კომპიუტერული
შესწავლის
www.coe.int/cybercrime

დანაშაულის
პროექტი

ეკონომიკური დანაშაულის დეპარტამენტი
ადამიანის უფლებებისა და სამართლებრივი
საკითხების გენერალური დირექტორატი
საფრანგეთი, სტრასბურგი
მარტი, 2010, ვერსია XVII

მოსამართლეების ტრენინგი კომპიუტერული დანაშაულის შესახებ:

ტრენინგის

სახელმძღვანელო

(პროექტი)

წინამდებარე სახელმძღვანელოს პირველადი ვარიანტი მომზადებულია დოქტორ მარკო გერკეს მიერ, გერმანია. დოკუმენტი შეიქმნა ევროსაბჭოს ეკონომიკური დანაშაულის განყოფილებისათვის (ადამიანის უფლებებისა და სამართლებრივი საკითხების გენერალური დირექტორატი) კომპიუტერული დანაშაულის შესახებ პროექტის ფარგლებში. დოკუმენტის შემუშავებაში მონაწილეობა მიიღეს ნაიჯელ ჯონსმა (ტექნოლოგიების რისკი, გაერთიანებული სამეფო), ფრედესვინდა ინსამ (CYBEX, ესპანეთი), იან სპოენლიმ (მაქს პლანის ინსტიტუტი, გერმანია, ფრებურგი) და სხვა ექსპერტებმა. ნაშრომში შესწორებების შეტანა მოხდა ევროკომისიის და ევროსაბჭოს PROSECO პროექტის განხორციელების შედეგად, რომელიც ეხებოდა სამართლებრივ საკითხებთან დაკავშირებით სამხრეთ-აღმოსავლეთ ევროპის ქვეყნების თანამშრომლობას. www.coe.int/economiccrime

საკონტაქტო პირი

ალექსანდრე სეგელი
ეკონომიკური დანაშაულის განყოფილება
ევროსაბჭო
საფრანგეთი, სტრასბურგი
ტელ +33 3 9021 4506
ტელ +33 3 9021 5650
Alexander.seger@coe.int

შინაარსი

1. შესავალი: როგორ გამოვიყენოთ წინამდებარე სახელმძღვანელო

წინამდებარე სახელმძღვანელოს მიზანია არის ტრენინგის ორგანიზების ხელშეწყობა მოსამართლეებისათვის კომპიუტერული/კიბერდანაშაულის საკითხებთან დაკავშირებით.

ბოლო წლებში, მთელი მსოფლიოს მასშტაბით შეიმჩნევა საზოგადოების დამოკიდებულების მნიშვნელოვანი ზრდა საინფორმაციო საშუალებებისადმი. დღეს, ინფორმაციამ და საინფორმაციო ტექნოლოგიებმა ადამიანების ცხოვრების თითქმის ყველა სფეროში შეაღწია. საინფორმაციო ტექნოლოგიებზე მზარდი დამოკიდებულება საზოგადოებას ისეთი საფრთხის წინაშე აყენებს, როგორიც არის კომპიუტერული დანაშაული, რაც ნიშნავს დანაშაულის ჩადენას კომპიუტერის საშუალებით და კომპიუტერული სისტემებისა და მონაცემების წინააღმდეგ.

მიუხედავად იმისა, რომ ბევრ ქვეყანაში სამართალდამცავმა ორგანოებმა შეძლეს საკუთარი შესაძლებლობების გაძლიერება კომპიუტერული დანაშაულის გამოძიებისა და ელექტრონული მტკიცებულების უზრუნველყოფის მიზნით, ეს არანაირად არ ამცირებს მოსამართლეების მნიშვნელობას, რომლებიც გადამწყვეტ როლს თამაშობენ სისხლის სამართლის საქმეების სამართლიანი განხილვის პროცესში.

სწორედ ამიტომ არის საჭირო კონკრეტული ძალისხმევა მოსამართლეებისათვის ტრენინგის ჩატარების მიზნით, რაც უზრუნველყოფს მათ აღჭურვას სათანადო ცოდნით, რომელიც აუცილებელია კომპიუტერულ დანაშაულთან და ელექტრონულ მტკიცებულებასთან დაკავშირებულ საქმეზე განაჩენის გამოსატანად.

წინამდებარე სახელმძღვანელო შედგება ძირითადი, შესავალი ტრენინგ-კურსისგან, რომელიც უნდა ჩატარდეს, სულ მცირე, ორი დღის განმავლობაში. ცხადია, შესაძლოა, ზოგი საკითხის შემოკლება ან გამოტოვება და ერთდღიანი ტრენინგის ჩატარება, ან პირიქით, ტრენინგის ვადის ერთ კვირამდე ან მეტით გაზრდა და იმ საკითხების განხილვაც, რომლებიც მითითებულია შენიშვნებში.

სახელმძღვანელოს სტრუქტურა გამომდინარეობს ტრენინგის რეკომენდირებული კურსიდან:

- შესავალი ნაწილი მოიცემულია თავში 2 და იგი აღწერს კომპიუტერული დანაშაულის რაობას და იმ გამოწვევებს, რომლებსაც ეს მოვლენა უყენებს მოსამართლეებს. ასევე, წარმოგვიდგენს ევროსაბჭოს "ბუდაპეშტის" კონვენციას კომპიუტერული დანაშაულის შესახებ, რომელიც წარმოადგენს ძირითად საერთაშორისო სტანდარტს მსოფლიოს მასშტაბით კომპიუტერული კანონმდებლობის ჰარმონიზაციის კუთხით.

- თავი 3 გააცნობს მოსამართლეებს საინფორმაციო ტექნოლოგიებს.
- თავი 4 აღწერს, თუ როგორ არის განსაზღვრული სხვადასხვა სახის ქმედება, რომელიც შეადგენს კომპიუტერულ დანაშაულს, როგორც სისხლის სამართლის დანაშაული. ამ ნაწილში მოცემულია კომპიუტერული დანაშაულის კონვენციის დებულებები. ტრენინგის დროს მნიშვნელოვანია, კონვენციის დებულებების დაკავშირება და განხილვა ეროვნულ საკანონმდებლო ბაზასთან მიმართებაში.
- თავი 5 წარმოადგენს შესავალს კომპიუტერული დანაშაულის ექსპერტიზისა და ელექტრონული მტკიცებულების შესახებ.
- თავი 6 აღწერს პროცედურული კანონით განსაზღვრულ ღონისძიებებს, რომელიც ხელმისაწვდომია სისხლის სამართლის ორგანოებისათვის, რათა მათ გამოიძიონ კომპიუტერული დანაშაულის საქმეები და უზრუნველყონ ელექტრონული მტკიცებულების ეფექტიანად წარმოდგენა.
- თავი 7 შეეხება საერთაშორისო თანამშრომლობას. კომპიუტერული დანაშაული ყველაზე მეტად წარმოადგენს ტრანსნაციონალურ დანაშაულს და შეუძლებელია მასთან ბრძოლა ეფექტიანი საერთაშორისო თანამშრომლობის გარეშე. მოსამართლეები მნიშვნელოვან როლს თამაშობენ ასეთი თანამშრომლობის გააქტიურების მიზნით.

დანართში მოცემულია ტერმინთა განმარტება და ის მაგალითები, რომელთა გამოყენებით შესაძლებელია იმ საკითხების ილუსტრირება, რომელთა შესახებ საუბარი იყო წინა თავებში.

ტრენინგის კურსის დასრულების შემდეგ, მოსამართლეებმა უნდა შეძლონ კომპიუტერული დანაშაულის მნიშვნელობის გააზრება; ის, თუ საერთო სამართლის რომელი კანონები, საკანონმდებლო აქტები და პროცედურული კანონები უნდა იქნეს გამოყენებული და რატომ არის მნიშვნელოვანი ეფექტიანი ღონისძიებებისა და საერთაშორისო თანამშრომლობის განხორციელება.

მაგალითი: ტრენინგი კომპიუტერული დანაშაულისა და ელექტრონული მტკიცებულებების თაობაზე - საბაზო ცოდნის მისაღები ტიპური მოდული

კურსის მიზანი	კურსის დასასრულს მოსამართლეებსა და პროკურორებს ზოგადი ცოდნა უნდა ჰქონდეთ, თუ რა არის კომპიუტერული დანაშაული და ელექტრონული მტკიცებულება, როგორ შეუძლიათ მოსამართლეებსა და პროკურორებს მათთან გამკლავება, რომელი მატერიალური და პროცესუალური ნორმების, ისევე როგორც ტექნოლოგიების, გამოყენება შეიძლება, როგორ შეიძლება გადაუდებელი და ეფექტური ზომების განხორციელება და ფართო საერთაშორისო თანამშრომლობის დანერგვა
სესია 1	კომპიუტერული დანაშაულის შესახებ
	➢ რატომ შევწუხდეთ კომპიუტერულ დანაშაულზე ფიქრით? ➢ რა არის კომპიუტერული დანაშაული? ➢ სირთულეები მოსამართლეებისა და პროკურორებისთვის ➢ ეროვნული კანონმდებლობა და საერთაშორისო სტანდარტები
სესია 2	ტექნოლოგია
	➢ ინტერნეტის ფუნქციონირება (ძირითადი ცნებები) ➢ ტერმინთა განმარტება

	➢ პროტოკოლები
სესია 3	კომპიუტერული დანაშაული, როგორც დანაშაულებრივი ქმედება შიდა კანონმდებლობაში
	➢ დანაშაულები კომპიუტერული მონაცემებისა და სისტემების წინააღმდეგ ➢ კომპიუტერთან დაკავშირებული თაღლითობა და სიყალბე ➢ შინაარსთან დაკავშირებული დანაშაულები (არასრულწლოვანთა პორნოგრაფია, ქსენოფობია, რასიზმი) ➢ ინტელექტუალურ საკუთრებასთან დაკავშირებული დანაშაულები ➢ სასამართლო გადაწყვეტილება/სასამართლო პრაქტიკა
სესია 4	ელექტრონული მტკიცებულებები
	➢ ელექტრონული მტკიცებულებების შესახებ: განსაზღვრებები და მახასიათებლები ➢ ელექტრონული მტკიცებულებების მოთხოვნები ➢ კომპიუტერული ექსპერტიზა
სესია 5	საპროცესო სამართალი/საგამძიებო ღონისძიებები
	➢ იურისდიქცია და ტერიტორიული კომპეტენციები ➢ კომპიუტერული მონაცემების სწრაფი დაცვა ➢ წარმოდგენის ბრძანებები/ორდერები ➢ კომპიუტერული მონაცემების ჩხრეკა და ამოღება ➢ მონაცემთა გაცვლისა და შინაარსობრივი მონაცემების ამოღება ➢ დაცვის გარანტიები
სესია 6	კერძო სექტორთან ურთიერთობა
სესია 7	საერთაშორისო თანამშრომლობა
	➢ კონვენცია კომპიუტერული დანაშაულის შესახებ, როგორც საერთაშორისო თანამშრომლობის ჩარჩო ➢ ზოგადი პრინციპები ➢ შუალედური ღონისძიებები და 24/7 საკონტაქტო პირების როლი ➢ საერთაშორისო სამართლებრივი დახმარება და კომპეტენტური ორგანოების როლი
სესია 8	შეფასება და დასკვნა
ორგანიზაცია და მასალები	ტრენინგი შესაძლოა, ჩატარდეს ელექტრონულად ან საკლასო ოთახში. თუ ტრენინგი კლასში ტარდება: ➢ ოთახში პერსონალური კომპიუტერი და პროექტორი საკმარისია (რადგან ეს კურსი არ ითვალისწინებს პრაქტიკულ სავარჯიშოებს, როგორიცაა საექსპერტიზო კომპიუტერული პროგრამის ან საგამოძიებო ტექნიკის დემონსტრაცია, კომპიუტერული ლაბორატორია საჭირო არ არის) ➢ შიდა მატერიალური და საპროცესო კანონმდებლობის შესაბამისი ამონარიდები ➢ კომპიუტერული დანაშაულის შესახებ ბუდაპეშტის კონვენცია, განმარტებითი ბარათითურთ ➢ სასწავლო მასალა, რომელიც მოიცავს ტერმინთა განმარტებასა და სხვა ზოგად ინფორმაციას ➢ თუ ლექციები უცხო ენაზე ტარდება, თარგმანი უნდა იყოს გათვალისწინებული და მასალა უნდა ითარგმნოს.

მაგალითი: ტრენინგი კომპიუტერული დანაშაულისა და ელექტრონული მტკიცებულებების თაობაზე - საშუალო/მომხმარებლის დონის ცოდნის მისაღები ტიპური მოდული[1]

კურსის მიზნები	კურსის დასასრულს მოსამართლეებსა და პროკურორებს უნდა ჰქონდეთ საშუალო/მომხმარებლის დონის ცოდნა, რომლის გამოყენება უნდა მოხდეს პრაქტიკაში კომპიუტერებისა და ქსელების ფუნქციონირებაზე, იმის შესახებ, თუ რა არის კომპიუტერული დანაშაული, კომპიუტერული დანაშაულის თაობაზე კანონმდებლობის შესახებ, ქვემდებარობის, საგამოძიებო საშუალებებისა და ელექტრონული მტკიცებულებების და საერთაშორისო თანამშრომლობისშესახებ
სესია 1	კომპიუტერები და ქსელები
	➢ კომპიუტერული და კომპიუტერული დანაშაულის შესახებ ტერმინების განმარტება ➢ საინფორმაციო და საკომუნიკაციო ტექნოლოგიების ფუნქციონირება/ინტერნეტ ინფრასტრუქტურა - პროტოკოლები და ტექნოლოგია - როგორ ახდენენ კომუნიკაციას კომპიუტერები - ინტერნეტ პროტოკოლის გამოძიება და ელექტრონული მტკიცებულებები - ციფრები და კომპიუტერების სახელები - მომსახურების მომწოდებლების როლი ➢ ინფორმაცია ინტერნეტში - ინფორმაციის შეგროვება - (დაფარული) ინტერნეტ მონაცემთა ბაზების გამოყენება ➢ სოციალური ჯგუფების პროფილები - კომუნიკაციის მანერები - ანონიმურობის მანერები ➢ კომპიუტერების, ინტერნეტში ნანახი კომპანიებისა და ადამიანების აღმოჩენა/ადგილსამყოფელის განსაზღვრა
სესია 2	კომპიუტერული დანაშაული და უსაფრთხოების რისკები
	➢ ტენდენციები კომპიუტერულ დანაშაულში ➢ ტიპოლოგია: კომპიუტერული დანაშაულის კონკრეტული ტიპები და ტექნიკა (მაგ., ფიშინგი, ბოტნეტები და სხვა ვირუსები, არასრულწლოვანთა პორნოგრაფია) ➢ როგორ იყენებენ კრიმინალები საინფორმაციო და საკომუნიკაციო ტექნოლოგიებს ➢ დამნაშავენი ➢ კომპიუტერული დანაშაულის გავლენა/შედეგი ➢ როგორ გავზარდოთ საინფორმაციო და საკომუნიკაციო ტექნოლოგიების უსაფრთხოება ➢ პრაქტიკული მაგალითები და სიმულაციები
სესია 3	კომპიუტერულ დანაშაულთან დაკავშირებული კანონმდებლობა: სისხლის სამართლის მატერიალური კანონმდებლობა
	➢ კომპიუტერული მონაცემებისა და სისტემების წინააღმდეგ მიმართული დანაშაული ➢ კომპიუტერთან დაკავშირებული თაღლითობა და სიყალბე ➢ შინაარსთან დაკავშირებული დანაშაულები (არასრულწლოვანთა პორნოგრაფია, შუღლის გაღვივება) ➢ ინტელექტუალურ საკუთრებასთან დაკავშირებული დანაშაულები ➢ სასამართლო გადაწყვეტილება/პრეცედენტული სამართალი
სესია 4	გამოძიება და ელექტრონული მტკიცებულება
	➢ ელექტრონული მტკიცებულება - კვალი კომპიუტერებზე,ინტერნეტში, ციფრულ კომუნიკაციაში - ელექტრონული მტკიცებულებების ჩხრეკის, ამოღების და შენახვის ნაბიჯები - ექსპერტიზის კომპიუტერული პროგრამის მახასიათებლები - ეჭვმიტანილთა იდენტიფიცირება

[1] kiTxvarze gacemul pasuxebze da niderlandebis mier mowodebul magaliTze dayrdnobiT.

	- დანაშაულებრივი გზით მოპოვებული ფულის კვალს მიდევნება - დაცვის გარანტიები და პირობები - საქმის მართვა/მომზადება - ელექტრონული მტკიცებულებების შენახვა სასამართლოში ➢ კომპიუტერული დანაშაულთან/ელექტრონული მტკიცებულებასთან მიმართებით სამართალდამცავთა ორგანიზება ➢ პრაქტიკული მაგალითების განხილვა
სესია 5	კანონმდებობა კომპიუტერული დანაშაულის შესახებ: საპროცესო სამართალი
	➢ კომპიუტერული მონაცემების სწრაფი შენახვა ➢ ინფორმაციის წარმოდგენის შესახებ ბრძანება ➢ კომპიუტერული მონაცემების ჩხრეკა და ამოღება ➢ ინფორმაციის მოძრაობისა და შინაარსის შესახებ მონაცემების მიღება/გადაჭრა ➢ გარანტიები ➢ ინტერნეტის მომსახურების მომწოდებლებთან/კერძო სექტორთან ურთიერთობა ➢ პრაქტიკული მაგალითების განხილვა
სესია 6	ქვემდებარობა და ტერიტორიული კომპეტენციები
	➢ ზოგადი პრინციპები ➢ კომპიუტერული დანაშაულის ქვემდებარეობა - სირთულეები ➢ ქვემდებარეობის შესახებ დებულებები კომპიუტერული დანაშაულის შესახებ კონვენციაში ➢ პრაქტიკული მაგალითების განხილვა
სესია 7	საერთაშორისო თანამშრომლობა
	➢ კომპიუტერული დანაშაულის შესახებ კონვენცია, როგორც საერთაშორისო თანამშრომლობის ჩარჩო ➢ ზოგადი პრინციპები ➢ დროებითი ღონისძიებები, 24/7 საკონტაქტო ერთეულის როლი და პოლიციის თანამშრომლობა ➢ საერთაშორისო სამართლებრივი დახმარება და კომპეტენტური ორგანოების როლი ➢ პრაქტიკული მაგალითების განხილვა
სესია 8	შეფასება და დასკვნები
ორგანიზება და მასალა	ტრენინგი შესაძლოა, ჩატარდეს ელექტრონულად ან საკლასო ოთახში. თუ საკლასო ოთახში ჩატარდება, საჭიროა: ➢ სასწავლო ოთახი, სადაც პერსონალური კომპიუტერი და პრექტორია პრეზენტაციებისთვის ➢ სასარგებლო იქნება მსმენელთათვის ინტერნეტში ჩართული კომპიუტერის ქონა (თუმცა, ეს პირობა არ არის) ➢ შესაბამისი ამონარიდები შიდა მატერიალური და საპროცესო კანონმდებლობიდან ➢ კომპიუტერული დანაშაულის შესახებ ბუდაპეშტის კონვენცია განმარტებითი ბარათითურთ ➢ სახელმძღვანელო ტექრმინთა განმარტებით და სხვა ზოგადი ინფორმაციით ➢ თუ ლექციები უცხო ენაზე ტარდება, უზრუნველყოფილი უნდა იყოს თარგმანი და მასალა ნათარგმნი უნდა იყოს.

2. კომპიუტერული დანაშაულის შესახებ

ტრენინგის კურსის დასრულებისას მონაწილეებმა უნდა შეძლონ შემდეგის გააზრება:

- რატომ უნდა ფლობდნენ მოსამართლეები ინფორმაციას კომპიუტერული დანაშაულის შესახებ
- რა საქმიანობა განისაზღვრება, როგორც კომპიუტერული დანაშაული (ტიპოლოგია)
- მოსამართლეების წინაშე არსებულო კონკრეტული გამოწვევები
- რატომ უნდა მოხდეს ეროვნული კანონმდებლობის ჰარმონიზაცია საერთაშორისო სტანდარტებთან, ანუ კონვენციასთან კომპიუტერული დანაშაულის შესახებ

2.1. რატომ არის კომპიუტერული დანაშაული პრობლემა?

ინტერნეტის განვითარება და მისი სწრაფი ზრდა დიდ ზეგავლენას ახდენს მსოფლიო საზოგადოებაზე. [2] განვითარებული, ისევე როგორც განვითარებადი ქვეყნების მოსახლეობა საინფორმაციო საზოგდოებად[3] გარდაიქმნა. პროცესი ხასიათდება საინფორმაციო ტექნოლოგიების მზარდი გამოყენებით ინფორმაციის მიღებისა და მისი გავრცელების მიზნით.[4] აღნიშნული პროცესი უამრავ შესაძლებლობებს გვთავაზობს, დაწყებული ინფორმაციის ხელმისაწვდომობიდან, დამთავრებული კონტაქტით ყველა იმ ადამიანთან, ვისაც აქვს ინტერნეტი.[5] მსოფლიოს ბევრ რეგიონში, ინფორმაციის ხელმისაწვდომობამ და კომუნიკაციის შესაძლებლობამ გააძლიერა დემოკრატია, ადამიანის უფლებების დაცვა და სამართლებრივი სახელმწიფოს მშენებლობის პროცესი.

აღნიშნული შესაძლებლობები ხელს უწყობს საინფორმაციო ტექნოლოგიების მუდმივ და ყოველდღიურ ინტეგრირებას ადამიანების ყოველდღიურ ცხოვრებაში მსოფლიოს მასშტაბით.[6]

[2] ინტერნეტის განვითარებასთან დაკავშირებით, იხილეთ: იანგ მაიო, გამოთვლითი ტექნიკის ასოციაციის კონფერენცია, ტომი 113, ელექტრონული ბიზნესის VII საერთაშორისო კონფერენციის დასკვნები, გვ.52-56

[3] ინფორმაციული საზოგადოების შესახებ დამატებითი ინფორმაციის სანახავად, იხილეთ: მასუდა, ინფორმაციული საზოგადოება –პოსტ-ინდუსტრიული საზოგადოება; დუტა/დე მეიერი/იანი/რიხტერი, ინფორმაციული საზოგადოება გაფართოებულ ევროპაში; მალდუმი/მარსდენი/სიდაკი/სინგერი/: როგორ შეუძლია ბრიუსელს დააკავშიროს საინფორმაციო საზოგადოება; გლობალური საინფორმაციო საზოგადოებაში საერთაშორისო სამართლისა და იურიდიული საკითხების სალზბურგის ცენტრი; ჰორნბი/კლარკი: საინფორმაციო საზოგადოების გამოწვევები და ცვლილებები.

[4] მსოფლიო უმაღლესი დონის შეხვედრა საინფორმაციო საზოგაადოების საკითხებთან დაკავშირებით: დოკუმენტები: WSIS-03/ჟენევა/დოკ/5/-ე, 2003 წლის დეკემბერი. ხელმისაწვდომია შემდეგ მისამართზე: www.itu.int/wsis/docs/geneva/official/poa.html/.

[5] იხილეთ: კომუნიკაცია კომისიასა და საბჭოს შორის, ევროპის პარლამენტი, ევროპის ეკონომიკური დახმარებისა და სოციალური საკითხების კომიტეტი; ასევე, რეგიონების, ევროპის საინფორმაციო საზოგადოების გამოწვევების კომიტეტი, გვ3. შეგიძლიათ მოიძიოთ: http://ec.europa.eu/information_society/eeurope/i2010/docs/communications/new_chall_en_adopted.pdf.

[6] იხილეთ გუდმენის „სამოქალაქო ავიაციის ანალოგია – საერთაშორისო თანამშრომლობა სამოქალაქო ავიაციის დაცვის მიზნით ტერორიზმისა და კომპიუტერული დანაშაულისაგან“; „ტერორიზმისა და კომპიუტერული დანაშაულის ტრანსნაციონალური ბუნება“, 2001, გვ.69. ვებ-გვერდი: http://media.hoover.org/documents/0817999825_69.pdf. მანქანებში განთავსებული კომპიუტერები წინააღმდეგ შესაძლო შეტევებთან დაკავშირებით, იხილეთ ბიბისის ახალი ამბები, კომპიუტერული ვირუსებისაგან თავისუფალი მაქანები, 110.05.2005. http://news.bbc.co.uk/1/hi/technology/4536307.stm.

ინტერნეტს უკვე იყენებს მილიარდზე მეტი ადამიანი.[7] ამ რიცხვში შედიან არა მხოლოდ ინდივიდები, არამედ ბიზნესებიც, რომელთაც, ასევე, სარგებელი აქვთ ინტერნეტისა და საინფორმაციო ტექნოლოგიებისაგან, რადგან აღნიშნული ხელს უწყობს საქონლისა და მომსახურების შეთავაზებას მსოფლიო მასშტაბით და ნაკლები ფინანსური დანახარჯებით.[8]

კომპიუტერული სისტემა და ინტერნეტმომსახურება ადამიანების პირად ცხოვრებაშიც სულ უფრო ხშირად ფიგურირებს. ადამიანები იყენებენ საინფორმაციო ტექნოლოგიებს საკუთარი აზრების განვითარებისა და გაზიარების მიზნით, აკეთებენ ფილმებს, ინახავენ სურათებს, დოკუმენტებს და ამყარებენ კომუნიკაციას.

საინფორმაციო ტექნოლოგიების განვითარებამ არა მხოლოდ კერძო მომხმარებლების და საწარმოების შესაძლებლობები გააუმჯობესა. არამედ შესაძლებლობაც მისცა მისცეს დამნაშავეებს, მიზანში ამოიღონ კონკრეტული კომპიუტერი ან მომსახურება. მსგავსი დანაშაული შეიძლება იყოს შეტევა ელექტრონულ-კომერციულ ობიექტებსა და მნიშვნელოვან ინფრასტრუქტურაზე; იგი, ასევე, შეიძლება მოიცავდეს კერძო კომპიუტერებიდან ან კომპანიების მონაცემთა ბაზიდან იდენტობასთან დაკავშირებული ინფორმაციის მოპოვებას. სწორედ ამიტომ, საინფორმაციო ტექნოლოგიების დაცვა, კომპიუტერული მონაცემებისა და სისტემის კონფიდენციალურობის, მთლიანობისა და მასში შეღწევისაგან დაცვა იმავდროულად ნიშნავს პირადი ცხოვრების, სიტყვის თავისუფლებისა და სხვა ფუნდამენტური უფლებების დაცვას.

მოკლედ, რაც უფრო მეტად ხდება საზოგადეობა დამოკიდებული საინფორმაციო ტექნოლოგიებზე, მით მეტად იზრდება მისი დაუცველობა და საფრთხისათვის პასუხის გაცემის საჭიროება. აღნიშნული საფრთხის დასარეგულირებლად საჭირო სტრატეგია გახლავთ კომპიუტერული დანაშაულის წინააღმდეგ შესაბამისი კანონმდებლობის შემუშავება და მისი განხორციელება. ამ პროცესში დიდია მოსამართლეების როლი.

2.2. რა არის კომპიუტერული დანაშაული?

კომპიუტერული დანაშაულის რაობის შესახებ მოსაზრებები განსხვავებულია.[9] მთავარი კითხვა აქ გახლავთ ის, არის ეს

[7] 2007 წლის დასაწყისისათვის ინტერნეტის მომხმარებელთა რიცხვი იყო 1.14 მილიარდი. http://www.itu.int/ITU-D/icteye.default.asp

[8] იხილეთ: პერსონალური კომიუტერის განვითარების ზეგავლენა ეკონომიკასა და ფინანსებზე. დიდი შვიდეულის ფინანსთა მინისტრების ანგარიში, 2000, http://www.mof.go.jp/english/if/if020.pdf.

[9] კომპიუტერული დანაშაულის განმარტებისა და კატეგორიებად დაყოფის თვალსაზრისით, იხილეთ: კომპიუტერული დანაშაული, განმარტება დ აზოგადი ინფორმაცია, ავსტრალიის კრიმინოლოგიის ინსტიტუტი: http://www.aic.gov.au/topics/cybercrime/definitions.html; gordo/fordis ანგარიში №8 კომპიუტერული დანაშაულის კონვენციას, კომიუტერული დანაშაულის განმარტებისა და კლასიფიკაციის შესახებ, ჟურნალი: კომპიუტერის ვირუსოლოგია, ტომი2; №1, 2006, გვ:13-20; ჩაუკი, კომპიუტერული დანაშაული საფრანგეთში: მიმოხილვა, 2005: http://www.crime-research.org/articles/cybercrime-in-france-overview/; უილსონი, ბიტნეტსი: კომპიუტერული დანაშაული და კომპიუტერული ტერორიზმი: სუსტი ადგილები და პოლიტიკის საკითხები კონგრესისათვის, 2007, გვ.4: http://www.fas.org/sgp/crs/terror/RL32114.pdf; კომპიუტერული დანაშაული, პარლამენტის ერთობლივი კომიტეტის ანგარიში ავსტრალიის

მხოლოდ კომპიუტერული მონაცემებისა და სისტემის წინააღმდეგ ჩადენილი დანაშაული (ვიწრო გაგება), თუ იგი, ასევე, მოიცავს იმ დანაშაულს, რომელიც ჩადენილია კომპიუტერული მონაცემებისა და სისტემის საშუალებით (ფართო გაგება).[10] კომპიუტერული დანაშაულის კონვენციის ავტორებმა ამ ცნებაში ორივე განმარტება შეიტანეს და კომპიუტერული დანაშაული განსაზღვრეს ოთხი ტიპის დანაშაულად:

1. კომპიუტერული მონაცემებისა და სისტემის კონფიდენციალურობის, ინტეგრირებულობისა და მასში შეღწევის წინააღმდეგ ჩადენილი დანაშაული;
2. კომპიუტერის საშუალებით ჩადენილი დანაშაული;
3. შინაარსთან დაკავშირებული დანაშაული;
4. ინტელექტუალური საკუთრებისა და მსგავსი უფლებების წინააღმდეგ ჩადენილი დანაშაული;

2.2.1. კომპიუტერული მონაცემებისა და სისტემის კონფიდენციალურობის, ინტეგრირებულობისა და მასში შეღწევის წინააღმდეგ ჩადენილი დანაშაული("CIA)

ეს კატეგორია წარმოადგენს კომპიუტერულ დანაშაულს ვიწრო გაგებით, რომელიც მიმართულია კომპიუტერული სისტემისა და მონაცემების წინააღმდეგ:

- კომპიუტერულ სისტემაში არასანქცირებული/უკანონო შეღწევა წარმოადგენს კომპიუტერული დანაშაულის ერთ-ერთ უძველეს მეთოდს. ამაში შედის კოდური სიტყვის ან სხვა დამცავი მექანიზმების გატეხვა ან მათი შემოვლა კომპიუტერულ სისტემაში უფლებამოსილების/სანქციის გარეშე შეღწევის საშუალებით.[11]
- ინფორმაციის ხელში უკანონო/არასანქცირებული ჩაგდება მისი გადაცემის დროს. ეს დანაშაული შეესაბამება კომპიუტერული ქსელის მიღმა წარმოებული არასაჯარო კომუნიკაციის არასანქცირებულ ხელში ჩაგდებას, როგორებიცაა: სატელეფონო საუბრების მოსმენა.

დანაშაულის კომისიის შესახებ, 2004, გვ.5: http://www.aph.gov.au/Senate/Committee/acc_ctte/completed_inquiries/2002-04/cybercrime/report/report.pdf; heideni, kompiuteruli danaSaulis gavlena sainformacio sazogadoebaze, kompiuteruli danaSauli da usafrTXoeba, gv. 3; heili, kompiuteruli danaSauli: globaluri dilemis faqtebi da cifrebi, 2002, tomi 18: http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37; ფორსტი: კომპიუტერული დანაშაული: სააპელაციო სასამრთლოს ინტერპრეტაცია, 1999, გვ.1;

[10] იხილეთ: კარტერი, კომპიუტერული დანაშაულის კატეგორიები: როგორ მუშაობენ ტექნო-დამნაშავეები, გამოძიების ფედერალური ბიუროს კანონი, 1995, გვ.21: http://www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20-%20Types%20of%20computer%20crime.pdf; ჩარნი: კომპიუტერული დანაშაული: სამართალდამცავების გადასვლა კორპორაციული გარემოდან კომპიუტერული სივრცის არამატერიალურ, ელექტრონულ სამყაროში, ფედერალური სამართლებრივი საკითხები, 1994, ტომი 41, ნომერი 7, გვ.489; გუდმენი, რატომ არ აინტერესებს პოლიტიკას კომპიუტერული დანაშაული? ჰარვარდი სამართალის და ტექნოლოგიების ჟურნალი, ტომი 10, ნომერი 3, გვ.469;

[11] ჰაკერობასთან დაკავშირებით, იხილეთ: ლევი, ჰაკერები, 1984, ჰაკერული დანაშაული, ავსტრალიის კრიმინოლოგიის ინსტიტუტი, 2005: http://www.aic.gov.au/publications/htcb/htcb005.pdf.; ტეილორი, დაკარგული ეთიკის ძიებაში? უოლ-სტრიტ ჟურნალში: დანაშაული დაინტერნეტი, 2001, გვ.61; ჰაკერული დანაშაულის მსხვერპლთა გასაცნობად, იხილეთ: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; ჯოინერ/ლატრიონეტე, სამარლებრივი ჩარჩოს ელემენტები, 2002, №5, გვ.825; შედებენის შესახე, იხილეთ: ბიგელი: ჩვენს კონტროლს მიღმა, სამართლებრივი სისტემის საზღვრები კიბერსივრცის ერაში, 2001, გვ.231.

ელექტრონული ფოსტით და უკაბელო ინტერნეტით სარგებლობის ზრდასთან ერთად[12], რომელიც ხშირად დაუცველი და დაუშიფრავია, იზრდება ინფორმაციის არაკანონიერად ხელში ჩაგდების საშუალება.

- მონაცემებში ჩარევა/ზეგავლენა. არასანქცირებული/არაკანონიერი შეღწევის ეს გზა ცდილობს დააზიანოს ან შეცვალოს კომპიუტერში არსებული მონაცემები სისტემაში ვირუსის[13] ან თვითგავრცელებადი ვირუსების (warm)[14] შეყვანით. კომპიუტერის მინაცემებზე ზემოქმედება, ასევე, შესაძლებელია უკანა/საიდუმლო კარის შექმნით, რომლიდანაც შესაძლოა კომპიუტერში შესვლა ან მისი გარედან გაკონტროლება. ასევე, შეიძლება "რუტკიტის" დაყენება, რომელიც არ გაძლევთ საშუალებას მიხვდეთ, რომ კომიუტერთან ვიღაცას აქვს კავშირი. ასევე, შესაძლებელია პროგრამა შპიონის[15] ან კლავიშზე ყოველი ხელის დაჭერის რეგისტრატორი პროგრამის ან ტექნიკის[16] ინსტალაცია (მაგალითად, როცა ხდება პაროლის ან პერსონალური საიდენტიკაციო ნომრის აკრეფა, რომლის შედეგად აღნიშნული ინფორმაცია გადაეცემა კრიმინალებს.
- სისტემაში ჩარევა/ზემოქმედება. კომპიუტერის დამაზიანებლი ვირუსის შეყვანა სისტემაში აზიანებს არა მხოლოდ მონაცემებს, არამედ მთლიანად გამოყავს კომპიუტერი წყობიდან. სისტემაში ჩარევის ერთ-ერთი ფორმა გახლავთ შეტევა - "უარი მომსახურებაზე"[17], რომლის დროს კომპიუტერის სისტემას ეგზავნება მრავალი მიმართვა/მოთხოვნა მისი ფუნქციონირების დაბრკოლების მიზნით. ხშირად, ასეთი მიმართვა/მოთხოვნა იგზავნება ბევრი სხვადასხვა ინდივიდუალური კომპიუტერიდან (ვრცელდება შეტევა "უარი მომსახურებაზე" DoS), რომლის შეტანა ხდება

[12] კომიუტერული დანაშაულის გამოძიებასთან დაკავშირებული პრობლემები უკაბელო ქსელების ჩათვლით, იხილეთ კანგის: უკაბელო ქსელების უსაფრთხოება – კიდევ ერთი საკითხი კომპიუტერული დანაშაულის წინააღმდეგ ბრძოლაში; ურბას/კრონი, მობილური და უკაბელო ტექნოლოგიები: უსაფრთხოება და რისკის ფაქტორები, ავსტრალიის კრიმინოლოგიის ინსტიტუტი, 2006: http://www.aic.gov.au/publications/tandi2/tandi329t.html.

[13] კომპიუტერის ვირუსი არის პროგრამა, რომელსაც შეუძლია საკუთარი თავის გამეორება და კომიუტერის დაინფიცირება, მომხმარებლსი ნებართვის გარეშე. იხილეთ სპაფორდი :ინტერნეტის ვირუსის პროგრმა: ანალიზი, გვ.3; კოენი – კომპიუტერული ვირუსი – თეორია და ექსპერიმენტი - : http://all.net/books/virus/index.html. კოენი, კომპიუტერის ვირუსები; ადლემანი – „ კომპიუტერული ვირუსების აბსტრაქტული თეორია". კომპიუტერული ვირუსების ეკონომიკური შედეგების შესახებ, იხილეთ კაშელი, ჯეკსონი, ჯიკლინგი და უებელი – „კომპიუტერული შეტევების ეკონომიკური ეფექტი", გვ.12; სიმანტეკი – ანგარიში კომპიუტერების შეტევის შესახებ, იელისი-დეკემბერი, 2006: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

[14] ტერმინი „worm" პირველლად გამოიყენა სოჭ/ჰუპმა, „ვირუსების პროგრამა – გავრცელებული გამოთვლების ადრეული პრაქტიკა, 1982. შეგიძლიათ იხილოთ: http://vx.netlux.org/lib/ajm01.html. ამასთან დაკავშირებით, დაიწერა ფანტასტიკური რომანი ჯონ ბრუნერის მიერ, რომელშიც აღწერილია ვირუსის თავისუფალი მოძრაობა კიბერნეტიკულ სივრცეში.

[15] შპიონი ვირუსის შესახებ , იხილეთ ჰაკპორტის „ვირუსი – შპიონი, კომპიუტერული დანაშაული და უსაფრთხოება.

[16] იხილეთ სიებერის, ევროსაბჭოს ორგანიზებული დანაშაულის შესახებ ანგარიში, 2004, გვ.65

[17] ეს ვირუსი მიზნად ისახავს მიუწვდომელი გახადოს კომპიუტერული სისტემა. უამრავი კომუნიკაციის მოთხოვნით გადატვირთვის გამო, იგი ვერ ახერხებს ლეგიტიმურ ტრაფიკზე პასუხს. დამატებითი ინფორმაციისათვის, იხილეთ: http://www.us-cert.gov/cas/tips/ST04-015.html. და http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html.

დამაზიანებელი პროგრამით, რომელიც საშუალებას აძლევს დამნაშავეებს განახორციელონ შეტევა. აღნიშნული DoS შეტევები ხორციელდება რობოტული ქსელებიდან[18] (Botnet), რაც სერიოზული შფოთვის საგანს წარმოადგენს, რადგან მისი გამოყენება შეიძლება მნიშვნელოვანი ინფრასტრუქტურის ფუნქციონირებისათვის ხელის შეშლის ან წყობიდან გამოყვანის მიზნით.

- ტექნიკის არადანიშნულებით გამოყენება. დამნაშავეები იყენებენ იმ ინსტრუმენტებს, რომლებიც არსებობს ინტერნეტში და რომლის საშუალებით შეუძლიათ ჩაიდინონ კომპიუტერული დანაშაული.[19] ასეთ ინსტრუმენტებად მოიაზრება კომპიუტერული ვირუსების შექმნის საშუალებები, თვითგავრცელებადი ვირუსი და სხვა, რომლებიც გამოიყენება კომპიუტერულ სისტემაში უკანონო შეღწევის, ინფორმაციის მიღების, მონაცემთა განადგურების, რობოტი ქსელების ან "ფიშინგ" გვერდების შექმნის მიზნით. ხშირად, ასეთი ინსტრუმენტების შექმნა, გაყიდვა, შეძენა, იმპორტი, გავრცელება ან მათი სხვა სახით ხელმისაწვდომობა გახლავთ დანაშაულის მოსამზადებელი ეტაპი.

2.2.2. კომპიუტერის საშუალებით ჩადენილი დანაშაული – გაყალბება და თაღლითობა

ამ კატეგორიაში შედის კომპიუტერის საშუალებით ჩადენილი გაყალბება და თაღლითობა.

რეალურ სამყაროში არსებული გაყალბების მსგავსად, საინფორმაციო და ტექნოლოგიური საშუალებები იძლევა კომპიუტერული მონაცემებით მანიპულირების უამრავ შესაძლებლობას ისეთი ფორმით, რომ არააუთენტური ინფორმაცია ვიზუალურად გამოიყურებოდეს სრულიად აუთენტურად და მოხდეს მისი სამართლებრივი მიზნით გამოყენება. საინფორმაციო ტექნოლოგიური საშუალებები, ასევე, ამრავლებს თაღლითობის შესაძლებლობებს, რაც ნიშნავს კომპიუტერული მონაცემებით მანიპულაციის ან კომპიუტერის სისტემაში ჩარევის[20] შედეგად ერთი ადამიანის მიერ ქონების დაკარგვას და, შესაბამისად, დამნაშავეების ეკონომიკურ სარგებელს.

---

[18] ბოტნეტი არის დავირუსებული კომპიუტერებს ჯგუფი, რომელთა პროგრამებიც გარედან იმართება. დამატებითი ინფორმაციისათვის, იხილეთ: ბოტნეტები, კომპიუტერული დანაშაული და კიბერტერორიზმი: დაცვის სუსტი ადგილები და პოლიტიკის საკითხები კონგრესისათვის, 2007, გვ4: http://www.fas.org/sgp/crs/terror/RL32114.pdf.

[19] გამოყენებული ინსტრუმენტების შესახებ, იხილეთ: ელაი- „სიახლეები ჰაკერული შეტევების სფეროში: ტიპების, მეთოდების, ინსტრუმენტების და პრევენციის გზების ზოგადი მიმოხილვა: http://www.212cafe.com/download/e-book/A.pdf. ფასთან დაკავშირებით (200-500 ამერიკული დოლარი), იხილეთ: http://www.mcafee.com/us/threat_center/white_paper.html.
გამოყენებული ინსტრუმენტების შესახებ, იხილეთ: ელაი- „სიახლეები ჰაკერული შეტევების სფეროში: ტიპების, მეთოდები, ინსტრუმენტების და პრევენციის გზების ზოგადი მიმოხილვა: http://www.212cafe.com/download/e-book/A.pdf. ქილოგერების ფასთან დაკავშირებით (200-500 ამერიკული დოლარი), იხილეთ: http://www.mcafee.com/us/threat_center/white_paper.html.

[20] დეტალებისათვის, იხილეთ შემდეგი თავი.

ბოლო წლებში შეიმჩნევა გარკვეული ცვლილება შეტევის მასშტაბებში: ფართო და მრავალმიზნიანი შეტევები შეცვალა კონკრეტულმა შეტევებმა კონკრეტულ მომხმარებლებზე, ჯგუფებზე, ორგანიზაციებზე და საწარმოებზე. ეს განსაკუთრებით ეკონომიკურ-კრიმინალური მიზნით ხდება და მოიცავს:

- საკრედიტო ბარათთან დაკავშირებულ თაღლითობას[21]
- წინასწარ გადახდასთან დაკავშირებული თაღლითობა[22]
- ინტერნეტმარკეტინგს და საცალო თაღლითობას
- აუქციონთან დაკავშირებულ თაღლითობას[23] და მანიპულაციებს საფონდო ბირჟაზე.

2.2.3. შინაარსთან დაკავშირებული დანაშაული: ბავშვთა პორნოგრაფია, რასიზმი და ქსენოფობია

მიუხედავად იმისა, რომ ინტერნეტი შესანიშნავ საშუალებას იძლევა, რომ ადამიანებმა გამოავლინონ საკუთარი შემოქმედებითობა და გამოხატონ განსხვავებული მოსაზრებანი, იგი, ასევე, ქმნის კიბერნეტიკული სივრცის არასწორი დანიშნულებით გამოყენების საშუალებას. ინტერნეტი გახდა ის ადგილი, სადაც ხდება ბავშვების პორნოგრაფიით ვაჭრობა, რაც ნიშნავს, ინტერნეტში იმ პორნოგრაფიის განთავსებას, სადაც მასალა ასახავს ადამიანს, რომელიც ვიზუალურად არის არასრულწლოვანი (ჩანს, რომ არის არასრულწლოვანი, ან რეალურად არის ასეთი) და რომელიც მონაწილეობს აშკარა სექსუალურ სცენაში.[24] ბავშვების პორნოგრაფიასთან დაკავშირებული საქმიანობები მოიცავს მსგავსი სახის ფილმების წარმოებას, გავრცელებასა და შენახვას.

არაკანონიერი შინაარსის მასალა ინტერნეტში არ შემოიფარგლება ბავშვების პორნოგრაფიით. რადიკალური ჯგუფები იყენებენ მასობრივი კომუნიკაციის საშუალებებს, მათ შორის ინტერნეტს,

---

[21] ამ საკითხთან დაკავშირებით, იხილეთ მომხმარებლებთან დაკავშირებული თაღლითობა და ქურდობის საჩივრების მონაცემები, 2005 წლის დეკემბერი, ფედერალური სავაჭრო კომისია, 2006, გვერდი 3: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

[22] ტერმინი აღწერს დანაშაულს, რომლის დროს დამნაშავე არწმუნებს სამიზნე პირს, გადაიხადოს მცირე თანხა დიდი თანხის მიღების იმედით. დამატებითი ინფორმაციისათვის იხილეთ რეიჰის წინასწარ გადახდასთან დაკავშირებული თაღლითობა ქვეყნის შიგნით დამ ის გარეთ, კომპიუტერული დანაშაული და უსაფრთხოება, გვ.1, სმიტი, ჰოლმსი, კაუფმანი. ასევე, ნიგერიის წინასწარი გადახდებით თაღლითობა, მიმართულებები და საკითხები სისხლის სამართალში, #121:http://www.aic.gov.au/publications/tandi/ti121.pdf; *ორიოლა*, თაღლითობა წინასწარი გადახდით: ნიგერიის მარეგულირებელი პასუხი, "კანონი კომპიუტერების შესახებ და უსაფრთხოების ანგარიში", ტომი 21, ხანდაზმულობის კომიტეტი, 2004, გვ. 7: http://www.ftc.gov/os/2004/03/bealsfraudtest.pdf

[23] ტერმინი, აუქციონთან დაკავშირებული თაღლითობა აღწერს თაღლითურ საქმიანობას, რომელიც მოიცავს ელექტრონულ აუქციონს ინტერნეტის საშუალებით. ამასთან დაკავშირებით იხილეთ, ბაიყელი. ოპენჰეიმის თაღლითობა ინტერნეტით წარმოებულ აუქციონებზე: http://www.aslib.co.uk/proceedings/protected/2001/jul-aug/03.pdf; *შნაიდერის* ინტერნეტ-აუქციონის თაღლითობა: აკეთებენ თუ არა აუქციონები ყველაფერს იმისათვის, რომ თვიდან აიცილონ თაღლითობები? ფედერალური კანონმდებლობის კომუნიკაციის ჟურნალი, 52 (2), გვ.453; *ჩალუ/ფალოუსტოსი*, თაღლითობის გამოვლენა ინტერნეტოთ აუქციონის მოწყობის დროს: http://www.cs.cmu.edu/~dchau/papers/chau_fraud_detection.pdf; დოლანი, ინტერნეტ-აუქციონთან დაკავშირებული თაღლით ბა: ჩუმი მსხვერპლები, ეკონომიკური დანაშაულის მართვის ჟურნალი, ტომი. 2, ნომერი 1 https://www.utica.edu/academic/institutes/ecii/publications/articles/BA2DF0D2-D6ED-10C7-9CCB88D5834EC498.pdf.

[24] გავრცელების საშუალებებთან დაკავშირებით, იხილეთ უორტლეი, სმოლბოუნის ბავშვების პორნოგრაფია ინტერნეტში. გვ.10

პროპაგანდის[25] მიზნით. ვებგვერდების რაოდენობა, სადაც მოცემულია რასისტული განცხადებები და სიძულვილის შემცველი გამოსვლები, მუდმივად იზრდება ბოლო წლების განმავლობაში.[26]

ევროსაბჭო ამ საკითხებს აგვარებს კომპიუტერული დანაშაულის შესახებ პროტოკოლის საშუალებით: ქსენოფობია და რასიზმი კომპიუტერული სისტემების საშუალებით, 1986.[27]

2.2.4. ინტელექტუალურ საკუთრებასთან და მსგავს უფლებებთან დაკავშირებული დანაშაული

ციფრული ტექნიკის გამოჩენამ მუსიკის, ვიდეო-ფილმებისა და წიგნების გავრცელებაში გზა გაუხსნა საკუთრების უფლების დარღვევის ახალ ფორმებს. ფაილების გაცვლა-გაზიარების სისტემები, რაც საშუალებას აძლევს მომხმარებლებს ერთმანეთს გაუზიარონ საკუთარი ფაილები, [28] ასევე საშუალებას აძლევს მათ, შეაღწიონ ინტელექტუალური საკუთრების დაცულ ფაილებში.[29]

2.2.5. დანაშაულის კომბინაცია

ფიშინგი (იმეილები ინფორმაციის მიღების მიზნით) და პერსონალური იდენტობის მოპარვა

აღსანიშნავია, რომ ყველა დანაშაული ვერ თავსდება ზემოაღნიშნული ოთხი კატეგორიიდან ერთ-ერთის ქვეშ, რადგან მათი შემადგენლობა იმ მახასიათებლებზე მეტია, ვიდრე ერთი რომელიმე კატეგორია მოიცავს. ერთ-ერთი მაგალითი არის "ფიშინგი".[30] ეს დანაშაული აღწერს ქმედებებს, რომელიც აიძულებს მსხვერპლს, გაამჟღავნოს საკუთარი/საიდუმლო ინფორმაცია.[31] ყველაზე ხშირად გავრცელებული ფიშინგის დროს, დამნაშავეები უკავშირდებიან მსხვერპლს იმეილის საშუალებით, ეუბნებიან, რომ წარმოადგენენ ლეგალურ კომპანიას და ცდილობენ ისეთი ინფორმაციის მიღებას, რომელიც დაეხმარება მათ დანაშაულის ჩადენაში. ეს შეიძლება იყოს კომპიუტერის საშუალებით ჩადენილი

---

[25] რადიკალურმა ჯგუფებმა აშშ-ში აღიარეს ინტერნეტის უპირატესობები თავიანთი მიზნების აღსრულებაში. იხილეთ, მარკოფის ზოგი კომპიუტერული საუბარი ცვლის ადამიანების კონტაქტს, ნიუ-იორკ თაიმსი, 13.15.90

[26] სიბერი, ევრიკავშირის ანგარიში ორგანიზებული დანაშაულის შესახებ, 2004; გვ.138

[27] იხილეთ, www.coe.int/cybercrime

[28] რჩეული უნივერსიტეტების იუწყებიან საპატენტო უფლებების დარღვევების შემცირებისაკენ საქმიანობის შესახებ: http://www.gao.gov/new.items/d04503.pdf. რიპეანუ/ფოსტერი/იამნიფტი: გნუტელას ქსელის რუქის შედგენა, ერთგვარი სისტემების მახასიათებლები და სისტემის შემუშავების დეტალები" http://people.cs.uchicago.edu/~matei/PAPERS/ic.pdf. აშშ ფედერალური ვაჭრობის კომისია, გაზიარების ტექნოლოგია: მომხმარებლების დაცვა და კონკურენციის საკითხები; გვ. 3: http://www.ftc.gov/reports/p2p05/050623p2prpt.pdf; საროიუ/გუმადი.გრიბელი: ფაილების გაზიარების სისტემა: http://www.cs.washington.edu/homes/gribble/papers/mmcn.pdf.

[29] 2005 წელს, 1.8 მომხმარებელმა გამოიყენა გნუტელა. იხილეთ მენეკი: http://www.slyck.com/news.php?story=814.

[30] ფიშინგთან დაკავშირებით, იხილეთ დჰამიჯა/ტაიგერი/ჰერსტი – რატომ მუშაობს ფიშინგი:: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; "ანგარიში ფიშინგზე", ანგარიში კანადის საჯარო უსაფრთხოებისა და გადაუდებელი მზადყოფნის საქმეთა მინისტრს და აშშ გენერალურ პროკურორს, 2006:: http://www.usdoj.gov/opa/report_on_phishing.pdf.

[31] ტერმინი ფიშინგი დასაწყისში ნიშნავდა ემეილების გამოყენებას მომხმარებლის კოდური სიტყვისა და ფინანსური მდგომარეობის გაგების მიზნით. იხილეთ ფიშინგის გააზრება და მისთვის ხელის შეშლა: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

გაყალბება, თაღლითობა და სავაჭრო ნიშნებთან დაკავშირებული დარღვევები.

ამასთან დაკავშირებული მაგალითი გახლავთ "იდენტობის მოპარვა"[32]. ეს ტერმინი ეხება იდენტობასთან დაკავშირებული ინფორმაციის მოპოვებას და გადაცემას, ან იდენტობასთან დაკავშირებული ინფორმაციის გამოყენებას მესამე პირის მიერ ან სინთეტური იდენტობის გამოყენებას კრიმინალურ კონტექსტში; ასევე, კრიმინალურ დანაშაულს, რომელიც ჩადენილია იდენტობის გამოყენებით (როგორიც არის თაღლითობა)[33].

კომპიუტერული დანაშაულის ორგანიზება

საინფორმაციო ტექნოლოგიური საშუალებები ხელს უწყობს სისხლის სამართლის ორგანიზებულ დანაშაულებრივ საქმიანობებს. თუმცა, აღსანიშნავია, რომ კომპიუტერული დანაშაულის ბუნება საკმაოდ შეიცვალა ბოლო წლებში. კომპიუტერული დანაშაულის ცენტრმა არაორგანიზებული შეტევებიდან კრიმინალურ დანაშაულებებზე გადაინაცვლა, რაც კომპიუტერული დანაშაულის ორგანიზებულობის სინქრონულად ხდება.

კომპიუტერული დანაშაულისათვის ორგანიზება ნიშნავს ტრადიციული ორგანიზებული დანაშაულის ელემენტებს დამატებული კომპიუტერის საშუალებით განხორციელებული თაღლითობა და გაყალბება, ინტელექტუალური საკუთრების წინააღმდეგ ჩადენილი დანაშაული, მონაცემებსა და სისტემაში ჩარევა/შეღწევა (ბოტნეტების გამოყენება) და სხვა საქმიანობა.

- იმდენად, რამდენადაც ეკონომიკური დანაშაული ორგანიზებული დანაშაულის მთავარი საქმიანობა გახდა, საინფორმაციო ტექნოლოგიური საშუალებები ხელს უწყობს ისეთი დანაშაულების ჩადენას, როგორიცაა საკრედიტო ბარათებთან და ფასიან ქაღალდებთან დაკავშირებული სქემები (pump-and-dump) და სხვა სახის მაქინაციები, ფულის გათეთრება, ყალბი მონეტების გამოშვება ან იდენტობის მოპარვასთან დაკავშირებული

[32] იდენტობის მოპარვასთან დაკავშირებით, იხილეთ: ჩაუკი/აბდელი/ უაჰაბი, იდენტურიბის მოპარვა კიბერსიბვრცეში: პრობლემების და მათი მოგვარება, Lex Electronica. ტომი. 11, No. 1, 2006; კეტონი, იდენტობის კულტურული ფენომენი, სამეცნიერო ტექნოლოგიების ბიულეტენი, 2007, ტომი. 27, 2008, გვერდი 11; ელსტონი/შტეინი, საერთაშორისო თანამშრომლობა იდენტობის მოპარვის გამოძიებასთან დაკავშირებით: იმედიანი მომავალი და ფრუსტრაციული აწმყო: http://www.isrcl.org/Papers/Elston%20and%20Stein.pdf; *ემპი*, იდენტობის მოპარვის ტექნოლოგიები და კონტრღონისძიებები, 2005; *ჰალპერინი*, იდენტობა კვლევის ახალი თემა, Datenschutz und Datensicherheit, 2006, გვ. 533; *კუპსი/ლინესი*, იდენტობის მოპარვა, იდენტობასთან დაკავშირებული მაქინაცია და დანაშაული, Datenschutz und Datensicherheit, 2006, გვ.553 et seq.; ლევი, იდენტობისა და სხვა სახის დანაშაულის დამარცხება გაერთიანებულ სამეფოში; ანალიტიკური ისტორია, გამოქვეყნებულია მაკნელი/ნიუმენი, იდენტობის მოპარვის პერსპექტივა; *ვან დერ მოლენი*, იდენტობის მოპარვის წინააღმდეგ: ბოლოდროინდელი სიტუაცია აშშ-ში, გაერთიანებულ სამეფოსა და ევროკავშირში.

[33] ჰერკე, იდენტობის მოპარვა ინტერნეტის საშუალებით 2007: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_co-operation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

მაქინაციები და ტრადიციული დანაშაულის სხვა თანამედროვე ფორმები, როგორიცაა ბანკების ელექტრონული გაქურდვა და კომპიუტერული გამოძალვა.

- კონტაქტების დეპერსონალიზაცია, ადვილი შეღწევა სისტემაში და ელექტრონული გადარიცხვების სისწრაფე, საკმაოდ მომხიბვლელს ხდის საინფორმაციო ტექნოლოგიებს ფულის გათეთრების მიზნით. ვირტუალური კაზინოები, აუქციონები, სმარტ ბარათები, ელექტრონული საბანკო მომსახურება და ინტერნეტის საშუალებით აქციების, ფასიანი ქაღალდებისა და ფიუჩერსების ყიდვა-გაყიდვა ფულის გათეთრების შესანიშნავ საშუალებებს ქმნის.
- ორგანიზებული დანაშაული იყენებს საზოგადოების, საჯარო ინსტიტუტების, ბიზნესის სექტორის და ინდივიდების გახსნილობას მათ მიერ ინტერნეტის გამოყენების გზით. არა მხოლოდ კორპორაციები, რომლებიც მონაწილეობენ ელექტრონულ ოპერაციებში და სხვა ბიზნესოპერაციებში, არამედ ინდივიდებიც, რომლებიც იყენებენ ინტენეტბანკის მომსახურებას ან მონაწილეობენ ინტერნეტბიზნესში, ხდებიან ელექტრონული გაქურდვის და ფიშინგის მსხვერპლნი. მსხვერპლთა ჯგუფში შედიან ბავშვებიც, როგორც საზოგადოების ყველაზე დაუცველი ნაწილი.
- საინფორმაციო ტექნოლოგიური საშუალებები იძლევა ანონიმურობის საშუალებას, ააღვილებს ლოჯისტიკას და ამცირებს წარმატებული გამოძიების შანსებს. იგი იძლევა საშუალებას, დისტანციურად განხორციელდეს ოპერაციები, საიდუმლო გარიგებები, გადაზიდვის ოპერაციები, ქსელური კავშირები და კომუნიკაცია.
- საინფორმაციო ტექნოლოგიური საშუალებანი არის ინსტრუმენტი, რომელიც დამნაშავეებს ეხმარება გლობალურ კომუნიკაციაში და პოტენციური მსხვერპლის მოძებნაში. ამის მაგალითია ნიგერიული თაღლითობის სქემა, რომელიც გავრცელდა ინტერნეტის საშუალებით, რომელიც ითვალისწინებდა პატარა თანხის წინასწარ გადარიცხვას დიდი თანხის მიღების იმედით.
- ბოტნეტების საშუალებით შესაძლებელია დიდი რაოდენობის კომპიუტერების წყობიდან გამოყვანა და მათი ზომბებად გადაქცევა, რაც ითვალისწინებს კომპიუტერების დისტანციურ მართვას დამნაშავეების მიერ, რაც ორგანიზებული დანაშაულის ინსტრუმენტს წარმოადგენს.

საინტერესოა, თუ როგორ ცვლიან საინფორმაციო ტექნოლოგიები ორგანიზებული დანაშაულის ფორმას, ანუ იმას, თუ როგორ ემზადებიან ადამიანები დანაშაულის ჩასადენად. კომპიუტერული დანაშაულისათვის არ არის საჭირო გეოგრაფიული ტერიტორიის გაკონტროლება, ჭირდება ნაკლები დოზით პიროვნული კონტაქტი და, შესაბამისად, ნაკლები ურთიერთობა, რომელიც ეფუძნება ნდობას და დისციპლინას დამნაშავეების ორგანიზებულ დაჯგუფებაში, ანუ მცირდება ორგანიზაციის არსებობის საჭიროება. სხვათა შორის, ორგანიზებული დანაშაულებრივი ჯგუფების კლასიკური სტრუქტურა შეუფერებელიც კი არის ინტერნეტ დანაშაულისათვის. საინფორმაციო ტექნოლოგიები უპირატესობას

ანიჭებს ქსელურ მუშაობას, მან შესაძლოა შეცვალოს დამნაშავეების ბუნება. რეალურ სამყაროში, ლეგალური ბიზნესმენები ერთვებიან ეკონომიკურ დანაშაულში; საინფორმაციო ტექნოლოგიებისადმი ცოუნებამ, შესაძლოა, გამოიწვიოს მათი მონაწილეობა ორგანიზებული დანაშაულის ფორმებში, ანუ გახდნენ ორგანიზებული კომპიუტერული დამნაშავეები.

ინტერნეტის გამოყენება ტერორისტების მიერ

კომპიუტერული დანაშაულის კიდევ ერთი სახე, რომელიც იყენებს დანაშაულის სვადასხვა კატეგორიას არის საინფორმაციო ტექნოლოგიების გამოყენება ტერორისტების მიერ. მიუხედავად იმისა, რომ ტერმინი "კომპიუტრული დანაშაული" გარკვეულად წინააღმდეგობრივია, მაინც ცხადია, რომ ტერორისტები იყენებენ საინფორმაციო ტექნოლოგიებს საკუთარი საქმიანობისათვის, მაგალითად:

- პროპაგანდა: თუ 1998 წელს აშშ სახელმწიფო დეპარტამენტის მონაცემთა ბაზაში[34] არსებული უცხოური ტერორისტული ორგანიზაციებიდან მხოლოდ თორმეტს ჰქონდა საკუთარი ვებგვერდი, 2004 წელს ეს თითქმის ყველას აქვს, მათ შორის, ჰამასს, ჰაზბულაჰს, პკკ-ს და ალ-ქაიდას.[35] გარდა ვებგვერდებისა, ტერორისტებმა დაიწყეს ელექტრონული კომუნიკაცია პროპაგანდისა[36] და ვიდეო-მასალების გავრცელების მიზნით.
- ინფორმაციის შეკრება: ელექტრონული საშუალება საკმაოდ კარგი ინსტრუმენტია პოტენციურ მსხვერპლთა შესახებ ინფორმაციის მოსაძიებლად.[37] დღეისათვის, მაღალი სიზუსტის სატელიტური ფოტოები, რომლებიც რამდენიმე წლის წინ მხოლოდ სპეციალურ სამხედრო განაყოფებს შეეძლოთ ქონოდათ, თავისუფლად არის განთავსებული ინტერნეტში.[38] გარდა ამისა, ინტერნეტში განთავსებულია ბომბების შექმნის შესახებ ინფორმაციისა და იარაღის გამოყენების ვირტუალური ბაზების გვერდები.[39] კონფიდენციალური ინფორმაცია, რომელიც არ არის სათანადოდ დაცული მაძებარი რობოტებისაგან, შეიძლება მოპოვებული იქნეს მაძიებელი სისტემის საშუალებით.[40] 2003 წელს, აშშ თავდაცვის დეპარტამენტმა

[34] განახლება ტერორიზმის შესახებ, 1998: http://www.adl.org/terror/focus/16_focus_a.asp.

[35] ვეიმანის ანგარიში, როგორ იყენებენ ტერორისტები ინტერნეტს, 2004, გვ.3; ინტერნეტის პროპაგანდის მიზნით გამოყენებისათვის, იხილეთ გრილის საინფორმაციო ომი, ახალი ბრძლოა: ტერორიზმი, პროპაგანდა და ინტერნეტი, ტ.53; №7 (2001), გვ.253

[36] ტერორისტების მიერ იუ ტუ ბის-ს გამოყენების შესახებ, იხილეთ ჰეიზის ახალი ამბები, 11 ოქტომბერი, 2006: http://www.heise.de/newsticker/meldung/79311; *Staud* in Sueddeutsche Zeitung, 05.10.2006.

[37] დაკავშირებულ გამოწვევებთან, იხილეთ: კომპიუტერულ დანაშაულთან ბრძოლის გამოწვევები. 2008, გვ.292.

[38] ლევინი, გლობალური უსაფრთხოება, 27.06.2006: http://www.globalsecurity.org/org/news/2006/060627-google-earth.htm.; 'Google Earth: Neues chinesisches Kampf-Uboot entdeckt', 11.07.2007, available at http://www.derstandard.at/?url/?id=2952935.

[39] შემდეგი ინფორმაციისათვის იხილეთ ჰერკეს: ბრძოლა კომპიუტერული დანაშაულის წინააღმდეგ, მულტიმედია და რეჰტი, 2008, გვ.292.

[40] დამატებითი ინფორმაციისათვის საიდუმლო ინფორმაციის მოძიების საქმეში, იხილეთ ლონგი, სკოული დავან ეიჯკელენბორგი, გუგლის ჰაკერობა და შედწევის ტესტერები.

მიიღო ინფორმაცია ალ-ქაიდას ტრენინგის სახელმძღვანელოს შესახებ, სადაც აღწერილი იყო, თუ როგორ უნდა გამოიყენოთ საჯარო წყაროები პოტენციური სამიზნეების შესახებ ინფორმაციის მოპოვების მიზნით.[41]

- ინფორმაციის მიწოდება: ონლაინ მომსახურება შეიძლება გამოყენებული იქნეს სატრენინგო მასალის გავრცელების მიზნით, როგორიცაა ინსტრუქციები იარაღის გამოყენებისა და სამიზნეს შერჩევის შესახებ. ასეთი მასალა ხელმისაწვდომია ინტერნეტში.[42] 2008 წელს აღმოჩენილი იქნა ინტერნეტ სერვერი, რომლის საშუალებით ვრცელდებოდა სატრენინგო მასალა და ხდებოდა კომუნიკაცია ტერორისტებს შორის.[43] ასევე, ფუნქციონირებდა სხვადასხვა ვებგვერდი ტერორისტების საქმიანობების კოორდინაციის მიზნით.[44]
- კომუნიკაცია: 9/11 თავდასხმის შემდეგ, ცნობილი გახდა, რომ საკუთარი შეტევის კოორდინაციის მიზნით[45] ტერორისტებმა გამოიყენეს იმეილი. პრესაში გაჩნდა ინფორმაცია სამიზნეებზე დეტალური ინსტრუქციების შესახებ და იმეილების რაოდენობაზე, რომელიც მოძიებული იქნა ინტერნეტით.[46]
- ტერორისტების დაფინანსება: ტერორისტული ორგანიზაციების დიდი რაოდენობა დამოკიდებულია მესამე მხარისაგან მიღებულ დაფინანსებაზე. ასეთი ფინანსური ოპერციების კვალის აღმოჩენა ტერორიზმის წაინაღმდეგ ბრძოლის ერთ-ერთი მნიშვნელოვანი კომპონენტო გახდა, განსაკუთრებით, 9/11 თავდასხმის შემდეგ. ამ თვალსაზრისით, ერთ-ერთი დიდი პრობლემა არის ის, რომ არ არის აუცილებელი, ტერორისტული შეტევებისათვის საჭირო ფინანსური რესურსები უაზარმაზარი ოდენობის[47] იყოს. ტერორისტების დაფინანსების მიზნით არსებობს ინტერნეტის მომსახურების გამოყენების ორი გზა:

---

[41] საჯარო წყაროების გამოყენებით ისე, რომ არ გამოიყენო არაკანონიერი საშუალებები, შესაძლებელია მტერზე ინფორმაციის 80% მოძიება, იხილეთ კონვეის ინტერნეტის გამოყენება ტერორისტების მიერ, ინფორმაცია და უსაფრთხოება, 2006, გვ.17.

[42] ბრუნსტი, კომპიუტერული ტერორიზმი, ინტერნეტის გამოყენება ტერორისტული მიზნებისათვის, ევროკავშირის გამომცემლობა, 2007; აშშ უსაფრთხოების მრჩეველთა საბჭო, ტერორიზმთან ბრძოლის ჯგუფის ანგარიში, იანვარი 2008, გვ.5, შტენერსენი, ინტერნეტი: ვირტუალური ტრენინგის ბანაკი? ტერორიზმი და პოლიტიკური ძალადობა, 2008, გვ.215.

[43] მუშარბაში, ბინ ლადენის ნტრანეტი, შპიგელი, ტომი39, 2008, გვ.127.

[44] ვეიმანი, როგორ იყენებს ტერორიზმი ინტერნეტს, აშშ მშვიდობის 116 ინსტიტის სპეცილური ანგარიში, 2004, გვ.10

[45] 9/11 კომისიის ანგარიში, ნაციონალური კომისიის საბოლოო ანგარიში აშშ-ზე განხორციელებული თავდასხმის შესახებ, 2007; გვ.249

[46] საბოლოო გზავნილის ტექსტი იყო ასეთი: „სემესტრი იწყება სამ კვირაში. ჩვენ გვაქვს 19 დადასტურება იურიდიულ ფაკულტეტზე, ურბანული დაგაგმარების ფაკულტეტზე, სახვითი ხელოვნების ფაკულტეტზე და საინჟინრო ფაკულტეტზე კვლევის ჩატარების შესახებ. ფაკულტეტების სახელი იყო სხვადასხვა სამიზნეების კოდი. დეტალებისათვის, იხილეთ ვეიმანი, როგორ იყენებს ტერორიზმი ინტრნეტს, საერთაშოროისო უსაფრთხოების ჟურნალი, 2005 წლის გაზაფხული, №8; თომასი, ალ ქაედა და ინტერნეტი: კომპიუტერული დაგეგმვის საშიშროება, 2003, იხილეთ:
http://findarticles.com/p/articles/mi_m0IBR/is_1_33/ai_99233031/pg_6; ზელერი, ღია ინტერნეტი, ბნელი გზების ქსელი, ნიუ-იორკ თაიმსი, 20.12.2004, იხილეთ:
http://www.nytimes.com/2004/12/20/technology/20covert.html?
pagewanted=print&position=;.

[47] 9/11-ის გამომძიებელმა კომისიამ დაითვალა, რომ შეტევის ხარჯები იყო დაახლოებით 400 000 500 000 აშშ დოლარი, იხილეთ კომისიის ანგარიში, გვ.187. ანგარიშის მომზადების ხანგრძლიობისა და მონაწილე პირების რაოდენობის გათვალისწინებით, ხარჯი იყო მცირე. ასევე, იხილეთ კონგრესის კვლევის სამსახურის მიერ მომზადებული ანგარიში- ტერორისტების დაფინანსება: 9/11 კომისიის რეკომენდაციები, გვ.4.

