Scientific and Practical Cyber Security Journal (SPCSJ) 8(4): 31 – 42 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

სატელეკომუნიკაციო ქსელებშიინფორმაციისუსაფრთხოების დარღვევის გამომწვევიმიზეზები და ინფორმაციის დაცვის მეთოდები

ელვირა ბჟინავა[1], სალომე მახარაძე[2], მანანა გოგბერაშვილი[3]
[1,2,3]ციფრული სატელეკომუნიკაციო ტექნოლოგიების დეპარტამენტი, საქართველოს ტექნიკური უნივერსიტეტი
s.makharadze@gtu.ge, e.bzhinava@gtu.ge, m.gogberashvili@gtu.ge

CAUSES OF INFORMATION SECURITY BREACHES IN THE TELECOMMUNICATION NETWORKSAND METHODS OF PROTECTING INFORMATION

Elvira Bzhinava[1], Salome Makharadze[2], Manana Gogberashvili[3]
[1,2,3]Department of Digital Telecommunication Technologies, GeorgianTechnical University
s.makharadze@gtu.ge, e.bzhinava@gtu.ge, m.gogberashvili@gtu.ge

რეზიუმე. ადამიანების საქმიანობის ყველა სფეროს ციფრულ ფორმატში გადასვლამ, კაცობრიობას მოუტანა დიდი მიღწევები, გაამარტივა კომუნიკაცია და გაზარდა ბიზნეს პროცესების ეფექტურობა. დადებით ასპექტებთან ერთად მნიშვნელოვნად გაიზარდა კონფიდენციალურობაზე მოთხოვნა. მონაცემების უმეტესობა ინახება ციფრული ფორმით, რაც უბიძგებს თავდასხმელებს ინფორმაციის მოპარვის ახალი გზების ძიებაზე. ბიზნესის სფერო და ფიზიკური პირები ყოველწლიურად აწყდებიან კიბერსაფრთხეებს, რომელთა მთავარი მიზანია ზიანი მიაყენოს ელექტრონულ კომპიუტერულ სისტემებსა და ქსელებს, ასევე ინფორმაცია უნებართვოდ მიითვისონ. ინფორმაციის დაცვის საშუალებების ტექნოლოგიურმა განვითარებამ დღეისათვის მიაღწია იმ დონეს, როდესაც პირველ პოზიციებზე უკვე წამოწეულია მათი გამოყენების აუცილებლობა. განსხვავებული კიბერშეტევები, ერთის მხრივ მოითხოვს განსხვავებულ ტექნოლოგიურ გადაწყვეტილებებს, მეორეს მხრივ დაცვის კომპლექსური სისტემის შექმნას, კომპლექსში გამოყენებული დაცვის საშუალებების მინიმალური რაოდენობის შერჩევის საფუძველზე, რაც ხარჯების შესაბამისად, ოპტიმიზაციის პროცესის განხორციელების ექვივალენტურია. სამუშაოს მიზანია, ინფორმაციის უსაფრთხოების უზრუნველსაყოფად განისაზღვროს შესაბამისი კონკრეტული მიზეზები, გაანალიზდეს შედეგები და შეირჩეს დაცვის საშუალებები. მეთოდოლოგია: კვლევაში გამოყენებულია თვისობრივი კვლევის მიდგომები, რაც გულისხმობს ვრცელი ლიტერატურის თეორიულ მიმოხილვასა და ანალიზს. დასკვნები შედგენილია მთავრობის ანგარიშებიდან და რეცენზირებადი ჟურნალებიდან. გაანალიზებულია უსაფრთხოების გამოკვლევის მეთოდები და ტექნიკური საშუალებები, ასევე მომავალი პერსპექტივები და მათემატიკური გაანგარიშების აუცილებლობა.

საკვანძო სიტყვები: ციფრული, უსაფრთხოება, ინფორმაციული, ანტივირუსი, მომხმარებელი,ინტერნეტ ქსელი, ჰაკინგი, ფიშინგი.

ABSTRACT: The transition of all spheres of human activity to digital format has brought great achievements to humanity, simplified communication and increased the efficiency of business processes. Along with the positive aspects, the demand for privacy has increased significantly. Most data is stored in digital form, which pushes attackers to look for new ways to steal information. Businesses and individuals face meet cyber threats every year, the main goal of which is to damage

electronic computer systems and networks, also to misappropriate information without authorization. The technological development of information protection tools has now reached a level where the necessity of their use has already been put at the forefront. Different cyberattacks, on the one hand, require different technological solutions, on the other hand, the creation of a complex protection system based on the selection of the minimum number of protection means used in the complex, which is equivalent to implementing an optimization process in accordance with costs. The goal of the work is to identify relevant specific reasons, analyze the results, and select protection measures to ensure information security. Methodology: the study uses qualitative research approaches, which involves a theoretical review and analysis of extensive literature. The conclusion are compiled from government reports and peer-reviewed journals. Are analyzed methods and technical means of security research, also future prospects and the need for mathematical calculations.

KEYWORDS*:* Digital, Security, Information, Antivirus, User, Internet network, Hacking, Phishing.

1. 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 სისტემებისთვის. ტექნოლოგიური თვალსაზრისით პრობლემა, რომ არ მოხდეს, ინფორმაციის გაჟონვის სახით საჭიროა ორგანიზაციული და ტექნიკური ღონისძიებების გატარება, აუცილებელია მომხმარებელთა აუტენტიფიკაცია და ავტორიზაცია სათანადო დონეზე, კავშირგაბმულობის არხებში შიფრაციის განხორციელება, პერსონალურ მონაცემებთან ხელმისაწვდომობის შეფასება და სატელეკომუნიკაციო არხებში მონაცემების გადაცემის მთლიანობის დაცვა. ამასთანავე, გასათვალისწინებელია, რომ დაცული ინფორმაცია ლოკალურ ქსელში შეიძლება მომხმარებლებისათვის პრაქტიკულად მიუწვდომელი გავხადოთ. მაგრამ, ინტერნეტის ქსელში ეს შეუძლებელია, ვინაიდან ინფორმაციული საზოგადოებისათვის ასეთი ღონისძიება მიუღებელია. ჩვენ ვცხოვრობთ ღია ინფორმაციულ სამყაროში, სადაც სახელმწიფო ორგანოების მოღვაწეობის შესახებაც კი მონაცემები უნდა იყოს მაქსიმალურად ღია [2].

