

ირაკლი მინაშვილი

**ციფრული დანაშაულის
გამოძიების ტექნიკა
და მეთოდика**



თბილისი 2019

ნაშრომი „ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდოლოგია“ გამოცემულია საქართველოს ტექნიკური უნივერსიტეტის სამართლისა და საერთაშორისო ურთიერთობების ფაკულტეტის სამეცნიერო-კვლევითი პროექტის „მტკიცების (მტკიცებულებათა შეგროვების, საპროცესო დამაგრების შემოწმებისა და შეფასების) აქტუალური პრობლემების“ ფარგლებში.

მთავარი რედაქტორი:	ირაკლი გაბისონია
რედაქტორები:	ჯემალ გაბელია თეიმურაზ დარსანია
რეცენზენტები:	ჯემალ გახოკიძე შოთა რიყამაძე
ტექნიკური რედაქტორი:	ელენე ჩალაძე
ტექნიკური უზრუნველყოფა:	თამარ ბარამია

© გამომცემლობა „მერიდიანი“, 2018

© ირაკლი მინაშვილი



გამომცემლობა „მერიდიანი“,
თბილისი, ალ. ყაზბეგის გამზ., №47.

☎ 239-15-22

E-mail: meridiani777@gmail.com

ISBN 978-9941-25-700-1



ნაშრომი „ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდები“ სამართლისა და საერთაშორისო ურთიერთობების ფაკულტეტის სამეცნიერო-კვლევითი პროექტის „მტკიცების (მტკიცებულებათა შეგროვების, საპროცესო დამაგრების შემოწმებისა და შეფასების) აქტუალური პრობლემების“ ფარგლებში მომზადდა.

საქართველოს ტექნიკური უნივერსიტეტის სამართლისა და საერთაშორისო ურთიერთობების ფაკულტეტი აქტიურად ცდილობს, რომ ხელი შეუწყოს სხვადასხვა დარგების ახალი მიმართულებების შექმნას და განვითარებას, სწორედ ამ მიზანს ემსახურება ფაკულტეტზე მიმდინარე სხვადასხვა სამეცნიერო-კვლევითი პროექტები.

აღსანიშნავია, რომ ნაშრომი არის ინოვაციური, ვინაიდან წარმოდგენილია ორი — იურიდიული და კომპიუტერული მეცნიერებების მოკლე ანალიზი და აღნიშნული დარგების პრაქტიკული ცოდნის მოცულობითი განხილვა. იგი უდავოდ პასუხობს დროის მოთხოვნებს და მას არამხოლოდ დიდი პრაქტიკული მნიშვნელობა აქვს არამედ სავსებით შესაძლებელია სახელმძღვანელოდ იქნეს გამოყენებული საერთაშორისო და ეროვნული უსაფრთხოების, კერძოდ, კიბერტერორიზმისა და ციფრულ დანაშაულთან დაკავშირებული სასწავლო პროგრამების განხილვისა და შედგენისათვის.

ნაშრომი რეკომენდირებულია სამართლისა და საერთაშორისო ურთიერთობების ფაკულტეტის ბაკალავრების, მაგისტრებისა და დოქტორანტებისათვის. მისი გამოყენება ასევე სასარგებლო იქნება ოპერატიული და საგამოძიებო-სამსახურის მუშაკებისათვის, რომლებიც იძიებენ ციფრული დანაშაულს.

სარჩევი

შესავალი	7
კარი I ციფრული დანაშაულის ცნება, არსი და კლასიფიკაცია	9
თავი I ციფრული დანაშაული	9
1.1. ციფრული დანაშაულის ცნება და არსი	9
1.2. ციფრულ დანაშაულის კლასიფიკაცია ქართულ სისხლის სამართალში	18
თავი II ციფრულ დანაშაულთან დაკავშირებული ტერმინოლოგია	24
2.1. საერთაშორისო სამართლებრივი ტერმინოლოგია ციფრული დანაშაულის შესახებ	24
2.2. ციფრული დანაშაულის შესახებ სამართლებრივი ტერმინოლოგია ქართულ კანონმდებლობაში	26
თავი III ციფრულ დანაშაულთან ბრძოლის	34
სამართლებრივი რეგულაციები	34
1.1. ციფრულ დანაშაულთან ბრძოლის საერთაშორისო სამართლებრივი რეგულაციები	34
1.2. ციფრულ დანაშაულთან ბრძოლის სამართლებრივი რეგულაციები ამერიკის შეერთებული შტატებში	42
1.3. ციფრულ დანაშაულთან ბრძოლის სამართლებრივი რეგულაციები რუსეთის ფედერაციაში	44
კარი II ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდика	46
თავი IV ციფრული მტკიცებულება	46
4.1. ციფრული მტკიცებულების რაობა და ადგილი მტკიცებულებათა კლასიფიკაციაში 4.....	6
თავი V ციფრული ინფორმაციის შემცველი მოწყობილობის ამოღების მეთოდика და ტექნიკა	50
5.1. ციფრული ინფორმაციის შემნახველი კომპიუტერული მოწყობილობის ამოღების სამართლებრივი საფუძვლები	50
5.2. დეტალიზაციის მეთოდური პრობლემა კომპიუტერული მოწყობილობის ამოღების დროს	54
5.3. ციფრული ინფორმაციის შემნახველი კომპიუტერული მოწყობილობების სახეები	57
5.4. პერსონალური კომპიუტერის ამოღების ტექნიკური პროცედურები და მეთოდები	61

5.5. ციფრული ინფორმაციის შემნახველი კომპიუტერის ნაწილების ძეგნის დამოღების ტექნიკური პროცედურები და მეთოდები	65
5.6. ციფრული ინფორმაციის შემნახველი სხვა მოწყობილობების ძეგნის და ამოღების ტექნიკური პროცედურები და მეთოდები	71
5.7. კომპიუტერული მოწყობილობის ამოღებისათვის საჭირო აღჭურვილობა და შეფუთვის და გადატანის დროს გასათვალისწინებელი საკითხები	82

თავი VI კომპიუტერული სისტემიდან ციფრული ინფორმაციის

გამოთხოვის ტექნიკა და მეთოდიკა	86
6.1. კომპიუტერული სისტემიდან ციფრული ინფორმაციის გამოთხოვის ზოგადი სამართლებრივი საფუძვლები და პროცედურები	86
6.2. კომპიუტერული სისტემიდან ციფრული ინფორმაციის გამოთხოვის სამართლებრივი საფუძვლები და პროცედურები დაცვის მხარისათვის	107
6.3. მომსახურების მომწოდებლებისაგან ციფრული ინფორმაციის გამოთხოვის ტექნიკური პროცედურები და მეთოდები	113
6.4. კომპიუტერული მოწყობილობიდან ციფრული ინფორმაციის გამოთხოვის ტექნიკური პროცედურები და მეთოდები	117
6.5. დეტალიზაციის მეთოდური პრობლემა ინფორმაციის გამოთხოვის დროს	154
6.6. სოციალური ქსელის – facebook-ის დათვალიერების და ინფორმაციის გამოთხოვის ტექნიკური პროცედურები და მეთოდები	155

თავი VII კომპიუტერულ მოწყობილობაში დაცული ციფრული

ინფორმაციის დათვალიერების ტექნიკა და მეთოდიკა	161
7.1. კომპიუტერულ მოწყობილობაში დაცული ციფრული ინფორმაციის დათვალიერების სამართლებრივი საფუძვლები და პროცედურები	161
7.2. პერსონალურ კომპიუტერში დაცული ციფრული ინფორმაციის დათვალიერების ტექნიკური პროცედურები და მეთოდები	166
7.3. მობილურ ტელეფონში დაცული ციფრული ინფორმაციის დათვალიერების ტექნიკური პროცედურები და მეთოდები	186
7.4. კომპიუტერის IP მისამართის დადგენის ტექნიკური პროცედურები და მეთოდები	195

თავი VIII გამომძიებლის მიერ წარმოებული ციფრული ვიდეო

და ფოტო გადაღების ტექნიკა და მეთოდიკა	203
8.1. ციფრული ვიდეო და ფოტო გადაღების ტექნიკური პროცედურები და მეთოდები	203

თავი IX კომპიუტერულ-ტექნიკური ექსპერტიზა	210
9.1. კომპიუტერულ-ტექნიკური ექსპერტიზის სახეობები	210
თავი X საგამოძიებო მოქმედების ჩატარებისათვის საჭირო კომპიუტერის ფუნქციური კლავიშები	215
10.1. კლავიატურის სტრუქტურა	215
10.2. Wondows სისტემის პროგრამის კლავიშთა კომბინაციები	217
10.3. Mac os სისტემის პროგრამის კლავიშთა კომბინაციები	224
10.4. Linux სისტემის პროგრამის კლავიშთა კომბინაციები 2	25
თავი XI ციფრული ინფორმაციის გამოთხოვასთან დაკავშირებული საპროცესო და საგამოძიებო დოკუმენტების ნიმუშები	227

შესავალი

ნაშრომი „ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდები“ არის არასტანდარტული სტილის, ვინაიდან თქვენს წინაშე წარმოდგენილია ორი სხვადასხვა დარგის - სამართალის და კომპიუტერული მეცნიერების ერთობლივი ნაშავი, რომლებიც ქმნიან ერთ მნიშვნელოვან მიმართულებას-ციფრული დანაშაულის გამოძიების მეთოდოკას.

ნაშრომის პირველ ნაწილში წარმოდგენილი არის თეორიული საკითხები - რომლებიც შეეხება ციფრული დანაშაულის ცნების და არსის განმარტებას. აღსანიშნავია ისიც, რომ „ციფრული დანაშაული“ ქართულ კანონმდებლობაში როგორც დანაშაულის ცალკე ცნება არ გვხვდება, მაგრამ იმ შემთხვევაში, როდესაც დანაშაული ჩადენილია ციფრული საგნის საშუალებით სახეგუა სწორედ ციფრული დანაშაული.

ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდოკაში, თქვენ ვერ ნახავთ სხვადასხვა სახის ნიმუშების აღებას, ვერ ნახავთ სტანდარტულ ექსპერტიზებს, სამაგიეროდ წარმოდგენილი იქნება კომპიუტერული სისტემიდან ინფორმაციის გამოთხოვა, კომპიუტერული პროგრამები და მათთან მუშაობის სპეციფიკა, რომელიც აუცილებელია იმ გამომძიებლებისათვის, ვინც იძიებს მსგავსი ტიპის დანაშაულს.

რაც შეეხება ნაშრომის მეთოდოლოგიას, იგი ახლოს არის არსებულ პრაქტიკასთან და თანხვედრაშია ამ მიმართულებით არსებულ თეორიულ კვლევებთან.

ნაშრომში შეხვდებით სააპელაციო და საკონსტიტუციო სასამართლოს გადაწყვეტილებებს და მათ ანალიზს, ვინაიდან საკითხს - რომელიც თეორიულად რეგულირებული არ არის - სამართლებრივ კრილში არეგულირებს სწორედ სააპელაციო სასამართლოს განჩინებები თუ საკონსტიტუციო სასამართლოს გადაწყვეტილებები.

არასტანდარტულია თავად ნაშრომის სტრუქტურა, რაც გამოწვეულია იმით, რომ არის ფოტოლიუსტრაცია, რაც გაცილებით ამარტივებს და თვალსაჩინოს ხდის საგამომიებო მოქმედებების წარმოებას. ასევე, მნიშვნელოვანია სამართლებრივი ტერმინოლოგიის განმარტება, რაც ეხება ციფრულ დანაშაულებს, რის შემდეგაც წარმოდგენილი არის საერთაშორისო, ევროპის, აშშ-ს და რუსეთის პრაქტიკული გამოცდილება ციფრულ დანაშაულთან ბრძოლის კუთხით.

ასევე დამუშავებულია ქართულ სისხლის სამართალში არსებული მუხლები და მათი შესაბამისობა საერთაშორისო დანაშაულის კლასიფიკაციასთან, განხილულია დანაშაულის გამოძიების მეთოდოკა; კომპიუტერის აპოლებს სამართლებრივი და ტექნიკური პროცედურები, კომპიუტერული სისტემიდან ინფორმაციის გამოთხოვის სამართლებრივი და ტექნიკური პროცედურები და კომპიუტერული სისტემის დათვალიერების სამართლებრივი ტექნიკური პროცედურები. ასევე მნიშვნელოვანი ადგილი უჭირავს IP მისამართის დადგენას და ექსპერტიზის დანაშინის თავისებურებებს. ნაშრომის ბოლოს კი წარმოდგენილია მნიშვნელოვანი კომპიუტერის კლავიშთა კომბინაციები, რომლებიც აუცილებელია იცოდეს თითოეული საგამომიებო მოქმედების ჩამტარებელმა.

აქვე გვინდა აღვნიშნოთ, რომ ამ კუთხით მუშაობა გრძელდება, მომავალში შემოგთავაზებთ ნაშრომის მეორე ნაწილს, სადაც საუბარი იქნება პლასტიკური ბარათების საშუალებით და ციფრული ხელმოწერის გამოყენებით ჩადენილი დანაშაულების გამოძიების მეთოდოკაზე და ფარული საგამომიებო მოქმედებების შედეგად მოპოვებულ აუდიო-ვიდეო მასალაზე-როგორც ციფრულ მტკიცებულებებზე.

გამომცემლობის მიერ, ავტორისა და რედაქტორებისათვის შემოთავაზებული იქნა სქოლიოს შედგენა თანამედროვე QR კოდური ფუნქციით. რაც გულისხმობს იმას, რომ სქოლიოში მითითებული ყველა ელექტრონული გვერდი მასზე განთავსებული შესაბამისი ინფორმაციით, სქოლიოში აღრიცხული იქნება QR კოდის საშუალებით.

ავტორის მიერ მიწოდებული სქოლიოში ასახული ტექსტობრივი ინფორმაციის თანხვედრაზე სქოლიოში მითითებულ QR კოდებთან, პასუხისმგებლობას იღებს გამომცემლობა.

QR კოდი „Quick Response“ – „სწრაფი პასუხი“ არის ორგანოზომილებიანი კოდი, რომელიც შეიქმნა იაპონიაში 1994 წელს, კოდი ინახავს დაშიფრულ მონაცემებს/ინფორმაციას ამა თუ იმ პროდუქტის შესახებ. QR კოდი შეიძლება შეიცავდეს ტექსტებს, ვებ-გვერდის მისამართს, SMS ან E-mail; შეცვლინებასა და სხვადასხვა სახის ინფორმაციას. QR კოდის საშუალებით ინფორმაციის გაცვლის მრავალი გზა არსებობს, თუმცა მსოფლიოში ყველაზე პოპულარულია Mobile Tagging-ი, მობილური ტელეფონის საშუალებით კომპიუტერის მონიტორიდან ან ნაბეჭდი მასალიდან QR კოდის სწრაფი წაკითხვა და მასში შენახული ინფორმაციის მყისიერი მიღება. QR კოდის სკანერი (სპეციალური პროგრამა) ავტომატურად ამოიცნობს დაშიფრულ ინფორმაციას ნებისმიერ ბრაუზერში ან ფურცელზე.¹

როდესაც ნაშრომის სქოლიოში იხილავთ QR კოდს, შეგიძლიათ შესაბამისი მოწყობილობის კანერით დაადოქსიროთ ის და მალევე ავტომატურად გაგისვინთ შესაბამის ვებ-გვერდს.

QR კოდის წამკითხველი პროგრამები;

ინტერნეტის საძიებო სისტემაში აკრიბეთ QR Scanner ან QR Reader, კომპიუტერი მოგცემთ რამდენიმე შესაბამის ვერსიას, საიდანაც შეგიძლიათ აირჩიოთ და გადმოწეროთ თქვენთვის მისაღები ნებისმიერი პროგრამა, რომლის გააქტიურების შემდეგაც პროგრამა დაიწყებს ფუნქციონირებას.

მაგალითად:

ანდროიდის სისტემის მქონე ტელეფონებში და სმარტფონებში შესაბამისი პროგრამის გადმოსაწერად ეწვიეთ ვებ-გვერდს - <https://play.google.com/store/search?q=qr> სადაც არის არჩევანი შესაბამისი QR პროგრამების.

ანდროიდის სისტემის მქონე ტელეფონებში და სმარტფონებში შესაბამისი პროგრამის გადმოსაწერად შედით ფუქციონალში - Play Market სადაც ძებნა ფუნქციონალში აკრიბეთ QR Scanner ან QR Reader, ჩემოთვლილი პროგრამებიდან აირჩიეთ გადმოწერეთ თქვენთვის მისაღები პროგრამა.

iPhone, iPad, or iPod - ში შესაბამისი პროგრამის გადმოსაწერად ეწვიეთ ვებ-გვერდს - <https://apps.apple.com/us/app/qr-reader-for-iphone/id368494609> და გადმოწერეთ პროგრამა.

iPhone, iPad, or iPod - ში შესაბამისი პროგრამის გადმოსაწერად შედით ფუქციონალში - App Store სადაც ძებნა ფუნქციონალში აკრიბეთ QR Scanner ან QR Reader და ჩემოთვლილი პროგრამებიდან გადმოწერეთ თქვენთვის მისაღები პროგრამა.

კარი I

ციფრული დანაშაულის ცნება, არსი და კლასიფიკაცია

თავი I

ციფრული დანაშაული

1. 1.1. ციფრული დანაშაულის ცნება და არსი

მსოფლიოს მასშტაბით დღითი-დღე ვითარდება კომპიუტერული მოწყობილობები და უფრო სრულყოფილი და მრავალფუნქციური ხდება კომპიუტერული სისტემები, ხოლო მთავარი საგანი, რის საფუძველზეც ყოველივე აღნიშნულის სწრაფი განვითარება ხდება არის შესაბამისი ციფრული პროგრამები.

დღეის მდგომარეობით მსოფლიოში და მათ შორის საქართველოშიც გვაქვს სამართლებრივი ცნებები „კიბერდანაშაული“, „კომპიუტერული დანაშაული“ და ასე შემდეგ, მაგრამ როდესაც უკვე გამოძიება იწყება, პრაქტიკაში საქმე გვაქვს სხვა რეალობასთან, გამოძიება ეძებს არა კომპიუტერულ მოწყობილობას — როგორც მტკიცებულებას, არამედ კომპიუტერულ სისტემაში დაცულ ინფორმაციას, რომელიც თანამედროვეობაში არის ციფრული ბუნების.

ამდენად, გამოძიებელი იძიებს ციფრულ და არა კომპიუტერულ დანაშაულს, მაგალითისათვის შესაძლოა მოვიყვანოთ შემთხვევა, როდესაც დამნაშავე ციფრული ვიდეოკამერის გამოყენებით გადაიღებს პიროვნების პირადი ცხოვრების ამსახველ ჩანაწერს, შემდგომ გადაიწერს მას მობილურ ტელეფონში და შესაბამისი დანაშაულებრივი განზრახვით და მიზნით ავრცელებს სოციალური ქსელის საშუალებით, ასეთ შემთხვევაში სახეზეა საქართველოს სისხლის სამართლის კოდექსით გათვალისწინებული (შემდგომში სსკ) დანაშაული, მაგრამ – რა არის დანაშაულის საგანი – ვიდეოკამერა – მობილური ტელეფონი – თუ სოციალური ქსელი –? დანაშაულის საგნის ბუნებიდან გამომდინარე აშკარაა, რომ არცერთი ზემოაღნიშნული, აღნიშნულ და მსგავს შემთხვევებში დანაშაულის საგანი არის გადაღებული ვიდეოჩანაწერი, მაგრამ რა სახის ინფორმაცია აღნიშნული ჩანაწერი? – ეს არის ციფრული ინფორმაცია, ხოლო რაც შეეხება ვიდეოკამერას და შემდგომ მობილურ ტელეფონს – აღნიშნული ნივთები გვევლინებიან დანაშაულის ხერხად და საშუალებად.

წარმოდგენილი ნაშრომის შექმნა, განაპირობა სწორედ სისხლის სამართლის პროცესის წარმოების ეტაპზე — ციფრული დანაშაულის გამოძიებისას თეორიული და პრაქტიკული ცოდნის არათანმიმდევრულობამ და პრაქტიკაში არსებულმა იმ პრობლემებმა, რომელთა რეგულირების მიზნითაც სააპელაციო სასამართლო აკეთებს განმარტებებს და აღნიშნული განმარტებები არაპრეცედენტული სამართლის სისტემის ქვეყნის – საქართველოს სისხლის სამართალში, ხდება პრეცედენტული სახისათვის მტარებელი იმიტომ, რომ ცალკე დანაშაულად არ გვაქვს ციფრული დანაშაული და არ არსებობს აღნიშნულის თუნდაც ნაშრომის დონეზე წარმოდგენილი განმარტება.

როდესაც ვმსჯელობთ ციფრულ დანაშაულზე, უპირველეს ყოვლისა აღსანიშნავია, რომ ციფრული დანაშაულის მთავარ ბიოტვს წარმოადგენს ციფრული საგანი, რადგან მის შემთხვევაში, მონაცემთა კომპიუტერული სისტემების და კომპიუტერული მოწყობილობების საშუალებით დამუშავება, არსებითი მნიშვნელობის მქონეა, მიუხედავად იმისა, რომ ბევრ დანაშაულს შემადგენლობაში სიტყვა ციფრული არ უწერია, ხშირად არის ხოლმე შემთხვევები – როდესაც დანაშაულები, ელექტრონული გზით ჩადენის შემთხვევაში ანაცვლებენ ტრადიციული დანაშაულის

შემაღგენლობებს, მაგალითად ქურდობა - როდესაც იგი ჩადენილია ციფრული საგნის გამოყენებით - გადადის ციფრულ დანაშაულში.

ციფრული დანაშაულის ობიექტზე მსჯელობისას დავეთანხმებით ალ. კაცმანს, იმ კონტექსტში, რომ ვინაიდან ინფორმაციის არამართლზომიერი გამოყენების შედეგი სხვადასხვაგვარია, მან შეიძლება დაარღვიოს, როგორც ინტელექტუალური საკუთრების ხელშეუხებლობა, ასევე გამოიწვიოს მოქალაქეთა პირადი ცხოვრების შესახებ ცნობების გახმაურება, ქონებრივი ზიანი, რეპუტაციის შელახვა, წარმოების, დარგის ნორმალური საქმიანობის დარღვევა და სხვა.

რაც შეეხება აღნიშნული დანაშაულის გვარობით ობიექტს; მასში უნდა მოვიზაროთ სისხლის სამართლის კანონით დადგენილი ერთგვაროვანი ან იგივეობითი საზოგადოებრივი ურთიერთობები, რომელთა წინააღმდეგაც მიმართულია დანაშაულებრივი ხელყოფა¹, აქვე გასათვალისწინებელია, რომ მიუხედავად იმისა, რომ ქართულ კანონმდებლობაში არ გვაქვს ციფრული დანაშაულის ცნება, ვხვდებით კომპიუტერულ დანაშაულებს, შესაბამისად გარკვეული პარალელის გავლება მის შემადგენლობასთან შესაძლებელია, მაგრამ არა ზედმიწევნით ანალოგიური პარალელის, მაგალითისათვის - სისხლის სამართლის კოდექსში 35-ე თავი რომელიც ეხება კიბერდანაშაულს, მოცული აქვს სისხლის სამართლის კოდექსის მე-9 კარს რომლის სათაურიც არის „დანაშაული საზოგადოებრივი უშიშროებისა და წესრიგის წინააღმდეგ“, შესაბამისად კიბერდანაშაულის გვარობითი ობიექტი იმპერატიულად არის საზოგადოებრივი უშიშროება და წესრიგი, მაგრამ ციფრული დანაშაულის შემთხვევებს შესაძლოა შეეხვედეთ სხვადასხვა კარში, მაგალითად - როდესაც საავტორო უფლების დარღვევით ხდება ინტერნეტიდან სხვადასხვა ინფორმაციის გადმოწერა. ვინაიდან საქართველოს სისხლის სამართლის კოდექსში კომპიუტერის საშუალებით საავტორო უფლების დარღვევის სპეციალური მუხლი არ არის გათვალისწინებული, პირის ქმედება კვალიფიცირდება ორი მუხლით: საქართველოს სისხლის სამართლის კოდექსის 284-ე (კომპიუტერულ სისტემაში უნებართვო შეღწევა) და 189-ე (საავტორო, მოპოვანვე უფლების მფლობელისა და მონაცემთა ბაზის დამამზადებლის უფლების ხელყოფა) მუხლებით - ასეთ შემთხვევაში ქმედების გვარობით ობიექტად ვერ იქნება მოაზრებული მხოლოდ საზოგადოებრივი უშიშროება და წესრიგი, ვინაიდან საკუთრების წინააღმდეგ მიმართული დანაშაულის გვარობით ობიექტს წარმოადგენს საკუთრების ურთიერთობა მთლიანად, ამ შემთხვევაში უკვე გადავდივართ ძირითად და დამატებით ობიექტიან დანაშაულზე და სახეზე იქნება სამართლებრივი სიკეთე საკუთრების სახით და საზოგადოებრივი უშიშროების და წესრიგის სახით.

რაც შეეხება სახეობითი ობიექტის განსაზღვრას, აღნიშნულის კონკრეტიზაცია ციფრული დანაშაულის კონტექსტში ამ მოცემულობის სისხლის სამართლის კოდექსის საფუძველზე შეუძლებელია, მაგრამ უნდა აღინიშნოს, რომ უმეტესწილად სახეზე გვექნება ორ ან მეტ ობიექტიანი დანაშაულები.

ციფრული დანაშაული, უნდა მივაკუთვნოთ დანაშაულთა იმ ჯგუფს, რომელშიც ყოველთვის არსებობს დანაშაულის საგანი, ამგვარი დანაშაული გამოხატულებას პოულობს არამატერიალური სამყაროს საგანზე - ანუ ციფრულ საგანზე მართლსაწინააღმდეგო ზემოქმედების შედეგად, უფრო კონკრეტულად რომ განვიხილოთ, ციფრული დანაშაულის საგანი არის ციფრული ინფორმაცია; რომლის დამუშავებაც ხდება ციფრული სისტემის საშუალებით, რომელიც „[...] არის ციფრული ფორმით (კოდებით) წარმოდგენილი ინფორმაციის დამუშავების სისტემა. ინფორმაციის ციფრული ფორმით წარმოდგენა ფართოდ გამოიყენება ინფორმაციის დამუშავების სისტემებში, მართვის ავტომატიკისა და ავტომატიზებულ სისტემებში, ციფრულ საკომუნიკაციო სისტემებში და ა.შ. ამდენად, ციფრული ფორმით წარმოდგენილი ინფორმაციის გამოყენების არეალი დღეისათვის მეტად ფართოა და ციფრული სისტემების განვითარების თავბრუდამხვევი ტემპების გამო, გამოყენების სფეროების მართო ჩამოთვლაც კი რთული საქმეა. ციფრული სისტემა, როგორც ნებისმიერი სხვა

სისტემა, ხასიათდება სტრუქტურით, იერარქიულობით და ფუნქციით.“²

თავად „ტერმინი «ციფრული სისტემა» (ცს) სამეცნიერო-ტექნიკურ ლიტერატურაში სშირად გამოიყენება, მაგრამ უმეტეს შემთხვევაში არ მოიცემა მისი ცხადი განმარტება. სშირად იხმარება «ციფრული სისტემის» სინონიმები: «კომპიუტერული სისტემა», «ციფრული ელექტრონიკა» და სხვა.“³

„ციფრული სისტემის სტრუქტურა არის მისი ელემენტების და მათ შორის კავშირების სივრცეში და დროში მყარი მოწესრიგებულობა. ციფრული სისტემებისათვის დამახასიათებელია სხვადასხვა ელემენტების და მათ შორის კავშირების არსებობა, რაც განაპირობებს ციფრული სისტემების სხვადასხვა სტრუქტურებს. ამრიგად, ელემენტების ქვესისტემებში შესვლის წესი, ხოლო შემდგომ ქვესისტემების თანმიმდევრობითი გაერთიანება ერთიან სისტემაში წარმოქმნის სისტემის დანაწევრების სტრუქტურას. აქედან გამომდინარე ასეთი სტრუქტურა მუდამ იერარქიულია და გააჩნია არანაკლები ორი დონისა: მაღალი დონე – სისტემა და დაბალი დონე – ელემენტი“.⁴

„ციფრული სისტემების ანალიზის შედეგად შეიძლება გამოვყოთ მათი აგების იერარქიის შემდეგი დონეები:

- სისტემა;
- ფუნქციონალური ქვესისტემა;
- ბლოკი (პროცესორი, მეხსიერების ბლოკი და ა.შ.);
- კვანძი (ციფრული კვანძები, აგებული ლოგიკურ ელემენტებზე);
- ელემენტი (ტრივიალური ლოგიკური ელემენტები).“⁵

მაგალითისა და თვალსაჩინოებისათვის განვმარტოთ;

- ტექსტური ინფორმაცია;
- გრაფიკული ინფორმაცია;
- ბგერითი ინფორმაცია;

„ტექსტური ინფორმაცია; წარმოადგენს ანბანური სიმბოლოების ერთობლიობას. თუ თითოეულ ანბანურ სიმბოლოს რიცხვით კოდს შეესაბამებთ, მაშინ მივიღებთ ტექსტის რიცხვების საშუალებით გამოსახვის შესაძლებლობას, მაგალითად“:⁶

ა	ბ	გ	დ	ე	ვ	ზ	თ	ი	კ	ლ	მ	ნ	ო	პ	ჟ	რ
0224	0225	0226	0227	0228	0229	0136	0230	0231	0232	0233	0234	0235	0236	0237	0238	0239
ს	ტ	უ	ფ	ქ	ღ	ყ	შ	ჩ	ც	ძ	წ	ჭ	ხ	ჯ	პ	
0240	0241	0242	0243	0244	0245	0246	0247	0248	0249	0250	0251	0252	0253	0254	0255	

² ლევან იმნაიშვილი, ციფრული სისტემების სინთეზის პრინციპების დამუშავება მრავალფუნქციურობის ბაზაზე. დისერტაცია, სამეცნიერო კონსულტანტი ბ-ნი არჩილ ფრანგიშვილი. 2006 წელი. გვ.17.

³ იქვე. გვ.3-4

⁴ ლევან იმნაიშვილი, ციფრული სისტემების სინთეზის პრინციპების დამუშავება მრავალფუნქციურობის ბაზაზე. დისერტაცია, სამეცნიერო კონსულტანტი ბ-ნი არჩილ ფრანგიშვილი. 2006 წელი. გვ.17.

⁵ იქვე. გვ.17.

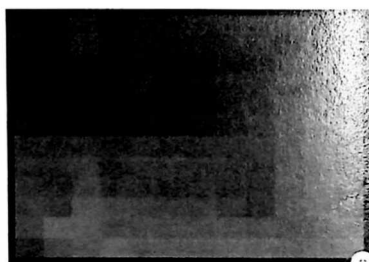
⁶ ვ.ჩხაიძე. ი.სალუქვაძე. ინფორმაციული ტექნოლოგიები ბგეოგრაფიაში. 2016 გვ..7

⁷ იქვე.

ი ნ ფ ო რ მ ა ც ი ა
0231-0235-0243-0236-0239-0234-0224-0249-0231-0224.

გრაფიკული ინფორმაციის წარმოდგენის შემთხვევაში გამოსახულება პირობითად “იშლება” წერტილოვან ელემენტებად. ბუნებრივია რომ რაც უფრო მეტია წერტილების რაოდენობა, ანუ მცირეა ელემენტარული წერტილის ზომა, მით უფრო ხარისხიანია ციფრული გამოსახულება. თითოეული წერტილი აღიწერება მისი ეკრანზე მდებარეობის კოორდინატთა წყვილით (რიცხვებით) და ფერის კოდით. ამ რიცხვების ერთობლიობა ქმნის ე.წ. რასტრს, რომელიც შეიძლება ასე გამოიყურებოდეს: ⁹

10



ბგერითი ინფორმაციის წარმოდგენისათვის ხმოვანი სიგნალი ანალოგიურად იშლება ერთეულოვან ელემენტებად (მაგ. ნოტებად ან სიხშირეებად) და თითოეულ გამოყოფილ ერთეულს მიენიჭება შესაბამისი რიცხვითი კოდი”. ¹¹

გრაფიკულ გამოსახულებათა ერთობლიობა შეიძლება წარმოდგენილ იქნას თანმიმდევრული რასტრების მეშვეობით და აღწერილ იქნას როგორც ე.წ. ნაკადი. გამოსახულებათა ნაკადური ცვლილება ქმნის მოძრაობის ეფექტს. ¹²

გრაფიკული და ბგერითი (ხმოვანი) ინფორმაციის გაერთიანებას ნაკადში კიდევ მულტი-მედირსაც უწოდებენ. მონაცემთა თითოეულ სტრუქტურულ ჯგუფს გააჩნია კლასიფიკირების მახასიათებლები (კრიტერიუმები)”. ¹³

ციფრული დანაშაულის საგანი არ შეიძლება იყოს არაციფრული ინფორმაციის მატარებელი ნივთი. მაგალითად: დავეშვათ დანაშაულის ჩამდენმა პირმა დააზიანა კომპიუტერული მოწყობილობის ეკრანი. იმ მიზნით, რომ კომპიუტერში ინახება მისთვის არასასურველი ინფორმაცია — ზიანი

⁹ ვ. ჩხაიძე, ი.სალუქვაძე. ინფორმაციული ტექნოლოგიები ბგეოგრაფიაში. 2016 გვ.გვ.7

⁹ ვ. ჩხაიძე, ი.სალუქვაძე. ინფორმაციული ტექნოლოგიები ბგეოგრაფიაში. 2016 გვ.გვ.7

¹⁰ იქვე.

¹¹ იქვე.

¹² იქვე.

¹³ ვ. ჩხაიძე, ი.სალუქვაძე. ინფორმაციული ტექნოლოგიები ბგეოგრაფიაში. 2016 გვ.გვ.7

განისაზღვრა 200 ლარით, ასეთ შემთხვევაში, მიუხედავად იმისა, რომ დანაშაულის საგანი - სახე-ზეა კომპიუტერული მოწყობილობის ეკრანი, ბუნებრივია სახეზე ვერ იქნება ციფრული დანაშაული, რადგან დანაშაულის საგანს არ წარმოადგენს ციფრული ინფორმაცია, მაგრამ იმ შემთხვევაში თუ დამნაშავემ გამოიყენა სხვა პირის პლასტიკური ბარათი და ე.წ. ბანკომატიდან განახორციელა აღნიშნული ბარათის გამოყენებით ფულადი ტრანზაქცია - სახეზე გვექნება ციფრული დანაშაული ვინაიდან, კი მართალია გამოყენებული საგანი ერთი შეხედვით არის მატერიალური ნივთი - პლასტიკური ბარათი, მაგრამ დანაშაულის ჩასადენად გამოყენებულ იქნა არა თავად ბარათი, არამედ მასზე არსებული ციფრული ინფორმაცია შესაბამისი პიროვნების საბანკო რეკვიზიტების და პარამეტრების შესახებ.

გეოაღნიშნულიდან გამომდინარე, ნივთი - როგორც ციფრული დანაშაულის ჩადენის საგანი, შესაძლოა მოვიზიაროთ მხოლოდ იმ შემთხვევაში, თუ აღნიშნულ ნივთში დაცულია ციფრული ინფორმაცია, რომელიც გამოყენებულ იქნა დანაშაულის ჩასადენად.

რაც შეეხება ციფრული დანაშაულის ობიექტურ მხარეს, პირველ რიგში ხასიათდება მართლ-საწინააღმდეგო მოქმედებით. მაგალითად: მოქმედებით ჩადენილ ციფრულ დანაშაულად შესაძლოა მოვიზიაროთ, შესაბამისი მართლსაწინააღმდეგო მოტივით, მიზნით და განზრახვით, ციფრული საგნის გამოყენებით ჩადენილი:

- კიბერტერორიზმი;
- ჰაკერობა;
- კიბერ ქურდობა;
- იდენტიფიკაციის ქურდობა;
- ვირუსული პროგრამები;
- კიბერ გადაკიდება;
- ბავშვთა დაყოლიება;
- პირადი ცხოვრების ამსახველი ინფორმაციის ან პერსონალური მონაცემების ხელყოფა;
- პირადი ცხოვრების საიდუმლოს ხელყოფა;
- კერძო კომუნიკაციის საიდუმლოების დარღვევა;
- პირადი მიმოწერის, ტელეფონით საუბრის ან სხვაგვარი ხერხით შეტყობინების საიდუმლოების დარღვევა;
- და სხვა.

როგორც უკვე აღინიშნა, თითოეულ დანაშაულს შესაძლოა ჰქონდეს ინდივიდუალური შემადგენლობის ნიშნები, მაგრამ როდესაც ვსაუბრობთ ციფრულ დანაშაულზე აუცილებელია განისაზღვროს, რომ ყველა აღნიშნული დანაშაულის ჩადენის ხერხი/საშუალება არის - კომპიუტერული სისტემა, ხოლო დანაშაულის საგანი - კომპიუტერული სისტემის გამოყენებით შექმნილი ციფრული ინფორმაცია - ტექსტური ინფორმაცია (მაგ. დოკუმენტი), გრაფიკული ინფორმაცია (მაგ. ფოტო, ვიდეო), ბგერითი ინფორმაცია (მაგ. აუდიოჩანაწერი, მუსიკა), ტექსტურ - გრაფიკული ინფორმაცია (მაგ. ელექტრონული ფული), გრაფიკულ-ბგერითი ინფორმაცია და ასე შემდეგ. ასევე კომპიუტერულ მოწყობილობაში ან მის გარეთ - შესაბამის ელექტრონულ მეხსიერების მოწყობილობაში დაცული ციფრული მასალა - მაგ (ID ბარათზე, პლასტიკურ ბარათზე, სიმ ბარათზე) და ა.შ.

განვიხილოთ ციფრული დანაშაულის ჩადენის ხერხი/საშუალება, რომელიც რა თქმაუნდა არის კომპიუტერული სისტემა, იმიტომ, რომ ციფრული მასალის შექმნა ხდება კომპიუტერული სისტემის საშუალებით, კერძოდ:

„კლასიკური სტრუქტურის მიხედვით აგებული მანქანა მუშაობს შემდეგნაირად. მანქანის ავტომატური მუშაობის დაწყებამდე მართვის პულტიდან გაიცემა ბრძანებები, რომელთა მიხედვითაც გარე მოწყობილობებიდან ხდება მანქანის მახსოვრობაში კონკრეტული ამოცანის შესრულებისათვის საჭირო მონაცემების და შესასრულებელი პროგრამის ჩატვირთვა. შემდეგ მართვის პულტიდან ოპერატორი ჩაწერს მართვის მოწყობილობის ბრძანების მისამართის რეგისტრში იმ უკრედის მისამართს, რომელშიც ინახება პროგრამის პირველი ბრძანება. ამის შემდეგ ხდება მართვის მოწყობილობის ჩართვა. მართვის მოწყობილობიდან მახსოვრობის მოწყობილობაში იგზავნება მმართველი სიგნალი, რომლის საშუალებითაც ხდება მახსოვრობის მოწყობილობაში მითითებული უკრედის წაკითხვა და მისი შგთავსი გადაიწერება მართვის მოწყობილობის რეგისტრში. ეს ინფორმაცია წარმოადგენს ბრძანებას – ინსტრუქციას. ხდება ინსტრუქციის გაშფვრა და შესაბამისი მმართველი სიგნალების გამოშვება მახსოვრობის მოწყობილობისათვის, რის საფუძველზეც ხდება ოპერანდების წაკითხვა და არითმეტიკულ მოწყობილობაში გადაწერა. მმართველი სიგნალები გაიცემა აგრეთვე არითმეტიკული მოწყობილობისთვისაც, რათა მან შეასრულოს ინსტრუქციით (ბრძანებით) მოთხოვნილი ოპერაცია. ამის შენდეგ მმართველი სიგნალების მიხედვით უნდა მოხდეს შედეგის არითმეტიკული მოწყობილობიდან მითითებული მისამართით მახსოვრობის მოწყობილობაში გადაწერა. ამასთანავე, მმართველ მოწყობილობაში ბრძანების მისამართის რეგისტრში უნდა მოხდეს ახალი ბრძანების მისამართის ფორმირება. ეს შეიძლება მოხდეს რეგისტრის შიგთავსისათვის ერთის დამატებით.“¹⁴

„პირველი ბრძანების შესრულების შემდეგ მართვის მოწყობილობა გასცემს ახალ სიგნალს შემდეგი ბრძანების წასაკითხად და ანალოგიურად იწყებს ახალი ბრძანების შესრულებას. ზოგიერთი ბრძანების კოდი, რომელიც მითითებულია ინსტრუქციაში, შეიძლება აღნიშნავდეს არა არითმეტიკულ ოპერაციას, არამედ ოპერაციას თვით მართვის მოწყობილობისათვის.“¹⁵

–კიდევ ერთხელ გავუსვათ ხაზი კომპიუტერის აგების კლასიკურ სტრუქტურაში ჩადებულ ორ ფუნდამენტურ იდეას, რომლებმაც დიდად შეუწყო ხელი გამოთვლითი ტექნიკის განვითარებას [...].“¹⁶

„პირველი, კომპიუტერში პროგრამები და საწყისი მონაცემები შეიტანება ერთი და იგივე გარე მოწყობილობებიდან და ინახება ერთი და იგივე დამხსოვებელ მოწყობილობაში. ეს უზრუნველყოფს კომპიუტერის ოპერატიულ გადასვლას ერთი ამოცანიდან მეორეზე და აქცევს მას უნივერსალურ გამოთვლელ მოწყობილობად.“¹⁷

„მეორე, ინსტრუქციები, რომლებიც ქმნის პროგრამებს, კოდირებულია რიცხვების მსგავსად. ეს საშუალებას იძლევა პროგრამების შესრულების დროს ინსტრუქციებიც გადაგზავნილ იქნას არითმეტიკულ მოწყობილობაში მათზე გარკვეული მოქმედებების ჩასატარებლად და შემდეგ დაბრუნებული იქნას დამხსოვებელ მოწყობილობაში. ამრიგად, პროგრამის შესრულებასთან ერთად შეიძლება მისი გარდაქმნაც ან ახალი პროგრამის შექმნაც.“¹⁸

რაც შეეხება ციფრული ტექნოლოგიებით რაიმე სახის დანაშაულის ჩადენას უპირველეს ყოვლისა უნდა დავადგინოთ და გამოვიძიოთ ვინ შეიძლება შექმნას, დაამზადოს და შემდგომ გამოიყენოს ციფრული ტექნოლოგიები დანაშაულის ჩასადენად.

¹⁴ თეიმურაზ კვილაძე, ინფორმატიკის ისტორია, 2018, გვ. 24.

¹⁵ იქვე.

¹⁶ იქვე.

¹⁷ იქვე.

¹⁸ იქვე.

ქმედების სუბიექტი შესაძლოა იყოს; ნებისმიერ ფიზიკური პირი, იურიდიული პირი და სახელმწიფო.

„კომპიუტერული დანაშაულის შესახებ“ კონვენციის თანახმად (ბუდაპეშტი 23.11.2001) მომსახურების მიწოდებელი არის; „ნებისმიერი საჯარო ან კერძო პირი, რომელიც მისი სერვისის მომხმარებლებს უზრუნველყოფს კომპიუტერული სისტემის საშუალებით ურთიერთობის შესაძლებლობით, და ნებისმიერი სხვა პირი, რომელიც გადაამუშავებს ან ინახავს კომპიუტერულ მონაცემებს ამგვარი საკომუნიკაციო მომსახურების ან ამგვარი მომსახურების მომხმარებელთა სახელით.“

სუბიექტზე მსჯელობისას გამოვყოთ რამდენიმე სპეციალური სუბიექტი და ასევე სუბიექტები, რომლებსაც გააჩნიათ სპეციიური მახასიათებლები;

სპეციალური სუბიექტად შესაძლოა შეგვხვდეს;

„სახელმწიფო - უცხოეთის ქვეყნების სადაზვერვო სამსახურები კომპიუტერულ ტექნოლოგიებს იყენებენ ინფორმაციის შეგროვებისა და ჯაშუშობისთვის. მსგავსი ქმედებები სადაზვერვო სამსახურების მხრიდან შეიძლება მიმართული იყოს როგორც მეგობარი, ისე მოწინააღმდეგე ქვეყნების მიმართ, ან არასახელმწიფო სუბიექტების წინააღმდეგ. სახელმწიფო თავისი სადაზვერვო სამსახურების გამოყენებით, ახორციელებს კიბერშეტევებს პოტენციური მოწინააღმდეგე სახელმწიფოების მიმართ დეზინფორმაციის, დესტაბილიზაციის, დაშინების ან ფართომასშტაბიანი კიბერბრძოლის წარმოების მიზნით. ასევე საყურადღებოა ის გარემოება, რომ ხშირად ხდება პიროვნების უსაფრთხოებისა და უფლებების დარღვევა. კერძოდ, სახელმწიფოს სპეციალურმა სამსახურებმა შეიძლება მიმართონ ისეთ ქმედებებს, რომელთა გამოყენებითაც ხდება მოქალაქეთა პერსონალური მონაცემების გადაჭრა, მოპარვა და გამოყენება. მსგავსი ქმედებები ხშირ შემთხვევაში ხდება სახამართლოს შესაბამისი ორგანოების სანქციისა და სწორი დემოკრატიული კონტროლის გარეშე.“¹⁹

„კორპორაციები, კომპანიები — დაკავებულნი არიან სამრეწველო/კორპორაციული ჯაშუშობითა და/ან დივერსიული საქმიანობით, რაშიც ისინი ხშირად იყენებენ ჰაკერებსა და ორგანიზებულ დანაშაულთა ჯგუფებს. კომპანიების, კორპორაციებისა და კერძო სექტორის სხვა წარმომადგენლებს ასევე შეუძლიათ დაარღვიონ ადამიანის უფლებები პიროვნების პერსონალური მონაცემების შეგროვებისა და ანალიზის გზით, ან ზოგ შემთხვევაში მოცემული მონაცემების სახელმწიფო ორგანოებთან ან სხვა დაინტერესებულ პირებთან გაცვლით.“²⁰

„კიბერ დივერსანტები - ქსელის უკმაყოფილო მომხმარებელთა რიცხვიდან - ზოგადად, უკმაყოფილო მომხმარებლები წარმოადგენენ სერიოზულ საფრთხეს, ვინაიდან ისინი კარგად იცნობენ სისტემის მუშაობის პრინციპებს და შეუძლიათ თავიანთი ეს ცოდნა გამოიყენონ დესტრუქციული მიზნებისთვის. მაგალითად, სისტემის დასაზიანებლად ან კონფიდენციალური ინფორმაციის მოსაპარად. შეერთებული შტატების ფედერალური საგამოძიებო ბიუროს (FBI) მონაცემებით, სისტემის მომხმარებლებისა და გარე წყაროების მხრიდან კიბერშეტევის ორგანიზების შესაძლებლობის ერთმანეთთან შეფარდება შეადგენს 2:1.“²¹

¹⁹ ვლადიმერ სვანაძე, ნაშრომი „კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები“. 2015 წ. გვ. 71/131-75/131 ელ. გვერდი;  ნანახია 06.06.2019.

²⁰ იქვე.

²¹ ვლადიმერ სვანაძე, ნაშრომი „კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები“. 2015 წ. გვ. 71/131-75/131 ელ. გვერდი;  ნანახია 06.06.2019.

კიბერ ტერორისტები - ცდილობენ ინფრასტრუქტურის მნიშვნელოვანი ობიექტები გამოიყვანონ მწყობრიდან, საერთოდ გაანადგურონ ან გამოიყენონ თავიანთი მიზნებისთვის. მათი ქმედება სერიოზული საფრთხის ქვეშ აყენებს ქვეყნების ეროვნულ უსაფრთხოებას, იწვევს ადამიანთა მასიურ მსხვერპლს, ასუსტებს ეკონომიკას, ასევე ზიანს აყენებს საზოგადოების მორალურ მდგომარეობასა და ამცირებს მათ სანდოობას ხელისუფლების მიმართ. ყველა ტერორისტული ორგანიზაცია და დაჯგუფება არ ფლობს საკმარის ცოდნასა და ტექნიკურ საშუალებებს ეფექტური კიბერშეტევის განხორციელებისთვის, თუმცა არსებობს თეორიული დაშვება, რომ მათ მიიღონ მსგავსი ცოდნა და შესაძლებლობა, ან დახმარებისთვის მიმართონ ორგანიზებული დანაშაულის წარმომადგენლების მომსახურებას.²²

სუბიექტებად, რომლებსაც გააჩნიათ სპეციალური მახასიათებლები შესაძლოა განვიხილოთ;

„ჰაკერები - იყო დრო როცა ჰაკერების მხრიდან ქსელებში არასანქცირებული შეღწევა ან პროგრამების გატეხვა დაკავშირებული იყო ჰაკერთა საზოგადოებაში ავტორიტეტის მოპოვებასთან ან წვრილმან პულიგნობასთან. დღესდღეისობით სურათი კარდინალურად არის შეცვლილი, კერძოდ ჰაკერთა უმრავლესობის ქმედება ატარებს კრიმინალურ ხასიათს. ადრე თუ ჰაკერებისთვის ქსელის გატეხვისათვის საჭირო იყო კომპიუტერული ტექნოლოგიების სფეროში სპეციალური უნარჩვევების ცოდნა, როცა ამჟამად საკმარისია ინტერნეტიდან შესაბამისი ინსტრუქციებისა და პროტოკოლების გადმოქაჩვა და მათი გამოყენება შერჩეულ საიტზე კიბერშეტევის ორგანიზებისთვის. ამის გამო, კიბერშეტევის განხორციელება მომხმარებლისთვის გახდა უფრო ადვილად ხელმისაწვდომი. ჰაკერთა მომსახურებით სარგებლობენ არამარტო კორპორაციები და კომპანიები, არამედ საღაზერო ან სხვა სახის სპეციალური სამსახურებიც.²³

„ჰაკტივისტები - ტერმინი „ჰაკტივიზმი“ (hacktivism) წარმოიშვა ორი სიტყვის „Hack“ და „Activism“ შეერთებით და ის აღნიშნავს სოციალური პროტესტის გამოხატვის ახალ მოვლენას, რომელიც წარმოადგენს თავისებურ სინთეზს რალაციის მიმართ გამოხატული პროტესტის სოციალური აქტიურობისა და ჰაკერობის, რომელიც მიმართულია გარკვეული ვებ-გვერდების ან საფოსტო სერვისების წინააღმდეგ. თავიანთი პოლიტიკური მიზნების მისაღწევად, ჰაკტივისტები მისიწ-რაფივან დააზიანონ ან საერთოდ მწყობრიდან გამოიყვანონ ზოგიერთი ვებ - გვერდი.“²⁴

„ბოტნეტი — ინტერნეტ - ბოტის შემქნელი ფიზიკური ან/და იურიდიული პირი, „ბოტნეტი წარმოადგენს პროგრამას, რომელიც ფარულად არის დაყენებული მსხვერპლის/ობიექტის კომპიუტერულ მოწყობილობაში, რაც დამნაშავეს/ბოროტმოქმედს საშუალებას აძლევს „დავირუსებული“ კომპიუტერის რესურსების გამოყენებით, შეასრულოს გარკვეული ქმედებები. ჰაკერების ეს სახეობა თავისი პროგრამებით „ავირუსებენ“ კომპიუტერების დიდ რაოდენობას, რომელთა რესურსებსაც შემდეგ იყენებენ კიბერშეტევის კოორდინირებისთვის, ასევე „სპამის“

²² ვლადიმერ სვანაძე, ნაშრომი „კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები“. 2015 წ. გვ. 71/131-75/131 ელ. გვერდი:  ნანახია 06.06.2019.

²³ ვლადიმერ სვანაძე, ნაშრომი „კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები“. 2015 წ. გვ. 71/131-75/131 ელ. გვერდი  ნანახია 06.06.2019.

²⁴ ვლადიმერ სვანაძე, ნაშრომი „კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები“. 2015 წ. გვ. 71/131-75/131 ელ. გვერდი  ნანახია 06.06.2019

გასაგზავნად, "ფიშინგისთვის" და სხვა მავნე ქმედებისთვის. მსგავსი სახის ქსელები წარმოადგენენ არალეგალური ვაჭრობის ობიექტს." ²⁵

„ფიშერები“ - ეს არის ფიზიკური პირები ან პატარა დაჯგუფებები, რომლებიც იყენებენ "ფიშინგის" ტექნოლოგიებს პერსონალური რეკვიზიტების მოპარვისა და ფასიანი ინფორმაციების გადაყიდვის მიზნით. თავიანთი მიზნების მისაღწევად ფიშერები ხშირად იყენებენ „სპამებს" და ჯაშუშურ პროგრამებს." ²⁶

„სპამერები“ - ფიზიკური ან იურიდიული პირები, რომლებიც მასიურად აგზავნიან არამოთხოვნილ ელექტრონულ ფოსტას დაფარული ან მცდარი ინფორმაციით, რომლის მიზანია ფიშინგითა და ჯაშუშური პროგრამების გამოყენებით კონკრეტულ ორგანიზაციებზე კიბერშეტევის განხორციელება; ჯაშუშური და მავნე პროგრამების შემქმნელები — ფიზიკური ან იურიდიული პირები, რომლებსაც გააჩნიათ დანაშაულებრივი ზრახვები კომპიუტერების მომხმარებლებზე კიბერშეტევის განახორციელებლად." ²⁷

„მედოფილები“ - ეს კატეგორია სულ უფრო აქტიურად იყენებს ინტერნეტს საბავშვო პრონოგრადიის გასაყვრელად, ასევე სოციალური ქსელებისა და ინტერნეტ ჩათების გამოყენებით, პოტენციური მსხვერპლების გასაცნობად." ²⁸

ასევე აღსანიშნავია, რომ დროთა განმავლობაში, დამნაშავეებმა, რომლებიც იყენებენ მალაქ ტექნოლოგიებს, ე.წ. ჰაკერებმა²⁹, „დანაშაულის ახალი ფორმები და მიმართულებები შექმნეს. მათ უკვე არ იზიდავთ დანაშაულის ჩადენის ძველი მეთოდები. კომპიუტერული საშუალებები ჰაკერებს შესაძლებლობას აძლევს, მიზნის მიღწევისთვის სრულიად ახალი სქემები გამოიყენონ. თავიანთ ანგარიშით მიზნებს ისინი კომპიუტერის მეშვეობით ახორციელებენ, კერძოდ, ქმნიან და გამოიყენებენ ე.წ. ვირუსებს ან ჩაღიან სხვა სახის კიბერდანაშაულს. არსებობს კომპიუტერული დანაშაულის სამი კატეგორია;" ³⁰

ზემოაღნიშნული სუბიექტების მიერ;

„1. კომპიუტერი გამოიყენება, როგორც ელექტრონული ინფორმაციის შექმნის, შენახვის, მისით მანიპულაციის და ელექტრონული კომუნიკაციის საშუალება. ამ შემთხვევაში

²⁵ ვლადიმერ სვანაძე, ნაშრომი „კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები“. 2015 წ. გვ. 71/131-75/131 ელ. გვერდი  ნანახია 06.06.2019.

²⁶ იქვე.

²⁷ იქვე.

²⁸ იქვე.

²⁹ ჰაკერები (ინგლ. hacker, ტერმინის ფუძეა to hack — ჭრილობა, ჭრილი, კვეთილი; გაპობა, გაჭრა, გაყევა, კიწვა. ნაკუწ-ნაკუწად ქცევა, დაკბილვა. გათლა (ქვისა)) ეწოდება კომპიუტერული პროგრამების განსაკუთრებულ ჯგუფს. პირველად ეს ტერმინი 1960-იან წლებში გაჩნდა და ამის შემდეგ მას მრავალი მნიშვნელობა გაუჩნდა. ჰაკერი აუცილებლად, სულ ცოტა, 2 პროგრამირების ენას უნდა ფლობდეს. ერკვეოდეს ქსელში და იყენებდეს ძლიერ ოპერაციულ სისტემებს ("nix — UNIX, BSD, Linux და ა.შ.)  ელ. გვერდი; ნანახია 03.05.2019

³⁰ ვლადიმერ სვანაძე, ნაშრომი „კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები“. 2015 წ. გვ. 71/131-75/131 ელ. გვერდი;  ნანახია 06.06.2019.

კომპიუტერი არ არის დანაშაულის იარაღი, თუმცა, მისი მეშვეობით შესაძლებელია განხორციელდეს კრიმინალურ აქტივობასთან დაკავშირებული ქმედებები, მაგალითად, ამოღებულ იქნას (გადმოიქაჩოს) ნარკოდოზის შავი ბუღალტერია;

2. კომპიუტერი შეიძლება გამოყენებულ იქნას, როგორც დანაშაულის ინსტრუმენტი. ასე მაგალითად, მისი მეშვეობით შესაძლებელია დაიბეჭდოს ყაღბი ფული, გაყალბდეს საბუთები, ინტერნეტში გავრცელდეს არასრულწლოვანთა პორნოგრაფია, ჩაიტვირთოს თაღლითური ვებ-გვერდები და ა.შ;
3. „კომპიუტერი ასევე შეიძლება იქცეს დანაშაულის იარაღად. ამ შემთხვევაში თავდასხმა ხორციელდება ინფორმაციის მოპოვების შესაძლებლობაზე, მის მთლიანობაზე და დაცულობაზე (ასეთია, მაგალითად, ინფორმაციისა და სერვისების მითვისება, კომპიუტერული ექსპედიციის დაზიანება). ამ სახეობის დანაშაული უკავშირდება ვირუსების უკანონო გავრცელებას, სერვისებისა და ქსელების არა ავტორიზებულ დაბლოკვას. ასეთ დანაშაულს ხშირად ჩადიან ე.წ. „კიბერ-ვანდალები“. ბოლო წლებში მთელ მსოფლიოში საგრძნობლად გაიზარდა სხვადასხვა ორგანიზაციების წინააღმდეგ მიმართული კიბერთავდასხმების რაოდენობა.“³¹

1.2 ციფრულ დანაშაულის კლასიფიკაცია ქართულ სისხლის სამართალში

საქართველოს სისხლის სამართლის კოდექსი ახდენს მასში მოთავსებული 415 მუხლის კლასიფიცირებას სხვადასხვა კარების და თავების მიხედვით, მაგრამ არცერთ მუხლში არ გვაქვს მოცემული სიფრთხილი დანაშაული, ან დანაშაული ჩადენილი ციფრული საგნის გამოყენებით, შესაბამისად როდესაც ციფრული დანაშაული მოხდება, მისი დაკვალიფიცირება ხდება სხვადასხვა მუხლებით, ამასთან საქართველოს სისხლის სამართლის კოდექსი ფეხს ვერ უბამს საერთაშორისო კლასიფიკაციით გათვალისწინებული თუნდაც კიბერდანაშაულის ტიპებს, აღნიშნულიდან გამომდინარე, მიზანშეწონილად ვთვლით წარმოგიდგინოთ დანაშაულთა ციფრული დანაშაულის ტიპები, რომელთა კვალიფიკაციისათვის უნდა მოქმედნოთ საქართველოს სისხლის სამართლის კოდექსში არსებული შესაბამისი მუხლები და შევესაბამოთ ქმედების სამართლებრივ ბუნებას და შემადგენლობას.

ბაკერობა: ნიშნავს სხვისი კომპიუტერული უსაფრთხოების შექცევის დარღვევას, სხვის კომპიუტერში არსებული პირადი ინფორმაციის ხელმისაწვდომობას. არსებობს როგორც დანაშაულებრივი, ასევე ე.წ. „ეთიკური ბაკერობა“ რომელსაც ორგანიზაციები იყენებენ მათი ინტერნეტ უსაფრთხოებისათვის, შესაბამისად ბუნებრივია „ეთიკურ ბაკერობას“ როგორც დანაშაულს ვერ მოვიზარებთ თუ მისი გამოყენების მიზანია სისტემის დაცვა, ხოლო რაც შეეხება სხვა სახის ბაკერობას - აღნიშნული არის დანაშაული, ბაკერობა დანაშაულად გვევლინება ამერიკის შეერთებულ შტატებში. რაც შეეხება საქართველოს, სისხლის სამართლის კოდექსში ასეთი დანაშაული არ გვაქვს, მაგრამ ქმედების ობიექტური შემადგენლობის ნიშნებიდან გამომდინარე შესაძლოა ვიმსჯელოთ, რომ აღნიშნული დანაშაული საქართველოს სისხლის სამართლის

³¹ იხ. ალექსანდრე ლლონტი, კიბერდანაშაულის პრობლემა საქართველოსა და უცხოეთის ქვეყნებში. ელ.გვერდი  ნანახია 03.05.2019

კანონმდებლობის მიხედვით შესაძლოა დავაკვალიფიციროთ საქართველოს სისხლის სამართლის კოდექსის 284-ე მუხლით, რომლის თანახმად დანაშაულია;

„1. კომპიუტერულ სისტემაში უნებართვო შეღწევა;

ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით იმავე ვადით.

2. იგივე ქმედება:

- ა) წინასწარი შეთანხმებით ჯგუფის მიერ;
- ბ) სამსახურებრივი მდგომარეობის გამოყენებით;
- გ) არაერთგზის;
- დ) რამაც მნიშვნელოვანი ზიანი გამოიწვია, — ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით ვადით ორიდან ხუთ წლამდე.“³²

კიბერტერორიზმი: მიუხედავად იმისა, რომ საქართველოს სისხლის სამართლის კოდექსის 323-ე მუხლი ითვალისწინებს პასუხისმგებლობას ტერორისტული აქტისთვის, საქართველოს კანონმდებელმა ამ კუთხით ფეხი აუბა საერთაშორისო სტანდარტებს და სისხლის სამართლის კოდექსში გვხვდება 324-ე მუხლი - კიბერტერორიზმი, „ესე იგი კანონით დაცული კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლება, მისი გამოყენება ან გამოყენების მუქარა, რაც ქმნის მძიმე შედეგის საშიშროებას, ჩადენილი მოსახლეობის დაშინების ან/და ხელისუფლების ორგანოზე ზემოქმედების მიზნით“. აღნიშნული განმარტება სისხლის სამართლის კოდექსში გვხვდება 2012 წლის 2 მარტის ცვლილების შემდეგ.

„კიბერ ქურდობა: აღნიშნული სახეზეა, როდესაც საავტორო უფლების დარღვევით ხდება ინტერნეტიდან სხვადასხვა ინფორმაციის გადმოწერა. უმეტეს შემთხვევაში ვებ-გვერდები თავად სთავაზობენ მომხმარებელს პირატულ მასალას. საქართველოს სისხლის სამართლის კოდექსში კომპიუტერის საშუალებით საავტორო უფლების დარღვევის სპეციალური მუხლი არ არის გათვალისწინებული. ასეთი დანაშაულის ჩადენის შემთხვევაში პირის ქმედება კვალიფიცირდება ორი მუხლით: საქართველოს სისხლის სამართლის კოდექსის 284-ე (კომპიუტერულ სისტემაში უნებართვო შეღწევა) და 189-ე (საავტორო, მომიჯნავე უფლების მფლობელისა და მონაცემთა ბაზის დამამზადებლის უფლების ხელყოფა) მუხლებით. ეს უკანასკნელი (189-ე მუხლი), საავტორო, მომიჯნავე უფლების მფლობელის ან მონაცემთა ბაზის დამამზადებლის უფლების ხელყოფა, ისჯება ჯარიმით ან თავისუფლების შეზღუდვით ვადით ორ წლამდე. იგივე ქმედება ჩადენილი განსაკუთრებით დიდი ოდენობით შემოსავლის მიღების მიზნით ან წინასწარი შეთანხმებით ჯგუფის მიერ, ისჯება თავისუფლების შეზღუდვით ვადით სამ წლამდე ან თავისუფლების აღკვეთით იმავე ვადით.“³³

„ილენტიფიკაციის ქურდობა: ბოლო რამდენიმე წლის განმავლობაში სწორედ ასეთი ქმედება

³² საქართველოს სისხლის სამართლის კოდექსი, (22/07/1999 წლის) 29.05.2019 წლის მდგომარეობით. მუხლი 284.

³³ საქართველოს მთავარი პროკურატურის ანალიტიკური სამმართველო, ინფორმაცია კიბერდანაშაულის შესახებ. ელ.გვერდი;



წარმოადგენს კიბერდანაშაულებში მთავარ პრობლემას. დამნაშავე ნახულობს ბაზას პირის საბანკო ანგარიშის, საკრედიტო ინფორმაციის, დაზღვევის და სხვა მნიშვნელოვანი ინფორმაციის შესახებ, ხოლო შემდგომ იყენებს ამ ინფორმაციას მისი ნების გარეშე სხვადასხვა ფულადი ტრანზაქციებისა და საბანკო კრედიტებისათვის. აღნიშნულმა შესაძლოა გამოიწვიოს არა მხოლოდ მნიშვნელოვანი მატერიალური ზიანი, არამედ გააფუჭოს დაზარალებულის საბანკო ისტორიაც. საქართველოს სისხლის სამართლის კოდექსში იდენტიფიკაციის ქერდობის სპეციალური მუხლი არ არის გათვალისწინებული. ასეთი დანაშაულის ჩადენის შემთხვევაში პირის ქმედება კვალიფიცირდება ორი მუხლით: საქართველოს სისხლის სამართლის კოდექსის 284-ე (კომპიუტერულ სისტემაში უნებართვო შეღწევა) და 177-ე (ქერდობა) მუხლებით. თუ დაუფლებული ქონების ღირებულება/ფულადი თანხის ოდენობა არ აღემატება 150 ლარს ქერდობა ისჯება ჯარიმით ან თავისუფლების შეზღუდვით ვადით ერთიდან სამ წლამდე ანდა თავისუფლების აღკვეთით იმავე ვადით. თუ დაუფლებული ქონების ღირებულება/ფულადი თანხის ოდენობა აღემატება 150 ლარს, მაგრამ არ აღემატება 10 000 ლარს, იგი ისჯება თავისუფლების აღკვეთით ვადით სამიდან ხუთ წლამდე, ხოლო თუ დაუფლებული ქონების ღირებულება/ფულადი თანხის ოდენობა აღემატება 10 000 ლარს ქერდობა ისჯება თავისუფლების აღკვეთით ვადით ექვსიდან ათ წლამდე.”³⁴

„ვირუსული პროგრამები: ეს გულისხმობს სპეციალური პროგრამების შექმნას, რომლებიც მიზნად ისახავს ქსელიდან კომპიუტერის გამოთიშვას. ამგვარი პროგრამების საშუალებით დამნაშავეს ეძლევა საშუალება უპრობლემოდ ჰქონდეს წვდომა სხვა პირთა პირად ინფორმაციაზე. საქართველოს სისხლის სამართლის კოდექსის 286-ე მუხლის თანახმად, დანაშაულია კომპიუტერული მონაცემის უნებართვო დაზიანება, წაშლა, შეცვლა ან დაფარვა და ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ან/და თავისუფლების აღკვეთით იმავე ვადით. თუ ქმედებამ გამოიწვია მნიშვნელოვანი ზიანი ან თუ იგი ჩადენილია წინასწარი შეთანხმებით ჯგუფის მიერ, სამსახურებრივი მდგომარეობის გამოყენებით ან ამგვარი ქმედებისათვის ნასამართლევი პირის მიერ ისჯება ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით ვადით სამიდან ხუთ წლამდე.”³⁵

„კიბერ გადაკიდება: კიბერ გადაკიდების დროს დამნაშავეს მიზანია მსხვერპლის საჯარო ან პირადი შეურაცხყოფა, რაც დაზარალებულის პირად ცხოვრებაზე ახდენს ძლიერ ფსიქოლოგიურ გავლენას. აღნიშნული ქმედება მას შემდეგ მოექცა ყურადღების ქვეშ, რაც მკვეთრად გაიზარდა ინტერნეტ შეურაცხყოფისა და აბუჩად აგდების საფუძველზე თვითმკვლელობისა შემთხვევები. კიბერ-გადაკიდებას, როგორც დანაშაულის ცალკე სახეს, არ იცნობს საქართველოს კანონმდებლობა, თუმცა საქართველოს სისხლის სამართლის კოდექსი ითვალისწინებს სისხლისსამართლებრივ პასუხისმგებლობას თვითმკვლელობამდე მიყვანისათვის, რომელიც გამოიწვია მსხვერპლისადმი განხორციელებულმა მუქარამ, მისი პატივის ან ღირსების სისტემატურმა დამცირებამ.”³⁶

ბავშვთა დაცოლიება: ბავშვთა დაცოლიების დროს, სოციალური ქსელების და კომპიუტერული

³⁴ საქართველოს მთავარი პროკურატურის ანალიტიკური სამმართველო, ინფორმაცია კიბერ-დანაშაულის შესახებ. ელ.გვერდი:  ნანახია 03.05.2019

³⁵ საქართველოს მთავარი პროკურატურის ანალიტიკური სამმართველო, ინფორმაცია კიბერ-დანაშაულის შესახებ. ელ.გვერდი  : ნანახია 03.05.2019

³⁶ იქვე.

სისტემების გამოყენებით ცდილობენ არასრულწლოვნები დაითანხმონ საბავშვო პორნოგრაფიაზე ან სხვა დანაშაულებრივ ქმედებებზე. საქართველოს სისხლის სამართლის კოდექსი კომპიუტერული სისტემებისა და სოციალური ქსელის გამოყენებით არასრულწლოვნის პორნოგრაფიაზე დათანხმების სპეციალურ მუხლს არ ითვალისწინებს. ასეთი დანაშაულის ჩადენის შემთხვევაში შესაძლებელია ქმედებას მებრგოს საქართველოს სსკ-ის 255 პრიმა მუხლის შემადგენლობა, რომლის მიხედვითაც:

- „1. პორნოგრაფიული ნაწარმოების, ნაბეჭდი გამოცემის, გამოსახულების ან პორნოგრაფიული ხასიათის სხვა საგნის უკანონოდ დამზადება, გავრცელება ან რეკლამირება, აგრეთვე ასეთი საგნით ვაჭრობა ანდა მისი შენახვა გაციდვის ან გავრცელების მიზნით, — ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით იმავე ვადით.
2. წინასწარი შეცნობით არასრულწლოვნის გამოსახულების შემცველი პორნოგრაფიული ნაწარმოების შექმნა, შენახვა, ჩვენებაზე დასწრება, შეთავაზება, გავრცელება, გადაცემა, რეკლამირება, ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა ან ასეთი ნაწარმოებით სარგებლობა, — ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ან/და თავისუფლების აღკვეთით ვადით სამ წლამდე.
3. წინასწარი შეცნობით არასრულწლოვნის გამოსახულების შემცველი პორნოგრაფიული ნაწარმოების დამზადება ან გასაღება, — ისჯება ჯარიმით ან თავისუფლების აღკვეთით ვადით სამიდან ხუთ წლამდე.
4. ამ მუხლის პირველი, მე-2 ან მე-3 ნაწილით გათვალისწინებული ქმედება, ჩადენილი არაერთგზის, — ისჯება თავისუფლების აღკვეთით ვადით ოთხიდან ექვს წლამდე.“³⁷

აღნიშნული მუხლის ციფრულ დანაშაულად მიჩნევისათვის მნიშვნელოვანია ყურადღება გავამახვილოდ მუხლის შენიშვნაზე, რომლის მიხედვითაც „არასრულწლოვნის გამოსახულების შემცველი პორნოგრაფიული ნაწარმოები არის ნებისმიერი მეთოდით შექმნილი ვიზუალური ან აუდიოვიზუალური მასალა, აგრეთვე დადგმული წარმოდგენა, რომელშიც სხვადასხვა საშუალებით წარმოდგენილია არასრულწლოვნის ან არასრულწლოვნის გამოსახულების მქონე პირის მონაწილეობა ნამდვილ, სიმულირებულ ან კომპიუტერული ტექნოლოგიის მეშვეობით გენერირებულ სექსუალურ სცენებში ან ნაჩვენებია არასრულწლოვნის გენიტალური ორგანოები მომხმარებლის სექსუალური მოთხოვნილების დაკმაყოფილების მიზნით. პორნოგრაფიულად არ ჩაითვლება ნაწარმოები, რომელსაც აქვს სამედიცინო, სამეცნიერო, საგანმანათლებლო ან სახელოვნებო ღირებულება“, თუ ასეთი მასალა მოპოვებულია ან/და გავრცელებულია ციფრული ინფორმაციის სახით, ასეთ შემთხვევაში სახეზე გვექნება ბავშვთა დაყოფიება, როგორც ციფრული დანაშაულის განმტოება, ხოლო იმ შემთხვევაში თუ არასრულწლოვნის გადაბირება მიზნად ისახავს არასრულწლოვნის ექსპლუატაციას, სახეზე გვაქვს საქართველოს სსკ-ის 143 სექსუალური მუხლით გათვალისწინებული დანაშაული - არასრულწლოვანი ვაჭრობა (ტრეფიკინგი), ანუ „არასრულწლოვნის ყიდვა ან გაყიდვა, ან მის მიმართ სხვა უკანონო გარიგების განხორციელება, აგრეთვე მისი გადაბირება, გადაყვანა, გადამალვა, დაქირავება, ტრანსპორტირება, გადაცემა, შეფარება ანდა მიღება ექსპლუატაციის მიზნით“.

³⁷ საქართველოს სისხლის სამართლის კოდექსი, (22/07/1999 წლის) 29.05.2019 წლის მგდომარეობით. მუხლი 255.

პირადი ცხოვრების ამსახველი ინფორმაციის ან პერსონალური მონაცემების ხელყოფა;

საქართველოს სისხლის სამართლის კოდექსის 157-ე მუხლის თანახმად, დასჯად ქმედებას წარმოადგენს „პირადი ცხოვრების ამსახველი ინფორმაციის ან პერსონალური მონაცემების უკანონოდ მოპოვება, შენახვა, გამოყენება, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა [...]“³⁸ და „პირადი ცხოვრების ამსახველი ინფორმაციის ან პერსონალური მონაცემების უკანონოდ გამოყენება ან/და გავრცელება ამა თუ იმ ხერხით გავრცელებული ნაწარმოების, ინტერნეტის, მათ შორის, სოციალური ქსელის, მასობრივი მაუწყებლობის ან სხვა საჯარო გამოსვლის მეშვეობით, რამაც მნიშვნელოვანი ზიანი გამოიწვია“³⁹ იმ შემთხვევაში თუ ასეთი ქმედება ჩადენილია ციფრული ტექნიკის გამოყენებით - მაგალითად ნაწარმოებია ფოტო - ვიდეოგადაღება ან აუდიოჩაწერა, ან სხვადასხვა სახით ელექტრონული ინფორმაციის მოპოვება პირადი ცხოვრების შესახებ - სახეზე გვაქვს ციფრული დანაშაული, ხოლო რაც შეეხება არნიშნული მუხლის მე-2 ნაწილს - თავად მუხლის შინაარსი გვაძლევს მოცემულობას რომ ეს დაკავშირებულია ციფრულ დანაშაულთან, როდესაც ინფორმაციის „გავრცელება ამა თუ იმ ხერხით გავრცელებული ნაწარმოების, ინტერნეტის, მათ შორის, სოციალური ქსელის, მასობრივი მაუწყებლობის ან სხვა საჯარო გამოსვლის მეშვეობით“⁴⁰.

პირადი ცხოვრების საიდუმლოს ხელყოფა;

საქართველოს სისხლის სამართლის კოდექსის 157¹-ე მუხლის თანახმად, დასჯად ქმედებას წარმოადგენს „პირადი ცხოვრების საიდუმლოს უკანონოდ მოპოვება, შენახვა, გამოყენება, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა“⁴¹ შესაბამისად, იმ შემთხვევაში თუ ასეთი ქმედება ჩადენილია ციფრული ტექნიკის გამოყენებით - მაგალითად ნაწარმოებია ფოტო - ვიდეოგადაღება ან აუდიოჩაწერა, ან სხვადასხვა სახის ელექტრონული ინფორმაციის მოპოვება პირადი ცხოვრების შესახებ - სახეზე გვაქვს ციფრული დანაშაული, ხოლო რაც შეეხება არნიშნული მუხლის მე-2 ნაწილს - თავად მუხლის შინაარსი გვაძლევს მოცემულობას რომ ეს დაკავშირებულია ციფრულ დანაშაულთან იმ შემთხვევაში, თუ პირადი ცხოვრების საიდუმლოს უკანონოდ გამოყენება ან/და გავრცელება ხორციელდება „ინტერნეტის, მათ შორის, სოციალური ქსელის, მასობრივი მაუწყებლობის ან სხვა საჯარო გამოსვლის მეშვეობით“⁴².

კერძო კომუნიკაციის საიდუმლოების დარღვევა;

საქართველოს სისხლის სამართლის კოდექსის 158-ე მუხლის თანახმად, დასჯად ქმედებას წარმოადგენს „კერძო საუბრის უნებართვო ჩაწერა ან მიყურადება, აგრეთვე კომპიუტერულ სისტემაში ან სისტემიდან კერძო კომუნიკაციისას გადაცემული კომპიუტერული მონაცემის ან ამგვარი მონაცემის მატარებელი ელექტრომაგნიტური ტალღების უნებართვო მოპოვება ტექნიკური საშუალების გამოყენებით ან კერძო კომუნიკაციის ჩანაწერის, ტექნიკური საშუალებით მოპოვებული ინფორმაციის ან კომპიუტერული მონაცემის უკანონოდ შენახვა, აღნიშნული დანაშაული მიეკუთვნება“⁴³ ხოლო ამავე მუხლის მე-2 ნაწილის თანახმად „კერძო კომუნიკაციის

³⁸ საქართველოს სისხლის სამართლის კოდექსი, (22/07/1999 წლის) 29.05.2019 წლის მგდომარებით. მუხლი 157 ნაწილი 1-ლი.

³⁹ იქვე. ნაწილი მე - 2;

⁴⁰ იქვე.

⁴¹ იქვე. მუხლი 157¹ მუხლის 1-ლი ნაწილი.

⁴² იქვე. მე-2 ნაწილი

⁴³ საქართველოს სისხლის სამართლის კოდექსი, (22/07/1999 წლის) 29.05.2019 წლის მგდომარებით. მუხლი 158 მუხლის ნაწილი 1-ლი

ჩანაწერის, ტექნიკური საშუალებით მოპოვებული ინფორმაციის ან კომპიუტერული მონაცემის უკანონოდ გამოყენება, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა,⁴⁴ შესაბამისად აღნიშნული მუხლით სანქცირებული ქმედება მიეკუთვნება ციფრულ დანაშაულთან კატეგორიას.

პირადი მიმოწერის, ტელეფონით საუბრის ან სხვაგვარი ხერხით შეტყობინების საიდუმლოების დარღვევა;

საქართველოს სისხლის სამართლის კოდექსის 159-ე მუხლის თანახმად, დასჯად ქმედებას წარმოადგენს „პირადი მიმოწერის ან საფოსტო გზავნილის, ტელეფონით ან სხვა ტექნიკური საშუალებით საუბრის ჩანაწერის ან ტელეგრაფით, კომპიუტერული სისტემით, ფაქსით ან სხვა ტექნიკური საშუალებით მიღებული ან გადაცემული შეტყობინების უკანონოდ მოპოვება, გახსნა, შინაარსის გაცნობა ან შენახვა“⁴⁵ ხოლო ამავე მუხლის მე-2 ნაწილით დასჯადია: „პირადი მიმოწერის ან საფოსტო გზავნილის, ტელეფონით ან სხვა ტექნიკური საშუალებით საუბრის ჩანაწერის ან ტელეგრაფით, კომპიუტერული სისტემით, ფაქსით ან სხვა ტექნიკური საშუალებით მიღებული ან გადაცემული შეტყობინების უკანონოდ გამოყენება, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა“⁴⁶. შესაბამისად აღნიშნული დანაშაული მიეკუთვნება ციფრულ დანაშაულთან კატეგორიას.

⁴⁴ იქვე, ნაწილი მე-2

⁴⁵ იქვე, მუხლი 159 მუხლის 1-ლი ნაწილი;

⁴⁶ იქვე, მე-2 ნაწილი;

თავი II

ციფრულ დანაშაულთან დაკავშირებული ტერმინოლოგია

2.1. საერთაშორისო სამართლებრივი ტერმინოლოგია

ციფრული დანაშაულის შესახებ

აღნიშნულ პარაგრაფში წარმოდგენილია ყველა ის საერთაშორისო სამართლებრივი ტერმინი და მათი განმარტება, რაც ციფრული დანაშაულის სფეროში დღეის მდგომარეობით საერთაშორისო აქტების დონეზე არსებობს, აღნიშნული ტერმინოლოგიის და მათი განმარტებების ცოდნა უცილებელია ყველა იმ სამართალდამცავი ორგანოს თანამშრომლისათვის და ექსპერტისათვის, ვინც აწარმოებს ან ვისაც შესაძლოა შემხებლობა ჰქონდეს ციფრული დანაშაულის გამოძიებასთან.

როდესაც ნაშრომზე ვმუშაობდით მიხვდით, რომ ვიყენებდით ძალიან ბევრ არაქართულენოვანი ტერმინს, დავინტერესდით და დავიწყეთ შესაბამისი ტერმინების ძიება ქართულ ენაზე, მაგრამ ვერ მოვიძიეთ, ამიტომ იმისათვის, რათა მკითხველმა არ იფიქროს, რომ ნაშრომის ავტორმა ძალ-ღონე დაუკალოა შესაბამისი ტერმინოლოგიის ქართულ ენაზე თარგმნას, გვინდა შემოვთავაზოთ აღნიშნული თავი, სადაც განმარტებული იქნება თუ რა არის კომპიუტერული ტერმინოლოგია და რატომ ვერ ხდება მისი ქართულ ენაზე თარგმნა.

„ვინაიდან კომპიუტერის ენა ინგლისურია, არც არის გასაკვირი, რომ მსოფლიოს სხვადასხვა ენის ლექსიკა მდიდარია ინგლისურენოვანი სიტყვებით. სხვადასხვა ენაში, უპირველეს ყოვლისა, ხდება მათი პროტოტიპისა თუ სინონიმის მოძიება, რაც ხშირ შემთხვევაში არ ხერხდება. ორიგინალური ტერმინებისა თუ ცნებების შემუშავების მაგივრად, ინგლისურენოვანი სიტყვები პირდაპირ შედის სხვადასხვა ენის ლექსიკაში და რა თქმა უნდა, ხანგრძლივი დროით მკვიდრდება. ამ ენობრივი მოვლენის განვითარება და გავრცელება უდაოდ შეტყველებს კომპიუტერული ტექნიკის რბამ დაინტერესებს თანამედროვე საზოგადოების ცხოვრებაში. ამ ტერმინოლოგიამ დღეისათვის განმავლობაში ისევე, როგორც ზოგიერთი სფეროს სპეციფიკურმა ლექსიკამ, შეაღწია სალიტერატურო ენაში და მალე იქაც დაიმკვიდრებს ადგილს.“⁴⁷

„კომპიუტერული ენის ლექსიკის ანალიზის საფუძველზე შეიძლება დავასკვნათ, რომ მეცნიერების ეს სფერო მოიცავს აბრევიატურების ყველაზე დიდ რაოდენობას. უმეტესწილად, შემოკლებულ ერთეულებს ვხვდებით ისეთ კომპიუტერულ ენებში, როგორებიცაა: Hardware, Operating Systems, Editors and Shells, Programming Languages.“⁴⁸

„რაც შეეხება კომპიუტერულ შემოკლებებს, როგორც ვხედავთ, მათ ბოლომდე ვერ მივაკუთვნებთ ვერც სალიტერატუროს, ვერც არასალიტერატურო ლექსიკას. შეგვიძლია უბრალოდ განვიხილოთ, როგორც მოვლენა, რომელსაც თითოეულისთვის დამახასიათებელი ნიშნები აქვს. ეს კი გვაძლევს უფლებას, კომპიუტერული შემოკლება-ტერმინები ჩავთვალოთ სიტყვებად, რომელსაც იყენებს საზოგადოების ის ჯგუფი, ვისაც მუდმივი შეხება აქვს ინტერნეტთან. ამ სიტყვების უმეტესობა, როგორც ვიცით, გამოირჩევა სასაუბრო-სალაპარაკო, ხშირად უხეში ფამილარული ელფერით, მაგრამ არც იმის დავიწყება შეიძლება, რომ კომპიუტერული და ინტერნეტის შემოკლებები ძირითადად პროფესიული ტერმინებიდან ნაწარმოები სიტყვებია.“⁴⁹

⁴⁷ ეკატერინე ბაკრაძე ინგლისური ენის ლექსიკის განვითარების თანამედროვე ტენდენციები, დ ი ს ე რ ტ ა ც ი ა 2009. ნანახია ელ. გვერდი 

⁴⁸ იხ. იქვე.

⁴⁹ ეკატერინე ბაკრაძე ინგლისური ენის ლექსიკის განვითარების თანამედროვე ტენდენციები, დ ი ს ე რ ტ ა ც ი ა 2009. ნანახია ელ. გვერდი 

„ციფრული მტკიცებულება“ - ნებისმიერი ელექტრონული ფორმის დოკუმენტი ან მონაცემი, რომელიც შენახულია, გაგზავნილია ან მიღებულია კომპიუტერული სისტემის მიერ და შეიცავს სისხლის სამართლის საქმის ფაქტობრივი ან სამართლებრივი გარემოების დასადგენად საჭირო ინფორმაციას.⁵⁰

კომპიუტერული დანაშაულის შესახებ ბუდაპეშტის 2001 წლის 23 ნოემბრის კონვენცია გვთავაზობს შემდეგ ტერმინთა განმარტებას:

„კომპიუტერული სისტემა — ნებისმიერი მექანიზმი ან ერთმანეთთან დაკავშირებულ ან ურთიერთდაკავშირებულ მექანიზმთა ჯგუფი, რომელთაგან ერთი ან მეტი, პროგრამის მეშვეობით, ასრულებს მონაცემთა ავტომატურ დამუშავებას;

კომპიუტერული მონაცემები - კონცეფციითაა ნებისმიერი გამოსახვა ფაქტების, ინფორმაციის ან კომპიუტერულ სისტემაში დამუშავებისათვის ხელსაყრელი ფორმით, მათ შორის პროგრამა, რომელიც უზრუნველყოფს კომპიუტერული სისტემის ფუნქციონირებას;

მომსახურების მოწოდებელი - ნებისმიერი საჯარო ან კერძო პირი, რომელიც მისი სერვისის მომხმარებლებს უზრუნველყოფს კომპიუტერული სისტემის საშუალებით ურთიერთობის შესაძლებლობით, და ნებისმიერი სხვა პირი, რომელიც გადაამუშავებს ან ინახავს კომპიუტერულ მონაცემებს ამგვარი საკომუნიკაციო მომსახურების ან ამგვარი მომსახურების მომხმარებელთა სახელით;

ინტერნეტ-ტრაფიკის მონაცემები - კომუნიკაციებთან დაკავშირებული და კომპიუტერული სისტემის მიერ გენერირებული ნებისმიერი კომპიუტერული მონაცემები, რომელიც წარმოადგენს კომუნიკაციასა და ქაჭვის ნაწილს, მიუთითებს კომუნიკაციის წყაროს, დანიშნულების ადგილს, მიმართულებას, დროს, თარიღს, ზომას, ხანგრძლივობას, ძირითადი მომსახურების ტიპს.“⁵¹

ევროპის საბჭოს 2005 წლის 24 თებერვლის ჩარჩო გადაწყვეტილება ინფორმაციულ სისტემებზე თავდასხმის შესახებ გვთავაზობს რამდენიმე ტერმინის საერთაშორისო დეფინიციას:

„კომპიუტერული მონაცემები - ფაქტების, ინფორმაციის ან პროგრამების გამოსახვა, ინფორმაციულ სისტემაში გადაამუშავებისთვის განკუთვნილი ფორმით, ისეთი პროგრამის ჩათვლით, რომელსაც ინფორმაციული სისტემის მეშვეობით ფუნქციების შესრულების მოქმედებაში მოყვანა შეუძლია.“⁵²

„არაუფლებამოსილი მოქმედება - ისეთი შეღწევა ან თავდასხმა, რომელიც სისტემის ან სისტემის ნაწილის მესაკუთრის ან სხვა კანონიერად მფლობელის მიერ არ არის ნებადართული, ან ცალკეული სახელმწიფოებრივი სამართლებრივი ნორმების მიხედვით დაუშვებელია.“⁵³

რაც შეეხება კიბერდანაშაულს — არსებობს „კიბერდანაშაული“-ს ტერმინის სხვადასხვა განმარტება, ამ ტერმინთან დაკავშირებით არ არსებობს რაიმე სახის ერთიანი მიდგომა და მსოფლიოს სხვადასხვა ქვეყნის კანონმდებლობაში სწორად განსხვავებული მნიშვნელობა აქვს. არსებობს კიბერდანაშაულის შინაარსობრივად მსგავსი ტერმინები.

კიბერდანაშაული — წარმოადგენს ორი სიტყვის „კიბერ“ და „დანაშაულის“ ერთობლიობას. სიტყვა „კიბერ“ — კომპიუტერული ქსელი, ვირტუალური რეალობა.

⁵⁰ Eoghan Casey. „ციფრული მტკიცებულება და კომპიუტერული დანაშაული: სასამართლო მეცნიერება, კომპიუტერები და ინტერნეტი“ (ინგლისურად), მესამე გამოცემა. ელ. გვერდი 

⁵¹ ოთხივე ტერმინი: კომპიუტერული დანაშაულის შესახებ კონვენცია 2001 წლის 23 ნოემბერი ბუდაპეშტი.

⁵² იქვე. მუხლი 1-ლი ქვეპუნქტი „ბ“;

⁵³ იქვე. მუხლი 1-ლი ქვეპუნქტი „დ“;

სიტყვა „დანაშაული“ — სისხლის სამართლის კოდექსით გათვალისწინებული მართლსაწი-
ნააღმდეგო, ბრალეული ქმედება.

კიბერვიქტიმიზაცია — კიბერდანაშაულის მსხვერპლად გახდომის პროცესების შესწავლა.

„სართლებრივი ინფორმატიკა - გამოყენებითი მეცნიერებაა, რომელიც შეისწავლის სამართლის
ხეობაში ინფორმაციის (ნორმატიული, საცნობარო და სხვა) შეგროვების, შენახვის, დამუშავების
და გამოყენების პრობლემებს, გადაწყვეტის მეთოდებსა და საშუალებებს. ანუ, სამართლებრივი
ინფორმატიკა ინფორმატიკაა, რომელიც შეისწავლის სამართლებრივი ინფორმაციის ფორმირე-
ბის, ინტერპრეტაციის და კომუნიკაციის პროცესებს.“⁵⁴

2.2. ციფრული დანაშაულის შესახებ სამართლებრივი ტერმინოლოგია ქართულ კანონმდებლობაში

პარაგრაფში, წარმოდგენილია ქართულ საკანონმდებლო სივრცეში არსებული სამართლებრი-
ვი ტერმინოლოგია და მათი განმარტებები, აღნიშნული ტერმინოლოგია აუცილებელია ციფრული
დანაშაულის გამოსაძიებლად და ციფრული მტკიცებულებების ძიების პროცესში.

„კომპიუტერული სისტემა — ნებისმიერი მექანიზმი ან ერთმანეთთან დაკავშირებულ მექანიზმ-
თა ჯგუფი, რომელიც პროგრამის მეშვეობით, ავტომატურად ამუშავებს მონაცემებს (მათ შორის,
პერსონალური კომპიუტერი, ნებისმიერი მოწყობილობა მიკროპროცესორით, აგრეთვე მობილური
ტელეფონი).“⁵⁵

„კომპიუტერული მონაცემი — კომპიუტერულ სისტემაში დამუშავებისათვის ხელსაყრელი
ნებისმიერი ფორმით გამოსახული ინფორმაცია, მათ შორის, პროგრამა, რომელიც უზრუნველყოფს
კომპიუტერული სისტემის ფუნქციონირებას.“⁵⁶

„უნებართვო შეღწევა — უნებართვო გულისხმობს უკანონოს, აგრეთვე იმ შემთხვევას,
როდესაც უფლების მფლობელს პირდაპირ ან არაპირდაპირ არ გადაუცია უფლება ქმედების
ჩამდენი პირისათვის.“⁵⁷

„მომსახურების მომწოდებელი — ნებისმიერი ფიზიკური ან იურიდიული პირი, რომელიც
მომხმარებლებს უზრუნველყოფს შესაძლებლობით, ურთიერთობა განახორციელონ კომპიუ-
ტერული სისტემის საშუალებით, ასევე ნებისმიერი სხვა პირი, რომელიც ამუშავებს ან ინახავს
კომპიუტერულ მონაცემებს ამგვარი საკომუნიკაციო მომსახურების ან ასეთი მომსახურების
მომხმარებელთა სახელით.“⁵⁸

⁵⁴ ციური ნოზაძე, სამართლებრივი ინფორმატიკა, ლექციების კურსი, გვ. 2. ელ. გვერდი. .
ნანახია 24.6.2019.

⁵⁵ საქართველოს სისხლის სამართლის კოდექსი, (22/07/1999 წლის) 29.05.2019 წლის მგდომარეობით.
მუხლი 284, შენიშვნა, ნაწილი 1;

⁵⁶ საქართველოს სისხლის სამართლის კოდექსი, (22/07/1999 წლის) 29.05.2019 წლის მგდომარეობით.
მუხლი 284, შენიშვნა, ნაწილი 1;

⁵⁷ იქვე, ნაწილი 3;

⁵⁸ საქართველოს სისხლის სამართლის საპროცესო კოდექსი (09/10/2009 რედ) 29.05.2019 წლის
მგდომარეობით.. მუხლი 3. ნაწილი 29.

“ინტერნეტრაფიკის მონაცემი — კომუნიკაციებთან დაკავშირებული და კომპიუტერული სისტემის მიერ გენერირებული ნებისმიერი კომპიუტერული მონაცემი, რომელიც კომუნიკაციათა ჯაჭვის ნაწილია, მიუთითებს კომუნიკაციის წყაროს, დანიშნულების ადგილს, მიმართულებას, დროს, თარიღს, ზომას, ხანგრძლივობას, ძირითადი მომსახურების ტიპს.”⁵⁹

„ინფორმაციის მოხსნა და ფიქსაცია კავშირგაბმულობის არხიდან — შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს მიერ ელექტრონული კავშირიდან (ელექტრონული ფოსტა), კავშირგაბმულობის ქსელიდან, სატელეკომუნიკაციო ან საინფორმაციო სისტემიდან მიმდინარე, გადაცემული, მიღებული, შეკრებილი, დამუშავებული ან დაგროვებული ინფორმაციის მოხსნა და ფიქსაცია ტექნიკურ ან/და პროგრამულ საშუალებათა გამოყენებით.”⁶⁰

„ინფორმაციის მოხსნა და ფიქსაცია კომპიუტერული სისტემიდან — შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს მიერ კომპიუტერული სისტემიდან გადაცემული, მიღებული, აგრეთვე კომპიუტერულ სისტემაში მიმდინარე, შეკრებილი, დამუშავებული ან დაგროვებული ინფორმაციის მოხსნა და ფიქსაცია ტექნიკურ ან/და პროგრამულ საშუალებათა გამოყენებით.”⁶¹

„ინფორმაციული უსაფრთხოება — საქმიანობა, რომელიც უზრუნველყოფს ინფორმაციისა და ინფორმაციული სისტემების წვდომის, ერთიანობის, ავთენტიფიკაციის, კონფიდენციალურობისა და განგრძობადი მუშაობის დაცვას.”⁶²

„ინფორმაციული უსაფრთხოების პოლიტიკა — ამ კანონით, საქართველოს სხვა ნორმატიული აქტებითა და საერთაშორისო შეთანხმებებით გათვალისწინებული ნორმებისა და პრინციპების, აგრეთვე პრაქტიკის ერთობლიობა, რომელიც ემსახურება ინფორმაციული უსაფრთხოების უზრუნველყოფას და შეესაბამება მისი დაცვის სფეროში დადგენილ საერთაშორისო სტანდარტებს.”⁶³

„კიბერსივრცე — სივრცე, რომლის განმასხვავებელი ნიშანია ელექტრონული მოწყობილობებისა და ელექტრომაგნიტური სპექტრის გამოყენება ქსელით დაკავშირებული სისტემებისა და დამხმარე ფიზიკური ინფრასტრუქტურის მეშვეობით მონაცემთა შენახვისათვის, შეცვლისათვის ან გაცვლისათვის.”⁶⁴

„კიბერშეტევა — ქმედება, როდესაც ელექტრონული მოწყობილობა ან/და მასთან დაკავშირებული ქსელი ან სისტემა გამოიყენება კრიტიკულ ინფორმაციულ სისტემაში შემავალი სისტემების, ქონების ან ფუნქციების მთლიანობის დარღვევის, შეფერხების ან განადგურების ან ინფორმაციის უკანონოდ მოპოვების გზით.”⁶⁵

„კომპიუტერული ინციდენტი — ინფორმაციული უსაფრთხოების პოლიტიკის რეალური ან პოტენციური დარღვევა, რომელიც ხორციელდება ინფორმაციული ტექნოლოგიის გამოყენებით

⁵⁹ იქვე. ნაწილი 30.

⁶⁰ იქვე. ნაწილი 33.

⁶¹ იქვე. მუხლი 3. ნაწილი 34.

⁶² საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ. (5.06.2016 წლის რედაქციით. კონოლიდირებული 08.07.2017) მუხლი 2. ქვეპუნქტი “ა”.

⁶³ საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ. (5.06.2016 წლის რედაქციით. კონოლიდირებული 08.07.2017) მუხლი 2 ქვეპუნქტი “ბ”.

⁶⁴ იქვე. ქვეპუნქტი “გ”.

⁶⁵ იქვე. ქვეპუნქტი “დ”.

