ინფორმაციული შეტევების, უსაფრთხოების და დაცვის თანამედროვე საშუალებები

თამაზ შეროზია, გულბაათ ნარეშელაშვილი, აკაკი შონია
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

თავდასხმების, შეტევების და უსაფრთხოების დაცვის ისტორია, კაცობრიობის ისტორიის პარალელურად იქმნებოდა და ვითარდებოდა. დროთა განმავლობაში ხდებოდა სულ უფრო და უფრო მეტი დასაცავი ობიექტის წარმოქმნა. გაჩნდა სუსტი წერტილები დაცვის მთელ სისტემაში, რომელშიც ეს ობიექტები შედიოდნენ. გახშირდა მათზე თავდასხმები, რომლებიც ბოროტმოქმედების მხრიდან ხორციელდებოდა სხვადასხვა მეთოდებით. ამის შესაბამისად ვითარდებოდა სისტემის დაცვის საშუალებები, რაც უზრუნველყოფდა მის უსაფრთხოებას. ამჟამად, კომპიუტერული ტექნიკის განვითარების შედეგად წარმოიშვა ინფორმაციული თავდასხმისა და დაცვის აპარატურულ-პროგრამული მეთოდები და საშუალებები. მავნე პროგრამებად განხილულია ვირუსები, ჯაშუში პროგრამები, ქსელური ჭიები, სპამები. დაცვის საშუალებებად კი დახასიათებულია კრიპტოგრაფიული მეთოდები, ანტივირუსები, ფაირვოლები, ბრანდმაიერები, ქსელური ეკრანები, ანონომიზატორები, მარშრუტიზატორები, ნაჩვენებია მათი დადებითი და უარყოფითი მხარეები, მოცემულია მათი გამოყენების რეკომენდაციები.

საკვანძო სიტყვები: ინფორმაციული შეტევა. უსაფრთხოება. დაცვის სამსახური. პროგრამა-ვირუსები. ქსელური ჭიები. სპამი. კრიპტოგრაფია. ანტივირუსი. ფაირვოლი. ბრანდმაიერი. ქსელური ეკრანი. მარშრუტიზატორი. ანონომაიზერი.