2. ინფორმაციის გაჟონვა. როცა 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[7].

ყველა კომპანიას, მიუხედავად მისი ინდუსტრიისა და განვითარების მასშტაბისა, აქვს ამა თუ იმ სახის კონფიდენციალური ინფორმაცია (პირადი და კომერციული ინფორმაცია, ინტელექტუალური საკუთრება და ა.შ.). ნებისმიერი ორგანიზაციისთვის სავალდებულო მოთხოვნაა ასეთი აქტივების დაცვა გარე და შიდა თავდამსხმელებისგან. მაგრამ ხშირად არის პრობლემები, რომლებიც დაკავშირებულია იმასთან, რომ კომპანიები ყოველთვის ვერ აცნობიერებენ გარკვეული მონაცემების მნიშვნელობას და არ აქცევენ საკმარის ყურადღებას მათ დაცულობას. შედეგად, კონფიდენციალური ინფორმაცია შეიძლება იყოს რისკის ქვეშ და კომპანიამ შეიძლება სერიოზული ზიანი მიიღოს. სტატიაში მოცემულია რა

პრობლემების წინაშე დგანან კომპანიები, რა საფრთხეს წარმოადგენს უსაფრთხოების არასრულყოფილი სისტემები და თანამშრომლებზე კონტროლის ნაკლებობა. ასევეგანხილულია სისუსტეების აღმოფხვრისა და რისკების მინიმიზაციის მეთოდები. ორგანიზაციულად მნიშვნელოვანი მონაცემები არის ინფორმაცია, რომელიც საჭიროა ბიზნეს მიზნებისა და ამოცანების მისაღწევად და სტრატეგიული გადაწყვეტილებების მისაღებად. ეს შეიძლება იყოს მონაცემები კლიენტების, გაყიდვების, ფინანსური მაჩვენებლების, წარმოების პროცესების, კონკურენტების და ა.შ. ეს მონაცემები უნდა იყოს ზუსტი, განახლებული და სანდო, რათა ორგანიზაციამ შეძლოს ეფექტური ფუნქციონირება და დაეხმაროს მას განვითარებაში.

კორპორატიული ინფორმაციის შენახვისა და დამუშავების ორგანიზებაში არაადეკვატურობამ შეიძლება გამოიწვიოს გაჟონვა.გარკვეულმასისუსტეებმა განსაკუთრებით ხშირად შეიძლება გამოიწვიოს შემდეგი სახის ინციდენტები:

- მონაცემთა დაცვის არაადეკვატური შიდა სისტემა, მოძველებული ხელსაწყოების ან პროგრამული უზრუნველყოფის გამოყენება დაუდასტურებელი ეფექტურობით.
- თანამშრომლების გადაჭარბებული უფლებამოსილებები, რაც გულისხმობს მონაცემთა გაფართოებულ წვდომას, რომლებთან მუშაობა არ არის მათი სამუშაო პასუხისმგებლობის ნაწილი.
- არასანდო მეხსიერების გამოყენება, რომელზეც თანამშრომლების უმეტესობას აქვს წვდომა.
- კონფიდენციალურ ინფორმაციასთან ურთიერთქმედების მკაფიო ალგორითმების ნაკლებობა.
- მომხმარებლის ქმედებებზე სათანადო კონტროლის ნაკლებობა.
- მონაცემების გამოყენება შეუძლიათ არა მხოლოდ გარე თავდამსხმელებს, რომლებსაც სურთ მისი მოპარვა ან კომპანიის რეპუტაციის შელახვა. არამედ,არ არის გამორიცხული საფრთხეები შიდა თანამშრომლებისგანაც მოდიოდეს, რომელთაგან შეიძლება შემთხვევით ან განზრახ გაჟონოს ინფორმაციამ ან გამოიყენონ იგი პირადი სარგებლობისთვის. ასევე არსებობს კომერციული ჯაშუშობა, რომელიც დაკვეთილია კონკურენტების მიერ.

3.ინფორმაციის გაჟონვის მიზეზები [4].

შიდა საფრთხეები შეიძლება გამოწვეული იყოს სხვადასხვა ფაქტორებით, როგორიცაა:

- კომპანიის უსაფრთხოების პოლიტიკის შესახებ თანამშრომელთა ინფორმირებულობის არასაკმარისი დონე.
- კონფიდენციალური ინფორმაციის დამუშავების მკაფიო ინსტრუქციებისა და პროცედურების ნაკლებობა.
- მონაცემთა წვდომის უფლებების ბოროტად გამოყენება.
- კონფიდენციალური ინფორმაციის არასათანადო შენახვა და გადაცემა.
- თანამშრომლების შეგნებული და შემთხვევითი ქმედებები, რომლებიც მიზნად ისახავს მონაცემების მოპარვას ან განადგურებას.

აუცილებელია მკაფიოდ განისაზღვროს ვის შეუძლია კონფიდენციალურ ინფორმაციაზე წვდომა და რა პირობებში. ამისათვის აუცილებელია წვდომის დონეების სისტემის შემუშავება, რომელიც უზრუნველყოფს ორგანიზაციის თანამშრომლებისთვის განსხვავებულ როლებს და წვდომის უფლებებს.