და იწვევს ინფორმაციის უნებართვო წვდომას, გამჟღავნებას, დაზიანებას ან შეფერხებას ან ინფორმაციული რესურსის მიტაცებას.“⁶⁶

„ინფორმაციული სისტემა — ინფორმაციული ტექნოლოგიებისა და ამ ტექნოლოგიების გამოყენებით განხორციელებული ქმედებების ნებისმიერი კომბინაცია, რომელიც ხელს უწყობს მართვას ან/და გადაწყვეტილების მიღებას.“⁶⁷

„ქსელური სენსორი — მოწყობილობა, რომელიც სპეციალურად გამიზნულია ქსელის სეგმენტის მონიტორინგისთვის, ისეთი ქმედებების გამოსავლენად, რომლებიც მიუთითებს ინფორმაციული სისტემის წინააღმდეგ წარმოებულ შეტევაზე ან მასში შეღწევაზე.“⁶⁸

„მონაცემთა გაცვლის სააგენტო — საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირი (შემდგომ — მონაცემთა გაცვლის სააგენტო).“⁶⁹

„კიბერუსაფრთხოების ბიურო — საქართველოს თავდაცვის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირი (შემდგომ — კიბერუსაფრთხოების ბიურო).“⁷⁰

„ინტერფეისი — ელექტრონული საკომუნიკაციო ქსელის ელემენტების, ტექნიკური საშუალებების, საოპერაციო პროგრამული რესურსებისა და სისტემების ურთიერთმოქმედების ფიზიკური ან ლოგიკური ფორმატი, რომელიც განსაზღვრულია საერთო ფუნქციონალური, ელექტრული, ოპტიკური, კონსტრუქციული და სხვა თავსებადობის მახასიათებლებით, პროტოკოლის მიმართ ერთგვაროვანი მოთხოვნებით.“⁷¹

„აბონენტი — ბოლო მომხმარებელი, რომელსაც ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებელთან წინასწარ გაფორმებული წერილობითი ხელშეკრულების საფუძველზე მიეწოდება საერთო სარგებლობის ელექტრონული საკომუნიკაციო მომსახურება.“⁷²

„აბონენტის ინდივიდუალური დაშვების სისტემა — ტექნოლოგიური სისტემა, ტექნიკური საშუალებები და მათთან დაკავშირებული საოპერაციო მართვის პროგრამული უზრუნველყოფის რესურსები, რომლებიც უზრუნველყოფს აბონენტის მიერ ინდივიდუალური, კოდირებული ციფრული მუწყებლობის მომსახურების მიღებას.“⁷³

„ელექტრონული საკომუნიკაციო ქსელის ელემენტები — ელექტრონული საკომუნიკაციო ქსელის შემადგენელი, ფუნქციონალურად განცალკევებული (ან განცალკევებადი) ტექნიკური ან ტექნოლოგიური საშუალებები, მათი საოპერაციო ფუნქციონალური რესურსები და სიმძლავრეები, რომლებიც თავიანთი მახასიათებლებით უზრუნველყოფს: გამოძახებებისა და საინფორმაციო სიგნალების გატარებას, გადაცემას, დამისამართებას (კომუტაციას); ბილინგის ინფორმაციის

⁶⁶ საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ. (5.06.2016 წლის რედაქციით. კონოლიდირებული 08.07.2017) მუხლი 2 ქვეპუნქტი "ე".

⁶⁷ იქვე. ქვეპუნქტი "ლ".

⁶⁸ იქვე. ქვეპუნქტი "შ".

⁶⁹ საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ. (5.06.2016 წლის რედაქციით. კონოლიდირებული 08.07.2017) მუხლი 2 ქვეპუნქტი "ნ".

⁷⁰ იქვე. ქვეპუნქტი "ო".

⁷¹ საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2-3;

⁷² იქვე. ქვეპუნქტი "ა";

⁷³ იქვე. ქვეპუნქტი "ბ";

შეგროვებას; ბოლო მომხმარებლისათვის მიწოდებული მომსახურების პირობების მართვას და ურთიერთობერაბელურობას; სააბონენტო ნომრების პორტაბელურობას; ოპერატორის საოპერაციო, საცნობარო, დამხმარე და საგანგებო მომსახურებას; ქსელების სინქრონიზაციასა და სიგნალიზაციას; გამოძახებებთან დაკავშირებულ მონაცემთა ბაზებში შეღწევას; მულტიმედიას; ციფრული მაუწყებლობის მომსახურების მიწოდებას; კონვერსიას, კოდირებას, უსაფრთხოების დაცვას; პეიჟინგს; ციფრული მონაცემების ტელედამუშავებას და ინტერნეტის ან სხვა პროტოკოლის გამოყენებით გადაცემას და სხვა.”⁷⁴

„ადგილობრივი დაშვების ქსელი – ადგილობრივი მომსახურების ზონაში ოპერატორის სადენიანი (ელექტროსადენიანი ან ოპტიკურ-ბოჭკოვანი) საკაბელოსახაზო მეურნეობა ან უსადენო (ფიქსირებული რადიოსიხშირული ან ლია ოპტიკური) დაშვების ტექნიკური საშუალებები ელექტრონული საკომუნიკაციო მომსახურების მიწოდების მიზნით, ბოლო მომხმარებლის ფიქსირებულ ტერმინალურ მოწყობილობასა და საკომუნიკაციო ან გადაცემსადგურს შორის გამომსახვებების ან საინფორმაციო სიგნალების გასატარებლად, ციფრული მაუწყებლობის სიგნალების გადასაცემად.”⁷⁵

„ადგილობრივი მომსახურების ზონა – მომსახურების ბაზრის გეოგრაფიული (ტერიტორიული) ხეგმენტი, სადაც ავტორიზებული პირი ახორციელებს ბოლო მომხმარებლისთვის საერთო სარგებლობის ელექტრონული საკომუნიკაციო მომსახურების მიწოდებას.”⁷⁶

„ავტორიზაცია – საქართველოს კომუნიკაციების ეროვნული კომისიის მიერ საერთო სარგებლობის ელექტრონული საკომუნიკაციო ქსელებითა და საშუალებებით უზრუნველყოფის ან/და ელექტრონული საკომუნიკაციო მომსახურების მიწოდების განმახორციელებელი ფიზიკური ან იურიდიული პირის საქმიანობის რეგისტრაცია ამ კანონით დადგენილი ერთიანი წესით.”⁷⁷

„ავტორიზებული პირი – საქართველოს კომუნიკაციების ეროვნული კომისიის მიერ რეგისტრირებული ნებისმიერი სამეწარმეო პირი, აგრეთვე ნებისმიერი არასამეწარმეო იურიდიული პირი, რომელიც ახორციელებს ელექტრონული საკომუნიკაციო ქსელებით უზრუნველყოფას (ელექტრონული საკომუნიკაციო ქსელის ოპერატორი) ან/და ელექტრონული საკომუნიკაციო მომსახურების მიწოდებას (ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებელი).”⁷⁸

„ავტორიზებული პირების ერთობლივი მნიშვნელოვანი საბაზრო ძალაუფლება – მომსახურების ბაზრის შესაბამის ხეგმენტზე ორი ან მეტი ავტორიზებული პირის ერთობლივი მნიშვნელოვანი საბაზრო ძალაუფლება, ანუ ისეთი მდგომარეობა, როცა საქართველოს კომუნიკაციების ეროვნული კომისიის მიერ ჩატარებული ანალიზი ადასტურებს, რომ ბაზრის ამ ხეგმენტზე ჩამოყალიბებული კონიუნქტურა და კონკურენციის მახასიათებლები მათი შეთანხმებულად მოქმედებისა და ბაზარზე არაკონკურენტული უპირატესობის ერთობლივად მოპოვების შესაძლებლობას იძლევა, მაშინაც კი, თუ მათ შორის არ არსებობს სტრუქტურული ან სხვა სახის, მათ შორის, სახელშეკრულებო ურთიერთობები.”⁷⁹

⁷⁴ საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2-“337”;

⁷⁵ იქვე. ქვეპუნქტი “გ”;

⁷⁶ იქვე. ქვეპუნქტი “დ”;

⁷⁷ იქვე. ქვეპუნქტი “ე”;

⁷⁸ საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2- ქვეპუნქტი “ვ”;

⁷⁹ იქვე. ქვეპუნქტი “ზ”;

„ამოწურვადი რესურსი - რადიოსიხშირული სპექტრი ან/და ნუმერაციის რესურსი.“⁸⁰

„არაპირდაპირი დაშვება — ელექტრონული საკომუნიკაციო ქსელის ოპერატორის მიერ საკუთარი ქსელის ელემენტებთან, მათ ფუნქციონალურ რესურსებთან და თავისუფალ სიმძლავრეებთან, ან მათი გამოყენებით განხორციელებულ (ან განხორციელებად) ელექტრონული საკომუნიკაციო მომსახურების სახეებთან მომხმარებლის ან მსურველი ავტორიზებული პირის დაშვება სხვა ტრანზიტული კავშირის (მომსახურების) ოპერატორის ქსელების გავლით.“⁸¹

„ბილინგის ინფორმაცია — მომხმარებლისთვის მიწოდებული მომსახურების ან ოპერატორის ქსელის შესაბამისი ელემენტების დადგირთვის (ტრაფიკის) და მათი საოპერაციო რესურსების გარკვეულ პერიოდში გამოყენებული მოცულობის შესახებ მონაცემები, რომელთაც ოპერატორები აწვდიან ერთმანეთს ან ბოლო მომხმარებელს ანგარიშსწორების ჩატარების მიზნით.“⁸²

„ბოლო მომხმარებელი — მომხმარებელი, რომელიც საკუთარი მოხმარებისათვის იყენებს ან განზრახული აქვს გამოიყენოს საერთო სარგებლობის ელექტრონული საკომუნიკაციო ქსელებითა და საშუალებებით განხორციელებული მომსახურება და მიზნად არ ისახავს მის შემდგომ მიყიდვას სხვა მომხმარებლისათვის.“⁸³

„გამოყენებითი პროგრამული ინტერფეისი — ციფრული მაუწყებლობის ან ელექტრონული საკომუნიკაციო მომსახურების მიწოდების მომსახურების სახეების სამომხმარებლო რესურსებისა და ციფრული მაუწყებლობის ტექნიკური საშუალებების ფუნქციონალური რესურსების დამაკავშირებელი პროგრამული ინტერფეისი.“⁸⁴

„დაშვება — ელექტრონული საკომუნიკაციო ქსელის ოპერატორის მიერ განსაზღვრული პირობებით (მათ შორის, ტარიფებით) საკუთარი ქსელის შესაბამისი ელემენტებით, ტექნიკური საშუალებებით, მათი თავისუფალი ფუნქციონალური რესურსებითა და სიმძლავრეებით, ან მათი გამოყენებით განხორციელებული (ან განხორციელებადი) ელექტრონული საკომუნიკაციო მომსახურების სახეებით სარგებლობის უზრუნველყოფა, რომელიც მოიცავს:

ელექტრონული საკომუნიკაციო ქსელის ოპერატორის საკუთარი ქსელის ფიზიკური ინფრასტრუქტურის შესაბამისი ელემენტებითა და ტექნიკური საშუალებებით სარგებლობის უზრუნველყოფას; ადგილობრივი დაშვების ქსელის ელემენტებითა და მათი თავისუფალი რესურსებით, მათ შორის, საკანალიზაციო არხებითა და ჭებით, სააბონენტო წყვილებით, ანძებით და ბოძებით სარგებლობის უზრუნველყოფას; თანალოკაციის ფართობით სარგებლობის უზრუნველყოფას; ფიქსირებული და მობილური საკომუნიკაციო ქსელის ოპერატორების ქსელის შესაბამისი ელემენტებით, მათი თავისუფალი საოპერაციო ფუნქციონალური რესურსებითა და სიმძლავრეებით (მათ შორის, როუმინგის მიწოდებასთან დაკავშირებული რესურსებით) სარგებლობის უზრუნველყოფას; აბონენტის ინდივიდუალური დაშვების სისტემისა და პროგრამების (მომსახურების) ელექტრონული სარჩევის (მეგზურის) რესურსებით სარგებლობის უზრუნველყოფას; ელექტრონული საკომუნიკაციო ქსელების საოპერაციო პროგრამული მართვისა და მომხმარებელთა საინფორმაციო ბაზების,

⁸⁰ საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2- ქვეპუნქტი "თ";

⁸¹ იქვე. ქვეპუნქტი "კ";

⁸² საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2- ქვეპუნქტი "ნ";

⁸³ იქვე ქვეპუნქტი "ო";

⁸⁴ იქვე ქვეპუნქტი "ჟ";

სააბონენტო ნომრების პორტაბელურობასთან (ტრანსლირებასთან) დაკავშირებული რესურსებით სარგებლობის უზრუნველყოფას; ვირტუალური ქსელების მომსახურების სახეებით სარგებლობის უზრუნველყოფას; ელექტრონული საკომუნიკაციო ქსელის სხვა შესაბამისი ელემენტების ფუნქციონალური რესურსებითა და სიმძლავრეებით ან საკომუნიკაციო მომსახურების სახეებით სარგებლობის უზრუნველყოფას.“⁸⁵

„დშვების (ურთიერთმართვის) წერტილი – თანალოკაციის ფართობზე განთავსებული წერტილი, სადაც მთავრდება ერთი ოპერატორის და იწყება მეორე ოპერატორის დაშვებასთან ან/და ურთიერთმართვასთან დაკავშირებული პასუხისმგებლობა.“⁸⁶

„ელექტრონული საკომუნიკაციო მომსახურება – საერთო სარგებლობის ელექტრონული საკომუნიკაციო ქსელებითა და საშუალებებით განხორციელებული მომსახურება, რომელსაც მომსახურების მიწოდებული ავტორიზებული პირი განსაზღვრული საფასურის სანაცვლოდ სთავაზობს მსურველ ოპერატორს ან მომხმარებელს.“⁸⁷

„ელექტრონული საკომუნიკაციო ქსელები (ელექტრო-კავშირგაბმულობის ქსელები) – გამოძახებებისა და სხვადასხვა საინფორმაციო სიგნალების ელექტრონული დამუშავების, დამისამართების (კომუტაციის), გატარების და გადაცემის ტექნოლოგიური სისტემა, რომელიც მოიცავს სადენიან (მათ შორის, ოპტიკურბოჭკოვან), თანამგზავრულ, რადიოსიხშირულ ან ოპტიკურ ადტუვილობას, სხვა ტექნოლოგიურ საშუალებებს და საოპერაციო ტექნიკურ რესურსებს, მათ შორის, ფიქსირებული (არხული და პაკეტური კომუტაციის, მათ შორის, ინტერნეტის) და მობილური კომუნიკაციების, ციფრული მაუწყებლობის, საეთერო და საკაბელო ქსელებს. სახელმწიფო თავდაცვის, უშიშროებისა და მართლწესრიგის დაცვის ორგანოების ელექტრონული საკომუნიკაციო ქსელებით უზრუნველყოფა ითვალისწინებს ელექტრონული საკომუნიკაციო სპეციალური ქსელების არსებობასაც.“⁸⁸

„ელექტრონული საკომუნიკაციო ქსელებით უზრუნველყოფა – ქსელების, ტექნიკური საშუალებების ან ქსელის შესაბამისი ელემენტების მონტაჟი, საოპერაციო მართვა, ექსპლუატაცია და მათი გამოყენებით ეკონომიკური საქმიანობა, აგრეთვე ქსელის ამ ელემენტებთან, მათ რესურსებთან და სიმძლავრეებთან მსურველი ავტორიზებული პირების დაშვება.“⁸⁹

„ელექტრონული საკომუნიკაციო უწყებრივი ქსელი – ქსელი, რომელიც შექმნილია არაკომერციული მიზნით, ფუნქციონირებს შიდასაწარმოო საჭიროებისათვის და ჩართულია საერთო სარგებლობის ელექტრონულ საკომუნიკაციო ქსელში.“⁹⁰

„ელექტრონული საკომუნიკაციო ქსელის ოპერატორი – ავტორიზებული პირი, რომელსაც განზრახული აქვს ან ახორციელებს საერთო სარგებლობის ელექტრონული საკომუნიკაციო ქსელებით ან ქსელის შესაბამისი ელემენტებით უზრუნველყოფას და განსაზღვრული საფასურის სანაცვლოდ მსურველი ავტორიზებული პირის ამ ელემენტებთან, მათ რესურსებთან და

⁸⁵ საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2-“რ-რ8”;

⁸⁶ იქვე ქვეპუნქტი “უ”;

⁸⁷ იქვე. ქვეპუნქტი “ლ”;

⁸⁸ იქვე-ქვეპუნქტი “ყ”;

⁸⁹ საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2- ქვეპუნქტი “შ”;

⁹⁰ იქვე ქვეპუნქტი “ჩ”;

სიმძლავრეებთან დაშვებას, ასევე მათი გამოყენებით მომხმარებლებისათვის ელექტრონული საკომუნიკაციო მომსახურების მიწოდებას.“⁹¹

„ელექტრონული საკომუნიკაციო მომსახურების მიმწოდებელი – ელექტრონული საკომუნიკაციო ქსელის ოპერატორი ან მისი ქსელის შესაბამის ელემენტებთან ან რესურსებთან დაშვებული ავტორიზებული პირი, რომელსაც განზრახული აქვს ან ახორციელებს ქსელის ამ ელემენტებით ან რესურსებით ელექტრონული საკომუნიკაციო მომსახურების მიწოდებას.“⁹²

„მომხმარებელი – იურიდიული ან ფიზიკური პირი, რომელიც იყენებს ან განზრახული აქვს გამოიყენოს ელექტრონული საკომუნიკაციო მომსახურება.“⁹³

„მომხმარებლის ტერმინალური მოწყობილობა – აბონენტის ან ბოლო მომხმარებლის მიერ ელექტრონული საკომუნიკაციო მომსახურების მისაღებად განკუთვნილი, მობილური ან ფიქსირებულ მისამართზე განთავსებული ტექნიკური აღჭურვილობა, რომელიც არ არის ოპერატორის ქსელის ნაწილი, თუმცა დაკავშირებულია მასთან.“⁹⁴

„ნუმერაციის სისტემა – სიმბოლოების განსაზღვრული კომბინაცია, რომელიც გამოიყენება ელექტრონული საკომუნიკაციო მომსახურების მიწოდების პროცესში ელექტრონული საკომუნიკაციო ოპერატორის ქსელის ან მომხმარებლის ტერმინალური მოწყობილობის იდენტიფიცირებისათვის.“⁹⁵

„სააბონენტო ნუმერაცია – ნუმერაციის სისტემის საფუძველზე არსებული ციფრული სისტემა აბონენტის ტერმინალური მოწყობილობის იდენტიფიცირებისათვის.“⁹⁶

„საერთო სარგებლობის ელექტრონული საკომუნიკაციო ქსელი – ელექტრონული საკომუნიკაციო ქსელების ერთიანი სისტემა, რომელიც განკუთვნილია მომხმარებლებისთვის საზოგადოებისათვის შეუზღუდავად ხელმისაწვდომი, საერთო სარგებლობის ელექტრონული საკომუნიკაციო მომსახურების მისაწოდებლად.“⁹⁷

„ელექტრონული საკომუნიკაციო სპეციალური ქსელები – საერთო სარგებლობის ელექტრონული საკომუნიკაციო ქსელისგან ფიზიკურად განცალკევებული ქსელები, რომლებიც შექმნილია არაკომერციული მიზნით, სახელმწიფო თავდაცვის, უშიშროებისა და მართლწესრიგის დაცვის ღონისძიებათა ჩასატარებლად.“⁹⁸

„ტექნიკური საშუალებები – ელექტრონული საკომუნიკაციო გამოძახებებისა და საინფორმაციო

⁹¹ საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2- ქვეპუნქტი "ც";

⁹² იქვე. ქვეპუნქტი "ძ";

⁹³ იქვე. ქვეპუნქტი "პ9";

⁹⁴ იქვე ქვეპუნქტი "პ10";

⁹⁵ საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2- ქვეპუნქტი "პ13";

⁹⁶ იქვე ქვეპუნქტი "პ17";

⁹⁷ იქვე. ქვეპუნქტი "პ18";

⁹⁸ იქვე. ქვეპუნქტი "პ22";

სიგნალების ფორმირების, დამუშავების, გატარების, გადაცემის ან მიღების მიზნით გამოყენებული ელექტრონული საკომუნიკაციო ქსელის აღჭურვილობა და საშუალებები. " ⁹⁹

„ტრაფიკი – ოპერატორის ქსელის ელემენტებისა და ტექნიკური საშუალებების ჯამური დატვირთვა დროის ინტერვალში. " ¹⁰⁰

„ელექტრონული საკომუნიკაციო ქსელების სახაზო საშუალებები და ნაგებობები – ელექტრონული საკომუნიკაციო ქსელების საკაბელო, საჰაერო, რადიოსარეულო, თანამგზავრული ხაზების ფიზიკური წრედები და სახაზო ტრაქტები ან/და მათი ტექნოლოგიური სისტემის შემადგენელი დანადგარების, მოწყობილობებისა და ნაგებობების ერთიანი კომპლექსები, რომლებიც გამოიყენება ელექტრონული საკომუნიკაციო გამოძახებისა და საინფორმაციო სიგნალების გატარებისათვის ან/და გადაცემისათვის. " ¹⁰¹

„ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემები — მომხმარებლის მაიდენტიფიცირებელი მონაცემები; კომუნიკაციის წყაროს კვალის დადგენისა და იდენტიფიცირებისათვის საჭირო მონაცემები; კომუნიკაციის ადრესატის იდენტიფიცირებისათვის საჭირო მონაცემები; კომუნიკაციის თარიღის, დროისა და ხანგრძლივობის იდენტიფიცირებისათვის საჭირო მონაცემები; კომუნიკაციის სახის იდენტიფიცირებისათვის საჭირო მონაცემები; მომხმარებლის კომუნიკაციის აღჭურვილობის ან შესაძლო აღჭურვილობის იდენტიფიცირებისათვის საჭირო მონაცემები; მობილური კომუნიკაციის აღჭურვილობის ადგილმდებარეობის იდენტიფიცირებისათვის საჭირო მონაცემები. " ¹⁰²

„ობიექტის ტექნიკური იდენტიფიკატორი – საქართველოს სისხლის სამართლის საპროცესო კოდექსის მე-3 მუხლის 37-ე ნაწილით განსაზღვრული იდენტიფიკატორი, აგრეთვე „კონტრდაზვერვითი საქმიანობის შესახებ“ საქართველოს კანონის მე-2 მუხლის „რ“ ქვეპუნქტით გათვალისწინებული იდენტიფიკატორი. " ¹⁰³

„კომუნიკაციის რეალურ დროში მოპოვების ნახევრად სტაციონარული ტექნიკური შე-
საძლებლობა – ელექტრონული საკომუნიკაციო ქსელით გადაცემული კომუნიკაციის და მისი მაიდენტიფიცირებელი მონაცემების გადაჭერა უფლებამოსილი ორგანოს მიერ კომუნიკაციის მიმდინარეობისას ან მისი დასრულებისთანავე, ელექტრონული კომუნიკაციის კომპანიის ქსელურ ან/და სასადგურ ინფრასტრუქტურაზე შესაბამისი აპარატული ან/და პროგრამული უზრუნ-
ველყოფის საშუალებების დროებითი ან მუდმივი განთავსებით/მონტაჟით. " ¹⁰⁴

⁹⁹ იქვე. ქვეპუნქტი "325";

¹⁰⁰ იქვე ქვეპუნქტი "328";

¹⁰¹ საქართველოს კანონი ელექტრონული კომუნიკაციის შესახებ. 08.05.2019 წლის მდგომარეობით. მუხლი. 2- "344";

¹⁰² იქვე ქვეპუნქტი - "362";

¹⁰³ იქვე. ქვეპუნქტი "365"

¹⁰⁴ იქვე. ქვეპუნქტი "366";

თავი III

ციფრულ დანაშაულთან ბრძოლის სამართლებრივი რეგულაციები

3.1 ციფრულ დანაშაულთან ბრძოლის საერთაშორისო სამართლებრივი რეგულაციები

აღსანიშნავია, რომ მსოფლიოს მასშტაბით ძალზედ ინტენსიურად წარმოებს ციფრულ მტკიცებულებების საფუძველზე ჩადენილ დანაშაულებთან ბრძოლა, რასთან დაკავშირებითაც შექმნილი იქნა რამდენიმე საერთაშორისო ძალის მქონე დოკუმენტი, მათ შორის საერთაშორისო და საქართველოსთვის მნიშვნელოვანი ძალის მქონე დოკუმენტს წარმოადგენს ევროსაბჭოს კონვენცია „კიბერდანაშაულის შესახებ“, რომელიც მიღებულია 2001 წლის 23 ნოემბერს ქ. ბუდაპეშტში, დოკუმენტი მიღებულია ევროსაბჭოს 41 წევრი სახელმწიფოს მიერ.

გარდა სხვა დებულებებისა, კონვენციის 35-ე მუხლის თანახმად, ყველა წევრ სახელმწიფოს ეკისრება ვალდებულება, რომ დანიშნოს საკონტაქტო პირი, რომელსაც დაუკავშირდებიან კვირაში 7 დღის მანძილზე, 24 საათის განმავლობაში რათა უზრუნველყოფილ იქნეს კომპიუტერულ სისტემებთან და მონაცემებთან დაკავშირებულ დანაშაულების გამოძიება და დევნა - ბუნებრივია ასეთი საჭიროების არსებობის შემთხვევაში, ხოლო ამგვარი დახმარება უნდა უზრუნველყოფდეს ტექნიკური რჩევებით, მტკიცებულებათა მოპოვებისათვის და დაცვისათვის მიცემული რჩევებისა და დანაშაულის ჩამდენ შესაძლო პირთა ადგილმდებარეობის დადგენის მიზნებისათვის რჩევების გაცემას. გასათვალისწინებელია, რომ საქართველოს შინაგან საქმეთა სამინისტროს გააჩნია უფასო ცხელი ხაზი - 112 და შესაბამისი ელექტრონული ფოსტა cybercrime@mia.gov.ge.

მსგავსი ცხელი ხაზის შექმნასთან დაკავშირებით „ეუთო“-მა¹⁷⁶ მოუწოდა მისი გადაწყვეტილებით სახელმწიფოებს, რომ შეუერთდნენ ევროსაბჭოს მიღებულ კონვენციას „კიბერდანაშაულის შესახებ“ და „დიდი რვიანის“ ქვეყნების მიერ კომპიუტერული დანაშაულის წინააღმდეგ ბრძოლისთვის შექმნილ მუდმივმოქმედ ქსელს, რომლის მიზანია კვირაში შვიდი დღე ოცდაოთხი საათი მოკავშირე სახელმწიფოებისთვის ინფორმაციის მიწოდება და კომპეტენციის ფარგლებში სათანადო დახმარების აღმოჩენა. მსგავსი ქსელი ასევე შექმნილია „ინტერპოლის“ ფარგლებშიც. იგი მთელი მსოფლიოს მასშტაბით აერთიანებს ასამდე მუდმივმოქმედ დაწესებულებას, რომელიც ინტერპოლის წევრსახელმწიფოებს ეხმარება მოძებნონ საჭირო სპეციალისტი სხვადასხვა ქვეყანაში, დროულად მიიღონ მათი დახმარება კომპიუტერული დანაშაულის გამოძიების და მასზე მტკიცებულების შეგროვებასთან დაკავშირებით.¹⁷⁶

„უნდა აღინიშნოს ასევე საბჭოს 2005 წლის 24 თებერვლის ჩარჩო გადაწყვეტილება ინფორმაციის სისტემებზე თავდასხმის შესახებ, რომლის მიზანია ცალკეული სახელმწიფოების სისხლისსამართლებრივი ნორმების პარამონიაციის გზით ინფორმაციულ სისტემებზე თავდასხმების აღსაკვეთად წევრი სახელმწიფოების იუსტიციურ და სხვა უფლებამოსილ ორგანოებს შორის თანამშრომლობის გაუმჯობესება. აღსანიშნავია, რომ უკანასკნელ პერიოდში, განსაკუთრებით ორგანიზებული დანაშაულის ფარგლებში, ხშირად ხორციელდება ინფორმაციულ სისტემებზე თავდასხმები და იზრდება ამგვარ სისტემებზე ტერორისტული თავდასხმების რისკი. ამით კი, საფრთხე ეშუქრება საზოგადოების ინფორმაციულ უსაფრთხოებასა და თავისუფლების, უსაფრთხოებისა და სამართლოს სივრცის აშენების მიზანს. აღნიშნული საშიშროებების გადასაღლხად, 2001 წლის 5 სექტემბერს, ევროპულმა პარლამენტმა თავის გადაწყვეტილებაში მიუთითა ამ პრობლემისათვის

¹⁷⁶ იხ. უნა ზაქაშვილი. ნაშრომი „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში“. 2014 წელი. გვ. 24

პრაქტიკული დახმარების მხარდაჭერის აუცილებლობაზე, ამ მიზით კი 2005 წლის 24 თებერვალს, ევროკავშირის საბჭომ, ევროპის კავშირის ხელშეკრულების, განსაკუთრებით 29-ე, 30-ე მუხლის 1-ლი ნაწილის "ა", 31-ე მუხლის 1-ლი ნაწილის "ე" და 34-ე მუხლის მე-2 ნაწილის "ბ" პუნქტებზე დაყრდნობით, კომისიის ინიციატივით, ევროპარლამენტის მიერ პოზიციის გამოსათვის შემდეგ, მიიღო წარმოდგენილი ჩარჩო — გადაწყვეტილება. ჩარჩო გადაწყვეტილება იცავს ძირითად უფლებებსა და თავისუფლებებს და პატივს სცემს იმ პრინციპებს, რომელიც ევროპის კავშირის ხელშეკრულების მე-6 მუხლითა და ევროპის კავშირის ძირითად უფლებათა ქარტიით, უპირველეს ყოვლისა მე-2 და მე-4 თავებით არის აღიარებული." ¹⁰⁶ აღნიშნული გადაწყვეტილება შედგება პრეამბულისა და 13 ძირითადი დებულებისაგან.

როდესაც ვსაუბრობთ ციფრულ დანაშაულზე, მნიშვნელოვანია განვიხილოთ ევროპის ქვეყნებში აღნიშნულ დანაშაულთან ბრძოლის სამართლებრივი მექანიზმები, რომელთა საფუძველზეც საქართველომ უნდა აიღოს მგალობითი და გაატაროს ისეთი ღონისძიებები, როგორც ევროპაში. განვიხილოთ რამდენიმე მნიშვნელოვანი მიღწევების მქონე სახელმწიფო:

„გერმანია — გერმანიაში კომპიუტერული ინფორმაციის სფეროში ჩადენილ დანაშაულებზე სისხლისსამართლებრივი პასუხისმგებლობის საკითხი 1986 წლიდან დადგა. 1987 წლის აგვისტოდან განხორციელდა შესაბამისი ცვლილებები გერმანიის სისხლის სამართლის კოდექსში, რითიც დადგინდა პასუხისმგებლობა კომპიუტერული დანაშაულისთვის." ¹⁰⁷

„გერმანიაში საკანონმდებლო ცვლილებაზე მსჯელობა 2007 წლიდან დაიწყო. ევროსაბჭოს ექსპერტი მარკო გერკე, რომელიც მიწვეული იყო გერმანიის საკანონმდებლო ორგანოში ცვლილებების პროექტის მომზადების პროცესში, ჯერ კიდევ 2007 წლის ივლისში, აცხადებდა, რომ გერმანიის კანონმდებლობა განსხვავებით ბევრი სხვა ქვეყნისგან არ აწესებდა სისხლისსამართლებრივ პასუხისმგებლობას კომპიუტერში არ მის ქსელში უნებართვო შეღწევისთვის. ეს ქმედება დასაჯადი იყო მხოლოდ მაშინ, თუ იგი ინფორმაციის მოპოვებას გამოიწვევდა. მ. გერკეს დასაბუთებულად მიაჩნდა, რომ აღნიშნული ხარვეზი საჭიროებდა აღმოფხვრას და კომპიუტერულ სისტემაში უნებართვო შეღწევა უნდა ყოფილიყო დასაჯადი, მიუხედავად იმისა დადგა თუ არა რაიმე შედეგი. მ. გერკეს აუცილებლად მიაჩნდა „კიბერდანაშაულის შესახებ“ კონვენციის მე-6 მუხლით გათვალისწინებული ქმედების კრიმინალიზაცია. მისი აზრით, ცვლილება უნდა შეხებოდა გერმანიის სისხლის სამართლის 303-ბ მუხლსაც, რომლის ძველი რედაქციით დასაჯადი იყო იმ ინფორმაციის დამუშავების პროცესის ხელყოფა, რომელიც განსაკუთრებული მნიშვნელობის იყო ბიზნესის, საწარმოს ან ადმინისტრაციული ორგანოსთვის. მ. გერკეს აზრით, ცვლილების შედეგად ქმედება დასაჯადი უნდა ყოფილიყო იმ შემთხვევაშიც თუ მოხდებოდა იმ ინფორმაციის დამუშავების პროცესის ხელყოფა, რომელიც ინახებოდა კერძო პირის კომპიუტერში. მ. გერკეს პოზიციას ყველა ნაწილში ვიზიარებ. იგი კიბერდანაშაულის სფეროში ერთ-ერთი საუკეთესო ექსპერტია, თუმცა მისი პოზიცია 2007 წელს გაზიარებული არ იქნა, მაგრამ გერმანიაში «კიბერდანაშაულის შესახებ» კონვენციის რატიფიცირება 2009 წლის მარტში მაინც მოახდინა. ამჟამად, გერმანულ სისხლის სამართლის კოდექსში გათვალისწინებულია, მ. გერკეს პოზიცია[...]" ¹⁰⁸.

¹⁰⁶ მერაბ ტურავა, "ევროპული სისხლის სამართალი" 2010 წ. გვ. 472.

¹⁰⁷ იხ. უჩა ზაქაშვილი, ნაშრომი „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში". 2014 წელი. გვ. 18

¹⁰⁸ უჩა ზაქაშვილი, ნაშრომი „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში". 2013 წ. გვ. 120. ელ. გვერდი



მნიშვნელოვანია, გერმანიის სისხლის სამართლის კოდექსის მიმოხილვაში გავითვალისწინოთ კიოლოს უნივერსიტეტის პროფესორის პაულ მარტინ ვასმერი მსჯელობა, რომელიც 2017 წლის 24 ოქტომბერს. საქართველოს უნივერსიტეტში გაკეთებული მოხსენების დროს იქნა გაჟღერებული. სადაც იგი კომენტარს უკეთებს გერმანიის სისხლის სამართლის კოდექსის მუხლებს ციფრულ დანაშაულთან დაკავშირებით, და აღნიშნავს, რომ გერმანიის სისხლის სამართლის კოდექსის 303-ე მუხლის შემადგენლობაში მოიაზრებს რა ქონების ელექტრონულ დაზიანებას, თავის შემადგენლობაში აერთიანებს სხვადასხვა ფორმებსა თუ გზებს კომპიუტერულ სისტემაზე თავდასხმისა და ინფორმაციის მოპოვების მიმართულებით, მაგალითად - 303-ე მუხლის „ა“ პუნქტით, ისევეა პირი, რომელიც მართლსაწინააღმდეგო წაშლის ან დამალავს მონაცემებს ან შეუძლებელს გახდის მათ გამოყენებას, ამავე მუხლის „ბ“ პუნქტით კი ისევეა პირი, რომელიც ხელს უშლის სხვისთვის მნიშვნელოვანი მონაცემის დამუშავების პროცესს, იმით, რომ იგი მონაცემებში შედის იმ მომენტით, რომ ზიანი გამოიწვიოს ან მათ გადამისამართებას ახდენს ან მონაცემების დამუშავების სისტემას ან მონაცემთა მატარებელს აზიანებს, ანადგურებს, მის გამოყენებას შეუძლებელს ხდის, შლის ან ცვლის. თუკი მონაცემთა დამუშავება უცხო საწარმოსთვის, უცხო კომპანიისათვის ან სახელმწიფო

ორგანოსათვის არსებითი მნიშვნელობის მქონეა, აქვე აუცილებლად ყურადღება უნდა გამახვილდეს.

ასევე გერმანიის სსკ-ის 202b (მონაცემების ხელში ჩაგდება) მიხედვით, ისევეა პირი, რომელიც უფლებამოსილების გარეშე თავისთვის ან სხვა პირისთვის ტექნიკური საშუალებების გამოყენებით მონაცემთა არასაჯარო გაცვლის პროცესში ჩარევით ან მონაცემთა დამუშავების სისტემის ელექტრომაგნიტური გამოსხივების საფუძველზე მოიპოვებს მონაცემებს, რომელიც მისთვის არაა განკუთვნილი - აღნიშნულ მუხლს პაულ მარტინ ვასმერი განმარტავს, რომ; ამ შემთხვევაში მოიაზრება მონაცემთა გადაცემის ნებისმიერი ფორმა (მაგალითად, უკაბელო ინტერნეტის, ელექტრონული შეტყობინების, ტელეფონის, ხმოვანი შეტყობინების, ფაქსის მეშვეობით). დანაშაულის შემადგენლობა მოითხოვს „არასაჯაროების“ ელემენტის არსებობას, რისთვისაც გადაწყვეტია არა მონაცემების სახეობა და შინაარსი, არამედ მონაცემების გადაცემის პროცესი. მონაცემთა მოპოვებისათვის არ აქვს მნიშვნელობა მონაცემთა კოდირების ფაქტის არსებობას. ამ შემთხვევაში არ მოიაზრება მაგალითად, ე. წ. Phishing, რომლის დროსაც, მსხვერპლი წდომის მონაცემებს თავისი სურვილით უგზავნის დამნაშავეს.

„დღეის მდგომარეობით გერმანიაში ინფორმაციული უსაფრთხოების პოლიტიკის განვითარების, იმპლემენტაციის და კრიტიკული ინფრასტრუქტურის დაცვის საქმეში განსაკუთრებული პასუხისმგებლობა ეკისრება შინაგან საქმეთა სამინისტროს. 2011 წელს მზარდი კიბერ-საფრთხეების საპასუხოდ სამინისტროს გადაწყვეტილებით შეიქმნა ეროვნული კიბერ-თავდაცვის ცენტრი («Nationale Cyber-Abwehrzentrum») (NCAZ). ცენტრი კოორდინაციას უწევს ინფორმაციული უსაფრთხოების სფეროში სამთავრობო უწყებების, მათ შორის, თავდაცვის სამინისტროს, ფედერალური პოლიციის და საგარეო დაზვერვის სააგენტოს საქმიანობას. ცენტრის მისიას წარმოადგენს კიბერ-უსაფრთხოების ინციდენტების სწრაფი და დეტალური შეფასება და კოორდინირებული რეაგირებისთვის რეკომენდაციების შემუშავება. შინაგან საქმეთა სამინისტრო ზედამხედველობს სხვა უწყებებსაც (კერძოდ, სამოქალაქო თავდაცვის ფედერალურ ოფისს, ინფორმაციის უსაფრთხოების ფედერალურ ოფისს, კრიმინალური პოლიციის ფედერალურ სამსახურს), რომლებიც ასევე მუშაობენ კიბერ-საფრთხეების შეფასების, ანალიზის და თავდაცვითი კონცეფციების განვითარების საკითხებზე.“¹⁰⁹

¹⁰⁹

იხ. ერეკლე წიკლაური, კანონპროექტისთვის: „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შედინის თაობაზე“ (07-3/255, 19.09.13) ელ. გვერდი ნანახია 06.06.2019



„გერმანიაში ფუნქციონირებს ცალკე სამთავრობო სააგენტო - ინფორმაციული უსაფრთხოების ფედერალური ოფისი, რომლის ძირითადი მოვალეობაა გერმანიის მთავრობისთვის კომპიუტერული და კომუნიკაციური უსაფრთხოების უზრუნველყოფა. ოფისი განთავსებულია ბონში და ჰყავს 400-ზე მეტი თანამშრომელი. ოფისის ძირითად ფუნქციებს შეადგენს: ინფორმაციული უსაფრთხოების მართვა, ინტერნეტის უსაფრთხოება, ქსელური უსაფრთხოება, ფედერალური ინფორმაციის ტექნოლოგიებისადმი არსებული საფრთხეების პრევენცია, ფედერალური კომუნიკაციური სისტემების დაცვა და ა.შ. გერმანიაში მოქმედებს კომპიუტერულ ინციდენტებზე დახმარების 20 ჯგუფი. აქედან ერთი ჯგუფი (Computer Emergency Response Team BundeswehrCERTBw) იმყოფება უშუალოდ თავდაცვის უწყების დაქვემდებარების ქვეშ და პასუხისმგებელია თავდაცვის სფეროში წარმოშობილი კომპიუტერული ინციდენტების მართვაზე.“¹¹⁰

ლატვია — ლატვიაში კიბერუსაფრთხოების პოლიტიკის განსაზღვრასა და პრაქტიკულ განხორციელებაზე პასუხისმგებლობა ეკისრება ლატვიის რესპუბლიკის ინფორმაციული უსაფრთხოების ინციდენტებზე რეაგირების ინსტიტუტს ე.წ. CERT.LV (ინფორმაციულადებულია მათივე ელ. გვერდიდან - <https://cert.lv/en/about-us>), როგორც მათ ელექტრონულ გვერდზე არის მითითებული აღნიშნული ინსტიტუტი ექვემდებარება ლატვიის თავდაცვის სამინისტროს, ხოლო მისი საქმიანობა რეგულირდება ინფორმაციული ტექნოლოგიების უსაფრთხოების შესახებ კანონით. ინსტიტუტს გააჩნია 24/7 - ზე ცხელი ხაზი, რომლის მიზანია ინციდენტების მოგვარება და სხვადასხვა სახის დახმარების გაწევა, ასევე IT უსაფრთხოებასთან დაკავშირებული ღონისძიებები და ინფორმირებულობა საქმიანობის ამბობს. აღსანიშნავია, რომ თავის მხრივ აღნიშნული ინსტიტუტი არის FIRST -ს სრული წევრი.

FIRST — არის გლობალურ სივრცეში აღიარებული უმაღლესი ორგანიზაცია ინციდენტებზე რეაგირებისთვის და მისი წევრობა საშუალებას აძლევს ინციდენტების რეაგირების გუნდებს უფრო ეფექტურად რეაგირდნენ უსაფრთხოების ინციდენტებზე, როგორც რეაქტიული, ასევე პროაქტიული მიმართულებებით, FIRST აერთიანებს სხვადასხვა სახის კომპიუტერული უსაფრთხოების ინციდენტებზე რეაგირების გუნდებს სამთავრობო, კომერციული და საგანმანათლებლო ორგანიზაციებისგან. FIRST მიზნად ისახავს ინციდენტების პრევენციის სფეროში თანამშრომლობისა და კოორდინაციის გაღრმავებას, ინციდენტებზე სწრაფი რეაგირების სტიმულირებას და წევრებისა და საზოგადოების ფართო საზოგადოებაში ინფორმაციის გაზიარებას. ნდობის ქსელის გარდა, რომელიც FIRST ქმნის გლობალურ ინციდენტებზე რეაგირების საზოგადოებაში, აღნიშნული ორგანიზაციის ელექტრონული გვერდი არის (<https://www.first.org/>).

დიდი ბრიტანეთი — დიდ ბრიტანეთში კანონი „კომპიუტერული ტექნოლოგიის არასანქცირებული გამოყენების შესახებ“, ფუნქციონირებს 1990 წლიდან, დიდი ბრიტანეთის რეგულაციები მსგავსებაშია გერმანიაში არსებულ რეგულაციებთან ციფრული დანაშაულის კუთხით, ვინაიდან ისევე როგორც გერმანიაში, დიდ ბრიტანეთშიც დასჯად ქმედებად ითვლება კომპიუტერში, მასში დაცულ ინფორმაციაში ან/და პროგრამაში უკანონო შეღწევა, ინფორმაციის ბლოკირება, მოდიფიცირება, განადგურება ან კოპირება რომლის შემაღდგენლობის მთავარი ნაწილი არის წინასწარ განზრახვა.

„დღევანდელი მდგომარეობით დიდ ბრიტანეთში ინფორმაციული უსაფრთხოების პოლიტიკის მიმართულებებს განსაზღვრავს „კიბერუსაფრთხოების და ინფორმაციული უზრუნველყოფის“ სამსახური, რომელიც თანამშრომლობს სხვადასხვა უწყებებთან, მათ შორის, თავდაცვის სამინისტროსთან, ბრიტანეთის თავდაცვის სამინისტროს წამყვანი ადგილი უკავია იმ სტრატეგიების

შემუშავების პროცესში, რომლებიც კიბერუსაფრთხოების რისკების მართვის ეფექტურობის ამაღლებას ისახავს მიზნად. სამინისტროს სადაზვერვო სააგენტოები მნიშვნელოვან როლს ასრულებენ ინფორმაციული უსაფრთხოების სფეროში არსებული გამოწვევების შემცირების პროცესში. ამ კუთხით განსაკუთრებით აღსანიშნავია „სამთავრობო კომუნიკაციების შტაბის“ საქმიანობა, რომელიც პასუხისმგებელია მთავრობის ინფორმაციული სისტემების, კომუნიკაციებისა და კრიტიკული ინფრასტრუქტურის უსაფრთხოების დაცვაზე. დიდ ბრიტანეთში 2012 წლის აპრილიდან თავდაცვის სამინისტროს დაქვემდებარებაშია „კიბერ-ოპერაციებისგან თავდაცვის ჯგუფი“ (Defence Cyber Operations Group). რომელსაც პასუხისმგებლობა ეკისრება თავდაცვის სექტორში კიბერ-შესაძლებლობების განვითარებაზე, ოპერაციების ეფექტურობის ამაღლებასა და კიბერსივრცეში უსაფრთხოების დონის ზრდაზე. ¹¹¹

ისევე როგორც სხვა სახელმწიფოებმა ბრიტანეთის თავდაცვის სამინისტრომაც „დააფუძნა გლობალური ოპერაციების და უსაფრთხოების კონტროლის ცენტრი“. ცენტრის საქმიანობა ორიენტირებულია შეიარაღებული ძალებისთვის ინფორმაციული თავდაცვის უზრუნველყოფაზე; მის დაქვემდებარებაში მყოფი სტრუქტურული ერთეული (Joint Cyber Unit) შეიმუშავებს ტექნიკურ საშუალებებს და იღებს პროაქტიულ ზომებს იმ საფრთხეების აღმოსაფხვრელად, რომელიც ემუქრება თავდაცვის სექტორის კიბერსივრცეს. ბრიტანეთში მოქმედი კომპიუტერულ ინციდენტზე დახმარების 17 ჯგუფიდან - 1 უშუალოდ ექვემდებარება თავდაცვის უწყებას (MODCERT – Ministry of Defence Computer Emergency Response Team). აღნიშნული ჯგუფი, თავის მხრივ, აერთიანებს შემდეგ სტრუქტურულ ქვედანაყოფებს: უსაფრთხოების კოორდინაციის ცენტრს, მონიტორინგისა და ანგარიშგების ცენტრებს, რჩევის და გაფრთხილების ერთეულებს და უსაფრთხოების ინციდენტზე პასუხის მცირე ჯგუფებს. ¹¹²

„შვეიცარია - შვეიცარიის ფედერალურმა ადმინისტრაციამ ბოლო წლებში აქტიური ზომები გაატარა კიბერშეიშვების საწინააღმდეგო საშუალებების და ინფორმაციული ინფრასტრუქტურის დაცვის გაძლიერების მიზნით. სხვადასხვა ორგანოები ფედერალურ დონეზე ჩართული არიან კიბერ-უსაფრთხოებასთან დაკავშირებული პრევენციული და რეაქტიული ამოცანების გადაწყვეტაში.“ ¹¹³

თავდაცვის სფეროში ინფორმაციული უსაფრთხოების პოლიტიკის განსაზღვრასა და იმპლემენტაციაში მონაწილეობს შვეიცარიის თავდაცვის სამინისტროს დაქვემდებარებაში მყოფი 3 ორგანო:

1. „ინფორმაციული უსაფრთხოების და ობიექტთა დაცვის ინსტიტუტი“ (Information Security and Facility Protection Institute (ISFP). იმისათვის, რომ უზრუნველყოს ინფორმაციის და ინფორმაციული სისტემების კონფიდენციალურობის, ხელმისაწვდომობის, ერთიანობის და განგრძობადობის დაცულობა, აღნიშნული ინსტიტუტი შეიმუშავებს ინფორმაციული უსაფრთხოების რეგულაციებს. ზოგადად, ინსტიტუტი წარმოადგენს კიბერ-უსაფრთხოებასთან დაკავშირებული საკითხების გადაწყვეტის მთავარ ეროვნულ ორგანოს და წამყვან როლს ასრულებს შვეიცარიის ფედერაციული ადმინისტრაციის ინფორმაციული უსაფრთხოების შესახებ კანონმდებლობის დახვეწაში. ¹¹⁴
2. „შეიარაღებული ძალების სარდლობის მხარდაჭერის ორგანიზაცია Armed Forces Command Support

¹¹¹ იხ. ერეკლე წიკლაური, კანონპროექტისთვის: „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ (07-3/255, 19.09.13) ელ. გვერდი ნანახია 06.06.2019



¹¹² იქვე.

¹¹³ იქვე.

¹¹⁴ იქვე.

Organisation (CSO). ორგანიზაციასთან ფუნქციონირებს კომპიუტერული ქსელური ოპერაციების მართვაზე პასუხისმგებელი ორგანო - ელექტრონული ოპერაციების ცენტრი; ცენტრი აანალიზებს საფრთხეებსა და ინციდენტებს, რის შემდეგაც ახდენს შესაბამის რეაგირებას. აღნიშნული ორგანიზაცია (CSO) ასევე მართავს სამხედრო სფეროში კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს (Military Computer Emergency Response Team (milCERT)), რომელიც მონიტორინგს უწევს შეიარაღებული ძალების ინფორმაციული ტექნოლოგიების ინფრასტრუქტურის დაცულობას."

115

3. „სამხედრო სადაზვერვო სამსახური (Military Intelligence Service (MIS) - პასუხისმგებელია სამხედრო ინფორმაციის მოპოვებაზე, თანამშრომლობს გაერთიანებულ შტაბთან და ქმნის ოპერაციებისთვის საჭირო სადაზვერვო ბაზას. ორგანიზაცია უზრუნველყოფს ფედერალურ სადაზვერვო სამსახურს კიბერ-რისკებთან დაკავშირებული ინფორმაციისა და სამხედრო კვლევების მიწოდებით.“¹¹⁶

იტალია - იტალიელი მეცნიერის ჯგუშე კორასანიტის აზრით, „ევროპის საბჭოს კონვენცია აბსტრაქტულ კანონმდებლობას არ წარმოადგენს, ის კიდევ უფრო ეფექტური გახდება მას შემდეგ, როცა წაიშლება საზღვარი და ყველა ქვეყანა მოახდენს მის რატიფიცირებას.“

უნდა აღინიშნოს, რომ იტალიური კანონმდებლობა ჯერ კიდევ 1993 წლიდან ითვალისწინებდა სახელს კომპიუტერულ სისტემაში უნებართვო შეღწევისთვის, კომპიუტერული თაღლითობისთვის, კომპიუტერული მონაცემის გადაცემის ხელყოფისთვის და ა.შ. იტალია კონვენციას სრულად კი მართალია შეუერთდა, ანუ საკუთარ კანონმდებლობაში გადაიტანა ყველა ის პრინციპი და ტერმინი, რომელიც კონვენციამ განსაზღვრა,¹¹⁷ მაგრამ - იტალიაში კიბერდანაშაულის შესახებ კონვენცია ძალაში შევიდა 2008 წლის 1 ოქტომბრიდან.

იტალიური სისხლის სამართლის კოდექსში გვაქვს რეგულაცია, რომლითაც იტალიური სისხლის სამართლის კოდექსი ჰგავს გერმანულ სისხლის სამართალს ციფრული დანაშაულის სფეროში, კერძოდ, იტალიის სისხლის სამართლის კოდექსით სანქცირებულია კომპიუტერული თაღლითობა, კერძოდ: აღნიშნული გულისხმობს ელექტრონული ხელმოწერის უკანონო გამოყენებას, რომლის საშუალებითაც დამნაშავე საკუთარი ან სხვა პირისათვის იღებს შემოსავალს არალეგალური გზებით, აღნიშნული მუხლი მსგავსებაშია გერმანიის სს-ის 263ა მუხლთან, რომლის მიხედვითაც 5 წლამდე თავისუფლების აღკვეთით ან ფულადი ჯარიმით ისჯება პირი, რომელიც საკუთარი თავისათვის ან მესამე პირისათვის მართლსაწინააღმდეგო გზით ქონებრივი სარგებლის მიღების განზრახვით, სხვა პირის ქონებას იმით აზიანებს, რომ მონაცემთა დამუშავებით მიღებულ შედეგს მოიპოვებს რამდენიმე გზით; პროგრამის არასწორად აწყოების საფუძველზე, არასწორი ან არასრულყოფილი მონაცემების გამოყენების საფუძველზე, მონაცემების არაავტორიზებული გამოყენებით ან არასანქცირებული ზეგავლენით პროგრამის მოქმედების პროცესში.

იტალიის სისხლის სამართლის კოდექსის 640-IV მუხლით (თაღლითობის) გათვალისწინებული ქმედების სუბიექტი შეიძლება იყოს მხოლოდ ელექტრონული ხელმოწერის გამოყენებაზე უფლებამოსილი პირი. ეს განსაკუთრებული სიახლეა, რადგან მსოფლიოში ელექტრონული ხელ-

115

ერეკლე წიკლაური, კანონპროექტისთვის: „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ (07-3/255, 19.09.13) ელ. გვერდი



ნანახია 06.06.2019

116

იქვე.

117

უზა ზაქაშვილი, ნაშრომი „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში“. 2013 წ. გვ. 122-123. ელ. გვერდი



ნანახია 06.06.2019 წელი.

მოწერის გამოყენება აქტიურად ხდება. შესაბამისად, გაზრდილია მისი გაყალბების საფრთხეც და სწორედ ამიტომ იტალიელმა კანონმდებელმა გადაწყვიტა ქმედების კრიმინალიზაცია. უნდა აღინიშნოს, რომ მსგავსი დანაშაულის გავრცელების საფრთხე საქართველოს ჯერ არ ემუქრება, რადგან ელექტრონული ხელმოწერა, როგორც ოფიციალური იურიდიული მოქმედება, ჯერაც არაა ფართოდ გავრცელებული. იტალიის სისხლის სამართლის კოდექსის 635-ბის მუხლით დასაჯადია კომპიუტერის ან კომპიუტერული სისტემის მუშაობის შეფერხება. სისხლისსამართლებრივი პასუხისმგებლობა განსაზღვრულია იმ პირისთვის, რომელმაც დაამზადა ან გაავრცელა ისეთი მოწყობილობა ან კომპიუტერული პროგრამა რომელიც უზრუნველყოფს კომპიუტერულ სისტემაში უნებართვო შეღწევას. იტალიელი კანონმდებლის მიერ კომპიუტერის, კომპიუტერული სისტემის და კომპიუტერული მონაცემის დანაშაულისთვის დამამძიმებელ გარემოებად გათვალისწინებულია დამინება და შანთავი, ან თუ ქმედება კომპიუტერული ქსელის ოპერატორის მიერ ანგარებითაა ჩადენილი.”¹¹⁸

„ჩეხეთის რესპუბლიკა — აღნიშნულ სახელმწიფოში ინფორმაციული უსაფრთხოების უზრუნველყოფის პოლიტიკაში ჩართული არიან შემდეგი სახელმწიფო ორგანოები: კიბერ-უსაფრთხოების დეპარტამენტი (ექვემდებარება შინაგან საქმეთა სამინისტროს); ეროვნული უშიშროების საბჭო, ვაჭრობისა და ინდუსტრიის სამინისტრო, ჩეხეთის ინფორმაციული უსაფრთხოების სამსახური და სხვ. კრიტიკული ინფრასტრუქტურის და ინფორმაციული სისტემების დაცვის კუთხით, ჩეხეთში მთავარ უწყებას წარმოადგენს შინაგან საქმეთა სამინისტრო, რომელიც ამავე დროს პასუხისმგებელია ინფორმაციული უსაფრთხოების პოლიტიკის კოორდინაციაზე. 2010 წელს ჩეხეთის მთავრობის გადაწყვეტილებით შინაგან საქმეთა სამინისტროსთან შეიქმნა უწყებათაშორისო ორგანო „კიბერუსაფრთხოების საკოორდინაციო საბჭო“. საბჭოს თავმჯდომარეობს შინაგან საქმეთა მინისტრი, წევრებს შეადგენენ ჩეხეთის პოლიციის, თავდაცვის სამინისტროს, ტელეკომუნიკაციების ოფისის, ეროვნული უსაფრთხოების ორგანოს, ინფორმაციული სამსახურის, სამხედრო დაზვერვის და სხვა უწყებების წარმომადგენლები. საბჭოს მიზანია კიბერუსაფრთხოების სფეროში შინაგან საქმეთა სამინისტროს კომპეტენციის გაძვირება და მისი, როგორც მაკოორდინირებელი ორგანოს, როლის მხარდაჭერა.”¹¹⁹

„შვედეთში ფუნქციონირებს „ეროვნული თავდაცვის რადიო-დაწესებულება“ (National Defence Radio Establishment), რომლის საქმიანობას ორგანიზებას უწევს შვედეთის თავდაცვის სამინისტრო. აღნიშნული დაწესებულება სამთავრობო ორგანოებს აწვდის როგორც მიმდინარე კიბერ-საფრთხეების შესახებ ინფორმაციას, ასევე ზოგად რჩევებს უსაფრთხოების გარემოს გაუმჯობესების მიმართულებით. შვედეთში აგრეთვე მოქმედებს თავდაცვის სამინისტროსადმი ანგარიშვალდებული ორგანო „თავდაცვის საკითხების კვლევის სააგენტო“, რომლის ერთ-ერთი ფუნქციაა კიბერ-საფრთხეების შესახებ კვლევების წარმოება და შედეგების თაობაზე შვედეთის თავდაცვის სამინისტროს ინფორმირება.”¹²⁰

„საფრანგეთი - საფრანგეთში თითოეული სამინისტრო მისი კომპეტენციის სფეროში ახდენს

¹¹⁸ უნაზაქაშვილი, ნამროში. „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში“. 2013 წ. გვ. 122-123. ელ. გვერდი 119. ნანახია 06.06.2019 წელი.



¹¹⁹ იხ. ერეკლე წიკლაური. კანონპროექტისთვის: „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ (07-3/255, 19.09.13) ელ. გვერდი 120. ნანახია 06.06.2019



¹²⁰ იქვე.

ინფორმაციულ უსაფრთხოებასთან დაკავშირებული რისკების ანალიზს. 2009 წელს საფრანგეთის მთავრობის გადაწყვეტილებით შეიქმნა „ქსელური და ინფორმაციული უსაფრთხოების სააგენტო“ (The French Network and Information Security Agency), რომელიც ინფორმაციული სისტემების დაცვის უზრუნველყოფაზე პასუხისმგებელ მთავარ ეროვნულ ორგანოს წარმოადგენს. სააგენტოს ფუნქციებია: კიბერ-შეტევების დაფიქსირება და სწრაფი რეაგირება, სამთავრობო ქსელებზე მუდმივი მეთვალყურეობა, საფრთხეების პრევენცია, მთავრობის ორგანოებისთვის და კრიტიკული ინფრასტრუქტურის ოპერატორებისთვის მხარდაჭერის აღმოჩენა და რჩევების მიცემა, კომპანიების და საზოგადოების ინფორმირება ინფორმაციული უსაფრთხოების გამოწვევების შესახებ. აღნიშნული სააგენტოს დაქვემდებარებაშია ინფორმაციული სისტემების უსაფრთხოების ოპერატიული ცენტრი (Operational Centre for Information Systems Security – COSSI), რომელიც ახდენს სამთავრობო უწყებების წინაშე მდგარი კიბერ-საფრთხეების პრევენციას, გამოვლენას და აღმოფხვრას, ასევე კრიზისული სიტუაციების მართვის კოორდინირებას.¹²¹

„საფრანგეთში აგრეთვე ფუნქციონირებს ინფორმაციულ ტექნოლოგიებთან და კომუნიკაციებთან დაკავშირებული დანაშაულის წინააღმდეგ ბრძოლის ცენტრალური ოფისი. მისი ფუნქციაა ლოკალურ და რეგიონულ დონეზე პოლიციის დახმარება, რაც გამოიხატება კიბერ-სივრცეში არსებული გამოძიებების წარმოებაში, ინფორმაციული უსაფრთხოების შესახებ საკითხების ანალიზში, მონაცემთა შეგროვებაში და კიბერ-დანაშაულთან დაკავშირებული სხვა საჭიროებების უზრუნველყოფაში.“¹²²

„ესტონეთი — თერთმეტი წლის წინ, ესტონეთი გახდა პირველი ქვეყანა მსოფლიოში, სადაც თანამედროვე ტიპის კიბერ-შეტევები ვიხილეთ. კიბერ-თავდასხმა რუსეთიდან განხორციელდა. ამ შემთხვევაში ესტონეთი სამუდამოდ შეცვალა. ესტონეთმა თავდასხმის შემდეგ ციფრული რევოლუცია განიცადა. დღეისათვის, ყოფილი საბჭოთა რესპუბლიკა მსოფლიოში ტექნოლოგიურად ერთ-ერთი ყველაზე განვითარებულია. ესტონეთის ციფრული გარდაქმნების ერთ-ერთი ცენტრალური რეფორმა „X-Road-ის“ პლატფორმაა, რომელიც სხვადასხვა მომსახურებას აერთიანებს, და მთავრობას მოქალაქეებთან აკავშირებს. პლატფორმას იყენებენ წამყვანი კერძო კომპანიებიც. პლატფორმის გამოყენებით მოქალაქეებს შეუძლიათ ისეთი მომსახურების მიღება როგორცაა ჯანდაცვა, საბანკო ოპერაციები, გადასახადების გადახდა, სამართალდაცვა, და განათლება. ბოჭკოვანი ქსელი მთელს ქვეყანას აკავშირებს. კანონდებლებს შეუძლიათ ელექტრო-კაბინეტის პროგრამის გამოყენებით, ციფრულად მიიღონ კანონები. ხოლო მოქალაქეებს აქვთ საშუალება ონლაინ ხმის მიცემის მეშვეობით აირჩიონ პოლიტიკოსები და იყენონ მათთან კავშირზე.“¹²³

„ციფრული ტექნოლოგიების გამოყენების ერთ-ერთი სარგებელი თანხების დაზოგვაა. ჩვენ ყოველ წელს მთლიანი შიდა პროდუქტის 2 პროცენტს ვზოგავთ ხარჯების ნაწილში, მათ შორის ხელფასებზე. ჩვენ ბიუროკრატია შევზღუდეთ. ბიუროკრატია თითქმის აღარ არსებობს. ეს დეცენტრალიზებული ინფორმაციული სისტემაა, რომელიც 1200 დაცულ და უსაფრთხო სისტემას აკავშირებს ერთმანეთთან“ - ამბობს მარტენ კაევალსი, პრემიერ-მინისტრის მრჩეველი ციფრულ საკითხებში. ლინარ ვიკი ელექტრონული მთავრობის სააგენტოს დამფუძნებელია, ის 2007

¹²¹ იხ. ერეკლე წიკლაური, კანონპროექტისთვის: „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ (07-3/255, 19.09.13) ელ. გვერდი 5; ნანახია 06.06.2019



¹²² იქვე.

¹²³ სტატია ესტონეთის ციფრული რევოლუცია ელ გვერდი 5; ნანახია 06.06.2019.



წელ ესტონეთზე კიბერ თავდასხმის დროს მთავრობის ციფრული მრჩეველი იყო. მისი თქმით, თავდასხმა დიდხანს არ გაგრძელებულა და მისი სამიზნე ძირითადად უცხოურ პარტნიორებთან კრიტიკული კომუნიკაცია იყო.“¹²⁴

3.2 ციფრულ დანაშაულთან ბრძოლის სამართლებრივი რეგულაციები ამერიკის შეერთებული შტატებში

ამერიკის შეერთებული შტატები არის ერთ-ერთი მოწინავე ციფრული დანაშაულის გამომძიების და აღნიშნული დანაშაულის ბრძოლის წინააღმდეგ განხორციელებულ რეგულაციებში, ასევე აშშ არის ერთ-ერთი მოწინავე, რომელმაც კომპიუტერის შექმნის საწყისი წლებიდანვე დაიწყო ბრძოლა რათა აღნიშნული გამოყენებული არ ყოფილიყო დანაშაულის ჩასადენად, კერძო; „კომპიუტერული დანაშაული ყურადღების ცენტრში პირველად აშშ-ში XX საუკუნის 70იან წლებში მოექცა. ნაციონალურ და საერთაშორისო დონეზე დაიწყო ამ ფენომენის გამოკვლევა. მაღეხულ იქნა სპეციალური ნორმები კიბერდანაშაულის მოსაწესრიგებლად. აშშში ჯერ კიდევ 1977 წელს შეიმუშავეს კანონპროექტი “ფედერალური კომპიუტერული სისტემების დაცვის შესახებ”, რომელიც ითვალისწინებდა სისხლისსამართლებრივ პასუხისმგებლობას ისეთი ქმედებისთვის, როგორიცაა: კომპიუტერულ სისტემაში ცრუ მონაცემების შეყვანა, კომპიუტერული მოწყობილობის უკანონო გამოყენება, ფულადი სახსრების მითვისება კომპიუტერული ტექნოლოგიების და კომპიუტერული ინფორმაციის მეშვეობით და სხვ. ამ კანონპროექტის საფუძველზე 1984 წლის ოქტომბერში მიღებულ იქნა „კომპიუტერული თაღლითობის და კომპიუტერის ბოროტად გამოყენების შესახებ“ კანონი. კომპიუტერული დანაშაულის წინააღმდეგ აქტიური ბრძოლის დასაწყებად კი ამერიკის შეერთებული შტატებში ექსპერტები გამოყოფენ სამ შემთხვევას, რომლებმაც ცხადი გახადა, რომ ახალი კომპიუტერული და სატელეკომუნიკაციო ტექნოლოგიები დიდ პრობლემებს შეუქმნიდა სამართალდამცავ ორგანოებს. საყოველთაო „კომპიუტინგი“¹²⁵ მართო ცხოვრების წესის შეცვლას კი არ ნიშნავდა, არამედ შეიცვლებოდა კრიმინალების მიერ დანაშაულებრივი საქმიანობის წარმართვის სპეციფიკაც.“¹²⁶

„მაგალითისთვის მოვიყვანოთ ზემოაღნიშნული სამი შემთხვევა:

1. 1986 წელს კალიფორნიის უნივერსიტეტის ასტრონომს დაევალა არასასიამოვნო, მაგრამ აშკარად მცირე მნიშვნელობის პრობლემის გადაჭრა უნივერსიტეტის კომპიუტერულ ლაბორატორიაში. უნივერსიტეტი ამუშავებდა ორ საბუღალტრო პროგრამას, რომლიც აღრიცხავდა კომპიუტერების გამოყენებას და არეგისტრირებდა მათ მომხმარებლებს. ვინაიდან, ამ პროგრამით ხდებოდა თანხებთან დაკავშირებით ერთი და იმავე ინფორმაციის დაფიქსირება, მათი შედეგიც ერთნაირი უნდა ყოფილიყო. თუმცა, გაურკვეველი მიზეზით სხვაობამ 75 აშშ დოლარი შეადგინა. გამომძიების ფედერალურმა ორგანოებმა უარი განაცხადეს საქმის გამომძიებაზე იმ მოტივით, რომ 75 დოლარიანი დანაკარგი უმნიშვნელო იყო, მაგრამ ასტრონომმა კლიფორდ სტოლმა თავად დაიწყო გამომძიება. ის იწერდა ჰაკერის მოქმედებებს და მუშაობდა როგორც ადგილობრივ ასევე უცხოურ სატელეფონო კომპანიებთან, რათა

¹²⁴ სტატია ესტონეთის ციფრული რევოლუცია ელ გვერდი  ნანახია 06.06.2019.

¹²⁵ „კომპიუტინგი“ ტერმინი — კომპიუტერების მასშტაბური ინტეგრაცია ყოველდღიურ ცხოვრებაში.

¹²⁶ უნაზაქაშვილი. ნაშრომი „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში“. 2014 წელი. გვ. 15-16

დაედგინა თავდასხმის წყარო. აღმოჩნდა, რომ გერმანელ ჰაკერს მარკუს ჰესს აფინანსებდა რუსეთის სახელმწიფო უსაფრთხოების კომიტეტი, რათა გაემჟღავნებინა აშშს სამხედრო საიდუმლოება. ამრიგად, ეს იყო მნიშვნელოვანი გაკვეთილი როგორც სამართალდამცავი ორგანოების, ასევე დაზვერვის სამსახურისთვის. პირველ რიგში, ცხადი გახდა, რომ ქსელური ინფორმაცია არ იყო დაცული მასში უნებართვო შეღწევისგან და მეორე — ფინანსური ზარალი ყოველთვის არ განსაზღვრავს ხელყოფის სერიოზულობას და ინფორმაცია კიბერდანაშაულის შესახებ არ უნდა შემოწმდეს მხოლოდ ფინანსური ზარალის მიხედვით;

2. ეორე შემთხვევა დაკავშირებული იყო კომპიუტერულ ვირუსთან ე.წ. მორისის მატლთან. 1988 წელს ქორნელის უნივერსიტეტის სტუდენტმა რობერტ მორისმა შექმნა პროგრამა ინტერნეტის მეშვეობით კომპიუტერში შესაღწევად. მას შემდეგ რაც კომპიუტერული ვირუსი შეაღწევდა სამომხე კომპიუტერში იგი დაიკავებდა კომპიუტერის მეხსიერებას, რაც გამოიწვევდა კომპიუტერის გამორთვას. სანამ კომპიუტერული ვირუსი გაუვნებელყოფილ იქნა, მან დააზიანა დაახლოებით 6200 კომპიუტერი და გამოიწვია 98 მილიონ დოლარზე მეტი ზარალი;
3. მესამე მაგალითი ეხება 1989 წლის თავდასხმას კომპანია „ბელსასუზე“, რომელიც განხორციელდა „სიკვდილის ლეგიონის“ სახელით ცნობილი ჰაკერთა ჯგუფის მიერ. მათთვის შესაძლებელი გახდა ადგილობრივ სატელეფონო სისტემაში ცვლილებების შეტანა და მონაცემების განადგურება.“¹²⁷

„ასევე აღსანიშნავია, რომ, კიბერუსაფრთხოების პირველი სტრატეგია შემუშავებულ იქნა ამერიკის შეერთებულ შტატებში 2000 წლების დასაწყისში. შეერთებული შტატები გახდა ის ქვეყანა, რომელმაც დაიწყო კიბერუსაფრთხოების აღქმა, როგორც სახელმწიფო მნიშვნელობის საკითხი. 2003 წელს შეერთებულ შტატებში გამოქვეყნდა კიბერსივრცის უსაფრთხოების ეროვნული სტრატეგია (National Strategy to Secure Cyberspace). მოცემული დოკუმენტი წარმოადგენს უფრო ფართო ეროვნული უსაფრთხოების უზრუნველყოფის სტრატეგიის ნაწილს (National Strategy for Homeland Security), რომელიც შეიქმნა 2001 წლის 11 სექტემბრის ტერორისტული შეტევის პასუხად.“¹²⁸

„ამავე აქტის 814-ე მუხლით ცვლილება შევიდა კანონთა კრებულის მე-18 ტიტულის 1030-ე მუხლში, რომელიც ეხება ცალკეულ კომპიუტერულ დანაშაულს. ამ ცვლილების შედეგად კომპიუტერული დანაშაულისთვის დადგენილი სასჯელის მაქსიმალური ზღვარი გაიზარდა და პირველად ჩადენილი დანაშაულისთვის გახდა თავისუფლების აღკვეთა 10, განმეორებითისთვის კი 20 წლამდე.“ „[...] ცვლილების შემდეგ ამერიკაში ქმედების დანაშაულად კვალიფიკაციისთვის აუცილებელი გახდა დამნაშავის მიზნის დადგენა, მასში განისაზღვრა ზიანის ცნება და იგი ჩამოყალიბდა, როგორც «მონაცემთა, სისტემის, პროგრამის ან ინფორმაციის მთლიანობის ნებისმიერი დაზიანება». ამერიკელი კანონმდებელი დასჯადად აცხადებს კომპიუტერულ სისტემაში არასანქცირებულ შეღწევას, მასში უნდა ვიგულისხმოდ, სანქცირებული შესვლის ფარგლების გადამეტებას. კანონმდებელმა განსაზღვრა კომპიუტერული ჯაშუშობის ცნება, რომელიც გულისხმობს პირის მიერ კომპიუტერულ სისტემაში არასანქცირებული შეღწევას ან სანქცირებულ შესვლის ფარგლების გადამეტებას, ასევე ისეთი ინფორმაციის მოპოვებას, რომელსაც კავშირი აქვს სახელმწიფო უსაფრთხოების, საერთაშორისო ურთიერთობის და ატომური ენერგიის საკითხთან.“ „[...] გარდა ზემოაღნიშნულისა, დასჯადია კომპიუტერული თაღლითობა, ესე იგი თაღლითური განზრახვით

¹²⁷ სამივე შემთხვევა — უჩა ზაქაშვილი. ნაშრომი „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში“. 2014 წელი. გვ. 15-16

¹²⁸ ვლადიმერ ცერცვაძე, „კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები“ გვ. 42/131 ელ. გვერდი https://gipa.ge/uploads/files/Cyber_Protection.pdf ნანახია 06.06.2019

ვიგულისხმობთ ნებისმიერი კომპიუტერული პროგრამაც, რუსული კანონმდებლის ვიწრო მიდგომა არასრულყოფილია, რადგან დანაშაული იწყება კომპიუტერულ სისტემაში უნებართვო შეღწევიდან და მხოლოდ ამის შემდეგ ხდება კომპიუტერული ინფორმაციის ხელყოფა. თუმცა, როგორც ჩანს, ეს გარემოება რუსეთში ყურადღების მიღმა დარჩა.“¹³⁰

„რუსი მეცნიერი პაველ დომკინი განმარტავს თუ რა უნდა ვიგულისხმობთ რუსეთის სისხლის სამართლის კოდექსის 272-ე მუხლის 1 ნაწილში მითითებულ ტერმინ «არამართლზომიერში»: არამართლზომიერი — ესე იგი კომპიუტერული ინფორმაციის ძებნის და მიღების დადგენილი წესის დარღვევით განხორციელებული ქმედება. კანონით დაცულ კომპიუტერულ ინფორმაციაში შეღწევა არამართლზომიერია, როდესაც ხდება ჩამოთვლილთაგან ერთ-ერთი წესის დარღვევა: ა) ინფორმაციის მოძებნა არაა ხელმისაწვდომი ყველასთვის; ბ) ინფორმაციაში შესვლას გააჩნია ტექნიკური შეზღუდვა, მაგალითად, პაროლი. გ) ინფორმაციის მიღების უფლებამოსილება ყველას არ გააჩნია; დ) კომპიუტერულ ინფორმაციაში შეღწევა შეუძლებელია ტექნიკური დაცვის საშუალების გადაღავის გარეშე. პ. დომკინი განმარტავს, რომ გარდა ზემოაღნიშნულისა, რუსული სასამართლო პრაქტიკა „არამართლზომიერ“ შეღწევაში გულისხმობს შემდეგს: ვთქვათ, პირი არის კომპიუტერული სისტემის ადმინისტრატორი და გააჩნია კომპიუტერული ინფორმაციის მოძებნის და მიღების უფლება, მაგრამ სამსახურის შინაგანაწესით, გარკვეულ ინფორმაციაში შესვლა აკრძალული აქვს. იმ შემთხვევაში, თუ ის მაინც განახორციელებს ამ ტიპის ინფორმაციის კოპირებას, ის არამართლზომიერად შეაღწევს კომპიუტერულ ინფორმაციაში. ასევე, „არამართლზომიერ“ შეღწევასთან გვექნება საქმე, როდესაც კომპიუტერული ინფორმაცია დაცულია რუსეთის კანონმდებლობით, ანუ იგი არის სახელმწიფო საიდუმლოება და კონფიდენციალური ინფორმაცია. სახელმწიფო საიდუმლო განსაზღვრულია კანონით „სახელმწიფო საიდუმლოების შესახებ“ და მასში შედის სამხედრო, ეკონომიკური, სამეცნიერო, შიდა პოლიტიკასთან დაკავშირებული, კონტრდაზვერვის, ოპერატიულ-სამძებრო და სხვა ინფორმაცია. კონფიდენციალური მონაცემებია: პერსონალური, საგამოძიებო და სამართალწარმოების მონაცემი, ასევე სამსახურებრივი საიდუმლო (განსაზღვრულია რუსეთის სამოქალაქო კოდექსით), საადვოკატო, საექიმო საიდუმლო, სატელეკომუნიკაციო კავშირის, პირადი მიმოწერის საიდუმლო, კომერციული საიდუმლო და ა.შ.“¹³¹

¹³⁰ უჩა ზაქაშვილი, ნაშრომი „კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში“. 2013 წ. გვ. 124-125. ელ. გვერდი



ნანახია 06.06.2019 წელი.

კარი II

ციფრული დანაშაულის გამოძიების ტექნიკა და მეთოდოლოგია

თავი IV

ციფრული მტკიცებულება

4.1. ციფრული მტკიცებულების რაობა და ადგილი

მტკიცებულებათა კლასიფიკაციაში

ჩინა თავებში განმარტებულ იქნა ციფრული დანაშაულის არსი და მნიშვნელობა, მისი ობიექტური და სუბიექტური შემადგენლობა და ციფრული დანაშაულის ადგილი საქართველოს სისხლის სამართლის მატერიალური კანონმდებლობაში, მაგრამ იმისათვის, რომ სისხლის სამართლის კანონმდებლობა იყოს სამართლებრივ ჰარმონიაში, აუცილებელია, რომ სისხლის სამართლის პროცესმა მოგვეცეს საშუალება — გამოვიყენოთ სისხლის სამართლის კოდექსით გათვალისწინებული დანაშაული და მიხვიდე შედეგამდე.

სწორედ აღნიშნული მიზეზებიდან გამომდინარე, წარმოდგენილი თავი შეეხება ციფრული მტკიცებულების ადგილის განსაზღვრას სისხლის სამართლის პროცესში, მაინც სად არის აღნიშნულის ადგილი — რომელიმე მტკიცებულებათა ჯგუფში, თუ დამოუკიდებელი სახით?

მოქმედი საქართველოს სისხლის სამართლის საპროცესო კოდექსის მე-3 მუხლის თანახმად, მტკიცებულება ეს არის — „კანონით დადგენილი წესით სასამართლოში წარდგენილი ინფორმაცია, ამ ინფორმაციის შემცველი საგანი, დოკუმენტი, ნივთიერება ან სხვა ობიექტი, რომლის საფუძველზედაც მხარეები სასამართლოში ადასტურებენ ან უარყოფენ ფაქტებს, სამართლებრივად აფასებენ მათ, ასრულებენ მოვალეობებს, იცავენ თავიანთ უფლებებსა და კანონიერ ინტერესებს, ხოლო სასამართლო ადგენს, არსებობს თუ არა ფაქტი ან ქმედება, რომლის გამოც ხორციელდება სისხლის სამართლის პროცესი, ჩაიდინა თუ არა ეს ქმედება გარკვეულმა პირმა, დამნაშავეა თუ არა იგი, აგრეთვე გარემოებებს, რომლებიც გავლენას ახდენს ბრალდებულის პასუხისმგებლობის ხასიათსა და ხარისხზე, ახასიათებს მის პიროვნებას. დოკუმენტი მტკიცებულებაა, თუ ის შეიცავს სისხლის სამართლის საქმის ფაქტობრივი და სამართლებრივი გარემოებების დასადგენად საჭირო ცნობას. დოკუმენტად ითვლება ნებისმიერი წყარო, რომელშიც ინფორმაცია აღბეჭდილია სიტყვიერ-ნიშნობრივი ფორმით ან/და ფოტო-, კინო-, ვიდეო-, ბეგრისა თუ სხვა ჩანაწერის სახით ან სხვა ტექნიკური საშუალების გამოყენებით.“¹³²

ზემოაღნიშნული მუხლიდან გამომდინარე გვაქვს რამდენიმე სახის მტკიცებულება, ესენია ინფორმაცია, ამ ინფორმაციის შემცველი საგანი, დოკუმენტი, ნივთიერება ან სხვა ობიექტი.

„ინფორმაცია — მისიზინარსითმრავლისმომცველიტერმინია, მაგალითისათვის ინფორმაციის შემცველი მტკიცებულებაა მოწმის მიერ სასამართლოსთვის მიცემული ჩვენება. აღსანიშნავია, რომ ნებისმიერი ინფორმაცია მტკიცებით ძალას იძენს სასამართლოში მტკიცებულებებით მისი დადასტურების შემდეგ;

ინფორმაციის შემცველი საგანი — მართალია კანონმდებელმა ნივთისგან განასხვავა საგანი რომელიც შეიცავს გარკვეულ ინფორმაციას, მაგრამ აღნიშნულის გამოიყენა ნივთისგან მაინც რთულია, მაგალითისათვის ინფორმაციის შემცველ საგნად შესაძლოა განვიხილოთ ელექტრონული დისკი,

¹³² საქართველოს სისხლის სამართლის საპროცესო კოდექსი 29.05.2019 წლის რედ.

რომელიც არის საგანი და შეიცავს ინფორმაციას მასში განთავსებული ვიდეო ჩანაწერის გამო, ასევე საგანი შესაძლოა გვაძლევდეს ნივთიერი მტკიცებულების იგივეობას;

ნივთიერი მტკიცებულება — ჩამონათვალი სანიმუშოა და მას შესაძლებელია ეწოდებოდეს ნებისმიერი საგანი/ნივთიერება/კვალი, რომელსაც მნიშვნელობა აქვს საქმისათვის. ამასთან, ნივთიერ მტკიცებულებას აღნიშნული საგნები წარმოადგენს იმ შემთხვევაში თუ მათი არსი და დანიშნულება გასაგებია ფოთლითა და ქიმიისათვის, რაც შესაძლებელია გამოყენებული იქნეს სასამართლოში საკუთარი პოზიციის დასადასტურებლად და რომელთა გადაცემა შესაძლებელია ხელიდან ხელში (რომელთა ფიზიკური დათვალიერებაა შესაძლებელი. მაგალითად, თითის ანაბეჭდი, რომელიც გადატანილია შესაბამის ლენტზე, დანაშაულის ჩასადენად გამოყენებული სამზარეულოს დანა, დაზარალებულის სისხლიანი პერანგი, აუდიო/ვიდეო ჩანაწერი და სხვა).¹³³

„ნივთიერ მტკიცებულებას წარმოადგენს ასევე სულიერი ცხოველი/არსება, რომელიც წარმოადგენდა დანაშაულის ჩადენის საგანს ან გამოყენებული იყო დანაშაულის ჩასადენად (მაგალითად, შინაური პირუტყვის ქერდობის შემთხვევაში, სხვისი ქონების (მსხვილფეხა პირუტყვის) განზრახ განადგურებისას და სხვა), თუმცა აღნიშნულის სხდომის დარბაზში წარდგენა დათვალიერებისათვის არ დაიშვება, ნივთიერ მტკიცებულებას არ წარმოადგენს მატერიალური სამყაროს ნივთები/საგნები, რომელთა აღქმა პროცესის მონაწილეების გრძნობის ორგანოების მიერ შეუძლებელია. მაგალითად, ნაწონაწილაკები/მიკრონაწილაკები, რომელთა დათვალიერება შესაძლებელია მხოლოდ მიკროსკოპის მეშვეობით და საჭიროებს სპეციალურ ცოდნას. მაგრამ ნივთიერ მტკიცებულებას წარმოადგენს შემთხვევის ადგილიდან ამოღებული შალითა, რომელზეც საექსპერტო კვლევის შედეგად აღმოჩენილი იქნება აღნიშნული ნაწონაწილაკები, თუ ეს მიუთითებს საქმისათვის მნიშვნელოვან გარემოებაზე (მაგალითად, რომ ბრალდებული იქ იყო).“¹³⁴

„დოკუმენტი — დოკუმენტს მტკიცებულებითი ძალა ენიჭება კუმულაციურად სამი სპეციალური წინაპირობის არსებობისას: 1. ცნობილია მისი წარმომავლობა; 2. ავთენტიკურია; 3. შესაძლებელია დაიკითხოთ პირი რომელმაც შექმნა/მოიპოვა ან ვისთანაც ინახებოდა დოკუმენტი სასამართლოში წარდგენამდე, იგი შესაძლებელია არსებობდეს როგორც წერილობითი, ასევე ნებისმიერი სხვა ფორმით (აუდიო-ვიდეოჩანაწერი, კომპიუტერული ფაილების, სმს-ს, მშს-ის, მესიერების ბარათების სახით და ა.შ.), ოფიციალური/საქმიანი ქაღალდის, ასევე არაოფიციალური სახით, მაგალითად, საჯარო/სამოქალაქო რეესტრიდან ამონაწერი, სანოტარო წესით დამოწმებული ნასყიდობის ხელშეკრულება, ცნობა ხელფასის შესახებ, ცნობა ნასამართლეობის შესახებ, განმრთელობის ცნობა, ამონაწერი მობილური კავშირგაბმულობის ოპერატორისგან განხორციელებული სატელეფონო კომუნიკაციის (შემავალი-გამავალი ზარების ხანგრძლივობის, რაოდენობის, ლოკაციის, სიხშირის და ა.შ.), ინტერნეტ სერვის პროვაიდერის მიერ მიწოდებული ინფორმაცია ინტერნეტაქტივობის შესახებ, ე.წ. შინაურული ხელწერილი, მესიჯი, ელექტრონული წერილი, ფოტოსურათი, და ა.შ. (დოკუმენტის განმარტება, სსსკ მე-3 მუხლის 23-ე ნაწილი). ოფიციალური დოკუმენტები პირობითად შეიძლება დაიყოს თავის მხრივ ორ სახედ: 1. პროცესის მწარმოებელი ორგანოს მიერ შექმნილი (მაგალითად, საგამომიებო მოქმედების ოქმები); 2. სხვა დაწესებულების

¹³³ სამივე ტერმინი — ავტორთა კოლექტივი, საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი. 2015 წლის 1 ოქტომბრის მდგომარეობით. ამერიკის იურისტთა ასოციაცია კანონის უზენაესობის ინიციატივის მხარდაჭერით. 2015 წელი. გვ. 38-39

¹³⁴ ავტორთა კოლექტივი, საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი. 2015 წლის 1 ოქტომბრის მდგომარეობით. ამერიკის იურისტთა ასოციაცია კანონის უზენაესობის ინიციატივის მხარდაჭერით. 2015 წელი. გვ. 38-39

ოფიციალური დოკუმენტაცია, რომელსაც გააჩნია საქმისათვის მნიშვნელოვანი ინფორმაცია პროცესში მისი არსებობა უკავშირდება პროცესის მონაწილის მიერ მის მოპოვებას გარეშე წყაროებიდან, ან პროცესის მონაწილის მიერ მის ნებაყოფლობით წარმოდგენას. მაგალითად, სსკ 177-ე მუხლით გათვალისწინებული დანაშაულით დაზარალებული პირის მიერ სალაროს აპარატის ჩეკის/სავარანგო ტალონის წარმოდგენა, რომლითაც დასტურდება მოპარული ნივთის მის საკუთრებაში არსებობა, ღირებულება, სერიული ნომერი, მარკა და ა.შ.¹³⁵

ხოლო თავად „ციფრული მტკიცებულების რაობაზე როდესაც ვსაუბრობთ, პირველ რიგში განვიხილოთ მისი ზოგადი განმარტება; ციფრული მტკიცებულებები ან ელექტრონული მტკიცებულებები არის ციფრული ფორმით შენახული ან გადაცემული ნებისმიერი სავარაუდო ინფორმაცია, რომელიც სასამართლოში საქმის განხილვისას შეიძლება იქნეს გამოყენებული. ციფრული მტკიცებულებების მიღებაზე სასამართლო განსაზღვრავს, არის თუ არა მტკიცებულება შესაბამისი, ავთენტიკური, არის თუ არა ორიგინალი.“¹³⁶

„მტკიცებულებათა ჩამონათვალის საფუძველზე იბადება კითხვა – შედის თუარა ციფრული მტკიცებულება მისი ბუნებიდან გამომდინარე რომელიმე მტკიცებულებათა სამართლებრივ შემადგენლობაში, შესაძლოა ვივარაუდოთ, რომ ზემოაღნიშნულს მოიცავს დოკუმენტი, რადგანაც დოკუმენტი თავის თავში გარკვეულწილად მოიცავს ინტერნეტ სერვის პროვაიდერის მიერ მიწოდებული ინფორმაციას ინტერნეტ აქტივობის შესახებ, მესიჯებს, ელექტრონული წერილებს, ფორუსურათებს, და ა. შ. აღნიშნულ ვარაუდს გვიმყარებს საფრანგეთის სამოქალაქო კოდექსი, რომელიც წერილობით მტკიცებულებებს აკუთვნებს ყველა სახის წერილებს, სიმბოლოებს, ციფრებს ან სხვა ნიშნებს, რომლებსაც აქვთ შინაარსი, მნიშვნელობა და მათი გაცემა შესაძლებელია, მიუხედავად იმისა თუ რა ფორმით არიან ისინი გადმოცემული. როგორც ვხედავთ, ფრანგულმა კანონმდებელმა ფართოდ განმარტა წერილობითი მტკიცებულებები და მოიცვა როგორც კონკრეტული ისე აბსტრაქტული მონაცემები.“¹³⁷

მაგრამ, მივიჩნევთ, რომ ციფრული მტკიცებულება, როგორც მტკიცებულების სახე, მკაფიოდ დეფინირებასთან ერთად აუცილებლად უნდა იქნეს შეტანილი საქართველოს სისხლის სამართლის საპროცესო კანონმდებლობაში, ვინაიდან 21-ე საუკუნე ციფრული ეპოქაა და როგორც ბიზნეს ასევე სხვა სახის კომუნიკაცია და ურთიერთობები ინტერნეტ სივრცეში და კომპიუტერულ ტექნიკაში წარმოებული დოკუმენტაციის საფუძველზე წარმოებს, უფრო მეტიც, ბრუნვაშია ელექტრონული ფული, შეიქმნა ხელოვნური ინტელექტი და ა.შ.

როდესაც განვიხილავთ ციფრულ მტკიცებულებებს, უნდა ვაღიაროთ, რომ „ელექტრონული წერილობითი დოკუმენტაციის წარმოება [...] ამცირებს რისკებს, როგორიცაა: წერილობითი მტკიცებულებების ფალსიფიკაცია, გათეთრება, თაღლითობა და ა.შ. ამ ყველაფრის აღმოფხვრას ხელს უწყობს და აიოლებს მართლმსაჯულებაში ახალი ტექნოლოგიების დანერგვა. დღეს ყველაფერი უფრო უსაფრთხოდ და სანდოდ შეგვიძლია მივიჩნიოთ ვიდრე წლების წინ...

¹³⁵ ავტორთა კოლექტივი, საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი. 2015 წლის 1 ოქტომბრის მდგომარეობით. ამერიკის იურისტთა ასოციაცია კანონის უზენაესობის ინიციატივის მხარდაჭერით. 2015 წელი. გვ. 275

¹³⁶ ელ. გვერდი  ნანახია. 21.07.2019

¹³⁷ Fabien Kerbouci სტატია ელექტრონული მტკიცებულება — ახალი გამოწვევა ფრანგულ მართლმსაჯულებაში თარგმანი: თამთა მიქაია (თბილისის სააპელაციო სასამართლოს თავმჯდომარის ბიუროს სტაჟიორი) ელ. გვერდი 

ელექტრონულად წარმოდგენილ მტკიცებულებების სუსტ მხარედ შეიძლება ჩაითვალოს, ასეთი სახით წარმოდგენილი ესა თუ ის ტექსტი, ტექსტური შეტყობინება (SMS) და ტელეფონის ზარი. ყველა ეს საშუალება ძალიან დაუცველი და არასანდოა, რაც ზრდის შეცდომის დაშვების რისკს და შესაძლებელია მოსამართლეს მასზე დაყრდნობით არასწორი წარმოდგენაც კი შეექმნას, რაც დღესდღეობით სერიოზულ პრობლემას წარმოადგენს და რასაც ხშირად მოსდევს უსამართლო გადაწყვეტილებები. თანამედროვე ტექნოლოგიები არ უნდა აძლევდეს მხარეებს მანიპულირების საშუალებას. შეჯიბრითობის პრინციპიდან გამომდინარე მხარეებს აქვთ სრული თავისუფლება თავად გადაწყვიტონ: რა სახის მტკიცებულებები წარმოადგინონ სასამართლოში და როგორც დაიცვან თავი, თუმცა აღსანიშნავია ის გარემოებაც რომ, არცერთ მტკიცებულებას არ აქვს წინასწარ დადგენილი ძალა და მხოლოდ მოსამართლეზეა დამოკიდებული, როგორ შეაფასებს მას.¹³⁸

„საფრანგეთის სამოქალაქო კოდექსის 1316-ე მუხლის 1-ელი ნაწილი მიუთითებს რომ, ელექტრონული ფორმით დასაშვებია ისეთი მტკიცებულებები, რომლის გამომგზავნი პირი, გამცემი ორგანო ცნობილია და ინახება ისეთ პირობებში, რომელიც წარმოადგენს გარანტს მისი მთლიანობის. მისი ნამდვილობისთვის, ის დამოწმებული უნდა იყოს გამომგზავნის ელექტრონული ხელმოწერით, რომელიც უნდა აკმაყოფილებდეს კანონიერი უსაფრთხოების მოთხოვნებს (1316-ე მუხლის მე-4 ნაწილი). კომპიუტერული პროგრამების გამოყენებით კრიპტოგრაფიული ალგორითმები უზრუნველყოფენ დოკუმენტების მთლიანობასა და ნამდვილობას. ელექტრონული ხელმოწერის მიმართ მოქმედებს პრეზუმცია, იგი ითვლება სარწმუნოდ იქამდე, სანამ საწინააღმდეგო არ დამტკიცდება. მტკიცებულების გამოკვლევისას მოსამართლეს უფლება აქვს უხმოს ექსპერტს. ელექტრონული სახით შეიძლება წარმოდგენილი იყოს აუდიო, ვიდეო ფაილები, ფოტოები.“¹³⁹

ამდენად, ვფიქრობთ, რომ ციფრული მტკიცებულების ადგილი სამართლებრივ კლასიფიკაციაში უნდა იყოს დამოუკიდებელი და განსაზღვრული უნდა იყოს მტკიცებულების ერთ ერთ დამოუკიდებელ სახეობად.

¹³⁸ Fabien Kerbouci სტატია ელექტრონული მტკიცებულება — ახალი გამოწვევა ფრანგულ მართლმსაჯულებაში თარგმანი: თამთა მიქაია (თბილისის სააპელაციო სასამართლოს თავმჯდომარის ბიუროს სტაჟიორი) ელ. გვერდი



თავი V

ციფრული ინფორმაციის შემცველი მოწყობილობის ამოღების მეთოდისა და ტექნიკა

5.1. ციფრული ინფორმაციის შემნახველი კომპიუტერული მოწყობილობის ამოღების სამართლებრივი საფუძვლები

არის შემთხვევები, როდესაც გამოძიების ინტერესებიდან გამომდინარე აუცილებელია არა კომპიუტერული სისტემიდან ინფორმაციის გამოთხოვა, არამედ თავად კომპიუტერის ამოღება, იმისათვის, რომ გამოძიებლის მიერ ჩატარებულ იქნეს აღნიშნული საგამოძიებო მოქმედება, აუცილებელია გამოძიებელი კარგად ფლობდეს საგამოძიებო მოქმედების სამართლებრივი საფუძვლებს და კომპიუტერის აგებულების იმ მნიშვნელოვან კომპონენტებს, რომელიც საჭიროა მსგავსი ხასიათის საგამოძიებო მოქმედების ჩასატარებლად.

არსებობს საგამოძიებო მოქმედების ჩატარების 3 სამართლებრივი შემთხვევა:

1. მესაკუთრის/მფლობელის წერილობითი თანხმობა;
2. პროკურორის დადგენილება - გადაუდებელი აუცილებლობის შემთხვევაში;
3. სასამართლოს განჩინება;

განვიხილოთ თითოეული მათგანი;

მესაკუთრის/მფლობელის წერილობითი თანხმობა;

„მესაკუთრის, მფლობელის ან კომუნიკაციის ერთი მხარის თანხმობის შეფასებისას, ყოველ კონკრეტულ შემთხვევაში, ყურადღება უნდა მიექცეს იმას, თუ რა ტიპის საგამოძიებო მოქმედება ტარდება და რა არის საგამოძიებო მოქმედების ჩატარების მიზანი - საგამოძიებო მოქმედება დაკავშირებულია მხოლოდ საკუთრებაში ან მფლობელობაში შესვლასთან თუ საკუთრებიდან, მფლობელობიდან ან პირისგან იმავდროულად რაიმე ნივთის ამოღებასთან. ამოღების და ჩხრეკის ჩატარების დროს თანხმობის შეფასებისას აუცილებელია პირის თანხმობა არა მხოლოდ საგამოძიებო მოქმედების ჩატარებაზე, არამედ საგამოძიებო მოქმედების შედეგად ნივთის/ნივთების ამოღებაზე. ვინაიდან აღნიშნული საგამოძიებო მოქმედებების მიზანი დასაწყისშივე ნივთის ამოღებაა. უფრო კონკრეტულად, გამოძიებელმა, საგამოძიებო მოქმედების დაწყებამდე, პირს, ვისთანაც ატარებს საგამოძიებო მოქმედებას, უნდა განუმარტოს საგამოძიებო მოქმედების ჩატარების მიზნები, საფუძვლები, და მისი შედეგები. კერძოდ, გამოძიებელმა პირს უნდა აუხსნას, რომ საგამოძიებო მოქმედების მიზანია არა მხოლოდ ბინაში შესვლა, არამედ ბინიდან მტკიცებულების ამოღება. შესაბამისად, ბინის მესაკუთრემ თანხმობა უნდა განაცხადოს როგორც ბინაში საგამოძიებლის შესვლაზე, ისე ბინიდან მტკიცებულების ამოღებაზე. წინააღმდეგ შემთხვევაში, სახეზე იქნება პირის თანხმობის გარეშე გადაუდებელი აუცილებლობით ჩატარებული საგამოძიებო მოქმედება, რომელსაც საერთო წესით სჭირდება დაკანონება.“¹⁴⁰

გადაუდებელი აუცილებლობით ჩატარებული საგამოძიებო მოქმედება;

საქართველოს სისხლის სამართლის საპროცესო კოდექსის 112-ე მუხლის თანახმად: „როდესაც დაფიქსირდება შეიძლება გამოიწვიოს გამოძიებისათვის მნიშვნელოვანი ფაქტობრივი მონაცემების

¹⁴⁰

ავტორთა კოლექტივი, საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი. 2015 წლის 1 ოქტომბრის მდგომარეობით. ამერიკის იურისტთა ასოციაცია კანონის უზენაესობის ინიციატივის მხარდაჭერით. 2015 წელი. გვ. 369-370

განადგურება ან როცა დაყოვნება შეუძლებელს გახდის აღნიშნული მონაცემების მოპოვებას, ან როცა საქმისათვის საჭირო საგანი, დოკუმენტი, ნივთიერება ან ინფორმაციის შემცველი სხვა ობიექტი აღმოჩენილია სხვა საგამოძიებო მოქმედების ჩატარებისას (თუ აღმოჩენილია მხოლოდ ზედაპირული დათვალიერების შედეგად), ან როცა არსებობს სიცოცხლის ან ჯანმრთელობის ხელყოფის რეალური საფრთხე, საგამოძიებო მოქმედება შეიძლება ჩატარდეს სასამართლოს განჩინების გარეშე, რის შესახებაც მოსამართლეს, რომლის სამოქმედო ტერიტორიაზედაც ჩატარდა აღნიშნული საგამოძიებო მოქმედება, ან გამოძიების ადგილის მიხედვით მოსამართლეს პროკურორმა უნდა აცნობოს საგამოძიებო მოქმედების დაწყებიდან 24 საათის განმავლობაში და უნდა გადასცეს სისხლის სამართლის საქმის მასალები (ან მათი ასლები), რომლებიც ასაბუთებს საგამოძიებო მოქმედების გადაუდებლად ჩატარების აუცილებლობას. მოსამართლე მასალების შესვლიდან არა უგვიანეს 24 საათისა ზეპირი მოსმენის გარეშე წყვეტს შუამდგომლობას. მოსამართლე უფლებამოსილია შუამდგომლობა განიხილოს მხარეთა (თუ სისხლისსამართლებრივი დევნა დაწყებულია) და იმ პირის მონაწილეობით, რომლის მიმართაც ჩატარდა საგამოძიებო მოქმედება. შუამდგომლობის განხილვისას მოსამართლე ამოწმებს სასამართლო გადაწყვეტილების გარეშე ჩატარებული საგამოძიებო მოქმედების კანონიერებას. მოსამართლე უფლებამოსილია განმარტების მისაცემად გამოიძახოს ის პირი, რომელმაც საგამოძიებო მოქმედება სასამართლოს განჩინების გარეშე ჩატარა. ამ შემთხვევაში შუამდგომლობის განხილვისას გამოიყენება ამ კოდექსის 206-ე მუხლით გათვალისწინებული წესი.”¹⁴¹

სასამართლოს მიერ განჩინების გამოტანა;

„მასალების განხილვის შემდეგ სასამართლოს გამოაქვს განჩინება:

- ა) ჩატარებული საგამოძიებო მოქმედების კანონიერად ცნობის შესახებ;
- ბ) ჩატარებული საგამოძიებო მოქმედების უკანონოდ ცნობისა და მიღებული ინფორმაციის დაუშვებელ მტკიცებულებად ცნობის შესახებ.”¹⁴²

სასამართლოს განჩინებით ჩატარებული საგამოძიებო მოქმედება;

„მოსამართლის განჩინების გამოთხოვა ხორციელდება მხარის (ბრალდების და დაცვის) წერილობითი შუამდგომლობის საფუძველზე. შუამდგომლობა უნდა იყოს დასაბუთებული, მასში დეტალურად უნდა იყოს ჩამოყალიბებული მხარის მოთხოვნა, საგამოძიებო მოქმედების ჩატარების მიზანი და საფუძველი, ფაქტები და მათი დამადასტურებელი მტკიცებულებები, მსჯელობა და არგუმენტაცია ფაქტებსა და მტკიცებულებებზე, კანონი, რომელიც არგუმენტებს და მსჯელობას ამყარებს. მხარე ვალდებულია შუამდგომლობაში დაასაბუთოს მტკიცებულებათა იმ სტანდარტის (დასაბუთებული ვარაუდის) არსებობა, რომელსაც საგამოძიებო მოქმედების ჩატარებისთვის აუცილებელ წინაპირობად მიიჩნევს საქართველოს სსსკ-ის მე-3 მუხლის მე-11 ნაწილი;”¹⁴³

მხარის შუამდგომლობა სტრუქტურულად სამი ნაწილისაგან უნდა შედგებოდეს: შესავალი, აღწერილობითი (სამოტივაციო) და სარეზოლუციო ნაწილებისგან.

