ლამარა სურგულაძე

კომპიუტერული დანაშაული

კომენტარი

თბილისი
2003

კომპიუტერული დანაშაულის შესახებ ქართული სისხლის სამართლის ლიტერატურა შედარებით მწირია. წინამდებარე ნაშრომის მიზანია ნაწილობრივ მაინც შეავსოს ეს ხარვეზი და ამით გარკვეული დახმარება გაუწიოს როგორც სამართალდამცავ ორგანოებს, ისე იურიდიული ფაკულტეტის სტუდენტებს და ამ საკითხით დაინტერესებულთ.

რედაქტორი: ზაზა ნანობაშვილი

გამომცემელი: იურიდიული ფირმა
"ბონა კაუზა"

თბილისი, 2003

ISBN 99940-764-5-0

კომპიუტერული დანაშაული

შესავალი

ელექტრონულ-გამომთვლელი ტექნიკის და მისი შემადგენელი ნაწილის – კომპიუტერის დანერგვამ მრავალ დადებით მოვლენასთან ერთად უარყოფითი შედეგიც – კომპიუტერული დანაშაული გამოიწვია. ეს ნეგატიური ტენდენცია მნიშვნელოვნადაა დამოკიდებული მეცნიერულ-ტექნიკური პროგრესის შეუფერხებელ სრდაზე და კომპიუტერიზაციის მზარდი ტემპების კვალდაკვალ ამ დანაშაულის დონე კიდევ უფრო მაღლა აიწევს. როგორც გაერთიანებული ერების ორგანიზაციის გენერალური მდივნის მოხსენებაშია ნათქვამი – დანაშაულებრივი დაჯგუფებები ახალი ტექნოლოგიური საშუალებების გამოყენებით უკანონოდ ითვისებენ მილიონობით თანხებს, "აცოცხლებენ" დანაშაულებრივი გზით მოპოვებულ უზარმაზარ ფულად სახსრებს, თავს არიდებენ გადასახადს, კომპლექსურ ღონისძიებებს ატარებენ სხვადასხვა დანაშაულის მოსამზადებლად, ჩასადენად და შესანიღბად.[1] სპეციალისტების მიერ პროგნოზირებულია კომპიუტერის გამოყენებით ორგანიზებული დანაშაულის სწრაფი ზრდის ტემპები.

ეს უპირველესად იმითაა პირობადებული, რომ მეცნიერულ-ტექნიკურმა რევოლუციამ სერიოზული

[1] Доклад генерального секретаря ООН. Воздействие организованной преступной деятельности на общество в целом. Мат. комиссии по предупреждению преступности и уголовному правосудию. Вена, 19-23 апреля E (с № 15) 1993/3).

სოციალური ძერები გამოიწვია, რომელთა შორის აღსანიშნავია საზოგადოებრივი ურთიერთობებისა და საზოგადოებრივი რესურსის ახალი სახის – ინფორმაციული ურთიერთობების წარმოშობა. ინფორმაცია თანამედროვე საზოგადოებრივი ცხოვრების ერთ-ერთი ძირითადი საფუძველთაგანი, ამ საზოგადოების საქმიანობის საგანი და პროდუქტია. თანამედროვე საზოგადოება ოთხ ძირითად რესურსს იყენებს – ბუნებრივ სიმდიდრეს, შრომას, კაპიტალს და ინფორმაციას[2]. რამდენადაც ინფორმაცია თანამედროვე საზოგადოების ცხოვრების მნიშვნელოვანი ნაწილი გახდა, ამდენად მისი წარმოქმნის, შეგროვების, დამუშავების, შენახვის, გავრცელების პროცესმა სტიმული მისცა ამ პროცესის წარმოების იარაღის – ელექტრონულ - გამომთვლელი ტექნიკის (ეგტ), ტელეკომუნიკაციის, კავშირგაბმულობის პროგრესს.

ნორმები კომპიუტერული დანაშაულის შესახებ პირველ რიგში ინფორმაციის დაცვის მიზნითაა შექმნილი და ნორმები, რომლითაც ელექტრონულ-გამომთვლელი ტექნიკის მოქმედების სამართლებრივი ასპექტებია რეგლამენტირებული სამართლის სხვადასხვა დარგში, მათ შორის სისხლის სამართალშია გათვალისწინებული. მაგრამ ამ ნორმების უშუალო ანალიზამდე მიზანშეწონილია კომპიუტერულ ტექნიკასთან დაკავშირებით იმ ცნებების ელემენტარულ დონეზე მაინც ანოტირება, რომლებიც კომპიუტერულ

[2] Вехов В.Б. Компьюерные преступления вчера, сегодня, завтра. Караганда, 1995. стр. 21.

დანაშაულობებშია მოხსენიებული ან საერთოდ მათ უკავშირდება.

კომპიუტერი არის ელექტრონულ-გამომთვლელი მანქანა (ეგმ-ი), რომელიც ინფორმაციას რიცხობრივ ფორმაში გარდაქმნის. იგი განკუთვნილია ინფორმაციის მისაღებად, დასამუშავებლად, შესანახად და გასაცემად.

ეგმ-ის სისტემაში მოიაზრება კომპლექსი, რომელშიც თუნდაც ერთი ეგმ-ი წარმოადგენს სისტემის ელემენტს ანდა რამდენიმე ეგმ-ი ქმნის სისტემას, ანუ ეს არის ელექტრონული მოწყობილობის კომპლექსი, რომელიც პროგრამით ან მოსარგებლის მითითებით აწარმოებს ოპერაციას ინფორმაციაზე, კერძოდ, ინფორმაციის შეტანის, გამოტანის, განადგურების, ბლოკირების, მოდიფიცირების, მოპოვების და სხვა სახის ოპერაციას.

ამოცანის ერთობლივი გადაჭრის მიზნით, რამდენიმე კომპიუტერი ერთიანდება. ეს მაშინ ხდება, როდესაც ცალკე აღებულ თითოეულ მათგანს, სიმძლავრის ან სწრაფქმედების უკმარისობის გამო, არ ძალუძს დასახული ამოცანის გადაწყვეტა. ასეთი გაერთიანება პროგრამულ-ორგანიზაციული უზრუნველყოფის მიზნით გულისხმობს კავშირს ტელეკომუნიკაციურ არხთან.

ეგმ-ის ქსელი არის კომპიუტერების, კავშირგაბმულობის საშუალებებისა და არხების ერთობლიობა, რომელიც დაშორებულ ეგმ-ებს შორის კავშირის დამყარებას უზრუნველყოფს.

ეგმ-ის ქსელით მოსარგებლე თავისი სამუშაო ადგილიდან იღებს იმ ინფორმაციასთან შეღწევის და გამოთვლითი რეზულტატებით სარგებლობის შესაძლებლობას, რომელიც ქსელში და მასთან დაკავშირებულ ეგმ-ში ცირკულირებს. ეს არ გამორიცხავს მოსარგებლისათვის დახურულ კომპიუტერულ ინფორმაციასთან შეღწევის გზაზე ბარიერის შექმნას.

ელექტროკავშირის ქსელი გამომთვლელი ტექნიკის საშუალებასთან ერთად წარმოადგენს ინფორმაციის შეკრების, დამუშაევბის, დაგროვების და გავრცელების პროცესის ტექნიკურ ბაზას.

ელექტროკავშირის ქსელს განეკუთვნება ერთიანი, ცენტრალიზებული მართვით უზრუნველყოფილი, ტექნოლოგიურად შეუღლებული ელექტროკავშირის ქსელის კომპლექსი.

საერთო სარგებლობის ელექტროქსელი საქართველოს ურთიერთდაკავშირებული ელექტროკავშირის შემადგენელი ნაწილია, რომლით სარგებლობა ყველას შეუძლია და არავის არ შეიძლება უარი ეთქვას მომსახურებაზე.

ელექტროკავშირის უწყებრივი ქსელი იქმნება საწარმოო და სხვა სპეციალური მიზნებისათვის და ჩართულია საერთო სარგებლობის ელექტროკავშირის ქსელში.

შიდასამრეწველო და ტექნოლოგიური ელექტროკავშირის ქსელში მოიაზრება საქართველოს აღმასრულებელი ორგანოების, საწარმოების, დაწესებუ-

ლებების, ორგანიზაციების ელექტროკავშირის ქსელი, რომელიც იქმნება შიდასამრეწველო და ტექნოლოგიური პროცესების სამართავად და არ არის ჩართული საერთო სარგებლობის ელექტროკავშირის ქსელში.

ელექტროკავშირის საერთო ქსელიდან გამოიყოფა ფიზიკური და იურიდიული პირების ელექტროკავშირის ქსელი, რომელიც არ არის ჩართული საერთო სარგებლობის ელექტროკავშირის ქსელში.

ელექტროკავშირის ამ ქსელებით მოსარგებლეს შეუძლია შეაღწიოს როგორც ელექტროკავშირის საერთო სარგებლობის ქსელში, ისე საზღვარგარეთის ცალკეულ ქვეყანაში ფუნქციონირებად ელექტროკავშირის ქსელში (ინტერნეტში).

სავალდებულო არ არის ეგმ-ის მუდმივი ჩართვა ელექტროკავშირის ქსელში. შესაძლებელია მისი გამორთვა და გარედან შემომავალი კომპიუტერული ინფორმაციის ბლოკირება. მოსარგებლეს, რომლის კომპიუტერი მუდმივად არ არის ჩართული ელექტროკავშირის ქსელში, შეუძლია ტელეფონის საშუალებით განსაზღვრული დროით (მაგალითად, ორი-სამი საათით) მიიღოს კოდი ელექტროკავშირის ქსელში ჩასართავად.

მანქანა-მატარებელი არის ყოველგვარი სახის მაგნიტური დისკი, მაგნიტური ლენტა, მაგნიტური დოლი, პერფიკარტი, ნახევარგამტარი სქემები და სხვა, რომლებიც კლასიფიცირდებიან მათი ფიზიკური და კონსტრუქციული თავისებურებების მიხედვით.

ინფორმაციაში დამოუკიდებლად მისი გადმოცემის ფორმისაგან, ზოგადად იგულისხმება მონაცემები პირის, საგნის, ფაქტის, მდგომარეობის, გარემოების და პროცესების შესახებ.

დოკუმენტური ინფორმაცია (დოკუმენტი) არის მანქანა-მატარებელზე დაფიქსირებული ინფორმაცია რეკვიზიტებითურთ, რაც მისი იდენტიფიცირების საშუალებას იძლევა. ინფორმაცია მოქალაქეების შესახებ (პერსონალური მონაცემები) არის მონა-ცემები მოქალაქის ცხოვრების, ფაქტების, ხდომი-ლების, გარემოების შესახებ, რაც მისი პიროვნების იდენტიფიცირების საშუალებას წარმოადგენს.

ინფორმაცია, რომელიც ელექტროკავშირის ქსელშია ან ცირკულირებს, კომპიუტერული ინფორმაციის სახელწოდებით არის ცნობილი ანუ კომპიუტერული ინფორმაცია არის მანქანა – მატარებელზე დაფიქსირებული ან ტელეკომუნიკაციური არხებით გადაცემული ინფორმაცია, რომელიც შეიცავს მონაცემებს პირის, საგნის, ფაქტის, ხდომილების, გარემოების შესახებ და განთავსებულია ეგმ-ში, ეგმ-ის სისტემაში ან მათ ქსელში.

კომპიუტერული ინფორმაციის თავისებურება მის მარტივ გადაგზავნასა, შეცვლასა და გამრავლებაშია. იგი ადვილად ინახება პირველწყაროში, ეგმ-ის მეხსიერებაში და რეალიზდება მანქანა-მატარებლის მეშვეობით, რომელიც ასევე გამოიყენება როგორც დამამახსოვრებადი მოწყობილობა. კომპიუტერული ინფორმაცია შეიძლება იყოს გარეგანი (მაგალითად, ნებისმიერად დაყენებული დისკეტი) და შინაგანი,

რომელიც ჩართულია ეგმ-ის კონსტრუქციაში. ეგმ-ის შინაგანი მეხსიერება რეალიზდება პროცესორის მეშვეობით და შეიცავს იმ მონაცემებს, რომლებიც უშუალოდ მონაწილეობენ ოპერაციაში.

კომპიუტერული ინფორმაცია შეიძლება გადაიცეს ტელეკომუნიკაციის არხით ერთი ეგმ-დან მეორეზე, ეგმ-იდან გამოსახულების ამსახველ მოწყობილობაზე (მაგალითად, დისპლეიზე), ეგმ-დან მოწყობილობის სამართავ გადამცემზე. ტელეკომუნიკაციის არხები შესატყვისი საპროგრამო უზრუნველყოფით აკავშირებენ ცალკეულ ეგმ-ს სისტემასთან ან ქსელთან.

<u>ინფორმაციული სისტემა</u> არის დოკუმენტების და ინფორმაციული ტექნიკის ორგანიზაციულად მოწესრიგებული ერთობლიობა, სადაც ინფორმაციული პროცესების რეალიზაციისათვის გამოყენებულია კომპიუტერული ტექნიკა და კავშირგაბმულობის საშუალებები.

<u>ინფორმაციულ პროცესად</u> მიჩნეულია ინფორმაციის მოძიების, დამუშავების, დაგროვების, შენახვის და გავრცელების პროცესი.

საზოგადოებაში მიმდინარე ინფორმაციული პროცესების შედეგია ახალი სოციალური ურთიერთობების შექმნა-ჩამოყალიბება და უკვე არსებულის შეცვლა.

<u>ინფორმაციულ რესურსს</u> წარმოადგენს ინფორმაციულ სისტემაში (ბიბლიოთეკაში, არქივში, ფონდში, მონაცემების ბანკში და სხვა) არსებული ცალკეული დოკუმენტი ან დოკუმენტების კრებული.

ინფორმაციული რესურსის მესაკუთრე არის სუბიექტი, რომელსაც გააჩნია ინფორმაციული რესურსის საკუთრების, მფლობელობის, სარგებლობის, განკარგვის სრული უფლებამოსილება.

ინფორმაციით მოსარგებლე (მომხმარებელი) არის ის, ვინც მიმართავს მისთვის საჭირო ინფორმაციულ სისტემას ან შუამავალს ინფორმაციის მისაღებად ან ინფორმაციით სარგებლობისათვის. ინფორმაცია და ინფორმაციული რესურსი წარმოადგენს საქონელს, აქედან გამომდინარე ყველა შედეგითურთ.[3]

ყოველივე ზემოაღნიშნული მოცულია ახალი საინფორმაციო ტექნოლოგიის ცნებით (ასტ).[4]

ეგმ-ის პროგრამა არის მოცემულობის და კომანდის ერთობლიობის ობიექტური ფორმა, რომელიც გარკვეული რეზულტატის მისაღებად ელექტრონულ-გამომთვლელი მანქანის (ეგმ) და სხვა კომპიუტერული მოწყობილობის ფუნქციონირებისათვისაა განკუთვნილი. ეგმ-ის პროგრამაში იგულისხმება დამუშავების პროცესში მიღებული მასალა და მის მიერ წარმოქმნილი აუდიოვიზუალური გამოსახულება.

ეგმ-ის პროგრამით რეალიზდება რაიმე ამოცანის გადაწყვეტის ალგორითმი. ეგმ-ის პროგრამის შექმნა

---

[3] Карас И.З. Экономический и правовой режим информационных ресурсов. В кн. Право и информатика. М., 1990, с. 40 -41.

[4] Айламазян А.К., Стась Е.В. Информатика и теория развития. М., 1989, с. 31.

ნიშნავს მისი ალგორითმის დაწერას ანუ ლოგიკური ბრძანებების თანმიმდევრობას, შემდეგში მათი ეგმ-ის მანქანურ ენაზე გარდასაქმნელად.

არსებულ პროგრამაში ცვლილებების შეტანა გულისხმობს ალგორითმის შეცვლას, მისი ფრაგმენტების გამოდევნის, სხვითი შეცვლის ან სხვა ალგორითმის დამატების გზით.

