების პრობლემა მრავალ საკითხს მოიცავს, რომელიც დაკავშირებულია რიგ ადამიანურ გადაცდომებთან. უსაფრთხოების უზრუნველყოფის სამსახურები ცდილობენ, რომ ცალკეულმა პიროვნებებმა ვერ შეძლონ ინფორმაციის წაკითხვა, მით უმეტეს, ვერ შეცვალონ მიმღებისათვის გაგზავნილი ცნობა. უსაფრთხოების სამსახურები ცდილობენ აღკვეთონ მიერთება სერვისებთან, იმ მომხმარებელთათვის, რომელთაც არ აქვთ მათი სარგებლობის უფლება. ინფორმაციის უსაფრთხოების სისტემა ახდენს მომხმარებლის იდენტიფიცირებას და აგვარებს ისეთ პრობლემებს, რომლებიც დაკავშირებულია ინფორმაციის მითვისებასთან და შეუძლიათ შეტყობინების განმეორებითი აღდგენა იმ პირებისათვის, რომლებიც ცდილობენ უარყონ, რომ ისინი დაკავშირებულნი არიან მოცემულ შეტყობინებასთან.

ინფორმაციის უსაფრთხოების უზრუნველყოფის უმთავრესი პრობლემები წარმოიქმნება ბოროტმომქმედებისაგან, რომლებიც ცდილობენ მოიპოვონ სხვისთვის განკუთვნილი ინფორმაცია ან სხვებს მიაყენონ ზიანი. განვიხილოთ საინფორმაციო თაღლითობის მსხვერპლთა ტიპები და მათი ქმედების მიზნები.

მომსახურების ხარისხის ტერმინს ინგლისურენოვან ნაშრომებში შეესაბამება შემდეგი შესატყვისები: Quality of service (QoS). ITU-T დოკუმენტებში მომსახურების ხარისხთან დაკავშირებული ტერმინები განისაზღვრება E.800 რეკომენდაციებით[47]. ამ რეკომენდაციებში მომსახურების ხარისხის მაჩვენებლები განხილულია, როგორც ძირითადი მახასიათებლების ერთობლივად შესრულების შესაძლებლობების უზრუნველყოფის აუცილებლობა. ნახაზ 3–ზე, რომელიც შემოთავაზებულია ITU-T-ს E.800 რეკომენდაციებში, განსაზღვრულია მომსახურების ხარისხის შემადგენელი კომპონენტები და მათი ურთიერთკავშირები. წყვეტილი, ჰორიზონტალური ხაზი ნახაზს ყოფს ორ ნაწილად, ნახაზის ზედა ნაწილში ჩამოთვლილია მომსახურების ხარისხის ძირითადი მახასიათებლები, ხოლო ნახაზის ქვედა ნაწილში ჩამოთვლილია ქსელის მახასიათებლები. ნახაზის ყველა უჯრედის დასახელება მითითებულია ქართულ ენაზე, ამიტომ საჭიროდ მიგვაჩნია ამ ტერმინების ჩამოთვლა ორიგინალის ენაზეც:

მომსახურების ხარისხის შეფასების მახასიათებლები:

- მომსახურების ხელშეწყობა (Service support);
- მომსახურების მოხერხებულობა (Service operability);
- მომსახურების მიწოდება (Service ability);
- მომსახურების უსაფრთხოება (Service security).

მომსახურების ხელშეწყობის მახასიათებლები წარმოაჩენს ოპერატორ–კომპანიის უნარს მომსახურების მიწოდებაში და მომხმარებლის მხრიდან მისი სრულყოფილად გამოყენების ხელშეწყობაში.

მომსახურების მიწოდების მახასიათებლები იყოფა სამ ჯგუფად:

- მომსახურების მისაწვდომობა (Service accessibility);

- მომსახურების მდგრადობა (Service integrity);
- მომსახურების სრულყოფილება (Service integrity).

მომსახურების მისაწვდომობის მახასიათებლებით შეფასდება მომხმარელის მხრიდან მომსახურების მიღების შესაძლებლობები, საჭირო დროის განმავლობაში და ხარისხის შემცირების გარეშე.

