შპს გურამ თავართქილაძის სახელობის თბილისის

სასწავლო უნივერსიტეტი

სამართლის ფაკულტეტი

სისხლის სამართლის სამაგისტრო პროგრამა

თემა: კიბერდანაშაულის სისხლისსამართლებრივი ასპექტები

ნაშრომი შესრულებულია სამართლის მაგისტრის

აკადემიური ხარისხის მოსაპოვებლად

სტუდენტი: ლაშა ტყეშელაძე

ნაშრომის ხელმძღვანელი

პროფესორი სერგო ჭელიძე

თბილისი

2019

შინაარსი

ანოტაცია

სამაგისტრო ნაშრომში განხილულია კიბერდანაშაულის სისხლის სამართლებრივი ასპექტები. ნაშრომში აღწერილია კიბერდანაშაულის განსაზღვრება , დანაშაულის შემადგენლობა. ადგილობრივი და საერთაშორისო პრაქტიკის მიმოხილვა. დაყენებულია სხვადასხვა პრობლემური საკითხები რომელიც უნდა იქნეს გამოსწორებული რომ სახელმწიფო არ გახდეს კიბერდანაშაულის ჩამდენი სუბექტი. ასევე საუბარია კიბერტერორიზმზე რომელიც დღევანდელი მსოფლიოს ერთ-ერთ მნიშვნელოვან გამოწვევად რჩებ,ა რომელთანაც აუცილებელია სწორი ბრძოლის სტრატეგის ჩამოყალიბება და ეფექტური მექანიზმის შექმნა რომელიც კიბერუსაფრთხოებას მეტად დაცულს გახდის ვიდრე ის დღეს არის.

Annotation

The master's thesis deals with criminal aspects of cybercrime. The work describes the definition of cybercrime, the composition of the crime. Review of local and international practices. Various problematic issues have been set up, which should be corrected that the state does not become the subject of cybercrime. It is also about Cyberterrorism which is one of the most challenging challenges in today's world, with which it is necessary to establish a right strategy and create an effective mechanism that will safeguard cyber security more than it is today.

შესავალი

წინამდებარე ნაშრომში განხილულია კიბერდანაშაულის სისხლისსამართლებრივი ასპექტები. კიბერდანაშაულისა და კიბერტერორიზმის განსაზღვრება. დანაშაულის შემადგელობა. საერთაშორისო და ადგილობრივი პრაქტიკა.

კომპიუტერულ დანაშაულს ხშირად 21-ე საუკუნის კრიმინალურ ფორმას უწოდებენ. ამ ტიპის დანაშაულის მუდმივად მზარდი რიცხვი საერთო კრიმინალურ სტატისტიკაში და ეგმ-ის განუზომელი პოტენციალი მიუთითებს იმაზე, რომ დღევანდელი მდგომარეობა ამ სიაში პრობლემის მხოლოდ დასაწყისია. [1]

ნებისმიერი განგარიშებით, შეიძლება ითქვას, რომ გლობალური ინფორმაციული ტექნოლოგიების ინფრასტრუქტურის ფენომენალური ზდა იყო ერთ-ერთი ყველაზე გადამწყვეტი მოვლენა რომლითაც გამოირჩევა თანამედროვეობა, სულ რაღაც უკანასკნელ 10 წელიწადში, ინტიერნეტის მომხმარებელთა რაოდენობა იმდენად სწრაფად გაიზარდა,რომ მისმა ნიშნულმა 0.3 მილიარდიდან 2.5 მილიარდს მიახწია - რაც ფაქტიურად სამჯერ ზდა არის.

ამ პროცესში ჩამოყალიბდა სრულიად ახალი სამყარო-კიბერსივრცე.ეს ახალი ვირტუალური სამყარო წააგავს, ველურ დასავლეთს,ძალინ ცოტა კანონითა თუ ნორმით რომლებიც არეგულირებენ ადამინებისა და მრავალი კანონგარეშედ გამოცხადებულის ქმედებებს,რომლებსაც სურთ ამ სივრცის უმანკო ტერიტორის

[1] უ. ზაქაშვილი, კიბერდანაშაულის სისხლისამართლებრივი რეგულირების პრობლემები საქართველოში, დისერტაცია, თბ. 2013, გვ. 7

ექსლუატაცია, ცხადია რომ კიბერსივრცისგან სარგებლის მიღება შეუძლებელია სათანადო კანომდებლობის არსებობის ან სხვადასხვა ქვეყნების კანონდებლობების ჰარმონიზაციის გარეშე.[2]

