ელექტრონული მტკიცებულების ამოღება

დასრულებულია: ვერსია 1.01 (15.12.2003)

ევროკავშირის პროექტი პროგრამიდან Oisin II
ადმინისტრირებულია იუსტიციისა და შინაგან საქმეთა საკითხების გენერალური დირექტორატის მიერ

მონაწილე ორგანიზაციები:

A-SIT დაცული საინფორმაციო ტექნოლოგიების ცენტრი - ავსტრია

ავსტრიის ფედერალური შინაგან საქმეთა სამინისტრო

სამართალდამცავ ეროვნულ სპეციალისტთა ცენტრი (დიდი ბრიტანეთი)

Bundesministerium des Innern vertreten

durch MI / Landeskriminalamt Niedersachsen (გერმანია)

Landeskriminalamt Niedersachsen

O.I.P.C. – ინტერპოლის გენერალური სამდივნო

ევროპოლი

ეროვნული კრიმინალური
საგამოძიებო დეპარტამენტი
(შვედეთი)

წინასიტყვაობა

კრიმინალები საინფორმაციო ტექნოლოგიებით ფართოდ სარგებლობენ. ელექტრონული მტკიცებულებების ეფექტური ამოღება მნიშვნელოვან როლს თამაშობს დანაშაულის გამოწვევებთან მუშაობის საქმეში.

ელექტრონული მტკიცებულებების სწორი საექსპერტო დამუშავების გარანტირებისთვის საჭიროა შესაბამისი სახელმძღვანელო პრინციპებისა და ინსტრუქციების შემუშავება. ამგვარი წესები არა მხოლოდ უზრუნველყოფენ მტკიცებულების დაშვებას სასამართლოს მიერ, არამედ შეამცირებენ ზიანის ანაზღაურების მოთხოვნების შესაძლებლობას.

ელექტრონული მტკიცებულების ამოღების თაობაზე წინამდებარე გზამკვლევი, რომელიც ევროკავშირის შესაბამისი დირექტივების დაცვით არის შედგენილი, წინა ხაზზე მომუშავე ყველა ოფიცრისთვის ღირებულ დახმარებას წარმოადგენს დანაშაულის პრევენციისა და მასთან ბრძოლის საქმეში.

ეს გვერდი შეგნებულად არის დატოვებული ცარიელი

წინათქმა

წინამდებარე დოკუმენტის გამოყენება შესაძლებელია ყველა საქმესთან მიმართებით, სადაც ელექტრონული მტკიცებულების ამოღება არის საჭირო.

ყველა წევრმა სახელმწიფომ, წინამდებარე დოკუმენტით შემოთავაზებული ღონისძიებების ინტერპრეტაციისას მხედველობაში უნდა მიიღოს საკუთარი სამართლებრივი დოკუმენტები და რეგულაციები. ამასთან, თითოეულმა წევრმა სახელმწიფომ საკუთარი საექსპერტო სამსახურის საკონტაქტო ინფორმაცია უნდა დაამატოს წინამდებარე დოკუმენტს.

იმ ორგანიზაციამ, ან სამსახურმა, რომელსაც სურს რეკომენდირებული პროცედურების გამოყენება, თითოეული ნაბიჯის/მოქმედების განხორციელებაზე პასუხისმგებელი პირი უნდა დანიშნოს, საკუთარი სტრუქტურის შესაბამისად.

ეს გვერდი შეგნებულად არის დატოვებული ცარიელი

სარჩევი

1. შესავალი

ელექტრონული მტკიცებულება, ელ-მტკიცებულება ან კომპიუტერზე დაფუძნებული მტკიცებულება ეწოდება საგამოძიებო ღირებულების მქონე ინფორმაციას ან მონაცემებს, რომლებიც ელექტრონულ ხელსაწყოში ან ციფრულ საშუალებაში ინახება ან მათი მეშვეობით გადაიცემა. ელ-მტკიცებულება არის [5]
მყიფე და მისი შეცვლა, დაზიანება
ან განადგურება ადვილად შეიძლება მოხდეს. შესაბამისად, ამ მტკიცებულებას ძალიან დიდი სიფრთხილით უნდა მოპყრობა;
ელ-მტკიცებულება ხშირად თითის ანაბეჭდებისა ან დნმ-ის მსგავსად ლატენტურია;
ელ-მტკიცებულების საზღვრებს მიღმა გადატანა ადვილია და
ელ-მტკიცებულება ზოგჯერ დროსთან მიმართებით სენსიტიურია.

საინფორმაციო ტექნოლოგიების[1] სისტემებში გადაცემისას ინფორმაცია აღარ არის იმდენად "მატერიალური", როგორც ის საინფორმაციო ტექნოლოგიების ფართოდ გამოყენებამდე იყო. ელექტრონული მტკიცებულებების ამოღებისას გამომძიებლებს ძირითადად ორი ტიპის პრობლემა უჩნდებათ [3]:
უამრავი ელექტრონული ინფორმაცია არსებობს, რომლის შექმნა, მოდიფიცირება, გადატანა და წაშლა ძალიან სწრაფად შეიძლება.
საინფორმაციო ტექნოლოგიების სისტემები მრავალგვარია. ისინი შესაძლოა, არა მხოლოდ ისეთი მოწყობილობებისგან შედგებოდნენ, რომელთა ამოცნობა ადვილია, როგორც კომპიუტერებისა. საინფორმაციო ტექნოლოგიების შემადგენელი მოწყობილობები შესაძლოა ასევე ნაკლებად ადვილად ამოსაცნობი მოწყობილობები იყოს, როგორებიცაა მობილური ტელეფონები, პეიჯერები, ორგანაიზერები, ფაქსის მანქანები, ან სატელეფონო ავტომოპასუხეები. იგივე შეიძლება მივუსადაგოთ ელექტრონული მონაცემების შემნახველ საშუალებას, რაც შეიძლება იყოს არა მხოლოდ ე.წ. "დისკეტა" ან კომპაქტური დისკი, არამედ ასევე უნივერსალური მეხსიერება (ე.წ. "USB") ან სიმ-ბარათი.

ამ სახელმძღვანელოს უპირველესი სამიზნე პირველი რეაქციის ვალდებულების მქონენი - ანუ პირველი რეაგირების სამართალდამცავი ორგანოების ოფიცრები და/ან საზოგადოებრივი უსაფრთხოების დამცველი სხვა პირები არიან, რომლებიც დანაშაულის ადგილზე ცხადდებიან [5], ისე როგორც სხვა, არა საინფორმაციო ტექნოლოგიების, ექსპერტები. ეს ელექტრონული მტკიცებულების აღმოჩენის, შეგროვებისა და დაცვის მიზნით დამხმარე სახელმძღვანელო უნდა იყოს მათთვის იმ შემთხვევაში, როდესაც საექსპერტო დახმარება უზრუნველყოფილი არ არის. პირველი რეაგირების მქონენი შესაძლოა, ელექტრონულ მტკიცებულებებთან მუშაობისას საექსპერტო დახმარებას ყოველთვის ვერ იღებდნენ. შესაბამისად, მათ ელექტრონული მტკიცებულების სწორად ამოღებისა და შენახვისთვის სპეციალური მომზადება სჭირდებათ. კარგი

[1] საინფორმაციო ტექნოლოგიები - IT

პრაქტიკის დამკვიდრება ხელს შეუწყობს დანაშაულის ადგილზე ექსპერტის არ ყოლის მიზეზით ელექტრონული მტკიცებულების დაკარგვის ან დაზიანების მინიმიზირებას შეუწყობს ხელს. წინამდებარე დოკუმენტის მიზანი ამგვარი ელექტრონული მტკიცებულების მოძიების, ამოცნობის, შეგროვებისა და დოკუმენტირების კარგი პრაქტიკის რეკომენდირებაა [1].

1.1 დოკუმენტის მეგზური

წინამდებარე დოკუმენტი შემდეგნაირად არის ორგანიზებული:
მე-2 თავი ელექტრონულ მტკიცებულებაზე მუშაობისას დასაცავ ზოგად პრინციპებს შეეხება.
მე-3 თავი ელექტრონული მტკიცებულების ამოღების ძირითად ტიპებს განიხილავს.
მე-4 თავი აღწერს ამოღების ზოგადი პროცედურის მთავარ ფაზებს აღწერს.
მე-5 თავი ელექტრონული მოწყობილობების სხვადასხვა ტიპის გამოყენების დეტალურ ინსტრუქციებს მოიცავს.

ამ მეგზურში გამოყენებული ტერმინების განსაზღვრებები მე-7 თავშია მოცემული, სადაც სხვადასხვა მოწყობილობების სურათებიც მოცემულია.
ელექტრონული მოწყობილობების PDA-ების ამოღების ორი ჯიბის წიგნაკი მოცემულია მე-8 თავში (დანართი ა). მე-9 თავი (დანართი ბ) წინასწარი ინტერვიუების მაგალითებს, აღწერის სიის მაგალითსა და ქსელთან დაკავშირებული რეკომენდირებული კითხვების ჩამონათვალს მოიცავს.
დამატებითი ინფორმაციისთვის იხლეთ მე-6 თავი (წყაროები) და მე-10 თავი (დანართი გ: ბიბლიოგრაფია შენიშვნებთან ერთად).

2. ზოგადი პრინციპები

ელექტრონული მტკიცებულების დამუშავებისას უმნიშვნელოვანესია ზოგადი პრინციპების [1-3] დაცვა შემდეგ საკითხებთან დაკავშირებით:
დანაშაულის ადგილზე მოწმეობა,
მონაცემთა შეუბღალველობა,
საკონტროლო ჟურნალი,
ექსპერტული მხარდაჭერა,
ოფიცრების მომზადება და
პრინციპების კანონიერება და მათი დაცვა.

ორი პრინციპი მომდევნო პარაგრაფებშია განხილული.

2.1 დანაშაულის ჩადენის ადგილზე მოწმეობა

პრინციპი: *ოფიცერი დანაშაულის ჩადენის ადგილზე მარტო არასდროს უნდა გამოცხადდეს [2].*

ამგვარ საქმიანობაში მინიმუმ ორი ოფიცერი უნდა იყოს ჩართული. ამით ერთის მხრივ ოფიცერთა დაცვის უზრუნველყოფა ხდება ხოლო მეორეს მხრივ კი დანაშაულის ადგილზე უფრო მეტი დეტალის დაფიქსირებას უწყობს ხელს. ოფიცრებმა საკუთარი მოქმედებები უნდა

დაგეგმონ და შეათანხმონ. გაუთვალისწინებელი პრობლემის შემთხვევაში მათი გადაწყვეტა უფრო ადვილია, რადგა "ორი თავი ერთს სჯობია".

2.2 მონაცემთა შეუბღალველობა

პრინციპი: *სამართალდამცავი ორგანოებისა ან მათი ოფიცრების არც ერთმა ქმედებამ არ უნდა შეცვალოს ელექტრონული მოწყობილობების ან მონაცემთა შემნახველი საშუალება, რაზეც შემდეგ სასამართლოში დაყრდნობა შეიძლება მოხდეს.*

ელექტრონული მოწყობილობებისა და მონაცემების დამუშავებისას არც პროგრამულ და არც ტექნიკურ ნაწილში მათი შეცვლა არ უნდა მოხდეს. დანაშაულის ადგილზე მოპოვებული მასალის დაცვის, და შესაბამისად მიღებული მასალის ექსპერტიზის ჩატარების პროცესის დაწყების ვალდებულება სამართალდამცავი ორგანოს ოფიცერს ეკისრება [2].

2.3 საკონტროლო ჟურნალი

პრინციპი: *საკონტროლო ჟურნალი ან ეკექტრონულ მტკიცებულებებთან მოპყრობის ამსახველი ყველა ქმედების ამსახველი სხვაგვარი ჩანაწერები უნდა შედგეს და იქნეს შენახული. დამოუკიდებელ მესამე მხარეს შექმნილი ჩანაწერების მეშვეობით იმავე შედეგის მიღწევის შესაძლებლობა უნდა მიეცეს.*

მესამე მხარისთვის დანაშაულის ადგილზე გამოცხადებული პირველი ოფიცრის მიერ განხორციელებული ყველა ქმედების ზედმიწევნით დაფიქსირება უმნიშვნელოვანესია, რათა ჩანაწერების სასამართლოში გამოყენების შესაძლებლობა იყოს უზრუნველყოფილი. ელექტრონული მტკიცებულების ამოღებასთან, მის ხელმისაწვდომობასთან, შენახვასა და გადაცემასთან დაკავშირებული ყველა ქმედება სრულად დოკუმენტირებული, შენახული და განსახილველად მუდამ მზად უნდა იყოს [4].

2.4 ექსპერტული მხარდაჭერა

პრინციპი: *თუ ივარაუდება, რომ პოლიციის მიერ ჩატარებული ოპერაციისას ელექტრონული მტკიცებულების აღმოჩენაა შესაძლებელი, პასუხისმგებელმა ოფიცერმა დროულად უნდა შეატყობინოს ექსპერტებს/გარე მრჩევლებს* [2].

იმ გამოძიებისთვის, რომლებიც ელექტრონული მტკიცებულების ჩხრეკასა და ამოღებას მოიცავენ, გარე ექსპერტებთან კონსულტაციის საჭიროება შესაძლოა, დადგეს. ყველა ექსპერტისთვის ცნობილი უნდა იყოს ამ ან სხვა მსგავს სახელმძღვანელოში გამყარებული პრინციპები. ექსპერტს უნდა ჰქონდეს [1]:
სფეროს სპეციალური ცონდა და შესაბამისი გამოცდილება,
საჭირო საგამოძიებო და სამართლებრივი ცოდნა,
საჭირო კონტექსტური და სამართლებრივი ცოდნა და
შესაბამისი კომუნიკაციის უნარები (როგორც წერილობითი ისე ზეპირი განმარტებებისთვის).

2.5 ოფიცრების მომზადება

პრინციპი: *პირველი მარეაგირებლები შესაბამისად უნდა იყვნენ მომზადებულნი ელექტრონული მტკიცებულებების მოსაძიებლად და ამოსაღებად იმ შემთხვევისთვის, თუ დანაშაულის ადგილზე ექსპერტები არ არიან* [3].

განსაკუთრებულ შემთხვევებში, როდესაც საჭიროა, რომ პირველი რეაგირების მომხდენმა შეაგროვოს ელექტრონული მტკიცებულება და/ან მიიღოს ელექტრონულ მოწყობილობასა ან ციფრულ შემნახველ საშუალებაში არსებული პირველადი მონაცემები, მისი შესაბამისი მომზადება უნდა მოხდეს შესაბამისი ღონისძიებების მართებულად გასატარებლად და საკუთარი ქმედებების საჭიროებისა და შედეგების ასახსნელად [1].

2.6 პრინციპების კანონიერება და მათი დაცვა

პრინციპი: *საქმეზე პასუხისმგებელი ოფიცერი და სამსახური კანონის, ზოგადი ექსპერტიზისა და პროცედურული პრინციპებისა და ზემოთ ჩამოთვლილი პრინციპების დაცვის უზრუნველყოფაზე პასუხისმგებელნი არიან. ეს ელექტრონული მტკიცებულებების ფლობასა და მათზე წვდომას შეეხება* [1, 4].

ყველა წევრმა სახელმწიფომ მხედველობაში უნდა მიიღოს საკუთარი სამართლებრივი ბაზა ამ დოკუმენტით შემოთავაზებული ღონისძიებების ინტერპრეტაციისას.

საერთაშორისოდ მნიშვნელოვანი ერთ-ერთი დოკუმენტი, ევროპის საბჭოს კონვენცია კომპიუტერული დანაშაულის შესახებ (2003 წლის ივლისისთვის) ღიაა წევრი სახელმწიფოებისა და ამ დოკუმენტის ტექსტის შემუშავებაში მონაწილე მხარეების მიერ ხელმოსაწერად და სხვა სახელმწიფოების მიერ მასთან მისაერთებლად [6].

3. ამოღების ტიპები

ელექტრონული მტკიცებულების ამოღების ოთხი ძირითადი ტიპი არსებობს [2-3]:

- ელექტრონული მოწყობილობებისა და მონაცემთა შესანახი საშუალების კონფისკაციით;
- სრული მეხსიერების შემადგენლობის ასლის გაკეთებით (გამოსახულების ხელახალი შექმნით ან სარკისებური პრინციპით არეკვლით);
- მონაცემთა შენახვის სარეზერვო (ბექაფ) შემნახველი საშუალების კონფისკაციით; და
- შერჩევითი მონაცემთა ასლის გაკეთებით.

ამოღების სხვადასხვა ტიპს განვიხილავთ მომდევნო ნაწილში. ყურადსაღებია ის ფაქტო, რომ ამოღების სხვადასხვა ტიპის ერთდროულად გამოყენება შესაძლებელია ამოღების ერთი პროცედურის ჩატარებისას. მაგალითად, შესაძლოა, საჭირო გახდეს როგორც ელექტრონული მოწყობილობის კონფისკაცია, ისე მონაცემთა შენახვის სარეზერვო (ბექაფ) შემნახველი საშუალების კონფისკაცია.

3.1 ელექტრონული მოწყობილობისა და მონაცემთა შემნახველი საშუალების ამოღება

ამ ტიპის ამოღება შემდეგ შემთხვევებში შეიძლება იყოს გამოსაყენებელი:

თუ საკონფისკაციო არ არის ბევრი მოწყობილობა, მაგ., ცალკე მდგომი პერსონალური კომპიუტერი ან მცირე ქსელი (მაგ., ეჭვმიტანილის საცხოვრებელში);

დიდი ფინანსური ან სხვა სახის ზარალის რისკი არსებობს, რომელიც შესაძლოა, გამოწვეული იყოს კონფისკირებული მოწყობილობის უმოქმედობით/გამოუყენებლობით/ხელმიუწვდომლობით;

კონფისკაცია აბსოლუტურად საჭიროა კონკრეტული დანაშაულის ხასიათიდან გამომდინარე;

საკონფისკაციო მოწყობილობით მხარდაჭერილი მოქმედების შეწყვეტა საჭიროა/მოთხოვნილია.

ამ ტიპის ამოღების უპირატესობა შემდეგია:

მისი ჩატარება ჩვეულებრივ შესაძლებელია დანაშაულის ადგილზე ექსპერტის ყოფნის გარეშე;

ამოღების პროცედურა ჩვეულებრივ დიდ დროს არ მოითხოვს;

ელექტრონული მტკიცებულება კონტროლს ქვეშ ხვდება; და

ელექტრონული მტკიცებულება კონტროლირებულ გარემოში შეიძლება გაანალიზდეს.

ამ ტიპის ამოღების უარყოფითი მხარეები შემდეგია:

აღჭურვილობის დაზიანების რისკი არსებობს;

კონკრეტულ დანაშაულთან კავშირის არ მქონე ადამიანების დაზარალების რისკი არსებობს; და

კონკრეტულ დანაშაულთან კავშირის არ მქონე ქმედებებში ჩარევის რისკი არსებობს.

ამოღების პროცესი აღწერილია მე-4 და მე-5 თავებში.

3.2 მთელი მეხსიერების მონაცემების ასლის გაკეთება

ამ ტიპის ამოღებისთვის, რომელსაც ზოგჯერ გამოსახულების ხელახლა შექმნას ან სარკისებური პრინციპით არეკვლას უწოდებენ, სპეციალური მოწყობილების გამოყენება ხდება ელექტრონული მოწყობილობის (ან ელექტრონული მონაცემების შემნახველი საშუალების) მეხსიერების შინაარსის ზუსტი ასლის შექმნისთვის მონაცემთა შენახვის გარეშე საშუალებაზე.

ამ ტიპის ამოღება შესაძლოა, ხელსაყრელი იყოს შემდეგ შემთხვევებში:

მხედველობაში მოწყობილობების მნიშვნელოვანი რაოდენობაა მისაღები (მაგ., მცირე ან საშუალო ზომის საწარმო);

დიდი ფინანსური ან სხვა სახის ზარალის რისკი არსებობს, რომელიც შესაძლოა, გამოწვეული იყოს კონფისკირებული

მოწყობილობის უმოქმედობით/გამოუყენებლობით/ხელმიუწვდომლობით (მაგ., ელექტრონული ტექნოლოგიების სისტემა ეჭვმიტანილისთვის ან მესამე მხარისთვის საციცოხლო მნიშვნელობისად შეიძლება იყოს მიჩნეული); და

კონფისკაცია არ არის მიჩნეული საჭიროდ კონკრეტული დანაშაულის ხასიათიდან გამომდინარე.

ამ ტიპის ამოღების უპირატესობა შემდეგია:

მოწყობილობის დაზიანების მცირე რისკი;

კონკრეტულ დანაშაულთან კავშირის არ მქონე პირების დაზარალების მცირე რისკი;

კონკრეტულ დანაშაულთან კავშირის არ მქონე ქმედებებში ჩარევის მცირე რისკი; და

ელექტრონული მტკიცებულების გაანალიზება შეიძლება მოხდეს კონტროლირებულ გარემოში.

ამ ტიპის ამოღების უარყოფითი მხარეები შემდეგია:

დანაშაულის ადგილზე სპეციალური მოწყობილობაა საჭირო;

ექსპერტის დახმარება როგორც წესი დანაშაულის ადგილზე საჭიროა;

მტკიცებულების ნაწილის მხედველობიდან გამორჩენის რისკია;

ამოღების პროცედურა დროს მოითხოვს; და

შესაბამისი აღჭურვილობა კონტროლს ქვეშ არ ხვდება.

3.3. ამოღება მონაცემთა შენახვის სარეზერვო (ბექაფ) შემნახველი საშუალების კონფისკაციით

ამოღების ეს ტიპი შესაძლოა იმავე სიტუაციებში იყოს მოსახერხებელი, როგორშიც მთელი მეხსიერების მონაცემების ასლის გაკეთებაა (იხ. თავი 3.2), ეს განსაკუთრებით მაშინ, თუ მხედველობაში მისაღები მოწყობილობები და მონაცემები ძალიან დიდი რაოდენობით არის (მაგ., დიდი ქსელები, უნივერსალური გამომთვლელი მანქანების გარემო).

დადებითი მხარეები მე-3.2 თავში აღწერილის მსგავსია (ზიანის ან დამაზარალებელი ქმედებების რისკი პრაქტიკულად არ არის). დამატებითი დადებითი მხარეებია ის, რომ:

დანაშაულის ადგილზე სპეციალური აღჭურვილობა საჭირო არ არის; და

დანაშაულის ადგილზე ხანგრძლივი ასლის გადასაღები პროცედურების ჩატარების საჭიროება არ არის.

ამ ტიპის ამოღების უარყოფითი მხარეები შემდეგია:

ექსპერტის მხარდაჭერა ჩვეულებრივ საჭიროა დანაშაულის ჩადენის ადგილზე;

ადგილობრივი სისტემის ადმინისტრატორის მხარდაჭერა ჩვეულებრივ საჭიროა;

მტკიცებულების ნაწილის მხედველობიდან გამორჩენის რისკი არსებობს (რადგან სარეზერვო (ბექაფ) მონაცემების სისრულე ჩვეულებრივ წინასწარ არ შეიძლება იყოს ცნობილი); და

შესაბამისი აღჭურვილობა არ არის კონტროლს ქვეშ.

3.4 შერჩევითი მონაცემთა ასლის გაკეთებით

ამ ტიპის ამოღება მხოლოდ გამონაკლის შემთხვევებში უნდა განხორციელდეს, თუ არც ერთი ზემოთ ჩამოთვლილი ამოღების ტიპის გამოყენება შესაძლებელი არ არის, ანუ, მხოლოდ შერჩეული (ანუ, ყველაზე მნიშვნელოვანი) მონაცემის კოპირებაა შესაძლებელი შედგომ ანალიზის ჩასატარებლად. **ექსპერტის მხარდაჭერა** ჩვეულებრივ საჭიროა დანაშაულის ჩადენის ადგილზე.

მონაცემთა კოპირებისთვის გამოიყენეთ შესაბამისი[2] ამოღების დისკი/კომპაქტ დისკი. ამასთან, მოძებნის კრიტერიუმების შესაბამისი ერთობლიობა უნდა იყოს ხელმისაწვდომი. შესაბამისი მონაცემების ძებნა დაფუძნებული შეიძლება იყოს ძირითად სიტყვებზე (ქი ვორდებზე) და უნდა მოიცვას ფაილების მთელი სისტემა და მასალის შენახვის მთელი საშუალება (მაგ., ფაილის სახელის გაფართოება შეიძლება შეცვლილი იყოს. ამდენად, მხოლოდ ფაილის სპეციფიური ტიპის ძებნა საკმარისი არ იქნება; ამასთან, ჩვეულებრივ შეუძლებელია იმ მონაცემების პოვნა, რომლებიც შენახულია როგორც არქივი, დისკის მიუწვდომელი ნაწილები, ან დაფარული ან დაშიფრული ფაილები სტანდარტული ძირითადი სიტყვებით (ქი ვორდებით) ძებნისას).

ამ ტიპის ამოღების უპირატესობები და უარყოფითი მხარეები მონაცემთა შენახვის სარეზერვო (ბექაფ) შემნახველი საშუალების კონფისკაციის მსგავსია (იხ. მე-3.3 თავი). კიდევ ერთი უარყოფითი მხარე იქნება ის, რომ კომპიუტერის სისტემის ნებისმიერი ისტორიული რეკონსტრუქცია შეუძლებელი იქნებოდა. ეს მათ გამოძიების ღირებულებას სერიოზულად შეამცირებდა. ამასთან ერთად, განსაკუთრებული ყურადღება უნდა მიექცეს ამგვარად ამოღებული ინფორმაცის მტკიცებულებითი ღირებულების შენარჩუნებას.

4 ელექტრონული მტკიცებულების ამოღების პროცედურა

როგორც შესავალში აღვნიშნეთ, წინამდებარე დოკუმენტი ელექტრონული მტკიცებულებების ამოღების პროცედურაზე აკეთებს აქცენტს, რაც მოიცავს ელექტრონული მტკიცებულების ძიებას, ამოცნობას, მოგროვებასა და დოკუმენტირებას. პროცედურე შემგედი გაზებისგან შედგება [5], რომელბიც მომდევნო თ ვეშია აღწერილია:

ამოღებისთვის მომზადება (ნაწილი 4.1),
დანაშაულის ადგილის დაცვა (ნაწილი 4.2),
დანაშაულის ადგილის დოკუმენტირება (ნაწილი 4.3),
მტკიცებულები მოგროვება (ნაწილი 4.4), და
შეფუთვა, გადატანა და შენახვა (ნაწილი 4.5).

ბლოკ-სქემა/ჯიბის წიგნაკი რომელიც ძირით დ ნბიჯებს აღწერს, მოცემულია მე-8 თავში (დანართი ა).

[2] მაგ., ცარიელი და ვირუსებისგან თავისუფალი

საინფორმაციო ტექნოლოგიების გარემოს ჩხრეკის ძირითადი პრინციპები, რომლების რეკომენდირებას ახდენს ევროკავშირის საბჭო [3] სრულად იყო მხედველობაში მიღებული მომდევნო თავებში აღწერილი პროცედურების წერისას. ზოგადი პოლიტიკის ტექნიკისა და პრაქტიკის გათვალისწინებაც [12] ასევე რეკომენდირებულია.

4.1 ამოღებისთვის მომზადება

წინასწარი გამოძიებისას, რომელიც ჩხრეკის შესახებ ნებართვის მიღებაზეა ორიენტირებული, უნდა განისაზღვროს, ელექტრონული მტკიცებულება, რომელიც მნიშვნელოვანი შეიძლება იყოს საქმისთვის, იქნება თუ არა ნაპოვნი. ამგვარ შემთხვევაში პასუხისმგებელმა ოფიცერმა უნდა შეატყობინოს მონაცემთა მიღების ადგილობრივ სამსახურს და/ან გარე ექსპერტებს უმოკლეს დროში [2]. პირველი გადაწყვეტილება, რომელიც უნდა იქნეს მიღებული, არის რა ტიპის ამოღება უნდა განხორციელდეს (ამოღების ტიპების მე-3 თავშია განხილული). იმ საინფორმაციო ტექნოლოგიების სისტემის შესახებ, რომლის ამოღებაც უნდა განხორციელდეს, მაქსიმალური ინფორმაციის შეგროვება უნდა მოხდეს წინასწარ და ექსპერტის მხარდაჭერით, როგორიც არის, მაგალითად:

კომპიუტერის ჰარდვეარის/ოპერაციული სისტემის/პროგრამული უზრუნველყოფის/პროგრამული აპლიკაციის/და მონაცემთა შენახვის საშუალებასთან დაკავშირებული ინფორმაცია,

კომუნიკაციასა და ქსელთან დაკავშირებული ინფორმაცია (ინტერნეტ მომსახურების მომწოდებელი[3], ტელეფონი, ფაქსი, მოდემი, ადგილობრივი ქსელი[4], ქსელის აღჭ რვილობა, სხვ.),

ვინ არის პასუხისმგებელი კომპიუტერულ სისტემაზე და/ან ქსელზე (მაგ., ჰყავს თუ არა მას ადგილობრივი ადმინისტრატორი თუ მისი ადმინისტრირება გარე კომპანიის მიერ ხდება),

რა რაოდენობის აღჭურვილობის ამოღებაა მოსალოდნელი (მე-3.1 თავში აღწერილი ამოღების ტიპის შესაბამისად),

რა რაოდენობის მონაცემების კოპირება უნდა მოხდეს (მე-3.2 და მე-3.4 თავებში აღწერილი ამოღების ტიპების შესაბამისად) და

არსებობს თუ არა სისტემის ბექაფი შენახვის საშუალებაზე (მე-3.3 თავში აღწერილი ამოღების ტიპის შესაბამისად).