დაშიფვრა გულისხმობს მონაცემთა დაშიფვრას ისეთ ფორმას, რომ მისი წაკითხვა შეუძლებელია. ეს ღონისძიება იცავს არაავტორიზებული წვდომისგან, ჯაშუშური პროგრამებისგან და სხვა თავდასხმებისგან, რომლებიც მიზნად ისახავს ინფორმაციის

მოპარვას. ინფორმაციის წასაკითხად დაგჭირდებათ სპეციალური გასაღები. თუგამოყენებული იყო სიმეტრიული დაშიფვრის ტექნოლოგია, ეს იგივე იქნება კოდირებისთვის და დეკოდირებისთვის. ასიმეტრიული მიდგომის შემთხვევაში გამოიყენება ორი გასაღები - საჯარო მონაცემების გარდაქმნის მიზნით და კერძო პირვანდელ ფორმატში გადასაყვანად.

უსაფრთხოების აუდიტი შეიძლება განხორციელდეს როგორც კომპანიის, ასევე მესამე მხარის ექსპერტების მიერ. ინსპექტირების ოპტიმალური სიხშირე არის 6 თვეში ერთხელ.

Firewalls და Access Controls: Firewall-ები უსაფრთხოების სავალდებულო ინსტრუმენტებია, რომლებიც შექმნილია მონაცემთადაუცველობისაღმოსაჩენად, ტრაფიკისსრულყოფილად შესამოწმებლად და საეჭვო კავშირებისა და შეტყობინებების პაკეტების დაბლოკვისთვის. ასევე არის ახალი თაობის firewalls - NGFW.შემდეგი თაობის Firewall-ის პროდუქტებს აქვთ უფრო ფართო ფუნქციონირება, რადგან ასეთი გადაწყვეტილებები ახორციელებს რამდენიმე დამცავ ინსტრუმენტს, რომლებსაც შეუძლიათ პარალელურად მუშაობა.

შიდა რესურსებზე წვდომის გასაკონტროლებლად და მომხმარებლის ანგარიშების მართვისთვის გამოიყენება IdMდა Identity Management კლასის გადაწყვეტილებები. ისინი საშუალებას იძლევა თავიდან იქნეს აცილებული გადაჭარბებული უფლებების გაჩენა, ოპტიმიზაცია გაუწიოთ მუშაობას სისტემებს, მონაცემებზე წვდომის მოთხოვნით და დაინერგოს უფლებების მინიჭების როლური მოდელი.

მომხმარებლის იდენტიფიკაცია და ავთენტიფიკაცია:

იდენტიფიკაცია - არის პროცესი, რომლითაც რესურსი ან სისტემა ადასტურებს მომხმარებლის არსებობას, რომელიც ცდილობს მასში შესვლას. ტიპიური მაგალითია სისტემაში შესვლა. სისტემა ამოწმებს არის თუ არა ასეთი მომხმარებელი რეგისტრირებული. თუ კი, შემდეგი ეტაპი იწყება.

ავთენტიფიკაცია - არის პროცედურა, რომელიც ადასტურებს მომხმარებლის ავთენტურობას. მაგალითი - პაროლის შეყვანა შესვლის დადასტურების შემდეგ. ეს არის ჩვეულებრივი ერთფაქტორიანი ავთენტიფიკაცია, რომელიც არასრულყოფილად ითვლება, რადგან თავდამსხმელებს შეუძლიათ პაროლის მოპარვა ან უბრალოდ გამოცნობა. მრავალფაქტორიანი (ყველაზე ხშირად ორფაქტორიანი) პროცედურა მოიცავს დამატებით გადამოწმებას, მაგალითად, კოდის შეყვანას ტელეფონიდან ან ელექტრონული ფოსტიდან, ბიომეტრიული მახასიათებლების (თითის ანაბეჭდის, ხმის ჟღერადობის და ა.შ.) წარმოდგენას. ორივე ეს პროცესი ერთმანეთთან მჭიდრო კავშირშია და ძალიან მნიშვნელოვანია ინფორმაციისუსაფრთხოების უზრუნველსაყოფად და მონაცემთადაუცველობის აღმოსაფხვრელად.

შეჭრის აღმოჩენისა და პრევენციის სისტემები ეს არის IPS და IDS გადაწყვეტილებების კლასები (სრული სახელები - Intrusion Prevention System და Intrusion Detection System), რომლებიც საშუალებას გაძლევთ ამოცნობილი იქნეს თუნდაც ატიპიური საფრთხეები. არჩეული პროდუქციის სახეობიდან გამომდინარე, მათ შეუძლიათ შეისწავლონ ანომალიები, ჩაატარონ კვლევა ხელმოწერების ან წესების საფუძველზე [5].

DLP სისტემები - ესარისმონაცემთადაკარგვისპრევენციის კლასის პროდუქტები, რომლებიც ხელს უშლიან მონაცემთადაუცველობის ექსპლუატაციას, აკონტროლებენ ქსელის აქტივობას, აკონტროლებენ ინფორმაციის გადაცემის არხებს და აწარმოებენ დეტალურ ანგარიშებს ინფორმაციის მდგომარეობის შესახებ. ეს ფუნქციებით მდიდარი ინსტრუმენტები განიხილება, როგორც ყველაზე ეფექტური შიდა ინციდენტების თავიდან ასაცილების საშუალება. DLP სისტემაში ფოსტის კონექტორი - აკონტროლებს მონაცემთა გადაცემას ელექტრონული ფოსტით. მოდული მუშაობს როგორც მონიტორინგის, ასევე აქტიური საწინააღმდეგო რეჟიმებში, ანუ მას შეუძლია დაბლოკოს საეჭვო ოპერაციები.

Endpoint Agent - აკონტროლებს თანამშრომლების ქმედებებს სამუშაო სადგურებზე, ფინანსური ინფორმაციის ჩათვლით.