კომპიტერული დანაშაულის წარმოქმნის შემდეგ ხშირი იყო მცდელობა, შემოეღოთ კომპიუტერული დანაშაულის ერთიანი ცნება თუმცა ეს მცდელობა უშედეგოდ სრულდებოდა. ერთ საერთაშორისო ცნებას მერე ორგანიზაისს მიერ გაკეთებული განმარტება ენაცვლებოდა. საბოლოოდ. მივიღეთ ის, რომ არც ევროპის საბჭოს კონვენცია და არც მსოფლიოს რომელიმე ქვეყნის კანომდებლობა არ იძლება ამ ცნების ზოგად განმარტებას. საუბარი არაა ცალკეული დანაშაულის შემადგენლობაზე, რადგან ადვილია განმარტო კომპიუტერული სისტემში უნებაართვო სერვისის ცნება. თუმაცა იგი მხოლოდ ერთ-ერთი კომპიუტერული დანაშაულის განმარტება იქნება და არა დანაშაულებრვი ფენომენის -კიბერდანაშაულისა.

აღნიშნული ნაშრომის მიზანია უკეთესად იქნეს შესწავლილი კიბერდანაშაულის არსი, დანაშაულის შემადგენლობა, საერთაშორისო აქტები, ადგილობრივი კანონმდებლობის და პრაქტიკის ანალიზი და მათი გადაჭრის გზები.

[2] ლ.ბოძაშვილი, ნ.კოხრეიძე, კიბერსივრცის სამართალი, თბ, 2012, გვ 5

თავი I. ლიტერატურის მოკლე მიმოხილვა

წიანამდებარე ნაშრომში გამოყენებულია ქართული ასევე უცხოური ლიტერატურა: საქართველოს სისხლის სამართლის კოდექსი, კიბერ უსაფრთხოების თემაზე სადისერტაციო ნაშრომი, ევრო საბჭოს დებულებები რომლემბშიც განსაზღვრულია კიბერ უსაფრთხოების პოლიტიკა ასევე საკოსტიტუციო სასამრთლოს გადაწყვეტილება, ინფორმაციის თავისუფლების განვიათარების ისტიტუტის კვლევა რომელშიც განხილულია სახელმწიფოს მიერ მოსმენების პრაკტიკა და სახელმწიფო მოხელების მიერ არსებული კანომდებლობის დარღვევის სასამართლო პრაკტიკა.

ასევე წიანმდებარე ნაშრომში გამოყენებულია ავტორთა კოლექტივი, სისხლისსამართლის კერძო ნაწილი, წიგნი 2, გურეშიძე ს., სტატია, „ტერორიზმი ინტერნეტში“, ახლო აღმოსავლეთი და საქართველო. კიბერტეროიზმთან დაკავშირებული ლიტერატურა სადაზვერვო ასპექტები, გამომცე

სადაზვერვო ასპექტები, გამომცემლობა

ნაკაშიძე გ., სტატია, „კიბერტერორიზმი - XXI საუკუნის მწვავე გამოწვევა“, ჟურნალი ეკონომიკა და ბიზნესი, №4 ივლისი-აგვისტო,

ჩიხლაძე კ.,კიბერტერორიზმი (ინფორმაციული ესე), ინფორმაციული ტექნოლოგიები, ყოველკვარტალური სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი“

თავი II. პრობლემის კვლევა/ანალიზი

2.1. კიბერ დანაშაულის ზოგადი დეფინიცია და მისი წარმოშობის ისტორია

კიბერდანაშაულის დეფინიციის განსაზღვრა რთულია. ფართო გაგების მიხედვით, აღნიშნულის ქვეშ მოიაზრება ყველა სისხლისსამართლებრივი დანაშაული, რომელიც ჩადენილია საინფორმაციო ან საკომუნიკაციო ტექნოლოგიების გამოყენებით ან მათ მიმართ. გავრცელებულია დიფერენციაცია „კომპიუტერულ დანაშაულსა” და „ინტერნეტ დანაშაულს” შორის, კერძოდ, დანაშაულებს შორის, რომელთა ჩადენის დროსაც დანაშაულის ჩადენის საშუალებას ან დანაშაულის ობიექტს კომპიუტერი ან ინტერნეტი წარმოადგენს. თუმცა ეს დაყოფა მკაცრი არ არის, რადგან მათი სფეროების გადაფარვა ხდება. მიუხედავად ამისა, დანაშაულის საპოლიციო სტატისტიკა (PKS) აღნიშნულ დაყოფას ეყრდნობა, როდესაც აღწერს „ინტერნეტს, როგორც დანაშაულის საშუალებას” და „კომპიუტერულ დანაშაულს”, როგორც დანაშაულის სპეციალურ