მომზადების ფაზა შემდეგ ნაბიჯებს მოიცავს:

ელექტრონული მტკიცებულების ამოღების ნებართვის სწორად გაცემის უზრუნველყოფა (მაგ., შესაბამისი კანონის დაცვით მოპოვებული ჩხრეკის უფლება);

ამოსაღები საინფორმაციო ტექნოლოგიების შესახებ მაქსიმალური ინფორმაციის მოგროვება (იხ. ზემოთ);

ჯგუფის წევრების შერჩევაა (გარეშე ექსპერტების ჩართვით, თუ ეს საჭიროა);

ჯგუფის წევრებზე ინდივიდუალური ვალდებულებების გადანაწილება;

---

[3] ISP - ინტერნეტის მომსახურების მომწოდებელი

[4] LAN - ადგილობრივი ქსელი

ჯგუფის წევრებთან საუბარი იმასთან დაკავშირებით, თუ როგორ განახორციელონ მათზე დაკისრებული ვალდებულებები (მათ შესაბამისი ზოგადი მომზადება გავლილი უნდა ჰქონდეთ); და

ამოღებისთვის საჭირო ხელსაწყოების, საშუალებებისა და აღჭურვილობის მოწიდება (ლოგისტიკა).

როგორც უკვე აღინიშნა, ყველა ქმედება უნდა შეესაბამებოდეს სამსახურის პოლიტიკას, ევროკავშირის, სახელმწიფოსა და ადგილბრივ სამართლებრივ ბაზას.

4.1.1 ამოღების ჯგუფის წევრები

თუ ცნობილია, რომ ელექტრონული მტკიცებულებები იქნება ნაპოვნი დანაშაულის ადგილზე, ამოღების ჯგუფში უნდა შევიდნენ საინფორმაციო ტექნოლოგიების აღჭ რვილობისა და ელექტრონული მტკიცებულების ჩხრეკისა და ამოღებისთვის სპეციალურად მომზადებული ოფიცრები. ზოგ შემთხვევაში დამოუკიდებელ ექსპერტთა რჩევაც შეიძლება საჭირო იყოს (იხ. ასევე მე-2.4 ნაწილი). მაგალითად, თუ სისტემის ადმინისტრირება გარეშე კომპანიის ან ადმინისტრატორის მიერ ხორციელდება, მათი, როგორც ექსპერტი მოწმის, ჩართვა შეიძლება იყოს განხილული (თუ ისინი ეჭვმიტანილებად არ მიიჩნევიან). მინიმალური მოთხოვნაა ის, რომ პირველი რეაგირების მომხდენი ოფიცრები ელექტრონული მტკიცებულების მოგროვების შესახებ მინიმალურ დონეზე გაწრთვნილნი უნდა იყვნენ.

ჯგუფის წევრების შერჩევა და მათზე პასუხისმგებლობის გადანაწილება უნდა მოხდეს პასუხისმგებელი ოფიცრის მიერ, ამოღების პროცედურის ფაზების შესაბამისად (იხ. ასევე მე-4 თავის დასაწყისი). ფაზები და შესაბამისი ფუნქციები მომდევნო თავებშია განხილული (მე-4.2-4.5 თავები).

ჯგუფის ყველა წევრს შესაბამისი ინსტრუქცია უნდა ჰქონდეთ მიღებული საკუთარი ფუნქციების შესრულების თაობაზე. მაგ., მათ უნდა იცოდნენ, როდის გამოიყენონ იგივე პრინციპები ელექტრონულ მტკიცებულებასთან მუშაობისას, რომელსაც გამოიყენებენ სხვა ფიზიკურ მტკიცებულებასთან მუშაობისას, და როდის გამოიყენონ ზოგი სპეციალური ღონისძიება (მაგ., ალუმინიუმის ფხვნილის გამოყენება არ უნდა მოხდეს ელექტრონული მოწყობილობებიდან თითების ანაბეჭდების ასაღებად). მათ ასევე უნდა იცოდნენ, რომ ზოგ შემთხვევაში ისინი საექსპერტო დანაყოფს უნდა დაუკავშირდნენ და შესაბამისად, ეს საკონტაქტო ინფორმაცია წინასწარ უნდა მოიძიონ.

4.1.2 ამოღების საშუალებები და აღჭურვილობა

სპეციალური საშუალებები და აღჭურვილობა შეიძლება იყოს საჭირო ელექტრონული მტკიცებულების შესაგროვებლად. ტექნოლოგიურმა წინსვლებმა შეიძლება მოთხოვნილი საშუალებებისა და აღჭურვილობის შეცვლა შეიძლება მოითხოვოს. შესაბამისი აღჭურვილობა/ძირითადი საშუალებების ნაკრები შესაძლოა,

გამოსადეგი იყოს ჩხრეკისა და ამოღებისას და ამ აღჭ რვილობით ჯგუფის წევრების უზრუნველყოფა უნდა მოხდეს ჯგუფის იმ წევრის მიერ, რომელიც ლოგისტიკაზეა პასუხისმგებელი [1,2,5]:

დემონტაჟისა და მოცილების ხელსაწყოები:

სახრახნისები (ბრტყელი და ჯვარედინი, და მწარმოებლის სპეციფიკის გათვალისწინებით, მაგ., Compaq, Macintosh);

ქანჩგასაღებები (ექვსკუთხოვანი, ვარსკვლავისებური და ბასრპირა);

ბრტყელტუჩები (სტანდარტული და ნემსისებური პირით);

გაყვანილობის გადამჭრელები (კაბელების ხაზების გამოსაცალკევებლად);

პატარა პინცეტები;

დოკუმენტირება: ჩხრეკისა და ამოღების აღნუსხვა (საკუთრების რეესტრი);

დასაკრავი ქაღალდები და ლენტა (სისტემის შემადგენელი ნაწილების აღსანიშნად და იდენტიფიცირებისთვის, მათ შორის ჩასართავების);

კაბელების თავები;

ლუქები (შემოსაკრავი და მისაწებებელი);

სხვა საჭირო ფორმები (იხ. მე-9 თავი);

არა ჩამორეცხვადი ფერადი მარკერი პასტები (ამოღებული ნივთების კოდირებისა და იდენტიფიცირებისთვის);

კამერა და/ან ვიდეო კამერა (დანაშაულის ადგილისა და ეკრანზე გამოტანილი ნებისმიერი ელემენტის ფოტოგრაფირებისთვის);

შეფუთვისა და ტრანსპორტირების ხელსაწყოები:

ანტისტატიკური ჩანთები (გატანილი აღჭურვილობის, როგორიც შეიძლება იყოს სამონტაჟო პლატა, დასაცავად; მასალა, რომელსაც სტატიკური ელექტრო ებერგიის შექმნა შეუძლია, როგორიცაა პოლიეთილენის ჩანთები, არ უნდა იყოს გამოყენებული);

ანტისტატიკური ბურთულებიანი შესაფუთი მასალა;

კაბელის შესაფუთები (კებელების უსაფრთხოდ დასამაგრებლად);

მტკიცებულების შესანახი ჩანთები და ლენტები;

ფლოპი დისკეტების შესანახი ყუთები, JAZ/ZIP-კარტრიჯები, DVD-ები ან CD-ები;

შესაფუთი მასალა (მასალა, რომელსაც სტატიკური ელექტრო ენერგიეს წარმოება შეუძლია, როგორიცაა პენოპლასტი ან პენოპლასტის მსგავსი მასალა არ უნდა იყოს გამყენებული);

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 ინფორამცია (მაგ., საექსპერტო დანაყოფის ტელეფონის ნომრები).

სხვა ნივთები:

ჯიბის ფანარი სამაგრით;

ხელთათმანი;

ხელის ურიკა;

დიდი ზომის რეზინის შესაფუთი საშუალებები;

ლუპა;

პრინტერის ქაღალდი;

ამოსაღები დისკი/კომპაქტ დისკი (თუ გაწრთვნილია მისი ექსპერტიზისთვის გამოსაყენებლად);

გამოუყენებული ფლოპი დისკეტები;

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

4.2 დანაშაულის ადგილის დაცვა

პირველი რეაგირების მომხდენმა ყველა ადამიანის უსაფრთხოება უნდა დაიცვას დანაშაულის ადგილზე და ყველა მტკიცებულების, როგორც ტრადიციულის, ისე ელექტრონულის შეულახველობა.

ეს ფაზა შემდეგ ნაბიჯებს მოიცავს [5,2]:

დაიცავით იურისდიქციული პოლიტიკა დანაშაულის ადგილის დასაცავად;

ყველა ადამიანი გაარიდეთ უშუალო ადგილს, სადაც მტკიცებულების მოგროვება უნდა მოხდეს (მათ შორის აღჭურვილობასა და ელექტრო ენერგიეს წყაროს);

წაშლადი მონაცემები დაიცავით ფიზიკურად და ელექტრონულად;

წაშლადი მონაცემის შემცველი თითოეული მოწყობილობის იდენტიფიცირება, დაცვა, დოკუმენტირება და ფოტოგრაფირება მოახდინეთ (მე- 5.1 და მე-5.2 თავები);

დააკვირდით სავარაუდო ეჭვმიტანილებსა და სხვა ადამიანებს მათ მიერ მტკიცებულების შეცვლისა ან დაზიანების ასაცილებლად;

საინფორმაციო ტექნოლოგიების კომპონენტებს დააკვირდით მტკიცებულებების შეცვლისა ან დაზიანების თავიდან ასარიდებლად;

მოახდინეთ დაკავშირებული ელექტრონული კომპონენტების იდენტიფიცირება და დოკუმენტირება, რომლის წაღებაც ვერ მოხდება;

მოწყობილობასთან დაკავშირებული ტელეფონისა და ქსელის ხაზების იდენტიფიცირება და დოკუმენტირება მოახდინეთ და აღნიშნეთ იარლიყით;

გადაწყვიტეთ, გჭირდებათ თუ არა ამ მოწყობილობიდან სხვა მკიცებულების აღება (მაგ., დნმ, თითის ანაბეჭდები, ნარკოტიკი, კატალიზატორები);

თუ ასეა, დაიცავით ზოგადი პროცედურა ამ ტიპის მტკიცებულების მოსაპოვებლად;

გადადეთ განადგურების ტექნიკის გამოყენება მას **შემდეგ** პერიოდამდე, სანამ არ მოხდება ელექტრონული მტკიცებულების აღდგენა;

მოაგროვეთ ლატენტური ანაბეჭდები **მას შემდეგ**, რაც ელექტრონული მტკიცებულების აღდგენა დასრულდება (რადგან კომპიუტერის კლავიატურაზე, მაუსზე, დისკეტებზე, კომპაქტურ

დისკებზე, ან სხვა კომპონენტებზე შესაძლოა, ლატენტური თითის ანაბეჭდები ან სხვა ფიზიკური მტკიცებულება იყოს, შესანახი);

არ გამოიყენოთ ალუმინის ფხვნილი თითის ანაბეჭდების ასაღებად დანაშაულის ჩადენის ადგილიდან - ამან შეიძლება აღჭურვილობა და მონაცემები დააზიანოს.

დანაშაულის ჩადენის ადგილზე ეძებეთ არა-ელექტრონული, მაგრამ დაკავშირებული მტკიცებულებები, როგორიცაა:

დაწერილი პასვორდები და სხვა ხელით ჩანაწერები,

ქაღალდის ბლოკნოტები ჩანაწერებით,

კომპიუტერული ჰარდვეარისა და სოფთვეარის სახელმძღვანელო, კალენდრები ან დღიურები,

ტექსტური ან გრაფიკური ამონაბეჭდები კომპიუტერიდან,

ფოტოები, ან

პერსონალური ინტერესების შესახებ იფნორმაცია, რაც შემდეგ შესაძლოა გამოსადეგი იყოს პასვორდების გამოსაცნობად (პასვორდების უმრავლესობა პირდაპირ დაკავშირებულია უშუალო გარემოსთან, როგორიცაა მაგ., მანქანის ნომერი, პარტნიორები/ბავშვები, ტელეფონის ნომრები, ჰობი, ა.შ.)

ჩაატარე წინასწარი გამოკითხვები;

ყველა ადამიანი დააშორეთ ერთმანეთს და მოახდინეთ მათი იდენტიფიცირება (მოწმეები, სუბიექტები ან სხვ.) დანაშაულის ჩადენის ადგილზე და ჩაინიშნეთ მათი მდებარეობა ამ ადგილზე მისვლისას;

მე-9 თავში მოცემული ან მსგავსი ფორმები/საკონტროლო სიები გამოიყენეთ ამ პირებისგან ინფორმაციის მოგროვებისა და ჩანიშვნისთვის;

თქვენი სამსახურის პოლიტიკისა და სამართლებრივი ბაზის დაცვით ამ პირებისგან მოიპოვეთ შემდეგი ინფორმაცია:

აღჭურვილობის/სისტემის მიზანი (მაგ., ბუღალტერიის წარმოება);

აღჭურვილობის/სისტემის მფლობელები და/ან მოსარგებლენი, რომლებიც დანაშაულის ადგილზე არიან, ისე როგორც პასვორდები (იხ. ქვემოთ), იუზერის სახელები, და ინტერნეტის მომსახურების მომწოდებელი;

სისტემაში, სოფთვეარში შესასვლელად ან მონაცემის მისაღებად საჭირო ნებისმიერი პასვორდი (პირს შესაძლოა რამდენიმე პასვორდი ჰქონდეს, მაგ., BIOS, სისტემაში შესასვლელი, ქსელის ან ინტერნეტ მომსახურების მომწოდებლია, გამოსაყენებელი ფაილების, დაშიფრული შესასვლელი ფრაზა როგორიცაა სისტემა PGP-სთვის (ალგორითმებისა და პროგრამების ნაკრები შეტყობინების დაშიფვრის მაღალი სანდოობისთვის, ღია გასაღებების გამოყენებით), ელექტრონული ფოსტა, წვდომის მარკერი, დამგეგმავი პროგრამა, ან საკონტაქტო სია);

უსაფრთხოების ნებისმიერი უნიკალური სქემა ან გამადგურებელი მოწყობილობა;

ნებისმიერი გარეშე მონაცემთა შემნახველი; და

სისტემაში დაინსტალირებული ნებისმიერი ჰარდვეარისა ან სოფთვეარის ამხსნელი ნებისმიერი დოკუმენტაცია.

4.3 დანაშაულის ადგილის დოკუმენტირება

დანაშაულის ადგილის დოკუმენტირება განგრძობადი პროცესია **ამოღების მთელი პროცედურის განხორციელებისას**. კომპიუტერების, შესანახი საშუალებების, სხვა ელექტრონული მოწყობილობების და ტრადიციული მტკიცებულებების მდებარეობისა და მდგომარეობის ზუსტ დოკუმენტირებას უდიდესი მნიშვნელობა აქვს [5]. მე-4 თავის წინა და მომდევნო ნაწილებში უფრო მეტი დეტალია მოცემული იმის თაობაზე, თუ რისი დოკუმენტირება უნდა მოხდეს. წინამდებარე ნაწილში ამ ინსტრუქციების მხოლოდ მიმოხილვაა მოცემული.

ზოგადად, უნდა მოხდეს შემდეგის დოკუმენტირება [1,2,5], თუმცა დამატებითი დოკუმენტაცია შეიძლება შეიქმნას მოგროვების ფაზაში:

ფიზიკური ადგილი

სისტემის სკეჩ-გეგმა შექმენით, რომელიც მოიცავს მაგ., მაუსის მდებარეობას და კომპონენტების განლაგებას;

მთელი ადგილის ფოტო და ვიდეო დოკუმენტირება მოახდინეთ[5] (დაფარვის 360 გრადუსი, თუ ეს შესაძლებელია);

კომპიუტერული სისტემები და ელექტრონული კომპონენტები/მოწყობილობები/აღჭურვილობა

მოახდინეთ შემდეგის დოკუმენტირება:

ყველა რელევანტური აღჭურვილობა, მაგ., მარკა, მოდელი, სერიული ნომერი;

ელექტრონული მტკიცებულების შემცველი ან მწარმოებელი თითოეული კომპიუტერული სისტემის მდგომარეობა და მდებარეობა, კომპიუტერის დენში მიერთების სტატუსის ჩათვლით (ჩართული, გამორთული ან ძილის რეჟიმში);

მოახიდნეთ კომპიუტერულ სისტემასთან ან სხვა ხელსაწყოსთან არსებული ყველა მაკავშირებლის დოკუმენტირება (საკაბელო თუ უკაბელო);

იარლიყით მონიშნეთ ყველა პორტი და კაბელი (პერიფერიულ მოწყობილობებთან კავშირის ჩათვლით) მოგვიანებით სისტემის აწყობის სიზუსტის დასაცავად;

გამოუყენებელი კავშირის პორტები აღნიშნეთ სიტყვით "გამოუყენებელი". ლაპტოპ კომპიუტერების საბაზო ბლოკის იდენტიფიცირება მოახდინეთ მონაცემთა შემნახველი სხვა საშუალებების იდენტიფიცირებისთვის (იხ. ნახატი 1).

მონიტორის დეტალების დოკუმენტირება მოახდინეთ ჩარევის მომენტში.

კომპიუტერის წინა ნაწილის, ისე როგორც მონიტორის ეკრანისა და სხვა კომპონენტების ფოტოგრაფირება მოახდინეთ;

გააკეთეთ ჩანაწერი, რომელშიც აღწერთ, თუ რა ჩანს მონისტორის ეკრანზე;

---

[5] ზოგ შემთხვევაში ადგილი შესაძლოა მხოლოდ კომპიუტერული სისტემის შესანახ ადგილს მოიცავდეს, სხვა შემთხვევებში ეს შეიძლება იყოს მაგ., ბინის ყველა ოთ ხი და შენობის გარე ნაწილიც კი

ვიდეო გადაღებით აღბეჭდეთ აქტიური პროგრამები ან მონიტორის ეკრანზე ასახული საქმიანობის უფრო დეტალური დოკუმენტირება მოახდინეთ.

მოახდინეთ იმ რელევანტური ელექტრონული კომპონენტების დოკუმენტირება, რომელთა მოგროვება არ მოხდება;

ინფორმაცია დანაშაულის ჩადენის ადგილზე მყოფი ადამიანებისგან

გაესაუბრეთ ადამიანებს და მოახდინეთ მათი პასუხების დოკუმენტირება/შეავსეთ ფორმები (იხ. ასევე მე-9 თავი);

მოახდინეთ შემდეგის დოკუმენტირება:

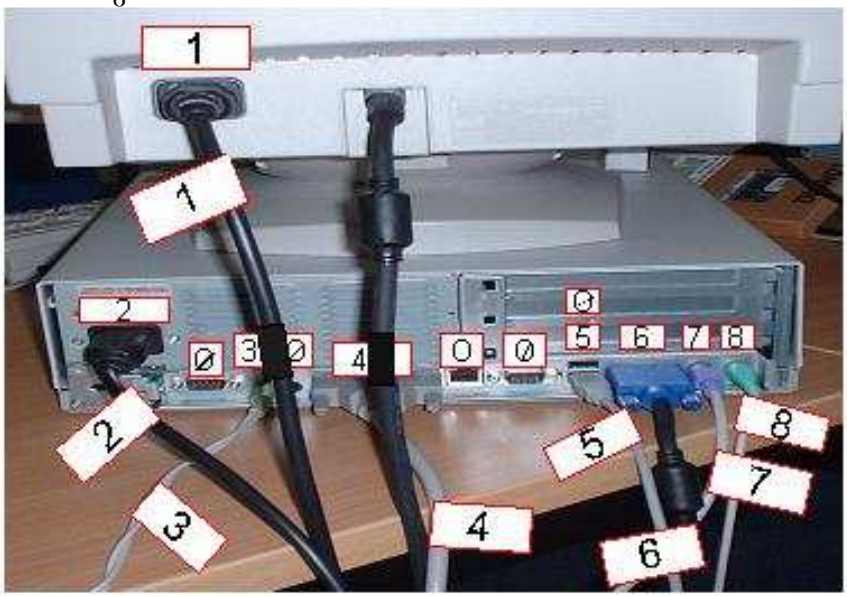
ჩხრეკას დაქვემდებარებულ ადგილზე მყოფი ყველა პირის დეტალები;

ყველა იმ პირის დეტალები, რომლებიც იყენებდნენ კომპიუტერულ სისტემას/აღჭურვილობას;

შენიშვნები, კომენტარები და კომპიუტერის გამომყენებლების/მეპატრონეების/მოწმეების მიერ მოწოდებული ინფორმაცია.

დანაშაულის ჩადენის ადგილზე გატარებული ღონისძიებები

შექმენით საკონტროლო ჟურნალი/ამოღების ამსახველი ჩანაწერი გატარებული ღ ნისძიების აჭრეითა და ამოღების ზუსტი თარიღისა და დროის მითითებით.



ნახატი 1: შემააერთებლების იარლიყებით მონიშვნა შემდგომ მათ ხელახლა ასაწყობად [10]

4.4 მტკიცებულების მოგროვება

საინფორმაციო ტექნოლოგიების სისტემა მხოლოდ იმიტომ არ უნდა იყოს ამოღებული მტკიცებულების სახით, რომ იგი დანაშაულის ჩადენის ადგილზე უბრალოდ ნაპოვნია. ასეთი ღონისძიება გამართლებული და შესაბამისი დანაშაულის პროპორციული უნდა იყოს [2], ამდენად ჩხრეკის შესახებ ბრძანების (ნებართვის) გამცემმა გააზრებული გადაწყვეტილება უნდა მიიღოს იმის შესახებ,

საგამოძიებო ორგანომ უნდა მოახდინოს თუ არა საგნის ამოღება.

ელექტრონული მტკიცებულება, ნებისმიერი სხვა მტკიცებულების მსგავსად, ფრთხილად უნდა იყოს დამუშავებული იმგვარად, რომ მოხდეს მისი მტკიცებულებითი ღირებულების შენარჩუნება. ეს არა მხოლოდ ნივთის ან მოწყობილობის ფიზიკურ შენარჩუნებას შეეხება, არამედ ასევე იმ ელექტრონულ მონაცემებს, რომლებსაც ის შეიცავს. ელექტრონული მტკიცებულების ზოგი ტიპი შესაბამისად მოითხოვს სპეციალურ მოგროვებას, შეფუთვას და ტრანსპორტირებას. ელექტრონული მტკიცებულება, რომელიც შესაძლოა ადვილად დაზიანდეს ან შეიცვალოს ელექტრონმაგნიტული ველებით (როგორიცაა მაგ., სტატიკური ელექტრო ენერგიით, მაგნიტებით, რადიო გადამცემებით და სხვა მოწყობილობებით შექმნილი) ადეკვატურად უნდა იყოს დაცული. ელექტრონული მტკიცებულებები ამოღებული უნდა იყოს შესაბამისი სამსახურის მიერ შემუშავებული სახელმძღვანელო პრინციპებისა და შესაბამისი ზოგადი საკანონმდებლო ბაზის შესაბამისად [5]. ელექტრონული მტკიცებულებების შემდეგი ტიპები განიხილება მე-5 თავში:

კომპიუტერული სისტემა (მე-5.1 თავი),
სხვა ელექტრონული მოწყობილობები (მე-5.2 თავი),
ციფრული შემნახველი საშუალებები (მე-5.1.5 თავი), და
ქსელთან დაკავშირებული ინფორმაცია (კონფიგურაცია და სერვისები/აპლიკაციები) (მე-5.1.3 თავი).

არა-ელექტრონული მტკიცებულების (ან ტრადიციული მტკიცებულების) ამოღება ასევე გადამწყვეტი შეიძლება იყოს ელექტრონული/კომპიუტერული დანაშაულების გამოძიებისას. ამგვარი მტკიცებულების ამოღებასა და შენახვას შესაბამისი ყურადღება უნდა მიექცეს. ელექტრონული მტკიცებულების შემდგომი განხილვისთვის საჭირო საგნები სხვა ფორმით შეიძლება არსებობდეს (მაგ., დაწერილი პასვორდები და სხვა ხელნაწერი შენიშვნები, ქაღალდის ბლოკნოტები, ჰარდვეარისა და სოფთვეარის სახელმძღვანელოები, კალენდრები, ლიტერატურე, კომპიუტერიდან ამობეჭდილი ტექსტი ან გრაფიკა, და ფოტოები) და ისინი უნდა დაიცვათ და შეინახოთ შემდგომი ანალიზისთვის. ეს საგნები ხშირად კომპიუტერსა ან დაკავშირებულ ჰარდვეართან უშუალო სიახლოვეშია. ყველა მტკიცებულება იდენტიფიცირებული, დაცული და შენახული უნდა იყოს შესაბამისი სამსახურის მიერ შემუშავებული სახელმძღვანელო პრინციპებისა და შესაბამისი ზოგადი საკანონმდებლო ბაზის შესაბამისად [5] (იხ. ასევე მე-4.2 თავი).

4.5 შეფუთვა, გადატანა და შენახვა

კომპიუტერები და მასთან დაკავშირებული მოწყბილობა და აღჭურვილობა ადვილად დაზიანებადი ელექტრონული ინსტრუმენტებია, რომლებიც ტემპერატურეს, ტენიანობას, ფიზიკურ შოკს, სტატიკური ელეტრო ენერგიეს, მაგნეტურ წყაროებს და ზოგიერთ მოქმედებასაც კი ცუდად უძლებენ (მაგ., ჩართვა/გამორთვას). შესაბამისად, სპეციალური სიფრთხილის ზომების გამოყენება უნდა მოხდეს ელექტრონული მტკიცებულების შეფუთვის, გადატანისა და შენახვისას.

მტკიცებულების შენახვის პროცესის დასაცავად შეფუთვა, გადატანა და შენახვა ადეკვატურად უნდა იყოს დაფიქსირებული [5].

ზოგადად კომპიუტერის ყველა კომპონენტი და შენახვის საშუალება განსაკუთრებული სიფრთხილით უნდა იყოს დამუშავებული, რადგან არა ექსპერტულმა მოპყრობამ შესაძლოა, ელექტრონული მტკიცებულების დაზიანება ან განადგურება გამოიწვიოს [1,2,5]:

შეფუთვა

შეგროვებული ყველა ელექტრონული მტკიცებულების შესაბამისი დოკუმენტირება და იარლიყით აღნიშვნა უზრუნველყავით შეფუთვამდე.

როდესაც ეს შესაძლებელია, მოგროვებული ელექტრობული 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 ენერგიეს წარმოქმნა შეუძლია, როგორიცაა სტანდარტული ცელოფნის პარკები.

არ მოკეცოთ, მოღუნოთ, ან დაჩხაპნოთ მონაცემთა შენახვის საშუალებები, როგორებიცაა დისკეტები, CD-ROM-ები და ფირები.

არ მიამაგროთ დასაწებებელი იარლიყები მონაცემთა შენახვის საშუალებების ზედაპირზე. როდესაც შესაძლებელია, მონაცემთა შენახვის საშუალებების შესაფუთად გამოიყენეთ ყუთები ან კონვერტები.

უზრუნველყავით, რომ მტკიცებულებების შემცველ ყველა შეკვრას შესაბამისი იარლიყი ჰქონდეს.

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

გადატანა

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

აღჭურვილობის დაცვა უზრუნველყავით შოკისა და დარტყმებისგან (ანუ, მექანიკური დაზიანება), სიცხისა და ტენიანობისგან.