„შუამდგომლობის შესავალ ნაწილში უნდა მიეთითოს:

- სასამართლოს დასახელება, რომელსაც მხარე მიმართავს შუამდგომლობით;
- შუამდგომლობის შედგენის ადგილი და თარიღი;

¹⁴¹ საქართველოს სისხლის სამართლის საპროცესო კოდექსი (09/10/2009 რედ) 29.05.2019 წლის მდგომარეობით... მუხლი 112

¹⁴² იქვე.

¹⁴³ ავტორთა კოლექტივი, საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი. 2015 წლის 1 ოქტომბრის მდგომარეობით. ამერიკის იურისტთა ასოციაცია კანონის უზენაესობის ინიციატივის მხარდაჭერით. 2015 წელი. გვ.369

- შუამდგომლობის ავტორთა ვინაობა;
- სისხლის სამართლის საქმის ნომერი;
- დანაშაულის კვალიფიკაცია;
- მხარის მოთხოვნა.“¹⁴⁴

„შუამდგომლობის აღწერილობით ნაწილში უნდა მიეთითოს:

- საქმის ფაქტობრივი გარემოებები;
- მტკიცებულებები, რომლებიც ადასტურებენ ფაქტობრივ გარემოებებს;
- შუამდგომლობის ავტორის მოსაზრებები და არგუმენტაცია გადასაწყვეტ საკითხებზე (შუამდგომლობის დასაბუთება);
- შესაბამისი კანონმდებლობა, მუხლის, ნაწილისა და ქვეპუნქტის მითითებით, რომლებიც ადასტურებენ მითითებულ მოსაზრებებსა და არგუმენტებს.“¹⁴⁵

„შუამდგომლობის დასკვნით ნაწილში უნდა მიეთითოს:

- მხარის მოთხოვნა ამა თუ იმ საგამოძიებო მოქმედების ჩატარების თაობაზე ნებართვის გაცემის შესახებ;
- საგამოძიებო მოქმედების ჩატარების ადგილი, ჩამტარებული პირის და იმ პირის ვინაობა, რომელთანაც ტარდება საგამოძიებო მოქმედება.“¹⁴⁶

ამოღების და ჩხრეკის წესი;

„საგამოძიებო მოქმედების დაწყებამდე გამომძიებელი, პირველ რიგში, არკვევს აცხადებს თუ არა შესაკუთრე, მფლობელი ან კომუნიკაციის ერთი მხარე თანხმობას საგამოძიებო მოქმედების ჩატარებაზე. თანხმობის შემთხვევაში, გამომძიებელი ატარებს საგამოძიებო მოქმედებას და ადგენს შესაბამისი საგამოძიებო მოქმედების ოქმს. ის შემთხვევაში, გამომძიებელი იღებს გადაწყვეტილებას საგამოძიებო მოქმედება ჩაატაროს მოსამართლის განჩინებით თუ განჩინების გარეშე გადაუდებელი აუცილებლობით. ამ უკანასკნელ შემთხვევაში გამომძიებელს გამოაქვს დადგენილება. დადგენილების გამოტანის აუცილებლობა, როგორც უკვე აღინიშნა, შესაბამისი მუხლების კომენტირებისას, ყველა სახის საგამოძიებო მოქმედების ჩატარებისას არ არსებობს. ამოღება და ჩხრეკა საგამოძიებო მოქმედებათა იმ კატეგორიას განეკუთვნება, რომელთა ჩატარებამდე გამომძიებელმა უნდა გამოიტანოს დადგენილება.“¹⁴⁷

„ორივე შემთხვევაში (საგამოძიებო მოქმედების განჩინებით და განჩინების გარეშე ჩატარებისას), საგამოძიებო მოქმედების დაწყებამდე, გამომძიებელს ეცისრება იმ დოკუმენტის (განჩინების, დადგენილების) წარდგენის ვალდებულება, რაც საფუძვლად უდევს საგამოძიებო მოქმედების ჩატარებას. კერძოდ, გამომძიებელმა მოსამართლის განჩინება ან საკუთარი დადგენილება უნდა წარუდგინოს და ხელმოწერით გააცნოს იმ პირს, ვისთანაც ტარდება საგამოძიებო მოქმედება. ვინაიდან სწორედ აღნიშნული განჩინების (დადგენილების) საფუძველზე მოიპოვებს გამომძიებელი საცემი, სადგომი სათავსო ან სხვა მფლობელობაში საგნის, დოკუმენტის, ნივ-

¹⁴⁴ ავტორთა კოლექტივი, საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი. 2015 წლის 1 ოქტომბრის მდგომარეობით. ამერიკის იურისტთა ასოციაცია კანონის უზენაესობის ინიციატივის მხარდაჭერით. 2015 წელი. გვ.369.

¹⁴⁵ იქვე.

¹⁴⁶ იქვე.

¹⁴⁷ იქვე. გვ.390-392.

თიერების თუ ინფორმაციის შემცველი სხვა ობიექტის აღმოსაჩენად და ამოსაღებად შესვლის უფლებამოსილებას და შემდგომში პირის თანხმობას.¹⁴⁸

„განჩინების (დადგენილების) გაცნობაზე ან/და ხელმოწერაზე უარის შემთხვევაში, გამომძიებელი განჩინებაზე (დადგენილებაზე) აკეთებს შესაბამის მინაწერს. განჩინების, ხოლო გადაუდებელი აუცილებლობის შემთხვევაში — დადგენილების წარდგენის შემდეგ გამომძიებელი პირს, რომელთანაც ტარდება ამოღება ან ჩხრეკა, სთავაზობს ამოსაღები საგნის, დოკუმენტის, ნივთიერების თუ ინფორმაციის შემცველი სხვა ობიექტის ნებაყოფლობით გადაცემას.“¹⁴⁹

„აღსანიშნავია, რომ 1998 წლის 20 თებერვლის სსსკ-ი ამოღებასა და ჩხრეკას ნებაყოფლობითობის ნიშნით განასხვავებდა ერთმანეთისგან. კერძოდ, საქმისთვის მნიშვნელობის მქონე ნივთის ნებაყოფლობით გადაცემის შემთხვევაში, გამომძიებელს უნდა ჩაეთარებინა ამოღება, ხოლო ნივთის ნებაყოფლობით გადაცემაზე უარის შემთხვევაში — ჩხრეკა. შესაბამისად, აღნიშნული კოდექსი უშვებდა ამოღების ჩხრეკაში გადაზრდის შესაძლებლობას მაშინ, როცა ნივთის ამოსაღებად მიხულ გამომძიებელს მის ნებაყოფლობით გადაცემაზე უარს ეტყოდნენ. მსგავს შემთხვევაში გამომძიებელი ვალდებული იყო შეედგინა ჩხრეკის ოქმი. მოქმედი საპროცესო კოდექსი კი როგორც ჩხრეკის, ისე ამოღების შემთხვევაში, უშვებს იძულების პროპორციული ზომების გამოყენების შესაძლებლობას. კერძოდ, ამოსაღები ობიექტის ნებაყოფლობით გადაცემის შემთხვევაში, აღნიშნული ფაქტი ფიქსირდება ოქმში, ხოლო მის ნებაყოფლობით გადაცემაზე უარის თქმის ან მისი არასრულად გადაცემის შემთხვევაში, ამოღება ხდება იძულებით.“¹⁵⁰

„ამასთან, გამომძიებელი უფლებამოსილია, გააღოს დაკეტილი საცავი, სადგომი და სათავსი, თუ გასაჩხრეკი პირი უარს ამბობს მათ ნებაყოფლობით გადაცემაზე. ამოღებისა და ჩხრეკის განჩინებაში (დადგენილებაში) მეთითება იმ საგნის, დოკუმენტის, ნივთიერების თუ ინფორმაციის შემცველი სხვა ობიექტის შესახებ, რომლის ამოღებაც უნდა განხორციელდეს. შესაბამისად, გამომძიებელი, საგამომძიებო მოქმედების ჩატარების ადგილზე ეძებს და იღებს იმ საგანს, დოკუმენტს, ნივთიერებას თუ ინფორმაციის შემცველ სხვა ობიექტს, რომელიც აღნიშნულია განჩინებაში ან დადგენილებაში. სსსკ-ი ადგენს საგანის, დოკუმენტის, ნივთიერების, თუ ინფორმაციის შემცველი სხვა ობიექტის ამოღების და შენახვის სპეციალურ წესებს, რომელთა დაუცველობამ შესაძლოა მტკიცებულებათა დაუშვებლად ცნობა გამოიწვიოს.“¹⁵¹

„როგორც წესი, ჩხრეკის ან ამოღების დროს აღმოჩენილი საგანი, დოკუმენტი, ნივთიერება თუ ინფორმაციის შემცველი სხვა ობიექტი ამოღებამდე უნდა წარედგინოს ამ საგამომძიებო მოქმედებაში მონაწილე პირებს, შემდეგ ამოღებულ იქნეს, დაწვრილებით აღიწეროს, დაილუქოს და შეიფუტოს, შეფუთულ ნივთზე, ლუქის გარდა, აღნიშნება თარიღი და იმ პირთა ხელმოწერები, რომლებიც საგამომძიებო მოქმედებაში მონაწილეობდნენ, ამ წესიდან სსსკ-ის 120-ე მუხლი გამონაკლისს ითვალისწინებს. კერძოდ, ამოსაღები ობიექტი მხოლოდ მაშინ წარედგინება საგამომძიებო მოქმედების მონაწილეებს და ამოღების შემდეგ მხოლოდ მაშინ დაილუქება, თუ ამ საპროცესო მოქმედებების შესრულება შესაძლებელია, ანუ თუ ამოსაღები ობიექტი მისი გაბარიტების და ნიშან-თვისებების გათვალისწინებით იძლევა საგამომძიებო მოქმედების მონაწილეთათვის წარდგენისა და ამოღების შემდეგ დალუქვის შესაძლებლობას.“¹⁵²

¹⁴⁸ ავტორთა კოლექტივი, საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი. 2015 წლის 1 ოქტომბრის მდგომარეობით. ამერიკის იურისტთა ასოციაცია კანონის უზენაესობის ინიციატივის მხარდაჭერით. 2015 წელი. გვ.390

¹⁴⁹ იქვე.

¹⁵⁰ იქვე. გვ.391.

¹⁵¹ იქვე. გვ.391-392

¹⁵² იქვე. გვ.392

5.2. დეტალიზაციის მეთოდური პრობლემა კომპიუტერული მოწყობილობის ამოღების დროს

როდესაც გამომძიებელი იწყებს საგამოძიებო მოქმედებას - ამოღებას, დგება საკითხი, ხომარ ხდება ზედმეტი კომპიუტერის ნაწილების ამოღება და ხომარ ჰყოფს აღნიშნული რაიმე სხვა კონსტიტუციით გათვალისწინებულ უფლებას.

ხშირად არის ხოლმე შემთხვევები, როდესაც საგამოძიებო მოქმედების - ჩხრეკის ან ამოღების დროს, გამომძიებელი მიდის საგამოძიებო მოქმედების ადგილზე და იღებს კომპიუტერის ყველა მოწყობილობას, მათ შორის მავსს, ე.წ. პრინტერს, სკანერს და ა.შ. ან შესაძლოა გამომძიებელმა ამოიღოს კომპიუტერის პროცესორი - მაგრამ მასში არ იყოს კომპიუტერის შემნახველი შესაბამისი მოწყობილობა - რაზეც ქვემოთ იქნება საუბარი, როგორ უნდა მოიქცეს ასეთ დროს გამომძიებელი -? მან უნდა ამოიღოს მხოლოდ ის ნივთი რომელიც არის ინფორმაციის მატარებელი, უფრო კონკრეტულად კი რომელშიც დაცულია ციფრული ინფორმაცია.

ამ საკითხის გადასაწყვეტად ძალზედ მნიშვნელოვანი კვლევა აქვს ჩატარებული ქალბატონ ლალი ფაფიაშვილს, რომელიც მიიჩნევს, რომ „ბრალდების მხარის მიერ სასამართლოს წინაშე დაყენებული შუამდგომლობის და შესაბამისად, სასამართლოს განჩინების დეტალიზაცია განსაკუთრებულ მნიშვნელობას იძენს, როდესაც ჩხრეკის ფარგლებში იგეგმება კომპიუტერულ მონაცემთა შესანახი საშუალებების ამოღება, რაც განპირობებულია მათზე არსებული ინფორმაციის მოცულობით და ხასიათის მრავალფეროვნებით. შესაბამისად, შუამდგომლობაში და სასამართლოს განჩინებაშიც, როგორც მინიმუმ, აღნიშნული უნდა იყოს ამოსაღები კომპიუტერული მონაცემების შესანახი საშუალებები, ამ საშუალებების საოპერაციო სისტემა, მყარი დისკის მხასიათებლები და ა.შ.“¹³³

ზემოაღნიშნულიდან გამომდინარე ძალზედ მნიშვნელოვანია რომ;

პროკურორმა სწორად მითითოს შუამდგომლობაში ის თუ რისი ამოღება სურს და დაასაბუთოს საქმისათვის რა მნიშვნელობის მატარებელია აღნიშნული, ან - დადგენილებაში გადაუდებლად ჩხრეკის მატარების დროს დეტალიზება მოხდეს რა ნივთი და რატომ უნდა იქნეს ამოღებული.

როდესაც მოსამართლე განჩინებას გასცემს - „თუ განჩინება დეტალურად განსაზღვრავს, კომპიუტერის რომელი მყარი დისკები უნდა იქნეს ამოღებული, მაგრამ არაფერს უთითებს ჩხრეკის მე-2 სტადიასთან მიმართებით, კერძოდ, არ იძლევა მითითებას იმის შესახებ, თუ რა მტკიცებულებას შეიძლება შეიცავდეს კომპიუტერი, ან, მაგალითად, განჩინება დეტალურად ასახელებს კომპიუტერის ფაილებს, რომლებიც უნდა გადამოწმდეს მე-2 ეტაპზე წარმოებული ჩხრეკის ფარგლებში, მაგრამ არაფერს აღნიშნავს იმის შესახებ, თუ რომელი კომპიუტერები უნდა იქნეს ამოღებული ჩხრეკის ადგილიდან, ასეთ შემთხვევებში რომელიმე ამ განჩინებებიდან არის საკმარისად დეტალიზებული? იმის განსაზღვრისათვის, ჩხრეკაზე განჩინება არის თუ არა საკმარისად დეტალიზებული, მხედველობაში მიიღება შემდეგი გარემოებები:

1. არსებობს თუ არა დასაბუთებული ვარაუდი განჩინებაში მითითებული კონკრეტული ტიპის ყველა საგნის ამოღებისათვის?

¹³³ ლალი ფაფიაშვილი. სტატია: ციფრული მტკიცებულებების ამოღება: პირადი ცხოვრების ხელშეუხებლობის საკმარისი თუ ილუზორული გარანტია? სტადიათა კრებული, ადამიანის უფლებათა დაცვა და სამართლებრივი რეფორმა საქართველოში. თბილისი, 2014. გვ. 146

2. განიხილება ადგენს ობიექტურ კრიტერიუმს, რომლის მეშვეობით აღმასრულებელ პირს შეეძლება, გამოყოს ამოღებას დაქვემდებარებული საგნები იმ საგნებიდან, რომელთა ამოღებაც არ უნდა განხორციელდეს?
3. შეეძლო თუ არ პროცესის მწარმოებელ ორგანოს, უფრო დეტალურად აღეწერა ამოსაღები საგნები იმ ინფორმაციის გათვალისწინებით, რომელიც მის ხელთ იყო განიხილების გაცემის მომენტისათვის?"¹⁵⁴

„საქმეზე – აშშ რიკარდის წინააღმდეგ (UNITED STATES V. RICCARDI) – პორნოგრაფიული მასალის გავრცელებასთან დაკავშირებით წარმოებული ჩხრეკის ორდერში მითითებული იყო, რომ ჩხრეკის მწარმოებელ სუბიექტებს კომპიუტერის ამოღებასთან ერთად, ასევე უნდა ამოეღოთ: „კომპიუტერში ჩაწერილი ნებისმიერი სახის ელექტრონული ინფორმაცია, ასევე ყველა ჩამწერი მოწყობილობა (კომპიუტერში/კომპიუტერულ სისტემაში ინტეგრირებული და გარემოებისეირება), მათ შორის, და არამხოლოდ: დისკები, დისკეტები, მყარი დისკები, მაგნიტური ლენტები, გამოცალკევებადი მე-დიადრავიკები, ფლეშბარათები, მეხსიერების ბარათები, პრინტერები, მოდემები და ნებისმიერი სხვა ელექტრონული ან მაგნიტური მოწყობილობა, გამოყენებული კომპიუტერის ან კომპიუტერული სისტემის დამხმარე მოწყობილობა და მათზე ჩაწერილი ელექტრონული ინფორმაცია“.¹⁵⁵

აღნიშნულ საქმეში მოთხოვნა და შემდეგ დაკმაყოფილება აღნიშნული მოთხოვნის იყო ძალიან მსუყე და რაც მთავარია დაუსაბუთებელი, ან უ საგამოძიებო მოქმედების განიხილების გაცემა მოხდა ზოგადი დასაბუთებიდან გამომდინარე, არ არის ინფორმაცია რა საქმისათვის მნიშვნელოვანი მასალა შესაძლოა ყოფილიყო მაგალითად მეხსიერების ბარათებში, ან რაში იყო საჭირო ისეთი მოწყობილობა როგორც არის პრინტერი, მოდემი და ასე შემდეგ, შესაბამისად არც ბრალდების მხარის მიერ ყოფილა დასაბუთებული არნიშნული, სასამართლომ კი გამოიტანა შემდეგი გადაწყვეტილება;

„სასამართლომ აღნიშნა, რომ განიხილება (აშშ-ის შემთხვევაში – ორდერი) არ აკმაყოფილებდა დეტალიზაციის მოთხოვნას და იყო ზედმეტად ფართო შინაარსის მატარებელი. კომპიუტერის ჩხრეკის განიხილებამ/ორდერმა უნდა შეზღუდოს ჩხრეკა კონკრეტული დანაშაულის ჩადენის მამხილებელი მტკიცებულების ან კონკრეტული ტიპის მასალის აღმოჩენით. ამ შემთხვევაში ორდერი არ იყო შემოფარგლული რომელიმე კონკრეტული დანაშაულით ან კონკრეტული ფაილებით. ამდენად, ორდერი უფლებას აძლევდა ჩხრეკის მწარმოებელ პირებს, განეხორციელებინათ ჩხრეკა ნებისმიერი საგნის აღმოსაჩენად – ბავშვთა პორნოგრაფიიდან საგადასახადო კანონმდებლობის დარღვევამდე.“¹⁵⁶

„ითვლება, რომ დეტალიზაციის მოთხოვნას აკმაყოფილებს სასამართლოს განიხილებები, რომლებშიც ამოსაღები საგნების ნუსხაში ერთდროულად მითითებულია ზუსტად განსაზღვრული ნივთები და ნივთები, რომელთა განსაზღვრისათვის სასამართლო იყენებს ე.წ. „ყოვლისმომცველ ცნებებს“, როგორებიცაა, მაგალითად: ელექტრონული მატარებლები ან ელექტრონული მოწყობილობები, რაც მოიცავს ნებისმიერი სახის ელექტრონულ მატარებელს, მათ შორის ჩხრეკის ადგილას არსებულ ყველა კომპიუტერს, გარემოებისეირებას, დისკებს, მეხსიერების ბარათებს და

¹⁵⁴ იქვე. 146

¹⁵⁵ ლალი ფაფიაშვილი. სტატი: ციფრული მტკიცებულების ამოღება: პირადი ცხოვრების ხელ-შეუხებლობის საკმარისი თუ ილუზორული გარანტია? სტატიათა კრებული, ადამიანის უფლებათა დაცვა და სამართლებრივი რეფორმა საქართველოში. თბილისი. 2014. გვ. 147

¹⁵⁶ იქვე.

ა.შ. ამ შემთხვევაში განჩინების დეტალიზაციას განაპირობებს განჩინების კონტექსტი, მასში მითითებული სხვა ამოსაღები საგნები. შედეგად, განჩინება წაკითხული უნდა იქნეს როგორც ჩხრეკის მწარმოებელი პირებისათვის ამოღებულ კომპიუტერებსა და ელექტრონულ მოწყობილობებში მხოლოდ განსაზღვრული საკითხების წრესთან დაკავშირებული ინფორმაციის შემცველი მასალის ჩხრეკაზე უფლების მიმნიჭებელი. განჩინების ამგვარი განმარტებისას სასამართლო მას თვლის საკმარისად დეტალიზებულად. წინააღმდეგ შემთხვევაში, თუ განჩინება ითვალისწინებს კომპიუტერში არსებული ყველა ჩანაწერის ჩხრეკის უფლებას აღწერის ან შეზღუდვის გარეშე, ის ვერ აკმაყოფილებს მე-4 შესწორებით განსაზღვრულ სტანდარტს (იხ. აშშ რიკარდის წინააღმდეგ (United States v. Ricciardi), 405 F.3d 852,862, 10th Cir. 2005).¹⁵⁷

ამდენად, ზემოაღნიშნული გადაწყვეტილება და განმარტებები, რომ მოვარგოთ საქართველოში არსებულ რეალობას, აუცილებელია რომ:

გამომძიებლის მიერ დადგენილებაში საგამომძიებო მოქმედების ჩატარების შესახებ და შემდგომ პროკურორის შუამდგომლობაში საგამომძიებო მოქმედების კანონიერების შემოწმების შესახებ დეტალურად უნდა იყოს დასაბუთებული;

1. რა საგანი (საგნები) უნდა იქნეს დაძებნილი და ამოღებული საგამომძიებო მოქმედების შედეგად;
2. რატომ უნდა მოხდეს აღნიშნული საგნის (საგნების) დაძებნა და შემდგომ ამოღება;
3. რა შემხებლობაშია ამოსაღები საგანი საქმესთან და რა ინფორმაცია ინახება ან შესაძლოა ინახებოდეს მასზე;
4. რა საპროცესო საფუძველი არსებობს საგამომძიებო მოქმედების გადაუდებლად ჩატარებისათვის;

ხოლო თუ მხარე შუამდგომლობით მიმართავს სასამართლოს და სთხოვს მას, რომ გასცეს განჩინება – ჩატარებულ იქნეს საგამომძიებო მოქმედება ჩხრეკა – ან/და ამოღება, პროკურორი ვალდებულია დაასაბუთოს

1. რა საგანი (საგნები) უნდა იქნეს დაძებნილი და ამოღებული საგამომძიებო მოქმედების შედეგად;
2. რატომ უნდა მოხდეს აღნიშნული საგნის (საგნების) დაძებნა და შემდგომ ამოღება;
3. რა შემხებლობაშია ამოსაღები საგანი საქმესთან და რა ინფორმაცია ინახება ან შესაძლოა ინახებოდეს მასზე;
4. რა საპროცესო საფუძველი არსებობს საგამომძიებო მოქმედებისათვის განჩინების გასაცემად;

¹⁵⁷

ლალი ფაფიაშვილი. სტატია: ციფრული მტკიცებულების ამოღება: პირადი ცხოვრების ხელშეუხებლობის საკმარისი თუ ილუზორული გარანტია? სტატიათა კრებული, ადამიანის უფლებათა დაცვა და სამართლებრივი რეფორმა საქართველოში. თბილისი. 2014. გვ. 147-148

5.3. ციფრული ინფორმაციის შემნახველი კომპიუტერული მოწყობილობების სახეები

ციფრული ინფორმაციის ამოღება როდესაც ხორციელდება, მთავარია გამომძიებელმა, რომელიც აწარმოებს საგამომძიებო მოქმედებას იცოდეს თუ რა საგანი უნდა ამოიღოს და რატომ, ამისათვის აუცილებელია გამომძიებელმა იცოდეს რა სახის კომპიუტერული სისტემები არსებობს, რაშიც შეიძლება საქმისთვის მნიშვნელოვანი ინფორმაცია იყოს განთავსებული.

აუცილებელია გაიმიჯნოს რა სახის ინფორმაციას უნდა ფლობდეს გამომძიებელი და რას არა, მნიშვნელოვანია რომ გამომძიებელმა იცოდეს კომპიუტერის აგებულება არაპროფესიონალურ არამედ იმ დონეზე, რაც ხელს შეუწყობს მის მიერ საგამომძიებო მოქმედების წარმოებას, ასევე იცოდეს რა ნაწილებისგან შედგება კომპიუტერი და სად არის დაცული მისთვის საჭირო ინფორმაცია აღნიშნულ კომპიუტერში.

აღნიშნული საკითხის დეტალიზება დავიწყეთ პერსონალური კომპიუტერით, რისთვისაც საწყის ეტაპზე მოლკედ მიმოვიხილოთ კომპიუტერის კლასიფიკაცია;

„კომპიუტერი არის ტექნიკურ საშუალებათა კომპლექსი, რომლის დანიშნულებაცაა ინფორმაციული და გამოთვლითი ამოცანების გადაწყვეტის პროცესში, ინფორმაციის ავტომატური დამუშავება. გამოთვლების შესაძლებლობისა და ზომის მიხედვით კომპიუტერები შეიძლება დაიყოს (იხილეთ სურათი N1):

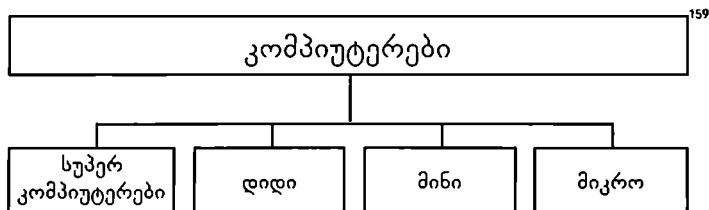
ზედიდი (სუპერ-კომპიუტერები);

დიდი;

მცირე;

ზემცირე (მიკროკომპიუტერები);“¹⁵⁸ (იხილეთ სურათი №1)

(კომპიუტერების დაყოფა – სურათი N1);



„სუპერკომპიუტერებს მიეკუთვნება მძლავრი მრავალპროცესორიანი გამოთვლელი მანქანები, რომელთა სისწრაფე ასეულ მილიონობით მილიარდოპერაციას შეადგენს წაშში. დიდ კომპიუტერებს საზღვარგარეთ უწოდებენ ეინფერმიებს; მათ მიეკუთვნება კომპიუტერები, რომელთაც აქვთ: წარმადობა არანაკლებ 100 MIPმ; ძირითადი მეხსიერების მოცულობა 512-დან 10000 მბაიტამდე; გარე მეხსიერება არანაკლებ 100 გბაიტი; მუშაობის მრავალ-მომხმარებლიანი რეჟიმით.“¹⁶⁰

¹⁵⁸ ომარ გაბედავა, კომპიუტერის არქიტექტურა (სახელმძღვანელო) თბილისი 2008 წელი

¹⁵⁹ სურათი; ომარ გაბედავა, კომპიუტერის არქიტექტურა (სახელმძღვანელო) თბილისი 2008 წელი

¹⁶⁰ იქვე.

„მეინფორმაციის ეფექტური მოხმარების მიმართულებით სამეცნიერო-ტექნიკური ამოცანების გადაწყვეტა. ინფორმაციის პაკეტური დამუშავებით, მუშაობა დიდი მოცულობის მონაცემთა ბაზებთან, გამოთვლითი ქსელებისა და მათი რესურსების მართვით. უკანასკნელ პერიოდში მეინფორმაციის გამოიყენებენ გამოთვლით ქსელებში დიდ სერვერებად.“¹⁶¹

„მცირე კომპიუტერები (მინი-კომპიუტერები) არის საიმედო, იაფი და მოსახერხებელი ექსპლუატაციაში, რომლებიც ფლობენ შედარებით მცირე შესაძლებლობებს.“¹⁶²

„მინი-კომპიუტერების მიღწევად შეიძლება აღინიშნოს: სპეციფიკური არქიტექტურა მოდულურობის პრინციპით; საუკეთესო შეფარდება წარმადობა/ფასი; გამოთვლების დიდი სიზუსტე. მინი-კომპიუტერები ორიენტირებულები არიან მმართველ-გამომთვლელ კომპლექსებში გამოსაყენებლად. აგრეთვე წარმატებით გამოიყენებიან მრავალი მოხმარების გამოთვლით სისტემებში, ჯგოფადინებული დაპროექტების სისტემებში, მამოდელირებელ სისტემებში, ხელოვნური ინტელექტის სისტემებში.“¹⁶³

„მიკროკომპიუტერების კლასს განეკუთვნებიან პერსონალური კომპიუტერები (PK), რომლებიც მათი მასობრივი გავრცელების გამო იმსახურებენ განსაკუთრებულ ყურადღებას. [...]“¹⁶⁴ ამჟამად კომპიუტერების მსოფლიო პარკი შეადგენს მილიარდის მეოთხედ ცალს, მათგან 90% პერსონალური კომპიუტერებია (IBM PC ტიპის კომპიუტერები შეადგენს მთელი რაოდენობის 80%).“¹⁶⁵

მნიშვნელოვანი საკითხია, რას ინახავს კომპიუტერული მოწყობილობა და რატომ უნდა ამოვიღოთ ის, კომპიუტერში ინახება ინფორმაცია, ინფორმაცია კი არის ყველაფერი ის რასაც ადამიანი აღიქვამს გრძნობათა ორგანოების მეშვეობით. ინფორმაცია ლათინური სიტყვაა და ქართულად – ცნობას ნიშნავს;

კომპიუტერი ინახავს სამი სახის ინფორმაციას. ესენია:

1. ტექსტური;
2. გრაფიკული;
3. აუდიო;

ტექსტური ინფორმაცია შედგება ციფრების, ასოების, სასვენი ნიშნებისა და სპეციალური სიმბოლოებისაგან.

გრაფიკული ინფორმაცია წარმოადგენს - ნახაზებს, ნახაზებს, ფოტო სურათებს, მოძრავ სურათებს და სხვა.

აუდიო (ანუ ხმოვანი) ინფორმაცია - არის მუსიკა, საუბარი, და სხვადასხვა ხმოვანი ეფექტები.

„ინფორმაციას, ისევე როგორც ნებისმიერ სხვა ფიზიკურ სიდიდეს გააჩნია საზომი ერთეულები. ინფორმაციის ყველაზე მცირე საზომ ერთეულს ბიტი (bit) ეწოდება. მას შეიძლება ჰქონდეს მხოლოდ ორი მნიშვნელობა. ის შეიძლება უდრიდეს 0 ან 1-ს. ორობითი თვლის სისტემის ერთ-ერთ ციფრს.“¹⁶⁶

„პრაქტიკაში ასევე გამოიყენება ბაიტი (Byte) რომელიც უდრის 8 ბიტს და ერთ ტექსტურ სიმბოლოს.“¹⁶⁷

¹⁶¹ ომარ გაბედავა, კომპიუტერის არქიტექტურა (სახელმძღვანელო) თბილისი 2008 წელი

¹⁶² იქვე.

¹⁶³ იქვე.

¹⁶⁴ იქვე.

¹⁶⁵ იქვე.

¹⁶⁶ იქვე.

¹⁶⁷ იქვე.

რადგანაც ბიტი და ბაიტი მცირე ზომის საზომი ერთეულებია უფრო სირად გამოიყენება მათგან წარმოებული ერთეულები:¹⁶⁸

კილობაიტი (KB); მეგაბაიტი (MB); გიგაბაიტი (GB);
ტერაბაიტი (TB); კილობიტი (Kb); მეგაბიტი (Mb);
გიგაბიტი (Gb); თერაბიტი (Tb);

დაახლოებით:	ზუსტად:
1KB = 1 000B	(1024B)
1MB = 1 000 000B	(1024KB)
1GB = 1 000 000 000B	(1024MB)
1TB = 1 000 000 000 000B	(1024GB)

ხოლო, როდესაც გამოძიებული შედის საგამოძიებო მოქმედების ჩასატარებლად და უნდა ამოიღოს რაიმე სახის კომპიუტერული მოწყობილობა, მნიშვნელოვანია კარგად იცოდეს რა უნდა ეძებოს მან და რა მოწყობილობა უნდა ამოიღოს რომელიც შესაძლოა იყოს ინფორმაციის მატარებელი. მიუხედავად იმისა, რომ ასეთი მოწყობილობები უამრავი შეიძლება იყოს, წარმოგიდგენთ პრაქტიკაში ხშირად გავრცელებულ სახეობებს (იხილეთ სურათი N2):

(პერსონალური კომპიუტერის ნაირსახეობები სურათი N2);



პორტატიული კომპიუტერი;

„ეს არის კომპიუტერი, რომელიც არის პერსონალური კომპიუტერების სწრაფად განვითარებადი ქვეკლასი. ვიდემონიტორად გამოიყენება ბრტყელი თხევად კრისტალური დისპლეი.“¹⁷⁰

კომპიუტერი ბლოკნოტი;

„კომპიუტერი — ბლოკნოტი ანუ ნოუთბუქი ასრულებს პერსონალური კომპიუტერის ყველა ფუნქციას, მასში შე-იძლება გამოყენებული იქნას იგივე ოპერაციული სისტემები და პროგრამები.“

¹⁶⁸ ელ. გვერდი : ნანახია 15.07.2019

¹⁶⁹ ომარ გაბედავა, კომპიუტერის არქიტექტურა (სახელმძღვანელო) თბილისი 2008 წელი

¹⁷⁰ იქვე.

კომპიუტერი-ბლოკნოტები იყოფიან კლასებად მათი გა-ბარიტების შესაბამისად (სქელი და თხელი). ეკრანის ზომებით. ხშირად მასში გამოყენებული მიკროპროცესორების მიხედვით. პრაქტიკულად ყველა ნოუთბუქი მუშაობს OC WINDOWS XP მართვით.”¹⁷¹

ჭიბის კომპიუტერები;

„ჭიბის კომპიუტერები არის ყველაზე სწრაფად განვითარებადი პორტატიული კომპიუტერების კლასი. ჭიბის კომპიუტერებში გამოიყენება თავისი ოპერაციული სისტემა, პერსონალური კომპიუტერისაგან განსხვავებით. ჭიბის კომპიუტერები არის სრულფასოვანი კომპიუტერები, რომელთაც აქვთ მიკროპროცესორები, ოპერატიული მეხსიერება, ფერადი თხევადკრისტალური დისპლეი, პორატიული ფიზიკური ან ვირტუალური კლავიატურა, პორტები (ხშირად უსადენო) გარე მოწყობილობასთან მისაერთებლად.”¹⁷²

ელექტრონული მდივანი;

„ელექტრონულ მდივანს ხშირად უწოდებენ (ხელით დამხმარეს), რომელსაც აქვს ჭიბის კომპიუტერის ფორმატი. მოწყობილობას გააჩნია ფართო ფუნქციონალური შესაძლებლობა. ის აღჭურვილია აპარატურულ და ჩადგმული პროგრამული უზრუნველყოფით, ორიენტირებულია ელექტრონული ცნობარის ორიენტაციაზე, რომელიც ინახავს სახელს, მისამართს და ტელეფონების ნომრებს, დღის განრიგისა და შეხვედრების ინფორმაციას, მიმდინარე საქმეების სიას, დანახარჯების შესახებ ჩანაწერებს და სხვ. უმთავრესად ასეთ მოწყობილობებს აქვთ მოდემების სხვა კომპიუტერებთან ინფორმაციის გასაცვლელად, თუ მიერთებული იქნება გამოთვლით ცენტრთან შესაძლებელი ხდება ელექტრონული ფოსტისა და ფაქსის გაგზავნა. ზოგიერთ მათგანს აქვს ავტომატური ნომრის ამკრები. უსადენო, დინსტანციური ინფორმაციის გასაცვლელად გამოიყენება რადიომოდემები და ინფრაწითელი პორტები. ზოგიერთ მოდელს აქვს სენსორული ეკრანი მაჩვენებელით.”¹⁷³

ელექტრონული ჩამწერი წიგნაკი;

„ელექტრონული ჩამწერი წიგნაკი - ორგანიზმური მიეკუთვნება პორტატიულ კომპიუტერებს (ამ კატეგორიას ამის გარდა ეკუთვნის კალკულატორები, ელექტრონული მთარგმნელები და ა. შ.). ორგანიზმური მომხმარებლის მიერ არ პროგრამირდება, მაგრამ აქვს მეხსიერება 2-256 კბაიტი, რომელშიდაც შეიძლება ჩაიწეროს აუცილებელი ინფორმაცია და მოხდეს მისი რედაქტირება, (აქვს ჩადგმული ტექსტური რედაქტორი); მეხსიერებაში შეიძლება შენახული იქნას სატელეფონო და სამისამართო წიგნები, საქმიანი წერილები, შეთანხმების ტექსტი, კონტრაქტი, დღის განრიგი და საქმიანი შეხვედრების განრიგი. ორგანიზმურში არის შიდა ტიპირი და შესაძლებლობა ხმოვანი სიგნალით მოგვცეს შეტყობინება საქმის შესახებ მოცემულ დროში. შესაძლებელია ინფორმაციის დაცვა არასანქცირებული ქმედებისაგან, ჩვეულებრივი პაროლის მეშვეობით.”¹⁷⁴

მობილური მოწყობილობები (mobile intelligent devices - მობილური ტელეფონები, კომუნიკატორები);

„წარმოადგენენ მოწყობილობებს, რომლებიც გამოიყენებიან ხმოვანი კავშირებისთვის, იშვიათად რაიმე ინფორმაციის დასაშუშავებლად ან ინტერნეტში შესასვლელად. მობილური მოწყობილობებისთვის მნიშვნელოვანი პარამეტრია ხმოვანი სიგნალის ხარისხი და ბატარეის ავტონომიური მუშაობის დრო. მათში ასევე მნიშვნელოვანია ციფრული ფოტო და ვიდეოკამერები. მობილური მოწყობილობებისთვის ოპერაციული სისტემა ხასიათდება დიდი კომპაქტურობით, მეხსიერებასთან უფრო მაკაყრი შეზღუდვებით. მობილური ტელეფონების ბაზარზე დომინირებდა

¹⁷¹ ომარ გაბედავა, კომპიუტერის არქიტექტურა (სახელმძღვანელო) თბილისი 2008 წელი.

¹⁷² იქვე.

¹⁷³ იქვე.

¹⁷⁴ იქვე.

ოპერაციული სისტემა Symbian, ამჟამად, გავრცელებულია თანამედროვე და მომხმარებლისათვის უფრო უკეთესი ინტერფეისის მქონე ოპერაციულ სისტემა OC Google Android და Microsoft Windows Mobile. მობილური მოწყობილობებისთვის, ისე როგორც ჯიბის კომპიუტერებისათვის, ოპერაციული სისტემის მნიშვნელოვანი მახასიათებელია მისი საიმედოობა. კერძოდ, მეხსიერების გადავსების შემთხვევაში მონაცემთა შენახვა, რომელიც შეიძლება წარმოიშვას დიდი რაოდენობის – SMS შეტყობინების მიღებისას, ფოტო ვიდეოგადაღებების ინტენსიურობისას. ამ მიმართულებით ოპერაციული Symbian სისტემა არც ისე საიმედოა. მაგალითად, „ზედმეტი“ შეტყობინებების მიღებისას, რომელიც არ ეტევა მეხსიერებაში ის იბლოკება „Memory full“ შეტყობინებით, რის შემდეგაც ხელით უნდა გამოირთოს და ჩაირთოს ტელეფონი და ამ გზით გადაიკვირთოს ოპერაციული სისტემა. რაც შეეხება მობილური მოწყობილობების სხვა პროგ-რამულ უზრუნველყოფას მათ დამუშავებაში დომინირებს Java- ტექნოლოგიები.“¹⁷⁵

5.4. პერსონალური კომპიუტერის ამოღების ტექნიკური პროცედურები და მეთოდები

მას შემდეგ რაც გამოძიებლის მიერ ნაპოვნი იქნება პერსონალური კომპიუტერის მოწყობილობა, მნიშვნელოვანია გამოძიებელმა არ ამოიღოს სრული მოწყობილობა, არამედ მან უნდა ამოიღოს უშუალოდ ის, რაც არის საქმისათვის მნიშვნელოვანი ინფორმაციის მატარებელი, აღნიშნულის დეტალიზებისთვის, მოკლედ მიმოვიხილოთ პერსონალური კომპიუტერის აგებულია და ვნახოთ თუ რა უნდა ამოიღოს გამოძიებელმა:

„კომპიუტერის შემადგენლობაში შეიძლება გამოიყოს ორი ნაწილი, ესენია მისი აპარატული უზრუნველყოფა და პროგრამული უზრუნველყოფა. მათი ურთიერთკავშირისა და თანამოქმედების უზრუნველყოფაც ხდება არქიტექტურის დონეზე.“¹⁷⁶

„პერსონალურ კომპიუტერს არ გააჩნია რაიმე სტანდარტული ან უცვლელი კონფიგურაცია. მისი შემადგენლობის განსაზღვრა ხდება კონკრეტულ შემთხვევაში და დამოკიდებულია იმაზე, თუ რა ამოცანების გადასაწყვეტად გვჭირდება მოცემული კომპიუტერი. სწორედ მისი შემადგენლობა, ანუ მასში გამოყენებული მოწყობილობები განსაზღვრავს მის შესაძლებლობებსა და ფასს. მაგრამ, მაინც არსებობს გარკვეული მინიმალური კონფიგურაცია ანუ საბაზო კონფიგურაცია, რომლის არსებობაც აუცილებელია იმისათვის, რომ კომპიუტერმა შესძლოს ფუნქციონირება. ამ კონფიგურაციაში დამატებითი მოწყობილობების ჩართვით ხდება მისი შესაძლებლობების გაზრდა ან მისთვის ახალი ფუნქციების დამატება.“¹⁷⁷

საბაზო კონფიგურაციაში შეიძლება გამოიყოს მისი შემდეგი ნაწილები:

- სისტემური ბლოკი;

¹⁷⁵ სტატია პერსონალური კომპიუტერის ძირითადი მოწყობილობები, ელ.გვერდი



¹⁷⁶ ელ. გვერდი

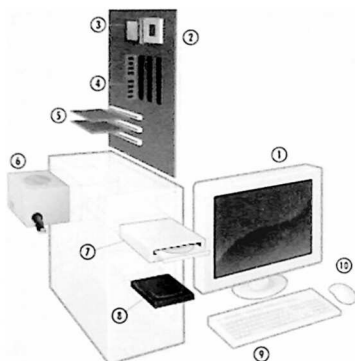


ნანახია. 28.07.2019. გვ.1

¹⁷⁷ იქვე.

- მონიტორი;
- კლავიატურა;
- მაუსი.

(კომპიუტერის აგებულება სურათი N3);



თანამედროვე სამაგიდო პერსონალური კომპიუტერის შემადგენლობა:

1. მონიტორი; 2. დედალატა; 3. მიკროპროცესორი (CPU); 4. ოპერატიული მეხსიერება (RAM); 5. გაფართოების დაფა; 6. დენის წყარო; 7. ოპტიკური დისკის ძრავი; 8. მყარი დისკი (HDD); 9. კომპიუტერის კლავიატურა; 10. თავი "მაუსი"

რა არის სისტემური ბლოკი და უნდა ამოვიღოთ თუ არა ის?

„არსებობს კომპიუტერის სისტემური ბლოკის ორი ტიპი: ჰორიზონტალური კორპუსი და ვერტიკალური კორპუსი.“¹⁷³ (სისტემური ბლოკი იხილეთ სურათი N4 და N5);

სამაგიდო პერსონალური კომპიუტერის სისტემური ბლოკი წარმოადგენს კარკასს, რომელშიც განლაგებულია პერსონალური კომპიუტერის კვანძები:

- დედალატა;
- მიკროპროცესორი;
- ადაპტერი;
- ოპტიკური დისკ-ამძრავი (CD-ROM);
- დენის წყარო;
- მყარი დისკი;
- ეპიტერული სიხშირის გადამრთველი;
- ოპერატიული მეხსიერება;
- ვიდეოკარტა;



- ქსელური კარტა;
- ხმის კარტა;
- დინამიკი;
- მართვის ლილაკები;
- და სხვა.¹⁷⁹

„უკანა მხარეს ჩანს „რობოტები“ კაბელების შესაერთებლად (კაბელების შესაერთებლების დაზუსტებული მოცემულობა N5). კვების ბლოკის შიგნით აყენებენ ცენტრალურ პროცესორთან დამაკავშირებელ მოწყობილობებს და გაფართოების პლატებს. კარკასი იხურება სახურავით. ამჟამად ფართოდაა გავრცელებული სისტემური ბლოკის სამი ფორმა: კოშკი (Tower), მინი კოშკი (Mini Tower) და ბრტყელი (Desktop).“¹⁸⁰

„Tower-ის გაბარიტები დიდია და იგი საშუალებას იძლევა მასში მოთავსდეს დიდი რაოდენობის ბლოკები. ხშირ შემთხვევაში მას იატაკზე დებენ;

Mini Tower-ში ძირითადად პლათას ვერტიკალურად აყენებენ, ხოლო შიგ ჩადებულ პლატებს ჰორიზონტალურად;

Desktop-ში სისტემური ბლოკი ყენდება გარკვეული კუთხით. ძირითადი პლატა ყენდება ჰორიზონტალურად, ხოლო მასში დასაყენებელი პლატები — ვერტიკალურად.“¹⁸¹

სურათი N4 სისტემური ბლოკი ;



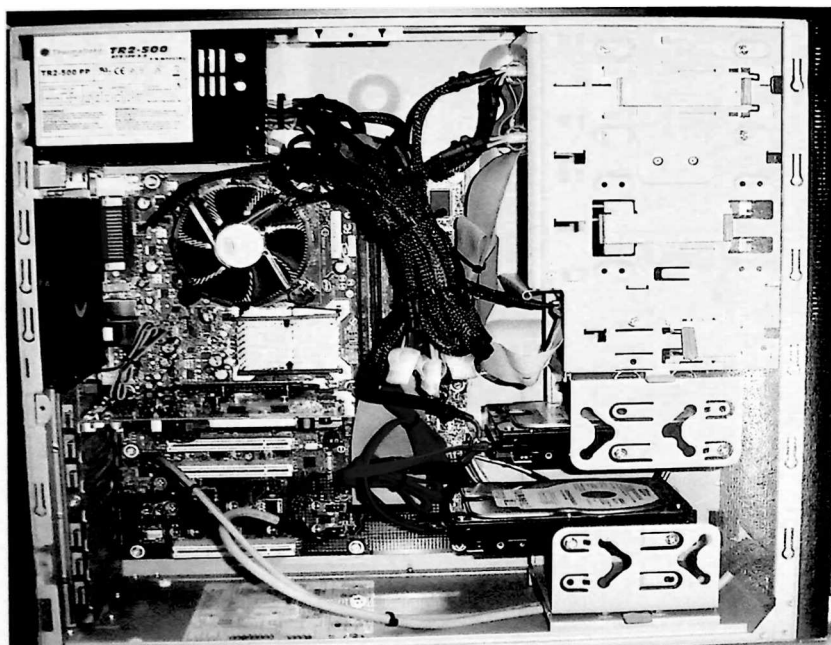
¹⁷⁹ ელ. გევრდი ; ნანახია 12.07.2019



¹⁸⁰ ელ. გევრდი ; ნანახია 12.07.2019



¹⁸¹ იქვე.



ზემოაღნიშნულიდან გამომდინარე, პირველი, რაც გამომძიებლის მიერ უნდა იქნეს ამოღებული ეს არის სისტემური ბლოკი, რომლის შიდა ნაწილებშიც დაცულია შესაბამისი ინფორმაცია და რომელზეც შემდგომში შესაძლებელია ჩაიკრებულ იქნეს ექსპერტიზა.

უნდა ამოიღოს თუ არა გამომძიებელმა კომპიუტერის სხვა მოწყობილობები, როგორიც არის მაუსი ანუ თაგვი, კომპიუტერის ეკრანი და კლავიატურა – ?

კომპიუტერის ეკრანი გათვალისწინებულია ტექსტური და გრაფიკული ინფორმაციის გამოსახვადად. მათ შეუძლიათ იმუშაონ ტექსტურ ან გრაფიკულ რეჟიმში, შესაბამისად ციფრული მტკიცებულების მოპოვების მიზნებისათვის, კომპიუტერის ეკრანის ამოღება, მნიშვნელოვან მონაცემს არ გვაძლევს. გარდა იმ შემთხვევისა, თუ ეკრანიდან არ გვინდა გარკვეული ნიმუშების — ხელის კვლის, გენეტიკური პროფილის ან სხვა აღება, იგივე შეგვიძლია ვთქვათ კომპიუტერის მასზე. ე.წ. თავგზეც.



5.5. ციფრული ინფორმაციის შემნახველი კომპიუტერის ნაწილების ძებნის და ამოღების ტექნიკური პროცედურები და მეთოდები

არის ხოლმე შემთხვევები, როდესაც საგამოძიებო მოქმედება-ჩხრეკაზე, ან ამოღებაზე შესულ თანამშრომლებს, ადგილზე არ ხვდებათ პერსონალური კომპიუტერი, ან ხვდებათ დაშლილ მდგომარეობაში.

მაგალითისათვის: გამოძიებელი ატარებს საგამოძიებო მოქმედება ჩხრეკას ან ამოღებას და სახლში საერთოდ ვერ იქნა ნაპოვნი პერსონალური კომპიუტერი, ან ასეთი ნივთი იქნა ნაპოვნი დაშლილ მდგომარეობაში, ასეთ შემთხვევაში გამოძიებელი ვალდებულია არამართო ამოიღოს დაშლის შედეგად არსებული ნივთები, არამედ მოძებნოს და ამოიღოს ის მთავარი მოწყობილობა, რაზეც ინახება შესაბამისი ინფორმაცია, რაც საქმისთვის არის მნიშვნელოვანი, ზემოაღნიშნული მიზნებისათვის მნიშვნელოვანია განვიხილოთ, კომპიუტერის რა ნაწილი უნდა მოძებნოს და ამოიღოს გამომძიებელმა;

„როგორც უკვე აღვნიშნეთ, საბაზო კონფიგურაციაში შეიძლება გამოიყოს მისი შემდეგი ნაწილები: სისტემური ბლოკი; მონიტორი; კლავიატურა; მაუსი.“¹⁸³

არსებობს კომპიუტერის სისტემური ბლოკის ორი ტიპი: პორიზონტალური კორპუსი და ვერტიკალური კორპუსი. სისტემური ბლოკის ძირითად ელემენტს წარმოადგენს სისტემური პლატა ანუ დედა პლატა.

სისტემური ბლოკი - ეს პერსონალური კომპიუტერის კორპუსია, რომელშიც მოთავსებულია მისი ძირითადი მოწყობილობები, მიუხედავად იმისა, რომ სისტემური ბლოკი ძალიან ბევრ მოწყობილობას მოიცავს ჩვენ ყურადღება გავამახვილოთ გამოძიებისათვის ყურადსაღებ და მნიშვნელოვან მოწყობილობაზე.

სისტემური ბლოკი მოიცავს შემდეგს:

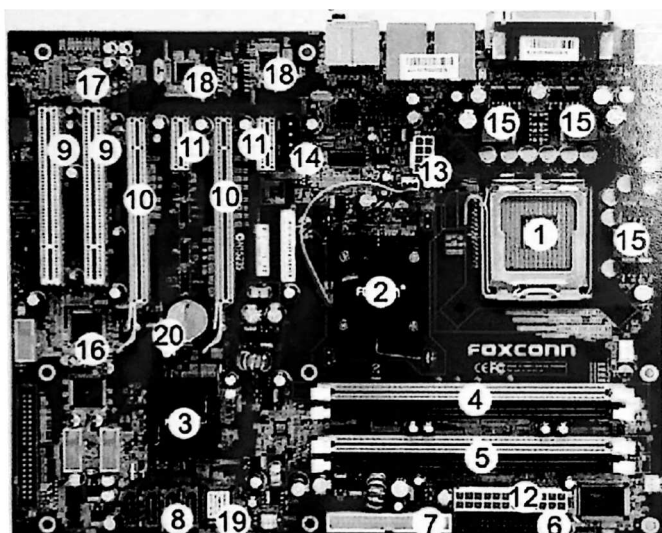
„სისტემური პლატა ანუ დედაპლატა - (System board) წარმოადგენს სისტემური ბლოკის ძირითად ნაწილს, რომელიც განსაზღვრავს კომპიუტერის არქიტექტურასა და მწარმოებლურობას (სურ.16). მას ასევე უწოდებენ დედაპლატას (motherboard), ძირითად ან მთავარ პლატას (main board). მასზე განლაგებულია შემდეგი ძირითადი კომპონენტები: (იხ. სურათი N6 N7 და N8);

- 1 – სოკეტი პროცესორისათვის;
- 2 – ჩრდილოეთის ხიდი;
- 3 – სამხრეთის ხიდი;
- 4,5 – სლოტები მეხსიერების მოდულისათვის;
- 6 – მოქნილი დისკის დისკამძრავი;
- 7 – განსართი ATA100/ATA133 მოწყობილობისათვის;
- 8 – განსართი Serial ATA მოწყობილობისათვის;
- 9 – PCI სლოტები;
- 10 – PCI-Express x16 სლოტები;
- 11 – PCI-Express x1 სლოტები;
- 12 – 24-კონტაქტიანი ATX განსართი კვების ბლოკისათვის;

¹⁸³ კომპიუტერის აგებულება. ელ. გვერდი  ნანახია. 28.07.2019. გვ.1

- 13 – 8-კონტაქტიანი დამატებითი ATX12V განსართი პროცესორისათვის;
- 14 – განსართი ვიდეოკარტის კვებისათვის;
- 15 – ძაბვის სტაბილიზატორი;
- 16 – კონტროლერი ინტერფეისისათვის IEEE 1384 (FireWire);
- 17 – აუდიოკონტროლერი;
- 18 – ქსელური კონტროლერი;
- 19 – BIOS ROM (CMOS);
- 20 – BIOS-ის ბატარეა.¹⁸⁴

სურათი N6 დედაპლათა:



185

.გემოაღნიშნულ აუცილებელ საშუალებებთან ერთად თანამედროვე სისტემური პლატების უმეტესობაზე აყენებენ LPT და COM პორტების ინტერფეისებს, USB პორტებს, ATA არხების წყვილსა და ან 2-4 SATA პორტს, ლოკალური ქსელის ადაპტერს. არსებობენ სისტემური პლატები ინტეგრირებული ვიდეო. აუდიო და სხვა მოწყობილობებით, რომლებიც უზრუნველყოფენ კომპიუტერის სრულ ფუნქციონალობას დამატებითი მოწყობილობების კონტროლერების გარეშე.¹⁸⁶

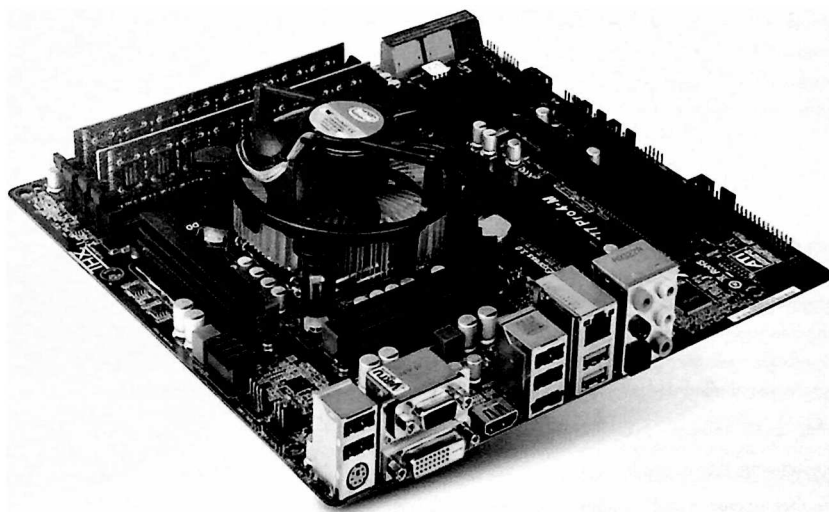
¹⁸⁴ ელ. გვერდი  : ნანახია 22.07.2019

¹⁸⁵ სურათი: იქვე.

¹⁸⁶ ელ. გვერდი:  : ნანახია 22.07.2019

„სისტემურ პლატაზე სხვა კონტროლერების განთავსების მიზანია კომპიუტერზე პლატების საერთო რაოდენობის შემცირება. [...] პირველი პერსონალური კომპიუტერების სისტემური პლატები (პროცესორები 8088/86), პროცესორთან ერთად შეიცავდნენ პერიფერიულ დიდ ინტეგრალურ სქემებს (წყვეტების, მეხსიერებაზე პირდაპირი მიღწევისა და სალტის კონტროლერები) და დამაკავშირებელ ლოგიკას მცირე და საშუალო ხარისხის ინტეგრაციის მიკრო სქემებზე. თანამედროვე პლატები მზადდება ჩიპსეტების საფუძველზე რამდენიმე დიდი ინტეგრალური სქემის ნაკრები, რომლებიც ახდენენ ძირითადი კომპონენტების (პროცესორი, მეხსიერება და გაფართოების პლატები) კავშირების ყველა აუცილებელი ფუნქციის რეალიზებას. ჩიპსეტი განსაზღვრავს სხვადასხვა ტიპის პროცესორების, ძირითადი და ქეშ მეხსიერების, ასევე სისტემის სხვა მახასიათებლების გამოყენების შესაძლებლობას. ჩიპსეტის ტიპი არსებითად ახდენს გავლენას მწარმოებლობაზე ერთნაირი დაყენებული კომპონენტებისას (პროცესორი, მეხსიერება, გრაფიკული ადაპტერი და მყარი დისკი) სხვადასხვა ჩიპსეტებზე აწყობილი კომპიუტერების მწარმოებლურობა შეიძლება 30%-ით განსხვავდებოდეს.“¹⁸⁷

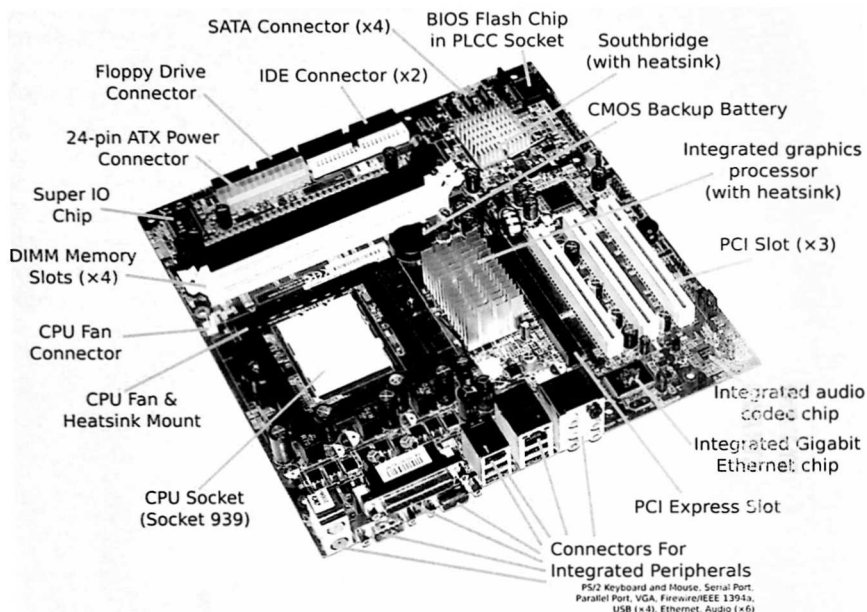
სურათი N7 დედაპლათა:



188

187 იქვე.

188 იქვე.



თუ გამომძიებელს ადგილზე არ დახვდა შესაბამისი სრული კომპიუტერის მოწყობილობა და ჯერი მიდგა დედა პლატის მოძიებაზე, რომელზეც არის დამაგრებული გამომძიებისათვის მნიშვნელოვანი ინფორმაციის მატარებელი ციფრული ინფორმაციის შემცველი მოწყობილობები. გამომძიებელმა უნდა გაითვალისწინოს, რომ დედაპლატა არსებობს 5 სიდიდის და სხვადასხვა ვიზუალის. გთავაზობთ არნიშნულის ჩამონათვალს და თვალსაჩინოებისათვის შესაბამის სურათს, რომელზეც აღწერილია ვიზუალურად ყველა მათგანი:

არსებობს რამდენიმე ზომის დედაპლატა:

სტანდარტული დედაპლატა;

მიკრო დედაპლატა;

მინი დედაპლატა;

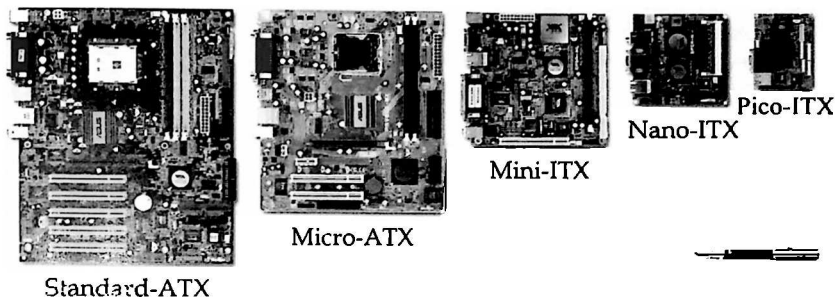
ნანო დედაპლატა;

პოკო დედაპლატა;¹⁹⁰

(ვიზუალური აღწერილობა იხილეთ სურათზე N9)

¹⁸⁹ ელ.გვერდი : ნანახია 10.07.2019

¹⁹⁰ სურათი: იქვე.



„დედა პლატის ბირთვია პროცესორი, იგი დედაპლატაზე ყველაზე დიდი მიკროსქემაა. მის დამიწნეულბას წარმოადგენს ორობით ფორმადში წარმოდგენილი ბრძანებების შესრულება და კომპიუტერის დანარჩენი მოწყობილობებისათვის მმართველი სიგნალების მიწოდება. პროცესორის ყველაზე მთავარ მახასიათებელს მისი სწრაფქმედება წარმოადგენს, რომელიც ხასიათდება სიხშირით, რომლითაც პროცესორი მუშაობს.[...] პროცესორი პირდაპირ კავშირში იმყოფება ოპერატიულ მეხსიერებასთან. პროცესორის მიერ და სამუშაოზე მონაცემები ოპერატიულ მეხსიერებაში იწერება და მოთხოვნის შემთხვევაში პროცესორს მიეწოდება.“¹⁹²

სურათი N10 პროცესორი;



იმ შემთხვევაში თუ გამომძიებლის მიერ ნაპოვნი ვერ იქნება კომპიუტერის სისტემური ბლოკი ან დედაპლატა, გამომძიებელმა უნდა მოიძიოს ერთი მნიშვნელოვანი მოწყობილობა - „ვინჩესტერი“ „[...] ვინაიდან კომპიუტერის გამორთვისას ოპერატიულ მეხსიერებაში მონაცემები იკარგება, ანუ კომპიუტერის ჩართვისას საჭირო პროგრამები თავიდან უნდა ჩაიტვირთოს ოპერატიულ მეხსიერებაში. მაგრამ საიდან? ამისათვის კომპიუტერის შემადგენლობაში უნდა არსებობდეს პროგრამებისა და მონაცემების მუდმივი საცავი, რომელიც ამ ინფორმაციას შეინახავს იმის მიუხედავად, ჩართული იქნება თუ არა კომპიუტერი. ასეთი საცავია მეხსიერების მოწყობილობა მყარ მაგნიტურ დისკზე ანუ ვინჩესტერი.“¹⁹³

„მეხსიერების მოწყობილობა მყარ მაგნიტურ დისკზე ანუ ვინჩესტერი წარმოადგენს დამოუკიდებელ მოწყობილობას და მოთავსებულია სისტემურ ბლოკში. პერსონალური კომპიუტერის ბირთვს ვინჩესტერი უკავშირდება სპეციალური კონტროლერის საშუალებით.“¹⁹⁴

¹⁹¹ სურათი; იქვე.

¹⁹² კომპიუტერის არქიტექტურა. გვ.3. ელ. გერდი  ; ნანახია 11.07.2019.

¹⁹³ კომპიუტერის არქიტექტურა. გვ.3. ელ. გერდი  ; ნანახია 11.07.2019.

¹⁹⁴ იქვე.

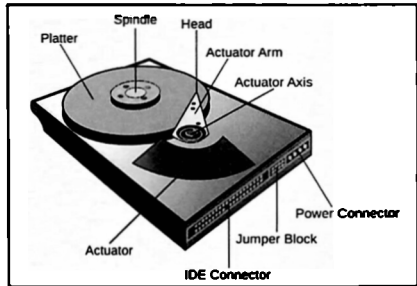
სად არის მოთავსებული ვინჩესტერი?

კონსტრუქციულად ვინჩესტერი მოთავსებულია პერმეტულ კორპუსში. მასში მონაცემების დამახსოვრება ხდება მყარ დისკზე, რომელიც დაფარულია მაგნიტური ნივთიერებით. დისკი ძალიან სწრაფად ბრუნავს. მბრუნავ დისკზე მონაცემების ჩაწერა ან წაკითხვა ხდება სპეციალური მაგნიტური თავაკების საშუალებით, რომლებიც დაგადადგილდებიან დისკის გასწვრივ. ვინჩესტერი სისტემურ ბლოკში ისეა განთავსებული, რომ მომხმარებელს მასთან ფიზიკური შეხება არა აქვს. მასთან მიმართვა შესაძლებელია მხოლოდ პროგრამულად.¹⁹⁵

ვინჩესტერი უმეტესად ხისტად ყენდება პერსონალური კომპიუტერის კორპუსში. იგი რამდენიმე ჩვეულებრივ ორი, ან სამი დისკისაგან შედგება. თუმცა არსებობენ 11 და მეტი დისკისგან შემდგარი მოწყობილობებიც. ინფორმაცია დისკების ორივე მხარეს იწერება. ერთტიპური (ერთმანეთის ქვევით განლაგებული) ბილიკები ცილინდრებად ერთიანდებიან.¹⁹⁶

ვინჩესტერის დისკები, დრეკადი დისკებისგან განსხვავებით, ალუმინის, ან არაკრისტალური მინისაგან (მინისა და კერა მიკის საფუძველზე შექმნილი კომპოზიტური მასალებისაგან) დამზადებულ ფირფიტებს წარმოადგენენ. მათი გადaluწვა შეუძლებელია. ამიტომ ვინჩესტერს ზოგჯერ ხისტ დისკურ მოწყობილობას -HDD, ან ხისტ დისკებზე დამგროვებელსაც უწოდებენ. მინის დისკი უფრო ხისტი და მტკიცეა ალუმინის დისკთან შედარებით და ტემპერატურის ცვლილებების მიმართ ნაკლები მგრძნობიარობით გამოირჩევა.¹⁹⁷

სურათი N11 ვინჩესტერი: ¹⁹⁸ - ¹⁹⁹



შესაბამისად გამოძიების მიერ, იმ შემთხვევაში თუ ადგილზე ვერ იქნება ნანახი კომპიუტერის სრული სისტემური ბლოკი, მოძიებულ და ამოღებულ უნდა იქნეს დედა პლათა და თუ ისიც ვერ იქნა ნაპოვნი, ან ამოღებულ იქნა მისგან ვინჩესტერი, აუცილებელია ნანახი იქნეს აღნიშნულ

¹⁹⁵ კომპიუტერის არქიტექტურა. გვ.3. ელ. გერდი  ; ნანახია 11.07.2019.

¹⁹⁶ იქვე.

¹⁹⁷ კომპიუტერის არქიტექტურა. გვ.3. ელ. გერდი  ; ნანახია 11.07.2019.

¹⁹⁸ ელ. გვერდი  ; ნანახია 12.07.2019

¹⁹⁹ ელ გვერდი  ; ნანახია 12.07.2019

მოწყობილობაც რომელიც იქნება ამოღებული, შესაძლებელია საგამოძიებო მოქმედება ჩხრეკის ჩატარებისას როდესაც საგამოძიებო ორგანოს თანამშრომლები გამოცხადდებიან ადგილზე - დედა პლათა ან ვინჩესტერი სპეციალურად იქნეს ამოღებული ჩხრეკამდე დანაშაულის ჩამდენი პირის ან მისი ახლობელი პირის მიერ, რა შემთხვევაშიც აუცილებლად უნდა ჩატარდეს იმ პირის პირადი ჩხრეკაც, ვინც ადგილზე იმყოფება და მოძიებულ იქნეს ზემოაღნიშნული მოწყობილობები.

5.6. ციფრული ინფორმაციის შემნახველი სხვა მოწყობილობების ძებნის და ამოღების ტექნიკური პროცედურები და მეთოდები

დღეის მდგომარეობით, არსებობს პრაქტიკაში დამკვიდრებული ციფრული ინფორმაციის შემნახველი რამდენიმე კომპიუტერის გარე მოწყობილობა - მესხიერება, რომლებიც ერთმანეთისგან განსხვავდებიან ფორმებით, შენახვის ხარისხით და ზომით, ამიტომ, გამომძიებელმა, რომელიც შევა საგამოძიებო მოქმედებაზე, აუცილებლად უნდა იცოდეს თუ რა ტიპის მესხიერების ბარათი უნდა მოიძიოს, მიუხედავად იმისა, რომ სრული ჩამონათვალი შესაძლოა ვერ შემოგთავაზოთ მისი სიმრავლის გამო, წარმოგიდგენთ პრაქტიკაში დამკვიდრებულ რამდენიმე ციფრული ინფორმაციის შემნახველ გარე მესხიერებას, რომლებიც აუცილებლად უნდა იქნეს მოძებნილი გამომძიებლის მიერ იმ შემთხვევაში, თუ ახდენს კომპიუტერული სისტემის ამოღებას ან ეძებს რაიმე სახის ციფრულ ინფორმაციას.

მაგალითად: გამომძიებელი გადაუღებელი აუცილებლობის საფუძველზე, შევიდა საგამოძიებო მოქმედება ჩხრეკაზე, რა დროსაც აქვს შესაბამისი ინფორმაცია, რომ საცხოვრებელ სახლში არსებულ კომპიუტერულ მოწყობილობაში ინახება ციფრული ინფორმაცია (მტკიცებულება), გამომძიებლის მიერ ამოღებულ იქნა შესაბამისი კომპიუტერი, ეს არ ნიშნავს, რომ გამომძიებელმა დაასრულა საგამოძიებო მოქმედება, მან აუცილებლად უნდა დაძებნოს სხვა მოწყობილობები, რომლებზეც შესაძლოა ჩაწერილ ან გადატანილი არის ციფრული მასალა, ასეთი მტკიცებულება შესაძლოა ან თან ჰქონდეს ადგილზე მყოფ პირს, რა შემთხვევაშიც უნდა ჩატარდეს მისი პირადი ჩხრეკა, რაც უნდა აისახოს საცხოვრებელი სახლის ჩხრეკის ოქმში;

მოწყობილობები, რომლებიც გამომძიებლის მიერ უნდა იქნეს პირვე რიგში მოძიებული არის;

1. მესხიერების ბარათი იგივე "ფლეშკა":

„ინფორმაციის მატარებლებიდან ერთერთ ყველაზე გავრცელებულ მოწყობილობას წარმოადგენს ფლეშ მესხიერება (ფლეშკას რომ უწოდებენ), იგი ძალიან პრაქტიკულია თავისი ფორმისა და ზომიდან გამომდინარე, პირველი ფლეშ მესხიერება შეიქმნა 2000 წელს ამერიკის შეერთებულ შტატებში და მას შეეძლო მხოლოდ 8 მეგაბაიტი ინფორმაციის შენახვა და იმ პერიოდისთვის დაახლოებით 50\$ ღირდა, წლის ბოლოს უკვე გამოჩნდა 16 MB და 32 MB ფლეშ მესხიერებები.“²⁰⁰

„დღეისობით უკვე არსებობს 8GB, 16GB, 32GB და 64 GB და უფრო დიდი ზომის ზომის ფლეშ მესხიერებები, აღნიშნული მესხიერება პრაქტიკულია თავისი ზომიდან გამომდინარე, არის მრავალჯერადი გამოყენებისთვის, ანუ შეგიძლიათ ინფორმაციის განუწყვეტლივ ჩაწერა და წაშლა (ქარხნულად გარანტიიდან გამომდინარე დასაშვებია მინიმუმ 5000 ჩაწერა და წაშლა,



არ საჭიროებს დამატებით მოწყობილობას, რადგან ერთდება USB პორტზე. ფლეშ-დისკის კონსტრუქციული ვარიანტები არსებობს მრავალი: ATA Flash (PC Card ATA); Compact Flash (CF); Smart Media (SM); xD-Picture; MultiMedia Card (MMC); Secure Digital Card (SD); Miniature Card (MiniCard); Memory Stick.²⁰¹ (ფლეშის ნაირსახეობები იხილეთ სურათზე N12, N13, 14, 15 და 16)

სურათი N12 სტანდარტული „ფლეშკა“²⁰²



გასათვალისწინებელია, რომ ფლეშ მეხსიერებას შესაძლოა ჰქონდეს ძალია ბევრი ვიზუალი, ამისათვის მნიშვნელოვანია ჩხრეკის წარმოებისას კარგად იქნეს დაძვნილი მსგავსი მეხსიერების ბარათები, მაგალითისათვის ფლეშკა სამაჩური, ფლეშკა ფლეშკა გელსაკიდი, ფლეშკა საწერკალაში, ფლეშკა პლასტიკური ბარათი და ა.შ. შემდეგ:

²⁰¹ ომარ გაბედავა. კომპიუტერის არქიტექტურა. (სახელმძღვანელო). თბილისი 2008 წელი

²⁰² ნანახია 14.07.2019





203_204



205 _ 206

ე.წ. „გარე ვინჩესტერი“;

„გარე ვინჩესტერი საკმაოდ გავრცელებული მოწყობილობაა, რომლითაც შეიძლება საკმაოდ დიდი ზომის ინფორმაციის გადატანა სხვა კომპიუტერში, იგი წარმოადგენს ჩვეულებრივ ვინჩესტერს, რომელიც კომპიუტერზე ერთდება USB პორტით. მასში მოთავსებულია 2.5" ვინჩესტერები და SA-TA-დან USB-ზე გადაყვანი სქემა.“²⁰⁷

„გარე ვინჩესტერებმა საკმაოდ დიდი გამოყენება ჰპოვეს მოსახლეობაში და მათ იყენებენ ინფორმაციის შესანახად არქივის შექმნის მიზნით, ანუ იმასავე ისეთ ინფორმაციას რომელიც

203  : ნანახია 14.07.2019

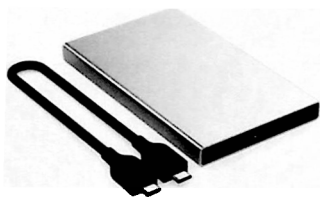
204  : ნანახია 14.07.2019

205 ელ. გვერდი  : ნანახია 14.07.2019

206 ელ. გვერდი:  : ნანახია 14.07.2019

207 ელ. გვერდი  : ნანახია 14.07.2019

ყოველდღიურად არ სჭირდებათ, როგორცაა პირადი ან საოჯახო სურათები, ბავშვების ვიდეო და ასევე სხვადასხვა პროგრამის საინსტალაციო პაკეტები. დღეისობით გაყიდვაში არის 500GB, 750GB, 1TB-იანი და უფრო მეტია იგარე ვინჩესტერები, აღნიშნული მოწყობილობები, პრაქტიკულია; არ საჭიროებს დამატებით მოწყობილობას, რადგან ერთდება USB პორტზე, ინახავს ძალიან დიდი ინფორმაციას²²⁸



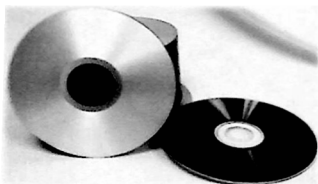
სურათი N17 გარე ვინჩესტერი



ელექტრონული დისკები;

..CD და DVD დისკები შეიძლება იყოს განკუთვნილი მხოლოდ წასაკითხად და ერთჯერადი ან მრავალჯერადი ჩაწერისათვის. კომპაქტდისკებზე შეიძლება დაახლოებით 700 მბ მონაცემის შენახვა, ხოლო DVD დისკის მართვით ერთ მხარეს შეიძლება 8.5 გბ მონაცემის დატევა.”²⁰⁹

(ელექტრონული დისკი იხილეთ სურათზე N18)



ელექტრონული დისკი იხილეთ
სურათი N18²¹⁰

..CD (კომპაქტ დისკი) — დისკოს ფორმის ინფორმაციის ოპტიკური მატარებელი ცენტრში ხვრელით, რომლიდანაც ინფორმაცია ლაზერის დახმარებით იკითხება. თავდაპირველად, კომპაქტ დისკი შეიქმნა აუდიოს ციფრული შენახვისთვის (ე. წ. Audio-CD), მაგრამ დღესდღეობით იგი ფართოდ გამოიყენება, როგორც ფართო დანიშნულების

მქონე მონაცემების მატარებელი მოწყობილობა (ე. წ. CD-ROM). აუდიო კომპაქტ დისკები, როგორც წესი, მონაცემების მატარებელი კომპაქტ დისკებისგან განსხვავდება და ამიტომაც, CD-ფლეიერებს მხოლოდ მათი დაკვრა შეუძლიათ (რა თქმა უნდა, კომპიუტერზე ორივე ტიპის დისკის წაკითხვა შესაძლებელია). არსებობს ისეთი დისკებიც, რომლებზეც ერთდროულად აუდიოინფორმაცია და მონაცემებია ჩაწერილი — მათი მოსმენა შესაძლებელია CD-ფლეიერზე, ხოლო წაკითხვა კომპიუტერზე.”²¹¹

..ოპტიკური დამგროვებლების რამდენიმე ტიპი არსებობს:

CD-ROM - წინასწარ ჩაწერილი კომპაქტდისკი, განკუთვნილი მხოლოდ წასაკითხად;

CD-R - კომპაქტდისკი ერთჯერადი ჩაწერისათვის;

CD-RW - გადასაწერი კომპაქტ-დისკი, რომელზეც მონაცემთა წაშლა და ჩაწერა მრავალჯერაა შესაძლებელი.”²¹²

²²⁸ ელ. გვერდი : ნანახია 14.07.2019

²²⁹ ელ. გვერდი : ნანახია 14.07.2019

²¹⁰ სურათი იხ. ელ. გვერდი : ნანახია 14.07.2019

²¹¹ ელ. გვერდი : ნანახია 03.07.2019

²¹² ელ. გვერდი : ნანახია 14.07.2019

„DVD დისკი;

„DVD (ინგლ. Digital Versatile Disc ან Digital Video Disc – ციფრული ვიდეო დისკი) — ოპტიკური დისკი, განკუთვნილი მედიის ფორმატის მონაცემთა შესანახად, რომელიც მოიცავს ვიდეოფილმებსაც, მაღალი ვიდეო და ხმის ხარისხით. გარეგნულად DVD ესმავასება კომპაქტ დისკებს, ვინაიდან მათი ფიზიკური განზომილებები ერთნაირია (120 მმ ან ზოგიერთ მოდელში 80 მმ დიამეტრით), თუმცა ისინი სხვადასხვა ფორმატში კოდირდება და, ამასთან, DVD-ს გაცილებით მაღალი ტევადობა აქვს.“²¹³

„ოპტიკური დამგროვებლების რამდენიმე ტიპი არსებობს:

DVD-ROM - წინასწარ ჩაწერილი DVD-დისკი, განკუთვნილი მხოლოდ წასაკითხად;

DVD+/- R - DVD-დისკი ერთჯერადი ჩაწერისათვის;

DVD+/-RW - გადასასწერი DVD-დისკი, რომელზეც მონაცემთა წაშლა-ჩაწერა მრავალჯერაა შესაძლებელი.“²¹⁴

ე.წ. Floppy Drive;

„რბილი დისკდამგროვებელი (დისკეტა) ისეთი დამგროვებელია, რომელშიც გამოიყენება 3.5 დუიშის დიამეტრის რბილი დისკები. რბილ მაგნიტურ დისკზე შეიძლება დაეტიოს 720 კბ ან 1.44 მბ მონაცემი. კომპიუტერულ სისტემებში რბილ დისკდამგროვებელს ჩვეულებრივ აღნიშნავენ A: სიმბოლოთი. თუკი იქნება ჩამტვირთავი, დისკეტა შეიძლება გამოვიყენოთ კომპიუტერის ოპერაციული სისტემის გასაშვებად (ჩასატვირთად).“²¹⁵

სურათი N19 Floppy Drive; ²¹⁶



ე.წ. „Zip დისკი“;

„Zip დისკი იყო ფლოპი დისკის მიერ შემუშავებული Iomega დისკის მოწინავე ვერსია - სახელწოდებით Zip დრაივი. Zip დისკები ხელმისაწვდომი იყო 100- და 250 MB-ს შესაძლებლობებში და იყენებდნენ მონაცემთა შენახვის, წილის და გადმოსაწერ მონაცემებს, რაც შეუძლებელი იყო ჩვეულებრივი ფლოპი დისკების გამოყენებით. ახალი და უკეთესი შენახვის შემცველების დანერგვით, როგორიცაა მეხსიერების ჩხირები და DVD-RWs - Zip დისკზე გახდა ნაკლებად მომხრე და საბოლოოდ გაქრა ბაზარზე.“²¹⁷

²¹³ ელ. გვერდი  ნანახია 03.07.2019

²¹⁴ ელ. გვერდი  ნანახია 14.07.2019

²¹⁵ იქვე.

²¹⁶ ელ. გვერდი  ნანახია 14.07.2019

²¹⁷ ელ. გვერდი  ნანახია 14.07.2019



ე.წ. „Memory card“;

„მეხსიერების ბარათი: (ინგლ. Memory card) არის ელექტრონული მოწყობილობა, რომელიც გამოიყენება ციფრული ინფორმაციის შენახვისა და გამოყენებისთვის. ზოგადად, მეხსიერების ბარათი გამოიყენება პორტატულ ელექტრონულ მოწყობილობებში, როგორებიცაა ციფრული კამერები, მობილური ტელეფონები, კომპიუტერები, პლანშეტები, MP3-ფლეიერები და სათამაშო კონსოლები.“ ²¹⁹

„ფიზიკურად არაეობს ამ ბარათის სამი ტიპი — SD, miniSD, MicroSD (ბარათების ტიპები ზომების მიხედვით იხილეთ ფოტოზე №). miniSD-მ უკვე თითქმის დატოვა ბაზარი. დარჩა. SD — ფილიპაპარაგებისთვის, ჩიხი SD — სმარტფონებისთვის, პლანშეტებისთვის, ექშენ-კამერებისთვის და ვიდეორეგისტრატორებისთვის. რა თქმა უნდა არსებობს გამონაკლისებიც, მაგრამ ელექტრონიკის ბაზარზე უმრავლესობა პროდუქტები ამგვარად არის წარმოდგენილი.“ ²²⁰



სურათი N20 Memory card – სხვადასხვა ზომები;



სურათი N21 Memory card – სხვადასხვა ფორმები და ზომები; ²²²

ელ. გვერდი : ნანახია 14.07.2019



ელ. გვერდი : 14.07.2019



ელ. გვერდი : ნანახია 14.07.2019.



ელ. გვერდი : ნანახია 14.07.2019.



ელ. გვერდი : ნანახია 14.07.2019.



სახელწოდება	ფიზიკური ზომა
PC Card	85.6 × 54 × 3.3 მმ.
CompactFlash I	43 × 36 × 3.3 მმ.
CompactFlash II	43 × 36 × 5.5 მმ.
SmartMedia	45 × 37 × 0.76 მმ.
Memory Stick	50.0 × 21.5 × 2.8 მმ.
Memory Stick Duo	31.0 × 20.0 × 1.6 მმ.
Memory Stick PRO Duo	31.0 × 20.0 × 1.6 მმ.
Memory Stick PRO-HG Duo	31.0 × 20.0 × 1.6 მმ.
Memory Stick Micro M2	15.0 × 12.5 × 1.2 მმ.
Miniature Card	37 × 45 × 3.5 მმ.
Multimedia Card	32 × 24 × 1.5 მმ.
Reduced Size Multimedia Card	16 × 24 × 1.5 მმ.
MiniMicro Card	12 × 14 × 1.1 მმ.
P2 card	
Secure Digital card	32 × 24 × 2.1 მმ.
SxS	
Universal Flash Storage	
miniSD card	21.5 × 20 × 1.4 მმ.
microSD card	15 × 11 × 0.7 მმ.
xD-Picture Card	20 × 25 × 1.7 მმ.
Intelligent Stick	24 × 18 × 2.8 მმ.
Serial Flash Module	45 × 15 მმ.
μ card	32 × 24 × 1 მმ.
NT Card	44 × 24 × 2.5 მმ.
XQD card	38.5 × 29.8 × 3.8 მმ.

Sim ბარათი;

SIM ბარათი (SIM ბარათი, ინგლისურიდან. აბონენტის იდენტიფიკაციის მოდული — აბონენტის იდენტიფიკაციის მოდული) — მობილური კავშირგაბმულობის საშუალებით გამოყენებული აბონენტის იდენტიფიკაციის მოდული.²²³

სიმ ბარათის ძირითადი ფუნქციაა ანგარიშის საიდენტიფიკაციო ინფორმაციის შენახვა, რაც აბონენტს საშუალებას აძლევს ადვილად და სწრაფად შეცვალოს ფიჭური მოწყობილობები ან უბრალოდ გადაიტანოს ისინი სხვა ტელეფონზე. ამისათვის SIM ბარათში შედის მიკროპროცესორული პროგრამული უზრუნველყოფა.²²⁵

სიმ ბარათს შეუძლია შემდეგი ინფორმაციის შენახვა;

²²³ ელ. გვერდი  : ნანახია 14.07.2019

²²⁴ ელ. გვერდი  : ნანახია 22.07.2019

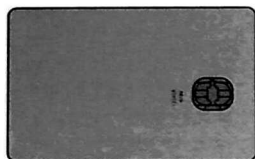
²²⁵ ელ. გვერდი  : ნანახია 22.07.2019

აბონენტის სატელეფონო წიგნი;

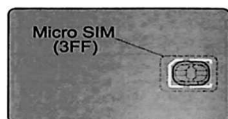
შემომავალი / გამავალი / გამოტოვებული სატელეფონო ზარების სიები;

ტექსტური შემომავალი / გამავალი SMS;

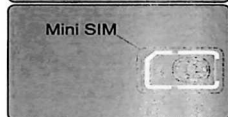
სურათი N22 სიმ ბარათების ზომები;



226



227



არის ხოლმე შემთხვევები, როდესაც თანამედროვე ტელეფონებში ეს მონაცემები სიმ ბარათზე არ ინახება, პირდაპირ ტელეფონის მეხსიერება ინახავს მათ.²²⁸

SIM- ბარათები რამდენიმე ათეული წლის განმავლობაში თანდათანობით შემცირდა, თუმცა მათ შეინარჩუნეს ფუნქციები და თავსებადობა ფორმატის მიუხედავად. თავდაპირველად, ბარათები გაიცემოდა სრულმასშტაბიანი ფორმატით, შემდეგ კი მინი-SIM ფორმატით. 2000-იანი წლებიდან მოყოლებული შემოღებულ იქნა მიკროკარტები, 2010 წლის დასაწყისიდან - ნანო-სიმ-ები.²²⁹

სიმ ბარათის ფორმატი	წელი გამოშვება	სიგრძე (მმ)	სიგანე (მმ)	სისქე (მმ)	მოცულობა (მმ ³)	ფიჭური თაობა
სრული ზომა (1FF)	1991 წ.	85.60	53.98	0.76	3511.72	
მინი-სიმ (2FF)	1996 წ.	25.00	15.00	0.76	285.00	2G, 3G
მიკრო SIM (3FF)	2003 წ.	15.00	12.00	0.76	136.80	3G, 4G
ნანო-სიმ (4FF)	2012 წ.	12.30	8.80	0.67	72.52	3G, 4G
ზაშენებული SIM (ზაშენებული SIM)		6.00	5.00	<1,0		

სრულფასოვანი სიმ ბარათი (86 × 54X0,84 მმ) — არის მოძველებული სტანდარტის ბარათი, რომელიც გამოიყენება ადრეულ მობილურ ტელეფონებში (არის საბანკო ბარათის ზომა);

Mini-SIM- ბარათი (25 × 15X0,76 მმ) — ფართოდ გამოიყენება GSM- ს ტელეფონებში და 3G- ის უმეტეს ტელეფონებში, ძირითადად გამოიყენებოდა 2000-იან წლებში და 2010 წლის დასაწყისში;

მიკრო SIM (3FF) — მინიატურული ალტერნატივა SIM ბარათისთვის, რომელიც შეიქმნა 2003 წელს მობილური მოწყობილობებისთვის აბონენტებისთვის. ბარათის ფიჭური ზომაა 12 × 15 მმ;

²²⁶ ელ. გვერდი : ნანახია 22.07.2019

²²⁷ იქვე.

²²⁸ იქვე.

²²⁹ ელ. გვერდი : ნანახია 22.07.2019

Nano-SIM (4FF) — ის ზომებია 12.3×8.8×0.67 მმ, ფუნქციონირება დაიწყო 2012 წლის ოქტომბერში. ისინი 12% - ით თხელია, ვიდრე ადრე გამოყენებული ვერსია 0.76 მმ.

მრავალსიმიანი ბარათები («Mullisim») არის მოწყობილობები, რომლებსაც აქვთ ჩვეულებრივი SIM ბარათის ფორმა (GSM სტანდარტი) და შედგება მიკროპროცესორული (PIC- პროცესორის PIC16F877) და დამატებითი მეხსიერების მოდული (24C64 - 24C256). მიკროპროცესორი ფუნქციონირებს სპეციალურ ფორმის კონტროლის ქვეშ (SIM-EMU 6.01), რომელიც დამატებით ასრულებს ჩვეულებრივი სიმ ბარათის ფუნქციას.²³⁰

SIM ბარათის PIN კოდი;

როდესაც SIM ბარათი გაიცემა, მას ენიჭება ოთხი ციფრისანი ციფრული PIN კოდი, რომელიც წერილობითია ბარათისთვის და ასევე გადაეცემა აბონენტს ბარათთან ერთად.²³¹

SIM ბარათის ICCID;

ICCID (ინგლისურიდან ინტეგრირებული მიკროსქემის იდენტიფიკატორი) - სიმ-ბარათის უნიკალური სერიული ნომერი. როგორც წესი, ეს კოდი იბეჭდება SIM ბარათზე. ICCID განისაზღვრება ITU-T E.118 სტანდარტის შესაბამისად [8]. ამ სტანდარტის შესაბამისად, ICCID არის 19 ციფრი (ძველი SIM ბარათების ICCID შეიძლება იყოს 20 ციფრისანი):

2 ციფრი - ძირითადი მრეწველობა იდენტიფიკატორი (ინდუსტრიის იდენტიფიკატორი, ISO / IEC 7812-1), SIM ბარათებისთვის ყოველთვის 89;

1-3 ციფრი — სატელეფონო ქვეყნის კოდი (E.164), 7 რუსეთისთვის, 380 უკრაინისთვის და ა.შ.

1-4 ციფრი — ემიტენტის კოდი (ამ და ბოლო დარგების მთლიანი საერთო სიდიდე არ უნდა აღემატებოდეს 5 ციფრს);

11 ან მეტი ციფრი — ოპერატორის მიერ შიდა წესების მიხედვით ბარათის წარმოებაში განსაზღვრული ნომერი;

1 ციფრი (ბოლო) არის მთლიანი რიცხვი, რომელიც გამოითვლება მთვარის ალგორითმის მიერ ყველა სხვა ნომრიდან.²³²

პლასტიკური ბარათი;

„პლასტიკური ბარათი არის ორი სახის: სადებეტო და საკრედიტო;

სადებეტო ბარათზე მომხმარებელს შეუძლია საკუთარი თანხის განთავსება. ძირითადად ბარათზე ოთხი სხვადასხვა ვალუტის ანგარიშია მიბმული: ლარი, აშშ დოლარი, გირვანქა სტერლინგი და ევრო. შესაძლებელია რომელიმე სხვა ვალუტის დამატებაც. საქართველოში ძირითადად Visa ან Mastercard ტიპის ბარათები გამოიყენება. პლასტიკური ბარათით შესაძლებელია ნებიერი სახის საბანკო ოპერაციის წარმოება — თანხის ჩარიცხვა, განაღდება, გადახდა, კონვერტაცია და ა.შ. თითქმის ყველა ბანკის ბარათით სარგებლობისას გადასახდელი ანგარიშის მომსახურების ყოველთვიური საკომისიო და ბარათის წლიური ღირებულება. საკომისიოს მოცულობა განსხვავებულია და დამოკიდებულია ბარათის ტიპზე, მომხმარებლის სახელუფასო პირობებზე და სხვა.“²³³

²³⁰ ელ. გვერდი : ნანახია 22.07.2019

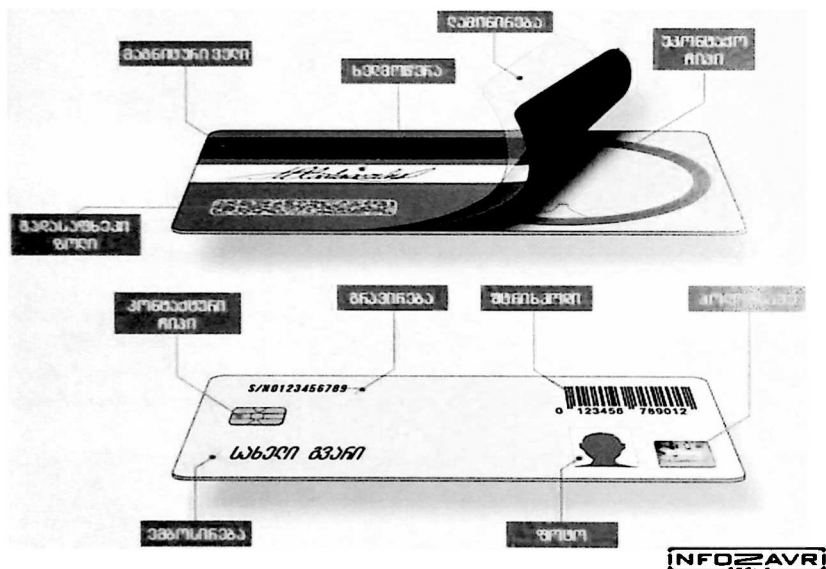
²³¹ იქვე.

²³² იქვე.