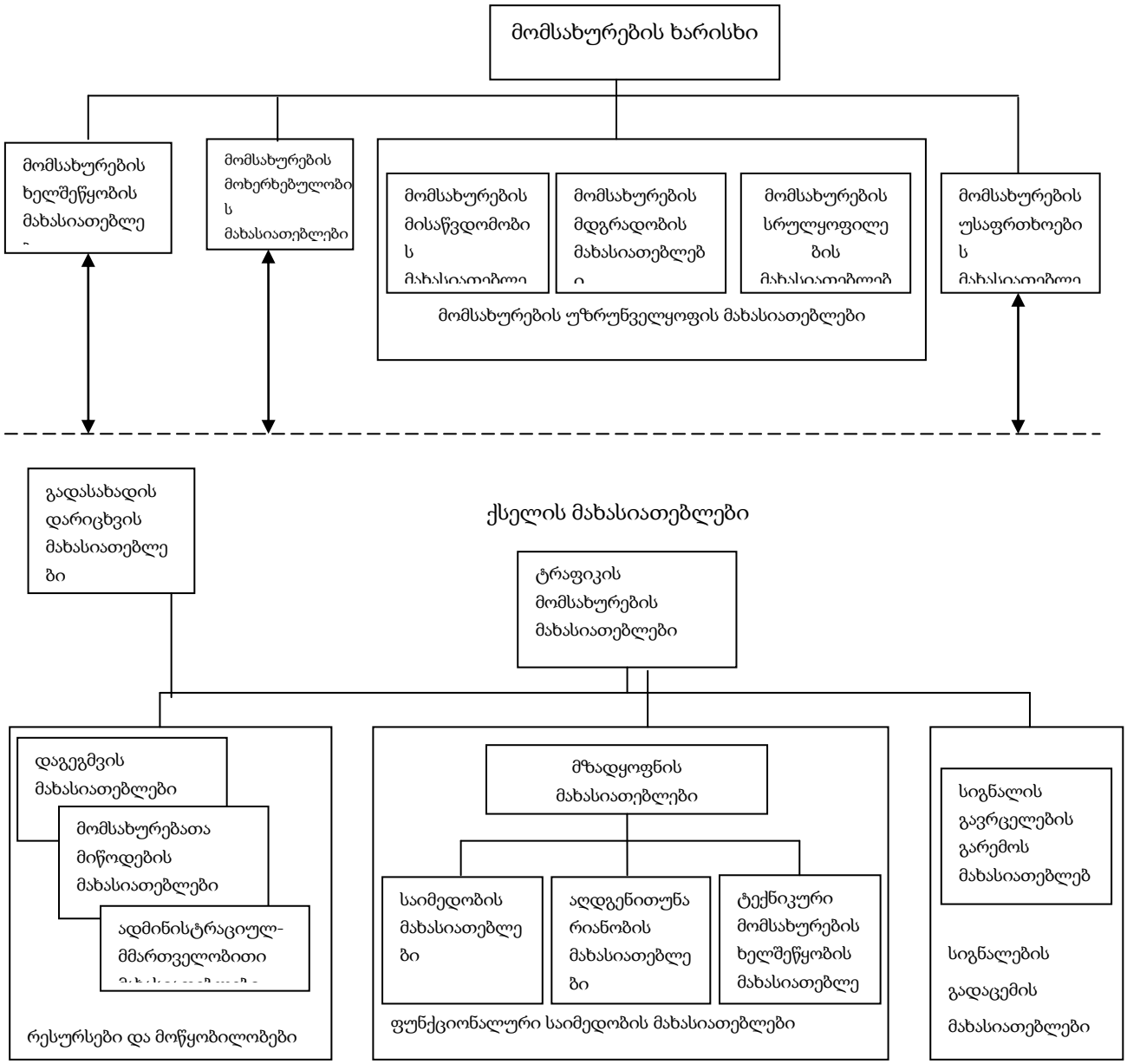
მომსახურების მდგრადობა განსაზღვრავს მოცემული დროის განმავლობაში მომსახურების უზრუვნელყოფას მისი ყველა შემადგენელი კომპონენტის შენარჩუნებით.

სრულყოფილების მახასიათებელი არის იმის ზოგადი საზომი, რომ მომსახურება მიმდინარეობს გაუარესების გარეშე.

მომსახურების უსაფრთხოების მახასიათებლები დაკავშირებულია კავშირგაბმულობის ქსელის ფუნქციონირების შემდეგ ასპექტებთან:

- არასანქციონირებული მონიტორინგი;
- თაღლითური გამოყენება;
- დაზიანება ბოროტი განზრახვით;
- არასწორი გამოყენება;
- ადამიანურ ფაქტორთან დაკავშირებული შეცდომა;
- სტიქიური უბედურება.

ზემოთ ჩამოთვლილი მომსახურების მახასიათებლები დამოკიდებულია ქსელის მართვისათვის დადგენილ მოქმედებების დონეზე და აგრეთვე მის ფუნქციონალურ შესაძლებლობებზე, რაც ასახულია ნახაზ 3-ზე მოცემული მოდელის ქსელის მახასიათებლების ნაწილში.



ნახ.3: ITU-T–ს მოდელი, მომსახურების ხარისხის ტერმინების განმარტებისათვის

გადასახადების დარიცხვის მახასიათებლები (charging performance) შეფასდება ტელეკომუნიკაციის საერთაშორისო კავშირის E.800 რეკომენდაციით, კერძოდ, გადახდის დარიცხვის კორექტულობის ალბათობის განსაზღვრით, დამყარებული კავშირის სახეობის, დანიშნულების პუნქტისა, სადღეღამისო დროისა და შეერთების ხანგრძლიობის შესაბამისად.

ტრაფიკის მომსახურების მახასიათებლები (trafficability performance) განისაზღვრება ტექნიკური საშუალებების უნარით - აწარმოონ ტრაფიკის მომსახურება დადგენილი პარამეტრებით. ეს მახასიათებლები გაყოფილია სამ ჯგუფად:

პირველი ჯგუფის – „რესურსები და მოწყობილობები“ ტერმინი დღეისათვის რაიმე დოკუმენტით განსაზღვრული არ არის, შესაბამისად ეს ეხება დაგეგმვის მახასიათებლებს (planing performance), მომსახურების მიწოდებას (provisioning performance) და ადმინისტრაციულ მართვას (administration performance).