შეფუთვის 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 აღჭურვილობის/მონაცემთა შესანახი საშუალების უფრო პატარა ზომის საგნებზე.

როდესაც შესაძლებელია, ელექტრონული მტკიცებულება **არ** შეინახოთ ავტომობილში დიდხანს.

შენახვა

მტკიცებულების ინვენტარიზაცია მოახდინეთ შესაბამის წესების მიხედვით.

მტკიცებულება უსაფრთხო ადგილას შეინახეთ, გადაჭარბებული ტემპერატურისა და ტენიანობისგან მოშორებით.

დაიცავით ის მაგნიტური წყაროებისგან, ნესტისგან, მტვრისგან, 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 მოწევა არ უნდა შეიძლებოდეს),

სადაც გაკონტროლებული იქნება ტემპერატურე და ტენიანობა, და

რომელიც დაცული იქნება მაგნიტური წყაროებისგან (მაგ., მართვადი რადიო მოწყობილობებიდან შორს).

არ შეინახოთ არანაირი აალებადი 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 მილები, 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 აღჭურვილობა, რომელიც მუშაობს ელემენტებით/ბატარეით (მაგ., PDA ან PC/CMOS) გადაუდებელ ყურადღებას საჭიროებს.

მეტი ინფორმაციისთვის იხ. მაგ., [7-8].

5. ელექტრონული მტკიცებულების ტიპები: მოპყრობის ინსტრუქციები

5.1 კომპიუტერული სისტემა

კომპიუტერული სისტემის მრავალი განსხვავებული ტიპი არსებობს, როგორებიცაა ლაპტოპები/ნოუთბუქები, დესკტოპები, კოშკურა სისტემები, მოდულარული დამონტაჟებული სისტემები, მინი-კომპიუტერები, და უნივერსალური გამომთვლელი მანქანები. პოტენციური მტკიცებულება ყველაზე უფრო ხშირად მოიპოვება იმ ფაილებში, რომლებიც შიდა (მაგ., მახსოვრობა, ჰარდ დისკი) და გარე (მაგ., CD, დისკეტა, USB) მონაცემთა შესანახ მოწყობილობებსა და საშუალებებში [5] ინახება.

პირველი რეაგირების მომხდენმა ყოველთვის უნდა ითხოვოს **ექსპერტის დახმარება**, განსაკუთრებით მაშინ, თუ აღჭურვილობის ამოღება არ უნდა მოხდეს (იხ. თავი 3).

კომპიუტერული სისტემა ტიპიურად შემდეგი კომპონენტებისგან შედგება, რომელთა გათვალისწინება უნდა მოხდეს ამოღების შემთხვევაში მოგროვებისთვის (იხ. მე-3.1 თავი):

ძირითადი ნაწილი (მაზერბორდის, ცენტრალური პროცესორის, მეხსიერების და შესაძლოა გამაფართოვებელი პლატის შემცველი),

მონიტორი (რომელიც ჩვეულებრივ ძირითად ნაწილზეა მიბმული),

კლავიატურა (რომელიც ჩვეულებრივ ძირითად ნაწილზეა მიბმული),

მაუსი,

კაბელები,

ენერგიის მომწოდებელი მოწყობილობები (მაგ., ელექტრო მომარაგების მოდული და თავისუფალი ელემენტები/ბატარეა),

შესაძლოა, დამატებითი კომპონენტები (მაგ., მოდემები, პრინტერები, სკანერები, საბაზო ბლოკები, პორტების რეპლიკატორები, ბარათის მკითხველები, დამცავი დამახშობლები, მიკროპროცესორიანი ბარათები, და გარე მონაცემთა შემნახველი მოწყობილობები, იხ. მე-5.1.4 და მე-5.2 თავები), და

ქსელის მოწყობილობები (იხ. მე-5.1.3 თავი).

გაითვალისწინეთ, რომ ძირითადი ნაწილის გარდა მოწყობილობებს შესაძლოა, გარედან შეუმჩნეველი შიდა მახსოვრობა ჰქონდეთ.

გაითვალისწინეთ, რომ კომპიუტერული სისტემა შესაძლოა, განსხვავებული მოწყობილობის ფორმით იყოს, როგორიც შეიძლება იყოს სტერეო მოწყობილობა ან მაცივარი.

პერსონალუ კომპიუტერებს აქვთ სხვადასხვა ტიპის პორტები (შეერთებებისთვის). დისკავოდის, საჩვენებელი ეკრანის, კლავიატურის, მოდემების, პრინტერების, მაუსების და სხვა პერიფერიული მოწყობილობების შესაერთებელი რამდენიმე პორტი შეიძლება არსებობდეს [5]. პერსონალურ კომპიუტერს მრავალი მოწყობილობა შეიძლება შეუერთდეს უკაბელო კავშირითად (მაგ., ბლუთუსი, ინფრარედი).

პერსონალური კომპიუტერები შემდეგ საოპერაციო სისტემებს იყენებენ: MSDOS, Microsoft Windows, Unix, Linux, ან Mac OS. კომპიუტერული სისტემა შესაძლოა, ავტონომიური იყოს ან ის შესაძლოა, ქსელში იყოს მიერთებული. კომპიუტერულ ქსელში დამატებით ქსელურ ელემენტებსაც ვხვდებით ხოლმე (მაგ., ქსელის კაბელები, რუტერები, ჰაბები, გამანაწილებლებს, რომლებმაც უკაბელო ჩართვის უზრუნველყოფა შეიძლება მოახდინონ; იხ. მე-5.1.3 თავი).

ელექტრონული საიდენტიფიკაციო ნიშნები და შენახვის საშუალებები, როგორც ასეთი, ყოველთვის ადვილად აღმოსაჩენი არ არის. მათ შესაძლოა, ჰქოდენთ საათის (მაგ., გასაღებზე დამაგრებული), ბიჟუტერიის, გასაღების, ელექტრონული სათამაშოების, ა.შ. ფორმა. ციფრული კამერით გადაღებული სურათები ჩვეულებრივ მრავალფუნქციურ მეხსიერების ბარათებზე ინახება (მაგ., ფლეშ

მეხსიერების ბარათებში) [2]. მე-5.1.2, მე-5.1.5 და მე-5.2 თავები, მე-7 თავში მოცემულ განმარტებებთან ერთად ყველაზე ხშირად გამოყენებული ხელსაწყოების და შესანახი საშუალებების მიმოხილვას მოიცავს, რომელიც დანაშაულის ჩადენის ადგილზე შეიძლება ნახოთ.

ციფრული შენახვის საშუალებები (იხ. მე-5.1.5 თავი) ხშირად შენახული არ არის კომპიუტერთან ახლოს. მათ ცალკე ოთახში ან ცალკე შენობაშიც კი ინახავენ. ზოგ შემთხვევაში ეს საშუალებები სპეცალურ ყუთებშია დაცული (მაგ., მონაცემთა დაცვის კარადებში) [2].

დაბოლოს, შემდეგი დამხმარე საგნები (არა ელექტრონული მტკიცებულებები) შეიძლება, ასევე განიხილებოდეს შეგროვებისთვის, რამდენადაც მათ შესაძლოა, დამატებითი დახმარება მოახერხონ კომპიუტერული სისტემის გამოკვლევისას [5]:

ჰარდვეარისა და სოფთვეარის სახელმძღვანელოები (თავდაპირველი CD ROM-ების ჩათვლით),

ჩანაწერები, დღიურები, კალენდრები და მსგავსი ნივთები, რომლებზეც პასვორდები ან სხვა დაკავშირებული ინფორმაცია შეიძლება იყოს მონიშნული,

ქაღალდის ბლოკნოტები,

კომპიუტერთან დაკავშირებული ლიტერატურა,

კომპიუტერიდან ამობეჭდილი მასალა,

შესაბამისი ფოტოები და

კომპიუტერთან დაკავშირებული გასაღებები.

შემდეგ ნაწილში აღვწერთ იმ ძირითად ნაბიჯებს, რომლებიც დაკავშირებულია კომპიუტერული სისტემის ან სხვა ელექტრონული მოქყობილობების მოგროვებასთან [5,2].

5.1.1 კომპიუტერული სისტემის/ელექტრონული მოწყობილების მოგროვება

ეს ნაწილი აღწერს კომპიუტერული სისტემის ამოღების პროცესში საჭირო ნაბიჯებს [1,2,5]. ამ ნაბიჯთაგან ზოგი წინა ნაწილებში უკვე განვიხილეთ.

მოახდინეთ დანაშაულის ჩადენის ადგილის განკგრძობადი დოკუმენტირება და ჩაიწერეთ თქვენ მიერ განხორციელებული ყველა ქმედება და თქვენი ქმედების შედეგად მომხდარი ცვლილებები, რომლებსაც თქვენ შეამჩნევთ მონიტორზე, კომპიუტერზე, პრინტერზე ან სხვა ხელსაწყოზე (იხ. მე-4.3 თავი).

არ გაითვალისწინოთ შესაძლო ეჭვმიტანლის არანაირი გადაუმოწმებელი რჩევა.

უზრუნველყავით დანაშაულის ჩადენის ადგილის უსაფრთხოება დაყ ველა პირი მოაშორეთ ტექნიკასა და ელექტრო ენერგიეს წყაროებს (იხ. მე-4.2 თავი).

ადგილზე მოძებნეთ შემდეგი კომპონენტები/ნივთები (იხ. მე-5.1 თავი):
კომპიუტერული სისტემის კომპონენტები,
ციფრული შენახვის საშუალებები,
დამატებითი კომპონენტები,
სხვა ელექტრონული მოწყობილობები და
არა ელექტრონული მტკიცებულებები.
თუ **კომპიუტერულ ქსელს** აღმოაჩენთ (იხ. მე-5.1.3 თავი), დახმარებისთვის **დაუკავშირდით კომპიუტერის ექსპერტიზის სპეციალისტს** თქვენ სამსახურში ან გარე ექსპერტს, რომელიც თქვენი სამსახურის მიერ არის იდენტიფიცირებული.

გახსოვდეთ, რომ ზოგი მოწყობილობა შესაძლოა, უკაბელო კავშირით იყოს სხვასთან დაკავშირებული (მაგ., ბლუთუსი, ინფრარედი).

გახსოვდეთ, რომ თუ არსებობს რამე ქსელური კავშირი, კომპიუტერულ სისტემაზე წვდომა და შესაძლო მანიპულაცია შეიძლება განხორციელდეს ამოღების პროცესში (ანუ, ნებისმიერ დროს, როდესაც ის ჩართულია და იმყოფება ქსელური კავშირის ფარგლებში).

ჩაატარეთ წინასწარი გამოკითხვა (იხ. მე-4.2 თავი).

დაათვალიერეთ კომპიუტერული სისტემა იმის დასადგენად, **ჩართულია** თუ **გამორთული** (იხ. მე-5.1.2 თავი).

მოახდინეთ ყველა კავშირისა და კომპონენტის დოკუმენტირება და მე-4.3 თავში აღწერილის შესაბამისად მოახდინეთ მათი იარლიყებით მონიშვნა.

მოახდინეთ კომპიუტერში/კომპიუტერიდან კავშირებისა და შესაბამისი კაბელების ფოტოგრაფირება ან დიაგრამით აღწერა.

მოახდინეთ მტკიცებულების თქვენი სამსახურის პროცედურების მიხედვით აღნუსხვა.

ფრთხილად მოხსენით აღჭურვილობა და აღნუსხეთ მათი უნიკალური განმასხვავებელი ნიშნები. მოწყობილობის გაგრილებას დაელოდეთ მათ შეფუთვასა და გადატანამდე.

თუ ტრანსპორტირებაა საჭირო, მე-4.5 თავში აღწერილის შესაბამისად შეფუთეთ კომპონენტები.

მე-8 თავში მოცემული ჯიბის წიგნაკი (დანართი ა) მოიცავს კომპიუტერული აღჭურვილობისა და პერსონალური ციფრული ასისტენტის ("ჯიბის კომპიუტერების") ამოღების კარგი პრაქტიკის მიმოხილვას მოიცავს.

5.1.2 ენერგიის სტატუსის შემოწმება (ჩართული/გამორთული)

წინამდებარე ნაწილი გამოსაყენებელია კომპიუტერული აღჭურვილობისა და შენახვის საშუალებების ამოღებისას (იხ. მე-3.1 თავი).

დაათვალიერეთ კომპიუტერული სისტემა და დაადგინეთ, **ჩართულია** თუ **გამორთული**:

კომპიუტერების უმრავლესობას სტატუსის მაჩვენებელი ნათურა აქვთ, რომლებიც მიუთითებენ, რომ კომპიუტერი ჩართულია. თუ გამაგრილებელი ვენტილიატორის ხმა ისმის, სისტემა სავარაუდოდ

ჩართულია. თუ კომპიუტერული სისტემა თბილია, ესეც შესაძლოა, იმის მაჩვენებელი იყოს, რომ ის ჩართულია ან მხოლოდ ახლახანს გამოირთო.

ზოგიერთი პორტატული მოწყობილობის გააქტიურება მისი სახურავის გახსნით ხდება.

ყოველთვის განიხილეთ პორტატული კომპიუტერებისა და მოწყობილობების ბატარიის მოხსნის შესაძლებლობა.

პორტატული კომპიუტერებს (მაგ., ნოუთბუქი ან ლაპტოპი) ჩვეულებრივ აქვთ დამატებითი ბატარეა. ზოგიერთ მათგანს მეორე ბატარეა ფლოპი დრაივის ან CD დრაივის ადგილას მრავალფუნქციურ ჭრილშიც კი აქვთ მოთავსებული. ამგვარი ბატარეის დატვირთვა ხდება მაშინ, როდესაც კომპიუტერი დენის წყაროზეა მიერთებული და სრულად დატენილმა შეიძლება დენის გარეშე რამდენიმე საათს იმუშავოს.

კომპიუტერული სისტემა, რომელიც გამორთულს ჰგავს, შეიძლება, ძილის რეჟიმზე იყოს გადართული და მასზე დისტანციური წვდომა შესაძლებელი იყოს, რაც ფაილების შეცვლის ან წაშლის შესაძლებლობას იძლევა. ზოგიერთი სკრინ-სეივერი ისეთ შთაბეჭდილებას ტოვებს, თითქოს კომპიუტერი გამორთულია. დააკვირდით მონიტორს და შეეცადეთ დაადგინოთ, ის ჩართულია, გამორთული თუ ძილის რეჟიმშია. მონიტორზე თქვენი დაკვირვების შედეგი შესაძლოა, იყოს შემდეგი [5]:

სიტუაცია 1: მონიტორი ჩართულია და სამუშაო პროდუქტი და/ან დესკტოპი ჩანს.

თქვენი ჩარევის დროისთვის მონიტორის მდგომარეობის დოკუმენტირება მოახდინეთ (იხ. მე-4.3 თავი).

გადადით ქვემოთ განხილულ "სიტუაცია ბ-ზე".

სიტუაცია 2: მონიტორი ჩართულია და ეკრანი შავია (ძილის რეჟიმი) ან სკრინ-სეივერი (მაგ., სურათი) ჩანს.

მაუსი მსუბუქად (კლავიშებზე დაჭერის გარეშე) გაამოძრავეთ. ეკრანი უნდა შეიცვალოს და გაჩვენოთ სამუშაო პროდუქტი ან მოგთხოვოთ პასვორდი.

თუ მაუსის გადაადგილება არ ცვლის ეკრანს, არ დააჭიროთ არანაირ კლავიშს ან არ აწარმოოთ არანაირი ოპერაცია მაუსით.

თქვენი ჩარევის დროისთვის მონიტორის მდგომარეობის დოკუმენტირება მოახდინეთ (იხ. მე-4.3 თავი).

გადადით ქვემოთ განხილულ "სიტუაცია ბ-ზე".

სიტუაცია 3: მონიტორი გამორთულია.

ჩაინიშნეთ, რომ კომპიუტერის სტატუსია "გამორთული".

ჩართეთ მონიტორი და ამის შემდეგ დაადგინეთ, მონიტორის სტატუსი შეესაბამება თუ არა ზემოთ სიტუაცია 1 ან სიტუაცია 2-ში აღწერილს და მიჰყევით შესაბამის ნაბიჯებს.

თქვენი დაკვირვების შედეგი (იმასთან დაკავშირებით, კომპიუტერი ჩართულია თუ გამორთული) შემდეგი შეიძლება იყოს:

სიტუაცია ა: თქვენ დაადგინეთ, რომ სისტემა გამორთულია; **არ** ჩართოთ!

მოაშორეთ დენში ჩართვის კაბელი სამიზნე მოწყობილობას (**არ** მოაშოროთ ის კედლის ჩამრთველს) და ჩაინიშნეთ ამის გაკეთების დრო.

თუ პორტატულ ხელსაწყოსთან მუშაობთ, ასევე გამოაცალკევეთ ბატარეა. გამოაცალკევეთ ნებისმიერი დამატებითი ბატარეა, თუ ასეთები არის (ზოგიერთ პორტატულ მოწყობილობას მეორე ბატარეა ფლოპი დრაივის ან CD დრაივის ადგილას მრავალფუნქციურ ჭრილში აქვთ მოთავსებული).

თუ კომპიუტერული სისტემა გამორთულია, დატოვეთ გამორთულად, რადგან კომპიუტერის ჩართვის პროცესი კომპიუტერული მონაცემების მოდიფიცირებას მოახდენს და პოტენციურად მტკიცებულებას გაანადგურებს.

სიტუაცია ბ: თქვენ დაადგინეთ, რომ სისტემა ჩართულია; **არ** გამორთოთ იგი!
შეეცადეთ ექსპერტთან დაკავშირებას.
თუ ექსპერტი ხელმისაწვდომია, მიჰყევით მის რჩევას.
თუ ექსპერტი ხელმისაწვდომი არ არის, გააგრძელეთ შემდგომი ინსტრუქციის შესაბამისად.
არ შეეხოთ კლავიატურას ან სხვა მიერთებულ მოწყობილობას.

დენის მიმწოდებელი კაბელი გამოაერთეთ სამიზნე აღჭურვილობიდან (**არ** გამორთოთ შტეფსელიდან, რადგან კომპიუტერულ სისტემას შესაძლოა, კომპიუტერულ სისტემას შესაძლოა, ჰქონდეს უწყვეტი კვების წყარო - UPS) და ჩაინიშნეთ ამის გაკეთების დრო.

გახსოვდეთ, რომ ამან მტკიცებულების დაკარგვა შეიძლება გამოიწვიოს (იხ. ასევე **ყუთი** ქვემოთ).

მონაცემთა შენახვის საშუალება მოაშორეთ შესაბამის მოწყობილობებს; მოათავსეთ ისინი მათ პირველად ყუთებში/შესაფუთ მასალაში და შესაბამისი იარლიყით აღნიშნეთ. გამოიყენეთ ან მონაცემთა ამოღებისთვის გამოსაყენებელი დისკი/კომპაქტური დისკი ან ცარიელი ფლოპი დისკი, თუ ასეთი ხელთ გაქვთ. **არ** გამოიღოთ კომპაქტური დისკი ან შეეხოთ კომპაქტური დისკის სამართავ არც ერთ ღილაკს [5].

გამოაერთეთ მოდემი, თუ ჩართულია, რადგან მისი უბრალოდ გამორთვა ყოველთვის საკმარისი შესაძლოა, არ იყოს.

თუ პორტატულ მოწყობილობასთან გაქვთ საქმე, ბატარეაც გამოაერთეთ. თუ დამატებითი ბატარეებიც არის, გამოაერთეთ ისინიც (ზოგ პორტატულ მოწყობილობას მეორე ბატარეა ფლოპი დრაივის ან CD დრაივის ადგილას მრავალფუნქციურ ჭრილში აქვთ მოთავსებული).

დენის მიწოდების კაბელის კომპიუტერული სისტემიდან გამოერთება გავლენას მოახდენს ყველა მოქმედ პროგრამასა და კომპიუტერის შემთხვევითი წვდომის მეხსიერებაში (RAM)[6] შენახულ ყველა მონაცემზე (შესაბამისი მონაცემების, როგორიცაა პასვორდები, ჩათვლით). ეს მოიცავს ინტერნეტში ჩართვას, ბეჭდვას ან დაშიფვრა.

სიტუაცია გ: ვერ ადგენთ, სისტემა გამორთულია, თუ არა.

ჩათვალეთ, რომ ის გამორთულია. **არ** დააჭიროთ ჩართვის ღილაკს.

დენის მომწოდებელი კაბელი გამოაერთეთ სამიზნე აღჭურვილობიდან (**არ** გამოაერთოთ შტეფსელიდან) და აღნიშნეთ ამის გაკეთების დრო.

თუ პორტატულ მოწყობილობასთან გაქვთ საქმე, გამოაერთეთ ბატარეაც. თუ დამატებითი ბატარეებიც არის, გამოაერთეთ ისინიც (ზოგ პორტატულ მოწყობილობას მეორე ბატარეა ფლოპი დრაივის ან CD დრაივის ადგილას მრავალფუნქციურ ჭრილში აქვთ მოთავსებული).

5.1.3 კომპიუტერული ქსელი

ყოველთვის ივარაუდეთ, რომ კომპიუტერული ქსელი იარსებებს.

თუ თქვენ დასაბუთებული ვარაუდი გაქვთ, რომ ქსელი არსებობს, დაუკავშირდით კომპიუტერული ქსელების ექსპერტს. თუ ექსპერტის მოძიება არ არის შესაძლებელი, წინამდებარე თავში მოცემული ინფორმაცია შესაძლოა, დაგეხმაროთ შესაბამისი მოწყობილობის ამოღებისას.

იმის მაჩვენებლები, რომ კომპიუტერულ ქსელთან გაქვთ საქმე, შეიძლება, მოიცავდეს შემდეგს [5]:

მრავალ კომპიუტერიანი სისტემის არსებობა.

ქსელის კომპონენტების არსებობა, მაგ.:

ქსელის ინტერფეისი ბარათები (NIC ან ქსელის ბარათები) და მათთან დაკავშირებული კაბელები (თუ უკაბელო არ არის);

უკაბელო ადგილობრივი ქსელის (LAN) ხელსაწყოები (მაგ., უკაბელო წვდომის წერტილი);

რუტერები, ჰაბები და სვიჩები;

სერვერები და

ქსელის კაბელები, რომლებიც კომპიუტერებსა ან ცენტრალურ ხელსაწყოებს, როგორც არის ჰაბები, შორის არის განლაგებული.

ინფორმანტების ან დანაშაულის ჩადენის ადგილზე მყოფი ადამიანების მიერ მოწოდებული ინფორმაცია (იხ. ასევე მე-4.2 და მე-9 თავები).

[6] შემთხვევითი წვდომის მეხსიერება

თუ კომპიუტერულ ქსელს ნახავთ, დაუკავშირდით კომპიუტერული ექსპერტიზის **ექსპერტს** თქვენ უწყებაში ან თქვენი სამსახურის მიერ რეკომენდირებულ გარეშე ექსპერტს დახმარებისთვის. სხვა შემთხვევაში იხელმძღვანელეთ მე-5.1.1 თავში მითითებული ინსტრუქციებით.

არ გაგზავნოთ მოგროვებული ინფორმაცია ინტერნეტით ღიად (ანუ, დაშიფვრისა და გზავნილის ნამდვილობის კოდის ან ელექტრონული ხელმოწერის გარეშე).

შესაძლო მტკიცებულება კომპიუტერულ ქსელებთან დაკავშირებით მოიცავს შემდეგს:
ინტერნეტ მომსახურების მომწოდებელს (ISP),
ინტერნეტ პროტოკოლის (IP) მისამართ(ებ)ს,
თარიღისა და დროის შესახებ ინფორმაცია, დროის ზონის მითითებით (რაც ინტერნეტით სარგებლობის შესახებ ერთ-ერთი უმნიშვნელოვანესი ინფორმაციაა),
ადგილობრივი ქსელის (LAN) კონფიგურაცია,
დომეინის სახელების მომსახურების (DNS) სერვერ(ებ)ი,
ელექტრონული ფოსტა,
უსაფრთხოება/დაშიფვრა,
ახალი ამბების ჯგუფები,
სასაუბრო ოთახები/ჯგუფები,
ელექტრონული მაღაზიები/მომსახურების მომწოდებლები (თუ პირადი/გადახდასთან დაკავშირებული ინფორმაციაა ჩართული) და IP მისამართები/სერვერების სახელები/სხვა მონაცემები სხვადასხვა ქსელის მომსახურებისთვის (მაგ., ftp, telnet, WWW).

ასევე იხილეთ საკონტროლო სია შესაბამისი კითხვებით წინასწარი გამოკითხვისთვის დანართში ბ3 (მე-9 თავი).

5.1.4 დამატებითი კომპონენტები
როგორც მე-5.1 თავშია ნახსენები, კომპიუტერული სისტემა შეიძლება მოიცავდეს ზოგიერთ დამატებით ცომპონენტს, როგორიცაა მაგ.:
კაბელებით ან სხვა ინტერფეისით დაკავშირებული გარე შესანახი მოწყობილობა;
გარე ჰარდ დრაივები,
გარე CD-RW ან DVD დრაივები,
ფლოპი დრაივები,
JAZ დრაივები,
ZIP დრაივერბი,
მაგნეტური ლენტის დრაივები და
ORB დრაივები.
დრაივის დუბლიკატორები;
MP3 ფლეიერები;
დამცველი დამახშობლები (მაგ., USB დამცველი დამახშობელი, პარალელური პორტის დამცავი დამახშობელი, სერიული პორტის დამცველი დამახშობელი);

მიკროპროცესორიანი ბარათები (იხ. მე-5.2.4 თავი) და
მიკროპროცესორიანი ბარათების მკითხველები;
პრინტერები (იხ. მე-5.2.8 თავი);
სკანერები (იხ. მე-5.2.9 თავი);
საბაზო ბლოკები;
პორტების რეპლოკატორი;
პერსონალური კომპიუტერის ბარათები და პერსონალური კომპიუტერის ბარათის მკითხველები;
ვებ კამერები (იხ. ციფრული კამერები);
მოდემები (შიდა ან გარე, ტელეფონზე დარეკვის მოწყობილობა/ანალოგი ან კაბელი, DSL, ISDN, უკაბელო მოდემები);
უკაბელო მოწყობილობები;
ინფრარედ-ადაპტორები (USB, სერიული, სისტემური პლატა),
ინფრარედით მომუშავე მოწყობილობები (უკაბელო LAN, ნოუთბუქებსა და პერსონალურ კომპიუტერებს შორის მაკავშირებლები, უკაბელო მოდემები, დამცავი სიგნალიზაციის მოწყობილობები),
ბლუთუსის ამამუშავებელი მოწყობილობები (მაგ., ბლუთუს USB დამცავი დამახშობლები ჯიბის კომპიუტერებისთვის (PDA-ებისთვისა) და პერსონალური კომპიუტერისთვის, პერსონალური კომპიუტერის ბარათები ნოუთბუქებისთვის), და
ბლუთუსით მომუშავე მწყობილობები (მაგ., ყურსასმენები, ჯიბის კომპიუტერები (PDA-ები), ნოუთბუქები, ტელეფონები, GPS მიმღებები).

გახსოვდეთ, რომ ზოგ კომპონენტს, შესაძლოა, განსხვავებული ფუნქცია ჰქონდეს (მაგ., კალმები, ხელის საათები, საიუველირო ნაწარმი).

იხ. მე-5.2.1 თავი ზოგადად გამოსაყენებელი ამოღების ინსტრუქციებისთვის.

5.1.5 ციფრული შემნახველი საშუალება

შემდეგი საშუალებები ხშირად კომპიუტერთან ახლოს არ არის შენახული, ის ან სხვა ოთახში ან სხვა შენობაშია დაცული (ზოგ შემთხვევაში საშუალება ეს საშუალება შეიძლება სპეციალურ ყუთებში, ე.წ. მონაცემთა უსაფრთხოების კარადებში იყოს შენახული) [2,5]:

ფლოპი დისკები,
სათადარიგო საშუალებები (მაგ., მაგნიტური ლენტები),
JAZ, ZIP და ORB დისკები,
კომპაქტური დისკები და DVD-ები,
კომპიუტერთან დაუკავშირებელი ჰარდდრაივები,
პერსონალური კომპიუტერის ბარათები,
მაგნიტური ლენტის ბარათი,
მეხსიერების ბარათები,
USB მახსოვრობის გასაღებები/,
დამცავი დამახშობლები,
მყარი დისკები, და
იხ. ასევე ჯიბის კომპიუტერები (PDA-ები) მე-5.2.2 თავში.