²³³ ელ. გვერდი : ნანახია 22.07.2019

„საკრედიტო ბარათი არის ორი საბანკო პროდუქტის — პლასტიკური ბარათისა და სამომხმარებლო სესხის სინთეზი. ეს არის საბანკო პროდუქტი, რომელიც მომხმარებელს საშუალებას აძლევს სავაჭრო ობიექტში საბანკო კრედიტით შეიძინოს საქონელი ან მომსახურება, ასევე ინტერნეტით. და/ან ბანკომატის მეშვეობით გაანაღდოს თანხა.“²³⁴

სურათი N23 პლასტიკური ბარათის აგებულება:



ID ბარათი - მოქალაქის პირადობის ელექტრონული მოწმობა;

„ნომინალური ზომები ID-1 ზომის ბარათისთვის: სიგანე: 85,60 მმ (85,47 მმ – 85,72 მმ, ISO/IEC 7810), სიგრძე: 54,00 მმ (53,92 მმ – 54,03 მმ, ISO/IEC 7810), სისქე: 0,80 მმ (0,76 მმ – 0,84 მმ, ISO/IEC 7810), კუთხე: 3,18 მმ (2,88 მმ – 3,48 მმ, ISO/IEC 7810). მოწმობის კიდის ამობურცვები არ უნდა აღემატებოდეს 0,08 მმ მოწმობის ძირითადი ზედაპირიდან.“²³⁵

„მოწმობას გააჩნია ორი მიკროსქემა (ინფორმაციის ელექტრონული მატარებელი) – კონტაქტური და უკონტაქტო;

კონტაქტური მიკროსქემა წარმოადგენს — „[...] ინფორმაციის ელექტრონულ მატარებელს, რომელიც უნდა აკმაყოფილებდეს საქართველოს იუსტიციის მინისტრის № 91 ბრძანებით

²³⁴ ელ. გვერდი  ნანახია 22.07.2019

²³⁵ ელ. გვერდი 

²³⁶ საქართველოს იუსტიციის მინისტრის ბრძანება № 91 2011 წლის 14 ივლისი, კონსოლიდირებული 14.07.2011. მუხლი 1-ლი ნაწილი მე-2;

დადგენილ მოთხოვნებს".²³⁷ „[...] ISO/IEC 7816-ის შესაბამისად კონტაქტური მიკროსქემა უნდა შეიცავდეს პროცესორს და კოპროცესორს, მეხსიერებას, კონტაქტურ ინტერფეისს“²³⁸

უკონტაქტო მიკროსქემა უნდა უზრუნველყოფდეს სხვადასხვა საქართველოს იუსტიციის მინისტრის № 91 ბრძანებით განსაზღვრულ ალგორითმებს.“

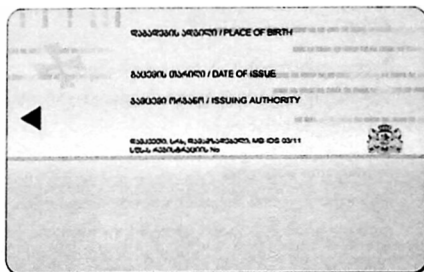
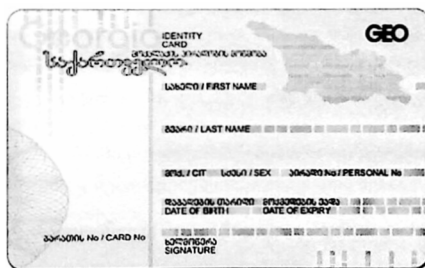
მოწმობა უნდა შეიცავდეს:

- | | |
|---------------------------------|---|
| ა) სახელს; | ბ) გვარს; |
| გ) სქესს; | დ) მოქალაქეობას; |
| ე) დაბადების თარიღს; | ვ) დაბადების ადგილს; |
| ზ) პირად ნომერს; | თ) ფოტოსურათს; |
| ი) პირად ხელმოწერას; | კ) მოწმობის გამცემი ორგანოს დასახელებას; |
| ლ) მოწმობის გაცემის თარიღს; | მ) მოწმობის მოქმედების ვადას; |
| ნ) ავთენტიფიკაციის სერტიფიკატს; | ო) ციფრული ხელმოწერის სერტიფიკატს. ²³⁹ |

მოწმობას გააყენა ინდივიდუალური ნომერი; რომელიც „გრაფიკებულია (ამოტვიფრულია) როგორც «OCR-B.tif» 2 მმ ზომის სიმბოლოებით. გამოყენებულია 9-ნიშნა რიცხვი.“²⁴⁰

„მოწმობის ინდივიდუალური ნომრის ნიმუში: 001A00001. პირველი ორი ციფრი – გამოშვების წელი; შემდეგი ორი სიმბოლო (სერია) – ასობის კომბინაცია (მაგალითად, AA) გარდა კომბინაციებისა PR და TR, შემდეგი (ბოლო) ხუთი ციფრი – რიგითი ნომერი 00001-დან 99999-მდე სერიის ფარგლებში (მაგალითად, 12345), გარდა კომბინაციებისა 666XX, X666X, XXX666.“²⁴¹

სურათი N24 ID ბარათი;²⁴²



²³⁷ იქვე. მუხლი მე-5;

²³⁸ იქვე.

²³⁹ საქართველოს იუსტიციის მინისტრის ბრძანება № 91 2011 წლის 14 ივლისი, კონსოლიდირებული 14.07.2011. მუხლი მე-7;

²⁴⁰ იქვე. მუხლი მე-4;

²⁴¹ იქვე.

²⁴² იქვე.

5.7. კომპიუტერული მოწყობილობის ამოღებისათვის საჭირო აღჭურვილობა და შეფუთვის და გადატანის დროს გასათვალისწინებელი საკითხები

სპეციალური საშუალებები და აღჭურვილობა შეიძლება იყოს საჭირო ელექტრონული მტკიცებულების შესაგროვებლად. ტექნოლოგიურმა წინსვლებმა შეიძლება პრაქტიკაში დამკვიდრებული საშუალებებისა და აღჭურვილობის შეცვლა მოითხოვოს. შესაბამისი აღჭურვილობა/ ძირითადი საშუალებების ნაკრები შესაძლოა, გამოსადეგი იყოს ჩხრეკისა და ამოღებისას და ამ აღჭურვილობით ჯგუფის წევრების უზრუნველყოფა უნდა მოხდეს ჯგუფის იმ წევრის მიერ, რომელიც ლოკისტიკაზე პასუხისმგებელი, (აღნიშნულ პარაგრაფზე მუშაობისას რი შემთხვევებში გამოყენებულია სახელმძღვანელოში „ელექტრონული მტკიცებულების ამოღება“ ვერსია 1.01 (15.12.2003) - მოცემული რეკომენდაციები);

დემონტაჟისათვის საჭირო მოწყობილობები:

ბრეცელენები;

სახრახნისები;

ხელთათმანები;

სკოჩი;

შემთხვევის ადგილის დასაფიქსირებლად საჭირო მოწყობილობები;

წებოვანი ფურცლები;

ფერადი ფლომასტერი ან მარკერი;

სხვადასხვა სახის დასალუქი საშუალებები;

ფოტო ან და ვიდეოკამერა.

შეფუთვისათვის საჭირო ხელსაწყოები:

ანტისტატიკური ჩანთები - გასათვალისწინებელია რომ არ უნდა იყოს გამოყენებული პოლიეთილენის ჩანთები;

შესაფუთი მასალა:

მტკიცებულების შესანახი ჩანთები და ლენტები;

დისკეტების შესანახი ყუთები, რომელთა შორისაც აურნდა იყოს დასალუქად გამოყენებული პენოპლასტი ან პენოპლასტის მსგავსი მასალა;

ბრტყელი კორპუსის შესაგროვებელი ყუთები ან მყარი ყუთები, სხვადასხვა ზომის (საკუთარი შესაფუთი მასალა უნდა იქნას გამოყენებული, როდესაც ეს შესაძლებელია); საკომუნიკაციო საშუალებები;

მობილური ტელეფონი ან მტკიცებულების მოსაპოვებლად კომუნიკაციის სხვა საშუალებები (კომპიუტერულ აღჭურვილობასთან ახლოს არ უნდა იყოს გამოყენებული); დახმარებისთვის საკონტაქტო ინფორმაცია (მაგ., საექსპერტო დანაყოფის ტელეფონის ნომრები);

სხვა ნივთები:

ჩიბის ფანარი სამაგრიტ;

ხელთათმანი;

ხელის ურიკა;

დიდი ზომის რეზინის შესაფუთი საშუალებები;

ლუპა;

ტრანსპორტი (დანაშაულის ადგილამდე და იქიდან, ჯგუფის წევრებისთვის, ამოღებისთვის საჭირო ინსტრუმენტები და აღჭურვილობა, და ამოღებული მტკიცებულებები).²⁴³

შეფუთვა, გადატანა და შენახვა;

„კომპიუტერები და მასთან დაკავშირებული მოწყობილობა და აღჭურვილობა ადვილად დაზიანებადი ელექტრონული ინსტრუმენტებია, რომლებიც ტემპერატურებს, ტენიანობას, ფიზიკურ შოკს, სტატიკური ელექტრო ენერგიის, მაგნეტურ წყაროებს და ზოგიერთ მოქმედებასაც კი ცუდად უძლებენ (მაგ., ჩართვა/გამორთვა). შესაბამისად, სპეციალური სიფრთხილის ზომების გამოყენება უნდა მოხდეს ელექტრონული მტკიცებულების შეფუთვის, გადატანისა და შენახვისას. მტკიცებულების შენახვის პროცესის დასაცავად შეფუთვა, და შენახვა ადეკვატურად უნდა იყოს დაფიქსირებული.“²⁴⁴

გადატანა;

„ზოგადად კომპიუტერის ყველა კომპონენტი და შენახვის საშუალება განსაკუთრებული სიფრთხილით უნდა იყოს დამუშავებული, რადგან არა ექსპერტულმა მოპყრობამ შესაძლოა, ელექტრონული მტკიცებულების დაზიანება ან განადგურება გამოიწვიოს.“²⁴⁵

შეფუთვა;

„შეგროვებული ყველა ელექტრონული მტკიცებულების შესაბამისი დოკუმენტირება და იარაღიყით აღნიშვნა უზრუნველყავით შეფუთვამდე;

როდესაც ეს შესაძლებელია, მოგროვებული ელექტრონული მტკიცებულება საკუთარ (თავდაპირველ) შესაფუთ საშუალებებში გადაიტანეთ;

თუ საკუთარი (თავდაპირველი) შესაფუთი საშუალებები ხელმისაწვდომი არ არის, ისარგებლეთ ანტისტატიკური შეფუთვით (მაგ., ქაღალდის ან ანტისტატიკური პლასტიკური ჩანთები). მოერიდეთ იმ მასალის გამოყენებას, რომელსაც სტატიკური ელექტრო ენერგიის წარმოქმნა შეუძლია, როგორცაა სტანდარტული ცელოფნის პარკები.

არ მოკეცოთ, მოლუნოთ, ან დაჩხაპნოთ მონაცემთა შენახვის საშუალებები, როგორებიცაა დისკეტები და ფირები;

არ მიაშვაროთ დასაწებელი იარაღიყები მონაცემთა შენახვის საშუალებების ზედაპირზე. როდესაც შესაძლებელია, მონაცემთა შენახვის საშუალებების შესაფუთად გამოიყენეთ ყუთები ან კონვერტები;

უზრუნველყავით, რომ მტკიცებულებების შემცველ ყველა შეკვრას შესაბამისი იარაღიყი ჰქონდეს;

თუ რამდენიმე კომპიუტერული სისტემა ამოღებული, თითოეული სისტემა შეფუთეთ და მათ იარაღიყი ისე მიაკარით, რომ მათი ხელახალი შეგროვება შესაძლებელი იყოს ისევე, როგორც მოხდა მათი აღმოჩენა.“²⁴⁶

²⁴³ „ელექტრონული მტკიცებულების ამოღება“ ვერსია 1.01 (15.12.2003);

²⁴⁴ „იქვე“.

²⁴⁵ იქვე.

²⁴⁶ „ელექტრონული მტკიცებულების ამოღება“ ვერსია 1.01 (15.12.2003);

გადატანა;

„ელექტრონული მტკიცებულებები მაგნიტური წყაროებისგან შორს შეინახეთ. რადიო გადაცემები, სპიკერების მაგნიტები და გათბობადი სკამები იმ საგნების მაგალითებია, რომლებმაც შეიძლება ელექტრონული მტკიცებულება დააზიანონ;

ალტურვილობის დაცვა უზრუნველყავით შოკისა და დარტყმებისგან (ანუ, მექანიკური დაზიანება), სიცხისა და ტენიანობისგან;

მეფუთვის გარეშე გადატანილი კომპიუტერებისა და სხვა მოწყობილობების მანქანაში შოკისა და გადაჭარბებული ვიბრაციისგან დაცვა უზრუნველყავით. მაგალითად, კომპიუტერები მანქანის იატაკზე უნდა იყოს დადებული, ხოლო მონიტორები ეკრანით ქვემოთ მანქანის სკამზე, და ღვედით დაბმული;

მძიმე საგნები არ დადოთ ალტურვილობის/მონაცემთა შესანახი საშუალების უფრო პატარა ზომის საგნებზე;

როდესაც შესაძლებელია, ელექტრონული მტკიცებულება არ შეინახოთ ავტომობილში დიდხანს.²⁴⁷

შენახვა;

„მტკიცებულების ინვენტარიზაცია მოახდინეთ შესაბამის წესების მიხედვით;

მტკიცებულება უსაფრთხო ადგილას შეინახეთ, გადაჭარბებული ტემპერატურისა და ტენიანობისგან მოშორებით;

დაიცავით ის მაგნიტური წყაროებისგან, ნესტისგან, მტერისგან, და სხვა დამაზიანებელი მოვლენებისგან;

გამოიყენეთ ადეკვატური დაცული შესანახი ოთახი, სადაც შესვლაზე შესაბამისი კონტროლი იქნება დაწესებული, რომელიც დაცული იქნება ცეცხლისგან (მაგ., იქნება ცეცხლის გამაფრთხილებელი სირენა, ცეცხლის ჩამაქრობელი მოწყობილობა, შენახვის ადგილას ან მის მიმდებარე ტერიტორიაზე მოწვევა არ უნდა შეიძლებოდეს), სადაც გაცონტროლებული იქნება ემპერატურა და ტენიანობა, და რომელიც დაცული იქნება მაგნიტური წყაროებისგან (მაგ., მართვადი რადიო მოწყობილობებიდან შორს);

არ შეინახოთ არანაირი აალეხადი ნივთი იმავე ოთახში, ან ამ ოთახთან ახლოს (მაგ., სარეცხი საშუალებები, ქაღალდის შეკვრა);

გამოიყენეთ იატაკის შესატყვისი საფარი და ერიდეთ (ელექტრო) სტატიკურ დატენვას;

არ შეინახოთ ელექტრონული მტკიცებულება ოთახში, სადაც არის წყლის მიღები, განსაკუთრებით ჭერში;

გაითვალისწინეთ, რომ შესაძლო მტკიცებულება, როგორიცაა თარიღი, დრო და სისტემის კონფიგურაცია შეიძლება დაიკარგოს ხანგრძლივი შენახვის შედეგად. რადგან ელემენტებს შეზღუდული აქვთ მოქმედების პერიოდი, მათი დაჯდომის შედეგად შესაძლოა, მონაცემები დაიკარგოს. შესაბამის პერსონალს უნდა ეცნობოს, რომ ალტურვილობა, რომელიც მუშაობს ელემენტებით/ბატარეით გადაუდებელ ყურადღებას საჭიროებს.“²⁴⁸

„ზოგადი ინსტრუქციები“

ელექტრონული მტკიცებულებების ამოღებისას გასათვალისწინებელი უნდა იყოს შემდეგი;

თუ მოწყობილობა ჩართულია, არ გამოერთოთ ის, რადგან გამორთვამ შესაძლოა, დაბლოკვის შექანში ააშუშავოს;

²⁴⁷ „ელექტრონული მტკიცებულების ამოღება“ ვერსია 1.01 (15.12.2003);

²⁴⁸ „ელექტრონული მტკიცებულების ამოღება“ ვერსია 1.01 (15.12.2003);

ეკრანზე გამოტანილი ინფორმაცია ფოტოგადაღებით დააფიქსირეთ (თუ ასეთი არის) და ჩაიწერეთ ნაჩვენები ინფორმაცია;

მოსხენით ელექტრო ენერგიის მიმწოდებელი ყველა კაბელი (ჩვეულებრივ, ჯოხია მათი სამიზნე ალტერნატივიდან გამოთიშვა, ნაცვლად შტეფსელიდან გამორთვისა);

არ შეეცადოთ შიდა მეხსიერების ან მონაცემთა რომელიმე შენახვის საშუალების წვდომას; თუ ის გამორთულია, არ ჩართოთ, რადგან ამან შესაძლოა მტკიცებულება შეცვალოს/განადგუროს (როგორც კომპიუტერულ სისტემებში;

გამორთეთ ყველა ტელეფონის ხაზი კედლიდან და არ გამოაერთოთ მოწყობილობიდან, რის შემდეგ მოახდინეთ მისი დოკუმენტირება და იარაღით აღნიშვნა;

მნიშვნელოვანი ინფორმაცია შეაგროვეთ/ჩაიწერეთ;

შეაგროვეთ სახელმძღვანელოები და სხვა ინსტრუქციები, თუ ასეთია. ჩაიწერეთ შესაბამისი მონაცემები (მაგ., ტელეფონის ნომერი);

ამოღების შემდეგ, გადაეცით მოწყობილობა ექსპერტს რაც შეიძლება სწრაფად. ჯიბის კომპიუტერებისა (PDA-ების) და მობილური ტელეფონების შემთხვევაში ეს გადაუდებლად უნდა მოხდეს.”²⁴⁹

თავი VI კომპიუტერული სისტემიდან ციფრული ინფორმაციის გამოთხოვის ტექნიკა და მეთოდика

6.1. კომპიუტერული სისტემიდან ციფრული ინფორმაციის გამოთხოვის ზოგადი სამართლებრივი საფუძვლები და პროცედურები

საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლის თანახმად: „თუ არსებობს დასაბუთებული ვარაუდი, რომ კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში ინახება სისხლის სამართლის საქმისათვის მნიშვნელოვანი ინფორმაცია ან დოკუმენტი, პროკურორი უფლებამოსილია გამოძიების ადგილის მიხედვით სასამართლოს მიმართოს შესაბამისი ინფორმაციის ან დოკუმენტის გამოთხოვის განჩინების გაცემის შუამდგომლობით.“²⁵⁰ აღნიშნული მუხლიდან ძალადაკარგულად იქნა ცნობილი 136-ე მუხლის პირველი და მე-4 ნაწილების ის ნორმატიული შინაარსი, რომელიც გამორიცხავს დაცვის მხარის მიერ კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში შენახული ინფორმაციის ან დოკუმენტის გამოთხოვის შესახებ განჩინების გაცემის შუამდგომლობით სასამართლოსათვის მიმართვას. ასევე თუ არსებობს დასაბუთებული ვარაუდი, რომ პირი დანაშაულებრივ ქმედებას ახორციელებს კომპიუტერული სისტემის გამოყენებით. პროკურორი უფლებამოსილია გამოძიების ადგილის მიხედვით სასამართლოს მიმართოს მომსახურების მომწოდებლისაგან მომხმარებლის შესახებ არსებული ინფორმაციის გამოთხოვის განჩინების გაცემის შუამდგომლობით. ხოლო ამ მუხლის მიზნებისათვის, მომხმარებლის შესახებ არსებული ინფორმაცია არის ნებისმიერი ინფორმაცია, რომელსაც მომსახურების მომწოდებელი ინახავს კომპიუტერული მონაცემების ან ნებისმიერი სხვა ფორმით, რომელიც დაკავშირებულია მისი მომსახურების მომხმარებლებთან, განსხვავდება ინტერნეტრაფიკისა და შინაარსობრივი მონაცემებისაგან და რომლის მიხედვითაც შესაძლებელია დადგინდეს/განისაზღვროს:

- ა) გამოყენებული კომუნიკაციის მომსახურების ტიპი, გამოყენებული ტექნიკური საშუალებები და მომსახურების დრო;
- ბ) მომხმარებლის ვინაობა, საფოსტო ან საცხოვრებელი მისამართი, ტელეფონის და სხვა საკონტაქტო ნომრები, ანგარიშისა და გადასახადების შესახებ ინფორმაცია, რომელიც ხელმისაწვდომია მომსახურების ხელშეკრულების ან შეთანხმების საფუძველზე;
- გ) დამონტაჟებული საკომუნიკაციო აღჭურვილობის ადგილმდებარეობის თაობაზე არსებული ნებისმიერი სხვა ინფორმაცია, რომელიც ხელმისაწვდომია მომსახურების ხელშეკრულების ან შეთანხმების საფუძველზე.“²⁵¹

აქვე უნდა აღინიშნოს, რომ ზემოაღნიშნულ საგამოძიებო მოქმედებებზე კანონმდებლობით ვრცელდება ფარული საგამოძიებო მოქმედების ჩატარების წესი (რაზეც დეტალურად იქნება საუბარი ქვემოთ).

საქართველოს სსსკ-ის 136-ე მუხლის მე-4 ნაწილის თანახმად, 2017 წლის 27 იანვრამდე ინფორმაციის გამოთხოვის შესაძლებლობის დაყენების საშუალება ჰქონდა მხოლოდ პროკურორს,

²⁵⁰ საქართველოს სისხლის სამართლის საპროცესო კოდექსი (რედ. 09/10/2009, კონსოლიდირებული 29.05.2019). მუხლი 136

²⁵¹ საქართველოს სისხლის სამართლის საპროცესო კოდექსი (რედ. 09/10/2009, კონსოლიდირებული 29.05.2019).

მაგრამ საქართველოს საკონსტიტუციო სასამართლოს გადაწყვეტილების²⁵² საფუძველზე, საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლის 1-მა ნაწილმა დაკარგა მისი ნორმატიული შინაარსი რომლის თანახმადაც, დაცვის მხარეს არ შეეძლო ასეთი საგამოძიებო მოქმედების ჩატარება. საკითხი - თუ რატომ არ შეეძლო დაცვის მხარეს მსგავსი უფლებით სარგებლობა, მდგომარეობდა მასში, რომ კომპიუტერული სისტემიდან ინფორმაციის გამოთხოვა ხდებოდა და გარკვეულწილად დღესაც ხდება ფარული საგამოძიებო მოქმედების ფარგლებში, რაც გულისხმობს შემდგომს;

თუ შეიქმნება დასაბუთებული ვარაუდი, ანუ ფაქტების და ინფორმაციის საკმარისი ერთობლიობა, რომელიც დაარწმუნებს ობიექტურ პირს, რომ კონკრეტულ კომპიუტერულ სისტემაში ინახება საქმისათვის მნიშვნელოვანი ინფორმაცია, მაშინ პროკურორი და არა გამომძიებელი უფლებამოსილია მიმართოს სასამართლოს შუამდგომლობით აღნიშნული ინფორმაციის გამოთხოვნის მოცივით, მაგრამ ამისათვის დასაბუთებულ ვარაუდთან ერთად პროკურორმა უნდა დაუმტკიცოს სასამართლოს, რომ დაკმაყოფილებულია რიგი სამართლებრივი მოთხოვნები, კერძოდ აღნიშნული ინფორმაციის გამოთხოვა [...] „აუცილებელია დემოკრატიულ საზოგადოებაში ლეგიტიმური მიზნის მისაღწევად — ეროვნული უშიშროების ან საზოგადოებრივი უსაფრთხოების უზრუნველსაყოფად, უწესრიგობის ან დანაშაულის ჩადენის თავიდან ასაცილებლად, ქვეყნის ეკონომიკური კეთილდღეობის ინტერესების ან სხვა პირთა უფლებებისა და თავისუფლებების დასაცავად“²⁵³.

მაგრამ ნიშანდობლივია, რომ ყველა ტიპის დანაშაულზე მსგავსი შუამდგომლობის დაყენება პროკურორს არ შეუძლია, პროკურორს უფლება აქვს მიმართოს მხოლოდ 3 შემთხვევაში;

„თუ გამოძიება დაწყებულია ან/და სისხლისსამართლებრივი დევნა ხორციელდება განზრახი მძიმე დანაშაულის ჩადენის ფაქტზე, ანუ თუ მუხლი რომლითაც წარმოებს გამოძიება ან/და სისხლისსამართლებრივი დევნა არის განზრახი დანაშაული“²⁵⁴ და ამასთან ერთად სასჯელის სახით ითვალისწინებს თავისუფლების აღკვეთას ვადით 5-დან 10 წლამდე;

თუ გამოძიება დაწყებულია ან/და სისხლისსამართლებრივი დევნა ხორციელდება განსაკუთრებით მძიმე დანაშაულის ჩადენის ფაქტზე, ანუ თუ მუხლი რომლითაც წარმოებს გამოძიება ან/და სისხლისსამართლებრივი დევნა სასჯელის სახით ითვალისწინებს თავისუფლების აღკვეთას 10 წელზე მეტი ვადით ან უვადოდ.

ან თუ გამოძიება დაწყებულია ან/და სისხლისსამართლებრივი დევნა ხორციელდება

²⁵² გადაწყვეტილება № 1/1/650.699. 2017 წლის 27 იანვარი

²⁵³ საქართველოს სისხლის სამართლის საპროცესო კოდექსი (რედ. 09/10/2009, კონსოლიდირებული 29.05.2019). მუხლი 1432

²⁵⁴ საქართველოს სისხლის სამართლის კოდექსი (რედ. 22/07/1999, კონსოლიდირებული 25.09.2019) მუხლი 9. განზრახი დანაშაული

1. განზრახ დანაშაულად ითვლება ქმედება, რომელიც ჩადენილია პირდაპირი ან არაპირდაპირი განზრახვით.
2. ქმედება პირდაპირი განზრახვითაა ჩადენილი, თუ პირს გაცნობიერებული ჰქონდა თავისი ქმედების მართლწინააღმდეგობა, ითვალისწინებდა მართლსაწინააღმდეგო შედეგის დადგომის შესაძლებლობას და სურდა ეს შედეგი, ანდა ითვალისწინებდა ასეთი შედეგის განხორციელების გარდაუვალობას.
3. ქმედება არაპირდაპირი განზრახვითაა ჩადენილი, თუ პირს გაცნობიერებული ჰქონდა თავისი ქმედების მართლწინააღმდეგობა, ითვალისწინებდა მართლსაწინააღმდეგო შედეგის დადგომის შესაძლებლობას და არ სურდა ეს შედეგი, მაგრამ შეგნებულად უშვებდა ან გულგრილად ეკიდებოდა მის დადგომას.

საქართველოს სისხლის სამართლის კოდექსის შემდეგი მუხლებითა და თავით გათვალისწინებული რომელიმე დანაშაულის გამო:

საქართველოს სსკ-ის 134-ე მუხლი;

1. სამკურნალოდ, გადასანერგად, ექსპერიმენტისათვის ან სამკურნალო პრეპარატის დასამზადებლად ადამიანის ორგანოს, ორგანოს ნაწილის ან ქსოვილის აღების იძულება;
2. იგივე ქმედება, ჩადენილი დამნაშავისათვის წინასწარი შეცნობით ორსული ქალის, არასრულწლოვნის, უმწეო მდგომარეობაში მყოფის ანდა დამნაშავეზე მატერიალურად ან სხვაგვარად დამოკიდებულის მიმართ."

საქართველოს სსკ-ის 139-ე მუხლის მე-2 ნაწილი;

„პირის სხეულში სექსუალური ხასიათის შეღწევის ან სექსუალური ხასიათის სხვაგვარი ქმედების იძულება, ჩადენილი ქონებრივი დაზიანების, სახელის გამტეხი ინფორმაციის, პირადი ცხოვრების ამსახველი ინფორმაციის ან ისეთი ცნობის გახმაურების მექანიზმით, რომელმაც შეიძლება არსებითად დაზიანოს ამ პირის უფლება, ანდა დაზარალებულის უმწეობის ან მატერიალური, სამსახურებრივი ან სხვაგვარი დამოკიდებულების გამოყენებით — რამაც გამოიწვია დაზარალებულის ჯანმრთელობის მძიმე დაზიანება ან სხვა მძიმე შედეგი;

143-ე მუხლის პირველი ნაწილი;

თავისუფლების უკანონო აღკვეთა;

143¹ მუხლის პირველი ნაწილი;

წინასწარი შეცნობით საქართველოს სსკ-ს 143¹ და 143² მუხლებით გათვალისწინებული დანაშაულის მსხვერპლის ან დაზარალებულის ისეთი მომსახურებით სარგებლობა, რომელიც, ამავე კოდექსის 143¹ მუხლის თანახმად, არის ექსპლუატაცია²⁵⁵;

საქართველოს სსკ-ის 180-ე მუხლის პირველი ნაწილი;

„თაღლითობა, ესე იგი მართლსაწინააღმდეგო მისაკუთრების მიზნით სხვისი ნივთის დაუფლება ან ქონებრივი უფლების მიღება მოტყუებით;“

²⁵⁵ ექსპლუატაცია - დამნაშავის მიერ მატერიალური ან სხვაგვარი სარგებლის მიღების მიზნით:

ა) შრომის ან მომსახურების გაწევის იძულება;

ბ) სექსუალური მომსახურების გაწევის იძულება;

გ) პირის დანაშაულებრივ საქმიანობაში, პროსტიტუციაში, პორნოგრაფიაში ან სხვა ანტისოციალურ ქმედებაში ჩაბმა;

დ) ადამიანის სხეულის ორგანოს, ორგანოს ნაწილის ან ქსოვილის იძულებით ან მოტყუებით ამოღება, გადანერგვა ან სხვაგვარად გამოყენება;

ე) ადამიანის მონობის მსგავს მდგომარეობაში ან მონობის თანამედროვე პირობებში ჩაყენება. ადამიანის მონობის თანამედროვე პირობებში ჩაყენება გულისხმობს მისთვის ისეთი მდგომარეობის შექმნას, როდესაც ის ანაზღაურებით, არაადეკვატური ანაზღაურებით ან ანაზღაურების გარეშე, სხვა პირის სასარგებლოდ ასრულებს სამუშაოს ან ეწევა მომსახურებას და მას არ შეუძლია ამ გარემოების შეცვლა ამ პირზე დამოკიდებულების გამო. პირზე დამოკიდებულება შეიძლება გამოწვეული იყოს, მათ შორის:

ე.ა) პროპონების საიდენტიფიკაციო დოკუმენტის ჩამორთმევით, კონტროლით ან განზრახ ხელყოფით;

ე.ბ) თავისუფალი გადაადგილების უფლების შეზღუდვით ან თავისუფალი გადაადგილების კონტროლით;

ე.გ) ოჯახის წევრთან ან სხვა პირთან კომუნიკაციის, მათ შორის, მიმოწერისა და სატელეფონო კონტაქტის, შეზღუდვით ან კონტროლით;

ე.დ) იძულებითი ან დამინიჭებული გარემოს შექმნით (საქართველოს სისხლის სამართლის კოდექსი რედ. 22/07/1999, კონსოლიდირებული 29.05.2019)

საქართველოს სსკ-ის 181-ე მუხლის პირველი ნაწილი;

„გამოძალდა, ესე იგი სხვისი ნივთის ან ქონებრივი უფლების გადაცემის ან ქონებრივი სარგებლობის მოთხოვნა, რასაც ერთვის დაზარალებულის ან მისი ახლო ნათესავის მიმართ ძალადობის გამოყენების ან მათი ნივთის განადგურების ან დაზიანების ანდა მათთვის სახელის გამტეხი ცნობის გახმაურების ან სხვა ისეთი ცნობის გავრცელების მუქარა, რომელმაც შეიძლება არსებითად დააზიანოს მათი უფლებები.“

საქართველოს სსკ-ის 186-ე მუხლის მე-2 ნაწილი;

„წინასწარი შეცნობით დანაშაულებრივი გზით მოპოვებული ქონებით სარგებლობა, ქონების შეძენა, ფლობა ან გასაღება ჩადენილი;

ა) წინასწარი შეთანხმებით ჯგუფის მიერ;

ბ) არაერთგზის²⁵⁶;

გ) ავტომათილის მიმართ;

დ) დიდი ოდენობით²⁵⁷;

ე) იმის მიერ, ვინც ორჯერ ან მეტჯერ იყო ნასამართლევი სხვისი მოძრავი ნივთის მართლსაწინააღმდეგო მისაკუთრებისათვის ან გამოძალვისათვის“.

საქართველოს სსკ-ის 187-ე მუხლის მე-2 ნაწილი;

„სხვისი ნივთის დაზიანება ან განადგურება, რამაც მნიშვნელოვანი ზიანი გამოიწვია ჩადენილი;

ა) ცეცხლის წაქიდანებით, აფეთქებით ან სხვა საყოველთაოდ საშიში საშუალებით;

ბ) არაერთგზის.“²⁵⁸

საქართველოს სსკ-ის 198-ე მუხლის პირველი ნაწილი;

„ადამიანის სიცოცხლისათვის ან ჯანმრთელობისათვის საშიში პროდუქციის დამზადება, შემოტანა ან რეალიზაცია, ანდა ასეთ პროდუქციაზე ეტიკეტის უკანონოდ გამოყენება“.

საქართველოს სსკ-ის 210-ე მუხლის პირველი ნაწილი;

„ყალბი საკრედიტო ან საანგარიშსწორებო ბარათის, სხვა საგადასახადო დოკუმენტის ან ქონებრივი უფლებამოსილების დამადასტურებელი ისეთი დოკუმენტის დამზადება ან შეძენა გასაღების ან გამოყენების მიზნით, გასაღება ან გამოყენება, რომელიც არ არის ფასიანი ქალაქი.“

საქართველოს სსკ-ის 253-ე მუხლის პირველი ნაწილი;

„პროსტიტუციაში ჩაბმა ძალადობით, ძალადობის ან ქონების განადგურების მუქარით, შანტაჟით ან მოტყუებით;

²⁵⁶ საქართველოს სსკ-ის 177-ე მუხლის შენიშვნა: 2. ამ კოდექსის 177-ე-186-ე მუხლებით გათვალისწინებული დანაშაული არაერთგზის ჩადენილად ითვლება, თუ მას წინ უსწრებდა ამ მუხლებით და 224-ე, 231-ე, 237-ე და 264-ე მუხლებით გათვალისწინებული რომელიმე დანაშაულის ჩადენა. (საქართველოს სისხლის სამართლის კოდექსი რედ. 22/07/1999. კონსოლიდირებული 29.05.2019)

²⁵⁷ საქართველოს სსკ-ის 177-ე მუხლის შენიშვნა: 3. კოდექსის ამ თავში მნიშვნელოვან ზიანად ითვლება ნივთის (ნივთების) ღირებულება 150 ლარის ზევით. (საქართველოს სისხლის სამართლის კოდექსი რედ. 22/07/1999. კონსოლიდირებული 29.05.2019)

²⁵⁸ საქართველოს სსკ-ის 177-ე მუხლის შენიშვნა: 2. ამ კოდექსის 177-ე-186-ე მუხლებით გათვალისწინებული დანაშაული არაერთგზის ჩადენილად ითვლება, თუ მას წინ უსწრებდა ამ მუხლებით და 224-ე, 231-ე, 237-ე და 264-ე მუხლებით გათვალისწინებული რომელიმე დანაშაულის ჩადენა. (საქართველოს სისხლის სამართლის კოდექსი რედ. 22/07/1999. კონსოლიდირებული 29.05.2019)

254-ე მუხლის პირველი ნაწილი:

პირის პროსტიტუციაზე დაყოლიება ან/და სხვა ისეთი არაძალადობრივი ქმედების განხორციელება, რომელიც ხელს უწყობს პირის პროსტიტუციაში მონაწილეობას;

254-ე მუხლის მე-2 ნაწილი:

პროსტიტუციისათვის ადგილის ან საცხოვრებლის გადაცემა.”

საქართველოს სსკ-ის 255¹ მუხლი:

1. „არასრულწლოვნის ჩაბმა პორნოგრაფიული ნაწარმოების ან პორნოგრაფიული ხასიათის სხვა საგნის უკანონოდ დამზადებაში, ასეთი მასალის გავრცელებაში, რეკლამირებაში ან მისით ვაჭრობაში;
2. იგივე ქმედება, ჩადენილი არაერთგზის²⁵⁹.”

საქართველოს სსკ-ის 259² მუხლი:

„ძეგლების, არქეოლოგიური ობიექტების ან საქართველოს კანონმდებლობით გათვალისწინებული სხვა კულტურული ფასეულობების საქართველოდან უნებართვო გატანა“.

საქართველოს სსკ-ის 284-ე მუხლი:

1. „კომპიუტერულ სისტემაში²⁶⁰ უნებართვო შეღწევა;
2. იგივე ქმედება:
 - ა) წინასწარი შეთანხმებით ჯგუფის მიერ²⁶¹;

²⁵⁹ საქართველოს სსკ-ის მუხლი 15. არაერთგზისი დანაშაული;

1. არაერთგზისი დანაშაული ნიშნავს წინათ ნასამართლევი პირის მიერ ამ კოდექსის იმავე მუხლით გათვალისწინებული დანაშაულის ჩადენას. ამ კოდექსის სხვადასხვა მუხლით გათვალისწინებული ორი ან მეტი დანაშაული მხოლოდ მაშინ ჩაითვლება არაერთგზისი დანაშაულად, თუ ამის შესახებ მითითებულია ამ კოდექსის შესაბამის მუხლში.

2. დანაშაული არაერთგზისი ჩადენილად არ ჩაითვლება, თუ კანონით დადგენილი წესით პირი წინათ ჩადენილი დანაშაულისათვის გათავისუფლებული იყო სისხლისსამართლებრივი პასუხისმგებლობისგან ანდა თუ მას წინათ ჩადენილი დანაშაულისათვის ნასამართლობა მოხსნილი ან გაქაჩაწყლებული ჰქონდა. (საქართველოს სისხლის სამართლის კოდექსი რედ. 22/07/1999. კონსოლიდირებული 29.05.2019)

²⁶⁰ 284-ე მუხლის შენიშვნა:

1. კომპიუტერული სისტემა არის ნებისმიერი მექანიზმი ან ერთმანეთთან დაკავშირებულ მექანიზმთა ჯგუფი, რომელიც პროგრამის მეშვეობით, ავტომატურად ამუშავებს მონაცემებს (მათ შორის, პერსონალური კომპიუტერი, ნებისმიერი მოწყობილობა მიკროპროცესორით, აგრეთვე მობილური ტელეფონი).

2. კომპიუტერული მონაცემი არის კომპიუტერულ სისტემაში დამუშავებისათვის ხელსაყრელი ნებისმიერი ფორმით გამოსახული ინფორმაცია, მათ შორის, პროგრამა, რომელიც უზრუნველყოფს კომპიუტერული სისტემის ფუნქციონირებას.

3. უნებართვო გულისხმობს უკანონოს, აგრეთვე იმ შემთხვევას, როდესაც უფლების მფლობელს პირდაპირ ან არაპირდაპირ არ გადაეცემა უფლება ქმედების ჩადენი პირისათვის. (საქართველოს სისხლის სამართლის კოდექსი რედ. 22/07/1999. კონსოლიდირებული 29.05.2019)

²⁶¹ საქართველოს სსკ-ის მუხლი 27. ჯგუფური დანაშაული;

1. დანაშაული ჯგუფის მიერაა ჩადენილი, თუ მის განხორციელებაში წინასწარ შეთანხმებულად ერთობლივად მონაწილეობდა ორი ან მეტი აპსრულებელი.

2. დანაშაული ჯგუფის მიერ წინასწარი შეთანხმებითაა ჩადენილი, თუ მის განხორციელებაში მონაწილენი წინასწარ შეკავშირდნენ დანაშაულის ერთობლივად ჩასადენად. (საქართველოს სისხლის სამართლის კოდექსი რედ. 22/07/1999. კონსოლიდირებული 29.05.2019)

- ბ) სამსახურებრივი მდგომარეობის გამოყენებით;
- გ) არაერთგზის²⁶²;
- დ) რამაც მნიშვნელოვანი ზიანი გამოიწვია²⁶³."

საქართველოს სსკ-ის 285-ე მუხლის პირველი ნაწილი;

„კომპიუტერული პროგრამის ან/და სხვა მოწყობილობის, აგრეთვე კომპიუტერულ სისტემაში შეღწევისათვის საჭირო პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის უნებართვო დამზადება, შენახვა, გაყიდვა, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა ამ თავითა და ამ კოდექსის 158-ე ან 159-ე მუხლით გათვალისწინებული დანაშაულის ჩადენის მიზნით.“

საქართველოს სსკ-ის 286-ე მუხლი;

1. კომპიუტერული მონაცემის (იხ. სქოლიო 124) უნებართვო დაზიანება, წაშლა, შეცვლა ან დაფარვა, –
2. ამ მუხლის პირველი ნაწილით გათვალისწინებული ქმედება, აგრეთვე კომპიუტერული მონაცემის უნებართვო ჩასმა ან გადაცემა, რამაც კომპიუტერული სისტემის ფუნქციონირების განზრახ მნიშვნელოვანი შეფერხება გამოიწვია, –
3. ამ მუხლის პირველი ან მე-2 ნაწილით გათვალისწინებული ქმედება:
 - ა) წინასწარი შეთანხმებით ჯგუფის მიერ (იხ. სქოლიო 125);
 - ბ) სამსახურებრივი მდგომარეობის გამოყენებით;
 - გ) არაერთგზის (იხ. სქოლიო 126);
 - დ) რამაც მნიშვნელოვანი ზიანი გამოიწვია (იხ. სქოლიო 127);

287-ე მუხლი;

სამრეწველო, სასოფლო-სამეურნეო, სამეცნიერო ან სხვა ობიექტის დაპროექტების, განლაგების, რეკონსტრუქციის, მშენებლობის, საექსპლუატაციოდ გადაცემის ან ექსპლუატაციის დროს გარემოს დაცვის წესის დარღვევა, რამაც გამოიწვია რადიაციული ფონის არსებითი გაუარესება, ადამიანის ჯანმრთელობის დაზიანება, ცხოველთა ან მცენარეული სამყაროს მასობრივი განადგურება ან სხვა მძიმე შედეგი.“

საქართველოს სსკ-ის 288-ე მუხლის პირველი ნაწილი;

„ტოქსიკური, ბაქტერიოლოგიური, ქიმიური ან გარემოსათვის საშიში სხვა ნივთიერებისადმი ან ნარჩენისადმი მოპყრობის წესის დარღვევა მისი წარმოების, ტრანსპორტირების, განთავსების,

²⁶² საქართველოს სსკ-ის მუხლი 15. არაერთგზისი დანაშაული;

1. არაერთგზისი დანაშაული ნიშნავს წინათ ნასამართლევ პირის მიერ ამ კოდექსის იმავე მუხლით გათვალისწინებული დანაშაულის ჩადენას. ამ კოდექსის სხვადასხვა მუხლით გათვალისწინებული ორი ან მეტი დანაშაული მხოლოდ მაშინ ჩაითვლება არაერთგზისი დანაშაულად, თუ ამის შესახებ მითითებულია ამ კოდექსის შესაბამის მუხლში.

2. დანაშაული არაერთგზისი ჩადენილად არ ჩაითვლება, თუ კანონით დადგენილი წესით პირი წინათ ჩადენილი დანაშაულისათვის გათავისუფლებული იყო სისხლისსამართლებრივი პასუხისმგებლობისაგან ანდა თუ მას წინათ ჩადენილი დანაშაულისათვის ნასამართლობა მოხსნილი ან გაქარწყლებული ჰქონდა. (საქართველოს სისხლის სამართლის კოდექსი რედ. 22/07/1999, კონსოლიდირებული 29.05.2019)

²⁶³ საქართველოს სსკ-ის 284-ე მუხლის შენიშვნა: 4. ამ თავში მნიშვნელოვნად ითვლება 2000 ლარზე მეტი ოდენობის ზიანი. (საქართველოს სისხლის სამართლის კოდექსი რედ. 22/07/1999, კონსოლიდირებული 29.05.2019)

შენახვის, ჩამარხვის ან გამოყენების დროს, რასაც შეეძლო გამოეწვია ადამიანის ჯანმრთელობის ან გარემოს არსებითი დაზიანება ან სხვა მძიმე შედეგი."

საქართველოს სსკ-ის 288-ე მუხლის მე-2 ნაწილი:

-ტოქსიკური, ბაქტერიოლოგიური, ქიმიური ან გარემოსათვის საშიში სხვა ნივთიერებისადმი ან ნარჩენისადმი მოპყრობის წესის დარღვევა მისი წარმოების, ტრანსპორტირების, განთავსების, შენახვის, ჩამარხვის ან გამოყენების დროს, რასაც შეეძლო გამოეწვია ადამიანის ჯანმრთელობის ან გარემოს არსებითი დაზიანება ან სხვა მძიმე შედეგი, რამაც გამოიწვია გარემოს დაბინძურება, მოწამულა ან დასნებოვნება, ან ადამიანის ჯანმრთელობის დაზიანება, ანდა ცხოველთა ან მცენარეული სამყაროს მასობრივი განადგურება, აგრეთვე ჩადენილი საგანგებო ეკოლოგიური მდგომარეობის დროს ან ეკოლოგიური უბედურების ზონაში."

საქართველოს სსკ-ის 289-ე მუხლი:

1. მიკრობიოლოგიური ან სხვა ბიოლოგიური აგენტისადმი ან ტოქსინისადმი მოპყრობის წესის დარღვევა, რამაც გამოიწვია ადამიანის ჯანმრთელობის დაზიანება, ეპიდემიის ანდა ეპიზოოტიის გავრცელება ან გარემოსათვის სხვა მძიმე შედეგი;
2. იგივე ქმედება, რამაც გამოიწვია ადამიანის სიცოცხლის მოსპობა."

საქართველოს სსკ-ის 290-ე მუხლი:

1. ვეტერინარიის სფეროში საქართველოს კანონმდებლობის დარღვევა, რამაც გამოიწვია ეპიზოოტიის გავრცელება ან სხვა მძიმე შედეგი, -
2. ვეტერინარიის სფეროში საქართველოს კანონმდებლობის დარღვევა, რასაც მოჰყვა ეპიზოოტიური, ზოონოზური, ზოოანთროპონოზური სნეულებების გავრცელება ან სხვა მძიმე შედეგი."

საქართველოს სსკ-ის 292-ე მუხლი:

1. წყლის ობიექტის დაბინძურება, დანაგვიანება, დაშრება ან მასზე სხვა ისეთი უარყოფითი ზემოქმედება, რომელმაც შეიძლება დააზიანოს მოსახლეობის ჯანმრთელობა, შეამციროს თევზის მარაგი, გააუარესოს წყალმომარაგების პირობები, გამოიწვიოს წყლის ფიზიკური, ქიმიური, ბიოლოგიური თვისებების გაუარესება, ბუნებრივი თვითგაწმენდის უნარის დაქვეითება, ჰიდროლოგიური და ჰიდროგეოლოგიური რეჟიმის დარღვევა, -
2. იგივე ქმედება, რამაც გამოიწვია ადამიანის ჯანმრთელობის დაზიანება, ანდა ცხოველთა ან მცენარეული სამყაროს მასობრივი განადგურება, აგრეთვე ჩადენილი სახელმწიფო ნაკრძალის ან ალკვეთილის ტერიტორიაზე ანდა საგანგებო ეკოლოგიური მდგომარეობის დროს ან ეკოლოგიური უბედურების ზონაში;
3. ამ მუხლის პირველი ან მე-2 ნაწილით გათვალისწინებული ქმედება, რამაც გამოიწვია ადამიანის სიცოცხლის მოსპობა ან სხვა მძიმე შედეგი."

საქართველოს სსკ-ის 293-ე მუხლი:

1. გემიდან, სხვა მცურავი საშუალებიდან, პლატფორმიდან ან ზღვაში ხელოვნურად აგებული სხვა კონსტრუქციიდან ადამიანის ჯანმრთელობისათვის ან ზღვის ცოცხალი ორგანიზმისათვის მავნე ნივთიერებების, სხვა ნარჩენის ანდა მასალის ზღვაში უკანონოდ ჩაყრა (ჩაშვება), აგრეთვე მათი ჩამარხვის წესის დარღვევით ზღვის დაბინძურება, რაც საფრთხეს უქმნის ადამიანის ჯანმრთელობას ან ზღვის ცოცხალ ორგანიზმს, ანდა

ხელს უშლის ზღვის მართლზომიერ გამოყენებას, ჩადენილი ასეთი ქმედებისათვის ადმინისტრაციული სახდელის დადების შემდეგ;

2. ხმელეთიდან და საჰაერო ხომალდიდან ადამიანის ჯანმრთელობისათვის ან ზღვის ცოცხალი ორგანიზმისათვის მავნე ნივთიერების ანდა სხვა ნარჩენის ან მასალის ზღვაში უკანონოდ ჩაყრა (ჩაშვება), აგრეთვე მათი ჩამარხვის წესის დარღვევით ზღვის დაბინძურება, რაც საფრთხეს უქმნის ადამიანის ჯანმრთელობას ან ზღვის ცოცხალ ორგანიზმს, ანდა ხელს უშლის ზღვის მართლზომიერ გამოყენებას;
3. ამ მუხლის პირველი და მე-2 ნაწილებით გათვალისწინებული ქმედება, რამაც მნიშვნელოვანი ზიანი მიიყენა ადამიანის ჯანმრთელობას, მცენარეულ სამყაროს, თევზის მარაგს ან წყლის სხვა ცოცხალ ორგანიზმს, დასვენების ზონას ანდა კანონით დაცულ სხვა სიკეთეს;
4. ამ მუხლის პირველი, მე-2 და მე-3 ნაწილებით გათვალისწინებული ქმედება, რამაც გამოიწვია ადამიანის სიცოცხლის მოსპობა."

საქართველოს სსკ-ის 294-ე მუხლი;

„გემის, სხვა მცურავი საშუალების, საჰაერო ხომალდის, პლატფორმის ან ზღვაში ხელოვნურად აგებული სხვა კონსტრუქციის სათანადო პასუხისმგებელი თანამდებობის პირის მიერ უახლოესი პორტის ადმინისტრაციისათვის, ხოლო ჩამარხვის მიზნით ჩაყრის შემთხვევაში — აგრეთვე ჩაყრის ნებართვის მიმცემი ორგანიზაციისათვის შეუტყობინებლობა იმისა, რომ საქართველოს შიდა ზღვის ან ტერიტორიული წყლების ფარგლებში ანდა ლია ზღვაში მზადდება ან უკიდურესი აუცილებლობის გამო მოხდა ჩაყრა ან აუცდენელი დაკარგვა ადამიანის ჯანმრთელობისათვის ან ზღვის ცოცხალი ორგანიზმისათვის მავნე ნივთიერებისა ან ისეთი შენარჩენისა, რომელიც ასეთ ნივთიერებას დადგენილი ნორმის გადამეტებით შეიცავს, ანდა სხვა ნარჩენისა ან მასალისა, რომელსაც შეუძლია დააზიანოს დასვენების ზონა ან ხელი შეუშალოს ზღვის მართლზომიერ გამოყენებას.“

საქართველოს სსკ-ის 295-ე მუხლი;

- „1. მავნე ნივთიერების ატმოსფერულ ჰაერში გაფრქვევის ანდა გამწმენდი დანადგარის, ნაგებობის ან სხვა ობიექტის ექსპლუატაციის წესის დარღვევა, რამაც გამოიწვია ატმოსფერული ჰაერის ხარისხის მნიშვნელოვანი გაუარესება;
2. იგივე ქმედება, რამაც გამოიწვია ადამიანის ჯანმრთელობის დაზიანება;
3. ამ მუხლის პირველი ნაწილით გათვალისწინებული ქმედება, რამაც გამოიწვია ადამიანის სიცოცხლის მოსპობა.“

საქართველოს სსკ-ის 296-ე მუხლი;

- „1. საქართველოს კონტინენტურ შეღწე, ტერიტორიულ წყლებში ან მიმდებარე ზონაში ნაგებობის უკანონოდ აღმართვა, მის გარშემო ან განსაკუთრებულ ეკონომიკურ ზონაში ხელოვნური კუნძულის, ნაგებობის ან მოწყობილობის ირგვლივ უსაფრთხოების ზონის უკანონოდ დაწესება, აგრეთვე შენელობის, რეკონსტრუქციის, ექსპლუატაციის, ნაგებობის დაცვის, ლიკვიდაციის ან კონსერვაციის, ანდა საზღვაო ნაოსნობის უსაფრთხოების წესის დარღვევა ასეთივე დარღვევისათვის ადმინისტრაციული სახდელის დადების შემდეგ, —
2. საქართველოს კონტინენტური შეღწის ან განსაკუთრებული ეკონომიკური ზონის სათანადო ნებართვის გარეშე გამოკვლევა ან დაზვერვა ანდა მისი ბუნებრივი სიმდიდრის დამუშავება ასეთივე დარღვევისათვის ადმინისტრაციული სახდელის დადების შემდეგ.“

საქართველოს სსკ-ის 297-ე მუხლი:

1. სამეწარმეო, სამეურნეო ან სხვაგვარი საქმიანობისას მავნე ნივთიერებით მიწის მოწამვლა, დეგრადაცია ან მიწის სხვაგვარი გაუვარესება, განპირობებული სასუქის, მცენარეთა ზრდის სტიმულატორის, შხამქიმიკატის, სხვა ქიმიური ან ბიოლოგიური ნივთიერების შენახვის, გამოყენების ან გადაზიდვის დროს მისდამი მოპყრობის წესის დარღვევით, რამაც გამოიწვია ადამიანის ჯანმრთელობის ან გარემოს დაზიანება, –
2. იგივე ქმედება, ჩადენილი საგანგებო ეკოლოგიური მდგომარეობის დროს ან ეკოლოგიური უბედურების ზონაში, რამაც მიწის მნიშვნელოვანი ფართობის გაუვარესება გამოიწვია, –
3. ამ მუხლის პირველი ან მე-2 ნაწილით გათვალისწინებული ქმედება, რამაც გამოიწვია ადამიანის სიცოცხლის მოსპობა."

საქართველოს სსკ-ის 298-ე მუხლი:

„სამთომოპოვებითი საწარმოს ან მიწისქვეშა ნაგებობის დაპროექტების, განლაგების, რეკონსტრუქციის, ლიკვიდაციის, საექსპლუატაციოდ გადაცემის ან ექსპლუატაციის დროს წიაღ-სეულის გამოყენების ან დაცვის წესის დარღვევა, აგრეთვე თვითნებური მშენებლობა სასარგებლო წიაღისეულის განლაგების ადგილას, რამაც გამოიწვია მნიშვნელოვანი ზიანი."

საქართველოს სსკ-ის 299-ე მუხლი:

1. წიაღით (გარდა მიწისქვეშა მტკნარი წყლისა) სარგებლობა სათანადო ლიცენზიის გარეშე, ჩადენილი ასეთი ქმედებისათვის ადმინისტრაციული სახდელის დადების შემდეგ, ან წიაღით სარგებლობა სათანადო ლიცენზიის გარეშე, რამაც მნიშვნელოვანი ზიანი გამოიწვია:
2. იგივე ქმედება, ჩადენილი არაერთგზის (იხ. სქოლიო 126)."

საქართველოს სსკ-ის 300-ე მუხლი:

1. თევზჭერა ელექტროდენით, ელექტროშოკის აპარატით ან სხვა აკრძალული იარაღით, ასაფეთქებელი ან მომწამლავი ნივთიერებით, თევზის ან წყლის სხვა ცოცხალი ორგანიზმის მასობრივი განადგურების სხვა საშუალებით, ან 100 ტონის ან მასზე ნაკლები საერთო ტევადობის, 8 მეტრზე მეტი სიგრძის ან 100 ტონაზე მეტი საერთო ტევადობის წყლის სატრანსპორტო საშუალებიდან თევზსარეწი იარაღით თევზის ან წყლის სხვა ცოცხალი ორგანიზმის უკანონოდ მოპოვება, ან საქართველოს „წითელ ნუსხაში" შეტანილი თევზის ან წყლის სხვა ცოცხალი ორგანიზმის მოპოვება, ასეთივე დარღვევისათვის ადმინისტრაციული სახდელის დადების შემდეგ.
2. თევზჭერა ელექტროდენით, ელექტროშოკის აპარატით ან სხვა აკრძალული იარაღით, ასაფეთქებელი ან მომწამლავი ნივთიერებით, თევზის ან წყლის სხვა ცოცხალი ორგანიზმის მასობრივი განადგურების სხვა საშუალებით, ან საქართველოს „წითელ ნუსხაში" შეტანილი თევზის ან წყლის სხვა ცოცხალი ორგანიზმის მოპოვება, რამაც მნიშვნელოვანი ზიანი გამოიწვია;
3. ელექტროდენით, ელექტროშოკის აპარატით ან სხვა აკრძალული იარაღით, ასაფეთქებელი ან მომწამლავი ნივთიერებით, თევზის ან წყლის სხვა ცოცხალი ორგანიზმის მასობრივი განადგურების სხვა საშუალებით, ან 100 ტონის ან მასზე ნაკლები საერთო ტევადობის, 8 მეტრზე მეტი სიგრძის ან 100 ტონაზე მეტი საერთო ტევადობის წყლის სატრანსპორტო სა-

შუალედრიდან თევზსარეწი იარაღით თევზჭერა, ჩადენილი აკრძალულ დროს ან აკრძალულ ადგილას, ან საგანგებო ეკოლოგიური მდგომარეობის დროს ან ეკოლოგიური უბედურების ზონაში, ან სახელმწიფო ნაკრძალის, ეროვნული პარკის ბუნების მკაცრი დაცვის ზონის, ბუნების ძეგლის, ბიოსფერული რეზერვატის ბირთვის (ბუნების მკაცრი დაცვის) ზონის ან მსოფლიო მემკვიდრეობის უბნის ტერიტორიაზე.

საქართველოს სსკ-ის 301-ე მუხლი;

- „1. ნადირობა სათანადო ნებართვის გარეშე, ანდა აკრძალულ ადგილას ან აკრძალულ დროს, ან აკრძალული იარაღით ან საშუალებით, რამაც მნიშვნელოვანი ზიანი გამოიწვია;
2. ნადირობა სახელმწიფო ნაკრძალში ან სხვა დაცულ ტერიტორიაზე, სადაც ნადირობა მთლიანად აკრძალულია, ანდა მექანიკური სატრანსპორტო ან მასობრივი განადგურების საშუალებით, ან საქართველოს „წითელ ნუსხაში“ შეტანილ ან უმწეო მდგომარეობაში მყოფ ნადირ-ფრინველზე, აგრეთვე საგანგებო ეკოლოგიური მდგომარეობის დროს ან ეკოლოგიური უბედურების ზონაში.“

საქართველოს სსკ-ის 302-ე მუხლი;

- „1. საქართველოს „წითელ ნუსხაში“ შეტანილი, გადაშენების საფრთხის წინაშე მყოფი გარეული ცხოველის ან ველური მცენარის ბუნებრივი საბინადრო ან გამრავლების არეალის მოშლა ან იმ ადგილების სხვა დანიშნულებით გამოყენება, სადაც საქართველოს „წითელ ნუსხაში“ შეტანილი სახეობა ბუნებრივად ბინადრობს ან ხარობს, რამაც გაუფრთხილებლობით ამ ადგილებში ცხოველის ან მცენარის სახეობის გადაშენების საფრთხე შექმნა;
2. იგივე ქმედება, რამაც გაუფრთხილებლობით გამოიწვია საქართველოს „წითელ ნუსხაში“ შეტანილი, გადაშენების საფრთხის წინაშე მყოფი გარეული ცხოველის ან ველური მცენარის გადაშენება.“

საქართველოს სსკ-ის 303-ე მუხლის პირველი - მე-3 ნაწილი;

- „1. ხე-ბუჩქნარის უკანონოდ გაჩეხვა საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსის 641 მუხლის პირველი ნაწილით, 66-ე მუხლის მე-2 ნაწილით, 151-ე მუხლის მე-2 ნაწილით ან 1511 მუხლის მე-2 ნაწილით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის ჩადენისთვის ადმინისტრაციულ სახდელდადებული პირის მიერ, ან ხე-ბუჩქნარის უკანონოდ გაჩეხვა, რამაც მნიშვნელოვანი ზიანი გამოიწვია;
2. იგივე ქმედება, ჩადენილი არაერთგზის (იხ. სქოლიო 126);
3. სახელმწიფო ტყის ფონდის მიწებზე ან დაცულ ტერიტორიებზე საქართველოს „წითელ ნუსხაში“ შეტანილი ხე-ბუჩქნარის უკანონოდ გაჩეხვა საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსის 641 მუხლის მე-2 ნაწილით გათვალისწინებული ადმინისტრაციული სამართალდარღვევის ჩადენისთვის ადმინისტრაციულ სახდელდადებული პირის მიერ.“

საქართველოს სსკ-ის 304-ე მუხლის პირველი ნაწილი;

„ტყის ან ნარგავის დაზიანება ან განადგურება ცეცხლთან ან მომეტებული საფრთხის წყაროსთან გაუფრთხილებელი მოპყრობით, ანდა მისი დაბინძურება მავნე ნივთიერებით.“

საქართველოს სსკ-ის 305-ე მუხლი;

„სახელმწიფო ნაკრძალის, აღკვეთილის, ეროვნული პარკის, ბუნების ძეგლის, დაცული ლანდშაფტის ან სხვა დაცული ტერიტორიის რეჟიმის დარღვევა, რამაც გამოიწვია მნიშვნელოვანი ზიანი.“

საქართველოს სსკ-ის 306-ე მუხლი;

„საქმიანობის განხორციელება გარემოზე ზემოქმედების ნებართვის გარეშე, ჩადენილი ასეთი ქმედებისათვის ადმინისტრაციული სახდელის დადების შემდეგ.“

საქართველოს სსკ-ის 306¹ მუხლი;

„სკრინინგის პროცედურისადმი დაქვემდებარებული საქმიანობის სკრინინგის გადაწყვეტილების გარეშე განხორციელება, რამაც მნიშვნელოვანი ზიანი გამოიწვია, ან გარემოზე ზემოქმედების შეფასებისადმი დაქვემდებარებული საქმიანობის გარემოსდაცვითი შეფასების კოდექსით გათვალისწინებული გარემოსდაცვითი გადაწყვეტილების გარეშე განხორციელება, ჩადენილი ასეთი ქმედებისთვის ადმინისტრაციული სახდელის დადების შემდეგ.“

საქართველოს სსკ-ის 318-ე მუხლის პირველი ნაწილი;

1. საქართველოს დასუსტების მიზნით სახელმწიფო ან სხვა საწარმოს, დაწესებულების, ორგანიზაციის ან სამსახურის ნორმალური ფუნქციონირებისათვის ხელის შეშლა;
2. საქართველოს დასუსტების მიზნით საწარმოს, სატრანსპორტო, კავშირგაბმულობის ან მასობრივი მაუწყებლობის საშუალების, გზის, ნაგებობის, ტექნიკის, დოკუმენტის, დიდი რაოდენობით სტრატეგიული ნედლეულის, მასალის ან პროდუქციის, აგრეთვე მოსახლეობისათვის სასიცოცხლო მნიშვნელობის დაწესებულების ან ორგანიზაციის ნორმალური ფუნქციონირებისათვის აუცილებელი, საზოგადოებრივი უშიშროების ან წესრიგის დაცვისათვის განკუთვნილი ან სხვა განსაკუთრებული დანიშნულების ობიექტის დაზიანება, მწყობრიდან გამოყვანა ან განადგურება;
3. ამ მუხლის მე-2 ნაწილით გათვალისწინებული ქმედება, ჩადენილი აფეთქებით, ცეცხლის წაყიდებით ან სხვა საყოველთაოდ საშიში საშუალებით, აგრეთვე ბირთვული ენერგიის კონტროლიდან გამოყვანა, ეპიდემიის ან ეპიზოოტიის გავრცელება, მასობრივი მოწამვლა ანდა სხვა ქმედება, რომელმაც ადამიანის სიცოცხლის მოსპობა ან მისი ჯანმრთელობის დაზიანება გამოიწვია.“

საქართველოს სსკ-ის 322¹ მუხლი;

1. უცხო ქვეყნის მოქალაქის ან მოქალაქეობის არმქონე პირის ოკუპირებულ ტერიტორიებზე შესვლა „ოკუპირებულ ტერიტორიების შესახებ“ საქართველოს კანონით დადგენილი წესის დარღვევით, –
2. ამ მუხლის პირველი ნაწილით გათვალისწინებული ქმედება, ჩადენილი:
 - ა) ჯგუფურად (იხ. სქოლიო 125);
 - ბ) არაერთგზის (იხ. სქოლიო 126);
 - გ) ძალადობით ან ძალადობის მუქარით;
 - დ) ასეთი დანაშაულისათვის მსჯავრდებულის მიერ;

შენიშვნა: ამ მუხლით გათვალისწინებული დანაშაულის ჩადენისათვის სისხლისსამართლებრივი პასუხისმგებლობისაგან თავისუფლდება უცხო ქვეყნის მოქალაქე ან მოქალაქეობის არმქონე პირი,

რომელიც საქართველოში უშუალოდ იმ ტერიტორიებიდან შემოვიდა, სადაც მის სიცოცხლეს ან თავისუფლებას „ლტოლვილთა სტატუსის შესახებ“ გავროს 1951 წლის კონვენციის პირველი მუხლით გათვალისწინებული საფრთხე ემუქრებოდა და რომელიც საქართველოში უნებართვოდ იმყოფება და იმავე კონვენციისა და საქართველოს კანონმდებლობის შესაბამისად თავშესაფარს სთხოვს საქართველოს ხელისუფლებას, იმ პირობით, რომ ის დაუყოვნებლივ გამოცხადდება ხელისუფლების ორგანოში და წარადგენს სათანადო განმარტებას საქართველოში უკანონო შემოსვლის ან უნებართვო ყოფნის შესახებ, და თუ მის ქმედებაში არ არის სხვა დანაშაულის ნიშნები, აგრეთვე პირი, რომელმაც აღნიშნული ქმედება ადამიანით ვაჭრობის (ტრეფიკინგის) მსხვერპლად ყოფნის გამო, ადამიანით ვაჭრობის (ტრეფიკინგის) მსხვერპლის სტატუსის მოპოვებამდე ჩაიდინა.“

საქართველოს სსკ-ის 344² მუხლის პირველი ნაწილი;

„1. პირის მიერ ფინანსური ან სხვა მატერიალური სარგებლის მიღების მიზნით საქართველოს მოქალაქის უცხო ქვეყანაში წინასწარი შეცნობით უკანონოდ დარჩენისთვის შესაბამისი პირობების შექმნა/ორგანიზების გაწევა ან/და პირის მიერ ამავე მიზნით უცხო ქვეყანაში საერთაშორისო დაცვის მისაღებად საქართველოს მოქალაქის მიერ მისი უფლებების ან თავისუფლებების დარღვევის თაობაზე წინასწარი შეცნობით მცდარი ინფორმაციის წარდგენის ხელშეწყობა/ორგანიზება;

2. იგივე ქმედება, ჩადენილი:

- ა) წინასწარი შეთანხმებით ჯგუფის მიერ²⁶⁴;
- ბ) არაერთგზის (იხ. სქოლიო 126);
- გ) ორი ან მეტი პირის მიმართ;
- დ) ყალბი დოკუმენტის გამოყენებით, —

3. ამ მუხლის პირველი ან მე-2 ნაწილით გათვალისწინებული ქმედება, ჩადენილი ორგანიზებული ჯგუფის მიერ;²⁶⁵

შენიშვნა:

- 1. ამ მუხლით გათვალისწინებული დანაშაულის ჩადენისთვის სისხლისსამართლებრივი პასუხისმგებლობა არ დაეკისრება იმ პირს, რომელმაც ახლო ნათესავის უცხო ქვეყანაში უკანონოდ დარჩენისთვის შესაბამისი პირობები შექმნა ან/და ორგანიზება გაუწია ამ პირის უცხო ქვეყანაში უკანონოდ დარჩენას.
- 2. ამ მუხლით გათვალისწინებული დანაშაულის ჩადენისთვის სისხლისსამართლებრივი პასუხისმგებლობა არ დაეკისრება იმ პირს, რომელმაც უცხო ქვეყანაში საერთაშორისო დაცვის მისაღებად ახლო ნათესავს ხელი შეუწყო მცდარი ინფორმაციის წარდგენაში ან/და ორგანიზება გაუწია ამ პირის მიერ მცდარი ინფორმაციის წარდგენას.“

²⁶⁴ საქართველოს სსკ-ის 27-ე მუხლი 2. დანაშაული ჯგუფის მიერ წინასწარი შეთანხმებითაა ჩადენილი, თუ მის განხორციელებაში მონაწილე წინასწარ შეკავშირდნენ დანაშაულის ერთობლივად ჩასადენად. (საქართველოს სისხლის სამართლის კოდექსი რედ. 22/07/1999. კონსოლიდირებული 29.05.2019);

²⁶⁵ საქართველოს სსკ-ის 27-ე მუხლი 3.. დანაშაული ორგანიზებული ჯგუფის მიერაა ჩადენილი, თუ იგი განხორციელდა დროის განსაზღვრულ პერიოდში არსებულმა, შეთანხმებულად მოქმედმა, სტრუქტურული ფორმის მქონე ჯგუფმა, რომლის წევრები წინასწარ შეკავშირდნენ ერთი ან რამდენიმე დანაშაულის ჩასადენად ან რომლის მიზანია პირდაპირ ან არაპირდაპირ ფინანსური ან სხვა მატერიალური სარგებლის უკანონოდ მიღება (საქართველოს სისხლის სამართლის კოდექსი რედ. 22/07/1999. კონსოლიდირებული 29.05.2019)

საქართველოს სსკ-ის XXXIX თავი²⁶⁶ - რომელიც მოიცავს შემდეგ სამოხელეო დანაშაულებს;

მუხლი 332. სამსახურებრივი უფლებამოსილების ბოროტად გამოყენება;

1. მოხელის ან მასთან გათანაბრებული პირის მიერ სამსახურებრივი უფლებამოსილების ბოროტად გამოყენება საჯარო ინტერესის საწინააღმდეგოდ, თავისთვის ან სხვისთვის რაიმე გამოჩენის ან უპირატესობის მისაღებად, რამაც ფიზიკური ან იურიდიული პირის უფლების, საზოგადოების ან სახელმწიფოს კანონიერი ინტერესის არსებითი დარღვევა გამოიწვია;
2. სამსახურებრივი უფლებამოსილების ბოროტად გამოყენება სახელმწიფო-პოლიტიკური თანამდებობის მქონე პირის მიერ, -
3. ამ მუხლის პირველი ან მე-2 ნაწილით გათვალისწინებული ქმედება, ჩადენილი:
 - ა) არაერთგზის (იხ. სქოლიო 126);
 - ბ) ძალადობით ან იარაღის გამოყენებით;
 - გ) დაზარალებულის პირადი ღირსების შეურაცხყოფით."

მუხლი 333. სამსახურებრივი უფლებამოსილების გადამეტება

1. მოხელის ან მასთან გათანაბრებული პირის მიერ სამსახურებრივი უფლებამოსილების გადამეტება, რამაც ფიზიკური ან იურიდიული პირის უფლების, საზოგადოების ან სახელმწიფოს კანონიერი ინტერესის არსებითი დარღვევა გამოიწვია;
2. სამსახურებრივი უფლებამოსილების გადამეტება სახელმწიფო-პოლიტიკური თანამდებობის მქონე პირის მიერ;
3. ამ მუხლის პირველი ან მე-2 ნაწილით გათვალისწინებული ქმედება, ჩადენილი:

²⁶⁶ მენიშენა:

1. ამ თავით გათვალისწინებული დანაშაულის სუბიექტები ასევე არიან საჯარო სამართლის იურიდიული პირების (გარდა პოლიტიკური და რელიგიური გაერთიანებებისა) ის თანამშრომლები, რომლებიც ახორციელებენ საჯარო სამართლებრივ უფლებამოსილებას, საქართველოს პარლამენტის დროებითი კომისიების წევრები და თანამშრომლები, საარჩევნო სუბიექტები (მხოლოდ ამ კოდექსის 338-ე მუხლით გათვალისწინებული დანაშაულის მიზნებისათვის), კერძო აღმასრულებლები, აგრეთვე ნებისმიერი სხვა პირი, რომელიც საქართველოს კანონმდებლობის საფუძველზე ახორციელებს საჯარო სამართლებრივ უფლებამოსილებას.
2. ამ თავის მიზნებისათვის, მოხელესთან გათანაბრებული პირი ასევე გულისხმობს უცხო ქვეყნის სახელმწიფო თანამდებობის პირს (მათ შორის, საკანონმდებლო ან/და ადმინისტრაციული უფლებამოსილების განმახორციელებელი სახელმწიფო ორგანოს წევრს), ნებისმიერ პირს, რომელიც ასრულებს რაიმე საჯარო ფუნქციას სხვა სახელმწიფოსთვის, საერთაშორისო ორგანიზაციის ან ორგანოს თანამდებობის პირს ან ხელშეკრულების საფუძველზე დაქირავებულ თანამშრომელს, აგრეთვე ნებისმიერ მივლინებულ ან არამივლინებულ პირს, რომელიც ასრულებს ამ თანამდებობის პირის ან თანამშრომლის ფუნქციების შესაბამის ფუნქციებს, უცხო ქვეყნის ნაფიცი მსახურებს, რომლებიც ასრულებენ თავიანთ ფუნქციებს უცხო ქვეყნის კანონმდებლობის საფუძველზე, საერთაშორისო საპარლამენტო კრების წევრს, სისხლის სამართლის საერთაშორისო სასამართლოს წარმომადგენელს, საერთაშორისო სასამართლოს ან სასამართლო ორგანოს მოსამართლეს და თანამდებობის პირს.
3. ამ კოდექსის 338-ე და 339-ე მუხლებით გათვალისწინებულ დანაშაულთა სუბიექტები ასევე არიან საქართველოსა და უცხო ქვეყნის არბიტრაჟების წევრები, ხოლო ამ კოდექსის 338-ე-339-მუხლებით გათვალისწინებულ დანაშაულთა სუბიექტები — ნაფიცი მსახურები (ნაფიცი მსახურობის კანდიდატები), რომლებიც საქართველოს კანონმდებლობის საფუძველზე ახორციელებენ აღნიშნულ უფლებამოსილებას.

- ა) არაერთგზის (იხ. სქოლიო 126);
- ბ) ძალადობით ან იარაღის გამოყენებით;
- გ) დაზარალებულის პირადი ღირსების შეურაცყოფით.“

მუხლი 334. ბრალდებულის სისხლისსამართლებრივი პასუხისმგებლობისაგან უკანონო გათავისუფლება:

„ბრალდებულის სისხლისსამართლებრივი პასუხისმგებლობისაგან უკანონო გათავისუფლება.“

მუხლი 335. განმარტების, ჩვენების ან დასკვნის მიცემის იძულება

„1. მოხელის ან მასთან გათანაბრებული პირის მიერ მუქარით, მოტყუებით, შანტაჟით ან სხვა უკანონო ქმედებით პირის იძულება განმარტების ან ჩვენების მიცემისათვის ანდა ექსპერტისა – დასკვნის მიცემისათვის, –

2. იგივე ქმედება, ჩადენილი:

- ა) სიცოცხლისათვის ან ჯანმრთელობისათვის საშიში ძალადობით ანდა ასეთი ძალადობის გამოყენების მუქარით;
- ბ) ორგანიზებული ჯგუფის მიერ (იხ. სქოლიო 129).“

მუხლი 337. სამეწარმეო საქმიანობაში უკანონო მონაწილეობა

„მოხელის ან მასთან გათანაბრებული პირის მიერ პირადად ან სხვისი მეშვეობით საწარმოს, დაწესებულების ან ორგანიზაციის დაარსება სამეწარმეო საქმიანობის მიზნით ანდა, კანონით დადგენილი აკრძალვის მიუხედავად, მის მართვაში მონაწილეობა, თუ ეს დაკავშირებულია მისთვის უკანონო შეღავათის ან უპირატესობის დაწესებასთან ან მის სხვა ფორმით მფარველობასთან.“

მუხლი 338. ქრთამის აღება:

„1. მოხელის ან მასთან გათანაბრებული პირის მიერ პირდაპირ ან არაპირდაპირ, ფულის, ფასიანი ქაღალდის, სხვა ქონების, ქონებრივი სარგებლის ან სხვა რაიმე არამართლზომიერი უპირატესობის მიღება ან მოთხოვნა, ასევე ასეთის თაობაზე შეთავაზების ან დაპირების მიღება თავის ან სხვა პირის სასარგებლოდ, რათა ამ მოხელემ ან მასთან გათანაბრებულმა პირმა თანამდებობრივი უფლება-მოვალეობების შესრულებისას ქრთამის მიმცემის ან სხვა პირის სასარგებლოდ განახორციელოს რაიმე ქმედება ან თავი შეიკავოს რაიმე ქმედების განხორციელებისაგან ან გამოიყენოს თავისი თანამდებობრივი ავტორიტეტი ანალოგიური მიზნის მისაღწევად, აგრეთვე განახორციელოს სამსახურებრივი მფარველობა;

2. ქრთამის აღება:

- ა) სახელმწიფო-პოლიტიკური თანამდებობის მქონე პირის მიერ;
- ბ) დიდი ოდენობით²⁶⁷;
- გ) წინასწარი შეთანხმებით ჯგუფის მიერ (იხ. სქოლიო 127)

3. ამ მუხლის პირველი და მე-2 ნაწილით გათვალისწინებული ქმედება, ჩადენილი:

- ა) მექრთამეობისათვის მსჯავრდებულის მიერ;
- ბ) არაერთგზის (იხ. სქოლიო 126) ;

²⁶⁷ შენიშვნა: დიდი ოდენობით ქრთამად ითვლება ფულის, ფასიანი ქაღალდის, სხვა ქონების ან ქონებრივი სარგებლის სახით თანხა ათი ათასი ლარის ზევით, ხოლო განსაკუთრებით დიდი ოდენობით ქრთამად – თანხა ოცდაათი ათასი ლარის ზევით.

გ) გამოძალკვით;

დ) ორგანიზებული ჯგუფის მიერ (იხ. სქოლიო 128);

ე) განსაკუთრებით დიდი ოდენობით."

მუხლი 339. ქრთამის მიცემა:

- ..1. მოხელისათვის ან მასთან გათანაბრებული პირისათვის პირდაპირ ან არაპირდაპირ, მის ან სხვა პირის სასარგებლოდ ფულის, ფასიანი ქაღალდის, სხვა ქონების, ქონებრივი სარგებლის ან სხვა რაიმე არამართლზომიერი უპირატესობის დაპირება, შეთავაზება ან მინიჭება, რათა მან თანამდებობრივი უფლებების განხორციელებისას და მოვალეობების შესრულებისას ქრთამის მიმცემის ან სხვა პირის სასარგებლოდ განახორციელოს რაიმე ქმედება ან თავი შეიკავოს რაიმე ქმედების განხორციელებისაგან, ან გამოიყენოს თავისი თანამდებობრივი ავტორიტეტი ანალოგიური მიზნის მისაღწევად, აგრეთვე განახორციელოს სამსახურებრივი მფარველობა;
2. იგივე ქმედება, ჩადენილი უკანონო ქმედების ჩასადენად;
3. ამ მუხლის პირველი ან მე-2 ნაწილით გათვალისწინებული ქმედება, ჩადენილი ორგანიზებული ჯგუფის მიერ,

შენიშვნა:

1. *სისხლისსამართლებრივი პასუხისმგებლობისაგან თავისუფლდება ქრთამის მიმცემი, თუ მანამის თაობაზე ნებაყოფლობით განუცხადა სისხლის სამართლის პროცესის მწარმოებელ ორგანოს. პასუხისმგებლობისაგან გათავისუფლების შესახებ გადაწყვეტილებას იღებს სისხლის სამართლის პროცესის მწარმოებელი ორგანო."*

მუხლი 339¹. ზეგავლენით ვაჭრობა:

- ..1. იმ პირისათვის, რომელიც ამტკიცებს ან ადასტურებს, რომ მას შეუძლია არამართლზომიერი ზეგავლენის მოხდენა მოხელის ან მოხელესთან გათანაბრებული პირის მიერ გადაწყვეტილების მიღებაზე პირდაპირ ან არაპირდაპირ, მის ან სხვა პირის სასარგებლოდ ფულის, ფასიანი ქაღალდის, სხვა ქონების, ქონებრივი სარგებლის ან სხვა რაიმე არამართლზომიერი უპირატესობის დაპირება, შეთავაზება ან მინიჭება იმ პირის მიერ, რომელიც მოქმედებს საკუთარი ან სხვა პირის ინტერესებისათვის, მიუხედავად იმისა, განხორციელდა თუ არა ასეთი ზეგავლენა ან/და მიღებულ იქნა თუ არა ამ ზეგავლენის სასურველი შედეგი;
2. პირის მიერ, რომელიც ამტკიცებს ან ადასტურებს, რომ მას შეუძლია არამართლზომიერი ზეგავლენის მოხდენა მოხელის ან მასთან გათანაბრებული პირის მიერ გადაწყვეტილების მიღებაზე თავის ან სხვა პირის სასარგებლოდ იმ პირისაგან, რომელიც მოქმედებს საკუთარი ან სხვა პირის ინტერესებისათვის, პირდაპირ ან არაპირდაპირ, ფულის, ფასიანი ქაღალდის, სხვა ქონების, ქონებრივი სარგებლის ან სხვა რაიმე არამართლზომიერი უპირატესობის მოთხოვნა ან მიღება, ასევე ასეთის თაობაზე დაპირების ან შეთავაზების მიღება, მიუხედავად იმისა, განხორციელდა თუ არა ასეთი ზეგავლენა ან/და მიღებულ იქნა თუ არა ამ ზეგავლენით სასურველი შედეგი,
3. ამ მუხლის მე-2 ნაწილით გათვალისწინებული ქმედება, ჩადენილი ორგანიზებული ჯგუფის მიერ (იხ. სქოლიო 128), –

შენიშვნა:

1. ამ მუხლის პირველი ნაწილით გათვალისწინებული დანაშაულისათვის სისხლისა-მართლებრივი პასუხისმგებლობისაგან თავისუფლდება პირი, რომელმაც ამის თაობაზე ნებაყოფლობით განუცხადა სისხლის სამართლის პროცესის მწარმოებელ ორგანოს. პასუხისმგებლობისაგან გათავისუფლების შესახებ გადაწყვეტილებას იღებს სისხლის სამართლის პროცესის მწარმოებელი ორგანო."

მუხლი 340. კანონით აკრძალული საჩუქრის მიღება;

„1. მოხელის ან მასთან გათანაბრებული პირის მიერ კანონით აკრძალული საჩუქრის მიღება;

2. იგივე ქმედება, ჩადენილი არაერთგზის (იხ. სქოლიო 126)."

მუხლი 341. სამსახურებრივი სიყალბე ;

„სამსახურებრივი სიყალბე, ესე იგი მოხელის ან მასთან გათანაბრებული პირის მიერ ოფიციალურ დოკუმენტში ან დავთარში ყალბი ცნობის ან ჩანაწერის შეტანა, ანდა ყალბი დოკუმენტის შედგენა ან გაცემა, აგრეთვე საწარმოს, დაწესებულების ან ორგანიზაციის საქმეში არსებული ოფიციალური ან კერძო დოკუმენტის გაყალბება, ჩადენილი ანგარებით ან სხვა პირადი მოტივით."

მუხლი 342. სამსახურებრივი გულგრილობა;

„1. სამსახურებრივი გულგრილობა, ესე იგი მოხელის ან მასთან გათანაბრებული პირის მიერ თავისი სამსახურებრივი მოვალეობის შეუსრულებლობა ან არაჯეროვნად შესრულება მისდამი დაუდევარი დამოკიდებულების გამო, რამაც ფიზიკური ან იურიდიული პირის უფლების, საზოგადოების ან სახელმწიფოს კანონიერი ინტერესების არსებითი დარღვევა გამოიწვია;

2. იგივე ქმედება, რამაც გამოიწვია ადამიანის სიცოცხლის მოსპობა ან სხვა მძიმე შედეგი."

მუხლი 342¹. სპეციალური პენიტენციური სამსახურის მოსამსახურის ან მასთან გათანაბრებული პირის მიერ სამსახურში დადგენილი წესის დარღვევა;

„1. საქართველოს იუსტიციის სამინისტროს სისტემაში შემავალი სახელმწიფო საქვეყნებო დაწესებულების — სპეციალური პენიტენციური სამსახურის მოსამსახურის ან მასთან გათანაბრებული პირის მიერ სამსახურში დადგენილი წესის შეუსრულებლობა ან არაჯეროვნად შესრულება მისდამი დაუდევარი დამოკიდებულების გამო, რასაც შედეგად მოჰყვა პენიტენციური დაწესებულებიდან, გავყანისას/გადაყვანისას ან ექსტრადიციისას ბრალდებულის/მსჯავრდებულის გაქცევა ან/და პენიტენციური დაწესებულების საქმიანობის დეზორგანიზაცია, —

2. იგივე ქმედება, რამაც გამოიწვია ადამიანის სიცოცხლის მოსპობა ან სხვა მძიმე შედეგი;

შენიშვნა: ამ მუხლის მიზნებისათვის საქართველოს იუსტიციის სამინისტროს სისტემაში შემავალი სახელმწიფო საქვეყნებო დაწესებულების — სპეციალური პენიტენციური სამსახურის მოსამსახურესთან გათანაბრებულ პირად ითვლება საქართველოს იუსტიციის სამინისტროს საგამოძიებო დეპარტამენტის თანამშრომელი."

ინფორმაციის გამოთხოვა სასამართლოს განჩინების საფუძველზე უნდა დავყოთ რამდენიმე სამართლებრივ ნაბიჯად;

ნაბიჯი 1. შუამდგომლობის შედგენა პროკურორის მიერ;

ნაბიჯი 2. სასამართლოს მიერ განჩინების გაცემა;

ნაბიჯი 3. სახელმწიფო ინსპექტორის სამსახურსათვის განჩინების მიწოდება;

ნაბიჯი 4. გამომძიებლის მიერ საგამომძიებო მოქმედების ჩატარება და ოქმის შედგენა;

განვიხილოთ თითოეული ნაბიჯი:

ნაბიჯი 1. შუამდგომლობის შედგენა პროკურორის მიერ;

მას შემდეგ კი რაც სახეზე იქნება ზემოაღნიშნული სისხლის სამართლის კოდექსით გათვალისწინებული დანაშაული და სხვა საპროცესო მოთხოვნების დაკმაყოფილების სტანდარტი, პროკურორმა უნდა შეადგინოს შუამდგომლობა „[...] რომელშიც უნდა აისახოს ინფორმაცია იმ საგამომძიებო მოქმედების შესახებ (ასეთის არსებობის შემთხვევაში), რომელიც შუამდგომლობის წარდგენამდე ჩატარდა საქართველოს სისხლის სამართლის კოდექსით დადგენილი წესით და რომლითაც დასახული მიზანი ვერ იქნა მიღწეული.“²⁶⁸

აქ მნიშვნელოვანია განხილულ იქნეს საკითხი: პროკურორმა სასამართლოს უნდა მიმართოს ფარულ კონვერტში ჩადებული და დალუქული დოკუმენტით, თუ ჩვეულებრივ ღია სახის შუამდგომლობით, რომელიც უნდა აკმაყოფილებდეს ფარული საგამომძიებო მოქმედების დასაბუთებულობის სტანდარტებს? პასუხს ამ კითხვაზე სცემს თბილისის სააპელაციო სასამართლოს 2019 წლის 17 აისის №1გ/752-19 განჩინება, სადაც სასამართლომ გააკეთა მნიშვნელოვანი პრეცედენტული განმარტება, კერძოდ, სასამართლომ განმარტა, რომ:²⁶⁹

„საქართველოს სსსკ-ის 136-ე მუხლის 1-ლი ნაწილის თანახმად, თუ არსებობს დასაბუთებული ვარაუდი, რომ კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში ინახება სისხლის სამართლის საქმისთვის მნიშვნელოვანი ინფორმაცია, ან დოკუმენტი, პროკურორი უფლებამოსილია გამოძიების ადგილის მიხედვით, სასამართლოს მიმართოს შესაბამისი ინფორმაციის ან დოკუმენტის გამოთხოვის განჩინების გაცემის შუამდგომლობით [...]“²⁷⁰.

თბილისის სააპელაციო სასამართლო განმარტავს, რომ „აღნიშნული დებულებები ბრალდების მხარეს აძლევს უფლებამოსილებას, სისხლის სამართლის საქმისათვის აუცილებელი მტკიცებულებები მოიპოვოს საქართველოს კანონმდებლობის შესაბამისად, შუამდგომლობა მტკიცებულების მოპოვების შესახებ, უნდა ეფუძნებოდეს გარკვეულ ობიექტურ ინფორმაციებს, ყოველგვარი დასაბუთებული საფუძვლების გარეშე, კომპიუტერული ინფორმაციის გადაცემა დაუშვებელია, ამასთან, მხარე ვალდებულია გაითვალისწინოს ინფორმაციის თვისობრივი მახასიათებლები, მესამე პირების თაობაზე ინფორმაციის არსებობის შესახებ და განსაკუთრებული დასაბუთების პირობებში მოითხოვოს ამ სახის მტკიცებულების გადაცემა.“²⁷¹

„საქართველოს სსსკ-ის 136-ე მუხლის მე-4 ნაწილის თანახმად, ამ მუხლით გათვალისწინებულ საგამომძიებო მოქმედებაზე ვრცელდება ამავე კოდექსის 143² – 143¹⁰ მუხლების დებულებები, თბილისის სააპელაციო სასამართლო განმარტავს, რომ ეს ძალზედ მნიშვნელოვანი დებულებებია, თუმცა ეს სულაც არ ნიშნავს იმას, რომ საქართველოს სსსკ-ის 136-ე მუხლით გათვალისწინებულ საგამომძიებო მოქმედებებზე ფარული საგამომძიებო მოქმედებების მარეგულირებელი დებულებები ვრცელდება სრული მოცულობით ინფორმაციის გამოთხოვასა და ფარულ საგამომძიებო მოქმედებებს შორის არსებობს შინაარსობრივი მნიშვნელოვანი განმასხვავებელი განსხვავებები,

²⁶⁸ საქართველოს სისხლის სამართლის საპროცესო კოდექსი (რედ. 09/10/2009, კონსოლიდირებული 29.05.2019), მუხლი 143¹ მუხლის მე-3 ნაწილი;

²⁶⁹ იქვე.

²⁷⁰ იქვე.

²⁷¹ იქვე.

და საგამოძიებო მოქმედებების წარმოების პროცესში, ისენი გათვალისწინებული უნდა იქნეს, საგამოძიებო კოლეგია, მიუთითებს, რომ სსსკ-ის 136-ე მუხლის მე-4 ნაწილის დებულებები მიემართება იმგვარი სამართლებრივ ურთიერთობებზე, რასაც არ არეგულირებს სსსკ-ის 136-ე — 138-ე მუხლები.”²⁷²

თბილისის სააპელაციო სასამართლო განმარტავს, რომ „აღნიშნული მითითებითი ნორმის გათვალისწინება, უნდა ეხებოდეს 143²-143¹⁰ მუხლების შინაარსობრივ მხარეს და არა პროცედურულ გარემოებებს. სასამართლოსათვის მიმართვის ფორმა კი სწორედ პროცედურული საკითხია.“²⁷³

„ამ არ საგამოძიებო მოქმედებებს შორის განსხვავების ნათელი მაგალითია დასაბუთებულობის სტანდარტები. თუ სსსკ-ის 136-ე მუხლის შინაარსი პირდაპირ მიუთითებს საგამოძიებო მოქმედების ჩასატარებლად დასაბუთებული ვარაუდის საკმარისობაზე, უშუალოდ ფარული საგამოძიებო მოქმედებების ჩასატარებლად ეს საკმარისი არ არის და აუცილებელია სახეზე იყოს დემოკრატიულ საზოგადოებაში, დემოკრატიული მიზნების მიღწევა-ეროვნული უშიშროების ან საზოგადოებრივი უსაფრთხოების უზრინველსაყოფად, უწყსრიგობის ან დანაშაულის თავიდან ასაცილებლად და ასე შემდეგ, საგამოძიებო კოლეგიას მიაჩნია, რომ ამ საგამოძიებო მოქმედებებს შორის განსხვავებები თვალსაჩინოა, შესაბამისად მათი ჩატარების გარემოებებიც უნდა იყოს განსხვავებული. ფარული საგამოძიებო მოქმედებები აშკარად ოპერატიულ-სამძებრო ღონისძიებებია, რომლებიც თავის თავში აუცილებლად გულისხმობს ფარულობის, მოულოდნელობის ეფექტის არსებობას, შესაბამისად მისი გარემოებების სახელმწიფო საიდუმლოებისათვის მიკუთვნება ლოგიკური და კანონის შესაბამისია. მაგრამ ინფორმაციის გამოთხოვისათვის იგივე თვისებების მინიჭება შეუძლებელია, მნიშვნელოვანია რომ კანონის შესაბამისად დამონტაჟებული გარე სათვალთვალო კამერები აფიქსირებენ მათ მიმდებარედ ზოგად ვითარებას, და არ უთვალთვალებენ კონკრეტულ ადამიანს, მათი ინტერესი და ფოკუსი არ არის კონკრეტული ადამიანი, შესაბამისად მათი ჩანაწერები შედარებით დაბალი ხარისხით ზღუდავენ ადამიანის პირად თავისუფლებას.“²⁷⁴

ამდენად, თბილისის სააპელაციო სასამართლო განმარტავს, რომ „საქართველოს სსსკ-ის 136-ე მუხლის მე-4 ნაწილის დებულებები რეალურად მიემართება სსსკ-ის 143³-ე მუხლის დებულებებზე, რაც იმ დანაშაულთა კლასიფიკაციას გულისხმობს, რისთვისაც ნებადართულია ფარული საგამოძიებო მოქმედებების ჩატარება. ამ მოცემულობაში აშკარაა, რომ ინფორმაციის გამოთხოვის, როგორც საგამოძიებო მოქმედების პროცესი, უნდა ჩატარდეს სისხლის სამართლის საპროცესო კოდექსის 111-112-ე მუხლების დებულებების გათვალისწინებით, რის გამოც მხარე არ არის ვალდებული მიმართოს სასამართლოს დალუქული კონვერტებით, შესაბამისი შტამპებით და ა.შ.“²⁷⁵

საგამოძიებო კოლეგიის აზრით, „ამ საკითხის გადაწყვეტა, ასევე შესაძლებელია შედარებითი ანალიზის გაკეთებით — რაც უკავშირდება აცვის მხარის იგივე უფლებას მოიპოვოს კომპიუტერული ინფორმაცია, ამ შემთხვევაზე ცხადია შეუძლებელია სსსკ-ის 143²-143¹⁰ მუხლების პროცედურული საკითხების გავრცელება, დაცვის მხარე ვერ მიმართავს სასამართლოს დალუქული კონვერტებით და ინფორმაციის სახელმწიფო საიდუმლოების ნიშნების გათვალისწინებით, შესაბამისად რატომ უნდა იყოს განსხვავებული წესი ბრალდების მხარისათვის ბუნდოვანია.“²⁷⁶

შესაბამისად, პროკურორის სჭირდება საგამოძიებო მოქმედების ჩატარებისათვის აუცილებელი მტკიცებულებათა სტანდარტი და საფუძვლები, ხოლო პროცედურულად, აღნიშნული ტიპის საგამოძიებო მოქმედება თუ ის მისი შინაარსით არ სცდება 136-ე მუხლის დებულებებს და არ გადადის

²⁷² თბილისის სააპელაციო სასამართლოს 2019 წლის 17 აიხის №1გ/752-19 განჩინება

²⁷³ იქვე.

²⁷⁴ იქვე.

²⁷⁵ თბილისის სააპელაციო სასამართლოს 2019 წლის 17 აიხის №1გ/752-19 განჩინება

²⁷⁶ იქვე.

მინაარსობრივ ფარულ საგამოძიებო მოქმედებებში — არ საჭიროებს ფარული საგამოძიებო მოქმედებისათვის დამახასიათებელ პროცედურულ ნაბიჯებს.

ნაბიჯი 2. სასამართლოს მიერ განჩინების გაცემა;

მოსამართლე პროკურორის შუამდგომლობისა და მისი დასაბუთებისთვის საჭირო, თანდართული მასალის სასამართლოში წარდგენიდან არაუგვიანეს 24 საათისა განიხილავს შუამდგომლობას [...] „საქართველოს სისხლის სამართლის საპროცესო კოდექსის 112-ე მუხლით დადგენილი წესით... მოსამართლეს შეუძლია შუამდგომლობა ზეპირი მოსმენის გარეშე განიხილოს. მოსამართლე შუამდგომლობას ზეპირი მოსმენით, პროკურორის მონაწილეობით, დახურულ ან ღია სასამართლო სხდომაზე განიხილავს და განჩინებით იღებს გადაწყვეტილებას [...] საგამოძიებო მოქმედების ჩატარების ნებართვის გაცემის შესახებ ან მისი ჩატარების ნებართვის გაცემაზე უარის თქმის შესახებ. განჩინება დგება 4 ეგზემპლარად, რომელთაგან ერთი რჩება სასამართლოში, ორი გადაეცემა შუამდგომლობის წარმდგენ პროკურორს ან შესაბამისი საგამოძიებო ორგანოს უფლებამოსილ წარმომადგენელს, რომელთაგან ერთი მიეწოდება შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს.“²⁷⁸

ნაბიჯი 3. სახელმწიფო ინსპექტორის სამსახურსათვის განჩინების მიწოდება;

აღნიშნული ნაბიჯი არის პროცედურული და ჩვენის აზრით საგამოძიებო მოქმედება თუ ის მისი მინაარსით არ სცდება 136-ე მუხლის დებულებებს და არ გადადის შინაარსობრივ ფარულ საგამოძიებო მოქმედებებში — არ საჭიროებს სახელმწიფო ინსპექტორისათვის ინფორმაციის მიწოდებას, მაგრამ დღევანდელი მოცემულობით, სასამართლო მაინც აწვდის მსგავს რეკვიზიტებს პერსონალურ მონაცემთა დაცვის ინსპექტორს, აღნიშნულის პროცედურა შემდეგია: [...] „განჩინება, რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარგოლუციო ნაწილს, სასამართლოს მიერ მიეწოდება სახელმწიფო ინსპექტორის სამსახურს. მოსამართლის განჩინების ეგზემპლარები შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს და სახელმწიფო ინსპექტორის სამსახურს წარედგინება განჩინების გამოტანისთანავე, დაუყოვნებლივ, მაგრამ არაუგვიანეს 48 საათისა. მატერიალური (დოკუმენტური) სახით. თუ ამ ნაწილით გათვალისწინებული ფარული საგამოძიებო მოქმედების ჩატარების ნებართვის გაცემის შესახებ ან მისი ჩატარების ნებართვის გაცემაზე უარის თქმის შესახებ განჩინება მოსამართლემ სახელმწიფო ინსპექტორის სამსახურის მიერ წარმოებულ სისხლის სამართლის საქმეზე გამოიტანა, სასამართლოს მიერ ერთი განჩინება (განჩინების მე-4 ეგზემპლარი), რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარგოლუციო ნაწილს. განჩინების გამოტანისთანავე, დაუყოვნებლივ, მაგრამ არაუგვიანეს 48 საათისა, მატერიალური (დოკუმენტური) სახით მიეწოდება ზედამხედველ მოსამართლეს.“²⁷⁹

ნაბიჯი 4. გამოძიებლის მიერ საგამოძიებო მოქმედების ჩატარება და ოქმის შედგენა;

შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს წარმომადგენელი საგამოძიებო მოქმედების მიმდინარეობის შესახებ [...] ადგენს ოქმს, ოქმში ზუსტად უნდა იყოს აღნიშნული საგამოძიებო მოქმედების ჩატარების სამართლებრივი საფუძველი, მისი დაწყებისა და

²⁷⁷ საქართველოს სისხლის სამართლის საპროცესო კოდექსი (რედ. 09/10/2009, კონსოლიდირებული 29.05.2019). მუხლი 143³ მუხლის მე-5 ნაწილი;

²⁷⁸ საქართველოს სისხლის სამართლის საპროცესო კოდექსი (რედ. 09/10/2009, კონსოლიდირებული 29.05.2019). მუხლი 143³ მუხლის მე-5 ნაწილი;

²⁷⁹ იქვე.

დასრულების დრო, ოქმის შედგენის ადგილი, ჩატარებული საგამოძიებო მოქმედების სახე და მისი ჩატარებისას გამოყენებული ტექნიკური საშუალებები, საგამოძიებო მოქმედების ჩატარების ადგილი, საგამოძიებო მოქმედების ობიექტი და სხვა მნიშვნელოვანი რეკვიზიტები.

