საქართველოს ტექნიკური უნივერსიტეტი

ხელნაწერის უფლებით

ლუკა შონია

კორპორაციული ქსელის მრავალდონიანი უსაფრთხოების უზრუნველყოფის მეთოდების და საშუალებების კვლევა

სადოქტორო პროგრამა: ინფორმატიკა

შიფრი - 0401

დოქტორის აკადემიური ხარისხის მოსაპოვებლად

წარდგენილი დისერტაციის

ავტორეფერატი

თბილისი

2020

საავტორო უფლება © 2020 წელი ლუკა შონია

სამუშაო შესრულებულია საქართველოს ტექნიკური უნივერსიტეტში
ინფორმატიკის და მართვის სისტემების ფაკულტეტი
მართვის ავტომატიზებული სისტემების დეპარტამენტი

ხელმძღვანელი: პროფესორი ოთარ შონია

რეცენზენტები: ----------

დაცვა შედგება ---------- წლის ”------” ----------, --------- საათზე, საქართველოს ტექნიკური უნივერსიტეტის ინფორმატიკისა და მართვის სისტემების ფაკულტეტის საუნივერსიტეტო სადისერტაციო საბჭოს სხდომაზე, კორპუსი ----------, აუდიტორია ----------

მისამართი: 0175, თბილისი, კოსტავას 77.

დისერტაციის გაცნობა შეიძლება სტუ-ს ბიბლიოთეკაში,
ხოლო ავტორეფერატის - ფაკულტეტის ვებგვერდზე

საუნივერსიტეტო სადისერტაციო საბჭოს მდივანი ----------

ნაშრომის ზოგადი დახასიათება

თემის აქტუალობა. ინფორმაციული ტექნოლოგიების საყოველთაოდ გავრცელება-დანერგვამ, საწარმოების, ბიზნეს პროცესების, სახელმწიფო მართვის პროცესების ავტომატიზებამ, ელექტრონული ურთიერთობათა მოდელების საყოველთაო აღიარება-გამოყენებამ წინა პლანზე წამოწია ინფორმაციის, როგორც საკუთრების უფლების ობიექტის სამართლებრივი დაცვის აუცილებლობა. თავის მხრივ მოყვანილია მაგალითები, რაც აშკარად მიგვანიშნებს ამ ამოცანის პრობლემატურობაზე. ამის უმთავრესი მიზეზი კი, მდგომარეობს, პირველ რიგში, ინფორმაციის როგორც საკუთრების უფლების ობიექტის თავისებურებაში - ის საკუთრების უფლების ტრადიციული მატერიალური ობიექტისგან განსხვავებით ადვილად კოპირებადია, ადვილად გადაეცემა სხვა საკუთრების უფლების მქონე პირს საკუთრების უფლების რაიმე აშკარა (შესამჩნევი) დარღვევის გარეშე. გარდა ამისა ინფორმაციის კოპირებისა და გადაცემის საფრთხეს ამწვავებს ის გარემოება, რომ ის ინახება და მუშავდება დიდი ოდენობის სუბიექტების მისაწვდომ გარემოში, რომლებიც არ არიან ამ ინფორმაციის საკუთრების უფლების მატარებლები. ესაა, მაგალითად, ფართო სპექტრი საყოველთაოდ გავრცელებული ავტომატიზებული სისტემებისა, დაწყებული ცალკეული ადამიანების კომპიუტერული სამუშაო ადგილებით, დამთავრებული კორპორატიული ავტომატიზებული სისტემებით, ელექტრონული ხელისუფლებით და ინტერნეტით.

კომპიუტერული ქსელებისა და პროგრამირების მეთოდების განვითარებასთან არის დაკავშირებული კორპორაციული ქსელების უსაფრთხოების ამოცანა, რომელიც მოითხოვს უსაფრთხოების მხარდამჭერი ავტომატიზებული სისტემის შექმნას. აღნიშნული პრობლემა წარმოადგენს გამოკვლევის აქტუალურ სფეროს და დღესდღეობითაც აქტიურად მიმდინარეობს მუშაობა ამ პრობლემის გადასაჭრელად.

ბოლო პერიოდში კორპორაციულ ქსელებში უსაფრთხოება და მომსახურების ხარისხი უაღრესად მნიშვნელოვანი და აქტიური კვლევის

საგანი გახდა, რის მიზეზსაც მონაცემთა პაკეტების გადაცემის მხარდაჭერის მზარდი მოთხოვნა წარმოადგენს. ადეკვატური უსაფრთხოების გარეშე ორგანიზაციები თავს აარიდებენ კორპორაციული ქსელების გამოყენებას. უსაფრთხოების საკითხები კორპორაციულ ქსელებში მნიშვნელოვან დაბრკოლებას წარმოადგენს ასეთი ქსელების ფართო ადაპტირებისთვის. შესაბამისად, მსგავსი კორპორაციული ქსელების უსაფრთხოება მნიშვნელოვანი სფეროა, რაც რეაგირებას მოითხოვს, თუკი ასეთი ქსელები ფართოდ იქნება გამოყენებული. აუცილებელია, რომ აღნიშნული სფეროს მკვლევარებმა მოახდინონ ღია პრობლემების იდენტიფიცირება და უზრუნველყონ შესაბამისი გადაწყვეტილებები ამ პრობლემებთან მიმართებით თითოეული ასეთი მცდელობა კორპორაციულ ქსელს ოდნავ უფრო უსაფრთხოს ხდის.

ამასთან დაკავშირებით, წინამდებარე ნაშრომში მოყვანილია უსაფრთხოების ფუნდამენტური პრინციპები, ისევე, როგორც ღია პრობლემები. განხილულია კორპორაციული ქსელების უსაფრთხოების საკითხები. უნდა აღინიშნოს, რომ კორპორაციული ქსელების მარშრუტიზაციის პროტოკოლები სპეციფიკაციებში არ განსაზღვრავს რაიმე სახის პრევენციულ ღონისძიებებს ან უსაფრთხოების მექანიზმებს. ამდენად, კორპორაციული ქსელების მარშრუტიზაციის პროტოკოლების უსაფრთხოება გადაუდებელ აუცილებლობად იქცა ქსელის გაშვების სტიმულირებისა და გამოყენების სფეროს გაფართოებისთვის. შესაბამისად, წინამდებარე ნაშრომში შემოთავაზებულია და განსაზღვრული განსხვავებული გადაწყვეტილებები და კონცეფციები უსაფრთხოების მიმართულებით. ძირითადი ყურადღება თავდაპირველად გამახვილებულია საწყის ნაბიჯზე – მარშრუტიზაციის პროტოკოლების ხარვეზების შესწავლასა და ანალიზზე.

კვლევის მიზანი: სადისერტაციო ნაშრომის ძირითად მიზანს წარმოადგენს ის, რომ შემუშავდეს მთელი რიგი ღონისძიებები, რომლებიც აამაღლებს კორპორაციული ქსელების უსაფრთხოებას და მისი საშუალებით

მოხდება მოცილებული სამუშაო ადგილების მართვა, აგრეთვე უსაფრთხოების სისტემის თვისებების გამოკვლევისათვის ფორმალური მეთოდების დამუშავება და ამის საფუძველზე სისტემის პრაქტიკული რეალიზაცია.

კვლევის ობიექტი: კვლევის ობიექტს წარმოადგენს კორპორაციული სისტემები, რომელთა შექმნა განვითარება, არსებობა დამოკიდებულია თანამედროვე ინფორმაციული ტექნოლოგიების, საერთო სისტემური კანონზომიერებების გათვალისწინებით, დანერგვასა და ფუნქციონირების პროცესებში წარმოქმნილი ან შესაძლო რისკების მართვა, ესაა როგორც ურთულესი სისტემის, ის შემადგენელი ძირითადი საყრდენი ელემენტები, რომელთა ეფექტური ფუნქციონირება თვით კორპორაციული სისტემების მდგრადი განვითარების აუცილებელი პირობაა.

კვლევის საგანია კორპორაციული სისტემების ინფორმაციული უსაფრთხოების პრობლემების, მათი გადაწყვეტის მეთოდების და საშუალებების კვლევა, დასმული საწყისი მიზნის რეალურობის დასაბუთების, შექმნა-გაშვების და ფუნქციონირების, ამ დროს არსებული, მოსალოდნელი რისკების შეფასების, მართვისა და კონტროლის, ავტომატიზაციისა და ინფორმაციული უსაფრთხოების უზრუნველყოფის პროცესები, მათი წარმატებით გადაწყვეტის სამეცნიერო-პრაქტიკული პირობები.