ფორმას. „კიბერდანაშაულის შესახებ ფედერაციაში არსებული მდგომარეობის ამსახველი ანგარიშიც" (Bundeslagebild Cybercrime) ერთმანეთისაგან ასხვავებს დანაშაულებს, რომლებიც ინტერნეტის, მონაცემთა ბაზების, საინფორმაციო ტექნოლოგიური სისტემების ან მათი მონაცემების წინააღმდეგ არის მიმართული (კიბერდანაშაული ვიწრო გაგებით) და დანაშაულებს, რომლებიც აღნიშნული ტექნიკის გამოყენებით ხორციელდება (კიბერდანაშაული ფართო გაგებით).[3]

კომპიუტერული დანაშაული, ყურადღების ცენტრში პირველად, აშშ-ში XX საუკუნის [4]70-იან წლებში მოექცა.ნაციონალურ და საერთაშორისო დონეზე დაიწყო ამ ფენომენის გამოკვლევა. მიღებულ იქნა სპეციალური ნორმები კიბერდანაშაულის მოსაწესრიგებლად. აშშ-ში ჯერ კიდევ 1977 შეიმუშავს კანონპრექტი „ფედერალური კომპიტერულ სისტემების დაცვის შესახებ",რომელიც ითვალისწინებდა სისხლისსამართლებრვ პასუხისმგებლობას ისეთი ქმედებისთვის, როგორიცა:კომპიუტერულ სისტემაში ცრუ მონაცემების შეყვანა კომპიუტერული მოწყობილობის უკანონო გამოყენება, ფულადი სახსრების მითვისება კომპიუტერული ტექნოლოგიების და კომპიუტერული ინფორმაცის მეშვეობით და სხვ.ამ კანონპროექტის საფუძველზე 1984 წლის ოქტომბერში მიღებულ იქნა ;კომპიუტერული თაღლითობის და კომპიუტერის ბოროტად გამოყენების შესახებ" კანონი. კომპიუტერული დანაშაულის წინააღმდეგ აქტიური ბრძოლის დასაწყებად აშშ-ში ექსპეტები გამოყოფენ სამ შემთხვევას, რომლებმაც ცხადი გახადა, რომ ახალი კომპიუტერული და სატელეკომუნიკაციო ტექნოლოგიები დიდ პრობლემებს შეუქმნიდა სამართალდამცავ ორგანოებს. საყოველთაო ;კომპიუტინგი" (კომპიუტრების მაშტაბური ინტეგრაცია ყოველდღიურ ცხოვრებაში) მარტო ცხოვრების წესის შეცვლას კი არ ნიშნავდა არამედ შეიცვლებოდა კრიმინალების მიერ დანაშაულებრივი საქმინობის წარმართვის სპეციფიკაც. მაგალითისთვის მოვიყვან სამივე შემთხვევას.

[3] მ.პ. ვასმერი, კიბერდანაშაული - აწყმყო და მომოვალი, გვ, 13

[4] უ.ზაქაშვილი,კიბერდანაშაულის სისხლისამართლებრივი რეგულირების პრობლემები საქართველოში, დისერტაცია, თბ, 2013, გვ, 10-12

პირველი. 1986 წელს კალიფორნის უნივერსიტეტის ასტრონომს დაევალა [5] არასასიამოვნო, მაგრამ აშკარად მცირე მნიშვნელობის პრობლემის გადაჭრა უნივერსიტეტის კომპიუტერულ ლაბორატორიაში. უნვერსიტეტი ამუშავებდა ორ საბუღალტრო პროგრამას, რომელიც აღრიცხავდა კომპიუტერების გამოყენებას და არეგისტრირებდა მათ მომხმარებელს. ვინაიდან, ამ პროგრამით ხდებოდა თანხებთან დაკავშირებით ერთიდა იგივე ინფორმაციის დაფიქსირება მათი შედეგიც ერთნაირი უდნა ყოფილიყო. თუმცა, გამურკვეველი მიზეზით სხვაობა 75 აშშ დოლარი შეადგინა.