გახსოვდეთ, რომ ზოგ საშუალებას შესაძლოა, განსხვავებული ფუნქცია ჰქონდეს (მაგ., კალმები, ხელის საათები, საიუველირო ნაწარმი).

იხ. მე-4.5 თავი შეფუთვის, გადატანისა და შენახვის ზოგადი ინსტრუქციებისთვის.

5.2 სხვა ელექტრონული მოწყობილობები

პერსონალური ციფრული ასისტენტები (PDA ან ჯიბის კომპიუტერები), იხ. ასევე მე-5.2.2 თავი, როგორიცაა, მაგ.,
ელექტრონული ორგანაიზერი,
კომუნიკატორი, ან
მიკროპროცესორიანი ტელეფონი.
ვიდეო აღჭურვილობა (ვიდეო კამერა, ვიდეოს კასეტის ჩამწერი (VCR) ან ფლეიერი);
აუდიო ჩამწერები;
ჩიპები;
სამონტაჟო პლატები;
გამფართოვებელი პლატები;
ციფრული კამერები (იხ. მე-5.2.6 თავი);
წვდომის მარკერები (ბარათისა და იუზერის ინფორმაციის იდენტიფიცირებისთვის/ავთენტიფიცირებისთვის, კონფიგურაციებისთვის, ნების დართვისთვის, ან თავად მოწყობილობის მიერ), მაგ.,
მიკროპროცესორიანი ბარათები (იხ. მე-5.2.4 თავი),
დამცავი დამახშობლები (უსაფრთხოების დამცავი დამახშობლები), რასაც ასევე ეწოდება ჰარდვეარის გასაღები, ან
ბიომეტრიული სკანერები.
ტელეფონები (იხ. მე-5.2.3 თავი);
ტელეფონის აპარატების მოპასუხე (იხ. მე-5.2.5 თავი);
ფაქსის მანქანები (იხ. მე-5.2.7 თავი);
დიქტოფონები/ხმის ჩამწერები (იხ. ასევე ტელეფონის აპარატების მოპასუხეები);
პეიჯერები (იხ. მე-5.2.12 თავი);
მახსოვრობის ბარათებიანი სათამაშო მოწყობილობები, კარტრიჯებიანი სათამაშო მანქანები, Xbox-ები, gamecube-ები, ა.შ.;
GPS მოწყობილობები და სხვა სატელიტური მოწყობილობები (იხ. მე-5.2.13 თავი);
ციფრული საათები (იხ. მე-5.2.14 თავი);
კრედიტ ბარათების სქიმერები (ან მაგნიტური ლენტის მკითხველი, იხ. ასევე მე-5.2.15 თავი);
ასლის გადამღებები (ასლის გადამღები მანქანები, იხ. მე-5.2.10 თავი).

გახსოვდეთ, რომ ზოგ საშუალებას შესაძლოა, განსხვავებული ფუნქცია ჰქონდეს (მაგ., კალმები, ხელის საათები, საიუველირო ნაწარმი).

იხ. მე-5.2.1 თავი ზოგადად გამოსაყენებელი ინსტრუქციებისთვის ამოღებისას. მოწყობილობების აღწერა ასევე შეიძლება იხილოთ მე-7 თავში.

იხ. მე-4.5 თავი შეფუთვის, გადატანისა და შენახვის ზოგადი ინსტრუქციებისთვის.

5.2.1 ელექტრონული მოწყობილობების ამოღების ზოგადი ინსტრუქციები

ელექტრონული მტკიცებულებების ამოღებისას გათვასლიწნებული უნდა იყოს შემდეგი [2,5]:
თუ მოწყობილობა ჩართულია, **არ** გამორთოთ ის, რადგან გამორთვამ შესაძლოა, დაბლოკვის მექანიზმი აამუშავოს.
ეკრანზე გამოტანილი ინფორმაცია ფოტოგადაღებით დააფიქსირეთ (თუ ასეთი არის) და ჩაიწერეთ ნაჩვენები ინფორმაცია.
მოხსენით ელექტრო ენერგიის მიმწოდებელი ყველა კაბელი (ჩვეულებრივ, ჯობია მათი სამიზნე აღჭურვილობიდან გამოთიშვა, ნაცვლად შტეფსელიდან გამორთვისა).
არ შეეცადოთ შიდა მეხსიერების ან მონაცემთა რომელიმე შენახვის საშუალების წვდომას.
თუ ის გამორთულია, **არ** ჩართოთ, რადგან ამან შესაძლოა მტკიცებულება შეცვალოს/გაანადგუროს (როგორც კომპიუტერულ სისტემებში, იხ. ასევე მე-5.1.1 თავი).
გამორთეთ ყველა ტელეფონის ხაზი კედლიდან და არ გამოაერთოთ მოწყობილობიდან, რის შემდეგ მოახდინეთ მისი დოკუმენტირება და იარლიყით აღნიშვნა.
მნიშვნელოვანი ინფორმაცია შეაგროვეთ/ჩაიწერეთ (იხ. ასევე მე-4.3 თავი).
შეაგროვეთ სახელმძღვანელოები და სხვა ინსტრუქციები, თუ ასეთია.
ჩაიწერეთ შესაბამისი მონაცემები (მაგ., ტელეფონის ნომერი).
იხ. მე-4.5 თავი შეფუთვის, გადატანისა და შენახვის ზოგადი ინსტრუქციებისთვის.
რადგან ბატარეები დროის მოკლე ხანს მუშაობს, მათი დაჯდომის შემთხვევაში მონაცემების დაკარგვა შესაძლებელია. ამდენად, შესაბამისი პერსონალის ინფორმირება უნდა მოხდეს, რომ ბატარეაზე მომუშავე ტელეფონს გადაუდებელი ყურადღება ესაჭიროება.
ამოღების შემდეგ, გადაეცით მოწყობილობა ექსპერტს რაც შეიძლება სწრაფად. ჯიბის კომპიუტერებისა (PDA-ების) და მობილური ტელეფონების შემთხვევაში ეს გადაუდებლად უნდა მოხდეს.

გახსოვდეთ, რომ ამოღების შემდეგ მოწყობილობა ექსპერტს დაუყოვნებლივ უნდა გადაეცეს. ჯიბის კომპიუტერებისა (PDA-ების) დამობილური ტელეფონების შემთხვევაში ეს გადაუდებლად უნდა მოხდეს.

5.2.2 პერსონალური ციფრული თანაშემწეები (ჯიბის კომპიუტერები)

პერსონალური ციფრული თანაშემწე (PDA, ან ჯიბის კომპიუტერი) მცირე ზომის ხელსაწყოა, რომელიც შეიძლება მოიცავდეს კომპიუტერის, ტელეფონის/ფაქსის, პეიჯერის, ქსელის და სხვა მახასიათებლებს. ის ჩვეულებრივ გამოიყენება როგორც პერსონალური ორგანაიზერი (ან ელექტრონული ორგანაიზერი). ჯიბის კომპიუტერი

ასრულებს დესკტოპ კომპიუტერული სისტემის ყველა ფუნქციას. ზოგიერთი პერსონალური ციფრული თანაშემწე (PDA, ან ჯიბის კომპიუტერი) შეიცავს დისკ დრაივებს, და ზოგი პერსონალური კომპიუტერის ბარათის ნაწილს, რომელმაც შეიძლება დაიმაგროს მოდემი, ჰარდ დრაივი, ან სხვა მოწყობილობა. ჩვეულებრივ ისინი მოიცავენ მექანიზმს, რომლის მეშვეობით ხდება მათი მონაცემების სინქრონიზება სხვა კომპიუტერულ სისტემებთან, ყველაზე უფრო ხშირად საწყის წერტილში დაკავშირებით. თუ ეს საწყისი მაკავშირებელი წარმოდგენილია, შეეცადეთ მასთან ასოცირებული ჯიბის აღჭურვილობის დადგენა [5]. პერსონალური ციფრული თანაშემწე (PDA, ან ჯიბის კომპიუტერი) თავად შეიძლება პოტენციურ მტკიცებულებას წარმოადგენდეს (როგორც მონაცემთა შენახვის საშუალება) ან იგი შეიძლება შეიცავდეს პოტენციურ ელექტრონულ მტკიცებულებებს ისევე როგორც კომპიუტერული სისტემა.

პერსონალური ციფრული თანაშემწეები (PDA, ან ჯიბის კომპიუტერი) მოიცავს მცირე მიკროკომპიუტერებს რეალური ან ვირტუალური მინიატურული კლავიატურით და ლიკვიდური კრისტალური ეკრანით მახსოვრობის ჩიპებთან ერთად სადაც ყველა ინფორმაცია ინახება. სამუშაო მასხოვრობის მოცულობა (ანუ, RAM) ხშირად მითითებულია PDA-ის სახელში მაგ., 2 MB, 16 MB, 32 MB. მახსოვრობა აქტიურია ბატარეების მეშვეობით და მათი მუშაობის შეწყვეტის შემთხვევაში PDA-ში დაცული ყველა ინფორმაცია შესაძლოა, დაიკარგოს. ხშირად ორი წყება ბატარეა გამოიყენება:
ძირითადი წყება, რომელიც შექმნილია იმისთვის, რომ ეკრანი და კლავიშები ამუშავოს, როდესაც PDA ჩართულია და
სარეზერვო ბატარეა, რომელიც ინფორმაციას ინარჩუნებს მახსოვრობაში, თუ და როდესაც ძირითადი ბატარეა წყვეტს მუშაობას.
ზოგ PDA-ს ერთი წყება დასატენი ბატარეა აქვს, რომელიც როგორც წესი დატენილია კომპიუტერის საწყის ენერგიის წყაროსთან მიერთებით. ეს ბატარეა ძალიან სწრაფად იცლება (რამდენიმე დღეში) თუ მისი დატენვა არ ხდება. ამ ტიპის PDA-ს მტკიცებულებად შესანახად სპეციალური ღონისძიებების გამოყენება უნდა მოხდეს [1].

PDA-ების უმეტესობა იყენებს შემდეგ საოპერაციო სისტემებს: Palm OS, the Psion EPOC, ან Windows CE საოპერაციო სისტემებს. Windows CE საოპერაციო სისტემის გამოყენება PDA-ს Windows -ზე დაფუძნებული პერსონალური კომპიუტერების სრულად შესატყვისად აქცევს [1].

PDA-ების მტკიცებულებად ამოღებისას შემდეგი უნდა გაითვალისწინოთ [2]:
შეგროვება;
თუ **კომპიუტერული ქსელი** იქნება აღმოჩენილი (იხ. მე-5.1.3 თავი), **დაუკავშირდით კომპიუტერის ექსპერტიზის ექსპერტს** თქვენ სამსახურში ან გარე ექსპერტს, რომელიც თქვენი უწყების მიერ დასახმარებლად არის იდენტიფიცირებული.

გახსოვდეთ, რომ ზოგი PDA შესაძლოა, უკაბელო კავშირით იყოს დაკავშირებული (მაგ., ბლუთუსი, ინფრარედი).
გახსოვდეთ, რომ თუ არის რომელიმე ქსელთან კავშირი, PDA-ზე წვდომა და მასზე არსებული ინფორმაციის მანიპულირება ამოღების დროს შესაძლებელია (მაგ., მაშინ როდესაც ის ჩართულია და ქსელის კავშირის ფარგლებშია).
თუ ჩართულ PDA-ს ნახავთ დანაშაულის ჩადენის ადგილზე, **არ** დააჭიროთ ღილაკს RESET (გადატვირთვა) და **არ** გამოიღოთ ბატარეა, რადგან ამან PDA-ზე შენახული მონაცემების სრული დაკარგვა შეიძლება გამოიწვიოს.
არ ჩართოთ ან გახსნათ PDA ამოღებისას.
ენერგიის მიმწოდებლები და პერიფერიული მოწყობილობა ამოიღეთ, მაგ., მეხსიერების გამაძლიერებლები ან PDA-ს პერსონალურ კომპიუტერთან მიერთების მოწყობილობები (მაგ., ენერგიის მოწოდების საწყისი, კაბელი, დამტენი).
PDA-ებს ჩვეულებრივ ავტომატური გამორთვის ფუნქცია აქვთ, რამაც შესაძლოა, ჩამკეტი ან დამშიფრავი მექანიზმი აამოქმედოს (მათი აქტივიზირება მისი გამორთვითაც შეიძლება მოხდეს).
აირიდეთ დეშიფრვის აქტივიზაცია, რაც შესაძლებელია PDA-ს მუშა რეჟიმში დატოვებით (მაგ., ეკრანის ცარიელ ნაწილზე დაწკაპუნებით) სანამ საექსპერტო რჩევა გახდება ხელმისაწვდომი.
შეფუთვა, გადატანა და შენახვა;
მოათავსეთ PDA საწყისი ენერგიის წყაროს გამოსაკვლევად.
იხ. მე-4.5 თავი შეფუთვის, გადატანისა და შენახვის ზოგადი ინსტრუქციებისთვის.

ჯიბის წიგნაკი ა2 მე-8 თავში PDA-ების ამოღების კარგი პრაქტიკის მონახაზს მოიცავს.

5.2.3 ტელეფონები
ტელეფონი ხელის მოწყობილობაა, რომელიც ან
დამოუკიდებელად, თავისით არსებობს (როგორც მაგ., მობილური ტელეფონები),
დამოკიდებულია დისტანციურ საბაზო სადგურზე (უკაბელო), ან
პირდაპირ მიერთებულია სტაციონალურ სისტემას [5].

მობილურ ტელეფონს შესაძლოა, ზოგი დამატებითი ფუნქცია ჰქონდეს, როგორიცაა, მაგ., ციფრული კამერა (მობილური ტელეფონის კამერა).

ტელეფონმა შესაძლოა, ენერგია მიიღოს შიდა ბატარეიდან, ელექტრონული ჩამრთველის მეშვეობით, ან პირდაპირ სატელეფონო სისტემიდან. ორმხრივი კომუნიკაცია მყარდება ერთი აპარატიდან მეორესთან სტაციონალური ხაზების, რადიო გადამცემების, ბოჭკოვანი სისტემები, ან მათი კომბინაციის გამოყენებით. მრავალ ტელეფონს შეუძლია სახელების, ტელეფონის ნომრებისა და დამრეკავის მაიდენტიფიცირებელი ინფორმაციის დამახსოვრება. ამასთან ერთად, ზოგიერთი მობილური ტელეფონი ინახავს სახელებს, მისამართ ბს, შეხვედრის შესახებ ინფორმაციასა და შემომავალი ზარების შესახებ

ინფორმაციას, იღებს ელექტრონულ ფოსტას, პეიჯერის შეტყობინებასა და სხვადასხვა შეტყობინებას (მაგ., SMS/MMS), და შეიძლება ხმის ჩამწერად იყოს გამოყენებული. დაბოლოს, ზოგიერთი მობილური ტელეფონი PIN-ს, პასვორდსა და სხვა წვდომის კოდებს მოითხოვს, და შეიძლება ინტერნეტში სამუშაოდ იყოს გამოყენებული (ანუ, შეიცავდეს ინტერნეტის წვდომის შესახებ ინფორმაციას) [2,5]. იხ. მე-5.2.1 თავი ამოღების დროს გამოსაყენებელი ზოგადი ინსტრუქციებისთვის.

5.2.4 მიკროპროცესორიანი ბარათები და მაგნიტური ლენტიანი ბარათები

მიკროპროცესორიანი ბარათი მცირე ზომის პორტატული მოწყობილობაა, რომელიც მიკროპროცესორს შეიცავს (ანუ, "ჩიპს", შესაბამისად, მას ზოგჯერ ჩიპიან ბარათს უწოდებენ) რომელსაც მასზე დაშიფრული ფულადი ღირებულების ან აუთენთიფიკაციის ინფორმაციის (პასვორდი), ციფრული სერთიფიკატის, ან სხვა ინფორმაციის შენახვა შეუძლია [5]. ზოგიერთი მიკროპროცესორიანი ბარათი ფაქტიურად მცირე ზომის კომპიუტერია, რადგან მათ ასევე ოპერატიული სისტემა აქვთ (ე.ი. მიკროპროცესორიანი ბარათის ოპერატიული სისტემა). შესაბამისად, მიკროპროცესორიანი ბარათი შეიძლება თავად იყოს პოტენციური მტკიცებულება (როგორც მონაცემთა შესანახი საშუალება) და/ან ის შესაძლოა, შეიცავდეს პოტენციურ ელექტრო მტკიცებულებას თითქმის ისევე, როგორც კომპიუტერული სისტემა.

მიკროპროცესორიანი ბარათები შესაძლოა, სხვადასხვა მიზნითა და ოპერაციისთვის იყოს გამოყენებული, როგორიცაა, მაგალითად,
დაცულ ადგილებში/შენობებში/ოთახებში ფიზიკურად შესაღწევად,
კომპიუტერებზე ან პროგრამებზე ან ფუნქციებზე (მაგ., დაშიფვრის გასაღებად) წვდომისთვის სამართავ მარკერად,
საბანკო მანქანებიდან თანხის გამოსატანად,
საბანკო მანქანებით გადასახადის გადასახდელად,
როგორც ელექტრონული საფულე,
როგორც მომხმარებლის ბარათი/საბანკო ბარათი,
როგორც სოციალური უზრუნველყოფის ბარათი (როგორც ეს ავსტრიაში 2004 წლიდან),
როგორც ხელმოსაწერი ბარათი, ელექტრონული ხელმოწერის შესაქმნელად,
ელექტრონული მმართველობის მომსახურებისთვის (მაგ., მოქალაქის ბარათი ავსტრიაში),
როგორც მონეტით ტელეფონზე სასაუბრო ბარათი, ან
როგორც პერსონალური მონაცემების, მისამართების, შეღწევის კოდების შემნახველი საშუალება.

პოტენციური მტკიცებულება შესაძლოა, იყოს ზემოთ ნახსენებ ფუნქციებთან დაკავშირებული ნებისმიერი მონაცემი, ისე როგორც თავად ბარათი [5].

მიკროპროცესორიანი ბარათის ზომა განზრახ არის სტანდარტიზებული და ის 85.6 x 54 x 0.76 მმ-ია (ანუ, ფორმატი ID-1, ე.წ. "საბანკო ბარათის

ზომა"). მას ელექტრო საკონტაქტო ადგილი აქვს ბარათის ზედაპირზე. მიკროპროცესორიანი ბარათები ხშირად მაგნიტურ ლენტასაც შეიცავენ. სხვა ჩიპური ბარათებიც არსებობს, რომლის ფორმატი ID-0-ა (ზომა - 25x15x0.76 მმ). ეს ბარათები, როგორც წესი, მობილურ ტელეფონებში გამოიყენება (SIM ბარათი). დაბოლოს, USB სულ უფრო პოპულარული ხდება, რადგან ისინი შეიცავენ როგორც ჩიპს (იმავე სტანდარტების გათვალისწინებით, როგორც ჩიპი მიკროპროცესრიან ბარათში) და ჩიპის ბარათის წამკითხველის ფუნქციას.

უკონტაქტო მიკროპროცესორიანი ბარათები არ შეიცავენ საკონტაქტო ზედაპირს, თუმცა სხვაგვარად, როგორც წესი, ისევე გამოიყურებიან, როგორც საკრედიტო ბარათები ან საკონტაქტო ზედაპირის მქონე მიკროპროცესორიანი ბარათები. დაბოლოს, ე.წ. "სუპერ მიკროპროცესორიანი ბარათები" შეიცავენ მცირე დისფლეისა და ციფრულ კლავიატურას, რამაც მნიშვნელოვნად შეიძლება გაზარდოს გამოყენების უსაფრთხოება.

მიკროპროცესორიანი ბარათის მონაცემები და ფუნქციები ჩვეულებრივ დაცულია საიდუმლო პერსონალური კოდით (მაგ., პირადი მაიდენტიფიცირებელი ნომერი, PIN), მაგ., ბარათი მხოლოდ მას შემდეგ ხდება ხელმისაწვდომი, რაც მოხდება კომპიუტერის კლავიატურაზე ან ბარათის წამკითხველი მოწყობილობის კლავიატურაზე (ან თავად სუპერ მიკროპროცესორიან ბარათზე) ამ კოდის აკრეფვა.

მიკროპროცესორიანი ბარათის ამოღებისას შემდეგის გათვალისწინება უნდა მოხდეს:
არ გადაკეცოთ ის.
არ მოახდინოთ განსაკუთრებული ტემპერატურების გავლენის ქვეშ.
არ შეეხოთ ელექტრონული საკონტაქტო ადგილს.
დაიცავით დაკაწვრისგან, სითხისგან, მაგნიტური გავლენისგან, ა.შ.
შეეცადეთ პირადი მაიდენტიფიცირებელი ნომერი - PIN მოიპოვოთ (ეძებეთ ბარათთან ახლოს ჩანაწერებში, კითხეთ სანდო მომხმარებლებს. **არ** შეეცადოთ ბარათზე არსებულ მონაცემებზე ან მის ფუნქციებზე წვდომის მოპოვებას, მაშინაც კი, როდესაც ვითომდა სწორი პირადი მაიდენტიფიცირებელი ნომერი - PIN გითხრათ პოტენციურმა ეჭვმიტანილმა. არაზუსტი პირადი მაიდენტიფიცირებელი ნომერის - PIN-ის შეყვანამ შესაძლოა, მონაცემთა აღუდგენელი დაკარგვა/ბარათის დაბლოკვა გამოიწვიოს (ზოგ შემთხვევაში ბარათის განბლოკვა შესაძლებელია სხვა საიდუმლო პერსონალური კოდით, რომელსაც PUK ჰქვია, პერსონალური განბლოკვის გასაღები).
გადაიღეთ ფოტო/ჩაინიშნეთ/გააკეთეთ ასლი ინფორმაციისა ამობეჭდილიდან ბარათზე. მან შესაძლოა ღირებული ინფორმაცია გაამჟღავნოს (მაგ., ბარათის მფლობელის პირადი მონაცემები, საბანკო ანგარიშების ნომრები, საკრედიტო ბარათების კომპანიები, ბიზნეს კონტაქტები, ა.შ.).
თუ შესაძლებელია/საჭიროა, ამოიღეთ მიკროპროცესორიანი ბარათის წამკითხველი მანქანაც (იხ. ასევე მე-5.2.1 თავი).

5.2.5 ტელეფონის მოპასუხე აპარატები

ტელეფონის მოპასუხე აპარატი ელექტრონული მოწყობილობაა, რომელიც ტელეფონის ნაწილია ან ტელეფონსა და სტაციონალურ კავშირს შორის არსებულია. ზოგი მოდელი მაგნიტურ ლენტებს იყენებს, მაშინ როდესაც სხვები ელექტრონულ (ციფრულ) ჩამწერ სისტემებს იყენებენ. ტელეფონის მოპასუხე აპარატი იწერს ხმოვან შეტყობინებებს დამრეკველებისგან მაშინ, როდესაც ის მხარე, რომელსაც დაურეკეს, ვერ პასუხობს ან არ პასუხობს სატელეფონო ზარს. ეს ჩვეულებრივ ახმოვანებს იმ მხარის შეტყობინებას, რომელსაც დაურეკეს, მანამ, სანამ ჩაიწერს შეტყობინებას [5].

ტელეფონის მოპასუხე აპარატებს შეუძლიათ ხმოვანი შეტყობინებების და, ზოგ შემთხვევაში, შეტყობინების დატოვების დროისა და თარიღის შენახვა. მათ ასევე შეიძლება მოიცვან სხვა ხმოვანი ჩანაწერები.
პოტენციური მტკიცებულებაა [5]
დამრეკავის მაიდენტიფიცირებელი ინფორმაცია,
წაშლილი შეტყობინებები,
ბოლო დარეკილი ნომერი,
მემო,
ტელეფონის ნომრები და სახელები, და
ფირები.

იხ. მე-5.2.1 თავი ზოგადად გამოსაყენებელი ამოღების ინსტრუქციებისთვის.

5.2.6 ციფრული კამერები
ციფრული კამერა გამოსახულებისა და ვიდეოს ჩამწერი ციფრული მოწყობილობაა, რომელსაც შიდა მეხსიერება, დაკავშირებული შესანახი საშუალება და კონვერსიის შემძლე ჰარდვეარი აქვს, რომელსაც შეუძლია გამოსახულებისა და ვიდეოს გადატანა კომპიუტერებში. ციფრული კამერები აფიქსირებენ გამოსახულებასა და/ან ვიდეოს ციფრულ ფორმატში რაც ადვილად გარდაიქმნება კომპიუტერული შენახვის საშუალებაში სანახავად და/ან რედაქტირებისთვის [5]. ზოგიერთი მობილური ტელეფონი ციფრული კამერაც არის ასევე (მაგ., მობილური ტელეფონი კამერით).
პოტენციური მტკიცებულებაა [5]
თავად კამერა,
გამოსახულებები,
განცალკევებადი კარტრიჯები,
ხმა,
დროისა და თარიღის აღმნიშნველი ჩანაწერი, და
ვიდეო.

იხ. მე-5.2.1 თავი ზოგადად გამოსაყენებელი ამოღების ინსტრუქციებისთვის.

5.2.7 ფაქსის მანქანები

ფაქსის მანქანა არის მოწყობილობა, რომელიც ახდენს გამოსახულებისა და ტექსტის სკანირებას და გზავნის მათ სატელეფონო ხაზებით. ეს ფუნქცია კომპიუტერებშიც არის (მაგ., ფაქსი/მოდემი პერსონალური კომპიუტერის ბარათები). ფაქსის მანქანები შესაძლოა შემდეგ მტკიცებულებებს მოიცავდეს [2,5]:

ფირის კარტრიჯი,
წინასწარ დაპროგრამებული ტელეფონის ნომრები (ე.ი. მოკლე რეკვის სიები),
გადაცემული და მიღებული დოკუმენტების ისტორია,
მრავალ გვერდიანი გასული, შენახული ან მოგვიანებით გაგზავნილი ან შემოსული შესანახი და მოგვიანებით ამოსაბეჭდი ფაქსის დასკანერების შემძლე მეხსიერება,
ფაქსის გადაცემი ოქმი (ე.ი. გაგზავნა/მიღების სია),
ფაქსის მფლობელის სახელი და
საათის რეგულირება.

იხ. მე-5.2.1 თავი ზოგადად გამოსაყენებელი ამოღების ინსტრუქციებისთვის.

5.2.8 პრინტერები

პრინტერებმა შესაძლოა, შეინახონ გამოყენების სია, დროისა და თარიღის ამსახველი ინფორმაცია, და, თუ ქსელშია ჩართული, მათ შეიძლება ქსელის მაიდენტიფიცირებელი ინფორმაცია შეინახონ. ამასთან ერთად, უნიკალური მახასიათებლებით, შესაძლოა, პრინტერის ამოცნობა მოხდეს. პოტენციური მტკიცებულება მოიცავს [5]

დოკუმენტებს,
ჰარდ დრაივს,
მელნის კარტრიჯებს,
ქსელის მაიდენტიფიცირებელ ინფორმაციას,
როლერზე დადებულ ინფორმაციას,
დროისა და თარიღის მაჩვენებელს, და
მომხმარებლის მიერ მისი მოხმარების ისტორიას.

იხ. მე-5.2.1 თავი ზოგადად გამოსაყენებელი ამოღების ინსტრუქციებისთვის.

5.2.9 სკანერები

სკანერები ციფრული მოწყობილობებია, რომლებითაც ტექსტისა და გამოსახულების დასკანერება და მათი ციფრულ ფორმატში შენახვა ხდება. თავად მოწყობილობა შეიძლება, მტკიცებულება იყოს. დასკანერების შესაძლებლობის ქონა შესაძლოა, უკანონო ქმედების დამტკიცებაში დაგვეხმაროს (მაგ., ბავშვთა პორნოგრაფია, ჩეკების გაყალბება, ფულის გაყალბება, პირადობის დამადასტურებელი დოკუმენტების გაყალბება). ამასთან, წუნმა, როგორიცაა კვალი მინაზე, შესაძლოა დოკუმენტების დასამუშავებლად გამოყენებული სკანერი უნიკალურ მაიდენტიფიცირებლად აქციოს [5].

იხ. მე-5.2.1 თავი ზოგადად გამოსაყენებელი ამოღების ინსტრუქციებისთვის.