კვლევის ამოცანა: ზემოთაღნიშნული მიზნიდან გამომდინარე, ნაშრომში ყურადღება ექცევა ისეთი ამოცანების გადაჭრას, როგორიცაა: კორპორაციულ ქსელებში ინფორმაციული პაკეტების მარშრუტიზაციის უსაფრთხოების ამაღლება; დაშიფვრისა და აუტენტიფიკაციის მექანიზმების გამკაცრება; კორპორაციულ ქსელებში სხვადასხვა კავშირგაბმულობის არხის ანალიზი და უსაფრთხოების ამაღლების მიზნით ახალი მეთოდების დამუშავება; მოცილებული სამუშაო ადგილების (ადგილობრივი თუ რეგიონული ოფისები) ადმინისტრირება და მართვა კორპორაციული ქსელების გამოყენებით; სისტემაში გამოყენებული აპარატურული

მოწყობილობების პარამეტრების დისტანციური მართვა და ადმინისტრირება; სხვადასხვა ადგილობრივ თუ მოცილებულ ობიექტებზე წვდომის გრაფიკების დამუშავება და ანალიზი (ერთიან სისტემაში მონაწილე მხარეების დონეზე); დოკუმენტბრუნვის სისტემის აგება; თითოეული პერსონალის დონეზე ისტორიების შექმნა და მათი ანალიზი; ერთიანი ინფორმაციული არქივის შექმნა და მის საფუძველზე სტატისტიკური ანალიზის ჩატარება ცხრილებისა და დიაგრამების სახით; ავტომატიზებული სისტემის აგება და რეალიზაცია.

კვლევის მეთოდები: კორპორაციული ქსელების უსაფრთხოების მხარდამჭერი ავტომატიზებული სისტემის დამუშავებისათვის გამოყენებულია ინფორმაციის დაცვის კრიპტოგრაფიული, გამოთვლითი მათემატიკისა და ავტომატიზებული დაპროექტების მეთოდები.

ნაშრომის ძირითადი შედეგი და მეცნიერული სიახლე: კვლევის შედეგად:

- განხილულია VPN ქსელში უსაფრთხოების უზრუნველსაყოფად არსებული კრიპტოგრაფიული მეთოდები, მოყვანილია მათი დადებითი და უარყოფითი მხარეები და არსებული პრობლემებიდან გამომდინარე შემუშავებულია სიმბოლოების დაშიფვრის კომბინირებული მეთოდი;

- დეტალურად განხილულია უსადენო ლოკალური ქსელის კომპონენტები და სისტემები, გაანალიზებულია ასეთი ქსელის გამოყენებასთან დაკავშირებული საფრთხეების სხვადასხვა ფორმები და აღნიშნული საფრთხეების აღმოსაფხვრელად შემოთავაზებულია ახალი მეთოდები, რომელიც უზრუნველყოფს ინფორმაციული პაკეტების მარშრუტიზაციის უსაფრთხოების ამაღლებას;

- უსაფრთხოების მხარდამჭერი ავტომატიზებული სისტემის ძირითადი ამოცანების საფუძველზე განისაზღვრა და ჩამოყალიბებული იქნა სისტემის ალგორითმები, დამუშავებული იქნა ინფორმაციული უზრუნველყოფა, დიალოგური პროცედურები და შეიქმნა ავტომატიზებული სისტემის პროგრამული კომპლექსი;

- დამუშავებული მეთოდებისა და პროგრამული კომპლექსის საფუძველზე რეალიზებულია უსადენო ქსელების უსაფრთხოების მხარდამჭერი ავტომატიზებული სისტემა.

ნაშრომის პრაქტიკული მნიშვნელობა: სადისერტაციო ნაშრომში მიღებული შედეგების პრაქტიკული ღირებულება მდგომარეობს იმაში, რომ მისი გამოყენება ბევრად შეუწყობს ხელს სხვადასხვა ობიექტების ინფორმაციულ უსაფრთხოებას.

სადისერტაციო ნაშრომის სტრუქტურა და მოცულობა: სადისერტაციო ნაშრომი შედგება შესავლის, სამი თავის, დასკვნისა და გამოყენებული ლიტერატურის სიისგან. საერთო მოცულობა შეადგენს 122 გვერდს.

ნაშრომის შინაარსი

შესავალში მოცემულია პრობლემის საერთო დახასიათება - აქტუალურობა. მოყვანილია კორპორაციულ ქსელებთან დაკავშირებული უსაფრთხოების საკითხები, ფორმულირებულია დისერტაციის ძირითადი მიზნები და ამოცანები.

პირველ თავში წარმოდგენილია ძირითადი ცნობები კორპორაციული ქსელების ტექნოლოგიებისა და კომპონენტების შესახებ. მოყვანილია ინფორმაციული უსაფრთხოების უზრუნველყოფასთან დაკავშირებული რისკების ზოგადი დახასიათება.

მოკლედ განხილულია უსადენო ქსელების ყველა ნაირსახეობა, აღწერილია მათი სტრუქტურის თავისებურებები და გამოყენების მეთოდები. მოყვანილია უსადენო ქსელებთან დაკავშირებული უსაფრთხოების საკითხები და ჩატარებულია მათი ანალიზი განხილულია უსადენო ქსელების უსაფრთხოების პრობლემის აქტუალობა და მათი თავისებურებანი. აღწერილია შესაძლო საფრთხეები და ამავე თავში დახასიათებულია ის თავადასხმები, რომლებსაც შეიძლება ადგილი ჰქონდეს უსადენო ქსელებში. დეტალურად წარმოდგენილია კორპორაციული საინფორმაციო სისტემების ინფორმაციული

უსაფრთხოების უზრუნველყოფიდან მომდინარე საფრთხეები. მოყვანილია უსაფრთხოების არსებული სისტემები და გაკეთებულია მათი ანალიზი. ჩამოყალიბებულია კორპორაციული საინფორმაციო სისტემების უსაფრთხოების უზრუნველყოფის ავტომატიზებული სისტემის ძირითადი ამოცანები. მოყვანილია კორპორაციული ქსელების გამოყენების სხვადასხვა სფერო.

მეორე თავში დამუშავებულია კორპორაციული საინფორმაციო სისტემების უსაფრთხოების უზრუნველყოფის მეთოდები თავიანთი ფუნქციონალური დანიშნულებებით.

ინფორმაციული ტექნოლოგიები გადამწყვეტ როლს თამაშობენ ნებისმიერი კომპანიის ეფექტურად ფუნქციონირებასა და მართვაში. როცა ოპერატიულად ხელმისაწვდომია საჭირო ინფორმაცია _ ტექნოლოგიური, საკადრო, მარკეტინგული ან ფინანსური, შესაძლებელია სწორად შეფასდეს მიმდინარე სიტუაცია, მიღებული იქნას დროული გადაწყვეტილება. ამავდროულად, ინფორმაცია ხელმისაწვდომი უნდა იყოს მხოლოდ მათთვის, ვისთვისაც ის განკუთვნილია და დაფარული სხვა უცხო პირთათვის.

მას შემდეგ, რაც სხვადასხვა კომპანიებმა და ორგანიზაციებმა თავიანთი მუშაობის სხვადასხვა სფეროში აქტიურად დაიწყეს კომპიუტერების გამოყენება, გაჩნდა მოთხოვნილება იმისა, რომ ეს კომპიუტერები გაერთიანებული ყოფილიყვნენ ერთ საერთო ქსელში, მონაცემთა სწრაფი გადაცემისთვის და ეფექტური ურთიერთქმედებისთვის. ამასთან, ეს კავშირი აუცილებლად უნდა ყოფილიყო საიმედო და დაცული.

ზემოთაღნიშნულიდან გამომდინარე, სხვადასხვა ორგანიზაციები და ბანკები დაინტერესდნენ Internet არხების გამოყენების შესაძლებლობებით, კრიტიკული კომერციული და სამართავი ინფორმაციების გადაცემისთვის. თუმცა, Internet აგებულების პრინციპები ბოროტმოქმედებს შესაძლებლობას უქმნის, მოიპარონ და განზრახ დაამახინჯონ ინფორმაცია. კორპორატიული და საუწყებო ქსელები, რომლებიც დაფუძნებულია TCP/IP პროტოკოლების

ბაზაზე და აგებულია სტანდარტულ Internet-დანართებზე (e-mail, Web, FTP), უცხო პირთა შეჭრისგან გარანტირებული არ არის.

ბიზნესსა თუ საბანკო სფეროში ქსელური იერიშების წინააღმდეგ ეფექტურად საბრძოლველად და აქტიური და უსაფრთხო გამოყენების შესაძლებლობის უზრუნველსაყოფად, 1990 წლების დასაწყისში შეიქმნა და აქტიურად ვითარდება ვირტუალური კერძო ქსელების აგების კონცეფცია _ VPN (Virtual Private Network). სიტყვა „ვირტუალური“ VPN ტერმინში ჩართულია იმისათვის, რათა ხაზი გაესვას იმას, რომ ორ კვანძს შორის შეერთება განხილული უნდა იყოს ისე, როგორც დროებითი შეერთება, რამდენადაც ის არ არის მუდმივი (მყარი) შეერთება და არსებობს მხოლოდ ღია ქსელში ინფორმაციული ნაკადების გადაცემის დროს.