Solar Dozorსისტემა ეხმარება აღმოაჩინოს და თავიდან აიცილოს გაჟონვა, ებრძვის კორპორატიულ თაღლითობას და უზრუნველყოფს თაღლითობისეფექტურპრევენციას. კონფიდენციალური ინფორმაციის გაჟონვისგან საიმედო დაცვის უზრუნველსაყოფად, Solar Dozor იყენებს სპეციალიზებულ მოდულებს - ჩამჭრელებს. ისინი აგროვებენ და ანალიზისთვის გადასცემენ თანამშრომელთა კომუნიკაციებს სხვადასხვა არხებიდან, აკონტროლებენ მომხმარებლის ქმედებებს პერსონალურ კომპიუტერებზე, ასევე აწარმოებენ ინვენტარიზაციას და აკონტროლებენ ადგილობრივ და ღრუბლოვან ფაილურ რესურსებს [1].

ტექნიკური მახასიათებლებიდან გამომდინარე, თითოეული არხისთვის შეირჩევა ინფორმაციის ჩასმის ოპტიმალური წერტილი. ეს შეიძლება იყოს ფოსტის სერვერი, ქსელის კარიბჭე, პროქსი სერვერი ან სამუშაო სადგური. ეს მიდგომა საშუალებას იძლევა თანაბრად გადაანაწილდეს დატვირთვა IT ინფრასტრუქტურაზე და უზრუნველყოფილი იქნეს ორგანიზაციის ბიზნეს პროცესების უწყვეტობა, მინიმუმამდე იქნეს დაყვანილი სისტემის გადატვირთვის გამო მუშაობის შეფერხების რისკები.

OCR (ოპტიკური სიმბოლოების ამოცნობა) - საშუალებას იძლევაგადაყვანილი იქნეს გრაფიკული ფორმით გადაცემული მონაცემები (ფოტოები, ეკრანის ანაბეჭდები, სკანირება) და განზრახ დეფორმირებული, რათა ამოცნობა გართულდეს წასაკითხ ფორმატში.

File Crawler - საშუალებას იძლევადადგინდეს კონფიდენციალური ინფორმაციის შენახვის წესების დარღვევა.

დოკუმენტის ნაკადის ანგარიში სხვადასხვა საკომუნიკაციო არხებზე დოკუმენტების განაწილების ავტომატურად თვალყურის დევნებისთვის. საშუალებასიძლევა სწრაფად და ეფექტურად გაკონტროლოდეს კონფიდენციალური ინფორმაციის მოძრაობა, განისაზღვროს მიმღებები და გამგზავნები, გადაცემის დრო, ასევე მოვლენის კრიტიკულობის დონეები.

4. ქსელში ინფორმაციის უსაფრთხოების საფრთხის სახეები:

უნებლიე თუ შემთხვევით.ისინი წარმოიქმნება პროგრამული უზრუნველყოფის შეცდომების, ტექნიკის გაუმართაობის და მომხმარებლების და სისტემის ადმინისტრატორების არასწორი ქმედებების შედეგად. არ არსებობს მიზანმიმართული ხასიათი - ეს დამახასიათებელია მეორე კატეგორიისთვის [5].

განზრახ.მიზნად ისახავს ქსელის მომხმარებლების დაზიანებას. შეიძლება იყოსაქტიური და პასიური. პასიური მიზნად ისახავს ქსელის საინფორმაციო რესურსების უნებართვო გამოყენებას და არ ახდენს რაიმე განსაკუთრებულ გავლენას ქსელების ფუნქციონირებაზე. უსაფრთხოების აქტიურ საფრთხეებს აქვს მიზანმიმართული ზემოქმედება აპარატურულ, პროგრამულ და საინფორმაციო ქსელის რესურსებზე, რაც იწვევს ამ უკანასკნელის მუშაობაში ჩავარდნას. ეს ეხება საკომუნიკაციო ხაზების, ოპერაციული სისტემების და კომპიუტერული აღჭურვილობის განადგურებას. აქტიური საფრთხეები ასევე მოიცავს მომხმარებლის მონაცემთა ბაზებიდან ინფორმაციის დამახინჯებას.

ყველაზე გავრცელებული პრობლემები, რომლებსაც ონლაინ მომხმარებლები აწყდებიან, არის მონაცემთა ქურდობა, ვირუსები და ჰაკერები. თითოეული საფრთხის მახასიათებლები: სანამ განვიხილავთ ინტერნეტში ინფორმაციის დაცვის აუცილებლობას, ჩვენ გავაანალიზებთ საფრთხეების ძირითად ტიპებს, რომლებსაც მომხმარებლები აწყდებიან.როდესაც ვსაუბრობთ უსაფრთხოების საფრთხეებზე, ვგულისხმობთ ქმედებებს

და მოვლენებს, რომლებიც ამახინჯებენ, იწვევენ მონაცემთა დაკარგვას და უკანონო გამოყენებას.

ჰაკინგი. თავდამსხმელები იღებენ წვდომას პროფილების, ელ.ფოსტის, ვებსაიტების და კომპიუტერული სისტემების ანგარიშის ინფორმაციაზე. თუ ქსელის დაუცველობაზე თავდასხმა წარმატებულია (მათ შორის RDP პროტოკოლის გამოყენებით, რომლის მეშვეობითაც ხდება კავშირები დისტანციურ სამუშაო სადგურებთან), თაღლითები შეძლებენ მიიღონ სრული დისტანციური წვდომა მიმდინარე მომხმარებლის მოწყობილობებზე.