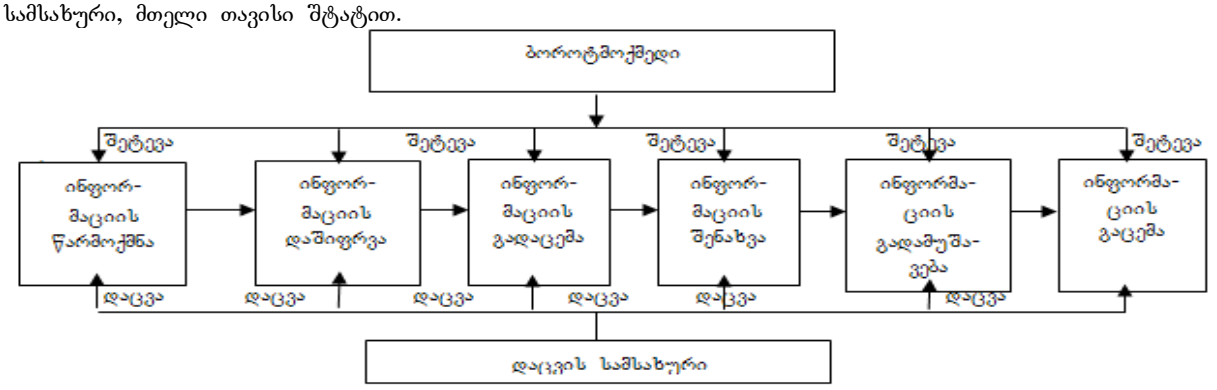
1. შესავალი

ცხოვრება წარმოუდგენელია დაცვის გარეშე. უხსოვარი დროიდან დაცვას საჭიროებდა პიროვნება, ოჯახი, საკუთრება, ორგანიზაცია, ტერიტორია, შენობა-ნაგებობა, მოწყობილობა და მრავალი სხვა. დაცვა სჭირდება აგრეთვე ინტელექტს, აზროვნებას. ამ მრავალფეროვნებას შორის ერთ-ერთია ინფორმაციის დაცვა, რომელიც შეიძლება წარმოქმნას, გადასცეს და მიიღოს როგორც ტექნიკურმა მოწყობილობებმა, ისე ცოცხალმა ორგანიზმებმა, ლაპარაკით, ჟესტებით, რადიო და ელექტრო-მაგნიტური სიგნალებით, დაფიქსირდეს ქაღალდზე და სხვა. დაცვის ისტორია კაცობრიობის ისტორიასთან არის დაკავშირებული [1]. იგი დროთა განმავლობაში ვითარდებოდა და იხვეწებოდა. გაჩნდა დაცვის მექანიკური, ელექტრო, მაგნიტური, ლაზერული, სენსორული, ბიოლოგიური და სხვა საშუალებები. გამოთვლითი ტექნიკის განვითარებამ წარმოიშვა დაცვის აპარატურული და პროგრამული საშუალებები.

საზოგადოების და ტექნიკურ-ეკონომიკური განვითარების შედეგად დაცვას საჭიროებდა სულ უფრო და უფრო მეტი ახალი ობიექტი. წარმოიქმნა დაცვის ახალი ადგილები. ობიექტი დაცვას საჭიროებს იმიტომ, რომ გაჩნდნენ ბოროტმოქმედებნი, რომლებმაც დაიწყეს შეტევები დაცვის სუსტ ადგილებზე. ჩატარებული სამუშაოს ანალიზის შედეგად იხვეწებოდა და ინერგებოდა დაცვის ახალი მეთოდები, რომლებიც ზრდიდნენ დაცვის მდგრადობას და იცავდნენ მას „გატეხვისაგან“. თუმცა უნდა აღინიშნოს, რომ მიუხედავად ჩატარებული უზარმაზარი სამუშაოსი, დაცვის სრულყოფილი საშუალებები ჯერ კიდევ არ არსებობს. შეიძლება ითქვას, რომ ყოველი ახალი „კლიტისათვის” ბოროტმოქმედი ამზადებდა „გასაღებს“ და ტეხდა „კლიტეს“, რაც მუდმივად იწვევდა ახალი „კლიტეების“ და „გასაღებების“ დამზადებას და დაყენებას.

2. ძირითადი ნაწილი

დაცვის მთელ სისტემაში, ინფორმაციის მოძრაობის გზაზე შეიძლება წარმოვადგინოთ დასაცავი ადგილები, რომლებზეც ხდება შეტევა, სუსტი წერტილების აღმოჩენა და გატეხვა, რაც საჭიროებს მათ დაცვას (ნახ.1). ორგანიზაციაში მთელ ამ დაცვის სისტემას ემსახურება უსაფრთხოების, ან დაცვის სამსახური, მთელი თავისი შტატით.



ნახ.1

დაცვას საჭიროებს ამ გზის ყველა პუნქტი, ამიტომ ინფორმაციული უსაფრთხოება ეს არის ინფორმაციული გარემოს დაცულობის მდგომარეობა. ინფორმაციის დაცვა კი წარმოადგენს მოღვაწეობას, რათა არ მოხდეს დაცული ინფორმაციის გაჟონვა და არასანქციონირებული მოქმედებები დაცულ ინფორმაციაზე. დაცვა იწყება ჯერ კიდევ ინფორმაციის წარმოქმნის მომენტიდან. ინფორმაცია შეიძლება წარმოიქმნას ლაპარაკით, ჟესტებით, დოკუმენტში დაფიქსირებით, ხელსაწყოს მოქმედებით, კლავიატურის საშუალებით შეტანით და სხვა. ამიტომ ამ დროს საჭიროა სიფრთხილე, რათა ბოროტმოქმედის მიერ არ მოხდეს მისი დანახვა, ან შესაბამისი ხელსაწყოთი დაფიქსირება.