5.2.10 ასლის გადამღებები (ასლის გადამღები მანქანები)
ზოგიერთი ასლის გადამღები მანქანა ინარჩუნებს მომხმარებლის მიერ მათი გამოყენების შესახებ ინფორმაციას და მასზე გაკეთებული ასლების ისტორიას. ასლის გადამღები მანქანები, რომლებსაც აქვთ ერთხელ დასკანერების/მრავალი დაბეჭდვის ფუნქცია, დოკუმენტების მეხსიერებაში ერთჯერადად სკანირების შესაძლებლობას იძლევა, რომ მოხდეს მათი მოგვიანებით ბეჭდვა. პოტენციური მტკიცებულება მოიცავს დოკუმენტებს, დროისა და თარიღის ამსახველ ინფორმაციას, და გამოყენების ისტორიას [5]. იხ. ასევე სკანერები მე-5.2.9 თავში.

იხ. მე-5.2.1 თავი ზოგადად გამოსაყენებელი ამოღების ინსტრუქციებისთვის.

5.2.11 მრავალფუნქციური მანქანები
მე-5.2.7-დან მე-5.2.10 თავებში აღწერილი მოწყობილობები შესაძლოა, ერთ მოწყობილობაში გაერთიანდნენ (მაგ., ასლის გადამღები მანქანა, სკანერი და ფაქსის მანქანა). ასევე, სხვადასხვა ფიზიკურად ცალ-ცალკე მყოფი მოწყობილობა შესაძლოა, ლოგიკურად ფუნქციონირებდეს, როგორც ერთი მრავალფუნქციური მანქანა, თუ ისინი ერთმანეთთან ქსელის მეშვეობით არიან დაკავშირებულნი.

5.2.12 პეიჯერები
პეიჯერი არის მოწყობილობა, რომელიც ელექტრონული შეტყობინებების, ციფრული (მაგ., ტელეფონის ნომრები) და ასო-ციფრული შეტყობინებების (ტექსტი, ხშირად ელექტრონული ფოსტის ჩათვლით) გასაგზავნად და მისაღებად შეიძლება, იყოს გამოყენებული [5].

მობილური კომპიუტერული მოწყობილობებიც შეიძლება გამოყენებული იყოს, როგორც პეიჯერები (იხ. მე-5.2.2 თავი).

იხ. მე-5.2.1 თავი ზოგადად გამოსაყენებელი ამოღების ინსტრუქციებისთვის.

5.2.13 GPS მოწყობილობები და სხვა სატელიტურად მოწყობილი აღჭურვილობა

გლობალურად განწყობილი სისტემების (GPS) მოწყობილობები წინა მგზავრობის შესახებ ინფორმაციის მატარებელნი არიან დანიშნულების ადგილის, გზის მონაკვეთებისა და მარშრუტების შესახებ ინფორმაციის მოწოდებით. ზოგიერთი მათგან წინა დანიშნულების ადგილის შესახებ ინფორმაციას ავტომატურად ინახავს და მოიცავს მგზავრობის შესახებ ისტორიას. პოტენციური მტკიცებულებაა [5]:
საცხოვრებელი ადგილი,
წინა დანიშნულების ადგილები,
მგზავრობის ისტორია,

გზების შესახებ ინფორმაცია,
საგზაო მონაკვეთის აღმნიშვნელი კოორდინატები და
საგზაო მონაკვეთის სახელი.

იხ. მე-5.2.1 თავი ზოგადად გამოსაყენებელი ამოღების ინსტრუქციებისთვის.

არგოსი კიდევ ერთი მაგალითია სატელიტურად განლაგებული მოწყობილობებისა (იხ. ტერმინთა განმარტება მე-7 თავში).

5.2.14 ელექტრონული საათები
ელექტრონული საათების რამდენიმე სახეობა არსებობს, რომლებსაც პეიჯერების ფუნქციის შესრულება შეუძლია, ელექტრონული შეტყობინების შენახვით. მათ დამატებითი ინფორმაციის, როგორიცაა მისამართის წიგნები, შეხვედრების დანიშვნის კალენდარი, ელექტრონული ფოსტა და ჩანაწერები, შენახვაც შეუძლიათ. ზოგერთ მათგანს კომპიუტერებთან ინფორმაციის სინქრონიზების ფუნქციაც აქვთ ასევე [5]. პოტენციური მტკიცებულება მოიცავს
მისამართების წიგნს,
შეხვედრების ცალენდარს,
ელექტრონულ ფოსტას,
ჩანაწერებს და
ტელეფონის ნომრებს.

ციფრული საათები ასევე შეიძლება, შეიცავდნენ მონაცემთა შემნახველ მოწყობილობას, როგორიცაა USB, ან კამერაც კი.

იხ. მე-5.2.1 თავი ზოგადად გამოსაყენებელი ამოღების ინსტრუქციებისთვის.

5.2.15 მაგნიტური ლენტის მკითხველები
მაგნიტური ლენტის მკითხველები (მაგ., საკრედიტო ბარათის სქიმერები) გამოიყენება პლასტიკური ბარათის მაგნიტურ ლენტაზე არსებული ინფორმაციის წასაკითხად. პოტენციური მტკიცებულება მაგნიტური ლენტის ნაკვალევზე არსებული ბარათის მფლობელის ინფორმაციაა, რომელიც მოიცავს [5]
მაგ., ბარათის მოქმედების ვადასა და საკრედიტო ბარათის ნომრებს და უსაფრთხოების ინფორმაციას.

იხ. მე-5.2.1 თავი ზოგადად გამოსაყენებელი ამოღების ინსტრუქციებისთვის.

6. ბიბლიოგრაფია

[1] პოლიციის ხელმძღვანელ ოფიცერთა ასოციაცია (დიდი ბრიტანეთი), “კარგი პრაქტიკის სახელმძღვანელო კომპიუტერზე დაფუძნებული მტკიცებულებისთვის” ვერსია 2.0: 1999 წლის ივნისი, ვერსია 3.0: 2003 წლის აგვისტო.

[2] შინაგან საქმეთა ფედერალური სამინისტრო (ავსტრია), "ელექტრონული მტკიცებულების ამოღებისა და შეფასების სახელმძღვანელო" (გერმანულ ენაზე), ვერსია 1.0, 2001 წლის ნოემბერი.

[3] პოლიციის თანამშრომლობის სამუშაო ჯგუფი (ევროპის კავშირის საბჭო), "საინფორმაციო ტექნოლოგია და ჩხრეკისა და ამოღების კარგი პრაქტიკა", 2001.

[4] კომპიუტერული მტკიცებულების საერთაშორისო ორგანიზაცია, "პირველი რეაგირების მომხდენთა კარგი პრაქტიკის სახელმძღვანელოს მაგალითი," *Proc. OCE* 2000 კონფერენცია, როსინ სუ ბუა, საფრანგეთი, 2000 წლის დეკემბერი.

[5] აშშ იუსტიციის დეპარტამენტი, სამართლის პროგრამების სამსახური, იუსტიციის ეროვნული ინსტიტუტი, ტექნიკური სამუშაო ჯგუფი ელექტრონული დანაშაულის ჩადენის ადგილის გამოძიებისთვის, "გამოძიება ელექტრონული დანაშაულის ჩადენის ადგილზე: სახელმძღვანელო პირველადი რეაგირების მომხდენთათვის," 2001 წლის ივლისი, http://www.ncjrs.org/pdffiles1/nij/187736.pdf.

[6] ევროპის საბჭო, "კომპიუტერული დანაშაულის შესახებ კონვენცია", ევროპული ხელშეკრულებების სერია № 185, 2001 წლის ნოემბერი, http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185&CM=8&DF=11/07/03.

[7] საჯარო მომსახურებისა და სპორტის ფედერალური სამინისტრო (ავსტრია). "IT-Sicherheitshandbuch für die öffentliche Verwaltung, Teil 2: IT-Sicherheitsmaßnahmen," (გერმანულ ენაზე), ვერსია 2.0, 2001 წლის სექტემბერი, http://www.a-sit.at/beratung/sicherheitshdb/a_sihdb_t_2.pdf.

[8] Bundesamt für Sicherheit in der Informationstechnik (გერმანია) "საინფორმაციო ტექნოლოგიების საბაზისო დაცვის სახელმძღვანელო," http://www.bsi.bund.de/gshb/english/menue.htm.

[9] ინტერპოლი, "ინტერნეტ დანაშაულთან ბრძოლა", ინტერნეტ ვიდეო მასალა, 2002.

[10] მაღალი ტექნოლოგიებით ჩადენილი დანაშაულის წინააღმდეგ ბრძოლის სწავლების ეროვნული ცენტრი (დიდი ბრიტანეთი), "სტაჟიორთა მომზადება: მაღალი ტექნოლოგიებით ჩადენილი დანაშაულის მიმოხილვა", ვერსია 1.1 (სლაიდები), 2002.

[11] გზამკვლევი ტექნიკური სამიზნის ქსელში, http://searchtechtarget.techtarget.com.

[12] ევროპოლი, "ევროპის სამართალდამცავ ორგანოებში პოლიციის მიერ გამოყენებული ტექნიკისა და პრაქტიკის სახელმძღვანელო", 2003.

7. ტერმინთა განმარტება

ტელეფონის მოპასუხე აპარატი	ელექტრონული მოწყობილობა, რომელიც ტელეფონის ნაწილია, ან ტელეფონსა და სტაციონალურ ხაზს შორის არის მიმაგრებული [5].  ტელეფონის მოპასუხე აპარატი (http://discallowphonerates.bizland.com)

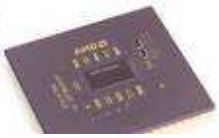
არგოსი	სატელიტზე დაფუძნებული მდებარეობა და მონაცემთა მოგროვება (http://www.cls.fr/). არგოსი გამოგონებული იყო 1978 წელს და ახლა 300-ზე მეტი ორგანიზაცია იყენებს 40 ქვეყანაში.  არგოსის მიმღები
არქივი	არქივი კომპიუტერული ფაილების ერთობლიობაა, რომელთა მოგროვება მოხდა მონაცემთა სარეზერვოდ შესანახად, სხვა ადგილზე გადასატანად, კომპიუტერიდან მოშორებით შესანახად, რომ მოხდეს ჰარდ დისკზე მეტი ადგილის გამოთავისუფლება, ან სხვა მიზნის მისაღწევად. პერსონალურ კომპიუტერზე, რომელზეც Windows ოპერატიული სისტემა მუშაობს, WinZip პოპულარული პროგრამაა, რაც საშუალებას იძლევა, შეიქმნას არქივი ან მოხდეს მისი ფაილების მიგან გამოცალკევება (არქივის ფაილის სახელის ბოლოსართია ".zip"). WinZip ასევე აპატარავებს დაარქივებულ ფაილებს [**როორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
საბანკო მანქანა (ATM)	საბანკო მანქანა (ავტომატურად მთვლელი მანქანა). მანქანა ნაღდი ფულის გამოსატანად გამოიყენება.

	 ATM (http://www.maxim-ic.com)
სარეზერვო ინფორმაცია	ყველანაირი ინფორმაციის ასლი, რომელიც ინახება კომპიუტერში იმ შემთხვევისთვის, თუ პირველად ვერსიას რამე დაემართება [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
ბიომეტრიული სკანერი	კომპიუტერულ სისტემაზე მიერთებული მოწყობილობა, რომელიც პირის ფიზიკურ მახასიათებლებს ამოიცნობს (მაგ., თითის ანაბეჭდები, ხმა, ბადურა) [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  თითის ანაბეჭდების სკანერი (http://www.eyenetwatch.com)
BIOS	ძირითადი შენატანისა და შედეგის სისტემა. რუტინების ერთობლიობა, შენახული მხოლოდ წასაკითხად ხელმისაწვდომ მეხსიერებაში, რაც კომპიუტერს შესაძლებლობას აძლევს, სისტემის ოპერირება დაიწყოს და მოახდინოს დაკავშირება სხვადასხვა მოწყობილობასთან, როგორებიცაა დისკის დრაივები, კლავიატურა, მონიტორი, პრინტერი და კომუნიკაციის პორტები [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
ბლუთუსი	ტელეკომუნიკაციების ინდუსტრიის მახასიათებელი, რომელიც აღწერს, როგორ შეუძლიათ ადვილად დაკავშირება მობილურ ტელეფონებს, კომპიუტერებს და PDA ერთმანეთთან და სახლისა და სამსახურის ტელეფონებსა და კომპიუტერებთან, მცირე უკაბელო ქსელის გამოყენებით. ბლუთუსი დაბალ ხარჯიანი რადიოგადამცემი ჩიპის არსებობას საჭიროებს ყველა მოწყობილობაში [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].

	 ბლუთუსი (http://www.bsi.de)  ბლუთუსის USB დამცავი დამახშობელი (http://mightygps.com)
ბარათის წამკითხველი	იხ.: მიკროპროცესორიანი ბარათის წამკითხველი ან პერსონალური კომპიუტერის ბარათის წამკითხველი.
CD-ROM CD-R CD-RW	კომპაქტ დისკი - მხოლოდ წაკითხვის მეხსიერება (CD-ROM): დისკი, რომლიდანაც მონაცემის წაკითხვაა შესაძლებელი. კომპაქტ დისკი - ჩამწერი (CD-R): დისკი, რომელზეც მონაცემების ჩაწერა შეიძლება, მაგრამ წაშლა - არა [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**]. კომპაქტ-დისკი- გადაწერვადი (CD-RW): დისკი, რომელზე მონაცემის ჩაწერა და წაშლა შესაძლებელია [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  CDROM (http://www.discoverengineering.org)
სამონტაჟო პლატა	თხელი დაფა მასზე დაყენებული ჩიპებით, მოწყობილობებით და სხვა ელექტრონული კომპონენტებით [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**] (ასევე უწოდებენ საბეჭდ სამონტაჟო პლატას).

	 სამონტაჟო პლატა (http://www.asl-systems.com)
CMOS	დამატებითი (კომპლემენტარული) მეტალ-ოქსიდის ტრანზისტორი. ტრანზისტორის ტექნოლოგიაა, რაც დღევანდელი კომპიუტერების უმრავლესობის მიკროჩიპებშია გამოყენებული. ის ტიპიურად BIOS-ის კომპიუტერულ უპირატესობას ფლობს ენერგიის გამორთვისას, ბატარეის დახმარებით (ადაპტირებულია [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**]-დან).
კომპიუტერზე დაფუძნებული მტკიცებულება	იხ. ელექტრონული მტკიცებულება.
კომპიუტერის კაბელი კომპიუტერის დამაკავშირებელი	კომპიუტერული სისტემის კომპონენტების მთავარ ნაწილთან დასაკავშირებლად გამოიყენება. მას შესაძლოა, სხვადასხვა ფერი, სისქე და ფორმა, და განსხვავებული მაკავშირებლები ჰქონდეს, გამომდინარე იქიდან, თუ რა კომპონენტებზე არიან ისინი მიერთებულნი.  PS2 კაბელი (http://lanstore.com.au)  SCSI კაბელი (http://www.iworldconnection.com)  პარალელური პორტების

	კაბელი (http://fog.ccsf.org)  სერიული პორტის კაბელი (http://www.rozakk.freeserve.co.uk)  USB კაბელი (http://www.cablesnmor.com)  აუდიო ვიდეო კაბელი (http://www.ramelectronics.net)
უკონტაქტო მიკროპროცესორიანი ბარათი	Smart cards without contact plate that otherwise look the same as the smart cards with contacts.  Contactless smart card (http://www.fta.dot.gov)
ასლის გადამღები მანქანა	იხ. ფოტოკოპირების მოწყობილობა
ცენტრალური პროცესორი (CPU)	ცენტრალური პროცესორი. კომპიუტერის გამომთვლელი და კონტროლის ერთეული. იგი კომპიუტერის შიგნით არის განთავსებული და კომპიუტერში ყველა არითმეტიკული, ლოგიკური და კონტროლის ფუნქციის განმხორციელებელ "ტვინს" წარმოადგენს [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].

	 CPU (http://www.kosscomputers.com)
ენერგიის საწყისი - საწყისი წერტილი	ჯიბის - პერსონალური ციფრული თანაშემწის - მონაცემების სინქრონიზება სხვა კომპიუტერულ სისტემებში.  პერსონალური ციფრული თანაშემწის ენერგიის საწყისი - საწყისი წერტილი (http://computingreview.bizrate.com)
საკრედიტო ბარათის სკიმერი	საკრედიტო ბარათის წამკითხველები მაგნიტის ლენტით. იხ.: მაგნიტური ლენტის წამკითხველი.
კრიპტოგრაფია	ინფორმაციის დაშიფვრის მეცნიერება, მისი საიდუმლოების დასაცავად, მისი შეუბღალველობის დასაცავად და/ან უსაფრთხოების სხვა ღონისძიებების უზრუნველსაყოფად.
დიქტოფონი	ხელის ელექტრონული მიკროფონიანი მოწყობილობა, ხმოვანი შეტყობინებების შენახვის შესაძლებლობით.  დიქტოფონი (http://www.medword.com)
ციფრული კამერა	ციფრულ ფორმატში ფოტოგრაფებისა და ვიდეოს შემნახველი კამერა. ვებ კამერები (იხ. ნახატი ქვემოთ) ზრდადი პოპულარობით სარგებლობენ და შეიძლება, ვიდეო კონფერენციებისთვის მოხდეს მათი გამოყენება.

	 ვებ კამერა (http://fotoapparat-verkauf.de)
ციფრული სერთიფიკატი ციფრული ID	ციფრული იდენტიფიცირება. უნიკალური პერსონალური მაიდენტიფიცირებელი მონაცემებია ციფრულ ფორმატში (იხ. ასევე საჯარო წვდომის სერთიფიკატი - პუბლიც კეყ ცერტიფიცატე).
ციფრული ხელმოწერა	ციფრული ღირებულება, რაც მის მიმღებს საშუალებას აძლევს, შეამოწმოს გამომგზავნის პიროვნება და დარწმუნდეს, რომ გზავნილი გზაში არ შეცვლილა [**Error! Reference source not found.**].
ციფრული საათი	ქრონომეტრული მოწყობილობა, რომელსაც პეიჯერის ფუნქციით მუშაობაც შეუძლია, ელექტრონული გზავნილებისა და დამატებითი ინფორმაციის შენახვის, როგორიცაა მისამართების ცნობარები, შეხვედრების კალენდრები, ელექტრონული ფოსტა და შენიშვნები, ჩათვლით. ზოგიერთ მათგანს ასევე აქვთ კომპიუტერთან ინფორმაციის სინქრონიზაციის შესაძლებლობა [**რროორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  ციფრული საათი (http://www.shopthedotcoms.com)
დისკის დანაწევრება	პერსონალურ კომპიუტერებში, დანაწევრება შექმნილი ჰარდდისკის ლოგიკური გაყოფაა იმისთვის, რომ სხვადასხვა ოპერაციული სისტემების ერთი და იმავე ჰარდდისკზე გამოყენება მოხდეს ან მოხდეს ცალკე მყარი დისკის შექმნის იმიტაცია ფაილების სამართავად, მრავალი მმხმარებლის მიერ გამოსაყენებლად, ან სხვა მიზნებისთვის. დისკის დანაწევრება ხდება მაშინ, როდესაც ხდება მყარი დისკის დაფორმატება. ჩვეულებრივ, ერთ ნაწილიანი მყარი დისკი ცნობილია "C:" დისკის სახელით. დისკები ("A:" and "B:"ჩვეულებრივ დისკეტის

	დრაივერებისთვის არის განკუთვნილი და ბოლო ხელმისაწვდომი ასოთი აღინიშნება CD-ROM-ების დრაივები [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
დომეინის სახელის მომსახურება (DNS)	დომეინის სახელის მომსახურება. ინტერნეტის მომსახურება, რომელიც სტანდარტიზებული პროტოკოლების წყებას ეფუძნება, რომელთა მეშვეობით IP მისამართებისთვის მასპინძლის სახელის მინიჭება ხდება და პირიქით. (“თეთრი გვერდები”). მაგალითად, თუ იკითხავთ სერვერის დომეინის IP მისამართისთვის 192.67.198.7 მასპინძლის სახელს, პასუხად უნდა მიიღოთ “www.europol.org”.
საბაზო ბლოკი	მოწყობილობა, რომელზეც პორტატული კომპიუტერი (მაგ., ლაპტოპი, ნოუთბუქი) შეიძლება მიემაგროს დესკტოპ კომპიუტერის მსგავსად გამოსაყენებლად, რომელსაც ჩვეულებრივ მაკავშირებელი აქვს გარეშედ დასაკავშირებელი მოწყობილობებისთვის, როგორებიცაა მყარი დისკები, სკანერები, კლავიატურა, მონიტორები და პრინტერები [5].  საბაზო ბლოკი (http://www.territorialsupplies.com)
დამცავი დამახშობელი	მცირე ზომის გარეშე ჰარდვეარის მოწყობილობა, რომლის მიერთება ხდება კომპიუტერის პორტზე, რომელიც ჩვეულებრივ მოიცავს იმ ინფორმაციის მსგავსი ტიპის ინფორმაციას, რაც მიკროპროცესორიან ბარათზეა (ადაპტირებულია: [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**]).  დამცავი დამახშობელი (http://www.bluetooth-laden.de)
დრაივის დუბლიკატორი	სხვადასხვა მონცემთა შენხვის საშუალებების, მაგ., მყარი დისკების ან კომპაქტ დისკების, სწრაფად კოპირების (დუბლირების)

	მოწყობილობა.  დრაივის დუბლიკატორი (http://www.ce-s.com)
ციფრული ხელმოწერის ხაზი (DSL)	ციფრული ხელმოწერის ხაზი. პროტოკოლების ერთობლიობა, რომელნიც გამიზნულია მონაცემთა მაღალ სიჩქარეზე გაცვლა არსებული სატელეფონო ხაზების მეშვეობით საბოლოო მომხმარებელსა და სატელეფონონო კომპანებს შორის [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
უნივერსალური ციფრული დისკი (DVD)	უნივერსალური ციფრული დისკი. კომპიუტერული დისკის მსგავსია, მაგრამ მონაცემთა უფრო მეტი რაოდენობის შენახვა შეუძლია [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
ელ-მტკიცებულება	იხ. ელექტრონული მტკიცებულება
ელექტრონული ფოსტა	კომპიუტერში შენახული შეტყობინებების ცვლა ტელეკომუნიკაციის მეშვეობით [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
ელექტრნული ფოსტის შეტყობინების ტიპიური დასაწყისი (header)	ელექტრონული შეტყობინებები ორი ნაწილისგან შედგება: წერილის ძირითადი ნაწილი და ელექტრონული შეტყობინების ტიპიური დასაწყისი (header). ფოსტის ტიპიურ დასაწყისში (header)-ში მოცემული ინფორმაცია შეტყობინების მიმღებს აძლევს იმის საშუალებას, რომ დაადგინოს ინფორმაცია გაგზავნის დროსთან, თარიღთან, გამომგზავნთან და საგანთან დაკავშირებით. ყველა ელექტრონულ შეტყობინებას ასევე აქვს განვრცობილი ელექტრნული ფოსტის შეტყობინების ტიპიური დასაწყისი (header) - ეს არის ინფორმაცია, რომელიც ელექტრონული ფოსტის პროგრამებისა და გადამცემი მოწყობილობების მიერ არის დამატებული - რომელიც უფრო მეტ ინფორმაციას აჩვენებს გამგზავნის შესახებ, რომ მოხდეს შეტყობინების ზოგადი მონაცემების მიხედვით ინტერნეტში მიერთებული კონკრეტული კომპიუტერის იდენტიფიცირება (ადაპტირებულია: [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**]).

	მაგალითი: From(გამგზავნი): rth@bieberdorf.edu (R.T. Hood) To(მიმღები): tmh@immense-isp.com Date(თარიღი): Tue, Mar 18 1997 14:36:14 PST X-Mailer: Loris v2.32 Subject(საგანი): Lunch today?
ელექტრონული მტკიცებულება	გამოძიებისთვის ღირებულების მქონე ინფორმაცია და მონაცემები, რომელიც ინახება ან გადაიცემა ელექტრონულ მოწყობილობაში, ან ციფრული შენახვის საშუალებით [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**], ზოგჯერ მას ციფრულ, ან კომპიუტერზე დაფუძნებულ, მტკიცებულებას უწოდებენ.
ელექტრონული ხელმოწერა	იხ.: ციფრული ხელმოწერა.
დაშიფვრა	მონაცემთა გადაადგილებისა და დაშიფვრის მეთოდი. მისი გამოყენება ხდება მარტივი ტექსტის დაშიფრულ ტექსტად გარდაქმნისთვის (მათემატიკური პარამეტრის გამოყენებით, რომელსაც კრიპტოგრაფული გასაღები ეწოდება) იმისთვის, რომ გარდა იმ პირისა, რომლისთვისაც მომზადდა ტექსტი, არავის მიეცეს შესაძლებლობა, წაიკითხონ [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**, **რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
ქსელი Ethernet (ადგილობრივი ქსელების ორგანიზების სტანდარტი)	ფართოდ გამოყენებადი LAN ტექნოლოგია. სპეციფიკაცია მოწოდებულია სტანდარტში IEEE 802.3, ის Xerox-ის მიერ შემუშავდა და მოხდა მისი შემდგომი განვითარება Xerox, DEC, and Intelის მიერ. Ethernet LAN ტიპიურად იყენებს კოაქსიალურ კაბელს ან მავრთულების ერთმანეთზე გადაჯაჭვული სპეციალურ წყაროსთან მისაერთებელს [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**]. Ethernet მისამართი შესაძლოა, იყოს, მაგ., , 08:00:20:03:72:DC.  კოაქსილური კაბელი

	(http://www.coolspringsdesigns.com)
გამფართოვებელი პლატა	ამობეჭდილი სამონტაჟო პლატა შეიძლება მიუერთდეს კომპიუტერს ისეთი შესაძლებლობების დასამატებლად, როგორიცაა LAN ან ვიდეო [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
ფაქსის მანქანა	გამოსახულებისა და ტექსტის მასკანირებელი მოწყობილობა, რომელიც მათ ტელეფონის ხაზით გზავნის [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  ფაქსის მანქანა (http://www.theswensongroup.com)
ფაილების სისტემა	მეთოდი, რომლის მიხედვით ფაილებს სახელი მიენიჭება და ხდება კომპიუტერში შესანახად და ხელახლა გამოსაყენებლად მათი ლოგიკური განთავსება. DOS-ze, Windows-ze, OS/2-ze, Macintosh-ze, და UNIX-ზე დაფუძნებულ ყველა ოპერატიულ სისტემას აქვს ფაილის სისტემები, სადაც ფაილები განლაგებულია სადნე იერარქიული (ხის) სტრუქტურით. ფაილი განთავსებულია დირექტორიაში (საქაღალდე - ფოლდერ ინ ჭინდოწს-ში) ან ქვედირექტორიაში სასურველ ადგილზე ხის სტრუქტურაში [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
ბრანდმაუერი (Firewall) ქსელთაშორისი დაცვის აპარატულ-პროგრამული საშუალება	დაკავშირებული პროგრამების ერთობლიობა, რომლებიც განთავსებულია ქსელის გეითვეი სერვერზე (ე.ი. ქსელის წერტილში, რომელიც მოქმედებს მეორე ქსელთან დაკავშირების პუნქტად), რომელიც იცავს კერძო ქსელის რესურსებს სხვა ქსელების მომხმარებელთაგან [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
პირველი რეაგირების მომხდენი	პირველი რეაგირების მომხდენი სამართალდამცველი ოფიცერი და/ან სხვა საზოგადოებრივი უსაფრთხოების დაცვაზე პასუხისმგებელი პირი, რომელიც დანაშაულის ჩადენის ადგილზე ცხადდება [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
ფლეშ-მახსოვრობის	იხ.: მახსოვრობის ბარათი. ფლეშ-მასხოვრობა

ბარათი	(ზოგჯერ "flash RAM"-ს უწოდებენ), მუდმივად ენერგიით უზრუნველყოფილი ხანგრძლივი მახსოვრობაა, რომლის წაშლა და გადაპროგრამირება შესაძლებელია.
ფლოპი დისკი ფლოპი დისკეტა	დისკი, რომელზე მაგნიტურად არის ინფორმაცია დამაგრებული. ორი ძირითადი ტიპის გვხვდება: 3 ½ ინჩიანი და 5-¼ ინჩიანი. ორივე ოთხკუთხედი და ბრტყელია [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  ფლოპი დისკი (http://www.soapplab.auckland.ac.nz)
ფაილის გადაცემის პროტოკოლი (FTP)	ფაილის გადაცემის პროტოკოლი, სტანდარტული ინტერნეტ პროტოკოლი, უმარტივესი გზაა ფაილების გასაცვლელად კომპიუტერებს შორის ინტერნეტით [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
სათამაშო (Gameboy)	ხელის სათამაშო ელექტრო მოწყობილობა (კარტრიჯებით).  სათამაშო (Gameboy) (http://anduril.ca)
სათამაშო კუბი (Gamecube)	სათამაშო კონსოლი.  სათამაშო კონსოლი (http://www.gamenationtv.com)
GPS (გლობალური პოზიციონირების სისტემა) მოწყობილობა	GPS (გლობალური პოზიციონირების სისტემა) არის 24 კარგად განლაგებული სატელიტის “თანავარსკვლავედი”, რომლებიც დედამიწის ორბიტაზე მოძრაობენ დედამიწაზე შესაბამისი მიმღების მქონე ადამიანებს მათი გეოგრაფიული მდებარეობის გარკვევის შესაძლებლობას აძლევენ. მდებარეობის სიზუსტე დაახლოებით 100-დან 10 მეტრამდე მერყეობს აღჭურვილობის უმეტესობისთვის