გამოძიების ფედერალურამ ორგანოებმა უარი განაცხადეს საქმის გამოძიებაზე იმ მოტივით, რომ 75 დოლარიანი დანაკარგი უმნიშვნელო იყო, მაგრამ ასტრნოვმა კლიფორტ სტოლმა თავად დაიწყო გამოძიება. ის წერდა ჰაკერის მოქმედებებს და მუშაობდა როგორც ადგილობრივ ასევე უცხოურ სატელეფონო კომპანიებთან, რათა დაედგინა თავდასხმის წყარო.აღმოჩნდა რომ გერმანელ ჰაკერ მარკუს ჰესს აფინსებდა რუსეთის სახელმწიფო უსაფრთხოების კომიტეტი, რათა გაემჟღავნებინა აშშ-ს სამხედრო საიდულოება. ამ რიგად ეს იყო მნიშნველოვანი გაკვეთილი როგორც სამართალდმცავი ორგანოების, ასევე დაზვერვის სამსახურისთვის.

პირველ რიგში, ცხადი გახდა, რომ ქსელური ინფორმაცია არ იყო დაცული მასში უნებართვო შეხწევისგან და მეორე-ფინანსური ზარალი ყოველთვის არ განსაზღვრავს ხელყოფის ზერიოზულობას და ინფორმაცია კიბერდანაშაულის შესახებ არ უნდა შემოწმდეს მხოლოდ ფინანსური ზარალის მიხედვით.

მერე შემთხვევა დაკავშირებული იყო კომპიუტერულ ვირუსთან ე.წ მორისის მატლთან (Morrs Worm). 1988 წელს ქორნელის უნივერსიტეტის სტუდენტმა რობერტ მორისონმა შექმნა პროგრამა ინტერნეტის მეშვეობით კომპიუტერში შესახწევად. მას შემდეგ რაც კომპიუტერული ვირუსი შეახწევდა სამიზნე კომპიუტერში იგი დაიკავებდა კომპიუტერის მეხსიერებას, რაც გამოიწვევდა კომპიუტერის გამორთვას. სანამ კომპიუტერული ვირუსი

[5] SCOTT CHARNEY, KENT ALEXANDER, Types of computer crime,25.11.2005 http://www.crimeresearch.org/articles/types-of-computer-crime/2

გაუვნებელყოფილი იქნა, მანდ დაზიანა დახლოებით 6200 კომპიუტერი და გამოიწვია 98 მილიონ დოლარზე მეტი ზარალი.

მესამე შემთხვევა ეხება 1989 წლის თავდასხმას კომპანია „ბელსაუსზე“,რომელიც განხორციელადა სიკვდილის ლეგიონის სახელით ცნობილი ჰაკერთა ჯგუფის მიერ.მათთვის შესაძლებელი გახდა ადგილობრივ სატელეფონო სისტემაში ცვლილებების შეტანა და მონოცემების განადგურება

მიუხედავად იმისა, რომ ამერიკელი გამომძიებლები განხილულ დანაშაულს წარმატებით გაუმკლავდენ, აუცილებელი გახდა კომპიუტერული დანაშაულის შესახებ საკანომდებლო ინიციატვის მომზადება, რომელსაც მხარე დაუჭირა ამერიკის გენერალური პროკურორის ეკონომიკური დანაშაულის საბჭომ უკვე 1991 წლის სექტემბერში კი იუსტიცის დეპარტამენტის გენერალურ სასარჩელო განყოფილებაში შეიქმნა კომპიუტერული დანაშაულის წინაღმდეგ ბრძოლის განყოფილება.

ზემოაღნიშნული მაგალითი არის სახელმძღვანელო შემთხვევა მსფლიოს სხვადასხვა სახელმწიფოსთვის კიბერდანაშაულის წინაღმდეგ ბრძოლაში და ცალსახაა, რომ საქართველო ამ საკითხში განსაკუთრებული ყურადღება უნდა მიაქციოს უცხოურ გამოცდიელბას .

დიდი ბრიტანეთი მრავალი წლის მანძილზე უშედეგოდ ცდილობდა კომპიუტერული დანაშაულის წინაღმდეგ გამოეყენებინა სასამართლო წარმოებაში მიღებული მრავალ საუკუნოვანი გამოცდილება, თუმცა უშედეგოდ. 1990 წლის აგვისტოში ძალაში შევიდა კანონი „კომპიუტერული ტექნოლოგის არასაქცირებული გამოყენების შესახებ“, რომლითაც დასჯადად გამოცხადდა კომპიუტერში ან მასსში დაცულ ინფორმაციაში ან/და პროგრამაში წინასწარ განძრახული უკანონო შეხწევა, ასევე ამ ინფორმაცის ბლოკირება, მოდიფიცირება, განადგურება ან კოპირება.