ინფორმაციის დაცვის ერთ-ერთ საშუალებას წარმოადგენს კრიპტოგრაფია, ანუ ინფორმაციის გასაიდუმლოება (დაშიფრვა) [2]. მასაც მრავალსაუკუნოვანი ისტორია აქვს და დღესაც ძალზე აქტუალურია, რადგან კომპიუტერი და ინტერნეტ ქსელი, რომლითაც ხდება ინფორმაციის გავრცელება, ფართოდ ინერგება ადამიანთა მოღვაწეობის თითქმის ყველა სფეროში. დაშიფრვისათვის საჭიროა დაშიფრვის ალგორითმი და გასაღები, რომლითაც ასევე მოხდება გაშიფრვა. შიფრი მით უფრო მდგრადია, რაც უფრო რთულია ალგორითმი და მეტია გასაღებების რაოდენობა. დღეს ფართოდ არის გავრცელებული ისეთი მეთოდები, როგორიცაა სიმეტრიული და ასიმეტრიული კრიპტოგრაფია, აუტენტიფიკაცია, ციფრული ხელმოწერა, მონაცემთა ხეშირების ალგორითმები, ფსევდო-ალბათური რიცხვების თანამიმდევრობის ალგორითმები და სხვა. თანამედროვე კრიპტოგრაფიული პროგრამები იძლევიან საშუალებას შიფრაცია-დეშიფრაციის გასაღების მნიშვნელობა წარმოვადგინოთ 128 ბიტიანი ორობითი რიცხვით, რაც იმას ნიშნავს, რომ ასეთი მნიშვნელობის გასაღებების რაოდენობა წარმოუდგენლად დიდია ($\approx 2^{128}$), რაც თითქმის შეუძლებელს ხდის ბოროტმოქმედის მიერ დაშიფრული ტექსტის აღდგენას საწყისი სახით.

კომპიუტერზე შეტევის ერთ-ერთ ნაირსახეობას წარმოადგენს ე.წ. ვირუსული პროგრამები [3]. ვირუსი, პროგრამის ნაირსახეობაა, რომელსაც შეუძლია გამრავლება და მომხმარებლისათვის გარკვეული ზიანის მიყენება. მიუხედავად იმისა, რომ მრავალ ქვეყანაში სამართლებრივი კოდექსები კრძალავს მათ შექმნას და გამოყენებას, ისინი ინტერნეტის საშუალებით ფართოდ ვრცელდება მთელ მსოფლიოში.

ვირუსული პროგრამების გვერდით არსებობს ე.წ. მზვერავი, ჯაშუში პროგრამები (Spyware, Adware), რომლებიც მალულად თავსდება კომპიუტერებში და შეუძლია ინფორმაციის შეგროვება კომპიუტერის კონფიგურაციის, აგრეთვე მომხმარებლის შესახებ, მისი ნებართვის გარეშე. მას შეუძლია განახორციელოს სხვა მოქმედებებიც, როგორიცაა კომპიუტერის წყობის შეცვლა, რაიმე პროგრამის დაყენება, მომხმარებლის მოქმედების მიმართულების შეცვლა, ოპერაციული სისტემის პარამეტრების ცვლილება და სხვა.

მავნე პროგრამების სახით შეგვიძლია განვიხილოთ აგრეთვე ე.წ. ქსელური ჭიები, რომლებიც დამოუკიდებლად ვრცელდება ლოკალური თუ გლობალური ქსელებით. ისინი იყენებენ სისტემის სუსტ წერტილებს და შეცდომებს პროგრამულ უზრუნველყოფაში, ოპერაციულ სისტემებში და შეუძლიათ გამრავლება დამოუკიდებლად. ეს პროგრამები ირჩევს კომპიუტერებს და ახორციელებს მათზე შეტევებს, მთლიანად ავტომატურ რეჟიმში.