მეორე ჯგუფს ეწოდება ფუნქციონალური საომედობის მახასიათებლები (dependebility). ეს კრებადი ტერმინი ითვალისწინებს მზადყოფნის მახასიათებლებზე ზემომქმედ ფაქტორებს. აქ უნდა აღინიშნოს, შემდეგი ოთხო მნიშვნელოვანი მახასიათებელი:

- მზადყოფნა (availability) - ტექნიკური საშუალების უნარი, დროის მოცემულ მომენტში შეასრულოს საჭირო ფუნქციები.
- საიმედობა (reliability) - ტექნიკური საშუალების უნარი შეასრულოს საჭირო ფუნქციები, მოცემულ პირობებში და დროის მოცემულ პერიოდში.
- აღდგენითუნარიანობა (maintainability) - ტექნიკური საშუალებების უნარი, რომ მისი გამოყენების გარკვეულ პირობებში ის ექვემდებარებოდეს ის ექვემდებარებოდეს ისეთ აღდგენითუნარიანობას, რომელშიც ის შეასრულებს მოთხოვნილ ფუნქციებს, იმ პირობით, რომ ტექნიკური მომსახურება მიმდინარეობდეს დადგენილი წესებითა და რესურსებით.
- ტექნიკური მომსახურების უზრუნველყოფა (maintenance support) – საექსპლუატაციო კომპანიის უნარი, ტექნიკური მომსახურების დადგენილი წესებით გამოიყენოს ის რესურსები, რომლებიც აუცილებელია ტექნიკური საშუალებების ქმედითუნარიანობის უზრუნველსაყოფად.

მესამე ჯგუფს მიეკუთვნება სიგნალების გადაცემის მახასიათებლები (transmission performance). ეს მახასიათებლები განისაზღვრება კავშირგაბმულობის სისტემით გადაცემული სიგნალების მიღების ხარისხით. ტელეკომუნიკაციის საერთაშორისო კავშირის E.800 რეკომენდაციით, გამოყოფილია გევრცელების გარემოს (propagation performance) მახასიათებლები. ისინი განსაზღვრულია გარემოს შესაძლებლობებით გაატაროს სიგნალი დადგენილი ნორმებით, გადაცემის პროცესის ხელოვნურად რეგულირების გარეშე.

ცხადია, მომსახურების ხარისხთან დაკავშირებული საკითხების კვლევა საერთო სარგებლობის სატელეფონო ქსელში, ისევე როგორც ნებისმიერ სატელეკომუნიკაციო ქსელში, საჭიროებს ურთიერთდაკავშირებული ამოცანების სრული კომპლექსის გადაწყვეტას. მიუხედავად ამისა, ტელეკომუნიკაციის საერთაშორისო კავშირის (ITU-T) შემოთავაზება საშუალებას იძლევა გამოიყოს გარკვეული ამოცანები, რომელთა გადაწყვეტა საერთო სარგებლობის სატელეფონო ქსელისათვის შეიძლება განხილულ იქნას, როგორც დამოუკიდებელი საკითხები. ერთ–ერთი მნიშვნელოვანი ამოცანა, რომელიც დაკავშირებულია საერთო სარგებლობის სატელეფონო ქსელის შექმნასთან, იმაში მდგომარეობს, რომ მოთხოვნის მომსახურება, რომელსაც ესაჭიროება მომსახურების სხვადასხვა ეტაპების განხორციელება, უნდა სრულდებოდეს ყველა დადგენილი ნორმის დაცვით, ხოლო სატელეფონო საუბრის პროცესში უნდა იყოს შენარჩუნებული სამეტყველო სიგნალის გადაცემის ყველა მაჩვენებელი. ეს ნორმები და მაჩვენებლები ცალკეულ ქვეყვებში რეგლამენტირებულია კავშირგაბმულობის ნაციონალური ადმინისტრაციების მხრიდან, ITU–სა და ETSI (კავშირგაბმულობის საერთაშორისო სტანდარტიზაციის ევროპული ინსტიტუტი) დოკუმენტების მოთხოვნათა გათვალისწინებით.

საქართველოს საერთო სარგებლობის სატელეფონო ქსელისათვის მომსახურების ხარისხის მაჩვენებლები იყოფა ორ დიდ ჯგუფად. პირველ ჯგუფს განეკუთვნებიან მოთხოვნათა მომსახურების ხარისხის

მაჩვენებლები, რომელიც ნახაზზე განეკუთვნებიან მომსახურების უზრუნველყოფის მახასიათებლებს, ხოლო სამეტყველო სიგნალების გადაცემის განმსაზღვრელი პარამეტრები განეკუთვნებიან ტრაფიკის მომსახურების მახასიათებლებს.

საერთო სარგებლობის სატელეფონო ქსელის მომსახურების ხარისხის მაჩვენებლების თავისებურება იმაში მდგომარეობს, რომ ეს მაჩვენებლები დროის შესაბამისად იცვლებიან.