მავნე პროგრამები და ვირუსები. ჩვენ ვსაუბრობთ ჭიებზე, ტროიანებზე და სხვა მავნე პროგრამებზე. ასეთი პროგრამული უზრუნველყოფა შექმნილია სპეციალურად სერვერების, კომპიუტერების, ქსელების დაზიანების მიზნით, კონფიდენციალური ინფორმაციის მოპარვის მიზნით. ვირუსები შეიძლება გავრცელდეს მავნე რეკლამის სახით. მომხმარებელი აჭერს შეტყობინებას, რის შემდეგაც მის მოწყობილობაზე დაინსტალირდება ვირუსი. ასევე, მრავალი მოწყობილობის მფლობელი „იჭერს“ მავნე პროგრამას ინფიცირებული საიტების მონახულების შემდეგ. ამიტომ, ნუ გახსნით გაუგებარ ბმულებს, თუნდაც მეგობრების შეტყობინებებიდან, ნუ უგულებელყოფთ ანტივირუსულ გაფრთხილებებს და აუცილებლად გამოიყენეთ ანტივირუსული პროგრამები.

პირადობის ქურდობა. თავდამსხმელები დაინტერესებულნი არიან მომხმარებელთა პერსონალური მონაცემებით, რათა გამოიყენონ ისინი საკუთარი ინტერესებისთვის ან შემოსავლის გამომუშავების მიზნით გადაყიდვის გზით. ყველაზე ხშირად, ფინანსური და სხვა ინფორმაცია მიზანმიმართულია. ყველა თანამედროვე მომხმარებლის ამოცანაა მიიღოს ყველა შესაძლო ზომა, რომელიც გაზრდის პერსონალური მონაცემების უსაფრთხოებას. ინფორმაციის ქონა საგრძნობლად ამცირებს მომავალში წარმოქმნილი პრობლემების რისკს.

ფიშინგი. ასევე ელ.ფოსტის საერთო საფრთხეა. ეს ძველი ონლაინ უსაფრთხოების საფრთხე ჯერ კიდევ არსებობს. საუბარია მიზანმიმართულ კიბერშეტევაზე, რომლის მთავარი ინსტრუმენტი ყალბი ელ.წერილების გაგზავნაა. მომხმარებელი იღებს შეტყობინებას ბანკიდან ან სხვა სანდო კომპანიისგან, ხსნის მას და მიჰყვება ბმულს. ამ უკანასკნელს მომხმარებელიგადაჰყავს მავნე საიტზე, ამიტომ ვირუსი ავტომატურად იტვირთება მოწყობილობაში. თავდამსხმელები იღებენ წვდომას მომხმარებლის პირად ინფორმაციაზე და შეუძლიათ გამოიყენონ ისინი საკუთარი შეხედულებისამებრ[8].

5. ინფორმაციის გაჟონვის შედეგები.

საინფორმაციოსისტემაშიყოველთვისარისმონაცემთადაკარგვის, მოდიფიკაციის, ქურდობისადაგანადგურებისრისკი.

ამისსაპირისპიროდგამოიყენებაინფორმაციისდაცვისსხვადასხვამეთოდი, რომელიცხორციელდებასპეციალიზებულიპროგრამულიუზრუნველყოფისდაყოვლისმომცველიუსაფრთხოებისსისტემებისდანერგვით.

პერსონალური მონაცემების დაცვა არის სახელმწიფოებრივ დონეზე, ერთ-ერთი უმნიშვნელოვანესი მიმართულება ინფორმაციული უსაფრთხოების უზრუნველყოფის ერთიან სისტემაში[7].

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 მონაცემების დაცვასთან დაკავშირებით არსებობს მნიშვნელოვანი შედეგები, თუ რა შეიძლება ზემოქმედებდეს პერსონალური მონაცემების გაჟონვის ალბათობაზე - ძირითადია, დასამუშავებელ პერსონალურ მონაცემებში ცნობების მოცულობა [7] (ცხრილი 1, ცხრილი 2).

ცხრილი 1. პერსონალური მონაცემების შესახებჩანაწერების 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%

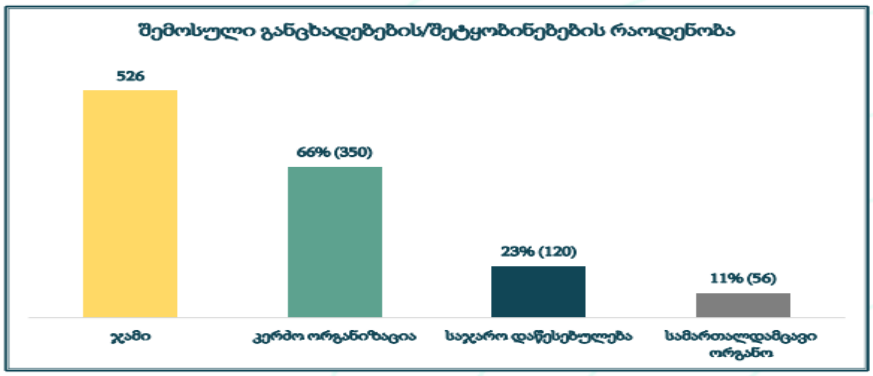
(ინფორმაციის წყარო [6])

ცხრილი 2. პერსონალურ მონაცემებზე წვდომის შესაძლო მაჩვენებლები

მონაცემთა უსაფრთხოების დაცვის მოთხოვნათა შეუსრულებლობა	30%
მონაცემთა დამუშავება კანონით გათვალისწინებული საფუძვლების გარეშე	20%
მონაცემების დამუშავების პრინციპების დარღვევა	15%
პირდაპირი მარკეტინგის მიზნებისათვის მონაცემთა წესების დარღვევით გამოყენება	9%
მონაცემთა სუბიექტის ინფორმირების წესების დარღვევა	8%
ვიდეოთვალთვალის წესების დარღვევა	6%
განსაკუთრებული კატეგორიის მონაცემთა დამუშავება კანონით გათვლისწინებული საფუძვლების გარეშე	4%
უფლებამოსილი პირის მიერ მონაცემთა დამუშავება კანონით გათვალისწინებული წესების დარღვევით	3%
მონაცემთა დამმუშავებლის მიერ მონაცემთა დამუშავების უფლებამოსილი პირისთვის დავალება წესების დარღვევით	2%
მონაცემთა სხვა სახელმწიფოსა და საერთაშორისო ორგანიზაციისათვის გადაცემის წესის დარღვევა	1%