ვირუსების წინააღმდეგ ბრძოლის ეფექტური საშუალებაა პროაქტიული ტექნოლოგიები, ანუ ტექნოლოგიებისა და მეთოდების ერთობლობა, რომელიც გამოიყენება ანტივირუსულ პროგრამულ უზრუნველყოფაში. რეაქტიული (სიგნატურული) ტექნოლოგიებისაგან განსხვავებით მათი დანიშნულებაა არა უკვე ცნობილი მავნე პროგრამების მოძიება, არამედ მომხმარებლის სისტემის დასნეულების თავიდან აცილება. დღესდღეობით ფართოდ გამოიყენება ისეთი პროაქტიული დაცვის ტექნოლოგიები, როგორიცაა: ევრისტიკული ანალიზი; კოდის ემულაცია; ქცევის ანალიზი, შესრულების პრივილეგიების შეზღუდვა და სხვა. ისინი წარმოადგენს ანტივირუსული პროგრამული უზრუნველყოფის არსებით და განუყოფელ კომპონენტს. მათი ერთობლივი გამოყენება გვაძლევს საშუალებას გავზარდოთ თანამედროვე ანტივირუსული პროდუქტების ეფექტიანობა, სულ ახალ-ახალი მავნე პროგრამების წინააღმდეგ.

აქვე არ შეიძლება არ განვიხილოთ ერთ-ერთ მავნე პროგრამა სპამი (Spam), რომლის დანიშნულებაა კომერციული, პოლიტიკური, სოციალური თუ სხვა სახის რეკლამის (ინფორმაციის) გადაგზავნა მომხმარებლისათვის, რომლებსაც ამის სურვილი არა აქვთ. თუმცა უნდა აღინიშნოს, რომ ქვეყნების კანონმდებლობით ნებადართულია ზოგიერთი სახის ინფორმაციის მასიური გაგზავნა, მომხმარებლების ნებართვის გარეშე. მაგალითად ეს შეიძლება იყოს შეტყობინებები მომავალი სტიქიური უბედურებების, კატასტროფების, ასევე მოქალაქეთა მასობრივი მობილიზაციის შესახებ. ასეთი შეტყობინებები ცნობილია სპიმის (Spim) სახელწოდებით.

ინტერნეტ ქსელში მუდმივად ჩნდება სულ ახალახალი ვირუსები, რომელთა წინააღმდეგ იქმნება ანტივირუსული პროგრამები. რაღაც ყველაფრით სრულყოფილი ანტივირუსი, რომელიც გაანადგურებდა ყველა მავნე პროგრამას, ჯერჯერობით არ არსებობს და ალბათ უახლოეს მომავალშიც არ იარსებებს. ამიტომ, შეიძლება ვისაუბროთ მხოლოდ კარგ ანტივირუსულ პროგრამებზე. მათი რაოდენობა ამჟამად საკმაოდ დიდია. თითოეულ მათგანს აქვს როგორც დადებითი, ასევე უარყოფითი მხარეები. შეიძლება გამოვყოთ ის ძირითადი მახასიათებლები, რომლებითაც აღჭურვილი უნდა იყოს ხარისხიანი ანტივირუსული

პროგრამა. ეს მახასიათებლებია: სწრაფქმედება, თვითდაცვა, რუტკიტების აღმოჩენა, მკურნალობა. ერთ-ერთ მახასიათებლად ალბათ უნდა ვიგულისხმოთ აგრეთვე მათი ღირებულება.

ანტივირუსი თავის მუშაობის პროცესში იყენებს კომპიუტერის რესურსებს, რაც იწვევს მისი სწრაფქმედების შემცირებას. ამიტომ პროგრამამ ოპტიმალურად უნდა გამოიყენოს ეს რესურსები. გარდა ამისა, თითოეულმა ანტივირუსმა უნდა შეძლოს თავისი ფაილების, პროგრამების და სხვათა დაცვა. მან აგრეთვე უნდა შეძლოს ჯერ კიდევ უცნობი ვირუსული პროგრამების წინააღმდეგ ბრძოლა. ბრძოლის ეს მეთოდები სხვადასხვა ანტივირუსული პროგრამებისათვის შეიძლება სხვადასხვა იყოს. ანტივირუსულმა პროგრამამ უნდა უზრუნველყოს აგრეთვე დაცვა უახლესი მავნე პროგრამებისაგან, რადგან ყველაზე დიდი დანაკლისი მიიღება ამ ახალი ვირუსული პროგრამების მუშაობის შედეგად.