§1. კომპიუტერული დანაშაული

ზოგადი მიმოხილვა

კომპიუტერული დანაშაული სოციალური კონტროლის სფეროში 70-იანი წლების დასაწყისში შემოვიდა. ჯერ კიდევ 1950 წლიდან მოყოლებული აშშ-ში მრავალი ასეთი სახის ქმედება გამომჟღავნდა. ამ ფაქტმა მაშინ სისხლის სამართლის იუსტიციისა და მეცნიერ იურისტთა ყურადღება მიიზიდა და დაიწყო ამ ფენომენის ინტენსიური კვლევა ეროვნულ თუ საერთაშორისო დონეზე. თავდაპირველად იუსტიციის ორგანოები, რომლებიც კომპიუტერულ დანაშაულს წააწყდნენ, შეეცადნენ მასთან ბრძოლა ქურდობის, თაღლითობის, ნდობის ბოროტად გამოყენების და ა.შ. ტრადიციული დანაშაულის ნორმებით ეწარმოებინათ. მაგრამ საკითხისადმი მსგავსი მიდგომა წარუმატებელი აღმოჩნდა იმ უბრალო მიზეზის გამო, რომ ტრადიციულ დანაშაულთა შემადგენლობა ვერ მოიცავდა მრავალ

კომპიუტერულ დანაშაულს (მაგალითად, კომპიუტერის "მოტყუებით" ფულის ერთი ანგარიშიდან მეორეზე გადატანა). ეს დანაშაული ვერც ქურდობის და ვერც თაღლითობის მუხლებით ვერ დაკვალიფიცირდებოდა. პირველ შემთხვევაში არაა ქურდობის საგანი – "მატერიალური ნივთი" (ფული აქ არა ნივთის, არამედ კომპიუტერულ მატარებელზეა ინფორმაციის სახით დაფიქსირებული), მეორე შემთხვევაში კომპიუტერული მოტყუება სინამდვილეში ისევეა შესაძლებელი, როგორც დავუშვათ, სეიფის გასაღების მოტყუება. ასევე კომპიუტერული სისტემის მატერიალური ელემენტის დაზიანების გარეშე, ამ სისტემის ინფორმაციული ელემენტის განადგურება არც ქონების დაზიანების ან ქონების განადგურების კვალიფიკაციით იყო შესაძლებელი, თუნდაც მსგავს ქმედებას მნიშვნელოვანი ქონებრივი ხასიათის ზიანი გამოეწვია.

კრიმინალური რეალობისა და სისხლისსამართლებრივი ნორმების ერთმანეთთან შეუსაბამობამ დღის წესრიგში ამ უკანასკნელის განვითარების მოთხოვნა დააყენა. განვითარება ძირითადად ორი მიმართულებით წავიდა: 1. არსებული სისხლისსამართლებრივი ნორმების უფრო ფართო განმარტებისა და 2. კომპიუტერული დანაშაულის შესახებ სპეციალური ნორმების შემუშავების გზით. პირველი მიმართულება მოქცეულია გარკვეულ ჩარჩოებში; უკანონობას რომ არ მიეცეს გასაქანი, ამ საზღვრების გადაცილება დაუშვებელია. ამიტომაც ევროპის ქვეყნების უმრავლესობამ კომპიუტერული დანაშაულის შესახებ

სპეციალური ნორმების შემუშავება არჩია. უკვე 1973 წელს, შვედეთმა მიიღო კანონი კომპიუტერული დანაშაულის შესახებ. ნორმები კომპიუტერული დანაშაულის შესახებ, შედარებით გვიან მიიღო დიდმა ბრიტანეთმა, ავსტრიამ, დანიამ, საფრანგეთმა, აშშ-მა, კანადამ, ავსტრალიამ და სხვა ქვეყნებმა.

გამომუშავდა კომპიუტერული დანაშაულის ცნებაც. მაგალითად, პარიზში, 1983 წელს ეკონომიკური თანამშრომლობის ორგანიზაციის ექსპერტთა ჯგუფმა ჩამოაყალიბა კომპიუტერული დანაშაულის სისხლის-სამართლებრივი ცნება როგორც ყოველგვარი მონაცემების დამუშავებისა და მათი გადაცემის სფეროში უკანონო, არაეთიკური და ნებადაურთველი ქმედება.[5]

გამოიკვეთა კომპიუტერული დანაშაულის სხვადასხვა ჯგუფები: კომპიუტერული ეკონომიკური დანაშაული, კომპიუტერული დანაშაული პირადი უფლებებისა და ხელშეუხებლობის სფეროში, კომპიუტერული დანაშაული საზოგადოებისა და სახელმწიფო ინტერესების წინააღმდეგ და სხვა.

ეკონომიკურ კომპიუტერულ დანაშაულთაგან ყველაზე გავრცელებული და საშიშია თაღლითობა (ავტომატიზირებული ინფორმაციული სისტემის ბორიტად გამოყენებით სხვის ხარჯზე არამართლ-ზომიერი გამდიდრება), კომპიუტერული - ეკონომიკური

---

[5] Уголовное право Российской Федерации. Особенная часть. Учебник для Вузов (под. ред. Б.В. Здравомыслова), М., 1996, стр. 347.

ვაშუშობა, პროგრამების ქურდობა, კომპიუტერული საბოტაჟი, კომპიუტერული მომსახურებისა და დროის ქურდობა, საინფორმაციო ავტომატურ სისტემაში თვითნებური შეღწევა და კომპიუტერის დახმარებით ტრადიციული ეკონომიკური დანაშაულის ჩადენა.

როგორც ლიტერატურაში აღინიშნა კომპიუტერული თაღლითობა, კომპიუტერულ მატარებელზე არსებული საბანკო ანგარიშებთან დაკავშირებული დანაშაული, პროგრამების ქურდობა, კომპიუტერული "მეკობრეობა" კომპიუტერული მომსახურების არამართლზომიერი მიღება, კომპიუტერული დროის ქურდობა ფართოდ არის გავრცელებული თანამედროვე ევროპასა და აშშ-ში და კომპიუტერული დანაშაულის მნიშვნელოვან ნაწილს შეადგენს.[6]

კომპიუტერული დანაშაული პირადი უფლებების ხელშეუხებლობის სფეროში ყველაზე ხშირად კომპიუტერულ სისტემაში პიროვნების შესახებ არასწორი და არაკორექტული მონაცემების შეტანით, სწორი მონაცემების დამახინჯებით ან პიროვნების შესახებ მონაცემების უკანონო ხერხით შეგროვებაში გამოიხატება (მაგალითად, საბანკო ან საექიმო საიდუმლოების გახმაურება, ბანკების მიერ თავიანთი კლიენტების ნებართვის გარეშე მათი ინფორმაციის გახმაურება.

კომპიუტერული დანაშაული საზოგადოებრივი და სახელმწიფო ინტერესების წინააღმდეგ მოიცავს ინფორმაციის საზღვარგარეთ გადაცემის წესების

---

[6] Зибер У. Международная книга по компьютерной преступности. Чачестер, 1986.

დარღვევის, თავდაცვის სისტემის მუშაობის დეზორგანიზაციის, არჩევნების დროს ხმების დათვლისას და პარლამენტის გადაწყვეტილების მიღებისას ავტომატური სისტემის ბოროტად გამოყენების შემთხვევებს და ა.შ.

კომპიუტერული დანაშაულის ტრანსნაციონალურმა ხასიათმა ამ საკითხში სახელმწიფოთა საერთაშორისო გაერთიანების აუცილებლობა წარმოშვა. გარკვეული ნაბიჯები ამ მიმართულებით ჯერ კიდევ 1981 წლის 8 იანვარს გადაიდგა, როდესაც მიღებული იქნა ევროსაბჭოს კონვენცია პერსონალური მონაცემების დამუშავებასთან დაკავშირებით პიროვნების დაცვის თაობაზე. კონვენციის მე-7 მუხლის თანახმად, კონვენციის ხელმომწერმა სახელმწიფოებმა ივალდებულეს მიიღონ სათანადო ზომები მონაცემების ბაზაში დაგროვილი პერსონალური მონაცემების დასაცავად, კერძოდ, მონაცემები დაცული უნდა ყოფილიყო შემთხვევითი ან არასანქციონირებული განადგურებისა და გავრცელებისაგან.

გარკვეული ღონისძიებები ამ მხრივ გატარდა დამოუკიდებლ სახელმწიფოთა თანამეგობრობის მიერაც. 1996 წლის 18 ოქტომბერს ამ სახელმწიფოთა მეთაურებმა შეიმუშავეს ერთობლივი კონცეფცია ინფორმაციული სივრცის ჩამოყალიბების შესახებ. კონცეფციის მე-7 მუხლში ლაპარაკია ამ სახელმწიფოთა საკუთარი ინფორმაციული უსაფრთხოების უზრუნველყოფისა და ინფორმაციული სუვერენიტეტის დაცვის ღონისძიებების შესახებ.

საქართველო დამნაშავეობასთან ბრძოლის ურთიერთდახმარების შავი ზღვის სახელმწიფოთა ეკონომიური თანამშრომლობის ხელშეკრულების მონაწილეა. ამ ხელშეკრულებას ხელი მოაწერა ალბანეთმა, აზერბაიჯანმა, ბულგარეთმა, მოლდავეთმა, რუმინეთმა, რუსეთმა, თურქეთმა, სომხეთმა, უკრაინამ. მხარეები შეთანხმდნენ განსაკუთრებით მძიმე დანაშაულის წინააღმდეგ ბრძოლაში თანამშრომლობის საკითხებზე. ამ დანაშაულთა შორის დასახელებულია დანაშაული მაღალი ტექნოლოგიის სფეროში – მათ შორის კომპიუტერული დანაშაული.

ელექტრონული ტექნიკის მე-4 და მე-5 თაობის შექმნამ კიდევ უფრო მაღალი და განუსაზღვრელი წარმოებითი შესაძლებლობებით, მათმა ფართოდ დანერგვამ ეკონომიკის, სოციალურ და მმართველობით საქმიანობაში, ინფორმაციის ღირებულებითი მნიშვნელობის გაზრდამ წარმოშვა პროცესების საერთაშორისო სამართლებრივი რეგულირების კიდევ უფრო დიდი მოთხოვნილება. ლაპარაკია ინფორმაციული "ტერორიზმის" წინააღმდეგ ბრძოლის საერთაშორისო ბრძოლის ღონისძიებების შემუშავების აუცილებლობაზე. "დღეს უკვე იქმნება მწვავე აუცილებლობა საერთაშორისო სამართლებრივი ბაზის შესამუშავებლად ინფორმაციის გაცვლასთან დაკავშირებული ინციდენტების თავიდან ასაცილებლად, საერთაშორისო ხასიათის კომპლექსური ზომების შესამუშავებლად, რომელიც დაგვიცავს ეროვნული და გლობალური ხასიათის ინფორმაციულ

რესურსებზე ზემოქმედების საშუალებების დესტრუქციული გამოყენებისაგან."[7]

2000 წლის ვენის დეკლარაციის მე-18 პუნქტში ჩაიწერა რეკომენდაციების შემუშავების აუცილებლობაზე იმ დანაშაულთა შესახებ, რომლებიც კომპიუტერის გამოყენებასთანაა დაკავშირებული და წინადადება მიეცა დამნაშავეობის თავიდან აცილების სისხლის სამართლის მართლმსაჯულების კომისიას შეუდგეს მუშაობას ამ მიმართულებით.

ინფორმაციის და ინფორმაციული რესურსების გამოყენების წესების დარღვევამ შეიძლება მრავალი არასასურველი შედეგი გამოიწვიოს, როგორიცაა მათი დაკარგვა, გატაცება, დამახინჯება, გაყალბება, მართვისა და კონტროლის ავტომატიზირებული სისტემის პროგრამის დარღვევა, ეგმ-ის და მისი სისტემის მუშაობის მოშლა, რაც თავის მხრივ ასევე შეიძლება უმძიმესი შეუქცევადი პროცესების მიზეზი გახდეს.

საქართველოში ეკონომიკურ, სოციალურ თუ პოლიტიკურ სფეროებში გარდამავალი პერიოდისათვის დამახასიათებელი სიძნელეების გათვალისწინებით და ასევე კომპიუტერული დანაშაულის საერთაშორისო ზრდის დინამიკიდან და ქვეყნის საყოველთაო კომპიუტერიზაციიდან გამომდინარე უნდა გაგვჩენოდა მისი ფართოდ გავრცელების

---

[7] Вус М.А., Войтович Н.А., Гусев В.С. Россия на пороге информационного общества. Материалы семинара 22 апреля, 1997 г, Спб. 1997.

ვარაუდი. რამდენედაც პარადოქსალურად არ უნდა მოგვეჩვენოს საქართველოს უზენაესი სასამართლოს სტატისტიკური განყოფილების მონაცემების თანახმად, დღესდღეობით სასამართლო პრაქტიკაში ეს დანაშაული საერთოდ არ არის ფიქსირებული. ეს გარემოება შეიძლება ორი ძირითადი მიზეზით აიხსნას; პირველი: დანაშაულთა ერთობლიობის წესის გვერდის ავლით კომპიუტერული დანაშაულის შერწყმა იმ დანაშაულთან, რომელიც კომპიუტერულ დანაშაულთან ერთად კვალიფიცირდება ისე, რომ თვით კომპიუტერული დანაშაული უკვე აქ აღარ ფიგურირებს; მეორე: პრაქტიკოს მუშაკთა უმრავლესობისათვის ჯერჯერობით გაუგებარია აღნიშნული დანაშაულის არსი და მნიშვნელობა. აქ მხოლოდ ის შეიძლება ითქვას, რომ ჩვენს სინამდვილეში კომპიუტერული დანაშაული ტრადიციული დანაშაულის ზრდის ტემპებს გაუსწრებს. ამაზე თუნდაც 2003წ. 2 ნოემბრის სამპარლამენტო არჩევნებიც მეტყველებს, როდესაც საარჩევნო ბარათების კომპიუტერული დამუშავების პროცესში მოხდა საარჩევნო სიების არნახული გაყალბება.

კომპიუტერული დანაშაული პირველად 1999 წლის 22 ივლისს მიღებულმა საქართველოს სისხლის სამართლის კოდექსმა გაითვალისწინა. ამით კანონმდებელი შეეცადა სისხლისსამართლებრივი ღონისძიებებით მაქსიმალურად შეემცირებინა ის ნეგატიური მოვლენები, რაც ეგმ-სა და შესაბამის ინფორმაციასთან არაკეთილსინდისიერ მოპყრობას მოსდევს.

საერთოდ, კომპიუტერული დანაშაულის ცალკე, დამოუკიდებელ ჯგუფად გამოყოფას მრავალი მომხრე

გამოუჩნდა, მაგრამ მათ განსხვავებული შეხედულება აქვთ იმ სიკეთის ანუ ობიექტის თაობაზე, რასაც უშუალოდ ხელყოფს კომპიუტერული დანაშაული. მაგალითად, ნ. პოლევოი თვლის, რომ კომპიუტერულ დანაშაულში იგულისხმება ის მართლსაწინააღმდეგო ქმედება, რომლის ობიექტს ან ჩადენის იარაღს ელექტრონულ-გამომთველელი მანქანა წარმოადგენს.[8] არ შეიძლება არ გაიზიაროთ ნ. პოლევოის აზრი იმის თაობაზე, რომ კომპიუტერულ დანაშაულში ელექტრონულ გამომთველელი მანქანა იარაღის როლს ასრულებს, მაგრამ ვერ დავეთანხმებით მის მტკიცებას, თითქოს ელექტრონულ-გამომთველელი მანქანა ამ დანაშაულის ობიექტს წარმოადგენდეს. საყოველთაოდ მიღებული შეხედულების თანახმად, დანაშაულის ობიექტია ის სამართლებრივი სიკეთე, რაც ზიანდება ან რასაც დაზიანების საფრთხე ემუქრება და რასაც იცავს სისხლის სამართალი, ანუ დასჯადი უმართლობა, დაზიანებული სისხლისსამართლებრივი სიკეთის ერთმნიშვნელოვანია.[9] თუ ელექტრონულ-გამომთველელი მანქანა დაზიანდა ან განადგურდა, მაშინ დანაშაული ქონებრივ დანაშაულთან ერთობლიობით უნდა დაკვალიფიცირდეს.

ჯერ ერთი, ამ სისტემის "მუშაობის მოშლაში", რომელიც კოდექსის (284, 285, 286) მუხლებშია

---

[8] Полевой Н.С. и др. Правовая информатика и кибернетика. Учебник. М., 1993. стр. 43.

[9] Mezger, Straftrecht. En lehrbuch. Muncherr und Leipzig, 1933, 5, 69 (ნასარგებლებია: თ. წერეთელი, გ. ტყეშელიძე. მოძღვრება დანაშაულზე. თბილისი, 1969, გვ. 162).

მითითებული, აუცილებლობით სისტემის განადგურება ან დაზიანება როდი იგულისხმება; მეორეც გამომთვლელი მანქანა, რომელიც კომპიუტერულ დანაშაულში იარაღის როლს ასრულებს, არ მიეკუთვნება იმ მნიშვნელობის ქონებრივი ხასიათის საკეთეს, რომლის გათვალისწინებით კანონმდებელი სისხლის სამართლის კოდექსში დამოუკიდებელ, ახალ თავს შექმნიდა.