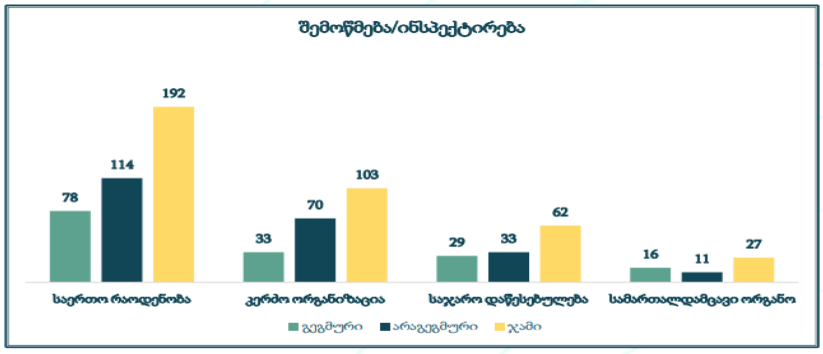
(ინფორმაციის წყარო [6])

პრაქტიკულად, მხოლოდ უსაფრთხოების სამსახურის თანამშრომლების დაშვება პერსონალურ მონაცემებთან შეესაბამება 4%, ხოლო ინფორმაციული ტექნოლოგიების სამსახურის თანამშრომლები ყველაზე ხშირად (41%) არიან პერსონალურ მონაცემებთან, რაც ძალზე დამაფიქრებელია.
საანგარიშოპერიოდში, სამსახურმამიიღო 526 განცხადება/შეტყობინება, რომელთაგან 350 (66%) შეეხებოდამონაცემთადამუშავებასკერძოორგანიზაციებში, 120 (23%) — საჯაროუწყებებში, ხოლო 56 (11%) — სამართალდამცავორგანოებში (ფიგურა 1).

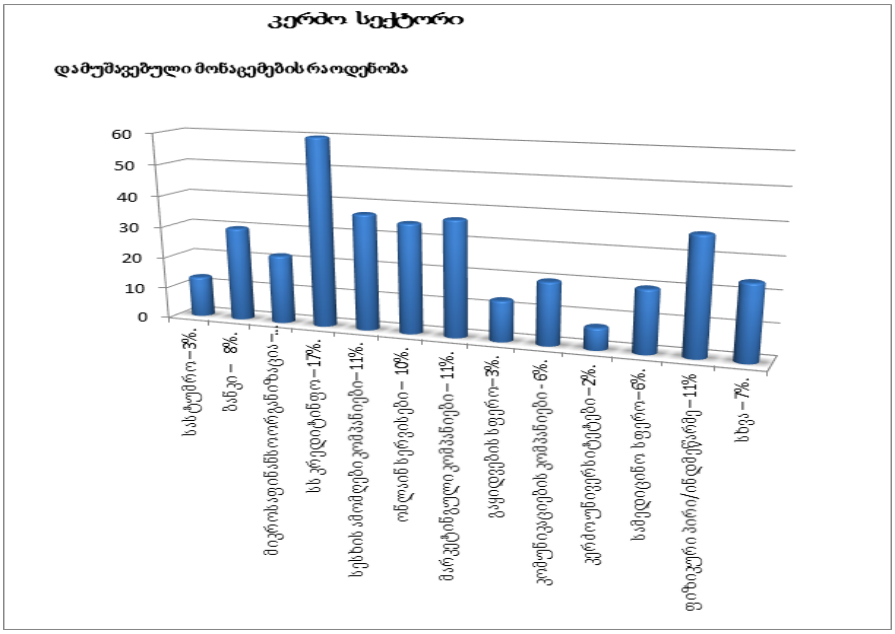


ფიგურა 1.მონაცემთადამუშავებისკანონიერებისშემოწმება[6]

სამსახურმაჩაატარამონაცემთადამუშავებისკანონიერებისშემოწმება (ინსპექტირება) 192 ფაქტზე. მათგან 41% (78) ჩატარდაგეგმურად, ხოლო 59% (114) — არაგეგმურად (ფიგურა 2, ფიგურა 3).



ფიგურა2. გამოვლენილი ადმინისტრაციული სამართალდარღვევები[6]



ფიგურა3.საქართველოს, პერსონალურ მონაცემთა დაცვის სახელმწიფო ინსპექტორის სამსახურის 2018 წლის ანგარიშიდან – მდგომარეობა კერძო სექტორში

6. ინფორმაციის დაცვის საშუალებები

ინფორმაციის დაცვის საშუალებების ნაკრების ოპტიმალურობის კრიტერიუმი, ემყარება ინფორმაციის დაცვის საშუალებების ურთიერთგადაფარვის შესაძლებლობების არსებობას.

ინტერნეტ ქსელებში მონაცემთა დაცვის მეთოდები [3].

ქსელებზე ინფორმაციის დაცვა მნიშვნელოვანი ღონისძიებაა ყველასთვის, ვინც იყენებს ქსელის რესურსებს პირადი და საქმიანი მიზნებისთვის. ოპტიმალური შედეგის მიღწევა შესაძლებელია მხოლოდ ინტეგრირებული მიდგომით. ის მოიცავს ანტივირუსულ დაშიფვრის პროგრამებს, ფაიერვოლებს, ლოკალურ ქსელებზე წვდომის უფლებებს და/ან პასუხისმგებელია კომპანიის შიდა ქსელების ადექვატურ ფიზიკურ იზოლაციაზე სხვა სუბიექტებისგან.

კრიპტოგრაფია ან დაშიფვრა. ასეთი არხების გამოყენებისას მონაცემთა დაცვის დონე დამოკიდებულია დანერგილი ალგორითმების სირთულეზე. ორიგინალური ინფორმაცია იქნება კოდირებული და გადაეცემა მომხმარებლებს შორის. მასალების გამოყენებისას გამოიყენება სპეციალური დეკოდირების გასაღები. ტექნოლოგია უზრუნველყოფს გადაცემული ინფორმაციის სრულ უსაფრთხოებას.