ყველა ანტივირუსულ პროგრამას გააჩნია თავისი დადებითი და უარყოფითი მხარეები. მიუხედავად ამისა, უმჯობესია დაცვისათვის შეირჩეს ერთი ანტივირუსული პროგრამა, ვიდრე რამდენიმე, რადგან ეს უკანასკნელი ხერხი ვერ გაზრდის უსაფრთხოებას. უფრო მეტიც, შეიძლება მივიღოთ სავალალო შედეგები.

შეიძლება დავახასიათოთ ზოგიერთი მათგანი. ანტივირუსი esetnod-ის ძირითადი უპირატესობაა სწრაფი მუშაობა და მინიმალური მოთხოვნილება სისტემის რესურსებზე, მაგრამ ვერ უმკლავდება აქტიურ ვირუსებს. ანტივირუსს Symantec გააჩნია უსაფრთხოების დიდი უნარი, კარგად იცავს თავს, შეუძლია უახლესი ანტივირუსების აღმოჩენა, განახლება ხდება საათში ერთხელ, უმკლავდება აქტიურ დაავადებებს. ანტივირუსს DrWeb გააჩნია კარგი ინტერფეისი, უმკლავდება პროგრამებს, აქვს კარგი დაცვის უნარი. ანტივირუსი Avast კარგად ებრძვის ვირუსებს, ტროიანებს, თავის ფაილებს იცავს მავნე კოდებისაგან, თუმცა ცუდად აღმოაჩენს უახლეს ვირუსებს. ანტივირუსი Avira არ მოითხოვს ბევრ რესურს, კარგად აღმოაჩენს საშიშროებას, თუმცა უჭირს უახლოესი საშიშროების აღმოჩენა. ანტივირუსი Comodo მუშაობს კარგად, იცავს თავის ფაილებს, კარგად აღმოაჩენს ვირუსებს, თუმცა, უჭირს აქტიური და ჯერ კიდევ უცნობი ვირუსების აღმოჩენა. ანტივირუს Mcafee-ს გააჩნია კარგი თავდაცვის უნარი, კარგად ებრძვის უახლეს და უცნობ ვირუსებს, მაგრამ უჭირს აქტიური ვირუსების განადგურება. ანტივირუსს Viruslab გააჩნია დაცვის თითქმის ყველა ფუნქცია, ახასიათებს კარგი სწრაფქმედება, მაგრამ ვერ ებრძვის აქტიურ დაავადებებს და უახლეს ვირუსებს.

დაცვის მეთოდებს შორის შეიძლება განვიხილოთ აგრეთვე ფაირვოლების დაყენება, პროგრამების მუდმივი განახლება. ფაირვოლების გვერდით გამოიყენება ისეთი ცნებები, როგორიცაა ბრანდმაიერები [4], ქსელთაშორისი ეკრანები და სხვა. ისინი გვაძლევენ საშუალებას ავიცილოთ ბოროტმოქმედთა არასანქცირებული შეტევები კომპიუტერში შესაღწევად. როგორც დაცვის სხვა მეთოდები და საშუალებები, ისინიც შეიძლება იყოს აპარატურული და პროგრამული. აპარატურული ფაირვოლი წარმოადგენს მოწყობილობას, რომელიც მიერთებულია კომპიუტერს, ხოლო პროგრამული – ეს არის პროგრამა, რომელიც დაყენებულია მომხმარებლის კომპიუტერზე.

შეიძლება ზოგადად დავახასიათოთ ფაირვოლები და გამოვყოთ მათი დადებითი და უარყოფითი მხარეები, რომლებიც გასათვალისწინებელი იქნება მათი დაყენებისას. პირველ რიგში იგი არ უნდა აფერხებდეს კომპიუტერის მუშაობას, თავსებადი იყოს ოპერაციულ სისტემასთან, დრაივერებთან, უნდა ხდებოდეს მათი მუდმივი განახლება.