ვირტუალურად დაცული ქსელების VPN აგების კონცეფციას საფუძვლად უდევს საკმაოდ მარტივი იდეა: თუ გლობალურ ქსელში არის ორი კვანძი, რომელთაც უნდათ ინფორმაციის გაცვლა, მაშინ ამ ორ კვანძს შორის აუცილებელია აიგოს ვირტუალურად დაცული გვირაბი, ღია ქსელით გადაცემული ინფორმაციის კონფიდენციალობისა და დაუზიანებლობის უზრუნველსაყოფად. ამ გვირაბთან ხელმისაწვდომობა უნდა იყოს ძალზე გართულებული, ყველა შესაძლო აქტიური და პასიური გარე დამკვირვე-ბელთათვის.

როგორც აღვნიშნეთ, ორ მოცილებულ კომპიუტერს შორის, რომელიც იყენებს გლობალური ქსელის - ინტერნეტის ინფრასტრუქტურას, უსაფრ-თხო კავშირის არხის შექმნისთვის, ვირტუალური კერძო ქსელების VPN (Virtual Private Network) აგების ტექნოლოგია დღეისათვის წარმოადგენს ერთ-ერთ ყველაზე ოპტიმალურ ვარიანტს. წამოჭრილი ამოცანა ძალზედ მნიშვნელოვანია, ვინაიდან საიმედო კავშირი, სადაც შესაძებელია გადაიცეს კონფიდენციალური ინფორმაცია, უბრალოდ აუცილებელია ადამიანის მოღვაწეობის უამრავ სფეროში, მაგალითად, საბანკო საქმეში, ელექტრონულ კომერციაში და სხვა. აქედან გამომდინარე, ვირტუალური კერძო ქსელები ძალზედ მოსახერხებელია აღნიშნული ამოცანის

გადასაჭრელლად და ადამიანების უმრავლესობა გლობალურ ქსელში სხვადასხვა კავშირების დასამყარებლად VPN ტექნოლოგიას მიიჩნევს ერთ-ერთ ყველაზე მძლავრ და მოსახერხებელ საშუალებად. თუმცა, საქმე მთლად ასე მარტივად არ წარმოგვიდგება. ვირტუალურ კერძო ქსელებს გააჩნიათ თავიანთი ნაკლოვანებები და სუსტი მხარეები.

ვირტუალური კერძო ქსელების ტექნოლოგია აგებულია კრიპტო-გრაფიული მეთოდების გამოყენებაზე. კერძოდ, ყველა ინფორმაცია, რომელიც მიედინება დაცული კავშირის არხში, იმყოფება დაშიფრულ მდგომარეობაში. აქედან გამომდინარე, VPN-ის საფუძველს წარმოადგენს კრიპტოგრაფია და მის არეალში აგრეთვე მოქმედებს ზოგიერთი დამატებითი მექანიზმები, როგორებიცაა, მაგალითად მომხმარებლების აუტენტიფიკაცია, მონაცემთა მთლიანობის კონტროლი და სხვა. თუმცა, კრიპტოგრაფიულ მეთოდებს გააჩნიათ თავიანთი სუსტი ადგილები.

ნებისმიერი კრიპტოგრაფიული მეთოდის გამოყენების საიმედოობა დაფუძნებულია მასში გამოყენებული დაშიფვრის ალგორითმზე. და, რა თქმა უნდა, მონაცემების სუსტი დაშიფვრა ბოროტგანმზრახველს საშუალებას აძლევს ადვილად მოიპოვოს წვდომა მისთვის სასურველ ინფორმაციაზე. ბუნებრივია, ჩნდება კითხვა, თუ რომელი კრიპტოგრაფიული მეთოდი უნდა იქნას გამოყენებული მონაცემების უსაფრთხოებისთვის.

დღეისათვის გამოიყენება ღია და დახურული კრიპტოგრაფიული ალგორითმები. ღია ალგორითმების ჯგუფს მიეკუთვნება ისეთი ცნობილი ტექნოლოგიები, როგორებიცაა: DES (Data Encryption Standard), TripleDES (Triple Data Encryption Algorithm), RSA (Rivest, Shamir and Adleman), AES (Advanced Encryption Standard) და სხვა. ისინი გაერთიანებულნი არიან სხვადასხვა ქვეყნის ნაციონალურ სტანდარტებში. დახურული კრიპტოგრაფიული ალგორითმები მუშავდება სხვადასხვა კომპანიის მიერ და გამოიიყენება თავიანთ საკუთრებაში.

ინფორმაციის დაშიფვრისთვის გამოიყენება კრიპტოგრაფიული გასაღები და დიდი მნიშვნელობა ენიჭება დაშიფვრის მექანიზმს და გასაღების სიგრძეს. ვინაიდან, რაც უფრო რთულია დაშიფვრის მექანიზმი და რაც უფრო დიდია გასაღების სიგრძე, მით უფრო გაუჭირდება ბოროტგანმზრახველს მისი ამოცნობა.

ყველა ზემოთ განხილული არსებული თუ აქამდე შემოთავაზებული კრიპტოგრაფიული ტექნოლოგია დაფუძნებულია მატრიცული მეთოდების გამოყენებაზე. რა თქმა უნდა, რაც უფრო გართულებულია მონაცემების დაშიფვრის მექანიზმი, მით უფრო გაუჭირდება ბოროტგანმზრახველს მისი გაშიფვრა. თუმცა, ამასთან ჩნდება ახალი პორბლემა, ეს არის მონაცემების გადაცემის სიჩქარე. დაშიფვრის მექანიზმის გართულებას მოსდევს მონაცემების გადაცემის სიჩქარის შემცირება, მით უმეტეს მაშინ, როდესაც მომხმარებელს უწევს მუშაობა განაწილებულ მონაცემთა ბაზების მართვის სისტემასთან. მონაცემთა ბაზაში ჩანაწერების რაოდენობის გაზრდა იწვევს მომხმარებლის მიერ მოცილებული სამუშაო ადგილიდან მონაცემთა წამოღების სიჩქარის ვარდნას. მონაცემთა ბაზების ოპტიმიზაციის პრობლემა დღეისათვის წარმოადგენს ერთ-ერთ საპრობლემო სფეროს და დღეისათვის აქტიურად მიმდინარეობს მუშაობა ამ პრობლემის აღმოსაფხვრელად. აქედან გამომდინარე, უნდა შემუშავდეს ისეთი დაშიფვრის მექანიზმი, რომელიც თავისი თვისებებით იქნება მარტივი, დიდ გამოთვლით პროცესებთან არ იქნება დაკავშირებული და, რაღა თქმა უნდა, გარეშე უცხო პირისთვის მისი ამოცნობის ალბათობა იქნება ძალზე მცირე.

არსებულ დაშიფვრის მეთოდებს გააჩნიათ კიდევ ერთი პრობლემა. დაშიფვრის გასაღები უმეტესად არ არის ცვალებადი, ან თუ არის იშვიათად, რაც ბოროტგანმზრახველს ხელს უწყობს გარკვეული დროის განმავლობაში გაშიფროს იგი. ამიტომ, სასურველია სისტემაში შემოღებულ იქნას დამატებითი პარამეტრები (კოეფიციენტები), რომლებიც გასაღებს გახდის ცვალებადს. კერძოდ, სისტემაში მომხმარებლის

ყოველი ავტორიზაციის დროს დაშიფრვისა და ამოშიფვრის გასაღები იქნება უნიკალური (ანუ არასდროს განმეორდება) და შეუძლებელი იქნება მისი გატეხვა.

ზემოთ აღნიშნული პრობლემებიდან გამომდინარე, შემუშავებულია სიმბოლოების დაშიფვრის კომბინირებული მეთოდი. სიმბოლოების დაშიფვრა და მისი ამოცნობა, თავისი თვისებებიდან გამომდინარე, შეიცავს განსაკუთრებულ პრობლემებს, რომელთა გადაწყვეტაც წარმოადგენს უსაფრთხოების ავტომატიზებული სისტემის აგების აუცილებელ პირობას. სიმბოლოების დაშიფვრის კომბინირებული მეთოდი მოიცავს შემდეგ ეტაპებს:

1) მომხმარებლის მიერ შეტანილი პაროლის დაშლა სიმბოლოებად;

2) თითოეული სიმბოლოს გადაყვანა ASCII(decimal) კოდირებაში და მათი კოდების განსაზღვრა;

3) მიღებული კოდებით სპეციალური ოპერაციის დახმარებით დამატებითი სიმბოლოების განსაზღვრა სისტემაში დაყენებული პარამეტრის მიხედვით;

4) სიმბოლოების და დამატებითი სიმბოლოების გაერთიანება და მათი სიტყვებად დაშლა (ჯგუფების შექმნა) სისტემაში დაყენებული პარამეტრის მიხედვით;

5) თითოეული ჯგუფის სიმბოლოებისთვის ASCII(decimal) კოდირებაში ხდება მათი შესაბამისი კოდების განსაზღვრა;

6) სპეციალური ოპერაციის დახმარებით მიღებული კოდების რიცხობრივი მნიშვნელობა გარდაიქმნება სხვა რიცხობრივ მნიშვნელობად და მიიღება ახალი კოდების სიმრავლე;

7) მიღებული კოდების სიმრავლისაგან მიიღება სპეციალური სიმბოლოებისაგან შემდგარი ჯგუფები;

8) მიღებული ჯგუფების გაერთიანებით მიიღება სპეციალური სიმბოლოების ერთობლიობისგან შემდგარი დაშიფრული ინფორმაცია.