ქსელის დაცვა. ეს ინსტრუმენტები მოიცავს მიმდინარე მოვლენების აუდიტს, ორფაქტორიან ავტორიზაციას და ავთენტიფიკაციას. მრავალფაქტორიანი ავთენტიფიკაცია არის მომხმარებლის იდენტურობის მრავალი დონის შემოწმება. ორი ან მეტი გადამოწმების მეთოდი შეიძლება გამოყენებულ იქნას ერთდროულად. შესვლა-პაროლის წყვილის სტანდარტული მოთხოვნის გარდა, სისტემას შეუძლია მოითხოვოს ერთჯერადი დამატებითი პაროლები, კოდის კითხვები ან ბიომეტრიული ინფორმაცია (თითის ანაბეჭდი, სახის ID და ა.შ.).

პროგრამული უზრუნველყოფის დაცვა. ჩვენ ვსაუბრობთ სპეციალიზებული პროგრამული უზრუნველყოფის გამოყენებაზე, რომელიც ხელს შეუშლის თავდამსხმელებს მონაცემთა მოპარვისკენ მიმართული მოქმედებების ერთობლიობის განხორციელებაში. დაცვის პროგრამული ტიპი მოიცავს ინფორმაციის დაშიფვრას და წვდომის დონის განაწილებას მომხმარებლებს შორის. თქვენ უბრალოდ უნდა ყურადღებით აკონტროლოთ ანტივირუსული განახლებების დროულობა და სამუშაო ოპერაციების განსახორციელებლად ონლაინ ბრაუზერების არჩევანი. ბრაუზერები არის ადგილი, სადაც კონფიდენციალური მონაცემები გაჟონავს.

ჩაშენებული ანტივირუსული დაცვა. ხელს უშლის ქსელებში არაავტორიზებულ წვდომას ინფიცირებული ობიექტების ჯერ აღმოჩენით და შემდეგ იზოლირებით[9].

კავშირის მონიტორი. აკონტროლებს ყველა დამყარებულ კავშირს, განსაზღვრავს არხის დატვირთვას, ტრაფიკის ტიპებს და სამუშაოს ხელმისაწვდომ მიმართულებებს.

ანტივირუსი. პროგრამა ამოწმებს FTP, HTTP ნაკადებს და ფაილებს მათში, ქსელის სიჩქარის შენელების გარეშე. ანტივირუსი საჭიროა ინტერნეტ რესურსებზე წვდომის დასარეგულირებლად, გამორიცხავს პოტენციურად საშიშ საიტებს კლიენტის ქსელების დასაცავად.

პორტის გადაგზავნის წესები. უსაფრთხოების ამჟამინდელი დონის გაზრდის მიზნით, ცენტრალიზებულ დონეზე დაყენებული პორტის ნომრები შეიცვლება თვითნებურად შერჩეული პროტოკოლებისთვის. ამ შემთხვევაში, ICS სისტემები გადაამისამართებენ მიმდინარე პაკეტებს ახალზე. ეს გაართულებს ადგილობრივ ქსელებზე გარედან წვდომას და იქნება ეფექტური ღონისძიება დამატებითი დაცვის უზრუნველსაყოფად.

IDS Snort . შეჭრის გამოვლენის სისტემა არის თავისუფალი ტიპის პროტოკოლი, რომელიც შეიქმნა გარე შეტევების მცდელობების იდენტიფიცირებისა და ანალიზისთვის და

მუშაობს რეალურ დროში განუწყვეტლივ. შეჭრის გამოვლენას და ყველაზე ცბიერ შეტევებსაც კი აქვთ საერთო მახასიათებლები - ისინი ტიპიურია და მათი ზუსტად გამოვლენა შესაძლებელია. შესაბამისად, მონაცემთა ქურდობა შეიძლება ეფექტურად იქნას აცილებული.

მაგიდის ARP ტრეკერი. როდესაც ვსაუბრობთ ARP-ზე, ვგულისხმობთ პროტოკოლს, რომელიც ჩაწერს ფაქტებს MAC მისამართების შესატყვისი IP მისამართების სესიის ბოლოს ან სანამ მისამართი რაიმე მიზეზით შეიცვლება. თუ კორესპონდენციაში მოხდა არასანქცირებული ცვლილება, თვალთვალის მოდული ნებისმიერ მოქმედებას აღიქვამს, როგორც შენიღბვის ან ჩანაცვლების მიზანმიმართულ მცდელობას და დაიწყებს განგაშის ატეხვას [10].

დღეს საინფორმაციო ქსელის უსაფრთხოება ახალ დონეს აღწევს. ტრაფიკი უნდა გაანალიზდეს რაც შეიძლება სრულყოფილად - განაცხადიდან ფიზიკურ დონეებამდე. კერძოდ, ICS იყენებს მონაცემთა დაცვის სხვადასხვა მეთოდს. ეს საშუალებას იძლევამიიღწეს ქსელებში ინფორმაციის უსაფრთხოების მაქსიმალურიდონე. თქვენ თავად შეგიძლიათ გამოიყენოთ სხვადასხვა მეთოდი, მაგრამ ICS ითვლება მოწინავე, ყველაზე ეფექტურ სისტემად. მისი არჩევით თქვენ მიიღებთ გარანტირებულ შედეგებს. გარდა ამისა, ჩვენ გირჩევთ, მიჰყვეთ მიმოხილვაში მითითებულ რეკომენდაციებს და გამოიყენოთ მონაცემთა დაცვის გაფართოებული ტექნიკა [7].