ამჟერად განვიხილოთ საგამოძიებო მოქმედება - კომპიუტერული სისტემიდან ინფორმაციის გამოთხოვა გადაუდებელი აუცილებლობის შემთხვევაში;

ნაბიჯი N1; დადგენილების გამოტანა პროკურორის მიერ;

ნაბიჯი N2; საგამოძიებო მოქმედების ოქმის შედგენა;

ნაბიჯი N3; პერსონალურ მონაცემთა დაცვის ინსპექტორისათვის ინფორმაციის მიწოდება;

ნაბიჯი N4; საგამოძიებო მოქმედების კანონიერების შემოწმების შესახებ შეამდგომლობის შეტანა;

ნაბიჯი N5; სასამართლოს მიერ განჩინების გაცემა;

შესაძლებელია თუარა კომპიუტერული სისტემიდან ინფორმაციის გამოთხოვა ბრალდების მხარის მიერ გადაუდებელი აუცილებლობის შემთხვევაში, კანონი პროკურორს ამის სამართლებრივ შესაძლებლობასაც აძლევს, კერძოდ:

ნაბიჯი N1; დადგენილების გამოტანა პროკურორის მიერ;

გადაუდებელი აუცილებლობის შემთხვევაში, როდესაც დაყოვნებამ შეიძლება გამოიწვიოს საქმისთვის (გამოძიებისთვის) მნიშვნელოვანი ფაქტობრივი მონაცემების განადგურება ან შეუძლებელი გახადოს ამ მონაცემების მოპოვება, საგამოძიებო მოქმედება კომპიუტერული სისტემიდან ინფორმაციის გამოთხოვა შეიძლება ჩატარდეს/დაიწყოს მოსამართლის განჩინების გარეშე, პროკურორის მოტივირებული დადგენილებით, პროკურორის დადგენილება უნდა შეიცავდეს შესაბამის რეკვიზიტებს [...] დადგენილების შედგენის თარიღი და ადგილი; მითითება საქართველოს სისხლის სამართლის კოდექსის იმ მუხლზე, რომლითაც მიმდინარეობს გამოძიება; პროკურორის სახელი და გვარი, ხელმოწერა; საიდუმლოების აღმნიშვნელი გრიფი; ბეჭედი,²⁸⁰ ხოლო დადგენილების სარგოლუყოი ნაწილი უნდა შეიცავდეს „მითითებას ფარული საგამოძიებო მოქმედების ობიექტის/ობიექტების, აგრეთვე განსახორციელებელი ფარული საგამოძიებო მოქმედების სახის შესახებ და უნდა განსაზღვრავდეს მოქმედების განხორციელების პერიოდს (მისი დაწყებისა და დასრულების თარიღებისა და დროის მითითებით), რომელიც არ უნდა აღემატებოდეს 48 საათს.“²⁸¹

ნაბიჯი N2; საგამოძიებო მოქმედების ოქმის შედგენა;

შესაბამისი უფლებამოსილების მქონე სახელმწიფო ორგანოს წარმომადგენელი საგამოძიებო მოქმედების მიმდინარეობის შესახებ [...] ადგენს ოქმს, ოქმში ზუსტად უნდა იყოს აღნიშნული საგამოძიებო მოქმედების ჩატარების სამართლებრივი საფუძველი, მისი დაწყებისა და დასრულების დრო, ოქმის შედგენის ადგილი, ჩატარებული საგამოძიებო მოქმედების სახე და მისი ჩატარებისას გამოყენებული ტექნიკური საშუალებები, საგამოძიებო მოქმედების ჩატარების ადგილი, საგამოძიებო მოქმედების ობიექტი და სხვა მნიშვნელოვანი რეკვიზიტები.

²⁸⁰ საქართველოს სისხლის სამართლის საპროცესო კოდექსი (რედ. 09/10/2009, კონსოლიდირებული 29.05.2019). მუხლი 143³ მუხლის მე-5 ნაწილი;

²⁸¹ საქართველოს სისხლის სამართლის საპროცესო კოდექსი (რედ. 09/10/2009, კონსოლიდირებული 29.05.2019). მუხლი 143³ მუხლის მე-5 ნაწილი;

ნაბიჯი N3; პერსონალურ მონაცემთა დაცვის ინსპექტორისათვის ინფორმაციის მიწოდება;

აღნიშნული ნაბიჯი არის პროცედურული, და ჩვენის აზრით საგამოძიებო მოქმედება თუ ის მისი შინაარსით არ სცდება 136 - ე მუხლის დებულებებს და არ გადადის შინაარსობრივ ფარულ საგამოძიებო მოქმედებებში - არ საჭიროებს სახელმწიფო ინსპექტორისათვის ინფორმაციის მიწოდებას. მაგრამ დღევანდელი მოცემულობით, ვინაიდან სასამართლო მაინც აწვდის მსგავს რეკვიზიტებს პერსონალურ მონაცემთა დაცვის ინსპექტორს, მიზანშეწონილია პროკურატურამაც განახორციელოს აღნიშნული.

პროცედურა შემდეგია:

გადაუდებელი აუცილებლობის შემთხვევაში „ფარული საგამოძიებო მოქმედების ჩატარების შესახებ პროკურორის დადგენილებას, რომელიც შეიცავს მხოლოდ რეკვიზიტებსა და სარგოლუციო ნაწილს, ფარული საგამოძიებო მოქმედების დადგენილებაში მითითებული დაწყების დროიდან არაუგვიანეს 12 საათისა პროკურორი ან პროკურორის დავალებით გამომძიებელი მატერიალური (დოკუმენტური) სახით წარუდგენს სახელმწიფო ინსპექტორის სამსახურს.“²⁸²

ნაბიჯი N4; საგამოძიებო მოქმედების კანონიერების შემოწმების შესახებ შპ. მდგომლობის შეტანა;

„პროკურორი ვალდებულია ფარული საგამოძიებო მოქმედების დადგენილებაში მითითებული დაწყების დროიდან არაუგვიანეს 24 საათისა მიმართოს რაიონულ (საქალაქო) სასამართლოს, რომლის სამოქმედო ტერიტორიაზედაც ჩატარდა/ტარდება აღნიშნული ფარული საგამოძიებო მოქმედება, ან გამოძიების ადგილის მიხედვით სასამართლოს შუამდგომლობით გადაუდებელი აუცილებლობისას ჩატარებული/ მიმდინარე ფარული საგამოძიებო მოქმედების კანონიერად ცნობის შესახებ. შუამდგომლობაში პროკურორმა უნდა დაასაბუთოს რომ [...]“²⁸³

არსებობს დასაბუთებული ვარაუდი, რომ პირს, რომლის მიმართაც უნდა ჩატარდეს [...] „საგამოძიებო მოქმედება, ჩადენილი აქვს ამ ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული რომელიმე დანაშაული („დანაშაულთან პირდაპირ კავშირში მყოფი პირი“), ან პირი იღებს ან გადასცემს დანაშაულთან პირდაპირ კავშირში მყოფი პირისათვის განკუთვნილ ან მისგან მომდინარე ინფორმაციას, ან დანაშაულთან პირდაპირ კავშირში მყოფი პირი იყენებს პირის საკომუნიკაციო საშუალებებს.“²⁸⁴

„გამოძიება დაწყებულია ან/და სისხლისსამართლებრივი დევნა ხორციელდება განზრახი მძიმე ან და განსაკუთრებით მძიმე დანაშაულის ან საქართველოს სისხლის სამართლის კოდექსის შემდეგი მუხლებითა და თავით გათვალისწინებული რომელიმე დანაშაულის გამო: 134-ე მუხლი, 139-ე მუხლის მე-2 ნაწილი, 143-ე მუხლის პირველი ნაწილი, 143³ მუხლის პირველი ნაწილი, 180-ე მუხლის პირველი ნაწილი, 181-ე მუხლის პირველი ნაწილი, 186-ე მუხლის მე-2 ნაწილი, 187-ე მუხლის მე-2 ნაწილი, 198-ე მუხლის პირველი ნაწილი, 210-ე მუხლის პირველი ნაწილი, 253-ე მუხლის პირველი ნაწილი, 254-ე მუხლის პირველი და მე-2 ნაწილები, 255¹, 259⁴ და 284-ე მუხლები, 285-ე მუხლის პირველი ნაწილი, 286-ე და 287-ე მუხლები, 288-ე მუხლის პირველი და მე-2 ნაწილები, 289-ე, 290-ე და 292-ე — 302-ე მუხლები, 303-ე მუხლის პირველი — მე-3 ნაწილები, 304-ე მუხლის

²⁸² საქართველოს სისხლის სამართლის საპროცესო კოდექსი (რედ. 09/10/2009, კონსოლიდირებული 29.05.2019). მუხლი 143³ მუხლის 6-ე ნაწილი;:

²⁸³ საქართველოს სისხლის სამართლის საპროცესო კოდექსი (რედ. 09/10/2009, კონსოლიდირებული 29.05.2019). მუხლი 143³ მუხლის მე-5 ნაწილი;

²⁸⁴ იქვე, მე-2 ნაწილის „ბ“ ქვეპუნქტი;

პირველი ნაწილი, 305-ე, 306-ე და 306¹ მუხლები, 318-ე მუხლის პირველი ნაწილი, 322¹ მუხლი, XXXIX თავი, 344² მუხლის პირველი ნაწილი;²⁸⁵

[...] საგამოძიებო მოქმედების ჩატარება გამოწვეულია გადაუდებელი საზოგადოებრივი საჭიროებით და არის დემოკრატიულ საზოგადოებაში ლეგიტიმური მიზნის მისაღწევად — ეროვნული უშიშროების ან საზოგადოებრივი უსაფრთხოების უზრუნველსაყოფად, უწესრიგობის ან დანაშაულის ჩადენის თავიდან ასაცილებლად, ქვეყნის ეკონომიკური კეთილდღეობის ინტერესების ან სხვა პირთა უფლებებისა და თავისუფლებების დასაცავად — აუცილებელი, მისი მიღწევის შესაფერისი და პროპორციული საშუალება;²⁸⁶

ჩატარებული [...] საგამოძიებო მოქმედების შედეგად მოპოვებული იქნება გამოძიებისათვის არსებითი მნიშვნელობის მქონე ის ინფორმაცია, რომლის სხვა საშუალებით მოპოვება შეუძლებელია ან გაუმართლებლად დიდ ძალისხმევას [...]”²⁸⁷, საჭიროებდა.

„იმ გარემოებების არსებობა, რომლებმაც განაპირობა ფარული საგამოძიებო მოქმედების მოსამართლის განჩინების გარეშე ჩატარება.“²⁸⁸

ნაბიჯი N5; საგამოძიებო მოქმედების კანონიერების შემოწმების შესახებ განჩინების გამოტანა;

შუამდგომლობის განხილვისას მოსამართლე ამოწმებს, შეესაბამება თუ არა ჩატარებული/მიმდინარე ფარული საგამოძიებო მოქმედება საქართველოს სსკ-ის 143³ მუხლის მე-2 ნაწილის მოთხოვნებს და აუცილებელი იყო თუ არა აღნიშნული ფარული საგამოძიებო მოქმედების გადაუდებლად ჩატარება/დაწყება და განჩინებით იღებს გადაწყვეტილებას, ჩატარებული ფარული საგამოძიებო მოქმედების კანონიერად ცნობის შესახებ.

6.2. კომპიუტერული სისტემიდან ციფრული ინფორმაციის გამოთხოვის სამართლებრივი საფუძვლები და პროცედურები დაცვის მხარისათვის

ზემოაღნიშნული რეგულაციები შეეხება ბრალდების მხარის მიერ განსახორციელებელ მოქმედებებს, მაგრამ რა რეგულაციასთან გვაქვს საქმე, როდესაც დაცვის მხარეს სურს კომპიუტერული სისტემიდან ინფორმაციის გამოთხოვა - ?

ასეთ შემთხვევაში კანონმდებელი დაცვის მხარეს 2017 წლის 27 იანვრამდე არ აძლევდა უფლებამოსილებას ეწარმოებინა ინფორმაციის გამოთხოვა კომპიუტერული სისტემიდან, მაგრამ 2017 წლის 27 იანვარს, საქართველოს საკონსტიტუციო სასამართლოს პირველმა კოლეგიამ მიიღო გადაწყვეტილება, რომლის თანახმადაც - საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლის პირველი და მე-4 ნაწილების ის ნორმატიული შინაარსი, რომელიც გამორიცხავდა დაცვის მხარის მიერ კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში შენახული ინფორმაციის ან დოკუმენტის გამოთხოვის შესახებ განჩინების გაცემის შუამდგომლობით სასამართლოსათვის მიმართვას, ცნობილ იქნა არაკონსტიტუციურად საქართველოს კონსტიტუციის მე-40 მუხლის მე-3 პუნქტთან და 42-ე მუხლის პირველ და მე-3 პუნქტებთან მიმართებით.

²⁸⁵ იქვე. მე-2 ნაწილის „ა“ ქვეპუნქტი;

²⁸⁶ იქვე მე-2 ნაწილის „გ“ ქვეპუნქტი;

²⁸⁷ საქართველოს სისხლის სამართლის საპროცესო კოდექსი (რედ. 09/10/2009, კონსოლიდირებული 29.05.2019). მუხლი 143³ მუხლის მე-2 ნაწილის „დ“ ქვეპუნქტი;

²⁸⁸ იქვე. მე-5 ნაწილი;

თბილისის სააპელაციო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიამ, 2017 წლის გადაწყვეტილებაში განმარტა, რომ „საქართველოს საკონსტიტუციო სასამართლოს 2017 წლის 27 იანვრის №1/1/650,699 გადაწყვეტილებით არაკონსტიტუციურად იქნა ცნობილი საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლის პირველი და მე-4 ნაწილების მხოლოდ ზემოხსენებული ნორმატიული შინაარსი, ანუ ნორმის საკონსტიტუციო სასამართლოს გადაწყვეტილებაში ასახული შინაარსობრივი მხარე და არა მთლიანად ნორმა, რითაც შეზღუდვა მოიხსნა დაცვის მხარისათვის და მასაც მიეცა შესაძლებლობა ინფორმაცია მოიპოვოს პროკურორისათვის დადგენილი სტანდარტით და იმავე წესით, როგორცაა მას მოიპოვებდა ბრალდების მხარე. შესაბამისად, საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლის მიხედვით ინფორმაციის გამოთხოვაზე ვრცელდება ფარული საგამოძიებო მოქმედების გაცემისათვის დადგენილი წესი მხოლოდ შუამდგომლობის დასაბუთებისა და წარდგენის სტანდარტის ნაწილში ორივე მხარისათვის თანაბრად, ხოლო სხვა ნორმატიული შინაარსი რაც დამახასიათებელია სპეციფიკურად ფარული საგამოძიებო მოქმედებებისათვის ეხება მხოლოდ ბრალდების მხარეს. გამომდინარე იქიდან, რომ საქართველოს სისხლის სამართლის საპროცესო კოდექსის 143²⁸⁹ - 143²⁹⁰ - ე მუხლების შესაბამისად, სასამართლოსთვის შუამდგომლობით მიმართვის სუბიექტს წარმოადგენს პროკურორი და ამასთან, კომპიუტერულ სისტემაში დაცული ინფორმაციის გამოთხოვა განსხვავდება ფარული საგამოძიებო მოქმედებისაგან, რომელთა დაკავშირებითაც დაცვის მხარეს არანაირი უფლებამოსილება არ გააჩნია.“²⁸⁹

საკონსტიტუციო სასამართლოს მიერ განხილული საქმე ეხებოდა მოქალაქეების საღია ხურციძის და დიმიტრი ლომიძის საკონსტიტუციო სარჩელს საქართველოს პარლამენტის წინააღმდეგ, საკონსტიტუციო სარჩელების და წარდგენილი საქმის მასალების თანახმად ირკვეოდა, რომ: [...] „მოსარჩელე საღია ხურციძის ბრალი დაედო სისხლის სამართლის კოდექსის 260-ე მუხლის მე-3 ნაწილის „ა“ ქვეპუნქტით გათვალისწინებული ქმედების ჩადენისათვის. მოსარჩელის განმარტებით, ძირითადი მტკიცებულებები, რომელთაც ეფუძნება ბრალდების შესახებ დადგენილება, არის დაკავების და ჩხრეკის ოქმი, ასევე ოთხი პოლიციელის ჩვენება, თუმცა, მისი მტკიცებით, ერთ-ერთი პოლიციელი შემთხვევის ადგილზე საერთოდ არ იმყოფებოდა და, შესაბამისად, დაკავებისა და ჩხრეკის პროცესში არ მონაწილეობდა. მოსარჩელე აღნიშნავს, რომ პოლიციელის არყოფნა შესაძლოა დადასტურდეს როგორც შემთხვევის ადგილზე განთავსებული სათვალთვალო ვიდეოკამერებით, ისე სატელეფონო კომპანიის საკუთრებაში არსებული ჩანაწერებით, ხოლო დაფიქსირებული ინფორმაცია საკმარისია ჩხრეკისა და ამოღების ოქმის, ასევე მის საფუძველზე მოპოვებულ მტკიცებულებათა დაუშვებლად ცნობისთვის. თუმცა, მოსარჩელის განმარტებით, მოცემული ინფორმაციის გამოთხოვის შესახებ შუამდგომლობა სასამართლომ სადავო ნორმების საფუძველზე არ დააკმაყოფილა და აღნიშნა, რომ კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესახებ საშუალებიდან ინფორმაციის გამოთხოვის ჩატარების თაობაზე სასამართლოსთვის შუამდგომლობით მიმართვის უფლება დაცვის მხარეს არ გააჩნია.“²⁹⁰

ხოლო მოსარჩელე [...] „დიმიტრი ლომიძის 2015 წლის 19 აპრილს ბრალი დაედო სისხლის სამართლის კოდექსის 353-ე მუხლით გათვალისწინებულ დანაშაულში, კერძოდ, პოლიციის თანამშრომლებისთვის წინააღმდეგობის გაწევაში სიტყვიერი და ფიზიკური შეურაცხყოფის მიყენების გზით როგორც შემთხვევის ადგილზე, ასევე პოლიციის განყოფილების ადმინისტრაციულ შენობაში. მოსარჩელე არ აღიარებს პოლიციის თანამშრომლებისთვის წინააღმდეგობის გაწევის ფაქტს და აღნიშნავს, რომ თავდასხმა განხორციელდა პოლიციელთა მიერ, ხოლო მისი ქმედებები

²⁸⁹ თბილისის სააპელაციო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიის განჩინება 1გ/960-17 (2017-07-19)

²⁹⁰ საქართველოს საკონსტიტუციო სასამართლოს პირველი კოლეგიის გადაწყვეტილება № 1/1/650,699 — 2017 წლის 27 იანვარი. ქ. ბათუმი;

მიზნად ისახავდა მხოლოდ თავდაცვას. მოსარჩელე აღნიშნავს, რომ როგორც შემთხვევის ადგილზე, ასევე პოლიციის განყოფილების ადმინისტრაციულ შენობაში განთავსებულია სათვალთვალო კამერები, თუმცა მათი ვიდეოჩანაწერის ასლის მიღება სადავო ნორმათა მოქმედების პირობებში მან ვერ შეძლო. მოსარჩელე მითითა, რომ მან ჩანაწერთა გამოთხოვის მოთხოვნით მიმართა თბილისის საქალაქო სასამართლოს, თუმცა სასამართლომ მისი შუამდგომლობა არ დააკმაყოფილა იმ გარემოებაზე მითითებით, რომ აღნიშნული სახის ჩანაწერების გამოთხოვის უფლება მხოლოდ პროკურორს გააჩნია.²⁹¹

ორივე მოსარჩელის [...] განმარტებით, „სწორედ სადავო ნორმების საფუძველზე, დაცვის მხარეს არ მიუწვდება ხელი კომპიუტერულ მონაცემებთან დაკავშირებულ საგამოძიებო მოქმედებებზე, კერძოდ, სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლის პირველი ნაწილით დაცვის მხარე ამორიცხვულია სასამართლოსადმი აღნიშნული ინფორმაციის გამოთხოვის შუამდგომლობით მიმართვის უფლებამოსილების მქონე სუბიექტთა წრიდან, ხოლო იმავე ნორმის მეოთხე ნაწილი მითითებს კომპიუტერულ მონაცემებთან მიმართებით იმ ნორმების გამოყენების აუცილებლობაზე, რომლებიც საგამოძიებო მოქმედებების სუბიექტად მხოლოდ პროკურორს ასახელებს.“²⁹²

საკონსტიტუციო სასამართლომ განმარტა შემდეგი:

„[...] კომპიუტერული ტექნოლოგიის უპრეცედენტო სისწრაფით განვითარება ნებისმიერი ტიპის (წერილობითი დოკუმენტაცია, ვიდეო ან აუდიო ჩანაწერი თუ ფოტომასალა, საჯარო თუ დაცული/კონფიდენციალური ან/და საიდუმლო ინფორმაცია) ინფორმაციის ელექტრონული დაარქივების საშუალებას იძლევა პორტატული სახით. საჯარო დაწესებულებები, კერძო ორგანიზაციები და ფიზიკური პირები მონაცემის შენახვა-დაარქივების პროცესში სულ უფრო ფართოდ იყენებენ ციფრულ ტექნოლოგიებს. შესაბამისად, სისხლის სამართლის საქმეთა გამოძიება-განხილვისას სულ უფრო ფართოდ ხდება ციფრული მტკიცებულებების სახით კომპიუტერული მონაცემების გამოყენება. მაგალითად, პოლიციელის ფორმაზე დამაგრებული ვიდეორეკორდის გამოყენებით მოპოვებული ინფორმაცია, ე.წ. ქუჩის კამერების ჩანაწერები, მობილური ოპერატორების ინფორმაცია მომსახურე ანძების შესახებ, ინფორმაცია არქივიდან, საჯარო და სამოქალაქო რეესტრიდან, ინფორმაცია პირის მიერ სახელმწიფო საზღვრის კვეთის თაობაზე და ა.შ. აღნიშნულიდან გამომდინარე, აშკარაა, რომ სადავო ნორმით იზღუდება დაცვის მხარის წვდომა სისხლის სამართლის საქმისათვის რელევანტური ინფორმაციის ფართო სპექტრზე. დაცვის მხარეს ერთმევა დაცვისათვის მნიშვნელოვანი ციფრული ინფორმაციის დამოუკიდებლად მოპოვების შესაძლებლობა და დაცვის ეფექტიანად განხორციელება მნიშვნელოვანწილად ხდება დამოკიდებული ბრალდების მხარეზე, რომელსაც მოქმედი სისხლის საპროცესო კანონმდებლობით უფლება აქვს არ დააკმაყოფილოს დაცვის მხარის შუამდგომლობა და არ გამოითხოვოს დაცვისათვის მნიშვნელოვანი კომპიუტერული მონაცემების შემცველი ინფორმაცია. სადავო ნორმა ზღუდავს მხარეთა თანასწორობის პრინციპს და შესაბამისად ზღუდავს საქართველოს კონსტიტუციის 42-ე მუხლის პირველი პუნქტით დაცულ უფლებას.“²⁹³

„[...] შევიტყობითობის პრინციპი ეფუძნება მხარეთა თანაბარ შესაძლებლობას, აღიჭურვონ სათანადო საპროცესო ინსტრუმენტებით და გამოიყენონ ისინი საიმისოდ, რათა წარადგინონ მათი პოზიციების სასარგებლო არგუმენტები. იმავდროულად, ამ პრინციპის უმთავრესი მიზანი არის სწორი გადაწყვეტილების მიღების ხელშეწყობა და ამ მიზნისთვის ეს პრინციპი ეყრდნობა

²⁹¹ საქართველოს საკონსტიტუციო სასამართლოს პირველი კოლეგიის გადაწყვეტილება № 1/1/650,699 — 2017 წლის 27 იანვარი, ქ. ბათუმი;

²⁹² საქართველოს საკონსტიტუციო სასამართლოს პირველი კოლეგიის გადაწყვეტილება № 1/1/650,699 — 2017 წლის 27 იანვარი, ქ. ბათუმი;

²⁹³ საქართველოს საკონსტიტუციო სასამართლოს პირველი კოლეგიის გადაწყვეტილება № 1/1/650,699 — 2017 წლის 27 იანვარი, ქ. ბათუმი, აბზაცი 16;

ორივე მხარის მიერ არგუმენტების თავისუფლად წარდგენის შესაძლებლობას“ (საქართველოს საკონსტიტუციო სასამართლოს 2016 წლი 30 სექტემბრის გადაწყვეტილება №1/8/594 საქმეზე „საქართველოს მოქალაქე ხათუნა შუბითიძე საქართველოს პარლამენტის წინააღმდეგ“, ვკ, 27). იმ პირობებში როდესაც საქართველოს კანონმდებლობა არ იცნობს სასამართლოს ე.წ. ლეგალურ სუბსიდიარულ აქტივობას, მხარეს უნდა ჰქონდეს საქმისწარმოებაზე სამართლებრივი გავლენის მოხდენის მტკიცებულების იმ პირობებში მოპოვება-წარდგენის და საკუთარი ინტერესების დაცვის გონივრული შესაძლებლობა, რომელიც არ აყენებს მას მოწინააღმდეგე მხარესთან შედარებით არსებითად არახელსაყრელ მდგომარეობაში.“²⁹⁴

„სამართალწარმოების სამართლიანობა მნიშვნელოვანწილად არის დამოკიდებული მხარეთა საპროცესო თანასწორობაზე, რაც გულისხმობს სამართალწარმოების მხარეებისათვის თანაბარი გონივრული შესაძლებლობების მინიჭებას მოიპოვონ და წარმოადგინონ მტკიცებულებები. მხარეთა თანასწორობა ფარდობითი ხასიათისაა და მოწინააღმდეგე მხარესთან შედარების მიზანია სამართლიანი ბალანსის უზრუნველყოფა მხარეებს შორის.“²⁹⁵

სასამართლომ სადავო ნორმების ანალიზის შედეგად დაადგინა: „[...] რომ მხარეთა საგამოძიებო უფლებების ზოგადი რეგულირებისაგან განსხვავებული წესის დადგენის საფუძველს რეგულირების ობიექტი – კომპიუტერული წესით შენახული ინფორმაცია და დოკუმენტაცია წარმოადგენს. კანონმდებლობა არ განმარტავს, რას მოიცავს ნორმით გათვალისწინებული ტერმინი „ინფორმაცია და დოკუმენტი“. თუმცა სისხლის სამართლის საპროცესო კოდექსის მე-3 მუხლის 23-ე ნაწილი განმარტავს ტერმინ „მტკიცებულებას“ როგორც „სასამართლოში წარდგენილი ინფორმაცია... რომლის საფუძველზედაც მხარეები სასამართლოში ადასტურებენ ან უარყოფენ ფაქტებს, სამართლებრივად აფასებენ მათ, ასრულებენ მოვალეობებს, იცავენ თავიანთ უფლებებსა და კანონიერ ინტერესებს, ხოლო სასამართლო ადგენს, არსებობს თუ არა ფაქტი ან ქმედება, რომლის გამოც ზორციელდება სისხლის სამართლის პროცესი, ჩაიდინა თუ არა ეს ქმედება გარკვეულმა პირმა, დამნაშავეა თუ არა იგი“, ხოლო ტერმინი დოკუმენტი განმარტებულია როგორც „ნებისმიერი წყარო, რომელშიც ინფორმაცია აღბეჭდილია სიტყვიერ-ნიშნობრივი ფორმით ან/და ფოტო-, კინო-, ვიდეო-, ბეგრისა თუ სხვა ჩანაწერის სახით ან სხვა ტექნიკური საშუალების გამოყენებით“.²⁹⁶ ამდენად, სადავო ნორმების მოქმედება ვრცელდება კომპიუტერული წესით შენახულ ნებისმიერ მონაცემზე, რომელიც ხასიათდება რელევანტურობით და ეხება სსსკ-ის მე-3 მუხლის 23-ე ნაწილში მითითებულ საკითხებს. მათ შორის, კონსტიტუციურ სარჩელებში მითითებულ ვიდეორჩანაწერებზეც, გასაჩივრებული ნორმების მოქმედება ასევე არ შემოისაზღვრება რომელიმე კონკრეტული სახის დანაშაულთან დაკავშირებული გამოძიებით. შესაბამისად, კანონმდებლობა სპეციალურ მოწესრიგებას ადგენს რა „კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში“ განთავსებული მტკიცებულებათა სასამართლო წესით გამოთხოვის შესახებ შეამდგომლობის დაყენებასთან დაკავშირებით, დაცვის მხარის უზღუდავ სხენებულ შეამდგომლობის დაყენების უფლებას ნებისმიერ დანაშაულთან დაკავშირებული საქმის განხილვისას კომპიუტერული წესით შენახული ნებისმიერი მონაცემის (მათ შორის საჯარო ინფორმაციის) მიმართ.“²⁹⁷

²⁹⁴ საქართველოს საკონსტიტუციო სასამართლოს პირველი კოლეგიის გადაწყვეტილება №1/1/650,699 — 2017 წლის 27 იანვარი, ქ. ბათუმი, აბზაცი 8;

²⁹⁵ საქართველოს საკონსტიტუციო სასამართლოს პირველი კოლეგიის გადაწყვეტილება №1/1/650,699 — 2017 წლის 27 იანვარი, ქ. ბათუმი, აბზაცი 9;

²⁹⁶ საქართველოს საკონსტიტუციო სასამართლოს პირველი კოლეგიის გადაწყვეტილება №1/1/650,699 — 2017 წლის 27 იანვარი, ქ. ბათუმი, აბზაცი 14;

²⁹⁷ საქართველოს საკონსტიტუციო სასამართლოს პირველი კოლეგიის გადაწყვეტილება №1/1/650,699 — 2017 წლის 27 იანვარი, ქ. ბათუმი, აბზაცი 15;

„თანასწორობის და შევიძრებითობის უფლების შეზღუდვისას მნიშვნელოვანია დადგინდეს რა გავლენის მატარებელია შეზღუდვა მხარის უფლებების რეალიზაციაზე და რა გავლენის მოხდენა შეუძლია აღნიშნულ შეზღუდვას სასამართლოს გადაწყვეტილებაზე.“²⁹⁸

სასამართლოს მსჯელობით: „[...] განსახილველ საქმეში სადავო რეგულირებით კანონმდებელი სრულად ართმევს დაცვის მხარეს კომპიუტერული წესით შენახული ინფორმაციის, ანდა დოკუმენტის გამოთხოვის შესახებ სასამართლოსთვის მიმართვის უფლებას ნებისმიერი ტიპის ინფორმაციის მიმართ იმისდა მიუხედავად ზღუდავს თუ არ ეს ინფორმაცია შესაძლოა პირთა კონსტიტუციით დაცულ უფლებებს ან უქმნის თუ არა მისი გადაცემა საფრთხეს კონსტიტუციით დაცულ სხვა სიკეთეს. აღნიშნული უფლებამოსილების მხოლოდ პროკურორისთვის მინიჭებით იქმნება საპროცესო რეალობა, სადაც დაცვის მხარეს არ აქვს შესაძლებლობა ბრალდების პოზიციას დაუპირისპიროს დასაბუთებული კონტრარგუმენტები, როდესაც გამამართლებელი მტკიცებულებები შენახულია კომპიუტერული წესით. დაცვის მხარის მიერ კომპიუტერული მტკიცებულების მოპოვება სრულად უკავშირდება ბრალდების მხარის „კეთილ ნებას“ მათ შორის, თუნდაც აღნიშნული აფუძნებდეს გონივრულ ეჭვს დაცვის ქვეშ მყოფი პირის ბრალეულობის შესახებ ანდა წარმოადგენდეს ალიბს.“²⁹⁹

„სადავო რეგულირება ზღუდავს როგორც მხარეთა საპროცესო თანასწორობის, ასევე სამართალწარმოების შევიძრებითობის პრინციპის განხორციელებას, აბრკოლებს საქმის გარემოებათა ყოველმხრივი გამოკვლევის შესაძლებლობას, ვინაიდან იმ პირობებში, როდესაც კანონმდებლობა სასამართლოს მედიაციის როლს ანიჭებს და უკრძალავს საკუთარი ინიციატივით მტკიცებულების მოპოვებასა თუ გამოკვლევას, დაცვის მხარე მისთვის მნიშვნელოვანი მტკიცებულებების მოპოვების ნაწილში დამოკიდებულია ბრალდების მხარის დისკრეციულ უფლებამოსილებაზე. სადავო რეგულირება ქმნის იმის საფრთხეს, რომ ცალკეულ შემთხვევებში სასამართლო განხილვის შედეგი დაეფუძნოს ბრალდების მხარის გულგრილობას, შეცდომას, ანდა უფლებამოსილების ბოროტად გამოყენებას და პირს პასუხისმგებლობა დაეკისროს ისე, რომ ვერ დაიყვას თავი ბრალდებისაგან.“³⁰⁰

„კომპიუტერული სისტემებიდან ინფორმაციის გამოთხოვაზე გადაწყვეტილებას იღებს სასამართლო. შესაბამისად, როგორც ბრალდების მხარის მიერ შუამდგომლობის დაყენებისას, ასევე დაცვის მხარისათვის ანოლოგიური უფლების მინიჭების შემთხვევაში ინფორმაციის გამოთხოვის საჭიროებას და გამოსათხოვი ინფორმაციის მნიშვნელობას მართლმსაჯულების განხორციელებისათვის წყვეტს სასამართლო. როგორც უკვე აღინიშნა, საქმის არსებითი განხილვის სხდომაზე მოპასუხის წარმომადგენელს არ მიუთითებია სადავო ნორმებით დადგენილი შეზღუდვის ლეგიტიმური მიზნები და ლეგიტიმური მიზნის არსებობა არც სადავო ნორმების ლოგიკური ანალიზიდან გამომდინარეობს. გაურკვეველია, რა მიზანს შეიძლება ემსახურებოდეს დაცვის მხარისთვის სასამართლოს წინაშე შუამდგომლობის დაყენების და ამ შუამდგომლობის დასაბუთებულობის შემთხვევაში გამამართლებელი მტკიცებულების მოპოვების შესაძლებლობის ჩამორთმევა იმ პირობებში, როდესაც სისხლის სამართლის საპროცესო კანონმდებლობა დაცვის მხარეს ანიჭებს სასამართლოსთვის, მათ შორის ისეთი საგამოძიებო მოქმედების ჩატარების შესახებ შუამდგომლობით მიმართვის უფლებას, როგორიცაა ჩხრეკა-ამოღება, რაც

²⁹⁸ საქართველოს საკონსტიტუციო სასამართლოს პირველი კოლეგიის გადაწყვეტილება № 1/1/650,699 — 2017 წლის 27 იანვარი. ქ. ბათუმი, აბზაცი 18;

²⁹⁹ საქართველოს საკონსტიტუციო სასამართლოს პირველი კოლეგიის გადაწყვეტილება № 1/1/650,699 — 2017 წლის 27 იანვარი. ქ. ბათუმი, აბზაცი 20;

³⁰⁰ საქართველოს საკონსტიტუციო სასამართლოს პირველი კოლეგიის გადაწყვეტილება № 1/1/650,699 — 2017 წლის 27 იანვარი. ქ. ბათუმი, აბზაცი 21;

მესაძლებელია ცალკეულ შემთხვევებში უფრო მაღალი ინტენსივობით ქმნიდეს მესამე პირთა პირად ცხოვრებასა, თუ კერძო საკუთრებაში ჩარევის საფრთხეს. საკონსტიტუციო სასამართლოს პრაქტიკით „ლეგიტიმური მიზნის არარსებობის პირობებში ადამიანის უფლებაში ნებისმიერი ჩარევა თვითნებურ ხასიათს ატარებს და უფლების შებლღვდა საფუძველშივე გაუმართლებელი, არაკონსტიტუციურია“ (საქართველოს საკონსტიტუციო სასამართლოს 2013 წლის 5 ნოემბრის №31/1/531 გადაწყვეტილება „ისრაელის მოქალაქეები — თამაზ ჯანაშვილი, ნანა ჯანაშვილი და ირმა ჯანაშვილი საქართველოს პარლამენტის წინააღმდეგ“, ვვ-15).“³⁰¹

ყოველივე ზემოაღნიშნულიდან გამომდინარე, საკონსტიტუციო სასამართლომ დაადგინა, რომ: „საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლის პირველი და მე-4 ნაწილებით დადგენილი შებლღვდა ატარებს თვითმიზნურ ხასიათს და ხსენებული ნორმების ის ნორმატიული შინაარსი, რომელიც გამოირიცხავს დაცვის მხარის მიერ კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში შენახული ინფორმაციის ან დოკუმენტის გამოთხოვის განჩინების გაცემის შუამდგომლობით სასამართლოსათვის მიმართვის შესაძლებლობას, ეწინააღმდეგება საქართველოს კონსტიტუციის 42-ე მუხლის პირველ პუნქტს.“³⁰²

ამდენად, როგორც თბილისის სააპელაციო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიამ განმარტა, „საქართველოს საკონსტიტუციო სასამართლოს ხსენებული გადაწყვეტილებიდან გამომდინარე, დაცვის მხარეს ბრალდების მხარისათვის დადგენილი სტანდარტით მიეცა შესაძლებლობა მხარეთა თანასწორობისა და შეჯიბრებითობის თანაბარი ხელმისაწვდომობის პრინციპის დაცვით მოიპოვოს ინფორმაცია/მტკიცებულება მასთან დაკავშირებული ნებართვებით და ორივე მხარისათვის არსებული საკანონმდებლო შებლღვდებით, რა შემთხვევაშიც ნორმა არცერთ მხარეს არ აყენებს უპირატეს მდგომარეობაში.“³⁰³

მაგრამ ისმის შეკითხვა — როგორ უნდა განახორციელოს დაცვის მხარემ აღნიშნული იმ ვითარებაში, როდესაც მოქმედება მიეკუთვნება ფარულ საგამოძიებო მოქმედებათა ჩამონათვლს —? ამისთვის დაცვის მხარეს მოუწევს ყველა იმ სამართლებრივი ეტაპების გავლა რომელიც უწევს ბრალდების მხარეს, მაგრამ მაშინ იბადება შეკითხვა — რასაიღებო ნომერი უნდა მიანიჭოს დაცვის მხარემ შუამდგომლობას? როგორ უნდა მოახდინოს ინფორმაციის განსაიდუმლოება მაშინ, როცა ის თავად არ არის ამის უფლებამოსილებით არჭურვილი პირი —? ამ შეკითხვებზე სამართლებრივი პასუხები არ არსებობს, მაგრამ პასუხები მოგვცა პრაქტიკამ — რომლის საფუძველზეც დაცვის მხარე ჩვეულებრივ — ინფორმაციის გამოთხოვის შუამდგომლობით მიმართავს პირველი ინსტანციის სასამართლოს, შუამდგომლობა არ არის დალუქული და არც ფარულ ხასიათს არ ატარებს, აღნიშნულის შემდგომ მოქმედებაში მოდის საქართველოს სისხლის სამართლის საპროცესო კოდექსის 111-ე მუხლით დადგენილი რეგულაციები, კერძოდ: [...] „დაცვის მხარის დასაბუთებული შუამდგომლობით, სასამართლოს განჩინების საფუძველზე საგამოძიებო მოქმედებას ატარებს გამოძიებელი, რომელიც არ შეიძლება იყოს იგივე პირი, რომელიც მოცემული საქმის გამოძიებას აწარმოებს. გამოძიებელი უნდა შეარჩიოს საგამოძიებო ორგანოს ხელმძღვანელმა და მისი ვინაობა და საკონტაქტო მონაცემები დაცვის მხარეს უნდა ეცნობოს შუამდგომლობით მოთხოვნილი საგამოძიებო მოქმედების ჩატარებად. ამ შემთხვევაში საგამოძიებო მოქმედების ჩატარებასთან დაკავშირებული ხარჯების ანაზღაურება ეკისრება ბრალდებულს, გარდა იმ შემთხვევისა, როდესაც ბრალდებული სასამართლოს წარუდგენს მტკიცებულებებს, რომლებითაც დადასტურდება მის

³⁰¹ საქართველოს საკონსტიტუციო სასამართლოს პირველი კოლეგიის გადაწყვეტილება № 1/1/650,699 — 2017 წლის 27 იანვარი, ქ. ბათუმი, აბჰაცი 22;

³⁰² საქართველოს საკონსტიტუციო სასამართლოს პირველი კოლეგიის გადაწყვეტილება № 1/1/650,699 — 2017 წლის 27 იანვარი, ქ. ბათუმი, აბჰაცი 23;

³⁰³ თბილისის სააპელაციო სასამართლოს სისხლის სამართლის საქმეთა კოლეგიის განჩინება 1გ/960-17 (2017-07-19)

მიერ ამ ხარჯების ანაზღაურების შეუძლებლობა. დაცვის მხარეს უფლება აქვს, მონაწილეობა მიიღოს თავისი მოთხოვნით ჩატარებულ საგამოძიებო მოქმედებაში.³⁰⁴ „დაცვის მხარის უფლება, შეამდგომლობით მიმართოს სასამართლოს საგამოძიებო მოქმედების ჩატარების თაობაზე, არ ვრცელდება საქართველოს სისხლის სამართლის საპროცესო კოდექსის 112-ე მუხლის მე-5 ნაწილით გათვალისწინებულ გარემოებებზე. დაცვის მხარეს არა აქვს უფლება, სასამართლოს ნებართვის გარეშე ჩაატაროს ისეთი საგამოძიებო მოქმედება, რომლის ჩატარებისათვის, ამ კოდექსის თანახმად, საჭიროა ასეთი ნებართვა.“³⁰⁵

შესაბამისად, სსსკ-ის 111-ე მუხლის პირველი ნაწილი ადგენს დაცვის მხარის მიერ საგამოძიებო მოქმედების ჩატარების სპეციალურ წესს, რაც 2014 წლის 1 სექტემბრიდან ამოქმედდა. ამ ნორმის მიხედვით, „დაცვის მხარის დასაბუთებული შეამდგომლობის საფუძველზე სასამართლო განიხილის საფუძველზე საგამოძიებო მოქმედებას ჩატარებს გამოძიებელი, რომელიც არ შეიძლება იყოს იგივე პირი, რომელიც გამოძიებას აწარმოებს მოცემულ საქმეზე. სასამართლოსთვის წარდგენილი დაცვის მხარის შეამდგომლობა უნდა იყოს დასაბუთებული, მასში დეტალურად უნდა იყოს ჩამოყალიბებული მხარის მოთხოვნა, საგამოძიებო მოქმედების ჩატარების მიზანი და საფუძველი, ფაქტები და მათი დამადასტურებელი მტკიცებულებები, მსჯელობა და არგუმენტაცია ფაქტებსა და მტკიცებულებებზე, კანონი, რომელიც არგუმენტებს და მსჯელობას ამყარებს. მხარე ვალდებულია შეამდგომლობაში დაასაბუთოს მტკიცებულებათა იმ სტანდარტის (დასაბუთებული ვარაუდის) არსებობა, რომელსაც საგამოძიებო მოქმედების ჩატარებისთვის აუცილებელ წინაპირობად მიიჩნევს სსსკ-ის მე-3 მუხლის მე-11 ნაწილი.“³⁰⁶

შემდგომ პარაგრაფში წარმოგიდგენთ საგამოძიებო და საპროცესო მოქმედებების ოქმებს, რომელთა გარკვეული ნაწილი დამკვიდრებულია პრაქტიკაში, გარკვეული ნაწილი არის შედგენილი და სტრუქტურირებული ჩვენს მიერ.

6.3. მომსახურების მომწოდებლებისაგან ციფრული ინფორმაციის გამოთხოვის ტექნიკური პროცედურები და მეთოდები

როგორც ზემოთ უკვე აღინიშნა, ინფორმაციის გამოთხოვა შესაძლებელია საგამოძიებლის მიერ მოხდეს კომპიუტერული სისტემიდან, მაგრამ არის შემთხვევები, როდესაც ინფორმაციის გამოთხოვა ხდება შესაბამისი ინტერნეტ პროვაიდერებისა და მომსახურების მომწოდებლებისაგან, ასეთ შემთხვევაში, დასაბუთებული ვარაუდის არსებობის შემთხვევაში, პროკურორს შეაქვს სასამართლოში შეამდგომლობა – როგორც ზემოთ უკვე აღინიშნა შესაბამისი ინფორმაციის გამოთხოვის შესახებ განიხილების გაცემის მოთხოვნით, მსგავს შემთხვევებში თითქმის შეუძლებელია ასეთი საგამოძიებო მოქმედების გადაუდებელი აუცილებლობით ჩატარება, მაგრამ ვინაიდან კანონი ამას არ გამორიცხავს, მსჯელობა იმაზე, რომ და კატეგორიულად გამორიცხულია არ შეიძლება, მაგრამ პრაქტიკაში იშვიათად ასეთი რამ მოხდეს.

ასეთ შემთხვევაში მნიშვნელოვანია პროცედურა;

³⁰⁴ საქართველოს სისხლის სამართლის საპროცესო კოდექსი (რედ. 09/10/2009, კონსოლიდირებული 29.05.2019). მუხლი 111 მუხლის 1-ლი ნაწილი;

³⁰⁵ იქვე. მე-2 ნაწილი;

³⁰⁶ ავტორთა კოლექტივი, საქართველოს სისხლის სამართლის საპროცესო კოდექსის კომენტარი. 2015 წლის 1 ოქტომბრის მდგომარეობით. ამერიკის იურისტთა ასოციაცია კანონის უზენაესობის ინციტების მხარდაჭერით. 2015 წელი. გვ. 365-366;

მხარის შუამდგომლობის შეტანა სასამართლოში;

სასამართლოს მიერ განჩინების გაცემა;

არსებული დოკუმენტაციის განსაიდუმლოება (ასეთის საჭიროების შემთხვევაში ბრალდების მხარის მიერ);

ინტერნეტ პროვაიდერისადმი მიმართვის წერილი, რომლის საფუძველზეც ეცნობება მას, რომ უნდა გადმოსცეს მხარეს შესაბამისი ინფორმაცია და მოახდინოს აღნიშნული ინფორმაციის მოპოვება;

ინფორმაციის გამოთხოვის ოქმის შედგენა და შესაბამისი ინფორმაციის შემცველი დოკუმენტების ან ელექტრონული ინფორმაციის შემცველი შესაბამისი საშუალებების გამოთხოვა;

ჩვენს მიერ ზემოაღნიშნულ პარაგრაფებში განხილულ იქნა შუამდგომლობის შეტანასთან, შესაბამისი განჩინების გაცემასთან და ოქმის შევსებასთან დაკავშირებული სამართლებრივი პროცედურები. შესაბამისად აღნიშნულზე მსჯელობა არსებულ პარაგრაფში არ მოხდება, მაგრამ ამ შემთხვევაში ყურადღება უნდა გავამახვილოთ საკითხზე, რომ

როდესაც მხარეს შუამდგომლობა შეაქვს სასამართლოში რა შინაარსის ინფორმაციის გამოთხოვა უნდა მოახდინოს;

გასათვალისწინებელია, რომ აღნიშნული აუცილებლად იწერება იმ შუამდგომლობის სარგოლუციო ნაწილში, რომელიც ბრალდების მხარეს შეაქვს სასამართლოში.

განვიხილოთ რამდენიმე შუამდგომლობის სარგოლუციო ნაწილში ჩამოყალიბებული მოთხოვნის მაგალითი, თუ რა სახის ინფორმაცია შესაძლოა იქნეს გამოთხოვილი კონკრეტული ინტერნეტ პროვაიდერებისაგან ან/და მომსახურების მომწოდებლებისაგან;

გამოსათხოვი ინფორმაცია სოციალური ქსელების მომსახურების მომწოდებლებისგან (მაგ. FACEBOOK);

კონკრეტული მომხმარებლის რეგისტრაციის შესახებ არსებული სრული ინფორმაცია (მარეგისტრირებული პირი ფიზიკური/იურიდიული, მარეგისტრირებული IP, რეგისტრაციის დრო, ტელეფონის ნომერი);

ინფორმაცია კონკრეტული მომხმარებლის მფლობელი პირის დემოგრაფიული მონაცემების შესახებ;

ინფორმაცია კონკრეტული მომხმარებლის მიერ გამოძიებისათვის მნიშვნელოვან პერიოდში გამოყენებული IP მისამართების შესახებ;

ყველა გაგზავნილი და მიღებული ელექტრონული შეტყობინებების (აუდიო, ვიდეო, წერილობითი და ა.შ) სრული ასლები, (მათ შორის წაშლილი ელექტრონული შეტყობინებების), მათი გაგზავნის და მიღების დროების მითითებით;

შემოსული ელექტრონული შეტყობინებების IP მისამართები (ასეთის დადგენის შემთხვევაში);

ინფორმაცია მეგობრების შესახებ (როგორც ღია ასევე დახურული);

ინფორმაცია წაშლილი შეტყობინებების შესახებ (ასეთის საჭიროების შემთხვევაში);

ინფორმაცია (გამოძიებისათვის მნიშვნელოვანი) გაზიარებული ან/და მოწოდებული ინფორმაციის შესახებ და ინფორმაციის ასლები (კონკრეტული დროის და გამოიარებული IP მისამართის მითითებით);

ინფორმაცია კომუნიკაციის შესახებ განხორციელებული ზეპირი საუბრის საშუალებით, შესაბამისი დროების მითითებით (სოციალური ქსელის დარეკვის ფუნქციის საშუალებით);

გამოსათხოვი ინფორმაცია ინტერნეტ პროვაიდერებისგან;

IP მისამართის მფლობელის სრული დემოგრაფიული მონაცემები;

IP მისამართის საშუალებით განხორციელებული აქტივობების, მათ შორის ტრანზაქციების შესახებ სრული ინფორმაცია (გამოძიებისათვის საჭირო კონკრეტული დროების მითითებით);

გამოსათხოვი ინფორმაცია საბანკო დაწესებულებებიდან;

ინფორმაცია ანგარიშის მფლობელი სრული დემოგრაფიული მონაცემების შესახებ;

ინფორმაცია ანგარიშის გახსნის შესახებ (ვის მიერ, რა დროს, რომელ ფილიალში ან რომელი IP მისამართის მექანე კომპიუტერის საშუალებით, რა ვალუტაში);

ანგარიშის გახსნის დროს წარდგენილი სრული დოკუმენტაციის ასლები (არაკომპიუტერული ანგარიშის დროს);

ინფორმაცია (გამოძიებისათვის მნიშვნელოვან დროში) განხორციელებული სრული ტრანზაქციების შესახებ;

ინფორმაცია იმ IP მისამართების შესახებ რომლებთანაც განხორციელებულ იქნა შესაბამისი ფულადი ტრანზაქციები;

ინფორმაცია იმბანკომატების მონაცემების შესახებ, რომელთაგამოყენებითაც განხორციელებულ იქნა ფულადი თანხის ტრანზაქციები შესაბამის ანგარიშზე (ასეთის არსებობის შემთხვევაში);

ინფორმაცია იმ ანგარიშის მფლობელის სრული დემოგრაფიული მონაცემების მითითებით (რომელიც მნიშვნელოვანია გამოძიებისათვის) რომლებსაც კავშირი აქვთ აღნიშნულ ანგარიშთან ფულადი ტრანზაქციის ან სხვა სახით;

გამოსათხოვი ინფორმაცია ელექტრონული ფოსტის ოფიციალური წარმომადგენლობიდან:

კონკრეტული მომხმარებლის რეგისტრაციის შესახებ არსებული სრული ინფორმაცია (მარეგისტრირებული პირი ფიზიკური/იურიდიული, მარეგისტრირებული IP, რეგისტრაციის დრო, ტელეფონის ნომერი);

ელექტრონული ფოსტის პაროლი;

ინფორმაცია კონკრეტული მომხმარებლის მფლობელი პირის დემოგრაფიული მონაცემების შესახებ;

ინფორმაცია კონკრეტული მომხმარებლის მიერ გამოძიებისათვის მნიშვნელოვან პერიოდში გამოყენებული IP მისამართების შესახებ;

ყველა გაგზავნილი და მიღებული ელექტრონული შეტყობინებების (აუდიო, ვიდეო, წერილობითი და ა.შ.) სრული ასლები, (მათ შორის წაშლილი ელექტრონული შეტყობინებების), მათი გაგზავნის და მიღების დროების მითითებით;

შემოსული ელექტრონული შეტყობინებების IP მისამართები (ასეთის დადგენის შემთხვევაში);

მას შემდეგ რაც განვიხილეთ თუ რა სხის ინფორმაცია უნდა იქნეს შეტანილი შუამდგომლობის სარგოლუციო ნაწილში და რა უნდა გამოვითხოვოთ კონკრეტული პროვაიდერისა თუ მომსახურების მიმწოდებლისგან, განვიხილოთ მეორე მნიშვნელოვანი საკითხი;

ინფორმაციის გამოთხოვა საქართველოს სახლმწიფოს ფარგლებს გარეთ არსებული ინტერნეტ პროვაიდერებისა და მომსახურების მიმწოდებლებისაგან;

პრაქტიკაში არის ხშირი შემთხვევები, როდესაც ინფორმაციის გამოთხოვის საჭიროება არის საქართველოს სახლმწიფო საზღვრებს გარეთ რეგისტრირებული ინტერნეტ პროვაიდერებისაგან და მომსახურების მიმწოდებლებისაგან;

ასეთ შემთხვევაში ბრალდების მხარემ უნდა იხელმძღვანელოს სისხლის სამართლის სფეროში საერთაშორისო თანამშრომლობის შესახებ საქართველოს კანონის დებულებებით.

თუ წარმოიშვა უცხო სახელმწიფოს ტერიტორიაზე საქართველოს სისხლის სამართლის საპროცესო კოდექსით გათვალისწინებული საპროცესო მოქმედების ჩატარების საჭიროება და, ამასთანავე, არსებობს შესაბამისი სამართლებრივი საფუძველი, გამომძიებელი, პროკურორი

ან მოსამართლე (სასამართლო) უფლებამოსილია სათანადო შეამდგომლობით მიმართოს საქართველოს იუსტიციის სამინისტროს.

მაგალითად: ბრალდების მხარეს სურს ინფორმაცია გამოითხოვოს *ვინც* –ს სათაო ოფისიდან შესაბამისი კომუნიკაციის შესახებ.

ამისათვის ბრალდების მხარემ პირველ რიგში უნდა დაადგინოს იმ ორგანიზაციის (კონკრეტული მაგალითის საფუძველზე *ვინც*-ს) ოფიციალური იურიდიული მისამართი და ზუსტი დასახელება, რაც უნდა ასახოს შესაბამის საგამოძიებო მოქმედების ოქმში — იქნება ეს ოფიციალური ვებ-საიტის დათვალიერება თუ სხვა.

შემდგომ სისხლის სამართლის სფეროში საერთაშორისო დახმარების შესახებ საქართველოს კანონის მე-6 მუხლის მე-2 და მე-3 ნაწილების საფუძველზე³⁰⁷ უნდა მიმართოს სასამართლოს შესაბამისი შეამდგომლობით ინფორმაციის გამოთხოვაზე ნებართვის გაცემის შესახებ, შეამდგომლობაში აუცილებელია აისახოს ზუსტად ის მოთხოვნა თუ რა ინფორმაცია უნდა იქნეს გამოთხოვილი. შესაბამისი ორგანიზაციის ზუსტი დასახელება და შესაბამისი ორგანიზაციის ზუსტი იურიდიული მისამართი, განსხვავებით სხვა ინფორმაციის გამოთხოვის შეამდგომლობისაგან ამ ტიპის შეამდგომლობა არ უნდა შეიცავდეს საგამოძიებო მოქმედების ჩატარების ვადას (ვინაიდან ინფორმაცია არის პირადი ცხოვრების შესახებ, შეამდგომლობა რეკომენდებულია შევიდეს ფარული შეამდგომლობის წესების სრული დაცვით).

სასამართლოს მიერ გაიცემა შესაბამისი განჩინება, რომელშიც ასევე გადავა ის მნიშვნელოვანი რეკვიზიტებიროგორიცარისთურაინფორმაციაუნდაიქნესგამოთხოვილი,შესაბამისიორგანიზაციის ზუსტი დასახელება და შესაბამისი ორგანიზაციის ზუსტი იურიდიული მისამართი, განსხვავებით სხვა ინფორმაციის გამოთხოვის განჩინებისაგან ამ ტიპის განჩინება არ უნდა შეიცავდეს საგამოძიებო მოქმედების ჩატარების ვადას (ვინაიდან ინფორმაცია არის პირადი ცხოვრების შესახებ, განჩინება რეკომენდებულია გაიცეს ფარული განჩინების წესების სრული დაცვით).

აღნიშნულის შემდგომ უნდა მოხდეს როგორც შეამდგომლობის, ასევე განჩინების განსაიდუმლოება (თუ ნაწარმოებია საიდუმლო წესით).

განჩინების მიღების შემდგომ პროკურორი უფლებამოსილია პროკურატურის საერთაშორისო ურთიერთობების სამმართველოს გადაუგზავნის შეამდგომლობა, რომელიც თავის მხრივ განახორციელებს შემდგომ მოქმედებებს:

სამართლებრივი დახმარების აღმოჩენის შესახებ შეამდგომლობა შედგენილი უნდა იყოს წერილობითი ფორმით და, როგორც წესი, უნდა შეიცავდეს:

- ა) იმ სახელმწიფოს კომპეტენტური ორგანოს სახელწოდებას, რომელსაც ეგზავნება შეამდგომლობა;
- ბ) სისხლის სამართლის საქმის ფაქტობრივი გარემოებების აღწერას და მის სამართლებრივ კვალიფიკაციას;
- გ) კანონის იმ მუხლის შინაარსს, რომელთან დაკავშირებითაც მიმდინარეობს სისხლის სამართალწარმოება შესაბამის სისხლის სამართლის საქმეზე, აგრეთვე, საჭიროების შემთხვევაში, ამონაწერს სხვა, შესაბამისი საკანონმდებლო აქტებიდან; დ) მოთხოვნილი სამართლებრივი დახმარების შინაარსს;
- ე) სამართლებრივი დახმარების მოთხოვნის მიზანსა და საჭიროებას;

³⁰⁷ საქართველოს კანონი სისხლის სამართლის სფეროში საერთაშორისო თანამშრომლობის შესახებ, მუხლი მე-6 ნაწილი 2-3; თუ საქართველოს სისხლის სამართლის საპროცესო კოდექსი საპროცესო მოქმედების ჩასატარებლად მოითხოვს სასამართლო გადაწყვეტილებას (განჩინებას), მოსამართლის სულმოწერითა და სასამართლოს გერბიანი ბეჭდით დამოწმებული ეს გადაწყვეტილება უნდა დაერთოს სამართლებრივი დახმარების აღმოჩენის შესახებ შეამდგომლობას. 3. ამ მუხლის მე-2 პუნქტით გათვალისწინებული სასამართლო გადაწყვეტილების (განჩინების) გამოტანისას არ გამოიყენება საქართველოს სისხლის სამართლის საპროცესო კოდექსის 112-ე მუხლის მე-3 ნაწილით დადგენილი ვადები.

ვ) იმ პირის შეძლებისდაგვარად ზუსტ საიდენტიფიკაციო მონაცემებს, რომლის მიმართაც მოითხოვება სამართლებრივი დახმარების აღმოჩენა;

ზ) სხვა აუცილებელ მონაცემებს.³⁰⁸

აღნიშნულის შემდგომ შეამდგომლობა იგზავნება შესაბამის სახელწიფოში, „[...] შეამდგომლობა სრულდება უცხო სახელმწიფოს კანონმდებლობის შესაბამისად, ასევე თუ საქართველოს საერთაშორისო ხელშეკრულებით ან ინდივიდუალური შეთანხმებით ანდა ნაცვალგების პირობებით სხვა რამ არ არის გათვალისწინებული, საქართველოს იუსტიციის სამინისტრო უფლებამოსილია უცხო სახელმწიფოს მიმართოს თხოვნით საქართველოს კომპეტენტური ორგანოების წარმომადგენელში არსებულ სისხლის სამართლის საქმესთან დაკავშირებით სამართლებრივი დახმარების აღმოჩენის შესახებ შეამდგომლობის შესრულებისას საქართველოს კანონმდებლობის გამოყენების თაობაზე.“³⁰⁹

„უცხო სახელმწიფოს ტერიტორიაზე კანონმდებლობით დადგენილი წესით მოპოვებულ მტკიცებულებას აქვს საქართველოს ტერიტორიაზე მოპოვებული მტკიცებულების თანაბარი იურიდიული ძალა.“³¹⁰

6.4. კომპიუტერული მოწყობილობიდან ციფრული ინფორმაციის გამოთხოვის ტექნიკური პროცედურები და მეთოდები

კომპიუტერული მოწყობილობიდან ინფორმაციის გამოთხოვა დაკავშირებულია რიგ პროცედურებთან, არ შეიძლება გამოძიებლის მიერ საგამოძიებო მოქმედება განხორციელდეს არალიცენზირებული პროგრამებით, ასევე ყველა პროცედურა რასაც გამოძიებელი ახორციელებს ზედმიწევნით უნდა იქნეს ასახული საგამოძიებო მოქმედების ოქმში, ასევე პრაქტიკასი იკვეთება პრობლემები, როდესაც საგამოძიებო მოქმედება გამოთხოვა იმიტომ არის მოსამართლის მიერ უკანონოდ ცნობილი ან არ ხდება მისი გაზიარება — რომ გამოძიების ეტაპზე დაშვებულია მნიშვნელოვანი პროცედურული შეცდომები.

„ოპერაციული სისტემა არის პროგრამა, რომელიც აქტიუდება კომპიუტერის ჩატვირთვის დროს. კომპიუტერი აწარმოებს მრავალფეროვან მოქმედებებს და მათი რიცხვი უსაშველოდ დიდია. კერძოდ, როდესაც ჩვენ ვაძლევთ კომპიუტერს ტექსტის ამობეჭდვის ბრძანებას, იქ ხდება უამრავი წერილმანი ოპერაციები. ეშვება ბეჭდვის პროგრამა, რომელიც თავის მხრივ რიგ ბრძანებებს აძლევს სხვა პატარა პროგრამებს, რომელთა რიცხვიც საკმაოდ დიდია. ამობეჭდვის პროგრამა ერთხელ და სამუდამოდ გამზადებულია და შეტანილია პროგრამების პაკეტში, რომელსაც ეწოდება ოპერაციული სისტემა. გარდა ბეჭდვითი პროგრამებისა, აქ შედის პროგრამები, რომელსაც ტექსტი გამოაქვს მონიტორზე, სკანერიდან ტექსტი შეაქვს კომპიუტერის მესხიერებაში და სხვა მრავალი. მაშასადამე, შეგვიძლია ვთქვათ, რომ ოპერაციული სისტემა წარმოადგენს მწარმოებლის მიერ შემუშავებულ პროგრამათა ერთობლიობას, რომელიც მართავს კომპიუტერს ჩვენგან დამოუკიდებლად. იგი კომპიუტერის მუშაობის უმთავრესი პროგრამაა.“³¹¹

³⁰⁸ საქართველოს კანონი სისხლის სამართლის სფეროში საერთაშორისო თანამშრომლობის შესახებ, მუხლი მე-6 ნაწილი 1.

³⁰⁹ იქვე. მუხლი მე-5

³¹⁰ იქვე.

³¹¹ გაკვეთილი მეხუთე, ოპერაციული სისტემები, დამხმარე პროგრამები, კლავიატურა (ნაწ. III) ელ. გვერდი 222; ნანახია 19.07.2019



..ოპერაციული სისტემები მოდიფიცირდება და უმჯობესდება შეცდომების გამოსწორებისა და ახალი შესაძლებლობების დამატების ხარჯზე. სისტემების ახალ ვერსიებს სახელწოდება არ ეცვლება. არამედ იძენს ასეთ სახეს - მაგ. 7.1, 7.2 და ასე შემდეგ. ამ შემთხვევაში ციფრი 7 აღნიშნავს ძირეულ ცვლილებას, რაც განიცადა სისტემაში წინანდელ მეექვსე ვერსიასთან შედარებით, ხოლო წერტილის შემდგომ მდგარი ციფრების ცვლილება აღნიშნავს შეცდომების აღმოფხვრის შედეგად გაუმჯობესებულ ვერსიას. ანუ არცთუ მნიშვნელოვან ცვლილებებს. რაც დიდია ვერსიის ციფრი, მით მეტი შესაძლებლობების მქონეა ოპერაციული სისტემა.”³¹²

საკითხის საწყის ეტაპზე უნდა ითქვას, რომ დღეის მდგომარეობით უმეტესწილად, გვხვდება სამი კომპიუტერული სისტემის მქონე კომპიუტერები, ესენია:

WINDOWS - ის ოპერაციული სისტემის მქონე კომპიუტერები;

MACOS - ის ოპერაციული სისტემის მქონე კომპიუტერები;

LINUX - ის ოპერაციული სისტემის მქონე კომპიუტერები

და სხვა სისტემები;

განვიხილოთ თითოეული:

macOS - (ადრე Mac OS X და მოგვიანებით OS X) არის სერიული გრაფიკული ოპერაციული სისტემა, რომელიც შემუშავებულია და ბაზარზეა 2001 წლიდან. ეს არის ძირითადი ოპერაციული სისტემა Apple- ის Mac-ის ოჯახის კომპიუტერი. კომპიუტერის, ლეპტოპისა და სახლის კომპიუტერების ბაზარზე და ინტერნეტის საშუალებით. ეს არის მეორე ყველაზე ფართოდ გამოყენებადი desktop OS , Microsoft Windows- ის შემდეგ (სურათი N25 იხილეთ macOS სისტემის მქონე კომპიუტერები და მათი ეკრანები).

სურათი N25 Apple- ის Mac-ის ოჯახის კომპიუტერები;



Microsoft Windows არის რამდენიმე გრაფიკული საოპერაციო სისტემის ოჯახი, რომელთაგან თითოეული შემუშავებულია, ბაზარზე და გაყიდულია Microsoft- ის მიერ.

2018 წლის ოქტომბრის მონაცემებით Windows- ის უახლესი ვერსია Windows- ისთვის,



ტაბლეტებისთვის, სმარტფონებისათვის და ჩადგმული მოწყობილობებისთვის არის Windows 10. აღნიშნული სისტემა გამოიყენება Apple-ის Mac-ის ოჯახის კომპიუტერების გარდა თითქმის უმეტეს კომპიუტერებში windows სისტემის მქონე კომპიუტერების და მათი ეკრანები.

სურათი N26 Microsoft Windows სისტემის მქონე კომპიუტერები



LINUX — „არის თავისუფალად გავრცელებადი GPL ლიცენზიაზე დამყარებული საოპერაციო სისტემა, რომელიც შეიქმნა UNIX მაგვარი საოპერაციო სისტემა Minix-ის გავლენით (და არა მის ბაზაზე). მისი თავდაპირველი ვერსიის შემქმნელია ფინეთის ჰელსინკის უნივერსიტეტის სტუდენტი ლინუს ტორვალდსი (Linus Torvalds). საგულისხმოა ის ფაქტი, რომ სტუდენტმა ახალი საოპერაციო სისტემა საკუროს ნაშრომის ფარგლებში შექმნა. Linux წარმატებით შეიძლება გამოიყენონ, როგორც სამუშაო სადგურად, ასევე სერვერის პლატფორმად. დღესდღეობით Linux UNIX მაგვარი საოპერაციო სისტემების ღირსეული კლონია. Linux სრულყოფილი მრავალფუნქციონალური მრავალამოცანიანი საოპერაციო სისტემაა, რომელიც წარმატებით ართმევს თავს თანამედროვე საინფორმაციო ტექნოლოგიების მზარდ მოთხოვნილებებს.“³¹³ „აღსანიშნავია, რომ ვებ-სტატიისტიკის თანახმად ოპერაციული სისტემა Ubuntu-ს მომხმარებლები პერსონალურ კომპიუტერზე ლინუსის მომხმარებელთა 50%-ს შეადგენს. აგრეთვე იზრდება Ubuntu-ს, როგორც ვებ-სერვერის გამოყენება, Ubuntu ეს არის ოპერაციული სისტემა, რომელიც დაფუძნებულია Debian GNU/Linux-ის დისტრიბუტივზე. ვრცელდება, როგორც თავისუფალი და ღია კოდის მქონე პროგრამა (open source), დამატებით დაპატენტებულ პროგრამებთან ერთად. სახელი „Ubuntu“ ეფუძნება სამხრეთ აფრიკულ Ubuntu-ს ფილოსოფიას („შემანერობა ერთმანეთის მიმართ“). Ubuntu წარმოადგენს თანამედროვე, სტაბილურ საოპერაციო სისტემას საშუალო სტატიისტიკური მომხმარებლისთვის.



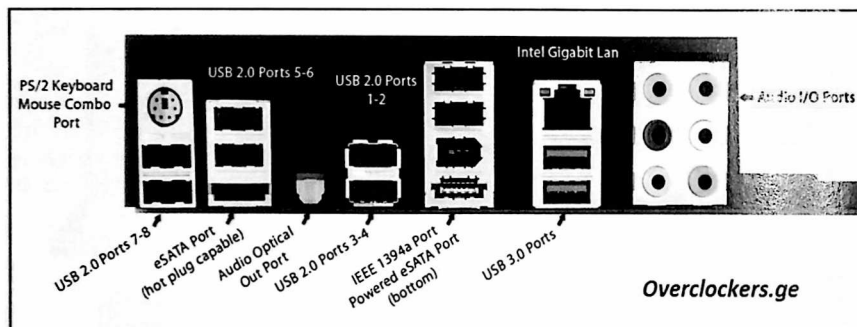
იგი ორიენტირებულია გამოყენებადობასა და ადვილად დაყენებაზე. „³¹²

ამჟერად გადავიდეთ კომპიუტერიდან ინფორმაციის გამოთხოვის ნაბიჯებზე, იმისათვის რომ გამოძიებელმა სისხლის სამართლის საქმეზე დამაგროს ინფორმაცია მან უნდა გაიაროს რამდენიმე ტექნიკური პროცედურა ინფორმაციის მოპოვებისათვის;

ნაბიჯი 1 — შესაბამისი კაბელების შემოწმება:

სანამ გამოძიებლის მიერ ჩართულ იქნება შესაბამისი კომპიუტერული მოწყობილობა, აუცილებელია რომ მის მიერ შემოწმებულ იქნეს შეერთებულია თუ არა კაბელები შესაბამის სწორ ადგილებზე. ამისათვის გთავაზობთ შესაბამისი კაბელების შესაერთებელი მოწყობილობების ადგილებს (იხ. სურათი N27);

სურათი N 27:



315

ნაბიჯი N2 — კომპიუტერის პაროლის გაგება და ჩართვა:

როდესაც მოხდება კომპიუტერის ჩართვა, შესაძლებელია კომპიუტერი არ გაიხსნას და მოგთხოვთ პასოლის შეყვანა, ასეთ შემთხვევაში ადგილზე მყოფ პირს კითხავთ კომპიუტერის პაროლს. რომელსაც შეიყვანთ შესაბამის გრაფაში (იხილეთ სურათი 10) და კომპიუტერი ჩაირთვება, აქვე აღსანიშნავია, რომ შესაძლებელია კომპიუტერი როდესაც ჩაირთვება, მან პირდაპირ არ გამოაჩინოს რომ ითხოვს პაროლს, მაგრამ არ შევიდეს ეკრანზე ასეთ შემთხვევაში გამოიყენეთ სამი კლავიშის კომბინაცია Ctrl + Alt + Del ერთობლივი დაჭერით (იხილეთ სურათი N29), რის შემდეგაც გააქტიურდება N28 სურათზე ნაჩვენები გრაფა, სადაც შეტანილ იქნება შესაბამისი პაროლი, მაგრამ გასათვალისწინებელია შემდეგი გარემოება:

გამომძიებელმა აღნიშნული ფაქტი, რომ კომპიუტერის პაროლი გადასცა მას ადგილზე მყოფმა პირმა და კომპიუტერის პაროლი, აუცილებლად უნდა ასახოს ინფორმაციის გამოთხოვის ოქმში, სადაც უნდა ჩაიწეროს რომ ადგილზე მყოფმა ფიზიკურმა პირმა მას გადასცა ინფორმაცია კომპიუტერის პაროლის შესახებ რომელიც არის შემდეგი მაგა.123; გასათვალისწინებელია, რომ ამისათვის ცალკეული ოქმის შედგენა არ არის რეკომენდირებული. (იხ. სურათი N28);

³¹⁴ ელ. გვერდი

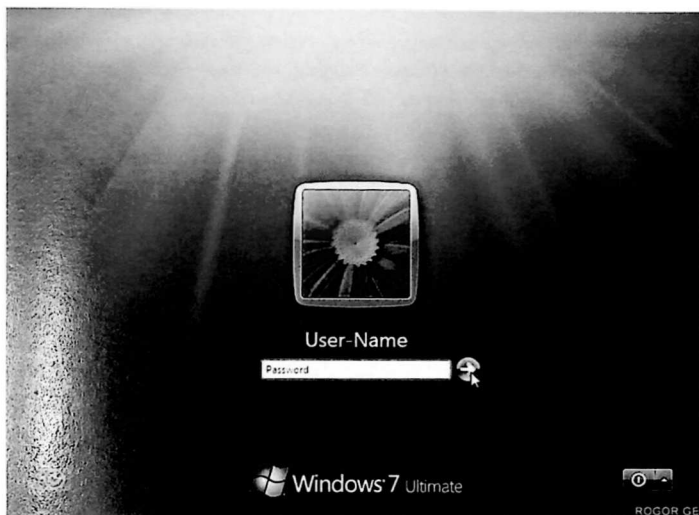


; 19.07.2019

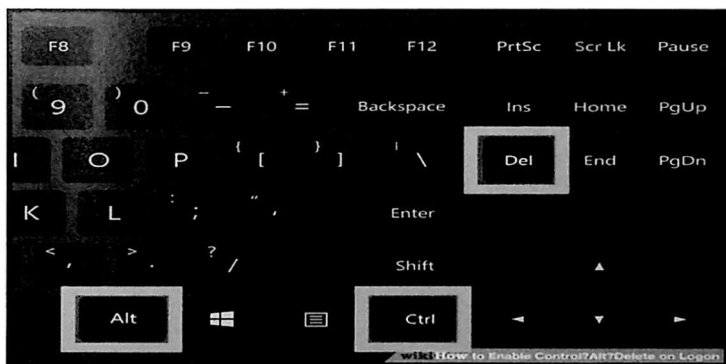
³¹⁵ სურათი აღებულია; ელ. გვერდიდან -



; 12.07.2019



სურათი N29 კლავიშების კომბინაცია (Windows - ის მქონე კომპიუტერებზე):



ნაბიჯი N3 — კომპიუტერის ეკრანზე მუშაობა:

ამდენად, თუ კომპიუტერი რომელთანაც თქვენ მუშაობთ განეკუთვნება Apple- ის Mac-ის ოჯახების კატეგორიას, დიდი ელბათობით თქვენ წინაშე იქნება Macos სისტემა, ხოლო სხვა ფირმის კომპიუტერებთან თუ გეძნებათ შეხებლობა — თქვენს წინაშე უმეტესწილად იქნება Microsoft Windows ან Linux სისტემა:

თითოეულ ზემოაღნიშნულ სისტემაზე მუშაობა მოითხოვს თავის სპეციფიკას, ამიტომ



ვინაიდან ინფორმაციის გამოთხოვის დროს კომპიუტერზე მუშაობა არის ძალიან მნიშვნელოვანი, განვიხილოთ ყველა მათგანი:

MICROSOFT WINDOWS - ოპ. სისტემის მქონე კომპიუტერების ეკრანის სტრუქტურა;

როდესაც კომპიუტერი ჩაირთვება, Windows - ის მქონე კომპიუტერებზე გაისხნება ვინდოუსის საწყისი ეკრანი, რომელზეც წარმოდგენილია სამუშაო მაგიდა (Desktop), ამოცანების პანელი (Task-bar), მენიუს ლილაკი (Start). (იხ. სურათი N27):

სურათი N30 Microsoft Windows ეკრანი:

317



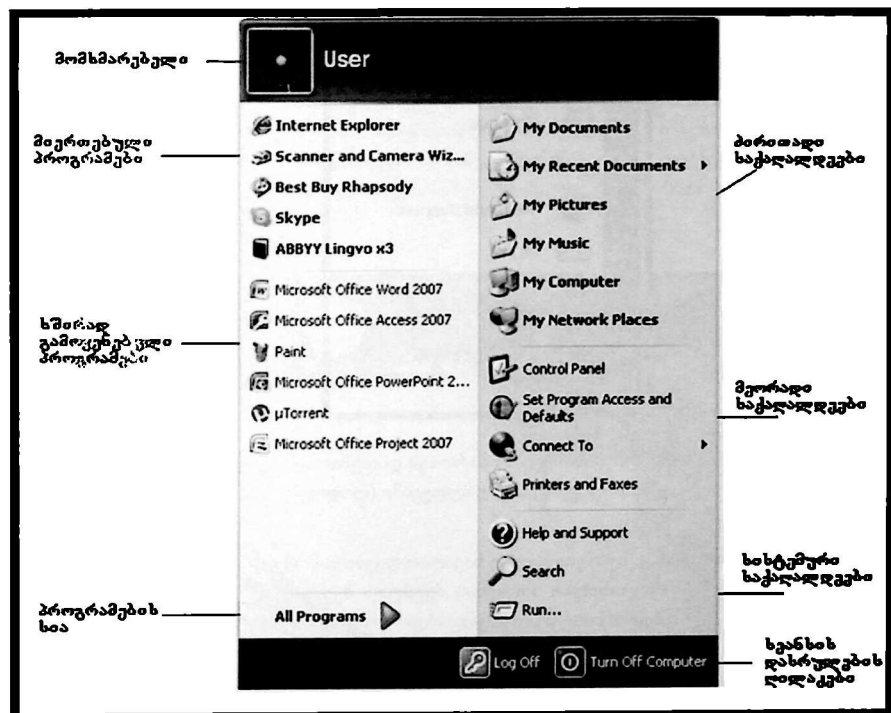
მარცხენა მხარეს არის ლილაკი Start. აღნიშნული ლილაკის ფუნქციური აგებულება შემდეგია: „Start“ ლილაკის ფანჯარაში წარმოდგენილია კავშირები კომპიუტერში ჩატვირთულ პროგრამებთან და იმ მოქმედებთან, რომლებიც ტარდება Windows ოპერაციული სისტემით. ფანჯრის ზემოთა სტრიქონში წარმოდგენილია მომხმარებლის ნიშანი და მისსახელი. მარცხენა ნაწილში პირველ პორიზონტალურ ხაზამდე მოთავსებულია მიერ შერჩეული მუდმივად ხმარების პროგრამები. აქ შეიძლება სტანდარტულად შეტანილი პროგრამებიც იყოს წარმოდგენილი. მაგალითად, ისეთპროგრამები, როგორიც არის Microsoft Internet Explorer და Microsoft OutlookExpress. თუ ისარგებლებთ სხვა ბრაუზერით ან საფოსტო პროგრამით, ეს სიაავტომატურად შეიცვლება. მომდევნო პორიზონტალური ხაზის წინ თავსდება იმ პროგრამების სია, რომლებიცბოლო დროს იყო გამოყენებული. მათი რაოდენობა შესაძლებელია მიუთითოთ. მარჯვნივ სამი ჯგუფია წარმოდგენილი. პირველში წარმოდგენილია საქალაქდები, რომლებშიც ინახება შექმნილი ფაილები და დოკუმენტები თავსდება. აქვეა ქსელითმიერთებული სხვა კომპიუტერების ღირეკტორიები და

³¹⁷ ცირა ჯაფიშვილი. ოპერაციული სისტემის Windows XP ადმინისტრირება ლექციების კურსი. გვ.რ. ელ გვერდი 317; ნანახია 02.07.2019



ზოგიერთი ინსტრუმენტი, საჭირო კომპიუტერზე მუშაობისთვის. ბოლო სტრიქონში კომპიუტერთან მუშაობის სენსის დამთავრების ღილაკებია.³¹⁸(იხ. სურათი N31);

სურათი N31 — Windows -ის ახალი ვერსიების სტარტ ღილაკის ფანჯარა;



³¹⁸ ცირა ჯაფიაშვილი. ოპერაციული სისტემის Windows XP ადმინისტრირება ლექციების კურსი. გვ. 9. ელ გვერდი 318; ნანახია 02.07.2019





როდესაც გამოძიებული კომპიუტერს ჩართავს და მუშაობას დაიწყებს, მან უნდა იცოდეს, რომ ფაილები ჯგუფდება კომპიუტერზე საქალაქლებში (ფოლდერებში). ოპერაციულ სისტემა 4 სისტემურ საქალაქს ქმნის:

1. Documents and Settings. იქმნება ცალკე საქალაქები სამომხმარებლო პროფილისთვის. ერთი მომხმარებლისთვის სისტემას შეუძლია შექმნას რამდენიმე პროფილი. თუ მომხმარებელი შედის სისტემაში სხვადასხვა პაროლით. თითოეულ პროფილში სისტემა ქმნის სამ საქალაქს: My Documents (ჩემი დოკუმენტები);
2. My Pictures (ჩემი სურათები), My Music (ჩემი მუსიკა). მათ შემასვენლობაზე მათი დასახელებები მეცვლებენ;
3. Program Files. ეს საქალაქი ემსახურება პროგრამულ ფაილებს, რომლებიც დაყენებულია კომპიუტერზე. აქ ხვდება პროგრამების გამშვები ფაილები. როგორც წესი, პროგრამის ინსტალირების შემდეგ, მათი სახელები და ძირითადი შემადგენელი პროგრამები აქ იყრის თავს;
4. Temp. ამ საქალაქში ოპერაციული სისტემა და სხვა პროგრამები ინახავენ დროებით ფაილებს;

319 ცირა ჯაფიაშვილი. ოპერაციული სისტემის Windows XP ადმინისტრირება ლექციების კურსი. გვ.6. ელ გვერდი 319 ; ნანახია 02.07.2019



WINDOWS ან WINNT. აქ ინახება სისტემური ფაილები და აქობებს მათ არ ახლოთ ხელი.”³²¹

„ფაილებს აქვთ დასახელება, რომელიც ორი ნაწილიდან შედგება: სახელი და გაფართოება. სახელი 256 სიმბოლოსგან წარმოებს. მასში არ შედის მოსამსახურე სილბოლოები, რომლებსაც სისტემური დატვირთვა აქვთ. მაგალითად: *, !, ;, : და სხვა. გაფართოება სამი სიმბოლოსაგან შედგება, შესაძლებელია ორი ან 4 სიმბოლოც და მიუთითებს ფაილის ტიპზე. ამ შემთხვევაში ტიპი ნიშნავს იმ პროგრამის იდენტიფიკატორს, რომელშიც იქმნება ფაილი. ფაილების გაფართოება სტანდარტულად დამალულია, მაგრამ მათი გამოტანა საჭიროების შემთხვევაში შესაძლებელია.

MACOS სისტემის მქონე APPLE-ის MAC-ის ოჯახის კომპიუტერების ეკრანის სტრუქტურა:

როდესაც Apple-ის Mac-ის ოჯახის კომპიუტერი ჩაირთვება, თუ მასზე macOS სისტემა არის, სახეზე გვექნება ეკრანი, რომელზეც იქნება თითქმის სრული მანეთი გახსნილი ეკრანის ქვედა მხარეს, სისტემას start ღილაკი არ გააჩნია, რადგან აღნიშნული ღილაკის შემადგენლობაში არსებული უმეტესი მოცულობები განლაგებულია ეკრანის ქვედა მხარეს. (იხ. სურათი N32);

სურათი N32 MacOS ეკრანი;



ასევე აღნიშნული კომპიუტერის მენიუში განლაგებული სხვადასხვა ინფორმაციის მოძიებისათვის თავის საშუალებით გავააქტიუროთ Launchpad. (იხ. სურათი N33);



Launchpad



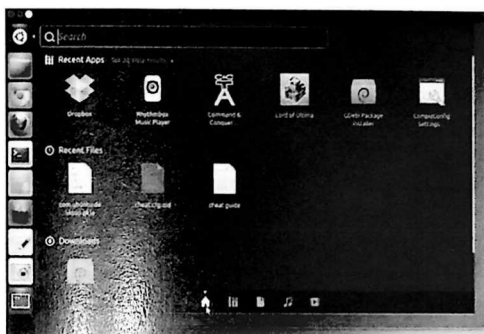
მას შემდეგ, რაც გამოძიებული კომპიუტერული სისტემიდან ინფორმაციის გამოთხოვას დაიწყებს, უნდა განახორციელოს რამდენიმე ნაბიჯი, რათა ინფორმაცია მის ხელთ აღმოჩნდეს.

LINUX-ის სისტემის მქონე კომპიუტერების ეკრანის სტრუქტურა:

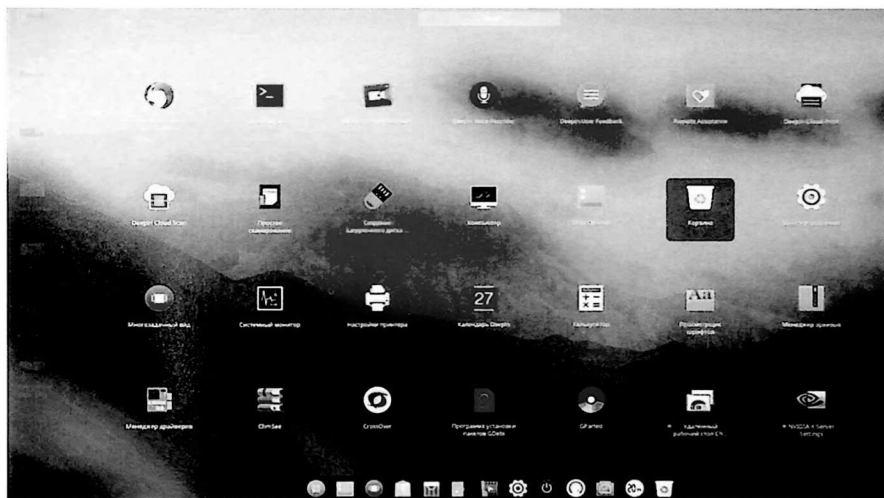
„Linux გამოირჩევა მრავალფეროვანი გრაფიკული ინტერფეისებით რომლებსაც მსოფლიოს სხვადასხვა ფირმები ქმნიან. მათგან გამოირჩევიან: KDE, Gnome, Window Maker და ა.შ.. სტანდარტულ გრაფიკულ ინტერფეისად მიჩნეულია KDE (KDE Desktop Environment), რომელიც დიდი პოპულარობით სარგებლობს მსოფლიოში. KDE-ს Desktop გრაფიკულად წააგავს Windows-ის Desktop-ს თუმცა მასზე მუშაობის პრინციპები განსხვავდება, მისი ეკრანი ასე გამოიყურება.“³²² (იხ. სურათი N34);

³²² Linux-ის სისტემის სტრუქტურა სერვერებისათვის. ნანახია ელ გვერდი 19.07.2019;





„Linux არც ოფისური შესაძლებლობების ნაკლებობას განიცდის, ფირმა Microsystems-მა სპეციალურად სისტემა Linux-ისთვის შეიმუშავა არაკომერციული პროგრამული პაკეტი StarOffice, რომელშიც გაერთიანებულია დოკუმენტის, საბრეზენტაციო, ელექტრონული ცხრილების, და სხვა მრავალი რედაქტორი. StarOffice-ს აქვს საკუთარი Desktop, რომელზეც განლაგებულია სხვადასხვა რედაქტორების გამოსაძახებელი პიქტოგრამები. იგი ასე გამოიყურება.“ ³²⁴ (იხ. სურათი N35);



„FAT (File allocation Table) ფაილური სისტემა წარმოადგენს ცხრილს, რომელშიც მითითებულია, ლოგიკური დისკის უშუალოდ დამისამართებელი ადგილები, სადაც თავსდება ფაილები ან მათი ფრაგმენტები, სტანდარტული კატალოგები Linux-ში შემდეგია;

³²³ ელ. გვერდი ; ნანახია 19.09.2019;

³²⁴ linux ოპერაციული სისტემა სერვერებისათვის. ნანახია ელ გვერდი : 19.07.2019;

³²⁵ ელ. გვერდი ; ნანახია 19.09.2019;

- ბი: — სისტემის ჩამტვირთველი;
- ხ:ი — შეიცავს სტანდარტულ პროგრამებს;
- home — შეიცავს მომხმარებლის სამუშაო კატალოგებს;
- usr — შეიცავს ყველა იმ პროგრამას რასაც იყენებს სისტემა;
- sb:ი — ბრძანებები სისტემური ადმინისტრირებისთვის;
- var — შეიცავს ისეთ ფაილებს, რომლებიც ხშირად იცვლებიან, მაგ. საფოსტო ყუთის ან პრინტერის დაყენებები, ბუფერული ფაილები;
- els — სისტემის დაყენებების ფაილები;
- dev — პერიფერიული მოწყობილობების შესახებ ფაილები;
- tmp — კატალოგები დროებითი ფაილებისათვის;
- mnt — ფაილები სხვადასხვა კატალოგების მიმაუნთების(მიერთების) შესახებ.³²⁶

ნაბიჯი N4 კომპიუტერის სახელის დადგენა:

განვიხილოთ:

კომპიუტერის სახელის დადგენა WINDOWS სისტემების მქონე კომპიუტერებში;

კომპიუტერის სახელის დადგენა MACOS სისტემების მქონე კომპიუტერებში;

კომპიუტერის სახელის დადგენა LINUX სისტემის მქონე კომპიუტერებში;

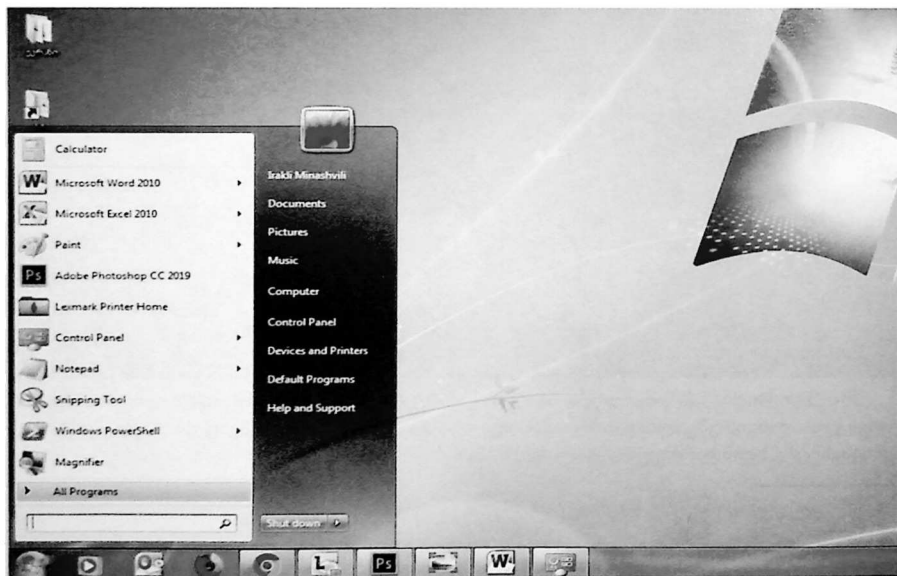
განვიხილოთ თითოეული მათგანი;

კომპიუტერის სახელის დადგენა ნებისმიერი Windows სისტემების მქონე კომპიუტერში;

ნაბიჯი 1.

შევდივართ ლილაკში start; (იხ. სურათი N36);

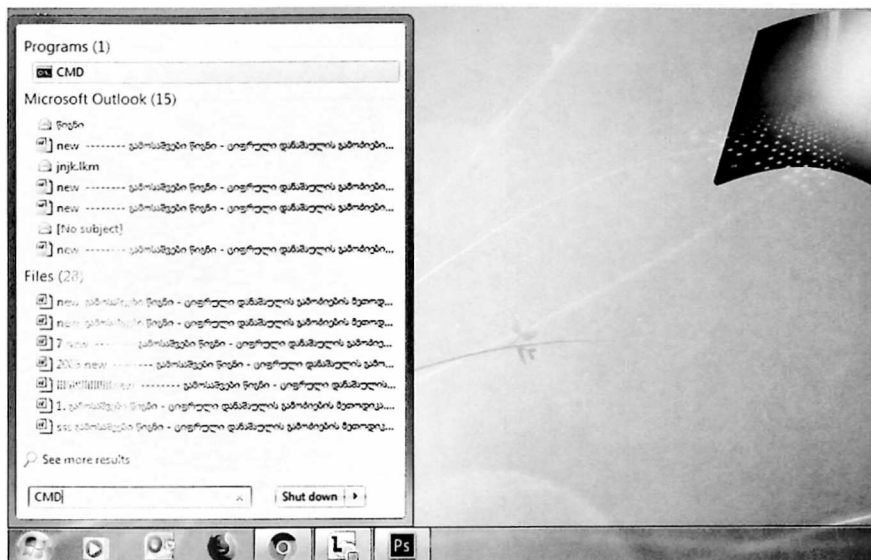
სურათი N36



ნაბიჯი 2.

Start ლილაკში ვკრებთ cmd რის შემდეგაც ვაწკაპუნებთ ლილაკს Enter; (იხ. სურათი N37);

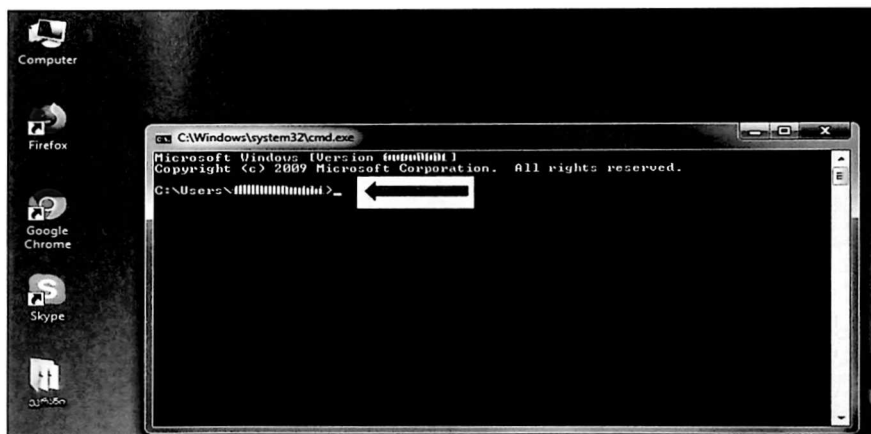
სურათი N37;



ნაბიჯი 3.

Enter ლილაკზე დატერის შემდეგ გამოვა შავი ფერის ფანჯარა; (იხ. სურათი N38);

სურათი N38;



ნაბიჯი N4;

იმ ადგილზე სადაც N39-ე სურათზე წითელი ისრით არის მითითებული, ჩაწერეთ `hostname` რის შემდეგაც დააწკაპუნეთ ღილაკს **Enter** და დაინახავთ რომ პროგრამა დაწერს კომპიუტერის სახელს, ამ შემთხვევაში სახელი არის `tesiname 0099`: (იხ. სურათი N39):

სურათი N39:



ნაბიჯი N5;

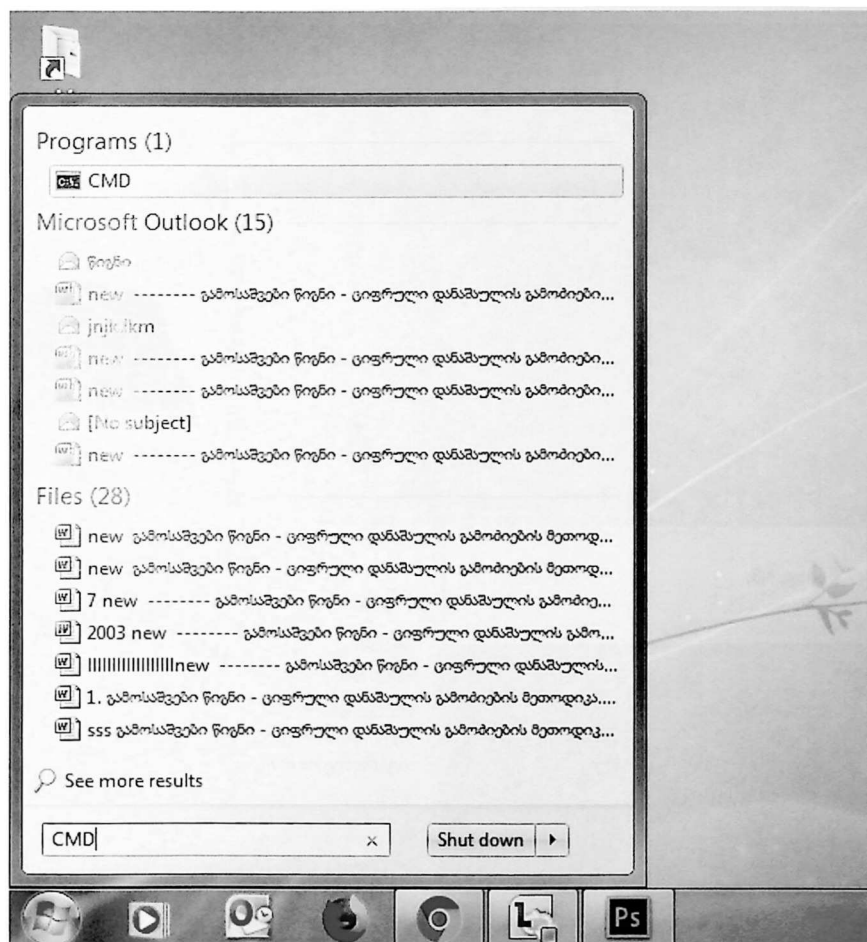
დავაკოპირებთ აღნიშნულ მონაცემს და გადავიტანთ საგამოძიებო მოქმედების ოქმში.

კომპიუტერის სისტემური მონაცემების დადგენა;

სხირად არის საჭიროება, კომპიუტერის დათვალიერებისას, საგამოძიებო მოქმედების ოქმში გადატანილი იქნეს შესაბამისი კომპიუტერის სისტემური მონაცემები, ამისათვის ყველა Windows სისტემის კომპიუტერზე შეგვიძლია განვახორციელოთ ქმედებები:

ნაბიჯი 1.

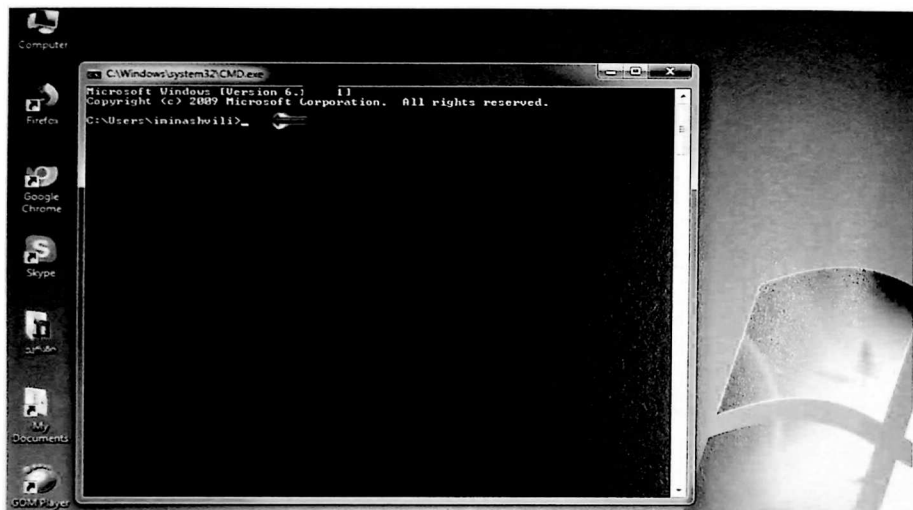
შევდივართ ლილაკში start და ვკრებთ cmd რის შემდეგაც ვაჭერთ ლილაკს Enter (იხ. სურათი N40);
სურათი N40;



ნაბიჯი 2.