ეს პროცესი განპირობებულია ორი ძირითადი მიზეზით. პირველი მიზეზი იმასთან არის დაკავშირებული, რომ აბონენტების უმრავლესობა დროთა განმავლობასი ზრდის მოთხოვნებს მომსახურების ხარისხის მიმართ. მეორე მიზეზი კი არის დროთა განმავლობაში აბონენტთა გარკვეული წესით თვითდაჯგუფების პროცესის შედეგი. აბონენტთა ზოგიერთი ჯგუფები, რომლებიც ოპერატორს უქმნიან მნიშვნელოვან შემოსავლებს, მოითხოვენ მათი ტრაფიკის მომსახურების მიმართ მკაცრ ნორმებს. საერთო სარგებლობის სატელეფონო ქსელის ოპერატორები დაინტერესებული არიან, რომ შეინარჩუნონ ასეთი აბონენტები. მითუმეტეს, რომ ისინი შესაძლოა გადავიდნენ კონკურენტ-ოპერატორთა ქსელში. ასეთი აბონენტებიშ შენაჩუნებისათვის, დასავლეთ ევროპასა და ჩრდილოეთ ამერიკის ქვეყნების გამოცდილებით, იყენებენ შეთანხმების გაფორმების წესს მომსახურების განსაკუთრებული ხარისხის უზრუნველსაყოფად, რასაც შეესაბამება ინგლისურენოვანი აბრევიატურა SLA (Service Level Agreement).

ასეთი შეთანხმების შემადგენელი ნაწილის ერთ–ერთ მახასიათებელს წარმოადგენს „ფუნქციონალური საიმედობის“ მახასიათებლების ბლოკი (იხ.ნახ.3). კერძოდ, მზადყოფნის კოეფიციენტი, SLA შეთანხმების გაფორმების დროს, შეირჩევა 0,99999 დონეზე და ტექნიკურ ლიტერატურაში გაჩნდა შესაბამისი ტერმინი „ხუთი ცხრიანის წესი“. T დროის განმავლობაში მზადყოფნის კოეფიციენტი განისაზღვრება სისტემის მოქმედუნარიან მდგომარეობაში ყოფნის დროის ფარდობით T

სიდიდესთან, ანუ უნდა ჩავთვალოთ, რომ T დროის განმავლობაში საკომუნიკაციო სისტემა არის ქმედითუნარიანი (T_A) ან არ ფუნქციონირებს, რადგანაც არ არის გამოყენებული, მაგრამ ქმედითუნარიანია. დროის ხანგრძლიობა, როდესაც სისტემა არ ექვემდებარება ექსპლუატაციას აღვნიშნოთ T_F . მაშინ მზადყოფნის კოეფიციენტის განსაზღვრისათვის გვექნება თანაფარდობა:

$$A = \frac{T_A}{T_A + T_F}$$

თუ ამ გამოსახულებაში ჩავსვამთ A=0.99999, შეიძლება განვსაზღვროთ T_F-ის დასაშვები მნიშვნელობა ექსპლუატაციისთვის შერჩეული დროის შესაბამისად. მაგალითად, ერთი წლის განმავლობაში T_F არ უნდა აღემატებოდეს 5,3 წუთს. ასეთი მკაცრი ნორმის შესასრულებლად, აუცილებელია ქსელის გარკვეული რესურსების რეზერვირება და ისეთი ცვლილებების პროგნოზირება, რომელიც დაკავშირებულია მომსახურების ხარისხის უზრუნველყოფასთან, რაც ქსელის ოპერატორისათვის მნიშვნელოვან ამოცანას წარმოადგენს.

დასკვნა

1. ობიექტებისათვის სატელეკომუნიკაციო ქსელებსა და სისტემებს უნდა გააჩნდეთ მზადყოფნის კოეფიციენტები კრიტიკულობის კოეფიციენტების შესაბამისად, სადაც მზადყოფნის კოეფიციენტების მნიშვნელობები განსაზღვრული იქნება მდგრადობის (სიცოცხლისუნარიანობის) შესაბამისად.
2. აუცილებელია ახალი, ფუნდამენტალური შედეგი, როგორც ინფორმაციაზე შემოტევებისაგან დაცვის პრობლემების მეცნიერულად ფორმულირებისათვის, ასევე მადესტაბილიზირებელი ინფორმაციის ზემოქმედებების აცილების მეთოდებისა და საშუალებების ანალიზისა

და სინთეზისათვის, იმის გათვალისწინებით, რომ შემოტევების მეთოდები და მექანიზმები აგრეთვე, განიცდიან სრულყოფას.

თავი 4. სატელეკომუნიკაციო ქსელში არასანქციონირებული ჩართვის აღმოჩენის შესაძლებლობა გადაცემული ინფორმაციის დაყოვნების გაზომვის შედეგის საფუძველზე [48]

NGN (Next Generation Networks ან Next step generation) არის შემდეგი თაობის - ჰეტეროგენული, მულტისერვისული ქსელი, რომელიც უზრუნველყოფს ყველა სახის მედიატრაფიკის გადაცემას და სატელეკომუნიკაციო მომსახურების ფართო სპექტრის სიახლეთა დამატებებს, რედაქტირებებს და განაწილებული ტარიფიკაციის შესაძლებლობებს.