სიმბოლოების დაშიფვრის კომბინირებული მეთოდის ეტაპები თავისი ფუნქციონალური დანიშნულებებით შეიძლება დახასიათდეს შემდეგნაირად:

პირველ ეტაპზე მომხმარებლის მიერ შეტანილი პაროლი იწერება სპეციალურ მასივში, სადაც განსაზღვრულია სიტყვის დასაწყისი და დასასრული. აგრეთვე, ხდება სიტყვის დაშლა სიმბოლოებად და ცალკეული სიმბოლოსთვის განსაზღვრულია მისი ინდექსი.

მე-2 ეტაპზე თითოეული სიმბოლო განიხილება ASCII(decimal) კოდირებაში და მათთთვის განისაზღვრება კოდები, რომლებიც იმახსოვრება სპეციალურ ცვლადებში;

მე-3 ეტაპზე ინფორმაციის უსაფრთხოება ბევრად არის დამოკიდებული მომხმარებლებზე. მაგალითად, მომხმარებელმა შეიძლება აირჩიოს ძალიან ადვილი პაროლი, რომელიც ამოსაცნობად მარტივი იქნება უცხო პირისთვის. აქედან გამომდინარე, აუცილებელია ავტომატიზებულად მოხდეს მისი „გართულება“. მეორე ეტაპზე მიღებული კოდებით სპეციალური ოპერაციის დახმარებით სისტემაში დაყენებული პარამეტრის მიხედვით განისაზღვრება მოდიფიცირებული კოდები, რომლებისგანაც მიიღება დამატებითი სიმბოლოები.

მე-4 ეტაპზე მიღებული სიმბოლოებითა და დამატებითი სიმბოლოების გაერთიანებით იქმნება „გართულებული“ პაროლი, რომელსაც ემატება მიმდინარე თარიღისა და დროის რიცხობრივი მნიშვნელობები. შემდეგ ხდება მისი სიტყვებად დაშლა (ჯგუფების შექმნა) სისტემაში დაყენებული პარამეტრის მიხედვით. სასურველია, რომ მომხმარებლის ავტორიზაციის პროცესში ცენტრალური სერვერისთვის პაროლის გადაცემა მოხდეს ნაწილ-ნაწილ (ცალკეულ ჯგუფებად) შუალედური დასტურების ვითარებაში.

მე-5 და მე-6 ეტაპებზე თითოეული ჯგუფის სიმბოლოებისთვის ASCII(decimal) კოდირებაში ხდება მათი შესაბამისი კოდების განსაზღვრა. შემდეგ სპეციალური ოპერაციის დახმარებით მიღებული

კოდების რიცხობრივი მნიშვნელობა გარდაიქმნება სხვა რიცხობრივ მნიშვნელობად და მიიღება ახალი კოდების სიმრავლე;

მე-7 და მე-8 ეტაპებზე მიღებული კოდების სიმრავლისაგან იქმნება სპეციალური სიმბოლოებისაგან შემდგარი ჯგუფები და ამ ჯგუფების გაერთიანებით გვაქვს სპეციალური სიმბოლოების ერთობლიობისგან შემდგარი დაშიფრული ინფორმაცია, რომელსაც ამოშიფრავს ცენტრალური სერვერი უკუალგორითმის საშუალებით.

განვიხილოთ სიმბოლოების დაშიფვრის კომბინირებული მეთოდის ფორმალური ნაწილი. ამისათვის შემოვიტანოთ აღნიშვნები.

$i-$ სიმბოლოს ინდექსი; $j-$ დამატებითი სიმბოლოს ინდექსი; n_1- სიმბოლოების რაოდენობა მომხმარებლის მიერ შეტანილ სიტყვაში (პაროლში), n_2- სიმბოლოების რაოდენობა დამატებით სიტყვაში.

დასაწყისისთვის:

$$i = 1; \qquad j = 1; \qquad n_1 = 0; \qquad n_2 = 0 \tag{1}$$

ვადგენთ მასივს:

$$S_{\{i\}}F, L \qquad i = \overline{1, n_1} \tag{2}$$

სადაც $S_{\{i\}}F$ არის სიმბოლოების სიტყვის დასაწყისი, $S_{\{i\}}L$ არის სიმბოლოების სიტყვის დასასრული, n_1 არის სიმბოლოების რაოდენობა სიტყვაში.

შემდეგ სიტყვაში სიმბოლოები იშლება და ცალკეული სიმბოლოსთვის ინდექსი განისაზღვრება:

$$\begin{aligned} &i = 1 \\ &S_{\{i\}} = S_{\{i\}}F \\ &S_{\{i\}}F = S_{\{i\}}F + 1 \\ &i = i + 1; \qquad n_1 = n_1 + 1 \end{aligned} \tag{3}$$

ვიდრე $i \le S_{\{i\}}L$

რის შედეგაც მიიღება სიმბოლოების ერთობლიობისაგან შემდგარი სიტყვა, მასში ცალკეული სიმბოლოსთვის განსაზღვრულია თავისი ინდექსი:

$$S_{\{i\}}F, L = (S_{\{1\}}, S_{\{2\}}, ..., S_{\{n_1\}}) \tag{4}$$

თითოეული სიმბოლო განიხილება ASCII(decimal) კოდირებაში და მათთთვის განისაზღვრება კოდები. ამისათვის შემოვიღოთ მასივი:

$$S_{ASCII\{i\}}F, L \qquad i = \overline{1, n_1} \tag{5}$$

სადაც $S_{ASCII\{i\}}F$ არის სიმბოლოების კოდების დასაწყისი, $S_{ASCII\{i\}}L$ არის სიმბოლოების კოდების დასასრული, n_1 არის სიმბოლოების კოდების რაოდენობა.

მომდევნო ეტაპზე ცალკეული სიმბოლოსთვის კოდი განისაზღვრება და ჩაიწერება სიმბოლოების კოდების მასივში:

$$\begin{aligned} &i = 1 \\ &S_{ASCII\{i\}} = S_{\{i\}}F, L \\ &i = i + 1; \end{aligned} \tag{6}$$

ვიდრე $i \le n_1$

რის შედეგაც მიიღება სიმბოლოების კოდების ერთობლიობისაგან შემდგარი რიცხვები, რომლებშიც ცალკეული სიმბოლოსთვის განსაზღვრულია თავისი ინდექსის კოდი:

$$S_{ASCII\{i\}}F, L = (S_{ASCII\{1\}}, S_{ASCII\{2\}}, ..., S_{ASCII\{n_1\}}) \tag{7}$$

შემდეგ უნდა შევავსოთ სიტყვა დამატებითი სიმბოლოებით. ამისათვის შემოვიტანოთ აღნიშვნა - P_1, რომელიც წარმოადგენს სიტყვის შევსების პარამეტრს ანუ რა რაოდენობისაგან უნდა შედგებოდეს სიმბოლოებითა და დამატებითი სიმბოლოების გაერთიანებით შედგენილი სიტყვა.

თავდაპირველად უნდა განისაზღვროს დამატებითი სიმბოლოების რაოდენობა – n_2.

$$n_2 = p_1 - n_1 \tag{8}$$

ვადგენთ მასივს, სადაც უნდა ჩაიწეროს დამატებითი სიმბოლოები:

$$D_{\{j\}}F, L \qquad j = \overline{1, n_2} \tag{9}$$

სადაც $D_{\{j\}}F$ არის დამატებითი სიმბოლოების სიტყვის დასაწყისი, $D_{\{j\}}L$ არის დამატებითი სიმბოლოების სიტყვის დასასრული, n_2 არის დამატებითი სიმბოლოების რაოდენობა სიტყვაში.