მიღებული რჩევაა, რომ ფაირვოლის შეფასება არ მოხდეს მისი ღირებულებებით, ზომით, დიზაინით. ასევე არ უნდა მოხდეს სტანდარტული ფაირვოლების გამოყენება, რომლებიც შედიან ოპერაციული სისტემის შემადგენლობაში, რადგან მავნე პროგრამებს აქვთ შესაძლებლობა გათიშონ მათი ქმედითუნარიანობა. შეიძლება დავახასიათოთ ზოგიერთი მათგანი. ფაირვოლი petools იცავს კომპიუტერს ინტერნეტის საშიშროებისაგან, ბლოკირებას უკეთებს არასასურველ შეერთებებს. პერსონალური ფაირვოლი Agnitum ახორციელებს შემავალი და გამომავალი მონაცემების კონტროლს, საიმედოა. ფაირვოლი Comodo აკონტროლებს პროგრამის მუშაობას, აფრთხილებს მომხმარებლებს ყურადღება მიაქციოს წარმოქმნილ სიტუაციებს.

როცა საქმე ეხება ქსელის უსაფრთხოებას, უნდა გამოვიყენოთ ყველა რესურსი. ამიტომ ანტივირუსების, ფაირვოლების, ბრანდმაიერების, ქსელური ეკრანების გვერდით უნდა განვიხილოთ სხვა საშუალებებიც. ერთ-ერთ ასეთ საშუალებას წარმოადგენს ანონიმაიზერები. იგი არის დაცვის პროგრამა, რომლის დანიშნულებაა: მოწყობილობების; გამოყენებული ქსელური პროგრამების; ინტერნეტ ბრაუზერების; ინტერნეტ ქსელში მომხმარებლების შესახებ მონაცემების შენახვა. ჩვეულებრივ, ასეთი საშუალება არის ვებ-საიტი, ან სპეციალური პროგრამა.

ვებ-საიტი არის ჩვეულებრივი Web-გვერდი, რომელზეც განთავსებულია სპეციალური ფორმა, ინტერნეტ ქსელში აუცილებელი მისამართის შესაყვანად. მას შემდეგ, რაც ამ ფორმაში შეიტანება აუცილებელი მისამართი, გვერდი იწყებს შემოსული კითხვის დამუშავებას და მის გადაგზავნას საძებნ რესურსზე, ისე, რომ არ ხდება მომხმარებლის მიკითხვა უშუალოდ თვითონ საჭირო საიტზე. ამ მომენტში გამოიყენება ანონომაიზერი, რომელიც თავის სერვერზე გადაქაჩავს მისაკითხ გვერდს და აჩვენებს მომხმარებელს. ასეთი ანონომაიზერების გამოყენება არ მოთხოვს განსაკუთრებულ ცოდნას პროგრამულ უზრუნველყოფაში, ასევე საჭირო არ არის მომხმარებლის მიერ კომპიუტერის გადატვირთვა და საძიებლებში ძიება, რითაც იზოგება მომხმარებლის მუშაობის დრო.

ანონომაიზერებს ჰყავთ მომხმარებლის ფართო სპექტრი. თუმცა იგი ვერ უზრუნველყოფს კერძო ინფორმაციის დაცვას, მომხმარებელსა და სერვერს შორის, ამიტომ არ არის რეკომენდირებული მისი გამოყენება საბანკო სისტემებში, საფინანსო სამსახურებში. ამას გარდა, მისი გამოყენებისას საჭიროა სიფრთხილე, რადგან ქსელში შეიძლება იყოს ე. წ. „შავი“, ანონიმური საიტები, რომელთა მიზანია, არა ზემოთ აღწერილი ფუნქციების შესრულება, არამედ მომხმარებელთა შეტანილი მონაცემების ჩაჭერა და მათი სხვა მიზნებით გამოყენება. ანონომაიზერების მოძიება შეიძლება ქსელში (luckymicro, beau, vrmp3, noblockagain და სხვა).