ქსელის ძირითადი საინფორმაციო-ტექნიკური მახასიათებლები, რომლებიც განსაზღვრავს მომხმარებელთა მომსახურების გარანტირებულ ხარისხს და საერთოდ ქსელის ქმედითუნარიანობას, არის შემდეგი:

- სატრანსპორტო მაგისტრალების გამტარუნარიანობა ან გადაცემის სიჩქარე;
- ქსელის კვანძებში შემომავალი და გამავალი ტრაფიკის მოცულობა;
- ქსელის ტრაქტებში და მაგისტრალებში ჯამური ტრაფიკის მნიშვნელობა;
- ქსელის საიმედობა და მზადყოფნის კოეფიციენტი.

თანამედროვე კავშირგაბმულობის ციფრული ქსელები დამატებით მოითხოვს ქსელის შემდგომი გაფართოებისა და განვითარების შესაძლებლობის არსებობას და შემდეგი ფაქტორებისგათვალისწინებას:

- საჭირო გატარების ზოლის უზრუნველყოფას;
- ქსელის გაფართოებისა და მასშტაბირების შესაძლებლობას;
- ქსელის მართვადობას;
- სხვა და სხვა ტრაფიკების ინტეგრაციის შესაძლებლობას;
- გადაცემის და კომუტაციის ნებისმიერი სისტემების ურთიერთთავსებადობას;

- ქსელის არხებისა და ტრაქტების რეზერვირებას, ქსელის საიმედობისა და მზადყოფნის უმაღლესი მაჩვენებლების უზრუნველსაყოფად.

ტრაფიკის განაწილების ანალიზის საფუძველზე ხორციელდება მაგისტრალური ქსელის დაგეგმვა და ორგანიზება, მაგრამ, ამასთანავე, ქსელში პირველადი ტრაფიკის ანალიზისა და კომუტაციის ფუნქციით ნაკადების გაცვლის იერარქიის საფუძველზე, განისაზღვრება ქსელის დატვირთულობა. კომუტაციის ტრადიციული SSP (Service Switching Point - მომსახურების სახეობათა კომუტაციის წერტილი) კვანძებიდან ქსელის ინტელექტისა და მომსახურების ლოგიკის გადატანა კომპიუტერული უზრუნველყოფის SCP (Service Control Point - მომსახურების სახეობათა მართვის წერტილი)-ში მორგებული იყო ინტელექტუალური ქსელის (Intelligent Network) კონცეფციაზე, ITU-ს Q-1200 რეკომენდაციის სპეციფიკაციით.

ტელეკომუნიკაციის ტექნოლოგიების სწრაფმა განვითარებამ და მომსახურების სახეობებზე მოთხოვნების ზრდამ გამოიწვია მომსახურების ახალი სახეობების შექმნისა და მათი სწრაფი დანერგვის აუცილებლობა. ამ ფაქტორების ზეგავლენით ჩამოყალიბდა ჰეტეროგენული პაკეტური ტექნოლოგიის, შემდგომი თაობის NGN ქსელის კონცეფცია, სადაც სამეტყველო სიგნალის გადაცემა განიხილება, როგორც მომსახურების ისეთი სახეობა, რომლებიც მოითხოვს დაყოვნების კიდევ უფრო მცირე მნიშვნელობას, ვიდრე სამეტყველო სიგნალის გადაცემა IP (Internet Protocol Address - ინტერნეტ პროტოკოლ მისამართი) ქსელით, შესაბამისად დაყოვნებების პრობლემამ მოახდინა მნიშვნელოვანი ზეგავლენა NGN ქსელის მახასიათებლებზე. [49] ავტორებმა ასეთი ქსელები გამოყვეს ახალ კლასად და უწოდეს ქსელები მცირე დაყოვნებებით.

განვიხილოთ ისეთი სატელეკომუნიკაციო ქსელის შემთხვევა, რომელიც შეიცავს მხოლოდ ერთ კვანძს SSP-ფუქციონალური შესაძლებლობებით. ინტელექტუალურ მომსახურებაზე მოთხოვნები SSP-ს მიეწოდება ქსელის ყველა კვანძებიდან, წინასწარ დადგენილი მარშრუტებით. ნახ.4-ზე მოცემულია ასეთი ქსელის ფრაგმენტი შესაბამისი კვანძებით [50], ხოლო შემა-

ერთებელი ხაზები, შეესაბამება კვანძებიდან SSP-მდე სიგნალების მიწოდების მარშრუტებს. (აქ სიგნალების მიწოდების შესაძლო შემოვლითი გზები აღნიშნული არ არის).

ჩავთვალოთ, რომ SSPგანთავსებულია Y_0 საკვანძოსადგურში, ხოლო დანარჩენი კვანძები $Y_i (i \neq 0)$ წარმოადგენენ დამაბოლოებელ სადგურებს, ანუ ყოველი მათგანი ქმნის ინტელექტუალურ მომსახურებაზე მოთხოვნების დატვირთვას.

ავღნიშნოთ: λ_0 -ით ინტელექტუალურ მომსახურებაზე მოთხოვნების საშუალო რიცხვი ერთი მომხმარებლისაგან, დროის ერთეულში; N_i არის i-ური კვანძის მომხმარებელთა რიცხვი;

ამ შემთხვევაში, ყოველი კვანძიდან შემოსული მოთხოვნების საშუალო რიცხვი ინტელექტუალურ მომსახურებაზე იქნება:

$$\lambda_i = \lambda_0 \cdot N_i ,$$

ხოლო SSP -ზე შემოსული ჯამური მოთხოვნები ყველა კვანძიდან:

$$\lambda = \sum_{i=1}^{K} \lambda_i ,$$

სადაც K არის SSP-ზე მიერთებული კვანძების საერთო რიცხვი.