- ტერორისტულ ორგანიზაციებს შეუძლიათ ელექტრონული გადახდის სისტემის გამოყენება ონლაინ რეჟიმში, [48] ან ინფორმაციის გამოქვეყნება, თუ როგორ უნდა მოხდეს თანხის გადარიცხვა.[49]
- მათი აღმოჩენის თავიდან აცილების მიზნით, ტერორისტული ორგანიზაციები ცდილობენ გაასაიდუმლონ საკუთარი ქმედებები და ამისათვის საქმეში რთავენ სუფთა (ეჭვმიუტანელ) მოთამაშეებს, როგორიცაა საქველმოქმედო ორგანიზაციები. კიდევ ერთი გზა გახლავთ ყალბი ვებ-მაღაზიების არსებობა.

➢ ტრენინგი რეალურ სამყაროზე შეტევის განხორციელების თვალსაზრისით: ანგარიშები მეტყველებენ იმაზე, რომ ტერორისტები იყენებენ ინტერნეტ თამაშებს, რათა მოემზადონ რეალური შეტევებისათვის. [50] არსებობს სხვადასხვა ინტერნეტ თამაშები, რომლებიც იძლევა რეალური სამყაროს სიმულაციის საშუალებას. ასეთი თამაშების მომხმარებელს, შეუძლია პერსონაჟის (ავატარის) გამოყენება ვირტუალურ სამყაროში. თეორიულად, ასეთი ინტერნეტ თამაშების გამოყენება შესაძლებელია შეტევის სიმულაციის მიზნით, მაგრამ არ არის ცნობილი, რა დონეზეა მათი გამოყენება.[51]

➢ ინტერნეტ-შეტევები მნიშვნელოვან ინფრასტრუქტურაზე: მნიშვნელოვანი (საინფორმაციო) ინფრასტრუქტურა ხშირად ხდება ტერორისტების სამიზნე, რადგან იგი სასიცოცხლო მნიშვნელობის არის სახელმწიფოს სტაბილურობის თვალსაზრისით.[52] ინფრასტრუქტურა ითვლება მნიშვნლოვნად, რადგან მის უუნარობას და უფუნქციობას შედეგად მოაქვს ქვეყნის ეკონომიკური უსაფრთხოებისა და თავდაცვის უნარის დაქვეითება.[53] ეს ეხება ელექტროენერგიის, ტელეკომუნიკაციის, გაზისა და ნავთობის საწყობის, ტრანსპორტირების, საბანკო და საფინანსო, წყლის და სასწრაფო დახმარების სისტემებს. სამოქალაქო არეულობის დონე, რომელიც გამოიწვია ქარშხალმა კატრინა, ნათელყოფს საზოგადოების დამოკიდებულების დონეს ასეთი მომსახურებისადმი ხელმისაწვდომობაზე.[54]

---

[48] ამავე კონტექსტში იხილეთ გრილის საინფორმაციო ომი: ახალი ბრძოლის ველი ტერორისტები, პროპაგანდა და ინტერნეტი, ტ.53, №7 (2001), გვ.253.

[49] ვეიმანი აშშ ინტერნეტის პროტოკოლოს ანგარიშში: როგორ იყენებენ ტერორისტები ინტერნეტს, 2004, გვ.7, ასევე, იხილეთ კონვეი – ტერორისტების მიერ ინტერნეტის გამოყენებადა როგორ ვებრძოლოთ მათ, ინფორმაცია და უსაფრთხოება, 2006, გვ.4.

[50] იხილეთ აშშ კომისიის ანგარიში უსაფრთხოებასა და თანამშრომლობაზე, 15.05.2008: http://csce.gov/index.cfm?FuseAction=ContentRecords.
ViewTranscript&ContentRecord_id=426&ContentType=H,B&ContentRecord
Type=B&CFID=18849146&CFTOKEN=53; obraieni, ვირტუალური ტერორისტები, ავსტრალია, 31.07.2007, http://www.theaustralian.news.com.au/story/
0,25197,22161037-28737,00.html;

[51] ტერორისტების სხვა საქმიანობასთან დაკავშირებით იხილეთ ჩენ/ტომასის კიბერექსტრემიზმი ქსელებში 2.0 – განმარტებითი კვლევა საერთაშორისო ჯიჰადის ჯგუფის შესახებ; დაზვერვა და უსაფრთხოების ინფორმატიკა, 2008, გვ.98.

[52] ბრუნსტი, კიბეტერორიზმი – ინტერნეტის გამოყენება ტერორისტული მიზნებისათვის, ევროსაბჭოს პუბლიკაცია, 2007.

[53] აშშ აღმასრულებელი ბრძანება 13010 – კრიტიკული ინფრასტრუქტურის დაცვა, ფედერალური რეესტრი, 1996, 17 ივლისი, ტ.61, №138.

[54] კრიტიკული ინფრასტრუქტურის დაცვა: სექტორული გეგმები და სექტორული საბჭოები აგრძელებენ დაარსებას, მთავარი საბიუჯეტო კონტროლის სამმართველოს კომუნიკაცია, 2007, 17 ივლისი: http://www.gao.gov/
new.items/d07706r.pdf.

საინფორმაციო ტექნოლოგიებზე სერიოზული დამოკიდებულება კიდევ უფრო დაუცველს ხდის მნიშვნელოვან ინფრასტრუქტურას.[55] ეს განსაკუთრებით ეხება შეტევებს ურთიერთდაკავშირებულ სისტემებზე, რომლებსაც აკავშირებს კომპიუტერი და საკომუნიკაციო ქსელები.[56] მომსახურებაში უმნიშვნელო შეყოვნებამაც კი შესაძლოა გამოიწვიოს უზარმაზარი ფინანსური ზარალი არა მხოლოდ სამოქალაქო სამსახურებისათვის, არამედ სამხედრო ინფრასტრუქტურისა და მომსახურებისათვის.[57] შეტევის განხორციელების მიზნით, დამნაშავეებს შეუძლიათ ანონიმური კომუნიკაციის და დაშიფრული ტექნოლოგიების გამოყენება საკუთარი იდენტობის დაფარვის მიზნით.[58]

ამრიგად, ინტერნეტის გამოყენება ტერორისტების მიერ წარმოადგენს დანაშაულთა კომბინაციას. კომპიუტერული დანაშაულის შესახებ კონვენციის სრული განხორციელება შესაძლებლობას მისცემს ქვეყნებს, რომ მისცენ სისხლის სამართლის დანაშაულის კვალიფიკაცია საინფორმაციო ტექნოლოგიურ საშუალებებზე შეტევებს, უზრუნველყონ მტკიცებულებების არსებობა ტერორისტების მიერ გამოყენებული კომპიუტერული სისტემების შესახებ და ითანამშრომლონ საერთაშორისო დონეზე. ევროსაბჭოს კონვენცია ტერორიზმის პრევენციის შესახებ[59], აკონკრეტებს იმ ღონისძიებებს, რომლებიც დაკავშირებულია ტერორისტების დაქირავებასა და მათ მომზადებასთან ტერორისტული აქტის განხორციელების მიზნით.

2.3. გამოწვევები მოსამართლეებისათვის

2.3.1. მოსამართლის როლი

მოსამართლეები გადამწყვეტ როლს თამაშობენ კომპიუტერული დანაშაულის წინააღმდეგ ბრძოლაში. მათი მონაწილეობის გარეშე შეუძლებელი იქნებოდა დამნაშავეების გასამართლება. არსებობს სპეციფიკური საკითხები, რომლებიც კომპიუტერული დანაშაულის გამოძიების პროცესში მოსამართლეების როლს უკავშირდება:

- მიუხედავად იმისა, რომ ზოგი კომპიუტერული დანაშაული, როგორიცაა იმეილით მაქინაცია, შესაძლოა განსაზღვრული იყოს ქვეყნის სისხლის სამართლს კოდექსით, არსებობს დანაშაულის სახეები, რომლებსაც სპეციალური დებულებები ჭირდებათ. ამ

[55] სოფაიერი/გუდმენი, კიბერდანაშაული და უსაფრთხოება – ტრანსნაციონალური სივრცე, 2001: http://media.hoover.org/documents/0817999825_1.pdf.
[56] ლუისი, კიბერტერორიზმის რისკის შეფასება, კიბერ ომი და სხვა კიბერ საფრთხეებუ, სტრატეგიული და საერთაშორისო კვლევების ცენტრი, დეკემბერი, 2002
[57] შიმეალი/უილიამსი/დულნევი, კიბერომის საწინააღმდეგოდ, ნატოს მიმოხილვა, 2001/2002 წლის ზამთარი: http://www.cert.org/archive/pdf/counter_cyberwar.pdf.
[58] კომპიუტერული დახმარების სასწრაფო ჯგუფის ანგარიში, გვ.7: http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.
[59] ტერორიზმის პრევენციის კონვენცია: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=196&CM=8&DF=3/2/2009&CL=ENG.

დებულებებთან დაკავშირებით, აუცილებელია მოსამართლეებს მიეწოდოთ საჭირო ინფორმაცია, დაკავშირებული მათ ინტერპრეტაციასა და გამოყენებასთან.

- მოსამართლეების წინაშე არსებული სირთულეებიდან ერთ-ერთი უკავშირდება დროს, რომელსაც ისინი უთმობენ საქმის შესწავლა-გამოძიებას. განსხვავებით ისეთი საქმეებისა, რომლებთან დაკავშირებითაც ეროვნული კანონმდებლობა მოითხოვს სასამართლო დადგენილებას[60] კონკრეტული სახის გამოძიების საწარმოებლად, აქ მოსამართლეების ჩართვა საქმეში ხდება ბოლო ეტაპზე – სასამართლო განხილვების დროს. როგორც უკვე ავღნიშნეთ, კომპიუტერული დანაშაულის საქმეები დამოკიდებულია ელექტრონულ მტკიცებულებაზე.[61] ინტერნეტ-პროტოკოლის მისამართი ეხმარება გამომძიებლებს დაადგინონ ის მომხმარებელი, რომელმაც გააგზავნა არასამართლებრივი შინაარსის დოკუმენტი და ეჭვმიტანილის ლოგ-ფაილები შესაძლოა გამოდგეს იმის დასადგენად, თუ რომელმა მომხმარებელმა ჩაიდინა დანაშაული. ასეთი მონაცემები ფრიად ეფემერულია და ამიტომ მათი სწრაფად მოგროვებაა საჭირო. იმ დროისათვის, როცა მოსამართლეები ერთვებიან საქმეში, როგორც წესი, დამატებითი მტკიცებულების მოპოვების ძალზედ ნაკლები შანსი არსებობს. იმ დროისათვის, როც მოსამართლე მიხვდება, რომ არ აქვს ხელთ მნიშვნელოვანი მტკიცებულება, უკვე გვიან არის ასეთი შეცდომის გამოსწორება. ამიტომაც, კომპიუტერულ დანაშაულთან დაკავშირებულ საქმეებზე მოსამართლეები თითქმის მთლიანად არიან დამოკიდებულნი გამოძიების მიერ მოპოვებულ მტკიცებულებებზე.
- მოსამართლეებს და ჟიურის შემთხვევაში – ჟიურის წევრებს – უნდა შეეძლოთ, შეაფასონ ელექტრონული მტკიცებულების მნიშვნელობა ისე, რომ მონაწილეობა არ მიიღონ მტკიცებულებების მოპოვება-შეგროვებაში. როცა არ ხარ კომპიუტერის კრიმინლურ-ტექნიკური ექსპერტი, რთულია შეფასება. მიუხედავად იმისა, რომ შეფასება ნაწილობრივ შესაძლებელია დელეგირებული იქნეს სასამრთლოს ექსპერტებზე და მოწმე-ექსპერტებზე, მოსამართლეებს, რომლებიც განიხილავენ კომპიუტერულ დანაშაულთან დაკავშირებულ საქმეს, მაინც მოეთხოვებათ კომპიუტერული ექსპერტიზის ფუნდამენტური პრონციპების საბაზისო ცოდნა. ამ სახის ტრენინგის ჩატარება შედარებით ადვილია იმ ქვეყნებში[62], სადაც ფუნქციონირებს სპეციალიზებული სასამართლოები, რომლებიც განიხილავენ კონკრეტულად კომპიუტერულ დანაშაულს, ვიდრე იქ, სადაც ყოველ მოსამართლეს შესაძლოა შეხვდეს ასეთი საქმე.

2.3.2. ელექტრონული მტკიცებულების ცვალებადი ბუნება

იმეილის გაგზავნას დანართთან ერთად, რომლშიც არის ქსენოფობური მასალა ან ბავშვების მონაწილეობით პორნოგრაფიული ფილმი, წამები ჭირდება. ინფორმაციას, რომელიც

[60] სასამრთლო გადაწყვეტილებებთან დაკავშირებით კონკრეტულ გამოძიებებზე იხილეთ კონვენციის განმარტებითი ანგარიში

[61] იხილეთ თავი 4

[62] სერბეთის კანონი მაღალი ტექნოლოგიების დანაშაულის შეზღუდვის სფეროში ხელისუფლების ორგანიზაცისა და იურისდიქციის შესახებ

სამართალდამცავ ორგანოებს ესაჭიროებათ დამნაშავის ვინაობის დასადგენად – თუკი უკვე არ არსებობს მონაცემთა შენახვის შესახებ ვალდებულება – ხშირად შლიან ამ ინფორმაციის გადაცემის პროცესის დასრულებისთანავე.[63] ეს კი ძალზედ ამცირებს გამოძიებისათვის განკუთვნილ დროს.[64]

2.3.3. მომხმარებელთა რაოდენობა

ამჟამად ინტერნეტს[65] ერთ მილიარდზე მეტი მომხმარებელი ჰყავს მთელ მსოფლიოში და ეს რიცხვი სწაფად იზრდება. შესაძლო დამნაშავეთა რიცხვი მნიშვნელოვანია ქსელის საერთაშორისო განზომილების გამო: მომხმარებლების ერთმა პროცენტმაც კი რომ გამოიყენოს საინფორმაციო ტექნოლოგიები კრიმინალური მიზნით, მათი მთლიანი რაოდენობა 10 მილიონს მიაღწევს. მომხმარებელთა და ინტერნეტის ვებგვერდების რაოდენობა აჩენს კითხვას, როგორ აღმოვაჩინოთ ის ვებ-გვერდები, რომლებიც არაკანონიერ შინაარსს შეიცავს და როგორ გამოვააშკარაოთ ისინი ამდენი მოქმედი ვებ-გვერდების ფონზე? ეს გვიჩვენებს, თუ რამდენად რთულია საგამოძიებო სტრუქტურებისათვის კომპიუტერულ დანაშაულთან ბრძოლა.

2.3.4. თანამშრომლობა სამართალდამცავ ორგანოებსა და კერძო ბიზნესს შორის

კომპიუტერული დანაშაულის წინააღმდეგ ბრძოლის ეფექტიანობა მხოლოდ სათანადო კანონმდებლობის არსებობაზე არ არის დამოკიდებული. ურთიერთობა სამართალდამცავ ორგანოებსა და კერძო ბიზნესს შორის, როგორიცაა ინტერნეტ სერვისის პროვაიდერები/მიმწოდებლები კიდევ ერთი მნიშვნელოვანი ინსტრუმენტია კომპიუტერული დანაშაულის წინააღმდეგ ბრძოლაში.[66] ევროსაბჭოს გადაწყვეტილებით, ზემოაღნიშნული თანამშრომლობის გაძლიერებისა და გაუმჯობესების მიზნით 2007 წელს შემუშავებული იქნა ინსტრუქციები.[67] ინსტრუქციები ეფუძნება იმ კვლევების დასკვნებს, რომლებშიც გაანალიზდა თანამშრომლობის არსებული ფორმები.[68] 2008 წლის ევროსაბჭოს ინტერფეისის კონფერენციაზე[69] აღნიშნული ინსტრუქციები

[63] ჰერკე, 2003, ლიპსონი, კიბერშეტევების მიკვლევა და ბრძლოა, ტექნიკური გამოწვევები და გლობალური პოლიტიკის საკითხები

[64] ჰერკე, კიბერდანაშაულის წინააღმდეგ ბრძოლის ნელი გამოღვიძება, 2006

[65] ინტერნეტის მსოფლიო სტატის მიხედვით, 1.15 მილიარდზე მეტი ადამიანი იყენებს ინტერნეტს, http://www.internetworldstats.com/stats.htm.

[66] იხილეთ სამართალდამცავ ორგანოებსა და სერვის პროვაიდერებს შორის თანამშრომლობის შესახებ ევროსაბჭოს ინსტრუქციები, №3.

[67] მეტი ინფორმაციისათვის იხილეთ ჰერკე, სამართალდამცავ ორგანოებსა და სერვის პროვაიდერებს შორის თანამშრომლობის შესახებ ევროსაბჭოს ინსტრუქციები, №4.

[68] გალანანი/ჰერკე, კვლევა სამართალდამცავ ორგანოებსა და სერვის პროვაიდერებს შორის თანამშრომლობის შესახებ კიბერდანაშაულის ინააღმდეგ

[69] კონფერენციის პროგრამა იხილეთ: http://www.coe.int/t/dg1/legalco-operation/economiccrime/cybercrime/cy%20activity%20Interface2008/567%20IF08-m-programme3b%20Provisional%20%20(26%20march%2008).PDF. კონფერენციის დასკვნები იხილეთ: http://www.coe.int/t/dg1/legalco-operation/economiccrime/cybercrime/cy%20activity%20Interface2008/567_IF08-d-concl1c.pdf..

დამტკიცებული იქნა, როგორც არაფორმალური, არასავალდებულო ინსტრუმენტი.[70]

2.3.5. საერთაშორისო სივრცე

მონაცემების გადაცემის პროცესი, როგორც წესი, ერთზე მეტ ქვეყანას მოიცავს.[71] ეს გახლავთ ქსელის დიზაინისა და პროტოკოლის შედეგი, რომელიც მაშინაც კი წარმატებით ახორციელებს მონაცემთა გადაცემას, როცა პირდაპირი ხაზები დროებით დაბლოკილია.[72] გარდა ამისა, ინტერნეტ მომსახურების დიდ რაოდენობას (მაგალითად ინფორმაციის განთავსების მომსახურებას/ჰოსთინგ მომსახურება) საზღვარგარეთ განთავსებული კომპანიები გვთავაზობს.[73]

იმ შემთხვევაში, როცა დამნაშავე არ იმყოფება იმ ქვეყანაში, სადაც პოტენციური მსხვერპლია, გამოძიებისათვის საჭიროა თანამშრომლობა იმ ქვეყნების სამართალდამცავ ორგანოებს შორის, რომელ ქვეყნებზეც ხდება ინფორმაციის მოძრაობა.[74] თანამშრომლობა სხვადასხვა ქვეყნებს შორის კომპეტენტური ორგანოების თანხმობის გარეშე რთულია ქვეყნის სუვერენიტეტის პრონციპიდან გამომდინარე. ეს პრინციპი არ აძლევს უფლებას ერთ ქვეყანას, განახორციელოს საგამოძიებო ქმედებები მეორე ქვეყანაში ამ ქვეყნის ხელისუფლების თანხმობის გარეშე.[75] ამგვარად, გამოძიების მიზნებისათვის, საჭიროა ყველა ჩართული მხარის/ქვეყნის ხელისუფლების დახმარება და მონაწილეობა.

იმის გათვალისწინებით, რომ ეფექტიანი გამოძიებისა და ელექტრონული მტკიცებულების მოსაპოვებლად, როგორც წესი, დრო მცირეა, ჩვეულებრივი თანამშრომლობის რეჟიმის გამოყენება არ არის საკმარისი. კომპიუტერული დანაშაულის შესახებ კონვენცია ითვალისწინებს ღონისძიებებს, მიმართულს მონაცემების

[70] ინსტრუქციები სამართალდამცავ ორგანოებსა და სერვის პროვაიდერებს შორის თანამშრომლობის შესახებ იხილეთ: http://www.coe.int/t/dg1/legalco-operation/economiccrime/cybercrime/cy%20activity%20Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf.

[71] ყველაზე მეტად საშიშ კიბერშეტევებში ტრანსნაციონალური შეტევების მასშტაბის გასაცნობად, იხილეთ: სოფაერი/გუდმენი, კიბერდანაშაული და უსაფრთხოება, ტრანსნაციონალური სივრცე; კიბერდანაშაულის და ტერორიზმის ტრანსნაციონალური განზომილება, 2001. გვ.7: http://media.hoover.org/documents/0817999825_1.pdf.

[72] ყველაზე მეტად სრულყოფილი და კარგად განსაზღვრული პროტოკოლებია: ტრანსმისიი კონტროლის პროტოკოლი და ინტერნეტ პროტოკოლი. დამატებითი ინფორმაციისათვის, იხილეთ: ტენაბაუმის კომპიუტერული ქსელები; კომერის ინტერნეტქსელები: პრინციპები, პროტოკოლები და არქიტექტურა.

[73] ჰუბნერი, ბემი: კომპიუტერული ექსპერტიზა-წარსული, აწმყო და მომავალი, №6: http://www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf; ქსელების შენახვის თვალსაზრისით იხილეთ: კლარკის შენახვის ვირტუალიზაციის ტექნოლოგოები მონაცემთა შენახვისა და მენეჯმენტის გაადვილების მიზნით

[74] საერთაშორისო თანამშრომლობის აუცილებლობის მიზნით კიბერდანაშაულის წინააღმდეგ ბრძოლაში იხილეთ პუტნამის, ელიოტის საერთაშორისო პასუხები კიბერდანაშაულებზე; სოფაერი, გუდმანის კიბერდანაშაულის და ტერორიზმის საერთაშორისო განზომილება, 2001,გვ.35: http://media.hoover.org/documents/0817999825_35.pdf; სოფაერი, გუდმანის კიბერდანაშაულის და ტერორიზმის საერთაშორისო განზომილება, 2001, გვ.1: http://media.hoover.org/documents/0817999825_1.pdf

[75] ეროვნული სუვერენიტეტი ფუნდამენტური პრონციპია საერთაშორისო სამართალში. იხილეთ როთი: სახელმწიფოს სუვერენიტეი, საერთაშორისო სამართალი და მორალური შეუთავსებლობები, 2005. გვ.1: http://www.law.uga.edu/intl/roth.pdf.

შენახვისაკენ, ყოველდღე 24 საათის განმავლობაში მომუშავე საკომუნიკაციო პუნქტების ჩათვლით.

2.3.6. დამოკიდებულება დანაშაულის ჩადენის ადგილზე მსხვერპლსა და დამნაშავის ყოფნას შორის

კომპიუტერული დანაშაულის ჩადენა, როგორც წესი, არ მოითხოვს დამნაშავის ყოფნას დანაშაულის ჩადენისა და მსხვერპლის ყოფნის ადგილას. ამ დამოკიდებულების არარსებობას დიდი სირთულეების გამოწვევა შეუძლია კომპიუტერული დანაშაულის გამოძიების საქმეში. დამნაშავეებს საშუალება ეძლევათ, თავიდან აიცილონ სისხლის სამართლის საქმის წარმოება იმ ქვეყანაში მოქმედებით, სადაც საკანონმდებლო ბაზა კომპიუტერული დანაშაულის შესახებ ნაკლებად არსებობს. [76] ამიტომ, კომპიუტერული დანაშაულის წინააღმდეგ ეფექტიანი ბრძოლისათვის, აუცილებელია დამნაშავეებისათვის ისეთი "უსაფრთხო სამოთხის" მსგავსი ადგილების შემცირება, რომლებიც საშუალებას აძლევენ მათ, დაფარონ საკუთარი დანაშაულებრივი საქმიანობა, განახორციელონ ქმედებები და დარჩნენ დაუსჯელები.[77]

ასეთი "უსაფრთხო სამოთხის" გამოყენების მაგალითს წარმოადგენს "სიყვარულის ხოჭო" – კომპიუტერული ვირუსი, რომელიც 2000 წელს გავრცელდა.[78] ვირუსი მსოფლიოს მასშტაბით მილიონებით სისტემაზე გავრცელდა და დააინფიცირა ისინი.[79] გამოძიება კვალმა ფილიპინებში მიიყვანა. იმის გამო, რომ მსგავსი საქმიანობა ფილიპინებში იმ დროისათვის არ ითვლებოდა სისიხლის სამრთლის დანაშაულად, სერიოზულად შეფერხდა ადგილობრივი გამოძიება.[80]

[76] მაგალითებად გამოდგება ფიშინგთან დაკავშირებული დანაშაულები. მიუხედავად იმისა, რომ გვერდების უმეტესობა შენახულია აშშ-ში (32%), ჩინეთში (13%), რუსეთში (7%) და კორეაში (6%), აშშ-ს გარდა არც-ერთ არ მოუხდენია საერთაშორისო შეთანხმებების რატიფიცირება, რაც დაავალდებულებდა მათ მონაწილეობა მიეღოთ საერთაშორისო გამოძიებაში.

[77] საკითხი დარეგულირდა საერთაშორისო ორგანიზაციების მიერ. გაერთიანებული ერების ორგანიზაციის გენერალურმა ანსამბლეამ მიიღო რეზოლუცია №55/63, რომელიც ამბობს: „სახელმწიფოებმა უნდა უზრუნველყონ მათი კანონებისა და ღონისძიებების მიერ დამნაშავეებისათვის უსაფრთხო ადგილების მოსპობა. მთლიანი ტექსტი იხილეთ: : http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. არ უნდა არსებობდეს უსაფრთხო ადგილები დამნაშავეებისათვის.

[78] დამატებითი ინფორმაციისათვის იხილეთ: ://en.wikipedia.org/wiki/ILOVEYOU, ვირუსებთან დაკავშირებული შედეგების სანახავად: http://www.gao.gov/archive/2000/ai00181t.pdf.

[79] ბი-ბი-სი ახალიი ამბები, პოლიცია ხურავს ვირუსების საშუალებას, 06,05,2000: http://news.bbc.co.uk/1/hi/sci/tech/738537.stm. ტექნოლოგიასთან დაკავშირებით: http://radsoft.net/news/roundups/luv/20000504,00.html.

[80] ცი-ენ-ენ, სასიყვარულო ვირუსის გამოყენება კიბერშეტევების მიზნით, 08.05.2000. http://edition.cnn.com/2000/LAW/05/08/love.bug/index.html; ჩაუკი კიბერდანაშაულის დარეგულირებაზე მნიშვნელოვანი მოსაზრებები, http://www.crime-research.org/articles/Critical/2; *sofaeri. გუდმანი*, კიბერდანაშაული და უსაფრთXოება – ტრანსნაციონალური განზომილება 2001, გვ. 10 – http://media.hoover.org/documents/0817999825_1.pdf;

2.3.7. ვირუსები

სამართალდამცავი ორგანოების წინაშე მდგარი ერთ-ერთ სერიოზული გამოწვევა გახლავთ ის, რომ ორგანიზებული დამნაშავე ჯგუფების დიდ რაოდენობას შეუძლია უამრავი კომპიტერული სისტემის გამოყენება ავტომატური შეტევის განხორციელების მიზნით.[81] ასეთი შეტევის მაგალითი გახლავთ ესტონეთის მთავრობის წინააღმდეგ განხორციელებული შეტევა.[82] შეტევის ანალიზმა გვიჩვენა, რომ პროცესში მონაწილეობდა ათასობით კომპიუტერი, რომლებიც ე.წ. ბოტნეტის ნაწილს წარმოადგენდნენ.

კრიმინალებისაგან განსხვავებით, რომლებსაც ხელთ აქვთ უამრავი საშუალება და არ იწუხებენ თავს საზღვრების პატივისცემით, მოსამართლეებისა და სისხლის სამართლის სფეროში მომუშავე ორგანოების რესურსები ბევრად შეზღუდულია.

საკითხი დგას ასე: როგორ არის შესაძლებელი მოსამართლეებისა და სამართალდამცავი ორგანოების წარმომადგენელბის მომზადება და აღჭურვა ისე, რომ მათ შეძლონ კომპიუტერული დანაშაულის გამოწვევების ღირსეულად გამკლავება?

2.3.8. ფუნდამენტური უფლებების დაცვა

სიტყვისა და პირადი ცხოვრების უფლება (პირადი ინფორმაციის დაცვის უფლების ჩათვლით) გახლავთ ის ორი საკითხი, რომლებიც ძალზედ მნიშვნელოვანია ინტერნეტის მომხმარებლებისათვის.[83]

შესაძლოა ჩაითვალოს, რომ ადამიანების დიდი უმრავლესობა იყენებს საინფორმაციო ტექნოლოგიებს სრულიად კანონიერი მიზნებისათვის. მნიშვნელოვანია მომხმარებლების უფლებების ეფექტიანი და ეფექტური დაცვა. ეს საკითხი კონვენციის მუხლ 15-ში არის განხილული:

---

[81] იხილეთ, კიბერდანაშაულთან დაკავშირებული საკითხების წარმოშობა საშიშროებას უქმნის ინფორმაციის ფედერალურლ სისტემას, 2005: http://www.gao.gov/new.items/d05231.pdf.

[82] შეტევებთან დაკავშირებით იხილეთ: ლუისის კიბერშეტევები, 2007: http://www.csis.org/media/csis/pubs/070615_cyber_attacks.pdf; კიბერდარბევა, ეკონომისტი,10.05.2007: http://www.economist.com/world/europe/PrinterFriendly.cfm?story_id=9163598; ესტონეთის შემდეგ გაჩენილი ციფრული შიშები, ნიუ-იორკ თაიმსი, 29.05.2007: http://www.nytimes.com/2007/05/29/technology/29estonia.html?ei=5070&en=2e77eb21a1ab42ac&ex=1188360000&pagewanted=print.

[83] იხილეთ თოტის, ესტონეთი და კიბერშეტევა: http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

მუხლი 15 – პირობები და გარანტიები

1. თითოეული მხარე იძლევა გარანტიას, რომ ამ დებულებით გათვალისწინებული ძალაუფლებისა და პროცედურების ჩამოყალიბება, რეალიზაცია და გამოყენება მისადაგებული იქნება ადგილობრივი კანონმდებლობის პირობებთან და გარანტიებთან, რომლებმაც უნდა უზრუნველყონ ადამიანის უფლებებისა და თავისუფლებების სათანადო დაცვა, იმ უფლებების ჩათვლით, რომლებიც გამომდინარეობს 1950 წლის ევროსაბჭოს ადამიანის უფლებებისა და ფუნდამენტური თავისუფლებების დაცვის კონვენციიდან, 1966 წლის გაერთიანებული ერების საერთაშორისო კონვენციიდან სამოქალაქო და პოლიტიკური უფლებების შესახებ და ადამიანის უფლებებთან დაკავშირებული სხვა საერთაშორისო ინსტრუმენტებიდან, რომლებიც უნდა ეფუძნებდნენ პროპორციულობის დაცვის პრინციპს.
2. ასეთი პირობები და გარანტიები, გამომდინარე მათში გათვალისწინებული უფლებამოსილებებისა და პროცედურების ბუნებისაგან, სხვა ინსტრუმენტებს შორის, უნდა შეიცავდეს სასამართლოს ან სხვა დამოუკიდებელი ორგანოების მიერ განხორიცლებულ ზედამხედველობას, მათი გამოყენების საფუძველს და ასეთი ძალაუფლების ან პროცედურის გამოყენების სფეროსა და ხანგრძლიობის შეზღუდვებს.
3. იმდენად, რამდენადაც ყველაფერი გამიზნულია საჯარო ინტერესების და, განსაკუთრებით სამართლის გამარჯვებისაკენ, ყველა მხარემ უნდა გაითვალისწინოს ასეთი უფლებამოსილებისა და პროცედურების გავლენა მესამე მხარის უფლებებზე, პასუხისმგებლობებსა და ლეგიტიმურ ინტერესებზე.

აუცილებელი და მნიშვნელოვანია ბალანსის შენარჩუნება კომპიუტერული დანაშაულის გამოძიების ეფექტიან ინსტრუმენტებსა და მომხმარებლის ფუნდამენტურ უფლებებს შორის, რასაც დიდი ყურადღება უნდა მიექცეს საქმის მოკვლევის, გამოძიების, ბრალის წაყენებისა და სასამართლოს მიერ განაჩენის გამოტანის დროს. ამ საკითხებში ყველაზე მნიშვნელოვან როლს მოსამართლეები თამაშობენ.

2008[84] წლის თებერვალში, გერმანიის კონსტიტუციურმა სასამართლომ განაცხადა, რომ კომპიუტერული სისტემების კონფიდენციალურობა, ინტეგრირებულობა და ხელმისაწვდომობა დაცული იქნება გერმანიის კონსტიტუციით. აღნიშნული ხაზს უსვამს დაცულობის მნიშვნელობას მაშინ, როცა მუშავდება გამოძიების სხვადასხვა ინსტრუმენტები.

[84] სიტყვის თავისუფლებასთან დაკავშირებით იხილეთ ტედფორდი, ჰერბერტ,ჰეიმანის სიტყვის თავისუფლება აშშ-ში, 2005; ბერენდტი, სიტყვის თავისუფლება, 2007; ბეიკერი: ადამიანის თავისუფლება და სიტყვის თავისუფლების უფლება; ემორდი: თავისუფლება, ტექნოლოგიები და პირველი ცვლილება, 1991; ელექტრონულ თვალყურზე პრონციპებთან დაკავშირებით: ვუუ და სოუ: საოცარი ფანარის ისტორია, 11 სექტემბრის ისტორია ცხადჰყოფს თვალყურის აუცლებლობას, ჰარვარდის ჟურნალი – კანონმდებლობა და ტექნოლოგიები. ტომი 15, №2, 2002, გვ.530; ვესტერმანი: სიტყვის თავისუფლება ავსტრალიის კანონმდებლობაში; ვოლოკო, სიტყვის თავისუფლება, კანონი რელიგიური შეურაცხყოფის შესახებ, ლაიოლას უნივერსიტეტის ჩიკაგოს იურიდიული ჟურნალი, ტომი 33, გვ.57: http://www.law.ucla.edu/volokh/harass/religion.pdf; *koeni*. სიტყვისა და პრესისი თავისუფლება: ამონარიდები პირველი ცვლილებიდან, ანგარიში კონგრესისათვის 95-815, 2007: http://www.fas.org/sgp/crs/misc/95-815.pdf.

ამავე დროს, თუ კომპიუტერული სისტემები დიდწილად შეიცავენ მოქალაქეების პირადი ცხოვრების ელემენტებს, ამ სისტემების დაცვის და სისხლის სამართლის ეფექტიანი ღონისძიებები უნდა იქნეს მნიშვნელოვანი გზა ადამიანთა ფუნდამენტური უფლებების დაცვასთან მიმართებაში. ამ კონტექსტში, დაცვა და ადამიანთა უფლებები ერთად განიხილება.

2.4. ეროვნული კანონმდებლობა და საერთაშორისო სტანდარტები: კონვენცია კომპიუტერული დანაშაულის შესახებ

2.4.1. სისხლის სამართლის ეროვნული კანონმდებლობა

როგორც უკვე ავღნიშნეთ, ადეკვატური კანონმდებლობა ძალზედ მნიშვნელოვანია წარმატებული გამოძიების, ბრალის წაყენებისა და განაჩენის გამოტანის პროცესში.

ეროვნულ დონეზე, სისხლის სამართლის კანონმდებლობაში ცვლილებები უნდა მოიცავდეს:

- კონკრეტული ქმედებებისათვის სისხლის სამართლის დანაშაულის კვალიფიკაციის მინიჭებას (სისხლის სამართლის კანონმდებლობა)
- პროცედურული ინსტრუმენტების შემუშავებას, რომელიც საშუალებას მისცემს სამართალდამცავ ორგანოებს, გამოიძიონ საქმე
- საერთაშორისო თანამშრომლობის საშუალებების გამოყენებას, რაც საშუალებას იძლევა ეფექტიანად განხორციელდეს სხვადასხვა ქვეყნების კომპეტენტური ორგანოების თანამშრომლობა.

კომპიუტერული დანაშაულის შესახებ კონვენცია წარმოადგენს ინსტრუქციებს, რომლებიც გვეხმარება საერთო და პროცედურული დებულებების და ქვეყნებს შორის კანონმდებლობის ჰარმონიზაციაში. ასევე, იმ ქვეყნებისათვის, რომლებიც მიუერთდნენ კონვენციას, იგი წარმოადგენს საერთაშორისო დონეზე თანამშრომლობის სახელმძღვანელო დოკუმენტს.

ქვეყნების პროფილი, რომელიც შემუშავებული იქნა ევროსაბჭოს კომპიუტერული დანაშაულის პროექტის ფარგლებში, საშუალებას იძლევა, კონვენციის დებულებები დავუკავშიროთ ეროვნული კანონმდებლობის კონკრეტულ დებულებებს.

2.4.2. კონვენცია კომპიუტერული დანაშაულის შესახებ

ზოგადი მიმოხილვა

კომპიუტერული დანაშაული ყველაზე მეტად არის ტრანსნაციონალური ხასიათის დანაშაული.[85] სწორედ ამიტომ, იგი მოითხოვს გლობალურ თანამშრომლობას სამართალდამცავ და სისხლის სამრთლის კომპეტენტურ ორგანოებს შორის.[86] საერთაშორისო თანამშრომლობასთან დაკავშირებული სირთულეების გამო, რაც გამოწვეულია განსხვავებული ეროვნული სტანდარტებით (განსაკუთრებით, "ორგვარი სისხლის სამართლის

[85] მომხმარებლების ფუნდამენტურ უფლებებთან დაკავშირებით იხილეთ საინფორმაციო საზოგადოების მსოფლიო შეხვედრა უმაღლეს დონეზე, პრინციპების დეკლარაცია, 2003: http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf.
[86] BVerfG, 1 BvR 370/07 vom 27.2.2008.

დანაშაულის"[87] მოთხოვნის გამო), საერთაშორისო თანამშრომლობის ხარისხის გაუმჯობესებისათვის აუცილებელი ფუნდამენტური კომპონენტი გახლავთ ეროვნული კანონმდებლობის ჰარმონიზაცია. უფრო კონკრეტულად, ქვეყნებმა თანხმობა უნდა განაცხადონ და მიიღონ საერთო სისხლის სამართლისა და პროცედურულ კანომდებლობასთან დაკავშირებული საერთო სტანდარტები და შეიმუშაონ საერთაშორისო თანამშრომლობისათვის საჭირო სამართლებრივი სტანდარტები.

კონვენცია კომპიუტერული დანაშაულის[88] შესახებ აყალიბებს ასეთი კანონმდებლობის შემუშავებისიათვის საჭირო საერთო სამართლებრივ ჩარჩოს. ევროსაბჭომ, არაწევრ ქვეყნებთან ერთად, როგორებიცაა კანადა, იაპონია, სამხრეთ აფრიკა და აშშ შეიმუშავა შეთანხმება (რომლის წევრების რაოდენობა დღეისათვის არის 47). შეთანხმება ღიაა ხელმოწერებისათვის 2001 წლიდან. იგი ძალაში შევიდა 2004 წელს.[89] აღნიშნული კონვენცია ღიაა ნებისმიერი ქვეყნისათვის.[90] მაგალითად, 2007 წლის თებერვალში კოსტა რიკა და მექსიკა, ხოლო 2008 წლის ნომებერში დომინიკის რესპუბლიკა შეუერთდა კკონვენციას. ასევე, უამრავი ქვეყანა ცდილობს გაწევრიანებას. მნიშვნელოვანია, რომ ბევრი ქვეყანა ამუშავებს საკუთარ კანონმდებლობას კომპიუტერულ დანაშაულთან დაკავშირებით და ამ მიზნით, კონვენცია გამოყენებულია, როგორც მოდელი.[91]

კონვენციის სტრუქტურა

ხელშეკრულების სტრუქტურა შემდეგნაირია:

- თავი I: კომპიუტერული სისტემის, მონაცემების, სერვის პროვაიდერის და ტრაფიკის მონაცემების განმარტება
- თავი II: ეროვნულ დონეზე განსახორციელებლი ღონისძიებები

  ნაწილი 1 - სისხლის სამართლის საერთო კანონი, რომელიც მოიცავს ქმედებას, რომელიც უნდა დაკვალიფიცირდეს, როგორც სისხლის სამართლის დანაშაული, რომელშიც შედის:

---

[87] ტრანსნაციონალური შეტევების მასშტაბების შესწავლის მიზნით იხილეთ სოფაერის და გუდმანი: კიბერდანაშაული და უსაფრთხოება – ტრანსნაციონალური სივრცე, 2001.გვ.7; http://media.hoover.org/documents/0817999825_1.pdf.

[88] ჰერკე, კიბერშეტევების წინააღმდეგ ნელი გლობალური გამოღვიძება, 2006, 142

[89] საერთაშორისო გამოძიებაში ორმაგ დანაშაულთან დაკავშირებით იხილეთ გაეროს სახელმძღვანელო კომპიუტერთან დაკავშირებული დანაშაულის აღკვეთისა და კონტროლის შესახებ: *შტჯოლბერგ/ უბბარდ*, ეროვნული სამართლის ჰარმონიზაცია კიბერდანაშაულთან მიმართებაში, 2005, გვ. 5 : www.itu.int/osg/spu/cybersecurity/ presentations/session12_schjolberg.pdf.

[90] ევროკავშირის კონვენცია კიბერდანაშაულზე: conventions.coe.int დამატებითი ინფორმაციისათვის იხილეთ თავი 6.1.; სოფაერი- საერთაშორისო კონვენციისაკენ კიბერდანაშაულის შესახებ, კიბერდანაშაულისა და ტერორიზმის ტრანსნაციონალური განზომილება, გვ.255: http://media.hoover.org/documents/0817999825_221.pdf; ჰერკე, ნელი გამოღვიძბე აკიბერდანაშაულის წინააღმდეგ, 2006,140; ჰერკე: ეროვნული, რეგიონული და საერთაშორისო მიდგომა კიბერდანაშაულის წინააღმდეგ ბრძოლაში, 2008, გვ.7; ალდესკო, ანონიმურობა: კომპიუტერული დანაშაულის კონვენციაში კონსტიტუციური ცვლიელება. კანონმდებლობის მიმოხილვა: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf. ჯონსი, ევროსაბშოს კონვენცია კიბერდანაშაულის წინააღმდეგ, თემები და კრიტიკა, 2005: http://www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf.

[91] კონვენციის დებულებების ძალაში შესვლის მოთხოვნები რეგულირდება კონვენციის მუხლი 36-ით.

- დანაშაული კომპიუტერული მონაცემების და სისტემების კონფიდენციალურობის, ინტეგრირებულობისა და ხელმისაწვდომობის წინააღმდეგ (უკანონო შეღწევა, უკანონო მოპოვება ინფორმაციის, მონაცემებში ჩარევა, სისტემაში ჩარევა, ტექნიკის არადანიშნულებით გამოყენება);
- კომპიუტერის საშუალებით ჩადენილი დანაშაული (გაყალბება, თაღლითობა);
- შინაარსთან დაკავსირებული დანაშაული (ბავშვების პორნოგრაფია, ქსენოფობია და რასიზმი);
- საპატენტო უფლებისა და სხვა მსგავსი უფლებების დარღვევა

ნაწილი 2 – პროცედურული კანონი ანუ კომპიუტერული დანაშაულის გამოძიების ეფექტიანი ღონისძიებები, რომელშიც შედის:

- პროცედურული გარანტიები
- კომპიუტერული მონაცემების ოპერატიული შენახვა
- ტრაფიკის მონაცემების ოპერატიული შენახვა და ნაწილობრივი გამჟღავნება
- ბრძანება ინფორმაციის მიწოდების შესახებ
- შენახული კომპიუტერული მონაცემების შემოწმება და ამოღება
- ტრაფიკის მონაცემების რეალურ დროში ამოღება
- შინაარსის მონაცემების მოპოვება

ნაწილი 3 - იურისდიქცია

- თავი III: საერთაშორისო თანამშრომლობა

  ნაწილი 1 – თანამშრომლობის ზოგადი პრინციპები, რაც მოიცავს საერთაშორისო თანამშრომლობის ზოგად პრინციპებს, ექსტრადიციასთან დაკავშირებულ პრონციპებს, ორმხრივი სამართლებრივი დახმარების პრინციპებს, სპონტანურ ინფორმაციას, ორმხრივ სამართლებრივ დახმარებას სათანადო საერთაშორისო ინსტრუმენტების არარსებობის პირობებში და კონფიდენციალურობა და გამოყენების შეზღუდვები

  ნაწილი 2 – კონკრეტული დებულებები უფრო ეფექტიანი თანამშრომლობისათვის. ეს საშუალებას აძლევს კონვენციის მონაწილე მხარეებს, გამოიყენონ პროცედურული ინსტრუმენტები საერთაშორისო დონეზე. დებულებები მოიცავს კომპიუტერული მონაცემების ოპერატიულ შენახვას, კომპიუტერული მონაცემების მიღებაში ორმხრივ დახმარებას, კომპიუტერული მონაცემების მიღების ტრანსსაზღვრულ მიდგომას, ტრაფიკის მონაცემების რეალურ დროში ამოღებაში და შინაარსის მოპოვებაში ორმხრივ დახმარებას. ასევე, ეს ნაწილი ეხება საკომუნიკაციო პუნქტების 24/7 (კვირაში 7 დღე, 24 საათი) შექმნას, რაც ხელს შეუწყობს სწრაფ თანამშრომლობას.

- თავი IV: დასკვნითი დებულებები. ეს თავი განსაკუთრებით საინტერესოა არაევროპული ქვეყნებისათვის, რადგან დაეხმარება მათ კონვენციაში გაწევრიანების საკითხებში.

კონვენციის სხვადასხვა დებულებები დეტალურად იქნება განხილული ერთ-ერთ თავში, რომელიც ყურადღებას ამახვილებს ისეთ ქმედებებზე, რომლებიც წარმოადგენს სისხლის სამართლის დანაშაულს.

3. ტექნოლოგია მოსამართლეებისათვის

3.1. შესავალი

ეს თავი ტრენერებს უზრუნველყოფს იმ ჩარჩოთი, რომელიც წარმოადგენს უფრო ფართო პროგრამის ნაწილს. შეუძლებელია მისი სრულყოფილება, რადგან ტექნოლოგიები იმდენად სწრაფად იცვლება, რომ ამ ნაშრომის გამოქვეყნებისთანავეც კი, შესაძლოა, ბევრი რამ უკვე მოძველებული აღმოჩნდეს. იმისათვის, რომ მოსამართლეებმა სამართლიანად გადაწყვიტონ მათ წინაშე მდგარი საკითხები, საჭიროა ერკვეოდნენ ტექნიკურ სფეროში. წინამდებარე თავი სწორედ ამ საკითხებთან არის დაკავშირებული. იგი შეიცავს ინფორმაციას ტექნოლოგიების შესახებ, რომლებსაც მოსამართლეები გადააწყდებიან მუშაობის პროცესში და, რომლებსაც დამნაშავეები იყენებენ დანაშაულის ჩადენის მიზნით, ხოლო სამართალდამცავი ორგანოები ცდილობენ მათ აღმოჩენას.

3.2. როგორ მუშაობს კომპიუტერი

ამ სესიის დასრულებისას, მონაწილეებმა უნდა შეძლონ:

- კომპიუტერის შემადგენელი ნაწილების ჩამოთვლა
- ახსნა, როგორ ხდება ინფორმაციის შენახვა კომპიუტერში
- განასხვავონ, კმპიუტერის სხვადასხვა სისტემა

იმისათვის, რომ მოსამართლეებმა ზუსტად გაიგონ, ტექნოლოგიების გავლენა დანაშაულზე, საჭიროა იცოდნენ როგორ მუშაობს ეს ტექნიკა. მაგალითად, ციფრული ექსპერტიზის ცოდნა დაეხმარება მათ კონტექსტის გააზრებასა და ინფორმირებული განაჩენის გამოტანაში.

3.2.1. კომპიუტერის შემადგენელი ნაწილები

კომპიუტერი შედგება ბევრი კომპონენტისაგან და მოსამართლეებმა უნდა იცოდნენ მათი სახელები და ფუნქციები:

- **სისტემური პლატა (Motherboard)** – ეს არის კომპიუტერის ძირითადი ნაწილი. ყველა დანარჩენი კომპონენტი სწორედ მასთან არის მიერთებული. სისტემური პლატის დანიშნულება არის მათ შორის ინფორმაციის გაცვლა. აქ მოთავსებულია ძირითადი შემავალ-გამავალი სისტემა, რომელიც არის პროგრამა, რომელიც იწყებს მუშაობას კომპიუტერის ჩართვისას. მასთანვეა დაკავშირებული მეხსიერება,

პროცესორი, გრაფიკული კარტა, ხმის კარტა, მყარი დისკი, დისკის დრაივერი და სხვა.

- **ელექტროენერგიის წყარო** – ეს კომპონენტი არეგულირებს და ელექტროენერგიას აწოდებს კომპიუტერის სხვადასხვა კომპონენტებს. სტანდარტულად, შემავალ 110 ან 220 ვოლტს გარდაქმნის კომპონენტებისათვის საჭირო ვოლტაჟად. ელქტროენერგიის წყაროებს აქვთ კონკრეტული გამომავალი სიმძლავრეები ვატებში, როგორც წესი სტანდარტულად ხდება 350 ვატის მიწოდება. რაც უფრო მეტია კომპონენტები, მით მეტი ენერგია ჭირდება კომპიუტერს.
- **CMOS და BIOS** – ეს აბრევიატურები ერთმანეთის შემცვლელებად გამოიყენება. შეიძლება ასეც განვიხილოთ: BIOS არის პროგრამა, ხოლო CMOS კი კომპონენტი, რომელიც მას ამუშავებს და რომელიც ასრულებს დაბალი დონის ფუნქციებს, ამუშავებს კომპიუტერის საათს, უზრუნველყოფს ინტერფეისს, რომ BIOS-მა შეასრულოს თავისი ფუნქციები. მას ჭირდება ძალზედ ცოტა ელექტროენერგია. გამოითქმის, როგორც -სიმოს.
  BIOS, გამოითქმის, როგორც – ბაიოს. ეს არის ინტერფეისი, რომელიც საშუალებას აძლევს მომხმარებელს, შეიტანოს ცოტაოდენი ცვლილებები კომპიუტერის სისტემურ პალტაში, მეხსირებასა და სხვა კომპონენტებში. ერთ-ერთი ყველაზე მნიშვნელოვანი ცვლილება, რაც გაუკეთდა ბაიოსს არის იმ თანმიმდევრობის შეცვლა, რომელსაც კომპიუტერი ეძებს, რომ დაიწყოს ფუნქციონირება. როგორც წესი, კომპიუტერული ექსპერტიზის დროს იყენებს კომპაქტ დისკზე არსებულ პროგრამას და ცვლის ბაიოსს ისე, რომ კომპიუტერმა დაიწყოს კომპაქტ დისკიდან და არა მყარი დისკიდან, რადგან ეს გამოიწვევდა მონაცემების შეცვლას.

- **პლატის გაფართოვების ბუდე** – კომპიუტერის უკანა ნაწილში არის ბუდეები, სადაც შეგიძლიათ მიუერთოთ ხმის კარატა, ვიდეო კარტა, უკაბელო ადაპტორი და სხვა.
- **ცენტრალური პროცესორი** – ხშირად ურევენ მას კომპიუტერის ტანში. პროცესორი კომპიუტერის შიდა ნაწილია, რომელიც გარედან არ ჩანს. პირველად გამოიყენეს 1960-იან წლებში. 1970-იანი წლებიდან მისი ზომები კიდევ უფრო შემცირდა, რამაც ხელი შეუწყო კომპიუტერის ზომების შემცირებას.
- მიუხედავად იმისა, თუ რა სახის არის კომპიუტერი, პროცესორი მუშაობს და ასრულებს უამრავ ინსტრუქციას, რომლებიც ცნობილია პროგრამის სახელით. პროცესორების უმეტესობა შეესაბამება ვონ ნიუმანის არქიტექტურას, რომლის მიხედვითაც პროცესორმა სწრაფად უნდა მიიღოს, გაშიფროს, გააანალიზოს და უკან გადააგზავნოს მონაცემები. მოკლედ, იგი არის კომპიუტერის ტვინი.
- **მეხსიერება** – არის მონაცემების ელქტრონული შენახვა, რომელთან შეღწევაც სწრაფად არის შესაძლებელი. ინფორმაციის მიღება იქნებოდა ძალიან ხანგრძლივი პროცესი, ეს რომ ხდებოდეს პროცესორის მიერ ინფორმაცის მყარი

დისკიდან მიღების გზით. ამიტომ, მონაცემები ინახება დროებით მეხსიერებაში, რაც ინფორმაციის მიღების პროცესს აჩქარებს. ეს მეხსიერება ცნობილია, როგორც რამი. პროცესორი ინფორმაციას ითხოვს რამიდან, გადაამუშავებს და აგზავნის უკან. ეს ხდება წამში მილიონჯერ. დრებითი მეხსიერების ცოდნა მნიშვნელოვანია ექსპერტიზის დროს მონაცემთა ამოღების მიზნით, რადგან მისი შენახვა არ ხდება, თუ კომპიუტერი დენის წყაროსთან არ არის მიერთებული, რასაც ხშირად ქონია ადგილი. ამიტომ, ახლა სამართალდამცავი ორგანოები ცდილობენ მონაცემების რამიდან ამოღებას მანამ, სანამ კომპიუტერს გამორთავენ დენის წყაროდან. ამას ეწოდება „მონაცემების ექსპერტიზა ეთერში/ლაივში“. ეს საქმიანობა სულ უფრო გახშირდა, რადგან შესაძლო დასაკარგი მონაცემების მოცულობა უფრო დიდია, ვიდრე რამდენიმე წლის წინ ყველაზე დიდი მყარი დისკის შესაძლებლობა იყო.

- **მყარი დისკი** – კომპიუტერს აქვს, სულ მცირე, ერთი ან მეტი მყარი დისკი. დიდ კომპიუტერებს ბევრი მყარი დისკი აქვთ. მყარი დისკი, ასევე აქვთ, მუსიკალურ ცენტრებს, რაც საშუალებას იძლევა დაიტიოს უამრავი ინფორმაცია. აქედან ადვილია ინფორმაციის ჩაწერა და წაშლა, რაც ხელს არ უშლის და არ აფუჭებს თავად დისკს. ინფორმაცია ინახება სექტორებში და ცალკე ბილიკებში/ტრეკებში. ბილიკები არის კონცენტრული წრეები, ხოლო სექტორები – ჩანართი ამ ბილიკებზე. მონაცემები მყარ დისკზე ინახება ფაილების სახით, რაც წარმოადგენს ბაიტების ჯგუფს. პროგრამებიც, ასევე, წარმოადგენს ფაილებს.
- **სიდი/დივიდი/ბლუ რეი დისკები** – მათ შეუძლიათ სხვადასხვა მოცულობის ინფორმაციის დატევა და, როგორც წესი, გამოიყენება მუსისკის, ვიდეოს და სხვა ინფორმაციის გავრცელების მიზნით. დივიდი იგივე ზომისაა რაც სიდი, მაგრამ იტევს შვიდჯერ მეტ ინფორმაციას. ბრუ რეი დისკი, რომელიც გამოიყენება მაღალი გამოსახულების მქონე ინფორმაციისათვის, დივიდიზე ათჯერ მეტ ინფორმაციას იტევს. მოკლედ, იტევენ უფრო მეტ ინფორმაციას, ვიდრე ეს შეეძლო მყარ დისკს რამდენიმე წლის წინ. ისინი ინახავენ ინფორმაციას სხვადასხვა გზით და ამიტომ მათძე შენახული ინფორმაცია უფრო ხანგრძლივია და ნაკლებად არის დამოკიდებული ელექტროენერგიაზე, ვიდრე მყარ დისკზე შენახული ინფორმაცია.
- **იუ-ეს-ბი დამაკავშირებელი** – მას ბევრ კომიუტერზე ნახავთ. იგი კომოიუტერთან აერთებს სხვადასხავ ნაწილებს: მაუსს, პრონტერს, მობილურ ტელეფონს და სხვა. ეს ყვალზე ფართოდ გავრცელებული მეთოდია. ადრე რასებობდა მიერთების პარალელური ან სერიული პორტები, რაც პრობლემატური იყო მისაერთებელი კომპონენტების რაოდენობასთან დაკავშირებით. ასევე, ინფორმაციის გადაცემის სიჩქარეც ნაკლები იყო. იუ-ეს-ბი ძასლიან მნიშვენლეოვანია ციფრული ექსპერტიზის დროს.
  დამატებითი ინფორმაციისათვის, იხილეთ:
  www. computer.howstuffworks.com/computer-hardware-channel.html.

გახსოვდეთ, მიიღოთ მფლობელის თანხმობა ინფორმაციის მიღებაზე, რომლის გამოყენებასაც აპირებთ ტრენინგზე.

3.2.2. მონაცემთა შენახვა

მტკიცებულების მოპოვება კომპიუტერიდან ან მობილური ტელეფონებიდან ყოველდღიურად ხდება. ტექნოლოგიების გაძლიერებულ მოხმარებასთან ერთად, ბევრი ტექნიკისათვის ჩვეულებრივი მოვლენა გახდა ციფრული ინფორმაციის შენახვა (მტკიცებულება), რაც შემდეგ გამოსადეგია გამოძიების პროცესში. ჩვენ უკვე ვაწყდებით შემთხვევებს, როცა საყოფაცხოვრებო ტექნიკიდანაც ხდება ასეთი ინფორმაციის მიღება. ამიტომაც მნიშვნელოვანია, რომ მოსამართლეებს ქონდეთ წარმოდგენა ციფრული მტკიცებულების შესახებ. დასაწყისისათვის, საჭიროა იცოდნენ, თუ როგორ ხდება ინფორმაციის შენახვა და მისი აღდგენა გამოძიების მიზნებისათვის.
ელქტრონული, ციფრული ინფორმაციის შენახვა სხვადასხვა ფორმით არის შესაძლებელი. ყველაზე მარტივია მყარ დისკზე შენახვა. ციფრული მტკიცებულების მოპოვების ყველაზე ტიპიური გზა არის ნაწილების შემოწმება სტატიკურ მდგომარეობაში, ანუ როცა კომპიუტერი გამორთულია. ციფრული ექსპერტიზის სპეციალისტები კარგად არიან ინფორმირებულები ამასთან დაკავშირებულ საერთაშორისო სტანდარტებზე. ერთ-ერთი ასეთი ინსტრუქცია ჩამოყალიბდა ევროკომისიის ოისინის პროგრამის ფარგლებში: www.e-evidence.info. აქ მოცემულია ზოგადი პრინციპები, რომლებსაც სამართალდამცავები იყენებენ. აუცილებელია, რომ მოსამართლეებმა იცოდნენ, თუ როგორ ხდება ინფორმაციის შენახვა და როგორ ხდება მტკიცებულების მოპოვება. ეს კი მოიცავს ციფრული ინფორმაციის არსის, შენახვის, ამოღებისა და სასამართლოში წარდგენის ცოდნას. ამის შესახებ ინფორმაციის სანახავად, შეგიძლიათ ეწვიოთ: www.soragereview.com/hard.
დღეისათვის მტკიცებულების მოპოვება რამიდან ან მობილრი ტელეფონებიდან ჩვეულებრივი მოვლენაა. მოსამართლეებმა უნდა იცოდნენ განსხვავება ასეთი მტკიციებულებების მოპოვების საშუალებებს შორის და უნდა ქონდეთ წარმოდგენა მის გავლენაზე მტკიცებულების ინტეგრირებულობასთან დაკავშირებით. ცვლადი ინფორმაციის მოპოვების სირთულე არის ის, რომ იგი იკარგება, როგორც კი ტექნიკა გამოირთვება. ასეთი ინფორმაციის აღმდგენი ტექნიკური მოწყობილობა უნდა ეთანხმებოდეს შენახვისა და აღდგენის ძირითად პრინციპებს. ასევე, შესაძლოა მათი აღდგენა ქსელური სისტემიდან, რომლებიც ვერ გამოითიშება სტატიკური ანალიზის ჩატარების დროს.

3.2.3. ოპერაციული სისტემები

ფუნქციონირებისათვის კომპიუტერებს და სხვა ციფრულ ტექნიკას ჭირდება ოპერაციული სისტემა. ეს გახლავთ პროგრამა, რომელიც საშუალებას აძლევს ტექნიკურ მოწყობილობას დაუკავშირდეს პროგრამებს. ოპერაციული სისტემის გარეშე კომპიუტერი ვერ

იფუნქციონირებს. გამომდინარე კომპიუტერიდან და სხვა ციფრული ტექნიკიდან, ოპერაციული სისტემებიც განსხვავებულია.

დღეისათვის ყველაზე გავრცელებულია ვინდოუსი, უნიქს/ლინუქსი და ეფლ მაკი. არის სხვა სისტემებიც სხვა ტექნიკისათვის, როგორიცაა პერსონალური ციფრული ასისტენტი და მობილურები. მათი სისტემა გახლავთ ძირითადი სისტემების შემოკლებული ვარიანტი.

მოსამართლეებისათვის მნიშვნელოვანია, გაიგონ ოპერაციული სისტემების არსი და იცოდნენ, რომ სხვადასხვა სისტემა სხვადასხვანაირად იქცევა. მეტი ინფორმაციისათვის, ეწვიეთ: www.en.wikipedia.org/wiki/Operating Systems.

3.3. როგორ მუშაობს ინტერნეტი

სესიის ბოლოს, მონაწილეებს უნდა შეეძლოთ:

- ახსნან, თუ როგორ განვითარდა ინტერნეტი დასაწყისიდან დღემდე
- განასხვავონ ინტერნეტის ფორმები
- განსაზღვრონ, თუ როგორ შეიძლება ინტერნეტი გამოიყენონ დამნაშავეებმა

ინეტრნეტი არის ურთიერთდაკავშირებული ქსელების შემოკლებული ტერმინი. ბევრი დანაშაული ხდება ინტერნეტის გამოყენებით. ასეთი დანაშაულებია: ჰაკრობა, ვირუსების გავრცელება და ფიშინგი, ასევე თაღლითობა. მოსამართლეებისათვის აუცილებელია ინტერნეტის საფუძვლების და მისი ფორმების, როგორიცაა World Wide Web და იმეილის ცოდნა.

3.3.1. ინტერნეტის ისტორია

ინტერნეტმა თავისი არსებობა სამოციან წლეში აპრანეტით დაიწყო. მიუხედავად იმისა, რომ ქვემოთმოყვანილი ინფორმაცია არ არის პირდაპირ დაკავშირებული საკითხთან, ის ფაქტი, რომ ინტერნეტი არასოდეს ითვალისწინებდა უსაფრთხოებას, ხსნის იმას, თუ რატომ უადვილდებათ დამნაშავეებს მისი გამოყენება. პირველი ფიზიკური კავშირი დამყარდა 1969 წელს, ოთხ საუნივერსიტო კვანძს/ადგილს შორის. პირველი იმეილი გაიგზავნა 1972 წელს. შემდგომ წელს შეიქმნა ახალი საკომუნიკაციო პროტოკოლი TCP/IP, რომელიც დღეს ინტერნეტის საფუძველს წარმოადგენს. თავიდან არსებობდა ერთმანეთთან დაუკავშირებლი ქსელები. შემდეგ შემუშავდა პაკეტი, რომელიც ითვალისწინებდა ამ ქსელების დაკავშირებას.

აღნიშნულმა მომავალში გააძლიერა ქსელების დაკავშირება, რაც სწრაფად განვითარდა დასავლეთში და შემდეგ უკვე მთელ

მსოფლიოში. დღესაც შესამჩნევია ციფრული ტექნიკის გამოყენების განსხვავებები მეტად და ნაკლებად განვითარებული ქვეყნების მიერ.

ამას მოყვა ინტერნეტის კომერციალიზაცია და ინტენეტ პროვაიდერების გამოჩენა 1980-იან წლებში. ამან ხელი შეუწყო ინტერნეტის პოპილარიზაციას, რაც კიდევ უფრო გაიზარდა 90-იან წლებში. ინტერნეტს დიდი გავლენა აქვს, როგორც ბიზნესზე, ისე კულტურაზე. დღეისათვის არსებობს იმეილი, სოციალური ქსელები, ფორუმები, და სხვა. იგი იზრდება, ვითარდება და აგროვებს სულ უფრო მეტ ინფორმაციას და ცოდნას. Web 2.0-ის დაბადება ჩვენზეა დამოკიდებული.

3.3.2. როგორ ფუნქციონირებს ინტერნეტი

ინტერნეტი შეიძლება განვიილოთ, როგორც ინფრასტრუქტურა, რომელიც ერთდროულად ბევრი მიზნით გამოიყენება. თუ ინტერნეტის ერთი ნაწილი არ მუშაობს, კომუნიკაცია მაინც გრძელდება. ინტერნეტს არავინ ფლობს. იგი თვითრეგულირებადია.
ყველაზე თანამედროვე ქსელები, როგორიცაა ინტერნეტი, განსაზღვრულია, როგორც „კავშირგარეშე“ ანუ „პაკეტური ცართვა“. ტრაფიკის იყოფა პატარა პაკეტებად, რომლებიც მოძრაობენ გამგზავნელსა და მიმღებს შორის. ისინი არ მოძრაობენ ერთი მარშრუტით და კვლავ ერთდებიან, როცა მიაღწევენ დანიშნულების ადგილს.
ადამიანები ინტერნეტში შედიან პროვაიდერების საშუალებით. ესენი არიან კომერციული ორგანიზაციები, რომლებიც ქირაობენ სივრცეს. ისინი აწარმოებენ აღრიცხვას, მაგრამ რამდენი ხნით? არსებობს ეროვნული და საერტაშორისო მონაცემტა დაცვისა და კონფიდენციალურობის საკითხები, რომლებიც უკავშირდება ინფორმაციის შენახვის ვადებს. ეს რა თქმა უნდა, პირდაპირ კავშირშია ციფრული ინფორმაციის მოპოვებასთან. კავშირი ინტერნეტთან ხორციელდება Dial Up, Broadband, ISDN, საკაბელო, უკაბელო და სატელიტის გზით.
ინტერნეტის არსის გასაგებად მშვენიერი ფილმია ქსელური მეომრები. იგი კარგად უხსნის ინტერნეტის რაობას მათ, ვინც ეს არ იცის. ფილმი 12 წუთიანია და ეხება ინტერნეტის რაობას და მის სტრუქტურას, ტრანსატლანტიკური კაბელების ჩათვლით. შესაძლებელია მისი ცამოტვირთვა: www.warriorsofthe.net გერმანულ, ინგლისურ, ესპანურ, ებრაულ და სხვა ენებზე. რეკომენდირებულია, სტატისტიკური ინფორმაციის მიწოდება მსმენელებისათვის, რაც უზრუნველყოფს მათ მიერ ინეტრნეტის მათ ქვეყანაზე გავლენის გააზრებას.
აქვე მოგვყავს რამდენიმე ტერმინი, დაკავშირებული ქსელებთან და ინტერნეტთან:

- Network Internet Card – პლატა, ან კარტა, რომელიც ჯდება კომპიუტერში ინტერნეტთან კავშირის დამყარების მიზნით.
- MAC address – კვაზი-უნიკალური იდენტიფიკატორი ქსელების ადაპტორებისათვის იდენტიფიკაციის მიზნით.
- Network Hub – ანუ კონცენტრატორი, რომელიც აერთებს ოპტიკო ბოჭკოვან ეთერნეტის მოწყობილობებს და ხელს

უწყობს მათ ფუნქციონირებას, როგორც ერთი ქსელისას. ჰაბები მუშაობს ფიზიკურ შრეზე და ტერმინი „შრე 1 ჩართვა“ არის ჰაბის სინონიმი. ამგავრად, ეს ხელსაწყო არის მრავალპორტიანი რეპეტორი. ქსელების ჰაბები, ასევე, გადასცემენ გადატვირთვის სიგნალს ყველა პორტს.

- Network Switch – ქსელის მოწყობილობა, რომელიც აკავშირებს ქსელის სეგმენტებს. წარსულში გამოიყენებოდა შრე 2, რაც უფრო სწრაფი იყო. შემდეგში, იგივე სისწრაფით ხდებოდა ძებნა IP და MAC მისამართებზე.
- Router – მოწყობილობა, რომელიც ადგენს ქსელის შემდეგ წერტილს, სადაც უნდა მივიდეს ინფორმაცია. ის უნა უკავშირდებოდეს, მინიმუმ, 2 ქსელს. ტერმინი „შრე სამი“ გამოყენება როუტერის სინონიმად.
- Server – კომპიუტერი ან მოწყობილობა, რომელიც აწვდის ინფორმაციას ან მომსახურებას სხვა კომიუტერებს ან ქსელებს. ნებისმიერი კომპიპიუტერი შეიძლება იყოს სერვერი სათანადო პროგრამის ქონის შემთხვევაში. უფრო ხშირად, ეს არის მძლავრი კომიუტერი. ერთ კომპიუტერს შეუძლია რამდენიმე მომსახურების განხორციელება: ვების, იმეილის, ფიალების, ბეჭდვის და ასე შემდეგ. ბიზნესის მიზნებისათვის, გონივრულია სხვადასხვა სერვერის გამოყენება სხვადასხავ კომპიუტერებისათვის, რაც ზრდის უსაფრთხოების შანსებს.
- Local Area Network – ადგილობრივი ქსელი ფარავს მცირე გეოგრაფიულ ტერიტორიას: სახლი, სამსახური, სკოლა და ასე შემდეგ.
- Wide Area Network – ქსელი, რომელიც ფარავს უფრო ფართო გეოგრაფიას. ქალაქებს, რეგიონებსა და ქვეყნებს შორის კავშირისათვის. იყენებს როუტერებს და საჯარო კომუნიკაციის კავშირებს. მისი ცნობილი სახეა ინტერნეტი.
- არის ასევე, ბანაკის ქსელები, პერსონალური ქსელები, რომლებიც ზუსტად დასახელების მიხედვით შემოიფარგლება.
- Ports – ეს არის ქსელური კომუნიკაციის ბოლო წერტილი ანუ არხი. პორტების რიცხვი იძლევა კომპიუტერიდან სხვადასხვა ფორმის კავშირის გამოყენების შესაძლებლობას.
- Bandwidth – ინფორმაციის რაოდენობა, რომელიც შეიძლება გადაიცეს სატელეფონო ხაზით, კაბელით, სატელიტით და სხვა. რაც უფრო დიდია იგი, მით მეტ ინფორმაციას გადასცემს სწრაფად. ანუ სწრაფია კავშირი.
- Internet Protocols – არსებობს რამდენიმე პროტოკოლი, რომელთაგან ყველაზე მნიშვნელოვანია ინტერნეტის პროტოკოლი. ინტერნეტთან მიერთებულმა ყველა კომპიუტერმა უნდა გამოიყენოს პროტოკოლი. თქვენი ინტერნეტ პროტოკოლის მისამართი არის თქვენი ინტერნეტის „ტელეფონის ნომერი“, რომლის გარეშეც ვერ გამოიყენებთ ინტერნეტს. სხვადასხვა ფორმები და მომსახურება სხვადასხავ პროტოკოლს იყენებს ქსელებთან კომუნიკაციის მიზნით: ტექსტის გადაცემის პროტოკოლი, მეილის გადაცემის

პროტოკოლი, ფაილის გადაცემის პროტოკოლი და ასე შემდეგ.[92]

3.3.3. ინტერნეტ მომსახურება

World Wide Web დაიბადა 1991 წელს, როცა ტიმ ბერნერ-ლიმ გამოიგონა ჰიპერტექსტური ენა HTML, რაც საშუალებას იძლეოდა გაერთიანებულიყო სიტყვები, სურათები და ბგერები. სტანდარტები შეიმუშავა World Wide Web კონსორციუმმა.