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

7. მოსალოდნელი საფრთხეების მოდელის შედგენა

ობიექტების ინფორმაციული უსაფრთხოების უზრუნველყოფის შემდეგი ზომები,მეთოდები და საშუალებები არსებობს [1]:

- საკანონმდებლო (სამართლებრივი) ზომები;
- ორგანიზაციული (ადმინისტრაციული) დაცვის ზომები;
- პროგრამულ - ტექნიკური ზომები;
- არასანქცირებული ჩართვებისა და მიერთებებისაგან დაცვის საშუალებები;
- იდენტიფიცირებისა და აუტენტიფიცირების საშუალებები;
- შეღწევების გამოჯვნის 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.

მიზანშეწონილია მოსალოდნელი საფრთხეების მოდელის შედგენა, მაგალითად:

$$Aj = (Pj ; Xj), \quad (1)$$

სადაც, Pj - არის მოსალოდნელი საფრთხის ალბათობა;

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

ცხადია, თუ ცნობილი იქნება ობიექტის დაცულობის ალბათობა და ბოროტმოქმედის შესაძლო პოტენციალი, ობიექტისათვის მოსალოდნელი საფრთხის, ლოგიკურ–ალბათური ფუნქციის გამოსახულება ასე ჩაიწერება:

$$Pj = (P1,P2), \qquad (2)$$

სადაც P1 – არის მისაღწევი დაცულობის ალბათობა;

P2 – ბოროტმოქმედის შესაძლებლობების (პოტენციალის) ალბათობა;

ობიექტზე უკვე არსებული დაცვის სისტემის შესაძლებლობებიდან გამომდინარე,მოსალოდნელი საფრთხის ლოგიკურ–ალბათური ფუნქციის გამოსახულებას ექნება შემდეგი სახე:

$$Pj = (P1 \text{ საწყისი }, P2), \qquad (3)$$

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

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

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 N_i რაოდენობის ფუნქციებს, მაშინ

$$\sum_{i=1}^{K} N_i = N_{\text{დაცვის}}$$

სადაც $N_{\text{დაცვის}}$ - არის ინფორმაციის დაცვის კომპლექსური სისტემის ფუნქციების რაოდენობა. იმის გათვალისწინებით, რომ ინფორმაციის დაცვის საშუალებებისათვის შერჩეულ კრიტერიუმებს უზრუნველყოფს განსხვავებული დანიშნულებების სისტემები. ცხადია:

$$\sum_{i=1}^{K} N_i < N_{\text{დაცვის}}$$

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:

$$\begin{cases} \sum_{i=1}^{K} N_i < N_{\text{დაცვის}} \\ X_i \cong X_{i\text{მოთხოვნილი}}, \quad i=1,K \end{cases}$$

8. დასკვნა

ობიექტებისათვის სატელეკომუნიკაციო ქსელებსა და სისტემებს უნდა გააჩნდეთ მზადყოფნის კოეფიციენტები კრიტიკულობის კოეფიციენტების შესაბამისად, სადაც მზადყოფნის კოეფიციენტების მნიშვნელობები განსაზღვრული იქნება მდგრადობის (სიცოცხლისუნარიანობის) შესაბამისად. აუცილებელია ახალი, ფუნდამენტური შედეგი, როგორც ინფორმაციაზე შემოტევებისაგან დაცვის პრობლემების მეცნიერულად

ფორმულირებისათვის, ასევე ინფორმაციის ზემოქმედებების აცილების მეთოდებისა და საშუალებების ანალიზისა და სინთეზისათვის. იმის გათვალისწინებით, რომ შემოტევების მეთოდები და მექანიზმები აგრეთვე, განიცდიან სრულყოფას, აუცილებელია ინფორმაციის დაცვის კომპლექსური სისტემის გათვალისწინება საერთო სარგებლობის ქსელებში.ტექნიკურ სრულყოფასთან ერთად შეიძლება შეიქმნას დაცული ინფორმაციული საზოგადოება. ამისათვის ტექნიკური საშუალებები არსებობს, მაგრამ არ არსებობს ნორმატიული ბაზა. ინფორმაციის მიმოცვლის პროცესში, სატელეკომუნიკაციო ქსელში შესაძლო ხიფათის წარმოქმნის გათვალისწინება და მისი მართვის უნარის არსებობა წარმოადგენს ინფორმაციული დაცულობის უზრუნველყოფის საფუძველს.საქართველოსთვის არსებულ განსაკუთრებულ საფრთხეს წარმოადგენს ყველაზე მაღალი ალბათობით სახელმწიფო საინფორმაციო რესურსებზე შემოტევები. 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.

ბიბლიოგრაფია

1. https://rt-solar.ru (15.11.2024)
2. ИСО / МЭК 27032:2012 – Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности (ISO/IEC 27032:2012 Information technology - Security techniques – Guiolelines forcybersecurity).

URL:http://www.iso.org/iso/ru/catalogue_detail?csnumber=44375, (15.11.2024).

3. 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
4. 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.
5. Сабанов А.Г. Анализ применимости методов оценки рисков к процессам аутентификации при удаленном электронном взаимодействии. //Электросвязь, №5,2014 стр.44-47.
6. პერსონალურმონაცემთადაცვისსამსახურის 2023 წლისსაქმიანობისსტატისტიკა.

URL:https://shorturl.at/wugEF

7. ყიფიანი ქ. „ინფორმაციის დაცვის მეთოდების კვლევა სატელეკომუნიკაციო ქსელებისა და სისტემების სტრუქტურისა და ფუნქციონირების ალგორითმის გათვალისწინებით“.დისერტაცია. 2019. გვ. 106.
8. https://sky-dynamics.ru/ (15.11.2024).
9. https://xserver.a-real.ru/blog/useful/zashchita-informatsii-v-seti-internet/(15.11.2024).
10. https://sky-dynamics.ru/stati/metody-i-sredstva-zashhity-informacii-v-internete/(15.11.2024).
11. https://www.edpb.europa.eu(15.11.2024).