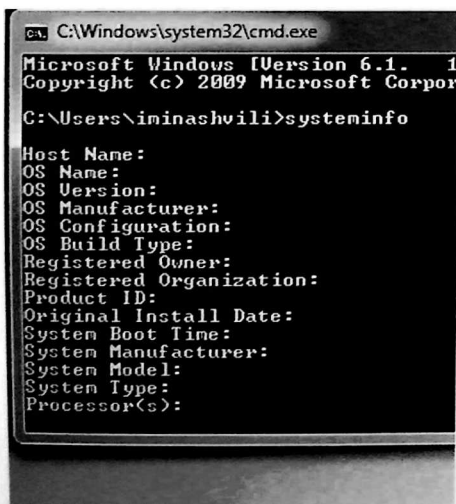
Enter ღილაკზე დაჭერის შემდეგ გამოვა შავი ფერის ფანჯარა; (იხ. სურათი N41);

სურათი N41:



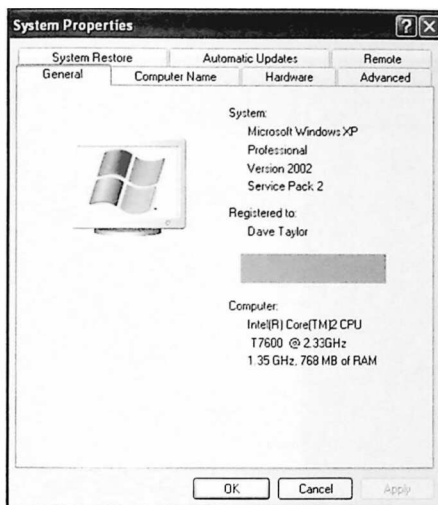
ნაბიჯი N3;

სურათი N42:



აღნიშნულ ფანჯარაში ჩაწერით სიტყვა Systeminfo რის შემდეგაც დააწვით ღილაკს Enter და გამოვა კომპიუტერის მონაცემები, დავაკოპირებთ აღნიშნულ მონაცემს და გადავიტანთ საგამოძიებო მოქმედების ოქმში; (იხ. სურათი N42);

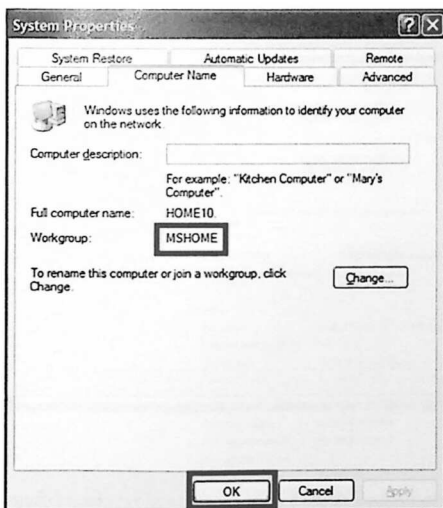
როგორც ზემოთ უკვე აღინიშნა ამ ტიპის ძებნა შესაძლოა განხორციელდეს Windows სისტემის ყველა კომპიუტერში, რადგან ყველას გააჩნია Cmd ფუნქციონალი, მაგრამ გამოძიებელს შეუძლია ინდივიდუალურად, თითოეულ კომპიუტერში გარკვეული ოპერაციების საშუალებით განხორციელოს სახელის და კომპიუტერის მონაცემების დადგენა, ამისათვის ამჟერად განვიხილოთ Windows სისტემის რამდენიმე პროგრამაში შესაბამისი პროცედურა როგორ უნდა ვაწარმოოთ ინდივიდუალურად;



სისტემის პარამეტრების და კომპიუტერის სახელის დადგენა Windows XP-ში;
Start ლილაკის ძეხვის ფუნქციაში ვწერთ system properties - ს, რის შემდეგაც გამოჩნდება ფანჯარა, სადაც ვირჩევთ general სადაც გამოჩნდება თუ რომელი კომპიუტერული პროგრამა არის ჩატვირთული შესაბამის კომპიუტერში (იხ. სურათი N42a);

სურათი N42a: ³²⁷

„Windows XP-სა და Windows Server 2003-ში ეს ფანჯარა თითქმის ერთნაირია. ახალი ვერსიებისგან განსხვავებით, აქ ინფორმაცია რამდენიმე ჩანართად (Tab) არის დაყოფილი. ძირითადი ინფორმაცია ამ სურათზე ჩანს.“³²⁸



„კომპიუტერის სახელის და სამუშაო ჯგუფის სანახავად Computer Name განყოფილებაში უნდა გადავიდეთ. ეს ნაჩვენებია ქვემოთ მოცემულ სურათზე.“³²⁹ (იხ. სურათი N43);

სურათი N43: ³³⁰

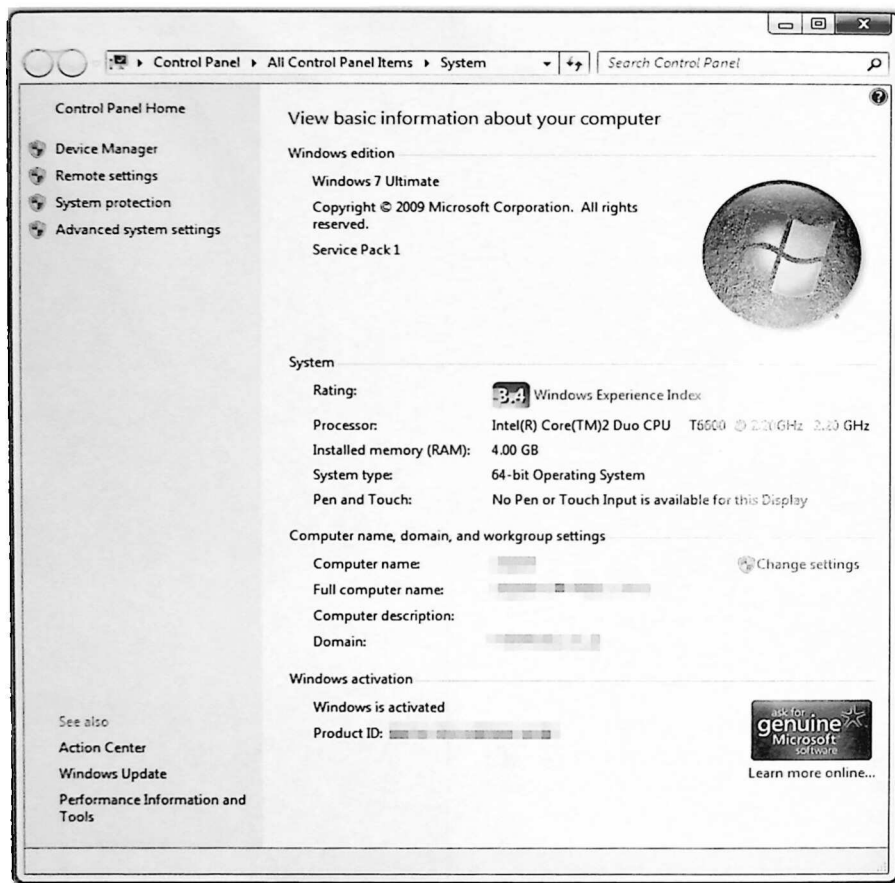
სისტემის პარამეტრების ფანჯარა Windows 7-ში;
Windows 7-სა და Windows Vista-ს შემთხვევაში ეს ფანჯარა ერთმანეთის მსგავსია. Start ლილაკის ძეხვა ფუნქციონალში ვწერთ control panel, რის შემდეგაც შევდივართ All Control panel Items, ხოლო შემდეგ System-ში; (იხ. სურათი N44);

³²⁷ ელ.გვერდი  ; ნანახია 19.07.2019

³²⁸ იქვე.

³²⁹ იქვე.

³³⁰ ელ.გვერდი  ; ნანახია 19.07.2019

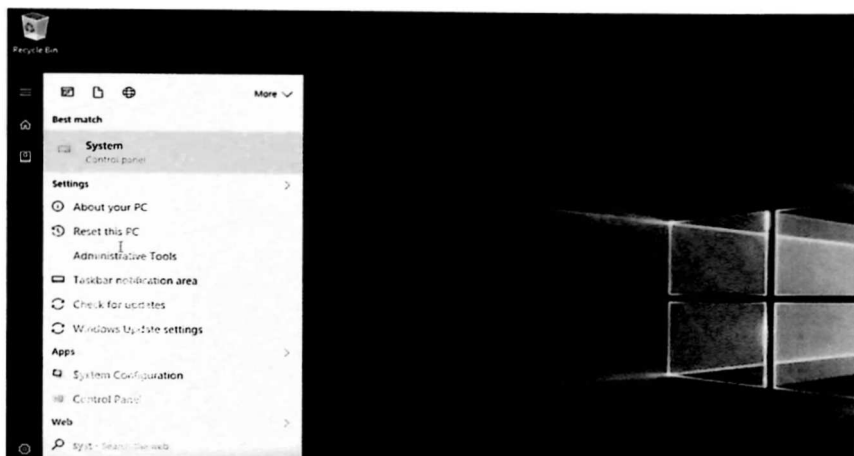


სისტემის პარამეტრების ფანჯარა Windows 10-ში:

...რაც შეეხება Windows 10-ს, აქ სისტემის ინფორმაციის ფანჯარა Windows 8-ს მსგავსია და იგივე ინფორმაციას გვაწვდის. კომპიუტერის ეკრანიდან შევდივართ ლილაკში start, საიდანაც ძეხნის ლილაკში ვწერთ: System ³³²; (იხ. სურათი N45);

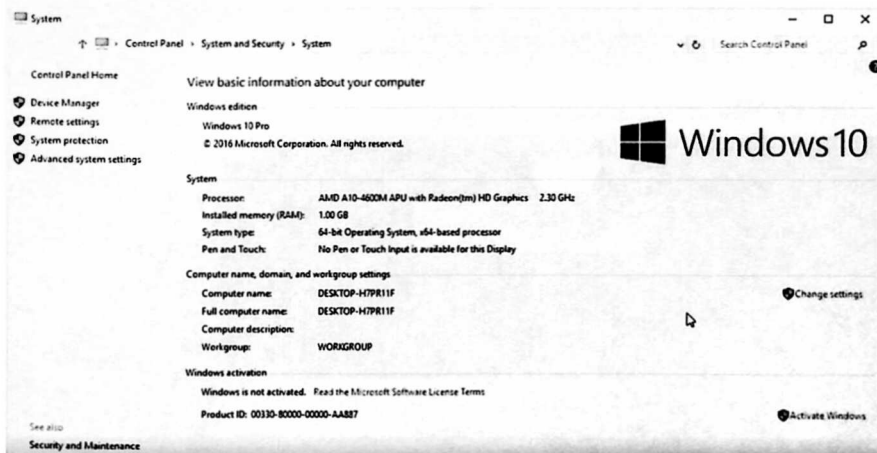
³³¹ ელ.გვერდი  : ნანახია 19.07.2019 .

³³² ელ.გვერდი  : ნანახია 19.07.2019



შემდეგ გაუხსნა დაჭერით შევლიდართ System-ში, სადაც იშლება კომპიუტერის შესახებ სრული ინფორმაცია.³³⁴ (იხ. სურათი N46);

სურათი N46:³³⁵



333

იქვე.

334

იქვე.

335



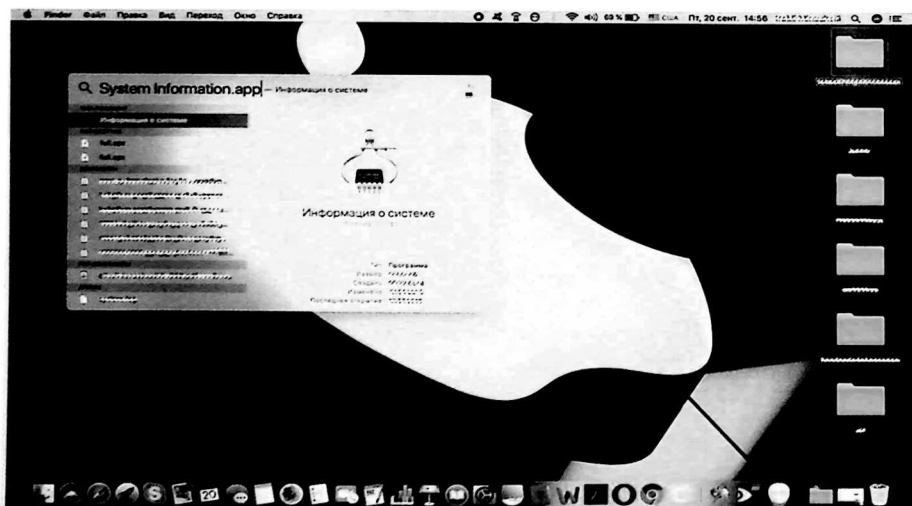
3. კომპიუტერის სახელის დადგენის მეთოდი MacOS სისტემის მქონე კომპიუტერებში: მივიღეთ ძეგნა ლილაკთან. რომელიც მდებარეობს ეკრანის ზედა მხარეს და აქვს ლუპის გამოსახულება. მათსი მარჯვენა ლილაკით ერთხელ დავაწვეთ აღნიშნულ ლუპას, (იხ. სურათი N47);

სურათი N47;



აღნიშნულია შემდგომ გახსნილ გრაფაში ავკრიბოთ System Information.app ხოლო თუ სისტემა რუსულ ენაზეა ავკრიბოთ Информация о системе, რის შემდეგაც დააჭირეთ ენცერ ლილაკს (იხ. სურათი N48);

სურათი N48:



ენტერ ლილაკზე დაჭერის შემდეგად თქვენს წინაშე გამოვა კომპიუტერის შესახებ სრული ინფორმაცია, სადაც მოცემულია კომპიუტერის სახელიც, (იხ. სურათი N48);

სურათი N49;



კომპიუტერის სახელის დადგენა linux სისტემის მქონე კომპიუტერებში;

Linux სისტემის მქონე კომპიუტერებზე შეგვიძლია განვახორციელოთ შემდეგი პროცედურები პროცედურები:

„ვიპოვოთ ეკრანზე ძებნა ლილაკი, რის შემდეგაც ავკრიბოთ command-line terminal app შემდეგ შევიღეთ select Applications > Accessories > Terminal, ხოლო შემდეგ ავკრიბოთ hostname რის შემდეგაც დაიწერება კომპიუტერის სახელი“. ³³⁶ (იხ. სურათი N50);

სურათი N50;

```
vivek@nixcraft:~$  
vivek@nixcraft:~$  
vivek@nixcraft:~$ hostname  
nixcraft
```

337

„თუ ჩვენ გვსურს დავადგინოთ კომპიუტერის სხვა მონაცემები მაშინ ავკრიბოთ hostnamectl ხოლო შემდეგ დავაწვებთ ეკრანს რის შემდეგაც ჩამოშლის კომპიუტერის სისტემურ მონაცემებს“ ³³⁸ (იხ. სურათი N50a);

³³⁶ ელ. გვერდი ნანახია 19.07.2019



³³⁷ ექვე.

³³⁸ ექვე.

იხ. სურათი N50ა:

```
vivek@nixcraft:~$  
vivek@nixcraft:~$ hostnamectl  
Static hostname: nixcraft  
Icon name: computer-laptop  
Chassis: laptop  
Machine ID: 291893e6499e4d99891c3cf4b  
Boot ID: 9fda2365b77841649e40a141f  
Operating System: Ubuntu 17.10  
Kernel: Linux 4.13.0-21-generic  
Architecture: x86_64  
vivek@nixcraft:~$  
vivek@nixcraft:~$
```

339

ნაბიჯი N5 ფაილის მოძებნა:

როგორც ზემოაღნიშნულ შემთხვევაშიც, ამჯერადაც განვიხილოთ ძებნის შემთხვევა:

საძიებო სისტემა WINDOWS სისტემების მქონე კომპიუტერებში;

საძიებო სისტემა MACOS სისტემების მქონე კომპიუტერებში;

საძიებო სისტემა LINUX სისტემების მქონე კომპიუტერებში;

ფაილის მოძებნა WINDOWS სისტემების მქონე კომპიუტერებში;

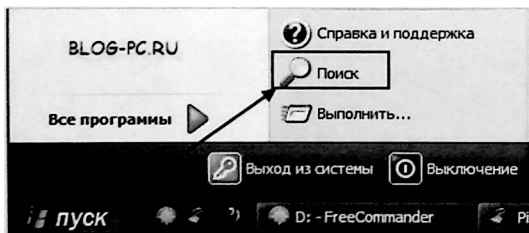
საწყის ეტაპზე აღვნიშნოთ, რომ ყველა Windows სისტემის მქონე კომპიუტერს როგორც ზემოთ უკვე აღნიშნა აქვს ლილაკი Start, როდესაც აღნიშნულ ლილაკს გავაპტიურებთ, ქვემოთ ყველა შემთხვევაში შეგვხვდება ძებნის ცარიელი გრაფა, სადაც ჩაწერით სასურველი დოკუმენტის სახელწოდებას და მოხდება მისი ძებნა, მაგრამ შესაძლოა აღნიშნული ძებნის ფუნქციონალი არ იყოს სრულყოფილი.

აღნიშნულის შემდგომ განვიხილოთ ძებნის დეტალური ფუნქციონალი windows - ის ყველაზე მეტად გავრცელებულ ოპერაციულ სისტემებში:

1. საძიებო ფუნქციონალი WINDOWS XP - ის ოპერაციული სისტემის მქონე კომპიუტერებში:

კომპიუტერში რომ ვნახოთ ფაილი ან პაპაკ, უნდა დავაჭიროთ ლილაკს start ს, რის შემდეგ უნდა დავაჭიროთ ლუპის ფორმის ძებნის ლილაკს ; (იხ. სურათი N51);

იხ. სურათი N51:



340

339 ელ. გვერდი : ნანახია 19.07.2019



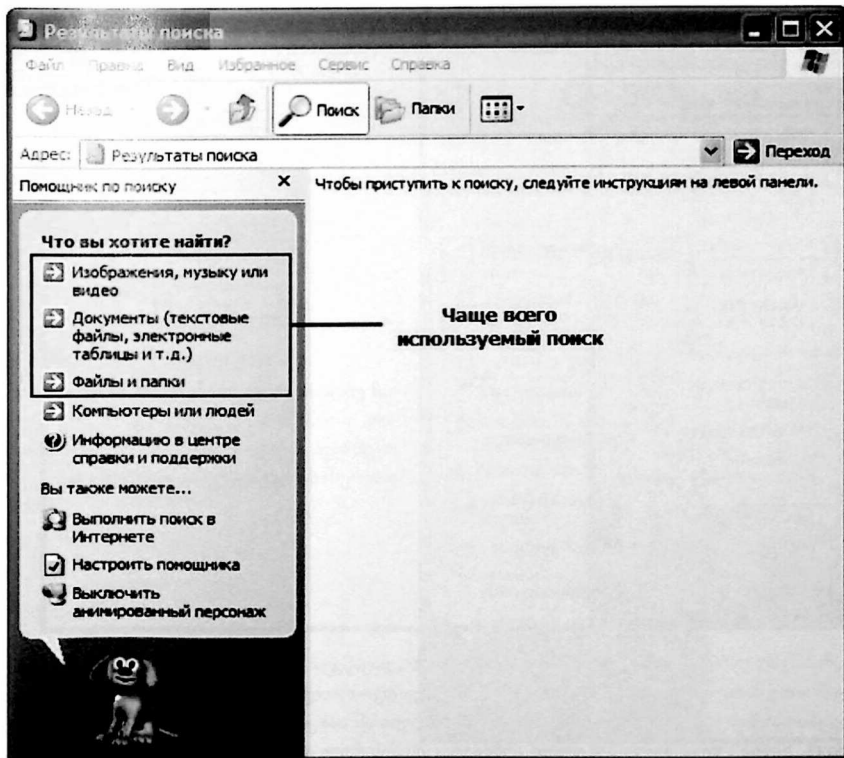
340 იხილეთ. ელ. გვერდი : ნანახია 19.07.2019



აღნიშნულის შემდეგ მოვხვდებით მენიუში, რომელიც საშუალებას გვაძლევს ავირჩიოთ ის რისი მოძიებაც გვინდა, აღნიშნულ დოკუმენტში ჩამოთვლილია რამდენიმე კატეგორია:

- სურათები, მუსიკა ან ვიდეო (Pictures, Music or Video);
- დოკუმენტები (საოფისე პროგრამების მიერ შექმნილი ფაილები) (Documents (Word processing, Spreadshits, etc.))
- ყველა ფაილი და საქალაქი (All Files and Folders);
- კომპიუტერები და ხალხი (Computers and people), ინფორმაცია დახმარების და მხარდაჭერის ცენტრიდან (Information in Help and Support center);
- ინტერნეტში ძებნა (Search the internet).
- მენიუში ბოლო პუნქტი კი ცვლის ძებნის ოპციებს. (იხ. სურათი NS2);³⁴¹

სურათი NS2:



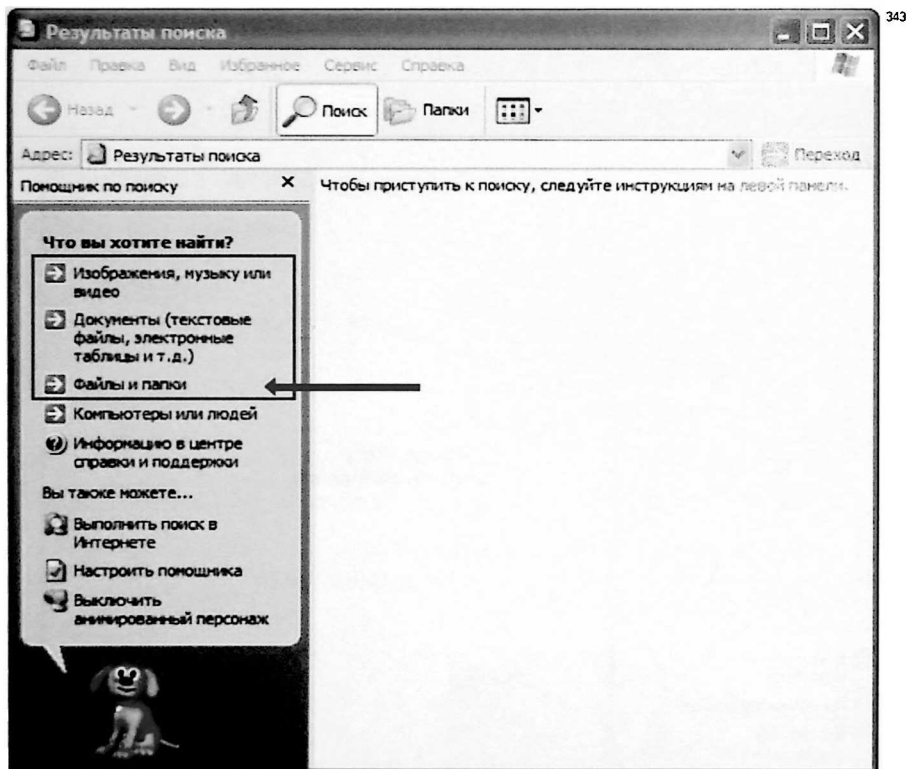
³⁴¹ ელ. გვერდი:  ნანახია 13.07.2019

³⁴² იხილეთ. ელ. გვერდი:  ნანახია 19.07.2019

ჩამოთვლილიდან ავირჩევთ იმ კომპონენტს, რომლის ძებნაც გვსურს, და მაუსი მიგვყავს და ვაწვევბით აღნიშნულ კომპონენტს. რის შემდეგაც ახალ ეკრანზე უკვე გამოდის ახალი ფანჯარა, რომელიც გვაძლევს ფაილების მონიშვნის საშუალებას:

როგორ მოვძებნოთ სურათები, მუსიკა ან ვიდეო (PICTURES, MUSIC OR VIDEO)?
დავეშვათ ვეძებთ მხოლოდ სურათებს. მაშინ ვნიშნავთ მარტო პირველ პუნქტს Pictures and Photos, (იხ. სურათი N53):

სურათი N53:



...მას შემდეგ რაც ავირჩევთ პუნქტს Pictures and Photos, დავაწვეთ მაუსის ღილაკით და გამოჩნდება ფანჯარა. თუ მარტო სურათებს კი არა არამედ ასევე ვიდეო ფაილებს ვეძებთ მოვნიშნოთ ვიდეოც. შევიყვანოთ სასურველი სურათის ან ვიდეოს სახელი ან სახელის ნაწილი და დავაწკაპუნოთ ღილაკს "ძებნა". მოცემული სახელით კომპიუტერში შენახულ ყველა სურათს და ვიდეო ფაილს დავინახავთ ფანჯრის მარჯვენა ნაწილში. თუ გვსურს ძებნის უფრო კონკრეტული კრიტერიუმების მითითება, მაშინ დააწკაპუნეთ Use Advanced search options (გამოიყენე ძებნის გაფართოებული ოპციები), მისი დაწკაპუნების შემდეგ გამოჩნდება შემდეგი ეკრანი: 3 მინდორი, პირველში უნდა ჩავწეროთ



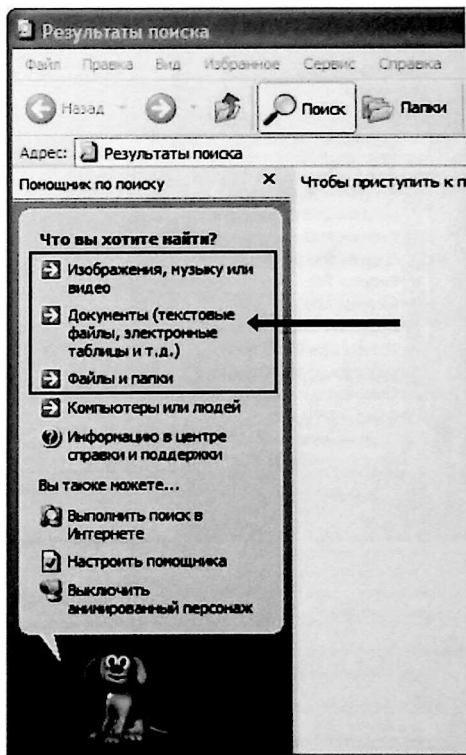
ფაილის სახელი ან სახელის ნაწილი, მეორეში - ფაილში არსებული ფრაზა ან სიტყვა, მესამეში კი უნდა მივუთითოთ სად ეძებოს ფაილი.”³⁴⁴ (იხ. სურათი N54);

იხ. სურათი N54;³⁴⁵

2. როგორ მოვძებნოთ დოკუმენტები (საოფისე პროგრამების მიერ შექმნილი ფაილები) (Documents (Word processing, Spreadshils, etc.) ?

იმისთვის რომ მოვძებნოთ პაპკა ან ფაილი, მაუსით უნდა დავაწვეთ მითითებულ სურათს, (იხ. სურათი N50);

სურათი N55;³⁴⁶



მის შემდეგ გაიხსნება ფანჯარა, სადაც ჩამოვშალოთ ფაილები და ავირჩიოთ დამატებითი პარამეტრები საიდანაც ავირჩევთ ჩვენთვის საჭირო დოკუმენტს; (იხ. სურათი N56);

³⁴⁴ ელ. გვერდი;  : ნანახია 13.07.2019

³⁴⁵ იქვე.

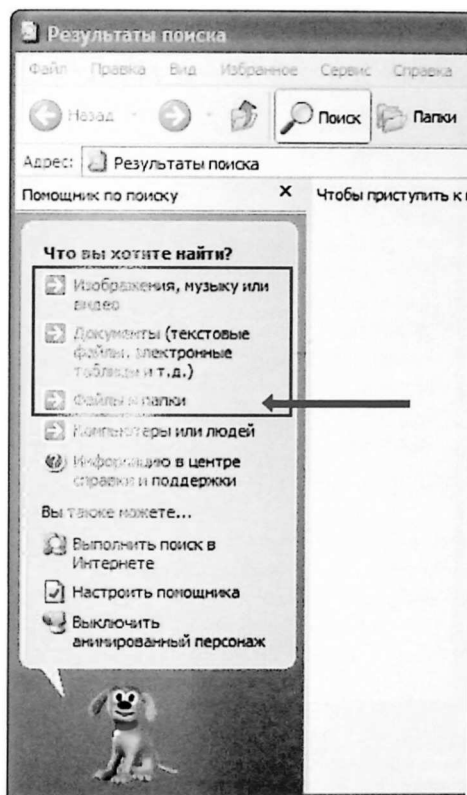
³⁴⁶ იხილეთ. ელ. გვერდი;  ნანახია 19.07.2019



როგორ უნდა მოვეძებნოთ ინფორმაცია ფაილის ტექსტის მიხედვით?

იმისათვის, რომ ინფორმაცია მოვეძებნოთ ფაილის ტექსტის მიხედვით, მასუსით უნდა დავაწვეთ მითითებულ ღილაკს, (იხ. სურათი N57):

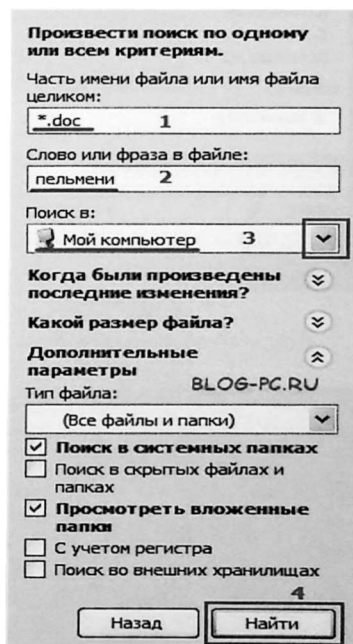




348

რის შემდეგაც გაიხსნება შემდეგი ფანჯარა, სადაც შეგვიძლია ვიპოვოთ რომელი ფაილი გვხვდება ჩვენთვის სასურველი სიტყვა, მაგალითისათვის, 1-ლ გრაფაში ვავსებთ დოკუმენტის ფორმატს - doc. მე-2 გრაფაში ვწერთ იმ სიტყვას რომლითაც დოკუმენტს ვეძებთ, ხოლო ბოლო გრაფაში ვირჩევთ იმ ფაილსა ან ფაილებს რომელშიც ვეძებთ აღნიშნული სიტყვის შემცველ დოკუმენტს, რის შემდეგაც მაუსით ვააქტიურებთ ლილაკს search; (იხ. სურათი N58);

იხ. სურათი N58; 349

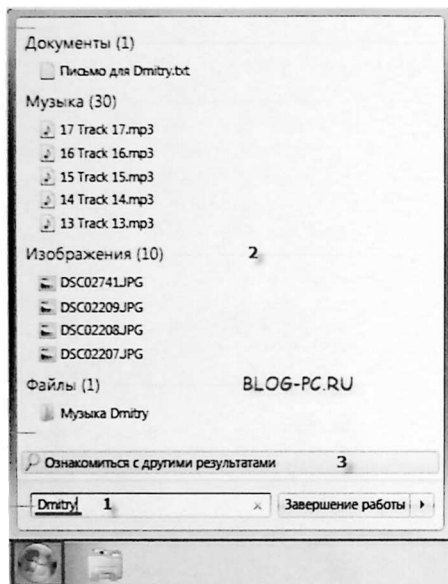


საძიებო ფუნქციონალი ოპერაციული სისტემა WINDOWS 7 ის მქონე კომპიუტერებში;

Windows 7 ში დოკუმენტის ძებნის რამდენიმე სერვისი არსებობს.

ეკრანზე ვნახულობთ ლილაკს Start, სადაც არის ძებნის გრაფაში (იხ. სურათი N59);

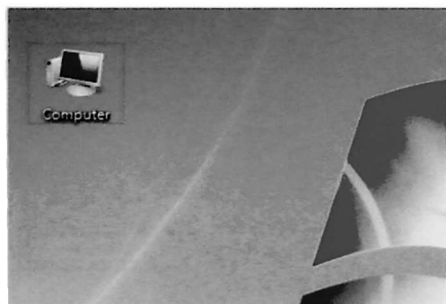




აღნიშნულის შემდგომ გრაფაში ჩვენ ვწერთ იმ დოკუმენტის დასახელებას, რომლის მოძებნაც გვსურს და ჩამოიშლება ყველა ის დოკუმენტი რასაც ჩვენ ვეძებთ, ასევე შეგვიძლია ჩავწეროთ სიტყვა ან/და წინადადება რომლის საშუალებითაც დოკუმენტი გვინდა მოვძებნოც და რომელიც ფიგურირებს დოკუმენტში, პროგრამა თავად გაგვიხსნის ყველა იმ დოკუმენტის ჩამონათვლს, რომელშიც მსგავსი სიტყვა ან/და სათაური დომინირებს, საიდანაც ავირჩევთ ჩვენთვის საჭირო დოკუმენტს და გავსხნით მას მუხის ლილაკის საშუალებით. (იხ. სურათი N60);

იხ. სურათი N60;³⁵¹

ასევე არის დოკუმენტის მოძიების სხვა შესაძლებლობაც, მათ შორის:



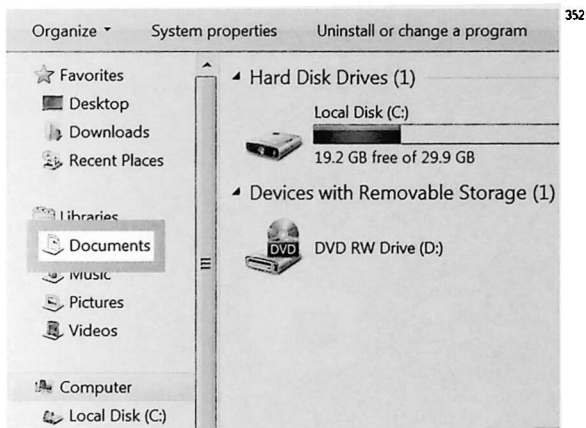
კომპიუტერის ეკრანზე ვნახულობთ ლილაკს Computer ან My computer (იხ.სურათი N61);

სურათი N61;



აღნიშნულ ღილაკში როდესაც შევალთ გაიხსნება შემდეგი მოცემულობის ეკრანი (იხ. სურათი N62):

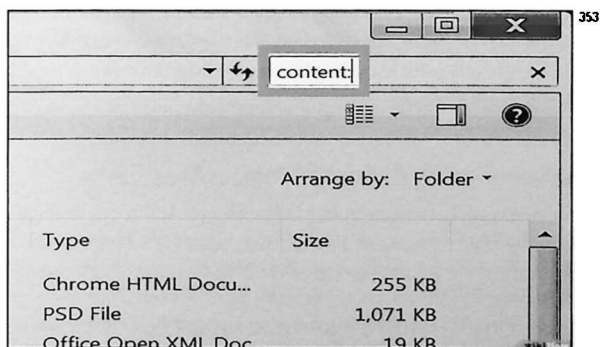
სურათი N62:



ავირჩევთ მოცემულობას როშელიც გვინდა მოვძებნოთ; მაგალითად Dokument, pictures და ა.შ.

მას შემდეგ რაც ავირჩევთ მარცხენა მხარეს არსებულ ძეხნის ფუნქციონალში ჩავენერთ შესაბამისი დოკუმენტის დასახელებას, შემდეგ Enter ღილაკს და მოიძებნება ის დოკუმენტი რომლის მოძებნაც გვინდოდა, (იხ. სურათი N63);

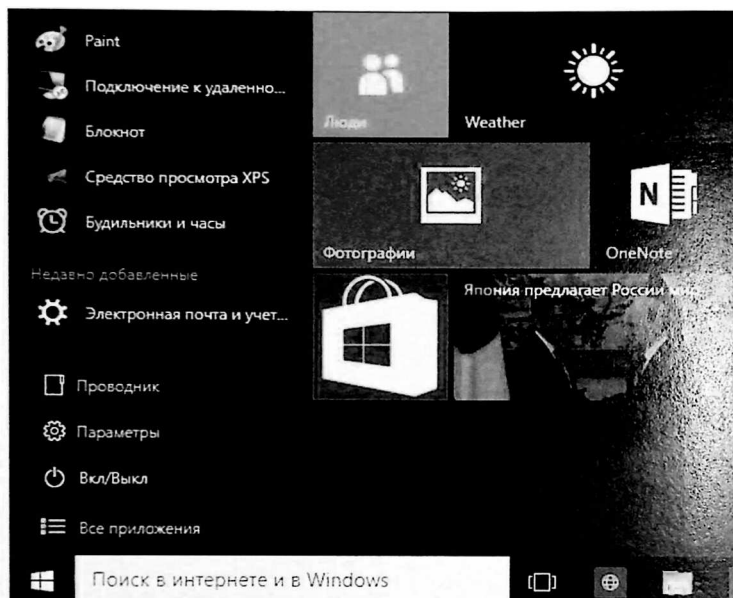
სურათი N63:



352 იხ. ელ.გვერდი 19.02.2019

353 იხ. ელ.გვერდი 19.02.2019

იხ. სურათი N64:



354

აღნიშნულ ოპერაციულ სისტემაში ძებნის ფუნქციონალი გამარტივებულია, Start ლილავის გახსნის შედეგად ძებნის ფუნქციონალში ვწერთ იმ დოკუმენტის დასახელებას, ხოლო შემდგომ ზედა მხარეს ჩამოთვლილი ფუნქციონალებიდან ვირჩევთ ერთ-ერთს. მაგალითად Document რის შედეგადაც პროგრამა თავად მოძებნის ჩვენს მიერ მითითებულ დოკუმენტს. ასევე შეგვიძლია მივუთითოთ სიტყვა ან წინადადება, რომლის საშუალებითაც გვსურს დოკუმენტის მოძებნა (იხ. სურათი N64)

3. საძიებო ფუნქციონალი Mac os სისტემების მქონე კომპიუტერებში;

მივიდეთ ძებნა ლილავთან, რომელიც მდებარეობს ეკრანის ზედა მხარეს და აქვს ლუპის გამოსახულება, მუხის მარჯვნივ ლილავით ერთხელ დავაწვეთ აღნიშნულ ლუპს, მას შემდეგ რაც აღნიშნულ ადგილზე ჩაწერთ იმ დოკუმენტის დასახელებას რაც გვსურს, კომპიუტერი დეტალურად გვიპოვის აღნიშნულ დოკუმენტს, ხოლო თუ თქვენს მიერ მითითებულ დასახელებას შეიცავს რამდენიმე დოკუმენტი, პროგრამა წარმოგიდგენთ ყველა დოკუმენტს, რომელთა შორისაც არჩევის მიზნით მოგიწევთ თითოეული დოკუმენტის ნახვა; (იხ.სურათი N65);





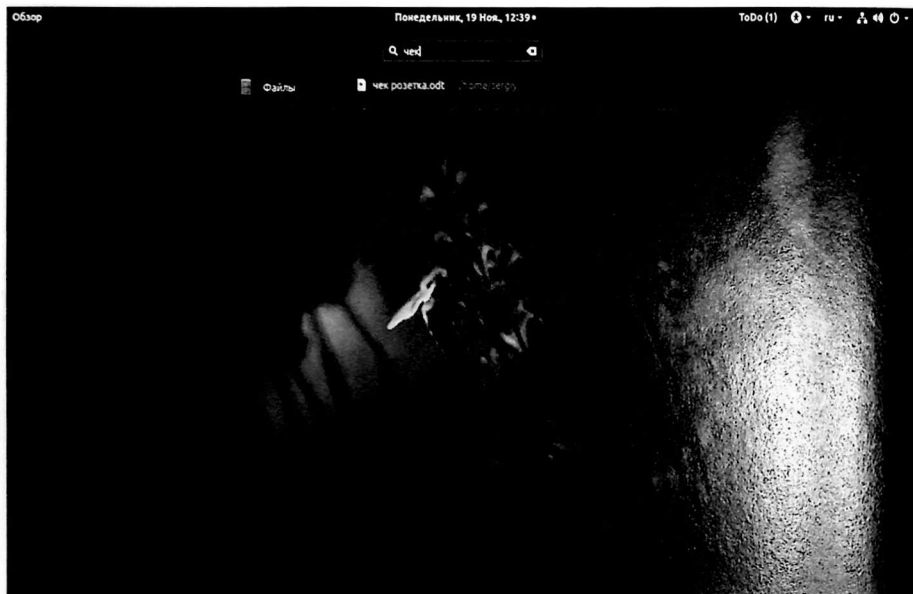
საძიებო ფუნქციონალი LINUX ოპერაციული სისტემის მქონე კომპიუტერებში:

LINUX სისტემის მქონე კომპიუტერებში ძებნა შესაძლოა განხორციელდეს რამდენიმე საშუალებით. განვიხილოთ სამი შესაძლებლობა:

ძებნა სისტემის მთავარი მენიუდან:

..ოპერაციული სისტემის მთავარი მენიუ, როგორც წესი არამარტო უშვებს პროგრამებს, არამედ ძებნის როგორც პროგრამებს ასევე ფაილებს, ასეთი საშუალებას გვაძლევს GNOME და CDE, კერძოდ, GNOME ს მთავარ მენიუში ჩვენ შეგვიძლია შევიყვანოთ საჭირო მოსაძებნი ფრაზა³⁵⁵ (იხ.სურათი N64)





„მაგრამ ასეთ მოძებნას აქვს გარვეული ნაკლოვანება, ის განკუთვნილია უფრო პროგრამების და არა ფაილების ძიებისთვის, ამიტომ ის ეძებს მხოლოდ home folder (домашней папке) და ფაილის სისტემაში უფრო ღრმად ძებნას არ ახორციელებს.“³⁵⁷

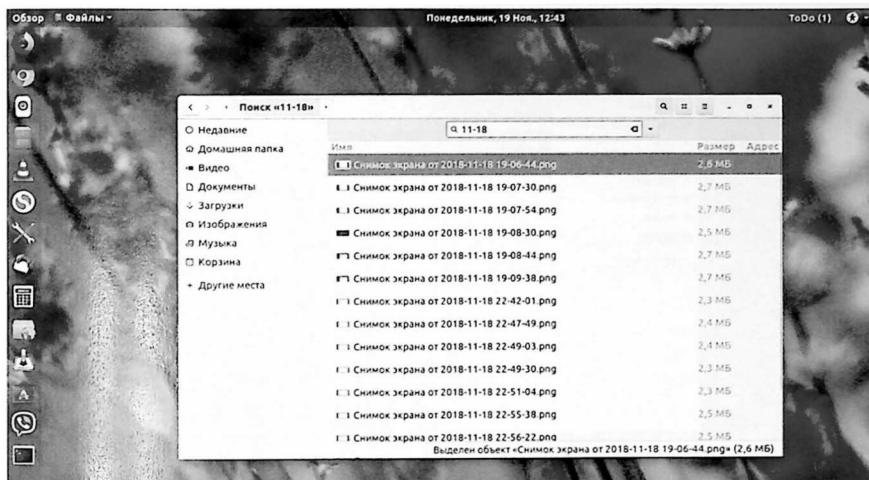
2. ფაილის მენეჯერის საშუალებით დოკუმენტის ძებნა;

უმეტესობა ფაილების მენეჯერებისა, გვაძლევს საშუალებას ფაილების ძებნისა, მათ შორის Dolphin и Nautilus. აქ თქვენ შეგიძლიათ აირჩიოთ პაკა, რომელშიც ხორციელდება ძებნა, [...] კერძოდ, Nautilus - ში ძებნის ჩასაშვებად მხოლოდ საჭიროა დააჭიროთ ლუპის ფორმის ლილავს და შემდეგ შეიცვანოთ მოსაძებნ სტრიქონში საჭირო მონაცემი, მაგალითად მოძებნოთ ყველა ფოტო, რომლებიც შექმნილია 18 ნოემბერს;³⁵⁸ (იხ.სურათი №67);

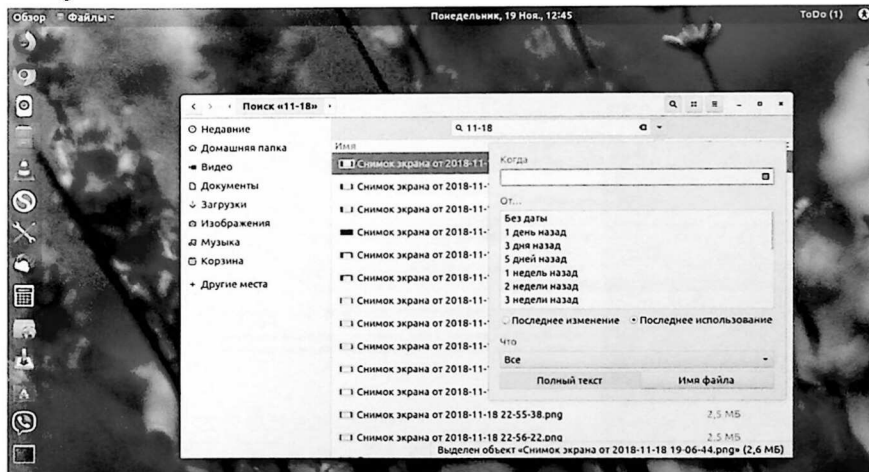
³⁵⁶ სტატია ლინუქსის ფაილების ძებნა. ელ. გვერდი:  ნანახია 19.07.2019.

³⁵⁷ იქვე.

³⁵⁸ იქვე.



დამატებითი პარამეტრების ღილაკის გახსნის შემდეგ, შესაძლოა ავირჩიოთ პერიოდი, როდესაც იყო შექმნილი ჩვენთვის საინტერესო დოკუმენტი ან დოკუმენტის ტიპი.³⁶⁰ (სურათი N68 და 69);

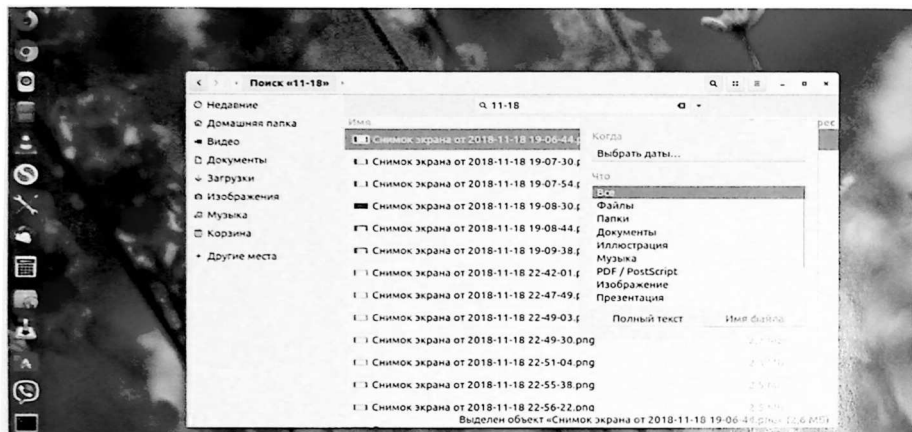


359 სტატია ლინუქსის ფაილების ძებნა. ელ. გვერდი;



360 ოქვე.

361 ოქვე.

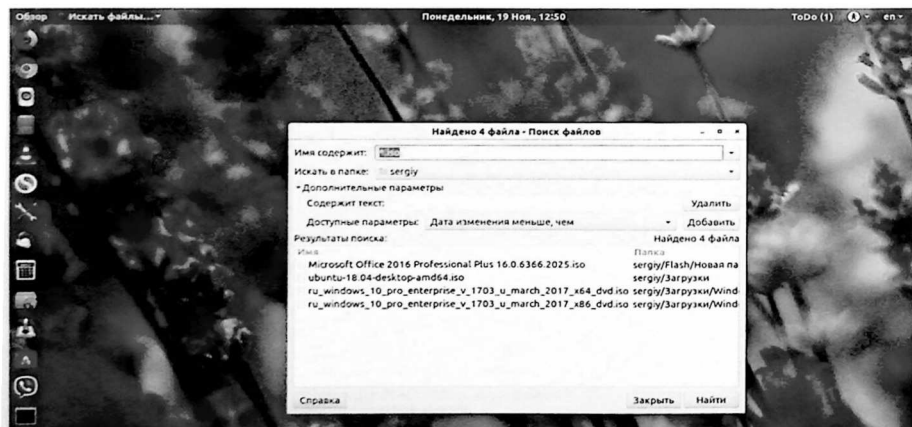


ძიების საშუალებიდან შეგვიძლია გამოვიყენოთ სიმბოლოები *.

დოკუმენტის ძებნა GNOME SEARCH - ით;

„Gnome Search ისეთივე შესაძლებლობებს გვთავაზობს, როგორც ფაილების მენეჯერი, ამასთან, დამატებით შეიძლება აღნიშნულით მოვიძიოთ დოკუმენტი შინაარსის მიხედვით [...]“³⁶³ (იხ. სურათი N70);

სურათი N70: ³⁶⁴



³⁶² სტაცია ლინუქსის ფაილების ძებნა. ელ. გვერდი;  ნანახია 19.07.2019

³⁶³ იქვე.

³⁶⁴ იქვე.

ნაბიჯი N6 ინფორმაციის კოპირება;

რაც გამოძიებულმა უნდა განახორციელოს, არის ინფორმაციის კოპირება ან ამოჭრა აღნიშნული კომპიუტერიდან, ამისათვის გამოძიებულს აქვს რამდენიმე ვარიანტი; 1. საერთოდ სრული დოკუმენტაციის კოპირება, ან კონკრეტული ინფორმაციის მატარებელი დოკუმენტის გახსნა და შიგნით არსებული ინფორმაციის კოპირება ახალ ფაილში, აღნიშნული მიზნებისათვის გამოძიებულმა უნდა შექმნას ახალი ე.წ. ფოლდერი იმავე კომპიუტერში, სადაც თავს მოიყრის ყველა გამოსათხოვი ინფორმაციის ასლები, რის შემდეგაც განხორციელდება მე-4 ნაბიჯი - ინფორმაციის გადატანა შესაბამის შესანახ საშუალებაზე (დისკი, ფლეშ მეხსიერება ან გარე ვინჩესტერი) და მე-5 ნაბიჯი აღნიშნული დისკის დალუქვა.

განვიხილოთ მე-3 ნაბიჯის მთავარი კომპონენტი - ინფორმაციის კოპირება; ფაილებისა და საქალაქების კოპირება ან გადატანა რამდენიმე ხერხით შეიძლება. განვიხილოთ რამდენიმე მათგანი:

„I ხერხი;

გახსნილი საქალაქიდან, მონიშნეთ საჭირო ფაილები ან საქალაქები;

კოპირებისთვის, დააწკაპუნეთ ლილაკი  (Copy) ინსტრუმენტების პანელიდან;

გახსენით საქალაქი, რომელშიც ფაილები უნდა დააკოპირდეს;

საქალაქში, სადაც უნდა ჩაიწეროს მითითებული ფაილები, დააწკაპუნეთ ლილაკი  (Paste) ინსტრუმენტების პანელიდან;

გადატანა კოპირების ანალოგიურად ხდება, მხოლოდ გადატანისას გამოიყენება ლილაკი  (Cut), ნაცვლად  (Copy) ლილაკისა.

შენიშვნა: გადატანისას მონიშნული ობიექტები ამოიჭრება და მითითებულ ადგილზე გადაიწერება, ხოლო კოპირებისას მონიშნული ობიექტები ადგილზეც დარჩება და მითითებულ ადგილზეც გადაიწერება.“³⁶⁵

II ხერხი:

„მონიშნეთ ფაილები ან საქალაქები;

კოპირებისთვის დააწკაპუნეთ ლილაკი  (Copy); ხოლო გადატანისთვის - ლილაკი  (Move);

ღიალოგურ ფანჯარაში ამოირჩიეთ საქალაქი, რომელშიც ათავსებთ ფაილებს და დააწკაპუნეთ OK. „

III ხერხი:

„მონიშნეთ ფაილები ან საქალაქები;

ეკრანზე გამოაჩინეთ საქალაქი, რომელშიც ფაილები გადაგაქვთ;

მონიშნულ ფაილებს მოკიდეთ "თაგვის" ისარი და გადითანეთ სასურველ საქალაქში.

³⁶⁵ ციური ნოზაძე, გოგა საზანდრიშვილი; ლექციების კურსი: კომპიუტერის საფუძვლები. გვ. 9 ელ.

 გვერდი: ნანახია 02.07.2019

თუ გინდათ შეასრულოთ არა გადატანა, არამედ კოპირება, (ე.ი. მონიშნული ფაილები არსებულ საქალაქო დარჩეს და სასურველ საქალაქო დარჩეს) მაშინ "თავით" გადატანისას აუცილებლად უნდა გეჭიროთ Ctrl კლავიში. კოპირებისას "თავის" ისარს + ნიშანი გაუჩნდება, ხოლო გადატანისას არა.³⁶⁶

რაც შეეხება არა სრულად ფაილის კოპირებას, არამედ კონკრეტული ტექსტის კოპირებას, აღნიშნულის ტექნიკური პროცედურები მოიცავს შემდეგს:

..სიტყვაზე "თავის" ორმაგი დაწკაპუნება მონიშნავს ამ სიტყვას;

სტრიქონის მარცხნივ "თავის" (ამ დროს თავის ისარი სტრიქონისკენაა გადახრილი) დაწკაპუნება მონიშნავს ამ სტრიქონს:

აბზაცის მარცხნივ "თავის" (ამ დროს თავის ისარი აბზაცისკენაა გადახრილი) ორმაგი დაწკაპუნება მონიშნავს ამ აბზაცს;

წინადადების ნებისმიერ პოზიციამ "თავის" დაწკაპუნება, დაფიქსირებულ Ctrl კლავიშთან ერთად მონიშნავს მიმდინარე წინადადებას;

ტექსტიდან მარცხნივ "თავის" დაწკაპუნება (ამ დროს თავის ისარი ტექსტისკენაა გადახრილი), დაფიქსირებულ Ctrl კლავიშთან ერთად მონიშნავს მთლიან ტექსტს.³⁶⁷

რაც შეეხება ტექსტის ნაწილის გადატანას და კოპირებას — ტექნიკური პროცედურები შემდეგია, ტექსტის ნაწილის ერთი ადგილიდან მეორეზე გადასატანად საჭიროა:

..ტექსტის ფრაგმენტის მონიშვნა;

შესწორება/ამოჭრა (Edit/Cut) ბრძანების შესრულება ან Word ინსტრუმენტთა პანელზე - ამოჭრა (Cut) ლილაზე დაწკაპუნება;

მიმთითებლის მოთავსება იქ სადაც გადასატანი ტექსტი უნდა ჩაისვას;

შესწორება/ჩასმა (Edit/Paste) ბრძანების შესრულება, ან ჩასმა (Paste) ლილაზე დაწკაპუნება.³⁶⁸

რაც შეეხება ტექსტის ნაწილის ერთი ადგილიდან მეორეზე დასაკოპირებლად საჭიროა შემდეგი ტექნიკური პროცედურები:

..ტექსტის ფრაგმენტის მონიშვნა;

შესწორება/კოპირება (Edit/Copy) ბრძანების შესრულება ან Word ის ინსტრუმენტთა პანელზე - კოპირება (Copy) ლილაზე დაწკაპუნება;

მიმთითებლის მოთავსება იქ სადაც გადასატანი ტექსტი უნდა ჩაისვას;

შესწორება/ჩასმა (Edit/Paste) ბრძანების შესრულება, ან ჩასმა (Paste) ლილაზე დაწკაპუნება.³⁶⁹

ნახიზ N7 ინფორმაციის გადატანა შესანახ საშუალებაზე;

მას შემდგომ, რაც გამოძიებლის მიერ დაკოპირებულ იქნება გამოსათხოვი ინფორმაცია და თავმოყრილი იქნება იმავე კომპიუტერში არსებულ ელექტრონულ ცალკე ფოლდერში, კომპიუტერიდან უნდა მოხდეს მისი გადატანა შესანახის ელექტრონულ დისკზე, ფლშ მეხსიერებაზე ან ე.წ. გარე ვინჩესტერზე.

³⁶⁶ ციური ნოზაძე, გოგა საზანდრიშვილი; ლექციების კურსი; კომპიუტერის საფუძვლები. გვ. 9 ელ. გვერდი; ნანახია 02.07.2019.



³⁶⁷ იქვე.

³⁶⁸ ციური ნოზაძე, გოგა საზანდრიშვილი; ლექციების კურსი; კომპიუტერის საფუძვლები. გვ. 9 ელ. გვერდი; ნანახია 02.07.2019



³⁶⁹ იქვე.

გადასატანად უნდა განხორციელდეს შემდეგი ქმედებები;

„ისარგებლეთ ბრძანებით StartMy Computer, გახსენით ფოლდერი, საიდანაც უნდა გადაწეროთ ფაილები დისკზე, მონიშნეთ ფაილი და მარცხნივ ამოცანების სიაში იმოქმედეთ ბრძანებაზე Copy this folder- შექმენი ასლი. ასლების კოპირების ფანჯარაში Copy Items აირჩიეთ დისკური მოწყობილობა და იმოქმედეთ ლილაკზე Copy. დაელოდეთ, სანამ შეიქმნება ასლი, შემდეგ გახსენით დისკი - მასზე უნდა ჩანდეს ასლის დასახელება - პიქტოგრამა ისრით. ამოცანების ნაწილში, ფანჯარაში CD Writing Tasks, მარჯვნივ, აირჩიეთ ბრძანება Write these files to CD. შესარულეთ ეკრანზე გამოსული ოსტატის CD Writing Wizard მითითებები, რათა დაასრულოთ გადაწერის პროცესი და ჩაწეროთ დისკზე ფაილები.“³⁷⁰

რაზე უნდა მოხდეს ინფორმაციის გადატანა;

1. „ფლეშ-დისკი არის მოდიფიცირებული ჰარდ დისკი და გამოიყენება ინფორმაციის დიდი ხნით შენახვისათვის, მრავალჯერადი გადაწერის შესაძლებლობით. არსებითად ფლეშ-დისკი არის "ნახევრადმუდმივი" დამახსოვრების მოწყობილობა, წაშლა, ამოკითხვა და ინფორმაციის ჩაწერა ხორციელდება ელექტრონული სივრცეებით.“³⁷¹
„ფლეშ-დისკის კონსტრუქციული ვარიანტები არსებობს მრავალი: ATA Flash (PC Card ATA); Compact Flash (CF); Smart Media (SM); xD-Picture; MultiMedia Card (MMC); Secure Digital Card (SD); Miniature Card (MiniCard); Memory Stick.“³⁷²
2. გარე ვინჩესტერი;
არსებობს პერსონალური კომპიუტერები, რომელთაც არ გააჩნიათ ელექტრონული დისკის ჩასადები, რა უნდა მოიმოქმედოს გამომძიებელმა ამ დროს - ? ამისათვის არსებობს სპეციალური ე.წ. "გარე ვინჩესტერი" რომელიც არის დიდი ტევადობის ფლეშ მეხსიარება, რომელიც აუცილებლად უნდა იყოს საგამოძიებო ორგანოში - საჭიროების შემთხვევაში გამოყენებს მიზნით, გამომძიებელმა, უნდა განახორციელოს თან ნაქონი აღნიშნული მოწყობილობის მიერთება პერსონალურ კომპიუტერზე, აღნიშნულ მოწყობილობებს აქვს ფლეშ მეხსიერების შესაერთებელში მისაერთებელი კაბელი, მიერთეთ თე აღნიშნული კომპიუტერს და ოპერაციული სისტემა აღმოაჩენს ახალ მოწყობილობას და დააყენებს დამოუკიდებლად. რის შემდეგაც შეგიძლიათ ნახოთ ახალი მოწყობილობა.
3. ელექტრონული დისკები;
CD (კომპაქტ დისკი) — დისკოს ფორმის ინფორმაციის ოპტიკური მატარებელი ცენტრში ხვრელით, რომლიდანაც ინფორმაცია ლაზერის დახმარებით იკითხება. თავდაპირველად, კომპაქტ დისკი შეიქმნა აუდიოს ციფრული შენახვისთვის (ე. წ. Audio-CD), მაგრამ დღესდღეობით იგი ფართოდ გამოიყენება, როგორც ფართო დანიშნულების მქონე მონაცემების მატარებელი მოწყობილობა (ე. წ. CD-ROM). აუდიო კომპაქტ დისკები, როგორც წესი, მონაცემების მატარებელი კომპაქტ დისკებისგან განსხვავდება და ამიტომაც, CD-ფლეიერებს მხოლოდ მათი დაკრა შეუძლიათ (რა თქმა უნდა, კომპიუტერზე ორივე ტიპის დისკის წაკითხვა შესაძლებელი). არსებობს ისეთი დისკებიც, რომლებზეც ერთდროულად აუდიოინფორმაცია და მონაცემებია ჩაწერილი — მათი მოსმენა შესაძლებელია CD-ფლეიერზე, ხოლო წაკითხვა კომპიუტერზე.³⁷³

DVD (ინგლ. Digital Versatile Disc ან Digital Video Disc — ციფრული ვიდეო დისკი) — ოპტიკური დისკი,

³⁷⁰ იქვე.

³⁷¹ ომარ გაბედავა. კომპიუტერის არქიტექტურა. (სახელმძღვანელო). თბილისი 2008 წელი

³⁷² ომარ გაბედავა. კომპიუტერის არქიტექტურა. (სახელმძღვანელო). თბილისი 2008 წელი

³⁷³ ელ.გვერდი



ნანახია 03.07.2019

განკუთვნილი მედიის ფორმების მონაცემთა შესანახად, რომელიც მოიცავს ვიდეოფილმებსაც, მაღალი ვიდეო და ხმის ხარისხით. გარეგნულად DVD ესმეგავსება კომპაქტ დისკებს, ვინაიდან მათი ფიზიკური განზომილებები ერთნაირია (120 მმ ან ზოგიერთ მოდელში 80 მმ დიამეტრით), თუმცა ისინი სხვადასხვა ფორმატში კოდირდება და, ამასთან, DVD-ს გაცილებით მაღალი ტევადობა აქვს.³⁷⁴

ნაბიჯი №8 – დალუქვა;

მას შემდეგ, რაც გამომძიებლის მიერ დასრულდება საგამოძიებო მოქმედება ინფორმაციის გამოთხოვა, შეივსება შესაბამისი ინფორმაციის გამოთხოვის ოქმი, რომელიც მითითებულია ნიმუშის სახით, ხოლო შემდგომ აუცილებლად უნდა განხორციელდეს გამოთხოვილი ინფორმაციის შემცვერი ელექტრონული შესანახი საშუალების კანონით დადგენილი წესით დალუქვა, კერძოდ, დისკი უნდა დაილუქოს და, შესაძლებლობის შემთხვევაში, შეიფუტოს. შეფუთულ ნივთზე, ლუქის გარდა, აღინიშნება თარიღი და იმ პირთა ხელმოწერები, რომლებიც საგამოძიებო მოქმედებაში მონაწილეობდნენ.

6.5. დეტალიზაციის მეთოდური პრობლემა ინფორმაციის გამოთხოვის დროს

გამომძიებლის ვალდებულებას წარმოადგენს გარკვევა იმისა, თუ რა ინფორმაცია უნდა იქნეს გამოთხოვილი:

ვინაიდან, [...] „კომპიუტერში არსებული მონაცემები შეიცავს პირად და ცალკეულ შემთხვევაში პროფესიულ საქმიანობასთან დაკავშირებულ ე.წ. პრივილეგიურ ინფორმაციას. შესაბამისად, განსაკუთრებული მნიშვნელობა ენიჭება იმ კრიტერიუმების განსაზღვრას, რომელთა მეშვეობითაც უნდა გაიმიჯნოს ამოღებას დაქვემდებარებული ინფორმაცია იმ ინფორმაციისაგან, რომლის ამოღებაც არ დაიშვება.“³⁷⁵

„ამოსაღები ფაილების იდენტიფიცირება უნდა განხორციელდეს ფაილების გარეგანი მახასიათებლების, მაგალითად: მოცულობის, გაფართოების, სახელწოდების და ა.შ., მიხედვით, თუ მათი შინაარსის დათვალიერებით? თუ ამოსაღები ინფორმაციის განსაზღვრისათვის ჩხრეკის მწარმოებელ პირს ენიჭება ელექტრონულ მატარებლებზე არსებული ინფორმაციის არა მხოლოდ გარეგანი დათვალიერების, არამედ გახსნის უფლებაც, ამან შეიძლება გამოიწვიოს პირადი ცხოვრების ხელშეშელობით დაცული ინფორმაციის გამჟღავნება. საკითხი დამატებით სიმწვავეს იძენს. მაგალითად, ადვოკატის კომპიუტერის შემთხვევაში, რომლის დროსაც შეიძლება აღმოჩენილ და გამჟღავნებულ იქნეს პრივილეგირებული ინფორმაცია.“³⁷⁶

„მეორე მხრივ, დამატებითი სირთულეა მტკიცებულების მოცულობა და დამალვის სიმარტივე. ციფრული მტკიცებულება უნიკალურია მისი კამუფლაჟისა და განთავსების შესაძლებლობის მრავალფეროვნებით. პირს შეუძლია, მამხილებელი ელექტრონული მტკიცებულება დამალოს ღია სივრცეში მისი დაზიანების გარეშე, რაც შეუძლებელია სხვა სახის მტკიცებულებებთან მიმართებით; ასევე შეუძლია, გამოიყენოს დამშვიფრავი პროგრამები და ა.შ., რაც მტკიცებულების აღმოჩენის

³⁷⁴ იქვე.

³⁷⁵ ლალი ფაფიაშვილი. სტატია: ციფრული მტკიცებულების ამოღება: პირადი ცხოვრების ხელშეშელობის საკმარისი თუ ილუზორული გარანტია? სტატიათა კრებული, ადამიანის უფლებათა დაცვა და სამართლებრივი რეფორმა საქართველოში. თბილისი. 2014. გვ. 160

³⁷⁶ იქვე. გვ. 161

პროცესს განსაკუთრებით ართულებს. ამიტომ ცალკეულ შემთხვევებში გამოძიებლების ყურადღების მიღმა რჩება ზოგიერთი მასალის მნიშვნელობა, ან/და ხდება იმ ინფორმაციის ამოღება, რომელიც არ არის გათვალისწინებული სასამართლოს ნებართვით.”³⁷⁷

„როდესაც კომპიუტერული ფაილები საკმარისი დეტალიზაციით არის დასათაურებული და არსებობს საკმარისი ვარაუდი, რომ განჩინებაში მითითებული ინფორმაცია აღმოჩენილ იქნება ამ ფაილებში, ამოღება უნდა შემოიფარგლოს სწორედ ამ ფაილებით. ამასთანავე, მხედველობაში უნდა იქნეს მიღებული საქმის გარემოებათა ერთობლიობა, მათ შორის ბრალდებულის პიროვნული მახასიათებლები, ჩადენილი დანაშაულის სპეციფიკა, აღნიშნული მოწყობილობისადმი სხვა პირთა წვდომის შესაძლებლობა და ა.შ. როდესაც ფაილები საკმარისი სიზუსტით არ არის დასათაურებული, გამოძიებელს ენიჭება უფლება, გასსნას ეს ფაილები საძიებო ობიექტის აღმოჩენის მიზნით.”³⁷⁸

„ამდენად, კომპიუტერული ფაილების დათვალიერების მოცულობა დამოკიდებულია მათი შიგთავსის განსაზღვრის შესაძლებლობაზე გარეგანი მახასიათებლებიდან, სახელწოდებებიდან გამომდინარე კონკრეტული საქმის გარემოებათა ერთობლიობის ტესტის საფუძველზე. თუ სახელწოდებიდან გამომდინარე, გონივრულად შეუძლებელია იმის განსაზღვრა, რა სახის მასალა ინახება ფაილში, დაიშვება მათი დათვალიერება და იმ ფაილების ამოღება, რომლებიც სხვა დანაშაულის ჩადენის მამხილებელი მტკიცებულების შემცველი აღმოჩნდება. ამ კრიტერიუმით მონაცემების გამოჩენა შეიძლება ზედმეტად ზღუდავდეს გამოძიების ორგანოებს. გამოძიებელი არ უნდა იყოს შებოჭილი ფაილების გაფართოების/ფორმატის ფაილის შიგთავსთანადეკვატურობის პრეზუმფციით. მან უნდა განახორციელოს კომპიუტერის სისტემური ჩხრეკა ფაილების სახელწოდებისა და დაბოლოების მიუხედავად, ვინაიდან კომპიუტერული ფაილები შეიძლება წინასწარი განზრახვით არასწორად იყოს დასათაურებული, ან არასწორი ფორმატით იქნეს შენახული, მით უმეტეს, რომ ციფრული მტკიცებულება შეიძლება ინახებოდეს ნებისმიერ ადგილას ბრალდებულის კომპიუტერულ ფაილებში.”³⁷⁹

ამდენად აუცილებელია, რომ გამოშვებულმა მოახდინოს დეტალიზაცია და გამოითხოვოს სწორედ ის ინფორმაცია, რომელიც გამოძიებისათვის არის მნიშვნელოვანი, ზედმეტი ინფორმაციის გამოთხოვამ შესაძლოა შექმნას გარკვეული სამართლებრივი პრობლემები.

6.6. სოციალური ქსელის – facebook – ის დათვალიერების და ინფორმაციის გამოთხოვის ტექნიკური პროცედურები და მეთოდები

სოციალური ქსელს <https://www.facebook.com> დღეის მდგომარეობით საქართველოში იყენებს ძალიან ბევრი მოქალაქე, ასევე აღნიშნული სოციალური ქსელის გამოყენებით ხშირად ხდება პირადი ცხოვრების ამსახველი გარკვეული ინფორმაციის გასაჯაროება, ან სხვადასხვა დანაშაულის ორგანიზება და ა.შ.

შესაბამისად მნიშვნელოვნად იქნა მიჩნეული ცალკე თავად მომხდარიყო აღნიშნული ქსელიდან ინფორმაციის გამოთხოვის პროცედურული საკითხები.

იმისათვის, რომ გამოძიებლის მიერ მოხდეს ინფორმაციის გამოთხოვა, მან უნდა განახორციელოს რამდენიმე ქმედება;

³⁷⁷ ლალა ფაფიაშვილი. სტატია: ციფრული მტკიცებულების ამოღება: პირადი ცხოვრების ხელშეუხებლობის საკმარისი თუ ილუზორული გარანტია? სტატიათა კრებული, ადამიანის უფლებათა დაცვა და სამართლებრივი რეფორმა საქართველოში. თბილისი. 2014. გვ. 161

³⁷⁸ იქვე.

³⁷⁹ იქვე.

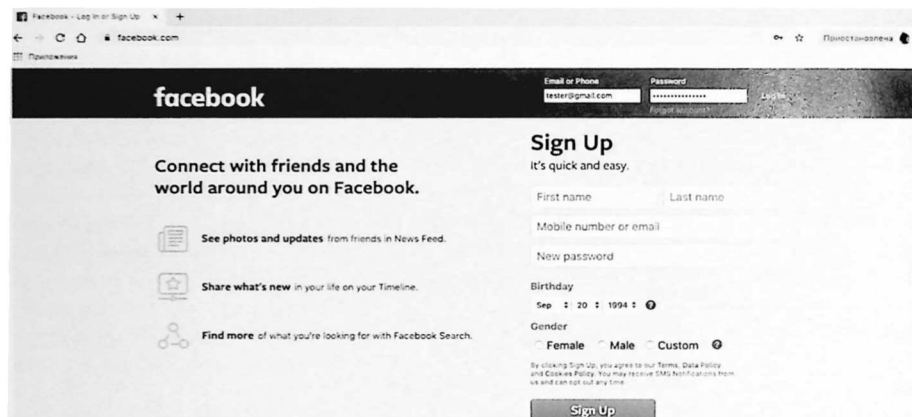
პირველი ნაბიჯი;

გამომცემლის მიერ უნდა იქნეს გაგებული მომხმარებლის პაროლი და შესაბამისი მომხმარებლის სახელი — რაც უნდა აისახოს საგამოცემო მოქმედების ოქმში;

მეორე ნაბიჯი;

მომხმარებლის სახელის და პაროლის გამოყენებით უნდა შევიდეთ სოციალურ ქსელში; (იხილეთ სურათზე N71);

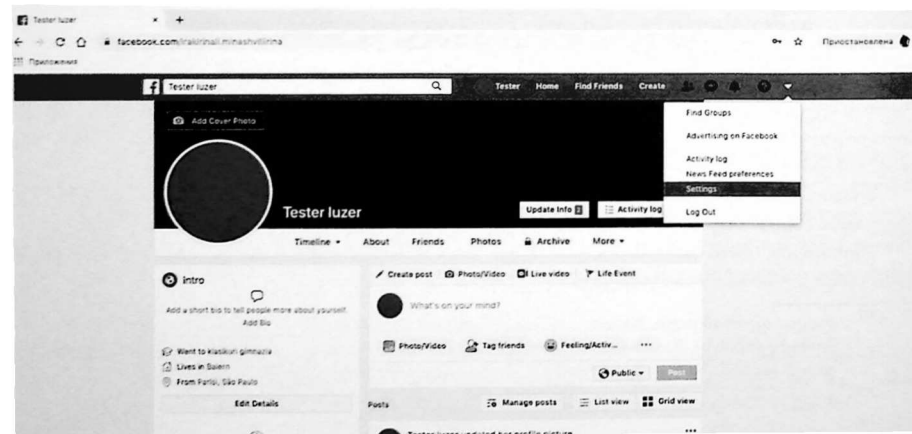
სურათი N71:



მესამე ნაბიჯი;

მას შემდეგ რაც შევალთ სოციალურ ქსელში, თქვენს წინაშე გაიხსნება შესაბამისი გვერდი, სადაც მათს ღირსებას მივითმით ნიშნულთან Settings და შევალთ აღნიშნულ მონაცემში; (იხ. სურათი N72)

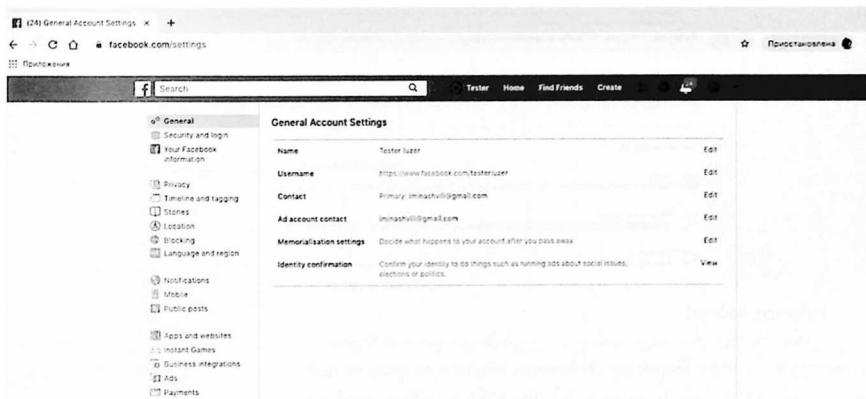
სურათი N72;



მეთხე ნაბიჯი;

მონაცემში შესვლის შემდეგ გაიხსნება ფანჯარა, სადაც General მონაცემში ასახულია ინფორმაცია სოციალური ქსელის მომხმარებლის შესახებ, გამოძიებლის მიერ უნდა მოხდეს აღნიშნული მომხმარებლის შესახებ ინფორმაციის გადატანა საგამოძიებო მოქმედების ოქმში (იხ. სურათი N73)

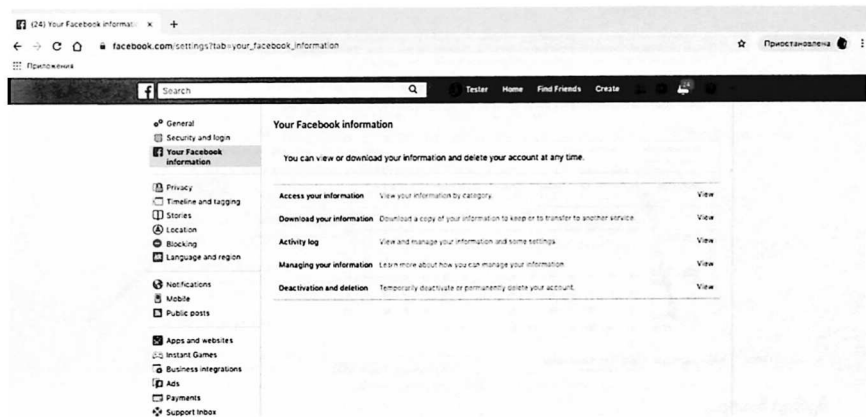
სურათი N73;



მეხუთე ნაბიჯი;

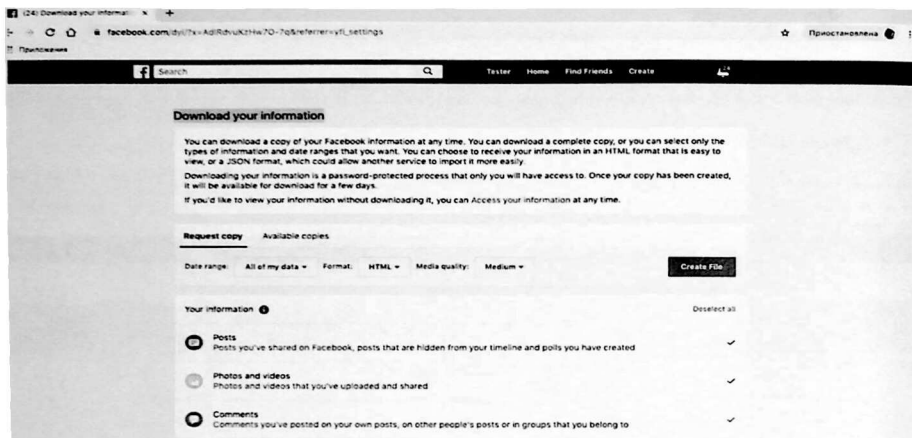
აღნიშნულის შემდგომ, მუხის ღილაკს მივიტანთ ნიშნულთან Your Facebook information - და შევალთ აღნიშნულ მონაცემში, რის შემდეგაც გაიხსნება მონაცემის შესაბამისი ფანჯარა (იხ. სურათი N74)

სურათი N74;



მეექვსე ნაბიჯი;

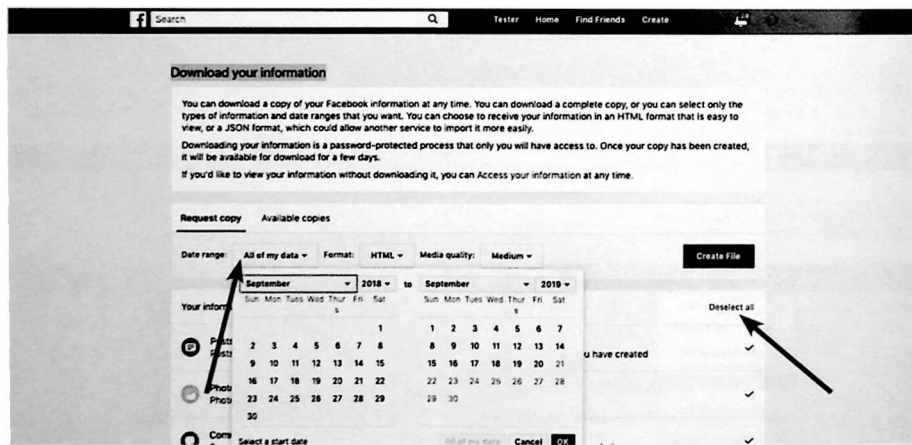
მუხის ღილაკს მივიტანთ ნიშნულთან Download your information - და შევალთ აღნიშნულ მონაცემში, რის შემდეგაც გაიხსნება მონაცემის შესაბამისი ფანჯარა (იხ. სურათი N75) სურათი N75;



მეშვიდე ნაბიჯი;

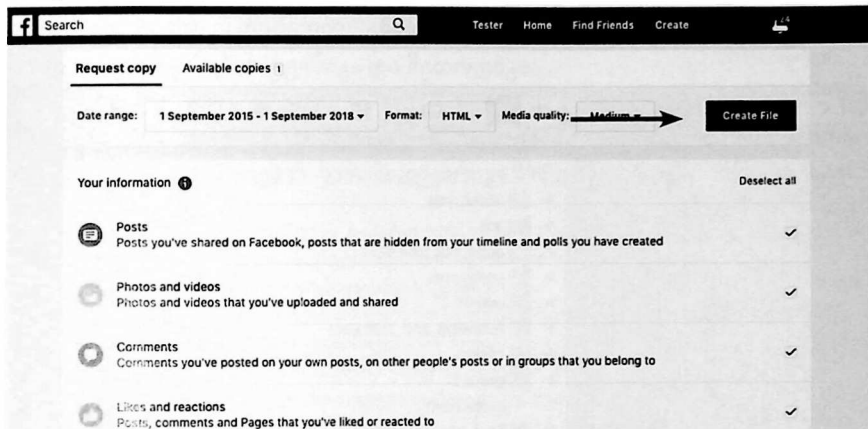
ფანჯარა შესაძლებლობას გვაძლევს მოვახდინოთ ჩვენთვის სასურველ თარიღში, ჩვენთვის სასურველი ინფორმაციის გამოთხოვა, ამისათვის ვხსნით ჩამოსასვლელ ფანჯარას all of my data, ასევე სურვილის შემთხვევაში ვირჩევთ გადმოსაწერი დოკუმენტის ფორმატს და ზომას. ვნიშნავთ შესაბამისი მონიშვნის ლილაკით იმ ინფორმაციას რაც გვსურს (იხ. სურათი N76);

სურათი N76:



მერვე ნაბიჯი;

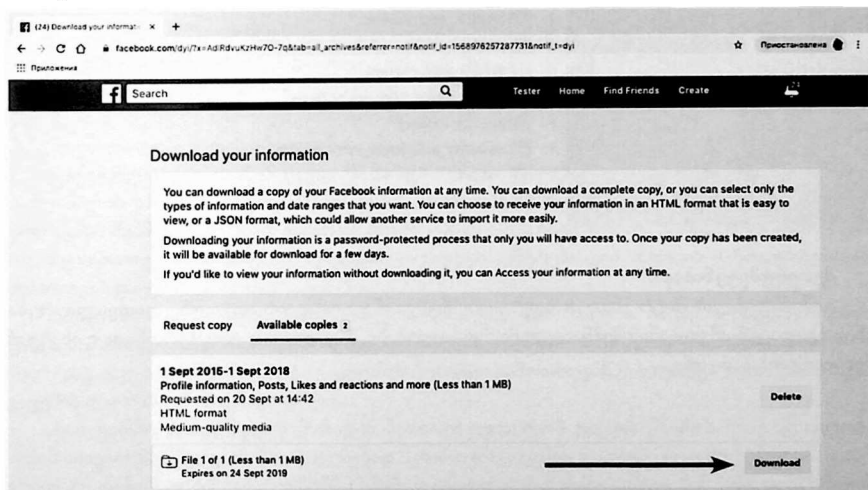
მას შემდეგ რაც არჩეული იქნება შესაბამისი თარიღი, ინფორმაცია რაც გვინდა გადმოვწეროთ ფორმატი და ზომა, ინფორმაციის გადმოსაწერად მუდის გამოყენებით უნდა დავაწვეთ ლილაკს Create File; (იხ. სურათი N77);



მეცხრე ნაბიჯი:

რის შედეგადაც ინფორმაცია გაერთიანდება ერთ პაკეტში რომელიც გამოძიებლის მიერ უნდა იქნეს გადმოწერილი Download ლილკის საშუალებით; (იხ. სურათი N78);

სურათი N78:

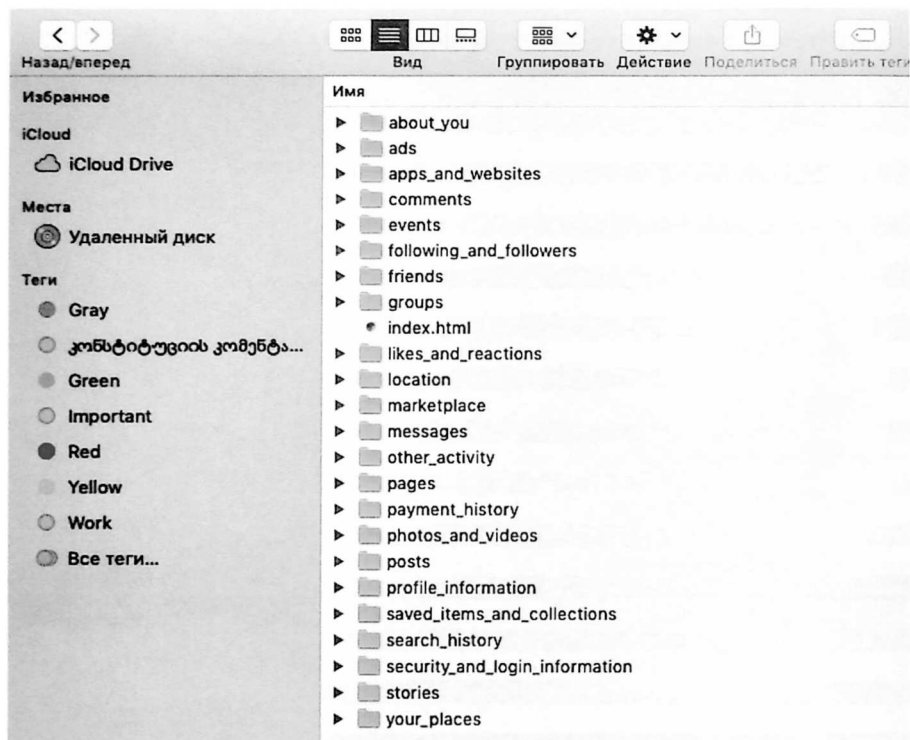


მეათე ნაბიჯი:

მას შემდეგ რაც ინფორმაცია გადმოიწერება, გამოძიებელი მას შეინახავს შესაბამის მისთვის საჭირო ადგილზე კომპიუტერში, მაგალითისათვის ეკრანზე, ინფორმაცია მოთავსებული იქნება ერთ დოკუმენტში, აღნიშნული დოკუმენტის კომპიუტერის ეკრანზე გახსნის შემდეგ კი გამოიწერება

ყველა ის ინფორმაცია, შესაბამის პაკეტებში, რომელსაც შეიცავს ჩვენს მიერ მითითებულ თარიღებში სოციალური ქსელის კონკრეტული მომხმარებლის მონაცემები:(იხ. სურათი N79):

სურათი N79:



მეთერმეტე ნაბიჯი;

გამომძიებლის მიერ უნდა მოხდეს აღნიშნული ინფორმაციის ადგილზე დათვალიერება, ან/და გადატანა შესაბამის შემნახველ მოწყობილობაზე, მაგალითად ელექტრონულ დისკზე ან მეხსიერების ბარათზე.

თავი VII

კომპიუტერულ მოწყობილობაში დაცული ციფრული ინფორმაციის დათვალიერების ტექნიკა და მეთოდика

7.1. კომპიუტერულ მოწყობილობაში დაცული ციფრული ინფორმაციის დათვალიერების სამართლებრივი საფუძვლები და პროცედურები

იმ შემთხვევაში, თუ სისხლის სამართლის საქმის სიმძიმე ან ფარული საგამოძიებო მოქმედებისათვის დამახასიათებელი სტანდარტი გამოძიებას სახეზე არ აქვს — რა უნდა მოიმოქმედოს გამოძიებამ ინფორმაციის მოპოვებისათვის.

მაგალითად: ჩადენილია საქართველოს სისხლის სამართლის კოდექსის 177-ე მუხლის 1-ლი ნაწილით გათვალისწინებული დანაშაული — ძალადიდან სურსათის ქურდობა, აღნიშნული დანაშაულის ჩადენის ფაქტი ასახულია ვიდეოჩანაწერზე, რომელიც ინახება კომპიუტერულ სისტემაში, ხოლო კომპიუტერის ამოღება ფიზიკურად შეუძლებელია, ვინაიდან გამოიწვევს დიდ პრობლემებს, კერძოდ საერთოდ გაითიშება ძალადიდან ჩამწერი მოწყობილობა, რა უნდა მოიმოქმედოს გამოძიებამ ამ შემთხვევაში?

აღნიშნულ შეკითხვაზე პასუხს ვპოულობთ თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის გადაწყვეტილებაში, საქმის № 1გ/456-19.

საქმის მასალების მიხედვით, 2019 წლის 28 თებერვალს ვ.ა.-ს წარედგინა ბრალდება საქართველოს სსკ-ის მე-11 პრიმა, 151-ე მუხლის პირველი ნაწილით — ოჯახის ერთი წევრის მიერ, ოჯახის სხვა წევრის მიმართ ჯანმრთელობის დაზიანების, სიცოცხლის მოსპობისა და ქონების განადგურების შექრა, როდესაც იმას, ვისაც ემუქრებიან გაუჩნდა მექარის განხორციელების საფუძვლიანი შიში — (ორი ეპიზოდი) და საქართველოს სსკ-ის მე-11 პრიმა, 381-ე პრიმა მუხლის პირველი ნაწილით — ოჯახის წევრების მიმართ გამოცემული შემაკავებელი ორდერით გათვალისწინებული მოთხოვნებისა და ვალდებულებების შეუსრულებლობა — (ორი ეპიზოდი) (იხ.: დადგენილება პირის ბრალდების შესახებ).

მოცემულ საქმეზე, 2019 წლის 18 მარტს თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა საგამოძიებო, წინასასამართლო სხდომისა და არსებითი განხილვის კოლეგიას შუამდგომლობით მიმართა ბრალდებულ ვ.ა.-ს ინტერესების დამცველმა ადვოკატმა ი.გ.-მ და ითხოვა საგამოძიებო მოქმედების — ვიდეოჩანაწერების გამოთხოვის — ჩასატარებლად ნებართვის გაცემა.

თბილისის საქალაქო სასამართლოს სისხლის სამართლის საქმეთა საგამოძიებო, წინასასამართლო სხდომისა და არსებითი განხილვის კოლეგიის 2019 წლის 19 მარტის განჩინებით ადვოკატ ი.გ.-ს შუამდგომლობა ვიდეოჩანაწერების გამოთხოვის ჩასატარებლად ნებართვის გაცემის თაობაზე არ დაკმაყოფილდა.

„საჩივარში მოსარჩელის მხრიდან მითითებულია, რომ დაცვის მხარის შუამდგომლობა საგამოძიებო მოქმედების ჩასატარებლად ნებართვის გაცემის თაობაზე დასაბუთებულია. ვ.ა.-ს ბრალად დდება, რომ მის მიმართ, 02.02.19-ში შემაკავებელი ორდერების გამოცემის შემდეგ, 2019 წლის 21 თებერვალს, დაახლოებით 13.30 საათზე, ვ.ა.-ს ქუჩა NX-ში მდებარე შენობაში, იგი მიუახლოვდა იქ მყოფ დედასა და დას, მ.ა.-სა და ს.ბ.-ს, დაემუქრა მათ და მიაყენა სიტყვიერი შეურაცხყოფა. ვ.ა. კატეგორიულად უარყოფს ბრალად შერაცხულ დროს შემთხვევის ადგილზე ყოფნას და ამდენად ბრალად შერაცხული ქმედებების განხორციელებას, რასაც ადასტურებს ასევე მოწმე ე.ბ.-ც. ბრალდებულის განმარტებით მასსა და დაზარალებულებს შორის მიმდინარეობს სამემკვიდრო დავა და დაზარალებულები დაინტერესებულები არიან ჩამოიშორონ კონკურენტი, რისთვისაც

ყველა ხერხს მიმართავენ. უწყობენ სხვადასხვა პროვოკაციებს და იძლევიან მის წინააღმდეგ ცრუ ჩვენებებს. იმის დადგენა, რომ ვ.ა. 21 თებერვალს 13.30 საათზე იმყოფებოდა თუ არა კ.ა.-ს ქუჩა NX-ში შესაძლებელია იმავე შენობაში განთავსებული ს.-ს ბანკის გარე ფასადზე არსებული სათვალთვალ ვიდეოკამერების ჩანაწერების მოპოვებით, რითაც დადგინდება საქმეზე ჭეშმარიტება და ამდენად სტრატეგიულად საჭიროა დაცვის მხარისათვის. დაცვის მხარეს გააჩნია დასაბუთებული ვარაუდი, რომ ვ.ა.-ს ბრაღად შერაცხული ქმედებები არ ჩაუდენია, რისი დადასტურებაც შესაძლებელია კ.ა.-ს ქუჩა NX-ში განთავსებული ს.-ს ბანკის გარე ფასადზე არსებული სათვალთვალ ვიდეოკამერების ჩანაწერების მოპოვებით და დათვალიერებით. ამდენად, გემოაღნიშნული მტკიცებულებამ შეიძლება გამოიწვიოს ვ.ა.-ს მიმართ დაწყებული სს დევნის შეწყვეტა.³⁸⁰

სააპელაციო სასამართლომ განმარტა:

„მოსამართლე გამოძიების ეტაპზე საგამოძიებო მოქმედების ჩატარების შესახებ გადაწყვეტილების მიღებისას ხელმძღვანელობს დასაბუთებული ვარაუდის სტანდარტით, რაც ნიშნავს საქართველოს სისხლის სამართლის საპროცესო კოდექსის მე-3 მუხლის მე-11 ნაწილის თანახმად. ფაქტების ან ინფორმაციის ერთობლიობას, რომელიც მოცემული სისხლის სამართლის საქმის გარემოებათა ერთობლიობით დააკმაყოფილებდა ობიექტურ პირს, რათა დაესკვნა პირის მიერ დანაშაულის შესაძლო ჩადენა, ასევე ამ კოდექსით პირდაპირ გათვალისწინებული საგამოძიებო მოქმედების ჩატარებისათვის მტკიცებულებით სტანდარტს. ანუ საგამოძიებო მოქმედების ჩატარება შესაძლებელია და თუ არსებობს სათანადო ინფორმაცია სისხლის სამართლის საქმისათვის მნიშვნელობის მქონე მტკიცებულების მოპოვებისათვის, სხვა შემთხვევაში შეამდგომლობა იქნება დაუსაბუთებელი.“³⁸¹

საგამოძიებო კოლეგია განმარტავს, რომ საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლის პირველი ნაწილის თანახმად, თუ არსებობს დასაბუთებული ვარაუდი, რომ კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში ინახება სისხლის სამართლის საქმისთვის მნიშვნელოვანი ინფორმაცია ან დოკუმენტი, მხარე უფლებამოსილია გამოძიების ადგილის მიხედვით, სასამართლოს მიმართოს შესაბამისი ინფორმაციის ან დოკუმენტის გამოთხოვის განჩინების გაცემის შეამდგომლობით, ხოლო რაც შეეხება თავად კომპიუტერულ სისტემასა და მონაცემს, საქართველოს სისხლის სამართლის საპროცესო კოდექსის მე-3 მუხლის 27-ე ნაწილის მიხედვით კომპიუტერული სისტემა არის ნებისმიერი მექანიზმი ან ერთმანეთთან დაკავშირებულ მექანიზმთა ჯგუფი, რომელიც პროგრამის მეშვეობით, ავტომატურად აშუშავებს მონაცემებს (მათ შორის, პერსონალური კომპიუტერი, ნებისმიერი მოწყობილობა მიკროპროცესორით, აგრეთვე მობილური ტელეფონი). აღნიშნული ნორმის დანაწესიდან გამომდინარე უდავოა, რომ ქალაქ თ.-ში, კ.ა.-ს ქუჩა NX-ში განთავსებული ს.-ს ბანკის გარე ფასადზე არსებული სათვალთვალ ვიდეოკამერების ჩანაწერები წარმოადგენს კომპიუტერულ სისტემაში არსებულ მონაცემებს, რომლის გამოთხოვის/მოპოვების წესი სპეციალურად გათვალისწინებულია სსკ-ის 136-ე და 143-ე მუხლებს შორის - 143-ე მუხლი პრიმა მუხლების დებულებებით, ხოლო მხარის შეამდგომლობა ინფორმაციის გამოთხოვის თაობაზე უნდა იყოს მოტივირებული. უნდა აღინიშნოს, რომ საქართველოს სსკ-ის 136-ე მუხლის მე-4 ნაწილით იმპერატიულად განსაზღვრულია, რომ

³⁸⁰ თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის გადაწყვეტილებაში, საქმის № 1გ/456-19. მოსამართლე: გიორგი გოგინაშვილი. 26 მარტი, 2019 წელი. ელ. გვერდი;  ნანახია 03.07.2019

³⁸¹ თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის გადაწყვეტილებაში, საქმის № 1გ/456-19. მოსამართლე: გიორგი გოგინაშვილი. 26 მარტი, 2019 წელი. ელ. გვერდი;  ნანახია 03.07.2019

მოცემული მუხლით გათვალისწინებულ საგამოძიებო მოქმედებაზე ვრცელდება საქართველოს სისხლის სამართლის საპროცესო კოდექსის 143-ე მეორე პრიმა - 143-ე მეთათე პრიმა მუხლების დებულებები. საქართველოს სისხლის სამართლის საპროცესო კოდექსის 143-ე მესამე პრიმა მუხლის პირველი ნაწილის თანახმად კი ფარული საგამოძიებო მოქმედება ტარდება მოსამართლის განჩინებით, განჩინებას მხარის მოივივრებული შეამდგომლობის საფუძველზე იღებს გამოძიების ადგილის მიხედვით რაიონული (საქალაქო) სასამართლოს მოსამართლე.³⁸²

სასამართლომ განმარტა, „გარდა პირველი ინსტანციის სასამართლოს განჩინების მოტივისა დასაბუთებულობის თაობაზე, მოცემულ შემთხვევაში მართალია სათვალთვლო კამერებით დაფიქსირებული ვიდეოჩანაწერი წარმოადგენს კომპიუტერულ სისტემაში დაცულ კომპიუტერულ მონაცემს, რომელშიც საქმისათვის მნიშვნელოვანი ინფორმაცია აღბეჭდილია ვიდეო-ჩანაწერის სახით, თუმცა საგამოძიებო კოლეგიას მიაჩნია, რომ აღნიშნული ვიდეოჩანაწერის გამოთხოვით არ იქნება დაცული შესაბამისი სტანდარტი. კერძოდ ის, რომ დაუშვებელია საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე და სსკ-ის 143-ე მეორე პრიმა - 143-ე მეთათე პრიმა მუხლების დებულებების გარდა სხვა საგამოძიებო თუ სხვა მოქმედებით ვიდეო ჩანაწერის ამოღება/მოპოვება. საგამოძიებო კოლეგია ყურადღებას გაამახვილებს საქართველოს სისხლის სამართლის საპროცესო კოდექსის 143-ე მესამე პრიმა მუხლის მეორე ნაწილის იმ ნორმატიულ შინაარსზე, რომლის მიხედვითაც ფარული საგამოძიებო მოქმედება ტარდება მხოლოდ იმ შემთხვევაში, თუ გამოძიება დაწყებულია ან/და სისხლისსამართლებრივი დევნა ხორციელდება მძიმე ან/და განსაკუთრებით მძიმე დანაშაულის ან საქართველოს სისხლის სამართლის კოდექსის განსაზღვრული მუხლებით გათვალისწინებული რომელიმე დანაშაულის ჩადენის გამო, ხოლო ასეთ მოცემულობაში ფარული საგამოძიებო მოქმედება სასამართლოს განჩინებით ვერ ჩატარდება, ვინაიდან გამოძიება მიმდინარეობს ნაკლებად მძიმე კატეგორიის დანაშაულზე საქართველოს სისხლის სამართლის კოდექსის მე-11-ე პრიმა, 151-ე მუხლის პირველი ნაწილით და საქართველოს სსკ-ის მე-11 პრიმა, 381-ე პრიმა მუხლის პირველი ნაწილით, რომელიც სასჯელის სახედ და ზომად ითვალისწინებს თავისუფლების აღკვეთას ერთ წლამდე ვადით, რაც ზემოაღნიშნული ნორმებიდან გამომდინარე გამორიცხავს ინფორმაციის გამოთხოვის კუთხით განჩინების გაცემის შესაძლებლობას.“³⁸³

„საგამოძიებო კოლეგიამ დამატებით განმარტა, რომ მოქმედი სისხლის სამართლის საპროცესო კანონმდებლობის შესაბამისად ვიდეო-ჩანაწერი ცალსახად წარმოადგენს კომპიუტერულ მონაცემთა შესანახ საშუალებაში დაცულ ინფორმაციას, რომელიც მხარის მიერ მოპოვებული უნდა იქნას საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე და 143-ე მეორე პრიმა - 143-ე მეთათე პრიმა მუხლების მიხედვით, თუმცა მოცემულ შემთხვევაში, ვინაიდან სს საქმეზე გამოძიება დაწყებულია ნაკლებად მძიმე დანაშაულის ჩადენის ფაქტზე, მხარეს კანონი აძლევს საშუალებას საქართველოს სისხლის სამართლის საპროცესო კოდექსის 125-ე და 126-ე მუხლების მიხედვით მოპოვებული იქნას სს საქმისათვის მნიშვნელოვანი ინფორმაცია, ანუ ჩატარებული იქნას დათვალთვლება და დათვალთვრებული იქნას ინფორმაციის შემცველი სხვა ობიექტი, ამ შემთხვევაში ვიდეოჩანაწერი. დათვალთვრების ოქმის შედგენით შეიქმნება ერთი კონკრეტული მტკიცებულება მასში მონაწილე პირების საშუალებით და დადგინდება ამ საგამოძიებო მოქმედების — დათვალთვრების ჩატარების შედეგად შემთხვევის ვითარება და გაირკვევა დანაშაულის

³⁸²

იქვე.