W3 შედგება დოკუმენტებისაგან, რომლებიც ერთმანეთს ლინკებით უკავშირდებიან, რაც ობობას ქსელს წააგავს. ამიტომაც ეწოდა ვები-ქსელი (ტიმ ბერნს ლი, 1992, სექტემბერი)

ბრაუზერის საშუალებით შედიხართ ვებში: ინტერნეტ ექსპლორერი, მოზილა ფაიერფოქსი, გუგლი, საფარი და ოპერა.

HTML ის ენაა, რომელსაც კავშირის მიზნით იყენებენ ბრაუზერები და მომსახურებანი. მიუხედავად იმისა, რომ ბრაუზერის საშულებით ხდება ბევრ პროტოკოლში შესვლა, HTTP ყველაზე ხშირად გამოყენებადი პროტოკოლია. ბევრი ფიქრობს, რომ www არის ინტერნეტი. ამსვე იყენებენ კრიმინალებიც.

ტრენინგის პროგრამაში უნდა შეიტანოთ დანაშაულის მაგალიტები www-დან.

იმეილი

ეს არის ციფრული მესიჯის გაგზავნის ფორმა. გამომყენებლის თვალით ისე ჩანს, რომ ის პირდაპირ ეგზავნება მიმღებს, თუმცა ნებისმიერი მეილი მინიმუმ ოთხ კომპიუტერს გადის გზად:

1. მესიჯი დგება კლიენტის კომპიუტერში და იგზავნება მეილის გასაგზავნ სერვერზე;
2. მეილის გასაგზავნი სერვერი აგზავნის მეილს მიმღების მეილის გასაგზავნ სერვერზე.
3. მიმღების მეილის სერვერი ნახულობს მის მეილს და დებს მიმღების საფოსტო ყუთში.
4. მიმღები უკავშირდება საკუთარ მეილს და იღებს მესიჯს, რომელიც, ამ პროცესში, იშლება მეილის სერვერიდან.

მეილის სერვერი – გამოყოფილი/სპეციალური სერვერი მეილებისათვის

არსებობს მეილების რამდენიმე სახე:

- ტრადიციული აუთლუქი;
- ვებზე დამოკიდებული – POP3 მეილი. IMAP მეილი, რომელსაც ხედავთ თქვენს კომპიუტერში, მაგრამ არის მოცილებულ სერვერზე.

ახსნისას კარგია მეილის წერილთან შედარება. მეილს აქვს თავი (კონვერტი) და ტანი (თავად ტექსტი), ასევე დანართები. თავი ანუ

[92] რეკომენდირებულია, ტრენინგის კურსი შეიცავდეს ქსელების მიმსამართების დეტალურ ახსნას: მაგალითად, რომ აიპი 4-ში არის მისამართების 4 ჯგუფი, სამი ციფრით. თითოეულ ჯგუფში არის მაქსიმუმ 256 არჩევანი. თითოეულ ჯგუფს ეწოდება ოქტეტი. უნდა აიხსნას, როგორ ხდება აიპი მისმართების შემუშავება. ამის გაკეთება უმჯობესია ვიზულაური საშუალებების გამოყენებით. ასევე, უნდა აიხსნას სტატიკური და დინამიკური აიპი მისამართები და მათი გავლენა გამოძიებაზე. ახსენით აიპო 6-ის ცვლიელებები და ამ ცვლილებების საჭიროება – ინეტრნეტის ფუნქციონირება აიპი მისამართის გარეშე.

კონვერტი არის გამომძიებლებისათვის საინტერესო, რადგან შეიცავს ინფორმაციას გამგზავნელ-მიმღების შესახებ, აიპი მისამართს და სხვა საჭირო ინფორმაციას, რაც გვეხმარება გამგზავნელის ვინაობის დადგენაში. კარგია, რომ მოსამართლეები ერკვეოდნენ განსხვავებაში იმ კონვერტს შორის, რომელიც ჩანს მეილის მიღებისთანავე და გაფართოებულ კონვერტს შორის, რომელიც შეიცავს ყველა საჭირო ინფორმაციას. მეილს ყველაზე ხშირად შეხვდებიან მოსამართლეები თავიანთი საქმიანობის დროს. ამიტომ, მნიშვნელოვანია, რომ კარგად ერკვეოდნენ თანამედროვე მეილების ტიპებსა და არსებულ განსხვავებებში და იმაში, თუ რა ინფორმაცია და როგორ შეიძლება მოვიპოვოთ მეილების საშუალებით. დამატებითი ინფორმაციისათვის: www.learnthenet.com/english/html/20how.htm

ფიერ თუ ფიერ (თანაბარუფლებიანობა)

ფიერ თუ ფიერ მომსახურება წლების მანძილზე უზრუნველყოფს არალეგალური ფაილების და ინტელექტუალური საკუთრების დარღვევასთან დაკავშირებული ინფორმაციის გაცვლა-გამოცვლას. მისი კლიენტები საკმაოდ პოპულარულები არიან კრიმინალური ჯგუფებისათვის. ფიერ თუ ფიერის პირველი თაობა მუშაობდა ცენტრალური სერვერით, რომელსაც უერთდებოდნენ ისინი, ვისაც უნდოდა ფიალების ჩატვირთვა. ამან გაადვილა მათი იდენტიფიკაცია და გაუვნებელყოფა. მეორე თაობა იყენებდა განსხვავებულ და მრავალფეროვან მეთოდებს დაწყებული ხელმისაწვდომი ფიალების სიიდან, რაც აადვილებს ძებნას, დამთავრებული ისეთებით, რომლებიც ფუნქციონირებენ, როგორც ფიალების შემნახველი კვანძები.
მოსამართლეებს ჭირდებათ იცოდნენ ფიერ თუ ფიერ საქმიანობის შესახებ, რადგან მასთან შეიძლება დაკავშირებული იყოს ბევრი დანაშაული. დეტალური ცოდნა არ არის აუცილებელი: www.ezinearticles.com/?how-Peer-to-Peer-(P2P)-Works&id=60126.

ფიალების გადაცემა-გადაგზავნის პროტოკოლი -FTP

ეს არის ძლიერი პროტოკოლი, რომლის საშუალებით ხდება ერთი კომიუტერიდან მეორეში ფაილების გადაგზავნს. ის ფუნქციონირებს კლიენტი/სერვერი საფუძველზე FTP პროგრამით. როცა მომხმარებელს სურს ფაილის გაგზავნა, იგი იყენებს თავის მომხარებლის პაროლს და აგზავნის ფაილს. რატომ ჭირდებათ ამის ცოდნა მოსამართლეებს? ისინი შესაძლოა წააწყდნენ ასეთ ფაილებს, როცა დამნაშავეები ერთმანეთს უზიარებენ ინფორმაციას, ან როცა ეს გამოიყენება, როგორც გადაცემის მეთოდი სხვა პროტოკოლების მიერ, მაგალითად, ინტერნეტით საუბარი.

ნიუსგრუფი

ნიუსგრუფი ცოტა დამაბნეველი ტერმინია. აქ ხდება დისკუსიები სხვადასხვა თემებზე. ისინი ტექნიკურად განსხვავებულია, მაგრამ ისევე ფუნქციონირებს, როგორც ფორუმი. ნიუსგრუფის სერვერი აქვთ სხვადასხვა ორგანიზაციებს, რომლებიც შეთანხმებულნი

არიან სხვებთან ინფორმაციის სინქრონიზაციაში. ეს საშუალებას იძლევა, გააგზავნოთ ინფორმაცია ერთ სერვერზე და ის ხელმისაწვდომი გახდეს უფრო დიდი აუდიტორიისათვის.

ინტერნეტით მიმოწერა/საუბარი (ჩატი)

ეს რეალურად არის ტელეკონფერენციის სისტემა, რომელიც გამოიყენება დამნაშავეების მიერ ფიალების გაცვლის მიზნით და კომუნიკაციისათვის. ის მუშაობს სერვერების საშუალებით, რომლებიც დაკავშირებულია ერთმანეთთან და ცვლიან ინფორმაციას. ჩამოთვლილია სადისკუსიო თემები და შეუძლიათ ჩართვა დისკუსიებში მონაწილეობის მიღების მიზნით. ეს არ არის მომხმარებლის მიმართ ყველაზე კეთილგანწყობილი მომსახურება და გამოიყენება გამოცდილი მომხმარებლების მიერ. ეს არის პროტოკოლი, რომელიც გამოიყენება დამნაშავეების მიერ და ამიტომ, მოსამართლეებისათვის რუდიმენტული ცოდნის აუცილებლობა ნამდვილად დგება დღის წესრიგში.

სასწრაფო მესიჯი და სოციალური ქსელები

ეს არის მეთოდი, რომელიც ბოლო წლებში ყველაზე მეტად პოპულარულია. ამ გვერდის უპირატესობა არის მის შესაძლებლობაში, შექმნას პერსონალური ფაილი და გაუზიაროს ინფორმაცია სხვებს, მათ შორის, გაცნობის მიზნით. შესაძლებელია მუსიკის, ფოტოებისა და ფილმების გაცვლა. პერსონალური ინფორმაციაა რაც იზიდავს დამნაშავეებს, იდენტობის ქურდებს, ბავშთა პორნოგრაფიის მოყვარულებს და სხვა. დამატებითი ინფორმაციისათვის, იხილეთ: www.communication.howstuffworks.com/how0social-networs-work.htm.
მისი საშუალებით ხდება კონკრეტულ სისტემში ჩართულ მომხმარებლებს შორის შეტყობინებების რეალურ დროში გაცვლა.

3.4. როგორ იყენებენ დამნაშავეები ტექნოლოგიებს

სესიის დასრულებისას, მონაწილეებმა უნდა შეძლონ:

- ახსნან იმ საშუალებები, რომლებსაც იყენებენ დამნაშავეები.

დასაწყისშივე მნიშვნელოვანია ავხსნათ, რომ არსებობს ბევრი ტერმინი ტექნოლოგიების დანაშაულებრივი მიზნით გამოყენების აღწერის მიზნით: კომპიუტერული დანაშაული, მაღალტექნოლოგიური დანაშაული, კიბერდანაშაული და სხვა, რაც შესაძლოა დავყოთ ასე:

3.4.1. ტექნოლოგია-მსხვერპლი

ტექნოლოგია, როგორც საშუალება ისეთი კომპიუტერული დანაშაულებისათვის, როგორიცაა ჰაკერობა, უარი მომსახურებაზე და ვირუსების გავრცელება;

3.4.2. ტექნოლოგია დანაშაულის დამხმარე საშუალება

კომპიუტერი და სხვა ტექნოლოგიები ეხმარებიან დამანშავეებს დანაშაულის ჩადენაში: დოკუმენტების გაყალბება, მუქარის წერილები, შანტაჟი და სხვა.

3.4.3. ტექნოლოგიები – კომუნიკაციის საშუალებანი

დამნაშავეები იყენებენ ტექნოლოგიებს, როგორც კომუნიკაციის საშუალებას, რაც ამცირებს მათი აღმოჩენის შანსებს, მაგალითად დაშიფვრის ტექნოლოგია.

3.4.4. ტექნოლოგიები – ინფორმაციის შენახვის მოწყობილობა

ინფორმაციის განზრახვით ან განუზრახველად შენახვა, რომელიც არსებობს მსხვერპლის, მოწმის ან ეჭვმიტანილის კომპიუტერში.

3.4.5. ტექნოლოგიები – დანაშაულის მოწმე

ეს ხდება, როცა მტკიცებულება არსებობსბ კომპიუტერში. ასე შეიძლება მოწმის მიერ შემოთავაზებული ალიბის დადასტურება ან უარყოფა.

3.5.მოკლე მიმოხილვა

ამ თავში შევეცადეთ გადმოგვეცა ტექნოლოგიების ტიპები და დონეები, რაც საჭიროა მოსამართლეებისათვის. ეს არ გახლავთ სრული ანალიზი ყველა არსებული ინფორმაციის ჩათვლით.
საჭიროა, რომ ტრენერებმა უზრინველყონ მასალის განახლება, რატა შეიცავდეს აუხლოეს მიღწევებს ტექნოლოგიებში. ტექნოლოგიებს გავლენა აქვთ დამანშავეების ქცევაზე, სამართლებრივ გადაწყვეტილებაზე და სხვა. არსებობს ისეთი ტექნოლოგიური ცვლილებები, რომლებსაც გავლენა აქვთ სისხლის სამრთლის სისტემაზე: მონაცმეთა შენახვა 2.0.

როგორც ყველა სხვა ტრენინგს, მოსამართლეების ტრენინგსაც უნდა ქონდეს ნათლად განსაზღვრული მიზნები, რომლებიც იქნება კონკრეტული, გაზომვადი, მიღწევადი, შესაბამისი და დროზე მორგებული. ეს უზრუნველყოფს მიზნების მიღწევას. მიზნების მიღწევის გასაზომად ნუ გამოიყენებთ სიტყვებს: გაგება და ცოდნა (ეს არ იზომება). გამოიყენეთ – ჩამოთვლა (გაზომვადია).
ასეთი ტრენინგისათვის შესაფერისია სიტუაციური სავარჯოშოების გაკეთება. ტრენერის ძირიტადი ფუნქციაა, უზრუნველყოს სასწავლო პროცესის ზოგადი და კონკრეტული ამოცანების მიღწევა. ეს თავი სწორედ ამისათვის არის განსაზღვრული.

4. კომპიეტერული დანაშაული – სისხლის სამრთლის დანაშაული

სესიის დასრულებისას მონაწილეებმა უნდა გაიაზრონ და ესმოდეთ:
- ის ქმედება, რომელიც შეადგენს სისიხლის სამართლის დანაშაულს

რეკომენდირებულია, რომ მონაწილეებს საშუალება ქონდეთ ნახონ კომპიუტერული დანაშაულის ევროსაბჭოს კონვენცია www.coe.int/cybercrime . კონვენცია ხელმისაწვდომია სხვადასხვა ენაზე.

მონაწილეებს, ასევე, საშუალება უნდა ქონდეთ, ნახონ საკუთარი კანონმდებლობა. პროფილის ნახვა შესაძლებელია www.coe.int/cybercrime.

შემდეგი თავი ეხება კომპიუტერული დანაშაულის ყველაზე მნიშვნელოვან სფეროებს და მათზე ევროსაბჭოს კონვენციის სამართლებრივ პასუხებს.

თქვენი ქვეყნის რომელი კანონმდებლობა ეხება კომპიუტერულ დანაშაულს?
ადგილობრივი შესაბამისი კანონმდებლობის მიმოხილვა.

4.1 არასანქცირებული/უკანონო შეღწვა (“ჰაკერობა”)

4.1.1 მოვლენა

მას შემდეგ, რაც კომპიუტერული ქსელები შეიქმნა, ხდებოდა მათი შესაძლებლობის გამოყენება სხვა კომპიუტერის მონაცემებში შესვლისა და მონაცემების მოპოვების კრიმინალური მიზნით. ტერმინი “ჰაკერობა” გამოიყენება კომპიუტერის სისტემაში[93] უკანონო შეღწევის აღწერის მიზნით. იმ ფაქტის გამო, რომ ბევრი ცნობილი ორგანიზაციის კომპიუტერულ სუსტემებზე, როგორიცაა ნასა, პენტაგონი, გუგლი, ესტონეთისა და გერმანიის მთავრობა, გახნორციელდა შეტევები, ჰაკერობა კომპიუტერული დანაშაულის ერთ-ერთი ყველაზე ცნობილი ფორმა გახდა.[94] ეს გახლავთ კომპიუტერული დანაშაულის უძველესი ფორმა.[95] პირველად კომპიუტერულ სისტემებში უკანონო შეღწევის ფაქტები აღმოჩენილი

[93] კონვენციაში გაწევრიანება რეგულირდება მუხლით 37.
[94] არაწევრი ქვეყნების მიერ კონვენციის გამოყენების შესახებ იხილეთ ჰერკე: ნაციონალური, რეგიონული და საერთაშორისო მიდგომა კიბერდანაშაულის წინააღმდეგ ბრძოლაში, 2008, გვ.7
[95] ადრეულ პერიოდში ჰაკერობა ნიშნავდა სისტემისაგან მეტიი ინფორმაციის მიღების მცდელობას, ვიდრე ეს იყო გათვალისწინებული. ამ კონტექსტში იგი ხშირად პოზიტიური მნიშვნელობით გამოიყენებოდა.

იქნა ქსელური ტექნოლოგიების[96] დანერგვასთან ერთად. ეს დღესაც საკმაოდ გავრცელებული ფორმაა.

უფლების გარეშე კომიუტერულ სისტემაში შეღწევა, ძალიან ხშირად, გახლავთ ისეთი კომბინაციების პირველი საფეხური, როგორიცაა ფიშინგი[97] და იდენტობის მოპარვა[98]. ის ფაქტი, რომ 2007 წლის აგვისტოში ჩატარებული კვლევის დროს მსოფლიოს მასშტაბით აღმოჩენილი იქნა ჰაკერობის 250 მილიონი ინციდენტი თავად მეტყველებს ამ სახის დანაშაულის მნიშვნელობაზე.[99]

აღიარებული საქმეებიდან გამომდინარე, დამნაშავეთა მოტივაცია, ხშირ შემთხვევაში, დადგენილი იქნა[100] და მოიცავდა პოლიტიკურიდან დაწყებული უბრალო მაქინაციურ მიზნებს. დამნაშავისათვის ქსელის საშუალებით შენახულ მონაცემებში შეღწევის უპირატესობა მდგომარეობს იმაში, რომ მას არ ჭირდება მოატყუოს სამიზნე კომპიუტერის უსაფრთხოების საშუალებები, გათვლილი ფიზიკურ შეღწევაზე და არც დანაშაულის ადგილას ყოფნა ჭირდება.

4.1.2 სამართლებრივი რეაგირება

ზემოაღნიშნულიდან გამომდინარე, უცნაურია, რომ ყველა ქვეყანა არ ახდენს კომპიუტერულ სისტემაში შეღწევის დანაშაულის კლასიფიკაციას. ქვეყანა, რომელიც ამას დიდი ხნის განმავლობაში არ აკეთებდა არის გერმანია. 2007 წლამდე ასეთი ქმედებები არ განიხილებოდა გერმანიის სისხლის სამართლის კოდქსით[101].

---

[96] ჰაკერული შეტევების მსხვერპლთა მიმოხილვის მიზნით იხილეთ: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, საინფორმაციო ომი და საერთაშორისო თანამშრომლობა, სამართლებრივი ელემენტები, 2002, №5, გვ. 825 შედეგის ნახვის მიზნით, იხილეთ ბიგელი: ჩვენს ცონტროლს მიღმა? ჩვენი სამართლებრივი სისტემის საზღვრები კიბერდანაშაულის ეპოქაში, 2001, გვ.231..

[97] ლევი: ჰაკერები, 1984; ჰაკერული დანაშაული, ავსტრალიის კრიმინოლოგიის ინსტიტუტი, 2005: ://www.aic.gov.au/publications/htcb/htcb005.pdf. ტეილორი, ჰაკტივიზმი: დაკარგული ეთიკის ძიებაში, გვ. 61.

[98] იმის გამო, რომ სისხლის სამართლის კანონმდებლობის უმეტესობა არ ცნობდა ასეთ დანაშაულს, ბევრ ქვეყანაში არ ხდებოდა ასეთი დარღვევების გამოძიება მანამ, სანამ არ მოხდა სისხლის სამართლის კანონმდებლობის შეცვლა.

[99] ტერმინი ფიშინგი აღწერს მნიშვნელოვანი ინფორმაციის თაღლითობისთ ხელში ჩაგდებას (კოდური სიტყვა), სანდო ადამიანად ან ბიზნესპიროვნებად წარდგენის გზით (ფინანსური ორგანიზაცია) ელექტრონული კომუნიკაციის დროს. ფიშინგის საწინააღმდეგო ჯგუფის მიერ მოპოვებული ინფორმაცია იხილეთ: www.antiphishing.org; ჯეკობსონი, ადამიანური ფაქტორი და ფიშინგი: http://www.informatics.indiana.edu/markus/papers/aci.pdf; ჰერკე: ტერმინი ფიშინგი ნიშნავს მოქმედებას, რომელიც მიმართულია მსხვერპლის მიერ საიდუმლო ინფორმაციის გამჟღავნებისაკენ. ადრე იგი ნიშნავდა, იმეილების გამოყენებას პაროლისა და ფინანსური ინფორმაციის გაგების მიზნით. ოლმანი, ფიშინგის სახელმძღვანელო: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. მისი გაგება და თავიდან აცილება: მეტი ინფორმაციისათვის იხილეთ ქვემოთ, თავი 2.

[100] იდენტობის მოპარვა ნიშნავს დანაშაულს და მოტყუების გზით ადამიანსი იდენტობის ინფორმაციის მოპოვებას. მეტი ინფორმაციისათვის, ჰერკე: ინტერნეტთან დაკავშირებული იდენტობის მოპარვა, 2007: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_co-operation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf;

[101] ინტერნეტის ჰაკერების სამეთვალყურეო გვერდზე იბეჭდება ანგარიშები ჰაკერული შეტევების შესახებ. წყაროებზე დაყრდნობით, 2007 წლის აგვისტოში განხორციელდა 250 მილიონი ჰაკერული შეტევა: www.hackerwatch.org.

გამოძიების დასაწყებად საჭირო იყო დამნაშავის მიერ მონაცემთა შეცვლა.

ქვეყნების მიერ კომპიუტერული დანაშაულის სისხლის სამართლის კვალიფიკაციის მინიჭების საკითხებში საკმაოდ დიდი არათანმიმდევრობა შეიმჩნევა. ზოგი ქვეყანა, მაგალითად რუმინეთი, სისხლის სამართლის დანაშაულებრივ კვალიფიკაციას ანიჭებს კომპიუტერულ სისტემაში შეღწევასაც კი[102], მაშინ როცა, სხვა ქვეყნები ასე თვლიან მხოლოდ იმ შემთვევაში, თუ შეღწევა ხდება დაცულ სისტემაში ან თუ დამნაშავეს აქვს ზიანის მიყენების ან მონაცემების მიღების, მოდიფიცირების ან დაზიანების[103] მიზანი. სხვა ქვეყნები სისტემაში უბრალო შეღწევას არ ანიჭებენ სისხლის სამართლის დანაშაულის კლასიფიკაციას. ასეთად კვალიფიცირდება შემდგომ ეტაპზე ჩადენილი დანაშაული.[104]

კომპიუტერული დანაშაულის შესახებ კონვენცია შეიცავს დებულებას არასანქცირებული/არაკანონიერი შეღწევის შესახებ, რაც იცავს კომპიუტერული სისტემის ინტეგრირებულობას. დაცვის მიზანი არის კომპიუტერული სისტემების ინტერგირებულობის დაცვა.[105]

მუხლი 2 – არაკანონიერი შეღწევა

ყველა მხარე განსაზღვრავს და დაამტკიცებს ისეთ საკანონმდებლო და სხვა ღონისძიებებს, რომლებიც საჭიროა დანაშაულის სისხლის სამართლის დანაშაულად მიჩნევისათვის იმ შემთხვევაში, როცა დანაშაული ჩადენილია წინასწარ განზრახვით და მოიცავს კომპიუტერული სისტემის ნაწილში ან მთლიანად სისტემაში უკანონო შეღწევას. მხარეს შეუძლია მოითხოვოს, რომ ქმედება ჩაითვალოს დანაშაულად თუ იგი განხორციელდა უსაფრთხოების ზომების დარღვევით, კომპიუტერული მონაცემების მოპოვების ან სხვა უპატიოსნო მიზნებით, ან კომპიუტერულ სისტემასთან მიმართებაში, რომელიც დაკავშირებულია სხვა კომპიუტერულ სისტემასთან.

აღნიშნული დებულება დანაშაულად არ განსაზღვრავს კომპიუტერულ სისტემაში შეღწევის კონკრეტულ მეთოდს. იმის უზრუნველსაყოფად, რომ ახალი ტექნოლობიების ყოველმა ახალმა განვითარებამ და აღმოჩენამ არ გამოიწვიოს კანონმდებლობის შეცვლა. აღნიშნული დებულებაში ტექნოლოგიებთან მიმართებაში

[102] ეს მოიცავს ტექნიკური საშუალებების ავლის მარტივი მტკიცებულებებიდან იმ მცდელობის ჩათვლით, რომელიც მიმართულია კომპიუტერში შენახული ინფორმაციის მიღებით.
[103] ჰერკე, კონვენციისა და გერმანიის არსებული კანონმდებლობის შედარება, 2004, 729.
[104] იხილეთ რუმინეთის კანონი 161/2003. ხელმისაწვდომია ევროსაბჭოს ვებ-გვერდზე.
[105] უბრალოდ კომპიუუერში შეღწევის დანაშაულად აღიარების მოწინააღმდეგეები მიუთითებენ ისეთ სიტუაციებზე, როცა ასეთი შეღწევით არ წარმოიქმნება საშიშორებანი ან როცა ისინი ხელს უწყობენ კომპიუტერული სისტემის სუსტი ადგილების აღმოჩენას. ეს მიდგომა არსებობს არა მხოლოდ ეროვნულ კანონმდებლობაში, არამედ რეკომენდირებული იყო ევროსაბჭოსთვისაც. იხილეთ, რეკომენდაციები №89 (9).

ნეიტრალური ტერმინებია გამოყენებული. თუმცაღა, დებულებაში მითითებულია, რომ დამნაშავე უნდა მოქმედებდეს წინასწარგანზრახულად[106] და უკანონოდ[107], უფლების არქონით.

აღნიშნული დებულების განხორციელების პროცესში, კონვენციის წევრ ქვეყნებს აქვთ ამ დებულების გამოყენების შეზღუდვის სხვადასხვა შესაძლებლობა. მაგალითად, მათ შეუძლიათ მოითხოვონ უსაფრთხოების ზომების გვერდის ავლის აუცილებლობა ან დამნაშავის მიერ კომპიუტერული მინაცემების მიღების სპეციალური განზრახვა.

პრაქტიკული ინფორმაცია მოსამართლეებისათვის:

ინფორმაციის უკანონო შეღწვასთან დაკავშირებული ორი ძირითადი გამოწვევა არის შეტევების ავტომატიზაცია და სოციალური ინჟინერიის ტექნიკის გამოყენება კომპიუტერულ სისტემაში შეღწევის მიზნით.

როგორც უკვე აღნიშნული იყო, კვლევების შედეგად დადგინდა, რომ დაახლოებით 200 მილიონი ჰაკერული შეტევა ხორციელდება ყოველ თვეში.[108] ასეთი დიდი ციფრი არის პროგრამული უზრუნველყოფის ხელმისაწვდომობის შედეგი, რაც საშუალებას აძლევს დამნაშავეს მოახდინოს შეტევების ავტომატიზაცია და შეუტიოს რამდენიმე ასეულ კომპიუტერულ სისტემას ყოველდღე.[109] ერთ-ერთი პრაქტიკული ხასიათის გამოწვევა მოსამართლეებისათვის და, საერთოდ სასამრთლოსათვის, არის ის ფაქტი, რომ განსხვავებით დამნაშავისაგან, მათ არ შეუძლიათ აუცილებელი სამართალწარმოების ავტომატიზაცია. ეს განსაკუთრებით ეხება შემთხვევებს, როცა ბრალდება ეფუძნება ერთეული მსხვერპლების მიერ აღნიშნულ ინციდენტებს.

კიდევ ერთი გამოწვევა თავს იჩენს, როცა დამნაშავე კომპიუტერულ სისტემაში შეღწევის მიზნით იყენებს არა ტექნიკურ საშუალებებს, არამედ სოციალური ინჟინერიას. სოციალური ინჟინერიას ახასიათებს ადამიანების მანიპულაცია, მაგალითად, კომპიუტერულ სისტემაში შეღწევის მიზნით.[110] თუ დამნაშავეს შეუძლია მოახდინოს მომხმარებლის მანიპულირება და, მაგალითად, მიიღოს მისგან კოდური სიტყვა, ეს არ იქნება საკმარისი დავამტკიცოთ, რომ იგი არ არის კანონიერი მომხმარებელი. ასეთ შემთხვევაში აუცილებელია, ზუსტად გავაანალიზოთ კონტექსტი, რომელშიც მოხდა კოდური სიტყვის მომხმარებლის მიერ დასახელება, რამაც საშუალება მისცა დამნაშავეს შეეღწია კომპიუტერულ სისტემაში, რათა დავამტკიცოთ, რომ კოდური სიტყვის გათქმა არ ხდის ჩადენილ დანაშაულს კანონიერს.

[106] ამის მაგალითია გერმანიის სისხლის სამართლის კოდექსი, რომელშიც დანაშაულად ითვლებდა მხოლოდ ინფორმაციის მოპოვება. ეს დებულება შეიცვალა. ქვემოთ მოცემული დებულება ძალაში იყო 2007 წლამდე:

ნაწილი 202ა-შპიონობა მონაცემებზე

(1) სანქცირების გარეშე ისეთი ინფორმაციის მოპოვება საკუთარი ან სხვისი მიზნებისათვის, რომელიც არ არის მათთვის განკუთვნილი და დაცული არის არასანქცირებული შეღწევისაგან, ისჯება ჯარიმით ან პატიმრობით სამი წლის ზევით.

(2) ზემოთმოყვანილ ქვეპუნქტთან დაკავშირებით, მონაცმეად ითვლება ის ინფორმაცია, რომელიც შენახულია ან გადაიცა ელექტრონულად ან სხვა ფორმით და არ წარმოადგენს მყისიერად აღსაქმელ ფორმას.

[107] ახსნა-განმარტებითი ანგარიში, №22.

[108] ახსნა-განმარტებითი ანგარიში ევროსაბჭოს კიბერდანაშაულის შესახებ, №39.

[109] ელემენტი „უფლების გარეშე“ არის კონვენციის საერთო კომონენტი სისხლის სამართლის კანონმდებლობაში.

[110] ჰაკერების სამეთვალყურეო გამომცემლობა აქვეყნებს ანგარიშებს ჰაკერული შეტევების შესახებ. წყარო იუწყება, რომ 2007 წლის აგვისტოში 250 მილიონი ჰაკერული შეტევა განხორციელდა.

როგორ არის განსაზღვრული ეს დანაშაული თქვენი ქვეყნის კანონმდებლობაში?
ადგილობრივი კანონმდებლობის დებულებების განხილვა და სიტუაციური სავარჯიშოები

4.2 ინფორმაციისა და მონაცემების არაკანონიერი ხელში ჩაგდება მათი გადაცემის დროს

4.2.1 მოვლენა

ინფორმაციის გადაცემის დროს შესაძლოა გადაცემის მონაცემების ხელში ჩაგდება, რისი ერთ-ერთი მაგალითიც გახლავთ კომუნიკაციის ჩაწერა უკაბელო ქსელში ინფორმაციის მოძრაობის დროს. მაგალითად, თუ დამნაშავე ხელში ჩაიგდებს კომუნიკაციას კომპიუტერულ სისტემასა და შეღწევის უკაბელო პუნქტს შორის, მას შეუძლია მოიპოვოს ყველა დაუშიფრავი კომუნიკაცია, როგორიცაა გაგზავნილი ან მიღებული იმეილი ან გახსნილი ვებ-გვერდები. თუ მხედველობაში მივიღებთ საკომუნიკაციო საშუალებებთან უკაბელო კავშირის ხელმისაწვდომობას (მობილურის კავშირი ბლუტუსის საშუალებით), აუცილებელი ხდება თვალყური ვადევნოთ ტექნოლოგიების დაუცველობას არაკანონიერი შეღწევის თვალსაზრისით.[111]

4.2.2 სამართლებრივი რეაგირება

კონვენცია კომპიუტერული დანაშაულის შესახებ მოიცავს დებულებას, რომელიც ეხება არასაჯარო ინფორმაციის გადაცემის პროცესის დაცვას მასში არასანქცირებული შეღწევისათვის დანაშაულის კვლაიფიკაციის მინიჭებით.[112] ასეთი მიდგომით, კონვენცია მიზნად ისახავს ინფორმაციის ელექტრონული გადაცემის დაცვის გათანაბრებას სატელეფონო საუბრების არასანქცირებული მოსმენისაგან დაცვასთან.[113]

მუხლი 3 – ინფრომაციისა და მონაცემების არაკანონიერი ხელში ჩაგდება გადაცემის პროცესში

ყველა მხარემ უნდა დაამტკიცოს საკანონმდებლო და სხვა სახის ღონისძიებები, რაც საჭიროა არაკანონიერად და წინასწარ განზრახვით ინფორმაციის გადაცემის პროცესში ხელში ჩაგდების დანაშაულებრივ ქმედებად კვალიფიკაციის მიზნით, როცა ეს ხორციელდება კომპიუტერული მონაცემებიდან არასაჯარო ინფორმაციის სხვა კომპიუტერულ სისტემაში გადაცემის დროს ტექნიკური საშუალებების გამოყენებით. ამაში შედის კომპიუტერის ინფორმაციის მატარებელი ელექტრომაგნიტური გამოსხივება. მხარეს შეუძლია მოითხოვოს, რომ ქმედება ჩაითვალოს დანაშაულად თუ იგი განხორციელდა უსაფრთხოების ზომების დარღვევით, კომპიუტერული მონაცემების მოპოვების მიზნით ან ან სხვა უპატიოსნო მიზნებით, ან კომპიუტერულ სისტემასთან მიმართებაში, რომელიც დაკავშირებულია სხვა კომპიუტერულ სისტემასთან.

[111] ავტომატიზირებულ შეტევებთან დაკავშირებით იხილეთ თავი 2.6.
[112] დამატებითი ინფორმაციისათვის იხილეთ მიტნიკი/საიმონი/ უორნიაკი" მოტყების ხელოვნება: უსაფრთხოების ადამიანური ელემენტის კონტროლი.
[113] კანგი, უკაბელო ქსელის უსაფრთხოება – კიდევ ერთი სირთულე კიბერდანაშაულთან მიმართებაში, კიბერდანაშაული და უსაფრთხოება, ტომი 2, გვ.6.

აღნიშნული მუხლი დანაშაულის კვალიფიკაციას ანიჭებს არასაჯარო ინფორმაციის არაკანონიერად ხელში ჩაგდებას მონაცემების გადაცემის დროს მისი ხელში ჩაგდებისას. ეს არ ეხება არც საჯარო ინფორმაციას და არც არატექნიკური საშუალებებით გადაცემული ინფორმაციის ხელში ჩაგდებას.[114] კონვენციის განმარტებით ბარათში მოცემულია, რომ გადაცემა არის არასაჯარო თუ გადაცემის პროცესი არის კონფიდენციალური.[115] სწორედ ამიტომ, საჭიროა გავაანალიზოთ გადაცემის პროცესი. საერთოდ, ინდივიდუალური კომუნიკაცია (იმეილების გაგზავნა ან ვებ-გვერდიდან ინფორმაციის მიღება) ითვლება არასაჯარო ინფორმაციად. დანაშაულებრივი ქმედება უნდა იქნეს ჩადენილი წინასწარ განზრახვით და არაკანონიერად.

პრაქტიკული ინფორმაცია მოსამართლეებისათვის:

ინფორმაციის არაკანონიიერი გზით გადაცემის პროცესში ხელში ჩაგდებასთან დაკავშირებული ერთ-ერთი გამოწვევა არის ის ფაქტი, რომ ამ დებულების მოქმედება საკმაოდ შეზღუდულია. დებულების მიხედვით ხდება გადაცემის პროცესის ხელში ჩაგდების დანაშაულად აღიარება და იგივე არ ეხება კომპიუტერში შენახული ინფორმაციის ხელში ჩაგდებას.[116] კომპიუტერში შენახულ ინფორმაციასთან შეღწევა არ ითვლება ინფორმაციის გადაცემის მომენტში ხელში ჩაგდებად.[117] მონაცემების გადაცემის პროცესის არსებობის მოთხოვნის გამო, აღნიშნული დებულება არ მოქმედებს სარეგისტრაციო პროგრამის მიერ(ლოგერი) შენახული ინფორმაციის ხელში ჩაგდებას.[118]

როგორ არის განსაზღვრული ეს დანაშაული თქვენი ქვეყნის კანონმდებლობაში?
ადგილობრივი კანონმდებლობის დებულებების განხილვა და სიტუაციური სავარჯიშოები

[114] მუხლი 2-ის მსგავსად, მუხლი 3 საშუალებას აძლევს წევრ ქვეყნებს მიუსადაგონ დანაშაულად აღიარება დამატებითი ელემენტების მოთხოვნის გზით აღსრულების პროცესში, როგორიცაა „უპატიოსნო მიზნები“ ან კავშირი კომპიუტერულ სისტემასთან, რომელიც მიერთებულია სხვა კომპიუტერულ სისტემასთან.
[115] ახსნა-განმარტებითი ანგარიში №60.
[116] ამ კონტექსტში, დებულება ეხება მხოლოდ ტექნიკური საშუალებების გამოყენებით ინფორმაციის გადაცემის პროცესში მის ხელში ჩაგდებას. მუხლის 3 არ ეხება სოციალურ ინჟინერიას.
[117] ახსნა-განმარტებითი ანგარიში №54
[118] ჰერკე, კონვენცია კიბერდანაშაულის შესახებ, 2004, გვ.730.

4.3 მონაცემებში ჩარევა

4.3.1 მოვლენა

ამჟამად, სულ უფრო და უფრო მეტი ინფორმაციის შენახვა ხდება ციფრულ ფორმატში, რაც ნიშნავს, რომ ასეთი ინფორმაციის განადგურებისაკენ მიმართულმა მანიპულაციამ შესაძლოა გამოიწვიოს დიდი ზარალი. კორპორაციული შემთხვევებისაგან განსხვავებით, როცა საგნის დაზიანების სურვილი, ზოგადად, მოითხოვს ფიზიკურ შეღწევას, კომპიუტერული მონაცემების დაზიანება ზოგ შემთხვევაში შესაძლოა ინფორმაციის შემნახავ ინსტრუმენტში ფიზიკურად არყოფნის შედეგადაც. ერთი მაგალითი არის ისეთი პროგრამული უზრუნველყოფა, როგორიცაა კომპიუტერული ვირუსი. კომპიუტერული ვირუსები არის პროგრამული უზრუნველყოფის ინსტრუმენტები, რომელთა ინსტალაცია ხდება მსხვერპლის კომპიუტერში მისი ნებართვის გარეშე წაშლის ოპერაციის განხორციელების მიზნით.[119]

არასანქცირებული შეღწევის მსგავსად, მონაცემებში შეღწვა შესაძლოა განვიხილოთ, როგორც ტრადიციული კომპიუტერული დანაშაული. პირველი ვირუსები გამოჩნდა 1970 წელს.[120] მას შემდეგ, მნიშვნელოვნად გაიზარდა[121] არა მხოლოდ ვირუსების რაოდენობა, არამედ მათ მიერ გამოწვეული ზიანიც. ქსელების მზარდი გამოყენება საშუალებას აძლევს ვირუსებს გავრცელდნენ ბევრად სწრაფად, ვიდრე ეს ხდებოდა ადრე, როცა გავრცელების ერთადერთი გაზა იყო დისკების გაცვლა, და დააინფიცირონ ბევრად მეტი რაოდენობის კომპიუტერული სისტემა მანამ, სანამ მოხდება დაცვის მექანიზმების მისადაგება.

ერთ-ერთი მაგალითი გახლავთ “სასიყვარულო ხოჭო” – “ლავ ბაგ”, რომელიც არის კომპიუტერის ვირუსი, შემუშავებული 2000 წლის ფილიპინების შემთხვევაში ეჭვმიტანილის მიერ[122] და, რომელმაც დააინფიცირა მილიონობით კომპიუტერი მსოფლიოს მასშტაბით.[123] გავრცელების მზარდმა ტემპმა გავლენა იქონია ზიანზე, რომელიც გამოიწვია ვირუსების შეტევამ. 2000 წელს ასეთი შეტევებით

[119] არ არის ზუსტი ამ კონტექსტში: ახსნა-განმარტებითი ანგარიში №53

[120] ინსტრუმენტების მიმოხილვის მიზნით: ახალი ამბები ჰაკერულ შეტევებში: ტიპების, მეთოდების, საშუალებებისა და პრევენციის ზოგადი მიმოხილვა: http://www.212cafe.com/download/e-book/A.pdf. კილოგერების ფასთან დაკავშირებით (200 – 500 აშშ დოლარი) : პაგეტი, იდენტობის მოპარვა, თეთრი ქაღალდი, მაკაფე, 2007: http://www.mcafee.com/us/threat_center/white_paper.html.

[121] სპაფორდი: ინტერნეტის ვირუსის პროგრამა: ანალიზი, გვ.3; კოენი, კომპიუტერული ვირუსები-თეორია და ექსპერიმენტი: – available at: http://all.net/books/virus/index.html. კოენი, კომპიუტერული ვირუსები; *იქვე*, “კომპიუტერული ვირუსების აბსტრაქტული თეორიავირუსების ეკონომიკური ზემოქმედების შესახებ იხილეთ კაშელი/ჯეკსონი/ჯიკლინგი/ვებელი: კიბერშეტევების ეკონომიკური შედეგი, გვ 12; სიმანტეკი “ ინტერნეტის უსაფრთხოების საფრთხე”, ივლისის ტენდენციები-დეკემბერი 2006: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf .

[122] კომპიუტერის ერთ-ერთი პირველი ვირუსი იყო ბარაიენი, რომელიც შექმნეს ბასიტმა და ამჯად ფარუკ ალვიმა. დამატებითი დეტალებისათვის: http://en.wikipedia.org/wiki/Computer_virus.

[123] უაიტი/კაფარტი/ჩესი: კომპიუტერის ვირუსები: გლობალური პერსპექტივა: http://www.research.ibm.com/antivirus/SciPapers/White/VB95/vb95.distrib.html.

გამოწვეულმა ფინანსურმა ზარალმა 17 მილიარდ ამერიკულ დოლარს მიაღწია.[124]

ადგილობრივ გამოძიებას ხელს უშლიდა[125] ის, რომ მსგავსი საქმიანობა ფილიპინებში[126] არ იყო სათანადოდ კლასიფიცირებული, როგორც სისხლის სამართლის დანაშაული.

4.3.2 სამართლებრივი რეაგირება

კონვენციის მუხლი 4 შეიცავს დებულებას, რომელიც მონაცემთა ინტეგრირებულობას იცავს არასანქცირებული და არაკანონიერი ჩარევისაგან.[127] დებულების მიზანი არის არსებული თეათრი ადგილების შევსება სისხლის სამართლის ეროვნულ კოდექსში და კომპიუტერული სისტემებისა და პროგრამების იმგვარი დაცვა, როგორიც აქვთ კორპორაციულ სუბიექტებს წინასწარგანზრახული დაზიანების საწინააღმდეგოდ.[128]

> მუხლი 4 – მონაცემებში ჩარევა
>
> (1) ყველა მხარე განსაზღვრავს და დაამტკიცებს ისეთ საკანონმდებლო და სხვა ღონისძიებებს, რომლებიც საჭირო იქნება ადგილობრივი კანონმდებლობის მიხედვით დანაშაულის სისხლის სამართლის დანაშაულად მიჩნევისათვის, როცა ეს დანაშაული ჩადენილია წინასწარი განზრახვით და არაკანონიერად და მოიცავს მონაცემთა დაზიანებას, წაშლას, დამახინჯებას, შეცვლას ან ბლოკირებას.
> (2) ნებისმიერ მხარეს შეუძლია დაიტოვოს უფლება, რომ დანაშაულის კვალიფიკაცია მიეცეს პუნქტი 1-ით განსაზღვრულ მხოლოდ იმ დანაშაულს, რომელსაც თან სდევს სერიოზული ზიანი.

მუხლი არა მხოლოდ სისხლის სამართლის კვალიფიკაციას ანიჭებს კომპიუტერული მონაცემების დაზიანებას და წაშლას, მაგალითად

---

[124] დამატებითი ინფორმაციისათვის, http://en.wikipedia.org/wiki/ILOVEYOU; ვირუსების კრიტიკულ ინფრასტრუქტურაზე ზემოქმედების შესახებ ინფორმაციისათვის: ბრუკი, "ILOVEYOU" ვირუსი ცხადჰყოფს მეტი კოორდინაციისა და სიფრხილის საჭიროებას, 2000: http://www.gao.gov/archive/2000/ai00181t.pdf.

[125] დანატებითი ინფორმაციისათვის იხილეთ განმარტებითი ანგარიში 60.

[126] დამატებითი ინფორმაციისათვის იხილეთ: ://en.wikipedia.org/wiki/ILOVEYOU; ვირუსების კრიტიკულ ინფრასტრუქტურაზე ზემოქმედების შესახებ ინფორმაციისათვის: ბრუკი, "ILOVEYOU" ვირუსი ცხადჰყოფს მეტი კოორდინაციისა და სიფრხილის საჭიროებას: http://www.gao.gov/archive/2000/ai00181t.pdf..

[127] ბი-ბი-სი: პოლიცია უახლოვდება ლავ ბაგის საქმეში დამნაშავეს: http://news.bbc.co.uk/1/hi/sci/tech/738537.stm. გამოყენებულ ტექნოლოგიებთან დაკავშირებით: http://radsoft.net/news/roundups/luv/20000504,00.html.

[128] სი-ენ-ენ: ლოვ ბაგ ვურუსი ზრდის კიბერტერორიზმის სპექტრს, 08.05.2000. http://edition.cnn.com/2000/LAW/05/08/love.bug/index.html; ჩაუკი, "კრიტიკული შეხედულება კიბერდანაშაულის რეგულირებაზე", http://www.crime-research.org/articles/Critical/2; სოფაერი/გუდმანინ, "კიბერდანაშაული და უსაფრთხოება – ტრანსნაციონალური განზომილება" სოფაერი/გუდმანინ, "კიბერდანაშაული და ტერორიზმის ტრანსნაციონალური განზომილება" 2001, გვ. 10.: http://media.hoover.org/documents/0817999825_1.pdf;

ვირუსის საშუალებით,[129] არამედ კონვენციის შემქმნელებმა დაამატეს ისეთი ქმედებაც, რომელმაც შესაძლოა გამოიწვიოს მსგავსი დაზიანება. ერთ-ერთი არის კომპიუტერულ მონაცემებში ცვლილებების შეტანა. თუ კომპიუტერის ვირუსი ცვლის მონაცემების შინაარსს, ეს უთანაბრდება ფაილის წაშლას. ამასთანავე, ქმედება ჩადენილი უნდა იყოს წინასწარი განზრახვითა და სანქციონირების გარეშე.

პრაქტიკული ინფორმაცია მოსამართლეებისათვის:

ერთ-ერთი გამოწვევა, რომელიც დაკავშირებულია მონაცემებში ჩარევასა და მათზე ზემოქმედებასთან არის მონაცემების წაშლა ისე, რომ მათი არსებობის დამტკიცება შეუძლებელია მყარი დისკის (ჰარდ დრაივ) ანალიზის საშუალებით.[130] ასეთი ქმედების დამტკიცებისათვის, საჭირო ხდება კომპიუტერული სისტემის უფრო დეტალური კრიმინალური ანალიზი. ფასეულ მტკიცებულებას შესაძლოა ინახავდეს ლოგ ფაილები, ინფორმაცია ფაილის ინდექსებში ან სისტემური ფაილები. ეს აშკარას ხდის სამართალდამცავ ორგანოებსა და კრიმინალურ ექსპერტებს შორის თანამშრომლობის მნიშვნელობას და მოსამართლეების პროცესში მოგვიანებით ჩართვასთან დაკავშირებულ სირთულეებს.[131]

როგორ არის განსაზღვრული ეს დანაშაული თქვენი ქვეყნის კანონმდებლობაში?
ადგილობრივი კანონმდებლობის დებულებების განხილვა და სიტუაციური სავარჯიშოები

[129] მუხლი 4 ქმედების შედეგის სერიოზულობის მოთხოვნის გამო, გვთავაზობს ქმედების დანაშაულად ცნობის შეზღუდვის შესაძლებლობებს.
[130] განმარტებითი ანგარიში №60.
[131] კომპიუტერული ვირუსი არის პროგრამა, რომელსაც შეუძ ია საკუთარი თავის გამეორება და კომპიუტერის დაინფიცირება კომპიუტერის მფლობელის ნებართვის გარეშე. იხილეთ სპფორდის ინტერნეტის ვირუსის პროგრამა, ანალიზი:, გვ.3; კოენი – კომპიუტერული ვირუსი, თეორია და ექსპერიმენტები: at: http://all.net/books/virus/index.html. *koeni,* "კომპიუტერის ვირუსები"; ადელმანი, "კომპიუტერული ვირუსების აბსტრაქტული თეორია". ეკონომიკურ შედეგებთან დაკავშირებით, კაშელი/ჯეკსონინ/ჯიკლინგი/ვებელი, "კიბერშეტევების ეკონომიკური შედეგი", გვ.12; სიმანტეკი "ანგარიში ინტერნეტის უსაფრთხოების შესახებ", ტენდენციები 2006 წლის ივლისისათვის: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

4.4 სისტემაში ჩარევა და მასზე ზემოქმედება

4.4.1 მოვლენა

საინფორმაციო ტექნოლოგიები ბიზნესის წარმოებისა და ბიზნესკომუნიკაციის მნიშვნელოვანი ელემენტს წარმოადგენს. როგორც ადრე ავღნიშნეთ,[132] საინფორმაციო-საკომუნიკაციო ტექნოლოგიებიის ინტეგრირებულობამ ისეთ დონეს მიაღწია, რომ საინფორმაციო ორგანიზაციები დამოკიდებულნი გახდნენ ასეთი მომსახურების გაწევაზე. მნიშვნელოვანი მომსახურების შეწყვეტა იწვევს უარყოფით ზემოქმედებას.[133] მაგალითად, თუ მიუწვდომელია სერვერი, რომელიც პასუხისმგებელია კომუნიკაციაზე, მომხმარებლები იძულებულნი ხდებიან, გადაერთონ კომუნიკაციის სხვა საშუალებებზე. ალტერნატიული მომსახურების არსებობა კომპიუტერული უსაფრთხოების სტრატეგიის მნიშვნელოვანი ნაწილია, თუმცა დამატებითი სისტემების შენახვისა და ფუნქციონირების ხარჯის გაწევის ფუფუნება არ გააჩნია ინტერნეტის მომხმარებლების უმრავლესობას.[134]
მომსახურების ხელმისაწვდომობაზე ზეგავლენა მრავალი გზით შეიძლება განხორციელდეს. 2008 წელს, ზღვისქვეშა კაბელის დაზიანების შედეგი, რომელიც გამოიწვია გემების მიერ ღუზის ჩაშვებამ, გახლდათ წყნარი ოკეანის სამრეთ ნაწილში გადაცემის სიჩქარის სერიოზული ვარდნა, რაც კარგი ილუსტრაციაა პოტენციური ავარიების შემთხვევებისათვის.[135] გარდა ავარიების შედეგად გამოწვეული წყვეტისა, არსებობს უამრავი საშუალება, რასაც იყენებენ დამნაშავეები ინტერნეტის ხელმისაწვდომობის შეზღუდვასთან დაკავშირებით. ერთ-ერთი საშუალება არის კრიტიკული ინფრასტრუქტურის ფიზიკური ტერმინაცია – მაგალითად, ინტერნეტის სერვერის ფიზიკური დაზიანება.

ფიზიკურად ადგილზე ყოფნის გარეშე კომპიუტერული სისტემის ფუნქციონირების წყვეტა შესაძლებელია ვისრუსის გამოყენებით, რომელიც შლის მნიშვნელოვან ფაილებს.[136] თუმცა, კომპიუტერული ვირუსის საშუალებით შეტევის წარმატებული განხორციელებისათვის, საჭიროა დამცავი საშუალებების გვერდი

[132] Windows XP-s saSualebiT failebis waSlis ufro pirobiT gzebTan dakavSirebiT izileT: http://www.microsoft.com/windowsxp/using/setup/learnmore/tips/waystodelete.mspx. ექსპერტულ გამოძიებასთან დაკავშირებით მეტი ინფორმაციისათვის იხილეთ კასეის კომპიუტერული დანაშაულის გამოძიების სახელმძღვანელო, 2001; კომპიუტერული მტკიცებულების მიგნება და ამოღება, სახელმძღვანელო; სამართლისა და საჯარო უსაფრთხოების ნიუ ჯერსის დეპარტამენტი, სისხლის სამართლის განყოფილება, 2000, გვ. 18: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[133] იხილეთ თავი 1.5.

[134] იხილეთ თავი 1.

[135] ეს განსაკუთრებით მნიშვნელოვანია მომხმარებელთა ნდობასთან მიმართებაში. თუ მიუწვდომლობის გამო, მომხმარებლები ვერ გამოყენებენ მნიშვნელოვან მომსახურებას, ისინი დაკარგავენ ნდობას სერვის პროვაიდერის მიმართ, რაც სერიოზულ ზეგავლენას მოახდენს მის ფუნქციონირებაზე. ელექტრონული ბიზნესისადმი ნდობის შესახებ იხილეთ რატსანინგამის ნდობის მნიშვნელობა ელექტრონულ კომუნიკაციაში, ინტერნეტის კვლევა, 1998, ტომი 8, გამოცემა 4, გვ.313; მიჩი/მარში/ ელექტრონული ბიზნესისი პერსონიზაციის სოციალური ფაქტორები: ://iit-iti.nrc-cnrc.gc.ca/iit-publications-iti/docs/NRC-43664.pdf; *შიმი/ვან სლაიკი/ჯიანგი/ჯონსონი*, ამცირებს თუ არა ნდობა შეშფოთებას ელექტრონულ კომუნიკაციაში ინფორმაციის დაცვის თავლსაზრისით?: http://sais.aisnet.org/2004/.%5CShim,%20VanSlyke,%20Jiang%20&%20Johnson.pdf.

[136] შედეგად, ის ფაქტი, რომ ბიზნესი ქმნის კომუნიკაციის საშუალებას, არ ნიშნავს რომ მომხმარებლებთან კომუნიკაციის უნარზე ზემოქმედება არ ხდება თუ მთავარი საკომუნიკაციო სისტემა ვერ იმუშავებს, რადგან მომხმარებლებს შესაძლოა არ ქონდეთ კომუნიკაციის გადართვის საშუალებანი.

ავლა. გამომდინარე დამცავი სისტემის კონფიგურაციიდან, შესაძლოა უნიკალური სირთულეებისა და ბარიერების შექმნა და, ამგვარად, კომპიუტერის სისტემის ფუნქციონირებაში ჩარევის მესამე საშუალება ძალზედ პოპულარული გახდა ბოლო ხანებში.

ცნობილი ვებ-გვერდების[137] დიდი რაოდენობა გახდა "მომსახურებაზე უარი" შეტევის მსხვერპლი/"Denial-of-Service" (DoS) attacks.[138] ასეთ დროს, დამნაშავეები კომპიუტერული სისტემისაკენ მიმართავენ იმაზე მეტ თხოვნას, რამდენის დამუშავების შესაძლებლობაც აქვს ამ სისტემას[139]. ასეთი შეტევით შესაძლებელია საკმაოდ დიდი შესაძლებლობების მქონე სისტემის დაზიანებაც კი.

4.4.2 სამართლებრივი რეაგირება

ოპერატორების ინტერესისი დაცვის და მომხმარებლებისათვის სატელეკომუნიკაციო საშუალებებთან სათანდო შეღწევის უზრუნველყოფის მიზნით, კონვენციაში ჩადებულია მუხლი 5, რომელიც სისხლის სამართლის დანააულის კვალიფიკაციას ანიჭებს კომპიუტერული სისტემის კანონიერი გამოყენების შეგნებულ შეფერხებას.

> მუხლი 5 – სისტემაზე ზემოქმედება/სისტემაში ჩარევა
>
> ყველა მხარე განსაზღვრავს და დაამტკიცებს ისეთ საკანონმდებლო და სხვა ღონისძიებებს, რომლებიც საჭირო იქნება ადგილობრივი კანმდებლობის მიხედვით დანაშაულის სისხლის სამართლის დანაშაულად მიჩნევისათვის, როცა ეს დანაშაული ჩადენილია წინასწარი განზრახვით/შეგნებულად და იწვევს კომპიუტერული სისტემის სერიოზულ შეფერხებას უფლების გარეშე კომპიუტერული მონაცემების შეყვანით, გადაცემით, დაზიანებით, წაშლით, შეცვლით ან დაბლოკვით.

[137] წყლისქვეშა კაბელების დაზიანებასთან დაკავშირებით, იხილეთ აშშ უსაფრთხოების დეპარტამენტის ღია წყაროების ინფრასტრუქტურის ანგარიში, თებერვალი 4, 2008: http://www.globalsecurity.org/security/library/news/2008/02/dhs_daily_report_2008-02-04.pdf; ჰამბლენი, ახლო აღმოსავლეთში გადაჭრილია მესამე წყალქვეშა კაბელი, კომპიუტერის სამყარო, თებერვალი 2008: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9060658; ბიბისის 2008 წლის თებერვლის ამბები: http://news.bbc.co.uk/2/hi/technology/7222536.stm.

[138] კომპიუტერული ვირუსი არის პროგრამა, რომელსაც შეუძ ია საკუთარი თავის გამეორება და კომპიუტერის დაინფიცირება კომპიუტერის მფლობელის ნებართვის გარეშე. იხილეთ სპაფორდის ინტერნეტის ვირუსის პროგრამა, ანალიზი:, გვ.3; კოენი – კომპიუტერული ვირუსი, თეორია და ექსპერიმენტები: at: http://all.net/books/virus/index.html. *koeni*, "კომპიუტერის ვირუსები"; ადელმანი, "კომპიუტერული ვირუსების აბსტრაქტული თეორია". ეკონომიკურ შედეგებთან დაკავშირებით, კაშელი/ჯეკსონინ/ჯიკლინგი/ვებელი, "კიბერშეტევების ეკონომიკური შედეგი", გვ.12; სიმანტეკი "ანგარიში ინტერნეტის უსაფრთხოების შესახებ", ტენდენციები 2006 წლის ივლისისათვის: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

[139] პაუერი, 2000, ფედერალური ბიუროს კომპიუტერული დანაშაულისა და უსაფრთხოების კვლევა, კომიუტერული უსაფრთხოების ჟურნალი, ტომი 16, №2, გვ.33; ლემოსი: ვებ შეტევები: http://news.zdnet.com/2100-9595_22-501926.html;

დებულება სისხლის სამართლის დანაშალის კვალიფიკაციას არ ანიჭებს ისეთ კონკრეტულ ქმედებას, რასაც შედეგად მოაქვს სისტემაზე ზემოქმედება, მაგრამ მოიცავს ყველა საქმიანობას, რომელიც ერევა კომპიუტერული სისტემის ნორმალურ ფუნქციონირებაში.[140] ამაში შედის სერვერის ფიზიკური დაზიანება, ვირუსი ან DoS შეტევები. ის ფაქტი, რომ დებულება სისხლის სამართლის დანაშაულის კვალიფიკაციას ანიჭებს გარკვეულ ქმედებებს, საშუალებას აძლევს კონვენციის ხელმომწერ მხარეებს ასეთი კვლიფიკაცია მიანიჭონ მხოლოდ ისეთ შეტევებს, რომლებიც ხორციელდება მნიშვნელოვანი სერვერების წინააღმდეგ ან როცა შედეგი არის სერიოზული დაზიანება.[141] ასეთი ქმედება უნდა იყოს წინასწარი განზრახვით/შეგნებული და არასანქცირებული/უკანონო.

პრაქტიკული ინფორმაცია მოსამართლეებისათვის:

შეტევის შედეგის გაძლიერების მიზნით, დამნაშავეები სულ უფრო ხშირად იყენებენ ე.წ. ბოტნეტებს, რათა განახორციელონ DoS შეტევები. ტერმინი ბოტნეტი გამოიყენება დაინფიცირებული კომპიუტერების ჯგუფის მისამართით, რომელთა პროგრამებიც კონტროლირდება გარედან.[142] თუ დამნაშავე იყენებს ასეთ ბოტნეტს, სამართალდამცავმა ორგანოებმა უნდა მისდიონ ათასობით კვალს დაინფიცირებული კომიუტერებისაკენ, რათა განსაზღვრონ, შეუძლიათ თუ არა საკმარისი მტკიცებულების მოპოვება იმისათვის, რომ მიადგნენ ადამიანს ან ადამიანთა ჯგუფს, რომლებიც აკონტროლებენ ბოტნეტს.

როგორ არის განსაზღვრული ეს დანაშაული თქვენი ქვეყნის კანონმდებლობაში?
ადგილობრივი კანონმდებლობის დებულებების განხილვა და სიტუაციური სავარჯიშოები

[140] 2004 წელს შეფერხა გერმანიის ავიახაზების ლუფტანზას ინტერნეტ მომსმახურება ასეთი დოს შეტევით. ინტერნეტ დავჯავშნა ვერ ხორციელდებოდა ორი თვის მანძილზე.

[141] დოს შეტევა –უარი მომსახრებაზე მიზნად ისახავს სისტემის წყობიდან გამოყვანას მისკენ ბევრი თხოვნის გაშვების გზით, რის შედეგადაც იგი ვეღარ რეაგირებს ლეგიტიმურ მოთხოვნებზე. ინფორმაციისათვის იხილეთ: http://www.us-cert.gov/cas/tips/ST04-015.html; *პაქსონი*, "მომსახურებაზე უარის თქმის შეტევის გააზრება": http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; სჩუბა/კრსული/კუნი/სპაფორდი/სუნდრამი/ზამბონი, "მომსახურებაზე უარის თქმის გაანალიზება"; *პოული/ვეიევერი*, "მომსახურებაზე უარის თქმის ტექნოლოგიების მიმართულებები", 200: http://www.cert.org/archive/pdf/DoS_trends.pdf. 2000 წელს ბევრი აშშ ელექტრონული ბიზნესი მოხვა=და მომსახურებაზე უეარის თქმის შეტევის ქვეშ. იურჩიკი იძლევა მათ სრულ სიას: http://www.projects.ncassr.org/hackback/ethics00.pdf. დამატებითი ინფორმაციისათვის: პაუერი, 2000 ფედერალური ბიუროს კომპიუტერისა და დანაშაულის კვლევა, კომპიუტერული უსაფრთXოების ჟურნალი, ტომი. 16, № 2, 2000, გვ. 33. ლემოსი: გამოძიების ფედერალური ბიურო: http://news.zdnet.com/2100-9595_22-501926.html; გიდმანი/ბრენერი, კონსენსუსი კიბერსივრცეში დანაშაულებრივი ქმედების შესახებ: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *ალლერ*, "პასუხი, აღდგენა და სისუსტეების შემცირება კიბერშეტევების მიმართ: გაკვეთილი გამოტანილია ქვეყნის უსაფრთხოების დეპარტამენტისათვის, 2003, გვ.3: http://www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

[142] განმარტებითი ანგარიში, №66.

4.5 ტექნიკური მოწყობილობის არაკანონიერი გამოყენება

4.5.1 მოვლენა

კომპიუტერულ დანაშაულთა მიმართებაში ძალიან მნიშვნელოვანია ისეთი ტექნიკური და პროგრამული ინსტრუმენტების ხელმისაწვდომობა, რომლებიც გამოიყენება დანაშაულის ჩადენის მიზნით. ასეთი მოწყობიობების უმეტესობა ხელმისაწვდომის, ხშირად უფასო, ადვილად ასამუშავებელი და მათი გამოყენება, ხშირად, შეუძლიათ სპეციფიური ცოდნის არმქონე ადამიანებსაც კი. პროგრამული უზრუნველყოფის გამოყენება შესაძლოა უკაბელო კომუნიკაციის გადაცემის დროს ხელში ჩაგდების მიზნით ან ღია, უკაბელო ქსელის ("Wardriving[143]"), აღმოჩენისათვის, დაშიფრული ფაილების გაშიფვრისა და (DoS)[144] შეტევებიისათვის. ასეტი დანაშაულის ჩადენა მოითხოვს გარკვეული მოწყობილობის ქონას, იქმნება შავი ბაზარი, სადაც ხდება მათი წარმოება და გასაღება. გარდა ამისა, ხშირია კოდური სიტყვების გაცვლაც, რაც საშუალებას აძლევს დამნაშავეებს მოახდინონ სისტემაში არასანქცირებული შეღწევა.

4.5.2 სამართლებრივი რეაგირება

კონვენციის შემომქმედებმა, გაითვალისწინეს რა ყველა მოვლენა, გადაწყვიტეს განესაზღვრათ კონკრეტული არაკანონიერი ქმედებები, დაკავშირებული მოწყობილობებთან და ტექნიკასთან ან მონაცემებში შეღწევასთან კომპიუტერული სისტემის ან მისი მონაცემების კონფიდენციალურობის, ინტეგრირებულობისა და ხელმისაწვდომობის ხელყოფის მიზნით,[145] როგორც დამოუკიდებელი სისხლის სამართლის დანაშაული.

> მუხლი 6 – ტექნიკური მოწყობილობის არაკანონიერი გამოყენება[146]
>
> (1) ყველა მხარე განსაზღვრავს და დაამტკიცებს ისეთ საკანონმდებლო და სხვა ღონისძიებებს, რომლებიც საჭირო იქნება ადგილობრივი კანონმდებლობის მიხედვით დანაშაულის სისხლის სამართლის დანაშაულად მიჩნევისათვის, როცა ეს დანაშაული ჩადენილია წინასწარი განზრახვით:
> (ა) შემდეგი მოწყობილობის წარმოება, გაყიდვა, გამოსაყენებლად შეძენა, იმპორტი, გავრცელება და სხვაგვარად ხელმისაწვდომად ქცევა:

[143] მიუხედავად იმისა, რომ, სერიოზულის მნიშვნელობა ზღუდავს მის გამოყენებას, ოპერაციების სერიოზული გადადებაც კი, შეტევის შედეგად გამოწვეული, შესაძლოა დაფაროს ამ დებულებამ.

[144] ბოტნეტი არის დაინფიცირებული კომპიუტერების ჯგუფი, რომლებშიც პროგრამები გარედან იმართება. იხილეთ უილსონის ბოტნეტები, კიბერდანაშაული და კიბერტერორიზმი: სისუსტეები და პოლიტიკის საკითხები კონგრესისათვის, 2007, გვ4: http://www.fas.org/sgp/crs/terror/RL32114.pdf.

[145] ვარდრაივინგი არის ტერმინი, რომელიც ნიშნავს უკაბელო ქსელების მოძიებას მოძრავი მანქანების საშუალებით. თუ ამ საქმიანობის ბოლო არ იქნა გამოყენებული არასათანადო მიზნებისათვის, ბევრი ქვეყანა მას არ განმართავს დანაშაულად. გერმანიის სიტუაციასთან დაკავშირებით იხილეთ ბაიერის ვარდრაივერი, 2005, 434.

[146] იხილეთ ევროსაბჭოს კონვენცია მუხლი 6.

(i) კომპიუტერული პროგრამის მოწყობილობა, რომელიც სპეციალურად არის შექმნილი იმ დანაშაულის ჩადენის მიზნით, რომლებიც განსაზღვრულია ზემოაღნიშნულ მუხლებში 2 და 5.
(ii) კომპიუტერის კოდური სიტყვა, შემსვლელი პაროლი, ან მსგავსი მონაცემები, რომლითაც შესაძლებელია კომპიუტერის სისტემაში შეღწვა მთლიანად ან ნაწილობრივ შექმნილი იმ დანაშაულის ჩადენის მიზნით, რომლებიც განსაზღვრულია ზემო მუხლებში 2 და 5.
(ბ) ზემოაღნიშნულ პარაგრაფებში განსაზღვრული ნივთების ფლობა იმ დანაშაულის ჩადენის მიზნით, რომლებიც განსაზღვრულია მუხლებში 2 და 5. მხარემ შესაძლოა მოითხოვოს ასეთი ტექნიკური აღჭურვილობის არსებობა და ფლობა, როგორც ფაქტი იმისათვის, რომ დაკვალიფიცირდეს სისხლის სამართლის პასუხისმგებლობა.

2. ეს მუხლი არ ანიჭებს სისხლის სამართლის პასუხისმგებლობას ისეთ შემთხვევებს, როცა პუნქტ 1-ში აღნიშნული აღჭურვილობის წარმოება, გაყიდვა, მოხმარებისათვის შეძენა, იმპორტი და გავრცელება არ ხდება დანაშაულის ჩადენის მიზნით, როგორც ეს განსაზღვრულია კონვენციის მუხლებით 2 და 5, არამედ, მისი მიზანია კომპიუტერული სისტემის ტესტირება ან მისი დაცვა.
3. ნებისმიერი მხარე ინარჩუნებს უფლებას, არ გამოიყენოს ამ მუხლის პუნქტი 1 იმ პირობით, რომ ეს არგამოყენება არ შეეხება ამ მუხლის პუნქტი 1aii-ით განსაზღვრული ტექნიკური აღჭურვილობის გაყიდვას, გავრცელებას ან სხვაგვარად ხელმისაწვდომად ქცევას.

ასეთი ტექნიკისაგან მომავალი საფრთხე კითხვის ნიშნის ქვეშ აყენებს სისხლის სამართლის დანაშაულის კვალიფიკაციის მინიჭებას მხოლოდ დანაშაულის ჩადენის მიზნით გამოყენების შემთხვევაში. ქვეყნების უმეტესობას, საკუთარ კანომდებლობაში გარდა დებულებისა "დანაშაულის ჩადენის მცდელობა" აქვთ დებულებანი, რომელიც სისხლის სამართლის კვალიფიკაციას ანიჭებს დანაშაულის მომზადებას[147]. ასეთი მიდგომა გამოიყენება ძალზედ სერიოზულ დანაშაულთან მიმართებაში. ევროკავშირის კანონმდებლობაში შეიმჩნევა ტენდენცია, რომ დანაშაულის კვალიფიკაცია მიენიჭოს ნაკლებად მძიმე დანაშაულს[148] და მოსამზადებელ ქმედებებს.