შემდგომ ცალკეული სიმბოლოს განსაზღვრული კოდისთვის განისაზღვრება მოდიფიცირებული კოდები. ამისათვის შემოვიღოთ აღნიშვნა – b_k, რომელიც არის დამატებითი სიმბოლოების შევსებისთვის საჭირო ძირითად სიმბოლოებში გასავლელი ბიჯების რაოდენობა. $k = \overline{1, m}$, სადაც m - არის ბიჯების რაოდენობა

ამისათვის შემოვიღოთ მასივი, სადაც ჩაიწერება მოდიფიცირებული კოდები:

$$D_{ASCII\{j\}}F, L \qquad j = \overline{1, n_2} \tag{10}$$

სადაც $D_{ASCII\{j\}}F$ არის დამატებითი სიმბოლოების კოდების დასაწყისი, $D_{ASCII\{j\}}L$ არის დამატებითი სიმბოლოების კოდების დასასრული, n_2 არის დამატებითი სიმბოლოების კოდების რაოდენობა.

მოცემული მეთოდის მიზანი მოდიფიცირებული კოდებით დასაშიფრი სიმბოლოების გადაყვანა სპეციალურ სიმბოლოებში. ASCII(decimal) კოდირების სისტემაში სიმბოლოების კოდები შეესაბამება 32-დან 126-ის ჩათვლით, ხოლო სპეციალური სიმბოლოების კოდები შეესაბამება 128-დან 255-ის ჩათვლით.

სიმბოლოების კოდების გარდაქმნა ხდება შემდეგნაირად. აიღება სიტყვის პირველი სიმბოლოს კოდი $S_{ASCII\{1\}}$, გადამოწმდება მისი მდებარეობის არეალი. თუ კოდი მდებარეობს 32-დან 50-ის ჩათვლით,

მაშინ შესრულდება შემდეგი მოქმედება: სიმბოლოს კოდს დაემატება მისი რიგითობა ანუ ინდექსი, შემდეგ მეორე სიმბოლოს კოდს დაემატება მეორე ინდექსი და ა.შ. სიტყვის ბოლომდე. თუ კოდი მდებარეობს 51-დან 126-ის ჩათვლით, მაშინ აკლდება. მიღებული ახალი კოდებით დგება დამატებითი სიმბოლოების ჯგუფი. ეს პროცესი მიმდინარეობს იქამდე, ვიდრე არ დაკმაყოფილდება p_1 პარამეტრის მნიშვნელობა. თუ b_k-სთვის $k=1$, ანუ პირველი ბიჯია, მაშინ სიმბოლოების რიგითობა იწყებს 1-დან, თუ $k=2$ - მე-2 ბიჯი, 2-დან და ა.შ.

$$
\begin{aligned}
&b_k = 1 \\
&\text{თუ } 32 \le S_{ASCII\{i\}}F,L \le 50, \text{ მაშინ} \\
&D_{ASCII\{j\}}F,L = S_{ASCII\{i\}}F,L + S_{ASCII\{i\}} \\
&\text{თუ } 51 \le S_{ASCII\{i\}}F,L \le 126, \text{ მაშინ} \\
&D_{ASCII\{j\}}F,L = S_{ASCII\{i\}}F,L - S_{ASCII\{i\}} \\
&k = k+1;\ \ i = i+1;\ \ j = j+1
\end{aligned}
\tag{11}
$$

მიღებული ახალი მოდიფიცირებული კოდებით დგება დამატებითი სიმბოლოების ჯგუფი:

$$
\begin{aligned}
&j = 1 \\
&D_{\{j\}} = D_{ASCII\{j\}}F,L \\
&j = j+1 \\
&\text{ვიდრე } \ j \le n_2
\end{aligned}
\tag{12}
$$

რის შედეგაც მიიღება დამატებითი სიმბოლოების ერთობლიობისაგან შემდგარი სიტყვა, რაშიც ცალკეული სიმბოლოსთვის განსაზღვრულია თავისი ინდექსი:

$$D_{\{j\}}F,L = (D_{\{1\}}, D_{\{2\}}, ..., D_{\{n_2\}}) \tag{13}$$

მიღებული სიმბოლოებითა და დამატებითი სიმბოლოების გაერთიანებით იქმნება „გართულებული“ სიტყვა (პაროლი), რომელსაც ემატება მიმდინარე თარიღისა და დროის რიცხობრივი მნიშვნელობები. შემოვიტანოთ აღნიშვნები – *DateTime*, რომელშიც ფიქსირდება მიმდინარე თარიღისა და დროის რიცხობრივი მონაცემი - *DateTime=now()*; $SD_{\{i\cup j\}}F,L$, რაშიც იწერება გაერთიანებული სიტყვა:

$$SD_{\{i\cup j\}}F,L = S_{\{i\}}F,L + D_{\{j\}}F,L + DateTime \qquad (14)$$

სადაც $i=\overline{1,n_1}$; $j=\overline{1,n_2}$

შედეგად მიიღება სიმბოლოებისაგან და დამატებითი სიმბოლოების ერთობლიობისაგან შემდგარი სიტყვა, რაშიც ცალკეული სიმბოლოსთვის განსაზღვრულია თავისი ინდექსი:

$$SD_{\{i\cup j\}}F,L = (S_{\{1\}},S_{\{2\}},...,S_{\{n_1\}},...,D_{\{1\}},D_{\{2\}},...,D_{\{n_2\}}) \qquad (15)$$

შემდეგ ხდება მიღებული სიტყვის დაშლა (ჯგუფების შექმნა) სისტემაში დაყენებული პარამეტრის მიხედვით. ამისათვის შემოვიტანოთ აღნიშვნები – p_2, რომელიც წარმოადგენს დასაშლელი სიტყვის რაოდენობას, ანუ რა რაოდენობით უნდა დაიშალოს მიღებული სიტყვა; $G_{\{\ell\}}SD_{\{i\cup j\}}F,L$, სადაც ფიქსირდება ჯგუფში შემავალი სიმბოლოები და ჯგუფის ინდექსი; m – ჯგუფების რაოდენობა.

დაშლილი სიტყვების რაოდენობა აღვნიშნოთ -ით და იგი გამოითვლება შემდეგნაირად:

$$\ell = (n_1 + n_2 + DateTime_{Count})divp_2; \qquad (16)$$

$$\ell = \overline{1,m}$$

სადაც *div* – ნიშნავს გაყოფას ნაშთის გარეშე. $DateTime_{Count}$ – თარიღისა და დროის რიცხობრივ მაჩვენებლებში სიმბოლოების რაოდენობა. შედეგად მივიღებთ ჯგუფების ერთობლიობას:

$$G_{\{\ell\}}SD_{\{i\cup j\}}F,L = (G_{\{1\}}SD_{\{i\cup j\}},G_{\{2\}}SD_{\{i\cup j\}},...,G_{\{m\}}SD_{\{i\cup j\}}) \qquad (17)$$

შემდეგ თითოეული ჯგუფის სიმბოლოებისთვის ASCII(decimal) კოდირებაში ხდება მათი შესაბამისი კოდების განსაზღვრა.

$$G_{ASCII\{\ell\}}SD_{\{i\cup j\}} = G_{\{\ell\}}SD_{\{i\cup j\}}F, L$$
$$\ell = \ell + 1 \qquad (18)$$
ვიდრე $\ell \le m$

რის შედეგაც მიიღება ჯგუფის სიმბოლოების კოდების ერთობლიობისაგან შემდგარი რიცხვები, რაშიც ცალკეული სიმბოლოსთვის განსაზღვრულია თავისი ინდექსის კოდი:

$$G_{ASCII\{\ell\}}SD_{\{i\cup j\}}F, L = (G_{ASCII\{1\}}SD_{\{i\cup j\}}, G_{ASCII\{2\}}SD_{\{i\cup j\}}, ..., G_{ASCII\{m\}}SD_{\{i\cup j\}}) \qquad (19)$$

მიღებული კოდების რიცხობრივი მნიშვნელობა გარდაიქმნება სხვა რიცხობრივ მნიშვნელობად და მიიღება ახალი კოდების სიმრავლე. მიღებული სიმბოლოების კოდების გარდაქმნა ხდება შემდეგნაირად. აიღება სიტყვის პირველი სიმბოლოს კოდი $G_{ASCII\{\ell\}}$, გადამოწმდება მისი მდებარეობის არეალი. თუ კოდი მდებარეობს 32-დან 99-ის ჩათვლით, მაშინ შესრულდება შემდეგი მოქმედება: სიმბოლოს კოდს დაემატება პარამეტრის მნიშვნელობა, რომლიც აღვნიშნოთ - p_3. სადაც $96 \le p_3 \le 156$. ხოლო, თუ კოდი მდებარეობს 100-დან 126-ის ჩათვლით, მაშინ სიმბოლოს კოდს დაემატება პარამეტრის მნიშვნელობა, რომლიც აღვნიშნოთ $- P_4$. სადაც $28 \le p_4 \le 129$.

თუ $32 \le G_{ASCII\{\ell\}}F, L \le 99$, მაშინ

$$P_{ASCII\{g\}}F, L = G_{ASCII\{\ell\}}F, L + p_3$$

თუ $100 \le G_{ASCII\{\ell\}}F, L \le 126$, მაშინ (20)

$$P_{ASCII\{g\}}F, L = G_{ASCII\{\ell\}}F, L + p_4$$

$$g = g + 1;\ \ \ell = \ell + 1;\ \ g = \overline{1,t}$$

სადაც $P_{ASCII\{g\}}F, L$ არის სპეციალური სიმბოლოების მოდიფიცირებული კოდებისაგან შემდგარი ერთობლიობის მასივი, რომელიც ფიქსირდება ჯგუფების მიხედვით.