გერმანიაში კომპიუტერული ინფორმაცის სფეროში ჩადენილ დანაშაულებზე სისხლის სამართლებრივი პასუხისმგებლობის საკითხი 1986 წლიდან დადგა. 1987 წლის აგვისტოდან განხორციელდა შესაბამისი ცვლილებები გერმანიის სისხლის

საამართლის კოდექსში, რითაც დადგინდა პასუხისმგებლობა კომპიუტერული დანაშაულისთვის. 1993 წელს მსგავსი ცვლილებები განიცადა ჰოლანდიის სისხლის სამართლის კოდექსმა და დანაშაულად გამოცხადდა კომპიტერში არასანქცირებული შეხწევა, კომპიტერული საპოტაჟი, ვირუსების გავრცელება, და სხვა.

ბოლო წლებში კომპიტერული დანაშაული აღიარებულია საერთაშორისო ხასაითის დანაშაულად და მის წინაღმდეგ ბრძოლა წარმაოდგენს მრავალი საერთაშორისო ორგანიზაციისთვის პირორიტეტულ მიმართულებას.

გაეროს მიერ მიღბული იქნა „ინფორმაციული ტექნოლოგიების გამოყენებით ჩადენილი დანაშაულის წინაღმდეგ ბრძოლის შესახებ“ რეზოლუციები, რომლებშიც ხაზგასმულია ყველა წევრი სახელმწიფოს მხრიდან, საკუთარი საკანომდებლო ბაზის გადახედვის და მისი სრულყოფის აუცილებლობა[6]

ეკონომიკური განვითარებისა და თანამშრომლობის ორგანიზაცია 1983 წლიდან სწავლობს და ამზადებს შესაბამის რეკომენდაციებს, რათა საერთაშორისო დონეზე მზგავს დანაშაულებრივ შემთხვევებზე განხორციელდეს ანალოგიური სისხლის სამართლებრივი პასუხისმგებლობის დაკისრება.

დიდი 8 ვიანის ქვეყნებს შექმნილი აქვთ საკნტროლო პუნქტების მუდმივ მოქმედი ქსელი, რომელსაც კომპიტერულ დანაშაულთან დაკავშირებით წამოჭრილი პრობლემების გამო შეუძლია მიმართონ საერთაშორისო თანამშრომლობის პროცესის მონაწილე ყველა წევრს.

მნიშვნელოვან დოკუმენტს წარმოადგენას ეუთო-ს მიერ მიღებული გადაწყვეტილება - ორგნიზაცია წევრ-სახელმწიფოებს აძლევს რეკომნდაციას შეუერთდდენ ევრო საბჭოს მიღებულ კონვენციას „კიბერდანაშაულის შესახებ“ და „დიდი რვიანის“ ქვეყნების მიერ კომპიუტერული დანაშაულის წინაღმდეგ ბრძოლისთვის შექმნილ მუდმივმოქმედ ქსელს, რომლის მიზანია კვირაში 7 დღე 24 საათი მოკავშირე სახელმწფოებისთვის

[6] Pedro Verdelho,Cybercrime and Electronic Evidence, E-Newsletter ”Electronic Newsletter on the Fight Against Cybercrime”(ENAC)” #1, jule, 2009, p2

ინფორმაცის მიწოდება და კომპენტენციის ფარგლებში სათანადო დახმარების აღმოჩენა.

მსგავსი ქსელი შექმნილია ინტერპოლის ფარგლებშიც. იგი მთელი მსოფლიოს მაშტაბით აერთიანებს 100 ამდე მუდმივ მოქმედ დაწესებულებას, რომელიც ინტეროლის წევრ სახელმწიფოებს ეხმარება მოზებნონ საჭირო სპეციალისტი სხვა ქვეყანაში,დროულად მიღონ მათი დახამრება კომპიუტერული დანაშაულის გამოძიების და მასზე მტკიცებულების შეგროვებასთან დაკავშირებით.[7]