³⁸³

თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის გადაწყვეტილებაში, საქმის № 1გ/456-19. მოსამართლე: ვიორგი გოგინაშვილი. 26 მარტი, 2019 წელი. ელ. გვერდი:  ნანახია 03.07.2019

ფაქტს ჰქონდა თუ არა ადგილი, ან მასზე არსებული/ალბეტადილი ინფორმაცია არის თუ არა კავშირში სისხლის სამართლის საქმისათვის მნიშვნელოვან გარემოებებთან.³⁸⁴

გარდა აღნიშნული გადაწყვეტილებისა, მნიშვნელოვანია მოყვანილ იქნეს თბილისის სააპელაციო სასამართლოს პრეცედენტული გადაწყვეტილება, რომლის თანახმადაც საპელაციო სასამართლომ ნება დართო გამოძიებას, აწარმოოს ზემოაღნიშნული კომპიუტერული მონაცემის დათვალიერებისას — დათვალიერებული ინფორმაციის ფოტო და ვიდეო გადაღება, კერძოდ აღნიშნული განჩინების თანახმად სასამართლომ განმარტა, რომ „[...] დათვალიერება არის საგამოძიებო მოქმედება, რომელიც ამ შემთხვევაში, დაცვის მხარემ ჩაატარა სისხლის სამართლის საქმისათვის მნიშვნელობის მქონე გარემოებების გარკვევის მიზნით. საქართველოს სისხლის სამართლის საპროცესო კოდექსის 126-ე მუხლის მე-3 ნაწილი შესაძლებლობას იძლევა დათვალიერება ჩატარდეს ტექნიკური საშუალებების გამოყენებით, თუ ეს არ გამოიწვევს საგნის, დოკუმენტის, ნივთიერებისა და ინფორმაციის შემცველი სხვა ობიექტის ან მასზე არსებული კვალის განადგურებას ან დაზიანებას. ამავ კოდექსის 134-ე მუხლის მე-4 ნაწილის შესაბამისად, თუ საგამოძიებო მოქმედების ჩატარებისას გამოყენებული იყო ხმის ან/და გამოსახულების ნებისმიერი ტექნიკური საშუალებით ჩაწერა, შედგა ნახაზი ან სქემა, საგამოძიებო მოქმედების ოქმში უნდა აღინიშნოს გამოყენებული ტექნიკური საშუალებების ტექნიკური მახასიათებლები, მათი გამოყენების პირობები და მიღებული შედეგები. ტექნიკურ საშუალებათა გამოყენების შესახებ საგამოძიებო მოქმედების მონაწილეებს წინასწარ უნდა ეცნობოს და ამის თაობაზე უნდა აღინიშნოს ოქმში. ამ ნაწილში მითითებული ინფორმაციის შემცველი მასალა უნდა დაილუქოს, დადასტურდეს საგამოძიებო მოქმედების მონაწილეთა ხელმოწერებით და დაერთოს საქმეს. საპროცესო კოდექსის 135-ე მუხლის მე-4 ნაწილის მიხედვით, დათვალიერების ოქმში, სხვა გარემოებებთან ერთად, უნდა აღინიშნოს რა ტექნიკური საშუალება იქნა გამოყენებული და რა შედეგი იქნა მიღებული.“³⁸⁵

საგამოძიებო კოლეგია განმარტავს, რომ „დათვალიერება, როგორც საგამოძიებო მოქმედება, ტარდება მტკიცებულების, საქმისათვის მნიშვნელობის მქონე ინფორმაციის მოპოვების მიზნით, როგორც შეიძლება იყოს, მათ შორის, დოკუმენტიც. სისხლის სამართლის საპროცესო კოდექსის მე-3 მუხლის 23-ე ნაწილის თანახმად, დოკუმენტი მტკიცებულებაა, თუ ის შეიცავს სისხლის სამართლის საქმის ფაქტობრივი და სამართლებრივი გარემოებების დასადგენად საჭირო ცნობას. დოკუმენტად ითვლება ნებისმიერი წყარო, რომელშიც ინფორმაცია ალბეტადილია სიტყვიერ-ნიშნობრივი ფორმით ან/და ფოტო-, კინო-, ვიდეო-, ბგერისა თუ სხვა ჩანაწერის სახით ან სხვა ტექნიკური საშუალების გამოყენებით.“³⁸⁶

„ზემოაღნიშნული საპროცესო ნორმებიდან ცხადია, რომ მოქმედი სისხლის სამართლის საპროცესო კოდექსი საგამოძიებო მოქმედების ჩატარების დროს ტექნიკური საშუალებების გამოყენებას მიიჩნევს ამ საგამოძიებო მოქმედებისას მტკიცებულებების მოსაპოვებლად

³⁸⁴ თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის გადაწყვეტილებაში, საქმის № 1გ/456-19. მოსამართლე: გიორგი გოგინაშვილი. 26 მარტი, 2019 წელი. ელ. გვერდი:  ნანახია 03.07.2019

³⁸⁵ იხ. თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის მოსამართლე გელა ბადრაიშვილის განჩინება გასაჩივრებული განჩინების გაუქმების შესახებ. საქმე №1გ/133-18; 02 თებერვალი, 2018 წელი.

³⁸⁶ იხ. თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის მოსამართლე გელა ბადრაიშვილის განჩინება გასაჩივრებული განჩინების გაუქმების შესახებ. საქმე №1გ/133-18; 02 თებერვალი, 2018 წელი.

განხორციელებული ქმედებების შემადგენელ, განუყოფელ ნაწილად, ფაქტებისა და მოვლენების უკეთესი ფიქსაციის საშუალებად, რომლის მეშვეობითაც შესაძლებელი იქნება ჩატარებული საგამოძიებო მოქმედების ცალკეული ეპიზოდების (ან მთლიანად საგამოძიებო მოქმედების) სურათის აღდგენა, დემონსტრირება, სასამართლოს და მხარეებისთვის თვალსაჩინოდ წარმოდგენა. როგორც აღინიშნა, ასეთი შეიძლება იყოს ფოტოგადაღებაც, რომელიც ამ შემთხვევაში, დათვალიერების პროცესის შემადგენელი და მისი მიმდინარეობის (პერაპეტიების) თვალსაჩინოდ ამსახველი ნაწილია. ამ შემთხვევაში, ფოტოგადაღება არ არის დამოუკიდებლად ჩატარებული საგამოძიებო ან საპროცესო მოქმედება, რომლის დასაშვებობაზე მსჯელობაც დათვალიერების ოქმისაგან დამოუკიდებლად იქნებოდა შესაძლებელი. ის არის დათვალიერების ოქმის განუყოფელი ნაწილი და მასში თვალსაჩინოების სახით არის ასახული ის, რაც დათვალიერების ოქმში სიტყვიერი ფორმით არის აღწერილი. ამიტომ, თუ სასამართლოს მიაჩნია, რომ დათვალიერება, როგორც საგამოძიებო მოქმედება, სისხლის სამართლის საპროცესო ნორმების დაცვით არის ჩატარებული, შესაბამისად, ფოტოგადაღებაც, რომელიც დათვალიერების პროცესის შემადგენელი ნაწილია, ვერ იქნება არსებული მოთხოვნების საწინააღმდეგო, რადგან ეს ყველაფერი ასახულია კანონის შესაბამისად ჩატარებულ დათვალიერების ოქმში.³⁸⁷

„სააპელაციო სასამართლო განმარტავს, რომ განსახილველ შემთხვევაში, დათვალიერების ჩატარებისას განხორციელებული ფოტოგადაღება აბსოლუტურად განსხვავდება სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლით დარეგულირებული დოკუმენტის ან ინფორმაციის გამოთხოვის პროცედურისგან როგორც თავისი არსით, ისე პროცესუალური ფორმით. დოკუმენტის ან ინფორმაციის გამოთხოვა არის უშუალოდ იმ ინფორმაციის ან დოკუმენტის მოპოვება სისხლის სამართლის საქმის მიზნებისთვის, რომელიც დაცულია კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში. ინფორმაციის ან დოკუმენტის გამოთხოვისგან განსხვავებით, ბრალდებულის პერსონალურ კომპიუტერში არსებული ფაილების დათვალიერებას და ამ დროს განხორციელებულ ფოტოგადაღებას (მოცემულ შემთხვევაში) აქვს მხოლოდ ინფორმაციული დაცვითა, რომ ამა თუ იმ კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში (ბრალდებულის კომპიუტერში) არსებობს, დაცულია ეს ინფორმაცია. თუმცა, გამოთხოვისგან განსხვავებით, დათვალიერებისას ამ დაცული ინფორმაციის ელექტრონული ფორმით მოპოვება (კოპირება) და საქმეზე დართვა არ ხდება. დათვალიერებისა და ამ დროს განხორციელებული ფოტოგადაღებისას მიღებულ ინფორმაციას ვერ ექნება პრეტენზია უტყუარობასთან დაკავშირებით, ვინაიდან ამ დროს არ არის მოპოვებული თვით ამ ინფორმაციის პირველწყარო, რომელზეც შეიძლება ჩატარდეს ტექნიკურ-კომპიუტერული ექსპერტიზა მისი ავთენტიკურობის და ნამდვილობის დასადგენად, აგრეთვე იმის დასადგენად, შეინიშნება თუ არა მასზე მონათვის ან სხვა კანონსაწინააღმდეგო მანიპულაციების ნიშნები. ამიტომ, სააპელაციო სასამართლოს საგამოძიებო კოლეგიას მიაჩნია, რომ დათვალიერება იმდამდგარად, რაც მოცემულ შემთხვევაში ჩაატარა დაცვის მხარემ ფოტოგადაღების თანხლებით, ვერც მტკიცებულებითი ძალის (უტყუარობის) თვალსაზრისით და ვერც პროცესუალურად, ვერ შეცვლის ინფორმაციის ან დოკუმენტის გამოთხოვას, რომელიც ასეთი დათვალიერებისაგან განსხვავებით, უტყუარი დასკვნის გაკეთების საშუალებას აძლევს სასამართლოს და მხარეებს მისი გამოკვლევის შემთხვევაში. შესაბამისად, საგამოძიებო კოლეგიას არ მიაჩნია, რომ ხსენებული დათვალიერება და ამ დროს განხორციელებული ფოტოგადაღება შეიცავს საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლით გათვალისწინებულ საგამოძიებო მოქმედების — დოკუმენტის ან ინფორმაციის გამოთხოვის ნიშნებს.“³⁸⁸

³⁸⁷ იქვე.

³⁸⁸ იხ. თბილისის სააპელაციო სასამართლოს საგამოძიებო კოლეგიის მოსამართლე გელა ბადრაიშვილის განჩინება გასაჩივრებული განჩინების გაუქმების შესახებ. საქმე №1გ/133-18: 02 თებერვალი, 2018 წელი.

ამდენად, ისეთ შემთხვევაში, როდესაც სახეზე გვაქვს იმ ტიპის დანაშაული — რომელზეც ფარული საგამოძიებო მოქმედების ჩატარება ვერ მოხდება, მხარეს უფლება აქვს განახორციელოს საგამოძიებო მოქმედება - დათვალიერება და დათვალიეროს კომპიუტერულ სისტემაში დაცული ინფორმაცია, რომელიც აისახება დათვალიერების ოქმში.

7.2 პერსონალურ კომპიუტერში დაცული ციფრული ინფორმაციის დათვალიერების ტექნიკური პროცედურები და მეთოდები

დათვალიერების დროს, ვინაიდან ვერ ხორციელდება ინფორმაციის გამოთხოვა, მიზანშეწონილია მოხდეს საგამოძიებო მოქმედება - დათვალიერების ასახვა რაიმე საშუალებით, იქნება ეს ფოტო ან და ვიდეოგადაღება, ან თავად კომპიუტერის მიერ ეკრანზე წარმოებული საგამოძიებო მოქმედების გადაღება კომპიუტერის ეკრანზე.

პირველი გზა აღნიშნულისათვის არის ეკრანზე სამუშაო რეჟიმის წარმოებისას ფოტოსურათის გადაღება:

ეკრანზე ფოტოს გადაღება ანუ ე.წ. Screenshot-ის გადაღება (ხანდახან მას უწოდებენ Print Screen) არ არის რთული საქმე და მისი გაკეთება სხვადასხვა მეთოდითაა შესაძლებელი, განვიხილოთ Screenshot - ის გადაღების მეთოდები Windows- ის სისტემის მქონე კომპიუტერებზე და MacOS სისტემის მქონე კომპიუტერებზე:

1. ეკრანზე ფოტოს გადაღება ანუ Screenshot მეთოდები Windows- ის სისტემის მქონე კომპიუტერებზე;

განვიხილოთ Screenshot - ის გადაღების რამდენიმე ვარიანტი, რაც შეგიძლიათ გამოიყენოთ აღნიშნული ოპერაციული სისტემის ფაქტგლებში, თუ ნახავთ, რომ კომპიუტერთან არ ფუნქციონირებს ერთი ვარიანტი გადადით მეორეზე. ერთი-ერთი ვარიანტი აუცილებლად იმუშავებს, ვინაიდან ეს არის აღნიშნული ოპ. სისტემის ყველა ვარიანტი:

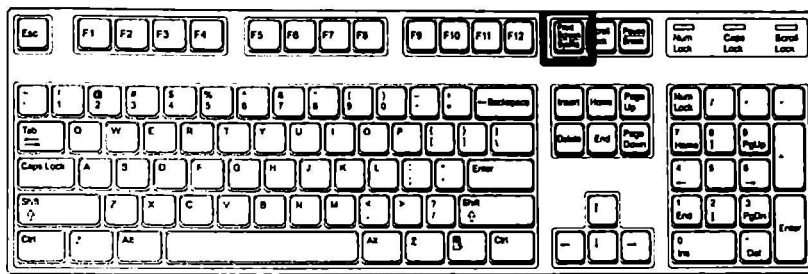
ყველაზე გავრცელებული ვარიანტია ლილაკი Print Screen - ის გამოყენება. აღნიშნული მოთოდი მუშაობს windows - ის ყველა ვერსიაზე.

„Print Screen - ის ლილაკი მდებარეობს, როგორც წესი კლავიატურის ზედა მარჯვენა ნაწილში, F12 ლილაკსა და Scroll Lock-ს შორის. ლეპტობებზე თქვენ უნდა გამოიყენოთ Fn ან Function იმისათვის რომ ისარგებლოთ Print Screen ლილაკით (Print Screen ლილაკს შეიძლება ასევე ეწეროს შემოკლებული ვარიანტები „Prt Sc“, „Pmt Scm“, „Print Scm“ და ა.შ.)³⁶⁹ სურათზე N80 იხილეთ ლილაკის მდებარეობა;

³⁶⁹ სტიკია: Screenshot-ის გადაღება (Windows) ელ.გვერდი



ნანახია 07.07.2019.



390



391

„მას შემდეგ რაც იპოვიტ და დააჭერტ Print Screen ლილავს თქვენს კლავიატურაზე უნდა გადაინაცვლოთ Start menu—ში, შემდეგ აირჩიოთ "All Programs", და დააკლიკოთ "Accessories", აქ კი ირჩევტ "Paint"—ს.“³⁹² (იხილეთ სურათზე 81);

³⁹⁰ სტატია: Screenshot—ის გადაღება (Windows) ელ.გვერდი



ნანახია 07.07.2019.

³⁹¹ ელ. გვერდი

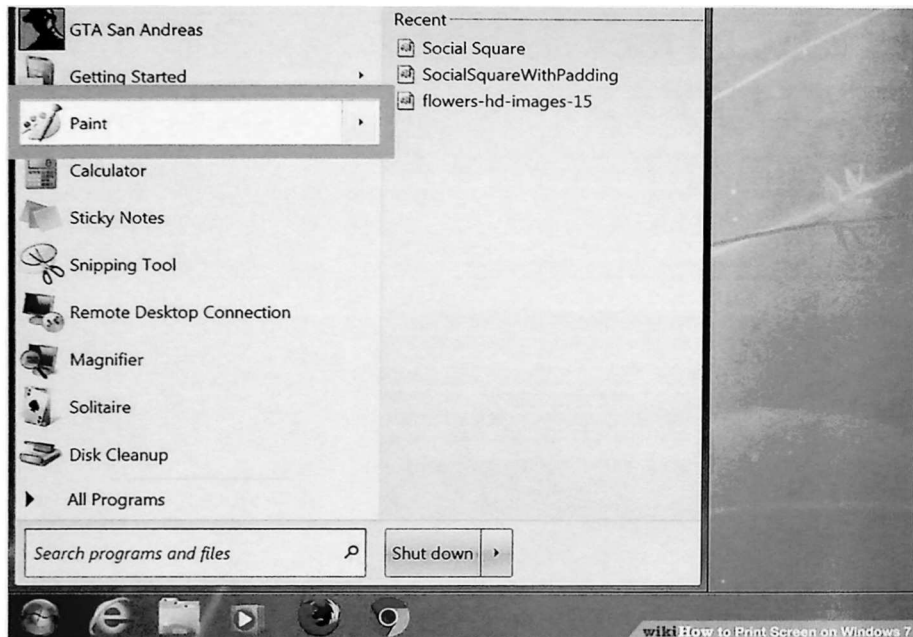


ნანახია 19.07.2019

³⁹² სტატია: Screenshot—ის გადაღება (Windows) ელ.გვერდი



ნანახია 07.07.2019.



„Paint“-ის გახნის შემდეგ აქტიურ ფანჯარაში უნდა ჩავსვათ ჩვენს მიერ გადაღებული სურათი, არსეობს რამოდენიმე მეთოდი:

უბრალოდ აქტიურ ფანჯარაში ვაჭერთ მარჯვენა ლილაკს მათზე და გამოსულ მენიუში ვირჩევთ „Paste“-ს;

კლავიატურაზე ვაჭრთ ლილაკებს „Ctrl“ და „V“-ს ერთდროულად რაც ასრულებს იგივე „Paste“-ს ფუნქციას:

Paint-ს შედა მენიუში ვირჩევთ „Edit“-ს და შემდეგ გამოსულ ქვე-მენიუში ვირჩევთ „Paste“-ს.³⁹⁴ (იხილეთ სურათზე N82):

³⁹³

ელ. გვერდი



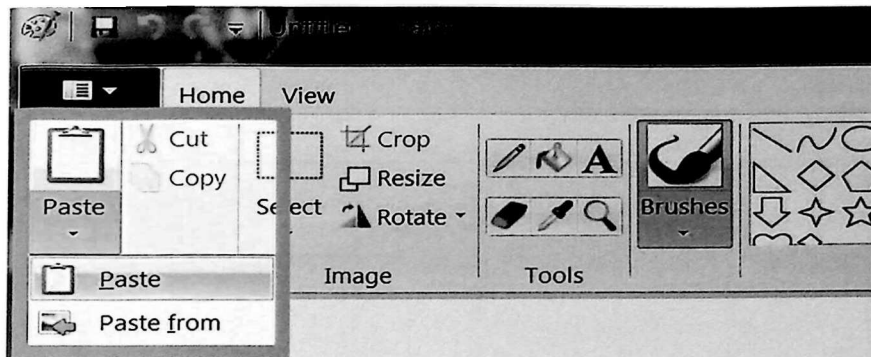
ნანახია 19.07.2019

³⁹⁴

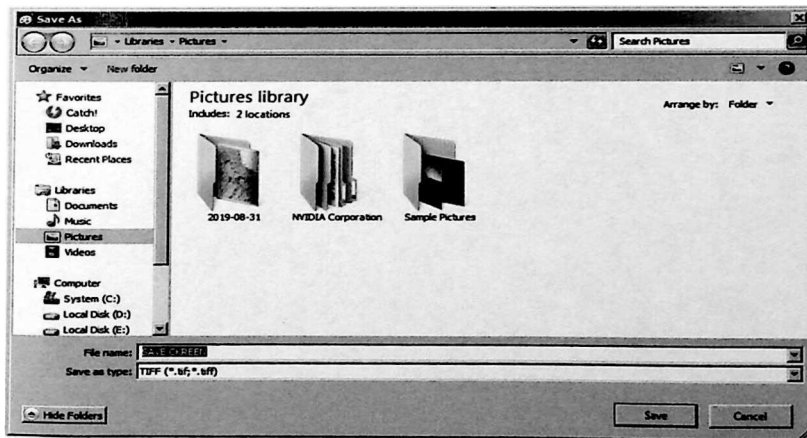
სტატია: Screenshot-ის გადაღება (Windows) ელ.გვერდი



ნანახია 07.07.2019.



მას შემდეგ რაც Paint-ში განათავსებთ და დაამუშავებთ თქვენს მიერ განთავსებულ Screenshot-ს საჭიროა მისი შენახვა. „Windows XP-ისა და უფრო ძველ ვერსიებში თქვენ უნდა დააკლიკოთ მარცხენა ზედა კუთხეში მდებარე მენიუში File-ს და გამოსულ ქვე-მენიუში უნდა აირჩიოთ "Save As..." ხოლო თუ თქვენ იყენებთ Windows Vista-ს ან შემდეგ ვერსიებს მაშინ უნდა დააკლიკოთ მენიუს ლილავს რომელიც მდებარეობს "Home" ლილავთან და შემდეგ გამოსულ ქვე-მენიუში ასევე უნდა აირჩიოთ "Save As..." ფუნქცია. "Save As..."-ის არჩევის შემდეგ თქვენ არქმევთ სასურველ სახელს დაამუშავებულ სურათს ირჩევთ ადგილს სადაც მას შეინახავთ და აწევბით "Save" ლილავს. 396 (იხილეთ სურათზე N83)



395 სტატია: Screenshot-ის გადაღება (Windows) ელ.გვერდი



ნანახია 07.07.2019.

396 იქვე

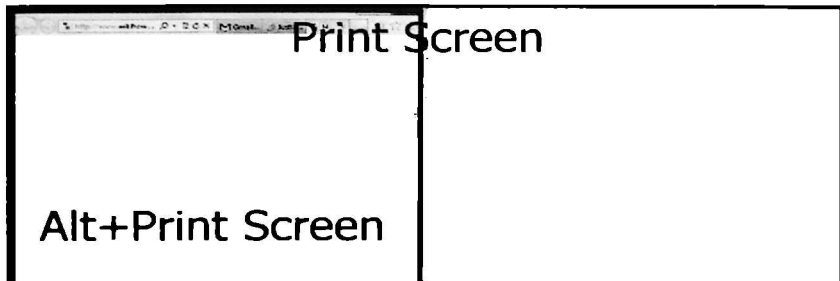
397 სტატია: Screenshot-ის გადაღება (Windows) ელ.გვერდი



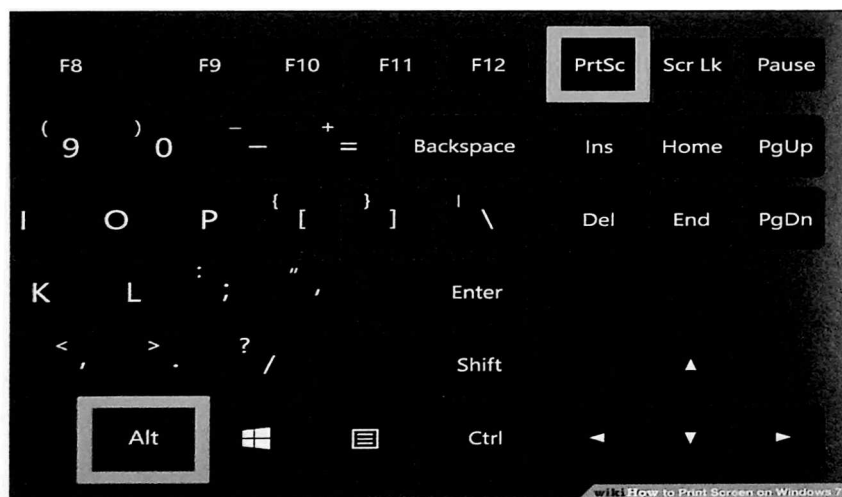
ნანახია 07.07.2019.

მეორე ვარიანტი:

.Print Screen—ის გამოყენებით თქვენ უღებთ სურათს მთელს ეკრანს, ხოლო თუ თქვენ გამოიყენებთ Alt + Print Screen ამ შემთხვევაში თქვენ გადაიღებთ მხოლოდ აქტიურ ფანჯარას. წარმოდგენისათვის სურათზე იხილეთ განსხვავება ALT+PrintScreen—სა და PrintScreen—ს შორის;³⁹⁸ (იხილეთ სურათზე N84 და N85)

სურათი N84: 

სურათი N85:



³⁹⁸ სტატია: Screenshot—ის გადაღება (Windows) ელ.გვერდი



ნანახია 07.07.2019.

³⁹⁹ იქვე.

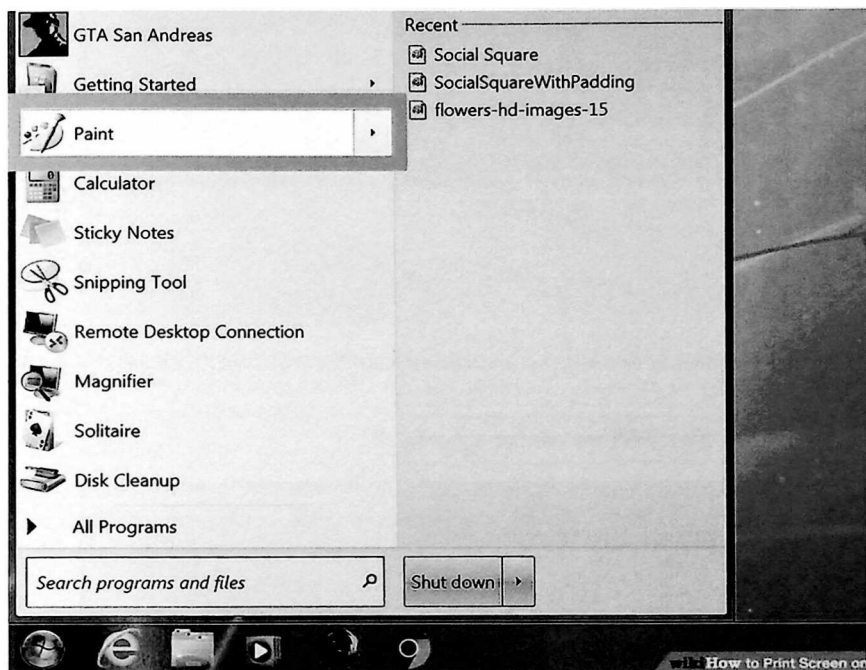
⁴⁰⁰ ელ. გვერდი.



ნანახია 19.07.2019

„მას შემდეგ რაც იპოვით და დააჭერთ All Print Screen ლილავს თქვენს კლავიატურაზე უნდა გადინაცვლოთ Start menu–ში, შემდეგ აირჩიოთ "All Programs", და დააკლიკოთ "Accessories", აქ კი ირჩევთ "Paint"–ს.“⁴⁰¹ (იხილეთ სურათზე N86)

სურათი N86: ⁴⁰²



„Paint–ის გახსნის შემდეგ აქტიურ ფანჯარაში უნდა ჩავსვათ ჩვენს მიერ გადაღებული სურათი, არსებობს რამოდენიმე მეთოდი:

უბრალოდ აქტიურ ფანჯარაში ვაჭერთ მარჯვენა ლილავს მანუსზე და გამოსულ მენიუში ვირჩევთ "Paste"–ს;

კლავიატურაზე ვაჭრთ ლილავებს "Ctrl" და "V"–ს ერთდროულად რაც ასრულებს იგივე "Paste"–ს ფუნქციას;

Paint–ს შედა მენიუში ვირჩევთ "Edit"–ს და შემდეგ გამოსულ ქვ-მენიუში ვირჩევთ "Paste"–ს.⁴⁰³ (იხილეთ სურათზე N87);

⁴⁰¹ სტატია: Screenshot–ის გადაღება (Windows) ელ.გვერდი



ნანახია 07.07.2019.

⁴⁰² ელ. გვერდი.

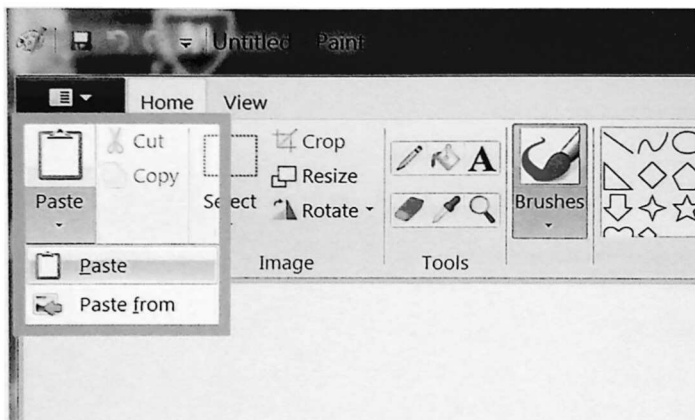


ნანახია 19.07.2019

⁴⁰³ სტატია: Screenshot–ის გადაღება (Windows) ელ.გვერდი



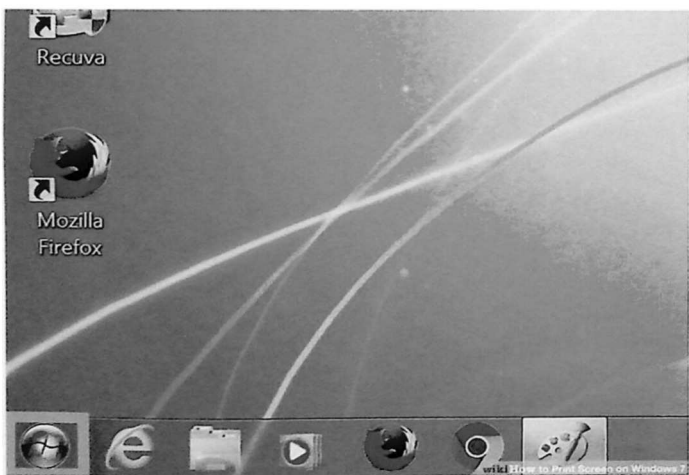
ნანახია 07.07.2019.



გთავაზობთ ეკრანზე სურათის გადაღების კიდევ ერთი გზას Windows Vista, 7, 8, 8.1 კომპიუტერული სისტემებისათვის.

ნახიკი 1: გახსენით Start მენიუ; (იხილეთ სურათზე N88):

სურათი N88:



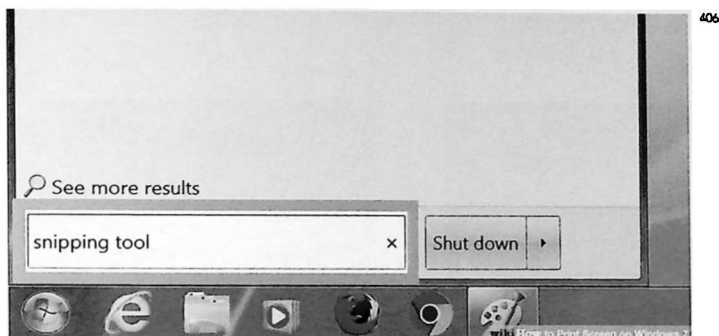
ელ. გვერდი. ნახიკი 19.07.2019



ელ. გვერდი. ნახიკი 19.07.2019

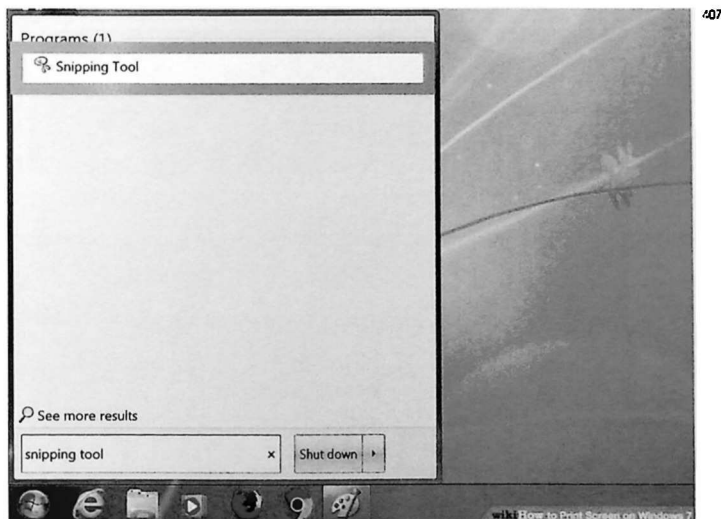
ნახატი 2. ძიების ველში ჩაწერეთ "Snipping Tool" ("Ножницы" რუსული ვერსიის შემთხვევაში);
(იხილეთ სურათზე N89)

სურათი N89:



ძიების შედეგებში გამოჩნდება მოცემული პროგრამა, გახსენით ის მასზე ერთი დაწკაპუნებით.
ან გახსენით პროგრამა შემდეგ მისამართზე: "Start Menu\Accessories\Snipping Tool" ("Старт Меню\Стандартные\Ножницы"). (იხილეთ სურათზე N90);

სურათი N90:



406

ელ. გვერდი.



ნანახია 19.07.2019

407

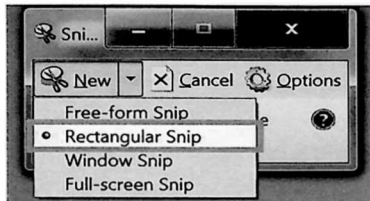
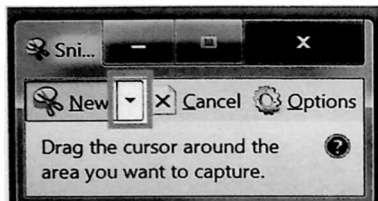
იქვე.

ნახები 3. როდესაც აირჩევთ "New" ლილასს, გამოჩნდება ჩამონათვალი. Snipping Tool გვთავაზობს სტრინშოტის გადაღების 4 მეთოდს: Free-form snip - ნებისმიერი ფორმის სურათი, Rectangular snip - მართკუთხედის ფორმის სურათი, Window Snip - ცალკეული ფანჯრის სურათი, Full-screen snip - მთლიანის ეკრანის სურათი.

აირჩიეთ სასურველი რეჟიმი და მონიშნეთ გადასაღები სივრცე მაუსით: (იხილეთ სურათზე N91 და N92)

სურათი N91: 

სურათი N92: 



ამის შემდეგ სურათი ავტომატურად გაიხსნება Snipping tool რედაქტორში, სადაც შეგიძლიათ სურათის კორექტირება, რის შემდეგაც სურათი უნდა შეინახოთ: სურათი შეგიძლიათ შეინახოთ Toolbar-ზე შესაბამის ლილკზე დაჭერით, ან მენიუდან "File -> Save as..." (Файл -> Сохранить как...), ან Ctrl + S ლილაკებზე ერთდროულად დაჭერით. სურათის შენახვა შესაძლებელია PNG, JPG, GIF ფორმატებში.⁴¹⁰ (იხილეთ სურათზე N93 და N94)

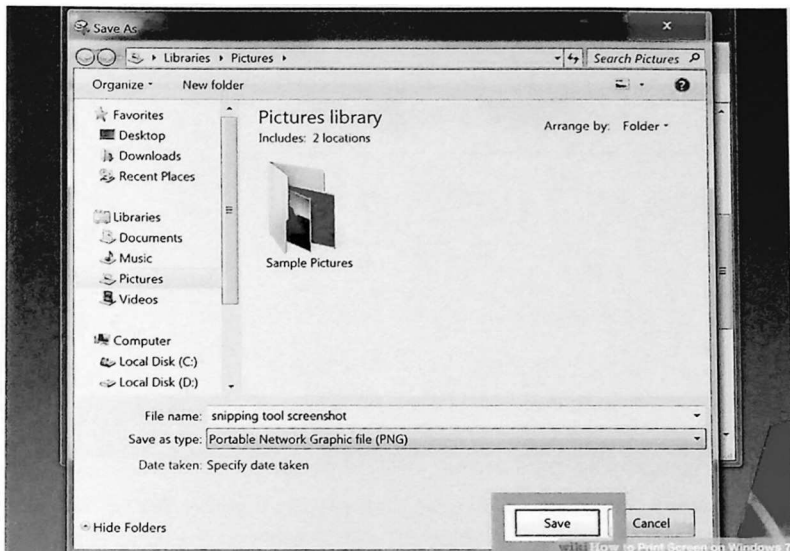
სურათი N93 



ელ. გვერდი.  ნანახია 19.07.2019

იქვე.
ელ. გვერდი.  ნანახია 14.07.2019

ელ. გვერდი.  ნანახია 19.07.2019



2. ეკრანზე ფოტოს გადაღება MacOS პროგრამაზე;

ყველაზე სწრაფი გზა არის დავაწვეთ შემდეგი სამი ლილაკის კომბინაციას:

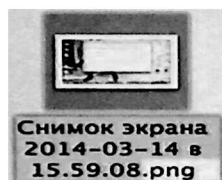
Command (ასევე შესაძლებელია შეგვხვდეს აბრევიატურა cmd) ლილაკს, მასთან ერთად Shift ლილაკს და ლილაკს, რომელსაც აწერია 3-იანი (თვალსაჩინოებისათვის კომბინაცია იხილეთ სურათზე N95 და 96);

სურათი N95:



აღნიშნული კომბინაციის შემდეგ თქვენ მიიღებთ ეკრანზე გადაღებულ ფოტოს PNG ფორმატში, რომელიც შეინახება კომპიუტერში (თვალსაჩინოებისთვის იხილეთ სურათი 93);

სურათი N96:



ბოლოს თქვენ შეგიძლიათ დაარქვათ აღნიშნულ დოკუმენტს სახელი და შეინახოთ.

MacOS პროგრამაზე ეკრანზე ფოტოს გადაღების მეორე გზა;

არსებობს ეკრანზე ფოტოს გადაღების მეორე გზაც, რომელიც უფრო ხარისხიან პროდუქტს გვთავაზოვს, შევდივართ მენიუდან ლილაკში Launchpad (იხილეთ სურათი N97)

სურათი N97:



შემდგომ ვნახულობთ პროგრამას screenshot რუსულად снимок экрана რომელშიც შევდივართ მაუსზე ხელის დაჭერით (იხილეთ სურათი N98);

ეკრანზე ფოტოს გადაღება linux პროგრამის მქონე კომპიუტერებზე:

ყველაზე სწრაფი გზა linux სისტემის მქონე კომპიუტერებზე, იმისათვის რომ ეკრანის ფოტო გადავიღოთ არის შემდეგი რამდენიმე ღილაკების კომბინაცია:

„**PrtSc** — გადაიღებს ფოტოს და ინახავს Pictures” directory-ში. (Save a screenshot of the entire screen to the “Pictures” directory):

Shift + PrtSc — შევიძლიათ გადავიღოთ ეკრანის კონკრეტული ნაწილის სურათი. (Save a screenshot of a specific region to Picture):

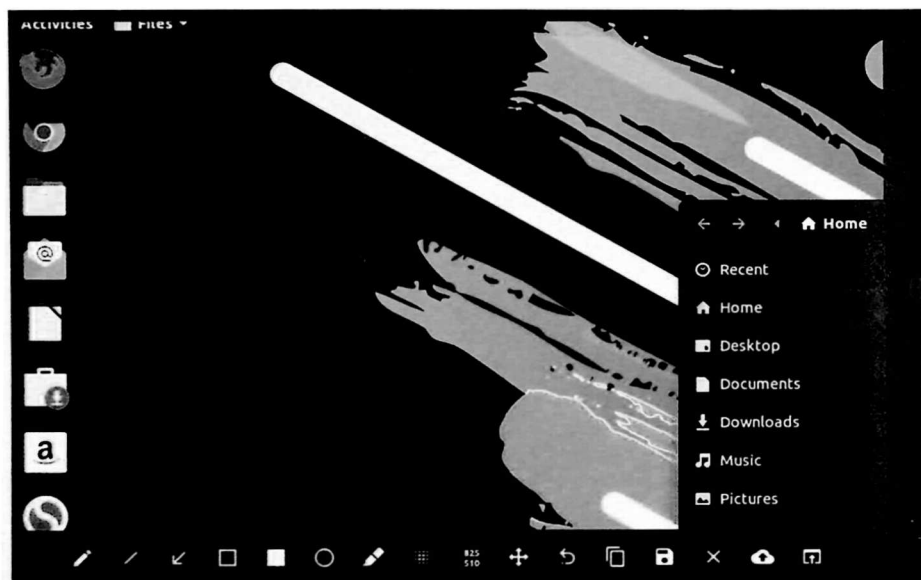
Alt + PrtSc — მიმდინარე ფანჯრის სურათის გადაღება (Save a screenshot of the current window to Pictures);

Ctrl + PrtSc — მიღებული ეკრანის ბუფერის დაკოპირება (Copy the screenshot of the entire screen to the clipboard);

Shift + Ctrl + PrtSc — სტრინშოტის კოპირება კონკრეტულ ადგილზე (Copy the screenshot of a specific region to the clipboard):

Ctrl + Alt + PrtSc — (სტრინშოტის კოპირება ეკრანზე) Copy the screenshot of the current window to the clipboard.”⁴¹³ (სურათი N100):

სურათი N100: ⁴¹⁴



ეკრანის ვიდეოგადაღება:

⁴¹³ ელ.გვერდი: ნანახია 19.07.2019



⁴¹⁴ ელ.გვერდი: ნანახია 19.07.2019



იმისათვის, რომ გამოძიების მიერ წარმოებულ იქნეს კომპიუტერის ეკრანზე მიმდინარე საგამოძიებო მოქმედების გადაღება - მიზანშეწონილია გამოძიებულ ფლემ მესხიერებაზე თან პქონდეს ისეთი პროგრამის საინსტალაციო ვერსია რომელიც შემდგომ მოახდენს ეკრანზე წარმოებული საგამოძიებო მოქმედების გადაღებას, ასეთი აპრობირებული პროგრამა არის "Fast Stone"⁴¹⁵ (ან სხვა ოფიციალური პროგრამა), თუ გამოძიებულს აღნიშნული პროგრამის საინსტალაციო ვერსია ფლემ მესხიარებაზე არ აქვს, მას შეუძლია იმ კომპიუტერიდან, რომელზეც მუშაობს, შევიდეს ელექტრონულ გვერდზე <https://www.faststone.org/FSCaptureDownload.html> საიდანაც გადმოწეროს აღნიშნული პროგრამა მითითებული ინსტრუქციით (იხილეთ სურათზე N98);

სურათი N98;

FastStone



Home | Download | Buy | Donate | Contact Us

Download FastStone Capture

FastStone Capture 9.1 2019-07-30

exe
download

exe (size 2)
download

zip
download

portable
download

FastStone Capture Tutorial

tutorial

Note:

exe

A single executable file that installs the application in your computer. **Recommended for most users.**

zip

A zip (compressed) format of the exe file above. In some networks, downloading exe files is strictly prohibited. If you are using such networks, download the zip file instead. After the download, just unzip it to get the exe file (installer).

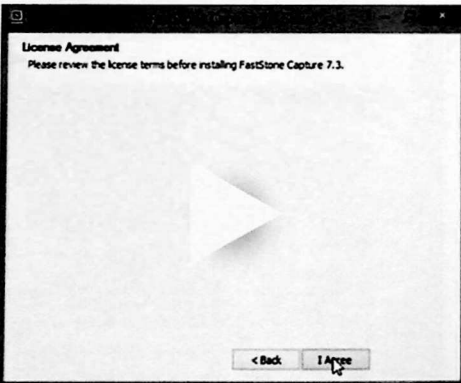
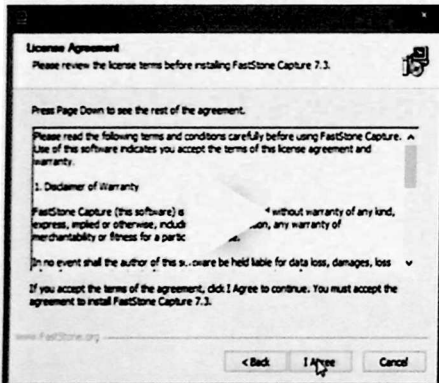
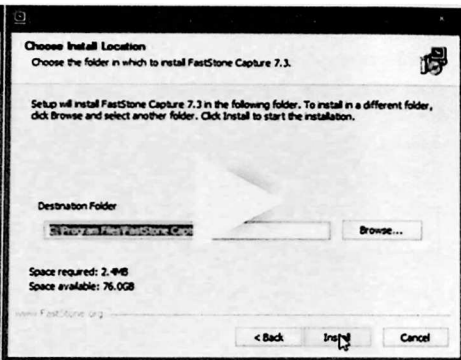
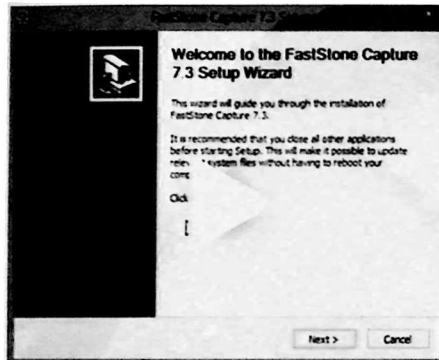
portable

A zip (compressed) file that includes all the required files to run the application independently from any folder you dump it in. Major advantage is that you can carry it around on a memory stick / USB flash drive, or copy / migrate from PC to PC via simple copying of files. No installation is necessary.

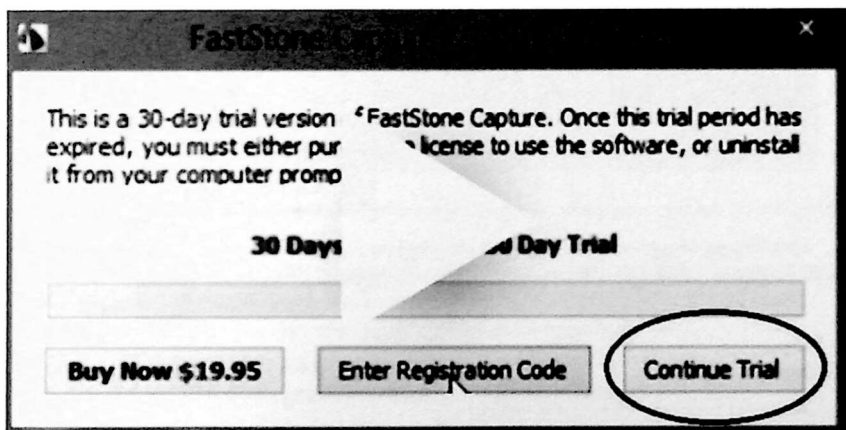
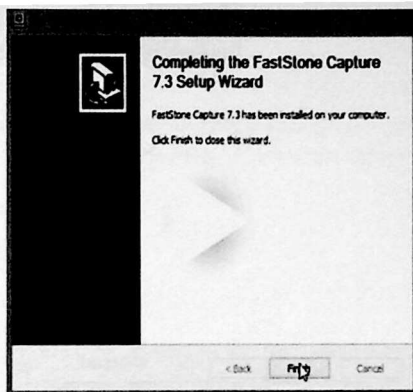
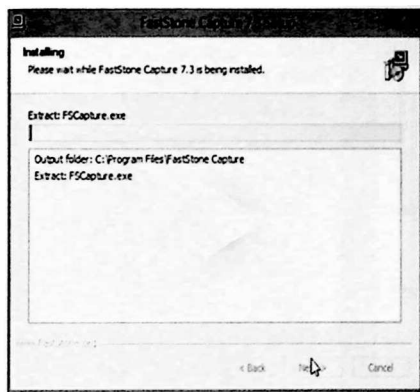
Copyright © 2019 FastStone Soft - All Rights Reserved. Privacy Policy

პროგრამის გადმოწერის შემდეგ, უნდა მოახდინოს პროგრამის ინსტალაცია, პროგრამის ინსტალაციის შესახებ ვიდეო იხილეთ ელექტრონულ გვერდზე <https://www.youtube.com/watch?v=1878485>, პროგრამის ინსტალაცია საჭიროებს რამდენიმე ქმედებას (პროგრამის ინსტალაციის მიმდინარეობა ნაჩვენებია სურათების სახით, სურათები ნაჩვენებია ელექტრონულ გვერდზე - <http://www.softnews.org/FastStone.html> არსებული ვიდეოს დამუშავების შედეგად) (იხ. სურათი N99, 100, 101, 102, 103, 104, 105);





სურათები N103, N104, N105;

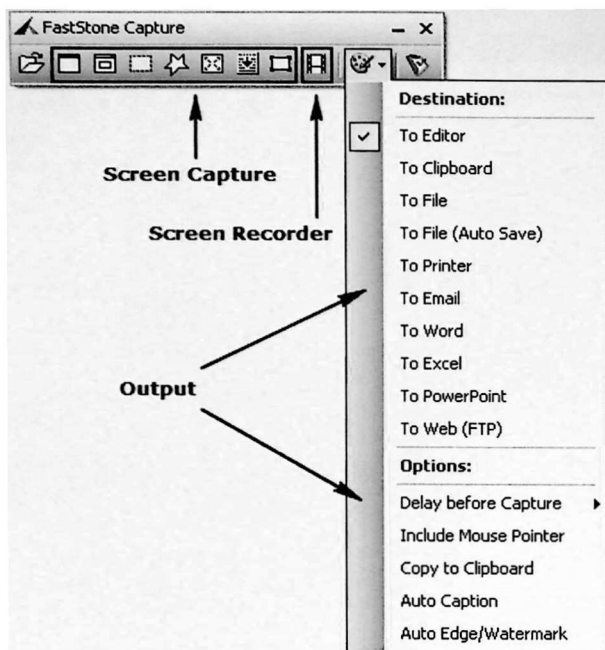


მას შემდეგ რაც პროგრამა იქნება დაინსტალირებული კომპიუტერში, სახეზე გვექნება ეკრანზე შემდეგი მონაცემის ფაილი (იხილეთ სურათი 106);

სურათი N106;



რაც ნიშნავს, რომ პროგრამა დაინსტალირებულია. როდესაც გავხსნით აღნიშნულ ფაილს, გაიხსნება შემდეგი ხასიათის პროგრამა (იხილეთ სურათი N107);



აღნიშნული პროგრამის გამოყენების ინსტრუქცია მარტივია, მაგრამ თუ ამის დეტალური გაცნობა გსურთ, ინსტრუქცია შეგიძლიათ იხილოთ ელექტრონულ გვერდზე



პროგრამის გახსნის შემდეგ, იმისათვის რათა მოვახდინოთ ეკრანზე არსებული ვიდეოს ჩაწერა — უნდა დავაწვეთ მაუსით ღილაკს screen recorder, ხოლო შემდეგ უნდა მოვნიშნოთ ეკრანის სრული გადაღება და დავაწვეთ ღილაკს Record. (იხ. სურათი N108);

სურათი N108;

იმ შემთხვევაში, თუ გამომძიებელს თან არ აქვს შესაბამისი მოწყობილობა - ვიდეოკამერა, ან სხვა საჭიროების შემთხვევაში, შესაძლებელია საგამომძიებო მოქმედების გადაღება მოხდეს კომპიუტერის ვებ-კამერის საშუალებით (თუ ასეთი კამერა კომპიუტერს აქვს), აღნიშნული გადაღების პროცედურები შემდეგია;

„ვებ კამერიდან ჩაწერა შეიძლება გადაღების და რედაქტირების დროს. ვებ კამერიდან ჩასაწერად ჩანართების ინსტრუქციულ პანელზე დაწკაპუნეთ ლილაკზე Record Camera (იხილეთ სურათი N109);

სურათი N109 ⁴¹⁶



„ლილაკზე დაწკაპუნების შემდეგ სერვისულ პანელზე გამოვაფანჯარა ვებ კამერიდან ჩაწერის პარამეტრების მისაცემად.“ ⁴¹⁷ (იხილეთ სურათი N110);

სურათი N110;



⁴¹⁸

„განყოფილებაში Record duration (ჩაწერის ხანგრძლივობა) არსებულ აღმების დანიშნულება შემდეგია:

Until manually stop or selection on timeline — გადალება განხორციელდეს დროითი შკალაზე გამოყოფილი უბნის ბოლო წერტილზე მისვლისას ან გადაძვლების მიერ;

Until end of clip — გადალება განხორციელდეს კლიპის დასასრულამდე;

Until end of timeline — გადალება განხორციელდეს დროითი შკალის ბოლომდე;

Auto-extend last video frame - ავტომატურად გაგრძელდეს გადალება გადაძვლების საუბრის დამთავრებამდე.“⁴¹⁹

„ჩამოშლადი სიიდან Avialabe video devices ამოირჩევა გადაძვლები ვიდეომონიტორილობა. Preview-ი წინასწარი დათვალიერების ფანჯარაა. ლილაკზე Properties დაწკაპუნებით გამოსულ ფანჯარაში ხორციელდება გადაღების ზოგიერთი პარამეტრი, ხოლო ლილაკზე Format— დაწკაპუნებით გამოსულ ფანჯარაში კი — ვიდეო ნაკადის ზოგიერთი პარამეტრის გაწყობა. ლილაკზე Default დაწკაპუნებით წარმოებს გაჩუქებით მითითებული პარამეტრების გაწყობა.“⁴²⁰

⁴¹⁶

ელ.გვერდი



ნანახია 06.07.2019

⁴¹⁷

იქვე.

⁴¹⁸

იქვე.

⁴¹⁹

იქვე.

⁴²⁰

ელ.გვერდი



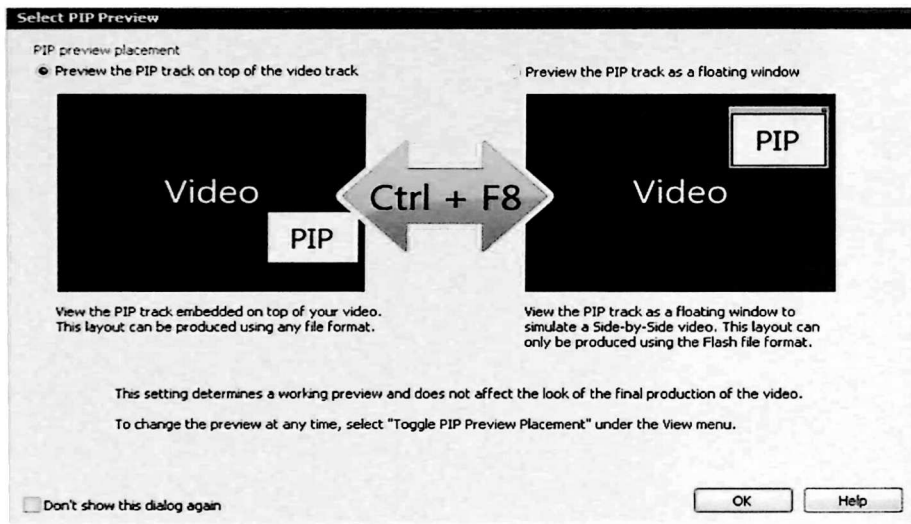
ნანახია 06.07.2019

..განყოფილებაში Audio, Record audio ალამის მონიშვნით ხორციელდება ხმის ჩაწერა, Mute speakers ალამის მონიშვნით კი ჩაწერის დროს გამოითიშება დინამიკები. ლილაკზე Setup დაწკაპუნების შემდეგ გაიშვება აუდიო მოწყობილობის გაწყობის პროგრამა ოსტატი.

ლილაკზე Start recording დაწკაპუნების შემდეგ იწყება გადაღება, წინასწარი დათვალიერების ფანჯარაში კი ჩანს ეკრანზე გადაღებული კადრები. თუ გვსურს ეკრანზე გადაღებული კადრების ჩვენების შეჩერება, მაშინ საჭიროა დაწკაპუნებულ იქნეს ლილაკზე Extend current frame.⁴²¹

..ჩაწერის დამთავრების ლილაკზე Stop recording დაწკაპუნების შემდეგ გამოვა ფანჯარა გადაღებული ფაილის ადგილისა და სახელის მისაცემად. ფაილის შენახვის ადგილისა და სახელის შერჩევის შემდეგ გამოვა ფანჯარა გადაღებული მასალის წინასწარი დათვალიერების რეჟიმის შერჩევის შესახებ.⁴²² (იხ. სურათი 111);

სურათი N111:



დათვალიერების სამი ვარიანტი:

..Preview the PIP track on top of the video track — ვებ კამერიდან გადაღებული მოთავსდება ძირითად ვიდეოში მცირე ზომის ფანჯრის სახით ანუ ადგილი აქვს სიტუაციას სურათი სურათში. შეიძლება შეიცვალოს ამ კადრის ადგილმდებარეობა და ზომები;

Preview the PIP track as a floating window - ვებ კამერიდან გადაღებული ვიდეო მოთავსებული იქნება მცურავ ფანჯარაში. ეს ვარიანტი უმჯობესია რეალიზებულ იქნეს Flash ფორმატში ვიდეოს ექსპორტისას.⁴²³

..რედაქტირებისას დათვალიერების რეჟიმები შეიძლება შეიცვალოს Ctrl+F8 კლავიშებით. დათვალიერების რეჟიმის შერჩევა დამოუკიდებელია შედეგების ექსპორტისაგან. ვებ კამერიდან

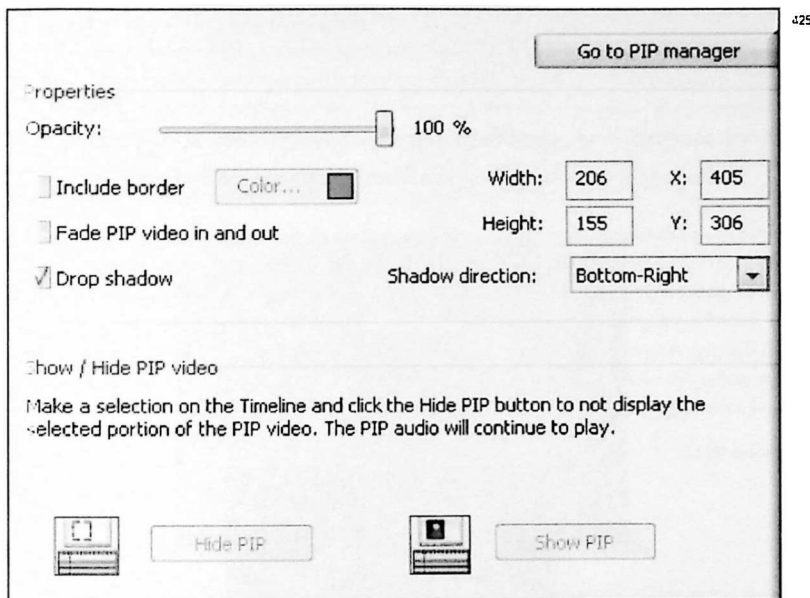
⁴²¹ ელ.გვერდი  ნანახია 06.07.2019.

⁴²² იქვე.

⁴²³ ელ.გვერდი  ნანახია 06.07.2019

ჩაწერის შემდეგ დროით შკალაზე გამოჩნდება დამატებითი ბილიკები PIP და PIP Audio. ჩანართების ინსტრუმენტულ პანელზე დააწკაპუნეთ ლილაკზე Picture-in-Picture⁴²⁴ (იხილეთ სურათი N112)

სურათი N112;



„სერვისულ პანელზე გამოჩნდება ვებ კამერიდან გადაღებული ვიდეოები“⁴²⁶

„არსებულ პიპერკაპშირების სტრიქონებს შემდეგი შინაარსობრივი დატვირთვა აქვთ:

Modify selected PIP clip – მოდიფიცირებულ იქნეს მონიშნული კლიპი;

Remove selected PIP clip – ამოშლილ იქნეს მონიშნული კლიპი;

Remove all PIP clip – ამოშლილ იქნეს ყველა კლიპი.

Modify selected PIP clip სტიქონზე დაწკაპუნების შემდეგ სერვისული პანელი მიიღებს.“⁴²⁷

„პირადი ცხოვრების ხელშეუხებლობის დაცვის მიზნებისათვის სასურველია, გამოძიების ორგანოები ციფრული ინფორმაციის მატარებლების დათვალიერებისას გამოძიებისათვის მნიშვნელოვანი ინფორმაციის მოსაძებნად ფართოდ იყენებდნენ სპეციალურ პროგრამებს/სოფტებს, რომლებსაც აქვთ სპეციფიკური პარამეტრების მექანიზმები ინფორმაციის მოძიების უნარი, ფაილების შიგთავსის მექანიკური დათვალიერებისა და გახსნის ნაცვლად. ეს, ერთი მხრივ, მნიშვნელოვნად გაამარტივებს პოტენციური მტკიცებულების ძებნის პროცესს და, მეორე მხრივ, უზრუნველყოფს კომპიუტერებსა და ციფრული მონაცემების შემნახველ მოწყობილობებთან მიმართებით პირადი

⁴²⁴ იქვე.

⁴²⁵ იქვე.

⁴²⁶ ელ.გვერდი  ნანახია 06.07.2019

⁴²⁷ იქვე.

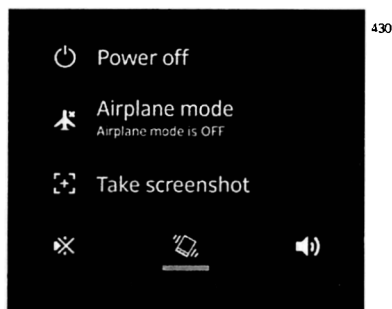
ცხოვრების ხელშეუხებლობის უფლების რეალიზაციას. როგორც საგამოძიებო პრაქტიკის შესწავლა ცხადყოფს. საგამოძიებო ორგანოები, მიუხედავად იმისა, რომ ცალკეულ შემთხვევებში იყენებენ მყარი დისკის წამკითხავ სპეციალურ პროგრამებს (მაგალითად, „Dock Station“), უპირატესობას მექანიკურ დათვალიერებას ანიჭებენ.“⁴²⁸

7.3 მობილურ ტელეფონში დაცული ციფრული ინფორმაციის დათვალიერების ტექნიკური პროცედურები და მეთოდები

ძირითადად იმისათვის, რომ გავაკეთოთ მობილური ეკრანის ფოტოგადაღება ანუ სკრინშოტი საჭიროა აპარატზე ერთდროულად დავაჭიროთ რამდენიმე ლილაკს. ყველაზე ხშირად ესაა ხმის დაკლებისა და ჩართვა-გამორთვის (Power Button) ლილაკები, ან მთავარ ეკრანზე გადასასვლელი და ჩართვა-გამორთვის ლილაკები.

„მას შემდეგ რაც თქვენ ერთდროულად დააჭერთ ამ ორ ლილაკს შეტობინებათა პანელზე მიიღებთ დასტურს იმის შესახებ რომ სურათი შენახულია მოწყობილობაზე. ხანდახან გაისმის ფოტოკამერის ჩამკეცის ხმა და ჩნდება მოლივლივე შედეგობინება.“⁴²⁹ (იხილეთ სურათი N113);

სურათი N113:



„ზოგიერთ შემთხვევაში ეკრანის სურათის გაკეთება მენიუდანაც შესაძლებელია, რომელიც გამოდის ჩართვის ლილაკზე დიღხანს დაჭერით. შესაძლოა ასე უფრო მოსახერხებელი იყოს როცა რთულია ერთდროულად რამდენიმე ლილაკზე დაჭერა, როგორც Sony Xperia V-ზე.“⁴³¹

⁴²⁸ ლალი ფაფიაშვილი. სტატია: ციფრული მედიაციების ამოღება: პირადი ცხოვრების ხელ-შეუხებლობის საკმარისი თუ ილუმზორული გარანტია? სტატიათა კრებული, ადამიანის უფლებათა დაცვა და სამართლებრივი რეფორმა საქართველოში. თბილისი. 2014. გვ. 162

⁴²⁹ როგორ გადავიღოთ ეკრანის სურათი (სკრინშოტი) ანდროიდ მოწყობილობაზე? ელ. გვერდი: ნანახია 07.07.2019

⁴³⁰ იქვე.

⁴³¹ როგორ გადავიღოთ ეკრანის სურათი (სკრინშოტი) ანდროიდ მოწყობილობაზე ელ. გვერდი: ნანახია 07.07.2019

„ზოგიერთი ანდროიდ პლანშეტებისა და სმარტფონების მწარმოებელი კომპანია ინტერფეისში ამატებენ თავიანთ მეთოდებს სკრინშოტების შესაქმნელად. როგორიცაა Galaxy Note, სადაც სკრინშოტის შექმნა შესაძლებელია ციფრული კალმით ე.წ. S Pen-ით.“⁴³²

„სამსუენის პლანშეტებზე შეგიძლიათ ნახოთ ვირტუალური ლილაკი სკრინშოტების შესაქმნელად რომელიც მდებარეობს ნავიგაციის პანელზე.“⁴³³

„HTC-ის მოწყობილობებზე ეკრანის სურათის გადაღება შესაძლებელია ჩართვის ლილაკსა და "home" (მთავარ გვერდზე გადასასვლელ) სენსორულ ლილაკზე ერთდროულად დაჭერით.“⁴³⁴

„Sony Xperia-ზე კი შესაძლებელია როგორც ჩართვის ლილაკზე დიდხანს დაჭერით გამოსული მენიუდან, ასევე ჩართვის ლილაკსა და ხმის შემცირების ლილაკებზე ერთდროულად დაჭერით.“⁴³⁵

„LG-ზე გარდა კომბინაციის ჩართვის ლილაკს + ხმის შემცირების ლილაკი, ასევე სკრინშოტის გაკეთება შესაძლებელია ჩანაწერების გასაქმებელი პროგრამით Quick Memo.“⁴³⁶



„Galaxy Nexus, Nexus 4, Nexus 7 და Nexus 10-ზე ტრადიციული მეთოდით ჩართვის ლილაკსა და ხმის შემცირების ლილაკებზე ერთდროულად დაჭერით.“⁴³⁸

„ასევე ზოგიერთ მოწყობილობაზე სკრინშოტის გადაღება შესაძლებელია ტელეფონის ეკრანზე ხელის გადასმით მარჯვნიდან მარცხნივ. უბრალოდ ეს ფუნქცია უნდა გააქტიურდეს „სეთინგებიდან“ Settings ==> Motions and gestures ==> Palm motion.“⁴³⁹ (იხილეთ სურათი N114);

432 იქვე.

433 იქვე.

434 იქვე.

435 იქვე.

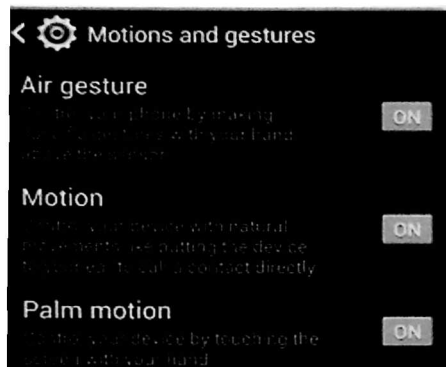
436 იქვე.

437 როგორ გადავიღოთ ეკრანის სურათი (სკრინშოტი) ანდროიდ მოწყობილობაზე?ელ. გვერდი: ნანახია 07.07.2019



438 იქვე.

439 იქვე.



უფრო დეტალურად რომ მიმოვიხილოთ აღნიშნული, წარმოდგენთ შემდეგს:

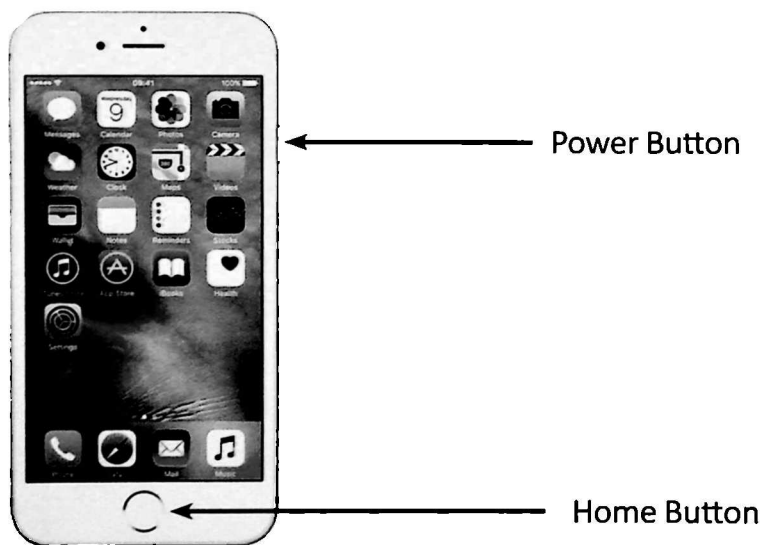
(კლავიატურის კომბინაციები არებულია ელ. გვერდიდან , ხოლო ფოტოები ინტერნეტიდან.)

1. ეკრანზე ფოტოს გადაღება iOS-ზე:

iPhone — power and home;

iPad — power and home;

სურათი N115:



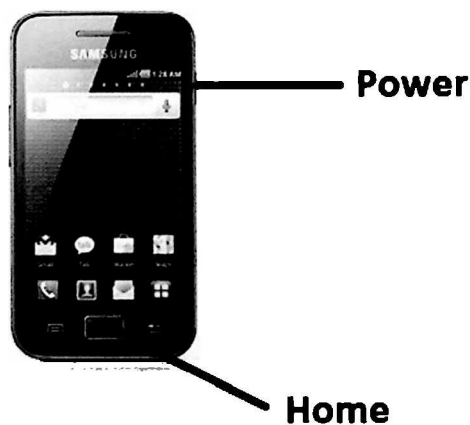
როგორ გადავიღოთ ეკრანის სურათი (სკრინშოტი) ანდროიდ მოწყობილობაზე? გვერდი: ნანახია 07.07.2019



2. ეკრანზე ფოტოს გადაღება ANDROID-ზე;

Samsung — power and home;

სურათი N116:

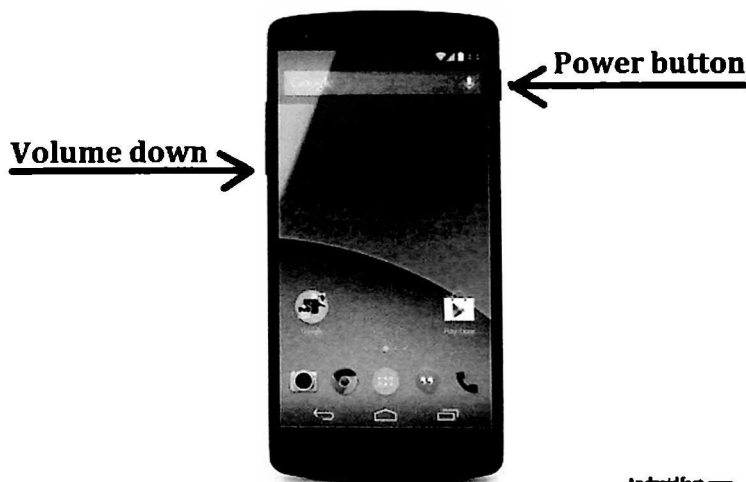


LG — power and volume down;

HTC — power and volume down;

Nexus — power and volume down;

სურათი N117:

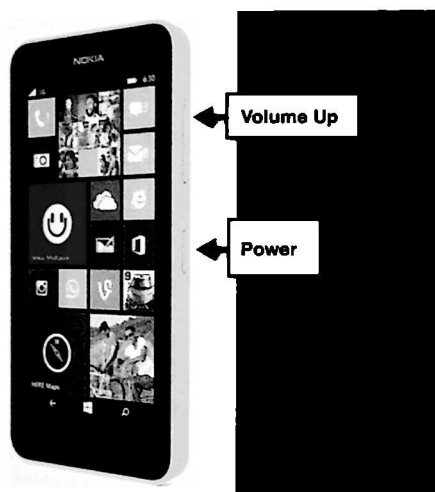


Androidfact.com

3. ეკრანზე ფოტოს გადაღება WINDOWS PHONE ზე;

Lumia — power and volume up;

სურათი N118:



4. ეკრანზე ფოტოს გადაღება BLACKBERRY 10-ზე;

press both the Volume Up and Volume Down keys.

მას შემდეგ რაც გადაღებულ იქნება შესაბამისი ფოტოები საგამოძიებო მოქმედების მიმდინარეობისას, აღნიშნული უნდა სახით საგამოძიებო მოქმედების ოქმში, ასევე მობილური ტელეფონი უნდა შეაერთოთ შესაბამისი კაბელით პერსონალურ კომპიუტერზე, რის შედეგადაც კომპიუტერში ძებნა ღილაკით იპოვით პაპკას Computer ან My Computer, სადაც იქნება მობილური ტელეფონის პატარა სურათი, მაგალითად მსგავსი ი. სურათზე N119:

სურათი N119:

► Portable Devices (1)



მსგავსი
Portable Media Player



რის შემდეგაც კომპიუტერიდან შევალთ მობილური ტელეფონის მენიუში, თუ მობილური ტელეფონის მენიუში ვერ შეხვალთ კომპიუტერიდან, მაშინ ნახეთ ხომარ ითხოვს მობილური ტელეფონი ნებართვას, რათა კომპიუტერს დაუკავშირდეს, და მიეცით თანხმობა. შემდგომ მოვძებნით პაპკას, სადაც ინახება ფოტოსურათები და გადმოვწერთ ჩვენთვის საჭირო და სასურველ ფოტოსურათს ელექტრონულ დისკზე.

ვიდეოს გადაღება მობილური ტელეფონის ეკრანზე

შეგვიძლია ასევე მობილურ ტელეფონის ეკრანს გადავუღოთ ვიდეოც როდესაც მასზე საგამოძიებო მოქმედებას ვაწარმოებთ, მაგალითად ვასდენთ მობილურ ტელეფონში არსებული მოკლეთქესტური შეტყობინებების დავალიერებას ან გამოთხოვას.

პირველ რიგში უნდა ითქვას, რომ მობილურ ტელეფონებში პრაქტიკაში ძირითადად გვხვდება Android სისტემა, რომელიც არის **Linux**-ზე დაფუძნებული **ოპერაციული სისტემა**, მუშაობს სმარტფონებზე, ტელევიზორებზე, საათებზე, მანქანებზე და პლანშეტურ კომპიუტერებზე. შეიქმნა Google-ის ფინანსური მხარდაჭერით, ხოლო **2005** წელს ის თავად გუგლმა შეისყიდა. ანდროიდის სისტემაზე მომუშავე პირველი ტელეფონი იყო **HTC Dream**, რომელიც **2008** წლის ოქტომბერში გამოვიდა გაყიდვაში. დღეს ანდროიდის ყველა აპლიკაცია თავმოყრილია **Google Play**-ზე. **2017** წელს აპლიკაციების რაოდენობა **2,7** მილიონი იყო. დღეისათვის ანდროიდი ყველაზე ფართოდ გავრცელებული ოპერაციული სისტემაა მთელ მსოფლიოში. **2015** წელს მისი საბაზრო წილი **84,7 %** იყო. **2017** წლის მაისის მონაცემით ამ ოპერაციულ სისტემას ყოველთვიურად ჰყავდა **2** მილიარდი აქტიური მომხმარებელი. დღეს ანდროიდის სისტემაზე მომუშავე ელექტრო მოწყობილობებს ქმნის რამდენიმე ცნობილი კომპანია: **HTC, სამსუნგი, Google Nexus, სონი, ჰუავეი** და ა.შ.

ხოლო **iPhone** - ს ფირმის მობილური ტელეფონები მუშაობს **Os** სისტემაზე. განვიხილოთ მობილურის ეკრანის ვიდეოგადაღების წარმოება **Android** სისტემის მქონე მობილურ ტელეფონებზე;

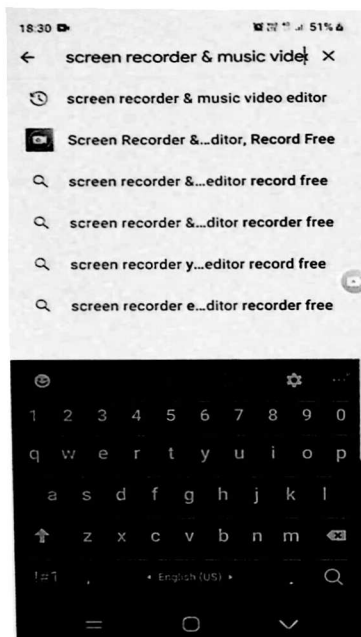
პირველ რიგში მობილური ტელეფონის მენიუში ვნახულობთ ხომარ აქვს მობილურ ტელეფონის მესაკუთრეს გადმოწერილი მასზე უკვე ვიდეოს ჩაშვური სისტემა, ვეძებთ შემდეგ დასახელებას: **Screen recorder**, თუ მსგავსი დასახელების პროგრამა ნაპოვნია ვერ იქნა უნდა შევიდეთ **Play Market** —ში (იხილეთ სურათი **N120**):

სურათი **N120**;



როდესაც შევალთ აღნიშნულ მენიშეში, ძებნა ღილაკში ვუთითებთ - My screen recorder (იხილეთ სურათი N121);

სურათი N121;



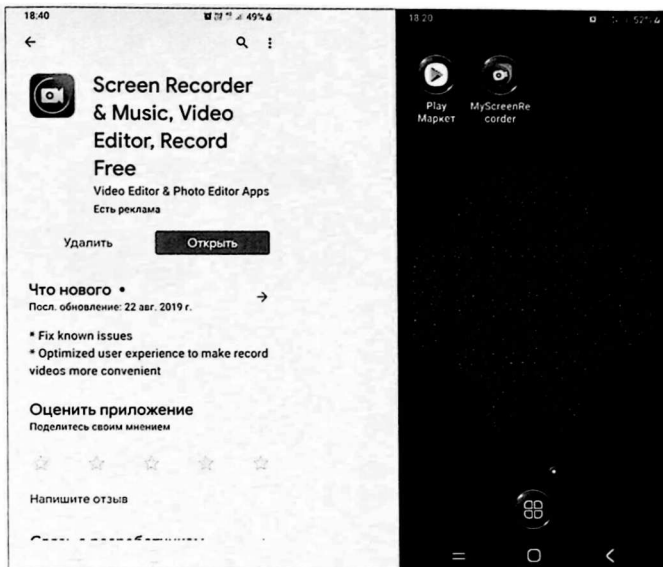
მას შემდეგ რაც აღნიშნული ფუნქციის პროგრამას ვიპოვით (შეგიძლიათ ისარგებლოთ რომელიმე პროგრამით, მათ შორის ფოტოზე მითითებულით), უნდა მოვახდინოთ მისი ინსტალაცია მობილურ ტელეფონზე, ამისათვის დავაწევებთ მწვანე ღილაკს და ვახდენთ პროგრამის გადმოწერას (იხილეთ სურათზე N122 და 123);

სურათი N122 და 123:



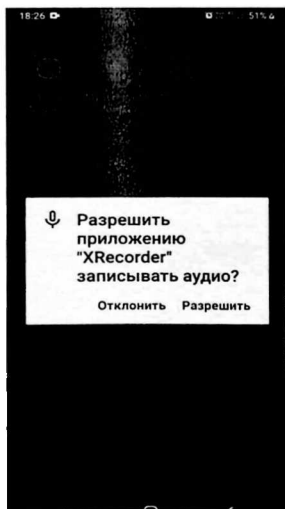
პროგრამის გადმოწერის შემდეგ, ან თავად პროგრამიდან ვხსნით აღნიშნულ პროგრამას ეკრანზე, ან მობილურ ტელეფონში ვნახულობთ შესაბამის ლოგოს წარჩერით MYscreen recorder (იხილეთ სურათი N124 და 125);

სურათები N124 და 125;



შემდეგ ვაძლევთ უფლებას პროგრამას რათა წვდომა განახორციელოს მობილურ ტელეფონზე მისი ფუნქციების შესრულების მიზნებისათვის (იხილეთ სურათი N126);

სურათი N126;



აღნიშნულის შემდგომ, ვიდეოკამერის მსგავს ლილაკზე ხელის დაჭერით გაიხსნება ლილაკები, რომლიდანაც წერტილისებრი ლილაკი ასრულებს ჩაწერის ფუნქციას, მას შემდეგ რაც დაჭერით აღნიშნულ ლილაკს, ტელეფონი დაიწყებს ავტომატურ ჩაწერას და ვიდეოს მსგავსი სურათის ადგილზე დაიწყებს წამშობი ათვლას, თუ თქვენ დაასრულებით საგამოძიებო მოქმედებას ოთკუთხედ ლილაკზე დაჭერით დასრულდება ვიდეოჩაწერაც, ჩანაწერი აკეთებს ხმის ჩაწერასაც (პროგრამის მეხუთე იხილეთ სურათზე N127 და 128)



მას შემდეგ რაც გადაღებულ იქნება შესაბამისი ვიდეო საგამოძიებო მოქმედების მიმდინარეობისას, აღნიშნული უნდა ასახოთ საგამოძიებო მოქმედების ოქმში, ასევე მობილური ტელეფონი უნდა შეაერთოთ შესაბამისი კაბელით პერსონალურ კომპიუტერზე, რის შედეგადაც კომპიუტერში ძებნა ლიდაკით იპოვით პაკკას Computer ან My Computer, სადაც იქნება მობილური ტელეფონის პატარა სურათი, მაგალითად მსგავსი იხილეთ სურათზე N129;

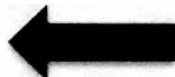
სურათი N129;

▲ Portable Devices (1)



სურათი N129

Portable Media Player



რის შემდეგაც კომპიუტერიდან შევალთ მობილური ტელეფონის მენიუში, თუ მობილური ტელეფონის მენიუში ვერ შევალთ კომპიუტერიდან, მაშინ ნახეთ ხომ არ ითხოვს მობილური ტელეფონი ნებართვას, რათა კომპიუტერს დაუკავშირდეს, და მიეცით თანხმობა. შემდგომ მოვძებნით საქაღალდეს, სადაც ინახება ვიდეოჩანაწერები და გადმოვწერთ ჩვენთვის საჭირო და სასურველ ვიდეოს ელექტრონულ დისკზე.

რაც შეეხება iPhone - ს ფირმის მობილური ტელეფონებს, აღნიშნულ ტელეფონებზე პროგრამის გადმოსაწერად უნდა ვიპოვოთ app store პაპკა (იხილეთ სურათზე N130), სადაც შევალთ და ვნახავთ მსგავსი ტიპის პროგრამას (ნახეთ ფოტო), რომელსაც ასევე გადმოვწერთ, დავაინსტალირებთ და გამოვიყენებთ.

სურათი N130;



7.4 კომპიუტერის IP მისამართის დადგენის ტექნიკური პროცედურები და მეთოდები

„IP-მისამართი წარმოადგენს მისამართების ძირითად ტიპს, რომლის საფუძველზეც ქსელური დონე აგზავნის პაკეტებს ქსელებს შორის. ეს მისამართები შედგება 4 ბაიტისგან, მაგ. 109.26.17.100. IP-მისამართი განისაზღვრება ადმინისტრატორის მიერ კომპიუტერისა და მარშრუტიზატორების კონფიგურაციისას. IP-მისამართი შედგება ორი ნაწილისგან: ქსელის ნომრისა და კვანძის ნომრისაგან. ქსელის ნომერი შეიარჩევა ადმინისტრატორის მიერ ნებისმიერი ან Internet-ის (Internet Network Information Center, InterNIC) სპეციალური ქვეგანყოფილების რეკომენდაციების მიხედვით, თუ ქსელმა უნდა იმუშაოს, როგორც ინტერნეტ-ის შემადგენელმა ნაწილმა. Internet-ის სერვისების მიმწოდებლები ჩვეულებრივ მისამართების დიაპაზონს იღებენ InterNIC-გან და შემდგომ ანაწილებენ თავიანთ აბონენტებს შორის. მარშრუტიზატორი განსაზღვრების თანახმად შედის რამოდენიმე ქსელში და ამიტომაც მის ყოველ პორტს გააჩნია საკუთარი IP-მისამართი. საბოლოო კვანძი შეიძლება შედიოდეს რამოდენიმე IP-ქსელში. ამ შემთხვევაში კომპიუტერს უნდა გააჩნდეს რამოდენიმე IP-მისამართი ქსელური კავშირების რიცხვის მიხედვით. მაშასადამე, IP-მისამართით ხასიათდება არა ერთი ცალკეული კომპიუტერი ან მარშრუტიზატორი, არამედ ერთი ქსელური შეერთება.“⁴⁴¹

IP-მისამართის დანიშნულება;

„IP-მისამართი (აი-პი მისამართი, შემოკლ. ინგლ. Internet Protocol Address-ინტერნეტ ოქმის მისამართი) – ლოკალურ ქსელში ან ინტერნეტში ჩართული მოწყობილობის (როგორც წესი კომპიუტერის) უნიკალური იდენტიფიკატორია (მისამართია).“⁴⁴²

„IP-მისამართი წარმოადგენს 32-ბიტურ (IPv4 ვერსიით) ან 128-ბიტურ (IPv6 ვერსიით) ორნიშნა რიცხვს, რომელიც ჩაიწერება ოთხი ათობითი რიცხვის სახით (0-დან 255-მდე), დაყოფილს

441 ადრესაცია IP-ქსელებში TCP/IP სტეკის მისამართების ტიპები; ლექცია 8. ადრესაცია IP-ქსელებში; Posted November 1, 2010; ელ-გვერდი; ნანახია 06.07.2019

442 იქვე.

წერტილებით. მაგ., 192.168.0.1. (ან 128.10.2.30 – ათობითი ფორმა, ხოლო ამავე მისამართის ორობითი ფორმა – 10000000 00001010 00000010 00011110).“⁴⁴³

IP-მისამართის სტრუქტურა;

„ლოგიკური IP-მისამართი იერარქიულია და შედგება ორი ნაწილისაგან. პირველი განსაზღვრავს ქსელს, ხოლო მეორე ამავე ქსელის ჰოსტს. მაგ. თუ ჰოსტს აქვს 192.168.18.57 IP-მისამართი, მაშინ პირველი სამი ოქტეტი განსაზღვრავს ქსელს (192.168.18), ბოლო ოქტეტი კი ჰოსტს. ასეთ დამისამართებას წყოდება იერარქიული.“⁴⁴⁴

„IP მისამართები იყოფა 5 ჯგუფად. A, B და C კლასის მისამართები კომერციულია და გამოიყენება ჰოსტებისთვის. D კლასი დანიშნულია ფართომკუთხედობისთვის (Multicast), ხოლო E კლასი ექსპერიმენტებისათვის.“⁴⁴⁵

„A კლასის მისამართში მხოლოდ ერთი ოქტეტი განკუთვნილია ქსელისათვის, ხოლო დანარჩენი სამი ჰოსტისთვის. შესაბამისი Subnet მასკა არის 8 ბიტიანი (255.0.0.0). A კლასის მისამართები გამოიყენება დიდი ორგანიზაციებისათვის;

B კლასის მისამართებში 2 ოქტეტი განკუთვნილია ქსელის ნაწილისათვის, მეორე ორი კი ჰოსტებისთვის. შესაბამისი Subnet მასკა შეიცავს 16 ბიტს (255.255.0.0). B კლასის მისამართები გამოიყენება საშუალო მაშტაბის ქსელებისათვის;

C კლასის მისამართებს გააჩნია 3 ოქტეტი ქსელის ნაწილისათვის, ხოლო ერთი ჰოსტისთვის. ხოლო შესაბამისი Subnet მასკა შეიცავს 24 ბიტს (255.255.255.0). C კლასის მისამართები გამოიყენება მცირე მაშტაბის ქსელებისათვის;

IP მისამართის კლასი განისაზღვრება პირველი ოქტეტის მნიშვნელობით. მაგ. თუ IP მისამართის პირველი ოქტეტის მნიშვნელობა ხვდება 192-223 დიაპაზონში, მაშინ ის მიეკუთვნება C კლასის მისამართს. მაგ. 200.14.193.67 C კლასის მისამართია.“⁴⁴⁶

ხშირად გვხვდება ხოლმე დანაშაულები, რომლებიც ჩადენილია კონკრეტული კომპიუტერის გამოყენებით და საჭიროა მოვიპოვოთ აღნიშნული კომპიუტერის აიპი მისამართის გამოყენებით განხორციელებული ქმედებები.

განვიხილოთ რამდენიმე სამართლებრივი კაზუსი;

შემთხვევა პირველი: დაუდგენელია დანაშაულის ჩამდენი პირი და კომპიუტერი, საიდანაცინაა დანაშაული ჩადენილი;

მაგალითი: დაუდგენელმა პირმა, ასევე დაუდგენელი კომპიუტერის გამოყენებით უნებართვოდ შეაღწია დაზარალებულ გიორგის საბანკო ანგარიშზე, საიდანაც ფულადი თანხა გადარიცხა „ონლაინ ენოვლიზატორში“.

იმისათვის, რომ გამოძიებამ დაადგინოს თუ რა ქმედებები განახორციელა დაუდგენელმა პირმა კონკრეტული კომპიუტერის გამოყენებით, ინფორმაციის გამოთხოვა უნდა მოახდინოს როგორც იმ ბანკიდან საიდანაც მოხდა ფულადი თანხის გადარიცხვა, ასევე იმ იურიდიული თუ ფიზიკური პირიდან სადაც მოხდა ფულადი თანხის გადარიცხვა და მოთხოვნის მთავარი რეკვიზიტი უნდა იყოს IP მისამართი იმ კომპიუტერის თუ საიდან მოხდა კომპიუტერული ქმედებების განხორციელება.

მას შემდეგ რაც გამოძიებამ უკვე იცის კონკრეტული IP მისამართი, დასადგენია თუ რომელ

⁴⁴³ ადრესაცია IP-ქსელებში TCP/IP სექციის მისამართების ტიპები; ლექცია 8. ადრესაცია IP-ქსელებში; Posted November 1, 2010; ელ-გვერდი: 

⁴⁴⁴ იქვე.

⁴⁴⁵ იქვე.

⁴⁴⁶ იქვე.

ინტერნეტ პროვაიდერს განეკუთვნება აღნიშნული IP მისამართი, რის შემდეგაც კონკრეტული ინტერნეტ პროვაიდერისაგან გამოძიება გამოითხოვს ინფორმაციას - ვისი კუთვნილებაა აღნიშნული IP მისამართის მქონე კომპიუტერი (კომპიუტერის ქსელი) და რა მისამართზე არის ის განთავსებული.

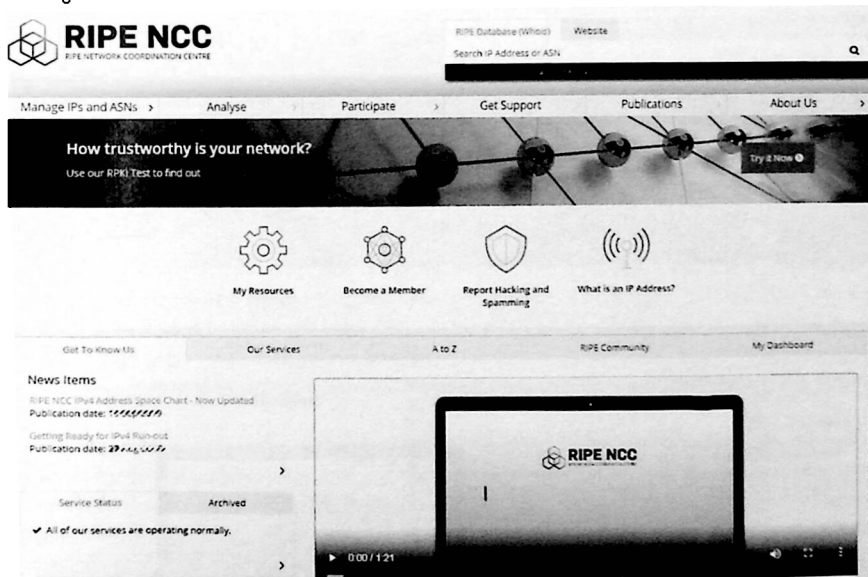
ინტერნეტ გვერდის - <http://caucasusoffline.com/isp/> - ის მონაცემებით, საქართველოში რეგისტრირებული არის 185 ინტერნეტ პროვაიდერი, თითოეულ ინტერნეტ პროვაიდერს გააჩნია თავისი ID, (დანართი N11-ში იხილეთ საქართველოში რეგისტრირებული ინტერნეტ პროვაიდერების ჩამონათვალი (მონაცემი აღებულია ელექტრონული გვერდიდან <http://caucasusoffline.com/isp/>))

იმისათვის, რომ გამოძიებელმა თითოეულ ინტერნეტ პროვაიდერს ინდივიდუალურად არ მიმართოს ინფორმაციის გამოთხოვით, უნდა დაადგინოს თუ რომელ პროვაიდერს განეკუთვნება კონკრეტული IP მისამართი, ამისათვის გამოძიებელმა უნდა იცოდეს ინტერნეტ საიტის მისამართი, რომლის საშუალებითაც გაიგებს თუ რომელ ინტერნეტ პროვაიდერს განეკუთვნება კონკრეტული IP მისამართი, ხოლო შემდეგ შუამდგომლობით მიმართავს სასამართლოს, რათა მითითებული ინტერნეტ პროვაიდერისაგან გამოითხოვოს ინფორმაცია კონკრეტული IP მისამართის მქონე კომპიუტერის მესაკუთრის, ადგილმდებარეობის შესახებ.

როდესაც ვიცით კომპიუტერის IP მისამართი და გვსურს დავადგინოთ მისი ინტერნეტ პროვაიდერი, ამისათვის გამოძიებელს შეუძლია ისარგებლოს საერთაშორისო ინტერნეტ საიტი <https://www.npe.net/>, კერძოდ:

ნაბიჯი 1: უნდა განახორციელოს საგამოძიებო მოქმედება ელექტრონული საიტის დათვალიერება, რომლის დროსაც შევიდეს ზემოაღნიშნულ საიტზე <https://www.npe.net/>, როდესაც გამოძიებელი საიტი შევა მას დახვდება შემდეგი გვერდი (იხ. სურათი 131):

სურათი N131:



ნაბიჯი 2: შემდგომ ვწერთ IP მისამართს მითითებულ ველში (იხ. სურათი 132):

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RIPE Database (Whois) Website
123.123.123
Your IP address is

Manage IPs and ASNs > Analyse > Participate > Get Support > Publications > About Us >

How trustworthy is your network?
Use our RPKI Test to find out

Try it Now

My Resources Become a Member Report Hacking and Spamming What is an IP Address?

Get To Know Us Our Services A to Z RIPE Community My Dashboard

News items

RIPE NCC IPv4 Address Space Chart - Now Updated
Publication date: *****

Getting Ready for IPv6 Run-out
Publication date: *****

Service Status: Archived

✓ All of our services are operating normally.

0:00 / 1:21

ნაბიჯი 3: მესხის ისრით უნდა დააწვეს ძეგნა ღილაკს, რომელსაც ლუპის ფორმა აქვს (ის. სურათი N133)

სურათი N133:

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RIPE Database (Whois) Website
123.123.123
Your IP address is

Manage IPs and ASNs > Analyse > Participate > Get Support > Publications > About Us >

How trustworthy is your network?
Use our RPKI Test to find out

Try it Now

My Resources Become a Member Report Hacking and Spamming What is an IP Address?

Get To Know Us Our Services A to Z RIPE Community My Dashboard

News items

RIPE NCC IPv4 Address Space Chart - Now Updated
Publication date: *****

Getting Ready for IPv6 Run-out
Publication date: *****

Service Status: Archived

✓ All of our services are operating normally.

0:00 / 1:21

ნახიჯი 4: მას შემდეგ რაც პროგრამა მოძებნის მითითებულ IP მისამართს, გამოძიებულს ეკრანზე გამოუჩნდება შემდეგი სახის ინფორმაცია (იხ. სურათი N134):

სურათი N134:

Search results

This is the RIPE Database search service. The objects are in RPSL format.
The RIPE Database is subject to Terms and Conditions.

Responsible organisation: AS13335
Abuse contact info: [redacted]

inetnum:
netname:
descr:
country:
admin-c:
tech-c:
status:
mnt-by:
mnt-by:
created:
last-modified:
source:

Login to update RIPEstat

route:
descr:
origin:
mnt-routes:
mnt-by:
created:
last-modified:
source:

Login to update RIPEstat

RIPE Database Software Version 1.95.1

ნახიჯი 5: აღნიშნული სურათიდან ჩვენ მივიღებთ ინფორმაციას ინტერნეტ პროვაიდერის შესახებ, რის შემდეგაც გამოძიებლის მიერ დათვალიერების ოქმში შეტანილ უნდა იქნეს აღნიშნული ინფორმაცია.

ნახიჯი 6: საგამოძიებო მოქმედების შემდეგ, პროკურორს ექნება შესაძლებლობა მიმართოს სასამართლოს აღნიშნული ინტერნეტ პროვაიდერიდან, მითითებული IP მისამართის მქონე კომპიუტერის შესახებ საქმისათვის საჭირო ინფორმაციის გამოთხოვის შესახებ, პროკურორის მიერ გამოთხოვილ უნდა იქნეს შემდეგი ინფორმაცია IP მისამართის მქონე კომპიუტერის მფლობელის დემოგრაფიული მონაცემების, მისამართის მითითებით და განხორციელებული ოპერაციების შესახებ.