	[**რორო! ღეფერენცე სოურცე ნოტ ფოუნდ.**]. GPS მოწყობილობებს შეუძლიათ წინა მგზავრობის შესახებ ინფორმაციის მოწოდება დანიშნულების ადგილის შესახებ ინფორმაციის მეშვეობით, საგზაო ნიშნულებისა და მარშრუტების ჩვენებით [**რორო! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  GPS მოწყობილობა (http://adventuregps.com)
ჰაბი	შეერთების ადგილი ქსელში, სადაც მონაცემების მიღება ხდება ერთი ან მეტი მიმართულებიდან და მათი გადამისამართება ხდება ერთი ან მეტი სხვა მიმართულებით. ის ჩვეულებრივ მუშაობს როგორც მრავალპორტიანი განმმეორებელი ერთი მოქმედებიდან რამდენიმე იდენტური შედეგის მისაღებად (ქმედება=შედეგი). ჰაბი შესაძლოა, მოიცავდეს გარკვეული ტიპის ჩამრთველს (ადაპტირებულია [**რორო! ღეფერენცე სოურცე ნოტ ფოუნდ.**]).  ჰაბი (http://www.bownie.com)
გამოსახულების ასახვა	ელექტრონული აღჭურვილობის მეხსიერების შინაარსის ზუსტი ასლის შექმნა (ასევე ეწოდება გამოსახულების არეკლვა, თუმცა ამ ტერმინის გამოყენება ვებ გვერდების დუბლირების დროსაც ხდება).
ინტერნეტ შეტყობინების წვდომის პროტოკოლი (IMAP)	ინტერნეტ შეტყობინების წვდომის პროტოკოლი. ინტერნეტის მომსახურება, რომელიც დაფუძნებულია მეილის სერვერიდან (მაგ., IMAP სერვერი) ელექტრონული ფოსტის შეტყობინებების გამოთხოვის ან მიღების სტანდარტიზებულ პროტოკოლზე.
ინფრარედი	ინფრარედის უკაბელო ტექნოლოგია გამოიყენება ხანმოკლე და საშუალო ხანგრძლივობის კომუნიკაციისთვის და აკონტროლებს სხვადასხვა საშუალებას (მაგ., უკაბელო აქდგილობრივ ქსელები, კავშირი ნოუთბუქებსა და დესკტოპ კომპიუტერებს

	შორის, უკაბელო მოდემები, დამცავის სიგნალიზაციის მოწყობილობა). ინფრარედი ელექტრომაგნიტური რადიაციის სპექტრის რაიონში არსებულ ენერგიას იყენებს, რომელიც ხილული სინათლის ტალღებზე გრძელი მაგრამ რადიო ტალღ ბზე მოკლეა. [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  ინფრარედი (http://www.jacobi.de)  ინფრარედის USB (http://www.jacobi.de)
ინტერნეტ პროტოკოლი (IP)	ინტერნეტ პროტოკოლი. ინტერნეტ საინჟინრო სამუშაო ჯგუფის მიერ სტანდარტიზებული პროტოკოლი, რომელიც გამოიყენება ინტერნეტსამუშაოს კავშირისთვის. ინტერნეტ პროტოკოლის მისამართი შესაძლოა, იყოს, მაგალითად, 192.67.198.7.
ინტერნეტ მაკავშირებლებლი (IRC)	ინტერნეტ მაკავშირებლები. ქსელური მომსახურება, რომელიც ვირტუალური შეხვედრის ადგილს უზრუნველყოფს, სადაც ადამიანებს სხვადასხვა საკითხის განხილვა შეუძლიათ. მონაწილეებს შეუძლიათ ჯგუფში დისკუსიებში მონაწილეობის მიღება მრავალი ათასიდან ერთ ინტერნეტ მაკავშირებლის ხაზზე, ან ისაუბრონ კერძოდ (ადაპტირებულია [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**]-დან).
ინტეგრირებული სერვისების ელექტრონული ქსელი (ISDN)	ინტეგრირებული სერვისების ელექტრონული ქსელი. მაღალი სიჩქარის ციფრული სატელეფონო ხაზი მაღალი სიჩქარის ქსელური კომუნიკაციისთვის [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
ინტერნეტ მომსახურების მომწოდებელი (ISP)	ინტერნეტ მომსახურების მომწოდებელი. ორგანიზაცია, რომელიც ინტერნეტზე წვდომას უზრუნველყოფს. ზოგი ინტერნეტ მომსახურების მომწოდებელი ამ

	მომსახურებას ტელეფონის ხაზების გამოყენებით უზრუნველყოფს (მაგ., მოდემი, ISDN) ან საკაბელო ხაზს იყენებს (მაგ., DSL), სხვები კი შეიძლება კერძო ხაზებით დაკავშირებას გთავაზობდნენ (მაგ., გამოყოფილი ხაზი) (ადაპტირებულია [**რეფერენცე სორცე ნოტ ფოუნდ.**]-დან).
JAZ®	მშორებადი მყარი დისკის სისტემა. JAZ დრაივი მცირე, პორტატული მყარი დისკია, რომელიც უპირველესად პერსონალური კომპიუტერის ფაილების დუბლირებისთვის და დაარქივებისთვის გამოიყენება. JAZ დრაივი გაყიდვაში აქვს Iomega Corporation-ს, იმავე კომპანიას, რომელმაც ZIP დრაივი შექმნა. როგორც JAZ დრაივი, ისე დისკებიი ორი ზომისაა 1 GB და 2 GB.  JAZ (http://www.cadinfo.net)
ადგილობრივი ქსელი (LAN)	ადგილობრივი ქსელი. IEEE-ს (ელექტრო და ელექტრონიკის ინჟინერიის) მიერ სტანდარტიზებული ქსელური ტექნოლოგიების საერთო სახელი.
LAN კონფიგურაცია	LAN-ის ტოპოლოგიური სქემა, როგორიცაა Ethernet ან მარკერული წვდომის წრიული ქსელი, ან MAC მისამართები, როგორიცაა Ethernet მისამართი(MAC: საშუალო წვდომის კონტროლი, საკაბელო დონის ნაწილი OSI-ის შვიდ დონიან მოდელში).
მსუბუქი დირექტორიის წვდომის პროტოკოლი (LDAP)	მსუბუქი დირექტორიის წვდომის პროტოკოლი. სტანდარტიზებული პროტოკოლების წყება, ონლაინ დირექტორიებზე ინტერნეტით წვდომისთვის (მაგ., ონლაინ მონაცემთა ბაზე სპეციალურ ფორმატში).
მაგნიტურ ლენტიანი ბარათი	პლასტიკური ბარათი მაგნიტური ლენტით, რომელსაც შეუძლია სხვადასხვა მიზნით გამოსაყენებელ მონაცემთა შენახვა (მაგ., მიდენტიფიცირებელი მონაცემი, საბანკო ანგარიშის შესახებ მონაცემები).  მაგნიტურ ლენტიანი ბარათი (http://calphotoid.berkeley.edu)

მაგნიტურ ლენტიანი ბარათი	წამკითხველი მონქანა მაგნიტურ ლენტიანი ბარათებისთვის.  მაგნიტურ ლენტიანი ბარათი (http://www.shopping.com)
მაგნიტური ლენტი	მაგნიტურად შეფუთული პლასტიკატის გრძელი ლენტი. მათი შენახვა ძირითადად კარტრიჯებში (ვიდეო, აუდიო ან ჩამწერი პორტატული ვიდეო კამერის ლენტის მსგავსი) ხდება, თუმცა ასევე შესაძლოა, ბაბინაზეც იყოს დახვეული (ბაბინაზე დახვეული აუდიო ლენტის მსგავსად). მისი გამოყენება ხდება კომპიუტერული მონაცემების ჩასაწერად, რგორც წესი, კომპიუტერის ინფორმაციის დუბლირებისთვის [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  მაგნიტური ლენტი (http://www.sony.net)
უნივერსალური გამომთვლელი მანქანა	დიდი კომპიუტერის აღსანიშნავი წარმოების მიერ გამოყენებული ტერმინი, რომელიც ჩვეულებრივ დიდი კომპიანიის მიერ, როგორიცაა IBM, იწარმოება. კომერციული გამოყენებისთვის და სხვა ფართომასშტაბიანი კომპიუტერული პროცესებისთვის [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  უნივერსალური გამომთვლელი მანქანა (http://www.lit.berlin.de)
ძირითადი კორპუსი	ჩვეულებრივ, პერსონალური კომპიუტერის ყველაზე დიდი ზომის ნაწილი, ყუთი, რომელიც უმნიშვნელოვანეს კომპონენტებს მოიცავს (ზოგჯერ პერსონალური კომპიუტერის კოშკს უწოდებენ). მას წინა ნაწილზე დრაივები აქვს და კლავიატურის, მაუსის, პრინტერისა და სხვა ნაწილების

	შესაერთებლად უკანა ნაწილზე აქვს პორტები [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  ძირითადი კორპუსი (http://www.color-case.com)
მახსოვრობის ბარათი	(ზოგჯერ ფლეშ მახსოვრობის ბარათს ან მონაცემთა შემნახველ ბარათს უწოდებენ). მონაცემთა მცირე ზომის საშუალება, რმლის გამოყენება ისეთი მონაცემების შესანახად ხდება, როგორც არის ტექსტი, სურათები, აუდიო და ვიდეო, მცირე, პორტატულ ან დისტანციური კომპიუტერული მოწყობილობებზე გამოსაყენებლად. რამდენიმე მახსოვრობის ბარათია ბაზარზე მიმოქცევაში, მათ შორის SD ბარაში (უსაფრთხო ციფრული), CF ბარათი (CompactFlash by SanDisk), SmartMedia ბარათი (Toshiba-ს მიერ ნაწარმოები), Memory Stick (Sony-ის მიერ ნაწარმოები), და MultiMediaCard (MMC SanDisk და Siemens AG/Infineon Technologies AG-ის მიერ ნაწარმოები). ბარათ ბის უმრავლესობას ენერგიით მუდმივად უზრუნველყოფილი, ენერგო დამოუკიდებელი მახსოვრობა აქვთ (მაგ., flash მახსოვრობა), რაც ნიშნავს, რომ მონაცემები ბარათზე სტაბილურად ინახება, ენერგიის წყაროს დაკარგვის საშიშროება არ ემუქრება, და პერიოდული დატენვა არ სჭირდება [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**]. მისი გამოყენება სხვადასხვა აღჭურვილობაში ხდება, მათ შორის კომპიუტერებში, ციფრულ კამერებში და PDA (პერსონალურ ციფრულ თანაშემწე)-ებში.  დაცული ციფრული ბარათი (http://www.southseek.com)

	 CompactFlash ბარათი (http://www.digital-camera-reviews.com)  SmartMedia ბარათი (http://www.digitalkamera-shop.de)  Memory Stick (http://www.cambridgeworld.com)
შეტყობინების ავთენტიზაციის კოდი (MAC)	ფაილისთვის მინიჭებული მათემატიკური ღირებულება, რომელიც გამოიყენება ფაილის შემდგომ ეტაპზე "შემოწმებისთვის" იმისთვის, რომ დადგინდეს, რომ მასზე არსებული მონაცემები არამართლზომიერად არ შეცვლილა [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
შეტყობინებების დაფა	ელექტრონული დაფა ელექტრონული შეტყობინებებისთვის ქსელური წვდომისთვის აღჭურვილი კომპიუტერული სისტემის მიერ გამოყენებული, რომელიც დისტანცირებული მომხმარებლებისთვის ინფორმაციისა და შეტყობინებების გატარების ცენტრის ფუნქციას ასრულებს, მაგ., ბიულეტების დაფა; დაფა ჩვეულებრივ ემსახურება სხვადასხვა სპეციალური ინტერესის მქონე ჯგუფებს. (ადაპტირებულია [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**]-დან).
კამერიანი მობილური ტელეფონი	მობილური ტელეფონი, რომელიც აღჭურვილია კამერით.  კამერიანი მობილური ტელეფონი (http://www.memorystick.com)

მოდემი	modულატორ/demodულატორი. მოწყობილობა, რომელიც კომპიუტერების მიერ გამოიყენება სატელეფონო ხაზებით დასაკავშირებლად. ის ჩვეულებრივ ამოცნობადია ტელეფონის ხაზთან მიერთებით, თუმცა საკაბელო მოდემებიც არსებობს, რომლებიც DSL ტექნოლოგიაზე (მაგ., საკაბელო მოდემი) არიან დაფუძნებულნი. მისი კომბინირება შესაძლებელია ფაქსის ფუნქციონირებასთან პერსონალური კომპიუტერის ბარათში (ადაპტირებულია [**რორორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**]-დან).  შიდა მოდემი (http://www.baber.com)  გარე მოდემი (http://www.b2net.co.uk)  საკაბელო მოდემი (http://www.myatari.org)
სისტემური პლატა (Motherboard)	ძირითადი სამონტაჟო პლატა კომპიუტერში, რომელიც კომპიუტერის ძირითად სქემებსა და კომპონენტებს მოიცავს (ადაპტირებულია [**რორორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**]-დან).
თაგვი (Mouse)	მისამაგრებელი მოწყობილობა, რომელიც მისი მოძრაობისას კომპიუტერზე მიმართავს მიმართულებასა და სიჩქარეს, ჩვეულებრივ ეს კომპიუტერის ეკრანზე მიმანიშნებლის ამოძრავებით ხდება. მას სხვადასხვა ფორმის მაკავშირებელბი შეიძლება, ჰქონდეს, როგორიცაა მაგ., PS/2, სერიული, USB, უკაბელო/ინფრარედით დაკავშირებული (ადაპტირებულია [**რორორ! ღეფერენცე**

	სოურცე ნოტ ფოუნდ.]-დან).  თაგვი (Mouse) (http://www.hbsoft.de)
MP3	MPEG-1 Audio Layer-3, სტანდარტული ტექნოლოგია და ხმოვანი გადაცემის ძალიან მცირე ფაილად გარდაქმნის ფორმატი (პირველადი ფაილის დაახლოებით 1/12), ხმის პირველადი ხარისხის შენარჩუნებით [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
ქსელი	ინფორმაციისა და რესურსების გაცვლისთვის ერთმანეთთან დაკავშირებული კომპიუტერების ჯგუფი. ეს შეიძლება იყოს მცირე ადგილობრივი ქსელი (ადგილობრივი ქსელი - Local Area Network) ან დიდი საერთაშორისო ქსელი, როგორიცაა ინტერნეტი (ადაპტირებულია [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**]-დან).  ქსელი (http://www.scd.ucar.edu)
ქსელის კაბელი ქსელის დამკავშირებელი	გამოიყენება კომპიუტერული ქსელის კომპონენტების დასაკავშირებლად. მას სხვადასხვა ფერი, სისქე და ფორმა შეიძლება ჰქონდეს და იმ კომპონენტებიდან გამომდინარე, რაზეც ისინი მიერთებულნი არიან, მათ სხვადასხვა დამაკავშირებლები აქვთ [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  RJ45 LAN კაბელი (http://www.bownie.com)

	 T-piece (http://www.legge40.freeserve.co.uk)  RJ11 სატელეფონო კაბელი (http://citt.ccsu.edu)
ქსელის მაკავშირებელი (ინტერფეის) ბარათი	უზრუნველყოფს ქსელის კავშირს (კაბელით ან კაბელის გარეშე). გამფართოებელი პლატას ან პერსონალური კომპიუტერის ბარათის ფორმით შეიძლება იყოს.  ქსელის მაკავშირებელი (ინტერფეის) ბარათი (http://www.computers-networks-routers.com)
ახალი ამბების ჯგუფი (Newsgroup)	კონკრეტული საკითხის შესახებ დისკუსია, რომელიც ცენტრალურ ინტერნეტ საიტზე განთავსებული ჩანაწერებისგან შედგება, რომელთა გადანაწილება Usenet ქსელის მეშვეობით ხდება. ეს უკანასკნელი ახალი ამბების განხილვის მსოფლიო ქსელია [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
არა-ელექტრონული მტკიცებულება	ელექტრონული მტკიცებულების გამოკვლევისთვის საჭირო საგნები, რომლებიც სხვა ფორმით არსებობენ (მაგ., დაწერილი პასვორდები და სხვა ხელნაწერილი შენიშვნები, ქაღალდის ბლოკნოტები, ჰარდვეარითა და სოფთვეარით სარგებლობის სახელმძღვანელოები, კალენდრები, ლიტერატურა, ტექსტი ან კომპიუტერიდან გრაფიკული ამონაბეჭდები და ფოტოგრაფიები) [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
ოპერატიული სისტემა	სოფთვეარის ნაკრები, რომელიც ჩვეულებრივ კომპიუტერის მეხსიერებაში იტვირთება

	კომპიუტერის ჩართვისას და რომელიც ნებისმიერი სხვა კომპიუტერილი პროგრამის ფუნქციონირების წინაპირობაა [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**]. პერატიული სისტემის მაგალითებია: პერსონალური კომპიუტერებისთვის MSDOS, Microsoft Windows, Unix, Linux, ან Mac OS, ან PDAs Palm OS-სთვის, Psion EPOC, ან Windows CE.
ობიექტთა მოთხოვნების ბროკერი (ORB)	დიდი ტევადობის მოხსნადი (მონტაჟირებადი) მყარი დისკის სისტემა. ობიექტთა მოთხოვნების ბროკერი (ORB) დისკები მაგნეტორეზისტულ magnetoresistive (MR) წასაკითხ/დამწერ სათავო ტექნოლოგიას იყენებენ.  ობიექტთა მოთხოვნების ბროკერი ORB (http://www.electronicsparadise.com)
პეიჯერი	ხელის პორტატული ელექტრონული მოწყობილობა, რომელშიც დროებითი მტკიცებულება შეიძლება იყოს მოცული (ტელეფონის ნომრები, ხმოვანი შეტყობინებები, ელექტრონული ფოსტა) [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  პეიჯერი (http://www.poseidon-tech.co.uk)
პარალელური პორტის დამცველი დამხშობი	მცირე მოწყობილობა, პარალელური პორტის დამცველი დამხშობის შემაერთებლით, რომელმაც შეიძლება დაპროგრამებადი მეხსიერება უზრუნველყოს და საკონტროლო ალგორითმებსა ან გადათვლის სქემებს ფლობდეს.  პარალელური პორტის დამცველი დამხშობი (http://www.keylok.com)

პასვორდი	ალფავიტურ-ციფრული და სპეციალური ნიშნების კომბინაცია, გამოყენებული კომპიუტერებსა თუ კომპიუტერულ პროგრამებზე წვდომის შემზღუდავი ღონისძიების სახით. თუ ის რამდენიმე სიტყვისგან შემდგარ ფრაზას მოიცავს, მას ჩვეულებრივ შეღწევის ფრაზად მოიხსენიებენ. თუ ის მხოლოდ ციფრულ ნიშნებს მოიცავს (მაგ., მოწყობილობების წვდომის კონტროლი მხოლოდ მოკლე PIN (საკომუნიტაციო პანელის) მეშვეობით), მას ჩვეულებრივ პერსონალურ მაიდენტიფიცირებელ ნომერს, ანუ PIN-ს უწოდებენ.
პერსონალური კომპიუტერი (PC)	პერსონალური კომპიუტერი, ტერმინი, რომელიც ჩვეულებრივ გამოიყენება IBM და მასთან შეთავსებადი კომპიუტერების ასაღწერად, რომლებიც ჩვეულებრივ შედგებიან ძირითადი კორპუსისგან, მონიტორის, კლავიატურისა და თაგვის (mouse)-სგან. ტერმინი ასევე აღწერს ერთდროულად ერთი ადამიანის მიერ გამოსაყენებელ ნებისმიერ კომპიუტერს [**როორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  პერსონალური კომპიუტერი (PC) (http://www.userfriendlybooks.com)  კომპიუტერი, რომელიც აკვარიუმის მსგავსად გამოიყურება (http://www.casemodding.com)  კომპიუტერი, რომელიც ჩემოდნის მსგავსად გამოიყურება

	(http://www.casemodding.com)
პერსონალური კომპიუტერის ბარათი (PC card)	იხ.: პერსონალური კომპიუტერის მახსოვრობის ბარათის საერთაშორისო ასოციაციის ბარათი (PCMCIA card)
პერსონალური კომპიუტერის ბარათის წამკითხველი (PC card reader)	იხ.: პერსონალური კომპიუტერის მახსოვრობის ბარათის საერთაშორისო ასოციაციის ბარათის მკითხველი (PCMCIA card reader)
პერსონალური კომპიუტერის მახსოვრობის ბარათის საერთაშორისო ასოციაცია (PCMCIA)	პერსონალური კომპიუტერის მახსოვრობის ბარათის საერთაშორისო ასოციაცია. ორგანიზაციაში შედის 500-მდე კომპანია. ორგანიზაციამ შეიმუშავა სტანდარტი მცირე, საკრედიტო ბარათის ზომის მოწყობილობებისთვის, რომლებსაც პერსონალური კომპიუტერების ბარათები ჰქვია. თავდაპირველად ისინი პორტატულ კომპიუტერებზე მეხსიერების დასამატებლად გამოიყენებოდა. პერსონალური კომპიუტერის მახსოვრობის ბარათის საერთაშორისო ასოციაციის (PCMCIA) სტანდარტი რამდენიმეჯერ გაფართოვდა და ამ ეტაპზე მათი მრავალი ტიპის მოწყობილობისთვის გამოყენება შესაძლებელია. იხ.: პერსონალური კომპიუტერის ბარათი (PC card).
პერსონალური კომპიუტერის მახსოვრობის ბარათის საერთაშორისო ასოციაციის ბარათი (PCMCIA card)	პერსონალური კომპიუტერის მახსოვრობის ბარათის საერთაშორისო ასოციაციის (PCMCIA) სტანდარტებზე დაფუძნებული ბარათი, რომლის პორტატულ და ხელის კომპიუტერებში შეტანა ხდება. ეს ბარათი ბევრ იმ ფუნქციას უზრუნველყოფს, რომლებიც ტიპიურად არ არის მანქანებში არსებული (მაგ., მეხსიერება ან შემავალი/გამავალი პორტები, როგორებიცაა მაგ., მოდემები, ადაპტორები, მყარი დისკები). პერსონალური კომპიუტერების ბარათების სამი ტიპი არსებობს: სამივე მათანს მსგავსი სწორკუთხა ფორმა (85.6 X 54 მილიმეტრი) და ერთმანეთისგან განსხვავებული სიფართე აქვთ (ადაპტირებულია [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**]-დან). იხ.: ასევე მახსოვრობის ბარათი.  პერსონალური კომპიუტერის მახსოვრობის ბარათის საერთაშორისო

	ასოციაციის ბარათები (PCMCIA cards (http://www.synchrotech.com)
პერსონალური კომპიუტერის მახსოვრობის ბარათის საერთაშორისო ასოციაციის ბარათის მკითხველი (PCMCIA card reader)	პერსონალური კომპიუტერის ბარათების მოწყობილობის წამკითხველი, სხვადასხვა ინტერფეისის მქონე შეიძლება იყოს(USB, პარალელური პორტი, ა.შ.).  პერსონალური კომპიუტერის მახსოვრობის ბარათის საერთაშორისო ასოციაციის ბარათის მკითხველი USB-ით (http://www.synchrotech.com)
პერსონალური ციფრული ასისტენტები (PDA)	მცირე (ე.ი., ჯიბის ზომის) მოწყობილობა, რომელიც შეიძლება მოიცავდეს გამომთვლელ, ტელეფონის/ფაქსის, პეიჯერის, ქსელისა და სხვა მახასიათებლებს [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  პერსონალური ციფრული ასისტენტები (PDAs) (http://www.jst-mfg.com)
ძალიან კარგი კონფიდენციალურობა (PGP)	ძალიან კარგი კონფიდენციალურობა. თავისუფალი პროგრამული საშუალებების კრიპტოგრაფიული სოფთვეარი (იხ, მაგ., www.pgpI.org), რომელიც ფილიპ რ. ციმერმანის მიერ 1991 წელს შეიქმნა. ის შესაძლოა, გამოყენებული იყოს ელექტრონული ფოსტის შეტყობინობების დასაშიფვრად ან ხელმოსაწერად ან კომპიუტერული ფაილების დასაშიფვრად. არსებობს მისი დაბალფასიანი კომერციული ასლიც.
ფოტოასლების გადამღები	ტექსტისა და გამოსახულების ფოტოასლის გადამღები მოწყობილობა. ზოგიერთი გადამღები მანქანა მომხმარებლის მიერ მანქანის გამოყენებისა და ასლების გადაღების ისტორიას იმახსოვრებს. ერთხელ სკანირების შედეგად მრავალი ასლის გადაღების შესაძლებლობის მქონე მანქანები ჯერ დოკუმენტების მეხსიერებაში სკანირებას ახდენენ და შეუძლიათ მოგვიანებით ბეჭდვა

	[**რორორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  ფოტოასლის გადამღები (http://www.avonlibrary.com)
სათამაშო მანქანა	კომპიუტერი ელექტრონული თამაშების სათამაშოდ (მახსოვრობის ბარათით).  სათამაშო მანქანა (http://joystick-verkauf.de)
საფოსტო ოფისის პროტოკოლი (POP) POP3	საფოსტო ოფისის პროტოკოლი. სტანდარტიზებულ პროტოკოლზე დაფუძნებული ინტერნეტ მომსახურება ელექტრონული ფოსტის შეტყობინებებ (მაგ., POP სერვერი).
პორტი	ამ ტერმინს ორი მნიშვნელობა შეიძლება ჰქონდეს: მოწყობილობის შემაერთებელი (მაგ., პარალელური პორტი, USB პორტი), ან TCP-დონის მისამართი, რომელიც, IP დონის მისამართთან ერთად საგამონაკლისოდ აღწერს ქსელის მომსახურებას (სერვერის მიერ მოწოდებულს)
პორტის რეპლიკატორი	მოწყობილობა, რომელიც მოიცავს პერსონალური კომპიუტერის ზოგად პორტებს, როგორებიცაა სერიული, პარალელური და ქსელის პორტები, რომლებიც პორტატულ კომპიუტერს უერთდება. პორტის რეპლიკატორი საბაზო ბლოკის მსგავსია, თუმცა საბაზო ბლოკები ჩვეულებრივ დამატებითი გამაფართოვებელი პლატის შეერთების შესაძლებელობას იძლევიან [**რორორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].