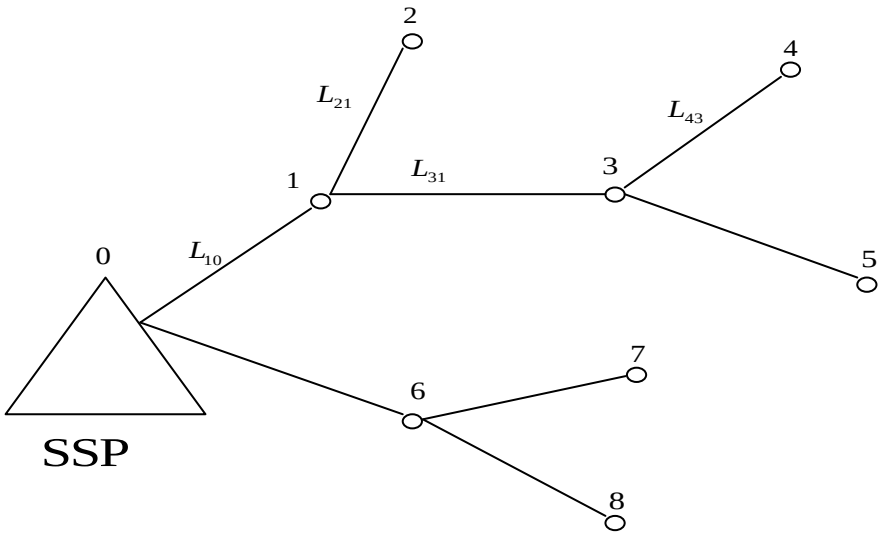
ავღნიშნოთ V_{ij} -ით მონაკვეთი, რომელიც აერთებს ქსელის Y_i და Y_j კვანძებს. ავღნიშნოთ B_i -ით ქსელის უბანი, რომელიც შეიცავს Y_i კვანძიდან, საკვანძო სადგურამდე მარშრუტის ყველა მონაკვეთებს. მაგალითად, ნახ.2-ზე Y_4 კვანძისათვის B_4 მარშრუტი შეიცავს მონაკვეთებს V_{01}, V_{13} და V_{14}.

ავღნიშნოთ V_{ij} მონაკვეთის შესაბამისი გზის სიგრძე L_{ij} -ით, ხოლო ქსელის B_i მონაკვეთის სიგრძე, რომელიც შეიცავს ყველა მარშრუტებს Y_i კვანძიდან საკვანძო სადგურამდე L_i -ით:

$$L_i = \sum_{Y_{ij} \in B_i} L_{ij} .$$

მაგალითად, ნახ.4-თვის გვექნება:

$$L_4 = L_{43} + L_{31} + L_{10},\ L_3 = L_{31} + L_{10},\ L_2 = L_{21} + L_{10}$$ და ა.შ.



ნახ.4. სატელეკომუნიკაციო კვანძებიდან SSP-კენ შესაძლო მარშრუტები.

ინტელექტუალურ მომსახურებაზე B_i მარშრუტით მოთხოვნის გავლის ალბათობა არის *i*-ური სატელეკომუნიკაციო კვანძიდან მოთხოვნათა ინტენსიობისპროპორციული:

$$P_i = \frac{\lambda_i}{\lambda}.$$

$L_{საშ.}$ გზის საშუალო სიგრძე, რომლის გავლასაც საჭიროებს მოთხოვნის შემოსვლის შესახებ ინფორმაციის სიგნალი, სატელეკომუნიკაციო კვანძიდან

SSP-მდე, განისაზღვრება თანაფარდობით:

$$L_{\text{საშ.}} = \sum_{i=1}^{K} P_i \cdot L_i \ .$$

ასეთივე მსჯელობით განისაზღვრება იმ კვანძების საშუალო რიცხვი, რომელთა გავლაც მოუხდება B_i მარშრუტით მოთხოვნის შესახებ ინფორმაციის სიგნალს:

$$K_{\text{საშ.}} = \sum_{i=1}^{K} P_i \cdot K_i \ ,$$

სადაც K_i არის B_i მარშრუტის კუთვნილი სატელეკომუნიკაციო კვანძების რიცხვი.

თუ ჩავთვლით, რომ ქსელში ხაზის უბანზე სიგნალის გავრცელების დრო შეადგენს $V_{\text{სიგნ.}}$, მაშინ ქსელის ხაზებში სიგნალის გავრცელების დროის შესაბამისად, სიგნალის დაყოვნების საშუალო მნიშვნელობა იქნება:

$$\tau_L = \frac{L_{\text{საშ.}}}{V_{\text{საშ.}}} \ .$$

როდესაც სატელეკომუნიკაციო კვანძი მიიღებს მომხმარებლის მოთხოვნას და ეს მოთხოვნა გაივლის ყველა ტრანზიტულ კვანძს, ცხადია ყველგან მოხდება დროში დაყოვნებები. თუ ჩავთვლით, რომ ყოველ კვანძში დაყოვნებების მნიშვნელობები ერთნაირია და ავღნიშნავთ მას $\tau_{\text{დაყ./კვ}}$, შეტყობინების ჯამური დაყოვნება, მარშრუტის შესაბამისად ყველა კვანძების გავლის შემდეგ, იქნება:

$$\tau_K = K_{\text{სიგნ.}} \cdot \tau_{\text{დაყ./კვ}} \ .$$

ამრიგად, დროში დაყოვნებების თვალსაზრისით, განშტოებული ქსელი შეიძლება პირობითად ჩანაცვლდეს ექვივალენტური განუშტოებელი უბნით, ხასიათდება ხაზებში სიგნალის გავრცელების იგივე დაყოვნებით და ქსელის კვანძებში შეტყობინების იმავე, საშუალოჯამური დაყოვნებით.