შუამდგომლობის დაყენებისას, გასათვალისწინებელია, რომ კომპიუტერულ სისტემაში უნებართვო შეღწევის მცდელობის ფაქტის გამოძიებისას „[...] ბრალდების მხარე უთითებს კონკრეტულ IP მისამართზე, რომლიდანაც განხორციელდა უნებართვო შეღწევის მცდელობა და რომელიც რეგისტრირებულია ბინის მესაკუთრის სახელზე, თუმცა რამდენად პასუხობს ამ მისამართის მითითება განჩინებაში დეტალიზაციის მოთხოვნას, ერთობ სადავოა, განსაკუთრებით, თუ საქმე გვაქვს ე.წ. უკაბელო ინტერნეტთან, რომელიც არ არის დაცული პაროლით და, შესაბამისად, მისდამი წვდომა შეიძლება ჰქონდეს ნებისმიერ პირს და კომპიუტერულ მოწყობილობასა თუ

ე.წ. სმარტფონებს. მსგავსი ფორმულირება, ერთი მხრივ, შესაძლებლობას იძლევა, ამოღებულ იქნეს ჩხრეკის ადგილას აღმოჩენილი ყველა კომპიუტერი და მობილური, ხოლო, მეორე მხრივ, ფართომასშტაბიანი ამოღების შესაძლებლობის მიუხედავად, საქმისათვის მნიშვნელოვანი ინფორმაციის მატარებლების ამოღების შესაფერის საშუალებად არ გამოდგება. მით უმეტეს, როდესაც ჩხრეკაზე ნებართვის გაცემისას სასამართლოს განჩინებაში საერთოდ არ გვხვდება რაიმე სახის მითითება ჩხრეკისას დასაძებნი და ამოსაღები ინფორმაციის მატარებლების შესახებ და იფარგლება მხოლოდ წინადადებით:⁴⁴⁷ „შუამდგომლობა დაკმაყოფილდეს – ჩატარდეს ქ. თბილისში ... მდებარე ბინის ჩხრეკა (თბილისის საქალაქო სასამართლოს 2012 წლის 31 ივლისის განჩინება ჩასატარებლად ნებართვის გაცემის შესახებ საქმეზე – № 086300712002)“.⁴⁴⁸

სისხლის სამართლის კოდექსის 197-ე მუხლის პირველი ნაწილით გათვალისწინებული დანაშაულის გამოძიების ფაქტზე თბილისის საქალაქო სასამართლომ ბრალდების მხარეს, საბუღალტრო-საანგარიშსწორებო დოკუმენტაციის ამოღებასთან ერთად, 136-ე მუხლზე დაყრდნობით უფლება მიანიჭა: „2. გამოითხოვონ კომპიუტერის პროცესორიდან, დისკებიდან, ფლეშ-ბარათებიდან და კომპიუტერულ მონაცემთა შესანახი საშუალებებიდან, ამავე პერიოდის კომპანიის საქმიანობასთან დაკავშირებული ელექტრონული ინფორმაცია“ (თბილისის საქალაქო სასამართლოს 2014 წლის 21 ივნისის განჩინება N11ა/4554-14 საგამოძიებო მოქმედების ჩასატარებლად ნებართვის გაცემის შესახებ). ამ შემთხვევაში, ერთი მხრივ, ხდება გამოსათხოვი ინფორმაციის კატეგორიის ზოგადად მითითება (მხოლოდ ის ინფორმაცია, რომელიც ეკავშირდება ნიის საქმიანობას), თუმცა ამ შემთხვევაშიც მოთხოვნილი ინფორმაცია ეხება კომპანიის რეგისტრაციიდან რეორგანიზაციამდე პერიოდში საქმიანობასთან დაკავშირებულ სრულ დოკუმენტაციას. ამ შემთხვევაში: 1. არ ხდება კომპიუტერისა და შესაბამისი პროცესორის რაიმე სახით განსაზღვრა, რის გამოც გაუგებარია, ოდესში რამდენიმე კომპიუტერის არსებობის შემთხვევაში, კონკრეტულად რომელი კომპიუტერიდან უნდა მოხდეს აღნიშნული ინფორმაციის გამოთხოვა. შესაბამისად, ამ შემთხვევაში განხორციელდება კომპანიაში არსებული ყველა კომპიუტერიდან შესაბამისი ინფორმაციის ამოღება; 2. გამოთხოვილი ინფორმაციის შეზღუდვა ხდება მხოლოდ დროითი პერიოდით, მაგრამ არა საქმიანობის კონკრეტული სახის/სფეროს მითითებით.“⁴⁴⁹

„შუამდგომლობაში მკაფიოდ უნდა იყოს მითითებული არა მხოლოდ იმ როლის შესახებ, რომელსაც ამოსაღები ციფრული მატარებლები და მოწყობილობები ასრულებენ, არამედ ასევე ნებისმიერი გონივრული როლის შესახებ, რომლის შესრულებაც მათ შეეძლოთ დანაშაულის ჩადენასთან დაკავშირებით. როდესაც კომპიუტერი არის დანაშაულის ჩადენის იარაღი, გამოძიების ორგანოებს უფრო ფართომასშტაბიანი ჩხრეკის ჩატარების შესაძლებლობა ეძლევათ, ვიდრე იმ შემთხვევაში, როდესაც ელექტრონული მოწყობილობა შეიძლება მხოლოდ ინახავდეს დანაშაულის ჩადენის მამხილებელ მტკიცებულებას.“⁴⁵⁰

როდესაც განჩინების გამტარება ხდება იმ ეჭვის საფუძველზე, რომ ხორციელდება დანაშაულებრივი საქმიანობა, როგორც წესი, არ ხდება ამოსაღები მტკიცებულებების კონკრეტიზაცია. მითითება ხდება მხოლოდ ამოსაღები ობიექტების კატეგორიაზე, თუმცა ამ შემთხვევაშიც მოითხოვება დეტალიზაციის გარკვეული ხარისხი.⁴⁵¹

⁴⁴⁷ ლალი ფაფიაშვილი. სტატია: ციფრული მტკიცებულების ამოღება: პირადი ცხოვრების ხელშეუხებლობის საკმარისი თუ ილუზორული გარანტია? სტატიათა კრებული, ადამიანის უფლებათა დაცვა და სამართლებრივი რეფორმა საქართველოში. თბილისი, 2014, გვ. 143-144

⁴⁴⁸ იქვე- გვ. 143-144

⁴⁴⁹ ლალი ფაფიაშვილი. სტატია: ციფრული მტკიცებულების ამოღება: პირადი ცხოვრების ხელშეუხებლობის საკმარისი თუ ილუზორული გარანტია? სტატიათა კრებული, ადამიანის უფლებათა დაცვა და სამართლებრივი რეფორმა საქართველოში. თბილისი, 2014, გვ. 143-144

⁴⁵⁰ იქვე- გვ. 144

⁴⁵¹ იქვე- გვ. 145

მართალია, ზედმეწეწებით სიზუსტით ამოსაღები ობიექტების მითითება ყოველთვის არ არის შესაძლებელი, საქმის სპეციფიკიდან გამომდინარე, თუმცა პრაქტიკა, რომლის თანახმად, არ ხდება ამოსაღები ობიექტების კონკრეტიზაცია, რათა თავიდან იქნეს აცილებული ჩხრეკისას აღმოჩენილი საქმისათვის მნიშვნელობის მქონე ისეთი მტკიცებულების ამოღება, რომელიც პირდაპირ არ არის მითითებული განჩინებაში, არასწორია.⁴⁵²

ნახაზი 7: მას შემდეგ რაც მიღებულ იქნება შესაბამისი განჩინება გამომძიებელმა უნდა აწარმოოს საგამოძიებო მოქმედება ინფორმაციის გამოთხოვა კომპიუტერიდან, რის შესახებაც უნდა შედგეს საგამოძიებო მოქმედების ინფორმაციის გამოთხოვის ოქმი.

ამჟერად განვიხილოთ საკითხი, თუ როგორ უნდა გაიგოს გამომძიებელმა კომპიუტერის IP მისამართი, როდესაც ათვალერებს კონკრეტულ კომპიუტერს რომლის IP მისამართის დადგენაც სურს:

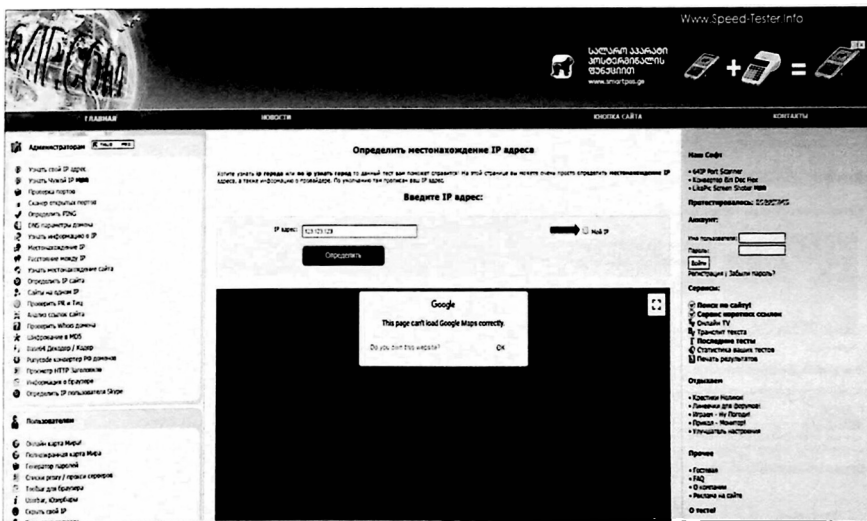
მაგალითად: გამომძიებელი ათვალერებს კომპიუტერს, საიდანაც სოციალურ ქსელში მიწერილი არის შეტყობინება, რომელიც შეიცავს შესაძლო დანაშაულის ნიშნებს, გამომძიებელს სურს შემდგომი გამოძიების წარმოების მიზნით გაიგოს აღნიშნული კომპიუტერის მისამართი, ამისათვის არსებობს რამდენიმე ელექტრონული საიტი;

http://speed-tester.info/ip_location.php (იხილეთ სურათი N135)

<http://ip-whois.net/> (იხილეთ სურათი N136 და N137)

მას შემდეგ, რაც გამომძიებელი შევა აღნიშნულ მისამართებზე, დაეწერება კომპიუტერის IP, ცდომილების გამოსარიცხად, მიზანშეწონილია გადამოწმებული იქნეს ორივე მისამართზე.

სურათი N135:



IP-whois.net

Скрыть рекламу:

Не интересуюсь этой темой

Товар куплен или услуга найдена

Нарушает закон или права

Имеет проблему контента

Скрыть рекламу:

Не интересуюсь этой темой

Товар куплен или услуга найдена

Нарушает закон или права

Имеет проблему контента

Может так случиться, что в какой-либо момент вы спросите: каков мой IP? Вам может понадобиться узнать основные данные о вашем теле соединения: узнать IP или проверить IP, проверить WHOIS домена, получить информацию о географическом положении вашего или любого IP адреса, узнать IP адрес любого сайта, проверить ТИЦ и PR (PR) сайта, узнать по IP или хоста. Также можете узнать местоположение по айпи.

В получении всей вышеперечисленной информации, Вам поможет наш сервис.

На нашем сайте Вы найдете все необходимые инструменты, которые помогут узнать нужную Вам информацию, с помощью которых вы обязательно сможете узнать свои IP (айпи), проверить whois и проверить ТИЦ (Тематический индекс цитирования PC Яндекс) и PR (PR) (Google Page Rank или PR).

Кроме того, вы сможете прочесть интересные статьи по теме Интернет, найти весьма интересную дополнительную информацию, которая откроет для вас все тайны взаимодействия в сети, и все особенности протекания сетевых процессов.

Анализ сайта. Также сможете проанализировать любой Интернет сайт на склейку, наличие в Яндекс каталоге (ЯН) / DMOZ каталоге и другие.

Также наш сервис предоставит точную проверку скорости интернета и конструктор обратных ссылок для вашего сайта.

Заработать в Сети

Что такое OpenNet

Что такое склейка

IP телефония

Что такое домены

Как зарабатывать студента

Заработать в Интернете

Что такое склейка

Что такое VPS и VDS

Что такое PR и TИЦ

Что такое Firewall

Конструкция рекламы

Что такое whois?

Что такое IP?

Спутниковый Интернет

Что такое PR и TИЦ

Как зарегистрировать домен?

Заработок в Интернете

Главная

Ваш IP адрес

Информация о IP

Проверить whois домена

Узнать по IP или хоста

Узнать IP адрес сайта

Проверить ТИЦ и PR сайта

Узнать сайты на одном IP

Анализ сайта

Тест скорости интернета

Интернет провайдеры - отзывы

Форма обратной связи для сайта

Дешевые VDS/VPS сервера

Мгновенная активация! 10%

Безлимитный трафик! Гарантированные ресурсы. Безопасное соединение. Windows/Linux

IP-whois.net

Ваш IP: 192.168.1.1

Получите полную информацию по айпи: географическое местоположение, whois ф и т.д. → 192.168.1.1

Аренда VDS/VPS серверов

Мгновенная активация! 10%

Безлимитный трафик! Гарантированные ресурсы. Безопасное соединение. Windows/Linux

VDS/VPS Облачные. Высокпроизводительные. Оптимизированные. Бюджетные

IP индикатор для вашего web сайта!

Скопируйте код из формы и установите на вашем сайте: ваши пользователи смогут видеть свой IP!

Ваш IP: 192.168.1.1

```

<script language=JavaScript>function show_ipwhoisdd(){var obj =
document.getElementById("show_ipwhoisdd");if (obj.style.display

```

Большая коллекция скриптов IP адресов для вашего сайта

Главная

Ваш IP адрес

Информация о IP

Проверить whois домена

Узнать по IP или хоста

Узнать IP адрес сайта

Проверить ТИЦ и PR сайта

Узнать сайты на одном IP

Анализ сайта

Тест скорости интернета

Интернет провайдеры - отзывы

Форма обратной связи для сайта

SIEMENS

Integrating the Life

New Innovations for Protection & Digital Substations

Watch part one >

თავი VIII

გამომძიებლის მიერ წარმოებული ციფრული ვიდეო და ფოტო გადაღების ტექნიკა და მეთოდика

8.1. ციფრული ვიდეო და ფოტო გადაღების ტექნიკური პროცედურები და მეთოდები

პრაქტიკაში, როდესაც მიმდინარეობს საგამომძიებო მოქმედება ინფორმაციის გამოთხოვა, ჩარევა, ამოღება ან დათვალიერება, პირის ამოცნობა თუ სხვა, არის შემთხვევები, როდესაც გამომძიებელი აუდიო/ვიდეო გადაღებას აწარმოებს თავად და არ ან დროის სიმცირიდან ან სხვა ობიექტური გარემოებიდან გამომდინარე, ვერ ახდენს ექსპერტის გამოძახებას. ასეთ შემთხვევაში, აუცილებელია გამომძიებელმა იცოდეს თუ როგორ უნდა მოახდინოს ციფრული მტკიცებულების შექმნა და მოპოვება შესაბამისი ტექნიკური საშუალებების გამოყენებით. ვინაიდან ყოფილა შემთხვევები პრაქტიკაში, როდესაც გამომძიებლის მიერ საგამომძიებო მოქმედების მიმდინარეობისას, მაგალითისათვის - საგამომძიებო ექსპერიმენტის მიმდინარეობისას წარმოებული ვიდეო გადაღება, ან ფოტომასალა, იმდენად უხარისხო ყოფილა, რომ მოსამართლეს უცვნია დაუშვებელ მტკიცებულებად, სწორედ ამიტომ არის აუცილებელი გამოძიების ჩამტარებელ პირს ჰქონდეს ბაზისური ცოდნა, რათა სწორად აწარმოოს ციფრული მტკიცებულების მოპოვება. ვინაიდან ვიდეო ან აუციო ჩანაწერი, რომელსაც მოიპოვებს გამომძიებელი, გახლავთ ციფრული მტკიცებულების ერთ-ერთი მნიშვნელოვანი სახეობა.

ციფრული მტკიცებულების ერთ-ერთი სახეა ის ვიდეოჩანაწერი, რომელსაც გამომძიებელი აწარმოებს საგამომძიებო მოქმედების მიმდინარეობისას, იმისათვის რომ აღნიშნული სახის ციფრული მტკიცებულება შეიქმნას და მას სრულყოფილი სახე ჰქონდეს, გამომძიებელმა უნდა იცოდეს რამდენიმე გარემოება:

რა ტექნიკური საშუალებები არსებობს ვიდეოს გადასაღებად?

„ვიდეოს გადასაღებად რამდენიმე საშუალება არსებობს. გაქვთ ციფრული ფოტოაპარატი? სავარაუდოდ მას ვიდეოს გადაღების ფუნქცია აქვს! მაგრამ, თუ ვიდეოკამერა გაქვთ, კიდევ უკეთესი! არ არის აუცილებელი იგი პროფესიონალური იყოს. მთავარია, ამბავი გადაიღოთ! ნაკლებად მნიშვნელოვანია, ტექნიკურად რა გზას აირჩევთ ამისათვის. გამოსავალი მაშინაც არსებობს, როცა არც ვიდეოკამერა გაქვთ და არც ციფრული ფოტოაპარატი. ამ შემთხვევაში შეგიძლიათ მობილური ტელეფონი გამოიყენოთ. თითქმის ყველა თანამედროვე მობილურ აპარატს აქვს ვიდეოსა და ფოტოს გადაღების ფუნქცია. მოდით, დეტალურად განვიხილოთ რა დადებითი და უარყოფითი მხარეები აქვს თითოეულს. ვიდეოგრაფი - ადამიანი, რომელიც იღებს მოძრავ გამოსახულებას - ვიდეოს“⁴⁵³.

⁴⁵³ ავტორთა კოლექტივი. ვიდეო ადვოკატირება (აქტიური მოქალაქის სახელმძღვანელო) ელ. გვერდი: ნანახია 07.07.2019.



ციფრული ფოტოაპარატი;

სერათი N138:



„ციფრულ ფოტოაპარატს ის უპირატესობა აქვს, რომ ის მცირე ზომისაა და ადვილია ყოველთვის თან იქონიოთ (ვინ იცის, რისი მოწმე გახდებით და რის გადაღებას გადაწყვეტთ!) [...]“. მაგრამ ციფრული ფოტოაპარატის უარყოფითი მხარეა დაბალი ხარისხის გამოსახულება. ასევე ის, რომ მას არ აქვს გარე მიკროფონის მიერთების შესაძლებლობა, რაც ძალიან მნიშვნელოვანია ხმის ჩასაწერად.⁴⁵⁴

ციფრული ვიდეოკამერა

სერათი N139:



„ციფრული ვიდეოკამერა ფოტოაპარატთან შედარებით [...]“⁴⁵⁵ „გარანტირებულია გამოსახულების ხარისხი და ხმის სისუფთავე. (ვიდეოკამერებს, ხშირ შემთხვევაში, გარე მიკროფონიც უერთდება), რადგანაც ვიდეოკამერა ფოტოაპარატზე უფრო ღირსა, თანაც აქვს დიდი აკუმულატორი, შტატივი და მიკროფონი, მისი ტარება გაცილებით რთულია! გარდა ამისა, თუ ძველი მოდელის კასეტებიანი ვიდეოკამერით სარგებლობთ, გადაღების დასრულების შემდეგ ჯერ ამ მასალის [...]“⁴⁵⁶ „გაციფრულება დაგვირდებათ. მაგრამ თუ გა-

გიმართლათ და მასალა ვიდეოკამერის მეხსიერების ბარათზე ინახება, ეს პრობლემა მოხსნილია: ნეგილიათ გადაღებული კადრები პირდაპირ გადაიტანოთ კომპიუტერში [...]“⁴⁵⁷

ფლიპ-კამერა

სერათი N140:



„ფლიპ-კამერა ციფრული ვიდეოკამერის სახეობაა, რომელიც ძალიან მოსახერხებელი ხელსაწყოა. იგი USB პორტით კომპიუტერს უკავშირდება და ძალიან სწრაფი მოქმედების საშუალებას გაძლევთ. შეგიძლიათ გადაღებისთანავე მასალა კომპიუტერში გადაიტანოთ [...] რამდენიმე წუთში! ფლიპ-კამერას გარე მიკროფონს ვერ დაუკავშირებთ — ეს მისი უარყოფითი მხარეა.“⁴⁵⁸

⁴⁵⁴ ავტორთა კოლექტივი. ვიდეო ადვოკატირება (აქტიური მოქალაქის სახელმძღვანელო) ელ. გვერდი: [redacted] ნანახია 07.07.2019.

⁴⁵⁵ იქვე.

⁴⁵⁶ ავტორთა კოლექტივი. ვიდეო ადვოკატირება (აქტიური მოქალაქის სახელმძღვანელო) ელ. გვერდი: [redacted] ნანახია 07.07.2019.

⁴⁵⁷ იქვე.

⁴⁵⁸ იქვე.

მობილური ტელეფონი;
სურათი N141;



„მობილური ტელეფონი მცირე ზომისაა და საშუალებას მოგცემთ მიმდინარე მოვლენები ისე გადაიღოთ, რომ არ მიიქციოთ არასასურველი ყურადღება.⁴⁵⁹ „[...] ახალი მოდელები გამოსახულებისა და ხმის ჩანაწერის მაღალ ხარისხსაც იძლევა (ზოგიერთ მათგანს გარე მიკროფონიც კი უერთდება). მობილური ტელეფონის უარყოფითი მხარეა, რომ ბევრ მათგანს შეზღუდული აქვს ვიდეოს ხანგრძლივობა და შეიძლება გადაღება ყველაზე მნიშვნელოვან მომენტში შეაჩეროს.“⁴⁶⁰

დამხმარე ხელსაწყოები;

შტატივი; სურათი N142;



„გამოიყენეთ შტატივი, როცა ამის საშუალება გექნებათ. ის დაგეხმარებათ დაბალფასიანი ფოტოაპარატით ან ვიდეოკამერით გადაღებული მასალა პროფესიონალურს დაამსგავსოთ. უმჯობესია გამოიყენოთ შტატივი, რომელსაც მოძრავი თავი აქვს. ეს კამერის მოძრაობას გააადვილებს!“⁴⁶¹

მიკროფონი;
სურათი N143;



„სუფთა ხმა ძალიან მნიშვნელოვანია! ხმის უხარისხო ჩანაწერმა შეიძლება კარგი გამოსახულება გაგიფუჭოთ. იმ შემთხვევაში, თუ ვიდეოკამერას გარე მიკროფონი უერთდება, შეგიძლიათ შედარებით იაფფასიანი მიკროფონიც კი შეარჩიოთ. ხშირ შემთხვევაში იგი ჩამონტაჟებულ მიკროფონზე გაცილებით მაღალი ხარისხით იწერს ხმას.“⁴⁶²

⁴⁵⁹ იქვე.

⁴⁶⁰ ავტორთა კოლექტივი. ვიდეო ადვოკატირება (აქტიური მოქალაქის სახელმძღვანელო) ელ. გვერდი; ნანახია 07.07.2019.



⁴⁶¹ იქვე.

⁴⁶² ავტორთა კოლექტივი. ვიდეო ადვოკატირება (აქტიური მოქალაქის სახელმძღვანელო) ელ. გვერდი; ნანახია 07.07.2019.



როგორ უნდა გვეჭიროს ვიდეოკამერა:

„ძალიან მნიშვნელოვანია, რომ გადაღების დროს კამერა სტაბილური იყოს. ამისათვის არსებობს შტატივი, რომელიც კამერის სტაბილიზებას უზრუნველყოფს. მაგრამ არის შემთხვევები, როცა შტატივი არ გაქვთ ან მოცემულ სიტუაციაში შეუძლებელია მისი გამოყენება. ამ დროს შტატივის მაგივრობას ხელი გაგიწევთ. მყარად დადებით მიწაზე. შეგიძლიათ ფეხები ოდნავ გაშალოთ. ვიდეოკამერა ერთი ხელით მყარად დაიჭირეთ, მეორე კი კორპუსის წინა ნაწილში მოჰკიდეთ, რომ მაქსიმალურად მოხდეს მისი სტაბილიზება. თუ მუხლებზე დგახართ, შეგიძლიათ ერთი მუხლი მოხართ და მას იმ ხელის იდაყვით დაეყრდნოთ, რომელშიც კამერა გიჭირავთ. შტატივის მაგივრობა შესაძლოა ღობემ ან კედელმაც გაგიწიოთ. არჩევანი თქვენზეა! მთავარია, კამერა არ ყანყალებდეს და მყარად გეჭიროთ!“⁴⁶³

მოძრაობა კამერით;

სურათი N144 და 145:



„მოძრავი ობიექტის გადაღებისას შეგიძლიათ შტატივზე მდგარი კამერა ჰორიზონტალური ან ვერტიკალური პანორამირების გამოყენებით „გადაღწეოთ“ მას ისე, რომ კამერას ადგილი არ უცვალოთ, მაგრამ არსებობს მეორე ალტერნატივა: კამერა შტატივს მოხსნათ და კამერით ხელში, ობიექტთან ერთად გადაადგილოდეთ.“⁴⁶⁴

„ასეთ შემთხვევებში გაითვალისწინეთ შემდეგი:

ეცადეთ მუხლები ოდნავ მოხართ და ისე იმოძრაოთ;

ფრთხილად გადადგით ნაბიჯები, რომ გამოსა-

ხულება სტაბილური იყოს. [...]

როდესაც ობიექტს კამერით მიჰყვებით, სასურველია, გყავდეთ დამხმარე, რომელიც მუდმივად თქვენს ზურგს უკან იქნება და გზას გაგიტავისუფლებთ;

მოძრავი ობიექტის გადაღებისას, კამერის მყარად დაფიქსირების მიზნით, შეგიძლიათ ბორბლებიანი სკამის ან ველოსიპედის გამოყენება, რომელზეც ვიდეოკამერას დაამაგრებთ და ობიექტს გაჰყვებით;

არ დაგავიწყდეთ, რომ კამერა მყარად უნდა გეჭიროთ ხელში - ორივე ხელით მაქსიმალურად უმოძრაოდ დაფიქსირებული!“⁴⁶⁵

კამერის მოძრაობა;

„კამერის მოძრაობა, სხვადასხვა სიტუაციაში, ადამიანის თვალის და თავის მოძრაობის იმიტაციას ქმნის. მაგალითად, თუ ვინმე წინ ჩაგირბენთ, ბუნებრივია, რომ მობრუნდებით და

⁴⁶³ ავტორთა კოლექტივი. ვიდეო ადვოკატირება (აქტიური მოქალაქის სახელმძღვანელო) ელ. გვერდი:  ნანახია 07.07.2019.

⁴⁶⁴ ავტორთა კოლექტივი. ვიდეო ადვოკატირება (აქტიური მოქალაქის სახელმძღვანელო) ელ. გვერდი:  ნანახია 07.07.2019.

⁴⁶⁵ იქვე.

მას თვალს გააყოლებთ. იგივე შეიძლება კამერამ გაიმეოროს. არსებობს კამერის მოძრაობის სხვადასხვა სახე, რომლებსაც ქვემოთ დაწვრილებით განვიხილავთ.”⁴⁶⁶

ტრანსფოკატორის („ზუმის“) გამოყენება;

სურათი N146;

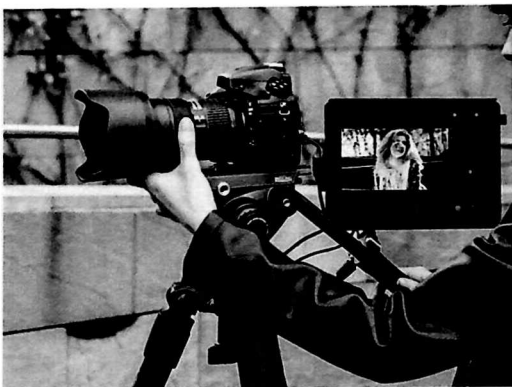


„როდესაც ტრანსფოკატორს (Zoom) იყენებთ, გამოსახულება ფართოვდება (Zoom out) ან ვიწროვდება (Zoom in). ტრანსფოკატორი სასარგებლო საშუალებაა, რომელიც გეხმარებათ კამერის გადაადგილების გარეშე შეცვალოთ კადრის სიმსხვილე. მისი გამოყენება შეგიძლიათ, როდესაც გსურთ რაიმე დეტალს ხაზი გაუსვით და უკარნახოთ მაყურებელს, რაზე გაამახვილოს ყურადღება.“⁴⁶⁷

„მაგალითად, თუ თავდაპირველად კადრში რამდენიმე ობიექტი ჩანს, ტრანს ფოკატორის მეშვეობით თქვენ უახლოვდებით (Zoom In) იმ კონკრეტულ ობიექტს, რომელზეც გსურთ მაყურებლის ყურადღების მიპყრობა. ტრანსფოკატორი გამოიყენება იმ შემთხვევაშიც, როცა გსურთ მაყურებელს აჩვენოთ რა სივრცეში, რა გარემოცვაში იმყოფება ობიექტი. მაგალითად, იღებთ დემონსტრაციაში მონაწილე ადამიანს. თავდაპირველად კადრში ჩანს თქვენი ობიექტი (ახლო ხედი); მაყურებლისათვის არ არის ნათელი, რა სივრცეში იმყოფება იგი. ტრანსფოკატორით შორდებით ობიექტს (Zoom out) და აფართოვებთ ხედს. კადრში ჩნდება სხვა ადამიანებიც, რომლებიც თქვენი ობიექტის გარშემო დგანან. მაყურებელი ხვდება, რომ ობიექტი დემონსტრაციის მონაწილეა.“⁴⁶⁸

ფოკუსი;

სურათი N147;



⁴⁶⁶

იქვე.

⁴⁶⁷

ავტორთა კოლექტივი. ვიდეო ადვოკატირება (აქტიური მოქალაქის სახელმძღვანელო) ელ. გვერდი;  ნანახია 07.07.2019.

⁴⁶⁸

იქვე.

..თითქმის ყველა ვიდეოკამერას აქვს ავტომატური ფოკუსირების რეჟიმი. რაც ნიშნავს, რომ კამერა თვითონვე ასწორებს ფოკუსს ობიექტზე. ფოკუსში მყოფი ობიექტი კი არ არის ბუნდოვანი. ავტომატური ფოკუსირების რეჟიმი ძალიან მოხერხებულია. განსაკუთრებით კი, როდესაც დრო არ გაქვთ, რომ ფოკუსი გაასწოროთ. თუ კამერა ავტომატური ფოკუსირების რეჟიმზეა გადაყვანილი, იგი თქვენს საქმეს თვითონ შეასრულებს. მაგრამ გახსოვდეთ, რომ თუ მთლიანად ავტოფოკუსს დაეყრდნობით და არ ისარგებლებთ მანუალური ფოკუსის რეჟიმით (კამერის ამ რეჟიმზე გადასაღებ ობიექტზე ფოკუსს ხელით ასწორებთ), მზად უნდა იყოთ სიურპრიზებისთვის. მაგალითად, თუ იღებთ ადამიანს, რომელიც რამდენიმე სხვა ადამიანთან ერთად ქუჩაში გადაადგილდება, და კამერა ავტომატური ფოკუსის რეჟიმშია - ფოკუსშია გადასაღები ობიექტი. მაგრამ, თუ მოულოდნელად, გადაღების პროცესში, ობიექტსა და კამერის ობიექტივს შორის, კამერასთან უფრო ახლოს (წინა ფონზე) სხვა ადამიანი ჩაიარა, კამერა ფოკუსს მაშინვე მასზე გადაიტანს და თქვენი გადასაღები ობიექტი ფოკუსგარეშე დარჩება.“⁴⁶⁹

..ავტომატური ფოკუსი: ამ რეჟიმის გააქტიურების შემთხვევაში კამერა თვითონვე, ავტომატურად ასწორებს ფოკუსს ობიექტზე.“

..მანუალური ფოკუსი: ამ რეჟიმის გააქტიურების შემთხვევაში ფოკუსის გასწორება ხელ ით, მანუალურად უნდა მოხდეს. წინააღმდეგ შემთხვევაში, გადასაღები ობიექტი ფოკუსს გარეშე ბუნდოვანი იქნება.“⁴⁷⁰

..ყოველთვის ეცადეთ ფოკუსირების მანუალური რეჟიმი გამოიყენოთ, ავტოფოკუსს კი მიმართეთ მაშინ, როდესაც სხვა გამოსავალი არ გაქვთ. ავტოფოკუსის რეჟიმში მუშაობა მისაღებია და ნაკლებ პრობლემას შექმნის, თუ კადრში მოძრაობა არ გაქვთ. ისიც გაითვალისწინეთ, რომ მანუალური ფოკუსის რეჟიმში მუშაობა ადვილი არ არის და მას ვარჯიშით გაწაფვა სჭირდება.“⁴⁷¹

ექსპოზიცია (Exposure);

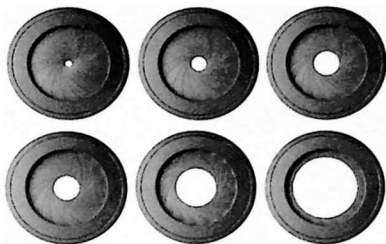
..ცუდი განათების დროს გამოსახულება პირქუშია, დეტალების გარჩევა კი, რთული. ჭარბი განათების დროს კი, გამოსახულება გადანათებულია და ძნელია ობიექტის კონტურების გარჩევა. თითქმის კადრში მოხვედრილი ყველა ობიექტი ერთნაირია. ამიტომ, მნიშვნელოვანია კადრი იყოს ზომიერად განათებული! ცუდად ან ზედმეტად განათებული გამოსახულების პრობლემის თავიდან ასაცილებლად, საჭიროა აკონტროლოთ გადაღებისას კამერაში მოხვედრილი სინათლის რაოდენობა. ამას კი დიაფრაგმის საშუალებით შეძლებთ. ვიდეოკამერა ადამიანის თვალის მსგავსადაა მოწყობილი. კამერის ობიექტივში მოთავსებული დიაფრაგმა თვალის გუგის პრინციპით მოქმედებს. დიაფრაგმა არის სპეციალური ხვრელი, რომელიც ფართოვდება (იხსნება) ან ვიწროვდება (იხურება), გამომდინარე იქიდან, თუ რა რაოდენობის სინათლე უნდა „შეუშვას“ კამერაში.“⁴⁷²

⁴⁶⁹ ავტორთა კოლექტივი. ვიდეო ადვოკატირება (აქტიური მოქალაქის სახელმძღვანელო) ელ. გვერდი:  ნანახია 07.07.2019.

⁴⁷⁰ იქვე.

⁴⁷¹ იქვე.

⁴⁷² იქვე.



„ყველა ვიდეოკამერას აქვს ექსპოზიციის რეგულირების ავტომატური რეჟიმი. რაც იმას ნიშნავს, რომ კამერა თვითონვე „აანალიზებს“ გადასაღებ სივრცეში არსებულ განათებას და იღებს „გადაწყვეტილებას“, რამდენად უნდა გახსნას ან დახუროს დიაფრაგმა, ანუ სინათლის რა რაოდენობა შეუშვას კამერაში ოპტიმალურად განათებული გამოსახულების მისაღებად. თუ განათება ძლიერია (ჭარბია), დიაფრაგმა იხურება (ვიწროვდება) და კამერაში მცირე რაოდენობით სინათლე აღწევს. თუ

განათება სუსტია, პირიქით, დიაფრაგმა იხსნება (ფართოვდება) და კამერაშიც მეტი სინათლე შედის. ექსპოზიციის მართვა შესაძლებელია მანუალურადაც, თუ კამერას შესაბამის რეჟიმზე გადაიყვანთ და თავად აკონტროლებთ დიაფრაგმას. მაგრამ დამწყები ვიდეოგრაფისთვის, ეს არცთუ ისე ადვილია და უმჯობესია, თუ საწყის ეტაპზე ავტომატური რეჟიმით ისარგებლებთ ავტომატურ რეჟიმში მუშაობისას, თუ კადრში განათებული ლაქა მოხვდება (მაგ. ერთ-ერთი გმირი ქურთუკს გაიხდის და თეთრ მაისურში დარჩება) დიაფრაგმა ავტომატურად დაიხურება, რაც კადრში არსებული ყველა ობიექტის გამოსახულებაზე იმოქმედებს. თუნათელ ობიექტს კადრიდან გაიყვანთ, დიაფრაგმა ისევ გაიხსნება.“⁴⁷³

ამდენად გაითვალისწინეთ აღნიშნული რჩევები, თუ გინდათ რომ შექმნილი ციფრული ჩანაწერი გამოყენებულ იქნეს როგორც მტკიცებულება.

473

ავტორთა კოლექტივი. ვიდეო ადვოკატირება (აქტიური მოქალაქის სახელმძღვანელო) ელ. გვერდი:  ნანახია 07.07.2019.

9.1. კომპიუტერულ-ტექნიკური ექსპერტიზის სახეობები

კომპიუტერულ ტექნიკური ექსპერტიზა არის გამოძიების გახსნისათვის უმნიშვნელოვანესი მტკიცებულების მოპოვების მთავარი საშუალება..

„კომპიუტერული დანაშაულებების ზრდასთან, ასევე, საინფორმაციო საკომუნიკაციო ტექნოლოგიების გამოყენებასთან ერთად, კომპიუტერულ-ტექნიკური ექსპერტიზა და ციფრული მტკიცებულებები თამაშობენ მნიშვნელოვან როლს სამართალდამცავი ორგანოებისა და სასამართლოების პრაქტიკულ საქმიანობაში. კერძოდ, იმ შემთხვევებში, როდესაც გამოძიების პირველი ნაბიჯები ეფუძნება მხოლოდ ციფრულ კვალს (კინაიდან ტრადიციული მტკიცებულებები, როგორებიცაა თითის ანაბეჭდები ან მოწმეები არ არსებობს), შესაძლებლობა იმისა, რომ წარმატებით მოხდეს დამნაშავის იდენტიფიცირება და მისი სამართლებრივი დევნა ეფუძნება ციფრული მტკიცებულებების სწორად შეგროვებასა და შეფასებას.“⁴⁷⁴

„ტერმინი „კომპიუტერულ-ტექნიკური ექსპერტიზა“ გამოიყენება ციფრული მტკიცებულებების ძებნის მიზნით საინფორმაციო-ტექნიკური მოწყობილობების სისტემური ანალიზის აღსანიშნავად. კომპიუტერულ ტექნიკური ანალიზი ჩვეულებრივ ხორციელდება დანაშაულის ჩადენის შემდგომ. ჩვეულებრივ გამოძიებებთან შედარებით, ამგვარი ანალიზის განხორციელება დაკავშირებულია სპეციფიკურ სირთულეებთან, ვინაიდან კომპიუტერული ტექნოლოგია მუდმივად იცვლება და სულ უფრო და უფრო მეტი ინფორმაცია ინახება ციფრულ ფორმატებში, რაც ზრდის პოტენციური მტკიცებულებების რაოდენობას. შესაბამისად, აქცენტი კეთდება მტკიცებულებების სამართალწარმოებაში გამოყენების შესაძლებლობაზე. ეს კი გარკვეულწილად ამცირებს კომპიუტერულ-ტექნიკური ექსპერტიზების ჩატარების შესაძლებლობას, ვინაიდან ისინი შეზღუდულები არიან სამართლებრივი სტანდარტებით. იმ შემთხვევაშიც კი, თუკი ახალი ტექნიკური მიღწევები შესაძლებელს გახდის ახალ კომპიუტერულ-ტექნიკურ გამოძიებებს, მათი გამოყენება დამოკიდებული იქნება იმაზე, თუ რამდენად იქნება ეს ახალი ინსტრუმენტები გათვალისწინებული არსებული საკანონმდებლო ბაზით.“⁴⁷⁵

„თანამდეროვე რეალობაში, შესაძლოა სახეზე გვექონდეს რამდენიმე სახის ექსპერტიზა ციფრულ დანაშაულთან მიმართებით, შესაძლებელია ამ კუთხით ძალიან ბევრი რაიმეს დადგენა შეგვიძლია. მაგრამ მიმოვიხილოთ რამდენიმე აქტუალური შემთხვევა ექსპერტიზების კუთხით.“⁴⁷⁶

შესაძლებელია განხორციელდეს მრავალრიცხოვანი კომპიუტერულ-ტექნიკური ექსპერტიზები. მართებული საგამომძიებლო ტექნიკის არჩევა დამოკიდებულია სხვადასხვა ფაქტორებზე – განსაკუთრებით კი იმაზე, თუ თუ რა სახის დანაშაული წარმოადგენს გამოძიების საგანს.⁴⁷⁷

ყველზე გაგრძელებულ ტექნიკურ ექსპერტიზებს შორის არის:

„აპარატურის ანალიზი;

თუკი გამოძიებულების მიერ ხდება კომპიუტერის აპარატურული უზრუნველყოფის კონფისკაცია,

⁴⁷⁴ მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ, ტრენინგის სახელმძღვანელო, სერასბურგი, მარტი 2010 წელი. ვერსია მე-17. ევროსაბჭოს ტრენინგი ქსელურ დანაშაულში.

⁴⁷⁵ იქვე.

⁴⁷⁶ იქვე.

⁴⁷⁷ მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ, ტრენინგის სახელმძღვანელო, სერასბურგი, მარტი 2010 წელი. ვერსია მე-17. ევროსაბჭოს ტრენინგი ქსელურ დანაშაულში.

კომპიუტერულ-ტექნიკურ ექსპერტებს შეუძლიათ ჩაატარონ მისი ანალიზი სისტემასთან დაკავშირებული ინფორმაციის შესაგროვებლად. ამგვარი გამოძიების გზით შესაძლებელია, მაგალითად, იმის დაბეჭდვა, ჰქონდა თუ არა დამნაშავეს შესაძლებლობა შეეერთებინა კომპიუტერული სისტემა ინტერნეტთან. გარდა ამისა, აპარატურის ანალიზი შესაძლებელია საჭირო იყოს, თუკი, რეგიონის პროცესში სისტემასთან დაკავშირებული ინფორმაციის გადაცემის გამო ცნობილი გახდება, რომ ექვმიტანილმა გამოიყენა აპარატურის კონკრეტული კონფიგურაცია.”⁴⁷⁸

„კომპიუტერის პროგრამული უზრუნველყოფის ფუნქციის ანალიზი; აპარატურის გარდა, კომპიუტერის პროგრამული უზრუნველყოფა თამაშობს მნიშვნელოვან როლს კომპიუტერული სისტემის მუშაობაში. მაგალითად, კომპიუტერულ-ტექნიკურ ექსპერტებს შეუძლიათ განსაზღვრონ კომპიუტერული ვირუსის ან ზიანის გამომწვევი პროგრამული საშუალებების სხვა ფორმების ფუნქციებიც. გარდა ამისა, მათ შეუძლიათ აღადგინონ პროგრამული უზრუნველყოფის ფუნქციონირების პროცესები, გარდა ამისა, პროგრამული უზრუნველყოფის ანალიზი შესაძლებელია მნიშვნელოვანი იყოს იმისათვის, რომ განისაზღვროს არის თუ არა კრიმინალიზირებული იმ პროგრამული უზრუნველყოფის წარმოება ან გაყიდვა, რომელიც შესაძლებელია გამოყენებული იქნეს როგორც კანონიერი, ასევე არაკანონიერი მიზნებისათვის (ორმაგი დანიშნულებით).“⁴⁷⁹

„[...] კომპიუტერულ სისტემაში დაინსტალირებული პროგრამული უზრუნველყოფის ანალიზი; კომპიუტერულ სისტემაში დაინსტალირებული პროგრამული უზრუნველყოფის ანალიზმა გამოძიებებს შეიძლება მიაწოდოს ღირებული ინფორმაცია შემდგომი გამოძიებისათვის. ეს განსაკუთრებით შეეხება დაშიფრვის პროგრამულ უზრუნველყოფას და საშუალებებს, რომლებიც გამოყენებულია ფაილების საიმედოდ წასაშლელად. თუკი ამგვარი პროგრამული უზრუნველყოფა დაინსტალირებულია ექვმიტანილის კომპიუტერზე, შემდგომი გამოძიებები შესაძლოა უშუალოდ შეეხოს ამ საკითხებს.“⁴⁸⁰

„შესაბამისი ციფრული ინფორმაციის იდენტიფიცირება;

კომპიუტერული მონაცემები შესაძლებელია შენახული იქნეს სხვადასხვა სახის შემნახველ მოწყობილობებზე. თავად მყარ დისკზეც კი არსებობს ფაილის შენახვის სხვადასხვა შესაძლებლობები. აქედან გამომდინარე, რთულია განისაზღვროს შესაბამისი მტკიცებულების შენახვის ადგილმდებარეობა. ერთ-ერთი ახალი ტენდენცია, რომელიც დამატებით სირთულეებს ქმნის შესაბამისი ციფრული ინფორმაციის იდენტიფიცირებისათვის არის დისტანციური შემნახვი მოწყობილობების სულ უფრო ფართო გამოყენება. როგორც ეს ზემოთ აღინიშნა, ფართოსარტყელიანი ინტერნეტის წყაროსა და დისტანციური შესანახი სერვერების ხელმისაწვდომობამ გავლენა მოახდინა ინფორმაციის შენახვის მეთოდზე. ამგვარი დისტანციური შემნახვი მოწყობილობის გამოყენებით, ექვმიტანილს შეუძლია თავიდან აიცილოს ექვმიტანილის კომპიუტერის იმ აპარატურული საშუალებების კონფისკაცია, რომლებიც საშუალებას აძლევს სამართალდამცავ ორგანოებს მოიპოვონ დისტანციურ შემნახვი მოწყობილობებში შენახული ინფორმაცია. კომპიუტერულ-ტექნიკური ექსპერტიზა ამ შემთხვევაში შესაძლებელია გამოყენებული იქნეს იმის შესამოწმებლად, გამოიყენა თუ არა ექვმიტანილმა დისტანციური შემნახვი სერვისები. შესაბამისი ციფრული ინფორმაციის იდენტიფიცირება არ შემოიფარგლება მხოლოდ ფაილებით. პროგრამული საშუალებების საინფორმაციო ბაზები, რომლებიც გამოიყენება ექვმიტანილის მიერ

⁴⁷⁸ მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ, ტრენინგის სახელმძღვანელო, სტრასბურგი, მარტი 2010 წელი. ვერსია მე-17. ევროსაბჭოს ტრენინგი ქსელურ დანაშაულში.

⁴⁷⁹ იქვე.

⁴⁸⁰ მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ, ტრენინგის სახელმძღვანელო, სტრასბურგი, მარტი 2010 წელი. ვერსია მე-17. ევროსაბჭოს ტრენინგი ქსელურ დანაშაულში.

მის კომპიუტერზე ინფორმაციის მოსაძებნად ასევე შეიძლება შეიცავდეს შესაბამის ინფორმაციას. სისტემის მიერ შექმნილი დროებითი ფაილებიც კი შესაძლოა შეიცავდნენ სისხლის სამართლის საქმის წარმოებისათვის საჭირო მტკიცებულებებს. ფარული ფაილების იდენტიფიცირება, დამნაშავეებმა შესაძლოა გამოიყენონ ფაილების შემნახავ მოწყობილობაში შენახვის ტექნიკა, რათა ხელი შეუშალონ სამართალდამცავ ორგანოებს მოახდინონ ფაილის შინაარსის ანალიზი. ეს განსაკუთრებით შეეხება არაკანონიერი შინაარსის გამოვლენასთან დაკავშირებით მიმდინარე გამოძიებებს. კომპიუტერულ-ტექნიკურ ექსპერტიზას შეუძლია მოახდინოს ფარული ფაილების იდენტიფიცირება და ანალიზი.⁴⁸¹

„წაშლილი ფაილების აღდგენა;

თუკი დამნაშავეები იყენებენ საშუალებებს, რომლებიც უზრუნველყოფენ ფაილების საიმედო წამლას, ამგვარი ინფორმაციის აღდგენა ზოგადად შეუძლებელია. მაგრამ იმ შემთხვევებში, როდესაც დამნაშავეებმა არ იციან ამგვარი საშუალებების არსებობა შესახებ, ციფრული ინფორმაციის წაშლა არ ნიშნავს მათი სამართალდამცავი ორგანოებისათვის ხელმიუწვდომობას, ვინაიდან ისინი შეიძლება აღდგენილი იქნეს კომპიუტერულ-ტექნიკური ექსპერტიზის სპეციალური პროგრამული საშუალებების გამოყენებით.⁴⁸²

„დაშიფრული ფაილებისა და ტომების განშიფრვა და პაროლების აღდგენა; დამნაშავეები სულ უფრო და უფრო ხშირად იყენებენ დაშიფრვის ტექნოლოგიას. ეს ტექნოლოგია სამართალდამცავ ორგანოებს მნიშვნელოვანი სირთულეების წინაშე აყენებს, ვინაიდან მათ არ შეუძლიათ მოიპოვონ და გამოიკვლიონ დაშიფრული ინფორმაცია. კომპიუტერულ-ტექნიკური ანალიზის ფარგლებში შესაძლებელია მიღებულ იქნეს ზომები დაშიფრული ფაილებისა და შემნახავი მოწყობილობების განშიფრვისათვის.⁴⁸³

„ფაილების ანალიზი;

შემნახავ მოწყობილობაზე შენახული ფაილები შეიძლება გაანალიზდეს სხვადასხვა გზებით. კომპიუტერულ-ტექნიკურ ექსპერტიზებს, მაგალითად, შეუძლიათ აქცენტი გააკეთონ ფაილების შინაარსზე. საეტვო ფაილების მანუალური შემოწმების გარდა, კომპიუტერულ-ტექნიკურმა გამოძიებებმა ასევე შეიძლება მოიცვას ტექსტობრივ ფაილებში ძირეული სიტყვების ავტომატური ძებნა და ის საშუალებები, რომლებიც ავტომატურად ეძებენ ნაცნობ გამოსახულებებს ეჭვმიტანილის კომპიუტერზე.⁴⁸⁴

„ავტორობის ანალიზი;

თუკი მექარის ტექსტების ან ქსენოფობიური მიმართვების განთავსება ხდება ინტერნეტის ქსელურ დღიურებში ან ფორუმებზე, რეგისტრაციის ჟურნალის ანალიზმა შეიძლება არ მიიყვანოს გამოძიებლები ტექსტის ავტორთან, თუკი ეჭვმიტანილი მოქმედებს ინტერნეტ კაფედან და იყენებს ანონიმურ საკომუნიკაციო მომსახურებას. დეტალური ლინგვისტური ანალიზის საშუალებით შესაძლებელია განისაზღვროს, დაწერა თუ არა ეჭვმიტანილმა სტატიები მანამდე და დატოვა თუ არა ინფორმაცია, რომლის საშუალებითაც შესაძლებელია მოხდეს პირის იდენტიფიცირება ამ კონტექსტში.⁴⁸⁵

⁴⁸¹ მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ, ტრენინგის სახელმძღვანელო, სტრასბურგი, მარტი 2010 წელი. ვერსია მე-17. ევროსაბჭოს ტრენინგი ქსელურ დანაშაულში.

⁴⁸² იქვე.

⁴⁸³ იქვე.

⁴⁸⁴ იქვე.

⁴⁸⁵ იქვე.

„ელექტრონული ფოსტის ანალიზი“;

ელექტრონული ფოსტის ანალიზი გახდა კომუნიკაციის ძალიან პოპულარული ფორმა და ამიტომ, იგი თამაშობს მნიშვნელოვან როლს კომპიუტერულ-ტექნიკური ექსპერტიზისათვის. იმის გათვალისწინებით, რომ შედარებით ადვილია შექარის ან არაკანონიერი შინაარსის მქონე თანდართული ფაილის შემცველი ელექტრონული ფოსტის გამგზავნის იდენტიფიცირება, დამნაშავეები ხშირად იყენებენ ელექტრონული ფოსტის თავისუფალ მისამართებს, რომლებიც დარეგისტრირებულია ყალბი პერსონალური ინფორმაციის გამოყენებით. ამ შემთხვევებშიც კი, ელექტრონული ფოსტის პროვაიდერის თავსართი ინფორმაციის და რეგისტრაციის ჟურნალის შესწავლა ზოგიერთ შემთხვევაში შესაძლებელს ხდის ეჭვმიტანილის იდენტიფიცირებას. ⁴⁸⁶

„ფინანსური ტრანზაქციების მიკვლევა“;

მთელი რიგი დანაშაულობები, მათ შორის ბავშვების პორნოგრაფიით ვაჭრობა, მოიცავს ფინანსურ ტრანზაქციებს. ფინანსურ ტრანზაქციებში ჩართული კომერციული სისტემებიდან და დაწესებულებებიდან მონაცემების გამოყენებით შესაძლებელია დამნაშავის იდენტიფიცირება. ამის ერთ-ერთ მაგალითს წარმოადგენს გერმანიაში ჩატარებული გამოძიება. მან გამოავლინა დამნაშავეები, რომლებმაც მოახდინეს ბავშვების პორნოგრაფიის ჩამოტვირთვა კომერციული ვებ-გვერდიდან საკრედიტო ბარათების გამცემი კომპანიების მეშვეობით, რომლებმაც ანალიზი გაუკეთეს იმ კლიენტების ამონაწერებს, რომლებმა გამოიყენეს მათი საკრედიტო ბარათები ბავშვების პორნოგრაფიის შესაძენად კონკრეტული ვებ-გვერდიდან. ამგვარი გამოძიებების ჩატარება რთულდება, თუკი დამნაშავეები იყენებენ გადახდის ანონიმურ მეთოდებს. ⁴⁸⁷

„ტრაფიკის მონაცემების შეგროვება რეალურ დროში და შინაარსის მონაცემების მოპოვება“;

კომპიუტერულ ტექნიკურმა გამოძიებებმა შეიძლება განახორციელონ რეალურ დროში გადაცემული მონაცემების მონიტორინგი. ეს კი შესაძლებლობას აძლევს გამოძიებულებს რეაგირება მოახდინონ პროცესებზე იმ დროს, როდესაც გამოძიების მიერ ეჭვმიტანილი პირი ჩადის ქმედებას. ⁴⁸⁸

„მონიტორინგის განხორციელება საჯაროდ ხელმისაწვდომ სერვისებთან მიმართებაში“;

საჯაროდ ხელმისაწვდომი სერვისები შესაძლებელია გამოიყენებულ იქნეს საავტორო უფლებებით დაცული ან არაკანონიერი შინაარსის მქონე მასალების გაცვლისათვის. გამოძიების ფარგლებში ამგვარ სერვისებზე შესაძლებელია განხორციელდეს მონიტორინგი კომპიუტერულ-ტექნიკური ექსპერტების მხრიდან. ეს მოიცავს, მაგალითად, ჩატ ფორუმებზე კონტროლსაც. ⁴⁸⁹

„დისტანციური კომპიუტერულ-ტექნიკური ექსპერტიზები“;

აქამად განიხილება დისტანციური კომპიუტერულ-ტექნიკური ექსპერტიზის საშუალებების საჭიროება. ეს შესაძლებელს გახდის უშუალოდ წყაროდან დისტანციურად შეგროვებული იქნეს მტკიცებულებები და ჩატარდეს დისტანციური მონიტორინგი, ისე რომ ეჭვმიტანლს არ ეცოდინება მის სისტემაზე განხორციელებული გამოძიებების თაობაზე. ⁴⁹⁰

გამოძიების მიერ დასასმელი შეკითხვები: კომპლექსური საინფორმაციო-ტექნოლოგიური და ფონო-ჰაბილოსკოპური ექსპერტიზის დროს;

მაგალითად; სახეზე არის დანაშაული, რომლის ფარგლებშიც ა-მ ბ-ს გადაუღო პირადი

⁴⁸⁶ მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ, ტრენინგის სახელმძღვანელო, სტრასბურგი, მარტი 2010 წელი. ვერსია მე-17, ევროსაბჭოს ტრენინგი ქსელურ დანაშაულში.

⁴⁸⁷ იქვე.

⁴⁸⁸ იქვე.

⁴⁸⁹ იქვე.

ცხოვრების ამსახველი ვიდეომასალა რომელიც სავარაუდოდ მისივე კომპიუტერიდან განათავსა სოციალურ ქსელში, გამოძიების მიერ მოხდა კომპიუტერული მოწყობილობების ამოღება და ხდება კომპლექსური საინფორმაციო-ტექნოლოგიური და ჰაბიდოსკოპური ექსპერტიზის დანიშვნა, ამ დროს რეკომენდებულია დაისვას შემდეგი შეკითხვები:

ა-ს კუთვნილი მობილურ ტელეფონიდან, იმეი კოდით 11111111, გთხოვთ, მოახდინოთ როგორც წაშლილი, ისე არსებული ინფორმაციის (მოკლე ტექსტური შეტყობინებების, სოც. ქსელების: Viber-ის, WhatsApp-ის მიმოწერის) აღდგენა და ამოღება, წერილობითი ინფორმაცია წარმოდგენილი იქნეს ბეჭდური სახით, ხოლო ვიდეო და ფოტო ფაილები — კომპიუტერულ დისკებზე. დისკები იქნეს დანომრილი, აღწერილი და მიეთითოს დასკვნაში.

ა-ს კუთვნილი კომპიუტერიდან სახელით Computer გთხოვთ, მოახდინოთ როგორც წაშლილი, ისე არსებული ინფორმაციის აღდგენა და ამოღება, წერილობითი ინფორმაცია წარმოდგენილი იქნეს ბეჭდური სახით, ხოლო ვიდეო და ფოტო ფაილები - კომპიუტერულ დისკებზე. დისკები იქნეს დანომრილი, აღწერილი და მიეთითოს იყოს დასკვნაში.

ვიდეო-ფაილების ამოღების შემთხვევაში, გთხოვთ განგვისაზღვრეთ აღენიშნება, თუ არა მონეტაჟის ნიშნები, დადებით შემთხვევაში, კონკრეტულად რა სახის?

ვიდეო და ფოტო-ფაილების ამოღების შემთხვევაში, რომელსაც მონეტაჟის კვალი არ აღენიშნება, გთხოვთ მოახდინოთ ფაილების გაწმენდა.

გთხოვთ შეადაროთ წარმოდგენილ "ა"-ს ფოტო ან/და ვიდეოჩანაწერს და განგვისაზღვროთ "ა" არის თუ არა ასახული ვიდეოჩანაწერზე და დადებით შემთხვევაში რომელ დროის მონაკვეთებში;

გთხოვთ განგვისაზღვროთ რა ფერის ტანსაცმელი აცვია "ა" -ს;

განვიხილოთ ასევე მაგალითი, როდესაც პირმა ჩაიდინა დანაშაული, რომელიც ასახულია ვიდეოჩანაწერზე. ასეთ შემთხვევაში გამოძიებელმა უნდა გამოითხოვოს შესაბამისი ინფორმაცია კომპიუტერული მოწყობილობიდან და დანიშნოს ვიდეოსკოპიური (ფონო-ჰაბიდოსკოპიური) ექსპერტიზა, რომელსაც უნდა დაუსვას შემდეგი შეკითხვები;

გთხოვთ განგვისაზღვრეთ არის თუარა არსებული ჩანაწერი უწყვეტი, აღენიშნება, თუ არა ჩანაწერს მონეტაჟის ნიშნები, დადებით შემთხვევაში, კონკრეტულად რა სახის და რომელ (დროის) მონაკვეთებში?

გთხოვთ მოახდინოთ ფაილების გაწმენდა.

მაგალითად: პირმა ჩაიდინა დანაშაული, რომელიც ასახულია ჩაწერ მონაცემილობაზე, ასეთ შემთხვევაში ინიშნება ფონოსკოპიური ექსპერტიზა, რომელსაც რეკომენდებულია დაესვას შემდეგი შეკითხვები:

გთხოვთ განგვისაზღვრეთ არის თუ არა არსებული ჩანაწერი უწყვეტი, აღენიშნება, თუ არა ჩანაწერს მონეტაჟის ნიშნები, დადებით შემთხვევაში, კონკრეტულად რა სახის და რომელ (დროის) მონაკვეთებში?

გთხოვთ მოახდინოთ ჩანაწერის გაწმენდა;

გთხოვთ მოახდინოთ გაშიფვრა წერილობითი ფორმით;

გთხოვთ გვაცნობოთ „ა“-ს ხმა იდენტიფიცირება თუ არა ვიდეოჩანაწერზე არსებული ხმისა და განგვისაზღვრეთ კონკრეტულად რომელი დროის მონაკვეთებში არსებული ხმისა?

თავი X

საგამოძიებო მოქმედების ჩატარებისათვის საჭირო კომპიუტერის ფუნქციური კლავიშები

10.1. კლავიატურის სტრუქტურა

იმისათვის, რომ საგამოძიებო ორგანოს თანამშრომელმა განახორციელოს კომპიუტერული სისტემიდან ინფორმაციის გამოთხოვა, ის უნდა ფლობდეს შესაბამის მეთოდოლოგიას და ცოდნას კომპიუტერული სისტემის შესახებ, უნდა იცოდეს კომპიუტერზე არსებული კლავიატურის და კონკრეტული სიმბოლოს გამოყენება, ისევე როგორც კომპიუტერული სისტემის შინაგანი აგებულება.

პირველ რიგში გავიხილოთ კლავიატურაზე არსებული ის მნიშვნელოვანი კლავიშები, რაც უნდა იცოდეს კომპიუტერთან საგამოძიებო მოქმედების ჩამტარებელმა გამოძიებელმა ინფორმაციის გამოთვლის მიზნებისათვის, მოდიოთ განვიხილოთ, Windows – ს სისტემის მქონე კომპიუტერების კლავიატურის აგებულება, რის შემდეგაც ყურადღება გავამახვილოთ MacOS სისტემის Apple- ის Mac-ის ოჯახების კატეგორიის კომპიუტერების კლავიშების კომბინაციებზე.

კლავიატურის აგებულება;

„კლავიატურა შედგება შემდეგი ჯგუფის კლავიშებისაგან (დანართი 5).

1. კლავიშების ძირითადი ჯგუფი;
2. მიმთითებლის მართვის კლავიშები;
3. დამხმარე კლავიშები;
4. ფუნქციური კლავიშები;
5. სპეციალური კლავიშები.“⁴⁹⁰

განვიხილოთ თითოეული მათგანი:

1. „კლავიშების ძირითადი ჯგუფი ციფრულ-ალფაბეტური კლავიშები;

Enter – ბრძანების შეყვანის (ანუ გადაწყვეტილების დადასტურების) კლავიში;

Shift – დიდი ასოების შესაყვანად, ზედა რეგისტრის გასააქტიურებელი კლავიში;

Caps Lock – ზედა რეგისტრის დაფიქსირების კლავიში;

Ctrl, Alt – მმართველი კლავიშები, რომლების გამოიყენება სხვა კლავიშების დანიშნულების შესაცვლელად;

Tab – ტაბულაციის კლავიშის დანიშნულებაა მიმთითებლის რამდენიმე პოზიციით მარჯვნივ გადაადგილება; (მიმთითებელი — ეს არის მოცემი ნიშანი ეკრანზე, რომელიც მიუთითებს შემდეგი სიმბოლოს შეყვანის ადგილს);

Backspace – სიმბოლოს წაშლა მიმთითებლის მარცხნივ.“⁴⁹¹

2. „მიმთითებლის მართვის კლავიშები;

⁴⁹⁰ ციური ნოზაძე, გოგა საზანდროშვილი; ლექციების კურსი; კომპიუტერის საფუძვლები. გვ. 2-3 ელ.გვერდი: <http://www.bpa.ge/book/book66.pdf> ნანახია 02.07.2019

⁴⁹¹ ციური ნოზაძე, გოგა საზანდროშვილი; ლექციების კურსი; კომპიუტერის საფუძვლები. გვ. 2-3 ელ.გვერდი: <http://www.bpa.ge/book/book66.pdf> ნანახია 02.07.2019

PgUp, PgDn – ეკრანული გვერდი ზემოთ/ ქვემოთ;

Home, End – მიმთითებლის გადაადგილება შესაბამისად სტრიქონის დასაწყისში და ბოლოში;

Delete – სიმბოლოს წაშლა მიმთითებლის მარჯვნივ;

Insert – ჩამატება/გადაწერის რეჟიმების გადასართველი კლავიში.⁴⁹²

3. დამხმარე კლავიშები;

..დამხმარე კლავიატურაზე ციფრული კლავიშები ემთხვევა მიმთითებლის მმართველ კლავიშებს. ციფრულ რეჟიმში ხდება ციფრების შეყვანა, მიმთითებლის მართვის რეჟიმში გადართვისას კი ამ კლავიშების დანიშნულება ემთხვევა მიმთითებლის მართვის კლავიშების ფუნქციებს. ამ რეჟიმებს შორის გადართვა ხდება Num Lock კლავიშით.⁴⁹³

4. ფუნქციური კლავიშები;

..F1 – F12 – ამ კლავიშების დანიშნულებაა ხშირად განმეორებადი ბრძანებების გამოძახება. სხვადასხვა პროგრამებში მათ სხვსდასხვა დანიშნულება აქვთ;

ლილაკი F1 პასუხისმგებელია მიმთითებელ ღია პროგრამაზე, მაგალითად, თუ თქვენ მუშაობთ Microsoft Word-ში. ნებისმიერ კომბინაციაში შეუწყობს ხელს ამ პროგრამის მუშაობას ინფორმაციის გახსნის შედეგად;

ლილაკი F2 ხელს უწყობს შერჩეულ ფაილს სახელის გადარქმევაში ყოველგვარი სხვა დამატებითი მოქმედებების გარეშე. ზოგიერთ შემთხვევაში (თამაშებსა და პროგრამებში) ეს ლილაკი ასრულებს შენახვის ფუნქციას;

ლილაკი F3 საძიებო მისია აქვს მოცემულ, ღია პროგრამის მოძებნაში. მისი ანალოგი კომბინაციაა Ctrl+F, თუმცა დამეთანხმებით, რომ F3 გაცილებით მარტივი ვარიანტია;

ლილაკების Alt+F4 კომბინაცია ხელს უწყობს ღია პროგრამების დახურვას, **Ctrl + F4** კი დახურავს მიმდინარე ჩანართს ბრაუზერში. თუ სტატიის ბოლომდე წაკითხვას გეგმავთ, ნუ დააჭერთ საცდელად კომბინაცია **Ctrl + F4**-ს;

ლილაკი F5 განკუთვნილია რათა განახლოს ღია ფანჯარა ბრაუზერში. სხვა პროგრამებში მისი ანალოგი კომბინაციაა **Ctrl+R**;

ლილაკი F6 გვეხმარება სწრაფად გადავიდეთ ამავე პროგრამის სხვა მენიუში. ზოგიერთ თამაშში კი ის სწრაფ შენახვას ემსახურება;

ლილაკი F7 ამოწმებს მართლწერას ტექსტის პროგრამებში Word, Open Office და სხვა;

ლილაკი F8 ალგებს «Start» მენიუს Windows-ში;

ლილაკი F9 ემსახურება გააგზავნოს და მიიღოს გზავნილები Outlook-ში, ასევე ანახლებს ინფორმაციას Word-ში;

ლილაკი F10 ახორციელებს ზარს მოცემულ მენიუში;

ლილაკი F11 ემსახურება სრულ ეკრანზე გადართვას მოცემულ ბრაუზერში;

ლილაკი F12 სხნის HTML დოკუმენტს ცალკე ფანჯარაში. Word-ში კი ის იწახვას დოკუმენტს.⁴⁹⁴

5. სპეციალური კლავიშები;

Esc – ბრძანების გაუქმების კლავიში; **Print Scrn** – ეკრანზე არსებული გამოსახულების ბეჭდვა პრინტერზე; **Pause (Break)** – პროგრამის დროებით შეჩერება.

⁴⁹² ციური ნოზაძე, გოგა საზანდროშვილი; ლექციების კურსი; კომპიუტერის საფუძვლები. გვ. 2-3 ელ.გვერდი:<http://www.bpa.ge/book/book66.pdf> ნანახია 02.07.2019.

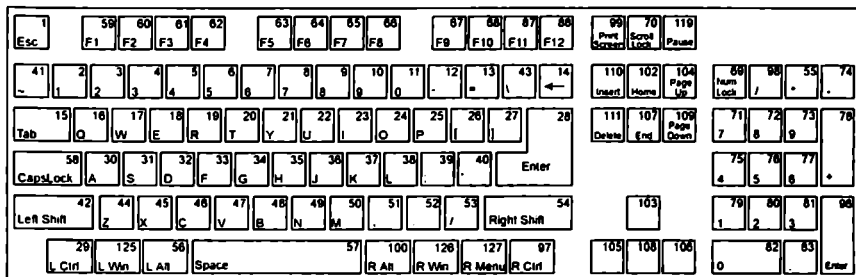
⁴⁹³ იქვე.

⁴⁹⁴ სტატია: იცოდით რისთვის არსებობს კლავიატურაზე ლილაკების ზედა მხარე? 2016, 22 დეკემბერი. ელ.გვერდი:



ბრძანებების სწრაფად გამოსაძახებლად გამოყენებად ღილაკთა კომბინაციებს "ცხელი ღილაკები" ეწოდება.⁴⁹⁵ კლავიატურის აგებულება (იხ. სურათი N149):

სურათი N149



10.2. Windows სისტემის პროგრამის კლავიშთა კომბინაციები

მნიშვნელოვანია, გამოძიებულმა, რომელიც მუშაობს კომპიუტერთან იცოდეს კლავიატურის კლავიშების კომბინაციები რომელთა საშუალებითაც განახორციელებს Windows პროგრამაზე სჭირთა ქმედებებს, აღნიშნული კლავიშების კომბინაცია იხილეთ სურათზე (დანართი - კომბინაციები აღებულია ინტერნეტ საიტიდან 

საერთო დანიშნულების «ცხელი კლავიშები» ²	
კლავიშების კომბინაცია	აღწერა
Ctrl + Es	გახსნის მენიუს «სტარტი» (Start).
Ctrl + Shift + Esc	გახსნის მენიუს «ამოცანების დისპეტჩერი»
Win + E	გახსნის დიალოგურ ფანჯარას «ჩემი კომპიუტერი»
Ctrl + Shift + N	ახალი საქაღალდის შექმნა (New Folder)
Win + R	გახსნის დიალოგურ ფანჯარას «Run»

⁴⁹⁵ ციური ნოზაძე, გოგა საზანდრიშვილი; ლექციების კურსი; კომპიუტერის საფუძვლები. გვ. 2-3 ელ.გვერდი:  ნანახია 02.07.2019

Win + D	სამუშაო მაგიდაზე (Desktop) გადამრთველი. (ჩახურავს ყველა ფანჯარას, ან დაუბრუნებს საწყის მდგომარეობას).
Win + M	ჩაკეცავს ყველა ფანჯარას.
Win + Shift + M	აღადგენს ყველა ჩაკეცილ ფანჯარას.
Win + L	გახსნის მენიუს «მოძიებარების არჩევა»
Win + F1	Windows-ის დახმარების გამოძახება
Win + Pause	გამოიძახებს ფანჯარას «System Properties»
Win + F	გახსნის ფანჯარას «ფაილების ძებნა»
Win + U	გახსნის მენიუს «სპეციალური შესაძლებლობების ცენტრი»
Win + Ctrl + F	გახსნის განჯარას «კომპიუტერების ძებნა»
Printscreen	გადიღებს კომპიუტერის ეკრანის «სქრინშოტს»
Alt + Printscreen	გადიღებს მიმდინარე აქტიური ფანჯრის 'სქრინშოტს»
Win + Tab Win + Shift + Tab	განახორციელებს «ამოცანათა პანელის» ღილაკებს შორის გადართვას.
Tab ან F6	პანელებს შორის გადაადგილება (მაგალითად სამუშაო მაგიდას და პანელ «სწრაფ სტარტს შორის).
Ctrl + A	მონიშნავს ყველაფერს (ობიექტები, ტექსტი).
Ctrl + C ან Ctrl + Insert	დააკოპირებს ნებისმიერ მონიშნულ ობიექტს.
Ctrl + V ან Shift + Insert	ჩასვამს სასურველ ადგილზე ნებისმიერ დაკოპირებულ ობიექტს.
Ctrl + X ან Shift + Delete	გადიღებს და უკან დააბრუნებს ბოლოს შესრულებულ მოქმედებას.
Ctrl + N	გახსნის მიმდინარე ბრაუზერის «დუბლიკატს» (ახალ ფანჯარას).
Ctrl + S	შეინახავს მიმდინარე დოკუმენტს, პროექტს და ა.შ
Ctrl + O	გახსნის დიალოგურ ფანჯარას «ფაილების არჩევა» (იგივე «ფაილების გზამკვლევი» (Explorer) - დოკუმენტის, ან სხვა სახის ფაილების გასახსნელად)
Ctrl + P	გახსნის დიალოგურ ფანჯარას «ბეჭდვა»

Ctrl + Z	მოახდენს ბოლოს შესრულებული მოქმედების უარყოფას. (გადაფიქრებას, ანუღირებას, უკან დაბრუნებას).
Shift	დაბლოკავს CD-ROM (დისკის) - ის ავტომატურ გაშვებას Windows-ის ჩატვირთვისას; აჩერებს Startup-ის პროგრამების ავტომატურ ჩატვირთვისას.
Alt + Enter	შერჩეული ობიექტის თვისებების გამოძახება; სრულეკრანიან რეჟიმში გადასვლა და პირიქით (მაგალითად მედიაფლეერში, gom player - ში და ა.შ)
Alt + Shift	ენების შეცვლა (Eng - Rus - Ka).
Alt + Shift + Print Screen	მაღალი კონტრასტულობის ჩართვა/გამორთვა.
Alt + Shift + Num Lock	თაგვის (მუხის) მართვის დიალოგური ფანჯრის ჩართვა.
Num Lock (5 წამის განმავლობაში)	გადართვების გახშოვანების (ToggleKeys) ჩართვა/გამორთვა
თემსტან მუშაობა	
Ctrl + A	ყველაფრის მონიშვნა.
Ctrl + C ან Ctrl + Insert	კოპირება.
Ctrl + X ან Shift + Delete	ამოჭრა.
Ctrl + V ან Shift + Insert	ჩასმა.
Ctrl + B	ტექსტის გაშუქება.
Ctrl + I	ტექსტის დახრა.
Ctrl + E	ტექსტის ცენტრში გასწორება.
Ctrl + Z	შესრულებული მოქმედების გაუქმება.
Ctrl + Y	შესრულებული მოქმედების ან შეტანილი ცვლილების გამოწერება.
Ctrl + U	ტექსტის ქვემოთ ხაზის გასმა (სიტყვებს შორის დაცილების («პრაბელების») ჩათვლით).
Ctrl+Shift+U	მხოლოდ ტექსტის შემადგენელ სიტყვებზე ხაზის გასმა.
Ctrl + ← Ctrl + →	ტექსტის სიტყვებს შორის გადაადგილება. მუშაობს არა მხოლოდ ტექსტის რედაქტორებში, ძალიან მოსახერხებელია ბრაუზერის მისამართის ველში გადასაადგილებლად.

Shift + ← Shift + → Shift + ↑ Shift + ↓	ტექსტის გამოყოფა.
Ctrl + Shift + ← Ctrl + Shift + →	ტექსტში სიტყვების (მიმდევრობით - სიტყვა-სიტყვით) გამოყოფა.
Home End	ტექსტის სტრიქონში თავში და ბოლოში გადაადგილება.
Ctrl + Home Ctrl + End	დოკუმენტის თავში და ბოლოში გადაადგილება.
Ctrl + W ან Alt + F4	დოკუმენტთან მუშაობის დასრულება.
ფაილებთან მუშაობა	
Shift + F10 Menu	მიმდინარე ობიექტის კონტექსტური მენიუს გამოძახება. მუხის (თავის) მარჯვენა ლილავის დაჭერის ანალოგია)
Alt + Enter	ობიექტის თვისებების გამოძახება.
Ctrl - ით გადაადგილება	ობიექტის (Folder, Word და ა.შ.) კოპირება.
Shift - ით გადაადგილება	ობიექტის (Folder, Word და ა.შ.) გადაადგილება.
Ctrl + Shift - ით გადაადგილება	ობიექტის (Folder, Word და ა.შ.) იარლიყის შექმნა.
კლიკები Ctrl - ით	რამოდენიმე ობიექტის გამოყოფა ნებისმიერი თანმიმდევრობით.
კლიკები Shift - ით	რამოდენიმე მოსაზღვრე (მომიჯნავე) ობიექტის გამოყოფა
Enter	იგივეა რაც ობიექტზე ორმაგი კლიკი (დაწკაპუნება).
Delete	ობიექტის წაშლა.
Shift + Delete	ობიექტის საბოლოოდ წაშლა (ურნაში გადანაცვლების გარეშე).
ფაილების გზამკვლევთან (Explorer) მუშაობა ⁴	
F3 ან Ctrl + F	გახსნის ან დამალავს გამკვლევეში ძებნის არეს.

← → + (ციფრულ კლავიატურაზე) - (ციფრულ კლავიატურაზე)	გზამკვლევაში ნავიგაცია (გზამკვლევაში არსებული კატალოგების ჩაქცევა და გაშლა)
F6	გზამკვლევის მენიუსებს შორის გადართვა.
* (ციფრულ კლავიატურაზე)	გამოყოფილ საქალაქში არსებული საქალაქების ჩვენება.
F5	გზამკვლევის ან ინტერნეტ ექსპლორერის თანჯრის განახლება.
Backspace	გზამკვლევაში, ან ინტერნეტ ექსპლორერში ერთი დონით ზემოთ ასვლა
F4	გზამკვლევაში ან ინტერნეტ ექსპლორერში მისამართების ველის გახსნა/ ჩახურვა
ფანჯრებთან მუშაობა *	
Alt + Tab Alt + Shift + Tab	აქტიურ ფანჯრებს და ელემენტებს შორის გადასვლა და გადასვლის მენიუს გამოძახება.
Alt + Esc Alt + Shift + Esc	ფანჯრებს შორის გადასვლა (იმ თანმიმდევრობით, რა თანმიმდევრობითაც მოხდა მათი ჩართვა).
Alt + F6	ერთი პროგრამის რამდენიმე ფანჯარას შორის გადართვა (მაგალითად WinWord -ის ლია ფანჯრებს შორის)
Ctrl + F4	აქტიური დოკუმენტების დახურვა პროგრამებში.
Alt + F4	სამუშაო მაგიდაზე (Desktop) - ვინდოუსის გამორთვის ბრძანების გამოძახება; აქტიური პროგრამების და პუნქტების დახურვა.
Alt F10	ფანჯრის მენიუს გამოძახება.
Alt + - (მინუსი)	«შვილობილი» ფანჯრის სისტემური მენიუს გამოძახება (მაგალითად დოკუმენტის ფანჯრის).
Esc	ფანჯრის მენიუდან გამოსვლა, ან გახსნილი დიალოგური ფანჯრის დახურვა.
Alt + ასო	მენიუს ბრძანების, ან მენიუს შესაბამისი პუნქტის გამოძახება.
Alt + Space (გრძელი კლავიში)	ფანჯრის სისტემური მენიუს გამოძახება.

F1	ეკრანის მენიუს გამოძახება.
Ctrl + Up (Pg Up) Ctrl + Down (Pg Dn)	ტექსტის ვერტიკალური ჩამოწევა-აწევა, ან აბზაც-აბზაც ზემოთ-ქვემოთ მოძრაობა.
დიალოგურ ფანჯრებთან მუშაობა 6	
Ctrl + Tab	ჩანართებში (ბრაუზერში გახსნილ ბმულებში) (Tab) წინ გადაადგილება.
Ctrl + Shift + Tab	ჩანართებში (ბრაუზერში გახსნილ ბმულებში) (Tab) უკან გადაადგილება.
Tab	ოფციებში წინ გადაადგილება.
Alt + მენიუში ხაზგასმული ასო	შესაბამისი ბრძანების შესრულება ან მენიუს შესაბამისი პუნქტის (ოფციის) ამორჩევა.
Enter	მიმდინარე ოფციის ან ლილაკის ბრძანების შესრულება.
ისრებიანი კლავიშები	ლილაკების არჩევა, თუ მიმდინარე ოფცია შედის გადამრთველების ჯგუფში.
Shift + Tab	ოფციებში უკან გადაადგილება.
ბრაუზერებთან მუშაობა 7	
Ctrl + N	გახსნის მიმდინარე ბრაუზერის «დუბლიკატს» (ახალ ფანჯარას).
Ctrl + R	განაახლებს მიმდინარე ვებ-გვერდს.
Ctrl + B	გახსნის დიალოგურ ფანჯარას - «რჩეულების სორტირება» (ინტერნეტ ექსპლორერში).
Ctrl + T	გახსნის ახალ ჩანართს ბრაუზერში.
Ctrl + Shift + T	გახსნის (აღადგენს) შემთხვევით ჩახურულ ჩანართს ბრაუზერში.
Ctrl + Shift + Delete	გახსნის ფანჯარას «ბრაუზერის ისტორიის გაწმენდა» (ბრაუზერის პარამეტრებში).
Ctrl + E	გახსნის «საიტების ისტორიას» ბრაუზერის აქტიურ ფანჯარაში (ინტერნეტ ექსპლორერში).

Ctrl + F	გახსნის ძებნის არეს (ძალიან მოსახერხებელია როდესაც ვებ-გვერდზე ძებნის არეში ჩაწერილი მსგავსი სიტყვების მოძიება)
Ctrl + I	გახსნის თანჯარას «რჩეულები» (ინტერნეტ ექსპლორერში).
Ctrl + L	მონიშნავს აქტიურ თანჯარაში გახსნილ ბმულს (ლინკს).
Ctrl + O	გახსნის «ფაილების გზამკვლევი» (Explorer).
Ctrl + P	გახსნის დიალოგურ თანჯარას - «ბეჭდვა».
Ctrl + W	ჩახურავს მიმდინარე (აქტიურ) «თანჯარას».
Fn + F11	გადავა «სრულეკრანიან რეჟიმში» და პირიქით.

10.3. MacOS სისტემის პროგრამის კლავიშთა კომბინაციები

2. Apple- ის Mac-ის ოქსების კატეგორიის კომპიუტერების კლავიატურა;

Apple- ის Mac-ის ოქსების კატეგორიის კომპიუტერების კლავიატურაზე კლავიშების კომბინაცია სხვაგვარად გვევლინება. კლავიატურა იხილეთ სურათი N150;

სურათი N150:



ზემოაღნიშნული ტიპის კლავიატურაზე Command ლილაკი, ატარებს Control ლილაკის ფუნქციას. წარმოიდგენთ რამდენიმე მნიშვნელოვან კლავიშთა კომბინაციას, რომელიც გამოძიებულს გამოადგება Apple- ის Mac-ის ოქსების კატეგორიის კომპიუტერების კლავიატურაზე მუშაობის პროცესში (დანართი - კომბინაციები აღებულია ინტერნეტ საიტიდან ):

აპლიკაციის გათიშვა; აპლიკაციის სრულიად გასაღწევი დააჭირეთ Cmd + Q;

აქტიური ფანჯრის დახურვა; თუ არ გსურთ აპლიკაციის სრულად გათიშვა და გსურთ უბრალოდ აქტიური ფანჯრის დახურვა გამოიყენეთ Cmd + W;

ახალი Tab-ის გახსნა - აპლიკაციების უმრავლესობას აქვს Tab-ების მხარდაჭერა. იმისათვის რომ ახალი ფანჯრის მაგივრად გახსნათ ახალი Tab-ი დააჭირეთ Cmd + T - აპლიკაციების გადამრთველი, აქტიურ აპლიკაციებს შორის მუშის გარეშე გადასართველად გამოიყენეთ Cmd + Tab

ძებნა Spotlight-ით - კლავიატურის კომბინაცია რომლის საშუალებით აქტიურდება Spotlight ძებნა არის Cmd - Space bar;

ოპერაციები. კოპირება, ჩაწეება, ამოტრა; Cul, Copy, Paste, Undo - თუ თქვენ იყენებდით ამ ოპერაციებისთვის კლავიატურის კომბინაციას PC-ზე, მაკის შემთხვევაშიც არ არის დიდი განსხვავება. Control ლილაკის ნაცვლად იყენებთ Cmd-ს და შესაბამისად X, C, V, Z.

კონკრეტული სიტყვის ან ფრაზის მოძებნა; თუ გსურთ რომელიმე ვებ გვერდზე რაიმე სიმბოლოს, სიტყვის ან ფრაზის მოძებნა გამოიყენეთ Cmd + F კომბინაცია.

Quick look - Quick look არის საკმაოდ კარგი საშუალება რათა ფაილის გახსნის გახსნის გარეშე შევძლოთ ამ კონკრეტული ფაილის Preview. მონიშნეთ სასურველი აპლიკაცია მასზე ერთხელ დაწაკაუნებით და შემდეგ დააჭირეთ Space bar-ს.

გამორთვა, გადატვირთვა, ძილის რეჟიმი; თქვენი მაკის კომპიუტერის გამოსართავად, გადასატირთად ან ძილის რეჟიმში გადასაყვანად, დააჭირეთ Control + Eject-ს და აირჩიეთ სასურველი ოპერაცია.

10.4. Linux სისტემის პროგრამის კლავიშთა კომბინაციები Linux სისტემის მქონე კომპიუტერების კლავიატურა;

(კომბინაციები აღებულია ინტერნეტ გვერდიდან)



4. უმარტივესი მოქმედებები.

ls	მიმდინარე დირექტორიაში ფაილების სია.
cd [დირექტორია]	მიმდინარე დირექტორიის შეცვლა.
cp [რა დავაკოპიროთ][სად დავაკოპიროთ]	ფაილების კოპირება.
mcopу [რა დავაკოპიროთ][სად დავაკოპიროთ]	DOS-ის ფაილურ სისტემასთან მუშაობის დროს ფაილების კოპირება. მაგ: mcopy a:\autoexec.bat ~\junk მსგავსი ბრძანებების (mdir, mcd, mren, mmove, mdel, mmd, mrd, mformat) შესახებ ინფორმაციას გაეცანით man mtolls-ში
mv [რა გადავაადგილოთ] [სად გადავაადგილოთ]	ფაილის გადატანა ან სახელის შეცვლა.
ln -s [რაზე შევქმნათ ბმული] [ბმულის სახელი]	სიმბოლური ბმულის შექმნა.
rm [ფაილები]	ფაილების წაშლა.
mkdir [დირექტორია]	დირექტორიის შექმნა.
rmdir [დირექტორია]	ცარიელი დირექტორიის წაშლა.
rm -r [ფაილები და/ან დირექტორიები]	(რეკურსიული წაშლა) ფაილების, დირექტორიების და მათი ქვედირექტორიების წაშლა.
cat [ფაილის _სახელი] more	ტექსტური ფაილის შიგთავსის ნახვა თითო-თითო გვერდით.
vi [ფაილი]	ფაილის რედაქტირება.
pico [ფაილი]	ტექსტური რედაქტორი.
lynx [html ფაილი ან ბმული]	ტექსტური ბროუზერი lynx
tar -zxvf [ფაილები]	tgz ან tar.gz არქივების გაშლა.
find / -name "ფაილის სახელი"	"ფაილის სახელი" ფაილის მოძებნა. ძებნა იწყება "/" დირექტორიიდან. "ფაილის სახელი" შეიძლება შეიცავდეს ნიშანს ძიებისათვის.
Pine	კარგი ტექსტური-ორიენტული პროგრამა ელექტრონული ფოსტის წასაკითხად. კიდევ ერთ ასეთ პროგრამას ეწოდება elm. pine გამოიყენება "ლოკალური" ფოსტის წასაკითხად, ანუ იმ ფოსტის წასაკითხად, რომელსაც თქვენ გიგზავნით son ან cron პროცესი.

Mc	ფაილური მენეჯერი "Midnight Commander". (გამოიყურება როგორც Norton Commander, მაგრამ თავისი შესაძლებლობებით უფრო Far Managar-თან არის ახლოს).
telnet [სერვერი]	telnet-ით სხვა მანქანებთან დაკავშირება. გამოიყენეთ მანქანის სრული სახელი ან IP მისამართი. შედით თქვენი პაროლის დახმარებით (თქვენ უნდა იყოთ დარეგისტრირებული იმ სხვა მანქანაზე). ეს თქვენ მოგცემთ საშუალებას სხვა მანქანაში შეხვიდეთ და მასზე იმუშავოთ ისე, თითქო მის კლავიატურასთან ზისხართ (თითქმის არავითარი განსხვავება).
ftp [სერვერი]	დაშორებულ მანქანასთან ftp-ით დაკავშირება. კავშირის ეს ტიპი კარგია დაშორებული მანქანიდან ან დაშორებულ მანქანაში ფაილების კოპირებისათვის.
./პროგრამის_სახელი	მიმდინარე დირექტორიაში პროგრამის გაშვება.
Minicom	Minicom - პროგრამა (გამოიყენება როგორც telix Linux-სათვის).
Startx	X-Windows სერვერის და დაყენებული ფანჯარული მენეჯერის გაშვება. ეს ჰგავს იმას, როცა win3.1-ის გასაშვებად dos-ში ჰკრიბავენ "win"-ს.
Xterm	(X ტერმინალში) X-Windows გრაფიკულ გარსში ჩვეულებრივი ტერმინალის გაშვება. გამოსვლისათვის აკრიბეთ "exit".
Xboing	(X ტერმინალში) ძალიან მაგარი, ძველი, კარგი არკანოიდი.
gimp	(X ტერმინალში) ძალიან მძლავრი გრაფიკული რედაქტორი. თავისი შესაძლებლობებით ახლოსაა Photoshop-თან. ძალიან კარგია მხატვრებისათვის.

თავი XI

ციფრული ინფორმაციის გამოთხოვასთან დაკავშირებული საპროცესო და საგამოძიებო დოკუმენტების ნიმუშები

სასამართლოს და მოსამართლის დასახელება

შ უ ა მ დ გ ო მ ლ ო ბ ა ინფორმაციის გამოთხოვის შესახებ

თარიღი:

ადგილი:

შუამავლობის აქტი

(არსებობს ან სად დარჩენი და სად წარმოებს გამოძიება)

(სისხლის სასმართლის საქმის ნომერი)

(დანამუშაოს კვალი/კაცია)

წარმომადგენელი გამოძიებით დადგენილ იქნა, რომ:

საპროცესო საფუძველზე;

საქართველოს სისხლის სამართლის საპროცესო კოდექსის 136-ე მუხლზე პირველი ნაწილით, არსებობს დასაბუთებული ვარაუდი, რომ კომპიუტერულ სისტემაში ან კომპიუტერულ მონაცემთა შესანახ საშუალებაში ინახება სისხლის სამართლის საქმისათვის მნიშვნელოვანი ინფორმაცია ან დოკუმენტი, პროკურორი უფლებამოსილია გამოიძიების ადგილის მიხედვით სასამართლოს მიმართოს შესაბამისი ინფორმაციის ან დოკუმენტის გამოთხოვის განჩინების გაცემის შუამდგომლობით.

აღნიშნული მუხლის მეორე ნაწილით ასეთი ხასიათის საგამოძიებო მოქმედებაზე უნდა დადგეს ფარული საგამოძიებო მოქმედებების ჩატარების წესი.

ფარული საგამოძიებო მოქმედების ჩატარების საფუძველიანობის დასაბუთება;

1. მძიმე დანაშაულის არსებობა;

საქართველოს სსსკ-ის 143-ე ტერმინი მუხლის თანახმად ფარული საგამოძიებო მოქმედება ტარდება მოსამართლის განჩინებით თუ გამოიძიება დაწყებულია ან/და სისხლის სამართლებრივი დევნა ხორციელდება განზრახი მძიმე ან/და განსაკუთრებით მძიმე დანაშაულის ან საქართველოს სისხლის სამართლის კოდექსის 284-ე მუხლით გათვალისწინებული დანაშაულის გამო.

არსებული სისხლის სამართლის საქმეზე გამოიძიება წარმოებს მძიმე დანაშაულისათვის.

2. გამოძიებისათვის მნიშვნელოვანი ინფორმაციის მოპოვება;

საქართველოს სსსკ-ის 143-ე ტერმინი მუხლის მეორე ნაწილის „დ“ ქვეპუნქტის თანახმად, მოთხოვნილი ფარული საგამოძიებო მოქმედების შედეგად მოპოვებული იქნება გამოძიებისათვის არსებითი მნიშვნელობის მქონე ის ინფორმაცია, რომლის სხვა საშუალებით მოპოვება შეუძლებელია ან გაუმართლებლად დიდ ძალისხმევას საჭიროებს.

უიზღოვებლად საქართველოს სისხლის სამართლის საპროცესო კოდექსის 143-ე ტერმინი მუხლის მეორე ნაწილის „ა“ და „დ“ პუნქტებით, პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონით

შ უ ა მ დ გ ო მ ლ ო ბ ა

გასცემს განჩინება, რათა:

ბელოძეძე:

**მოტივირებული დადგენილება
გადაუდებელი აუცილებლობის შემთხვევაში
საგამოძიებო მოქმედების წარმოების შესახებ**

„___“ _____ 201__ წ.

ქ. _____

(დადგენილება გასაცემი პირის სახელი ადგილი,

თანამდებობა, სახელი, გვარი)

განვიხილე რა სისხლის სამართლის № _____ საქმე, დანაშაული
გათვალისწინებული საქართველოს სისხლის სამართლის კოდექსის

და მივიღე მხედველობაში: არსებობს დასაბუთებული ვარაუდი, რომ _____

„დავით“ - უბრალოდ, სახელია და ექსპერტის საგამოძიებო მოქმედება.

საქმის ჩატარების შედეგად არსებული მონაცემები.

ინახება საქმისათვის მნიშვნელობის მქონე ინფორმაცია _____

(საგამოძიებო მოქმედების დასრულება)

ვიბეჭდებ ჩატარებული საქართველოს სსსკ-ის 112-ე მუხლის მე-5 ნაწილით, 1432-1434 მუხლებით

და ვ ა დ გ ი ნ ე:

ვიმართებ არსებობს გადაუდებელი აუცილებლობა:

- დაყოვნებამ შეიძლება გამოიწვიოს გამოძიებისათვის მნიშვნელოვანი ფაქტობრივი მონაცემების განადგურება ან როცა დაყოვნება შეუძლებელს გახდის აღნიშნული მონაცემების მოპოვებას;
- საქმისათვის საჭირო საგანი, დოკუმენტი, ნივთიერება ან ინფორმაციის შემცველი სხვა ობიექტი აღმოჩენილია სხვა საგამოძიებო მოქმედების ჩატარებისას (თუ აღმოჩენილია ზედამართული დათვალიერების შედეგად);
- არსებობს სიცოცხლის ან ჯანმრთელობის ხელყოფის რეალური საფრთხე

(საგამოძიებო მოქმედების დასრულება და დამატებითი მოქმედებების დაწყება)

(საგამოძიებო მოქმედების დასრულება)

ჩატარდეს საგამოძიებო მოქმედება - დადგენილებაში აღნიშნული ინფორმაციის გამოსათხოვად

/ /

დადგენილება გამოგვყავდა:

/ /

რეგიონალური გამოსვლის შესახებ

„...“ 20 წელი
(რეგიონალური გამოსვლის თარიღი)

„...“
(რეგიონალური გამოსვლის თარიღი)

ოქმის შემდგენი პირი: _____
(სახელი, გვარი, თანამდებობა)

სისხლის სამართლის საქმის №:

საგამოძიებო მოქმედების ჩატარების
კონკრეტული ადგილი:

საგამოძიებო მოქმედების
დაწყების დრო: საათი და წუთი: „...“ 20 წელი;
(თარიღი)

საგამოძიებო მოქმედების
დასრულების დრო: საათი და წუთი: „...“ 20 წელი;
(თარიღი)

ინფორმაციის გამოთხოვა განხორციელდა საქართველოს სისხლის სამართლის საპროცესო
კოდექსის 136-ე მუხლის საფუძველზე.

მონაწილე პირები: (რეგიონალური გამოსვლის, დოკუმენტი, განმარტება, საკულისტი, თარგმანი და ა.შ.):

1. _____
(საპროცესო ადვოკატი) (სახელი, გვარი)
2. _____
(საპროცესო სტატუსი) (სახელი, გვარი)

საგამოძიებო მოქმედებაში მონაწილე პირებს საგამოძიებო მოქმედების დაწყებამდე განუმარტათ
მათთვის სისხლის სამართლის საპროცესო კოდექსით გათვალისწინებული უფლებები და
მოვალეობები, საგამოძიებო მოქმედების ჩატარების წესი, მათ შორის უფლება საპროცესო
მოქმედების მიმდინარეობასთან დაკავშირებით გამოთქვან შენიშვნა, დამატება ან შესწორება,
რომელიც აისახება ოქმში.

საგამოძიებო მოქმედების დაწყებამდე _____
(სახელი, გვარი, თანამდებობა, საგამოძიებო მოქმედება)

წარედგინა 20 წლის „...“ № _____ განმარტება ინფორმაციის გამოთხოვის
შესახებ.

(მუხრანა)

საგამომიებო მოქმედებისას გამოყენებული იქნა ტექნიკური
ხაზშაღება: _____

(გამოყენებული ტექნიკური საშუალებების რამდენიმეხელის და მათი გამოყენების პირობები)

რომლის გამოყენების შესახებ წინასწარ ეცნობათ საპროექტო მოქმედების მონაწილეებს.

საგამომიებო მოქმედების მიმდინარეობის აღწერა:

(აღნიშვნა დეტალურად ჩა სწავი)

ინფორმაცია იქნა გამოთხოვილი, რა ფორმით, რა იდენტიფიკაციის ინფორმაციით და გვარდებით ნაშნ თვისების მართივით

აქვე, თვითონ გამოყენებული ქაღალდის პირობების ტიპი, გამოყენებული ტექნიკური საშუალებები და

ბოძებულების დრო, ბოძებულების კონსტრუქციის საფუძველი ან საფუძველი მოსაძებრი ტელეფონის და სხვა საკონტაქტო ნიშნები.

შეგარბისა და გადასაბადების შესახებ ინფორმაცია, ნებისმიერი სხვა ინფორმაცია დამრტავებული საკონტაქტო

აღჭრეულობის ადგილმდებარეობის თაობაზე).

საგამომიებო მოქმედებაში მონაწილე პირის შენიშვნა, შესწორება, დამატება ან
განცხადება:

(შენიშვნის შემტანი პირის სახელი გვარი)

(ხელმოწერა)

ინფორმაციის გამოთხოვის ოქმს გავეცანით, იგი გამომიებლის მიერ შედგენილია
ხრულად და სწორად.

საგამომიებო მოქმედებაში მონაწილე პირები:

(სახელი გვარი)

(ხელმოწერა)

ოქმის შემდგენი პირი:

(სახელი გვარი)

(ხელმოწერა)

ოქმის ასლი მივიღე:

დადგენილება

ინფორმაციის განსაიდუმლოების შესახებ

თარიღი:

ადგილი:

პროკურორის საბუღალსო და გარე ორგანოების

საქმის მართვაში ირგვლივ სხვათა სახელის სახით ნიშნის

მართვის, იმის დასაბუთება

გამოვარკვევები:

გამოძიებით დადგენილი ფაქტობრივი გარემოებები:

ვინაიდან:

დოკუმენტაციის ჩამოთვლა

აქვს საქმისათვის მტკიცებულებითი მნიშვნელობა, რომლის საფუძველზეც უნდა ჩატარდეს შემდგომი საგამოძიებო მოქმედებები, მიზანშეწონილია მიღებული იქნეს გადაწყვეტილება გამოთხოვილი ინფორმაციის და მასთან დაკავშირებული საპროცესო დოკუმენტების განსაიდუმლოების შესახებ, მისი მტკიცებულებების სახით გამოყენების მიზნით, ამასთან აღნიშნული დოკუმენტების განსაიდუმლოება არ ხელყოფს ქვეყნის სასიციფლოდ მნიშვნელოვან ინტერესებს თავდაცვის, ეკონომიკის, საგარეო ურთიერთობის, დაზვერვის, სახელმწიფო უშიშროების და მართლწესრიგის დაცვის სფეროში.

ზემოაღნიშნულიდან გამომდინარე, ვიხელმძღვანელებ რა საქართველოს სსსკ-ის 33-ე მუხლით და „ოპერატიულ-სამეზობრო საქმიანობის შესახებ“ საქართველოს კანონის მე-5 მუხლის 1-ე ნაწილით,

დავადადგინე:

/

განსაიდუმლოებული იქნეს:

დოკუმენტაციის ჩამოთვლა

პროკურორი

/ხელმოწერა/