სისხლის სამართლის დანაშაულად ცნობის ფაქტორი არის, ერთის მხრივ, პუნქტ 1-ში განსაზღვრული აღჭურვილობა[149], რომლითაც ხდება კომპიუტერული დანაშაულის ჩადენა და, მეორეს მხრივ, კოდური სიტყვები, რომლითაც ხდება შეღწევა სისტემაში. ამ მიმართებაში, კონვენცია დანაშაულის კვალიფიკაციას ანიჭებს ბევრ ქმედებას. გარდა წარმოებისა, დანაშაულად კვალიფიცირდება გაყიდვა, გამსაყენებლად შეძენა, იმპორტი, გავრცელება და ტექნიკისა და კოდური სიტყვების სხვაგვარად ხელმისაწვდომად

[147] განმარტებითი ანგარიში, №73
[148] ევროსაკავშირის ჩარჩო გადაწყვეტილება: 2.6.2001
[149] გავრცელება ნიშნავს მონაცემების სხვებისათვის აქტიურად გაგზავნას – ეს არის ევროსაბჭოს განმარტება. კონვენცია ასევეე აღნიშნავს ხელსაწყოების შეზღუდვას პროგრამული უზრუნველყოფის მიმართ. მუხლი გულისხმობს როგორც ტექნიკურ, ისე პროგრამულ უზრუნველყოფას.

ქცევა. იგივე მიდგომა არსებობს ევროკავშირის საპატენტო უფლებების ჰარმონიზაციის კანონმდებლობაში[150] (შემოიფარგლება იმ ტექნიკით, რომელიც საჭიროა ტექნიკური ღონისძიებების გვერდის ავლისათვის)

კონვენციაში შეტანილია ისეთი მოწყობილობები, რომელთა გამოყენება შესაძლებელია კანონიერადაც თუ დამნაშავე აპირებს კომპიუტერული დანაშაულის ჩადენას. განმარტებით ანგარიშში ახსნილია, რომ მხოლოდ იმ ტექნიკური მოწყობილობის[151] ჩამონათვალი, რომელთა საშუალებით ხდება დანაშაული, ძალზედ შეზღუდული იყო და იწვევდა დაუძლეველ სირთულეებს გამოძიების დროს და თითქმის შეუძლებელს ხდიდა მუხლის გამოყენებას, გარდა იშვიათი შემთხვევებისა.[152] მისი მოქმედების ძალზედ გაფართოვების თავიდან აცილების მიზნით, მოხდა შეზღუდვის ობიექტური დონის და გონებრივი ელემენტის კომბინაცია.

პრაქტიკული ინფორმაცია მოსამართლეებისათვის:

მთავარი გამოწვევა ტექნიკის არაკანონიერ გამოყენებასთან დაკავშირებით, არის მტკიცებულება, რომ ურთიერთობა მოხდა დანაშაულის ჩადენის მიზნით. ტექნიკის უბრალო ფლობა არ მიანიშნებს დანაშაულის ჩადენის გეგმაზე, რადგან კომპიუტერული უზრუნველყოგა სრულიად ლეგიტიმური მიზნებისთვისაც გამოიყენება.[153]

როგორ არის განსაზღვრული ეს დანაშაული თქვენი ქვეყნის კანონმდებლობაში?
ადგილობრივი კანონმდებლობის დებულებების განხილვა და სიტუაციური სავარჯიშოები

4.6 კომპიუტერული მონაცემების გაყალბება

4.6.1 მოვლენა

კლასიკური ფორმატის (ნაბეჭდი) დოკუმენტებიდან ელექტრონულ დოკუმენტებზე გადასვლის გამო, კომპიუტერთან დაკავშირებული მონაცემების გაყალბება სულ უფრო მნიშვნელოვან როლს თამაშობს. ეს

[150] დოს შეტევა –უარი მომსახურებაზე მიზნად ისახავს სისტემის წყობიდან გამოყვანას მისკენ ბევრი თხოვნის გაშვების გზით, რის შედეგადაც იგი ვეღარ რეაგირებს ლეგიტიმურ მოთხოვნებზე. ინფორმაციისათვის იხილეთ: http://www.us-cert.gov/cas/tips/ST04-015.html;. *პაქსონი*, "მომსახურებაზე უარის თქმის შეტევის გააზრება": http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html.

[151] განმარტებითი ანგარიში №65.

[152] ხელსაწყოების ფლობის დანაშაულად ცნობის შესახებ განსხვავებული მოსაზრებების გამო, კონვენცია, გარდა პუნქტი 1-სა გთავაზობთ მუხლი 6-ის პუნქტი 3-ის კომპლექსურ მიდგომას. ეს საშუალებას აძლევ უფრო ფართოდ გამოიყენოს ეს მუხლი, და არ აღიაროს დანაშაულად ასეთი მოწყობილობის ფლობა ან წარმოება.

[153] მაგალითად გამოდგება ევროსაბჭოს ჩარჩო გადაწყვეტილება.

დანაშაული განსაკუთრებით პოპულარული გახდა "ფიშინგის" თავდასხმებთან დაკავშირებით[154]. ტერმინი "ფიშინგი" გამოიყენება დანაშაულის ტიპის აღსანიშნავად, რომლისთვისაც დამახასიათებელია ოფიციალურ ელექტრონულ კომუნიკაციაში სანდო პიროვნებად ან ბიზნესად (მაგ. საფინანსო ინსტიტუტებად) მასკირების საშუალებით თაღლითური გზით იმგვარი მგრძნობიარე ინფორმაციის მოპოვების მცდელობები, როგორებიცაა პაროლები[155]. აღნიშნული "ფიშინგის" მცდლობათა უმრავლესობა ხორციელდება ელექტრონული ფოსტის საშუალებით. ამგვარი ელექტონული ფოსტის მიმღებ პირს, მაგალითად, ეძლევა დავალება დაადასტუროს მისი ელექტრონული საბანკო ანგარიში ("დააწკაპუნეთ აქ თქვენი საბანკო ანგარიშის დასადასტურებლად") მისი ანგარიშის ნომრის და პაროლის შეყვანის გზით იმ ვებ-გვერდზე, რომელიც შექმნილი იქნა დამნაშავეების მიერ და, რომლებიც შემდგომში ბოროტად იყენებენ ამ ინფორმაციას.

4.6.2 სამართლებრივი რეაგირება

მატერიალური ნივთების გაყალბების კრიმინალიზაციას დიდი ხნის ტრადიცია აქვს მრავალ ქვეყანაში.[156] კონვენცია მიზნად ისახავს შექმნას

---

[154] მაგალითისთვის იხილეთ: *Austria*, Forgery in Cyberspace: The Spoof could be on you, University of Pittsburgh School of Law, Journal of Technology Law and Policy, ტომი IV, 2004 - http://tlp.law.pitt.edu/articles/Vol5-Austria.pdf.

[155]"ფიშინგის" თაობაზე იხილეთ: *Dhamija/Tygar/Hearst*, "Why Phishing Works",

http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; და "Report on Phishing", A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, 2006, http://www.usdoj.gov/opa/report_on_phishing.pdf

[156] მაგალითისთვის იხილეთ: 18 U.S.C. § 495:

ვინც ცვლის, აყალბებს, ფალსიფიცირებას ახდენს ან ქმნის ყალბ აქტს, მინდობილობას, მიწერილობას, სერტიფიკატს, ქვითარს, კონტრაქტს ან სხვა წერილობით დოკუმენტს, იმისათვის, რომ ნებისმიერმა სხვა პირმა, პირდაპირ ან არაპირდაპირ, მოიპოვოს, მიიღოს ან შესაძლებლობა მიეცეს მოიპოვოს ან მიიღოს შეურთებული შტატებისაგან ან ნებისმიერი სხვა თანამდებობის პირისაგან ან აგენტებისაგან, ნებისმიერი თანხა;

ან ვინც გამოაცხადებს ან გამოაქვეყნებს ან გამოაცხადებს ჭეშმარიტად ნებისმიერ ამ მცდარ, გაყალბებულ, შეცვლილ ან ფალსიფიცირებულ დოკუმენტს იმ განზრახვით, რომ შეცდომაში შეიყვანოს შეურთებული შტატები, ეცოდინება რა, რომ ეს დოკუმენტი არის მცდარი, შეცვლილი, გაყალბებული ან ფალსიფიცირებული; ან

ვინც გადასცემს ან წარუდგენს შეურთებული შტატების ნებისმიერ სამსახურს ან თანამდებობის პირს ნებისმიერ ამგვარ დოკუმენტს ნებისმიერ ანგარიშთან ან სარჩელთან დაკავშირებით, იმ განზრახვით, რომ შეცდომაში შეიყვანოს შეურთებული შტატები, ეცოდინება რა, რომ ეს დოკუმენტი არის მცდარი, შეცვლილი, გაყალბებული ან ფალსიფიცირებული;

- იქნება დაჯარიმებული ამ ნაწილის შესაბამისად ან დაისჯება თავისუფლების აღკვეთით არაუმეტეს ათი წლის ვადით, ან ორივე.

მსგავსი მიდგომა შეიძლება მოიძებნოს გერმნული სისხლის სამართლის კოდექსის 267-ე მუხლში:

მუხლი 267. დოკუმენტების ფალსიფიკაცია

(1) ის ვინც, სამართლებრივ ურთიერთობებში მოტყუების მიზნით ქმნის ყალბ დოკუმენტს, ახდენს ნამდვილი დოკუმენტის ფალსიფიცირებას ან იყენებს ყალბ ან ფალსიფიცირებულ დოკუმენტს, უნდა დაისჯოს თავისუფლების აღკვეთით არაუმეტეს 5 წლის ვადით ან დაჯარიმდეს.

(2) მცდელობა იქნება დასჯადი.

(3) განსაკუთრებისთ სერიოზულ შემთხვევებში, დასჯა იქნება თავისუფლების აღკვეთა ექვსი თვიდან ათ წლამდე. განსაკუთრებით სერიოზული შემთხვევებში, როგორც წესი, იგულისხმება, რომ დანაშაულის ჩამდენი პირი:

1. მოქმედებს პროფესიონალურად ან როგორც იმ ორგანიზებული დანაშაულებრივი ჯგუფის წევრი, რომელიც შეიქმნა თაღლითობის ჩადენის ან დოკუმენტების ფალსიფიცირების მიზნით;

2. იწვევს დიდი ოდენობის ქონების დაკარგვას;

3. არსებითად უქმნის საფრთხეს სამართლებრივი ურთიერთობების უსაფრთხოებას დიდი რაოდენობის ყალბი ან ფალსიფიცირებული დოკუმენტების შექმნით; ან

4. ბოროტად იყენებს მის უფლებამოსილებას ან თანამდებობას, როგორც საჯარო მოხელე.

(4) ის, ვინც ადგენს ფალსიფიცირებულ დოკუმენტს პროფესიონალურად ან როგორც იმ ორგანიზებული დანაშაულებრივი ჯგუფის წევრი, რომელიც შეიქმნა 263-264 ან 267-269 მუხლებით

პარალელური დანაშაული, რომელიც შეეხება მატერიალური დოკუმენტების გაყალბებას, რათა ამოივსოს სისხლის სამართალში არსებული სიცარიელე ტრადიციულ გაყალბებასთან დაკავშირებით, რომელიც მოითხოვს იმ განცხადებების ან დეკლარაციების ვიზუალურ წაკითხვადობას, რომლებიც დატანილია დოკუმენტზე, და რომელიც არ შეეხება ელექტრონულად შენახულ მონაცემებს[157].

მუხლი 7 – კომპიუტერული მონაცემების გაყალბება

თითოეულმა მხარემ უნდა მიიღოს საკანონმდებლო ან სხვა სახის იმგვარი ზომები, რომლებიც შეიძლება საჭირო იყოს იმისათვის, რომ თავიანთ შიდა კანონმდებლობაში განსაზღვრონ სისხლის სამართლის დანაშაულად კომპიუტერული მონაცემების წინასწარგამიზნული ან უფლების გარეშე განხორციელებული შეყვანა, შეცვლა, წაშლა ან ჩახშობა, რასაც შედეგად მოჰყვება არააუთენტური მონაცემები, იმ განზრახვით, რომ ეს მონაცემები მიჩნეული იქნეს აუთენტურად ან მათი, როგორც აუთენტური მონაცემების გამოყენება ხდებოდეს სამართლებრივი მიზნებისათვის, იმისდა მიუხედავად, არის თუ არა ეს მონაცემები ადვილსაკითხავი და გასაგები. სისხლისსამართლებრივი პასუხისმგებლობის დადგომამდე ნებისმიერმა მხარემ შეიძლება მოითხოვოს შეცდომაში შეყვანის განზრახულობის ან სხვა არაპატიოსანი ჩანაფიქრის არსებობის დადასტურება.

კომპიუტერული მონაცემების გაყალბების სამიზნეს წარმოადგენს მხოლოდ მონაცემები – არა აქვს მნიშვნელობა, არის თუ არა ეს მონაცემები ადვილსაკითხავი და გასაგები. იმისათვის, რომ გაივლოს ზღვარი მატერიალურ დოკუმენტების გაყალბებასთან, მინიმუმ ფსიქიკის ელემენტის გათვალისწინებით, მე-7 მუხლი მოითხოვს, რომ მონაცემები საჯარო ან კერძო დოკუმენტის ექვივალენტური იყოს. ეს გულისხმობს იურიდიული დასაბუთების საჭიროებასაც. ამიტომ, იმ მონაცემთა გაყალბება, რომლებიც გამოყენებაც არ შეიძლება სამართლებრივი მიზნებისათვის, არ არის გათვალისწინებული ამ დებულებით.

პრაქტიკული ინფორმაცია მოსამართლეებისათვის:

როგორც ეს აღინიშნა მე-6 მუხლთან დაკავშირებით, სპეციალური განზრახვის მტკიცებულების არსებობა, რაც მოთხოვნილია ზოგიერთი დებულების მიხედვით (როგორიცაა მუხლი 6), ხშირად იწვევს განსაკუთრებულ სირთულეებს. "ფიშინგის" შემთხვევებთან დაკავშირებით სიტუაცია ოდნავ განსხვავებულია. ის გარემოებები, რომლებშიც გაგზავნილი იქნა ელექტრონული წერილები, ზოგადად მკაფიოდ მიუთითებს ამგვარი განზრახულობის თაობაზე.

განსაზღვრული დანაშაულების ჩადენის მიზნით, უნდა დაისაჯოს თავისუფლების აღკვეთით ერთიდან ათ წლამდე ვადით, ხოლო ნაკლებად სერიოზულ შემთხვევებში თავისუფლების აღკვეთით ექვსი თვიდან ხუთ წლამდე ვადით.

[157] ახსნა-განმარტებითი ანგარიში, №81

როგორ არის განსაზღვრული ეს დანაშაული თქვენი ქვეყნის კანონმდებლობაში? ადგილობრივი კანონმდებლობის დებულებების განხილვა და სიტუაციური სავარჯიშოები

4.7 კომპიუტერული თაღლითობა

4.7.1 მოვლენა

თაღლითობა კვლავაც რჩება კიბერსივრცეში გავრცელებულ ერთ-ერთ ყველაზე პოპულარულ დანაშაულად. ონლაინ შოპინგისა და განსაკუთრებით ინტერნეტ აუქციონების წარმატებამ უფრო მეტად ხელსაყრელი გარემო შექმნა დამნაშავეებისათვის. ყველაზე პოპულარულ დანაშაულთა შორის არის საკრედიტო ბარათებსა და აუქციონებთან დაკავშირებული თაღლითობა.[158] გარდა ამისა, კომპიუტერული სისტემებით ადმინისტრირებული აქტივები (ელექტრონული ფული, სადეპოზიტო ფული, ელექტრონული ოქრო) გახდა იგივე მანიპულაციების სამიზნე, როგორებიც ხორციელდება ქონების ტრადიციული ფორმების მიმართ. იმისათვის, რომ თავიდან იქნეს აცილებული ამგვარი, განსაკუთრებით კი ინტერნეტ აუქციონების მისამართით განხორციელებული კრიმინლური ქმედებები, მიღებული იქნა მთელი რიგი ტექნიკური სახის ზომები, რომლებიც დაკავშირებულია ნდობის განმტკიცებასთან.[159] თუმცა, გამყიდველსა და მყიდველს შორის პირადი კონტაქტის არარსებობა ამცირებს შესაძლო მსხვერპლების თვითდაცვის შესაძლებლობებს.

იმის გამო, რომ თაღლითობა არის გავრცელებული პრობლემა ინტერნეტის ფარგლებს გარეთაც, ეროვნული კანონთა უმრავლესობა შეიცავს დებულებებს, რომლების შეეხება ამგვარ დანაშაულთა კრიმინალიზაციას. ამ დებულებების გამოყენება ინტერნეტთან დაკავშირებული შემთხვევებისათვის შეიძლება იყოს რთული, თუკი ტრადიციული ეროვნული სისხლის სამართლის კანონის დებულებები დაკავშირებულია პიროვნების შეცდომასთან.[160] ინტერნეტში ჩადენილი თაღლითობის ბევრ შემთხვევაში დამნაშავის ქმედებაზე რეაგირებს არა ადამიანი, არამედ კომპიუტერული სისტემა. თუკი ტრადიციული დებულებები, რომლებიც ითვალისწინებს თაღლითობის კრიმინალიზაციას არ მოიცავენ კომპიუტერულ სისტემებსაც, საჭიროა ეროვნული კანონის განახლება.

4.7.2. სამართლებრივი რეაგირება

კონვენციის მიზანია მოახდინოს მონაცემთა დამუშავების პროცესში ყველა შეუსაბამო მანიპულაციას კრიმინალიზაცია იმ განზრახვით, რომ გავლენა იქონიოს ქონების უკანონო გადაცემაზე კომპიუტერული თაღლითობის შესახებ მუხლის უზრუნველყოფით.[161]

> მუხლი 8 – კომპიუტერთან დაკავშირებული თაღლითობა

[158] "Law Enforcement Efforts to combat Internet Auction Fraud", Federal Trade Commission, 2000, გვ. 1, http://www.ftc.gov/bcp/reports/int-auction.pdf; *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, გვ. 7, http://www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

[159] ამის მაგალითია PAYPAL-ის მიერ შემოთავაზებული მომსახურება: PAYPAL არის ინტერნეტ ბიზნესი, რომელიც საშუალებას აძლევს მომხმარებელს გადარიცხოს თანხა გადახდის იმგვარი ტრადიციული მეთოდის გვერდზე ავლით, როგორიცაა საგადასახო დავალებები. ის ასევე ახორციელებს საანგარიშსწორებო მომსახურებას აუქციონების ვებ-გვერდებისათვის.

[160] ამის მაგალითია გერმანიის სისხლის სამართლის კოდექსის 263-ე ნაწილი, რომელიც მოითხოვს პირის მცდარობის (შეცდომის) დადასტურებას. ამის გამო, დებულება არ მოიცავს კომპიუტერთან დაკავშირებული თაღლითობის შემთხვევების უმეტესობას: *ნაწილი 263, თაღლითობა*

(1) ის, ვინც, იმ განზრახვით, რომ მოიპოვოს მისთვის ან მესამე პირისათვის არაკანონიერი მატერიალური სარგებელი, დააზიანებს სხვის ქონებას, შეცდომის პროვოცირებით ან დადასტურებით, განახცხადებს რა, რომ არსებობს ცრუ ფაქტები ან შეახდენს ნამდვილ ფაქტების დამახინჯებას ან მიჩქმალვას, უნდა დაისაჯოს თავისუფლების აღკვეთით არაუმეტეს ხუთი წლის ვადით ან ჯარიმით.

[161] ახსნა-განმარტებითი ანგარიში, №86

თითოეულმა მხარემ უნდა მიიღოს საკანონმდებლო ან სხვა სახის ზომები, რომლებიც შეიძლება საჭირო იყოს იმისათვის, რომ თავიანთ შიდა კანონმდებლობაში განისაზღვროს დასჯად სისხლის სამართლის დანაშაულად წინასწარგამიზნული ან უფლების გარეშე განხორციელებული ნებისმიერი ის ქმედება, რომელიც მატერიალურ ზიანს მიაყენებს სხვა პირს შემდეგი გზებით:
ა. კომპიუტერული მონაცემების შეყვანა, შეცვლა, წაშლა ან ჩახშობა;
ბ. კომპიუტერული სისტემის ფუნქციონირებაში ნებისმიერი ჩარევა;
რათა თაღლითური ან არაპატიოსანი განზრახვით, უფლების გარეშე მიიღოს ეკონომიკური სარგებელი საკუთარი თავისთვის ან სხვა პირისთვის.

მუხლი 8 კომპიუტერულ თაღლითობასთან დაკავშირებული ქმედებების უმეტესობას (მონაცემების შეტანა, შეცვლა, წაშლა და ჩახშობა) აერთიანებს ზოგად ქმედებაში "კომპიუტერული სისტემის ფუნქციონირებაში ჩარევა", რათა შესაძლებელი იყოს მასში მომავალი მიღწევების გაერთიანებაც.[162]

უმეტესი ქვეყნების სისხლის სამართლის კანონმდებლობების მიხედვით, დანაშაულებრივმა ქმედებამ უნდა გამოიწვიოს ეკონომიკური ზარალი. დანაშაულის ელემენტებთან (განსაკუთრებით მანიპულაციასთან) მიმართებაში სამართალდარღვევა, ზოგადი განზრახულობის გარდა, მოითხოვს საკუთარი თავისთვის ან სხვა პირისთვის ეკონომიკური ან სხვა სახის სარგებლის მოპოვების მიზნით სპეციალური თაღლითური ან სხვა არაპატიოსანი განზრახულობის არსებობას. მაგალითად, იმ ქმედებებისათვის, რომლებზეც არ ვრცელდება სისხლისსამართლებრივი პასუხისმგებლობა სპეციალური განზრახვის არარსებობის გამო, ახსნა-განმარტებითი ანგარიშში აღნიშნულია საბაზრო კონკურენციასთან დაკავშირებით არსებული სავაჭრო პრაქტიკა, რომელმაც შეიძლება მატერიალური ზიანი მიაყენოს ერთ პირს და ასარგებლოს მეორე, თუმცა არ არის განხორციელებული თაღლითური ან არაპატიოსანი განზრახვით.[163]

პრაქტიკული ინფორმაცია მოსამართლეებისათვის:

ის ფაქტი, რომ თაღლითური საქმიანობა მოიცავს საინფორმაციო ტექნოლოგიას თავისთავად არ გულისხმობს იმას, რომ ქმედება შეიძლება ჩაითვალოს კომპიუტერული თაღლითობად. საკმაოდ ხშირად, გამოძიების საწყის ეტაპებზე არ ხდება დიფერენციაცია ელექტრონული საშუალებებით განხორციელებულ ტრადიციულ თაღლითობასა და კომპიუტერულ თაღლითობას შორის, რომელიც მოითხოვს მონაცემთა დამუშავების მანიპულაციას.

როგორ არის განსაზღვრული ეს დანაშაული თქვენი ქვეყნის კანონმდებლობაში?
ადგილობრივი კანონმდებლობის დებულებების განხილვა და სიტუაციური სავარჯიშოები

[162] შედეგად, ამ დებულებით გათვალისწინებულია არა მხოლოდ მონაცემებთან, არამედ აპარატურასთან დაკავშირებული დანაშაულებიც.

[163] კონვენციის ავტორები მიუთითებენ, რომ არ არის გამიზნული ამ ქმედებების შეტანა მე-8 მუხლით განსაზღვრულ დანაშაულთა ჩამონათვალში. ახსნა-განმარტებითი ანგარიში №90.

4.8. ბავშვების პორნოგრაფია

4.8.1. მოვლენა

ბოლო წლების განმავლობაში ინტერნეტი გახდა ბავშვების პორნოგრაფიით ვაჭრობის ძირითადი საშუალება.[164] ამ მოვლენას ხელს უწყობს ორი ძირითადი ფაქტორი:

- ინტერნეტი იძლევა უნიკალურ შესაძლებლობას შინაარსის გავრცელების თვალსაზრისით. კოლექტიური გამოყენების სისტემაში ფაილის განთავსებით მისი ჩამოტვირთვა შეუძლია მილიონობით მომხმარებელს მთელი მსოფლიოს მასშტაბით. ის ფაქტი, რომ ინტერნეტი უზრუნველყოფს ფაილების გლობალური მასშტაბით გავრცელებას, ზრდის პოტენციურ მომხმარებელთა რიცხვს დისტრიბუციის ტრადიციულ გზებთან შედარებით.
- პორნოგრაფიული მასალების შემცველი ვებ-გვერდების წარმატების მეორე მიზეზს წარმოადგენს იმ ფაქტი, რომ მომხმარებლები მიიჩნევენ, რომ უფრო ნაკლებად "ჩანან" ონლაინის გზით მასალის მოპოვებისას, ვიდრე მის ჩვეულებრივ მაღაზიაში შეძენისას. ეს წარმოადგენს გამოძიებების უპირატესობას, ვინაიდან მომხმარებელთა უმრავლესობამ არც კი იცის, თუ რა კვალს ტოვებენ ისინი ინტერნეტ-სერფინგის დროს.[165]

4.8.2. სამართლებრივი რეაგირება

იმისათვის, რომ სისხლის სამართლის კანონმდებლობის დებულებების დახვეწის გზით უზრუნველყოფილი იქნეს ბავშვების უკეთესი დაცვა სექსუალური ექსპლუატაციისაგან, კონვენციაში შეტანილია მუხლი ბავშვების პორნოგრაფიის შესახებ.

> მუხლი 9 – ბავშვების პორნოგრაფიასთან დაკავშირებული დანაშაულებები
>
> (1) თითოეულმა მხარემ უნდა მიიღოს ისეთი საკანონმდებლო ან სხვა სახის ზომები, რომლებიც შესაძლებელია საჭირო გახდეს იმისათვის, რომ მის საშინაო კანონმდებლობაში სისხლის სამართლის დანაშაულად განისაზღვროს წინასწარგანზრახულად და უფლების გარეშე ჩადენილი შემდეგი სახის ქმედებები:
>
> ა) ბავშვების პონოგრაფიასთან დაკავშირებული მასალების მომზადება მათი კომპიუტერული სისტემის მეშვეობით გავრცელების მიზნით;
> ბ) ბავშვების პონოგრაფიასთან დაკავშირებული მასალების შეთავაზება ან უზრუნველყოფა კომპიუტერული სისტემის მეშვეობით;
> გ) ბავშვების პონოგრაფიასთან დაკავშირებული მასალების გავრცელება ან გადაცემა კომპიუტერული სისტემის მეშვეობით;
> დ) ბავშვების პონოგრაფიასთან დაკავშირებული მასალების მოპოვება კომპიუტერული სისტემის მეშვეობით საკუთარი თავისთვის ან სხვა პირისათვის;

[164] *Krone*, A Typology of Online Child Pornography Offending, Trends & Issues in Crime and Criminal Justice, No. 279.

[165] კომპიუტერთან დაკავშირებულ დანაშაულთა ჩამდენთა კვალის მიგნებისათვის არსებული შესაძლებლობების თაობაზე, იხილეთ: *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

ე) ბავშვების პორნოგრაფიასთან დაკავშირებული მასალების ფლობა კომპიუტერულ სისტემაში ან კომპიუტერული მონაცემების მატარებელზე;
(2) ზემოთ 1-ლი პუნქტის მიზნებიდან გამომდინარე, "საბავშვო პორნოგრაფიასთან დაკავშირებულ მასალებში" უნდა იგულისხმებოდეს ნებისმიერი პორნოგრაფიული შინაარსის მასალები, რომლებიც ვიზუალურად ასახავენ:
ა) მცირეწლოვანს, რომელიც მონაწილეობას იღებს სქესობრივ ლტოლვის გამომწვევ ქმედებაში;
ბ) პირს, მცირეწლოვანის როლში, რომელიც მონაწილეობას იღებს სქესობრივ ლტოლვის გამომწვევ ქმედებაში;
გ) რეალისტურ გამოსახულებებს, რომლებშიც წარმოდგენილი იქნება მცირეწლოვანი, რომელიც მონაწილეობას იღებს სქესობრივ ლტოლვის გამომწვევ ქმედებაში;
3) ზემოთ მე-2 პარაგრაფის მიზნებიდან გამომდინარე, ტერმინი "მცირეწლოვანი" გულისხმობს 18 წლამდე ასაკის ყველა პირს. ამავე დროს, ნებისმიერ მხარეს შეუძლია 16 წლამდე დასწიოს ასაკობრივი ზღვარი.
4) თითოეულმა მხარემ შეიძლება დაიტოვოს უფლება არ გამოიყენოს, მთლიანად ან ნაწილობრივ, პუნქტები 1(დ), 1(ე), 2(ბ) და 2(გ).

მნიშვნელოვანია აღინიშნოს მე-9 მუხლით განსაზღვრულია დანაშაულის ორი ელემენტი, რომლებიც წინააღმდეგობრივად არის განხილული: ბავშვების პორნიგრაფიის ფლობის კრიმინალიზაცია და ფიქტიური გამოსახულებების ინტეგრაცია.

- ბავშვების პორნოგრაფიის მხოლოდ ფლობის კრიმინალიზაციის ხარისხი განსხვავდება სხვადასხვა ეროვნულ სისხლის სამართლის საკანონმდებლო სისტემებში.[166] ბავშვების პორნოგრაფიის ფლობის კრიმინალიზაციის მიზეზი მდგომარეობს იმაში, რომ დამნაშავეები სტიმულირებას უკეთებენ ამგვარ მასალაზე მოთხოვნას, რაც განაპირობებს ამ მასალების უწყვეტ წარმოებას. ამგვარი მასალის ფლობასა და ბავშვების სექსუალური ძალადობას შორის აღნიშნული კავშირის გამო, ავტორები აღნიშნავენ, რომ ბავშვების პორნოგრაფიის წარმოების შემცირებისათვის ეფექტურ გზას წარმოადგენს ის, რომ წარმოებიდან მფლობელობაში გადასვლადმე მთელი ჯაჭვის თითოეული მონაწილის ქმედებისათვის განისაზღვროს სისხლისამართლებრივი პასუხისმგებლობა.[167] მაგრამ კონვენციის მე-4 მუხლის თანახმად, მხარეებს შეუძლიათ გამორიცხონ ამგვარი მასალების მხოლოდ ფლობის კრიმინალიზაცია სისხლის სამართლის პასუხისმგებლობის შემოფარგვლით ბავშვების პორნოგრაფიის წარმოების, შეთავაზებისა და დისტრიბუციისათვის.

- მუხლი 9, პუნქტი 2(ბ) და (გ) აჩვენებს, რომ სამართლებრივი ინტერესები, რომლებიც განსაზღვრულია მე-2 პუქტით უფრო ფართოა, ვიდრე ბავშვების პირდაპირი დაცვა სექსუალური ძალადობისაგან. მაშინ, როდესაც პუნქტი 2(ა) პირდაპირ აქცენტს აკეთებს ბავშვთა ძალადობის წინაღმდეგ დაცვაზე, პუნქტები 2(ბ) და 2(გ) შეეხება იმ გამოსახულებებსაც კი, რომლებიც შეიქმნა ბავშვთა უფლებების

[166] ავსტრალიაში საბავშვო პორნოგრაფიული მასალების ფლობის კრიმინალიზაციის თაობაზე, იხილეთ: *Krone,* Does thinking make it so? Defining online child pornography possession offences Trends & Issues in Crime and Criminal Justice, №299; *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet, is comparing various national laws regarding the criminalisation of child pornography.

[167] ახსნა-განმარტებითი ანგარიში, №98

დარღვევის გარეშე, მაგალითად, გამოსახულებები, რომლებიც მთლიანად შეიქმნა 3D მოდელირების პროგრამული უზრუნველყოფის გამოყენებით. მიზეზი, რის გამოც გათვალისწინებულია ფიქტიურ ბავშვების პორნოგრაფიასთან დაკავშირებული ქმედებების კრიმინალიზაცია მდგომარეობს იმაში, რომ ეს გამოსახულებები შესაძლებელია, რეალური "ბავშვისათვის" ზიანის მიყენების გარეშე, გამოყენებული იქნეს ბავშვების ცდუნებისათვის, რათა ისინი დათანხმდნენ სექსუალურ აქტებს ან იმისათვის, რომ შეიქმნას მოთხოვნა ბავშვების პორნოგრაფიულ მასალებზე.[168]

სექსუალური ექსპლუატაციისაგან მცირეწლოვანთა დაცვის გაუმჯობესების მიზნით, 2007 წელს ევროპის საბჭომ მიიღო ახალი კონვენცია.[169] ხელმოსაწერად გამოტანიდან პირველივე დღესვე, კონვენციას ხელი მოაწერა 23 ქვეყანამ.[170] კონვენციის ერთ–ერთ უმთავრეს მიზანს წარმოადგენს სისხლის სამართლის კანონმდებლობის იმ დებულებების ჰარმონიზება, რომლებიც მიზნად ისახავს ბავშვების დაცვას სექსუალური ექსპლუატაციისაგან.[171] ამ მიზნის მისაღწევად, კონვენციაში შეტანილია სისხლის სამართლის კანონმდებლობის დებულებები. ბავშვების წინააღმდეგ სექსუალური ძალადობის კრიმინალიზაციის გარდა (მუხლი 18), კონვენციაში შეტანილია დებულება, რომელიც შეეხება ბავშვების პორნოგრაფიული მასალების გაცვლას (მუხლი 20) და ბავშვების ცდუნებას სექსუალური მიზნებიდან გამომდინარე (მუხლი 23).

კონვენცია სექსუალური ექსპლუატაციისა და სექსუალური ძალადობისაგან ბავშვების დაცვის შესახებ (CETS 201)

მუხლი 9 – ბავშვების პორნოგრაფიასთან დაკავშირებული დანაშაულებები

(1) თითოეულმა მხარემ უნდა მიიღოს საჭირო საკანონმდებლო ან სხვა სახის ზომები იმისათვის, რომ სისხლის სამართლის დანაშაულად განსაზღვრონ წინასწარგანზრახული და უფლების გარეშე ჩადენილი შემდეგი სახის ქმედებები:

ა) ბავშვების პონოგრაფიასთან დაკავშირებული მასალების მომზადება;
ბ) ბავშვების პონოგრაფიასთან დაკავშირებული მასალების შეთავაზება;
გ) ბავშვების პონოგრაფიასთან დაკავშირებული მასალების გავრცელება ან გადაცემა;
დ) ბავშვების პონოგრაფიასთან დაკავშირებული მასალების შეძენა საკუთარი თავისთვის ან სხვა პირისთვის;
ე) ბავშვების პონოგრაფიასთან დაკავშირებული მასალების ფლობა;
ვ) ბავშვების პორნოგრაფიული მასალების შეგნებული მოპოვება საინფორმაციო და საკომუნიკაციო ტექნოლოგიების გამოყენებით;
(2) წინამდებარე მუხლის მიზნებიდან გამომდინარე, ტერმინი "ბავშვების პორნოგრაფია" ნიშნავს მასალებს, რომლებიც ვიზუალურად ასახავს ბავშვს, რომელიც მონაწილეობს ნამდვილ ან სიმულირებულ სექსუალურად აღმგზნებ საქციელში ან ბავშვის სექსუალური ორგანოების გამოსახულებას პირველადი სექსუალური მიზნებისათვის.

[168] ახსნა-განმარტებითი ანგარიში, №102

[169] ევროპის საბჭო – ევროპის საბჭოს კონვენცია სექსუალური ექსპლუატაციისა და სექსუალური ძალადობისაგან ბავშვების დაცვის შესახებ

[170] ავსტრია, ბელგია, ბულგარეთი, ხორვატია, კვიპროსი, ფინეთი, საფრანგეთი, გერმანია, საბერძნეთი, ირლანდია, ლიტვა, მოლდოვა, ნიდერლანდები, ნორვეგია, პოლონეთი, პორტუგალია, რუმინეთი, სან-მარინო, სერბეთი, სლოვაკეთი, შვედეთი, ყოფილი იუგოსლავიის რესპუბლიკა მაკედონია, თურქეთი, დანია, ისლანდია, იტალია, უკრაინა და გაერთიანებული სამეფო (ივლისი 2008)

[171] დამატებითი დეტალებისათვის იხილეთ: *Gercke,* ZUM 2008, 550ff

(3) თითოეულმა მხარემ შეიძლება დაიტოვოს უფლება არ გამოიყენოს, მთლიანად ან ნაწილობრივ, პუნქტი 1(ა) და 1(ე) იმ პორნოგრაფიული მასალის წარმოებასა და ფლობასთან მიმართებაში, რომელიც:
– შეიცავს მხოლოდ სიმულირებულ გამოსახულებას ან არარსებული ბავშვის რეალისტურ გამოსახულებას;
– ასახავს ბავშვებს, რომლებმაც მიაღწიეს მე-18 მუხლის მე-2 პუნქტით განსაზღვრულ ასაკს, როდესაც ეს გამოსახულებები არის შექმნილი და მათ მფლობელობაში მათივე თანხმობით და მხოლოდ მათი პირადი მოხმარებისათვის.
(3) თითოეულმა მხარემ შეიძლება დაიტოვოს უფლება არ გამოიყენოს, მთლიანად ან ნაწილობრივ, პუნქტი 1(ვ).

მუხლი 23 - ბავშვების ცდუნება სექსუალური მიზნებისათვის

თითოეულმა მხარემ უნდა მიიღოს საჭირო საკანონმდებლო ან სხვა სახის ზომები, იმისათვის რომ მოხდეს საინფორმაციო და საკომუნიკაციო ტექნოლოგიების საშუალებით გაკეთებული უფროსი პირის წინასწარგანზრახული შეთავაზების კრიმინალიზაცია, რაც გულისხმობს იმ ბავშვთან შეხვედრას, რომლესაც არ მიუღწევია მე-18 მუხლის მე-2 პარაგრაფით განსაზღვრული ასაკისათვის, იმ მიზნით, რომ ჩაიდინოს მე-18 მუხლის 1(ა) პუნქტით ან მე-20 მუხლის 1(ა) პუნქტით განსაზღვრული ნებისმიერი დანაშაული მის წინააღმდეგ, როდესაც ამ შეთავაზებას მოსდევს მატერიალური ქმედებები, რომლებსაც მივყავართ ამგვარ შეხვედრამდე.

201-ე კონვენციის მე-20 მუხლი დიდწილად განსხვავდება კომპიუტერული დანაშაულის შესახებ კონვენციის მე-9 მუხლისაგან. პირველი ძირითადი განსხვავება მდგომარეობს იმაში, რომ კომპიუტერული დანაშაულის შესახებ კონვენცია აქცენტს აკეთებს იმ ქმედებებზე, რომლებიც დაკავშირებულია საინფორმაცია და საკომუნიკაციო მომსახურებებთან (“ბავშვების პონოგრაფიასთან დაკავშირებული მასალების მომზადება მათი კომპიუტერული სისტემის მეშვეობით გავრცელების მიზნით“), ხოლო ბავშვთა დაცვის შესახებ კონვენციაში უფრო ფართო მიდგომაა (“ბავშვების პორნოგრაფიული მასალების მომზადება“) და იმ ქმედებებსაც მოიცავს, რომლებიც არ არის დაკავშირებული კომპიუტერულ ქსელებთან. გარდა ამისა, ბავშვთა დაცვის შესახებ კონვენციის მუხლი 20 (1) (ვ) გულისხმობს ბავშვების პორნოგრაფიის მოპოვების ქმედების კრიმინალიზაციასაც.[172] კომპიუტერული დანაშაულის შესახებ კონვენცია არ შეიცავს ამგვარ დებულებას.

201-ე კონვენციის 23-ე მუხლი ახდენს საინფორმაციო და საკომუნიკაციო ტექნოლოგიების საშუალებით სექსუალური მიზნებისათვის ბავშვების ცდუნების ქმედების კრიმინალიზაციას. კომპიუტერული დანაშაულის შესახებ კონვენცია არ შეიცავს ამგვარ დებულებას.

პრაქტიკული ინფორმაცია მოსამართლეებისათვის:

დამნაშავეებმა შეიძლება გამოიყენონ საინფორმაციო ტექნოლოგია იმისათვის, რომ ბავშვების პორნოგრაფიული სურათების გაცვლისას ან ვაჭრობისას დამალონ თავიანი იდენტურობა. ამ შემთხვევებში, საკრედიტო ბარათების

[172] დებულება განსაკუთრებით შეეხება იმ შემთხვევებს, როდესაც დამნაშავე აფასებს ინფორმაციას კომპიუტერულ ქსელში, მისი ჩამოტვირთვის გარეშე. ამგვარ შემთხვევებში ინფორმაციის ხელმისაწვდომობა, კომპიუტერული სისტემის კონფიგურაციისა და გამოყენებული მომსახურებიდან გამომდინარე, არ გულისხმობს ინფორმაციის ფლობას.

შესახებ ინფორმაციის ხელმისაწვდომობა შესაძლებელია იყოს უფრო ეფექტური, ვიდრე რეგისტრაციის ჟურნალის ანალიზი.

როგორ არის განსაზღვრული ეს დანაშაული თქვენი ქვეყნის კანონმდებლობაში?
ადგილობრივი კანონმდებლობის დებულებების განხილვა და სიტუაციური სავარჯიშოები

4.9. ინტელექტუალური საკუთრება და მასთან დაკავშირებული დანაშაულები

4.9.1. მოვლენა

მუსიკისა და ვიდეოების ანალოგიურიდან ციფრულ დისტრიბუციაზე გადასვლამ წარმოშვა საავტორო უფლებების დარღვევის ახალი ფორმები. ყოველდღიურად საავტორო უფლებებით დაცული მილიონობით სიმღერისა და ფილმის გაცვლა ხდება ფაილების კოლექტიური გამოყენების სისტემების მეშვეობით.[173] ზოგიერთი კინოფილმი მოხვდა ფაილების კოლექტიური გამოყენების სისტემებში კინოთეატრებში მათ მსოფლიო პრემიერამდეც კი.[174]

გასართობმა ინდუსტრიამ რეაგირება მოახდინა ტექნიკური ზომების მიღებით (ციფრული უფლებების მენეჯმენტი – DRM), რათა ხელი შეეშალა რეპროდუქციისათვის[175], მაგრამ დღემდე ხდება ამ ზომების გვერდზე ავლის გზების პოვნა მათი შემოღებიდან მოკლე პერიოდის განმავლობაში. არსებობს მთელი რიგი პროგრამული ინსტრუმენტები, რომლებიც შესაძლებლობას აძლევს მომხამრებელს მოახდინოს მუსიკის და კინოფილმების შემცველი იმ დისკების კოპირება, რომლებიც დაცულია ციფრული უფლებების მენეჯმენტის (DRM) სისტემებით. გარდა ამისა, ინტერნეტი იძლევა საშუალებას მოხდეს ასლების გავრცელება მთელს მსოფლიოში. შედეგად, ინტელექტუალური საკუთრების უფლებების, განსაკუთრებით კი საავტორო უფლებების დარღვევები, ინტერნეტში ყველაზე ხშირად ჩადენილი დანაშაულებებს შორის ერთ-ერთ პირველ ადგილზეა.

[173] The latest analysis regarding file-sharing activities in Germany identify up to 7.3 million users who download music files from the Internet. Up to 80% of these downloads are related to file-sharing systems. Source: GfK, Brennerstudie 2005.

[174] მაგალითი არის ფილმი "ვარსკვლავების ომი – ეპიზოდი 3", რომელიც გამოჩნდა ფაილების კოლექტიური მოხმარების სისტემებში მისი ოფიციალურ პრემიერამდე რამოდენიმე საათით ადრე. იხილეთ: http://www.heise.de/newsticker/meldung/59762 that is taking regard to a MPAA press release.

[175] გამოყენებულ ტექნოლოგიას ეწოდება "ციფრული უფლებების მენეჯმენტი" (DRM). ტერმინი "ციფრული უფლებების მენეჯმენტი" (DRM) გამოიყენება რამოდენიმე ტექნოლოგიის აღსანიშნავად, რომლებიც გამოიყენება პროგრამული უზრუნველყოფის, მუსიკის, ფილმების და სხვა ციფრული მონაცემების კონტროლირებადი ხელმისაწვდომობის უზრუნველსაყოფად წინასწარგანსაზღვრული წესების შესაბამისად. ერთ-ერთ ძირითად ფუნქციას წარმოადგენს კოპირებისაგან დაცვა, რაც მიზნად ისახავს იმ ელექტრონული მოწყობილობებზე არსებულ ციფრული მედია შინაარსზე კონტროლის ან შეზღუდული გამოყენებისა და ხელმისაწვდომობის დაწესებას, რომლებზეც დაინსტალირებულია ამგვარი ტექნოლოგიები.

4.9.2. სამართლებრივი რეაგირება

კონვენციაში შეტანილია დებულება, რომელიც მიზნად ისახავს სხვადასხვა მიდგომების ჰარმონიზებას, რათა ეროვნულ კანონებში მოხდეს სისხლისსამართლებრივი რეაგირება საავტორო უფლებების დარღვევებზე.

მუხლი 10 – საავტორო უფლებებისა და მათი მომიჯნავე სხვა უფლებების დარღვევასთან დაკავშირებული დანაშაულები

(1) თითოეულმა მხარემ უნდა მიიღოს იმგვარი საკანონმდებლო ან სხვა სახის ზომები, რომლებიც შეიძლება საჭირო გახდეს იმისათვის, რომ თავიანთ შიდა კანონმდებლობაში განსაზღვრონ სისხლის სამართლის დანაშაულად საავტორო უფლების დარღვევა, როგორც ეს განსაზღვრულია მოცემული მხარის კანონით, იმ ვალდებულებების შესაბამისად, რომლებიც მას დაეკისრა 1971 წლის 24 ივლისის პარიზის აქტის შესაბამისად, რომლითაც ცვლილებები შევიდა ლიტერატურული და მხატვრული ნაწარმოებების დაცვის შესახებ ბერნის კონვენციაში, ინტელექტუალური საკუთრებაზე უფლებების სავაჭრო ასპექტების შესახებ ხელშეკრულებაში და საავტორო უფლებების შესახებ ინლეტექტუალური საკუთრების მსოფლიო ორგანიზაციის ხელშეკრულებაში, ნებისმიერი იმ მორალური უფლებების გამოკლებით, რომლებიც მინიჭებულია ამ კონვენციების შესაბამისად, როდესაც ამგვარი ქმედებები ხორციელდება ნებაყოფლობით, კომერციული მასშტაბით და კომპიუტერული სისტემის მეშვეობით.
(2) თითოეულმა მხარემ უნდა მიიღოს იმგვარი საკანონმდებლო ან სხვა სახის ზომები, რომლებიც შეიძლება საჭირო გახდეს იმისათვის, რომ თავიანთ შიდა კანონმდებლობაში განსაზღვრონ სისხლის სამართლის დანაშაულად მომიჯნავე უფლებების დარღვევა, როგორც ეს განსაზღვრულია მოცემული მხარის კანონით, იმ ვალდებულებების შესაბამისად, რომლებიც მას დაეკისრა შემსრულებელთა, ფონოგრამების შემქნელთა და სამაუწყებლო ორგანიზაციების დაცვის შესახებ საერთაშორისო კონვენციის (რომის კონვენცია), ინტელექტუალური საკუთრებაზე უფლებების სავაჭრო ასპექტების შესახებ ხელშეკრულებისა და შესრულებებისა და ფონოგრამების შესახებ ინლეტექტუალური საკუთრების მსოფლიო ორგანიზაციის ხელშეკრულების შესაბამისად, ნებისმირი იმ მორალური უფლებების გამოკლებით, რომლებიც მინიჭებულია ამ კონვენციების შესაბამისად, როდესაც ამგვარი ქმედებები ხორციელდება ნებაყოფლობით, კომერციული მასშტაბით და კომპიუტერული სისტემის მეშვეობით.
(3) ნებისმიერმა მხარემ შეიძლება დაიტოვოს უფლება გარკვეულ გარემოებებში არ დააკისროს სისხლის სამართლის პასუხისმგებლობა მოცემული მუხლის 1-ლი და მე-2 პუნქტების შესაბამისად, იმ პირობით, რომ არსებობს სამართლებრივი დაცვის სხვა ეფექტური საშუალებები და, რომ მოცემული უფლება არ ამცირებს მხარის იმ საერთაშორისო ვალდებულებებს, რომლებიც განსაზღვრულია მოცემული მუხლის 1-ლ და მე-2 მუხლებში აღნიშნულ საერთაშორისო დოკუმენტებში.

კომპიუტერული დანაშაულის შესახებ კონვენციის მე-10 მუხლსა და ეროვნული მიდგომების უმრავლესობას შორის არსებულ ერთ-ერთ ძირითად განსხვავებას წარმოადგენს ის ფაქტი, რომ მე-10 მუხლი მკაფიოდ არ განსაზღვრავს იმ ქმედებებს, რომელთა კრიმინალიზაციაც უნდა მოხდეს და მხოლოდ მიუთითებს მთელ რიგ საერთაშორისო ხელშეკრულებებზე, მათ შორის ინტელექტუალური ქონების მსოფლიო ორგანიზაციის ხელშეკრულებაზე საავტორო უფლებების შესახებ.[176]

კომპიუტერული დანაშაულის შესახებ კონვენციის მე-10 მუხლის მიერ განსაზღვრულ საავტორო უფლებებთან დაკავშირებულ დანაშაულთა კრიმინალიზაცია[177] შემოიფარგლება მხოლოდ სერიოზული შემთხვევებით და, აქედან გამომდინარე, გამორიცხავს საავტორო უფლებების უმნიშვნელო დარღვევებს.[178] ამ კონტექსტში, კონვენცია მოიცავს მხოლოდ იმ ქმედებებს, რომლებიც ჩადენილია კომპიუტერული სისტემის მეშვეობით. საავტორო უფლებების დარღვევები არ მოიცავს იმ საინფორმაციო ტექნოლოგიებს, რომლებიც არ არის განსაზღვრული ამ დებულებით.

კრიმინალიზაციასთან დაკავშირებული მეორე ძირითადი შეზღუდვა განპირობებულია კომერციული მასშტაბის დარღვევის არსებობის მოთხოვნით. იგივე შეზღუდვა არსებობს ინტელექტუალური საკუთრების უფლებების ვაჭრობასთან დაკავშირებული ასპექტების შესახებ ხელშეკრულებაშიც, რომელიც მოითხოვს სისხლისსამართლებრივ დასჯას მხოლოდ „კომერციული მასშტაბის პირატობის“ შემთხვევაში. ვინაიდან კოლექტიური გამოყენების სისტემებში საავტორო უფლებების დარღვევის შემთხვევების უმეტესობა არ არის კომერციული მასშტაბის, მათზე არ ვრცელდება მე-10 მუხლის დებულებები.

პრაქტიკული ინფორმაცია მოსამართლეებისათვის:

ფაილების კოლექტიური მოხმარების სისტემების ყველაზე პოპულარული ვერსიები შესაძლებლობას აძლევს სამართალდამცავ ორგანოებს მოახდინოს იმ მომხმარებელთა იდენტიფიკაცია, რომლებიც ხელმისაწვდომს ხდიან საავტორო უფლებებით დაცულ ხელოვნების ნიმუშებს. დამნაშავეთა მიკვლევის ეს პროცესი არის უფრო რთული, როდესაც დამნაშავე იყენებს ფაილების კოლექტიური მოხმარების მესამე თაობის სისტემას[179], რომელიც იძლევა ანონიმური კომუნიკაციის საშუალებას. ამ შემთხვევებში კვალს უეჭველად არ მივყავართ დამნაშავესთან. ეს გარემოება უნდა იქნეს მიღებული მხედველობაში მოსამართლის მიერ მტკიცებულების შეფასების დროს.

როგორ არის განსაზღვრული ეს დანაშაული თქვენი ქვეყნის კანონმდებლობაში?

[176] ამ კონტექსტში მნიშვნელოვანია აღინიშნოს, რომ კონვენციის ხელმოწერა არ ავალდებულებს სახელმწიფოებს გახდნენ ინტელექტუალური ქონების მსოფლიო ორგანიზაციის წევრი. საკმარისია, რომ მოხდეს იმ დარღვევების კრიმინალიზაცია, რომლებიც აღნიშნულია კომპიუტერული დანაშაულის შესახებ კონვენციის მე-10 მუხლში.

[177] მე-3 პუნქტი შესაძლებლობას აძლევს მხარეებს თავიდან აიცილონ საავტორო უფლებების დარღვევების კრიმინალიზაცია, იმის გათვალისწინებით, რომ ისინი უზრუნველყოფენ სხვა ეფექტური საშუალებების გამოყენებას და, რომ ამგვარი აცილება არ შემცირებს მხარეთა საერთაშორისო ვალდებულებებს.

[178] კონვენციაში განსაზღვრულია მინიმალური სტანდარტები ინტერნეტთან დაკავშირებული დანაშაულებებისათვის. ამიტომ, მხარეებს შეუძლიათ გასცდნენ საავტორო უფლებების დარღვევების კრიმინალიზაციისათვის განსაზღვრულ «კომერციულ მასშტაბის» ფარგლებს.

[179] *Clarke/Sandberg/Wiley/Hong*, “Freenet: a distributed anonymous information storage and retrieval system”, 2001; *Chothia/Chatzikokolakis*, “A Survey of Anonymous Peer-to-Peer File-Sharing”: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao;Xiao*, “A Mutual Anonymous Peer-to-Peer Protocol Desing”, 2005.

ადგილობრივი კანონმდებლობის დებულებების განხილვა და სიტუაციური სავარჯიშოები

5. კომპიუტერულ-ტექნიკური ექსპერტიზა და ელექტრონული მტკიცებულება

სესიის ბოლოს მისმა მონაწილეებმა უნდა იცოდნენ:
- კომპიუტერულ-ტექნიკური ექსპერტიზის საფუძვლები;
- ექსპერტიზის ყველაზე ფართოდ გამოყენებული მეთოდები;
- ზომები, რომელთა მიღებაც საჭიროა ელექტრონული მტკიცებულების მოპოვებისა და ანალიზისათვის.

წინამდებარე ნაწილი შეიცავს მითითებებს უფრო დეტალურ ინფორმაციაზე კომპიუტერულ-ტექნიკური ექსპერტიზისა და ციფრული მტკიცებულებების სხვადასხვა ასპექტების, მათ შორის, საგამომძიებლო მეთოდების პრაქტიკულ გამოყენების თაობაზე.

კომპიუტერული დანაშაულებების ზრდასთან, ასევე, საინფორმაციო-საკომუნიკაციო ტექნოლოგიების გამოყენებასთან ერთად, კომპიუტერულ-ტექნიკური ექსპერტიზა და ციფრული მტკიცებულებები თამაშობენ მნიშვნელვან როლს სამართალდამცავი ორგანოებისა და სასამართლოების პრაქტიკულ საქმიანობაში. [180]კერძოდ, იმ შემთხვევებში, როდესაც გამოძიების პირველი ნაბიჯები ეფუძნება მხოლოდ ციფრულ კვალს (ვინაიდან ტრადიციული მტკიცებულებები, როგორებიცაა თითის ანაბეჭდები ან მოწმეები არ არსებობს), შესაძლებლობა იმისა, რომ წარმატებით მოხდეს დამნაშავის იდენტიფიცირება და მისი სამართლებრივი დევნა ეფუძნება ციფრული მტკიცებულებების სწორად შეგროვებასა და შეფასებას.[181]

[180] *Casey*, Digital Evidence and Computer Crime, 2004, გვერდი 11; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1; *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, ტომი 1, №1, გვ. 1

[181] კომპიუტერულ-ტექნიკური ექსპერტიზის ფორმალიზების საჭიროებასთან დაკავშირებით, იხილეთ: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, ტომი 3, №2

5.1. ციფრული მტკიცებულებები[182]

კომპიუტერული ტექნოლოგიების განვითარებასა და დანაშაულთა ჩადენისათვის მის გამოყენებასთან ერთად, ციფრული მტკიცებულებები იქცა ახალი ტიპის მტკიცებულებებად.[183] ციფრული მტკიცებულებად მიიჩნევა ნებისმიერი მონაცემები, რომლებიც ინახება ან გადაიცემა კომპიუტერული ტექნოლოგიის გამოყენებით და, რომელიც მხარს უჭერს თეორიას იმის შესახებ, თუ როგორ მოხდა დანაშაული.[184] ტრადიციული ფორმატის დოკუმენტაციიდან კომპიუტერულ ფაილებზე გადასვლის გამო, ციფრული მტკიცებულება თამაშობს მნიშვნელოვან როლს როგორც ტრადიციული დანაშაულთა, ასევე კომპიუტერული დანაშაულთა გამოძიების თვალსაზრისით.[185]

კომპიუტერული ტექნოლოგიის გამოყენებამ არა მარტო დანერგა მტკიცებულებების ახალი კატეგორია, არამედ ასევე გავლენა მოახდინა იმაზე, თუ როგორ იყენებენ სამართალდამცავი ორგანოები და სასამართლოები მტკიცებულებებს.[186] წარსულში ტრადიციული დოკუმენტაციის წარდგენა სასამართლოში ხდებოდა ქაღალდზე დაბეჭდილი ორიგინალი დოკუმენტის სახით.

იმის გამო, რომ არ არსებობს კონკრეტული ნორმები ციფრული მტკიცებულებების სასამართლოში წარდგენისათვის, ამგვარი მტკიცებულებები ხშირად წარდგენილი იყო ფაილების ან სხვა სახის მონაცემების ამონაბეჭდების ფორმით.[187] მთელმა რიგმა ქვეყნებმა დაიწყეს თავიანთი კანონმდებლობის განახლება, რათა სასამართლოებს შესაძლებლობა ჰქონდეთ ამობეჭდვის გარეშე გამოიყენონ ციფრული მტკიცებულებები.[188] კომპიუტერული დანაშაულის ტრანსნაციონალური შინაარსის მიუხედავად, მტკიცებულებების შეგროვება ძირითადად რეგულირდება ეროვნული ნორმატიული დოკუმენტებით.

5.1.1. ციფრულ მტკიცებულებებთან დაკავშირებული სირთულეები

ციფრულ მტკიცებულებებს გააჩნია მთელი რიგი მსგავსებები მტკიცებულებების სხვა კატეგორიებთან. შედეგად, მსგავსი მოთხოვნები[189] უნდა იქნეს მიღებული მხედველობაში, როდესაც საქმე გვაქვს ციფრულ მტკიცებულებებთან. სამართალდამცავმა ორგანოებმა უნდა უზრუნველყონ, რომ მტკიცებულება არის აუთენტური, სრული, სანდო[190], ზუსტი და, რომ მტკიცებულების მოპოვების პროცესი მიმდინარეობს კანონის მოთხოვნების

---

[182] ეს ნაწილი ითვალისწინებს შემდეგ დოკუმენტს: Fredesvinda Insa, CYBEX.

[183] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1; კომპიუტერული ექსპერტიზისა და ციფრული მტკიცებულებების ისტორიული განვითარების შესახებ, იხილეთ: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, ტომი 1, №1

[184] *Casey*, Digital Evidence and Computer Crime, 2004, გვ.12; The admissibility of Electronic evidence in court: fighting against high-tech crime,2005, Cybex,
http://www.cybex.es/agis2005/elegir_idioma_pdf.htm.

[185] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, ტომი 119, გვ.532; *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, ტომი 5, №1

[186] ტრადიციული პროცედურებისა და დოქტრინების საფუძველზე ციფრული მტკიცებულებების მოპოვება/გამოყენებასთან დაკავშირებული სირთულეების თაობაზე, იხილეთ: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, ტომი 29, №1, გვ. 57 და შემდგომ

[187] იხილეთ: *Vacca*, Computer Forensics, Computer Crime Scene Investigation, მე-2 გამოცემა, 2005, გვ.3

[188] ეროვნული კანონმდებლობის სტატუსის შესახებ, მაგალითისათვის იხილეთ: The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex,
http://www.cybex.es/agis2005/elegir_idioma_pdf.htm; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, ტომი X, №5

[189] იხილეთ: *Vacca*, Computer Forensics, Computer Crime Scene Investigation, მე-2 გამოცემა, 2005, გვ.19

[190] ციფრული გამოძიებებთან დაკავშირებული პასუხისმგებლობის შესახებ, იხილეთ: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, ტომი 1, №2

შესაბამისად.[191] ამავე დროს, მთელი რიგი ასპექტები ხდის ციფრულ მტკიცებულებას უნიკალურს და ამიტომ საჭიროებს განსაკუთრებულ ყურადღებას:

- მყიფე[192]. კომპიუტერული სისტემის მეშვეობით დამუშავებული ზოგიერთი ციფრული მონაცემები ძალზედ მყოფია და ადვილად შეიძლება წაიშალოს[193] და მოდიფიცირდეს. ეს ასპექტი კავშირშია ციფრული მტკიცებულების არა მხოლოდ შეფასებასთან, არამედ მისი შეგროვების პროცესთანაც. მონაცემები, რომლებიც ინახება მხოლოდ ოპერატიულ მონაცემების სისტემის მეხსიერებაში ზოგადად შეიძლება დაიკარგოს სისტემის გათიშვის შემთხვევაში[194], თუკი არ იქნება მიღებული სპეციალური ტექნიკური ზომები ამ პროცესის თავიდან ასაცილებლად.[195] რამდენადაც სისტემის მეხსიერებაში შენახული ინფორმაციას შეიძლება დიდი მნიშვნელობა ჰქონდეს გამოძიებისათვის[196], ამ მტკიცებულების შეგროვების ტექნიკა შეიძლება განსხვავდებოდეს ტრადიციული მტკიცებულებების შეგროვების პროცესებისაგან.

- შეცვლას დაქვემდებარებული. ციფრული მონაცემები ადვილად ექვემდებარება შეცვლას. კომპიუტერულ-ტექნიკური ექსპერტიზის ერთ-ერთ ფუნდამენტურ პრინციპს წარმოადგენს ციფრული მონაცემების ხელშეუხებლობის უზრუნველყოფის აუცილებლობა.[197] პროცესის სრული დოკუმენტაციისა და იმ მეთოდების გამოყენება, რომლებიც უზრუნველყოფს კომპიუტერული მონაცემების ხელშეუხელბლობას არსებითია იმისათის, რომ თავიდან იქნეს აცილებული ეჭვმიტანილის განცხადება იმის თაობზე, რომ მტკიცებულება გაყალბებული იქნა.[198] შედეგად, კომპიუტერულ-ტექნიკური ექსპერიტიზის სპეციალისტები ცდილობენ ჩაანაცვლონ გამოძიების ის პროცესები, რომლებიც იწვევს ეჭვმიტანილის კომპიუტერზე ფაილების შეცვლას უფრო დახვეწილი პროცესებით.

- დეცენტრალიზირებული შენახვა. კომპიუტერული ქსელისა და მონაცემთა შენახვისათვის განკუთვნილი დისტანციური სერვერების ხელმისაწვდომობამ გავლენა იქონია ინფორმაციის შენახვის ფორმაზე. მაშინ, როდესაც წარსულში გამომძიებლებს შესაძლებლობა ჰქონდათ კომპიუტერული მონაცემების ძებნის დროს აქცენტი გაეკეთებინათ ეჭვმიტანილის საცხოვრებელ ადგილზე, დღეს მათ სჭირდებათ მხედველობაში მიიღონ ის გარემოება, რომ ციფრული ინფორმაცია შეიძლება ფიზიკურად შენახული იქნეს საზღვარგარეთ და, საჭიროების შემთხვევაში, დისტანციურად იყოს გამოყენებული ეჭვმიტანილის მიერ.[199]

- ტექნიკური განვითარების სიჩქარე. ტექნიკური განვითარება სწრაფი ტემპებით მიმდინარეობს. მიღწევების მნიშვნელოვანი რაოდენობა

[191] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, ტომი 6, №2, 2006, გვ.161

[192] იხილეთ: Casey, Digital Evidence and Computer Crime, 2004, გვ.16; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, მე-2 გამოცემა, 2005, გვ.39

[193] *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, ტომი 29, №1, 2004, გვ. 58

[194] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, გვ. 88

[195] იხილეთ: *Haldermann/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldmann/Applebaum/Felten*, Lest We Remember: Colt Boot Attacks on Encryption Keys

[196] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, გვ.92

[197] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, ტომი 1, №1, გვ.1

[198] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, ტომი 6, №2, 2006, გვ. 162.

[199] *Casey*, Digital Evidence and Computer Crime, 2004, გვ.20

ახალი სირთულეების წინაშე აყენებს სასამართლო ექსპერტიზას.[200] ეს პროგრესი მოითხოვს იმ პირების მუდმივ წვრთნას, რომლებიც მონაწილეობენ მტკიცებულებების შეგროვებაში და, ასევე, ექსპერტიზისათვის საჭირო მოწყობილობებს მუდმივ განახლებას.[201] ოპერატიული სისტემების ახალ ვერსიებს და სხვა პროგრამულ პროდუქტებს შეუძლიათ გენერირება გაუკეთონ განსხვავებულ მონაცემებს, რომლებიც შეიძლება ასევე დაკავშირებული იქნეს გამოძიებებთან. იგივე პროგრესს განიცდის აპარატურაც.[202] მაშინ, როდესაც წარსულში მონაცემები ინახებოდა რბილ მაგნიტურ დისკებზე, დღეს გამომძიებლებმა უნდა გაითვალისწინონ ის გარემოება, რომ შესაბამისი ინფორმაცია შეიძლება შენახული იქნეს MP3 პლეერებზე ან საათებში, რომლებიც შეიცავენ USB შესანახ მოწყობილობებს.

[200] *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, ტომი 1, №3, გვ. 1

[201] კომპიუტერული ექსპერტიზის ფორმალიზაციის საჭიროების შესახებ, იხილეთ: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, ტომი 3, №2, გვ. 2

[202] See *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, ტომი 119, გვ.538

5.1.2. ტრადიციული მტკიცებულებები კვლავ მნიშვნელოვანია

მიუხედავად იმ ფაქტისა, რომ კომპიუტერულ დანაშაულობათა შემთხვევების გამოძიებისას[203] აქცენტი გაკეთდება ციფრულ მტკიცებულებაზე, დამნაშავის იდენტიფიცირებაში მნიშვნელოვან როლს თამაშობს მტკიცებულებების სხვა კატეგორიებიც და ამიტომ არ უნდა გამოირიცხოს. ეს განსაკუთრებით ყურადსაღებია, ვინაიდან კომპიუტერით განხორციელებული ყველა ოპერაცია არ ტოვებს ციფრულ კვალს და ყველა არსებული კვალი არ არის დაკავშირებული ეჭვმიტანილთან.[204] მაგალითად, თუკი ეჭვმიტანილი იყენებს საზოგადოებრივ ინტერნეტ კაფეს ბავშვების პორნოგრაფიის ჩამოსატვირთად, შეუძლებელი იქნება ჩამოტვირთვის პროცესის დაკავშირება კონკრეტულ პიროვნებასთან, თუკი იგი არ დარეგისტრირდა[205] ან არ დატოვა პირადი ინფორმაცია. ამ შემთხვევაში სასარგებლო იქნება სათვალთვალო ვიდეო კამერის ჩანაწერი, ამგვარის არსებობის შემთხვევაში.

რაც შეეხება იმ დანაშაულებებს, რომლებიც მოიცავს ფინანსურ ტრანზაქციებს, დამნაშავის იდენტიფიცირების მიზნით გამოძიებამ უნდა გაითვალისწინოს საფინანსო ორგანიზაციების მიერ შენახული ჩანაწერები. ბავშვების პორნოგრაფიის წინააღმდეგ 2007 წელს ჩატარებული გლობალური მასშტაბის გამოძიება ეფუძნებოდა ეჭვმიტანილთა იდენტიფიცირებას იმ ფინანსური ტრანზაქციების ანალიზის მიხედვით, რომლებიც ხორციელდებოდა ბავშვების პორნოგრაფიის შესყიდვის მიზნით.[206]

[203] *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, ტომი 29, №1, 2004, გვ.58

[204] კომპიუტერში შენახული ჩანაწერებთან ეჭვმიტანილის დასაკავშირებლად გამოყენებული მიდგომების შესახებ იხილეთ, მაგალითად: *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, ტომი 6, №2, 2006, გვ. 165

[205] იტალიაში საზოგადოებრივი ინტერნეტ ტერმინალებით სარგებლობამდე დარეგისტრირების ვალდებულების თაობაზე, იხილეთ: *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, CRi 2006, გვ. 94

[206] იხილეთ: *Schnabel*, The Mikado Principle, Datenschutz und Datensicherheit, 2006, გვ. 426 და შემდგომ

5.2. კომპიუტერულ-ტექნიკური ექსპერტიზა

ტერმინი კომპიუტერულ-ტექნიკური ექსპერტიზა გამოიყენება ციფრული მტკიცებულებების ძებნის მიზნით საინფორმაციო-ტექნიკური მოწყობილობების სისტემური ანალიზის აღსანიშნავად.[207] კომპიუტერულ-ტექნიკური ანალიზი ჩვეულებრივ ხორციელდება დანაშაულის ჩადენის შემდგომ. [208] ჩვეულებრივ გამოძიებებთან შედარებით, ამგვარი ანალიზის განხორციელება დაკავშირებულია სპეციფიკურ სირთულეებთან, ვინაიდან კომპიუტერული ტექნოლოგია მუდმივად იცვლება და სულ უფრო და უფრო მეტი ინფორმაცია ინახება ციფრულ ფორმატებში, რაც ზრდის პოტენციური მტკიცებულებების რაოდენობას.[209] შესაბამისად, აქცენტი კეთდება მტკიცებულებების სამართალწარმოებაში გამოყენების შესაძლებლობაზე.[210]ეს კი გარკვეულწილად ამცირებს კომპიუტერულ-ტექნიკური ექსპერტიზების ჩატარების შესაძლებლობას, ვინაიდან ისინი შეზღუდულები არიან სამართლებრივი სტანდარტებით.[211] იმ შემთხვევაშიც კი, თუკი ახალი ტექნიკური მიღწევები შესაძლებელს გახდის ახალ კომპიუტერულ-ტექნიკურ გამოძიებებს, მათი გამოყენება დამოკიდებული იქნება იმაზე, თუ რამდენად იქნება ეს ახალი ინსტრუმენტები გათვალისწინებული არსებული საკანონმდებლო ბაზით.