მიღებული ახალი მოდიფიცირებული კოდებით დგება სპეციალური სიმბოლოების ჯგუფი:

$$\begin{aligned} &g = 1 \\ &P_{\{g\}} = P_{ASCII\{\ell\}} F, L \\ &g = g + 1 \\ &\text{ვიდრე} \quad g \le t \end{aligned} \tag{21}$$

შედეგად მივიღებთ სპეციალური სიმბოლოების ჯგუფების ერთობლიობას:

$$G_{\{\ell\}} P_{\{g\}} F, L = (G_{\{1\}} P_{\{g\}}, G_{\{2\}} P_{\{g\}}, ..., G_{\{m\}} P_{\{g\}}) \tag{22}$$

სპეციალური სიმბოლოებისაგან შემდგარი ჯგუფების გაერთიანებით მიიღება სპეციალური სიმბოლოების ერთობლიობისგან შემდგარი დაშიფრული ინფორმაცია:

$$W_{\{\ell\}} F, L = G_{\{\ell\}} P_{\{g\}} \tag{23}$$

$$\ell = \overline{1, m}; \quad g = \overline{1, t}$$

დაშიფრული ინფორმაცია ცენტრალურ სერვერს მიეწოდება ჯგუფების სახით. თუ პირველი ჯგუფის იდენტიფიკაცია წარმატებით დასრულდა, სერვერი ატყობინებს და ბრძანებას გამოსცემს მეორე ჯგუფის გამოშვებაზე და ა.შ. ჯგუფის ბოლომდე. თუ რომელიმე ჯგუფი არ დაემთხვა, სერვერი მაშინვე ბლოკავს აღნიშნულ მომხმარებელს. დაშიფრული ინფორმაციის ამოშიფვრა ცენტრალური სერვერის მიერ ხდება ზემოთგანხილული მეთოდის უკუალგორითმის საშუალებით იმავე პარამეტრების გამოყენებით.

დაშიფვრისა და ამოშიფვრის გასაღები სისტემაში გამოყენებული სპეციალური პარამეტრების წყალობით არის უნიკალური ანუ მომხმარებლის ყოველი ავტორიზაციის დროს გასაღებები იცვლება და არასდროს არ განმეორდება.

ნაშრომში აგრეთვე დეტალურად განხილულია კორპორაციული ქსელების, მათი კომპონენტების და სისტემების მიმოხილვა, ქსელში

არსებული მოწყვლადობების აღმოჩენა, კლასიფიცირება, პრიორიტიზირება და აღმოფხვრა. მოწყვლადობების მართვა არის პროცესი, რომლის საშუალებითად ხდება ქსელში არსებული მოწყვლადობების აღმოჩენა, კლასიფიცირება, პრიორიტიზირება და აღმოფხვრა. ეს პროცესი არის ინფორმაციული უსაფრთხოების ერთ-ერთი შემადგენელი კომპონენტი. საკუთრივ მოწყვლადობების მართვის პროცესი შედგება სხვადასხვა კომპონენტებისაგან.

მოწყვლადობების ძირითადი გამომწვევი მიზეზი არის პროგრამული უზრუნველყოფის მომართვისას დაშვებული შეცდომები და მათი განუახლებელი ვერსიები. მოწყვლადობები პროგრამული უზრუნველყოფის "სიცოცხლის ციკლის" განუყოფელი ნაწილია. არ არსებობს 100%-ით დაცული პროგრამული უზრუნველყოფა. ადრე თუ გვიან აუცილებლად აღმოჩნდება მოწყვლადობა მასში და ეს ნორმალურია.

არსებობს სხვადასხვა პროექტი სადაც უსაფრთხოების ანალიტიკოსები/ინჟინრები ცდილობენ იპოვონ სისუტეები სხვადასხვა ინფორმაციულ სისტემებში, შესაბამისი ანაზღაურების სანაცვლოდ. სისუსტის აღმოჩენის შემდეგ ინფორმაცია გადაეცემა მწარმოებელს, რომლის სისტემაშიც აღმოჩენილია ეს სისუსტე. ამის შემდეგ მწარმოებელი როგორც წესი უშვებს უსაფრთხოების განახლებას, რომლითაც აღმოფხვრის სისუსტეს. არსებობს ბევრი პლათფორმა, რომელიც გამოიყენება ამ საქმიანობისთვის. მაგალითად, Zerodium, Hakerone, ZDI, Safehats, Bugcrowd და სხვა. ასეთ პლათფორმებზე მუშაობენ ეგრედ წოდებული თეთრი ქუდის(whitehat), ან ნაცრისფერი ქუდის(grayhat) ჰაკერები. თუმცა ჩამოთვლილი პლათფორმების გარდა არსებობს შავი ბაზარი. სადაც შესაძლებელია ეგრედ წოდებული 0 დღის(Zero Day) სისუსტეზე ინფორმაციის და ამ სისუსტის გამოყენებაზე მიმართული პროგრამული კოდის(exploit) ყიდვა. ამ დროს სისუტეზე ინფორმაცია არ მიეწოდება მწარმოებელს. ასეთ სისუსტეებს იყენებენ ჰაკერული დაჯგუფებები მიზანმიმართული შეტევებისთვის. აღმოჩენილი სისუსტეები არის მიზეზი

იმისა, რომ გამოდის ეგრედ წოდებული უსაფრთხოების პაჩები. პროგრამული განახლების ეს ტიპი (უსაფრთხოების განახლება) არ აფართოებს პროგრამული უზრუნველყოფის შესაძლებლობებს. ის მხოლოდ აღმოფხვრის არსებულ სისუსტეს პროგრამულ უზრუნველყოფაში. მართალია აუცილებელია ყოველთვის განახლებული გვქონდეს პროგრამული უზრუნველყოფა თუმცა, მხოლოდ პროგრამული უზრუნველყოფის განახლება ვერ დაგვიცავს სისუსტეებისგან. თუკი სისტემა დაკონფიგურირებულია არასწორად, იმგვარად, რომ კონფიგურაცია იწვევს სისუსტეს, მხოლოდ პროგრამული განახლება ვერ აღმოფხვრის მას. ამისათვის საჭიროა მივყვეთ საუკეთესო პრაქტიკებს. ვაკეთოთ სისტემების ეგრედ წოდებული გამაგრება (hardening). რისი საშუალებითაც შევამცირებთ სავარაუდო სისუსტეების რაოდენობას სისტემებზე.

მოწყვლადობების აღმოჩენისთვის გამოიყენება მოწყვლადობის სკანერები. მათი საშუალებით შესაძლებელია სკანირების ჩატარება ქსელზე და მოწყვლადობების გამოვლენა. მოწყვლადობების აღმოჩენა შესაძლებელია როგორც ქსელის სკანირებით, ასევე აგენტის გამოყენებით. ქსელის სკანირების დროს ქსელში არსებობს გამოყოფილი კომპონენტი (სკანერი) რომელსაც აქვს წვდომა დასასკანირებელ სისტემებთან. არსებობობს სხვადასხვა ტიპის სკანერები. ზოგიერთი მათგანი ახორციელებს ზოგად სკანირებას, აღმოაჩენს ღია პორტებს. სერვისებს, რომლებიც პასუხისმგებლები არიან ამ პორტებზე. მათ ვერსიებს და ასე შემდეგ. ზოგიერთი მათგანს აქვს ფუნქციონალი, აღმოაჩინოს სისუსტეები კონკრეტული მიმართულებით, მაგალითად: სისუსტეები ვებ სერვისების მიმართულებით, სისუსტეები კონკრეტული კონტენტის მართვის სისტემის მიმართულებით, სისუსტეები კონკრეტულ მოწყვლადობაზე და ასე შემდეგ.

ზემოთაღნიშნული სკანერები ძირითადად გამოიყენება შეღწევადობის ტესტირების დროს. როდესაც ადამიანი ახორციელებს შეღწევადობის ტესტირებას. ადამიანის მიერ განხორციელებული შეღწევადობის

ტესტირება უფრო სიღრმისეულია. სკანერებს ავტომატურ რეჟიმში არ შეუძლიათ ისეთი სიღრმისეული ანალიზის გაკეთება, როგორც ადამიანს. მაგრამ ადამიანის მიერ ტესტირებას აქვს ერთი ნაკლი, ეს არის დანახარჯი, როგორც ადამიანური ასევე ფულადი რესურსისა. სისუსტეების ავტომატიზაციისთვის გამოიყენება მოწყვლადობების სკანერების გადაწყვეტილებები. ბაზარზე არსებობს, ბევრი სხვადასხვა მოწყვლადობის სკანერის გადაწყვეტილება. მათი არჩევისას აუცილებელია გათვალისწინებული იქნეს ბიზნესის მოთხოვნა.