მონაცემთა დაცვის საშუალებებს ასევე მიეკუთვნება ქსელთაშორისი, ან ქსელური ეკრანები. იგი წარმოადგენს აპარატურულ და პროგრამულ საშუალებებს, რომელიც, მოცემული წესების შესაბამისად ახორციელებს მასში გამავალი ქსელური პაკეტების კონტროლს და ფილტრაციას. ეკრანი იცავს კომპიუტერულ ქსელს, ან მის ცალკეულ ნაწილებს არასანქციონირებული შეღწევისაგან. ფაქტობრივად ისინი წარმოადგენენ ფილტრებს, რადგან არ ატარებენ პაკეტებს, რომლებიც ვერ აკმაყოფილებენ კონფიგურაციით განსაზღვრულ კრიტერიუმებს. ზოგიერთი ქსელური ეკრანი იძლევა საშუალებას, განვახორციელოთ მისამართების ტრანსლაცია, რომელიც მდგომარეობს შიდაქსელური მიმართვების დინამიურ შეცვლაში ქსელის გარეთა მისამართებით.

არსებობს ქსელური ეკრანების სახესხვაობები, რომელთა შერჩევა ხორციელდება კრიტერიუმების მიხედვით. ამის შესაბამისად, ეკრანები შეიძლება იყოს ქსელური და პერსონალური, ქსელურ დონეზე და სეანსების დონეზე, სტატიკური და დინამიური და სხვა. ეკრანების გამოყენების უარყოფით მხარედ ითვლება ის, რომ იგი ამცირებს ქსელის გამტარუნარიანობას, რადგან ფილტრაცია მოითხოვს გარკვეულ დროს. ამას გარდა საჭირო ხდება დამატებითი რესურსების გამოყენება, მაგალითად, ანტივირუსების, ამიტომ იგიც არ წარმოადგენს სრულყოფილს.

შევეხოთ დაცვის კიდევ ერთ საშუალებას – მარშრუტიზატორს [5]. იგი წარმოადგენს ქსელურ მოწყობილობას, რომელიც ქსელის ტოპოლოგიის შესახებ ინფორმაციისა და განსაზღვრული წესების საფუძველზე ღებულობს გადაწყვეტილებას, ქსელის სხვადასხვა სეგმენტებს შორის ქსელური დონის პაკეტების გადაცემის შესახებ,. არსებობს სხვადასხვა სახის მარშრუტიზატორები; მაგისტრალური არხებისათვის (cisco 7600 series router i. p. g.), ჩადგმული კომუტატორებით (cisco 771oco), Linkus კომპანიის (Router ipg) და სხვა.

მონაცემთა პაკეტების გადაცემის გზების და უმოკლესი მარშრუტების დადგენა ხორციელდება ცხრილების საშუალებებით, რომელიც გამოდის ეკრანზე და უნდა შეივსოს, ან განახლდეს ხელით, ან ავტომატურად. მარშრუტიზატორი, დანიშნულების ქსელებამდე აგებს ოპტიმალურ გზებს. ეს აგება ხორციელდება ისეთი კრიტერიუმებით, როგორიცაა: შუალედური კვანძების რაოდენობა, არხების გამტარუნარიანობა, მონაცემთა გადაცემის დრო და სხვა.

მარშრუტიზატორის გამოყენების უარყოფით მხარეს წარმოადგენს ის, რომ მოწყობილობებზე იზრდება დატვირთვა, რაც ზრდის ქსელის არასტაბილურობას. ეს კი, თავის მხრივ, იწვევს ქსელის მუშაობის დარღვევას და მონაცემების დაკარგვას. მარშრუტიზატორი შეიძლება იყოს როგორც დამოუკიდებელი სპეციალიზებული მოწყობილობა, ისე ჩვეულებრივი კომპიუტერი, რომელიც განახორციელებს მარშრუტიზატორის ფუნქციას. ამისათვის იგი აღჭურვილ უნდა იყოს სპეციალური პროგრამული უზრუნველყოფის პაკეტით (მაგ., Quagga Routing Suite).