5.2.1. კომპიუტერულ-ტექნიკური ექსპერტების მონაწილეობის ფაზები

კომპიუტერულ-ტექნიკური ექსპერტები მონაწილეობენ არა მხოლოდ სისხლის სამართლის საქმეების წარმოებაში, არამედ თამაშობენ მნიშვნელოვან როლს სამოქალაქო საქმეების წარმოებაშიც, დაცვის სტრატეგიის განვითარებასა და განათლებაში. სისხლის სამართლის საქმეების წარმოებასთან მიმართებაში, მათი ჩართულობა ხდება ოთხ ეტაპზე:[212]

- შესაბამისი მტკიცებულების იდენტიფიცირება. კომპიუტერულ-ტექნიკურ ექსპერტები თამაშობენ მნიშვნელოვან როლს საგამოძიებო სტრატეგიის შემუშავებაში. მათ შეუძლიათ დაეხმარონ სამართალდამცავ ორგანოებს გამოძიების დაწყებამდე განსაზღვრონ საუკეთესო საგამოძიებო ტექნიკა. გარდა ამისა, კომპიუტერულ-ტექნიკური ექსპერტ-კონსულტანტები თამაშობენ მნიშვნელოვან როლს გამოძიების პროცესში, მაგალითად, იმით, რომ აკეთებენ ქსელის ინფრასტრუქტურის ანალიზს ეჭვმიტანილის სახლში, რათა

[207] იხილეთ: *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, ტომი 6, №2, 2006, გვ. 162; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, მე-2 გამოცემა, 2005, გვ.21; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, ტომი 4, №1; *Reith/Carr/Gunsch*, Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, ტომი 1, №2, გვ. 3

[208] იხილეთ: *Vacca*, Computer Forensics, Computer Crime Scene Investigation, მე-2 გამოცემა, 2005, გვ.21

[209] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, ტომი 119, გვ.532 იხილეთ: *Vacca*, Computer Forensics, Computer Crime Scene Investigation, მე-2 გამოცემა, 2005, გვ.35

[210] იხილეთ: *Vacca*, Computer Forensics, Computer Crime Scene Investigation, მე-2 გამოცემა, 2005, გვ.35

[211] *Kenneally*, Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection, UCLA Journal of Law & Technology, 2005, ტომი 9, №2

[212] კომპიუტერული დამაშაულის გამოძიებების სხვადასხვა მოდელებთან დაკავშირებით, იხილეთ: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, ტომი 3, №1; ასევე, იხილეთ: *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, ტომი 4, №1, რომელიც დიფერენციაციას აკეთებს ექვს სხვადასხვა ფაზას შორის.

განსაზღვრონ შესანახი მოწყობილობების შესაძლო ადგილმდებარეობა.[213]

- მტკიცებულებების შეგროვება და შენახვა. ციფრული მტკიცებულებების შეგროვება შესაძლებელია მოხდეს როგორც ფიზიკურად იმ ადგილზე, სადაც ისინი ინახება, ასევე, დისტანციურად. გამომძიებლებს, რომლებიც პირველ ნაბიჯებს აკეთებენ მტკიცებულებების შესაგროვებლად (პირველი რესპონდერი), მნიშვნელოვანი პასუხისმგებლობა აკისრიათ გამოძიების მთელი პროცესის წარმართვისათვის.[214] თუკი ისინი მიიღებენ არამართებულ გადაწყვეტილებებს მონაცემების შენახვასთან მიმართებაში, შესაძლებელია დაიკარგოს მნიშვნელოვანი კვალი. მათი ამოცანის სირთულეზე მეტყველებს, მაგალითად, ის, თუ როგორ მოექცნენ ისინი ეჭვმიტანილის ჩართულ კომპიუტერებს. [215] კომპიუტერის გამორთვის მაგივრად, ოპერატიული სისტემის ბრძანებების გამოყენებით მისთვის ელექტროენერგიის მიწოდების შეწყვეტა ზოგადად რეკომენდრიებული პროცედურაა. მაგრამ იმ შემთხვევაში, თუკი დამნაშავე იყენებდა დაშიფრვის ტექნოლოგიას, ელექტროენერგიის მიწოდების შეწყვეტამ შეიძლება გამოიწვიოს ფაილების განშიფვრა. ამიტომ, პირველმა რესპონდერმა უნდა მიიღოს გადაწყვეტილება იმასთან დაკავშირებით, თუ რაზე გააკეთოს გამოძიებამ აქცენტი.

კომპიუტერულ-ტექნიკური ექსპერტიზა არ არის გამართლებული იმ გამოძიებებისათვის, რომლებიც ტარდება შესაბამისი მონაცემების შენახვის ადგილებზე. კომპიუტერულ-ტექნიკურ ექსპერტებს ასევე შეუძლიათ დახმარება გაუწიონ გამოძიებას იმით, რომ მოამზადებენ მოთხოვნას სერვისის პროვაიდერებისათვის წარდგენის მიზნით[216] და დაეხმარებიან გამომძიებლებს შესაბამისი საქმის დოსიების შექმნაში[217], რომლებიც საჭიროა შეგროვებული მტკიცებულებების სანდოობის დასამტკიცებლად.

- კომპიუტერული ტექნოლოგიის ანალიზი და ციფრული მტკიცებულებები. მესამე ეტაპი მოიცავს ციფრული მტკიცებულებების და, ასევე, ამოღებული აპარატურის ანალიზთან დაკავშირებულ ყველა ასპექტს. ზოგადად ეს არის ყველზე რთული ეტაპი გამოძიების მთელს პროცესში.[218] პირველი რესპონდერები ხშირად კონფისკაციას უკეთებენ რამოდენიმე შესანახ მოწყობილობას. თითოეული შესანახი მოწყობილობა შეიძლება შეიცავდეს ათასობით ფაილს. მონაცემთა მხოლოდ ის რაოდენობაც კი, რომელსაც სჭირდება ანალიზი თავისთავად დიდი სირთულეების წინაშე აყენებს გამომძიებლებს.[219] აქედან გამომდინარე, გამოძიებისათვის შესაბამისი ინფორმაციის იდენტიფიცირება და მისი დაკავშირება წარმოადგენს კომპიუტერულ-ტექნიკური ექსპერტების ერთ-ერთ უმთავრეს ამოცანას.[220] მათი სამუშაო

[213] სასამართლო ექსპეტებიც კი ყველა შემთხვევაში ვერ შესძლებენ შენახვის ადგილმდებარეობის იდენტიფიცირებას იმ ადანიამების დახმარების გარეშე, რომლებმაც იციან ადგილობრივი სისტემის კონფიგურაცია. გამოძიების მხარდაჭერის მიზნით სპეციალური ცოდნის მქონეს ადამიანების, როგორებიცაა სისტემის ადმინისტრატორები, მოთხოვნის შესაძლებლობის შესახებ იხილეთ: კომპიუტერული დანაშაულის შესახებ კონვენციის მე-4 პარაგრაფის მე-19 მუხლი.

[214] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, გვ.88

[215] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, გვ. 171

[216] იხილეთ: *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, გვ. 15

[217] იხილეთ: *Vacca*, Computer Forensics, Computer Crime Scene Investigation, მე-2 გამოცემა, 2005, გვ. 24

[218] *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, ტომი 14, №1

[219] კომპიუტერული ექსპერტიზის ფორმალიზაციის საჭიროების თაობაზე, იხილეთ: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, ტომი 3, №2, გვ.2

[220] *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, ტომი 4, №1

მოიცავს როგორც კომპიუტერულ სისტემაში არაკანონიერი შინაარსის ძიებას, ასევე, რეგისტრაციის ფაილების ანალიზს.[221] კომპიუტერული დანაშაულის ჩადენისას დამნაშავის მიერ განხორციელებული ყველა ქმედება არ ტოვებს კვალს. მიუხედავად ამის, ყველა ხელმისაწვდომი მტკიცებულებების ანალიზით კომპიუტერულ-ტექნიკური ექსპერტებს შეუძლიათ დაადგინონ, თუ რა გზით იქნა დანაშაული იქნა ჩადენილი.[222] მესამე ეტაპი ასევე მოიცავს სრული ანგარიშის მომზადებას, რომელშიც სხვა საკითხებთან ერთად მოცემულია გამოძიების იმ ეტაპებისა და მეთოდების ჩამონათვალი, რომლებიც გამოყენებული იქნა მტკიცებულებების მოსაპოვებლად.

- მკიცებულების წარდგენა სასამართლოში. ზოგადად, კომპიუტერულ-ტექნიკური ექსპერტები არ წარადგენენ მტკიცებულებას სასამართლოში, თუმცა მათ შეუძლიათ ითამაშონ მნიშვნელოვანი როლი სისხლის სამართლის საქმის წარმოებაში. კომპიუტერულ-ტექნიკურმა ექსპერტებმა შეიძლება შეასრულონ ექსპერტი-მოწმეების როლი, რითაც დაეხმარებიან სასამართლო პროცესში ჩართულ ადამიანებს გაიაზრონ მტკიცებულებების შექმნისა და მათი შეფასების პროცესები, ასევე, მტკიცებულებების შეგროვებისათვის გამოყენებული პროცედურები.[223]

5.2.2. კომპიუტერულ-ტექნიკური ექსპერტიზების ნიმუშები

ოთხი ეტაპის ფარგლებში (და განსაკუთრებით მესამე ეტაპზე) შესაძლებელია განხორციელდეს მრავალრიცხოვანი კომპიურტერულ-ტექნიკური ექსპეტიზები. მართებული საგამომძიებლო ტექნიკის არჩევა დამოკიდებულია სხვადასხვა ფაქტორებზე – განსაკუთრებით კი იმაზე, თუ თუ რა სახის დანაშაული წარმოადგენს გამოძიების საგანს.

ყველზე გავრცელებულ ტექნიკებს შორის არის:

- აპარატურის ანალიზი. თუკი გამომძიებლების მიერ ხდება კომპიუტერის აპარატურული უზრუნველყოფის კონფისკაცია, კომპიუტერულ-ტექნიკურ ექსპერტებს შეუძლიათ ჩაატარონ მისი ანალიზი სისტემასთან დაკავშირებული ინფორმაციის შესაგროვებლად. ამგვარი გამოძიების გზით შესაძლებელია, მაგალითად, იმის დამტკიცება, ჰქონდა თუ არა დამნაშავეს შესაძლებლობა შეეერთებინა კომპიუტერული სისტემა ინტერნეტთან. გარდა ამისა, აპარატურის ანალიზი შესაძლებელია საჭირო იყოს, თუკი, რეგისტრაციის პროცესში სისტემასთან დაკავშირებული ინფორმაციის გადაცემის გამო ცნობილი გახდება, რომ ეჭვმიტანილმა გამოიყენა აპარატურის კონკრეტული კონფიგურაცია.

- კომპიუტერის პროგრამული უზრუნველყოფის ფუნქციის ანალიზი. აპარატურის გარდა, კომპიუტერის პროგრამული უზრუნველყოფა თამაშობს მნიშვნელოვან როლს კომპიუტერული სისტემის მუშაობაში. მაგალითად, კომპიუტერულ-ტექნიკურ ექსპერტებს შეუძლიათ განსაზღვრონ კომპიუტერული ვირუსის ან ზიანის გამომწვევი პროგრამული საშუალებების სხვა ფორმების ფუნქციებიც. გარდა ამისა, მათ შეუძლიათ აღადგინონ პროგრამული უარუნველყოფის

[221] დამატებითი დეტალებისათვის იხილეთ ქვემოთ
[222] *Casey*, Digital Evidence and Computer Crime, 2004, გვ.16
[223] იხილეთ: *Vacca*, Computer Forensics, Computer Crime Scene Investigation, მე-2 გამოცემა, 2005, გვ.12

ფუნქციონირების პროცესები.[224] გარდა ამისა, პროგრამული უზრუნველყოფის ანალიზი შესაძლებელია მნიშვნელოვანი იყოს იმისათვის, რომ განისაზღვროს არის თუ არა კრიმინალიზირებული იმ პროგრამული უზრუნველყოფის წარმოება ან გაყიდვა, რომელიც შესაძლებლია გამოყენებული იქნეს როგორც კანონიერი, ასევე არაკანონიერი მიზნებისათვის (ორმაგი დანიშნულებით).[225]

- ეჭვმიტანილის კომპიუტერულ სისტემაში დაინსტალირებული პროგრამული უზრუნველყოფის ანალიზი. კომპიუტერულ სისტემაში დაინსტალირებული პროგრამული უზრუნველყოფის ანალიზმა გამომძიებლებს შეიძლება მიაწოდოს ღირებული ინფორმაცია შემდგომი გამოძიებისათვის. ეს განსაკუთრებით შეეხება დაშიფრვის პროგრამულ უზრუნველყოფას და საშუალებებს, რომლებიც გამოყენებულია ფაილების საიმედოდ წასაშლელად.[226] თუკი ამგვარი პროგრამული უზრუნველყოფა დაინსტალირებულია ეჭვმიტანილის კომპიუტერზე, შემდგომი გამოძიებები შესაძლოა უშუალოდ შეეხოს ამ საკითხებს.

- შესაბამისი ციფრული ინფორმაციის იდენტიფიცირება. კომპიუტერული მონაცემები შესაძლებელია შენახული იქნეს სხვადასხვა სახის შემნახველ მოწყობილობებზე. თავად მყარ დისკზეც კი არსებობს ფაილის შენახვის სხვადასხვა შესაძლებლობები. აქედან გამომდინარე. რთულია განისაზღვროს შესაბამისი მტკიცებულების შენახვის ადგილმდებარეობა.[227]

ერთ-ერთი ახალი ტენდენცია, რომელიც დამატებით სირთულეებს ქმნის შესაბამისი ციფრული ინფორმაციის იდენტიფიცირებისათვის არის დისტანციური შემნახავი მოწყობილობების სულ უფრო ფართო გამოყენება. როგორც ეს ზემოთ აღინიშნა, ფართოსარტყელიანი ინტერნეტის წყაროსა და დისტანციური შესანახი სერვერების ხელმისაწვდომობამ გავლენა მოახდინა ინფორმაციის შენახვის მეთოდზე. ამგვარი დისტანციური შემნახავი მოწყობილობის გამოყენებით, ეჭვმიტანილს შეუძლია თავიდან აიცილოს ეჭვმიტანილის კომპიუტერის იმ აპარატურული საშუალებების კონფისკაცია, რომლებიც საშუალებას აძლევს სამართალდამცავ ორგანოებს მოიპოვონ დისტანციურ შემნახავ მოწყობილობებში შენახული ინფორმაცია. კომპიუტერულ-ტექნიკური ექსპერტიზა ამ შემთხვევაში შესაძლებებლია გამოყენებული იქნეს იმის შესამოწმებლად, გამოიყენა თუ არა ეჭვმიტანილმა დისტანციური შემნახავი სერვისები.[228]

შესაბამისი ციფრული ინფორმაციის იდენტიფიცირება არ შემოიფარგლება მხოლოდ ფაილებით. პროგრამული საშუალებების საინფორმაციო ბაზები, რომლებიც გამოიყენება ეჭვმიტანილის მიერ მის კომპიუტერზე ინფორმაციის მოსაძებნად ასევე შეიძლება შეიცავდეს შესაბამის ინფორმაციას.[229] სისტემის მიერ შექმილი დროებითი ფაილებიც კი შესაძლოა შეიცავდნენ სისხლის სამართლის საქმის წარმოებისათვის საჭირო მტკიცებულებებს.[230]

---

[224] იხილეთ: *Vacca*, Computer Forensics, Computer Crime Scene Investigation, მე-2 გამოცემა, 2005, გვ.30

[225] იხილეთ ზემოთ: თავი 3.5

[226] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9.

[227] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 24.

[228] გამოძიების ტექნიკის შესახებ იხილეთ: *Casey*, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 204, გვ. 283 და შემდგომ

[229] *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, ტომი 5, №1

[230] *Howard*, Don't Cache out your Case: Prosecuting Child Pornography Possession Laws Based on Images located in Temporary Internet Files, Berkeley Technology Law Journal, 2004, ტომი 19, გვ. 1227 და შემდეგომ;

- ფარული ფაილების იდენტიფიცირება. დამნაშავეებმა შესაძლოა გამოიყენონ ფაილების შემნახავ მოწყობილობაში შენახვის ტექნიკა, რათა ხელი შეუშალონ სამართალდამცავ ორგანოებს მოახდინონ ფაილის შინაარსის ანალიზი. ეს განსაკუთრებით შეეხება არაკანონიერი შინაარსის გამოვლენასთან დაკავშირებით მიმდინარე გამოძიებებს. კომპიუტერულ-ტექნიკურ ექსპერტიზას შეუძლია მოახდინოს ფარული ფაილების იდენტიფიცირება და ანალიზი.[231]

- წაშლილი ფაილების აღდგენა. თუკი დამნაშავეები იყენებენ საშუალებებს, რომლებიც უზრუნველყოფენ ფაილების საიმედო წაშლას, ამგვარი ინფორმაციის აღდგენა ზოგადად შეუძლებელია.[232] მაგრამ იმ შემთხვევებში, როდესაც დამნაშავეებმა არ იციან ამგვარი საშუალებების არსებობს შესახებ, ციფრული ინფორმაციის წაშლა არ ნიშნავს მათი სამართალდამცავი ორგანოებისათვის ხელმიუწვდომობას, ვინაიდან ისინი შეიძლება აღდგენილი იქნეს კომპიუტერულ-ტექნიკური ექსპერტიზის სპეციალური პროგრამული საშუალებების გამოყენებით.[233]

- დაშიფრული ფაილებისა და ტომების განშიფრვა და პაროლების აღდგენა. დამნაშავეები სულ უფრო და უფრო ხშირად იყენებენ დაშიფრვის ტექნოლოგიას.[234] ეს ტექნოლოგია სამართალდამცავ ორგანოებს მნიშვნელოვანი სირთულეების წინაშე აყენებს, ვინაიდან მათ არ შეუძლიათ მოიპოვონ და გამოიკვლიონ დაშიფრული ინფორმაცია.[235] კომპიუტერულ-ტექნიკური ანალიზის ფარგლებში შესაძლებელია მიღებული იქნეს ზომები დაშიფრული ფაილებისა და შემნახავი მოწყობილობების განშიფრვისათვის.[236] გარდა ამისა, კომპიუტერულ-ტექნიკური ექსპერტიზის სპეციალისტები შეიძლება დაეხმარონ სამართალდამცავ ორგანოებს შეიმუშავონ სტრატეგია დაშიფრული ფაილების განსაშიფრად – მაგალითად, კლავიატურის მეშვეობით შეყვანილი ინფორმაციის ხელში ჩასაგდებად შექმნილი პროგრამის გამოყენებით.[237]

Gordon/Hosmer/Siedsma/Rebovich, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, გვ. 54

[231] იხილეთ *Vacca*, Computer Forensics, Computer Crime Scene Investigation, მე-2 გამოცემა, 2005, გვ.43; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, ტომი 29, №1, 2004, გვ. 59

[232] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, გვ.38

[233] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6;
Gordon/Hosmer/Siedsma/Rebovich, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, გვ.38

[234] *Casey*, Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, 2002, ტომი 1, №3

[235] *Goodman*, Why the Police don't care about Computer Crime, Harvard Journal of Law & Technology, 1997, ტომი 10, №3, გვ. 473; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, გვ. 38; *Gercke*, Challenges related to the Fight against Cybercrime, Multimedia und Recht, 2008, გვ. 297

[236] *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encrpytion Threat, International Journal of Digital Evidence, 2004, ტომი 2, №3. კომპიუტერულ-ტექნიკური გამოძიებებისას განშიფრვის პროცესის თაობაზე, იხილეთ: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, გვ. 59

[237] *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encrpytion Threat, International Journal of Digital Evidence, 2004, ტომი 2, №3. კომპიუტერულ-ტექნიკური ექსპერტიზის პროგრამული უზრუნველყოფის საპროექციო ფანარის თაობაზე, რომელიც შეიქმნა კლავიატურის მეშვეობით შეყვანილი ინფორმაციის ხელში ჩასაგდებად და გამოიყენება აშშ-ის სამართალდამცავი ორგანოების მიერ, იხილეთ: *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, ტომი 15, №2, 2005, გვ. 521 და შემდგომ; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, გვ.3;
Green, FBI Magic Lantern reality check, The Register, 03.12.2001:
http://www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/;
Salkever, A Dark Side to the FBI's Magic Lantern, Business Week, 27.11.2001:
http://www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; *Sullivan*, FBI software cracks encryption wall, 2001:

დამნაშავეებს შეუძლიათ არა მხოლოდ დაბლოკონ გარკვეული ინფორმაცია დაშიფრვის გამოყენებით, არამედ გამოიყენონ პაროლით დაცული სისტემებიც. კომპიუტერულ-ტექნიკურმა ანალიზმა შეიძლება გამოიყენოს პაროლის აღდგენის მეთოდი, რათა საშუალება მისცეს სამართალდამცავ ორგანოებს გახსნან პაროლით დაცული სისტემები.[238]

- ფაილების ანალიზი. შემნახავ მოწყობილობაზე შენახული ფაილები შეიძლება გაანალიზდეს სხვადასხვა გზებით. კომპიუტერულ-ტექნიკურ ექსპერტიზებს, მაგალითად, შეუძლიათ აქცენტი გააკეთონ ფაილების შინაარსზე. საეჭვო ფაილების მანუალური შემოწმების გარდა, კომპიუტერულ-ტექნიკურმა გამოძიებებმა ასევე შეიძლება მოიცვას ტექსტობრივ ფაილებში ძირეული სიტყვების ავტომატური ძებნა[239] და ის საშუალებები, რომლებიც ავტომატურად ეძებენ ნაცნობ გამოსახულებებს ეჭვმიტანილის კომპიუტერზე.[240]

  როგორც ზემოთ ავღნიშნეთ, საკმაოდ ადვილია კომპიუტერული მონაცემებით მანიპულირება.[241] კომპიუტერულ-ტექნიკურმა ექსპერტიზებმა შეიძლება გამოავლინონ ციფრულ დოკუმენტში შეტანილი ცვლილებები და გაყალბებები.[242]

  გარდა ამისა, გამოძიებებმა შესაძლებელია მხედველობაში მიიღოს მეტამონაცემები.[243] ამ ტიპის ანალიზებმა შეიძლება განსაზღვროს დოკუმენტის[244] ბოლოს გახსნისა და შეცვლის დრო.[245] გარდა ამისა, მეტამონაცემების ანალიზი შეიძლება გამოყენებული იქნეს მუქარის შემცველი ფაილის ავტორის ან იმ კამერის სერიული ნომრის იდენტიფიცირებისათვის, რომელიც გამოყენებული იქნა ბავშვების პორნოგრაფიული გამოსახულების შესაქმნელად.

- ავტორობის ანალიზი. თუკი მუქარის ტექსტების ან ქსენოფობიური მიმართვების განთავსება ხდება ინტერნეტის ქსელურ დღიურებში ან ფორუმებზე, რეგისტრაციის ჟურნალის ანალიზმა შეიძლება არ მიიყვანოს გამომძიებლები ტექსტის ავტორთან, თუკი ეჭვმიტანილი მოქმედებს ინტერნეტ კაფედან და იყენებს ანონიმურ საკომუნიკაციო მომსახურებას. დეტალური ლინგვისტური ანალიზის საშუალებით შესაძლებელია განისაზღვროს, დაწერა თუ არა ეჭვმიტანილმა სტატიები მანამადე და დატოვა თუ არა ინფორმაცია, რომლის

---

http://www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm; Abreu, FBI confirms "Magic Lantern" project exists, 2001:
http://www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf.

[238] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, გვ. 59.

[239] იხილეთ: *Vacca*, Computer Forensics, Computer Crime Scene Investigation, მე-2 გამოცემა, 2005, გვ.48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, გვ. 63

[240] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, გვ.57

[241] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, ტომი 6, №2, 2006, გვ. 162

[242] იხილეთ: *Vacca*, Computer Forensics, Computer Crime Scene Investigation, მე-2 გამოცემა, 2005, გვ.29

[243] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

[244] გარბენის დროის შესახებ მონაცემების მანიპულირების შესაძლებლობისა და კომპიუტერულ-ტექნიკური გამოძიებებში რესპონდერის თაობაზე, იხილეთ: *Gladyshev/Patel*, Formalising Event Time Bounding in Digital Investigations, International Journal of Digital Evidence, 2005, ტომი 4, №1; დინამიური დროის ანალიზთან დაკავშირებით, იხილეთ: *Weil*, Dynmaic Time & Date Stamp Analysis, International Journal of Digital Evidence, 2002, ტომი 1, №2

[245] *Casey*, Digital Evidence and Computer Crime, 2004, გვ.16

საშუალებითაც შესაძლებელია მოხდეს პირის იდენტიფიცირება ამ კონტექსტში.[246]

- მონაცემთა ხელშეუხებლობის უზრუნველყოფა. როგორც ზემოთ აღინიშნა, ციფრული მტკიცებულებების ხელშეუხებლობის დაცვა მნიშვნელოვანია სასამართლოს მიერ მათი მიღების თვალსაზრისით.[247] კომპიუტერულ-ტექნიკური ექსპერტიზის სპეციალისტებმა შესაძლებელია უზრუნველყონ ფაილების ხელშეუხებლობის დაცვა მტკიცებულებების შეგროვების პროცესში. ეს საშუალებას აძლევს სამართალდამცავ ორგანოებს ზოგიერთ შემთხვევაში თავი აარიდონ აპარატურის კონფისკაციას და სანაცვლოდ მოახდინონ შესაბამისი ფაილების კოპირება და უზრუნველყონ გამოძიების პროცესში მათი ხელშეუხებლობის დაცვა ნებისმიერი სახის ცვლილებისაგან.[248] კერძოდ, ეს გულისხმობს ინფორმაციის მატარებლის ასლების შექმნას.[249]

- ინტერნეტ პროტოკოლის (IP) მიკვლევა. დამნაშავეები, რომლებიც იყენებენ ინტერნეტს დანაშაულის ჩასადენად (მაგალითად, ახდენენ ბავშვების პრონოგრაფიული სურათების ჩამოტვირთვას ან ახორციელებენ თავდასხმებს კომპიუტერულ სისტემებზე), ტოვებენ კვალს.[250] ტრაფიკის მონაცემების ანალიზმა, კერძოდ, ინტერნეტ სერვერში შენახული რეგისტრაციის ფაილების შესწავლამ შესაძლებელია მიიყვანოს გამომძიებლები იმ კავშირამდე, რომელიც გამოყენებული იქნა დამნაშავის მიერ ინტერნეტთან დასაკავშირებლად.[251] ამგვარი გამოძიებები შესაძლებელია დაკავშირებული იყოს სირთულეებთან, თუკი დამნაშავეები იყენებენ ანონიმურ საკომუნიკაციო ტექნოლოგიას.[252] მაგრამ ამგვარ შემთხვევებშიც კი, გამოძიებების ჩატარება არ არის შეუძლებელი.[253] ამის ერთ-ერთ მაგალითს წარმოადგენს კომპიუტერულ-ტექნიკური ექსპერტიზის საშუალება, რომელსაც ეწოდება კომპიუტერისა და ინტერნეტ პროტოკოლის მისამართის ვერიფიკატორი (CIPAV), გამოყენებული აშშ-ში იმ ეჭვმიტანილთა იდენტიფიკაციისათვის, რომლებიც იყენებდნენ ანონიმურ საკომუნიკაციო მომსახურებას.[254]

---

[246] *Chaski*, Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, 2005, ტომი 4, №1

[247] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, ტომი 1, №1, გვ.1 და შემდგომ

[248] შესაბამისი პროცესუალური ინსტრუმენტის შესახებ, იხილეთ: კომპიუტერული დანაშაულის შესახებ კონვენციის მუხლი 19, პარაგრაფი 3

[249] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, გვ.49

[250] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, გვ.57

[251] სხვადასხვა წყაროების შესახებ, რომლებიც შესაძლებელია გამოყენებული იქნეს ტრაფიკის მონაცემების ამოღებისათვის, იხილეთ: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, გვ. 163 და შემდგომ

[252] დამნაშავეთა ძებნაზე გავლენის თაობაზე, იხილეთ: Nicoll, Concealing and Revealing Identity on the Internet in Nicoll/Prins/Dellen, Digital Anonymity and the Law, Tensions and Dimensions, 2003, გვ. 99 და შემდგომ

[253] *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, 2002, ტომი 1, №3

[254] CIPAV–ის (კომპიუტერისა და ინტერნეტ პროტოკოლის მისამართის ვერიფიკატორი) შესახებ დამატებითი ინფორმაციისათვის იხილეთ: *Keizer*, What we know (now) about the FBI's CIPAV spyware, Computerworld, 31.07.2007: http://www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; Secret Search Warrant: FBI uses CIPAV fort he first time, Heise Security News, 19.07.2007: http://www.heise-online.co.uk/security/Secret-online-search-warrant-FBI-uses-CIPAV-for-the-first-time--/news/92950; *Poulsen*, FBI's Secret Spyware Tracks Down Teed Who Teen Makes Bomb Threats, Wired, 18.07.2007: http://www.wired.com/politics/law/news/2007/07/fbi_spyware; *Leyden*, FBI sought approval to use spyware against terror suspects, The Register, 08.02.2008: http://www.theregister.co.uk/2008/02/08/fbi_spyware_ploy_app/; *McCullagh*, FBI remotely installs spyware to trace bomb threat, ZDNet, 18.07.2007: http://news.zdnet.com/2100-1009_22-6197405.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf.

- ელექტრონული ფოსტის ანალიზი. ელექტრონული ფოსტის ანალიზი გახდა კომუნიკაციის ძალიან პოპულარული ფორმა და ამიტომ, იგი თამაშობს მნიშვნელოვან როლს კომპიუტერულ-ტექნიკური ექსპერტიზისათვის.[255] იმის გათვალისწინებით, რომ შედარებით ადვილია მუქარის ან არაკანონიერი შინაარსის მქონე თანდართული ფაილის შემცველი ელექტრონული ფოსტის გამგზავნის იდენტიფიცირება, დამნაშავეები ხშირად იყენებენ ელექტროული ფოსტის თავისუფალ მისამართებს, რომლებიც დარეგისტრირებულია ყალბი პერსონალური ინფორმაციის გამოყენებით. ამ შემთხვევებშიც კი, ელექტრონული ფოსტის პროვაიდერის თავსართი ინფორმაციის[256] და რეგისტრაციის ჟურნალის შესწავლა ზოგიერთ შემთხვევაში შესაძლებელს ხდის ეჭვმიტანილის იდენტიფიცირებას.

- ფინანსური ტრანზაქციების მიკვლევა. მთელი რიგი დანაშაულობები, მათ შორის ბავშვების პორნოგრაფიით ვაჭრობა, მოიცავს ფინანსურ ტრანზაქციებს. ფინანსურ ტრანზაქციებში ჩართული კომერციული სისტემებიდან და დაწესებულებებიდან მონაცემების გამოყენებით შესაძლებელია დამნაშავის იდენტიფიცირება.[257] ამის ერთ-ერთ მაგალითს წარმოადგენს გერმანიაში ჩატარებული გამოძიება. მან გამოავლინა დამნაშავეები, რომლებმაც მოახდინეს ბავშვების პორნოგრაფიის ჩამოტვირთვა კომერციული ვებ-გვერდიდან საკრედიტო ბარათების გამცემი კომპანიების მეშვეობით, რომლებმაც ანალიზი გაუკეთეს იმ კლიენტების ამონაწერებს, რომლებმა გამოიყენებს მათი საკრედიტო ბარათები ბავშვების პორნოგრაფიის შესაძენად კონკრეტული ვებ-გვერდიდან.[258] ამგვარი გამოძიებების ჩატარება რთულდება, თუკი დამნაშავეები იყენებენ გადახდის ანონიმურ მეთოდებს.[259]

- ტრაფიკის მონაცემების შეგროვება რეალურ დროში და შინაარსის მონაცემების მოპოვება. კომპიუტერულ-ტექნიკურმა გამოძიებებმა შეიძლება განახორციელონ რეალურ დროში გადაცემული მონაცემების მონიტორინგი. ეს კი შესაძლებლობას აძლევს გამომძიებლებს რეაგირება მოახდინონ პროცესებზე იმ დროს, როდესაც გამოძიების მიერ ეჭვმიტანილი პირი ჩადის ქმედებას.[260]

- მონიტორინგის განხორციელება საჯაროდ ხელმისაწვდომ სერვისებთან მიმართებაში. საჯაროდ ხელმისაწვდომი სერვისები შესაძლებელია გამოყენებული იქნეს საავტორო უფლებებით დაცული ან არაკანონიერი შინაარსის მქონე მასალების გაცვლისათვის. გამოძიების ფარგლებში ამგვარ სერვისებზე შესაძლებელია განხორციელდეს მონიტორინგი კომპიუტერულ-ტექნიკური ექსპერტების მხრიდან. ეს მოიცავს, მაგალითად, ჩატ ფორუმებზე კონტროლსაც.[261]

- დისტანციური კომპიუტერულ-ტექნიკური ექსპერტიზები. ამჟამად განიხილება დისტანციური კომპიუტერულ-ტექნიკური ექსპერ-

[255] *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, ტომი 2, №4

[256] დამატებითი ინფორმაციისათვის იხილეთ: *Crumbley/Heitger/Smith*, Forensic and Investigative Accounting, 2005, თავი 14.12; *Caloyannides*, Privacy Protection and Computer Forensics, 2004, გვ.149.

[257] Casey, Digital Evidence and Computer Crime, 2004, გვ. 19

[258] დამატებითი ინფორმაციისათვის იხილეთ: Spiegel Online, Fahnder ueberpruefen erstmals alle deutschen Kreditkarten,08.01.2007
http://www.spiegel.de/panorama/justiz/0,1518,457844,00.html.

[259] *Goodman*, Why the Police don't care about Computer Crime, Harvard Journal of Law & Technology, 1997, ტომი 10, №3, გვ. 472

[260] შესაბამისი პროცესუალური ინსტრუმენტის თაობაზე, იხილეთ: კომპიუტერული დანაშაულის შესახებ კონვენციის მუხლი 20 და მუხლი 21

[261] Casey, Digital Evidence and Computer Crime, 2004, გვ. 18

ტიზის საშუალებების საჭიროება.[262] ეს შესაძლებელს გახდის უშუალოდ წყაროდან დისტანციურად შეგროვებული იქნეს მტკიცებულებები[263] და ჩატარდეს დისტანციური მონიტორინგი[264], ისე რომ ეჭვმიტანილს არ ეცოდინება მის სისტემაზე განხორციელებული გამოძიებების თაობაზე.

ამგვარი გამოძიებების ჩატარება საჭიროებს სპეციფიკურ ტრენინგსა და კარგად განსაზღვრულ პროცედურებს, რომლებიც ეფუძნება ფართოდ მიღებულ სტანდარტებსა და მეთოდოლოგიებს.

5.2.3. როგორ ხორციელდება კომპიუტერულ-ტექნიკური ექსპერტიზები

არსებობს კომპიუტერულ-ტექნიკური ექსპერტიზის განხორციელების ორი გზა:

- მანუალური ოპერაციები: მიუხედავად იმისა, რომ არსებობს ტექნოლოგია გამოძიების პროცესების ავტომატიზირებისათვის, კომპიუტერულ-ტექნიკური ექსპერტიზა მეტწილად კვლავაც რჩება მანუალურ სამუშაოდ.[265] განსაკუთრებით იმ გამოძიებების დროს, რომლებიც მოიცავენ დიდი რაოდენობის მონაცემებს, ამგვარი მანუალური ოპერაციებს შესაძლებელია თან სდევდეს სირთულეები.[266]

- ანალიზის მეთოდები. შესაძლებელია ზოგიერთი პროცესის, განსაკუთრებით, ძირეული სიტყვების ძიების, წაშლილი ფაილების აღდგენის ან დაშიფრული მასალების განშიფრვის ავტომატიზირება კომპიუტერულ-ტექნიკური ანალიზის თანამედროვე მეთოდების გამოყენებით. [267]

გამოძიებათა უმრავლესობა მანუალურ ოპერაციებთან ერთად იყენებს კომპიუტერულ-ტექნიკური ექსპერტიზის პროგრამულ საშუალებებს, რომლებიც ახდენენ პროცესების ავტომატიზირებას.

---

[262] გერმანიის სამართალდამცავი ორგანოების გეგმების თაობაზე კომპიუტერული უზრუნველყოფის შექმნასთან დაკავშირებით, რომლებიც უზრუნველყოფს ეჭვმიტანილის კომპიუტერის დისტანციურ ხელმისაწვდომობას და ძებნის პროცედურების დისტანციურად ჩატარებას, იხილეთ: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News – available at: http://www.news.com/8301-10784_3-9769886-7.html.

[263] *Kenneally*, Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection, UCLA Journal of Law & Technology, 2005, ტომი 9, №2

[264] იხილეთ: *Vacca*, Computer Forensics, Computer Crime Scene Investigation, მე-2 გამოცემა, 2005, გვ.52

[265] *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, ტომი 4, №1

[266] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, გვ.62

[267] იხილეთ: *Vacca*, Computer Forensics, Computer Crime Scene Investigation, მე-2 გამოცემა, 2005, გვ.39 და შემდგომ; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, გვ. 85; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, გვ.41 და შემდგომ

6. კომპიუტერული დანაშაულის გამოძიება: საპროცესო სამართლით გათვალისწინებული ზომები

სესიის ბოლოს მის მონაწილეებმა უნდა იცოდნენ:

- პროცესუალური საშუალებები, რომლებიც ხელმისაწვდომია სამართალდამცავი ორგანოებისათვის ეფექტური გამოძიების ჩასატარებლად;
- მოსამართლეთა როლი ამ პროცესში.

რეკომენდირებულია, რომ მონაწილეებს შესაძლებლობა ჰქონდეთ ნახონ კომპიუტერული დანაშაულის შესახებ კონვენციის ტექსტი და მასთან დაკავშირებული ახსნა-განმარტებითი ანგარიში (იხ. www.coe.int/cybercrime, სადაც შესაძლებელია კონვენციის ნახვა სხვადასხვა ენაზე).

ასევე, მონაწილეებს ხელი უნდა მიუწვდებოდეთ მათი ეროვნული კანონმდებლობის ტექსთან. მთელი რიგი ქვეყნებისათვის, ამგვარი ინფორმაციის მოძიება შესაძლებელია შემდეგ ვებ-მისამართზე: www.coe.int/cybercrime.

როგორც ზემოთ აღინიშნა, კომპიუტერულ დანაშაულთა გამოძიებები დაკავშირებულია მთელ რიგ სპეციფიკურ სირთულეებთან, როგორიცაა მონაცემთა გაცვლის პროცესების მაღალი სიჩქარე ან ელექტრონულ მტკიცებულებათა ცვალებადობა. იმისათვის, რომ მოხდეს ამ გამოწვევებზე რეაგირება, სამართალდამცავ ორგანოებს სჭირდებათ პროცესუალური ინსტრუმენტები, რომლებიც საშუალებას მისცემს მათ მიიღო ზომები დამნაშავეთა გამოვლენისა და მტკიცებულებების ეფექტური შეგროვებისათვის.[268] გამოძიების ტრადიციული მეთოდები, როგორებიცაა ძებნა და ამოღება შეიძლება არ აღმოჩნდეს საკმარისი. ამიტომ, კომპიუტერული დანაშაულის შესახებ კონვენცია მოიცავს მთელ რიგ სპეციალურ საშუალებებს.

პრაქტიკული ინფორმაცია მოსამართლეებისათვის:

ზოგადად, კონვენცია არ განსაზღვრავს გარანტიებსა და პროცესუალურ მოთხოვნებს თითოეული ინსტრუმენტის გამოყენებისათვის. კონვენციის ავტორმა გადაწყვიტა, რომ არ შეეტანა სპეციფიკური რეგულაციები კონვენციის ტექსტში, არამედ დაევალდებულებინა წევრი ქვეყნები, რომ უზრუნველყოთ გარანტიების ეროვნული თუ საერთაშორისო სტანდარტების დაცვა.[269] მე-15 მუხლი ემყარება პრინციპს, რომ კონვენციაზე ხელმომწერმა ქვეყნებმა უნდა გამოიყენონ ის პირობები და გარანტიები, რომლებიც უკვე არსებობს მათი ქვეყნების კანონმდებლობაში. თუკი კანონში

[268] კომპიუტერული დანაშაულის წინააღმდეგ ბრძოლასთან მიმართებაში მომხმარებლის მიდგომების შესახებ შეგიძლიათ იხილოთ: *Görling*, The Myth Of User Education, 2006 - www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. ასევე იხილეთ კომენტარი, რომელიც გააკეთა ჟან პიერ შევენემენტმა, საფრანგეთის შინაგან საქმეთა მინისტრმა "დიდი რვიანის" კონფერენციაზე პარიზში 2000 წელს: "ჩვენ უფრო მეტი განათლება უნდა მივცეთ მომხმარებლებს. მათ ყველას უნდა ესმოდეთ, რისი გაკეთება შეუძლიათ და რისი არა ინტერნეტში და გაფრთხილებულები იყვნენ პოტენციური საფრთხეების შესახებ. ინტერნეტის გამოყენების არეალის გაზრდასთან ერთად, ჩვენ ბუნებრივია უნდა გავაფართოვოთ ჩვენი საქმიანობა ამ მიმართულებით."

[269] "არსებობს გარკვეული საერთო სტანდარტები ან მინიმალური გარანტიები, რომლებიც უნდა დაიცვას კონვენციის მხარეებმა. მათ შორის არის სტანდარტები და მინიმალური გარანტიები, რომლებიც წარმოიშობა იმ ვალდებულებების შესაბამისად, რომლებიც მხარემ თავის თავზე აიღო ადამიანთა უფლებების მოქმედი საერთაშორისო ინსტრუმენტების ფარგლებში." იხილეთ: ახსნა-განმარტებითი ანგარიში კომპიუტერული დანაშაულის შესახებ ევროპის საბჭოს კონვენციაზე, №145.

გათვალისწინებულია ცენტრალური სტანდარტები, რომლებიც გამოიყენება გამოძიების ყველა ინსტრუმენტისათვის, იგივე პრინციპები გამოყენებული უნდა იქნეს ინტერნეტთან დაკავშირებული ინსტრუმენტებითვისაც. ეს გულისხმობს, მაგრამ არა მხოლოდ, მოსამართლეების ჩართულობას გამოძიებაში (მოთხოვნა სასამართლო განკარგულებებთან დაკავშირებით).

ადგილობრივი კანონმდებლობის რომელი დებულებები ეხება კომპიუტერულ დანაშაულს და მტკიცებულებების შეგროვებას?

დაადგინეთ და განიხილეთ შემდეგი ღონისძიებების შესახებ ადგილობრივ კანონმდებლობის დებულებები. სასურველია პრაქტიკული მაგალითები.

6.1. კომპიუტერული მონაცემების სასწრაფო შენახვა

6.1.1. მოვლენა

კომპიუტერული დამნაშავის იდენტიფიცირება ხშირად მოითხოვს ტრაფიკის მონაცემების ანალიზს. [270] კერძოდ, IP მისამართი, რომელსაც იყენებს დამნაშავე დანაშაულის ჩადენის დროს წარმოადგენს მნიშვნელოვან ინფორმაციას, რომელიც შეიძლება სასარგებლო აღმოჩნდეს ინდივიდის მისაკვლევად. გამოძიებისათვის ერთ-ერთ ძირითად სირთულეს წარმოადგენს არის ფაქტი, რომ შესაბამისი ტრაფიკის მონაცემები ხშირად ავტომატურად იშლება დროის საკმაოდ მოკლე პერიოდში.[271] ზოგიერთ ქვეყანას აქვს მკაცრი კანონები, რომლებიც კრძალავს გარკვეული ტრაფიკის მონაცემების შენახვას პროცესის დასურლების შემდეგ. ამგვარი აკრძალვის ერთ-ერთი მაგალითია ევროკავშირის დირექტივის მე-6 მუხლი "პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციის შესახებ.[272]

6.1.2. შესაბამისი პროცესუალური ინსტრუმენტი

კომპიუტერული დანაშაულის შესახებ კონვენციის მე-16 მუხლი შესაძლებლობას აძლევს სამართალდამცავ ორგანოებს გასცენ მიწერილობა ტრაფიკის და, ასევე, შინაარსის მონაცემების შენახვის თაობაზე ("სწრაფი გაყინვა").

> მუხლი 16 - კომპიუტერული მონაცემების სასწრაფო შენახვა
>
> (1) თითოეულმა მხარემ უნდა მიიღოს ისეთი საკანონმდებლო და სხვა სახის ზომები, რომლებიც შეიძლება საჭირო გახდეს იმისათვის, რომ კომპეტენტურ ორგანოებს მიეცეთ საშუალება გასცენ მიწერილობა ან მსგავსი საშუალებით უზრუნველყონ განსაზღვრული კომპიუტერული მონაცემების სასწრაფო შენახვა, მათ შორის ტრაფიკის მონაცემებისა, რომლებიც ინახება კომპიუტერული სისტემის საშუალებით, განსაკუთრებით იმ შემთხვევებში, როდესაც არსებობს საფუძველი ვარაუდისათვის, რომ არის ამ კომპიუტერული მონაცემების დაკარგვის ან შეცვლის საფრთხე.

[270] "ამ წარსული კომუნიკაციების წყაროსა და დანიშნულების ადგილის განსაზღვრით შესაძლებელია მოხდეს დამნაშავეთა იდენტიფიცირება. იმისათვის, რომ მოხდეს ამ კომუნიკაციების კვალზე გაყოლა მათი წყაროსა და დანიშნულების ადგილის განსაზღვრის მიზნით, საჭიროა ტრაფიკის მონაცემები ამგვარი წარსული კომუნიკაციების შესახებ." იხილეთ: ახსნა-განმარტებითი ანგარიში №155 კომპიუტერული დანაშაულის შესახებ ევროსაბჭოს კონვენციაზე; IP-ზე (ინტერნეტ პროტოკოლი) დაფუძნებული გამოძიებების მეშვეობით ეჭვმიტანილთა იდენტიფიცირების თაობაზე, იხილეთ: *Gercke*, Preservation of User Data, DUD 2002, 577 და შემდგომ

[271] მიზეზი ამ ავტომატური წაშლის პროცესისა არის ის ფაქტი, რომ პროცესის დასრულების (მაგ., ელექტრონული წერილის გაგზავნის, ინტერნეტში შესვლის ან ფილმის ჩამოტვირთვის) შემდგომ ტრაფიკის მონაცემები, რომლებიც წარმოიშვა ამ პროცესის განმავლობაში და, რომლებიც ადასტურებენ პროცესის განხორციელების ფაქტს, აღარ არის საჭირო და, რომ მონაცემების შენახვა გაზრდის მომსახურების საფასურს. მომსახურების ღირებულების საკითხს განსაკუთრებით დიდი ყურადღება დაეთმო მონაცემების შეჩერების თაობაზე ევროკავშირის კანონის განხილვისას. მაგალითისათვის იხილეთ: E-communications service providers remain seriously concerned with the agreement reached by EU Justice Ministers to store records of every e-mail, phone call, fax and text message, Euroispa press release, 2005 – available at: http://www.ispai.ie/EUROISPADR.pdf; See as well: ABA International Guide to Combating Cybercrime, გვ.59.

[272] ევროპარლამენტისა და ევროსაბჭოს დირექტივა 2002/58/EC, დათარიღებული 2002 წლის 12 ივლისით, რომელიც შეეხება პერსონალური მონაცემების დამუშავებას და პირადი ცხოვრების ხელშეუხებლობის დაცვას ელექტრონული კომუნიკაციების სექტორში (დირექტივა პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ). დოკუმენტის ნახვა შეგიძლიათ შემდეგ ინტერნეტ მისამართზე: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

(2) იმ შემთხვევებში, როდესაც მხარე იყენებს ზემოაღნიშნულ 1 პუნქტს პირის მფლობელობაში ან კონტროლქვეშ არსებული კონკრეტული კომპიუტერული მონაცემების შენახვის თაობაზე ამ პირისათვის მიწერილობის გაცემით, მხარემ უნდა მიიღოს ისეთი საკანონმდებლო და სხვა სახის ზომები, რომლებიც შეიძლება საჭირო გახდეს იმისათვის, რომ დაავალდებულის ეს პირი შეინახოს და უზრუნველყოს ამგვარი კომპიუტერული მონაცემების ხელშეუხებლობა საჭირო დროის განმავლობაში, არაუმეტეს 90 დღისა, რათა საშუალება მიეცეთ კომპეტენტურ ორგანოებს ჩაატარონ გამოძიება აღნიშნულ ფაქტთან დაკავშირებით. მხარემ შეიძლება გაითვალისწინოს მიწერილობის მოქმედების ვადის გაგრძელების შესაძლებლობა.
(3) თითოეულმა მხარემ უნდა მიიღოს ისეთი საკანონმდებლო და სხვა სახის ზომები, რომლებიც შეიძლება საჭირო გახდეს იმისათვის, რომ დაავალდებულოს მონაცემთა შემნახველი ან სხვა პირი, რომელმაც უნდა შეინახოს კომპიუტერული მონაცემები, არ გაამჟღავნოს ამგვარი პროცედურების განხორციელების ფაქტი დროის იმ მონაკვეთის განმავლობაში, რომელიც გათვალისწინებულია ქვეყნის შიგნით მოქმედი კანონმდებლობით.
(4) უფლებამოსილებები და პროცედურები, რომლებზეც ლაპარაკია ამ მუხლში, დამოკიდებულია მე-14 და მე-15 მუხლებით განსაზღვრული დებულებების ამოქმედებაზე.

ამ ინსტრუმენტმა უნდა მისცეს საშუალება სამართალდამცავ ორგანოებს, რომ მოახდინონ მყისიერი რეაგირება დანაშაულის შესახებ ინფორმაციის მიღებისთანავე და თავიდან აიცილონ მონაცემთა წაშლის რისკი დროში გაწელილი პროცედურების გამო.[273] ამგვარი მიწერილობის მიღების შემდეგ, პროვაიდერი ვალდებულია შეინახოს ის მონაცემები, რომლებიც დამუშავებული იქნა გაწეული მომსახურების განმავლობაში.[274] მე-16 მუხლი არ შეიცავს ინტერნეტ სერვისის პროვაიდერის ვალდებულებას გადასცეს შესაბამისი მონაცემები ხელისუფლების ორგანოებს. გადაცემის ვალდებულება რეგულირდება კომპიუტერული დანაშაულის შესახებ კონვენციის მე-17 და მე-18 მუხლებით.

ამ კონტექსტში მნიშვნელოვანია ხაზი გაესვას იმ გარემოებას, რომ მე-16 მუხლი არ შეიცავს ვალდებულებას მონაცემთა შენახვის თაობაზე. მონაცემთა შენახვის ვალდებულება აიძულებს ინტერნეტ სერვისის პროვაიდერს შეინახოს ყველა ტრაფიკის მონაცემი გარკვეული დროის განმავლობაში.[275] ეს შესაძლებლობას მისცემს უფლებამოსილ სამსახურებს მიიღონ ინფორმაცია, რომელიც საჭიროა დამნაშავის იდენტიფიცირებისათვის დანაშაულის ჩადენიდან ერთი თვის შემდეგაც

[273] თუმცა, რეკომენდირებულია, რომ აშშ განიხილოს იმ უფლებამოსილებისა და პროცედურების დადგენის საკითხი, რომელთა საფუძველზეც უზრუნველყოფილი იქნება ბრძანების მიმღების მიერ მონაცემების შენახვა, ვინაიდან ამ პირის სწრაფმა ქმედებამ გარკვეულ შემთხვევებში შეიძლება განაპირობოს შენახვის ზომების დაჩქარებული მიღება. კომპიუტერული დანაშაულის შესახებ კონვენციის ახსნა-განმარტებითი ანგარიში №160.

[274] "შენახვა" გულისხმობს, რომ მონაცემები, რომლებიც უკვე არსებობს შენახული ფორმით დაცული იყოს ყველფრისაგან, რამაც შეიძლება გამოიწვიოს მისი არსებული ხარისხის ან მდგომარეობის შეცვლა ან გაუარესება. კომპიუტერული დანაშაულის შესახებ კონვენციის ახსნა-განმარტებითი ანგარიში №159.

[275] ევროკავშირში მონაცემთა შესახვის შესახებ დირექტივასთან დაკავშირებით, იხილეთ: *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, Chicago Journal of International Law, 2007, ტომი 8, №1, http://eprints.law.duke.edu/archive/00001602/01/8_Chi._J.__Int'l_L._233_(2007).pdf; *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, გვ. 365 და შემდგომ.

კი.[276] ვალდებულება მონაცემთა შენახვის თაობაზე ცოტა ხნის წინ მიღებული იქნა ევროპარლამენტის მიერ[277] და ამჟამად განიხილება აშშ-ში.[278]

პრაქტიკული ინფორმაცია მოსამართლეებისათვის:

მონაცემთა დროებით შეკავებასა და მონაცემთა შენახვას შორის ყველაზე ფუნდამენტური განსხვავება მდგომარეობს იმაში, რომ მონაცემთა შენახვას გააჩნია შეზღუდული შესაძლებლობები რეტროაქტიულ გამოძიებებთან მიმართებაში, ვინაიდან მიწერილობა შენახვის თაობაზე აიძულებს პროვაიდერს შეინახოს მხოლოდ მოთხოვნის დროისათვის ხელმისაწვდომი მონაცემები. მოთხოვნამდე წაშლილი მონაცემების ნახვა შეუძლებელია. იმ ეტაპზე, როდესაც ერთვებიან მოსამართლეები, ამ ინსტრუმენტის გამოყენებას ზოგადად არ ექნება აზრი იმ მტკიცებულებების შესაგროვებლად, რომელთა შეგროვებაც არ მოხდა გამოძიების პირველ ეტაპებზე. როგორც უკვე აღინიშნა, განხორციელების პროცესში სახელმწიფოებმა უნდა დაამატონ გარანტიები და პროცესუალური მოთხოვნები. იმის გათვალისწინებით, რომ მე-16 მუხლმა უნდა მისცეს შესაძლებლობა სამართალდამცავ ორგანოებს მოახდინონ დაუყოვნებლივი რეაგირება და ხელი შეუშალონ ინფორმაციის წაშლას, მოთხოვნა (დროში გაწელილი) სასამართლო განკარგულების გაცემის თაობაზე კონტრპროდუქტიული იქნება.

[276] იხილეთ: მონაცემთა შეჩერების შესახებ ევროკავშირის დირექტივის წინასიტყვაობა 11: "სისხლის სამართლის დანაშაულებათა გამოძიების, გამოვლენისა და სასამართლო წესით დევნისათვის ტრაფიკისა და ადგილობრივი მონაცემების მნიშვნელობის გათვალისწინებით, როგორც ეს აჩვენა კვლევამ და რამოდენიმე წევრი ქვეყნის პრაქტიკულმა გამოცდილებამ, ევროპულ დონეზე საჭიროა იმის უზრუნველყოფა, რომ მონაცემები, რომლებიც წარმოიშვა და დამუშავდა საჯაროდ ხელმისაწვდომი ელექტრონულ-საკომუნიკაციო მომსახურების ან საზოგადოებრივი საკომუნიკაციო ქსელის პროვაიდერების მიერ მიწოდებული საკომუნიკაციო მომსახურების პროცესში, შეჩერებულია გარკვეული პერიოდის განმავლობაში წინამდებარე დირექტივით განსაზღვრული პირობების შესაბამისად."

[277] ევროპარლამენტისა და ევროსაბჭოს დირექტივა 2002/58/EC, დათარიღებული 2002 წლის 12 ივლისით, რომელიც შეეხება პერსონალური მონაცემების დამუშავებას და პირადი ცხოვრების ხელშეუხებლობის დაცვას ელექტრონული კომუნიკაციების სექტორში (დირექტივა პირადი ცხოვრების ხელშეუხებლობისა და ელექტრონული კომუნიკაციების შესახებ). დოკუმენტის ნახვა შეგიძლიათ შემდეგ ინტერნეტ მისამართზე: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

[278] მაგალითისათვის იხილეთ: Draft Bill to amend title 18, United States Code, to protect youth from exploitation by adults using the Internet, and for other purposes - Internet StoppingAdults Facilitating the Exploitation of Today's Youth Act (SAFETY) of 2007: http://www.govtrack.us/congress/bill.xpd?bill=h110-837. აშშ-ში ამჟამად არსებული სიტუაციის თაობაზე, იხილეთ: ABA International Guide to Combating Cybercrime, გვ. 59

6.2. მიწერილობა ინფორმაციის წარმოდგენის თაობაზე

6.2.1. მოვლენა

როგორც ეს აღნიშნულია ზემოთ, მე-16 მუხლი ავალდებულებს პროვაიდერს შეინახოს მხოლოდ ის მონაცემები, რომლებიც დამუშავებული იქნა პროვაიდერის მიერ და არ არის წაშლილი პროვაიდერის მიერ მიწერილობის მიღების მომენტისათვის.[279] დებულება არ ავალდებულებს პროვაიდერს გადასცეს შესაბამისი მონაცემები ხელისუფლების ორგანოებს.

6.2.2. შესაბამისი პროცესუალური ინსტრუმენტი

გადაცემის ვალდებულებას არეგულირებს კომპიუტერული დანაშაულის შესახებ კონვენციის მე-18 მუხლი.

მუხლი 18 – მიწერილობა ინფორმაციის წარდგენის თაობაზე

(1) თითოეულმა მხარემ უნდა მიიღოს ისეთი საკანონმდებლო და სხვა სახის ზომები, რომლებიც შეიძლება საჭირო გახდეს იმისათვის, რომ უფლებამოსილება მიანიჭოს კომპეტენტურ ორგანოებს წარუდგინონ მიწერილობა:

ა) მის ტერიტორიაზე მყოფ პირს, რათა მან მოახდინოს მიერ მფლობელობაში ან კონტროლქვეშ არსებული კონკრეტული კომპიუტერული იმ მონაცემების წარდგენა, რომლებიც ინახება კომპიუტერულ სისტემაში ან კომპიუტერული მონაცემების მატარებელში; და
ბ) სერვისის პროვაიდერს, რომელიც სთავაზობს მომსახურებას მხარის ტერიტორიაზე, წარადგინოს ის ინფორმაცია აბონენტის თაობაზე, რომელიც დაკავშირებულია ამგვარ მომსახურებასთან და არის მომსახურების უზრუნველმყოფის მფლობელობაში ან კონტროლქვეშ;

(2) უფლებამოსილებები და პროცედურები, რომლებზეც ლაპარაკია ამ მუხლში, დამოკიდებულია მე-14 და მე-15 მუხლებით განსაზღვრული დებულებების ამოქმედებაზე.
(3) წინამდებარე მუხლის მიზნებიდან გამომდინარე, ტერმინი "ინფორმაცია აბონენტის თაობაზე" ნიშნავს ნებისმიერ ინფორმაციას, რომელსაც ფლობს სერვისის პროვაიდერი კომპიუტერული მონაცემების სახით ან ნებისმიერი სხვა ფორმით მისი მომსახურების აბონენტის შესახებ, რომელიც განსხვავდება ტრაფიკის ან შინაარსის მონაცემებისაგან და რომლის მეშვეობითაც შესაძლებელია დადგინდეს:
(ა) გამოყენებული საკომუნიკაციო მომსახურების ტიპი, მასთან დაკავშირებული ტექნიკური დებულებები და სერვისის პერიოდი;
ბ) აბონენტის ვინაობა, მისი საფოსტო ან გეოგრაფიული მისამართი, ტელეფონის ან სხვა ნომერი, ინფორმაცია წარდგენილი ანგარიშებისა და მათი გადახდების შესახებ, რომელიც ხელმისაწვდომია მომსახურების თაობაზე შეთანხმების ან ხელშეკრულების საფუძველზე.
გ) ნებისმიერი სხვა ინფორმაცია საკომუნიკაციო მოწყობილობის დამონტაჟების ადგილის თაობაზე, რომელიც ხელმისაწვდომია მომსახურების თაობაზე შეთანხმების ან ხელშეკრულების საფუძველზე.

[279] "შენახვა გულისხმობს, რომ მონაცემები, რომლებიც უკვე არსებობს შენახული ფორმით დაცულია ყველაფრისაგან, რამაც შეიძლება გამოიწვიოს მისი არსებული ხარისხის ან მდგომარეობის ცვლილება ან გაუარესება". კომპიუტერული დანაშაულის შესახებ კონვენციის ახსნა-განმარტებითი ანგარიში, №159.

კომპიუტერული დანაშაულის შესახებ კონვენციის მე-18 მუხლი არ გამოიყენება მხოლოდ მონაცემების დაცვის შესახებ მიწერილობის გაცემის შემდეგ. დებულება არის ზოგადი ინსტრუმენტი, რომელიც შეიძლება გამოყენებული იქნეს სამართალდამცავი ორგანოების მიერ. თუკი ინტერნეტ სერვისის პროვაიდერები ნებაყოფლობით გადასცემენ მოთხოვნილ მონაცემებს, სამართალდამცავი ორგანოები არ შემოიფარგლებიან მხოლოდ მოწყობილობების კონფისკაციით და სანაცვლოდ გამოიყენონ ნაკლებად ინტენსიური მიწერილობა ინფორმაციის წარმოდგენის თაობაზე.

თუმცა, მე-18 მუხლის გამოყენება არ შემოიფარგლება მხოლოდ მონაცემებით, რომლებიც შენახულია მე-16 მუხლის საფუძველზე. მე-18 მუხლი ზოგადად შეიძლება გამოყენებული იქნეს გამოძიებასთან დაკავშირებულ ნებისმიერ კომპიუტერულ მონაცემებთან მიმართებაში. აქედან გამომდინარე, შესაძლებლობა, რომ მოხდეს მონაცემების გამჟღავნება წარმოადგენს არსებულ შესაძლებლობების დამატებას განხორციელდეს ძიებისა და კონფისკაციის პროცედურები, რომლებიც არ მოითხოვს თანამშრომლობას იმ პირის ან ინსტიტუტეს მხრიდან, რომელიც ფლობს მონაცემებს.

პრაქტიკული ინფორმაცია მოსამართლეებისათვის:

მონაცემების დაცვის ვალდებულების მათი გამჟღავნების ვალდებულებისაგან გამოცალკევების უპირატესობა მდგომარეობს იმაში, რომ შესაძლებელია მათი გამოყენებისათვის განსხვავებული პირობების მითხოვნა. როგორც ეს უკვე აღინიშნა, რეკომენდირებულია, რომ არ იქნეს მოთხოვნილი სასამართლო განკარგულება მე-16 მუხლის გამოყენებისათვის. ეს შესაძლებლობას აძლევს კომპეტენტურ ორგანოებს იმოქმედონ უფრო სწრაფად. ეჭვმიტანილის უფლებების დაცვის აუცილებლობა შესაძლებელია უზრუნველყოფილი იქნეს მონაცემთა გამჟღავნებისათვის სასამართლო განკარგულების მოთხოვნის გზით.[280]

6.3. ტრაფიკის მონაცემების ნაწილობრივი გამჟღავნება

[280] კომპიუტერული დანაშაულის შესახებ კონვენციის ავტორები შეეცადნენ სხვადასხვა გზებით გადაეჭრათ ის პრობლემები, რომლებიც დაკავშირებულია, ერთის მხრივ, სამართალდამცავი ორგანოების მიერ დაუყოვნებელი რეაგირების საჭიროებაზე და, მეორე მხრივ, გარანტიების უზრუნველყოფის მნიშვნელობაზე. პრობლემების გადაჭრის სხვაგვარი გზა დაკავშირებულია ინფორმაციის წარმოდგენის თაობაზე ბრძანების არსებობასთან (მუხლი 18). ავტორების შეთავაზებით, სამართალდამცავი ორგანოებისათვის მონაცემების გადაცემასთან დაკავშირებული მოთხოვნები შეიძლება დარეგულირდეს მონაცემთა კატეგორიების შესაბამისად. იხილეთ კომპიუტერული დანაშაულის შესახებ კონვენციის ახსნა-განმარტებითი ანგარიში №174: "მუხლის მე-2 პუნქტში აღნიშნულმა პირობებმა და გარანტიებმა, თითოეული მხარის საშინაო კანონმდებლობიდან გამომდინარე, შეიძლება გამორიცხოს პრივილეგირებული მონაცემები ან ინფორმაცია. მხარეს შესაძლებელია უნდოდეს სხვა პირობების, სხვა კომპეტენტური ორგანოების და სხვა გარანტიების განსაზღვრა კონკრეტული ტიპის კომპიუტერული მონაცემების ან აბონენტის შესახებ იმ ინფორმაციის წარდგენასთან დაკავშირებით, რომელიც ხელთ აქვთ პირთა ან სერვისის პროვაიდერთა გარკვეულ კატეგორიას. მაგალითად, გარკვეული ტიპის მონაცემებთან დაკავშირებით, როგორიცაა საჯაროდ ხელმისაწვდომი ინფორმაცია აბონენტის შესახებ, მხარემ შეიძლება ნება დართოს სამართალდამცავი ორგანოს წარმომადგენლებს გასცენ იმგვარი ბრძანება, რომლის მაგივრადაც სხვა შემთხვევებში საჭირო იქნებოდა სასამართლო განკარგულება. მეორე მხრივ, ზოგიერთ შემთხვევაში მხარემ შეიძლება მოითხოვოს, ან ადამიანთა უფლებების გარანტიებით მიენიჭოს უფლება მოითხოვოს, რომ სასამართლოს განკარგულება ინფორმაციის წარმოდგენის თაობაზე გაცემული იყოს მხოლოდ სასამართლო ორგანოების მიერ, რათა მათ შესაძლებლობა ჰქონდეთ მოიპოვონ გარკვეული ტიპის მონაცემები. მხარეებმა შესაძლებელია მოისურვონ წარუდგინონ ამგვარი მონაცემები სამართალდამცავ ორგანოებს იმ შემთხვევებში, როდესაც ბრძანება ინფორმაციის წარმოდგენის თაობაზე გაცემულია სასამართლო ორგანოების მიერ. ასევე, პროპორციულობის პრინციპი ბევრ ქვეყანაში უზრუნველყოფს გარკვეულ მოქნილობას საჭირო ზომების გამოყენებასთან მიმართებაში, რათა გამოირიცხოს მისი გამოყენება უმნიშვნელო საქმეებისათვის."

6.3.1. მოვლენა

როგორც უკვე აღინიშნა, კონვენცია მკაფიოდ განასხვავებს მოთხოვნის საფუძველზე მონაცემთა შენახვის ვალდებულებას კომპეტენტური ორგანოებისათვის მათი გამჟღავნების ვალდებულებისაგან.[281]

6.3.2. შესაბამისი პროცესუალური ინსტრუმენტი

მე-18 მუხლში განსაზღვრულია ვალდებულება, რომელიც დაკავშირებულია ტრაფიკის მონაცემთა შენახვასთან იმ შემთხვევებში, როდესაც პროცესში ჩართულია რამოდენიმე სერვისის პროვაიდერი, საჭირო ინფორმაციის გაცემის იმ დამატებით ვალდებულებასთან ერთად, რომელიც საშუალებას აძლევს სამართალდამცავ ორგანოებს მოაკვლიონ კვალს.

> მუხლი 17 – ტრაფიკის მონაცემების დაჩქარებული შენახვა და ნაწილობრივი გამჟღავნება
>
> (1) თითოეულმა მხარემ შესანახ ტრაფიკის მონაცემებთან მიმართებაში უნდა მიიღოს ისეთი საკანონმდებლო და სხვა სახის ზომები, რომლებიც შეიძლება საჭირო გახდეს იმისათვის, რომ
>
> ა) უზრუნველყოს, რომ ტრაფიკის მონაცემების ამგვარი დაუყოვნებლივი შენახვა შესაძლებელი იქნება იმისდა მიუხედავად, თუ რამდენი მომსახურების მომწოდებელი იყო ჩართული მოცემული ინფორმაციის გადაცემის პროცესში – ერთი თუ რამდენიმე; და
> ბ) უზრუნველყოს მხარის კომპეტენტური ორგანოსათვის ან პირისათვის, რომელიც დანიშნულია ამგვარი კომპეტენტური ორგანოს მიერ, ტრაფიკის მონაცემების სწრაფი მიწოდება იმ მოცულობით, რომელიც საკმარისი იქნება მხარისათვის სერვისის პროვაიდერებისა და იმ მარშრუტის იდენტიფიცირებისათვის, რომელზეც განხორციელდა ინფორმაციის გადაცემა.
>
> (2) უფლებამოსილებები და პროცედურები, რომლებზეც ლაპარაკია ამ მუხლში, დამოკიდებულია მე-14 და მე-15 მუხლებით განსაზღვრული დებულებების ამოქმედებაზე.

ამგვარი ნაწილობრივი გამჟღავნების გარეშე, სამართალდამცავ ორგანოებს ზოგიერთ შემთხვევაში არ ექნებათ საშუალება მიაკვლიონ დამნაშავეს და შეინახონ უფრო შესაფერისი მონაცემები, როდესაც საქმე გვაქვს ერთზე მეტ პროვაიდერთან.[282]

> პრაქტიკული ინფორმაცია მოსამართლეებისათვის:

[281] *Gercke*, The Convention on Cybercrime, MMR 2004, 802.

[282] "თუმცა, ხშირად არც ერთი სერვისის პროვაიდერი არ ფლობს ტრაფიკის მონაცემების იმ რაოდენობას, რომ განსაზღვროს კომუნიკაციის რეალური წყარო ან დანიშნულების ადგილი. თითოეული მათგანი ფლობს ინფორმაციის მხოლოდ ერთ ნაწილს. ინფორმაციის ყველა ეს ნაწილები უნდა იქნეს გამოკვლეული, რათა მოხდეს წყაროს ან დანიშნულების ადგილის იდენტიფიცირება". იხილეთ: კომპიუტერული დანაშაულის შესახებ კონვენციის ახსნა-განმარტებითი ანგარიში, №167.

გადაცემის დროს ზოგადად ინფორმაცია გადის სხვადასხვა პროვაიდერებს, როგორებიცაა ინტერნეტ მომსახურების მომწოდებელი[283] და მარშრუტიზატორები.[284] ამიტომ, სამართალდამცავ ორგანოებს რეგულარულად უნდა მიუწვდებოდეთ ხელი იმ ინფორმაციაზე, რომელიც საშუალებას აძლევს მათ გაჰყვნენ ეჭვმიტანილის კვალს. თუკი ნაწილობრივი გამჟღავნებისათვის საჭიროა სასამართლოს განკარგულება, სასამართლომ უნდა გაითვალისწინოს, რომ ხშირად დროის ძალიან მცირე მონაკვეთია გამოყოფილი ამგვარი გამოძიებებისათვის. ამიტომ, დროში გაჭიმულმა პროცედურებმა შეიძლება ხელი შეუშალოს ამგვარ გამოძიებებს.

[283] სერვისის პროვაიდერი არის ის პროვაიდერი, რომელიც შესაძლებლობას აძლევს მომხმარებლებს დაუკავშირდნენ ინტერნეტს სატელეფონო ხაზის ან მუდმივი ინტერნეტ კავშირის საშუალებით. დეტალური ინფორმაციისათვის იხილეთ: *Callanan/Gercke*, Study on the Co-operation between service providers and law enforcement against cybercrime, 2008.

[284] მარშრუტიზატორები შექმნილია ინფორმაციის გადამისამართებლად გამგზავნისაგან მიმღების მიმართულებით. დეტალური ინფორმაციისათვის იხილეთ: Khosravi/Anderson, Requirements for Separation of IP Control and Forwarding, 2003: ftp://ftp.rfc-editor.org/in-notes/rfc3654.txt.