სისხლის სამართლის ლიტერატურაში გამოითქვა აზრი, რომლის თანახმად კომპიუტერული დანაშაული არის სისხლის სამართლის კანონით გათვალისწინებული საზოგადოებრივად საშიში ქმედება, სადაც მანქანური ინფორმაცია წარმოადგენს დანაშაულის საგანს ან ობიექტს.[10]

არც ეს შეხედულება შეიძლება იქნეს გაზიარებული: მანქანური ინფორმაცია არ შეიძლება იყო დანაშაულის საგანი. დანაშაულის საგანი არის შესაბამისი დანაშაულის შემადგენლობით გათვალისწინებული მატერიალური ნივთი, რომელზედაც მიმართულია დამნაშავის მოქმედება. კომპიუტერულ ინფორმაციას კი არ გააჩნია დანაშაულის საგნისათვის დამახასიათებელი ეს ძირითადი ნიშანი, მას მატერიალურ ნივთად ვერც ერთ შემთხვევაში ვერ აღვიქვამთ. მით უმეტეს ვერ ჩავთვლით კომპიუტერულ

[10] Курс уголовного права. Учебник для вузов, под. ред. Г.Н. Борзенкова и В.С. Комиссарова. М., 2002, стр. 634.

ინფორმაციას დანაშაულის ობიექტად, რადგან მანქანური ინფორმაცია არც ზიანდება და არც დაზიანების საფრთხე ემუქრება.

არის გამოთქმული სხვა მსგავსი შეხედულებებიც, რომელთა გადმოცემას მხოლოდ იმიტომ ავუარეთ გვერდი, რომ ისინი უკვე გადმოცემული მოსაზრებების მოდიფიცირებულ ვარიანტებს წარმოადგენენ.[11]

ნაწილობრივ გასაზიარებელია ი.კლეპიცკის მოსაზრება კომპიუტერული დანაშაულის როგორც გვარეობითი, ისე უშუალო ობიექტის შესახებ. კერძოდ, კომპიუტერული დანაშაულის ზოგადი დახასიათებისას იგი აღნიშნავს, რომ აქ დანაშაულის გვარეობით ობიექტს წარმოადგენს მონაცემების ავტომატიზირებული სისტემის გამოყენებისას მონაცემების დამუშავებასთან დაკავშირებით ფიზიკური და იურიდიული პირების, საზოგადოების და სახელმწიფოს უფლებები და ინტერესები. კომპიუტერული ინფორმაციის სფეროში ცალკეულ დანაშაულთა ობიექტია კომპიუტერული სისტემის გამოყენებასთან დაკავშირებული კონკრეტული უფლებები და ინტერესები, როგორიცაა: სისტემის მფლობელის უფლება სისტემაში არსებული ინფორმაციის ხელშეუხებლობაზე, ასევე სისტემის სწორ ექსპლუატა-

[11] იხ. მაგალითად, Вехов В.В. Компьютерные преступления: способы совершения и раскрытия. М., 1996. стр. 24.

ციასთან დაკავშირებული ინტერესები.[12]

აღნიშნულიდან გამომდინარე გასაზიარებელია ლიტერატურაში გამოთქმული აზრი, რომლის თანახმად კომპიუტერული დანაშაულის ჯგუფურ ანუ გვარეობით ობიექტს იმ საზოგადოებრივი ურთიერთობის ერთობლიობა წარმოადგენს, რაც დაკავშირებულია ინფორმაციისა და ინფორმაციული რესურსების უსაფრთხო წარმოებასა, გამოყენებასა და გავრცელებასთან და მათი სათანადო დაცვის უზრუნველყოფასთან.[13] მაგრამ გასაზიარებელი არ არის ავტორის აზრი კომპიუტერული დანაშაულის საგნის შესახებ. აქ იგი აშკარად არათანმიმდევრობას იჩენს, როდესაც კომპიუტერული დანაშაულის საგნად ინფორმაციას აღიარებს და აღნიშნავს, რომ "სისხლის სამართლის კოდექსის 28-ე თავთან მიმართებაში (საქ. სსკ.-ის 35–ე თავი – ხაზგასმა ჩვენია – ლ.ს.) კანონმდებელმა დანაშაულის საგანი მხოლოდ იმ კომპიუტერული ინფორმაციით შემოფარგლა, რომელიც არის უშუალოდ ეგმ-ში, ეგმ-ის სისტემაში ან მათ ქსელში

"დანაშაულის საგანს წარმოადგენს კომპიუტერული ინფორმაცია".[14] თუმცა, ცოტა ქვევით იგივე ავტორი მიუთითებს, რომ "ინფორმაცია არ შეიძლება

---

[12] Уголовное право Российской Федерации. Особенная часть (под.ред. Б.В. Здравомыслова). М., 1996, стр. 350 – 351.

[13] Уголовное право Российской Федерации. Особенная часть (под.ред. Г.Н. Берзенкова и В.С. Комиссарова), М., 2002, стр. 537.

[14] там же

იყოს საკუთრების წინააღმდეგ მიმართული დანაშაულის მოცემული ჯგუფის საგანი, რადგან მას არ გააჩნია ფიზიკური ნიშანი. ამიტომ არ შეიძლება მისი გატაცება, დაზიანება ან განადგურება ამაშია კომპიუტერული ინფორმაციის თავისებურება".[15] უნდა ითქვას, რომ დანაშაულის საგანს ყველა შემთხვევაში ერთნაირი ნიშნები ახასიათებს, რომელიც საერთოა, როგორც ქონებრივი, ისე სხვა სახის, მათ შორის კომპიუტერული დანაშაულისათვის და ამაზე უკვე იყო ლაპარაკი.

კანონმდებელმა იმ შედეგების (ფართო მნიშვნელობით) გათვალისწინებით, რაც კომპიუტერულ დანაშაულს შეუძლია გამოიწვიოს (ეროვნული უსაფრთხოების სისტემის, უმსხვილესი საწარმოების, სადისპეტჩერო სამსახურის და სხვა სფეროში), იგი საზოგადოებრივი უშიშროების წინააღმდეგ დანაშაულთა კატეგორიას მიაკუთვნა და შესაბამისად, სისხლის სამართლის კოდექსის მე-9 კარში 35-ე თავად გაითვალისწინა. მაგრამ საკითხის ასეთი გადაწყვეტა მეტად ზოგადი ხასიათის იქნებოდა, თუ არ დავაკონკრეტებდით იმ სიკეთეს, რომელსაც უშუალოდ ხელყოფს კომპიუტერული დანაშაული. ამის დადგენა იმდენადაც არის მნიშვნელოვანი, რამდენადაც კომპიუტერული დანაშაულის სხვა დანაშაულისგან გამიჯვნის შესაძლებლობას იძლევა. როგორც

[15] Уголовное право Российской Федерации. Особенная часть (под.ред. Г.Н. Берзешкова и В.С. Комиссарова), М., 2002, стр. 537.

ცნობილია, დანაშაულის კონკრეტიზაციის ყველაზე დაბალ საფეხურს და ყველაზე მეტად პრაქტიკული მნიშვნელობის მქონესაც უშუალო ობიექტი წარმოადგენს.

მართალია, კომპიუტერული დანაშაული პარალელურად სხვა სიკეთესაც აზიანებს (პირადი უფლებები და ხელშეუხებლობა, ქონებრივი უფლებები და ინტერესები, საზოგადოებრივი და სახელმწიფოებრივი უშიშროება, კონსტიტუციური წესწყობილება და ა.შ.), მაგრამ მათ ვერ ვაღიარებთ კომპიუტერული დანაშაულის ობიექტებად.

კომპიუტერული დანაშაული მხოლოდ ინფორმაციულ სფეროში ჩადენილი დანაშაულია, როგორიცაა ელექტრონულ-გამომთვლელი სისტემის გამოყენებისას კონკრეტული უფლებები და ინტერესები (სისტემის მესაკუთრის უფლება იმ ინფორმაციის ხელშეუხებლობის თაობაზე, რომელიც სისტემაშია, სისტემის სწორ ექსპლუატაციასთან დაკავშირებული ინტერესები და ა.შ.) ამ დანაშაულს თავისი დამოუკიდებელი ობიექტი გააჩნია და არასწორი იქნებოდა გვეფიქრა, რომ ის სიკეთე, რომელიც ინფორმაციული ურთიერთობის ხელყოფით ზიანდება, ამ დანაშაულის ობიექტს წარმოადგენს. ეს რომ ასე იყოს, მაშინ სისხლის სამართლის კოდექსში კომპიუტერული დანაშაულის ცალკე თავად გამოყოფას აზრი დაეკარგებოდა. ხსნებული სხვა ობიექტების დაზიანების შემთხვევები დანაშაულთა ერთობლიობის წესისამებრ უნდა დაკვალიფიცირდეს.

რაც შეეხება ეგმ-ს, ეგმ-ის სისტემას და მათ

ქსელს, ისინი პრაქტიკაში განიხილება, როგორც დანაშაულის საგანი ან ინფორმაციის სფეროში დანაშაულის ჩადენის ტექნიკური საშუალება. მათი დაზიანების ან გატაცების შემთხვევაში იგი საკუთრების წინააღმდეგ დანაშაულის საგანად გვევლინება და შესაბამისად სსკ-ის 177–188 მუხლებით დაკვალიფიცირდება. კომპიუტერი, როგორც დანაშაულის ჩადენის ტექნიკური საშუალება, ისევე განიხილება როგორც იარაღი, ტრანსპორტი და სხვა. ამ თვალსაზრისით მას გამოყენებითი მნიშვნელობა აქვს.[16]

დროის თვალსაზრისით კომპიუტერული დანაშაულის ჩადენის დროდ ითვლება მართლსაწინააღმდეგო ქმედების ჩადენის დრო (ე.ი. კლავიატურის კლავიშზე ან "თაგვის" ღილაკზე თითის დაჭერის მომენტი), რითაც უკანასკნელი კომპიუტერული ბრძანება იგზავნება. შედეგის დადგომის დროს მნიშვნელობა არა აქვს. დრო, რომელიც შედეგს მოქმედებისაგან აშორებს, რაც ინფორმაციის არხში გავლას და კომპიუტერის მიერ ბრძანების შესრულებას დასჭირდება, შეიძლება მინიმალური იყოს და რამდენიმე წამს მოიცავდეს, მაგრამ ზოგჯერ დროის ეს მონაკვეთი შეიძლება გაიჭიმოს. ეს განსაკუთრებით სსკ-ის 285–ე და 286-ე მუხლებს შეეხება.)

უფრო რთულია კომპიუტერული დანაშაულის ადგილის განსაზღვრის საკითხი, რამდენადაც კომპიუტერულ დანაშაულთა უმრავლესობა კომპიუ-

---

[16] Уголовное право Российской Федерации под.ред. Г.Н. Берзенкова и В.С. Комиссарова, М., 1997, стр. 539-540.

ტერულ ქსელში ხდება, რომელიც რამდენიმე რეგიონს და ქვეყანას მოიცავს და რომელთა შორის წამყვანი ადგილი ინტერნეტს უკავია, ამდენად დანაშაულის ჩადენისა და შედეგის დადგომის ადგილს შეიძლება მრავალი კილომეტრიც და სახელმწიფო საზღვარი აშორებდეს.

საქართველოს სისხლის სამართლის კოდექსი არ შეიცავს დანაშაულის ჩადენის ადგილის განმსაზღვრელ ნორმას,[17] ამიტომაც დანაშაულის ჩადენის ადგილი შეიძლება იყოს, როგორც ქმედების ჩადენის, ისე შედეგის დადგომის ადგილი, ან ის ადგილი, სადაც დანაშაული აღიკვეთა ან დამთავრდა.

§2. კომპიუტერულ ინფორმაციასთან არამართლზომიერი შეღწევა (მუხლი 284)

1. კანონით დაცულ კომპიუტერულ ინფორმაციასთან, ესე იგი მანქანა–მატარებელზე, ელექტრონულ გამომთვლელ მანქანაზე (ეგმ-ზე) ეგმ-ის სისტემაში ან მათ ქსელში ასახულ ინფორმაციასთან არამართლზომიერი შეღწევა, რასაც ინფორმაციის განადგურება, ბლოკირება, მოდიფიცირება ან მოპოვება ანდა ეგმ-

[17] გერმანიის სსკ-ი შეიცავს ნორმას დანაშაულის ადგილის შესახებ: "დანაშაულის ჩადენის ადგილად ითვლება ის ადგილი, სადაც პირი მოქმედებდა და უნდა ემოქმედა, ანდა ის ადგილი სადაც დადგა სისხლის სამართლის კანონით გათვალისწინებული შედეგი. თანამონაწილისათვის დანაშაულის ჩადენის ადგილია ის ადგილი, სადაც ეს დანაშაული იქნა ჩადენილი, ხოლო თუ იგი სხვა ადგილას მოქმედებდა – მისი მოქმედების ადგილი (§9, პ. 1, 2). ანალოგიურად წყვეტს საკითხს პოსტსაბჭოური სივრციდან ლიტვის სსკ (მუხ. 4, პ.2)

ის, ეგმ-ის სისტემის ან მათი ქსელის მუშაობის მოშლა გამოიწვია, -

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

2. იგივე ქმედება, ჩადენილი:

ა) წინასწარი შეთანხმებით პირთა ჯგუფის მიერ;

ბ) სამსახურებრივი მდგომარეობის გამოყენებით;

გ) იმის მიერ, ვისაც ხელი მიუწვდებოდა ეგმ-ზე, ეგმ-ის სისტემაზე ან მათ ქსელზე, -

ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ან ტუსაღობით ვადით ოთხ თვემდე ანდა თავისუფლების აღკვეთით ვადით ხუთ წლამდე.

3. ამ მუხლის პირველი ან მე-2 ნაწილით გათვალისწინებული ქმედება, რამაც გამოიწვია მძიმე შედეგი, -

ისჯება ჯარიმით ან თავისუფლების აღკვეთით ვადით ხუთ წლამდე.

სსკ-ის 284-ე მუხლით გადმოცემული დანაშაული მატერიალური დელიქტია და მისი დამთავრებულად ცნობისათვის აუცილებელია მუხლში ჩამოთვლილი ალტერნატიული შედეგებიდან ერთ-ერთის მაინც განხორციელება.

დანაშაულის უშუალო ობიექტია კომპიუტერული სისტემის მფლობელის ხელშეუხებლობის უფლება სისტემაში არსებულ ინფორმაციაზე.

დანაშაულის ობიექტური მხარე მოქმედებით –

კანონით დაცულ ინფორმაციასთან არამართლზომიერი შეღწევით და ამ მოქმედებით გამოწვეული შედეგით – ინფორმაციის განადგურებით, ბლოკირებით, მოდიფიცირებით, მოპოვებით, ეგმ-ის, ეგმ-ის სისტემის და მათი ქსელის მუშაობის მოშლით გამოიხატება. ობიექტურ მხარეში მოიაზრება ასევე მიზეზობრივი კავშირი ჩადენილი მოქმედებასა და დამდგარ შედეგს შორის.

კანონის ტექსტის თანახმად, დანაშაულად ითვლება არა ყოველგვარ, არამედ მხოლოდ კანონით დაცულ ინფორმაციასთან შეღწევა.

საჭიროა გაირკვეს, თუ რა იგულისხმება "კანონით დაცულ ინფორმაციაში". საქმე ისაა, რომ საქართველოს დღესდღეობით არ გააჩნია ზოგადად ინფორმაციის და კერძოდ კომპიუტერული ინფორმაციის დაცვის კანონი. ამ კანონის მიღებამდე კომპიუტერული ინფორმაციის დაცვის საფუძველი სხვადასხვა ხასიათის ნორმატიულ აქტებში უნდა იქნეს მოძიებული. ასეთს წარმოადგენენ მაგალითად, საქართველოს ზოგადი ადმინისტრაციული კოდექსი (თავი III), კანონი "სახელმწიფო საიდუმლოების, შესახებ", აგრეთვე ნორმები საკუთრების, საავტორო უფლების, პირადი, კომერციული თუ სხვა საიდუმლოების შესახებ და სხვა.