3. დასკვნა

ინფორმაციული შეტევების, უსაფრთხოების და დაცვის საშუალებების ანალიზის საფუძველზე შეიძლება დავასკვნათ, რომ მართვის სისტემებში უამრავადაა სუსტი ადგილები, რომლებითაც სარგებლობენ ბოროტმოქმედნი და სხვადასხვა გზით ახორციელებენ მათზე შეტევას. ეს, თავის მხრივ, იწვევს დაცვის სხვადასხვა საშუალებების შემუშავებას, დასაცავი ობიექტების უსაფრთხოების უზრუნველყოფის მიზნით, არსებობს უამრავი ასეთი დაცვის საშუალება, მაგრამ თითოეულ მათგანს აქვს როგორც დადებითი, ისე უარყოფითი მხარეები. ისე, რომ არც ერთი საშუალება არ წარმოადგენს პანაცეას. დაცვის საშუალებების შერჩევა უნდა მოხდეს ზემოთ განხილული კრიტერიუმების საფუძველზე, იმ მიზნის გათვალისწინებით, რომლის მისაღწევადაც იგი გამოიყენება.

ლიტერატურა:

1. შონია ო., შეროზია თ.. ინფორმაციული ტექნოლოგიები და უსაფრთხოება. თბ., ტექნიკური უნივერსიტეტი, 2008
2. შეროზია თ., შონია ო., ოდიშარია კ., ტურაშვილი ი.. კრიპტოგრაფიისა და კრიპტოანალიზის მართვის ავტომატიზებული სისტემა. შრომების კრებული „მართვის ავტომატიზებული სისტემები“. №2(29). ტექნიკური უნივერსიტეტი, თბ., 2010, გვ. 71-77
3. Компьютерные вирусы / PCDays. http://www.pcdays.ru/articles/security/ /kompyuternye-virusy
4. Челмен Д.В., Фокс Э. Брандмайер Cjsco Secyre PIX. М. „Вильямс“, 2005
5. Леинванд А.., Пинеки Б. Конфигурирование маршрутизаторов. М., „Вильямс“, 2004.

THE MODERN FORMS OF INFORMATIONAL ATTACK, SECURITY AND SAFETY

Sherozia T., Nareshelashvili G., Shonia A.
Georgian Technical University

Summary

In parallel with the history of mankind has developed history of attacks, exploits, security and protection. Over time it becomes more and more objects of protection. There were critical points of protection in the system, which includes these objects. Offenders using a lot of methods for attacks on these objects. The developed and the methods of the system thus ensuring its security. As a result of computer technics development appears the apparatus-trading methods and also methods of informational attacks and it's security. Beneath them are viruses, spyware, Web bugs, spams. Methods of protection include cryptographic methods, antivirus, firewall, brain Maier, anonomizators, firewalls, routers, also showing their advantages and disadvantages, offers recommendations on their choice.

СОВРЕМЕННЫЕ СПОСОБЫ ИНФОРМАЦИОННОЙ АТАКИ, БЕЗОПАСНОСТИ И ЗАЩИТЫ

Шерозия Т. А., Нарешелашвили Г.Г., Шония, А.Б.
Грузинский Технический университет

Резюме

Параллельно с историей человечества создавалась и развивалась история нападения, атаки, безопасности и защиты. Со временем создавалось все больше и больше объектов охраны. Появлялись слабые точки в системе охраны, куда входили эти объекты. Участились нападения нарушителей на эти объекты с применением различных методов. В связи с этим развивались и методы охраны системы, что обеспечивало ее безопасность. В результате развития компьютерной техники появились аппаратно-програмные методы и средства информационной атаки и защиты. Под ними рассматриваются вирусы, программы шпионы, сетевые жучки, спамы. Под методами защиты подразумевают методы криптографии, антивирусы, фаирволы, брандмауэры, сетевые экраны, анономизаторы, маршрутизаторы, показаны их положительные и отрицательные стороны, даны рекомендации по их выбору.