6.4. აბონენტის შესახებ ინფორმაციის წარდგენა

6.4.1. მოვლენა

კომპიუტერულ დანაშაულთა უმრავლესობის მთავარი მიზანი არის დანაშაულის ჩადენაში ეჭვმიტანილ პირთა იდენტიფიკაცია. ამიტომ, ეჭვმიტანილის ინდივიდუალიზაცია წარმოადგენს პროცესუალური ინსტრუმენტების მთავარ ელემენტს. იდენტიფიცირება შესაძლებელია მოხდეს აბონენტის შესახებ ინფორმაციის მეშვეობით. ინტერნეტ სერვისების გამოყენება, როგორებიცაა ინტერნეტის მისაწვდომობა ან სერვერის შესანახი ადგილის დაქირავება, მოითხოვს რეგისტრაციას. აბონენტის შესახებ ინფორმაციამ, რომლის წარდგენაც ხდება რეგისტრაციის პროცესის დროს, შესაძლებელია ხელი შეუწყოს ინდივიდუალიზაციის პროცესს, განსაკუთრებით იმ შემთხვევაში, თუკი სერვისის პროვაიდერის მიერ ხდება აბონენტის შესახებ წარდგენილი ინფორმაციის შეფასება.

6.4.2. შესაბამისი პროცესუალური ინსტრუმენტი

კომპიუტერული მონაცემების წარდგენის ვალდებულების გარდა, კომპიუტერული დანაშაულის შესახებ კონვენციის მე-18 მუხლი უფლებას აძლევს სამართალდამცავ ორგანოებს გასცენ მიწერილობა აბონენტის შესახებ ინფორმაციის წარდგენის მოთხოვნით.

მუხლი 18 – მიწერილობა ინფორმაციის წარდგენის თაობაზე

(1) თითოეულმა მხარემ უნდა მიიღოს ისეთი საკანონმდებლო და სხვა სახის ზომები, რომლებიც შეიძლება საჭირო გახდეს იმისათვის, რომ უფლებამოსილება მიანიჭოს კომპეტენტურ ორგანოებს წარუდგინონ მიწერილობა:

ა) მის ტერიტორიაზე მყოფ პირს, რათა მან მოახდინოს მიერ მფლობელობაში ან კონტროლქვეშ არსებული კონკრეტული კომპიუტერული იმ მონაცემების წარდგენა, რომლებიც ინახება კომპიუტერულ სისტემაში ან კომპიუტერული მონაცემების მატარებელში; და
ბ) სერვისის პროვაიდერს, რომელიც სთავაზობს მომსახურებას მხარის ტერიტორიაზე, წარადგინოს ის ინფორმაცია აბონენტის თაობაზე, რომელიც დაკავშირებულია ამგვარ მომსახურებასთან და არის მომსახურების უზრუნველმყოფის მფლობელობაში ან კონტროლქვეშ;

(2) უფლებამოსილებები და პროცედურები, რომლებზეც ლაპარაკია ამ მუხლში, დამოკიდებულია მე-14 და მე-15 მუხლებით განსაზღვრული დებულებების ამოქმედებაზე.
(3) წინამდებარე მუხლის მიზნებიდან გამომდინარე, ტერმინი "ინფორმაცია აბონენტის თაობაზე" ნიშნავს ნებისმიერ ინფორმაციას, რომელსაც ფლობს სერვისის პროვაიდერი კომპიუტერული მონაცემების სახით ან ნებისმიერი სხვა ფორმით მისი მომსახურების აბონენტის შესახებ, რომელიც განსხვავდება ტრაფიკის ან შინაარსის მონაცემებისაგან და რომლის მეშვეობითაც შესაძლებელია დადგინდეს:
(ა) გამოყენებული საკომუნიკაციო მომსახურების ტიპი, მასთან დაკავშირებული ტექნიკური დებულებები და სერვისის პერიოდი;
ბ) აბონენტის ვინაობა, მისი საფოსტო ან გეოგრაფიული მისამართი, ტელეფონის ან სხვა ნომერი, ინფორმაცია წარდგენილი ანგარიშებისა და

მათი გადახდების შესახებ, რომელიც ხელმისაწვდომია მომსახურების თაობაზე შეთანხმების ან ხელშეკრულების საფუძველზე.
გ) ნებისმიერი სხვა ინფორმაცია საკომუნიკაციო მოწყობილობის დამონტაჟების ადგილის თაობაზე, რომელიც ხელმისაწვდომია მომსახურების თაობაზე შეთანხმების ან ხელშეკრულების საფუძველზე.

გამოძიების ამ ინსტრუმენტს დიდი მნიშვნელობა აქვს IP-ზე (ინტერნეტ პროტოკოლი) დაფუძნებული გამოძიებების დროს. თუკი სამართალდამცავი ორგანოები შეძლებენ იმ IP მისამართის იდენტიფიცირებას, რომელიც გამოყენებული იქნა დამნაშავის მიერ დანაშაულის ჩადენის დროს, ისინი ასევე მოახდენენ იმ პირის[285] იდენტიფიცირებაც, რომელმაც გამოიყენა ეს IP მისამართი დანაშაულის ჩადენის დროს. კომპიუტერული დანაშაულის შესახებ კონვენციის მე-18 მუხლის 1(ბ) ქვე-პუნქტის საფუძველზე, პროვაიდერი ვალდებულია წარადგინოს ის ინფორმაცია აბონენტის თაობაზე, რომელიც ჩამოთვლილია კომპიუტერული დანაშაულის შესახებ კონვენციის მე-18 მუხლის მე-3 ქვე-პუნქტში.

პრაქტიკული ინფორმაცია მოსამართლეებისათვის:

თუკი დანაშაულის ჩადენის დროს გამოყენებული იყო კონკრეტული მომხმარებლის ინტერნეტ წყარო ან ელექტრონული ფოსტის მისამართი, აბონენტის შესახებ არსებული ინფორმაცია შესაძლებელია გამოყენებული იქნეს ეჭვმიტანილის იდენტიფიცირებისათვის. მაგრამ უნდა აღინიშნოს, რომ ინფორმაციას აბონენტის შესახებ გარანტირებულად ვერ მივყავართ დამნაშავესთან. მაგალითად, ზოგიერთი სერვისის პროვაიდერი არ ახდენს რეგისტრაციის პროცესში მომხმარებლის მიერ წარდგენილი აბონენტის შესახებ ინფორმაციის შეფასებას. თუკი ეჭვმიტანილი დარეგისტრირდება სხვა პირის მონაცემების გამოყენების გზით, ინფორმაცია აბონენტის თაობაზე არ იქნება საკმარისი დამნაშავის იდენტიფიცირებისათვის. იგივე სირთულეებთან გვექნება შეხება, თუკი დამნაშავემ გამოიყენა ის პერსონალური მონაცემები, რომლებიც მან მანამდე უკანონოდ მოიპოვა ("პერსონალური მონაცემების მოპარვა").[286]

[285] IP (ინტერნეტ პროტოკოლი) მისამართი ყოველთვის დაუყოვნებლივ არ უზრუნველყოფს დამნაშავის იდენტიფიცირებას. თუკი სამართალდამცავმა ორგანოებმა იციან IP-მისამართი, რომელიც გამოიყენა დამნაშავემ დანაშაულის ჩადენისათვის, ეს ინფორმაცია მათ მხოლოდ იმის საშუალებას აძლევს, რომ მოახდინონ კავშირის იდენტიფიცირება, რომელიც გამოყენებული იქნა ინტერნეტთან დასაკავშირებლად. თუკი ადამიანთა ჯგუფს ჰქონდა ამ კავშირის გამოყენების საშუალება (მაგ. ინტერნეტ კაფე), დამნაშავის იდენტიფიცირებისათვის საჭიროა დამატებითი გამოძიება.

[286] *Gercke,* Internet-related Identity Theft, 2007 - http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_co-operation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

6.5. ინფორმაციის მოძიება

6.5.1. მოვლენა

ძებნა და კონფისკაცია წარმოადგენს ერთ-ერთ ყველზე მნიშვნელოვან ინსტრუმენტებს კომპიუტერული დანაშაულის გამოძიებაში.[287] მატერიალური ობიექტების ძებნა და კონფისკაცია წარმოადგენს ტრადიციულ საგამომძიებო ინსტრუმენტებს სისხლის სამართლის საპროცესო კოდექსების უმრავლესობაში. [288] მიზეზი, რის გამოც კომპიუტერული დანაშაულის შესახებ კონვენციის ავტორმა მაინც შეიტანა მასში დებულება ძებნისა და კონფისკაციის შესახებ არის ის, რომ ეროვნულ კანონებში ხშირად არ არის შეტანილი მონაცემთა მოძიებისა და კონფისკაციის პროცედურები.[289] ამ დებულებების საფუძველზე გამომძიებლებს შესაძლებლობა ექნებათ მოახდინონ მთლიანი სერვერის კონფისკაცია და არ გამორჩეთ შესაბამისი მონაცემები მათი კოპირების პროცესში.[290]

6.5.2. შესაბამისი პროცესუალური ინსტრუმენტი

მუხლი 19 – შენახული კომპიუტერული მონაცემების ძებნა და კონფისკაცია

(1) თითოეულმა მხარემ უნდა მიიღოს ისეთი საკანონმდებლო და სხვა სახის ზომები, რომლებიც შეიძლება საჭირო გახდეს იმისათვის, რომ უფლებამოსილება მიანიჭოს კომპეტენტურ ორგანოებს მოიძიოს ან სხვაგვარად მოიპოვოს:
ა. კომპიუტერული სისტემა ან მისი ნაწილი და მასში შენახული კომპიუტერული მონაცემები; და
ბ. მის ტერიტორიაზე არსებული კომპიუტერული მონაცემების მატარებელი, რომელშიც შესაძლებელია ინახებოდეს კომპიუტერული მონაცემები.
(2) თითოეულმა მხარემ უნდა მიიღოს ისეთი საკანონმდებლო და სხვა სახის ზომები, რომლებიც შეიძლება საჭირო გახდეს იმის უზრუნველყოფისათვის, რომ იმ შემთხვევებში, როდესაც მისი სამართალდამცავი ორგანოები მოიძიებენ ან სხვაგვარად მოიპოვებენ განსაზღვრულ კომპიუტერულ სისტემას ან მის ცალკეულ ნაწილს 1(ა) პუნქტის შესაბამისად, და გააჩნიათ საფუძველი ივარაუდონ, რომ ძებნადი მონაცემები ინახება მხარის ტერიტორიზე არსებულ სხვა კომპიუტერულ სისტემაში ან მის რომელიმე ნაწილში, და რომ ამგვარი მონაცემები კანონიერად ხელმისაწვდომია თავდაპირველი სისტემიდან ან სისტემისათვის, სამართალდამცავ ორგანოებს უნდა შეეძლოთ სწრაფად

[287] ძებნის პროცედურების ელემენტების შესახებ დეტალური ინფორმაცია მოცემულია ამერიკელ იურისტთა ასოციაციის კომპიუტერული დანაშაულის წინააღმდეგ საერთაშორისო ბრძოლის სახელმძღვანელოში, გვ.123 და შემდგომ. კომპიუტერთან დაკავშირებული ძებნისა და კონფისკაციის შესახებ დამატებითი ინფორმაციისათვის იხილეთ: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, ტომი 8, გვ.75 და შემდგომ; *Rhoden*, Challenging searches and seizures of computers at home or in the office: From a reasonable expectation of privacy to fruit of the poisonous tree and beyond, American Journal of Criminal Law, 2002, გვ. 107 და შემდგომ.

[288] იხილეთ კომპიუტერული დანაშაულის შესახებ კონვენციის ახსნა-განმართებითი ანგარიში №184

[289] "თუმცა, მთელ რიგ იურისდიქციებში, თავისთავად აღებული შენახული კომპიუტერული მონაცემები არ არის მიჩნეული მატერიალურ ობიექტად და, შესაბამისად, არ შეიძლება იქნეს დაცული სისხლის სამართლის გამოძიებათა და სამართალწარმოებათა სახელით, ისევე, როგორც ეს ხდება მატერიალური ობიექტების შემთხვევაში, მონაცემთა მატარებლის დაცვის გარდა, რომლეზეც იგი ინახება. ამ კონვენციის მე-19 მუხლის მიზანია განისაზღვროს შესაბამისი უფლებამოსილება შენახულ მონაცემებთან მიმართებაში." კომპიუტერული დანაშაულის შესახებ კონვენციის ახსნა-განმარტებითი ანგარიში, №184.

[290] ამან შეიძლება გამოიწვიოს სირთულეები იმ შემთხვევებში, როდესაც შესაბამისი ინფორმაცია ინახება სერვერზე ასობით სხვა მომხმარებელთა მონაცემებთან ერთად და იგი არ იქნება ხელმისაწვდომი მაშინ, როდესაც სამართალდამცავი ორგანოები მოახდენენ სერვერის კონფისკაციას.

> განავრცონ ძებნა ან მსგავსი გზით გადახონ მათთვის ხელმისაწვდომი სხვა სისტემაზეც.
> [...]

კონვენციის მე-19 მუხლის 1-ლი ქვე-პუნქტის მიზანია განსაზღვროს ინსტრუმენტი, რომლებიც შესაძლებლობას აძლევს გამომძიებლებს მოიძიონ კომპიუტერული სისტემები ისევე ეფექტურად, როგორც ამას აკეთებენ ტრადიციული ძებნის პროცედურების ჩატარებისას.[291] კომპიუტერული დანაშაულის შესახებ კონვენციის მე-19 მუხლის მე-2 ქვე-პუნქტი პასუხობს კომპიუტერულ დანაშაულთან დაკავშირებულ გამოძიებებთან მიმართებაში არსებული პრობლემას. კომპიუტერული სისტემის ფიზიკური ადგილმდებარეობის ადგილზე ინფორმაციის მოძიებისას, გამომძიებლები ხშირად ათვითცნობიერებენ, რომ ეჭვმიტანლმა შეინახა შესაბამისი ინფორმაცია (მაგალითად, ბავშვების პორნოგრაფია) არა ადგილობრივ მყარ დისკზე, არამედ გარე სერვერზე, რომელზეც მას ხელი მიუწვდება ინტერნეტის საშუალებით.[292] ინტერნეტ სერვერების გამოყენება ინფორმაციის შესანახად სულ მეტად პოპულარული ხდება.[293] იმისათვის, რომ უზრუნველყოფილი იქნეს გამოძიებების ეფექტური განხორციელება, მნიშვნელოვანია, რომ შენარჩუნებული იქნეს გამოძიებათა მოქნილობა. თუკი გამომძიებლები აღმოაჩენენ, რომ შესაბამისი ინფორმაცია შენახულია სხვა კომპიუტერულ სისტემაში, მათ შესაძლებლობა უნდა ჰქონდეთ განავრცონ ძებნა ამ სისტემაზეც.[294]

6.6. ინფორმაციის ამოღება

6.6.1. მოვლენა

კომპიუტერული სისტემების და, განსაკუთრებით, შიდა და გარე შესანახი მოწყობილობების შემოწმება წარმოადგენს კომპიუტერულ-ტექნიკური

[291] "თუმცა, კომპიუტერული მონაცემების ძებნასთან დაკავშირებით საჭიროა დამატებითი პროცესუალური დებულებები, რათა უზრუნველყოფილი იქნეს კომპიუტერული მონაცემების მოპოვება ისეთი სახით, რომ იგი ისეთივე ეფექტური იყოს, როგორც მატერიალურ მონაცემთა მატარებლის ძიება და კონფისკაცია. არსებობს ამის რამოდენიმე მიზეზი: პირველი, მონაცემები არსებობს არამატერიალური ფორმით, როგორიცაა ელექტრომაგნიტური ფორმა. მეორე, მიუხედავად იმისა, რომ მონაცემები შეიძლება წაკითხული იყოს კომპიუტერული მოწყობილობის გამოყენებით, ის არ შეიძლება იყოს კონფისკირებული ან ჩამორთმეული ისევე, როგორც ქაღალდზე ნაბეჭდი დოკუმენტი." კომპიუტერული დანაშაულის შესახებ კონვენციის ახსნა-განმარტებითი ანგარიში, №187.

[292] დაკავშირებულ კომპიუტერულ სისტემებზე ძიების გაფართოების შესაძლებლობის მნიშვნელობაზე უკვე აღინიშნა ევროსაბჭოს მინისტრთა კომიტეტის მიერ წევრი ქვეყნებისათვის შემუშავებულ რეკომენდაციაში № R (95) 13, რომელიც შეეხებოდა სისხლის სამართლის საპროცესო კანონმდებლობასთან მიმართებაში არსებულ პრობლემებს, რომლებიც დაკავშირებული იყო საინფორმაციო ტექნოლოგიასთან, რომელიც მიღებული იქნა მინისტრთა კომიტეტის მიერ 1995 წლის 11 სექტემბერს მინისტრთა მოადგილეების 543-ე შეხვედრაზე. რეკომენდაციის ტექსტი ხელმისაწვდომია შემდეგ მისამართზე: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/Rec_1995_13.pdf

[293] ინტერნეტ სერვერზე ინფორმაციის შენახვის ერთ-ერთ უპირატესობას წარმოადგენს ის ფაქტი, რომ ინტერნეტ კავშირის მეშვეობით ინფორმაცია ხელმისაწვდომია ნებისმიერ ადგილიდან.

[294] ამ კონტექსტში მნიშვნელოვანია გათვალისწინებული იყოს ეროვნული სუვერენიტეტის პრინციპი. თუკი ინფორმაცია შენახულია კომპიუტერულ სისტემაში ტერიტორიის გარეთ, ძიების შესახებ ბრძანების გავრცობამ შეიძლება დაარღვიოს ეს პრინციპი. ამიტომ, კომპიუტერული დანაშაულის შესახებ კონვენციის ავტორებმა აღნიშნეს: "მე-2 პუნქტი საშუალებას აძლევს გამომძიებელ ორგანოებს გააფართოვონ თავიანთი ძიება ან უფრო ხელმისაწვდომი გახადონ სხვა კომპიუტერული სისტემა ან მისი ნაწილი, თუკი მათ აქვთ საფუძველი იმისა, რომ სჯეროდეთ, რომ საჭირო მონაცემები ინახება იმ სხვა კომპიუტერულ სისტემაში. თუმცა, სხვა კომპიუტერული სისტემა ან მისი ნაწილი ასევე აუცილებლად უნდა იყოს "მის ტერიტორიაზე" - კომპიუტერული დანაშაულის შესახებ კონვენციის ახსნა-განმარტებითი ანგარიში, №193. ამ საკითხთან დაკავშირებით ასევე იხილეთ: New Jersey Computer Evidence Search and Seizure Manual, 2000, გვ.12: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

ექსპერტიზის მნიშვნელოვან ასპექტს.[295] ზოგადად, შესანახი მოწყობილობების გამოკვლევა საჭიროებს ფიზიკურად მყარი დისკის ქონას.[296]

6.6.2. შესაბამისი პროცესუალური ინსტრუმენტი

> მუხლი 19 – შენახული კომპიუტერული მონაცემების ძებნა და კონფისკაცია
> [...]
> (3) თითოეულმა მხარემ უნდა მიიღოს ისეთი საკანონმდებლო და სხვა სახის ზომები, რომლებიც შეიძლება საჭირო გახდეს იმისათვის, რომ უფლებამოსილება მიანიჭოს მის კომპეტენტურ ორგანოებს კონფისკაცია გაუკეთოს ან ამოიღოს კომპიუტერული მონაცემები, რომლებიც ხელმისაწვდომია 1-ლი ან მე-2 პუნქტების საფუძველზე. ეს ზომები უნდა გულისხმობდეს უფლებამოსილებას, რომ:
> ა) კონფისკირებული ან მსგავსი გზით ამოღებული იქნეს კომპიუტერული სისტემა ან მისი ნაწილი ან კომპიუტერული მონაცემების მატარებელი;
> ბ) გაკეთდეს და შენახული იქნეს ამ კომპიუტერული მონაცემების ასლი;
> გ) შენარჩუნებული იქნეს შესაბამისი შენახული კომპიუტერული მონაცემების ხელშეუხებლობა;
> დ) შეწყდეს ხელმისაწვდომობა ამგვარ კომპიუტერულ მონაცემებთან იმ კომპიუტერულ სისტემაში, რომელიც გახდა ხელმისაწვდომი, ან მოხდეს მათი წაშლა ამ სისტემიდან.
> (4) თითოეულმა მხარემ უნდა მიიღოს ისეთი საკანონმდებლო და სხვა სახის ზომები, რომლებიც შეიძლება საჭირო გახდეს იმისათვის, რომ უფლებამოსილება მიანიჭოს მის კომპეტენტურ ორგანოებს უბრძანოს ნებისმიერ პირს, რომელსაც გააჩნია ცოდნა კომპიუტერული სისტემის ფუნქციონირების ან იმ ზომების შესახებ, რომლებიც გამოყენებულია მასში არსბული კომპიუტერული მონაცემების დასაცავად, მიაწოდოს, რამდენადაც ეს მიზანშეწონილია, ინფორმაცია, რომელიც საჭიროა იმ ზომების მიღების უზრუნველსაყოფად, რომლებიც მითითებულია 1-ლ და მე-2 პუნქტებში.

კომპიუტერული დანაშაულის შესახებ კონვენციის მე-19 მუხლის მე-3 ქვე-პუნქტი შესაძლებლობას აძლევს სამართალდამცავ ორგანოებს მოახდინონ კომპიუტერის მყარი დისკის კონფისკაცია.[297] მყარი დისკის ტრადიციული წესით კონფისკაციის გარდა, კომპიუტერული დანაშაულის შესახებ კონვენცია შესაძლებლობას აძლევს სამართალდამცავ ორგანოებს მყარი დისკის კონფისკაციის სანაცვლოდ, მოახდინონ შესაბამისი მონაცემების

[295] *Hannan*, To Revisit: What is Forensic Computing, 2004: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf; *Etter*, The forensic challenges of e-crime, Australasian Centre for Policing Research, No. 3, 2001, გვ.4: http://www.acpr.gov.au/pdf/ACPR_CC3.pdf;

[296] ძებნისა და კონფისკაციის ტრადიციულ პროცედურებთან შედარებით დისტანციური კომპიუტერულ-ტექნიკური ექსპერტიზის საშუალებების უპირატესობების თაობაზე, იხილეთ: *Gercke*, Secret Online Search, CR 2008, გვ. 245 და შემდგომ. მაგრამ, დისტანციურ გამოძიებებს აქვთ უარყოფით მხარეებიც. იმ ფაქტის გარდა, რომ უშუალო ხელმისაწვდომობა შესაძლებლობას აძლევს სამართალდამცავ ორგანოებს შეისწავლონ შემნახავი მოწყობილობის ფიზიკური მდგომარეობა, კომპიუტერული სისტემის ფიზიკური ხელმისაწვდომობა არის ერთადერთი გზა იმისა, რომ გამოძიების პროცესში უზრუნველყოფილი იქნეს ეჭვმიტანილის კომპიუტერზე ფაილების ხელშეუხებლობა. გამოკვლეული კომპიუტერული სისტემის ხელშეუხებლობის დაცვის მნიშვნელობაზე, იხილეთ: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, გვ.6. http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

[297] კომპიუტერული ტექნიკის კონფისკაციის ჩატარების ინსტრუქცია შეიძლება იხილოთ: General Guidelines for Seizing Computers and Digital Evidence, State of Maryland, Maryland State Police, Criminal Enforcement,Command, Computer Crimes Unit, Computer Forensics Laboratory: http://ccu.mdsp.org/Guidelines%20-%20Seizure%20of%20Digital%20Evidence.htm; New Jersey Computer Evidence Search and Seizure Manual, State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

კოპირება.[298] თუკი სამართალდამცავი ორგანოები გადაწყვეტენ, რომ არ მოახდინონ კომპიუტერის მყარი დისკის კონფისკაცია და, სანაცვლოდ, არამედ უზრუნველყონ მხოლოდ შესაბამისი მონაცემების კოპირება, კომპიუტერული დანაშაულის შესახებ კონვენციის მე-19 მუხლი ითვალისწინებს მთელ რიგ ზომებს, რათა შენარჩუნებული იქნეს კოპირებული მონაცემების ხელშეუხებლობა და წაშლილი იქნეს ორიგინალი მონაცემები.[299]

ხშირად გამომძიებლებს არ შეუძლიათ მყარი დისკის ზუსტი ადგილმდებარეობის განსაზღვრა სისტემის ადმინისტრატორის მეშვეობით, რომელიც პასუხისმგებელია სერვერის ინსფრასტრუქტურაზე.[300] თუმცა, იმ შემთხვევაშიც კი, როდესაც გამომძიებლებს შეუძლიათ მისი იდენტიფიცირება, მათ შეიძლება ვერ შეძლონ შესაბამისი მონაცემების მოძიება მყარი დისკის არსებული დაცვის ზომების გამო. ამიტომ, კონვენციის ავტორების მიერ მასში შეტანილი იქნა სისტემის ადმინისტრატორისა და სხვა პირების ვალდებულება, რომლებმაც იციან შენახული ინფორმაციის ადგილმდებარეობის შესახებ, დაეხმარონ სამართალდამცავ ორგანოებს.

პრაქტიკული ინფორმაცია მოსამართლეებისათვის:
იმ კომპიუტერული მონაცემების ხელშეუხებლობის უზრუნველყოფა, რომლებიც საჭიროა ეჭვმიტანილის იდენტიფიცირებისათვის ან უკანონო ქმედებების მტკიცებულება წარმოადგენს არსებით მოთხოვნას კომპიუტერული დანაშაულთა გამოძიებისათვის. თუკი გამომძიებლებს არ აქვთ ნებართვა მიიღონ საჭირო ზომები კოპირებული მონაცემების ხელშეუხებლობის უზრუნველსაყოფად, ეს კოპირებული მონაცემები შეიძლება არ იქნეს მიღებული მტკიცებულებად სისხლისსამართლერივი სამართალწარმოების დროს.[301]

[298] მონაცემებთა კოპირების აქტის კლასიფიკაციის თაობაზე იხილეთ: *Brenner/Frederiksen,* Computer Searches and Seizure: Some Unresolved Issues in Cybercrime & Security, IB-1, გვ.58 და შემდგომ.

[299] "ვინაიდან ზომები შეეხება შენახულ არამატერიალურ მონაცემებს, საჭიროა კომპეტენტურმა ორგანოებმა მიიღონ დამატებითი ზომები მონაცემთა დაცვისათვის; კერძოდ, საჭიროა "მონაცემების ხელშეუხელბლობის შენარჩუნება", ან მონაცემთა მიმართებაში "პასუხისმგებლობისა და ხელშეუხებლობის უზრუნველყოფის ჯაჭვის" შენარჩუნება, რაც ნიშნავს იმას, რომ მონაცემები, რომლებიც შეიძლება დაკოპირდეს ან წაიშალოს შენახული უნდა იქნეს ქვეყანაში, რომელშიც ისინი იქნა ნაპოვნი კონფისკაციის დროს და დარჩეს უცვლელი სისხლის სამართლის საქმის წარმოების პროცესში. ტერმინი შეეხება მონაცემებზე კონტროლის დაწესებას ან მათ ჩამორთმევას." კომპიუტერული დანაშაულის შესახებ კონვენციის ახსნა-განმარტებითი ანგარიში, №197.

[300] "ეს შეეხება პრაქტიკულ პრობლემას, კერძოდ იმას, რომ შესაძლებელია რთული იყოს იმ მონაცემების მოპოვება და იდენტიფიცირება, რომლებიც იძებნებოდა როგორც მტკიცებულება, მონაცემთა იმ რაოდენობის გათვალისწინებით, რომლებიც შეიძლება დამუშავდეს და შეინახოს, ასევე, უსაფრთხოების ზომების გამოყენებისა და კომპიუტერული ოპერაციების ბუნების გათვალისწინებით. ის ადიარებს, რომ სისტემის ადმინისტრატორებს, რომლებსაც აქვთ კომპიუტერული სისტემის კონკრეტული ცოდნა, შეიძლება დასჭირდეთ კონსულტაცია ტექნიკური საშუალებების შესახებ, რათა განსაზღვრონ საუკეთესო გზა ძებნის ჩასატარებლად." კომპიუტერული დანაშაულის შესახებ კონვენციის ახსნა-განმარტებითი ანგარიში, №200.

[301] ეს პრინციპი ვრცელდება აპარატურის კონფისკაციაზეც. კოპირებული მონაცემების ხელშეუხებლობის შენარჩუნებასთან შედარებით, ხშირად უფრო ადვილია უზრუნველყოფილი იქნეს მონაცემთა ხელშეუხებლობა შემნახავ მოწყობილობაზე.

6.7. ტრაფიკის მონაცემების შეგროვება

6.7.1. მოვლენა

ტრაფიკის მონაცემები თამაშობს მნიშვნელოვან როლს კომპიუტერული დანაშაულთა გამოძიებაში.[302] შინაარსის მონაცემების ხელმისაწვდომობა შესაძლებლობას აძლევს სამართალდამცავ ორგანოებს გააკეთონ გაცვლილ ფაილებში შემავალი მესიჯების ტიპის ანალიზი და ეხმარება მათ მიაკვლიონ დამნაშავეს. ინტერნეტ სერვისის გამოყენების დროს წარმოქმნილი ტრაფიკის მონაცემების მონიტორინგის საშუალებით სამართალდამცას ორგანოებს შეუძლიათ მოახდინონ ინტერნეტ პროტოკოლის (IP) მისამართის იდენტიფიცირება და შემდეგ შეეცადნონ განსაზღვრონ მისი ფიზიკური ადგილმდებარეობა.

6.7.2. შესაბამისი პროცესუალური ინსტრუმენტი

კომპიუტერული დანაშაულის შესახებ კონვენციის მე-20 მუხლი იძლევა იურიდიულ საფუძველს ტრაფიკის მონაცემების შეგროვებისათვის რეალური დროის რეჟიმში.

> მუხლი 20 – ტრაფიკის მონაცემების შეგროვება რეალური დროის რეჟიმში
>
> (1) თითოეულმა მხარემ უნდა მიიღოს ისეთი საკანონმდებლო და სხვა სახის ზომები, რომლებიც შეიძლება საჭირო გახდეს იმისათვის, რომ უფლებამოსილება მიანიჭოს მის კომპეტენტურ ორგანოებს:
> (ა) იმ მხარის ტერიტორიაზე არსებული ტექნიკური საშუალებების გამოყენების გზით შეაგროვოს ან ჩაწეროს; და
> (ბ) აიძულოს სერვისის პროვაიდერი, მის ხელთ არსებული ტექნიკური საშუალებების ფარგლებში:
> (i) იმ მხარის ტერიტორიაზე არსებული ტექნიკური საშუალებების გამოყენების გზით შეაგროვოს ან ჩაწეროს; ან
> (ii) ითანამშრომლოს კომპეტენტურ ორგანოებთან და დაეხმაროს მათ შეაგროვოს ან ჩაწეროს რეალური დროის რეჟიმში ტრაფიკის მონაცემები, რომლებიც დაკავშირებულია კომპიუტერული სისტემის საშუალებით მის ტერიტორიაზე მონაცემების გადაცემის განსაზღვრულ ოპერაციებთან.
> 2) თუკი მხარეს მის ეროვნულ კანონმდებლობით განსაზღვრული პრინციპების გამო არ შეუძლია მიიღოს ზომები, რომლებიც მითითებულია პუნქტში 1(ა), მას შეუძლია სანაცვლოდ მიიღოს იმგვარი საკანონმდებლო ან სხვა სახის ზომები, რომლებიც შესაძლებელია საჭირო გახდეს იმისათვის, რომ უზრუნველყოს დროის რეალურ რეჟიმში ტრაფიკის შესახებ იმ მონაცემების შეგროვება ან ჩაწერა, რომელებიც დაკავშირებულია კომპიუტერული სისტემის საშუალებით მის ტერიტორიაზე მონაცემების გადაცემის განსაზღვრულ ოპერაციებთან.

[302] "კომპიუტერულ სისტემასთან დაკავშირებული სისხლის სამართლის დანაშაულის გამოძიების შემთხვევაში, საჭიროა ტრაფიკის მონაცემები კომუნიკაციის წყაროს მისაკვლევად, როგორც ამოსავალი წერტილი შემდომი მტკიცებულებების შესაგროვებლად ან როგორც დანაშაულის მტკიცებულების ნაწილი. ტრაფიკის მონაცემების ხანგრძლივობა დიდი არ არის, რაც საჭიროს ხდის მის დაჩქარებულ შენახვას. შესაბამისად, მისი სწრაფი გამჟღავნება შესაძლებელია საჭირო იყოს კომუნიკაციის მარშრუტის დასადგენად, რათა მოხდეს შემდგომი მტკიცებულებების შეგროვება მის წაშლამდე ან ეჭვმიტანილის იდენტიფიცირებამდე. ამიტომ, შესაძლებელია კომპიუტერული მონაცემების შეგროვებისა და გამჟღავნების ჩვეულებრივი პროცედურა საკმარისი არ იყოს. უფრო მეტიც, ამ მონაცემების შეგროვება ითვლება, რომ პრინციპში არის ნაკლებად სანდო, ვინაიდან ამ სახით იგი არ ავლენს კომუნიკაციის შინაარსს, რომელიც უფრო მგრძნობიარედ არის მიჩნეული." იხილეთ: კომპიუტერული დანაშაულის შესახებ კონვენციის ახსნა-განმარტებითი ანგარიში №29. კომპიუტერულ დანაშაულთა გამოძიებებში ტრაფიკის მონაცემების მნიშვნელობის შესახებ ასევე იხილეთ: ABA International Guide to Combating Cybercrime, გვ.125; *Gercke,* Preservation of User Data, DUD 2002, 577 და შემდგომ.

(3) თითოეულმა მხარემ უნდა მიიღოს ისეთი საკანონმდებლო და სხვა სახის ზომები, რომლებიც შეიძლება საჭირო გახდეს იმისათვის, რომ მოხდეს სერვისის პროვაიდერის დავალდებულება, რომ საიდუმლოდ შეინახოს წინამდებარე მუხლით განსაზღვრული უფლებამოსილების გამოყენების ფაქტი და მასთან დაკავშირებული ნებისმიერი ინფორმაცია.

(4) უფლებამოსილებები და პროცედურები, რომლებზეც ლაპარაკია ამ მუხლში, დამოკიდებულია მე-14 და მე-15 მუხლებით განსაზღვრული დებულებების ამოქმედებაზე.

დებულება არ არის შექმნილი არც კონკრეტული ტექნოლოგიისათვის და არც იმას ისახავს მიზნად, რომ განსაზღვროს სტანდარტები, რომლებიც განაპირობებენ ამ სფეროში დიდი ფინანსური ინვესტიციების აუცილებლობას.[303]

პრაქტიკული ინფორმაცია მოსამართლეებისათვის:

შინაარსის მონაცემების მოპოვებასთან შედარებით[304], ტრაფიკის მონაცემები ზოგადად ნაკლებად ინტენსიურ ინსტრუმენტს წარმოადგენს. ის უზრუნველყოფს არა შინაარსის მონაცემების, არამედ სხვა ინფორმაციის უშუალო ხელმისაწვდომობას, რომელიც შესაძლებელია საკმარისი იყოს გამოძიების ჩატარებისათვის. ეს ასპექტი თამაშობს მნიშვნელოვან როლს სასამართლოს განკარგულების გამოყენების თვალსაზრისით. ნაკლებად ინტენსიური ინსტრუმენტის არსებობის გამო, სასამართლომ შესაძლებელია არ გასცეს განკარგულება შინაარსის მონაცემების მოპოვებისათვის, თუკი ტრაფიკის მონაცემების შეგროვება შესაძლებელობას მისცემს სამართალდამცავ ორგანოებს განახორციელონ გამოძიება. ეს განსაკუთრებით შეეხება ეჭვმიტანილის ძებნას IP-ის (ინტერნეტ პროტოკოლი) საშუალებით.

[303] "ეს მუხლი [მუხლი 20] არ ავალდებულებს სერვისის პროვაიდერებს, რომ მათ გააჩნდეთ ტექნიკური შესაძლებლობები კოლექციების, ჩანაწერების, თანამშრომლობის ან დახმარების უზრუნველსაყოფად. იგი არ მოითხოვს მათგან, რომ შეიძინონ ან შექმნან ახალი მოწყობილობები, დაიქირავონ ექსპერტები ან მოახდინონ თავიანთი სისტემების ძვირადღირებული კონფიგურაცია." კომპიუტერული დანაშაულის შესახებ კონვენციის ახსნა-განმარტებითი ანგარიში, №221.

[304] იხილეთ ქვემოთ: თავი 4.8

6.8. შინაარსის მონაცემების მოპოვება

6.8.1. მოვლენა

ზოგიერთ შემთხვევაში ტრაფიკის მონაცემების შეგროვება არ არის საკმარისი იმ მტკიცებულებების შესაგროვებლად, რომლებიც საჭიროა ეჭვმიტანილისათვის განაჩენის გამოსატანად. ეს განსაკუთრებით ეხება იმ შემთხვევებს, როდესაც სამართალდამცავმა ორგანოებმა უკვე იციან საკომუნიკაციო პარტნიორისა და გამოყენებული მომსახურების თაობაზე, მაგრამ არ ფლობენ ინფორმაციას გაცვლილი ინფორმაციის შესახებ. მაგალითად, მათ იციან რომ მომხმარებლები, რომლებიც წარსულში მსჯავრდებულები იყვნენ ბავშვების პორნოგრაფიის გაცვლის ბრალდებით, რეგულარულად ტვირთავენ დიდ ფაილებს მათი კოლექტიური გამოყენების სისტემებიდან, მაგრამ მათ არ იციან არის თუ არა ეს ჩვეულებრივი ფილმები (საავტორო უფლებების არმქონე), თუ ბავშვების პორნოგრაფია.

6.8.2. შესაბამისი პროცესუალური ინსტრუმენტი

21-ე მუხლის საფუძველზე სამართალდამცავ ორგანოებს შესაძლებლობა აქვთ მოახდინონ მონაცემთა გაცვლის ჩაწერა და მისი შინაარსის ანალიზი.[305]

> მუხლი 21 – შინაარის შესახებ მონაცემების მოპოვება
>
> (1) თითოეულმა მხარემ უნდა მიიღოს ისეთი აუცილებელი საკანონმდებლო და სხვა სახის ზომები ეროვნული კანონით გათვალისწინებულ მთელი რიგი სერიოზულ დანაშაულებთან დაკავშირებით, რომლებიც შესაძლებლობას მისცემს მის კომპეტენტურ ორგანოებს:
>
> (ა) იმ მხარის ტერიტორიაზე არსებული ტექნიკური საშუალებების გამოყენების გზით შეაგროვოს ან ჩაწეროს; და
> (ბ) აიძულოს სერვისის პროვაიდერი, მის ხელთ არსებული ტენიკური საშუალებების ფარგლებში:
> (i) იმ მხარის ტერიტორიაზე არსებული ტექნიკური საშუალებების გამოყენების გზით შეაგროვოს ან ჩაწეროს; ან
> (ii) ითანამშრომლოს კომპეტენტურ ორგანოებთან და დაეხმაროს მათ შეაგროვოს ან ჩაწეროს რეალური დროის რეჟიმში შინაარსის მონაცემები, რომლებიც დაკავშირებულია კომპიუტერული სისტემის საშუალებით მის ტერიტორიაზე მონაცემების გადაცემის განსაზღვრულ ოპერაციებთან.
>
> 2) თუკი მხარეს მის ეროვნულ კანონმდებლობით განსაზღვრული პრინციპების გამო არ შეუძლია მიიღოს ზომები, რომლებიც მითითებულია პუნქტში 1(ა), მას შეუძლია სანაცვლოდ მიიღოს იმგვარი საკანონმდებლო ან სხვა სახის ზომები, რომლებიც შესაძლებელია საჭირო გახდეს იმისათვის, რომ უზრუნველყოს დროის რეალურ რეჟიმში შინაარსის შესახებ იმ მონაცემების შეგროვება ან ჩაწერა, რომელებიც დაკავშირებულია კომპიუტერული სისტემის საშუალებით მის ტერიტორიაზე მონაცემების გადაცემის განსაზღვრულ ოპერაციებთან.

[305] ერთ-ერთი საშუალება იმისა, რომ სამართალდამცავმა ორგანოებმა ვერ მოახერხონ ორ ეჭვმიტანილს შორის გაცვლილ მონაცემთა შინაარსის ანალიზი არის დაშიფრვის ტექნოლოგიის გამოყენება. დაშიფრვის პროცედურების ფუნქციონირების თაობაზე, იხილეთ: *Singh*; The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology: http://www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

(3) თითოეულმა მხარემ უნდა მიიღოს ისეთი საკანონმდებლო და სხვა სახის ზომები, რომლებიც შეიძლება საჭირო გახდეს იმისათვის, რომ მოხდეს სერვისის პროვაიდერის დავალდებულება, რომ საიდუმლოდ შეინახოს წინამდებარე მუხლით განსაზღვრული უფლებამოსილების გამოყენების ფაქტი და მასთან დაკავშირებული ნებისმიერი ინფორმაცია.

(4) უფლებამოსილებები და პროცედურები, რომლებზეც ლაპარაკია ამ მუხლში, დამოკიდებულია მე-14 და მე-15 მუხლებით განსაზღვრული დებულებების ამოქმედებაზე.

ეს მოიცავს ფაილებს, რომლებიც ჩამოტვირთული იქნა ვებ-გვერდებიდან ან ფაილების გაცვლის სისტემებიდან, დანაშაულის ჩამდენის მიერ გაგზავნილი ან მიღებული ელექტრონული წერილებიდან და "ჩატით" გამართული დიალოგებიდან.

პრაქტიკული ინფორმაცია მოსამართლეებისათვის:

მონაცემთა გადაცემის პროცესებზე კონტროლი არ აძლევს საშუალებას სამართალდამცავ ორგანოებს ანალიზი გაუკეთონ გაცვლილი მონაცემების შინაარსს, თუკი კომუნიკაცია დაშიფრული იყო.[306] დაშიფრვის ტექნოლოგია შესაძლებელია გამოყენებული იქნეს არა მხოლოდ ფაილების გაცვლის დროს, არამედ VoIP (IP ქსელებში ხმოვანი ტრაფიკის გადაცემა) კომუნიკაციების დაცვის მიზნითაც.[307]

[306] კომპიუტერულ-ტექნიკურ ექსპერტიზასა და კრიმინალურ გამოძიებებზე დაშიფრვის ტექნოლოგიის გავლენის შესახებ, იხილეთ: See *Huebner/Bem/Bem*, "Computer Forensics – Past, Present And Future", No.6: www.scm.uws.edu.au/compsci/computerforensics/ Publications/Computer_Forensics_Past_Present_Future.pdf; *Gercke*, The Challenge of fighting Cybercrime, MMR 2008, გვ. 291 და შემდგომ.

[307] სამართალდამცავი ორგანოების დახმარების მიზნით VoIP (IP ქსელებში ხმოვანი ტრაფიკის გადაცემა) მოპოვების თაობაზე იხილეთ: *Bellovin and others*, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP", available at http://www.itaa.org/news/docs/CALEAVOIPreport.pdf; Simon/Slay, "Voice over IP: Forensic Computing Implications", 2006,: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

7. საერთაშორისო თანამშრომლობა

ამ სესიის ბოლოს მონაწილეებს უნდა ესმოდეთ:

- კომპიუტერულ დანაშაულთან და ელექტრონულ მტკიცებულებებთან დაკავშირებული შემთხვევებისათვის მაქსიმალურად ფართო და ეფექტური საერთაშორისო თანამშრომლობის, მათ შორის მონაცემების შენახვისა და შეგროვებისათვის გადაუდებელი ზომების მიღების აუცილებლობა;
- კომპიუტერული დანაშაულის შესახებ კონვენციის დებულებები საერთაშორისო თანამშრომლობის შესახებ.

რეკომენდირებულია, რომ მონაწილეებს შესაძლებლობა ჰქონდეთ ნახონ კომპიუტერული დანაშაულის შესახებ კონვენციის ტექსტი და მასთან დაკავშირებული ახსნა-განმარტებითი ანგარიში (იხ. www.coe.int/cybercrime, სადაც შესაძლებელია კონვენციის ნახვა სხვადასხვა ენაზე).

ასევე, მონაწილეებს ხელი უნდა მიუწვდებოდეთ მათი ეროვნული კანონმდებლობის ტექსთან. მთელი რიგი ქვეყნებისათვის, ამგვარი ინფორმაციის მოძიება შესაძლებელია შემდეგ ვებ-მისამართზე: www.coe.int/cybercrime.

კომპიუტერულ დანაშაულს აქვს ძალიან ძლიერი ტრანსნაციონალური კომპონენტი[308] და რომელიმე ერთ ქვეყანაში ან იურისდიქციის ფარგლებში ერთი პირის მიერ დაწყებულმა თავდასხმებმა შეიძლება გავლენა იქონიოს პიროვნებებზე მრავალ სხვადასხვა ქვეყანაში, ხოლო ელექტრონულმა კომუნიკაციამ, რომელიც გაეგზავნება პირს იმავე ქვეყანაში შეიძლება წარმოშვას ელექტრონული მტკიცებულება სხვა ადგილას, ვინაიდან მონაცემები შეიძლება გადაცემული იქნეს რამოდენიმე ქვეყანაში განთავსებული სერვერების მეშვეობით.

ამავე დროს, ელექტონული მტკიცებულებები ცვალებადია. ამიტომ, მონაცემების შესანარჩუნებლად ქვეყნის დონეზე საჭიროა გადაუდებელი ზომების მიღება საერთაშორისო თანამშრომლობის ფარგლებშიც.

მოკლედ, საჭიროა მაქსიმალურად ფართო საერთაშორისო თანამშრომლობა, რომელიც გულისხმობს გადაუდებელ ზომებს მონაცემთა შენახვისათვის და ეფექტურ ორმხრივ იურიდიულ დახმარებას.

მოსამართლეები და პროკურორები თამაშობენ გადამწყვეტ როლს ამ თანამშრომლობაში, ვინაიდან ისინი ჩართულები არიან აღნიშნული ზომების როგორც დამტკიცების პროცესში, ასევე საქმეების განხილვასა და მათზე სასამართლო გადაწყვეტილებების მიღებაში იმ მტკიცებულებების საფუძველზე, რომლებიც მოპოვებულია საერთაშორისო თანამშრომლობის შედეგად.

[308] კომპიუტერული დანაშაულის ტრანსნაციონალური მასშტაბის შესახებ, იხილეთ: *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, ტომი 12, №2, გვ.289: http://www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf.

Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension - in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, გვ.1 და შემდგომ: http://media.hoover.org/documents/0817999825_1.pdf;

კომპიუტერული დანაშაულის შესახებ კონვენციის III თავში განსაზღვრულია სამართლებრივი ჩარჩოები საერთაშორისო თამანშრომლობისა და ზოგადი და კონკრეტული ზომებისათვის. სახელმძღვანელოს ამ ნაწილში მოცემულია აღნიშნული თავის ზოგიერთი დებულების მიმოხილვა.

არსებითია, რომ მოსამართლეები და პროკურორები გაეცნონ არა მხოლოდ ამ დებულებებს, არამედ სისხლის სამართლის საკითხებზე თანამშრომლობის შესახებ არსებულ სხვა საერთაშორისო და ორმხრივ ხელშეკრულებებს, რომლებიც შეიძლება გამოყენებული იქნეს კომპიუტერული დანაშაულის შემთხვევებისათვის და, განსაკუთრებით, პირდაპირი თანამშრომლობის შესაძლებლობებსა და კრიტიკულ გარემოებებში კომუნიკაციის დაჩქარებულ საშუალებებს.[309]

რომელი კანონები და ხელშეკრულებები შეიძლება იქნეს გამოყენებული საერთაშორისო თანამშრომლობის მიზნით ზოგადად დაკერძოდ, კომპიუტერულ დანაშაულთან მიმართებაში?

განიხილეთ შემდეგ ღონისძიებეთან დაკავშირებული ადგილობრივი კანონმდებლობის დებულებები. სასურველია პრაქტიკული მაგალითები.

7.1. საერთაშორისო თანამშრომლობის ზოგადი პრინციპები

მუხლი 23 განსაზღვრავს საერთაშორისო თანამშრომლობის სამ პრინციპს, რომლებიც გათვალისწინებულია კომპიუტერული დანაშაულის შესახებ კონვენციის III თავში:

- მხარეებს შორის უნდა არსებობდეს "მაქსიმალურად მჭიდრო" საერთაშორისო თანამშრომლობა. ეს პრინციპი მხარეებისაგან მოითხოვს ერთმანეთს შორის მჭიდრო თანამშრომლობას დ საერთაშორისო მასშტაბით ინფორმაციისა და მტკიცებულებების დაუბრკოლებელი და სწრაფი გაცვლისათვის არსებული ხელშემშლელი ფაქტორების აღმოფხვრას;
- თანამშრომლობამ უნდა მოიცვას ყველა კრიმინალური დანაშაული, რომელიც დაკავშირებულია კომპიუტერულ სისტემებთან და მონაცემებთან, ასევე, ნებისმიერი კრიმინალურ დანაშაულთან დაკავშირებით მტკიცებულების ელექტრონული ფორმით შეგროვებასთან. ეს ნიშნავს იმას, რომ როდესაც არსებობს ელექტონული მტკიცებულება იმისა, რომ დანაშაული ჩადენილია კომპიუტერული სისტების გამოყენებით, ან ჩვეულებრივი დანაშაული არ არის ჩადენილი კომპიტერული სისტემის გამოყენებით (მაგ. მკვლელობა), გამოყენებული უნდა იქნეს III თავის დებულებები;

- თანამშრომლობა უნდა განხორციელდეს "წინამდებარე თავის დებულებების შესაბამისად" ან "კრიმინალური საკითხებთან დაკავშირებით საერთაშორისო თანამშრომლობის შესახებ შესაბამისი საერთაშორისო შეთანხმებების, იმ ზომების გამოყენების გზით, რომლებიც შეთანხმებული იქნა საერთო ან ორმხრივი კანონმდებლობისა და ადგილობრივი კანონების საფუძველზე." ბოლო მუხლში განსაზღვრულია ზოგადი პრინციპი, რომ III თავის

[309] ამის კარგი მაგალითია სისხლის სამართლის საქმეებზე ორმხრივი იურიდიული დახმარების შესახებ კონვენციის მე-2 დამატებითი პროტოკოლის მე-4 მუხლი (CETS 182), რომელიც შეეხება სხვადასხვა ქვეყნების სასამართლო ხელისუფლებებს, ასევე, ორმხრივი იურიდიული დახმარების საკითხებზე კომპეტენტურ ორგანოებს შორის ან ინტერპოლის არხებით პირდაპირ კომუნიკაციას. მოთხოვნების გადაგზავნა შესაძლებელია ელექტრონული საშუალებების გამოყენებით.

დებულებები არ აღემატება საერთაშორისო ხელშეკრულებების დებულებებს, რომლებიც შეეხება ორმხრივ იურიდიულ დახმარებასა და ექსტრადიციას, მხარეების მიერ ორმხრივი ზომების მიღებას (უფრო დეტალურად განხილული იქნება ქვემოთ 27-ე მუხლის განხილვისას), ან საერთაშორისო თანამშრომლობის შესახებ ადგილობრივი კანონის შესაბამის დებულებებს.

მესამე პუნქტი ასევე იძლევა ახსნა-განმარტებას იმასთან დაკავშირებით, თუ რატომ იყენებენ ევროპისა და, ასევე, სხვა ქვეყნები კრიმინალურ საკითხებთან დაკავშირებით არსებულ მთელ რიგ ხელშეკრულებებს, და არა მხოლოდ კონვენციას კომპიუტერული დანაშაულის შესახებ, როდესაც თანამშრომლობენ ერთმანეთთან კომპიუტერული დანაშაულის წინააღმდეგ.

მუხლი 23 – საერთაშორისო თანამშრომლობასთან დაკავშირებული ზოგადი პრინციპები

მხარეებმა უნდა ითანამშრომლონ ერთმანეთთან წინამდებარე თავის დებულებების შესაბამისად და დანაშაულებრივ საკითხებთან დაკავშირებით საერთაშორისო თანამშრომლობის შესაბამისი საერთაშორისო ინსტრუმენტების გამოყენების გზით, იმ ზომების გატარებით, რომლებიც შეთანხმებულია საერთო ან ორმხრივი კანონმდებლობისა და ადგილობრივი კანონების საფუძველზე, რამდენადაც შესაძლებელია მასშტაბურად იმ გამოძიებების ან სასამართლო საქმის წარმოებათა მიზნებიდან გამომდინარე, რომლებიც შეეხება კომპიუტერული სისტემებთან და მონაცემებთან დაკავშირებულ კრიმინალურ დანაშაულებებს, ან კრიმინალური დანაშაულის შესახებ მტკიცებულებების ელექტრონული ფორმით შეგროვებისათვის.

7.2. ექსტრადიციასთან დაკავშირებული ძირითადი პრინციპები

ექსტრადიციასთან დაკავშირებული საკითხები განხილულია 24-ე მუხლში, რომელშიც შესულია რიგი ქვე-დებულებებისა და რომელიც ავალდებულებს მხარეებს, რომ კონვენციით (მუხლი 2-11) გათვალისწინებულ კიბერ-დანაშაულებაში მხილებული დამნაშავეები დაექვემდებარონ ექსტრადიციას. იქვე მითითებულია დანაშაულის ის მინიმალური ზღვარი, რომელიც თავისი არსით ექსტრადიციას არ ექვემდებარება.

24-ე მუხლი ასევე ითვალისწინებს ექსტრადიციასთან დაკავშირებულ საერთაშორისო და ორმხრივ ხელშეკრულებებს და მიუთითებს, რომ იმ შემთხვევაში, როდესაც ექსტრადიცია არ დაიშვება დამნაშავის ეროვნული კუთვნილების გამო (ბევრ ქვეყანაში ექსტრადაცია დაუშვებელია თუ დამნაშავე ამ ქვეყნის

ეროვნების წარმომადგენელია), გამოიყენება პრინციპი *'aut dedere aut judicare'* (ანუ ექვემდებარება ექსტრადიციას ან სასამართლო დევნას).

მუხლი 24 – ექსტრადიცია

1 ა ეს მუხლი ვრცელდება მხარეებს შორის ექსტრადიციის საკითხზე იმ სისხლის სამართლის დანაშაულებასთან დაკავშირებით, რომელიც გათავლისწინებულია წინამდებარე კონვენციის მუხლებით 2-დან 11-მდე, იმ პირობით თუ აღნიშნული დანაშაული დასჯადია ორივე მხარის კანონმდებლობით და ითვალისწინებს თავისუფლების აღკვეთას სულ მცირე ერთი წლით მაინც, ან ითვალისწინებს უფრო მკაცრ სასჯელს.

ბ თუ ორ ან მეტ მხარეს შორის ერთიანი ან ურთიერთშეთანხმებული კანონმდებლობის ან ექსტრადიციის ხელშეკრულების, *ექსტრადიციის შესახებ ევროპის კონვენციის* (ETS № 24) ჩათვლით, საფუძველზე მიღწეული შეთანხმების თანახმად დადგენილი მინიმალური სასჯელი განსხვავებულია, გამოყენებული იქნება ეს უკანასკნელი, რომელიც აღნიშნულ შეთანხმებას ან ხელშეკრულებას ეფუძნება.

2 ამ მუხლის პირველ პუნქტში აღწერილი სისხლის სამართლის დანაშაულებები უნდა ჩაითვალოს დანაშაულად, რომელიც ექვემდებარება ექსტრადიციას მხარეებს შორის მოქმედი ექსტრადიციის ნებისმიერი ხელშეკრულების საფუძველზე. მხარეები ვალდებულებას იღებენ აღნიშნული დანაშაულებები მხარეებს შორის მომავალში დადებულ ექსტრადიციის შესახებ ნებისმიერი ხელშეკრულების თანახმად ჩაითვალოს ისეთ დანაშაულად, რომელიც ექსტრადიციას ექვემდებარება.

3 თუ მხარე, რომელიც შესაბამისი ხელშეკრულების საფუძველზე ექსტრადიციას სავალდებულოდ თვლის, მეორე მხარისაგან ექსტრადიციის თაობაზე შუამდგომლობას მიიღებს, თუმცა ამ უკანასკნელს არ გააჩნია ექსტრადიციის ხელშეკრულება პირველ მხარესთან, წინამდებარე კონვენცია ჩაითვლება ექსტრადიციის იურიდიულ საფუძვლად ნებისმიერ იმ სისხლის სამართლის დანაშაულთან მიმართებაში, რომელიც მოცემულია ამ მუხლის პირველ პუნქტში.

4 თუ შესაბამისი ხელშეკრულების საფუძველზე მხარეები ექსტრადიციას სავალდებულოდ არ მიიჩნევენ, ისინი ვალდებული არიან აღიარონ ამ მუხლის პირველ პუნქტში ჩამოთვლილი დანაშაულებები ისეთ დანაშაულად, რომელიც მხარეებს შორის ექსტრადიციას ექვემდებარება.

5 ექსტრადიცია ექვემდებარება იმ პირობებს, რომელიც გათვალისწინებულია შუამდგომლობის მიმღები მხარის კანონით ან ექსტრადიციის შესაბამისი ხელშეკრულებით, იმ საფუძვლის ჩათვლით რომლის თანახმად შუმადგომლობის მიმღებმა მხარემ შეიძლება უარი თქვას ექსტრადაციაზე.

6 თუ ამ მუხლის პირველ პუნქტში ჩამოთვლილი სისხლის სამართლის დანაშაულისათვის მხარეს უარი ეთქვა ექსტრადიციაზე მხოლოდ ეჭვმიტანილის ეროვნული კუთვნილების გამო, ან იმის გამო, რომ შუამდგომლობის მიმღებ მხარეს მიაჩნია, რომ აღნიშნული დანაშაული მის იურისდიქციაშია, ეს უკანასკნელი შუამდგომი მხარის თხოვნით საქმის წარმართვის მიზნით საქმეს კომპეტენტურ ორგანოებს გადასცემს, ხოლო საბოლოო შედეგს შუამდგომ მხარეს დროულად შეატყობინებს. ხოლო კომპეტენტური ორგანოები ვალდებული არიან მიიღონ გადაწყვეტილება, ჩაატარონ გამოძიება და სასამართლო პროცესი, როგორც ეს მსგავსი დანაშაულისათვის ამ მხარის კანონმდებლობით არის გათვალისწინებული.

7.3. სამართლებრივი თანამშრომლობის ზოგადი პრინციპები

მუხლი 24 იმეორებს მუხლ 23-ში მოცემულ ზოგიერთ ზოგად პრინციპს; კონკრეტულად, იმას, რომ თანამშრომლობა უნდა განხორციელდეს მაქსიმალურად ფართო საკითხებში და რომ თანამშრომლობის ვალდებულება ვრცელდება არა მხოლო კიბერ-დანაშაულზე, არამედ ნებისმიერ ტრადიციულ დანაშაულზე, რომელიც ელექტრონულ სამხილს შეეხება.
აღნიშნული მუხლი ითვალისწინებს, რომ გამოყენებული იქნეს ხელშეკრულებები, კანონმდებლობები და შეთანხმებები, რომელიც იურიდიულ ურთიერთდახმარებას ეხება.
კონვენციასთან მიერთებული მხარეები ვალდებული არიან შექმნან ნაციონალური სამართლებლივი ბაზა იმ ზომების გასატარებლად, რომლებიც ჩამოთვლილია კონვენციის 29-35 მუხლებში.
ამ მუხლის მესამე პუნქტი მოწოდებულია დააჩქაროს ურთიერთდახმარების შუამდგომლობაზე პასუხი, რათა თავიდან იქნეს აცილებული არსებითი ინფორმაციის ან მტკიცებულების დაკარგვა, ვინაიდან იგი წაშალეს მანამ სანამ თხოვნა თანამშრომლობაზე მომზადდა, მხარეებს გადაეგზავნა და პასუხი მასზე მიღებული იქნა. იგი:

- უფლებას აძლევს მხარეებს კომუნიკაციის უფრო სწრაფი საშუალებები გამოიყენონ თანამშრომლობის თხოვნით მიმართვისას, ნაცვლად ტრადიციული გზებისა, რომლის თანახმად დაწერილი და დალუქული დოკუმენტები დიპლომატიური ფოსტის ან ჩვეულებრივი ფოსტის მეშვეობით გადაიგზავნება ხოლმე.
- მოითხოვს, რომ მეორე მხარემ კომუნიკაციის ასევე სწრაფი საშუალებებით გასცეს პასუხი. ამ დებულების საფუძველზე მხარეებს საშუალება ეძლევათ ისარგებლონ აღნიშნული საშუალებით, მაშინაც კი თუ იგი ურთიერთდახმარების ხელშეკრულებებით, კანონმდებლობითა თუ შეთანხმებებით გათვალისიწნებული ჯერ არ არის.

პუნქტ 4-ში ჩამოყალიბებულია პრინციპი, რომლის თანახმად ურთიერთდახმარების საკითხზე ვრცელდება ურთიერთდახმარების ხელშეკრულებებისა და სამამულო კანონმდებლობების პირობები. ეს გარემოება იცავს იმ პირთა უფლებებს, რომლებიც შუამდგომი მხარის ტერიტორიაზეა და რომელიც შეიძლება გახდეს ურთიერთდახმარების სუბიექტი. მაგალითად, იძულებითი ზომა, როგორიც არის ორდერი გაჩხრეკაზე ვერ გატარდება შუამდგომი მხარის სახელით, თუ მსგავს ვითარებაში ეს სავალდებულო ზომად არ არის მეორე მხარის მიერ მიჩნეული. მხარეებმა ასევე უნდა უზრუნველყონ პირთა უფლებების დაცვა, როდესაც ამ უკანასკნელთ დაუყადაღებენ ნივთებს და გადასცემენ მეორე მხარეს სამართლებლივი ურთიერთდახმარების ფარგლებში.
პუნქტი 5 იძლევა განმარტებას თუ რა იგულისხმება ისეთი დანაშაულის ქვეშ, რომელსაც, ამ თავში ჩამოყალიბებული ურთიერთდახმარების კუთხით, ორივე მხარე ასეთად აღიარებს.

შუამდგომლობის მიმღებ მხარეს უფლება აქვს გაუწიოს მეორე მხარეს დახმარება იმ პირობით, თუ აღნიშნულ ქმედებას ორივე მხარე დანაშაულის კვალიფიკაციას აძლევს. ქმედება შეიძლება ჩაითვალოს დანაშაულად ორივე მხარის მიერ იმ შემთხვევაში, თუ დანაშაული, რომლის დასახმარებლადაც მიმართეს მხარეს, ასევე წარმოადგენს სისხლის სამართლის დანაშაულს შუამდგომლობის მიმღები მხარის კანონმდებლობით, მაშინაც კი თუ ეს მხარე ამ დანაშაულს დანაშაულთა სხვა კატეგორიას მიაკუთვნებს ან მისი კვალიფიკაციისათვის სხვა ტერმინოლოგიას იყენებს.
კონვენციასთან მიერთებული მხარეები ვალდებული არიან კანონსაწინააღმდეგოდ ჩათვალონ 2-11 მუხლებით (არასანქცირებული შეღწევა, მონაცემთა ბაზებში შეღწევა, ბავშვთა პორნოგრაფია და სხვა) განსაზღვრული ქმედებები, რათა პირობა, რომელიც ორივე მხარის მიერ დანაშაულის აღიარებას იტხოვს დაკმაყოფილებული იქნეს[310].

მუხლი 25 – ურთიერთდახმარებასთან დაკავშირებული ზოგადი პრინციპები

1 მხარეები ვალდებული არიან მაქსიმალურად დაეხმარონ ერთმანეთს გამოძიების ჩატარებაში ან სამართალწარმოებაში, როდესაც საქმე ეხება კომპიუტერულ სისტემებთან, მონაცემებთან დაკავშირებულ სისხლის სამართლის დანაშაულს ან როდესაც საჭიროა მტკიცებულებების მოპოვება ელექტრონულ საშუალებებზე ჩადენილი სისხლის სამართლის დანაშაულთან მიმართებაში.

2 ყველა მხარე ვალდებულია მიიღოს ისეთი კანონმდებლობა ან გაატაროს ისეთი ღონისძიებები, რომელიც საჭირო 27-35 მუხლებში ჩამოყალიბებული ვალდებულებების შესასრულებლად.

3 განსაკუთრებულ ვითარებაში ყველა მხარეს უფლება აქვს მოითხოვოს დახმარება ან კომუნიკაციის დამყარება კომუნიკაციის სწრაფი საშუალებებით, ფაქსისა და ელექტრონული ფოსტის ჩათვლით იმ პირობით თუ აღნიშნული საშუალებები უსაფრთხოებისა და ავთენტურობის (კოდირების ჩათვლით, სადაც ეს საჭიროა) უზრუნველყოფის საშუალებას იძლევა და თუ საჭიროა მას თან უნდა მოყვეს შუამდგომი მხარის დასტური. მეორე მხარეც ვალდებულია იმავე დაჩქარებული ტიპის საშუალებით უპასუხოს.

4 თუ სხვა რამ ამ თავის მუხლებით გათვალისწინებული არ არის, ურთიერთდახმარება ექვემდებარება იმ შეზღუდვებს, რომელსაც შუამდგომლობის მიმღები მხარის კანონმდებლობა ან ურთიერთდახმარების ხელშეკრულებები ითვალისწინებს, იმ საფუძვლის ჩათვლით რომლის თანახმად ამ უკანასკნელს უფლება აქვს უარი უთხრას მეორე მხარეს თანამშრომლობაზე. შუამდგომლობის მიმღები მხარე ვერ გამოიყენებს ურთიერთდახმარებაზე უარის თქმის უფლებას იმ დანაშაულებებთან მიმართებაში, რომელიც ჩამოთვლილია 2-11 მუხლებში იმ საფუძველზე რომ თხოვნა ეხება ისეთ დანაშაულს, რომელიც ამ მხარის მიერ კვალიფიცირდება როგორც ფისკალური (საგადასახადო) დანაშაული.

5 თუ ამ თავის დებულებების თანახმად შუამდგომი მხარე უფლებამოსილია ურთიერთდახმარების პირობა დაასაბუთოს იმ ფაქტით, რომ აღნიშნულ ქმედებას ორივე მხარე დანაშაულად აღიარებს, ეს პირობა დაკმაყოფილებულად ჩაითვლება მიუხედავად იმისა მიაკუთვნებს თუ არა კანონი აღნიშნულ ქმედებას დანაშაულის იმავე კატეგორიას და იყენებს თუ არა იგი დანაშაულთან დაკავშირებით იგივე ფორმულირებას, რასაც შუამდგომი მხარის კანონმდებლობა, თუ ქცევა, რომელიც ქმედებას საფუძვლად უდევს და რომელთან დაკავშირებით დახმარება იქნა მოთხოვნილი შუამდგომი მხარის კანონმდებლობით სისხლის სამართლის დანაშაულად კვალიფიცირდება.

[310] ზოგიერთ მხარეს შეიძლება გარკვეული დათქმები ჰქონდეს ზოგიერთ მუხლთან დაკავშირებით.

7.4. სამართლებლივი ურთიერთდახმარება შესაბამისი საერთაშორისო ხელშეკრულებების არ არსებობის დროს

კონვენციის წინა დებულებებში ვრცლად იყო საუბარი მოქმედი ხელშეკრულებების თაობაზე, რომელიც საერთაშორისო თანამშრომლობას შეეხებოდა. ევროპის ქვეყნები, ფაქტობრივად, განიხილავენ მთელ რიგ ხელშეკრულებებსა და ორმხრივ შეთანხმებებს.

თუმცა, უნდა აღინიშნოს, რომ კონვენციას კიბერ-დანაშაულის შესახებ უერთდება სულ უფრო მეტი არა-ევროპული ქვეყანა, თუმცა ეს არ გულისხმობს, რომ იგივე ქვეყნები აუცილებლად მიუერთდებიან სხვა ხელშეკრულებებს სისხლის სამართლის საკითხებზე თანამშრომლობის შესახებ.

ამგვარი ვითარების დროს 27-ე მუხლში ჩამოყალიბებულია ის საბაზო დებულებები, რომელიც უზრუნველყოფს სამართლის სფეროში ურთიერთდახმარებას იმ ქვეყნებს შორის, რომელთაც სხვა იურიდიული ხელშეკრულება ერთმანეთთან არ აქვთ.

მუხლი 27 – პროცედურები, რომელიც შეეხება ურთიერთდახმარების მოთხოვნას საერთაშორისო ხელშეკრულებების არ არსებობის დროს

1 თუ შუამდგომ მხარესა და შუმადგომლობის მიმღებ მხარეს შორის არ არსებობს ურთიერთდახმარების ხელშეკრულება ან შეთანხმება, რომელიც ეფუძნება მოქმედ ერთიან ან ურთიერთვალდებულებათა კანონმდებლობას, ამოქმედდება ამ მუხლის 2-9 პუნქტებით გათვალისწინებული დებულებები. აღნიშნული მუხლის დებულებები არ იმოქმედებს თუ მხარეებს შორის არსებობს ზემოთ აღნიშნული ხელშეკრულება, შეთანხმება ან კანონმდებლობა, გარდა იმ შემთხვევებისა, როდესაც ორივე მხარე შეთანხმდება ნაცვლად არსებული კანონმდებლობისა თუ სხვა შეთანხმებისა ისარგებლონ აღნიშნული მუხლის ზოგიერთი ან ყველა დებულებით.

2 ა თითოეული მხარე ვალდებულია გამოყოს ცენტრალური ორგანო ან ორგანოები, რომელიც ვალდებული იქნება გააგზავნოს ან უპასუხოს თხოვნას ურთიერთდახმარების თაობაზე, აღასრულოს აღნიშნული თხოვნა ან აღსრულების მიზნით გადაუგზავნოს იგი შესაბამის კომპეტენტურ ორგანოს;

ბ ცენტრალური ორგანოები ვალდებული არიან უშუალო კავშირი იქონიონ ერთმანეთთან;

გ აღნიშნული პუნქტის მოთხოვნის შესაბამისად თითოეული მხარე ვალდებულია შეატყობინოს ევროსაბჭოს გენერალურ მდივანს შერჩეული პასუხისმგებელი ორგანოს დასახელება და მისამართი მას შემდეგ რაც ხელი მოეწერება ან მოხდება დოკუმენტის რატიფიცირება, მიღება, დამტკიცება ან მიერთება;

დ ევროსაბჭოს გენერალური მდივანი ვალდებულია აწარმოოს და განაახლოს მხარეების მიერ დასახელებული ცენტრალური ორგანოს მონაცემთა რეესტრი. მხარეები მუდმივად კისრულებენ ვალდებულებას რეესტრში შეტანილი ინფორმაციის სისწორეზე.

3 ამ მუხლით გათვალისწინებული ურთიერთდახმარებაზე თხოვნის აღსრულება უნდა განხორციელდეს იმ პროცედურის შესაბამისად, რომელიც განსაზღვრულია შუამდგომი მხარის მიერ, გარდა იმ გამონაკლისებისა, როდესაც აღნიშნული არ შეესაბამება შუმადგომლობის მიმღები მხარის კანონმდებლობას.