კომპიუტერული ინფორმაციის სამართლებრივი საფუძვლები ტელესაკომუნიკაციო ელექტროკავშირის საერთაშორისო ორგანიზაციის სამართლებრივი პრინციპებით და იმ ნორმებით რეგულირდება, რომელთა შემდგომი კონკრეტიზაცია მხარეთა შორის

დადებული ხელშეკრულებით ხდება. ხელშეკრულება იდება კომპიუტერული ინფორმაციული ურთიერთობების რამდენიმე სუბიექტს შორის: ინფორმაციის გადამცემსა (ინფორმატორი და გენერატორი), ინფორმაციის მიმღებსა (მოსარგებლე, მომხმარებელი), კავშირგაბმულობასა, რომლის საშუალებით გადაცემა ხორციელდება და ზოგჯერ შუამავალს შორის, რომელიც ინფორმატორს და მოსარგებლეს რთავს ქსელში. კონკრეტული ინფორმაციული ურთიერთობაში მხარედ ჩართვა მხოლოდ აღნიშნულ ჩარჩოშია შესაძლებელი.[18]

ინფორმაციული რესურსები საერთოდ ღია და ხელმისაწვდომია გარდა იმ დოკუმენტური ინფორმაციისა, რომელიც კანონით შეზღუდული შეღწევადობის კატეგორიას განეკუთვნება და, რომელთან არამართლზომიერ შეღწევას შეუძლია ზიანი მიაყენოს, როგორც ინფორმაციის მესაკუთრეს, ისე მის მფლობელსა და სხვა პირებს. ამ თვალსაზრისით კანონით დაცულ ინფორმაციაში მოიაზრება კანონით, თუ სხვა ნორმატიული აქტით, მათ შორის საუწყებო აქტით ან შინაგანაწესით დაცული დოკუმენტური ინფორმაცია, რომელიც ეფუძნება ამ აქტებს და ამოღებულია საჯარო (ღია) ბრუნვიდან. როგორც წესი, ასეთ ინფორმაციას გააჩნია შეზღუდული სარგებ-

[18] მარიამ ცაცანაშვილი. ინფორმაციული საზოგადოება და ინფორმაციის სამართლებრივი რეგულირება. თბილისი, 1999, გვ. 48-49

ლობის გრიფი, ანუ მისთვის კანონით დადგენილია დაცვის სპეციალური სამართლებრივი რეჟიმი.

შეზღუდული შეღწევადობის დოკუმენტური ინფორმაცია, მისი სამართლებრივი რეჟიმის პირობების მიხედვით იყოფა სახელმწიფო საიდუმლოების და კონფიდენციალურ ინფორმაციად.

კონფიდენციალურ ინფორმაციას მიეკუთვნება პერსონალური მონაცემები. არ დაიშვება სასამართლო გადაწყვეტილების გარდა, პირადი და ოჯახური მიმოწერის, სატელეფონო საუბრის, საფოსტო, სატელეგრაფო და სხვა შეტყობინების საიდუმლოების შესახებ ინფორმაციის შეგროვება, შენახვა, გამოყენება, გავრცელება იმ პირის თანხმობის გარეშე, ვისაც ინფორმაცია შეეხება.

ინფორმაცია რამდენიმე ჯგუფად იყოფა. მაგალითად, ცნობები: 1. პირადი ცხოვრების ფაქტების, ხდომილების, გარემოების შესახებ, რომლებიც პიროვნების იდენტიფიცირების შესაძლებლობას იძლევიან; 2. ცნობები, რომლებიც გამოძიების და სამართალწარმოების საიდუმლოებას შეიცავენ, ასეთი ცნობები შეიძლება გამომძიებლის და პროკურორის ნებართვით გახმაურდნენ; 3. სამსახურებრივი საიდუმლოების შემცველი ცნობები; 4. პროფესიული საიდუმლოების შემცველი ცნობები (საექიმო საიდუმლოება, ნოტარიალური საიდუმლოება, საადვოკატო საიდუმლოება, აღსარების საიდუმლოება) და სხვა ხასიათის ცნობები, რომლებიც გამოიყენება ფარული სამძებრო-ოპერატიული ღონისძიებების

ჩატარებისას; 5. კომერციულ საქმიანობასთან დაკავშირებული ცნობები (კომერციული საიდუმლოება). /ზოგჯერ კომერციული საიდუმლოება ემთხვევა სამსახურებრივ საიდუმლოებას; / 6. საბანკო საიდუმლოება, რომელიც არ განეკუთვნება კომერციულ საიდუმლოებას; 7. გამოგონების არსის, სასარგებლო მოდელის ან სამრეწველო ნიმუშის შესახებ ცნობების საიდუმლოება – მათ შესახებ ინფორმაციის ოფიციალურ პუბლიკაციამდე (ამ საიდუმლოს იცავს საპატენტო კანონი); 8. შეზღუდული შეღწევადობის ინფორმაციას განეკუთვნება აგრეთვე ნაწარმოების ტექსტი (მას იცავს საავტორო კანონმდებლობა); 9. შეზღუდული შეღწევადობით ხასიათდება ეგმ-ის მონაცემების ბაზის პროგრამის ტექსტი მანამ, სანამ წარმოიშობოდეს ასეთი ცნობების თავისუფალი გამოყენების შესაძლებლობა.

შეზღუდული შეღწევადობის ინფორმაციას არ წარმოადგენს დოკუმენტი, რომელიც შეიცავს ინფორმაციას განსაკუთრებული სიტუაციის (ეკოლოგიური, მეტეოროლოგიური, დემოგრაფიული, სანიტარულ-ეპიდემიოლოგიური და სხვა მსგავსი ხასიათის მდგომარეობის) შესახებ, რომელთა ცოდნა აუცილებელია საწარმოო ობიექტების და მოსახლეობის უსაფრთხოების უზრუნველსაყოფად.

შეზღუდული შეღწევადობის ინფორმაციად არ განიხილება ასევე ის დოკუმენტები, რომლებიც სახელმწიფო უშიშროების და ადგილობრივი თვითმმართველობის ორგანიზაციების საქმიანობის,

სახელმწიფო საბიუჯეტო საშუალებების, ადგილობრივი რესურსების და ეკონომიკის მდგომარეობის, მოსახლეობის მოთხოვნილებების შესახებ მონაცემებს შეიცავენ, გარდა იმ ცნობებისა, რომლებიც სახელმწიფო საიდუმლოებას განეკუთვნებიან.

არ მოიაზრება შეზღუდული შეღწევადობის კატეგორიად არც ის დოკუმენტები, რომლებიც ბიბლიოთეკების, არქივების ღია ფონდშია და სახელმწიფო ხელისუფლების, ადგილობრივი თვითმმართველობის ორგანოების, საზოგადოებრივი ორგანიზაციების ინტერესებს ასახავენ ანდა მოქალაქეთა უფლებების, თავისუფლებების და მოვალეობების რეალიზაციისათვის არიან აუცილებელი.

კანონით დაცულ კომპიუტერულ ინფორმაციასთან მხოლოდ არამართლზომიერი შეღწევა იწვევს სისხლისსამართლებრივ პასუხისმგებლობას. არამართლზომიერია ინფორმაციასთან შეღწევა, როდესაც პირს შეღწევის უფლება არ გააჩნია, ანდა თუმცა ასეთი უფლება აქვს, მაგრამ ინფორმაციის დაცვის წესების დარღვევით ახორციელებს მას.

ინფორმაციასთან არამართლზომიერი შეღწევა შეიძლება სხვადასხვა ხერხით გამოიხატოს. ჩადენის ხერხის მიხედვით იგი ძირითადად ორ ჯგუფად იყოფა: ა) ჩადენილი კომპიუტერული ტექნიკის გამოყენების გარეშე (ტრადიციული ხერხი) და ბ) შეღწევა მეცნიერების და ტექნიკის მიღწევების გამოყენებით. ამ უკანასკნელში შეღწევის მრავალი ხერხი მოიაზრება, მაგალითად "ელექტრონული შენიღბვა"

(სხვისი საიდენტიფიკაციო ნიშნების გამოყენება, როგორიცაა პაროლი, კოდი, პირადი საიდენტიფიკაციო ნომერი, სარეგისტრაციო ჟურნალის ჩანაწერი და ა.შ.), შეღწევა "კომპიუტერული აბორდაჟით" (კომპიუტერულ სისტემასთან შეღწევა სატელეფონო ხაზის გამოყენებით); "რღვეული" შეღწევა (კომპიუტერული ქსელის დამცავ სისტემაში სუსტი ადგილის პოვნით); "ელექტრონული მტვერის" მეშვეობით (მოსარგებლის მიერ წაშლილი, მაგრამ ჯერ კიდევ კომპიუტერულ მეხსიერებაში ნაწილობრივ შემონახული ფაილების შესწავლის გზით).[19]

გარდა აღნიშნულისა, კომპიუტერულ ინფორმაციასთან არამართლზომიერი შეღწევის სხვა ხერხებიც არსებობს. მაგალითად, მოსარგებლე, რომელიც დაშვებულია ერთ საინფორმაციო სისტემასთან ან კოლექტიური სარგებლობის ეგმ-თან, ჩვეულებრივ იმ ოპერაციის მიხედვით რანჟირდება, რომლის განხორციელების უფლებაც გააჩნია. ეს გამოიხატება როგორც ინფორმაციის ელემენტალურ გადახედვაში, ისე სისტემაში გამოყენებული მონაცემების ბაზასა და იმ პროგრამაში ცვლილების შეტანით, რომლითაც სისტემა მოქმედებს. მაგრამ ზოგჯერ ისეც ხდება, რომ ვინმე შეაღწევს რა, კომპიუტერულ სისტემაში, თავისთავს კანონიერ მოსარგებლედ აცხადებს. როგორც უკვე აღინიშნა,

[19] Айков Д., Сейгер К., Фокертох У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. М,, 1990.

კანონიერი მფლობელის ფაილში არამართლზომიერი შეღწევა სისტემის დაცვაში სუსტი ადგილის აღმოჩენითაც არის გაადვილებული. ამ ადგილის ერთხელვე აღმოჩენით, დამნაშავეს შეუძლია აუჩქარებლად გაეცნოს სისტემაში არსებულ ინფორმაციას, მრავალგზის დაუბრუნდეს მას, გადაიღოს იგი, ზუსტად ისევე, როგორც მყიდველი, რომელიც საქონელს ათვალიერებს ვიტრინაში ან კიდევ მკითხველი, რომელიც ბიბლიოთეკის თაროდან არჩევს მისთვის სასურველ წიგნს.

კომპიუტერულ ინფორმაციასთან არამართლზომიერი შეღწევა დაცვის ინტელექტუალური საშუალებების ნეიტრალიზაციითაც ხორციელდება. კომპიუტერულ ინფორმაციასთან არამართლზომიერი შეღწევა უმეტესწილად პოლიტიკური, კომერციული, ტექნოლოგიური საიდუმლოების შეტყობისა და ასევე იმ პროგრამული კომპლექსების გატაცების მიზნით ხორციელდება, რომლებიც არ არიან დაცულნი საავტორო სამართლის ნორმებით.[20]

აღნიშნულ საკითხთან დაკავშირებით სისხლის სამართლის ლიტერატურაში გამოითქვა აზრი, რომ თითქოს ინფორმაციის მიღებაზე ინფორმაციის მესაკუთრის ან მფლობელის თანხმობა არ უნდა გამორიცხავდეს აღნიშნულ დანაშაულს.[21]

---

[20] Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. М,, 1996.

[21] Наумов А.В. Коментарий к уголовному кодексу Российской Федерации. М., 1997., с. 669.

ამ მოსაზრებას ვერ დავეთანხმებით. ინფორმაცია და ინფორმაციული რესურსი ინტელექტუალური საკუთრების ობიექტია. "კომპიუტერული ინფორმაცია ეგმ-ის პროგრამისა და მონაცემების ბაზის სახით საავტორო სამართლის საგნად განიხილება, და როგორც საკუთრების ყოველ სხვა სახეზე, მასზედაც ვრცელდება სამოქალაქო სამართლის ნორმები საკუთრების შესახებ. კერძოდ, მესაკუთრეს უფლება აქვს თავისი შეხედულებისამებრ დაუბრკოლებლად განკარგოს საკუთრება, თუკი ეს არ ლახავს სხვათა კანონიერ უფლებებსა და ინტერესებს. პარადოქსულია, რომ ცოტა უფრო წინ იგივე ავტორი მიუთითებს: "ინფორმაციული რესურსების, ინფორმაციული სისტემების, ტექნოლოგიების, მათი უზრუნველყოფის საშუალებების მესაკუთრე არის სუბიექტი, რომელიც სრულად ახორციელებს ამ ობიექტის მფლობელობის, სარგებლობისა და განკარგვის უფლებამოსილებას..., ხოლო ჩამოთვლილი ობიექტების მფლობელი კი არის სუბიექტი, რომელიც ფლობს აღნიშნულ ობიექტს, სარგებლობს ამ ობიექტით და განკარგავს მათ კანონით დადგენილ ფარგლებში".[22]

ინფორმაციას, რომელიც შეზღუდული შეღწევადობით ხასიათდება, დაცვის თავისი რეჟიმი გააჩნია. რეჟიმი დგინდება ან კანონით ან საინფორმაციო რესურსების მესაკუთრის, ანდა ამისათვის სპეციალუ-

[22] Наумов А.В. Коментарий к уголовному кодексу Российской Федерации. М., 1997., с. 663.

რი რწმუნებით აღჭურვილი პირის მიერ. მაგალითად, სახელმწიფო საიდუმლოების შემცველი ინფორმაციის მიმართ – საქართველოს კანონით – "სახელმწიფო საიდუმლოების შესახებ", ხოლო კონფიდენციალური დოკუმენტური ინფორმაციის მიმართ – ინფორმაციული რესურსების მესაკუთრის მიერ ან სახელმწიფო კანონით განსაზღვრული უფლებამოსილი პირის მიერ, პერსონალური მონა-ცემების დოკუმენტების მიმართ - სახელმწიფო, კანონით.[23]

კომპიუტერული ინფორმაციის დაცვის საშუალებები მეტად მრავალფეროვანია. აქ მოიაზრება სასაშვო რეჟიმი, სიგნალიზაცია, გასამხედროებული დაცვა, ასევე ყოველგვარი ინტელექტუალური საშუალებები, რომლებიც აძნელებენ კომპიუტერულ ინფორმაციასთან არამართლზომიერ შეღწევას. ასეთია მაგალითად, შეღწევის ინდივიდუალური კოდი, სისტემასთან ინდენტიფიცირებული დიალოგი. ის სისტემები, რომელთაც არ გააჩნიათ აუტენტური იდენტიფიკაცია (მაგალითად, ფიზიოლოგიური მახასიათებლები: თითების ანაბეჭდი, თვალის ბადურის მოხაზულობა, ხმა და ა.შ.), დაუცველნი არიან. ინფორმაციასთან შეღწევის ყველაზე უმარტივესი გზაა კოდისა და კანონიერი მფლობელის ინდენტიფიცირებული შიფრის მიღება.

---

[23] Карас И.З. Экономический и правовой режим информационных ресурсов. В. кн. Право и информатика. М., 1990, стр. 40-41.

კომპიუტერული ინფორმაციის დაცვის საშუალებები ანუ ინფორმაციის დაცვის რეჟიმი შეიძლება ინფორმაციის მესაკუთრის მიერ ან მისი შეკვეთით, ინდივიდუალურად შეიქმნას. უმეტესად მაინც გამოიყენება დაცვის ტიპიური საშუალებები, რომლებიც შედიან ეგმ-ის პროგრამულ უზრუნველყოფაში.

ის ორგანოები, რომლებიც შეზღუდული შელწევადობის ინფორმაციას ამუშავებენ, აუცილებელ სერტიფიცირებას ექვემდებარებიან. ხოლო ორგანოები, რომლებიც კომპიუტერული ინფორმაციის დაცვის საშუალებებს აპროექტებენ, ღებულობენ ლიცენზიას ამ საქმიანობის თაობაზე.

თუ კომპიუტერული ინფორმაცია დახურულია, პროგრამა ავტომატურად წყდება. ზოგჯერ პერსონალის ყურადღების მისაქცევად გაისმის ხმოვანი სიგნალი.

კომპიუტერული ინფორმაციის დაცვის მრავალფეროვანი საშუალებების მიუხედავად, ათასი რჯულის "ხეკერები", "ელექტრონული კორსარები", "კომპიუტერული მეკობრეები"[24] ახერხებენ ამ ინფორმაციასთან შელწევას.

კომპიუტერული ინფორმაციის განადგურება ნიშნავს მის დაკარგვას, ეგმ-ის მეხსიერებიდან მის წაშლას, ე.ი. მის ან მისი ნაწილის გამოსაყენებლად უვარგის მდგომარეობაში მოყვანას; იმისგან დამო-

[24] ეს ის ხალხია, ვინც არამართლზომიერად იჭრება სხვის კომპიუტერულ ინფორმაციასთან.

უკიდებლად შესაძლებელია, თუ არა მისი აღდგენა. მაგრამ, როგორც წესი, ინფორმაციის განადგურებაში ისეთი შემთხვევა მოიაზრება, როდესაც ინფორმაციის დანაკარგის აღდგენა შეუძლებელია, რაც თავის მხრივ მისი წაკითხვისა და გამოყენების შესაძლებლობას სპობს. ინფორმაციის გადატანა სხვა მანქანა-მატარებელზე მხოლოდ იმ შემთხვევაში განიხილება ინფორმაციის განადგურებად, თუ ამ მოქმედებით გაძნელებული ან საერთოდ შეუძლებელია ინფორმაციასთან შეღწევა.