მოწყვლადობების მართვის პროცესს აქვს თავისი სასიცოცხლო ციკლი. სხვადასხვა კომპანია სხვადასხვანაირად უდგება ამ პროცესს. პროცესის გასამარტივებლად და მის ნათლად წარმოსაჩენად გამოვიყენებთ გამარტივებულ მეთოდს, რომელიც შეიცავს შემდეგ ნაბიჯებს: აღმოჩენა, პრიორეტიზირება, აღმოფხვრა. ცხადია ეს პროცესი მეტ-ნაკლებად განსხვავებულია ყველა კომპანიისთვის. ინფრასტრუქტურიდან გამომდინარე ეს პროცესი ცვალებადია, თუმცა ზოგადი იდეა იგივე რჩება. ამ პროცესის მიზანია ინფრასტრუქტურაში არსებული სისუსტეების აღმოჩენა და მათი აღმოფხვრა. ასევე გასათვალისწინებელია, რომ თუკი გავითვალისწინებთ ზემოთ გამოთვლილ საუკეთესო პრაქტიკების რჩევებს ინფრასტრუქტურაში არსებული სისუსტეების რაოდენობა საგრძნობლად შემცირდება.

აღმოჩენა არის პირველი ეტაპი. სისტემებზე სისუსტეების აღმოჩენა შესაძლებელია როგორც ხელით, ასევე ავტომატურ რეჟიმში სხვადასხვა ხელსაწყოს გამოყენებით. სწორედ აღმოჩენის ავტომატიზაციაში გვეხმარება მოწყვლადობის სკანერი. მოწყვლადობის სკანერში იქმნება პოლიტიკა, რომლის მიხედვით გარკვეული პერიოდულობით, მაგალითად კვირაში ერთხელ სისტემა ასკანერებს ქსელში ჩართულ კვანძებს და ცდილობს აღმოაჩინოს სისუსტეები.

პრიორეტიზაცია არის პროცესი, რომლის დროსაც სისტემებს და სისუსტეებს ვალაგებთ მათი მნიშვნელობიდან გამომდინარე. მაგალითისათვის სერვერი რომელზეც მუშავდება მნიშვნელოვანი

მონაცემები უფრო მნიშვნელოვანია, ვიდრე საბოლოო მომხმარებლის სამუშაო მაგიდა. შესაბამისად სისუსტეების აღმოფხვრის დროს პირველ რიგში მოვაგვარებთ პრობლემას სერვერზე შემდეგ კი სამუშაო მაგიდაზე. ესაა ზოგადი მაგალითი იმისა, თუ როგორ ხდება აქტივების პრიორეტიზირება, თუმცა ყველა ინფრასტრუქტურა ინდივიდუალურია და საჭიროებს ინდივიდუალურ მიდგომას. ასეთების მნიშვნელობასთან ერთად გასათვალისწინებელია, სისუსტეების ბოროტმოქმედების მიერ გამოყენების ალბათობა და გამოყენების შემთხვევაში ზემოქმედების დონე. რაც პირველ რიგში გულისხმობს იმას, თუ რამდენად არის შესაძლებელი სისუსტის რეალურად გამოყენება, არსებობს თუ არა ცნობილი პროგრამული კოდი, რომელიც იყენებს კონკრეტულ სისუსტეს, რამდენად რთულია ამ სისუსტის გამოყენება. მეორე რიგში კი, თუკი ბოროტმოქმედმა გამოიყენა სისუსტე რა სახის ზიანი მიადგება ამით სისტემას. ბოროტმოქმედი შეძლებს ინფორმაციის მოპარვას, სისტემაზე უფლებების მოპოვებას, თუ რა სახის ზიანის განხორციელებას შეძლებს ის.

აღმოჩენის და პრიორეტიზირების შედეგად ვიცით რა სახის სისუსტეები გვაქვს და რომელი სისუსტიდან უნდა დავიწყოთ მათი აღმოფხვრა. აღმოფხვრის პროცესი ინდივიდუალურია ყველა სისტემისათვის. ზოგიერთ მოწყვლადობის სკანერი სისუსტის აღმოჩენის შემდეგ გვაძლევს გარკვეულ “რჩევას“ თუ როგორ აღმოვფხვრათ სისუსტე. იქნება ეს უბრალო რჩევა სისტემის განახლების შესახებ, კონფიგურაციის ცვლილებაზე, თუ ბმული სტატიაზე სადაც განხილულია თუ როგორ უნდა აღმოიფხვრას სისუსტე. უმეტეს შემთხვევაში სისუსტის აღმოფხვრა შესაძლებელია პროგრამული უზრუნველყოფის განახლებით ან კონფიგურაციის ცვლილებით.

სკანირების შემდგომ საჭიროა შედეგების ანალიზი და მათ აღმოსაფხვრელად შესაბამისი ზომების მიღება, იქნება ეს კონფიგურაციის ცვლილება, პროგრამული განახლება თუ სხვა.

კორპორაციული ქსელების უსაფრთხოების ავტომატიზებული სისტემის ძირითადი ამოცანების საფუძველზე განისაზღვრა და ჩამოყალიბდა სისტემის ალგორითმები. თითოეული ალგორითმისთვის დადგინდა შემავალი და გამომავალი მონაცემები, შეიქმნა მონაცემთა ბაზები, რომელთა საფუძველზეც განხორციელდა ალგორითმებით გათვალისწინებული უსაფრთხოების პროცესები.

თითოეული ალგორითმისთვის დადგენილი იქნა შემავალი და გამომავალი მონაცემები, შეიქმნა მონაცემთა ბაზები, რომელთა საფუძველზეც განხორციელდა ალგორითმებით გათვა¬ლისწინებული უსაფრთხოების პროცესები. განსაზღვრულია ალგორითმული ბლოკების ფუნქციონალური დანიშნულებები და მოხდენილია თითოეული ალგორითმული ბლოკის ისეთი სახით დეტალიზაცია, რომ შესაძლებელი და გაადვილებული იყოს პროგრამირების პროცესი. ალგორითმებში ჩართულია იმ პროგრამების ერთობლიობა, რომლებიც მართავენ კომპიუტერის სხვადასხვა ნაწილების მუშაობას და მომხმარებელს საშუალებას აძლევენ თავისი ამოცანა გადაწყვეტილი იყოს მისთვის სასურველი სახით.

ავტომატიზებული სისტემის გადაწყვეტა წარმოადგენს ინფორმაციის მიღების, გადამუშავებისა და გადაცემის პროცესებს. სისტემის შემუშავებაში მთავარ როლს თამაშობს ინფორმაციული უზრუნველყოფის დამუშავება, რაც მართვის ამოცანის ინფორმაციულ ანალიზს და ინფორმაციული ბაზის დაპროექტებას გულისხმობს.

კორპორაციული ქსელების უსაფრთხოების მხარდამჭერ ავტომატიზებულ სისტემაში დიდი მნიშვნელობა აქვს დიალოგური რეჟიმის შემუშავებას, სადაც დიალოგის საშუალებით ხორციელდება მომხმარებელსა და სისტემას შორის ურთიერთობების ორგანიზაცია. სისტემის დიალოგური პროცესის ინიციატორია ადამიანი, რომელიც სახავს მუშაობის მიზანს და ირჩევს მისი მიღწევის საშუალებებს. სისტემა კი უნდა უზრუნველყოფდეს ადეკვატურ რეაქციას მომხმარებლის მოთხოვნებზე.

აგრეთვე, სქემატურად წარმოდგენილია უსაფრთხოების ავტომატიზებული სისტემის დიალოგური პროცედურები და თითოეული მათგანი აღწერილია ცალკ-ცალკე.

მესამე თავში აღწერილია კორპორაციული საინფორმაციო სისტემებში ინფორმაციული ნაკადების შეფასების მოდელი და საბოლოო ეტაპზე გააანალიზებულია სიმბოლოების დაშიფვრის კომბინირებული მეთოდის ექსპერიმენტული შემოწმების შედეგები.

დასკვნა

სადისერტაციო ნაშრომში განხილული კორპორაციული ქსელების უსაფრთხოების უზრუნველყოფის მეთოდებისა და საშუალებების კვლევის შედეგების ანალიზის საფუძველზე, შეიძლება გაკეთდეს შემდეგი დასკვნა:

1. წარმოდგენილია ძირითადი ცნობები კორპორაციული ქსელების ტექნოლოგიებისა და კომპონენტების შესახებ. მოკლედ განხილულია უსადენო ქსელების ყველა ნაირსახეობა, აღწერილია მათი სტრუქტურის თავისებურებები და გამოყენების მეთოდები.