4 გარდა 25-ე მუხლის 4 პუნქტში ჩამოყალიბებული უარის თქმის შესაძლებლობებისა, შუამდგომლობის მიმღებმა მხარემ შეიძლება უარი განაცხადოს დახმარების გაწევაზე, თუ:

ა თხოვნა შეეხება დანაშაულს, რომელიც შუამდგომლობის მიმღები მხარის მიერ კვალიფიცირდება როგორც პოლიტიკური დანაშაული ან პოლიტიკურ დანაშაულთან დაკავშირებულ სამართალდარღვევა, ან

ბ შუამდგომლობის მიმღებ მხარეს მიაჩნია, რომ აღნიშნული თხოვნის აღსრულება საფრთხეს უქმნის მის სუვერენიტეტს, უსაფრთხოებას, საზოგადოებრივ წესრიგს ან მის სხვა არსებით ინტერესებს.

5 შუამდგომლობის მიმღები მხარე უფლებამოსილია გადადოს თხოვნაზე რეაგირება, თუ მსგავსი ქმედება საფრთხის წინაშე აყენებს სისხლის სამართლის დანაშაულის გამოძიებას ან სასამართლო წარმოებას, რომელსაც აღნიშნული მხარის აწარმოებს.

6 სანამ აღნიშნული მხარე უარს განაცხადებს შუამდგომლობაზე ან გადადებს შუამდგომლობაზე რეაგირებას, შუამდგომ მხარესთან კონსულტაციების გავლის შემდეგ (საჭიროების შემთხვევაში) შუამდგომლობის მიმღები მხარე მიიღებს გადაწყვეტილებას შუამდგომლობის ნაწილობრივ დაკმაყოფილებაზე ან იმ პირობებით დაკმაყოფილებაზე, როგორც ამას ეს უკანასკნელი მიიჩნევს საჭიროდ.

7 შუამდგომლობის მიმღები მხარე ვალდებულია დაუყონებლივ შეატყობინოს შუამდგომ მხარეს თუ რა გადაწყვეტილება იქნა მიღებული დახმარების თხოვნაზე. ასევე, მხარე ვალდებულია დაასახელოს ის მიზეზები რის გამოც შუამდგომ მხარეს უარი ეთქვა შუამდგომლობაზე ან საჭირო გახდა მასზე რეაგირების გადადება. შუამდგომლობის მიმღები მხარე ასევე ვალდებულია შეატყობინობს შუამდგომ მხარეს იმ მიზეზების შესახებ, რის გამოც შუამდგომლობის აღსრულება შუამდგომლობის მიმღებ მხარეს არ შეუძლია ან საჭიროდ მიიჩნევს მისი ხანგრძლივი დროით გადადებას.

8 შუამდგომ მხარეს შეუძლია თხოვნით მიმართოს შუამდგომლობის მიმღებ მხარეს საიდუმლოდ შეინახოს მისი შუამდგომლობის ფაქტი და შუამდგომლობის საგანი, რამდენადაც ეს საჭიროა აღნიშნული შუამდგომლობის დაკმაყოფილებისათვის. თუ შუამდგომლობის მიმღებ მხარეს არ ძალუძს კონფიდენციალობის უზრუნველყოფა, მან დაუყონებლივ უნდა შეატყობინოს შუამდგომ მხარეს ამის თაობაზე, ხოლო ამის შემდეგ ეს უკანასკნელი თავად იღებს გადაწყვეტილებას ძალაში დატოვოს შუამდგომლობის მოთხოვნა თუ არა.

9 ა განსაკუთრებულ შემთხვევაში, შუამდგომი მხარის სასამართლო ხელისუფლებამ შეიძლება უშუალოდ გაუგზავნოს შუამდგომლობის მიმღები მხარის სასამართლო ხელისუფლებას თხოვნა ურთიერთდახმარებაზე ან ამასთან დაკავშირებული ინფორმაციის მიწოდებასთან დაკავშირებით. ამ შემთხვევაში თხოვნის ერთი ეგზემპლიარი შუამდგომი მხარის ცენტრალური ხელისუფლების ორგანოების გავლით პარალელურად ეგზავნება შუამდგომლობის მიმღები მხარის ცენტრალურ ორგანოებს.

ბ ამ პუნქტით გათვალისწინებული ნებისმიერი შუამდგომლობა ან მასთან დაკავშირებული ინფორმაციის მიწოდება უნდა განხორციელდეს ინტერპოლის მეშვეობით.

გ თუ შუამდგომლობა ამ მუხლის (ა) ქვე-პუნქტის შესაბამისად იგზავნება და მას იღებს ის ორგანო, რომელიც არ არის კომპეტენტური რეაგირება მოახდინოს შუამდგომლობაზე, იგი შუამდგომლობას შუამდგომლობის მიმღები მხარის კომპეტენტურ ორგანოს გადასცემს, რის შესახებ იგი შუამდგომ მხარეს შეატყობინებს.

დ თუ ამ პუნქტით გათვალისწინებული შუამდგომლობა ან მასთან დაკავშირებული ინფორმაციის მიწოდება არ ითვალისწინებს იძულებითი ზომების გატარებას, შუამდგომი მხარის კომპეტენტურმა ორგანომ შუამდგომლობა შეიძლება პირდაპირ გადასცეს შუამდგომლობის მიმღები მხარის კომპეტენტურ ორგანოს.

ე ხელის მოწერის ან რატიფიკაციის, მიღების, დამტკიცების ან მიერთების სიგელების გადაცემისას, ყველა მხარე ვალდებული სეატყობინოს ევროსაბჭოს გენერალურ მდივანს (პროცესის დაჩქარების მიზნით), რომ ამ პუნქტით გათვალისწინებული შუამდგომლობა უნდა განხორციელდეს ცენტრალური ხელისუფლების მიერ.

7.5. სპეციალური დებულებები: კომპიუტერული მონაცემების დაუყოვნებლივი უსაფრთხო შენახვა

კომპიუტერული მონაცემების დაჩქარებული უსაფრთხო შენახვა სავალდებულოა არა მხოლოდ ეროვნულ დონეზე (მუხლი 16) არამედ საერთაშორისო დონეზეც. ამის დასტურია კონვენციის მუხლის 29.

შუამდგომლობის მიმღები მხარე ვალდებულია სწრაფად იმოქმედოს და მონაცემები უსაფრთხო ადგილას შეინახოს. ორივე მხარის მიერ დანაშაულის დანაშაულად აღიარების პირობა მხოლოდ განსაკუთრებულ ვითარებაში მოქმედებს. უნდა ხაზგასმით აღინიშნოს, რომ ინტერნეტ-პროვაიდერის დონეზე მონაცემების შენახვა მხოლოდ დროებითი ზომაა. ინფორმაციის საჯაროდ გამოტანა შემდგომი ეტაპია. იმისათვის, რომ ეს განხორციელდეს იურიდული დახმარების თაობაზე ურთიერთშუამდგომლობის მოპოვება შეიძლება საჭირო გახდეს.

მუხლი 29 – კომპიუტერული მონაცემების დაუყონებლივი უსაფრთხო შენახვა

1 ერთმა მხარემ შეიძლება სთხოვოს მეორე მხარეს მოითხოვოს ან სხვა საშუალებებით მოახერხოს მონაცმეთა ოპერატიულად შენახვა იმ კომპიუტერულ სისტემაში, რომელიც მეორე მხარის ტერიტორიაზე მდებარეობს და რომელთან მიმართებაშიც შუამდგომი მხარე გეგმავს ითხოვს დახმარება, რათა მოიპოვის მონაცემების მოძიების ან მონაცემების გამოყენების, მათი ამოღების ან უსაფრთხი შენახვის ან მონაცემთა მიღების უფლება.

2 მონაცემთა შენახვის შესახებ შუამდგომლობაში პუნქტ 1-ის თანახმად მითითებული უნდა იყოს:

ა. რომელი ორგანო ითხოვს მონაცემთა შენახვის უზრუნველყოფას;

ბ. რა სახის არის დანაშაული, რომელიც ექვემდებარება სისხლის სამართლის გამოძიებას ან სამართალწარმოებას და მასთან დაკავშირებული ფაქტების მოკლე აღწერა;

გ. რა სახის კომპიუტერული მონაცემები უნდა იქნეს დაცული და რა დამოკიდებულება აქვს მას დანაშაულთან;

დ. ნებისმიერი ინფორმაცია, რომელიც იდენტიფიცირებას გაუკეთებდა იმ პირს, რომელიც ინახავს კომპიუტერულ მონაცემებს და სად მდებარეობს კომპიუტერული სისტემა;

ე. რით არის მისი უსაფრთხო შენახვა განპირობებული;

ვ. რა მიზნით სჭირდება მხარეს მონაცემთა მოძიება-მოიპოვება, მათი ამოღება ან უსაფრთხო შენახვა ან მონაცემთა მიღების უფლება.

3 მეორე მხარისაგან შუამდგომლობის მიღების შემდეგ, შუამდგომლობის მიმღებმა მხარემ უნდა გაატაროს შესაბამისი ღონისძიებები კონკრეტული მონაცემების სამამულო კანონმდებლობის შესაბამისად ოპერატიულად უსაფრთხო შენახვისათვის. იმისათვის, რომ შუამდგომლობა დაკმაყოფილდეს, დანაშაულის ორივე მხარის მიერ აღიარების პირობის არსებობა სავალდებულო არ არის, რათა მხარემ უზრუნველყოს აღნიშნული მონაცემების უსაფრთხო შენახვა.

.

4 თუ მხარე მოითხოვს დანაშაულის ორივე მხარის მიერ აღიარების პირობის დაკმაყოფილებას, რათა რეაგირება მოახდინოს ურთიერთდახმარების შესახებ თხოვნაზე, რათა მოიპოვის მონაცემების მოძიების ან მონაცემების გამოყენების, მათი ამოღების ან უსაფრთხო შენახვის ან მონაცემთა გამოაშკარავების უფლება, იმ დანაშაულებებთან დაკავშირებით, რომელიც არ არის მითითებული ამ კონვენციის მუხლებში 2-11, მხარე იტოვებს უფლებას უარი უთხრას მეორე მხარეს შუამდგომლობაზე ინფორმაციის შენახვის შესახებ, იმ პირობით თუ მხარეს აქვს საფუძველი ივარაუდოს, რომ ინფორმაციის გამოაშკარავების დროისათვის ჯერ კიდევ ვერ იქნება დადგენილი დანაშაულის ორივე მხარის მიერ აღიარების პირობის არსებობის ფაქტი.

5 გარდა ამისა, შუამდგომლობაზე მონაცემების შენახვის თაობაზე შეიძლება მხარეს უარი ეთქვას თუ:

ა შუამდგომლობა ეხება ისეთ დანაშაულს, რომელსაც შუამდგომლობის მიმღები მხარე პოლიტიკურ დანაშაულად მიიჩნევს ან მასთან არის დაკავშირებულია; ან

ბ შუამდგომლობის მიმღები მხარე მიიჩნევს, რომ აღნიშნული შუამდგომლობის დაკმაყოფილება საფრთხის ქვეშ აყენებს მის სუვერენიტეტს, უსაფრთხოებას, საზოგადოებრივ წესრიგს ან მის სხვა არსებით ინტერესებს.

6 თუ შუამდგომლობის მიმღები მხარე მიიჩნევს, რომ ინფორმაციის შენახვის პროცედურამ შეიძლება ეჭვის ქვეშ დააყენოს ამ ინფორმაციის ხელმისაწვდომობა მომავალში ან საფრთხის წინაშე აყენებს შუამდგომი მხარის გამოძიების კონფიდენციალობას ან სხვა რაიმეს, იგი დაუყონებლივ შეატყობინებს შუამდგომ მხარეს ამის შესახებ, ხოლო ამის შემდეგ ეს უკანასკნელი თავად მიიღებს გადაწყვეტილებას მაინც მოითხოვოს შუამდგომლობის დაკმაყოფილება თუ არა.

7 მონაცემების შენახვის ხანგრძლივობა პუნქტ 1-ში მითითებულ შუამდგომლობაზე უნდა იყოს არა ნაკლებ 60 დღისა, რათა შუამდგომ მხარეს დრო ჰქონდეს მოამზადოს თხოვნა, რათა მოიპოვოს მონაცემების მოძიების ან მონაცემების გამოყენების, მათი ამოღების ან უსაფრთხო შენახვის ან მონაცემთა გამოაშკარავების უფლება. მსგავსი თხოვნის მიღების შემდეგ, მონაცემები კვლავ შენახვის რეჟიმში დარჩება სანამ არ მოხდება თხოვნასთან დაკავშირებით გადაწყვეტილების მიღება.

7.6. სპეციალური დებულება: ქსელური ტრაფიკის შესახებ შენახული მონაცემების დაუყონებლივ გამოაშკარავება

ვინაიდან მონაცემები, როგორც წესი მრავალ ქვეყანაში გადაიცემა, საკმარისი არ არის ქსელური ტრაფიკის შესახებ მონაცემების შენახვის მოთხოვნით მხოლოდ ერთ ქვეყანას მიმართოთ. საჭიროა ამ თხოვნით ყველა ქვეყანას ან ყველა სერვერს მიმართოთ. ამგვარად, სერვის პროვაიდერი ვალდებულია გამოააშკარაოს შესაბამისი მონაცემები, რათა გამოაშკარავდეს ის არხი რომლის მეშვეობით მოხდა ამ ინფორმაციის გადაცემა და ეთხოვოს მას ამ ინფორმაციის შენახვა. ამას უზრუნველყოფს კონვენციის 30-ე მუხლი (რომელიც ექვივალენტურია მე-17 მუხლის დებულებისა ეროვნულ დონეზე).

მუხლი 30 – ქსელური ტრაფიკის შესახებ შენახული მონაცემების დაუყონებლივი გამოაშკარავება

1 თუ 29-ე მუხლის თანახმად ქსელური ტრაფიკის შესახებ მონაცემების შენახვაზე შემოსული შუამდგომლობის აღსრულების დროს შუამდგომლობის მიმღებმა მხარემ აღმოაჩინა, რომ ამ ინფორმაციის გატარებაში ჩაბმული იყო სხვა სახელმწიფოს სერვის-პროვაიდერი, შუამდგომლობის მიმღები მხარე ვალდებულია ოპერატიულად გაუმხილოს შუამდგომ მხარეს ქსელური ტრაფიკის შესახებ საკმარისი ინფორმაცია რათა დადგინდეს სერვის-პროვაიდერი და ის არხი, რომლის მეშვეობითაც მოხდა ინფორმაციის გადაცემა.

2 პირველი პუნქტის თანახმად არ დაიშვება ქსელური ტრაფიკის შესახებ ინფორმაციის გამოაშკარავება თუ:

ა. თხოვნა ეხება დანაშაულს, რომელსაც შუამდგომლობის მიმღები მხარე პოლიტიკურ დანაშაულად ან მასთან დაკავშირებულ დანაშაულად მიიჩნევს; ან

ბ. შუამდგომლობის მიმღები მხარე მიიჩნევს, რომ აღნიშნული თხოვნის დაკმაყოფილება საფრთხეს შეუქმნის მის სუვერენიტეტს; უსაფრთხოებას, საზოგადოებრივ წესრიგს ან სხვა არსებით ინტერესს.

7.7. სპეციალური დებულება: ურთიერთდახმარება შენახული კომპიუტერული მონაცემების ხელმისაწვდომობაზე

31-ე მუხლის თანახმად ერთ მხარეს უფლება აქვს თხოვნით მიმართოს მეორე მხარეს, რათა ამ უკანასკნელმა ნება დართოს ხელი მიუწვდებოდეს, ამოიღოს ან გამოააშკარაოს მის ტერიტორიაზე არსებულ კომპიუტერულ სისტემაში შენახული მონაცემი. ეს მუხლი ასევე უზრუნველყოფს მოთხოვნის დაუყონებლივ დაკმაყოფილებას.

მუხლი 31 - ურთიერთდახმარება შენახული კომპიუტერული მონაცემების ხელმისაწვდომობაზე

1 ერთმა მხარემ შეიძლება თხოვოს მეორე მხარეს, რომ მან გაჩხრიკოს ან შეაღწიოს, ამოიღოს ან უზრუნველყოს უსაფრთხოება და გამოააშკარაოს ინფორმაცია, რომელიც შენახულია კომპტერულ სისტემაში, რომელიც შუამდგომლობის მიმღები მხარის ტერიტორიაზე მდებარეობს, იმ მონაცემების ჩათვლით, რომელიც შენახულია 29-ე მუხლის შესაბამისად.

2 შუამდგომლობის მიმღები მხარე ვალდებულია რეაგირება მოახდინოს შუამდგომლობაზე საერთაშორისო სამართლებლივი დოკუმენტების, შეთანხმებებისა და კანონების საშუალებით, რომლიც მითითებულია 23-ე მუხლში, ასევე ამ თავის დებულებების შესაბამისად.

3 შუამდგომლობაზე რეაგირება დაუყონებლივ მოხდება თუ:

ა. არსებობს იმ ვარაუდის საფუძველი, რომ შესაბამისი ინფორმაცია შეიძლება დაიკარგოს ან შეიცვალოს; ან

ბ. მე-2 პუნქტში ჩამოთვლილი სამართლებლივი დოკუმენტები, შეთანხმებები და კანონები მოითხოვენ თანამშრომლობის დაჩქარებას.

7.8. სპეციალური დებულებები: ურთიერთდახმარება მონაცემების ხელში ჩაგდებასთან დაკავშირებით

ამ საკითხს ორი დებულება ეხმიანება, კერძოდ, 33-ე მუხლი, რომელიც მოიცავს ქსელური ტრაფიკის მონაცემების რეალურ დროში შეგროვებას და 34-ე მუხლი, რომელიც შინაარსობრივი ინფორმაციის ხელში ჩაგდებას ეხება. ვინაიდან შინაარსობრივი ინფორმაციის ხელში ჩაგდება მაღალი დონის ჩარევად კვალიფიცირდება, ურთიერთდახმარება ამ კუთხით შეზღუდულია და ექვემდებარება უსაფრთხოების კანონებს, ასევე სხვა ხელშეკრულებებსა და სამამულო კანონმდებლობას.

მუხლი 33 – ურთიერთდახმარება ქსელური ტრაფიკის მონაცემთა რეალურ დროში შეგროვებასთან დაკავშირებით

1 მხარეები ვალდებული არიან დახმარება გაუწიონ ერთმანეთს ქსელური ტრაფიკის მონაცემთა რეალურ დროში შეგროვებაში, რომელიც უკავშირდება კონკრეტულ ოპერაციებს მონაცემთა გადაცემასათან დაკავშირებით, რომელმიც მათი ტერიტორიაზე კომპიუტერული სისტემის მეშვეობით განხორციელდა. მე-2 პუნქტის დებულებების შესაბამისად, აღნიშნული თანამშრომლობა რეგულირდება სამამულო კანონმდებლობის პირობებითა და პროცედურებით.

2 ყველა მხარე ვალდებულია ითანამშრომლოს ამ კუთხით, იმ შემთხვევაში მაინც, როდესაც სახეზეა სისხლის სამართლის დანაშაული და რომლის დროსაც ქსელური ტრაფიკის მონაცემთა რეალურ დროში შეგროვება დასაშვებია მსგავსი სამამულო დანაშაულის შემთხვევაში.

მუხლი 34 – ურთიერთდახმარება შინაარსობრივი მონაცემების ხელში ჩაგდებასთან დაკავშირებით

მხარეები ვალდებული არიან დახმარება გაუწიონ ერთმანეთს რეალურ დროში მონაცმების შეგროვებაში ან შინაარსობრივი ინფორმაციის ჩაწერის საქმეში, როდესაც კონკრეტული ოპერაცია კომპიუტერული სისტემით ხორციელდება, იმდენად რამდენადაც ამას მოქმედი საერთაშორისო ხელშეკრულებები და სამამულო კანონმდებლობა უშვებს.

7.9. სპეციალური დებულება: 24-სათიანი ქსელის ფუნქციონირება

ოპერაქტიული რეაგირების უზრუნველსაყოფად, განსაკუთრებით იმ შემთხვევაში, როდესაც საკითხი სხვა ქვეყანაში არსებული მონაცემების შენახვას ეხება, კონვენციის[311] 25-ე მუხლის შესაბამისად შეიქმნა 24-საათიანი ქსელი. ყველა მხარე ვალდებულია დააარსოს საკონტაქტო პუნქტი გადაუდებელი საკითხების მოსაგვარებლად. აღნიშნული პუნქტი დამატებითია და არ არის მოწოდებული ჩაანაცვლოს თანამშრომლობის რომელიმე უკვე მოქმედი არხი.

მუხლი 35 – ოცდაოთხსაათიანი ქსელი

1 ყველა მხარე ვალდებულია დააარსოს 24-საათიანი საკონტაქტო პუნქტი, რომელიც კვირაში 7 დღე იმუშავებს. ეს საჭიროა, რათა ოპერატიულად განხორციელდეს დახმარება გამოძიების ან მოკვლევის განხორციელების დროს სისხლის სამართლის ისეთ დანაშაულებებთან დაკავშირებით, რომელიც დაკავშირებულია კომპიუტერული სისტემებისა და მონაცემების გამოყენებასთან, და ელექტრონულ ფორმაში არსებული მტკიცებულებების შეგროვებასთან. დახმარება გულისხმობს ქვემოთ ჩამოთვლილ ღონისძიებებში მხარდაჭერას ან უშუალო მონაწილეობას, თუ სამამულო კანონმდებლობა და პრაქტიკა ამას უშვებს:

ა ტექნიკური დახმარების გაწევა;

ბ 29-ე და 30-ე მუხლების შესაბამისად მონაცემთა შენახვა;

გ მტკიცებულებების შეგროვება, სამართლებლივი ინფორმაციის მიწოდება და ეჭვმიტანილთა მოძებნა.

2 ა ერთი მხარის მიერ დაარსებულ საკონტაქტო პუნქტს ოპერატიული კავშირი უნდა ჰქონდეს მეორე მხარის საკონტაქტო პუნქტთან.

ბ თუ აღნიშნული პუნქტი არ წარმოადგენს ამ მხარის ორგანოს ან ორგანოების შემადგენელ ნაწილს, რომელიც პასუხისმგებელია საერთაშორისო ურთიერთდახმარებაზე ან ექსტრადიციაზე, საკონტაქტო პუნქტი ვალდებულია აღნიშნულ ორგანოსთან ან ორგანოებთან უზრუნველყოს ოპერატიული კოორდინაცია.

3 ქსელის გამართული ფუნქციონირების უზრუნველსაყოფად, თითოეული მხარე ვალდებულია სათანადოდ მოამზადოს და აღჭურვოს პუნქტის პერსონალი.

[311] აღნიშნული დებულება დიდი რვიანის მაღალტექნოლოგიური დანაშაულის ქვე-ჯგუფის გამოცდილებას ეფუძნება, რომელმაც მსგავსი ქსელი ჯერ კიდევ 1997 წელს დააარსა.

8. დანართი

8.1. პრაქტიკული მაგალითები

არასანქცირებული შეღწევა: kgb ქსელის გატეხვა

1986 წელს, როდესაც ქსელური სისტემა, რომელსაც დღეს ინტერნეტი ეწოდება, ერთმანეთს ძირითადად სამეცნიერო და სამხედრო უწყებების კომპიუტერებს აკავშირებდა, გერმანელ კომპიუტერულ ენთუზიასტთა ჯგუფმა ჰანოვერიდან მცირე პროგრამის, სახელწოდებით *movemail-ი,* უსაფრთხოების სისტემაში დეფექტი აღმოაჩინა. ამ დეფექტის წყალობით მათ შეაღწიეს შორეულ კომპიუტერში და მის ფაილთა სისტემაში, ამგვარად, მათ შეეძლოთ წაეკითხათ და გადმოეწერათ ფაილები. ჯგუფმა, რომელიც *კარლ კოხის, მარკუს ჰესისა და დირკ ბრეჩინსკის* ირგვლივ შეიკრიბა, ისარგებლა პროგრამული უზრუნველყოფის დაუცველობით და არსებული ქსელის ურთიერთკავშირით უკავშირდებოდა და იკვლევდა მსოფლიოს სხვადასხვა კომპიუტერულ სისტემას; ზოგიერთი მათგანი კალიფორნიის უნივერსიტეტს (ბერკლიში), ნასა-სა და პენტაგონსაც კი ეკუთვნოდა.

გერმანელ ჰაკერთა ჯგუფმა გადაწყვიტა თავისი აღმოჩნა მოგების წყაროდ გაეხადა. მათ ისარგებლეს იმ ფაქტით, რომ მსოფლიოში მძვინვარებდა ცივი ომი, დაუკავშირდნენ საბჭოთა კავშირის საიდუმლო სამსახურს, კგბ-ს, აღმოსავლეთ ბერლინში და გარკვეული საზღაურის სანაცვლოდ შესთავაზას მათ მიერ ამერიკის შეერთებული შტატების კომპიუტერულ სისტემაში აღმოჩენილი საიდუმლო ინფორმაცია. გარკვეული სჯა- ბაასის შემდეგ შეთახმდნენ, რომ ჰაკერები წარმოადგენდნენ თავიანთი წინადადების ნიმუშს. მომდევნო რამდენიმე თვის განმავლობაში ჰაკერებმა კგბ-ს მუშაკებს ათეულ-ათასი გერმანული მარკის სანაცვლოდ გარკვეული საიდუმლო ინფორმაცია მიაწოდეს.

1987 წელს, ლორენს ბერკლის ეროვნულ ლაბორატორიაში სისტემის ადმინისტრატორად მუშაობდა *კლიფორდ შტოლი,* რომელმაც ფარდა ახადა ამ ავანტიურას. ერთხელ მან აღმოაჩინა, რომ დახარჯული იყო 0.75 ცენტის ღირებულების კომპიუტერული დრო, რომელიც კომპიუტერის მოსარგებლეს არ ჰქონდა გამოყენებული. ამ გზით მან მიაგნო, რომ ვიღაც უკანონოდ სარგებლობდა იმ კომპიუტრერული სისტემით, რომელზედაც თვითონ იყო პასუხისმგებელი. დამნაშავეების აღმოჩენის მიზნით *შტოლმა* აქტიურად ითანამშრომლა გერმანულ და ამერიკულ ორგანოებთან. სააბონენტო პაკეტის მონაცემებმა კვალი მარკუს *ჰესთან* მიიყვანა.

ჰესი და ბრეჩინსკი გაასამართლეს და სისხლის სამართლის კოდექსის დარღვევისათვის პირობითი სასჯელი მიუსაჯეს. ამ დროისათვის კოდექსი მათ მიერ ჩადენილ დანაშაულს ჯაშუშობის კვალიფიკაციას აძლევდა და მათი ქმედება 1986 წელს საბჭოთა კავშირის სასარგებლოდ ჩადენილ ჯაშუშობად ჩაითვალა. ვინაიდან *კოხმა* ითანამშრომლა გამოძიებასთან, იგი სასჯელისაგან გაათავისუფლეს, თუმცა მოგვიანებით იგი მიეძალა ნარკოტიკებს, ფსიქიკა მოეშალა და სიცოცხლა თვითმკვლელობით მან მანამ დაასრულა სანამ მის თანამზრახველებს განაჩენს გამოუტანდნენ. ჰაკერობის ამ საქმემ მსოფლიოს ყურადღება მიიპყრო და იგი ჩაითვალა პირველ საერთაშორისო კომპიუტერულ დანაშაულად. ამ შემთხვევამ თვალნათლივ აჩვენა თუ რამდენად დაუცველია ქსელური სისტემები და მასში შენახული ინფორმაცია, და რამდენად უმნიშვნელოა საინფორმაციო საშუალებების საუკუნეში გეოგრაფიული მანძილები.

თავი 3.2 – ინფორმაციის უკანონოდ ხელში ჩაგდება: TJX მონაცემთა ქურდობა

TJX-ი წარმოადგენს ცნობილ ამერიკულ მაღაზიათა ქსელის TJ Maxx-ის შვილობილ კომპანიას, რომელიც თავის მხრივ უდიდესი საცალო ობიექტია. იგი და მისი მომხმარებლები მონაცემთა უზარმაზარი ქურდობის მსხვერპლი გახდნენ. 2005- 2007 წწ თითქმის 100 მილიონამდე საკრედიტო ბარათების ნომრები მოიპარეს ინფორმაციის უკანონო გზით ხელში ჩაგდების წყალობით. ჰაკერთა ჯგუფმა, რომლესაც სათავეში *ალბერტ გონსალესი* ედგა, ხელში ჩაიგდო რამდენიმე პერსონალური კომპიუტერის ინფორმაცია და კომპანიის ქსელით შეუმჩნეველად სულ მცირე შვიდი თვის განმავლობაში სარგებლობდა.

ჰაკერთა ოპერაციის ცენტრში ჩაყენებული იყო პასიური მიყურადების მოწყობილობა, რომელიც ფაქტობრივად იყო პროგრამა, რომელიც ხელში იგდებდა ქსელით გადაცემულ

მონაცემთა ნაკადს. ბოროტმზრახველებმა აღმოაჩინეს, რომ სხვადასხვა ინფორმაციასთან ერთად TJX-ი ფინანსური მომსახურების სამსახურებს უსადენო ქსელით გადასცემდა საკრედიტო ბარათების ნომრებს. უფრო მეტიც, საკრედიტო ბარათების ნომრები სუსტი მოძველებული კოდირებული სისტემით იყო დაცული. ჯგუფმა *გონსალესის* ხელმძღვანელობით ისარგებლა ამ ფაქტით და TJX-ის კომპიუტერებში ჩაამონტაჟა პასიური მიყურადების მოწყობილობა. მოწყობილობა „ყურს უგდებდა“ უსადენო ქსელს და მომენტალურად იწერდა ინფორმაციას.

რეიდის დროს და მის შემდეგ, საკრედიტო ბარათების ნომრები იყიდებოდა დახლს ქვემოდან ე.წ. ‚მებარათეებზე’ ანუ იმ პირებზე, რომლებიც ყალბ საკრედიტო ბარათებს აწარმოებდნენ, ხოლო შემდეგ თანხებს ბანკომატებიდან ხსნიდნენ. ამბობენ, რომ ამ გზით TJX-ის ჰაკერებმა მილიონ დოლარზე მეტი იშოვეს. 2008 წელს დაადგინეს ვინ იყვნენ ისინი და დააპატიმრეს; ჯგუფი შედგებოდა ამერიკის შეერთებული შტატების სამი მოქალაქისაგან, სამი უკრაინისა და ორი ჩინეთის მოქალაქისაგან, მასში ასევე გაერთიანებული იყვნენ ბელარუსისა და ესტონეთის მოქალაქეები. 2009 წლის ზაფხულში, ჯგუფის ხელმძღვანელმა *გონსალესმა* აღიარა დანაშაული და მას 15-დან 25 წლამდე პატიმრობა მიესაჯა.

აღნიშნული ინციდენტის შედეგად TJX-მა 1.7 მილიარდი დოლარი ზარალი განიცადა. აღნიშნული ქურდობის გამო გადამხდელი ბარათების ინდუსტრიის უსაფრთხოების სტანდარტების საბჭოს მოუწია მითითებებისა და სტანდარტების შემუშავება, რომელიც სავალდებულოა აშშ-ს ყველა კომპანიისათვის, რომელიც ოპერაციებს საკრედიტო ბარათებით ახორციელებს.

მონაცემთა ურთიერთქმედება: სიყვარულის ვირუსი

საბედნიეროდ, მიუხედავად იმისა, რომ ნაწინასწარმეტყველი იყო, რომ 21 –ე საუკუნე დიდ პრობლემებს მოუტანდა მსოფლიოს, ციფრულმა სამყარომ მშვიდობიანად შეაბიჯა მესამე ათასწლეულში. თუმცა ამ სიმშვიდემ დიდხანს არ გასტანა: რამდენიმე საათში მსოფლიოში გავრცელდა საშინელი პროგრამა, რომელმაც კომპიუტერებს ისეთი ზიანი მიაყენა, რომელსაც ვერავინ წარმოიდგენდა. *სიყვარულის ვირუსი*, იგივე *სასიყვარულო წერილის ვირუსი*, იგივე *მე შენ მიყვარხარ ვირუსი* ფილიპინებში შეიქმნა და იქიდან გავრცელდა. პირველად იგი 2000 წლის 4 მაისში გამოჩნდა და სულ რაღაც ერთ დღეში მსოფლიოს მასშტაბით მან დააზიანა ინტერნეტში ჩართული ყველა კომპიუტერი.

ვირუსი თავისთავად შედგებოდა ვიზუალური საბაზო ტექსტისაგან, ანუ მცირე ზომის კომპიუტერული კოდისაგან, რომელიც იყენებდა „მაიკროსოფტ ვინდოუსის“ ოპერატიულ სისტემაში არსებულ უსაფრთხოების დეფექტს. ვირუსი წარმოდგენილი იყო, როგორც სასიყვარული წერილი, რომელიც თან ერთვოდა იმეილს, ხოლო წერილის გულუბრყვილო მიმღები დანდობილად აჭერდა ღილაკს დანართის გასაცნობად. თუ მოხდებოდა ამ წერილის გააქტიურება, ვირუსი ავტომატურად აგზავნიდა მსგავს იმეილებს ინფიცირებული კომპიუტერის მისამართების წიგნში არსებულ ყველა მისამართზე. სწორედ ამით აიხსნება ამ ვირუსის გავრცელების ამგვარი სწრაფი ტემპები. უფრო მეტიც, ამ ვირუსის ზემოქმედებით იშლებოდა მულტიმედიური ფაილები, მაგ., MP3 სიმღერები და JPG სურათები და მათ ადგილას თვითონ რჩებოდა და იმ სახელს ირქმევდა, რაც მის მიერ წაშლილ ფაილებს ჰქონდა. ვინაიდან ეს ვირუსი პროვოცირებას უკეთებდა ქსელური ტრაფიკის უსაზღვროდ დიდ მოცულობებს, იგი აზიანებდა ფოსტის სერვერებსა და სხვა სისტემებს, რის გამოც ისინი გამოდიდოდნენ მწყობრიდან, ხოლო შენახული ფაილები დროებით მოუწვდომელი ხდებოდა.

უპრეცედენტო ზიანი მიაყენა აღნიშნულმა ვირუსმა საინფორმაციო საშუალებებს: ინტერნეტში ჩართული კომპიუტერების თითქმის 10 პროცენტი დაზიანდა; ბეჭდური მედიის გამოცემები მკითხველებისათვის მხოლოდ მწირი ინფორმაციის მიწოდებას ახერხებდა, ხოლო საფოსტო სერვერები სახელმწიფო სტრუქტურებში, პარლამენტსა და საერთაშორისო კომპანიებში მწყობრიდან გამოვიდა. დაუდასტურებელი ინფორმაციით

სასიყვარულო ვირუსით მიყენებულმა ზარალმა სულ 5.5 მილიარდ აშშ დოლარს გადააჭარბა.

„მალვეარ“ ექსპერტებმა სწრაფად დაადგინეს, რომ წყარო ფილიპინებში იყო და ეფ-ბი-აის, ადგილობრივი ხელისუფლებისა და ინტერნეტ პროვაიდერების დახმარებით გამოავლინეს ის ადამიანები, რომელთაც შექმნეს და გაავრცელეს სიყვარულის ვირუსი. მიუხედავად იმისა რომ ჩხრეკის ორდერი დროზე იქნა გაცემული, დამნაშავეები არ წარდგნენ სასამართლოს წინაშე, ვინაიდან 2000 წელს პილიპინების სისხლის სამართლის კანონი არ ითვალისწინებდა დებულებას, რომელიც ზემოთ აღწერილ ქმედებას დასჯადი დანაშაულის კვალიფიკაციას მიანიჭებდა.

სისტემაში ჩარევა: „ლუფტანზას“ ბლოკადა

ვირტუალური „მჯდომარე“ გაფიცვის დემონსტრაცია თუ სისტემაში ჩარევა? ეს კითხვა დღის წესრიგში 2001 წელს გერმანიაში დადგა, როდესაც უფლება დამცველთა ჯგუფი დაუპირისპირდა გერმანულ ავიახაზების კომპანიას „ლუფტანზას“. „ლუფტანზა“ მგზავრთა გადაყვანის გარდა ასევე ახორციელებს იმ პირთა დეპორტაციას, რომელთაც ქვეყანაში დარჩენის უფლება არ აქვთ. „ლიბერტად!“-ში გაერთიანებული ჯგუფი გამოდიოდა ზოგადად დეპორტაციის და კონკრეტულად „ლუფტანზას“ მიერ დეპორტაციის განხორციელების წინააღმდეგ; მათ შეარჩიეს დღე, როდესაც ტარდებოდა „ლუფტანზას“ აქციონერთა ყოველწლიური შეკრება და ბლოკირება გაუკეთეს კომპანიის ვებსაიტს. ამით მათ აღნიშნულ საკითხთან დაკავშირებით საკუთარი კრიტიკული დამოკიდებულება გამოხატეს.

„ლიბერტად!“-ის წარმომადგენლებმა გაავრცელეს „ფლაიერები“, რომელშიც მითითებული იყო საკუთარი ვებსაიტის მისამართი და აღწერილი იყო დაგეგმილი აქციის მიზეზი. მათი ვებსაიტის მეშვეობით ნებისმიერს შეეძლო ჩამოეტვირთა პროგრამა, რომლის მეშვეობით კონკრეტულ დროს რამდენჯერმე ავტომატურად უკავშირდებოდნენ ვებსაიტს lufthansa.com. „ლიბერტად!“-ის მოწოდებას 13.000 ადამიანი გამოეხმაურა. ისინი პროგრამის მეშვეობით ან დამოუკიდებლად უკავშირდებოდნენ lufthansa.com. –ს; შედეგად „ლუფტანზას“ ვებსაიტზე განხორციელდა თავდასხმა, რის გამოც საიტი უარს ამბობდა მომსახურებაზე. მიუხედავად იმისა, რომ კომპანიისათვის ცნობილი იყო ამ აქციის შესახებ, სერვერის დამატებით გაძლიერებამ ვერ გაუძლო დატვირთვას და ჩაიკეტა. შესაბამისად, „ლუფტანზას“ კლიენტები ვერ ახერხებდნენ ბილეთების დაჯავშნასა და რეისების შესახებ ინფორმაციის მიღებას; კომპიუტერული სისტემის ნაწილობრივი ფუნქციონირება მხოლოდ ორ საათს გაგრძელდა.

მართალია, „ლიბერტად!“-მა აღნიშნული აქციით საკუთარი პროტესტის დემონსტრირება მოახდინა და, გარდა ამისა, ეს აქცია შეთანხმებული იყო გერმანიის ადმინისტრაციულ ხელისუფლებასთან, მაგრამ „ლუფტანზამ “ არ გაიზიარა მათი პროტესტის პოლიტიკური შეხედულება და „ლიბერტად!“-ის მფლობელის დომეინის წინააღმდეგ სისხლის სამართლის სარჩელი შეიტანა. 2005 წელს, ადგილობრივმა რაიონულმა სასამართლომ მოპასუხე ძალადობასა და სხვების წახალისებაში – ჩაედინათ კანონსაწინააღმდეგო ქმედებები დაადანაშაულა. თუმცა, 2006 წელს, რეგიონულმა სააპელაციო სასამართლომ გაამართლა მოპასუხე. კრიტიკა მოყვა ორივე განაჩენს: ერთი მხრივ, ადგილობრივმა რაიონულმა სასამართლომ არ გაითვალისწინა №303ა/ბ StGB, გერმანიის სისხლის სამართლის ძირითადი კოდექსის დებულებები, რომელიც კიბერ –დანაშაულის კონვენციის მე-5 მუხლს შეესაბამება, ხოლო რეგიონულმა სააპელაციო სასამართლომ ისეთი დროებითი ინტერპრეტირება გაუკეთა მონაცემთა ჩახშობის ელემენტს, რის გამოც დანაშაული დასჯადად არ ჩათვალა. კრიტიკოსებმა განაცხადეს, რომ თავდასხმა ვებსაიტზე, რის შედეგად მომსახურება ვერ განხორიცელდება არა დასჯადი გახდებოდა, თუ სააპელაციო სასამართლოს შეხედულებას მიიღებდნენ.

მოწყობილობების არასწორად გამოყენება: თვითგაკიცხვა გერმანიაში

გერმანია თავს იწონებს, რომ მას აქვს საინფორმაციო ტექნოლოგიების უსაფრთხოების დემონსტრირების დიდი ხნის ტრადიცია, ე.წ. „თეთრი ქუდის“ ჰაკერობა, ანუ სისტემებისა და პროგრამების შემოწმება დეფექტების გამოვლენის მიზნით, რათა შემდეგ მოხდეს მათი აღმოფხვრა კლიენტების ჭეშმარიტი ინტერესების დაცვის მიზნით. ამიტომ იყო, რომ კიბერ- დანაშაულის კონვენციის მე-6 მუხლის მიღებამ და მისმა შეტანამ გერმანიის სისხლის სამართლის კოდექსში №202 გ StGB, მწვავე კამათი გამოიწვია. Chaos Computer Club-ისა და საინფორმაციო ტექნოლოგიების უსაფრთხოების პროფესიონალთა მხრიდან წინააღმდეგობა პროვოცირებულია იმით, რომ ის უკავშირდებოდა მუხლის ორგვარ წაკითხვას.

მულტი-მედიის ინსტრუმენტი ტიპიური პროგრამული უზრუნველყოფაა, რომლითაც სარგებლობენ საინფორმაციო ტექნოლოგიების პროფესიონალები და თეთრ-ქუდიანი ჰაკერები, როდესაც ისინი იქცევიან, როგორც თავდამსხმელი ან ბოროტმზრახველი და ხშირად ამგვარი მოქმედება ერთადერთი გზაა იმის შესამოწმებლად თუ რამდენად ეფექტიანად მუშაობს უსაფრთხოებოს ზომები. მაშინ როცა კიბერ- დანაშაულის შესახებ კონვენციაში საუბარია იმ მოწყობილობებსა და კომპიუტერულ პროგრამებზე, რომელიც *უპირველეს ყოვლისა* დანაშაულის ჩადენის მიზნით შეიქმნა, №202 გ StGB მიხედვით კი დასჯადია დანაშაულისათვის მზადება, როდესაც ხდება პროგრამული უზრუნველყოფის შეთავაზება ან შეძენა, *რომლის მიზანია მსგავსი დანაშაულის* ჩადენა. კრიტიკოსები მიიჩნევენ, რომ მასში ცალსახად არ არის ჩამოყალიბებული, რომ ამ მოწყობილობების უსაფრთხოების მიზნებისათვის გამოყენება არ ჩაითვალოს დანაშაულად, რაც საფრთხის წინაშე აყენებს ნებისმიერ პირს, რომლიც კომპიუტერული სისტემების უსაფრთხოების სფეროში მუშაობს, რის გამოც ამ დებულებამ შეიძლება უარყოფითი ზემოქმედება იქონიოს მთლიანად ამ სფეროს განვითარებაზე.

როგორც კი კანონში ცვლილება შეიტანეს, და კანონი ძალაში შევიდა, საინფორმაციო ტექნოლოგიების ჟურნალის iX's მთავარმა რედაქტორმა *იურგენ ჩიგერმა* და ამავე სფეროში მომუშავე მეწარმემ *ჰერბერტ ტრაინენმა*, თვითგაკიცხვა გამოაცხადეს და მიმართეს ძალოვან უწყებებს თხოვნით დაესაჯათ ისინი რათა შექმნათ იურიდიული მტკიცებულება იმისა, რომ მათ სფეროში საქმიანობა უკანონო გახდა. თუმცა მათი სარჩელი დაკმაყოფილებული არ იქნა, ვინაიდან ნებაყოფილობითი განზხრახვა მათ ქმედებაში არ დადასტურდა. კიდევ ერთი სარჩელი გერმანიის მთავრობის საინფორმაციო ტექნოლოგიების უსაფრთხოების ოფისის *Bundesamt für Sicherheit in der Informationstechnik (BSI)* წინააღდეგ აღიძრა. *BSI* სთავაზობდა მომხმარებელს ინსტრუმენტების ნაკრებს, რომელიც მათი ვებსაიტიდან შეიძლებოდა ჩამოეტვირთათ და რომელიც შეიცავდა „ჯეკ გამომფატვრელს“, კოდური სიტყვის გატეხვის ინსტრუმენტს, რომელიც გარკვეული დროის წინ საკმაოდ პოპულარული იყო. ამჯერადაც სარჩელი არ დაკამყოფილდა დანაშაულის მომზადების ნებაყოფილობითი განზრახულობის არ არსებობის გამო.

დაბოლოს, გერმანიის კონსტიტუციურმა სასამართლომ არ დააკმაყოფილა რამდენიმე კონსტიტუციური სარჩელი, რომელიც 2009 წელს №202გ StGB-ს წინააღდეგ იქნა შეტანილი; ვინაიდან არ დაკმაყოფილება ფორმალური სამართლებლივი მოთხოვნილებებიდან გამომდინარეობდა, სასამართლოს არ დასჭირებია ძირითადი არგუმენტების დაკმაყოფილება და, სამწუხაროდ, არც იურიდიული მითითებები არ გამოუცია, სადაც განმარტებული იქნებოდა ტერმინი *მიზანი*.

კომპიუტერთან დაკავშირებული ფალსიფიკაცია: „ფიშინგი“

კრიმინალურ ქმედებათა ერთობლიობა, რომელსაც ხშირად „ფიშინგს“ უწოდებენ, უნდა განიხლულ იქნეს როგორც ფენომენი და არა როგორც ერთ -ერთი შემთხვევა. ეს ფაქტი იმით არის განპირობებული, რომ „ფიშინგი“ სულ უფრო ფართომასშტაბიან სახეს იღებს. თუ 2003-2004 წლებში „ფიშინგი“ მარტივად ხელით კეთდებოდა, ამჟამად იგი სულ უფრო მეტ პროფესიულობას იჩენს და ამჟამად პროგრამული უზრუნველყოფის ისეთი ნაკრებიც კი იშოვება, როგორიცაა *„როკ ფიში“*. *„როკ ფიში“* ავტომატიზირებულია და მისი მოხმარება საქმეში ნაკლებად

ჩახედული ადამიანებსაც შეუძლიათ, ისე რომ დეტალებში არ არ იყონ გათვითცნობიერებულები; საჭიროების შემთხვევაში ამ პროგრამით მოვაჭრე ორგანიზაციები დახმარებას „ჩატის“ სესიების მეშვეობითაც სთავაზობენ. გამოძიებამ აშშ-სა და ევროპის ქვეყნებში ცხადყო, რომ *„ფიშინგი“* ჯერ კიდევ აღმავლობის ტენდენციით ხასიათდება, რაც იმით არის გამოწვეული, რომ *„ფიშინგი“* აღარ წარმოადგენს ტექნიკურ სირთულეს.

მართალია, *„ფიშინგი“* ავტომატიზირებულია, იგი მაინც მოითხოვს გარკვეული ფალსიფიკაციების გაკეთებას. დასაწყისში იქმნება იმეილი იმისათვის, რომ წერილის მიმღები წერილის ავთენტურობაში დაარწმუნოს და იმაში, რომ იგი ნამდვილად იმ ბანკიდან მოვიდა, სადაც წერილის მიმღებს ანგარიში აქვს გახსნილი, შემდეგ წერილში ითხოვენ თითი დააჭირონ „ლინქს“, რომელიც ვითომდა უსაფრთხოების შესამოწმებლად არის. ამვდროულად, ვებსაიტი ისეთ დომეინში უნდა იყოს, რომელიც მსხვერპლის ეჭვს არ გამოიწვევს. ამისათვის იყენებენ ბანკის ოფიციალურ ლოგოებს, ხოლო ბანკის ვებსაიტი იმდენად ახლოს არის ორიგინალთან იმიტირებული, რომ თითქმის უნაკლოა. არსებობს *„ფიშინგის“* სხვა მაქინაციები, როდესაც ტროას ცხენებს იყენებენ, ანუ „მალვეარს“ (ბოროტების მომტანი პროგრამა) იმეილისა და ვებსაიტის ნაცვლად. ამგვარი პროგრამის გამოყენების დროს ხდება მსხვერპლის კომპიუტერსა და ბანკის ვებ სერვერს შორის კავშირის დამყარება და მონაცემთა ნაკადის მომენტალური შეცვლა. ამგვარი შემთხვევის დროს ამოქმედდება კიბერ-დანაშაულის შესახებ კონვენციის სხვა მუხლები.

კომპიუტერთან დაკავშირებული გაყალბება: საუკეთესო განაკვეთის ნომრის ამკრეფი

საუკეთესო განაკვეთის მქონე ნომრის ამკრეფები ძალიან პოპულარული იყო 1990-იანი წლების ბოლოს. პროვაიდერები მომხმარებელს სატელეფონო გადასახადით ახდევინებდნენ მომსახურების საზღაურს და თავს არიდებდნენ საკრედიტო ბარათის მონაცემების ვებსაიტზე განთავსებას. ნომრის ამკრეფი, როგორც წესი, მცირე კომპიუტერული პროგრამის ან „სცენარის“ (სკრიპტი) მსგავსად მუშაობს, რომელსაც დამატებით აქვს ქსელთან კავშირი და კრეფს საუკეთესო განაკვეთის მქონე ნომერს. თუმცა ნომრის ამკრეფმა მალე „თავი შეირცხვინა“. გამყალბებლებმა ისარგებლეს იმ ფაქტით, რომ ნომრის ამკრეფის პროგრამის დაპროგრამება შეიძლებოდა, რის შედეგად მას უჩუმრად შეეძლო სტანდარტული კავშირის პარამეტრები საუკეთესო განაკვეთის ნომრით შეეცვალა. ამგვარად, ამკრეფი მანიპულირებდა მსხვერპლის სისტემით, რის შედეგად ამ უკანასკნელს ტელეფონის უზარმაზარი გადასახადი მოსდიოდა. ფართოზოლიანი კავშირების (DSL) გავრცელებასთან ერათად, ნომრის ამკრეფთან დაკავშირებული შემთხვევების რაოდენობა შემცირდა.

რაც შეეხება აუქციონთან დაკავშირებულ მაქინაციებს საიტზე, როგორიც არის მაგალითად „eBay“, კომპიუტერული მაქინაციები აქ

არ გამოიყენება. ინტერნეტ კავშირის დროს, აუქციონის პლატფორმის ვებსაიტი და ინფორმაციის აუქციონზე შეტანა შეიძლება გამოყენებული იქნეს კრიმინალური ქმედებებისათვის, მსხვერპლის როგორც ფიზიკური პირის შეცდომაში შეყვანა მაქინაციის კვლავ აუცილებელი ელემენტია, რასაც ფატალურ ფასამდე მივყავართ. ამგვარად, აუქციონთან დაკავშირებული ნებისმიერი დანაშაული იფარება გაყალბების ტრადიციული დებულებებით.

ბავშვთა პორნოგრაფია: ოპერაცია მერსი

გასული საუკუნის 90-იანი წლებიდან, ბავშვთა პორნოგრაფიის კომერციული ვებსაიტების წინააღმდეგ წამოწყებული კამპანიის გამო, რომლის დროსაც კიბერ-პოლიციელები მუდმივად აკონტროლებდნენ ქსელებს – მსგავსი სპეციალური განყოფილებები მრავალ ქვეყანაში შეიქმნა – ბავშვთა პორნოგრაფიით მოსარგებლე კლიენტებს სხვა გზების მოძებნა მოუხდათ. ეს ფაქტი დააფიქსირა „ოპერაცია მერსიმ“, რომელიც წარმოადგენს ფართომასშტაბიან ინტერნეტულ გამოძიებას. ოპერაცია დაიწყო 2002 წელს და გამოავლინა 166 ქვეყნის დაახლოებით 25.000 ეჭვმიტანილი. აღნიშნულმა აღმოჩენამ სერიოზული გამოხმაურება მიიღო მედიაში, მას შემდეგ რაც 2003 წელს გამოქვეყნდა ორგანიზაციის პირველადი შედეგები.

„ოპერაცია მერსი“ მას შემდეგ ამოქმედდა, რაც მინიშნების დონეზე ცნობილი გახდა, რომ ინტერნეტში იყო ფორუმები, რომელიც ბავშვთა პორნოგრაფიულ სურათებს შეიცავდა. პოლიციის გამოძიების შედეგად ნელ-ნელ გამოვლინდა 38 კერძო წრე, სადაც გაწევრიანებული იყვნენ ადამიანები მსოფლიოს სხვადასხვა ქვეყნიდან და სადაც ხდებოდა უკანონო მასალის ერთმანეთთს შორის გაცვლა. ეჭვმიტანილები პაროლით დაცულ ვებ ფორუმებს იყენებდნენ. ამ გვერდზე შესვლის უფლებას მომხმარებელი მხოლოდ მას შემდეგ იღებდა, რაც მოხდებოდა მისი შემოწმება. ამისათვის გაწევრიანების ახალ მსურველებს უნდა წარმოედგინათ მათ ხელთ უკვე არსებული პორნოგრაფიული მასალა, რაც მათი ერთგულების უტყუარობის მტკიცებულება იქნებოდა. ზოგჯერ ფორუმი მხოლოდ კონტაქტის დასამყარებლად გამოიყენებოდა, ხოლო მასალის გადაცემა ინტერნეტის მიღმა ხორციელდებოდა ხოლმე.

„ოპერაცია მერსის“ წარმატება განაპირობა ერთ-ერთი საერთაშორისო პროვაიდერის პოლიციასთან თანამშრომლობამ, რომელმაც პოლიციას 26.500 გამოსახულებიანი ფაილი, 38.000 ელექტრონული ფოსტის მისამართი და 12 გიგაბაიტის მოცულობის ლოგ-ფაილების 14 მილიონი ჩანაწერის მასალა გადასცა. ოპერაციას იმ პირველი ეჭვმიტანილის სახელი ეწოდა (მარსელი), რომლიც დომინოს პირველი ქვა აღმოჩნდა და რომელსაც ეჭვმიტანილთა უპრეცედენტოდ დიდი რაოდენობა მოყვა, რომელიც კი კომპიუტერულ დანაშაულთა გამოძიებაში ოდესმე გამოვლენილა.

ინტელექტუალური საკუთრება: FTPWelt.com

ციფრულმა ტექნოლოგიებმა და მონაცემთა ფართოზოლიანმა კავშირებმა ხელი შეუწყო ნებისმიერი სახის ინფორმაციის უდანაკარგო გადაწერებსა და სწრაფ გადაცემას. მანამ სანამ გაცხარებული დებატები მიმდინარეობდა იმასთან დაკავშირებით თუ რა ზარალი მოაქვს ახალგაზრდების უსაყვარლეს დროის ტარებას – მუსიკის გადმოტვირთვას – მედია ინდუსტრიისათვის, ადამინთა ერთმა ჯგუფმა სიმღერების, ფილმების, თამაშებისა და პროგრამების გამოყენება ციფრული საშუალებების წყალობით კიდევ უფრო მაღალ დონეზე აიყვანა: ისინი მომხმარებლებს სთავაზობდნენ „პირატულ“ მუსიკას, ჰოლივუდის უახლეს ბლოკბასტერებსა და მოპარულ კომპიუტერულ პროგრამებს (warez), ხოლო სანაცლოდ ან თვიურ ან ერთჯერად გადასახადს ითხოვდნენ. ტექნოლოგიური რევოლუციით დამნაშავეებმაც ისევე ისარგებლეს, როგორც ახლგაზრდებმა ზემოთ აღწერილ შემთხვევაში.

ერთ-ერთი ასეთი პირატული და მოპარული კომპიუტერული პროგრამების საიტი FTPWelt.com –ი იყო. ამ საიტის ოპერატორებს ახლო კონტაქტები ჰქონდათ ე. წ. გამომშვებ ჯგუფებთან, რომლებიც კონკურენციას უწევდნენ ერთმანეთს თუ რომელი უფრო ადგრე გამოუშვებდა გატეხილ კომპიუტერულ პროგრამას ან ახალ ფილმს, მანამ სანამ ისინი მაღაზიებსა თუ კინოთეატრებში გამოჩნდებოდნენ. ეს ხდებოდა შესაძლებელი კინოთეატრების მომსახურეთა მოსყიდვით. FTPWelt.com –ი თავის მომხმარებელს ყველა სახის კომპიუტერულ პროგრამასა და მედია ფაილებს სთავაზობდა, რომელიც ნიდერლანდებში, აშშ-სა და რუსეთში ნაქირავებ საიმედო და სწრაფ FTP სერვერებზე იყო განთავსებული, რათა მომხმარებელს მაღალი ხარისხის პროდუქტი მიეღო. იყო მომენტები, როდესაც საიტი თვეში 45.000 მომხმარებელს ემსახურებოდა და მოგება თვეში 12.000 ევროს აღწევდა.

თუმცა, 2004 წელს, კომპიუტერული ჟურნალის „ *c't* “, ბერლინში დაფუძნებული გაზეთის „ *Tagesspiegel*“ და საავტორო უფლებების დარღვევის საზოგადოების „*GVU*“ საქმიანობის გამოძიების დროს ჩატარდა ჩხრეკა და ოპერაცია შეუჩერდა ოპერატორებსა და მიუნხენში მდებარე ადვოკატს, რომელიც პასუხს აგებდა გადახდებსა და სხვა ადმინისტრაციულ საკითხებზე. ბრიტანეთის ვირჯინიის კუნძულებზე, ტორტოლაში ბანდას დაფუძნებული ჰქონდა კომპანია სახელწოდებით „Internet Payment Systems Ltd. “ კიბერ-დანაშაულის შესახებ კონვენციის მე-10 მუხლის შესაბამისად ყველას წაუყენეეს ბრალდება, ხოლო 2007 წელს შეუფარდეს 23 თვით პირობითი სასჯელი და ჯარიმა 90.000 ევროს ოდენობით. ეს ოპერაცია საავტორო უფლებების დარღვევის კუთხით ერთ-ერთ უდიდეს წარამატებულ ოპერაციად ითვლება.

მონაცემთა დაუყონებლივი უსაფრთხო შენახვა და ტრაფიკის მონაცემთა ნაწილობრივი გამოაშკარავება: „ბოტნეტის“ კლიენტები – შუამავალი სერვერები

ონლაინზე ჩადენილი დანაშაულის აღმნიშვნელია არის IP მისამართი: უკეთეს შემთხვევაში ბოროტმზრახველს ავლენს შეუმჩნეველ ციფრთა მწყობრი; თუ ეს ასე არ მოხდა, ამ მისამართის საშუალებით შესაძლებელი ხდება ინტერნეტის სხვა ქსელთთნ დაკავშირება - ეს უფრო ხშირად ერთად ერთი მიმართულებაა. მაგრამ ვინაიდან გამოძიებების რაოდენობა სულ უფრო აღმავალი ტენდენციით ხასიათდება, დამნაშავის მიერ მითითებული IP მისამართი მესამე მხარესთან გადაგამისამართებთ; ამიტომ მოთხოვნა მონაცემების შენახვის თაობაზე მსხვერპლის ან მისი პროვაიდერის სისტემაზე შეიძლება საკმარისი არ აღმოჩნდეს.

ამის კარგი ნიმუშია „ბოტნეტის“ (botnet) კლიენტები, რომლებიც შუამავლ სერვერად გამოიყენება. „ბოტნეტი“ შედგება ასობით, ზოგჯერ ათასობით გატეხილი კომპიუტერისაგან, რომელსაც დამნაშავე ანუ „ბოტმასტერი “ (botmaster) მართავს. თაღლითურ ქსელში ჩართული გატეხილი კომპიუტერები ძირითადად კერძო პირების საკუთრებაშია და ვინაიდან გამართულად მუშაობენ არავითარ ეჭვს მფლობელებში არ იწვევს. „ბოტმასტერი“ მართავს ინფიცირებულ კლიენტებს და ქირაობს მათ მომსახურებას ფასიანი კლიენტების სასარგებლოდ. „ბოტნეტის “ კლიენტის დაქირავება შუამალი სერვერის როლში საკმაოდ გავრცელებული პრაქტიკაა და გარკვეულ ანონიმურობას უზრუნველყოფს: როდესაც კავშირი „ბოტნეტის “ მიერ გატეხილი კომპიუტერის კლიენტის მეშვეობით ხორციელდება, დამნაშავე ითვისებს IP მისამართს და გატეხილი კომპიუტერის საიდენტიფიკაციოს პარამეტრებს.

ამგვარ შემთხვევაში მონაცემთა ტრაფიკის ნაწილობრივი გამჟღავნება, რომელიც მესამე მხარის გატეხილი კომპიუტერიდან წამოვიდა შეიძლება გამოდგეს, ვინაიდან კომუნიკაციას, როგორც წესი, ორი მიმართულება აქვს. ბოროტმზრახველის თხოვნის შემთხვევაში, მონაცემთა ზოგიერთი პაკეტი შეიძლება უკან მას გაეგზავნოს. სამწუხაროდ შუამავალთა ჯაჭვი შეიძლება უსაზღვროდ გრძელი აღმოჩნდეს, ვინაიდან მონაცემთა ტრაფიკს ეფემერული ბუნება ახასიათებს; სირთულე იმაში მდგომარეობს, რომ ჯაჭვიდან გამოიხშიროს „ლინკები “, სანამ ყველა მონაცემის წაშლა მოხდება.

ინფორმაციის წარდგენის მოთხოვნა და აბონენტის შესახებ ინფორმაციის წარდგენა: საჭირო ინფორმაციის გავრცელება

სულ რაღაც ათიოდ წელიწადში მსოფლიოს ყველა კუთხეში აღმასრულებელ ხელისუფლებებს რადიკალური ცვლილებების გატარება მოუხდათ. გასული საუკუნის 90-იან წლებამდე, ტელეკომუნიკაციის ოპერატორები უმრავლეს ქვეყანაში ან სახელმწიფო ან საჯაროდ კონტროლირებადი უწყებები იყვნენ. იმ დროს, არავის არ უფიქრია იმ პრობლემების შესახებ, რაც დაკავშირებული იყო აბონენტის შესახებ ინფორმაციის ხელმისაწვდომობაზე რათა ეს უკანასკნელი გამოყენებული ყოფილიყო სატელეფონო ზართან ან დეპეშასთან დაკავშირებული სისხლის სამმართლის საქმის აღძვრისას. ზოგიერთი საჯარო

უწყება უკვე ფლობდა შესაბამის ინფორმაციას და ამ ინფორმაციის მისაწვდომობა მხოლოდ ადმინისტრაციის მხრიდან დახმარებაზე იყო დამოკიდებული. მას შემდეგ რაც მოხდა ტელეკომუნიკაციების სამსახურების უმრავლესობის პრივატიზაცია, ბევრ სახელმწიფოს დასჭირდა იურიდიულად უზრუნველეყო აღნიშნული ინფორმაციის მისაწვდომობა მომავალში, რომელიც იმ დროისათვის კერძო კომპანიების ხელში ჩავარდა და მალე მონაცემთა დაცვის რეგულაციების საგანი გახდა.

პარალელურად, ინტერნეტის გავრცელებამ, იმეილის, „ჩატისა“ და სხვა საშულებების დამკვიდრებასთან ერთად შესაძლებელი გახადა კომუნიკაციის მრავალფეროვანი საშუალებების მსოფლიოს მასშტაბით გამოყენება. ამგვარად, სცენაზე ახალი მოთამაშეები გამოჩნდნენ, მაგალითად, იმეილის პროვაიდერები, რომლებიც შეურთდნენ აბონენტთა შესახებ ინფორმაციის დამცველთა არმიას. მსოფლიო ქსელის განვითარების დასაწყისში, განსაკუთრებით მცირე ზომის სერვის პროვაიდერები უარს ამბობდნენ ძალოვან სტრუქტურებთან თანამშრომლობაზე, ვინაიდან ძალოვანი უწყებები საინფორმაციო ტექნოლოგიის მუშაკთა შორის იმ დროს დიდი ნდობით არ სარგებლობდნენ. მართალია, აბონენტთა შესახებ ინფორმაცია სასარგებლო იყო ეჭვიტანილთა, მსხვერპლთა და სხვა ადამიანთა გამოცხრილვისათვის, რომლებიც დაკავშირებული იყვნენ გამოძიებასთან, წარმოების განაწესის აუცილებლობა დღის წესრიგში არ იდგა.

დღეს კი საჭირო მონაცემები იმდენად მიმოფანტულია, და არა მხოლოდ აბონენტთა შესახებ ინფორმაცია, რომ მისი მართვა თითქმის შეუძლებელია. ე. წ. ვებ 2.0 ტექნოლოგიამ ხელი შეუწყო სოციალური ქსელების შექმნას, რომლის საშუალებით მილიონობით ადამიანი შეტყობინებებს, ფოტოებსა და სხვა მონაცემებს ერთმანეთს უგზავნიან; ასევე, „ბლოგებს“ და „მიკრო ბლოგებს“, როგორიც არის მაგალითად, „Twitter“ . უფრო მეტიც, ნებისმიერ ინტერნეტ მომხმარებელს შეუძლია ყოველგვარი საზრაურის გარეშე დააფუძნოს საკუთარი ფორუმი დაცული პაროლით ანგარიშის დასაცავად, რომელიც ასევე მოიცავს აბონენტის შესახებ ინფორმაციას. ამგვარად, ვებ 2.0 საუკუნეში, კიდევ უფრო არსებითია, რომ ხელმისაწვდომი იყო კომპიუტერში შენახული ინფორმაცია, განსაკუთრებით კი, აბონენტის შესახებ ინფორმაცია, მაშინაც კი თუ ეს ინფორმაცია ფორუმის მოყვარული ადმინისტრატორის ჩანაწერებშია შენახული.

გაჩხრეკვის ორდერი: მუშაკის კომპიუტერზე შენახული პერსონალური ინფორმაცია

ტრადიციულად სისხლის სამართლის გამოძიებებში მტკიცებულებად მატერიალური ნივთი: იარაღი, ქსოვილის ნიმუში ან თითის ანაბეჭდი, ითვლება. ამიტომ, როდესაც მტკიცებულების მოსაპოვებლად გაჩხრეკის ორდერი იცემა, მისი დებულება ითვალისწინებს მის ფიზიკურ თუ სივრცულ ვითარებას. ხოლო როდესაც საქმე გვაქვს ელექტრონულ მტკიცებულებასთან, აღნიშნული მოთხოვნა შეუსაბამო და ზოგჯერ ხელის შემშლელადაც კი შეიძლება ჩაითვალოს სამართლებლივი მდგომარეობის გათვალისწინებით. როდესაც ბრალმდებელი არამატერიალური ინფორმაციის მოსაძიებლად გაჩხრეკის ორდერს

გასცემს, იგი იიოლებს საქმეს და გაჩხრეკას ავრცელებს ეჭვმიტანილის ყველა ტექნიკაზე, რაც ეჭვმიტანილმა ან მესამე მხარემ შეიძლება არამართლზომიერად ჩათვალოს და დაცვის პოზიციიდან ზოგჯერ გაუმართლებლადაც.

ამის მაგალითია 2007 წლის საქმე, რომელსაც გერმანიისკონსტიტუციური სასამართლო იხილავდა. ეჭვმიტანილი საჯარო მოხელე იყო და კერძო თუ საქმიანი იმეილების მისაღებად და გასაგზავნად ოფისის კომპიუტერით სარგებლობდა, რომელიც სხვა ნივთებთან ერთად მისი დამქირავებლის კუთვნილებაში იყო. ძალოვან უწყებას, რომელიც გამოძიებას ატარებდა საფუძვლიანი ეჭვი ჰქონდა ევარაუდა, რომ ეჭვმიტანილი იმეილით იღებდა და შემდეგ გადააგზავნიდა ხოლმე „power point“ პრეზენტაციას, რომელიც დანაშაულებრივ მასალას შეიცავდა. ციფრული ინფორმაციის მოპოვების მიზნით კომპიუტერი გამომძიებელ ორგანოებს გადაეცა. ეჭვმიტანილმა უკმაყოფილება გამოთქვა და ადგილობრივ სასამართლოს თხოვნით მიმართა დაედგინათ რამდენად კანონიერი იყო გაჩხრეკის ჩატარება. მისი სარჩელი არც ადგილობრივმა და არც უფრო მაღალი ინსტაციის სასამართლომ არ განიხილა იმ მოტივით, რომ კომპიუტერი მისი საკუთრება არ იყო.

გერმანიის კონსტიტუციურმა სასამართლომ დაამტკიცა გადაწყვეტილება და უარი უთხრა ეჭვმიტანილს მისი სარჩელის განხილვაზე, ვინაიდან სისხლის სამართლის სასამართლოებმა სათანადოდ მიუსადაგეს შესაბამისი სამართლებლივი დებულება, რომელიც არ არღვევდა ეჭვმიტანილის ფუნდამენტურ კონსტიტუციურ უფლებებს. მართალია, ფორმალურად გადაწყვეტილება სწორია, გამოყენებული სამართლებლივი დებულებები აშკარად მიუთითებს, რომ არამატერიალური მტიკიცებულება არა სწორად იქნა გამოყენებული და გამოიწვია ოფიციალური დაცვის მხარის პოზიციის დაკარგვა. მონაცემები ადვილად შეიძლება ეჭვმიტანილს მივაკუთვნოთ; უეჭველია, რომ აღნიშნული ციფრული მტკიცებულება მის მიერ არის შექმნილი. ამგვარად, ლოგიკური იქნება თუ მას მიეცემა საშუალება დაცვას თავისი პოზიცია.

მონაცემთა ტრაფიკის შეგროვება: გამოძალვა იმელის მეშვეობით

როდესაც დამნაშავეები ცდილობენ საკუთარი „ონლაინ“ გადაადგილების დამალვას, სასარგებლოა მონაცემთა ტრაფიკის გაანალიზება. 2009 წელს, ბოროტმზრახველმა, რომელიც მიიჩნევდა, რომ ძალიან ჭკვიანი იყო, გადაწყვიტა მრავალ ევროპულ ქვეყანაში არსებული მაღაზიების საცალო ქსელისათვის გამოეძალა დიდი თანხა. მან დააშინა ქსელის მესვეურები, რომ მოწამლავდა მთელ რიგ პროდუქტებს, რომელიც მათ ქსელში იყიდებოდა. ეს მუქარა და გაფრთხილებები იმეილით იგზავნებოდა. აღსანიშნავია, რომ ბოროტმზრახველი სხვადასხვა იმელის ანგარიშებით სარგებლობდა, რომელსაც სხვადასხვა პროვაიდერი ემსახურებოდა. საჭიროების შემთხვევაში პროვაიდერები მხოლოდ ფალსიფიცირებული მონაცემების მოძიებას შეძლებდნენ, რომელსაც იგი რეგისტრაციის დროს იყენებდა. უფრო მეტიც IP მისამართის მონაცემი, რომელიც მიბმული იყო თითოეულ იმეილზე სხვადასხვა პროვაიდერზე

მიანიშნებდა, რომლებიც სხვადასხვა ქვეყნებში იყვნენ, მათ შორის ჩინეთსა და აშშ-ში.