	 პორტის რეპლიკატორი (http://www.keysan.com)
პორტატული კომპიუტერი	პერსონალური კომპიუტერი პორტატულ ფორმაში, მაგ., ნოუთბუქი ან ლაპტოპი.  ნოუთბუქი (http://www.microstarinc.com)
პრინტერი	მოწყობილობა, რომელიც კომპიუტერიდან ტექსტურ და გრაფიკულ გამოსახულებას იღებს და ინფორმაცია ქაღალდზე გადააქვს, ჩვეულებრივ ქაღალდის სტანდარტიზებულ ფურცელზე [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  პრინტერი (http://www.888camcorder.com)
ინფორმაციაზე წვდომის საშუალება (Public key certificate)	ხელმოწერილი ციფრული დოკუმენტი (ციფრული პირადობის მაიდენტიფიცირებლის მსგავსი), რომელიც სარწმუნო მხარისგან მოდის (ე.ი. მასერთიფიცირებელი ორგანოსა ან მასერტიფიცირებელი მომსახურების მომწოდებლისგან) და ადასტურებს, რომ ინფორმაციაზე წვდომის საშუალება კონკრეტულ ადამიანსა ან ორგანიზაციას ეკუთვნის. მისი გამოყენება ხდება ელექტრონული (ან ციფრული) ხელმოწერების შესამოწმებლად. ელექტრონული ხელმოწერები შესაბამისი პერსონალური კოდით იქმნება, რაც მისი მფლობელის მიერ საიდუმლოდ უნდა იყოს შენახული (მაგ., დაუდევარი მოპყრობისგან დაცულ ბარათში, სადაც ის PIN -ით დაცულია).
სიმაღლეზე შეკეთებული	აღწერს ელექტრონული მოწყობილობის ერთეულს, რომელიც მეტალის ჩარჩოშია

(Rack-mounted)	მოთავსებული, რომელსაც აღჭურვილობის საცავი ჰქვია [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  Rack-mounted system (http://www.micromech.com)
შერჩევით წვდომის მეხსიერება (RAM)	შერჩევით წვდომის მესიერება. ადგილი კომპიუტერში, სადაც ოპერატიული სისტემა, გამოსაყენებელი პროგრამები და გამოყენებული მონაცემებია ისე შენახული, რომ კომპიუტერის პროცესორმა მათი მოძებნა სწრაფად შეძლოს. RAM-იდან კომპიუტერზე, მყარ დისკზე, ფლოპი დისკსა და CD-ROM-ზე გაცილებით სწრაფად იკითხება და მასზე გაცილებით სწრაფად ხდება ინფორმაციის ჩაწერა. თუმცა, მონაცემები RAM-ზე რჩება მხოლოდ იმდენ ხანს, რამდენ ხანსაც კომპიუტერი ჩართულია. კომპიუტერის გამორთვისას RAM კარგავს მის ინფორმაციას [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
ტრასირების ალგორითმი (Router)	მოწყობილობა, ან ზოგ შემთხვევაში კომპიუტერული პროგრამა, რომელიც განსაზღვრავს მონაცემთა კრებულის გადაცემის შემდეგ წერტილს მისი დანიშნულების ადგილისკენ. ტრასირების ალგორითმი მინიმუმ ორ ქსელთან არის დაკავშირებული და წყვეტს იმას, თუ რომელი მიმართ ლებით გაგზავნოს მონაცემები მის მიერ იმ ქსელების აღქმის ფარგლებში, რომლებზეც ის მიერთებულია [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
სკანერი	ოპტიკური მოწყობილობა, რომელიც კომპიუტერზეა მიერთებული და რომელიც დოკუმენტს დამასკანერებელ მოწყობილობამდე უშვებს (ან პირიქით) და გზავნის მას კომპიუტერში, როგორც ფაილს [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  სკანერი (http://www.pixelpower.com)
ეკრანის დამცველი (Screen	მომსახურე პროგრამა, რომელიც მონიტორს

saver)	იცავს. მან წვდომის კონტროლის ფუნქციაც შეიძლება შეასრულოს [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
უსაფრთხოების დამცველი დამახშობელი	მცირე მოწყობილობა (მაგ., პარალელური პორტის დამცველი დამახშობელი ან USB დამცველი დამახშბელი), რომელიც კომპიუტერებზე, პროგრამებზე ან ფუნქციებზე წვდომას უზრუნველყოფს.
ამოღების დისკი	სპეციალურად მომზადებული ფლოპი დისკი, რომელიც მონაცემთა შემთხვევით შეცვლისგან კომპიუტერული სისტემის დასაცავად არის შექმნილი [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
სერიული პორტის დამცველი დამხშობი (Serial port dongle)	მცირე მოწყობილობა, რომელსაც სერიული პორტის დამკავშირებელი აქვს, რომელმაც დაპროგრამებადი მეხსიერება, მოშორებით განახლება, ალგორითმების ან რეგისტრების ფლობის კონტროლი შეიძლება უზრუნველყოს.
ხელმომწერის პირადობის მოდულის ბარათი (SIM card)	ხელმომწერის პირადობის მოდულის ბარათი. ინტელექტუალური ბარათის სპეციალური ტიპი, რომლის გამოყენება მობილურ ტელეფონებშია შესაძლებელი.  SIM ბარათები (http://www.ishop.co.uk)
დაცდის რეჟიმი (Sleep mode)	ენერგიის კონსერვაციის სტატუსი, რომელიც აჩერებს მყარი დისკისა და მონიტორის გარდაქმნას გამოსახულების გარეშე ეკრანად, ენერგიის დასაზოგად. ზოგჯერ მას შეჩერებულ რეჟიმსაც უწოდებენ [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
ინტელექტუალური ბარათი (Smart card)	მცირე მოწყობილობა, რომელიც საკრედიტო ბარათის მსგავსია (სტანდარტული ზომა). ის მოიცავს მიკროპროცესორს (ე.ი. ჩიპს), რომელსაც შეუძლია გამოთვლა და/ან ფულადი ღირებულების, დაშიფვრის კოდის ან ავთენტიფიკაციის ინფორმაციის (პასვორდის), ციფრული სერთიფიკატის ან სხვა ინფორმაციის შენახვა (ადაპტირებულია [**Error! Reference source not found.**]-დან). ინტელექტუალური ბარათები, როგორც წესი, დაცულია პერსონალური კოდით (ე.ი. პერსონალური იდენტიფიკაციის ნომერი, PIN),

	ანუ ბარათის მონაცემებსა და ფუნქციებზე წვდომა შესაძლებელი გახდება მხოლოდ ამ კოდის გამოყენებით.  ინტელექტუალური ბარათი (http://www.austriacard.at)
ინტელექტუალური ბარათის წამკითხველი (Smart card reader)	მოწყობილობა, რომელიც კითხულობს ინტელექტუალურ ბარათს და ბარათსა და კომპიუტერს შორის კავშირს ამყარებს.  ინტელექტუალური ბარათის წამკითხველი (http://www.smartcards.net)  ინტელექტუალური ბარათის წამკითხველი PIN-ის მოწყობილობით (http://www.quio.net)
უსაფრთხო/მრავალფუნქციური ინტერნეტ ფოსტის გაფართოება (S/MIME)	უსაფრთხო/მრავალფუნქციური ინტერნეტ ფოსტის გაფართოება. ელექტრონული ფოსტის გაგზავნის უსაფრთხო მეთოდი. უსაფრთხო/მრავალფუნქციური ინტერნეტ ფოსტის გაფართოება (S/MIME) ჩართულია Microsoft-ისა და Netscape-ის Web საძიებო სისტემის ახალ ვერსიაში და ისინი ასევე მოწონებულია სხვა მომწოდებლების მიერ, რომლებიც შეტყობინების გაგზავნის პროდუქტებს ქმნიან [**რორო! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
მოკლე შეტყობინებს სერვისი/მულტიმედია შეტყობინების მომსახურება (SMS/MMS)	მოკლე შეტყობინებს სერვისი/მულტიმედია შეტყობინების მომსახურება. მობილური ტელეფონების შეტყობინების ფორმატები.
მარტივი ფოსტის გადამგზავნი პროტოკოლი (SMTP)	მარტივი ფოსტის გადამგზავნი პროტოკოლი. საფოსტო სერვერის მეშვეობით ელექტრონული ფოსტის შეტყობინებების გაგზავნის ინტერნეტის მომსახურება, სტანდარტიზებულ პროტოკლზე დაფუძნებული (მაგ., SMTP სერვერი).

მყარი დისკი (Solid state disk)	შენახვის აქსელერატორი, რომელიც უერთდება სერვერს სტანდარტული მაგნეტური მბრუნავი დისკის მსგავსად. თუმცა, მყარი დისკი მონაცემებს ინახავს DRAM-ში (დიმანიური შემთხვევითი წვდომის მეხსიერება), იმავე ტიპის ნახევრად მიმყოლი მოწყობილობები, რომელთა გამოყენება ხდება CPU-ის ძირითადი მექსიერების შესაქმნელად. ის არ არის მბრუნავ მყარ დისკზე, მაგნიტური საფარით. ეს მახსოვრობა დაახლოებით 200-ჯერ უფრო სწრაფია ვიდრე დისკის დრაივისა [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
შენახვის ბარათი	იხ. მეხსიერების ბარათი.
სუპერინტელექტუალური ბარათი	მცირე ეკრანიან და ციფრული მოწყობილობის მქონე ინტელექტუალური ბარათი.
გადამრთველი (Switch)	მოწყობილობა, რომელიც შემომავალ მონაცემებს მიმართავს მრავალი პორტიდან სპეციფიური გასავალი პორტისკენ, რომელიც მონაცემებს მათი დანიშნულების ადგილისკენ გაგზავნის. Ethernet LAN-ზე გადამრთველი არკვევს - ფიზიკური მოწყობილობის გამოყენებით (მედიაზე წვდომის კონტროლი, MAC) შემოსული შეტყობინების ჩარჩოთი, რომელი გამგზავნი პროტისკენ და პორტიდან გაგზავნოს ის [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  გადამრთველი (Switch) (http://www.wti.com)
სისტემის ადმინისტრატორი	პიროვნება, რომელსაც კომპიუტერული სისტემის ზედამხედველობის ლეგიტიმური უფლება აქვს. ადმინისტრატორი სისტემაზე წვდომის უმაღლეს ხარისხს ინარჩუნებს. ის ასევე ცნობილია, როგორც sysop, sysadmin, და სისტემის ოპერატორი [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
ლენტის დისკი (Tape drive)	მოწყობილობა, რომელში ლენტა მოთავსდება კითხვისთვის/წერისთვის

	 ლენტის დისკი (http://www.linux-mag.com)
Telnet	სტანდარტული ინტერნეტის პროტოკოლი, რომლის მეშვეობით სხვა ადამიანის კომპიუტერზე წვდომის ორგანიზება ხდება, თითქოს მათ მიერ ამის ნებართვა გაცემულია [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
უწყვეტი ენერგიის მიწოდება (UPS)	უწყვეტი ენერგიის მიწოდება. მოწყობილობა, რომელიც ელექტრონულ მოწყობილობას შესაძლებლობას აძლევს, ჩართული იყოს მცირე დროის განმავლობაში მაინც მას შემდეგ, რაც ენერგიის პირველადი წყაროს დაკარგვა მოხდება. ის ენერგიის წყვეტისგან დაცვასაც უზრუნველყოფს [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  UPS (http://mitglied.lycos.de)
რესურსების ერთიანი ლოკატორი (URL)	რესურსების ერთიანი ლოკატორი, ფაილისი მისამართი (ე.ი. რესურსი), რომელიც ინტერნეტზე ხელმისაწვდომია (მაგ., “http://www.interpol.int”). ფაილისი ან რესურსის ტიპი დამოკიდებულია ინტერნეტის გამოყენების პროტოკოლზე (მაგ., ინტერნეტის - World Wide Web's - პროტოკოლი ჩვეულებრივ არის Hypertext Transfer Protocol, HTTP) [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
უნივერსალური თანამიმდევრული ბორბალი (USB)	უნივერსალური თანამიმდევრული ბორბალი. ჰარდვეარის ინტერფეისი/დაბალსიჩქარიანი პერიფერიული მოწყობილობების, როგორიცაა კლავიატურა, მაუსი, ჯოისტიკი, სკანერი, პრინტერი, სატელეფონო მოწყობილობების პორტი (ადაპტირებულია [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**]-დან). იხ. ასევე: USB დამცველი დამახშობელი.
USB დამცველი დამახშობელი	USB პორტიანი მცირე მოწყობილობა, შემართებლით, რომელმაც შეიძლება უზრუნველყოს მეხსიერება, დაპროგრამებადი მეხსიერება, ინფორმაციის განახლება დისტანციურად, მაკონტროლებელი

	ალგორითმებისა ან გამომთვლელების ფლობა.  USB დამცველი დამახშობელი (http://www.keylok.com)  USB მეხსიერება (http://www.dell.com)  USB კალამი (http://www.dell.com)
ვირუსი	დამპროგრამებელი კოდი, ჩვეულებრივ სხვა ფაილის ფორმაში დამალული, რაც მოულოდნელ და ჩვეულებრივ არასასურველ შედეგს იწვევს. ვირუსი ხშირად შექმნილია ისე, რომ ის ავტომატურად ვრცელდება სხვა კომპიუტერების მომხმარებლებზე. ვირუსების გადაცემა შეიძლება მოხდეს ელექტრონული ფოსტის შეტყობინებაზე თანდართული ფაილების სახით, როგორც ჩამოტვირთული ფაილებისა ან ისინი დისკეტაზე ან კომპაქტურ დისკზე შეიძლება, იყოს [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
ვებ გვერდის მისამართი	URL ან IP მისამართი.
უკაბელო წვდომის წერტილი	ჰაბი უკაბელო LAN-ში.  უკაბელო წვდომის წერტილი (http://www.routerreviews.net)
უკაბელო ადგილობრივი ქსელი (Wireless LAN)	უკაბელო ადგილობრივი ქსელი. ქსელური ტექნოლოგიების ზოგადი სახელი, რომელიც სტანდარტიზებულია IEEE (ელექტრო და ელექტრონული ინჟინერიის ინსტიტუტი)-ის

	მიერ.  უკაბელო PCMCIA (http://www.ntslabs.com)  უკაბელო ჰაბი (http://www.3com.at)
მსოფლიო ქსელი (World Wide Web (WWW))	ქსელში ხელმისაწვდომი ინფორმაციის მსოფლიო, ე.ი. ინტერნეტში არსებული ყველა რესურსი და მომხმარებელი, რომლებიც იყენებენ Hypertext Transfer Protocol (HTTP)-ს [**რორორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].
Xbox	სათამაშო მოწყობილობა  Xbox (http://www.game-cheats.com)
ZIP®	მოშორებადი მყარი დისკის სისტემა. ZIP-ის მოწყობილობა მცირე ზომის, პორტატული დისკის დისკავოდია, რომელიც უპირველესად პერსონალური კომპიუტერის ფაილების მონაცემთა კოპირებისა და დაარქივებისთვის გამოიყენება. ბრენდირებული ZIP დრაივი შექმნილი იყო და იყიდება Iomega Corporationის მიერ. Zip დრაივები და დისკები ორი ზომისაა [**რორორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**].  ZIP დრაივი და დისკები (http://www.hunter.cuny.edu)

1 დანართი ა: ბლოკ-სქემები/ჯიბის ზომის სახელმძღვანელოები

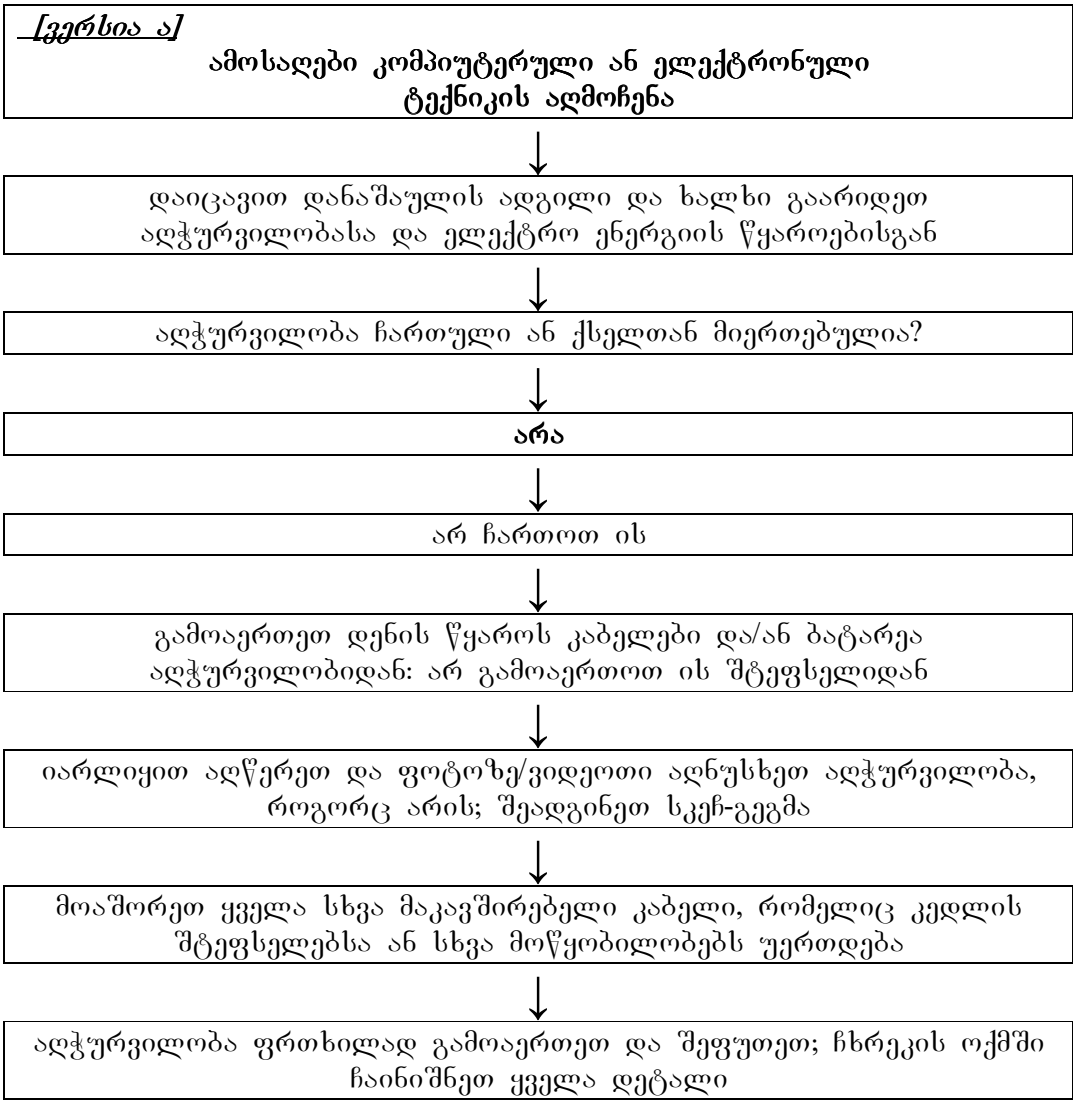
მომდევნო ორი ბლოკ-სქემა ელექტრონული მტკიცებულების ამოღების კარგი პრაქტიკის ამსახველია (ადაპტირებულია [**რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**]-დან).

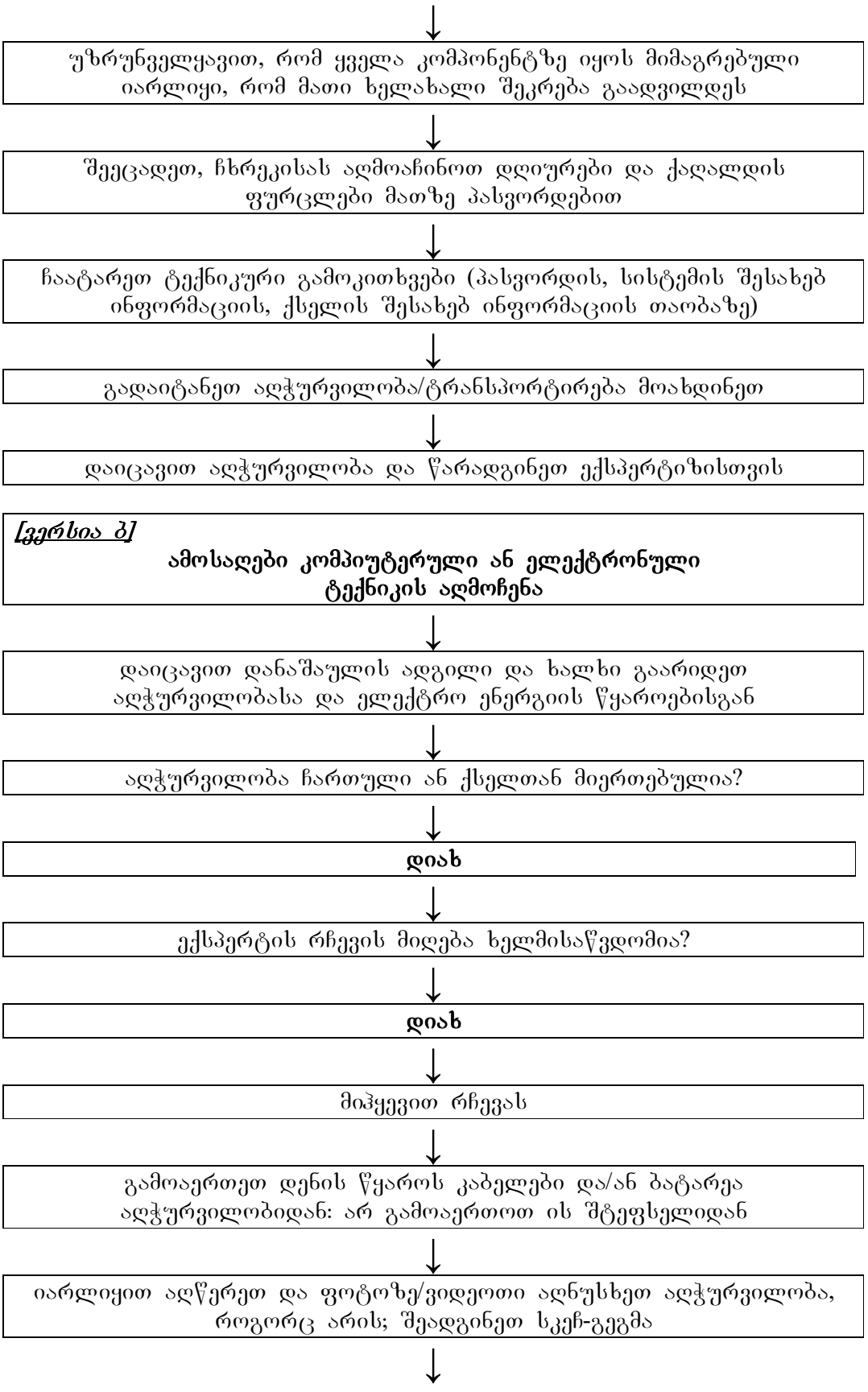
ა1 ბლოკ-სქემა/ჯიბის ზომის სახელმძღვანელო: ელექტრონული აღჭურვილობა

8. დანართი ა: ბლოკსქემა/ჯიბის სახელმძღვანელო

მომდევნო ორი ბლოკ-სქემა ელექტრონული მტკიცებულების ამოღების კარგი პრაქტიკის ამსახველია (ადაპტირებულია []-დან).

ა1 ბლოკ-სქემა/ჯიბის ზომის სახელმძღვანელო: ელექტრონული აღჭურვილობა




უზრუნველყავით, რომ ყველა კომპონენტზე იყოს მიმაგრებული იარლიყი, რომ მათი ხელახალი შეკრება გაადვილდეს
შეეცადეთ, ჩხრეკისას აღმოაჩინოთ დღიურები და ქაღალდის ფურცლები მათზე პასვორდებით
ჩაატარეთ ტექნიკური გამოკითხვები (პასვორდის, სისტემის შესახებ ინფორმაციის, ქსელის შესახებ ინფორმაციის თაობაზე)
გადაიტანეთ აღჭურვილობა/ტრანსპორტირება მოახდინეთ
დაიცავით აღჭურვილობა და წარადგინეთ ექსპერტიზისთვის
[ვერსია 2]
ამოსაღები კომპიუტერული ან ელექტრონული ტექნიკის აღმოჩენა
დაიცავით დანაშაულის ადგილი და ხალხი გაარიდეთ აღჭურვილობასა და ელექტრო ენერგიის წყაროებისგან
აღჭურვილობა ჩართული ან ქსელთან მიერთებულია?
დიახ
ექსპერტის რჩევის მიღება ხელმისაწვდომია?
დიახ
მიჰყევით რჩევას
გამოაერთეთ დენის წყაროს კაბელები და/ან ბატარეა აღჭურვილობიდან: არ გამოაერთოთ ის შტეფსელიდან
იარლიყით აღწერეთ და ფოტოზე/ვიდეოთი აღნუსხეთ აღჭურვილობა, როგორც არის; შეადგინეთ სკეჩ-გეგმა

მოაშორეთ ყველა სხვა მაკავშირებელი კაბელი, რომელიც კედლის შტეფსელებსა ან სხვა მოწყობილობებს უერთდება

↓

აღჭურვილობა ფრთხილად გამოაერთეთ და შეფუთეთ; ჩხრეკის ოქმში ჩაინიშნეთ ყველა დეტალი

↓

უზრუნველყავით, რომ ყველა კომპონენტზე იყოს მიმაგრებული იარლიყი, რომ მათი ხელახალი შეკრება გაადვილდეს

↓

შეეცადეთ, ჩხრეკისას აღმოაჩინოთ დღიურები და ქაღალდის ფურცლები მათზე პასვორდებით

↓

ჩაატარეთ ტექნიკური გამოკითხვები (პასვორდის, სისტემის შესახებ ინფორმაციის, ქსელის შესახებ ინფორმაციის თაობაზე)

↓

გადაიტანეთ აღჭურვილობა/ტრანსპორტირება მოახდინეთ

↓

დაიცავით აღჭურვილობა და წარადგინეთ ექსპერტიზისთვის

[ვერსია გ]

ამოსაღები კომპიუტერული ან ელექტრონული ტექნიკის აღმოჩენა

დაიცავით დანაშაულის ადგილი და ხალხი გაარიდეთ აღჭურვილობასა და ელექტრო ენერგიის წყაროებისგან

↓

აღჭურვილობა ჩართული ან ქსელთან მიერთებულია?

↓

არა

↓

გამოაერთეთ დენის წყაროს კაბელები და/ან ბატარეა აღჭურვილობიდან: არ გამოაერთოთ ის შტეფსელიდან

↓

იარლიყით აღწერეთ და ფოტოზე/ვიდეოთი აღნუსხეთ აღჭურვილობა, როგორც არის; შეადგინეთ სკეჩ-გეგმა

↓

მოაშორეთ ყველა სხვა მაკავშირებელი კაბელი, რომელიც კედლის შტეფსელებსა ან სხვა მოწყობილობებს უერთდება

↓

აღჭურვილობა ფრთხილად გამოაერთეთ და შეფუთეთ; ჩხრეკის ოქმში ჩაინიშნეთ ყველა დეტალი

↓

უზრუნველყავით, რომ ყველა კომპონენტზე იყოს მიმაგრებული იარლიყი, რომ მათი ხელახალი შეკრება გაადვილდეს

↓

შეეცადეთ, ჩხრეკისას აღმოაჩინოთ დღიურები და ქაღალდის ფურცლები მათზე პასვორდებით

↓

ჩაატარეთ ტექნიკური გამოკითხვები (პასვორდის, სისტემის შესახებ ინფორმაციის, ქსელის შესახებ ინფორმაციის თაობაზე)

↓

გადაიტანეთ აღჭურვილობა/ტრანსპორტირება მოახდინეთ

↓

დაიცავით აღჭურვილობა და წარადგინეთ ექსპერტიზისთვის

[ვერსია დ]

ამოსაღები კომპიუტერული ან ელექტრონული ტექნიკის აღმოჩენა

↓

დაიცავით დანაშაულის ადგილი და ხალხი გაარიდეთ აღჭურვილობასა და ელექტრო ენერგიის წყაროებისგან

↓

აღჭურვილობა ჩართული ან ქსელთან მიერთებულია?

↓

დიახ

↓

ექსპერტის რჩევის მიღება ხელმისაწვდომია?