მოსარგებლის მიერ პროგრამული საშუალებების გამოყენებთ განადგურებული ინფორმაციის აღდგენა ან სხვა მოსარგებლისგან ამ ინფორმაციის მიღება, არ გაათავისუფლებს დამნაშავეს პასუხისმგებლობისაგან.

ინფორმაციის განადგურებად არ განიხილება ინფორმაციის შემნახველი ფაილის სახელწოდების შეცვლა, ისევე როგორც დროის მიხედვით უკანასკნელი ფაილის მიერ ფაილის ძველი ვერსიის ავტომატური გამოდევნა.

კომპიუტერული ინფორმაციის ბლოკირებაში იგულისხმება ინფორმაციის რეალური ფიზიკური არსებობის პირობებში, კომპიუტერულ სისტემასთან ან მის მიერ წარმოდგენილ ინფორმაციულ რესურსებთან მოსარგებლისათვის შეღწევის ან მათი გამოყენების შესაძლებლობის მოსპობა ან შეზღუდვა, რაც კომანდების თანმიმდევრობის აკრძალვით ან რომელიმე ხელსაწყოს მწყობრიდან გამოყვანით ხორციელდება.

კომპიუტერული ინფორმაციის განადგურებისა და ბლოკირებისაგან განსხვავდება კომპიუტერული ტექნიკის მწყობრიდან გამოყვანა. ამ შემთხვევაში ეგმ-ის პროგრამა ინფორმაციის ფაილის სახით, მოსარგებლის გარდა, ყველასათვის ხელმისაწვდომია.

კომპიუტერული ტექნიკის მწყობრიდან გამოყვანა შესაბამის შემთხვევაში შეიძლება საქართველოს სსკ-ის 285-ე მუხლით დაკვალიფიცირდეს, ხოლო თუ კომპიუტერის დაზიანების მიზეზი იმ კომპიუტერული ინფორმაციის განადგურება ან ბლოკირებაა, რომლითაც პროგრამა ოპერირებს, ქმედება კომპიუტერულ ინფორმაციასთან არამართლზომიერ შეღწევად განიხილება (სსკ-ის 284-ე მუხლი).

კომპიუტერული ინფორმაციის მოდიფიცირება წარმოადგენს დანაშაულის ჩადენამდე დაფიქსირებული ინფორმაციის შინაარსის შეცვლას, რაც შეიძლება გამოიხატოს ინფორმაციის ყოველგვარი ცვლილებით, გარდა იმ შემთხვევისა, როდესაც ეს ცვლილება ეგმ-ის ან მონაცემების ბაზისათვის განკუთვნილ პროგრამას უკავშირდება. ასეთი შემთხვევა, შესაბამისი პირობების არსებობისას სსკ-ის 285-ე მუხლით უნდა დაკვალიფიცირდეს.

ამრიგად, ინფორმაციის მოდიფიცირებაში იგულისხმება მესაკუთრის ან კანონიერი მოსარგებლის თანხმობის გარეშე პირველადი ინფორმაციის შეცვლა მატერიალურ მანქანა-მატარებელზე დამოუკიდებლად იმისა, არის ეს პროგრამა, მონაცემების ბაზა, თუ ტექსტური ინფორმაცია. ინფორმაციის მოპოვება არის

ორიგინალის შენახვის პირობებში მისი თუნდაც ერთი ასლის შექმნა. გამრავლება, გადაღება, გადაწერა, მატარებლის ხასიათისგან დამოუკიდებლად, სხვა მატერიალურ მატარებელზე გადატანა (ქაღალდი, მაგნიტი, ლაზერი და სხვ).*

ინფორმაცია შეიძლება გადაიწეროს ეგმ-ის შინაგანი მეხსიერების ფაილიდან, მისი გახსნით და ა.შ.

ამრიგად, ფაქტიურად ინფორმაციის მოპოვება არის მისი ტირაჟირება. კომპიუტერული ინფორმაციის გაცნობის მიზნით მოპოვებას (ხელით გადაწერა, ფოტოგრაფირება, დისპლეის ეკრანიდან გადაღება, ეგმ-ის გამოსხივებათა დაჭერა, ინფორმაციის შეჯერება, პრინტერის ხმაურის გაშიფრვა) ზოგიერთი ავტორი ინფორმაციის იმ მოპოვებად მიიჩნევს, რომელსაც სსკ-ის 284-მუხლის შემადგენლობა ითვალისწინებს.

ინფორმაციის მოპოვებაში მისი გატაცებაც მოიაზრება, მაგრამ სისხლის სამართლის კანონმდებლობისათვის ცნობილი ტრადიციული გატაცებისაგან განსხვავებით, იგი გაცილებით რთული მოვლენაა. ინფორმაციის, მათ შორის პროგრამული უზრუნველყოფის ინფორმაციის მოპოვება, ასლის არასანქცირებული გადაღების ანუ კოპირების გზით არ დაკვალიფიცირდება როგორც გატაცება, ვინაიდან

* ტერმინი "მოპოვება" ვერ ასახავს მასში ნაგულისხმევ შინაარსს. ეს არის ინფორმაციის გამრავლება ანუ კოპირება (copy-right).

გატაცება ყოველთვის ამოღებას უკავშირდება, ხოლო ინფორმაციის არასანქცირებული გადაღებისას, იგი შეიძლება არც იქნეს ამოღებული. ამიტომ, ამ შემთხვევაში ინფორმაცია განიხილება, როგორც სისხლისსამართლებრივი დაცვის დამოუკიდებელი ობიექტი.

კომპიუტერული ინფორმაციის გადაღება, თუ ეს მოხდა ამ ინფორმაციით მართლზომიერი სარგებლობის პირობებში, პროგრამული საშუალებების ავტომატური გაუმართაობის გამო, (მაგალითად, ფაილები ყოველი შეხებისას პერიოდულად გადაირთვებიან) არ წარმოადგენს დანაშაულს.

ეგმ-ის პროგრამული ჩანაწერების, პირველადი მონაცემების ბაზის დოკუმენტების და სხვა მსგავსი ინფორმაციის გადაწერა საბეჭდ მანქანაზე ან პრინტერზე ანდა აკრეფილი ტოპოგრაფიული საშუალებით, არ ქმნის სისხლის სამართლის კოდექსის 284-ე მუხლით გათვალისწინებული დანაშაულის შემადგენლობას და შესაბამის შემთხვევაში შეიძლება პასუხისმგებლობა გამოიწვიოს სისხლის სამართლის კოდექსის სხვა მუხლებით.

კანონით დაცულ კომპიუტერულ ინფორმაციასთან არამართლზომიერმა შეღწევამ შეიძლება ეგმ-ის, ეგმ-ის სისტემის ან მათი ქსელის მუშაობის მოშლა გამოიწვიოს, რაც თავის მხრივ შეიძლება მათი დანიშნულებისამებრ ფუნქციონირებისათვის დროებითი ან ხანგრძლივი დაბრკოლების მიზეზი გახდეს. კერძოდ, აქ იგულისხმება არაშტატური

სიტუაციის შექმნა, რაც დაკავშირებულია მოწყობილობის მუშაობაში შეფერხებასთან (არასწორი, მცდარი ინფორმაციის გაცემა, ინფორმაციის გაცემაზე უარის თქმა, ეგმ-ის, მისი ელემენტების ან მათი ქსელის მწყობრიდან გამოყვანა და სხვა), ყველა მსგავს შემთხვევაში აუცილებელია შენარჩუნებული იქნეს ეგმ-ის, მისი სისტემის ამ მათი ქსელის ფიზიკური მთლიანობა. თუ ზემოთ ჩამოთვლილ შედეგებთან ერთად ირღვევა ეგმ-ის, მისი სისტემის ან მათი ქსელის მთლიანობა, მაშინ მოქმედება დამატებით კვალიფიკაციას მოითხოვს საკუთრების წინააღმდეგ დანაშაულთა მუხლებით.

რთული კომპიუტერული სისტემების ფუნქციონირებისას შესაძლებელია ეგმ-ის მუშაობის დარღვევა ტექნიკური გაუმართაობის ან პროგრამული შეცდომის გამო. ასეთ შემთხვევაში პირი, რომელმაც არამართლზომიერად შეაღწია კომპიუტერულ ინფორმაციასთან, პასუხს არ აგებს სისხლისსამართლებრივი წესით, განზრახვისა და მიზეზობრივი კავშირის არარსებობის გამო ჩადენილ ქმედებასა და დამდგარ შედეგებს შორის.

სსკ-ის 284-ე მუხლი რამდენიმე მაკვალიფიცირებელ გარემოებას შეიცავს. ამათგან პირველია დანაშაულის ჩადენა წინასწარი შეთანხმებით პირთა ჯგუფის მიერ. იგულისხმება ჯგუფის მონაწილეთა მიერ იმ მოქმედების ჩადენა, რომელსაც ითვალისწინებს სსკ-ის 284-ე მუხლში გადმოცემული დანაშაულის ობიექტური და სუბიექტური ნიშნები

და არ გამოიხატება, მაგალითად, ამსრულებლისათვის დახმარების გაწევის წინასწარ დაპირებაში, მის წაქეზებაში ჩაიდინოს დანაშაული, დანაშაულის ორგანიზაციაში, რაც თავის მხრივ ჯგუფის მიერ წინასწარი შეთანხმებით დანაშაულის ჩადენას, დანაშაულში თანამონაწილეობად გადააქცევდა.

პირთა ჯგუფზე მითითება აუცილებლად გულისხმობს დანაშაულში ერთზე მეტი პირის მონაწილეობას. ჯგუფის მონაწილენი ერთმანეთს წინასწარ უთანხმებდებიან არა მხოლოდ ზოგადად დანაშაულის ჩადენა'ზე, არამედ 'ხოგიერთ ისეთ კონკრეტულ გარემოებაზეც, რომელიც ამ დანაშაულის ჩადენის პროცესში შეიძლება წარმოიშვას. შეთანხმება შეიძლება გამოიხატოს როგორც სიტყვიერად, ისე წერილობით, უფრო იშვიათად, კონკლუდენტური ფორმით (ე.წ. "მდუმარე შეთანხმება"). შეთანხმებისას, როგორც წესი, ზუსტდება მონაცემები დანაშაულის ობიექტისა და საგნის, დანაშაულის ჩადენის ხერხისა და სხვათა შესახებ. თუ შეთანხმება მოხდა, დანაშაულის ჩადენის პროცესში, დანაშაული კარგავს "წინასწარი შეთანხმების" ნიშანს და კვალიფიციური გარემოებაც გამოირიცხება. ასეთ შემთხვევაში თითოეული დამნაშავე პასუხს იმ ქმედებისათვის აგებს, რომელიც მან უშუალოდ ჩაიდინა, კერძოდ, სსკ-ის 284-ე მუხლის პირველი ნაწილით.

სსკ-ის 284-ე მუხლით გათვალისწინებული დანაშაულის მეორე მაკვალიფიცირებელი ნიშანია დანაშაულის ჩადენა სამსახურებრივი მდგომარეობის

გამოყენებით. აქ იგულისხმება ის პირი, ვისაც ხელი მიუწვდება ეგმ-ზე, ეგმ-ის სისტემაზე ან მათ ქსელზე. ამ შემთხვევაში ეგმ-თან შეღწევის უფლება პირს უჩნდება სწორედ გარკვეული სამსახურებრივი მოვალეობის ან გარკვეული სამუშაოს შესრულებასთან დაკავშირებით, ე.ი. ფაქტიურად ეგმ-ში, ეგმ-ის სისტემაში და მათ ქსელში შეღწევის უფლება გააჩნია იმას, ვისი პროფესიული საქმიანობა კანონიერ საფუძველზე მუდმივად ან დროებით დაკავშირებულია კომპიუტერული სისტემის ან ქსელის ფუნქციონირებასთან. (პროგრამისტი, ვისაც ინფორმაცია შეყავს ეგმ-ის მეხსიერებაში, მონაცემების ბაზის ადმინისტრატორი, ინჟინერ-ელექტრიკოსი, რემონტის მწარმოებელი, გამოთვლითი ტექნიკის ექსპლუატაციის სპეციალისტი, ეგმ-ის მომსახურებით მოსარგებლე და ა.შ.). ამ დროს ხსენებული პირები სცილდებიან თავიანთი უფლებამოსილების ფარგლებს და იმ სფეროში იჭრებიან, სადაც მათი უფლებამოსილება წყდება ანუ მთავრდება. მაგრამ აქ ისეთი შემთხვევაც მოიაზრება, როდესაც პირს თავისი სამსახურებრივი მდგომარეობის გამო შეუძლია ზემოქმედება მოახდინოს მასზე, ვისაც კომპიუტერულ ინფორმაციასთან შეღწევის უფლება გააჩნია. არ არის აუცილებელი, რომ დამნაშავე სახელმწიფო მოხელე იყოს.

სსკ-ის 284-ე მუხლის მე-3 ნაწილი აღნიშნული ქმედებებით მძიმე შედეგის გამოწვევას ითვალისწინებს.

მძიმე შედეგში მოიაზრება ადამიანის დაღუპვა, მისი ჯანმრთელობის დაზიანება, ტექნოლოგიური

პროცესების საშიში განვითარება, ქონების დიდი ოდენობით განადგურება და სხვა.

სსკ-ის 284-ე მუხლის პირველი და მეორე ნაწილებით გათვალისწინებული ქმედება შეიძლება მხოლოდ განზრახ იქნეს ჩადენილი (სსკ-ის მე-10 მუხლის მე-4 ნაწ.) ამასთან შედეგების მიმართ (ინფორმაციის განადგურება, ბლოკირება, მოდიფიცირება, ეგმ-ის, მისი სისტემის, მათი ქსელის მუშაობის მოშლა), არაპირდაპირი განზრახვაც მოიაზრება. რაც შეეხება 284-ე მუხლის მე-3 ნაწილს, სადაც მძიმე შედეგის გამოწვევაზეა ლაპარაკი, ამავე კოდექსის მე-10 მუხლის მე-4 ნაწილის თანახმად, იგი შეიძლება გაუფრთხილებლობითაც განხორციელდეს, თუმცა მთლიანად დანაშაული განზრახ დანაშაულად ითვლება (სსკ-ის მე-11 მუხლი).

მძიმე შედეგის განხორციელების შემთხვევაში დანაშაული დაკვალიფიცირდება დანაშაულთა ერთობლიობის წესისამებრ.

თავისთავად კომპიუტერულ ინფორმაციასთან არამართლზომიერი შეღწევა, აღნიშნული შედეგების განხორციელების მიზნის გარეშე, სისხლისსამართლებრივი რეაგირების სფეროში არ შედის. სხვა საქმეა, თუ პირს ინფორმაციასთან შეღწევისას ზემოთჩამოთვლილი შედეგების განხორციელების მიზანი ამოძრავებდა. ამ შემთხვევაში მოქმედება მოცემული დანაშაულის მცდელობად განიხილება.*

---

* ამ საკითხთთან დაკავშირებით ლიტერატურაში გამოითქვა აზრი, რომლის თანახმად ინფორმაციასთან შეღწევა შედეგების გამო-წვევის მიზნის გარეშე ამ დანაშაულის მომზადებად განიხილება (Комментарий к Уголовному кодексу Российской Федерации. М., 2002. с. 729 - 734). ამ აზრს ვერ დავეთანხმებით, ვინაიდან ეს მოქმედება ბინაში ქურდობისათვის შეღწევის დარად, მოცემული დანაშაულის მცდელობად უნდა განიხილებოდეს.

დანაშაული შეიძლება ჩაიდინოს ყოველმა 14 წლის ასაკს მიღწეულმა, შერაცხადმა პირმა.

§3. ეგმ-ის დამაზიანებელი პროგრამის შექმნა, გამოყენება ან გავრცელება (მუხ. 285)

1. ეგმ-ის დამაზიანებელი პროგრამის შექმნა ან არსებულ პროგრამაში ცვლილებების შეტანა, რაც განზრახ იწვევს ინფორმაციის არასანქციონირებულ განადგურებას, ბლოკირებას, მოდიფიცირებას ან გადაღებას ანდა ეგმ-ის, ეგმ-ის სისტემის ან მათი ქსელის მუშაობის მოშლას, აგრეთვე ასეთი პროგრამის ან ასეთი პროგრამის შემცველი მანქანა-მატარებლის გამოყენება ან გავრცელება, -

ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით სამ წლამდე ან თავისუფლების აღკვეთით იმავე ვადით.