დეტალური გამოძიების შემდეგ, ამოიღეს IP მისამართის მონაცემი იმეილის ტიტულის სტრიქონიდან და გამოავლინეს შუამავალი სამსახური, რომელიც პროგრამის ანონიმურად ჩამოტვირთვის და გამოყენების სამსახურს სთავაზობდა. ოპერატორს კი ყოველთვის შეუძლია გამოითვალოს მომხმარებელი. ამიტომ პროვაიდერს დაუკვეთეს მონაცემთა ტრაფიკის რეალურ დროში შეგროვება შემდეგი პირობით: მონაცემთა ტრაფიკი მხოლოდ იმ ინდივიდთან დაკავშირებით უნდა შეგროვილიყო, რომელიც ეჭვმიტანილის იმეილთან დაკავშირებას ანონიმური სამსახურის გავლით მოინდომებდა. იდეამ გაამართლა. მონაცემთა ტრაფიკის რეალურ დროში შეგროვებამ გამოააშკარავა ეჭვმიტანილის ნამდვილი IP მისამართი, ხოლო შემდეგ დაადგინეს პირის სახელი და გვარი და მისამართი და გამოძიებაც დაიწყო.

შინაარსობრივი მონაცემის ხელში ჩაგდება: ორგანიზებული კიბერ-დანაშაულის გამოძიება

ინფორმაციის ხელში ჩაგდების პრაქტიკა სატელეფონო საუბრებთან დაკავშირებით კარგა ხანია ცნობილია. როდესაც აღნიშნულთან დაკავშირებით კანონშემქნელები კანონებს ქმნიდნენ, მათ აზრადაც არ ჰქონდათ ინტერნეტ ტექნოლოგიები. აღსანიშნავია, რომ როდესაც საქმე გვაქვს ინფორმაციის გაცვლასთან, მნიშვნელობა არ აქვს რა საშუალებით ხდება ეს: ტელეფონით, „ჩატით " თუ სერვერიდან ჩამოტვირთვით. ინფორმაციის შინაარსი ერთი და იგივე იქნება.

ვინაიდან სატელეფონო კავშირებს სულ უფრო აგრესიულად ცვლის ინფორმაციის ინტერნეტით გაცვლის პრაქტიკა, ბუნებრივია, რომ ძალოვანი სტრუქტურების ინტერესი კომუნიკაციის აღნიშნული არხების მიმართ სულ უფრო იზრდება. ბოლო დროის გამოძიებებმა ცხადყო, რომ კიბერ დამნაშავეთა ორგანიზებული ჯგუფები ანუ ადამიანები, რომლებიც სხვადასხვა იურიდიულად დანაშაულებრივ მომსახურებას სთავაზობენ, იქნება ეს ინფიცირებული კომპიუტერები თუ „ფიშინგის " საიტები, კომუნიკაციას დიდი ხანია უახლესი ტექნოლოგიებით ახორციელებენ და სხვა საშუალებებს აღარ იყენებენ. მაგალითად, მონაცემთა TJX ქურდობის საქმეში (იხ. თავი 3.2) დამნაშავეთა გამოაშკარავება „ჩატის " მიყურადების საშუალებით მოხერხდა. ფედერალური პოლიციის აგენტების თქმით, რომლებიც ამ საქმეს იცნობენ, აცხადებენ რომ ასევე წარმატებულია IRC არხების მოსმენა სტრუქტურული გამოძიებისათვის.

8.2 ტერმინთა განმარტება

ADDRESS - მისამართი

ტერმინს – მისამართი – მრავალი მნიშვნელობით გამოიყენება.

- ინტერნეტ მისამართი ანუ IP მისამართი ინტერნეტში (მთავარი) კომპიუტერის უნიკალური ადგილმდებარეობის მაჩვენებელია;
- ვებ გვერდის მისამართი გამოიხატება, როგორც კონკრეტული ცნობარის ბილიკი, რომელიც დაკავშირებულია კონკრეტულ სერვერზე მდებარე ფაილთან.
- ვებ გვერდის მისამართს ასევე უწოდებენ საინფორმაციო რესურსის უნიფიცირებულ საძიებელს ან URL –ს.
- იმეილის მისამართი ეს არის იმეილის მომხმარებლის ადგილმდებარეობა (რომელიც გამოისახება იმეილის მომხმარებლის სახელით, რომელსაც მოყვება ნიშანი (@), ხოლო შემდეგ მომხმარებლის სერვერის დომეინის სახელწოდება.

ADVANCE FEE FRAUD –თაღლითობა ავანსით

ეს არის თაღლითობის ერთ-ერთი სახეობა, რომლის დროსაც მსხვერპლს სთავაზობენ, რომ მან გარკვეული თანხა წინასწარ გადაიხადოს, რის სანაცვლოდ მას გარკვეულ ფულად ჯილდოს პირდებიან.

ADWARE – ადვეარი

ეს არის კომპიუტერული პროგრამა, რომელიც მომხმარებლის კომპიუტერზე პერიოდულად რეკლამას უშვებს.

ARCHIVE FILE - საარქივო ფაილი

ფაილი, რომელიც შეიცავს სხვა (როგორც წესი, შეკუმშულ) ფაილებს. იგი გამოიყენება იმ ფაილების შესანახად, რომელიც ხშირად არ გამოიყენება; მას ასევე იყენებენ ინტერნეტის ფაილების ბიბლიოთეკიდან ფაილის ჩამოსატვირთად.

AMERICAN STANDARD CODE FOR INFORMATION INTERCHANGE ASCII –ინფორმაციის ურთიერთგაცვლის ამერიკული სტანდარტული კოდი

კოდირების სტანდარტი, რომელიც გამოიყენება ძირითადად ინგლისური სიტყვებით გამოხატული ინფორმაციის ურთიერთგასაცვლელად. **ASCII** არის ინგლისურ ალფავიტზე დაფუძნებული სიმბოლური ნიშნებით შექმნილი ჩანაწერი და გამოიყენება ტექსტის კომპიუტერში, საკომუნიკაციო მოწყობილობაზე ან ტექსტზე მომუშავე სხვა საშუალებებზე წარმოსადგენად. თუ ადრე **ASCII** ყველაზე ფართოდ გამოყენებული

სიმბოლური ჩანაწერი იყო მსოფლიო ქსელში, 2008 წელს იგი ჩაანაცვლა UTF-8.

AUTHENTICATION /AUTHENTICITY – იდენტიფიკაცია/ ავთენტურობა

იდენტიფიკაცია არის, პროცესი რომელიც გამოიყენება უსაფრთხოების უზრუნველყოფის მიზნით და საშუალებას იძლევა მეტ-ნაკლები გარანტიით დადგინდეს ან დადასტურდეს ფიზიკური ან იურიდიული პირის ვინაობა. ავთენტურობის მექანიზმი გამოიყენება ინფორმაციულ სისტემებში შესვლის გასაკონტროლებლად.

იდენტიფიკაცია არის, პროცესი რომელიც საშუალებას იძლევა მეტ-ნაკლები გარანტიით დადგინდეს ან დადასტურდეს, რომ ელექტრონული შეტყობინება ან ტრანზაქცია ინიცირებულია კონკრეტული პირის ან წყაროს მიერ.

BACKDOORS[312] - უკანა კარი

უკანა კარი ეს არის „ბოროტი“ კოდი, რომელიც კომპიუტერულ სისტემაში ან ქსელში არასანქცირებული შეღწევის უფლებას იძლევა. ინტერნეტით შორეული კომპიუტერიდან მიღებული ბრძანების საფუძველზე „ბოროტი“ კოდი საშუალებას აძლევს ბოროტმზრახველს გამოიყენოს დისტაციური ბრძანებები და დაამონტაჟოს სხვა პროგრამა, რომელმაც შეიძლება თავის მხრივ საფრთხის წინაშე დააყენოს პაროლი ან სხვა პერსონალური ინფორმაცია ან საშუალება მისცეს მანქანას გამოყენებული იქნეს უპატიოსნო მიზნებისათვის. დისტანციურად შეღწევის ან „ბოროტი“ კოდის ფუნქცია, როგორც წესი, გააჩნია „ტროას“ და „ბოტ“ პროგრამების ურავლესობას. „ბოტ“ პროგრამა „უკანა კარის“ პრგრამის ერთ-ერთი სახეობაა, რომელიც ბოროტმზრახველებს საშუალებას აძლევს დისტაციურად ერთდროულად (ან ინდივიდუალურად) გააკონტროლონ საფრთხის წინაშე მდგომი მრავალი (ათასობოთ) ინფორმაციული სისტემა. უკანა კარების ფუნქცია შეგნებით თუმცა გაუფრთხილებლად სანქცირებული კომპიუტერული პროგრამის პაკეტში შედიოდა, ვინაიდან იგი მომხმარებელს საშუალებას აძლევდა დისტანციურად დაკავშირებოდა სხვა კომპიუტერებს. სწორედ მისი ეს დაუცველობა ბოროტად გამოიყენეს ბოროტმზრახველებმა.

BACKUP - ბექაფი

კომპიუტერში არსებული ყველა ინფორმაციის დუბლირება, რათა ინფორმაცია დაცული იყოს იმ ვითარებაში თუ ორიგინალ ეგზემპლიარს რაიმე შეემთხვევა.

BIOS – ბაიოსი

შეყვანა – გამოყვანის საბაზო სისტემა. ეს არის მშობელ პლატაზე დამახსოვრებული პროგრამა, რომელიც აკონტროლებს მოწყობილობის საბაზო ინიცირების ოპერაციებს. „ბაიოსი“ ეძებს პროცესორს, მეხსიერებას, IDE (ფორმირების ინტეგრირებული ელექტრონული სქემების) მოწყობილობებს, და პორტებს. „ბაიოს“ ემატება POST (თვითტესტირება ჩართვისას) შემოწმება და შედეგებს უდარებს CMOS. „ბაიოსი “ ამუშავებს Config.sys და Autoexec.bat,

[312] ეკონომიკური თანამშრომლობისა და განვითარებოს ორგანიზაციის ვირუსული პროგრამების კვლევა

რომლებიც ფესობრივ კატალოგშია დამახსოვრებული (dos-თვის ეს არის C:>)

BLUETOOTH – ბლუთუსი

„ბლუთუსი“ ტელეკომუნიკაციების ინდუსტრიის სტანდარტია, რომლის საშუალებით მობილური ტელეფონები, კომპიუტერები და ციფრული პერსონალური მდივნები (PDAs) მსგავს მოწყობილობებს მოკლე დიაპაზონის მქონე უსადენო კავშირებით უკავშირდებიან.

BOOKMARKING – ბუკმარკინგი

ეს არის პროცესი, რომლის დროსაც ხდება ვებსაიტის ან ინტერნეტ დოკუმენტის საკუთარ კომპიუტერზე დამახსოვრება, რათა მოგვიანებით მისი ადვილად პოვნა შეძლოთ.

BOOT – პირველადი ჩართვა

კომპიუტერის თავდაპირველად ჩართვა, უფრო ხშირად ხმარობენ ტერმინს

„რე-ბუტი “ (re-boot).

BOOT DISK – ბუთ დისკი

„ფლოპი“ დისკი, რომელიც შეიცავს ფაილებს, რომლის გარეშე ოპერაციული სისტემა ვერ ამუშავდება.

BOT - ბოტი

დაინფიცირებული კომპიუტერი, რომელსაც კომპიუტერის მფლობელის თანხმობის ან აზრზე ყოფნის გარეშე საკუთარი მიზნებისათვის თაღლითი აკონტროლებს. იგი ხშირად გამოიყენება DDos თავდასხმების, სპამის ინიცირებისათვის, შუამავალი სერვერის როლის შესასრულებლად და სხვა სისტემების დასაინფიცირებლად. დამატებითი ინტრუქტაჟის ან უახლესი ვირუსის მისაღებად იგი, როგორც წესი, უკავშირდება გამოთვლითი ტექნიკისა და კავშირგაბმულობის მექანიზმებს (C&C). C&C შეიძლება საფუძვლად HTTP an IRC ჰქონდეს, ან უფრო რთულად დასაფიქსირებელ P2P ქსელთან იყოს დაკავშირებული. „ბოტი “ შეიძლება დაინფიცირებული იყოს მრავალი ვირუსით და დაკავშირებული იყოს ერთდროულად მრავალ C&C –თან, და რომელსაც ერთი ან მეტი თაღლითი აკონტროლებს.

BOTNET – ბოტნეტი

ეს არის „ბოტების “ ჯგუფი, რომელიც იმავე ან მსგავს ზიანის მომტან პროგრამას უშვებს და იმავე C&C მექანიზმს აკავშირებს. თავისი სიდიდით „ბოტნეტი “ მრავალგვარია – რამდენიმე ცალკეული „ბოტით“ დაწყებული და ათასობით, ზოგჯერ კი მილიონობით დამთავრებული. მათი ეფექტიანობა ვირუსის მატარებელ კომპიუტერულ პროგრამაზეა დამოკიდებული, ანუ რა სახის ვირუსი გადააქვს და ასევე რა სახის ძირითადი კომპიუტერის დავირუსება მოხდება. თუ ერთი ან ორი კომპიუტერი, მაგალითად, კორპორაციაში ან უნივერსიტეტში ფართოზოლიან ინტერნეტ კავშირშია ჩართული, მათ უფრო მეტი ზიანის მოტანა შეუძლიათ, ვიდრე იმ შემთხვევაში, როდესაც ძირითადი კომპიუტერის

რაოდენობა მართალია, მრავალრიცხოვანია, თუმცა მათ მაქსიმალურად შეზღუდული კავშირები აქვთ.

BUFFER - ბუფერი

მეხსიერების სფერო, რომელსაც ხშირად „კეშ " (cache) მეხსიერებას უწოდებენ, რომელიც გამოიყენება მოწყობილობებში შეღწევის ტემპის ასაჩქარებლად. იგი ასევე გამოიყენება, როგორც მონაცემთა დროებითი შენახვის საშუალება, როდესაც ხორციელდება მონაცემებთან გაცნობა ან როდესაც ინფორმაცია მყარ დისკზე, „სიდიზე ", პრინტერზე ან ლენტურ „დრაივზე" გადასაწერად არის გამზადებული.

BULLETIN BOARD SERVICE (BBS) - განცხადებების ელექტრონული დაფა

BBS ელექტრონული კორპის დაფის მსგავსია. ეს არის კომპიუტერული სისტემა, რომელიც ქსელური მისაწვდომობით არის აღჭურვილი, რათა დისტანციურმა მომხმარებლებმა შეძლონ საინფორმაციო და შეტყობინებების გამტარებელი ცენტრით სარგებლობა. განცხადებების ელექტრონული დაფა, როგორც წესი, სპეციალურ სფეროებზეა ორიენტირებული, როგორიც არის სამეცნიერო ფანტასტიკა, ფილმები, ვინდოუს პროგრამა, მაკინტოჟის სისტემები. ზოგი უფასოა, ზოგიც გადასახადს ითხოვს, ზოგიც კი კომბინირებულია.

BYTE (binary term) - ბაიტი

კომპიუტერთა უმეტეს სისტემაში ბაიტი მონაცემთა დამუშავების ერთეულია, რომელიც 8 ბიტისაგან შედგება. ბაიტი შეიძლება წარმოდგენილი იყოს ერთი ნიშნით, ეს შეიძლება იყოს ასო, ციფრი ან პუნქტუაციის ნიშანი.

CACHE - კეში

„კეში" ეს არის ადგილი, სადაც შეიძლება ინფორმაცია მეტ-ნაკლებად ხანმოკლე პერიოდით იქნას შენახული. ის ვებ გვერდები, რომელსაც თქვენ ინტერნეტში „ძრომიალის" დროს მოინახულებთ ხოლმე, როგორც წესი, თქვენი „ბრაუზერის" „კეშის" დირექტორიაში მყარ დისკზე ინახება. თუ თქვენ იმ გვერდს მიუბრუნდებით, რომელიც ცოტა ხნის წინ მოინახულეთ, „ბრაუზერი" ამ ინფორმაციას „კეშიდან " გამოითხოვს და არა სერვერიდან, რაც ეკონომიურია დროის მხრივ და ასევე ნაკლები დატვირთვაა ტრაფიკზე. ორი ტიპის არის „კეში " – მეხსიერება და დისკი.

CDF – არხის მონაცემთა ფორმატი

არხის მონაცემთა ფორმატი არის სისტემა, რომელიც ინფორმაციას ინტერნეტით გადასაცემად ამზადებს.

CD-R – სიდი-არი

„სიდი-არი “ კომპაქტ-დისკია ერთჯერადი ჩაწერისათვის. დისკი, რომელზეც შეიძლება ინფორმაცია ჩავწეროთ, მაგრამ მის წაშლას ვერ შევძლებთ.

CD-R (COMPACT DISK READ-ONLY MEMORY OR MEDIA)– სიდი-რომი (კომპაქტური დისკი მხოლოდ წასაკითხად ან მედიისათვის)

კომპიუტერებში სიდი-რომის ტექნოლოგია წარმოადგენს ჩაწერის, შენახვისა და ელექტრონული ინფორმაციის ამოღების ფორმატსა და სისტემას. იგი იკითხება ლაზერული ოპტიკისა და არა მაგნიტური მოწყობილობების საშუალებით.

CD-RW – სიდი-არი

„სიდი-არვი “ არის კომაქტ-დისკი, რომელზედაც რამდენიმეჯერ შეიძლება ჩაწერის განხორიციელება. მასზე ჩაწერაც შეიძლება და წაშლაც.

CHAT ROOM - „ჩატ-რუმი “

„ჩატ-რუმი “ ფუნქციონირებს ონლაინ რეჟიმში და ასევე ელექტრონული განცხადებების დაფის მეშვეობით. მისი საშუალებით ხდება კონკრეტულ სისტემში ჩართულ მომხმარებლებს შორის შეტყობინებების რეალურ დროში გაცვლა.

CIRCUIT BOARD - პლატა

თხელი ფიფრფიტა მასზე დამონტაჟებული ჩიპებით, მოწყობილობებითა და სხვა ელექტრონული დეტალებით.

CLICK FRAUD – თაღლითობა თითის კლავიშზე დაჭერით („დაკლიკებით”)

დანაშაულის სახეობა, რომლის დროსაც პირი, ავტომატური სკრიპტი ან კომპიუტერული პროგრამა კანონიერი მომხმარებლის სიმულირებას ახდენს ონლაინ რეკლამაზე თითის დაჭერით. მიზანი შემოსავლის მიღებაა ან რეკლამის გამთავსებლის ხარჯების გაზრდაა, რომელსაც იმის მიხედვით ახდევინებენ თუ რამდენი პოტენციური კლიენტი გაეცნო ამ რეკლამას.

CMOS - COMPLEMENTARY METAL-OXIDE SEMI-CONDUCTANT – დამატებითი მეტალ-ოქსიდის ნახევარგამტარი

ეს არის დაბალი სიმძლავრის მეხსიერების ჩიპი, რომელიც, როგორც წესი, ინახავს ფუნქციურ მონაცემებს, როგორიც არის მაგალითად, ჩართული პაროლი, დრო და თარიღი, დრაივის ძიების თანმიმდევრობა და მყარი დრაივის ტიპები. მას ხშირად ურევენ BIOS ჩიპში. BIOS ჩიპი, ძირითადად, კომპიუტერს აამოქმედებს ხოლმე და მის მიერ ნაპოვნ ინფორმაციას უდარებს ბოლო დროს CMOS-ში შენახულ პარამეტრებს.

COMMAND AND CONTROL SERVER (C&C) - მართვის სისტემის სერვერ

მართვის სისტემის სერვერ (ანუ C&C) ვირუსის პროგრამისათვის არის მართვის პუნქტი. ეს შეიძლება ერთი სერვერი არ იყოს, ვინაიდან ვირუსული პროგრამა კავშირის განხორციელების სხვა და სხვა მექანიზმს იყენებს, რომელშიც შედის IRC, HTTP, AND P2P, ასევე როგორც მრავლობითი სწრაფად ცვლადი სერვერები.

COMPUTER DATA – კომპიუტერული მონაცემები

ნებისმიერი ფაქტის, ინფორმაციისა და ცნების ისეთი ფორმით წარმოდგენა, რომელიც მისაღები იქნება კომპიუტერული სისტემით მისი დამუშავებისათვის, ისეთი პროგრამის ჩათვლით რომელიც აიძულებს კომპიუტერულ სისტემას შეასრულოს კონკრეტული ფუნქცია[313].

COMPUTER SYSTEM[314] - კომპიუტერული სისტემა

კომპიუტერული სისტემა ეს არის ნებისმიერი მოწყობილობა ან ურთიერთდაკავშირებულ მოწყობილობათა ჯგუფი, რომელთაგან ერთი ან მეტი პროგრამის შესაბამისად ახორციელებს მონაცემთა ავტომატურ დამუშავებას.

CPU (CENTRAL PROCESSING UNIT) - ცენტრალური პროცესორი

ცენტრალური პროცესორი კომპიუტერის ყველაზე ძლიერი ჩიპია, რომელიც კომპიუტერში მდებარეობს. ეს არის კომპიუტერის „ტვინი“, რომელიც ასრულებს ყველა არითმეტიკულ, ლოგიკურ და მაკონტროლებელ ფუნქციას.

CRACKER - კრეკერი (კომპიუტერული სისტემის გამტეხი)

კომპიუტერის ექსპერტი, რომელიც თავის უნარს გასაღებით დაშიფრულ კომპიუტერულ პროგრამაში ან დივიდიში შეღწევას ახერხებს. როგორც წესი ეს საავტორო უფლებით დაცული საფირმო პროდუქტია. ამის შემდეგ „კრეკერი“ გატეხილ კომპიუტერულ პროგრამას ან დივიდის ან უფასოდ ან ძალიან დაბალ ფასში ავრცელებს.

CRYPTOGRAPHY - დაშიფვრა

კრიპტოგრაფია ხშირად უბრალო ტექსტის (ჩვეულებრივი ტექსტი, რომელსაც ზოგჯერ ღია ტექსტს უწოდებენ) დაშიფრულ ტექსტში გადაყვანასთან ასოცირდება (პროცესს დაშიფვრა ეწოდება), შემდეგ კი ისევ დაუშიფრავ ტექსტში დაბრუნებას (ანუ გაშიფვრა). ამ საქმით დაკავებულ პირებს კრიპტოგრაფებს ეძახიან. ეს პროცესი მიზნად ისახავს უზრუნველყოს კერძო ინფორმაციის უსაფრთხოება, რომელიც საჯარო ქსელების გავლით იგზავნება, რისთვისაც ხდება ამ ინფორმაციის დაშიფვრა, რის გამოც მის წაკითხვას ვერავინ

[313] მუხლი 1 კიბერ-დანაშაულის შესახებ კონვენციაში.
[314] მუხლი 1 კიბერ-დანაშაულის შესახებ კონვენციაში.

ახერხებს გარდა იმ პირისა, რომელსაც აქვს მათემატიკური გასაღები ანუ ცოდნა, რომლის მეშვეობით იგი გაშიფრავს მას.

DATABASE - მონაცემთა ბაზა

მონაცემტა ბაზა არის მონაცემთა ორგანიზაებული ნაკრები, რომელთანაც მისაწვდომობა სხვადასხვა გზით შეიძლება განხორციელდეს. მონაცემთა ბაზების გავრცელებული პროგრამებია: Dbase, Paradox, Access. იგი იყენებს: სამისამართო კავშირს (ლინკს), ინფორმაციის ინვოისს, და ა.შ.

DELETED FILES - წაშლილი ფაილები

თუ სუბიექტისათვის ცნობილია, რომ კომპიუტერში მისი მაკომპრომიტირებელი ფაილია, მტკიცებულების დამალვის მიზნით იგი შეეცდება მის წაშლას. კომპიუტერის ბევრ მომხმარებელს მიაჩნია, რომ მან ნამდვილად მოიცილა პრობლემური ინფორმაცია. სინამდვილეში კი ფაილების წაშლა იმაზეა დამოკიდებული თუ როგორ მოხდა წაშლა. ბევრ შემთხვევაში სასამართლო ექსპერტი შეძლებს ორიგინალური მონაცემების თუ მთლიანად არა ნაწილობრივ აღდგენას.

DENIAL OF SERVICE ATTACKS (DOS) - მომხმარებელთა ნორმალური მომსახურების დარღვევის მიზნით თავდასხმა

მომხმარებელთა ნორმალური მომსახურების დარღვევის მიზნით თავდასხმა დამიზნებულია ხოლმე კონკრეტულ ვებ საიტზე. თავდამსხმელი ვებსერვერს დაუსრულებლად ბომბავს განმეორებითი შეტყობინებებით. ეს ფაქტი ხელს უშლის სისტემას მუშაობაში და კანონიერ მომხმარებელს არ აძლევს პროგრამაში შესვლის უფლებას.

DIGITAL SIGNATURE – ციფრული ფაქსიმილე

ციფრული ფაქსიმილე არის კოდი, რომელიც იმის გარანტიას იძლევა, რომ იმეილი გამოგზავნილი იქნა კონკრეტული პირის მიერ.

DIGITAL VIDEO (DV) - ციფრული ვიდეო

ციფრული ვიდეო არის ხელში ჩაგდებული, შეცვლილი და ციფრულ ფორმატში შენახული ვიდეო.

DISK CACHE - დისკის კეშ- მეხსიერება

მეხსიერების ნაწილი, რომელიც დროებით ინახავს დისკიდან წაკითხულ ინფორმაციას.

DISC SPACE - დისკის სივრცე

მახსოვრობის მოწყობილობა დისკზე. სივრცე ვებსაიტზე, რომელიც მასპინძლობას უწევს კომპანიის სერვერს ან კომპიუტერებს და

რომელსაც უფლება აქვს ისარგებლოს ვებ საიტზე არსებული შინაარსით.

DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS) - მომხმარებელთა ნორმალური მომსახურების დარღვევის მიზნით თავდასხმა

მომხმარებელთა ნორმალური მომსახურების დარღვევის მიზნით თავდასხმა, რომელსაც ახორციელებს კონკრეტული სისტემების დიდი რაოდენობა, რომლებიც როგორც წესი „ბოტით " ან „ბოტნეტის " ნაწილით დაინფიცირებული არიან. ვინაიდან სახეზეა დიდი რაოდენობის წყარო, კანონიერი ტრაფიკის გამიჯვნა თავდასხმისაგან ძნელია და პრობლემის მოხსნას შეიძლება ხელი შეუშალოს.

DOMAIN NAME – დომეინის სახელი

დომეინი არის ინტერნეტით მოსარგებლე ნებისმიერი სუბიექტის განმსაზღვრელი ინსტრუმენტი ან მისამართი.

DOMAIN NAME REGISTRANT (REGISTRANT) – დომეინის სახელის დამრეგისტრირებელი

პირი ან კომპანია, რომელიც კონკრეტულ დომეინის სახელს კონკრეტული სახელით რეესტრში ატარებს. დამრეგისტრირებელი, როგორც წესი, არის დომეინის სახელის იურიდიული მფლობელი ან ადმინისტრატორი.

DOMAIN NAME REGISTRAR (REGISTRAR) – დომეინის სახელის რეესტრში გამტარებელი

კომპანია, რომელსაც შესაბამისი ორგანოს მიერ მინიჭებული აქვს უფლება რეესტრში გაატაროს ინტერნეტ დომეინის სახელები. ეს კომპანიები ემსახურებიან საბოლოო მომხმარებელს და შეიძლება განხილული იქნეს, როგორც „საცალო მოვაჭრე" დომეინის რეგისტრაციის ბიზნესის მოდელში და როგორც წესი, თუმცა არა ყოველთვის, გამიჯნულია დომეინის სახელის რეგისტრაციისაგან.

DOMAIN NAME REGISTRY (REGISTRY) – დომეინის სახელის რეგისტრატურა

ყველა დომეინის სახელების მონაცემთა ბაზა, რომელიც რეგისტრირებულია კონკრეტული ზედა დონის დომეინის ფარგლებში. ხშირად ეს ტერმინი ასევე გამოიყენება რეგისტრატურის ოპერატორის მიმართ, ანუ ორგანიზაციის მიმართ, რომელიც მართავს აღნიშნულ მონაცემთა ბაზას, აკონტროლებს სახელების რეგისტრაციის პოლიტიკას და ქმნის ზონურ ფაილებს ზედა დონის დომეინისათვის. რეგისტრატურა შეიძლება წარმოვიდგინოთ, როგორც დომეინის რეგისტრაციის ბიზნესის მოდელში „ბითუმად მოვაჭრე".

DOMAIN NAME SYSTEM (DNS) – დომეინის სახელის სისტემა

სისტემა, რომელიც გარდაქმნის ინტერნეტ დომეინის ან მასპინძლის სახელს, მაგალითად, **www.team-cymru.org** რესურს მისამართად ან განმასხვავებელ სახელად, რომელიც ხშირად ეს სერვერის, რომელიც დომეინს ან მასპინძელ სახელს ემსახურება, IP მისამართია, მაგალითად 68.22.187.6. დომეინის სახელის სისტემას ასევე შეუძლია ასახოს სახელის სერვერი, რომელიც პასაუხისმეგებელია დომეინზე ან ქვე-დომეინზე ან საფოსტო სერვერი, რომელსაც სპეციალურად ისეთი ფუნქცია აქვს მინიჭებული, რომ მან შეძლოს დაამუშაოს ფოსტა დომეინისთვის ან ქვე-დომეინისთვის.

DONGLE - დამცავი ჩამხშობი

ტერმინი, რომელიც გამოიყენება გარე ტექნიკური საშუალებების აღსანიშნად, რომელისაც ჩამონტაჟებული მექსიერება აქვს. კომპანიები, რომლებიც პროგრამული უზრუნველყოფის ძირადდირებულ პაკეტებს ყიდიან, დამცავ ჩამხშობს იმის დასამტკიცებლად იყენებენ, რომ კომპიუტერს ნამდვილად აქვს აღნიშნული პროგრამის გამოყენების ლიცენზია. ის ჩამოტაჟებულია, რათა პროგრამამ იპოვის დამცავი ჩამხშობი მანამ სანამ მას აამოქმედებს.

DVD -დივიდი

დიდვიდი არის მრავალმიზნობრივი ციფრული დისკი. წააგავს კომპაქტ დისკს, თუმცა უფრო დიდი მეხსიერება აქვს.

კოდირება (დაშიფვრა)

კოდირება არის ინფორმაციის დაშიფვრის ან გაშიფვრის პროცესი, რომელიც უზრუნველყოფს იმას, რომ მასთან გაცნობას მხოლოდ ის პირი შეძლებს, ვისთვისაც ეს ინფორმაციაა განკუთვნილი.

E-MAIL HEADER - იმეილის ქუდი

იმეილი ორი ნაწილისაგან შედგება – ტექსტი და ქუდი. როგორც წესი, ქუდში მოცემული ინფორმაცია იმის გვატყობინებს თუ რა დროს, რა რიცხვში იქნა იგი გამოგზავნილი და რას ეხება ის. იმეილს ასევე შეიძლება უფრო გაფართოებული ქუდი ჰქონდეს – ანუ ინფორმაცია, რომელიც ავტომატურად იმეილის პროგრამა და გადამცემი მოწყობილობები უმატებენ. იგი კიდევ უფრო მეტ ინფორმაციას იძლევა გამომგზავნთან დაკავშირებით და ხშირად მისი მიკვლევა შესაძლებელია.

EXPANSION BOARD - გაფართოების პლატა

გაფართოებული პლატა საბეჭდი ელეტრონული სქემის პლატაა, რომელიც შეიძლება ჩაემატოს კომპიუტერს მისი გაძლიერების მიზნით.

FILE TRANSFER PROTOCOL (FTP) - ფაილის გადაცემის / გადაგზავნის პროტოკოლი

ქსელის პროტოკოლი, რომელიც იმისათვის გამოიყენება, რომ მოხდეს ფაილების ურთიერთგაცვლა ქსელის მეშვეობით. იგი ფუნქციონირებს ღია ტექსტის მეშვეობით და უსაფრთხოების მაღალ ხარისხს ვერ უზრუნველყოფს. **SFTP** კი **FTP** –ს უფრო უსაფრთხო ვერსიაა, რომელიც **SSH** კავშირით ხორციელდება და ოპერატიულ კოდირებას უზრუნველყოფს.

FILTERING - გაფილტვრა

ინტერნეტის გაფილტვრის სისტემები იცავენ მომხმარებლებს, რათა ამ უკანასკნელებმა არ მიიღონ მათთვის მიუღებელი მასალა.

FIREWALL - ქსელთაშორისი დამცავი ეკრანი „ცეცხლოვანი კედელი“

იგი ზღუდავს გარე და შიდა ტრაფიკს.

GIGABYTE (GB) - გიგაბაიტი

1 გიგაბაიტი = 1024 მეგაბაიტს. გიგაბაიტი მეხსიერების საზომია და იგი დაახლოებით ათას მეგაბაიტს ან მილიარდ ბაიტს უდრის. იგი წარმოითქმის მაგარი „გ“-თი.

HACKER - ჰაკერი

კომპიუტერული და პროგრამული სისტემების ექსპერტები, რომლებიც გატაცებული არიან კომიუტერებისა და პროგრამების ზღვრული შესაძლებლობების გამოცდით. საზოგადოებისათვის და მედიისათვის ისინი შეიძლება სიკეთის ან, პირიქით, ბოროტების მომტანი იყვნენ. ზოგიერთ ჰაკერს კარგი იდეა უჩნდება და სხვებსაც უზიარებს მას და კომპიუტერს კიდევ უფრო ეფექტიანს ხდის. თუმცა, ზოგიერთი ჰაკერი შეგნებით ტეხავს სხვის პერსონალურ კომპიუტერს ინფორმაციის მოპოვების მიზნით და კომპიუტერული დანაშაულის ჩასადენად. ასევე იხილეთ *კრეკერი* (*კომპიუტერული სისტემის გამტეხი).*

HARD DISC - მყარი დისკი

მყარი დისკი პერსონალური კომპიუტერის შიგნით მდებარეობს. მასზე ინფორმაციის დამახსოვრება იმავე მექანიზმით ხდება, როგორც „ფლოპი “ დისკზე, თუმცა იგი უფრო მოცულობითია.

HARDWARE - ტექნიკური უზრუნველყოფა

კომპიუტერის ფიზიკური დეტალები. იგი გტანსხვავდება პროგრამული უზრუნველყოფისაგან.

HOST MACHINE - ცენტრალური კომპიუტერი

ამ დოკუმენტის ფარგლებში ცენტრალური კომპიუტერი არის კომპიუტერი, რომლის მეშვეობით მიზანში ამოღებულ მყარ დამგროვებელს სასამართლოს მიზნებისათვის აანალიზებს.

HYPERTEXT TRANSFER PROTOCOL (HTTP) - ჰიპერტექსტური ფაილების გადაცემის პროტოკოლი

პროტოკოლი, რომელსაც იყენებენ ვების მომნახულებლები (ბროუზერები) ვებ-გვერდების მოსანახულებლად.

INSTANT MESSAGE (IM) - მომენტალური შეტყობინება

ფართო ტერმინია, რომელიც გულისხმობს ორ ან მეტ ადამინს შორის რეალურ დროში ურთიერთობას და რომლის დროსაც ისინი ერთმანეთში ნაბეჭდ ტექსტს ცვლიან და გასაგზავნად ინტერნეტს იყენებენ. ზოგიერთი ქსელი და პროტოკოლი შეიცავს AOL მომენტალური შეტყობინების სერვისს (AIM), ICQ, Yahoo IM, MSN Messenger, Jabber და Google Talk-ი. IRC –ი ზოგჯერ მიიჩნევა, როგორც მომენტალური შეტყობინების საშუალება, თუმცა ეს უკანასკნელი ტრადიციულად ცოტა სხვა კატეგორიას მიეკუთვნება.

INTERNET PROTOCOL (IP)[315] - ინტერნეტ პროტოკოლი

ინტერნეტ პროტოკოლი ინტერნეტის პროგრამული კომუნიკაციის მშობლიური ენაა. ინტერნეტ პროტოკოლის მეშვეობით შესაძლებელი ხდება გეოგრაფიულად დაშორებული საინფორმაციო სისტემების ქსელები სწრაფად და ეკონომიკურად ერთმანეთს დაუკავშიროს სხვადასხვა ფიზიკური ლინკების მეშვეობით. IP მისამართი ციფრული მისამართია, რომლის მეშვეობით ხდება ტრაფიკის მარშრუტის დადგენა და მათ შორის კავშირების დამყარება.

INTERNET PROTOCOL ADDRESS (IP ADDRESS) - ინტერნეტ პროტოკოლის მისამართი

ციფრული მისამართი რომელიც ინტერნეტში ჩართულ კომპიუტერს ენიჭება, მაგალითად, 192.0.2.42 in IPv4 or 2001:db8:a8bc::4853 in IPv6.

IRC- INTERNET RELAY CHAT - ინტერნეტ ჩატი

ვირტუალური შეხვედრის ადგილი, სადაც ადამიანებს მსოფლიოს ნებისმიერი წერტილიდან შეუძლიათ ერთმანეთს დაუკავშირდნენ და ისაუბრონ სხვადასხვა ინტერესებზე, იდეებსა და საკითხებზე. ინტერნეტ ჩატის ათასობით არხის მეშვეობით მონაწილეების შეუძლიათ ჩაებან ჯგუფურ დისკუსიებში, ან პრივატული საუბარი ჰქონდეთ მეგობრებთან თუ ოჯახის წევრებთან მიუხედავად იმისა თუ სად იმყოფიან ისინი ტერიტორიულად.

ISP - INTERNET SERVICE PROVIDER - ინტერნეტ სერვისის პროვაიდერი

კომპანია რომელიც ყიდის ინტერნეტში შესვლის უფლებას ტელეფონით ან საკაბელო ხაზით, რომელიც თქვენს სახლში ან ოფისშია შემოყვანილი. თუ მომხმარებელი ადგილობრივ სატელეფონო ზარებში გადასახადს იხდის, მისთვის ეს მომსახურება უფასო იქნება, ან იგი მხოლოდ სააბონენტოს

[315] ეკონომიკური თანამშრომლობისა და განვითარებოს ორგანიზაციის ვირუსული პროგრამების კვლევა

გადაიხდის თვიურად, ხოლო ზარები უფასოა ან მინიმალური ფასი ღირს. იხილეთ აგრეთვე „სერვის პროვაიდერი“.

KEYLOGGER /LEYSTROKE LOGGERS[316] - კლავიატურის მუშაობის ოპერატორი

კლავიატურის მუშაობის ოპერატორი ფარული პროგრამაა რომელიც აფიქსირებს და „იწერს“ თითოეულ კლავიშს, რომელსაც გატეხილი სისტემის კლავიატურაზე დააჭერენ, როდესაც სისტემას კანონიერი მომხმარებელი ხმარობს და ახდენს პერსონალური მონაცემების, მაგალითად, მომხმარებლის ვინაობის, პაროლის, საკრედიტო ბარათის ნომრის ან საბანკო ანგარიშის ნომრის აკრეფას. აღნიშნული ოპერატორი უჩუმრად ინახავს მონაცემებს ფარულ ფაილებში, რომელსაც შემდეგ გადასცემს შორეულ პუნქტს ქსელის რომელიღაც წერტილში, სადაც ხდება ამ ინფორმაციის შეგროვება. კლავიატური მუშაობის ოპერატორის ფუნქცია, როგორც წესი, ტროიანული პროგრამების სემადგენელი ნაწილია.

KILOBYTE (KB) - კილობაიტი

1 კილობაიტი = 1024 ბაიტს.

LINUX - საოპერაციო სისტემა ლინუქსი

საოპერაციო სისტემა, რომელიც იმ მიზნით შეიქმნა, რომ მომხმარებელს უნიქსისა (Unix) და მაიკროსოფტის (Microsoft) უფასო ალტერნატივა ჰქონოდა. იმის გამო, რომ ამ საოპერაციო სისტემას მრავალი უფასო ვერსია ჰქონდა, იგი ფართოდ გამოიყენება სხვადასხვა კომერციულ პროდუქტში და ჩამონტაჟებულია სერვერებსა და ქსელის არქიტექტურაში, და ნაკლებად შეხვდებით მას მომხმარებლის დონეზე. ლინუქსსა და უნიქსზე შექმნილი საოპერაციო სისტემები ინტერნეტის არქიტექტურის 50% შეადგენს. ლინუქსი გამოცდილი ჰაკერების უსაყვარლესი ინსტრუმენტია, ვინაიდან მისი საშუალებით ისინი საკუთარი კომპიუტერიდან მაქსიმალურად აკონტროლებენ მსხვერპლის კომპიუტერზე შესრულებულ ნებისმიერ მოძრაობას. ასევე DOS-ის სისტემების ‚უსაფრთხოების’ ზომებს ისინი ადვილად უვლიან გვერდს.

MACRO VIRUS - მაკრო- ვირუსი

ეს არის ინსტრუქციებზე (რომელსაც მაკროს უწოდებენ) მიბმული ვირუსი, რომელიც ავტომატურად იწყებს ფუნქციონირებას, როდესაც დოკუმენტს ხსნიან.

MAGNETIC MEDIA - მაგნიტური მედია

დისკი, ფირი, კარტრიჯი, დისკეტა ან კასეტა, რომელიც მონაცემების მაგნიტურ ფორმაში შესანახად გამოიყენება.

MALWARE - ვირუსის მატარებელი პროგრამები

ვირუსის მატარებელი პროგრამა, რომელიც იმ მიზანით შეიქმნა, რომ შეაღწიოს ან დააზიანოს კომპიუტერი მისი მფლობელისაგან თანხმობის მიღების გარეშე.

MEGABYTE (MB) - მეგაბაიტი

1 მეგაბაიტი =1024 კილობაიტს.

MEMORY - მეხსიერება

ოპერატიული მოწყობილობის მეხსიერების (RAM) მოკლე სინონიმია.

[316] ეკონომიკური თანამშრომლობისა და განვითარებოს ორგანიზაციის ვირუსული პროგრამების კვლევა

მეხსიერება არის ადგილი, რომელიც ელექტრონულად ინახავს ინსტრუქციებსა და მონაცემებს, რომელშიც კომპიუტერის მიკროპროცესორი ადვილად შეაღწევს. იგი განთავსებული კომპიუტერში ჩამონტაჟებულ ერთ ან მეტ ჩიპზე.

MONITOR – მონიტორი

რაზედაც ხდება პერსონალური კომპიუტერის მიერ ინფორმაციის გამოტანა.

MOUSE - თაგუნა

მოწყობილობა, რომლიც მოძრაობის დროს კომპიუტერს გადასცემს სიჩქარესა და მიმართულებას და რომელიც, როგორც წესი, ხორციელდება კურსორის ეკრანზე გადაადგილებით.

OPERATING SYSTEM - საოპერაციო სისტემა

ეს სისტემა, როგორც წესი, კომპიუტერის მეხსიერებაში მისი ჩართვისთანავე იტვირთება; იგი ნებისმიერი პროგრამის ასამუშავებლად სავალდებულო წინაპირობაა.

ORB - ობიექტების მიმართ მოთხოვნის შუამავალი

მაღალი წარმადობის მობილური მყარი დისკის სისტემა. მასში გამოიყენება მაგნტო-რეზისისტული მონაცემების წაკითხვისა და ჩაწერის ტექნოლოგია.

PACKET [317]- პაკეტი

პაკეტი არის მონაცემთა მინიმალური კვანტი ავტონომიური მარშრუტით, რომელიც გადაიცემა თანამედროვე ციფრული პაკეტური კომუტაციის ქსელით. იგი შედგება მარშრუტის ქუდისაგან, ადრესაციისაგან და პროტოკოლის ინფორმაციისაგან, რომელსაც მოსდევს მონაცემთა სასარგებლო დატვირთვა. პაკეტი არის შეტყობინება, რომელიც შეიცავს ინფორმაციას, ასევე დანიშნულების მისამართს, რომელიც იმ ქსელის მეშვეობით გადაიცემა, რომელიც პაკეტებს ან პაკეტური კომუტაციის ქსელს გადასცემს.

PAYLOAD - სასარგებლო დატვირთვა

სასარგებლო დატვირთვა არსებითი მონაცემია, რომელიც გადაიცემა პაკეტის ან სხვა გადამცემი მოწყობილობის საშუალებით. სასარგებლო დატვირთვაში არ შედის „ზედნადები " მონაცემი, რომელიც საჭიროა იმისათვის, რომ პაკეტმა თავის დანიშნულების წერტილს მიაღწიოს. ის თუ რისგან შედგება სასარგებლო დატვირთვა კერძო შეხედულებაზეა დამოკიდებული. კომუნიკაციის შრისათვის, რომელსაც ზედნადები მონაცემი თავისი ფუნქციონირებისათვის სჭირდება, სასარგებლო დატვირთვა ზოგჯერ გულისხმობს ზედნადები მონაცემის ნაწილს, რომელსაც ეს შრე ამუშავებს. თუმცა, ზოგადად, სასარგებლო დატვირთვა ეს ისეთი მონაცემია, რომელიც მიეწოდება საბოლოო მომხმარებელს დანიშნულების ადგილას[318].

PASSWORD - პაროლი

[317] ეკონომიკური თანამშრომლობისა და განვითარებოს ორგანიზაციის ვირუსული პროგრამების კვლევა

[318] ეკონომიკური თანამშრომლობისა და განვითარებოს ორგანიზაციის ვირუსული პროგრამების კვლევა

სიტყვა, ფრაზა ან კლავიშთა კომბინაცია, რომელიც ზღუდავს კომპიუტერში ან პროგრამაში შესვლას მისი დაცვის მიზნით.

PCMCIA CARDS – ადაპტორის ბარათი პორტატიული მოწყობილობების კომპიუტერულ ქსელში ჩასართავად

ადაპტორის ბარათი საკრედიტო ბარათს ჰგავს, თუმცა მასზე სქელია. იგი თავსდება „ლეპტოპის“ ან „პალმტოპის“ ღიობში და მრავალი ფუნქციის შესრულების საშუალებას იძლევა; ისეთი ფუნქციებისა, რომელიც როგორც წესი, კომპიუტერს (მოდემს, ადაპტორს, მყარ დისკს და ა.შ.) არ გააჩნია.

PERSONAL COMPUTER (PC) – პერსონალური კომპიუტერი

ტერმინი, რომელიც როგორც წესი აღნიშნავს IBM ან სხვა თავსებად კომპიუტერს. იგი გამოიყენება ისეთი კომპიუტერის აღსანიშნად, რომელსაც კონკრეტული დროის მანძილზე მხოლოდ ერთი მომხმარებელი ჰყავს.

PERSONAL ORGANIZER OR PERSONAL DIGITAL ASSISTANT (PDA) – პირადი ციფრული ასისტენტი

ეს არის მცირე ზომის მოწყობილობა, რომელიც ითავსებს ტელეფონის, მისამართების წიგნისა და დღიურის ფუნქციებს. მასში ასევე ინახავენ სხვა სახის ინფორმაციასაც.

PHISHING – ფიშინგი

ფიშინგი (პაროლის მოპოვება) არის ტერმინი, რომელიც გამოხატავს ქმედებას, რომლის დროსაც გაყალბებული იმეილით და/ ან ვებ-გვერდის მეშვეობით ხდება კანონიერი ორგანიზაციის ან ვებ-გვერდის ვინაობის მისაკუთრება. ამ ქმედების მიზანია მომხმარებლის შეცდომაში შეყვანა რათა მან გასცეს პირადი ფინანსური ინფორმაცია, მაგალითად, საკრედიტო ბარათის ნომერი, ანაბრის მომხმარებლის ვინაობა და პაროლი, სოციალური დაზღვევის ნომერი და ა. შ. მიღებული ინფორმაციის საშუალებით კი შემდგომ ხდება თაღლითობის ჩადენა. ამ დანაშაულს ხშირად „ვინაობის ქურდობას “ უწოდებენ.

PIRATE SOFTWARE – მეკობრული კომპიუტერული პროგრამა

უკანონოდ გადაწერილი კომპიუტერული პროგრამა.

PORT – პორტი

სიტყვა პორტს სამი მნიშვნელობა აქვს.

პირველი – ეს არის ადგილი, სადაც ხდება ინფორმაციის კომპიუტერში შესვლა ან გამოსვლა. მაგალითად, პერსონალური კომპიუტერის თანმიმდევრულ პორტთან ხდება მოდემის მიერთება.

მეორე - ინტერნეტში პორტი აღნიშნავს ნომერს, რომელიც URL –ს ნაწილია და რომელიც ჩნდება ორი წეტილის (:) შემდეგ, უშუალოდ დომეინის სახელის შემდეგ. ეს კომპიუტერში შემავალი ან გამომავალი ისეთივე ვირტუალური ჭიშკარია, როგორც ზემოთ ნახსენები ფიზიკური ჭიშკარი. სპეციალურ პროგრამებს პორტი საშუალებას აძლევს ინტერნეტის მეშვეობით დაამყაროს კავშირი სხვადასხვა კომპიუტერებს შორის. მაგალითად, http –ს ვებ ტრაფიკი მე-80 პორტზე ფუნქციონირებს. ყველა სტანდარტული იმეილი კი 110-ე პორტზე ფუნქციონირებს.

მესამე – პორტი ასევე ნიშნავს პროცესს, რომლის დროსაც ხდება პროგრამის ერთი ტიპის კომპიუტერიდან მეორე ტიპის

კომპიუტერისათვის ადაპტირება. მაგალითად, „ვინდოუს " პროგრამის ისე გარდაქმნა, რომ მან „მაკინტოშის " ტიპის კომპიუტერზე მუშაობა შეძლოს (პორტინგ)

PRETTY GOOD PRIVACY (PGP) – უზრუნველყოფილი განმარტოება (პრივატულობა)

კომპიუტერული პროგრამა, რომელიც უზრუნველყოფს დაშიფრვის მეშვეობით განმარტოებასა (პრივატულობას) და ავთენტურობის დადგენას. PGP ხშირად გამოიყენება ხელმოწერის გასაგზავნად, იმეილების დასაშიფრად და გასაშიფრად იმეილის მეშვეობით კომუნიკაციის უსაფრხოების ხარისხის გაზრდის უზრუნველყოფის მიზნით. დია PGP სტანდარტი განისაზღვრება, როგორც RFC 4880, რათა შესაძლებელი ყოფილიყო იმ ბრძანებების თავსებადობა, რომელიც PGP-ს განხორციელებას უზრუნველლყოფდა.

PROXY SERVER – შუამავალი სერვერი

ინტერნეტის სერვერი, რომელიც შუამავლის როლს კისრულობს როდესაც კლიენტი სხვა სერვერიდან კონკრეტული წყაროს მოძიების თხოვნის ბრძანებას იძლევა. იგი შეიძლება გამოყენებული იქნეს კლიენტის ინტერნეტ კავშირის შეზღუდვის გვერდის ასავლელად და/ ან კლიენტის ვინაობას დასამალად. ვირუსის გამავრცელებელ სისტემებს ხშირად შუამავალი სერვერის კონფიგურაციას უკეთებენ, რათა „ბოტნეტის " ოპერატორებმა მისი გამოყენება ან მომსახურების გაყიდვა შეძლონ (მაგალითად, გაგზავნონ „სპამი " (spam), გატეხონ ვებ საიტი, და ა. შ.)

PUBLIC DOMAIN SOFTWARE – კომპიუტერული პროგრამების საჯარო დომეინი

უფასოდ ჩამოსატვირთვი პროგრამები, ასევე ცნობილია, როგორც უფასო პროგრამული უზრუნველყოფა.

QUERY – მოთხოვნა

ძებნა ან თხოვნა. სამძებრო სისტემაში, საგნობრივ ცნობარსა თუ მონაცემთა ბაზებში კონკრეტული ინფორმაციის მოძიების მოთხოვნის გაგზავნა.

RAM – ოპერატიული მეხსიერება

ოპერატიული მეხსიერება პერსონალური კომპიუტერის ხანმოკლე მეხსიერებაა. მისი მეშვეობით პერსონალურ კომპიუტერზე მონაცემებზე მუშაობაა შესაძლებელი. ოპერატიულ მეხსიერებაში შენახული ინფორმაციაკომპიუტერის გამორთვისთანავე იშლება.

REMOVABLE MEDIA – ინფორმაციის მატარებელი, რომელიც კომპიუტერს ეხსნება

ესენია, მაგალითად, ფლოპი დისკი, სი-დი, დი-ვი-დი, კარტრიჯი, ფირი ინფორმაციის შესანახად, რომელიც შემდეგ ეხსნება კომპიუტერს.

REMOVABLE MEDIA CARDS – მოსახსნელი მეხსიერების ბარათი ფოტოაპარატის კომპიურტერთან დასაკვშირებლად

მცირე ზომის მონაცემთა შესანახი მოწყობილობა, უფრო ხშირად გამოიყენება ისეთ ციფრულ ტექნიკაში როგორიც არის ფოტოაპარატი, ციფრული დღიური და „პლეიერი". თუმცა მათი გამოყენება ჩვეულებრივი ინფორმაციის შესანახად სავსებით შესაძლებელია, შემდეგ კი ეს ინფორმაცია შეიძლება კომპიუტერშიც იქნეს გადატანილი.

ბარათზე ინფორმაცია არ ქრება მას შემდეგ რაც ის ქსელიდან გამოირთვება; იგი ასევე სხვადასხვა მოწყობილობაზე შეიძლება გადატანილი იქნებს.

ROOTKIT[319] – ფესვური კომპლექტი (რუტკიტი)

„რუტკიტი“ არის პროგრამების კომპლექტი, რომელიც იმისათვის შეიქმნა, რომ შეინიღბოს ის ფაქტი, რომ კომპიუტერში მოხდა შეღწევა მაქსიმალურად პრივილიგირებულ „მთავარ, ფესვის “ დონეზე; ამისათვის იგი საოპერაციო სისტემური ფაილების მოდიფიცირებას ახდენს ან აქტიური პროცესის მექსიერებაში კოდის შეყვანის გზით. ვირუსის გამავრცელებელი პროგრამის მსგავსად, „რუტკიტს “ ადმინისტრატორის მოსაწვდომობა უნდა ჰქონდეს რათა მან ეფექტიანად იმუშაოს, ხოლო მას შემდეგ რაც მოხდება მისი დამონტაჟება პრაქტიკულად შეუძლებელია მისი აღმოჩენა. „რუტკიტის “ დანიშნულებაა, რომ მომხმარებელი ვერ მიხვდეს, რომ კომპიუტერი, საოპერაციო სისტემა და სხვა მოწყობილობები (მაგ., ანტ-ვირუსი ან ანტი- ჯაშუში პროგრამა,), რომლებიც მოწოდებულია აღმოაჩინონ მავნე ფაილების არსებობა და ამისთვის ისინი ჩამოტაჟებული არიან კომპიუტერში, გატეხილია. უმეტეს შემთხვევაში, როგორც კი მოხდება „რუტკიტის “ ჩამონტაჟება, ვერცერთი ანტი-ვირუსი ვეღარ ფუნქციონირებს. აღსანიშნავია, რომ „რუტკიტი “ საჭირო არ არის იმისათვის, რომ მოხდეს მავნე პროგრამების არსებობის შენიღბვა. მავნე პროგრამების უმრავლესობას თავად შეუძლია გააუვნებლოს უსაფრთხოების სისტემები ან „რუტკიტის “ გარეშე გვერდი აუაროს მათ.

SERVICE PROVIDER[320] – სერვის –პროვაიდერი (მომსახურების მიმწოდებელი)

I. ნებისმიერი საჯარო ან კერძო პირი, რომელიც მომხმარებელს სთავაზობს უზრუნველყოს მისი კომუნიკაცია კომპიუტერული სისტემის მეშვეობით; და
II. ნებისმიერი პირი, რომელიც ამუშავებს ან ინახავს კომპიუტერულ ინფორმაციას ამგვარი მომსახურების ან ამ მომსახურების კლიენტის სახელით.

SHAREWARE – პირობით უფასო პროგრამული უზრუნველყოფა

კომპიუტერული პროგრამა, რომელიც ტესტირების მიზნით უფასოდ ვრცელდება და იგულისხმება, რომ თუ მომხმარებელის მას ტესტირების პერიოდის შემდეგაც გამოიყენებს, იგი ამისათვის თანხას გადაიხდის. ზოგიერთ ასეთ პროგრამას შიგნით აქვს ვადა ჩადგმული.

SMART CARD – „გონიერი “ ბარათი (სმარტ-ბარათი)

პლასტმასისაგან დამზადებული ბარათი ჩამონტაჟებული ელექტრონული ჩიპით, რომელიც შეიცავს ელექტრონული მარკერის მნიშვნელობას. მისი შეძენა შესაძლებელია საცალო სავაჭრო ობიექტებში ან „ონლაინ “ მაღაზიებში.

[319] ეკონომიკური თანამშრომლობისა და განვითარებოს ორგანიზაციის ვირუსული პროგრამების კვლევა

[320] კონვენცია კიბერ-დანაშაულის შესახებ, მუხლი 1.

SOCIAL ENGINEERING – სოციალური ტექნიკა

სხვის კომპიუტერში შეღწევის ბოროტი განზრახვის ტაქტიკა, რომლის დროსაც პროგრამის გამტეხი მოტყუებით სძალავს მომხმარებელს ან ადმინისტრატორს ინფორმაციას ან აიძულებს კონკრეტული ქმედების ჩადენას, რის შედეგად ხდება საინფორმაციო სისტემის უსაფრთხოების ხელყოფა. სოცტექნიკის მეთოდის გამოყენების მაგალითია შემდეგი, საინფორმაციო ტექნოლოგიების დახმარების სერვისს უკავშირდება პირი, თავს აცნობს როგორც ამ ორგანიზაციის თანამშრომელი და სთხოვს პაროლის შეცვლას; სინამდვილეში კი ყოველივე ამის მიზანია მიიღოს ქსელში არასანქცირებული შესვლის უფლება; მეორე მაგალითი: პირს ეგზავნება იმეილი ამ პირის ბანკის სახელით, სადაც კლიენტს თხოვენ თითი დააჭიროს „ფიშინგის " რესურსის უნიფიცირებულ მაჩვენებელს (URL) და მიაწოდოს საბანკო ანგარიშის პაროლი ცრუ ვებსაიტს, რომელსაც ბოროტმზრახველი აკონტროლებს. სოცტექნიკა ან სოციალური ინჟინერია კომპიუტერულ ინდუსტრიაში გამოყენებული ტერმინია; მას აგრეთვე „ნდობით მანიპულაციას " უწოდებენ. ტერმინი იმისათვის შეიქმნა, რომ გამიჯნულიყო გამოთვლითი ტექნიკა და პროგრამული უზრუნველყოფის შექმნის ტექნიკა სოციალური ინჟინერიისაგან, რომლის დროსაც თავდასხმა ხორციელდება საინფორმაციო სისტემის ადამიანურ კომპონენტზე.

SOFTWARE – პროგრამული უზრუნველყოფა

წინასწარ დაწერილი პროგრამა, რომლის მიზანია დახმარება გაუწიოს მომხმარებელს კონკრეტული დავალების შესრულებაში, მაგალითად, ქსელის მართვაში, ვების შექმნაში, ფაილების მართვაში, ტექსტის დამუშავებაში, საბუღალტრო ანგარიშსა და ინვენტრაიზაციაში.

SPAM – სპამი

„სპამი " აღნიშნავს ნებისმიერი სახის, პოტენციურად მავნე ელექტრონულ უსარგებლო შეტყობინებას. მავნე პროგრამულ უზრუნველყოფასა და „სპამს " შორის სულ უფრო მეტი კავშირი ვლინდება. უნდა აღინიშნოს, რომ წინამდებარე ანგარიშისათვის საინტერესოა „სპამის " მხოლოდ ის მნიშვნელობა, რომელიც მავნე კომპიუტერული პროგრამის გავრცელებას უკავშირდება[321].

SPOOFING – სპუფინგი (წვდომის უფლების მოტყუებით მოპოვება)

IP პაკეტის შექმნა და გაგზავნა გაყალბებული წყაროს IP მისამართის მეშვეობით. ეს შეიძლება გაკეთდეს ან იმისათვის, რომ გამგზავნმა თავისი ვინაობა დამალოს ან თავი სხვა პირად მოაჩვენოს, ან „უკუგაფანტვის " ეფექტის შესაქმნელად, რის შედეგად მოტყუებით შექმნილი ტრაფიკი მიემართება მსხვერპლ მთავარ კომპიუტერში, რომელიც ყალბ IP წყაროდ იქნა გამოყენებული.

SPYWARE[322] – ჯაშუში კომპიუტერული პროგრამა

ჯაშუში კომპიუტერული პროგრამა მავნე კომპიუტერული პორგრამის ერთერთი ფორმაა, რომელსაც შეუძლია ხელში ჩაიგდოს

[321] ეკონომიკური თანამშრომლობისა და განვითარებოს ორგანიზაციის ვირუსული პროგრამების კვლევა

[322] ეკონომიკური თანამშრომლობისა და განვითარებოს ორგანიზაციის ვირუსული პროგრამების კვლევა

ინფორმაციის კონკრეტული რაოდენობა მომხმარებლის შემავალი (კლავიატურა, თაგუნა) და გამომავალი (ეკრანი) მოწყობილობებიდან, ასევე სხვა შესანახი მოწყობილობებიდან (მეხსიერება, მყარი დისკი და სხვა), და გაუგზავნოს მიღებული ინფორმაცია თავდამსხმელს მომხმარებლის თანხმობის ან მისი აზრზე ყოფნის გარეშე. ზოგიერთ ამგვარ პროგრამას შეუძლია თვალი მიადევნოს იმ ვებგვერდებს, რომლითაც მომხმარებელი სარგებლობს და შემდეგ ეს ინფორმაცია გაუგზავნოს სარეკლამო სააგენტოს, ამ დროს კი მავნე პროგრამა ცდილობს ხელში ჩაიგდოს პაროლე ან საკრედიტო ბარათის ნომერი მაშინ, როდესაც მომხმარებელი მას ვებგვერდზე აფიქსირებს.

SYSTEM UNIT – სისტემური ბლოკი

სისტემური ბლოკი პერსონალური კომპიუტერის ყველაზე დიდი დეტალია. ეს არის ყუთი, რომელში უმთავრესი კომპონენტები შედის. წინ მას დისკის მამოძრავებელი (დრაივი) აქვს, ხოლო უკან პორტები, რომელთა მეშვეობით ხდება კლავიატურასთან, თაგუნასთან, პრინტერთან და სხვა მოწყობილობებთან კავშირი.

TAPE – მაგნიტური ლენტი

მაგნიტური ლენტი მაგნიტით დაფარული პლასტმასის გრძელი ზოლია. იგი ჩვეულებრივ კარტრიჯზეა დამაგრებული (რომელიც ვიდეო, აუდიო ან ფოტოაპარატის ლენტს ჰგავს), თუმცა ზოგჯერ შეიძლება კოჭზეც იყოს დახვეული (აუდიო ლენტის მსგავსად). გამოიყენება კომპიუტერული მონაცემების ჩასაწერად, როგორც კომპიუტერის ინფორმაციის სარეზერვო ბლოკი.

TRAFFIC DATA – ტრაფიკის მონაცემები

ნებისმიერი სახის კომპიუტერული ინფორმაცია, რომელიც დაკავშირებულია კომპიუტერული სისტემით კომუნიკაციასთან, რომელიც შეიქმნა კუმპიუტერული სისტემით, რომელიც იყო კომუნიკაციის ჯაჭვის ნაწილი და რომელიც მიუთითებს წარმოშობის წყაროს, მდებარეობას, მარშრუტს, დროს, თარიღს, ზომას, გრძლიობას ან მომსახურების ტიპს[323].

TROJAN (HORSE)[324] – ტროას (ცხენი)

ტროას ცხენი კომპიუტერული პროგრამაა, რომელიც ლიცენზირებულ პროგრამას ჰგავს, სინამდვილეში კი გააჩნია საიდუმლო ფუნქცია, რომელიც საშუალებას აძლევს მას გვერდი აუაროს უსაფრთხოების ზომებს და განახორციელოს არასანქცირებული თავდასხმა (პროგრამაში შეღწევა). ტროას ცხენს შეუძლია თავი მოაწონოს მომხმარებელს, შეთავაზებული ინსტრუმენტით მოხიბლული მომხმარებელი ჩატვირთას აღნიშნულ პროდუქტს კომპიუტერში და ამგვარად, ტროას ცხენი შეაღწევს მის კომპიუტერში. ტროას ცხენს შეუძლია რეაგირება მოახდინოს კლავიატურის ლოგერის და სხვა ჯაშუშპროგრამის შესაძლებლობაზე, ასევე სხვადასხვა ფუნქციაზე და უსაფრთხოების სისტემა მწყობრიდან გამოიყვანოს.

UNIX – უნიქსი

პოპულარული საოპერაციო სისტემა, რომელიც ძირთადად დიდ მრავალ-მომხმარებლიან სისტემაში გამოიყენება. უნიქსის სისტემები

[323] კონვენცია კიბერ დანაშაულის შესახებ, მუხლი 1.

[324] ეკონომიკური თანამშრომლობისა და განვითარებოს ორგანიზაციის ვირუსული პროგრამების კვლევა

აკონტროლებს ინტერნეტის პირვალიდ ფუნქციების უმრავლესობას და ინტერნეტის ვებ სერვერების 50% ზე მეტი მასზეა დაფუძნებული.

USB STORAGE DEVICES – იუ-ეს-ბის მონაცემთა შესანახი მოწყობილობა

მცირე ზომის მონაცემთა შესანახი მოწყობილობა, რომელიც სარგებლობს იუ-ეს-ბის პორტით. მასზე შეიძლება შევინახოთ დიდი მოცულობის ინფორმაცია, ხოლო მოწყობილობა თავის მხრივ ადვილი მოსახმარი და დასამალია. სიდიდით მანქანის გასაღების ან მარკერის ზომისაა და შეიძლება კისერზეც ჩამოიკიდოთ.

VIDEO BACKER - უკუკავშირის ვიდეო სიგნალი

პროგრამა, რომლის მეშვეობით კომპიუტერული ინფორმაცია დუბლირდება სტანდარტულ ვიდეოზე. მისი დათვალიერების დროს ინფორმაცია წარმოდგენილია წერტლებისა და ხაზების წყებით.

VIDEO CONFERENCING - ვიდეო კონფერენცია

გეოგრაფიულად სხვადასხვა ადგილას მყოფ ადამიანებს შორის კომუნიკაციის ცოცხლად დამყარება აუდიო, ვიდეო და ტექსტური საშუალებებით.

VIRUS[325] - ვირუსი

ბიოლოგიური სეხნიის ანალოგია. ვირუსი საიდუმლო კოდია, რომელიც ვრცელდება სხვა პროგრამის დაინფიცირებით და თვითონ ჯდება პროგრამაში. იმისათვის, რომ ვირუსი გააქტიურდეს საჭიროა ძირითადი პროგრამის ამუშავება, ანუ ადამიანის ჩარევის გარეშე იგი ვერ გააქტიურდება. ვირუსს მიაქვს სასარგებლო დატვირთვა, რომელიც შეიძლება შეიცავდეს მარტივ შეტყობინებას ან გამოსახულებას, რის გამოც იგი იკავებს მონაცემთა შესანახ სივრცეს ან მეხსიერებას და ზიანს აყენებს თქვენს კომპიუტერს, ხოლო თუ ეს მრავლობითია, მან შეიძლება დააზიანოს ფაილი, მოახდინოს მყარი დისკის გადაფორმატება ან სხვა მხრივ დააზარალოს თქვენი კომპიუტერი. ვირუსი მავნე პროგრამების ყველაზე ადრეული ფორმაა, რომლიც პირველად გასული საუკუნის 70-იან წლებში გამოჩნდა. მაშინ ეს შემთხვევით მოხდა ექსპერიმენტის ჩატარების დროს.

WEBCAM - ვებკამერა

ვებკამერა ინტერნეტთან დაკავშირებული აპარატია. სურათები და ფოტოები აიტვირთება ვებსაიტზე ფოტოაპარატიდან დროის რეგულარულ პერიოდებში, როგორც წესი, რამდენიმე წუთში ერთხელ. თუ შეხედავთ ვებგვერდს, საიდანაც კამერა მუშაობს, თქვენც იმასვე ხედავთ, რასაც კამერა – თითქმის მყისიერად.

WEBLOG –ვებლოგი

ვებლოგს უფრო ხშირად ბლოგს უწოდებენ. ეს არის დღიურის ან ჟურნალის მსგავსი რამ. მასში შეაქვთ მოკლე შეტყობინებები, რომელსაც ხშირადა ანახლებენ ხოლმე და რომელიც ქრონოლოგიურად არის დალაგებული; უახლესი ინფორმაცია გვერდის თავშია. ტექსტის გარდა ბლოგში შეიძლება ფოტო,

[325] ეკონომიკური თანამშრომლობისა და განვითარებოს ორგანიზაციის ვირუსული პროგრამების კვლევა

გამოსახულება, ხმა, არქივი და მასთან დაკავშირებული ლინქიც იყოს, ასევე მომნახულებლებსაც აქვთ საშუალებსა, რომ თავიანთი კომენტარი შეიტანონ.

WORD PROCESSOR – ტექსტური პროცესორი

გამოიყენება წერილების, ანგარიშებისა და დოკუმენტების დასაბეჭდად. გავრცელებული პროცესორებია: „ვორდსტარი “, „ვორდპერფექტი “ და „ემ-ეს-ვორდი “.

WORM[326] - ვორმი

„ვორმი “ თვითგავრცელებადია ვირუსია და მის გააქტიურებას არც ძირითადი პროგრამა და არც ადამიანის ჩარევა არ სჭირდება. სარგებლობს რა კომპიუტერის საოპერაციო სისტემის ან ჩამონტაჟებული პროგრამის ნაკლით იგი სწრაფად ვრცელდება ქსელის ან ინტერნეტის მეშვეობით კომპიუტერიდან კომპიუტერში. ვირუსი და „ვორმი “ მავნე პროგრამების ერთადერთი სახეობების, რომელთაც თვითგამრავლების უნარი აქვთ. ეს ორი ტერმინი სულ უფრო ხშირად ერთი და იგივე მნიშვნელობით გამოიყენება.

WIRELESS NETWORK CARD – უსადენო ქსელის ბარათი

გაფართოების პლატა, რომელიც უზრუნველყოფს კომპიუტერულ ქსელში უსადენო კავშირს კომპიუტერებსა და სხვა მოწყობილობებს შორის. იგი ცვლის ტრადიციულ ქსელურ სადენებს. ქსელში ჩართული მოწყობილობების პლატასთან კავშირი რადიო სიგნალით ხორციელდება.

ZIP DRIVE /DISK – ზიპ-დამგროვებელი / ზიპ-დისკი

3.5- დიუმიანი მოსახსნელი მონაცემების დამგროვებელი. დამგროვებელი პაკეტის მაკომპლექტებელია, რომელსაც შეუძლია დისკები კატალოგში შეიტანოს და ფაილები უსაფრთხოების მიზნით ჩაკეტოს.

[326] ეკონომიკური თანამშრომლობისა და განვითარებოს ორგანიზაციის ვირუსული პროგრამების კვლევა