2. მოყვანილია კორპორაციულ ქსელებთან დაკავშირებული უსაფრთხოების საკითხები და ჩატარებულია მათი ანალიზი. ჩამოყალიბებულია კორპორაციული ქსელების უსაფრთხოების პრობლემის აქტუალურობის საკითხები. წარმოდგენილია უსადენო ქსელების გამოყენებასთან დაკავშირებული საფრთხეების ყველაზე გავრცელებული ფორმები და თითოეული მათგანი დახასიათებულია თავისი თვისებებით.

3. წამოდგენილია სხვადასხვა კავშირგაბმულობის არხების გამოყენების ტენდეციები უსაფრთხოების სისტემებში. მოყვანილია მსგავსი მეთოდები და მოდელები, თავისი დადებითი და უარყოფითი მხარეებით. დახასიათებულია უსაფრთხოების ავტომატიზებული სისტემის ძირითადი ამოცანები თავიანთი ფუნქციონალური დანიშნულებებით.

4. ნაშრომში დიდი ყურადღება ექცევა ვირტუალური კერძო ქსელის (VPN) აგების პრინციპებს, რომელიც უზრუნველყოფს დამოუკიდებელი დაცული ქსელის შექმნას ინტერნეტის ან სხვა ღია არხების მეშვეობით.

განხილულია VPN ქსელში უსაფრთხოების უზრუნველსაყოფად არსებული კრიპტოგრაფიული მეთოდები, მოყვანილია მათი დადებითი და უარყოფითი მხარეები და არსებული პრობლემებიდან გამომდინარე შემუშავებულია სიმბოლოების დაშიფვრის კომბინირებული მეთოდი.

5. დეტალურად განხილულია კორპორაციული ქსელის კომპონენტები და სისტემები, გაანალიზებულია ასეთი ქსელის გამოყენებასთან დაკავშირებული საფრთხეების სხვადასხვა ფორმები და აღნიშნული საფრთხეების აღმოსაფხვრელად შემოთავაზებულია ახალი მეთოდები, რომელიც უზრუნველყოფს ინფორმაციული პაკეტების მარშრუტიზაციის უსაფრთხოების ამაღლებას.

6. უსაფრთხოების მხარდამჭერი ავტომატიზებული სისტემის ძირითადი ამოცანების საფუძველზე განისაზღვრა და ჩამოყალიბებული იქნა სისტემის ალგორითმები, დამუშავებული იქნა ინფორმაციული უზრუნველყოფა და დიალოგური პროცედურები. თითოეული ალგორითმისთვის დადგენილი იქნა შემავალი და გამომავალი მონაცემები, შეიქმნა მონაცემთა ბაზები, რომელთა საფუძველზეც განხორციელდა ალგორითმებით გათვალისწინებული უსაფრთხოების პროცესები.

7. დამუშავებული მეთოდებისა და პროგრამული კომპლექსის საფუძველზე რეალიზებულია კორპორაციული ქსელების უსაფრთხოების მხარდამჭერი ავტომატიზებული სისტემა.

სადისერტაციო თემის ირგვლივ გამოქვეყნებული შრომები

1. ხელნაწერი სიმბოლოების ანალიზი და შედარების პროცესების ფორმირება მინი-მაქსის პრინციპით. სტუ, არჩილ ელიაშვილის მართვის სისტემების ინსტიტუტი, შრომათა კრებული N 18, თბ. 2014. 244-246. ო. შონია, ი. ქართველიშვილი, ლ. შონია.
2. Algorithm of Combined Method for Symbol Encoding in Virtual Private Networks (VPN). Journal of Technical Science and Technologies, Internacional Black Sea University, ¹2, 2012. 15-20 O. Shonia, T. Kaishauri, I. Kartvelishvili, L. Shonia, Z. Beridze I. Didmanidze
3. ინფორმაციული სისტემის დაცვის უზრუნველყოფის ამოცანის დასმის ეფექტურობა. სტუ, შრომები "მართვის ავტომატიზებული სისტემები" ¹1(13) 2012. 77-81. ო. შონია, ლ. შონია.
4. ვირტუალურ კერძო ქსელებში (VPN) სიმბოლოების დაშიფრვის კომბინირებული მეთოდი. სტუ, შრომები "მართვის ავტომატიზებული სისტემები" ¹1(12) 2012. 121-125. ო. შონია, ი. ქართველიშვილი, ზ. ბერიძე, ლ. შონია.
5. Recognition of symbols using the method of gravity center. Nova science publishers Computer Tecnology and Applications 2017-3rd Quarter. 9 O. Shonia, J. Kartvelishvili, N. Chorkhauli, L. Shonia.
6. Algorithm of Combined Method for Symbol Encoding In Virtual Private Networks (VPN). Journal of Technical Science & Technologies. No.2 (Vol.1), 2012. 6. O. Shonia, T. Kaishauri, L. Shonia, Z. Beridze, I. Didmanidze.
7. ვირტუალური კერძო ქსელის (VPN) აგების კონცეფცია, ქსელის ფუნქციები და მათი კლასიფიკაცია., Georgian Technical University. AUTOMATED CONTROL SYSTEMS-2(26), 2018; 205. J. Kartvelishvili, L. Shonia.
8. Development of Software of Testing system generation of Examination Prangishvili A.I., Shonia O.B., Kartvelishvili I.SH., Shonia L.O., IX Московская

международная конференция по исследованию операций (ORM2018) Москва, 22–27 октября 2018 ТРУДЫ.

9. უსადენო ქსელების უსაფრთხოების საკითხები და მათი ანალიზი. ოთარ შონია, იოსებ ქართველიშვილი, ლუკა შონია // SECURITY ISSUES OF WIRELESS NETWORKS AND THEIR ANALYSIS. Shonia Otar, Kartvelishvili Ioseb, Shonia Luka. 109-113. საქართველოს ტექნიკური უნივერსიტეტი, შრომები 2020 1(30).
10. კორპორაციული სისტემების ინფორმაციული უსაფრთხოების უზრუნველყოფასთან დაკავშირებული რისკების ანალიზი. ოთარ შონია, იოსებ ქართველიშვილი, ლუკა შონია // ANALYSIS OF THE RISKS ASSOCIATED WITH ENSURING INFORMATION SEFURITY OF CORPORATE INFORMATION SYSTEMS. Shonia Otar, Kartvelishvili Ioseb, Shonia Luka. 113-118. საქართველოს ტექნიკური უნივერსიტეტი, შრომები 2020 1(30).

Abstract

Methods for ensuring multi-level security of a corporate network

And means research

The widespread use of information technology, the automation of enterprises, business processes, and public administration processes, and the widespread use of electronic communications models have brought to the fore the need for legal protection of information as an object of property rights. In turn, examples are given, which clearly indicate the problematic nature of this task. The main reason for this is, first of all, the peculiarity of the information as an object of property right - it is easily copied unlike the traditional material object of property right, easily transferred to another person with the right of ownership without any obvious (noticeable) violation of property rights. In addition, the danger of copying and transmitting information is exacerbated by the fact that it is stored and processed in an environment accessible to a large number of entities who are not holders of the right to own this information. This is, for example, a wide range of commonly automated systems, ranging from individual people to computer workplaces, to corporate automated systems, to e-government and the Internet.

The dissertation presents the current problems of ensuring the protection of corporate information systems and the methods and means of solving them. It is characterized by the risks associated with the provision of information security (UC) of corporate information systems, the scale of cybercrime, and the threats posed by the provision of corporate information systems (UCS). The latest information protection services in corporate information systems, the risks associated with them are discussed and the main recommendations for providing corporate information systems are discussed.

In this regard, the present paper discusses the fundamental principles of security, as well as open problems. The security issues of corporate networks are discussed. It should be noted that corporate network routing protocols do not specify any kind of preventive measures or security mechanisms in the specifications. Thus, the security of corporate network routing protocols has become an urgent need to stimulate network launch and expand the scope of use. Accordingly, the present paper presents and defines different solutions and concepts in terms of security. The main focus is initially on the initial step - the study and analysis of the shortcomings of the routing protocols.

Based on the above, the paper focuses on solving the following tasks, such as increasing the security of routing information packages in corporate networks; Tightening encryption and authentication mechanisms; Analyze different communication channels in corporate networks and develop new methods to increase security; Administration and management of vacancies (local or regional offices) using corporate networks; Remote control and administration of the equipment used in the system; Development and analysis of access schedules for various local or remote facilities (at the level of the parties involved in the unified system); Construction of a document circulation system; Create stories at each staff level and analyze them; Create a unified information archive and conduct statistical analysis based on it in the form of tables and diagrams; Construction and sale of an automated system.

The existing cryptographic methods are discussed to ensure security in the VPN network, their pros and cons are listed, and, based on the existing problems, a combined method of encrypting symbols is developed.

The paper also discusses in detail the components and systems of a corporate network, analyzes the various forms of threats associated with the use of such a network, and proposes new methods to eliminate these threats.