2. იგივე ქმედება, რამაც გამოიწვია მძიმე შედეგი- ისჯება თავისუფლების აღკვეთით ვადით სამიდან ხუთ წლამდე.

კომპიუტერულ დანაშაულთა შორის ეს დანაშაული ყველაზე მძიმეა, რაც ასახვას პოულობს მუხლის სანქციის ზომაში, ყველაზე მეტ ზიანს კომპიუტერული საშუალებების და ინფორმაციული

რესურსების მესაკუთრეს, მფლობელსა და მოსარგებლეს სწორედ მავნე პროგრამები აყენებენ.

დანაშაულის უშუალო ობიექტია ინფორმაციული ურთიერთობების უსაფრთხოება, ეგმ-ის მესაკუთრის, მფლობელის, მოსარგებლის კანონიერი უფლებები და ინტერესები.

დანაშაული შეიძლება ჩადენილი იქნეს მხოლოდ მოქმედებით. რაც შეეხება დანაშაულის ობიექტური მხარისათვის დამახასიათებელ სხვა ნიშნებს, უნდა ითქვას, რომ 285-ე მუხლში გადმოცემული ნორმა საკანონმდებლო ტექნიკის თვალსაზრისით რედაქციულად უხეიროდ არის აგებული, რამაც შეიძლება გარკვეული სიძნელეები შეუქმნას პრაქტიკას. კერძოდ, ერთი შეხედვით აღნიშნული შემადგენლობა, ყოველ შემთხვევაში 285-ე მუხლის პირველი ნაწილის ის მონაკვეთი, რომელიც დამაზიანებელი პროგრამის შექმნას ან არსებულ პროგრამაში ცვლილებების შეტანას ითვალისწინებს, რაც განზრახ იწვევს ინფორმაციის არასანქციონირებულ განადგურებას, ბლოკირებას, მოდიფიცირებას ან გადაღებას ანდა ეგმ-ის, ეგმ-ის სისტემის ან მათი ქსელის მუშაობის მოშლას – მატერიალური დელიქტია და ამდენად აუცილებელია მიზეზობრივი კავშირის დადგენა ჩადენილ ქმედებასა და განხორციელებულ თუნდაც ერთ-ერთ შედეგს შორის. მაგრამ მუხლის ამავე პირველი ნაწილის მეორე მონაკვეთი, სადაც მითითებულია ასეთი პროგრამის ან ასეთი პროგრამის შემცველი მანქანა-მატარებლის გამოყენებასა ან

გავრცელებაზე – მხოლოდ მოქმედებაზე ამახვილებს ყურადღებას, ხოლო შედეგი კი აქ თითქოს არ ჩანს. ამდენად მუხლის ეს მონაკვეთი ფორმალური ხასიათის აბსტრაქტულ დელიქტს წარმოადგენს და მიზეზობრივი კავშირის დადგენაც გამორიცხულია. გამოდის, რომ თუ 285-ე მუხლის პირველი ნაწილის ტექსტს სიტყვა-სიტყვით გავყვებით, მთლიანად მუხლი მატერიალური და ფორმალური შემადგენლობების ეკლექტიკურ ნარევს წარმოადგენს. კანონმდებელს, რომ მუხლის პირველი ნაწილის მეორე მონაკვეთი ცოტა განსხვავებულად, მაგალითად, ასე ჩამოეყალიბებინა " აგრეთვე ასეთი პროგრამის გამოყენებას ან გავრცელებას" (ხაზგასმა ჩვენია – ლ.ს.), მაშინ აქაც აუცილებელი გახდებოდა მიზეზობრივი კავშირის დადგენა დამაზიანებელი პროგრამის შექმნასა ან არსებულში ცვლილებების შეტანასა და მანქანა-მატარებლის გამოყენებასა და გავრცელებას, როგორც აღნიშნული ქმედების შედეგს შორის.[25]

285-ე მუხლში აღნიშნული შედეგებიდან თუნდაც ერთის განხორციელებისას დანაშაული დამთავრებულად ითვლება. თუ პირისაგან დამოუკიდებელი

[25] ვერ დავეთანხმებით ლიტერატურაში გამოთქმულ შეხედულებებს, თითქოს რუსეთის ფედერაციის სსკ-ის 273-ე მუხლი, რომელიც საქართველოს 285-ე მუხლის ანალოგიურია, მთლიანად ფორმალურ დელიქტს წარმოადგენდეს. ფორმალური აღნიშნული მუხლის პირველი ნაწილის მხოლოდ მეორე მონაკვეთია (იხ. Курс уголовного права. т.4. Особенная часть. Учебник для вузов под. ред. Г.Н. Борзенкова, В.С. Комиссарова. М., 2002., с. 654-655).

მიზეზების გამო დასახელებული შედეგებიდან არც ერთი არ განხორციელდა, განზრახვის არსებობის პირობებში, მოქმედება ამ დანაშაულის მცდელობად განიხილება. ამასთან დაკავშირებით ვერ დავეთანხმებით ლიტერატურაში გამოთქმულ აზრს, რომლის მიხედვით დანაშაული დამთავრებულად ითვლება დამაზიანებელი პროგრამის შექმნის ან გავრცელების მომენტიდან, იმისგან დამოუკიდებლად განხორციელდნენ, თუ არა დასახელებული შედეგები. ავტორს, რომ თავისი მოსაზრება 273-ე მუხლის (საქ. სსკ-ის 285-ე მუხლი) პირველი ნაწილის მეორე მონაკვეთზე გამოეთქვა, სადაოც არაფერი იქნებოდა, ხოლო ვინაიდან ამ მუხლის პირველი ნაწილის პირველი მონაკვეთი, როგორც უკვე აღინიშნა, მატერიალურ დელიქტს წარმოადგენს, ამდენად მისი დამთავრებულად ცნობისათვის აუცილებელია მუხლით ჩამოთვლილი შედეგების განხორციელება.[26]

სსკ-ის 285-ე მუხლის პირველი ნაწილით გათვალისწინებული ქმედება, როგორც თვით მუხლის ტექსტში მითითებული, შეიძლება ჩადენილი იქნეს მხოლოდ განზრახ. რაც შეეხება ამ მუხლის მეორე ნაწილით გათვალისწინებულ მძიმე შედეგს, აქ გაუფრთხილებლობაც მოიაზრება. ელექტრონულ-გამომთველი ტექნიკის მუშაობის სპეციფიკიდან გამომდინარე, ასეთი პროგრამის გაუფთრხილებლობით

---

[26] Уголовное право Российской Федерации. Особенная часть под общей ред. Г.Н. Борзенкова, В.с. Комиссарова. М., 1977. стр. 544.

გავრცელება საყარაუდოა, მაგრამ არა აუცილებელი და გარდაუვალი. აღნიშნულიდან გამომდინარე, დანაშაულის სუბიექტური მხარე არა მხოლოდ პირდაპირი განზრახვით, არამედ შეიძლება როგორც არაპირდაპირი განზრახვით, ისე გაუფრთხილებლობითაც გამოხატოს, თუმცა ამ უკანასკნელ შემთხვევაში დანაშაული მაინც განზრახ ჩადენილად ჩაითვლება (სსკ-ის მე-11 მუხლის I ნაწილი).

გაუგებრობის თავიდან აცილების მიზნით, სასურველი იქნებოდა, თუ კანონმდებელი სამომავლოდ გაითვალისწინებს ამ გარემოებას და რუსეთის ფედერაციის კოდექსის 273-ე მუხლის მეორე ნაწილის მსგავსად შემადგენლობას შემდეგნაირად ჩამოაყალიბებს: "იგივე ქმედება, რამაც გაუფრთხილებლობით მძიმე შედეგი გამოიწვია".

დანაშაულის მიზანი და მოტივი არ წარმოადგენენ სსკ-ის 285-ე მუხლით გათვალისწინებული შემადგენლობის ნიშნებს და მხედველობაში არ მიიღებიან დანაშაულის კვალიფიკაციისას, მაგრამ მნიშვნელობა ენიჭებათ სასჯელის სახისა და ზომის შერჩევის დროს. ამ დანაშაულის ჩადენის თუნდაც უკეთილშობილესი მიზანი ("მეკობრული", პროგრამებისაგან ბაზრის დაცვა, გარემოს სისუფთავისათვის ბრძოლა, ატომური იარაღის წინააღმდეგ ბრძოლა და ა.შ.), თავისთავად არ გამორიცხავს დანაშაულებრივ ქმედებას.

დანაშაულის სუბიექტი 14 წლის ასაკს მიღწეული შერაცხადი პირია, მაგრამ იმის გათვალისწინებით, რომ დამაზიანებელი პროგრამების დამუ-

შავება მხოლოდ მაღალკვალიფიციურ პროგრამისტს ხელეწიფება, რომელსაც თავისი პროფესიული მომზადების დონის გამო, ასევე შეუძლია გათვალოს ამ პროგრამის გამოყენების შედეგებიც, ნაკლებ სავარაუდოა, რომ უიშვიათესი გამონაკლისის გარდა, დანაშაულის სუბიექტად 14 წლის ასაკს მიღწეული პირი მოგვევლინოს.

პროგრამის სასარგებლო თუ საზიანო ხასიათი არ არის დამოკიდებული მის მიერ მუხლში აღნიშნული შედეგების გამოწვევაზე. ეს შედეგები ლეგალური პროგრამის სავსებით ლეგალური ფუნქციაა. აქ მთავარი ისაა, იცის თუ არა კომპიუტერული ინფორმაციის მესაკუთრემ, მფლობელმა ან სხვა კეთილსინდისიერმა მოსარგებლემ პროგრამის ხასიათი და მიღებულია თუ არა მათი თანხმობა (სანქცია). ამ ორი პირობიდან თუნდაც ერთის დარღვევა, პროგრამას საზიანოდ გადააქცევს.

დამაზიანებელია პროგრამა, რომელიც სპეციალურად არის შექმნილი კომპიუტერული სისტემის და პროგრამების ნორმალური ფუნქციონირებისათვის ხელის შესაშლელად.

ნორმალურ ფუნქციონირებაში მოიაზრება იმ ოპერაციების შესრულება, რისთვისაც გათვლილია პროგრამა და, რაც ასახულია პროგრამის დოკუმენტაციაში.

დამაზიანებელ პროგრამას უნარი აქვს კომუნიკაციური ქსელის მეშვეობით გადავიდეს ერთი სისტემიდან მეორეზე, შეაღწიოს ეგმ-ში, ნებისმიერ

სხვა პროგრამას მიუერთდეს და გამოიწვიოს სხვადასხვა არასასურველი შედეგი (გააუვარგისოს ფაილი, დაამახინჯოს გამოთვლის რეზულტატი, წაშალოს კომპიუტერის მეხსიერება და ა.შ.). განსაზღვრული პერიოდის განმავლობაში ასეთი პროგრამა არ ამჟღავნებს თავს, მაგრამ შემდეგ კომპიუტერი "აცადდება", თითქოს უმიზეზოდ მწყობრიდან გამოდის. კომპიუტერის მუშაობის შეფერხება ინფორმაციის სრულ განადგურებას იწვევს.

ეგმ-ის დამაზიანებელ პროგრამებში უპირველესად კომპიუტერული ვირუსი სახელდება. პროგრამა – ვირუსი მას იმიტომ ეწოდება, რომ მისი მოქმედება ძლიერ წააგავს ბიოლოგიური ვირუსის მოქმედებას, რომელიც ჯანსაღ უჯრედებს იყენებს, აავადებს მათ და ვირუსის აღწარმოებას აიძულებს. თავისთავად კომპიუტერული ვირუსი არ არსებობს. ის იყენებს სხვა პროგრამებს, რომლებიც მოდიფიცირდებიან და ასრულებენ რა განსაზღვრულ ფუნქციებს, აწარმოებენ ვირუსს.[27]

კომპიუტერული ვირუსის საშიშროება ისაა, რომ მან შეიძლება გამოიწვიოს კომპიუტერული ინფორმაციული სისტემის სრული დეზორგანიზაცია.

კომპიუტერული ვირუსი საშიშია იმ მხრივაც, რომ მას გააჩნია თვითწარმოქმნის უნარი; ვირუსული პროგრამები ჩვეულებრივ რთავენ კომანდას, რაც

[27] Айков Д., Сейгер К., Фонертохту. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. М., 1990.

უზრუნველყოფს თვითგადაღებას და შენიღბვას. ვირუსის გავრცელება ისე ხდება, თითქოს მან დაასნებოვნა სისხლის თეთრი ბურთულაკები და მათთან ერთად მოგზაურობს მთელს ორგანიზმში. ვირუსი აძლევს კომანდას კომპიუტერს, რათა მან ჩაიწეროს პროგრამის დაავადებული ვერსია. ამის შემდგ იგი უბრუნებს პრაგრამას მართვის შესაძლებლობას. მოსარგებლე ვერ ამჩნევს, რომ მისი კომპიუტერი ვირუსის მატარებელია. ამ ვირუსის აღმოჩენა მხოლოდ მეტისმეტად განვითარებული პროგრამისტული ინტუიციის პირობებშია შესაძლებელი, რადგან ეგმ-ის მუშაობაში მოცემულ მომენტში დარღვევები არაფრით არ ვლინდება, მაგრამ ერთ მშვენიერ დღეს კომპიუტერი "ავად ხდება". ვირუსები შეიძლება საკმაოდ ხანგრძლივი დროის განმავლობაში უმოქმედოდაც იყვნენ, შემდეგ კი უცებ გაიღვიძონ და კატასტროფა გამოიწვიონ თავდაცვის, სახელმწიფო უშიშროების, დამნაშავეობასთან ბრძოლის საქმეში და სხვა სფეროში.[28]

თანამედროვე მსოფლიოში რამდენიმე ათასი პროგრამა – ვირუსია და მათი რიცხვი დღითი-დღე იზრდება. ზოგიერთი მონაცემების მიხედვით მსოფლიოში ყოველწლიურად სამიდან რვა ვირუსამდე იქმნება. მაგალითად, 2000 წლის დასაწყისი აღინიშნა ვირუსი "I love you"-ს გამოჩენით. ეს ვირუსი

[28] Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. М., 1991, стр. 25 – 30.

ელექტროფოსტით მიყვებოდა გზავნილს და გზავნილის გახსნისთანავე ამუშავდებოდა. ამ ვირუსმა მრავალი მოსარგებლის, კომპანიის მუშაობის დესტაბილიზაცია გამოიწვია. რაც უფრო ბევრია ვირუსული პროგრამების რაოდენობა, მით უფრო განსხვავებული და მრავალფეროვანია მათი მოქმედება. მაგალითად, ვირუსი "მიქელანჯელო" კომპიუტერის ავარიულ გაჩერებას და მონაცემების დაკარგვას იწვევს. ცნობილ ვირუსებს შორის შეიძლება დასახელდეს "საშობაო ნაძვის ხე", "მორისის ვირუსი", "666", "ივანე მრისხანე", "პინ-პონგი", "იანკი დუდლ" და სხვ.

სირთულის მიხედვით კომპიუტერული ვირუსი შეიძლება ორ ძირითად ჯგუფად დაიყოს – "ვულგარულ" და "გახლეჩილ" ვირუსებად.

"ვულგარული" ვირუსის პროგრამა ერთიანი ბლოკის მიერ არის დაწერილი და ეგმ-ის დაავადების თაობაზე ეჭვის გაჩენისთანავე ექსპერტს შეუძლია მისი აღმოჩენა, მაგრამ ეს ეპიდემიის გამოვლენისთანავე უნდა მოხდეს.

"გახლეჩილი" ვირუსის პროგრამა დანაწევრებულია. ამ ნაწილებს ერთმანეთთან ერთი შეხედვით რაიმე კავშირი არა აქვთ. ისინი შეიცავენ ინსტრუქციას, რომელიც მიუთითებს კომპიუტერს, თუ როგორ უნდა გააერთიანოს ეს ნაწილები, რაათა შექმნას და აქედან გამომდინარე, გაამრავლოს კიდევაც ვირუსი. როგორც წესი, ვირუსის შემქნელი მიუთითებს ვირუსის რეპროდუქციის რიცხვს, რომლის მიღწევის შემდეგ ვირუსი აგრესიული ხდება.

საეროოდ, ვირუსის ვარიანტები დამოკიდებულია მის შემქმნელის ბიზნესზე. ვირუსს შეუძლია კომპიუტერული პროგრამის შესრულების შეყოვნება ან დისპლეის ეკრანზე მანათობელი წერტილების გაჩენა (ე.წ. "იტალიური მოხტუნავი"). ევოლუციურია ვირუსი, როდესაც ავადმყოფობა მისი მიმდინარეობს პროცესში მწვავდება.