დასკვნა

დაყოვნებების მნიშვნელობათა ზუსტი გაზომვის შედეგები იქნება ინფორმაციის წყარო, ქსელში გადაცემული სიგნალისათვის მარშრუტის შეცვლის შესახებ, რაც იძლევა ახალი ამოცანების გადაწყვეტის საშუალებას, მათ შორის ქსელის ფუნქციონირებაში არასანქცირებული ჩართვის შესახებ.

საერთო 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.

გამოყენებული ლიტერატურა

1. Машин О.А., Платонов Б.Ф., Язов Ю.К. Методический подход к оценке ефективности выборочново контроля состояния защищенности информации в компьютерных системах. //Телекоммуникации №11.2013, стр. 32-36.

2. Сабанов А.Г. Анализ применимости методов оценки рисков к процессам аутентификации при удаленном электронном взаимодействии. //Электросвязь, №5,2014 стр.44-47.

3. Сабанов А.Г. Об оценке рисков удаленной аутентификации // Электросвязь, №4, 2013.

4. Сабанов А.Г. Методика идентификации рисков аутентификации //Докл. Томского гос. Университета систем управления и радиоэлектроники. 2013, №4 (30).

5. Сабанов А.Г. Многоуровневый анализ угроз безопасности процессов аутентификации //Вопросы защиты информасии. 2014. №1 (104).

6. Сабанов А.Г. Основные процессы аутентификации //Вопросы защиты информации. 2012. №3.

7. Сабанов А.Г. Классификация процессов аутентификации //Вопросы защиты информасии. 2013. №3.

8. Сабанов А.Г. Принципы классификации систем идентификации и аутентификации по признакам соответствия требованиям информационной безопасности // Электросвязь. № 2, 2014.

9. Сабанов А.Г. Концепция моделирования процессов аутентификации //Докл. Томского гос. Университета систем управления и радиоэлектроники. 2013, №3 (29).

10. Сабанов А.Г. Обзор иностранной нормативной базы по идентификации и аутентификации // Защита информации. Йнсайд. 2013. №4 (52).

11. Сабанов А.Г. Модели для исследования безопасности и надежности процессов аутентификации // Электросвязь. № 2, 2013.

12. Скрыль С.В., Корчагин В.В., Змеев А.А., Багринцева О.В., Герасимов А.А. Формализованное представление информационных процессов в условиях

угроз нарушения целостности и доступности информации. // Телекоммуникации №3.2015, стр.26-33.

13. Скрыль С.В., Малышев А.А., Волкова С.В., Герасимов А.А. Функциональное моделирование как методология исследования информационной деятельности //Интеллектуальные системы (INTELS 2010). Труды Девятово международного симпозиума. 2010. Стр. 590-593.

14. Зарубин В.С., Гурченко С.В. Проблемы повышения эффективности защиты информации в современных системах безопасности // Охрана, безопасность и связь. Материалы Всероссийской научно-практической конференции. 2009. Стр. 21-22.

15. Леньшин А.В., Кравцов Е.В., Сенюков Г.А. Программный модуль имитации специальных електронных устройств перехвата информации.// Телекоммуникации №6 .2015, стр.38-42.

16. Дейкун А.О., Зинин Е.Н., Кравцов Е.В. Информационные и измерительные системы радиомониторинга и пеленгования // Фундаментальные проблемы системной безопасности. Материалы V Международной научной конференции, посвященные 90-летию со дня рождения выдающегося ученого, генерального конструктора ракетно-космических систем, академика Уткина В.Ф. 2014. Стр. 168-173.

17. Кравцов Е.В., Нагалин А.В., Сенюков А.Г. Концептуальная модель оптимизации временных затрат на формирование компетенций на примере подготовки специалистов технической защиты информации // Вестник Воронежсково института МВД России. 2014. №3. Стр. 203-209.

18. Гречишников Е.В., Горелик С.П., Добрышин М.М. Способ обеспечения требуемой защищенности сети связи от внешних деструктивных воздействий // Телекоммуникации №6 .2015, стр.32-37.

19. Скрыль С.В., Спивак В.И., Щербаков А.В., Пономаренко С.В. Проблема оптимизации процедур комплексного технического контроля защищенности информации от утечки по каналам ПЕМИН: концепция решения. // Защита информации. Електромагнитная совместимость. Стр. 23-34.

20. Скрыль С.В., Никулин С.С., Щербаков А.В., Пономаренко С.А. Задача повышения эффективности комплексного технического контроля защищенности речевой информации от утечки по техническим каналам в деятельности объектов промышленно-деловой среды: основные методические положения // Телекоммуникации №5 .2016. стр.34-41.