↓

არა

↓

არ შეეხოთ კლავიატურას

↓

არ მიჰყვეთ ეჭვმიტანილის რჩევას შეუმოწმებლად

↓

გადაიღეთ ფოტო და მოინიშნეთ, რას ხედავთ

↓

გამოაერთეთ დენის წყაროს კაბელები და/ან ბატარეა აღჭურვილობიდან: არ გამოაერთოთ ის შტეფსელიდან

↓

იარლიყით აღწერეთ და ფოტოზე/ვიდეოთი აღნუსხეთ აღჭურვილობა, როგორც არის; შეადგინეთ სკეჩ-გეგმა

↓

მოაშორეთ ყველა სხვა მაკავშირებელი კაბელი, რომელიც კედლის შტეფსელებსა ან სხვა მოწყობილობებს უერთდება

↓

აღჭურვილობა ფრთხილად გამოაერთეთ და შეფუთეთ; ჩხრეკის ოქმში ჩაინიშნეთ ყველა დეტალი

↓

უზრუნველყავით, რომ ყველა კომპონენტზე იყოს მიმაგრებული იარლიყი, რომ მათი ხელახალი შეკრება გაადვილდეს

↓

შეეცადეთ, ჩხრეკისას აღმოაჩინოთ დღიურები და ქაღალდის ფურცლები მათზე პასვორდებით

↓

ჩაატარეთ ტექნიკური გამოკითხვები (პასვორდის, სისტემის შესახებ ინფორმაციის, ქსელის შესახებ ინფორმაციის თაობაზე)

↓

გადაიტანეთ აღჭურვილობა/ტრანსპორტირება მოახდინეთ

↓

დაიცავით აღჭურვილობა და წარადგინეთ ექსპერტიზისთვის

გახსოვდეთ:
ა) რა უნდა ამოიღოთ:

კომპიუტერული სისტემა:

- **ძირითადი კორპუსი; ჩვეულებრივ, ეს არის ყუთი, რომელსაც უერთდება კლავიატურა და მონიტორი;**
- **მონიტორი;**
- **კლავიატურა და თაგვი (მაუსი);**
- **ყველა შემაერთებელი (ენერგიის მიმწოდებელი კაბელების ჩათვლით);**
- **ენერგიის მიმწოდებელი დანადგარები;**
- **ჰარდ დისკები, რომლებიც არ არის კომიუტერში**

დამატებითი კომპონენტები:

- დამცავი დამახშობლები (მცირე ზომის შემაერთებლები, რომლებიც კომპიუტერის უკანა მხარეს არის შეერთებული);
- მოდემები;
- პრინტერები, სკანერები (ქაღალდისა და კარტრიჯის ჩათვლით);
- ქსელის კომპონენტები

გამოცალკევებადი მონაცემთა შემნახველი საშუალებები:

- ფლოპი დისკები, კომპაქტ-დისკები, DAT ლენტები;
- JAZ და ZIP კარტრიჯები;
- PCMCIA ბარათები;
- მყარი დისკები, რომლებიც კომპიუტერთან შეერთებული არ არის

არაელექტრონული მტკიცებულებები:

- სახელმძღვანელოები და კომპიუტერული პროგრამები;
- პასვორდების შემცველი ქაღალდები;
- დაფები;
- გასაღები

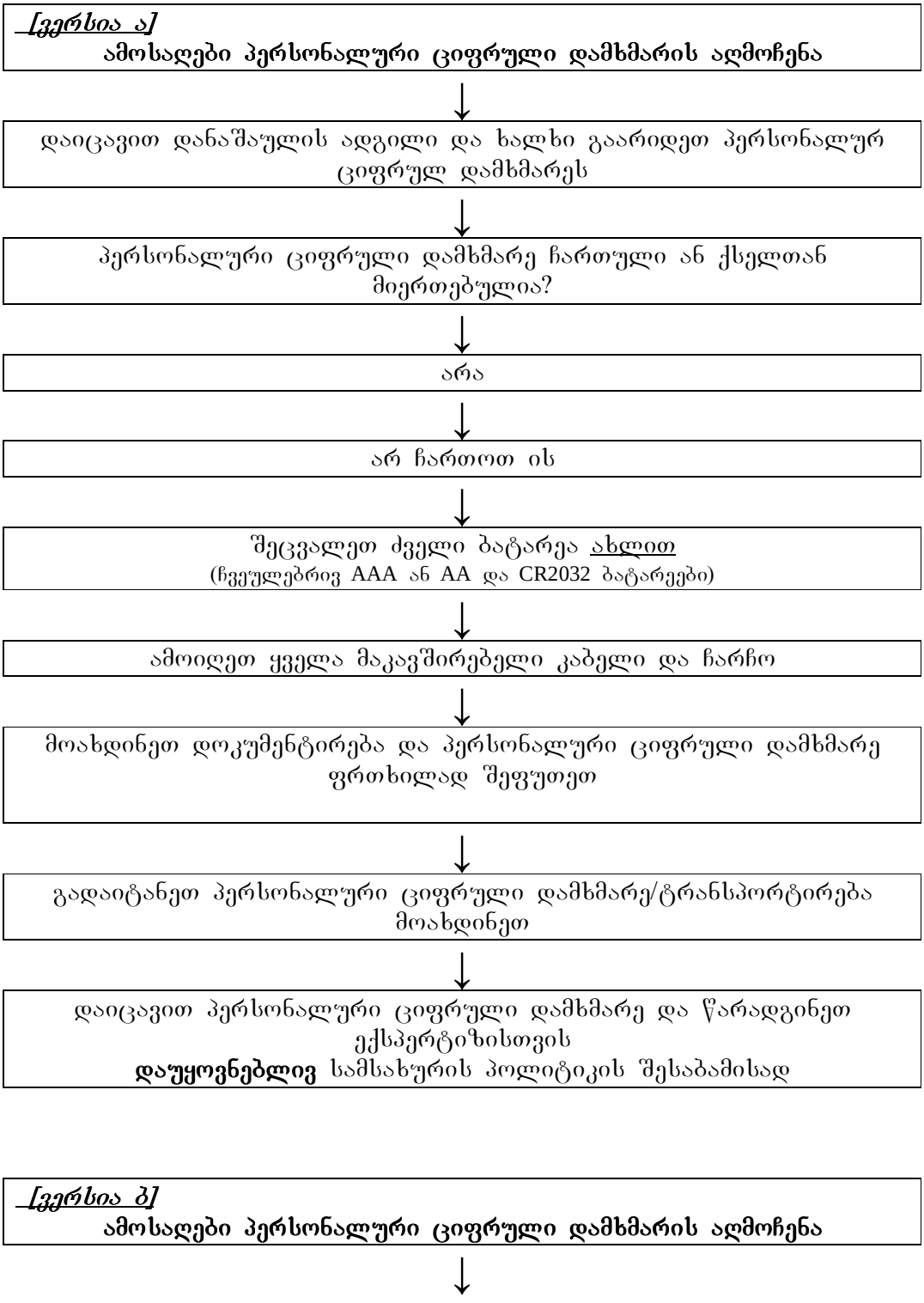
სხვა ელექტრონული მტკიცებულებები:

- პერსონალური ციფრული თანაშემწეები, ტელეფონები, ა.შ.

გახსოვდეთ:
ბ) ტრანსპორტირება:

- ყველაფერი ფრთხილად გადაიტანეთ
- ყველა მოწყობილობა მოაშორეთ მაგნიტური წყაროებისგან, როგორებიცაა უყურმილოდ მოლაპარაკე ტელეფონები, გამთბარი სავარძლები ან ფანჯრები, ან პოლიციის რადიო
- მყარი დისკები და საინფორმაციო დაფები ანტი-სტატიკურ ჩანთებში მოათავსეთ
- არ გადაკეცოთ ფლოპი დისკები ან არ მოათავსოთ მათზე სტიკერები პირდაპირ
- მონიტორები ეკრანით ქვემოთ გადაადგილეთ მანქანის უკანა სავარძელზე (ღვედით დამაგრებული)
- პერსონალური ორგანაიზერები და პალმტოპ კომპიუტერები ქაღალდი კონვერტებში მოათავსეთ
- კლავიატურები, კაბელები, თაგვი (მაუსი) და მოდემები ჰაერგამტარ ჩანთებში ჩადეთ. არ მოათავსოთ მძიმე საგნებს ქვეშ.

ა2 ბლოკსქემა/ჯიბის სახელმძღვანელო: ხელის მოწყობილობები (პერსონალური ციფრული დამხმარენი)



დაიცავით დანაშაულის ადგილი და ხალხი გაარიდეთ პერსონალურ ციფრულ დამხმარეს

↓

პერსონალური ციფრული დამხმარე ჩართული ან ქსელთან მიერთებულია?

↓

დიახ

↓

ექსპერტის რჩევის მიღება ხელმისაწვდომია?

↓

დიახ

↓

მიჰყევით რჩევას

↓

ამოიღეთ ყველა მაკავშირებელი კაბელი და ჩარჩო

↓

მოახდინეთ დოკუმენტირება და პერსონალური ციფრული დამხმარე ფრთხილად შეფუთეთ

↓

გადაიტანეთ პერსონალური ციფრული დამხმარე/ტრანსპორტირება მოახდინეთ

↓

დაიცავით პერსონალური ციფრული დამხმარე და წარადგინეთ ექსპერტიზისთვის
დაუყოვნებლივ სამსახურის პოლიტიკის შესაბამისად

[ვერსია გ]

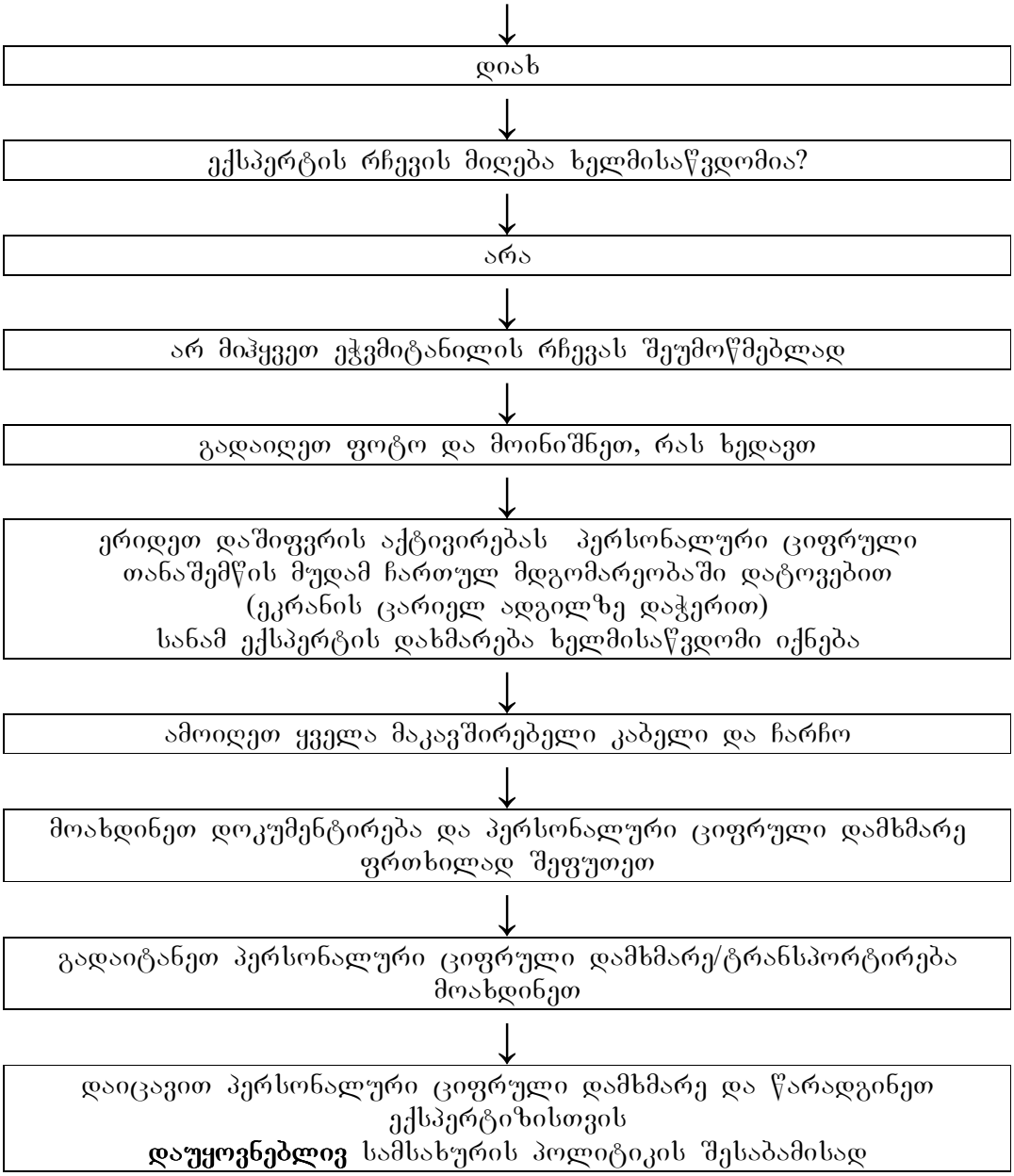
ამოსაღები პერსონალური ციფრული დამხმარის აღმოჩენა

↓

დაიცავით დანაშაულის ადგილი და ხალხი გაარიდეთ პერსონალურ ციფრულ დამხმარეს

↓

პერსონალური ციფრული დამხმარე ჩართული ან ქსელთან მიერთებულია?



როგორ ვიმუშავოთ PALM OS-თან

PALM OS პერსონალურ ციფრულ დამხმარეებში ერთ-ერთი ხშირად გამოყენებადი ოპერატიული სისტემაა.

PALM OS-ს ოპერირების სამი მოდული აქვს:

- დასვენების რეჟიმი - ენერგია მიდის ROM-ისა და RAM-ისკენ
- ძილის რეჟიმი - ენერგიის წყარო მიედინება ROM-ისა და RAM-ისკენ დაშიფვრა შესაძლოა, მოხდეს ძილის რეჟიმში
- მუშა რეჟიმი - პროცესორი აქტიურად მუშაობს

რა უნდა ამოიღოთ

ამოიღეთ ყველა სხვა მოწყობილობა, რომელიც პერსონალურ ციფრულ დამხმარესთან დაკავშირებულია:

- ბარათები და ბლოკები
- ქეისები - შესაძლოა, გარემოს შესახებ ინფორმაციას შეიცავდეს, ა.შ.

2 დანართი ბ: სანიმუშო ფორმები და საკონტროლო სიები (ბ1-ბ3)

ბ1 სანიმუშო ფორმა (ადაპტირებულია [რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**]-დან): ჩვენება**

(ბეჭედი)

სარეგსტრაციო № ..... (ადგილი), (თარიღი)

ჩვენება

მიღებულია (ვისგან): .....

პროფესია: .....

დაბადების თარიღი/ადგილი.....

მოქალაქეობა/ეროვნება: .....

მშობლების სახელები: .....

მისამართი: .....

ტელეფონი: .....

პირადობის მოწმობა: .....

რომელსაც ეცნობა საქმის შესახებ როგორც:

☐ მოწმეს

☐ ეჭვმიტანილს

აცხადებს, რომ იყოს დაკითხული:

დასაწყისი: ..... (დრო)

შემდეგი აპარატურაა ადგილზე:

☐ ცალკე მდგომი კომპიუტერი ნომერი: .....

☐ პორტატული კომპიუტერ(ებ)ი ნომერი: ..... (მაგ., ნოუთბუქები, ლაპტოპები)

☐ ქსელში ჩართული კომპიუტერი ნომერი:..... სამუშაო მანქანა ..... სერვერ(ებ)ი

☐ სხვა .....

.....

მდებარეობა: .....

კითხვა: ვის შეუძლია კომპიუტერის გამოყენება?
☐ მე შემიძლია

☐ .....

☐ .....

კითხვა: ვინ არის სისტემის ადმინისტრირებაზე პასუხისმგებელი?

.....

.....

კითხვა: კომპიუტერი დაცულია ნებადაურთველი შეღწევისგან?
☐ დიახ ☐ არა

კითხვა: რა ტიპის დაცვაა უზრუნველყოფილი ნებადაურთველი შეღწევისგან?

BIOS-პასვორდი: .....

პასვორდით დაცული სხვა მახასიათებლები: .....

კლავიატურის დაბლოკვა:.....

ეკრანის დაბლოკვა:.....

ეკრანის დამცველ(ებ)ი .....

კომპიუტერული პროგრამების სხვა დაცვა: .....

ჰარდვარის სხვა დაცვა:.....

საიდუმლო კითხვა და პასუხი პასვორდისთვის: .....

კითხვა: კომპიუტერული პროგრამა და/ან მასში არსებული მონაცემები დაცული არამართლზომიერი წვდომისგან?
☐ დიახ ☐ არა

პროგრამა/ფაილი .....

პასვორდი: .....

პროგრამა/ფაილი .....

პასვორდი: .....

პროგრამა/ფაილი .....

პასვორდი: .....

პროგრამა/ფაილი .....

პასვორდი: .....

პროგრამა/ფაილი .....

პასვორდი: .....

წვდომის სხვა მოწყობილობები (ინტელექტუალური ბარათი, დამცავი დამახშპორებლი, ბიომეტრიული სკანერები, მარკერები):
.....

.....

კითხვები: გაქვთ ინტერნეტზე წვდომა?

ინტერნეტის მომსახურების მომწოდებელი:

სისტემაში შესვლისას გამოყენებული სახელი/მომხმარებლის სახელი:

პასვორდი:

პასვორდისთვის გამოყენებული საიდუმლო კითხვა და პასუხი ამ კითხვაზე:

.....

.....

ელექტრონული ფოსტის მისამართი:

POP/SMTP სერვერი:

ვებ სივრცე, თავისუფალი სივრცე (ვირტუალური დრაივი)
.....

.....

კითხვა: კიდევ ვინ შეიძლება იცოდეს ამ სისტემის რომელიმე პასვორდი/წვდომის კოდი?
.....

.....

.....

კითხვა: რომელი ოპერატიული სისტემებია დაინსტალირებული მოწყობილობაზე?

დასახელება, ვერსია
.....

(მაგ., PC-სთვის: MSDOS, Windows, Unix, Linux, Mac OS; PDA-სთვის: Palm OS, Psion EPOC, Windows CE)

კითხვა: სისტემის დუბლირება (ბექაფი) რეგულარული ინტერვალებით ხდება? თუ კი:

ბექაფის კომპიუტერული პროგრამა:
.....

ბექფის აღმდგენი აგენტის კომპიუტერული პროგრამა:
.....

კითხვა: არის ქსელი[7]? თუ კი:

კითხვა: არის ქსელის გეგმა? (თუ არა, ითხოვეთ, დაგიხატონ ის).

კითხვა: რომელი ქსელის საოპერაციო სისტემ(ებ)ია დაყენებული?

დასახელება ვერსია
.....

კითხვა: წვდომის რა უფლება გაქვთ თქვენ ან სხვა პირებს?

---

[7] იხ. ასევე: მე- **რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.** თავი

მომხმარებლის სახელი	პასვორდი	ქსელის კოდი/წვდომის უფლება

.....

.....

კითხვა: ვინ ზრუნავს ქსელის ადმინისტრირებაზე?

.....

.....

შესაბამისად ვიყავი ინფორმირებული, რომ დამცავი მექანიზმების შესახებ მცდარი ინფორმაციის მიწოდებამ ან არ მითითებამ შეიძლება ჰარდვეარის დაზიანება და/ან მოდიფიცირება/მონაცემთა დაკარგვა შეიძლება გამოიწვის.

ჩემ მიერ მოწოდებული ინფორმაცია ნამდვილი და ზუსტია.

დასასრული: .....(დრო)

ვადასტურებ, რომ ყურადღებით წავიკითხე ეს ოქმი და ვეთანხმები მის შინაარსს:

.....

ხელმოწერასთან ერთად თითუეულ ფურცელზე დასვით ინიციალები

ამით ვადასტურებთ, რომ ელექტრონული მტკიცებულების ამოღების შესახებ სახელმძღვანელო პრინციპები მხედველობაშია მიღებული.

.....

ოფიცერი

ბ2 სანიმუშო ფორმა [2]: ამოღებული საგნების/ელექტრონული ტექნოლოგიების მტკიცებულების - საინვენტარიზაციო ფურცელი

ბეჭედი

ფაილის
№:

(ადგილი), (თარიღი)

საგანი:

წარმოდგენილი/ამოღებული საგნების სია

საქმის მწარმოებელი ოფიცერი: თარიღი/დრო მფლობელისგან მიღებული: ოფიციალური უწყება: ვისი სახელით: მიზეზი:	

საგნის ნომერი	#	აღწერა

გადაცემულია (მიუთითეთ დრო):	
ვის გადაეცა	
კომენტარი:	

ბ3 სანიმუშო საკონტროლი სია (ადაპტირებულია [რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ., რრორ! ღეფერენცე სოურცე ნოტ ფოუნდ.**]-დან და განვრცობილი): ქსელსა და უსაფრთხოებასთან დაკავშირებული კითხვები**

ეს საკონტროლო სია შეიძლება, გამოყენებული იყოს წინასწარი გამოკითხვის ჩასატარებლად მოწმეებსა და დაზარალებულებთან. ის ასევე გამოყენებული შეიძლება იყოს ექვმიტანილთა დაკითხვისას. გაითვალისწინეთ, რომ საკონტროლო სია არ არის ყველა მნიშვნელოვანი საკითხის ამომწურავი ჩამონათვალი.

1. ქსელის კონფიგურაცია
2. რა არის თქვენი IP მისამართი, მფლობელის სახელი და დროის ზონა?
3. რა არის თქვენი DNS სერვერი?
4. რა არის თქვენი LAN კონფიგურაცია?
5. გაქვთ ბრანდმაუერი (“ფაიარვოლი”)?
6. ბრანდმაუერის რომელ პროდუქტს იყენებთ?
7. გაქვთ ციფრული/ამობეჭდილი ასლი ბრანდმაუერის კონფიგურაციისა?
8. გაქვთ ფაიარვოლის ლოგ ფაილის ციფრული/ამობეჭდილი ასლი?
9. გაქვთ ვირუსის შემმოწმებელი სოფთვეარი?
10. რომელ სოფთვეარს იყენებთ?
11. როდის განაახლეთ ის ბოლოს?
12. ელექტრონული ფოსტა
13. რა არის თქვენი ელექტრონული ფოსტის მისამართი?
14. ელექტრონული ფოსტის რომელ პროგრამას იყენებთ?
15. რა არის თქვენი ელექტრონული ფოსტის პროვაიდერი (მაგ., POP/IMAP/SMTP/LDAP სერვერი)?
16. გაქვთ იმ პირის ელექტრონული ფოსტის მისამართი, რომელმაც გამოგზავნა ელექტრონული ფოსტა?
17. შეინახეთ ელექტრონული გზავნილი თქვენ კომპიუტერში?
18. “გაფართოებული სათაურის” ელექტრონული ასლი გაქვთ?
19. თუ არა, მისი ამობეჭდილი ასლი გაქვთ?
20. უსაფრთხოება
21. იყენებთ PGP, S/MIME ან ელექტრონული ფოსტის უსაფრთხოების სხვა პროდუქტს?
22. რა არის თქვენი ციფრული მაიდენტიფიცირებელი/ციფრული სერთიფიკატი?
23. ვინ მოგანიჭათ თქვენი ციფრული მაიდენტიფიცირებელი/ციფრული სერთიფიკატი (ორგანიზაციამ, სერვერმა)?
24. შეგიძლიათ მოგვაწოდოთ თქვენი ციფრული მაიდენტიფიცირებელი/ციფრული სერთიფიკატის ასლი?
25. შეგიძლია მოგვაწოდოთ შესაბამისი კომუნიკაციის პარტნიორების ციფრული მაიდენტიფიცირებელი/ციფრული სერთიფიკატები?
26. საიდან იღებთ სხვა ადამიანების ინფორმაციას (დაშიფვრას, ხელმოწერას)?
27. იყენებთ სხვა დაშიფვრის/ხელმოწერის პროგრამას?
28. ამ პროგრამის პროდუქტის სახელი/ვერსია რა არის?

29. რისთვის იყენებთ თქვენ ამ პროგრამას (მაგ., ფაილების სისტემის დაშიფვრა, ინდივიდუალური ფაილების დაშიფვრა, ა.შ.)?
30. სად ინახავთ კრიპტოგრაფიულ გასაღებს (დაშიფვრას, ხელმოწერას)?
31. იყენებთ სპეციალური დაცვის ჰარდვეარს?
32. რა არის პროდუქცის დასახელება/ვერსია (გამფართოებელი პლატა, ინტელექტუალური ბარათი, USB, ა.შ.)?
33. სად ინახავთ კრიპტოგრაფიულ გასაღებს (დაშიფვრას, ხელმოწერას)?
34. მსოფლიო ქსელი (WWW)
35. რა მოხდა ზუსტად?
36. რა არის ვებ-გვერდის მისამართი?
37. რა არის თქვენი ISP?
38. გაქვთ იმ ვებ-გვერდების ასლი, რომელიც ნახეთ?
39. რომელ დღესა და რა დროს ნახეთ ვებ-გვერდი?
40. რომელ დროის ზონაში?
41. სხვა ქსელების მომსახურებები
42. რომელი ელექტრონული მაღაზიები/მომსახურების მომწოდებლები ნახეთ? (პერსონალური/გადახდის ინფორმაცია თუა დაკავშირებული)?
43. რა არის თქვენი მომხმარებლის მაიდენტიფიცირებელი მონაცემი და პასვორდი ამ მომსახურებისთვის?
44. რა არის სერვერის IP მისამართი/სახელი/ვებ-გვერდის მისამართი (URL)?
45. გაქვთ შესაბამისი მონაცემების ციფრული ასლი?
46. თუ არა, გაქვთ მისი დაბეჭდილი ვერსია?
47. იყენებთ სხვა ქსელების მომსახურებას (მაგ., ftp, telnet)?
48. რა არის თქვენი მომხმარებლის სახელი და პასვორდი ამ სერვისებითვის?
49. რა არის ამ სერვერის IP მისამართი/სახელი/ვებ-გვერდის მისამართი (URL)?
50. გაქვთ შესაბამისი მონაცემების ელექტრონული ასლი?
51. თუ არა, გაქვთ მისი დაბეჭდილი ასლი?
52. შეტყობინების პანელები
53. რა არის თქვენი შეტყობინების ფორუმი (შეტყობინების პანელი, ბიულეტენის პანელი) მასპინძელი?
54. შეინახეთ შეტყობინება თქვენ კომპიუტერში?
55. თუ ასეა, შეგიძლიათ მისი ციფრული ასლის მოწოდება?
56. თუ არა, შეინახეთ ამ შეტყობინების ამობეჭდილი ასლი?
57. ახალი ამბების ჯგუფები
58. შეინახეთ შეტყობინება თქვენ კომპიუტერში?
59. თუ ასეა, შეგიძლიათ მისი ციფრული ასლი მოგვაწოდოთ?
60. თუ არა, შეინახეთ შეტყობინების ამობეჭდილი ასლი?
61. მნიშვნელოვანი ინფორმაცია: შეტყობინების ID, IP მისამართი
62. არის ეს ახალი ამბების ჯგუფი თქვენი ინტერნეტის მომსახურების მომწოდებლისგან პირდაპირ ხელმისაწვდომი? თუ კი:
63. ვინ არის თქვენი ინტერნეტ მომსახურების მომწოდებელი?
64. რა არის ახალი ამბების ჯგუფის სახელი?
65. რა არის თქვენი შეტყობინების დასახელება?
66. თუ ახალი ამბების ჯგუფი სპეციფიური სერვერიდან არის ხელმისაწვდომი:

67. რომელი ახალი ამბების ჯგუფის მომსახურებას იყენებთ?
68. რომელი კომპიუტერის სერვერი გამოიყენეთ ამ ახალი ამბების ჯგუფით სარგებლობისთვის?
69. რა არის ახალი ამბების ჯგუფის სახელი?
70. რა არის შეტყობინების სახელწოდება?
71. წერილობით სასაუბრო ოთახები
72. ინტერნეტ საუბრის ქსელი (IRC):
73. რა არის თქვენი ინტერნეტ მომსახურების მომწოდებელი?
74. რა არის საუბრის ქსელის სახელი?
75. ვინ არის საუბრის ქსელის ოპერატორი?
76. რა არის სერვერის დასახელება?
77. რა არის არამართლზომიერი ქმედების ჩამდენის ნიკი (მნემონური სახელი)?
78. საუბრის ასლი შეინახეთ თქვენ კომპიუტერში?
79. თუ ასეა, შეგიძლიათ მისი ელექტრონული ასლი მოგვაწოდოთ?
80. თუ არა, შეინახეთ საუბრის ამობეჭდილი ვერსია?
81. თუ ინტერნეტ მომსახურების მმწოდებელი გთავაზობთ საკუთარ ელექტრონულ სასაუბრო ოთახებს, რაც განსხვავდება ინტერნეტ საუბრის ქსელის (IRC)-გან:
82. ვინ არის ინტერნეტ მომსახურების მომწოდებელი?
83. რა ქვია ინტერნეტ სასაუბრო ოთახს?
84. რა არის არამართლზომიერი ქმედების ეკრანზე გამოყენებული სახელი?
85. გაქვთ საუბრის ასლი?
86. თუ კი, შეგიძლიათ მისი ასლი მოგვაწოდოთ?
87. თუ არა, შეინახეთ საუბრის ამობეჭდილი ვერსია?
88. საუბრის ოთახს ოპერატორი ან მედიატორი ჰყავდა?
89. თუ ასეა, რა სახელი იყო გამოყენებული?

3 დანართი გ: ბიბლიოგრაფია შენიშვნებითურთ (იხ. “ბიბლიოგრაფია”, საბოლოო ვერსია**1.0.pdf”)**