ბუნებრივია, რომ კომპიუტერული ვირუსების წინააღმდეგ მიღებული იქნა განსაზღვრული ზომები, რომელთა შორის აღსანიშნავია ტესტური ანტივირუსული პროგრამები. დამცველი პროგრამები სამ ძირითად სახედ იყოფა: მაფილტრირებელი, რომელიც ხელს უშლის პროგრამაში ვირუსის შეღწევას; ინფექციის საწინააღმდეგო ანუ სისტემის მაკონტროლებელი პროგრამები, რომლებიც აწყობილია ვირუსის გამოსამჟღავნებლად.

უნდა ითქვას, რომ ამ პროგრამების განვითარება ჩამორჩება კომპიუტერული ვირუსული ეპიდემიის ტემპებს, მითუმეტეს თუ იმასაც გავითვალისწინებთ, რომ სპეციალისტების ვარაუდით მომავალში გაჩნდებიან კომპიუტერული ვირუსების პრინციპულად ახალი სახეები.

2003 წლის დასაწყისში, კერძოდ თებერვალში, როგორც კომპიუტერული მომსახურების უსაფრთხოების სამსახური იტყობინებოდა, რომ აღმოჩენილი იქნა ვირუსების ახალი მოდიფიკაციები: "ლოვგითი", "ფიზური", "კლეზი", "ლენტინი" და "მიმაილი", რამაც პანიკაში ჩააგდო პროგრამული უზრუნველყოფის

სპეციალისტები. დღესდღეობით მსოფლიოს თითქმის ყველა ქვეყანაში რეგისტრირებულია ამ ვირუსებით კომპიუტერული ქსელის დაზიანების მილიონობით შემთხვევა[29].

აღნიშნულიდან გამომდინარე, მიღებული უნდა იქნეს ვირუსისგან დაცვის დამატებითი პროფილაქტიკური ღონისძიებები. კერძოდ, მსედველობაშია მისაღები ის გარემოება, რომ სხვა ეგმ-ზე გადატანილ დისკეტს და მაგნიტურ ლენტს შეუძლიათ ეგმ-ის დაავადება და პირიქით, დაავადებულ კომპიუტერში შეტანილი დისკეტი შეიძლება გახდეს ვირუსის მატარებელი. დიდი ეპიდემიების გავრცელების მოხერხებული საშუალებაა ტელეკომუნიკაციური ქსელი. ერთი კონტაქტიც კი საკმარისია, რომ კომპიუტერი დაავადდეს ან დაავადოს ის, ვისთანაც ჰქონდა კონტაქტი. ყველაზე ხშირად დაავადება პროგრამების გადაღებისას ვრცელდება, რაც საერთოდ პერსონალური კომპიუტერით მოსარგებლეთა ჩვეული პრაქტიკაა. ამ დროს უმეტესად ავადდებიან გადაღებული პროგრამები. სპეციალისტები აფრთხილებენ კომპიუტერის მფლობელებს თავი შეიკავონ მოპარული პროგრამების გადაღებისაგან. ზოგჯერ ოფიციალური გზით მიღებული პროგრამებიც კი დაავადებულნი არიან. მაგალითად "ბიმაილი" ჩადებულია ელექტრონული ფოსტის წერილებში. გამომგზავნელის

[29] თამარ როსტიაშვილი. როგორ უნდა გადავურჩეთ მოზღვავებულ ვირუსებს. გაზ. "ალია", 2003 წ. 23-25 VIII.

მისამართი ფალსიფიცირებულია, ასე, რომ მისი მოძებნა შეუძლებელია. წერილი კი დაახლოებით ასე გამოიყურება: "your account [end] hello there, I would like to inform you about important information regarding your email address. This email address will be expiring. Please read attachment for details.Best regards, Adminis.[30]

ვირუსისაგან თავდაცვის მიზნით აუცილებელია მათი ანივირუსულ პროგრამაზე შემოწმება.

საერთოდ, უნდა ვიცოდეთ, რომ ვირუსები იმიტომ იწერება, რათა გაიყიდოს ანტივირუსები. ამიტომაც ვირუსის დამწერი პროგრამისტი ითვალისწინებს ყველა მანამდე არსებულ ანტივირუსს. არცერთი სერიოზული დაწესებულების კომპიუტერული ქსელი ვირუსების შეყრისაგან არ არის თავისუფალი, იქნება ეს კანცელარია, სამინისტროები, ბანკები და ა.შ. ეს დაწესებულებები გამალებით იწყებენ კონკრეტულ ვირუსზე ანტივირუსების ძებნას. ვირუსების დამწერი პროგრამისტებიც სწორედ ამას ელიან და ანტივირუსები გამოაქვთ ბაზარზე.

ვირუსებისაგან გადასარჩენად არსებობს კომპიუტერული ეთიკის ელემენტარული ნორმები, რომელთა მისედვით დაუშვებელი უცნობი მისამართის წერილების გახსნა და ფაილების ინტერნეტიდან გადმოქაჩვა ანტივირუსის გაშვების გარეშე.

---

[30] ირაკლი სანებლიძე. როგორ უნდა გადავურჩეთ მოახლოვებულ ვირუსებს. გაზეთი "ალია" 2003 წ. 23-25/ VIII.

არსებულ პროგრამაში ცვლილებების შეტანა გ'ულისხმობს ეგმ-ში მომ'უშავე პროგრამის შესწორებას ანდა შესწორებული პროგრამის გადატანას ნებისმიერ მანქანა-მატარებელზე.

ვირ'უსებთან ერთად თავისი მავნე მოქმედებით ცნობილია სხვადასხვა დასახელების პროგრამა, მათ შორის გამოყოფენ: "ტროას ცხენის" პროგრამას. ამ პროგრამით ხდება ეგმ-ის ინფორმაციასთან შელწევა და სხვა პროგრამაში ისეთი კომანდის შეტანა, რომელიც მფლობელის მიერ დაუგეგმავი პროგრამ'ული ფ'უნქციის განხორციელების შესაძლებლობას იძლევა, თ'უმცა იმავდროულად ადრინდელი ფ'უნქციაც შენარჩ'უნებ'ულია. ამ ხერხით დამნაშავე მოსარგებლისაგან მალ'ულად კრეფს მისთვის საინტერესო ინფორმაციას და ამით იგი ინფორმაციასთან არამართლზომიერი შელწევის – სსკ-ის 284-ე მ'უხლით გათვალისწინებ'ულ შემადგენლობასაც ახორციელებს.

არსებობს "ტროას ცხენის" სახესხვაობა. მისი თავისებ'ურება ისაა, რომ თითქოსდა ს'ულყინარი პროგრამის ნაწილში ჩაერთვება ისეთი პროგრამა, რომელიც ასრ'ულებს "ბინძ'ურ სამ'უშაოს", აყალიბებს პროგრამას და მისი შესრ'ულების შემდეგ ანადგ'ურებს მას. ასეთ შემთხვევაში პროგრამისტმა, რომელიც "ტროას ცხენის" პოვნას ცდილობს, აუცილებელია მოიძიოს არა თვით "ტროას ცხენი", არამედ მისი წარმოქმნილი კომანდა. ჩვეულებრივ კომპიუტერული პროგრამ'ული ტექსტი მეტად რთ'ულია, იგი შედგება

ასი, ათასი, ზოგჯერ მილიონი კომან-დისაგანაც კი. ამიტომ "ტროას ცხენი" ასეულ კომანდაში ძნელი საპოვნელია და ისიც იმ შემთხვევაშია შესაძლებელი, თუ ამის შესახებ ეჭვი არსებობს. მაგრამ მაშინაც კი, პროგრამისტ-ექსპერტს მის აღმოსაჩენად დიდი დრო დასჭირდება.

"ტროიანელი მატროშკა" არის დამაზიანებელი პროგრამა (მავნე კომანდა ყალიბდება სხვა პროგრამის მეშვეობით ე.ი. გაშუალებულია).

"სალიამი" საბუღალტრო პროგრამებთან გამოიყენება. ამ პროგრამის საშუალებით ხორციელდება კომპიუტერის მეშვეობით თანხის გადაცემა. პროგრამის მუშაობის პრინციპია ყოველი დიდი რიცხვიდან ან ერთი სახის ვალუტიდან მეორეზე კონვერტაციისას მცირე თანხის ამოღება. პროგრამის სახელწოდება უკავშირდება ძეხვის ამავე სახელწოდებას (წვრილი ნაჭრების ჩამოჭრა). დამნაშავისათვის ეს პროგრამა მოხერხებულია, რადგან მიზერული თანხის გატაცების გამოვლენა ძნელია. თუმცა კომპიუტერის მუშაობის სისწრაფის და ჩადენილი დანაშაულებრივი ოპერაციების სიხშირის გათვალისწინებით (მაგალითად, მსხვილი ბანკის ფარგლებში), ამ გზით გატაცებული თანხა საბოლოოდ საკმაოდ სოლიდურია.

პროგრამა "ლოღიკური ყუმბარა" – განზრახ ცვლის პროგრამის კოდს, და წინასწარ განსაზღვრული პირობით, მაგალითად, განსაზღვრული დროს, ნაწილობრივ ან მთლიანად გამოყავს პროგრამა ან ეგმ-ის სისტემა მწყობრიდან.

"ლოღიკური ყუმბარის" ქვესახეს წარმოადგენს კომპიუტერული ვანდალიზმის ისეთი ფორმა, რომელმაც ფართო გავრცელება ჰპოვა აშშ-ში და რომელიც "დროებითი ყუმბარის" სახელწოდებით არის ცნობილი.

კომპიუტერის დახმარებით დანაშაულის ჩადენის შემდეგი სახე "მფრინავი გველის" სახელწოდებით არის ცნობილი. ამ დროს ბანკში იხსნება ანგარიში მცირე თანხაზე. შემდეგ თანხა ერთი ბანკიდან მეორეში გადაირიცხება და თანდათანობითი მატებით უკან ბრუნდება. ეს ციკლი რამდენჯერმე მეორდება, სანამ ანგარიშზე დიდი თანხა არ დაჯდება. თანხა ანგარიშიდან სასწრაფოდ იხსნება და ანგარიშის პატრონიც უკვალოდ ქრება.

პრინციპული განსხვავება "ლოღიკურ ყუმბარასა" და "კომპიუტერულ ვირუსს" შორის ისაა, რომ "ლოღიკური ყუმბარა" თავიდანვე პროგრამის ნაწილია და არ გადადის სხვა პროგრამებში, ხოლო "კომპიუტერული ვირუსი" წარმოადგენს დინამიურ პროგრამას და გავრცელება შეუძლია კომპიუტერულ ქსელშიც კი.

"ჭია" არის დამაზიანებელი პროგრამა, რომელსაც გააჩნია კომპიუტერული ქსელის დახმარებით, დაცვის საშუალებების გადალახვით, ქსელის მოსარგებლისაგან ფარულად საკუთარი კოდის განუსაზღვრელი კოპირების უნარი. ამით იგი ხასიათით კომპიუტერულ ვირუსს წააგავს. მაგრამ მისგან განსხვავებით, დამოუკიდებელი პროგრამაა.

ინფორმაციის არასანქციონირებული განადგურების ბლოკირების, მოდიფიცირების, ეგმ-ის,

ეგმ-ის სისტემის ან მათი ქსელის მუშაობის მოშლის თაობაზე იხ. 284-ე მუხლის კომენტარი.

დამაზიანებელი პროგრამის ან დამაზიანებელი პროგრამის შემცველი მანქანა–მატარებლის გამოყენებაში მოიაზრება ყოველი მოქმედება, რაც თავდაპირველი ან მოდიფიცირებული ფორმით ჩართავს დამაზიანებელ პროგრამას სამეურნეო ბრუნვაში.

დამაზიანებელი პროგრამის გავრცელება ნიშნავს ყოველგვარი ფორმით, მათ შორის ქსელური, თუ სხვა საშუალებებითაც მის გაყიდვას, გაქირავებას, გაჩუქებას, პროგრამის თვითგავრცელებისათვის პირობების შექმნას, ეგმ-ის აღწარმოებულ პროგრამასთან შეღწევის შესაძლებლობის მიცემას.

ეგმ-ის დამაზიანებელი პროგრამის პირადი საჭიროებისათვის გამოყენება (მაგალითად, საკუთარი კომპიუტერული ინფორმაციის განადგურება) აღნიშნული დანაშაულის შემადგენლობას არ იძლევა.

მძიმე შედეგის შესახებ იხ. 284-ე მუხლის კომენტარი.

თუ დამნაშავის მოქმედებაში არის არა მხოლოდ 285-ე მუხლით გათვალისწინებული, არამედ სხვა დანაშაულის ნიშნებიც (მაგ., მკვლელობის, ჯანმრთელობის დაზიანების, ქონების განადგურების და ა.შ.) მოქმედება დანაშაულთა ერთობლიობით დაკვალიფიცირდება (სსკ-ის მე-16 მუხლი), ზუსტად ისევე, როცა 285-ე მუხლის I ნაწილით გათვალისწინებული ქმედება სხვა დანაშაულის ჩადენის წინაპირობას წარმოადგენს.

§4. ეგმ-ის, ეგმ-ის სისტემის ან მათი ქსელის ექსპლუატაციის წესის დარღვევა (მუხ. 286)

1. ეგმ-ის, ეგმ-ის სისტემის ან მათი ქსელის ექსპლუატაციის წესის დარღვევა იმის მიერ, ვისაც ხელი მიუწვდებოდა ეგმ-ზე, ეგმ-ის სიტემაზე ან მათ ქსელზე, რამაც გამოიწვია ეგმ-ის კანონით დაცული ინფორმაციის განადგურება, ბლოკირება, მოდიფიცირება ან გადაღება ანდა რამაც მნიშვნელოვანი ზიანი გამოიწვია,-

ისჯება ჯარიმით ან საზოგადოებისათვის სასარგებლო შრომით ვადით ას ოთხმოციდან ორას საათამდე ანდა თავისუფლების შეზღუდვით ვადით ორ წლამდე, თანამდებობის დაკავების ან საქმიანობის უფლების ჩამორთმევით ვადით სამ წლამდე ან უამისოდ.

2. იგივე ქმედება, რამაც გამოიწვია მძიმე შედეგი-

ისჯება თავისუფლების აღკვეთით ვადით ოთხ წლამდე.

დანაშაულის ობიექტია გამომთვლელი ტექნიკის ინტელექტუალური და ნივთიერი საშუალებების ექსპლუატაციის უსაფრთხოება.

დანაშაულის ობიექტური მხარე ექსპლუატაციის წესების დარღვევით გამოიხატება.

რამდენადაც 286-ე მუხლის დისპოზიცია ზოგადად მიუთითებს ექსპლუატაციის წესების დარღვევაზე, ამდენად იგი ბლანკეტურია. ამ წესების

კონკრეტული შინაარსი გახსნილია სხვადასხვა სახის ნორმატიულ თუ არანორმატიულ ასპექტებში (კანონებში, წესებში, ინსტრუქციებში და ა.შ.). ძირითადად ამ წესებს ვხვდებით ეგმ-ის ხარისხის პასპორტში, ტექნიკური აღწერილობის ფურცელში, ექსპლუატაციის ინსტრუქციაში, სადაც ექსპლუატაციის პირობებია განსაზღვრული. (ასეთია ექსპლუატაციის დროის ხანგრძლივობა, ოპერაციის თანმიმდევრობა, მაქსიმალური დატვირთვა და ა.შ. ამ წესებს გადასცემენ მოსარგებლეს ეგმ-ის და მისი პერიფერიული მოწყობილობის შეძენისას. წესები შეიძლება დადგენილი იქნეს როგორც კომპეტენტური სახელმწიფო ორგანოს მიერ, ისე ტექნიკური ექსპლუატაციის და მუშაობის პროგრამებით, რომლებიც შედგენილია ეგმ-ისა და სხვა კომპიუტერული გამყიდველის, ასევე კომპიუტერული სისტემის მესაკუთრისა და სხვა უფლებამოსილი პირის მიერ. ამ წესების მიზანია ინფორმაციის და კომპიუტერული მოწყობილობის დაცვა, მათი ხანგრძლივი გამოყენების უზრუნველყოფა მესაკუთრისა და მოსარგებლის ინტერესების შესაბამისად.

ეგმ-ის ექსპლუატაციის წესების დარღვევა იყოფა ინტელექტუალური და ფიზიკური ხასიათის დარღვევებად.

<u>ინტელექტუალური ხასიათის</u> დარღვევაში მოიაზრება კომპიუტერულ პროგრამასთან მცდარი დიალოგი, ეგმ-ში ისეთი მონაცემების შეყვანა, რომლის დამუშავება მოცემული გამომთვლელი ტექნიკის შესაძლებლობას აღემატება.