21. Скрыль С.В., Никулин С.С., Щербаков А.В., Пономаренко С.А. Методика нахождения оптимальных параметров комплексного технического контроля обеспечения защищенности речевой информации в деятельности объектов промышленно-деловой среды // Телекоммуникации №7. 2016. стр.40-44.

22. Володина А.А., Костин А.О. Основополагающие принципы автоматизации процесса подбора средств защити информации для предпрятия. // Телекоммуникаций №4. 2016. стр.30-36.

23. Jaap de Waard. The Private Security Industry in International Perspective // European Journal on Criminal Policy and Research. 1999. V. 7. Issue 2. P. 143 – 174.

24. Advances in Information Security // Protecting Privacy in Data Release/ 2015. V. 57.

25. Self R. J., Voorhis D. Chapter 10 – Tools and Technologies for the Implementation of Big Data // Application of Big Data for National Security. A Practitioner's Guide to Emerging Technologies. 2015. P. 140-154.

26. Шишкин Н.В., Кузьмин М.А. Модель потоков данных интерактивной сети обеспечения анонимного доступа. // Вычислительные системы, сети и устройства телекоммуникаций. стр. 45- 48.

27. Барабанов А.В., Лучин Д.В., Марков А.С., Рауткин Ю.В. Методические вопросы оценки соответствия аппаратуры сетей связи требованиям по безопасности информации. //ISSN 0013-5771. Электросвязь, №8. 2015.

28. Гордиенко В.Н. Телекоммуникационные и вычислительные системы // Электросвязь. 2010. №2. Стр. 58-61.

29. Донос А.Е. Киберпространство под защитой РСС // Электросвязь. 2011. №5. Стр. 8-9.

30. Лучин Д.В., Сподобаев М.Ю. Системы ДКМВ радиосвязи: разработка, производство и перспективные решения // Вестник Самарского государственного аерокосмического университета им. Академика С.П. Королёва. 2014. №2(44). Стр. 74-79.

31. Марков А.С., Рауткин Ю.В., Фадин А.А. Состояние и перспективы анализа защищенности Wi-Fi сетей // Труды НИИР. 2012. №1. Стр.79-84.

32. Кузнецов И.А., Липатников В.А., Сахаров Д.В. Управление АСМК организации интегрированной структуры с прогнозированием состояния информационной безопасности // Электросвязь. №3. 2016. стр. 28-36.

33. Еременко В.Т., Мишин Д.С., Парамохина Т.М. Направления и проблемы интеграции автоматизированных систем управления для предприятий с непрерывным технологическим циклом // Информационные системы и технологии. 2014. №3. Стр. 51-58.

34. Костарев С.В., Липатников В.А. Анализ состояния и динамики качества обьектов автоматизированной системы менеджмента предприятия интегрированной структуры // Информационные системы и технологии. 2013. №3. Стр. 52-64.

35. Бухарин В.В., Липатников В.А., Сахаров Д.В. Метод управления информационной безопасностью организации на основе процессного подхода // Информационные системы и технологии. 2013. №3-77. Стр. 102-109.

36. 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.

37. Сабанов А.Г. Анализ применимости методов управления рисками к процессам аутентификации при удаленном электронном взаимодействии //Электросвязь. Эжемесячный научно-технический журнал, 2014, №6, с.39-42.

38. Сабанов А.Г. Методика идентификации рисков аутентификации //Докл. Томского гос. Университета систем управления и радиоэлектроники. 2013, №4 (30), с.136-141.

39. Утечки конфиденциальной информации: ИТОГИ 2013 года //Сети и тедекоммуникации. Ежемесячный научно-технический журнал, 2014, №1-2, с.54-61.

40. 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.

41. Доступность и защищенность персональных данных: как совместить несовместимое. //Электросвяь. Ежемесячный научно-технический журнал, №12, 2009, стр.40-42.

42. Ульянов В.В. Защита персональных данных: тенденции осени – 2009. //Электросвяь. Ежемесячный научно-технический журнал, №12, 2009, стр.43-45.

43. Михайлов В.Ю; Мазепа Р.Б. Кибербезопасность систем инфокоммуникаций // Электросвязь, №12, 2016, стр.36-40.

44. ИСО / МЭК 27032:2012 – Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности (ISO/IEC 27032:2012 Information technology - Security techniques – Guiolelines for cybersecurity) – URL: http://www.iso.org/iso/ru/catalogue_detail?csnumber=44375, 18.09.2016.

45. ITU – T Recommendation X. 800: Secutity architechure for Open Systems Interconnection for CCITT applications. – URL:http://www.itu.int/rec/T-REC-X.800-199103-I

46. 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.

47. Recommendation ITU-T E.800. Definitions of terms related to quality of service. http://ru.scribd.com/doc/51368290/ITU-T-E-800

48. 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.

49. Кучерявый А.Е., Парамонов А.И., Аль-Наггар Я.М. Сети связи с малыми задержками //Электросвязь. Эжемесячный научно-технический журнал, 2013, #12, с.15-19;

50. Лихтциндер Б.Я., Кузякин М.А., Росляков А.В., Фомичев С.М. Интелектуальные сети связи, ЭКО-ТРЕНД МОСКВА,2000 стр.197.