ფიზიკური ხასიათის დარღვევა გულისხმობს მოწყობილობის არასწორ განლაგებას, ტემპერატურის რეჟიმის დაუცველობას, კვების წყაროში ეგმ-ის არასწორ ჩართვას, დაცვის არასერტიფიცირებული და თვითნაკეთი მოწყობილობის გამოყენებას.

დანაშაული შეიძლება ჩადენილი იქნეს როგორც მოქმედებით, ისე უმოქმედობითაც. იგი შეიძლება სამი ფორმით გამოიხატოს: 1. ეგმ-ის, მისი სისტემის და მათი ქსელის ექსპლოატაციის უზრუნველმყოფელი წესების დაუცველობით (ელექტრო და ხანძარსაწინააღმდეგო წესების დარღვევა, შესაბამისი ინსტრუქციების მოთხოვნათა დაუცველობა და ა.შ.), 2. მუშაობის პარამეტრების არასათანადო დაცვით (მაგალითად, პროგრამის ალგორითმის დარღვევა), 3. აღნიშნული წესების უშუალო დარღვევით (მაგ., არამართლზომიერი შეღწევის მიზნით დაცვის სისტემის გამორთვით).

პირველი ორი ფორმა უმოქმედობით ხორციელდება, ბოლი კი – აქტიური მოქმედებით.

286-ე მუხლის სიტყვა-სიტყვითი ტექსტის მიხედვით გამოდის, რომ შედეგის ორ სახესთან გვაქვს საქმე: პირველი, ინფორმაციის განადგურებასა, ბლოკირებასა, მოდიფიცირებასა, გადაღებასა და მეორე, მნიშვნელოვანი ზიანის გამოწვევასთან. უნდა ითქვას, რომ აღნიშნული ნორმა საკანონმდებლო ტექნიკის თვალსაზრისით უხეიროდ არის ჩამოყალიბებული. აქ ნათლად ჩანს კანონმდებლის ნება, იგი მუხლში დასახელებულ მოქმედებას იმდენად ანიჭებს

სისხლისსამართლებრივ მნიშვნელობას, რამდენადაც ეს მოქმედება მიმართულია მნიშვნელოვანი ზიანის გამოწვევაზე ე.ი. ინფორმაციის არა ყოველგვარი განადგურება, ბლოკირება, მოდიფიცირება და გადაღება იწვევს სისხლისსამართლებრივ პასუხისმგებლობას, არამედ მხოლოდ ის, რომელიც რეალურად მნიშვნელოვან ზიანს იწვევს. აღნიშნულიდან გამომდინარე, საკანონმდებლო თვალსაზრისით მიზანშეწონილი იქნებოდა, თუ სსკ-ის 286-ე მუხლის პირველი ნაწილის ბოლო სიტყვები: "რამაც მნიშვნელოვანი ზიანი გამოიწვია", შეიცვლებოდა სიტყვებით" თუ ამ მოქმედებამ მნიშვნელოვანი ზიანი გამოიწვია". ასეთი საკანონდებლო ცვლილება დაიცავდა სასამართლო-საგამოძიებო პრაქტიკას შეცდომებისაგან და, რაც მთავარია, 286-ე მუხლის ეს ნაწილი აღარ იქნებოდა 284-ე მუხლის პირველი ნაწილის განმეორება.

მნიშვნელოვანი ზიანი - თავისთავად შეფასებითი კატეგორიაა და ყოველ კონკრეტულ შემთხვევაში იმ მონაცემებზეა დამოკიდებული, რაც გამოთვლითი ტექნიკის საშუალებებს ახასიათებთ; აქ მხედველობაშია მისაღები ინფორმაციის შინაარსი, მისი ღირებულება, დაზიანების ხარისხი, დაზარალებულ მოსარგებლეთა რაოდენობა, საწარმოს ან ორგანიზაციის საქმიანობის დეზორგანიზაციის ხარისხი, მატერიალური ან ფიზიკური ზარალის რაოდენობა, ეგმ-ის მესაკუთრის ან მფლობელის ქონებრივი მდგომარეობა და სხვა. მაგრამ ყოველ შემთხვევაში ზიანი მძიმე შედეგზე ნაკლები მნიშვნელობის უნდა იყოს.

მოცემული დანაშაულის ობიექტურ მხარეში მოიაზრება აგრეთვე მიზეზობრივი კავშირის დადგენა 286-ე მუხლში გადმოცემულ ქმედებასა - ექსპლუატაციის წესების დარღვევასა და განხორციელებულ შედეგს შორის – ინფორმაციის განადგურებასა, ბლოკირებასა, მოდიფიცირებასა, გადაღებასა და მნიშვნელოვან ზიანს შორის.

რამდენადაც ექსპლუატაციის წესების დარღვევა ქმედების ორივე სახის - მოქმედებით და უმოქმედობით ხორციელდება, ამდენად მიზეზობრივი კავშირის დასადგენად ამ ორი სახის მიმართ დამოკიდებულება განსხვავებული უნდა იყოს. კერძოდ, უმოქმედობის დროს მიზეზობრივი კავშირის დადგენისას აუცილებელია სამი პირობის არსებობა: 1. დამნაშავეს უნდა ევალებოდეს ექსპლუატაციის ამ წესების დაცვა; 2. მას უნდა შეეძლოს ამ წესების დაცვა; 3. ამ წესების დაცვის შემთხვევაში დანაშაული თავიდან იქნებოდა აცილებული.

/მძიმე შედეგის შესახებ იხ. 284-ე მუხლის კომენტარი/

დანაშაულის სუბიექტური მხარე სსკ-ის მე-10 მუხლის მე-4 ნაწილის თანახმად მხოლოდ განზრახვაა: რაც შეეხება 286-ე მუხლის მეორე ნაწილს – მძიმე შედეგის გამოწვევას – აქ შეიძლება გაუფრთხილებლობაც მოიაზრებოდეს, მაგრამ მთლიანად დანაშაული სსკ-ის მე-11 მუხლის პირველი ნაწილის მიხედვით განზრახ დანაშაულად ითვლება.

დანაშაულის მოტივი შეიძლება სხვადასხვაგვარი

იყოს, მაგრამ მას დანაშაულის კვალიფიკაციისათვის მნიშვნელობა არა აქვს. იგი შეიძლება მხედველობაში იქნეს მიღებული სასჯელის ინდივიდუალიზაციის დროს.

დანაშაული შეიძლება ჩაიდინოს ყოველმა შერაცხადმა 14 წლის ასაკს მიღწეულმა პირმა, თუკი მას ხელი მიუწვდებოდა ეგმ-ზე, ეგმ-ის სისტემაზე ან მათ ქსელზე, მაგალითად, ოპერატორი, ამწყობი ტექნიკოსი და ა.შ. კანონი არ მოითხოვს, რომ დამნაშავეს ჰქონდეს გარკვეული განათლება, მისდევდეს განსაზღვრულ საქმიანობას ან ეკავოს რაიმე თანამდებობა. თუ დამნაშავისგან დამოუკიდებელი მიზეზების გამო შედეგი არ განხორციელდა, დამნაშავის განზრახვის არსებობის პირობებში, ქმედება 286-ე მუხლით გათვალისწინებული დანაშაულის მცდელობად განიხილება.

იმ შემთხვევაში, როდესაც ეგმ-ის ექსპლუატაციის წესების დარღვევამ სხვა დანაშაულიც გამოიწვია, ბრალეული პასუხისმგებლობის პრინციპის გათვალისწინებით, დანაშაული ერთობლიობის წესისამებრ დაკვალიფიცირდება.

§5. კომპიუტერული დანაშაული საზღვარგარეთის ქვეყნების სისხლის სამართლის კანონმდებლობაში

საზღვარგარეთის ქვეყნების სისხლის სამართლის კანონმდებლობაში კომპიუტერულმა დანაშაულმა ასახვა ჯერ კიდევ მე-20 საუკუნის 70-იან წლებში ჰპოვა. მაგალითად, ამერიკის შეერთებული შტატების ფედერალური კანონი – კომპიუტერული სისტემის დაცვის შესახებ – 1979 წელს იქნა მიღებული. 1984 წელს ამ აქტის ახალი რედაქციით იგი გამკაცრდა. აშშ-ის მე-18 კანონთა კრებულის 47-ე თავი დანაშაულის შემდეგ შემადგენლობებს ითვალისწინებს, რომლებიც კომპიუტერის დახმარებით შეიძლება იქნეს ჩადენილი, კერძოდ, იგი მოიცავს: თავდაცვის, საერთაშორისო ურთიერთობების შესახებ დახურული ინფორმაციის შეგროვებას, ატომური ენერგიის საკითხებზე ინფორმაციის აშშ-ის საზიანოდ ან სხვა სახელმწიფოთა სასარგებლოდ გამოყენებას, ფინანსური ემიტენტის ფინანსური ჩანაწერებიდან ან დაწესებულებებიდან ან მომხარებლის აღრიცხვიანობის მართვის ფაილიდან მომხმარებლის ინფორმაციის მიღებას, აშშ-ის სამთავრობო უწყების განსაკუთრებული გამოყენებისათვის განკუთვნილი კომპიუტერის ფუნქციონირების მოშლას; ფედერალური მნიშვნელობის კომპიუტერში შესვლის გზით თაღლითობის ჩადენას და რაიმე ფასეულობების მიღებას; იმ კომპიუტერის დაუბრუნებლობას, რომლის მეშვეობითაც ხორციელდება შტატებს შორის ვაჭრობა;

პროგრამის, ინფორმაციის, კოდის ან კომპიუტერული სისტემის კომანდის შეგნებულად იმისათვის გადაცემას, ვისთვისაც გადაცემა აკრძალულია.

დანაშაულის ამ შემადგენლობებისათვის კანონი ითვალისწინებს ჯარიმას, თავისუფლების აღკვეთას ერთ წლამდე. დანაშაულის განმეორებით ჩადენისას თავისუფლების აღკვეთის ვადა ათ წლამდე იზრდება.

კომპიუტერულ დანაშაულთან საბრძოლველად სამართლის კონტინენტურ სისტემაში საკმაოდ მდიდარი არსენალია: შვედეთმა ჯერ კიდევ 1973 წელს მიიღო კანონი, რომლითაც სისხლისსამართლებრივი პასუხისმგებლობა დაწესდა კომპიუტერულ მატარებელზე არსებული ჩანაწერების შეცვლის, განადგურების ან მათთან შეღწევისათვის (ინფორმაციის ბოროტად გამოყენება).

გერმანიაში 1986 წელს სისხლისსამართლებრივი პასუხისმგებლობა დაწესდა კომპიუტერული თაღლითობისათვის (გერმანიის სსკ-ის 263-ე მუხლის პ. "ა") კომპიუტერული ჯაშუშობისათვის (მე-200 მუხლი, პ. "ა"), კომპიუტერული საბოტაჟისათვის და სხვა.

საფრანგეთის სსკ ითვალისწინებს ადამიანის უფლებების ხელყოფისათვის სისხლისსამართლებრივ პასუხისმგებლობას, რაც დაკავშირებულია კარტოთეკისა და ეგმ-ზე დამუშავებული მონაცემების გამოყენებასთან, იმ ინფორმაციული მონაცემების მანიპულიზაციისათვის, რომლებიც შეიცავენ მოქალაქეთა პერსონალური ხასიათის მონაცემებს (მუხ. 222-16, -22); მონაცემების ავტომატიზირებულ

სისტემასთან უკანონო შეღწევისათვის, მისი მუშაობისათვის ხელის შეშლისათვის, მოტყუების გზით მონაცემების შეტანისა და ინფორმაციის შეცვლისათვის და ა.შ. (მუხ. 323 – 1,3), უცხო სახელმწიფოსათვის გადასაცემად სახელმწიფო საიდუმლოების შემცველი ინფორმაციის შეგროვება-გადაცემისათვის (მუხ. 411-7-11).

ესპანეთის სსკ-ი სისხლისსამართლებრივ პასუხისმგებლობას აწესებს იმ ცნობების მიღებისა და გამოყენებისათვის, რომლებიც პირად ან ოჯახურ საიდუმლოებას წარმოადგენენ და ელექტრონულ ან სატელევიზიო ბარათებზე არიან განთავსებულნი (197–ე მუხლის მე-3 ნაწილი). აღნიშნული ქმედების შემადგენლობა მისი ჩადენა იმის მიერ, ვინც მართავს ან პასუხისმგებელია ამ სისტემაზე (მუხლის მე-4 ნაწილი), იცავს საავტორო უფლების ობიექტს, მათ რიცხვში ეგმ-ის პროგრამებს (27-ე მუხლი); კოდექსით რეგლამენტირებულია ეგმ-ის საშუალებების გამოყენებით კომერციული ინფორმაციის ხელში ჩაგდება და გავრცელება (278-ე მუხლი); კოდექსი ყურადღების გარეშე არ ტოვებს ინფორმაციული მოწყობილობის დაუფლება - განადგურების საკითხს (მუხლი 278-ე, ნაწ. მე-3). დაწესებულია პასუხისმგებლობა ჩამოთვლილი დანაშაულობების მომზადებისათვის (ინსტრუმენტის, მასალის, იარაღის, ნივთიერების, მანქანის, კომპიუტერული პროგრამის ან აპარატის დამზადებისა და ფლობისათვის, რომლებიც სპეციალურად ხსენებულ დანაშაულთა ჩასადენად არიან განკუთვნილნი).[31]

[31] Курс уголовного права. т.4. Особснная часть. Учебник для вузов. под. ред. Г.Н. Борзснкова, В.С. Комиссарова, т.4. М., 2002, с. 656-657.

გამოყენებული ლიტერატურის დასახელება

1. Айков Д., Сейгер Л., Фейнсторх У. – Компьютерные преступления. М., 1999.

2. Айламазян А.К., Стаев Е.В. Информатика и теория развития. М., 1989.

3. Батурин Ю.М., Жодзитский А.М. – Компьютерная преступность и компьютерная безопасность. М., 1991.

4. Вехов В.Б. – Компьютерные преступления: вчера, сегодня, завтра. Караганда, 1995.

5. Вехов В.Б. – Компьютерные преступления: способы совершения и раскрытия. М., 1996.

6. Вуе М., Войнтович Н.Л., Гусев Н.А., Гусев В.С. Россия на пороге информационного общества. Сп. 1997.

7. Зибер У. – Международная книга по компьютерной преступности. Чичестер, 1986.

8. Карас И.З. –Экономический и правовой режим информационных ресурсов (в кн. «Право и информатика», М., 1990).

9. Комментарий к уголовному кодексу Российской Федерации. М., 1997.

10. Комментарий к уголовному кодексу Российской Федерации. М., 1998.

11. Комментарий к Уголовному кодексу Российской Федерации. М., 1999.

12. Комментарий к Уголовному кодексу с постатейными материалами и судебной практикой Министерства юстиции Российской Федерации. М., 2000.

13. Комментарий к Уголовному кодексу Российской Федерации. М., 2002.

14. Курс уголовного права. Учебник для вузов. т.4. (под ред. Борзенкова Г.Н., Комиссарова В.С.) М., 2000.

15. Крылов В.В. – Информационные компьютерные преступления. М., 1997.

16. Ляпунов Ю., Максимов В. – Ответственность за компьютерные преступления. М., 1997.

17. Материалы комиссии по предупреждению преступности и уголовному правосудию. Вена. 1993.

18. Самкин Л.С. Программы для ЭВМ – правовая охрана (правовые аспекты против компьютерного пиратства. М., 1998).

19. Телеубекова В.Х. – Компьютерная преступность вчера, сегодня, завтра. Караганда, 1995.

20. Уголовное право Российской Федерации. Особенная часть (под. ред. Здравомыслова В.В.). М., 1996.

21. Уголовное право Российской Федерации. Особенная часть (под. ред. Берзенкова Г.Н., Комиссарова В.С.). М., 1997.

22. მარიამ ცაცანაშვილი – ინფორმაციული საზოგადოება და ინფორმაციის სამართლებრივი რეგულირება. თბილისი, 1999.

ს ა რ ჩ ე ვ ი

კომპიუტერული დანაშაული /შესავალი/.....3

§1 – კომპიუტერული დანაშაული (ზოგადი მიმოხილვა) 11

§2 – კომპიუტერულ ინფორმაციასთან არამართლ-ზომიერი შეღწევა (მუხ. 284) 26

§3. ეგმ-ის დამაზიანებელი პროგრამის შექმნა, გამოყენება ან გავრცელება 46

§4. ეგმ-ის, ეგმ-ის სისტემის ან მათი ქსელის ექსპლუატაციის წესის დარღვევა 62

§5. კომპიუტერული დანაშაული საზღვარგარეთის ქვეყნების სისხლის სამართლის კანონ-მდებლობაში 68

გამოყენებული ლიტერატურის დასახელება.....71