საერთაშორისო აქტებიდან საქართველოსთვის ყველაზე მნიშვნელოვან დოკუმენტს წარმაოდგენს ევრო საბჭოს კონვენცია „კიბერ დანაშაულის შესახებ“,რომელიც მიიღეს 2001 წლის 23 ნოემბერს ქ.ბუდაპეშტში[8] ევრო საჰჭოს 41 წევრი სახელმწიფოს მიერ აღნიშნული დოკუმნტი წარმოადგენს მოსფლიო მაშტაბით ერთ-ერთ პირველ სერიოზულ მცდელობას კიბერ დანაშაულის წინაღმდეგ ბრძოლაში:ნაცინალური უსაფრთხოების დასაცავად, ერთიანი სტრატეგიის ჩამოყალიბებისთვის და ურთერთ თანმშროლობისთვის. მას, გარდ ევროპული ქვეყნებისა, ხელი მოაწეერეს კანადამ, იაპონია,სამხრეთ აფრიკა, აშშ-მ.[9] 2008 წლის აპრილში რუსეთის ფედერაციამ უარი თქვა კონვენციის ხელმოწერაზე ამავე წლისს ივლისში კონვენციას ხელი მოაწეერა აზერბაიჯანმა [10]

კონვეცია განსაზღვრავს ექსტრადიციის და ორმხრვი დახმარების პრინციპებს. ევრო საბჭოს წევრ ქვეყნებიდან კონფეცის რატიფიცირება და შესაბამისად კონვენციაში მოცემული ქმედებების კრიმინალიზაცია და სხვა პრინციპების მოქმედება ეროვნული კანომდებლობის დონეზე განხორციელდა შემდეგ სახელმწიფოებში:ალბნეთი, სომხეთი,

[7] http://www.interpol.int/Public/ICPO/FactSheets/FHT02.pdf

[8] : http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_in_georgia/projectcyber_en.asp).

[9] http://en.wikipedia.org/wiki/Convention_on_Cybercrime

[10] http://www.today.az/news/society/46054.html

ბოსნია,ბულგარეთი,ხორვატია,კვიპროსი,დანია,ესტონეთი,ფინეთი,საფრანგეთი,გერმნი ა,უნგრეთი და სხვა ხელმომწერ სახელმწიფოებში.

დღეის მდგომარეობით კონვენცია კიბერდანაშაულის შესახებ წარმოადგენს ერთ-ერთ უმთავრეს დოკუმენტს და გარანტიას მსოფლიოს სახელმწიფოთა ნაცინალური უსაფრთხოები დასაცავად ურთერთ თანამშრომლობისთვის კომპიუტერული დანაშაულის წინაღმდეგ ბრძოლაში, საკანომდებლო ბაზის დახვეწისა და ჰარმონიზაციისთვის, გამოცდილების გაზიარებისა და ყვეალ სახელმწიფოს წინაშე, დასმული ყველაზე სწრაფად, განვითარებადი, გამოწვევა-კომპიტერული დანაშაულის მავნე შედეგისა შემცირებისთვის. თუმცა გამოცდილება ცხადყო,რომ მხოლოდ კონვენცის მიღება ზემოაღნიშნული ეფექტის მისაღებად არ აღმჩნდა საკმარისი,რადგან არც ევროსაბჭოს და არც ევროკავშირის წევრ სახელმწიფოთა უმრავლესობა არ მოახდიან კონვენციის რატიფიცირება, ნაწილმა კი მხოლოდ მისი ხელმოწერა განახორციელა. არაოფიცალურად ევროპის საბჭოს კონვენცის მიმართ ევროპის ქვეყნების მხრიდან, გამოჩენილი გულგრილობა, დაედო საფუძვლად ევრო კავშირის საბჭოს 2005 წლის 24 თებერვლის N2005/222 ჩარჩო გადაწყვეტილების მიღებას „კომპიუტერულ სისტემაზე შეტევის წინაღმდეგ“,რომლიც იმორებდა კონვენცის ძირითად პრინციპებს და ევროკავშირს წევრ სახელმწიფოებს ავალდებულებდა მოხედიანთ გადაწყვეთილებით განსაზღვრული ქმედებებს კრმინალიზაცია ნაციონალური სისხლის სამართლის ,კანომდებლობაში ცვლილებიების შეტანის გზით.

აღსანიშნავია, რომ განსხვავებით „კიბერდანაშაულის შესახებ“ კონვენციისგან, ევრო კავშირის საბჭოს ჩარჩო, გადაწყვეტილებსში ნაცვლად ტერმინისა „კომპიუტერული სისტემა“ გამოყენებულია ტერმინი „საინფორმაციო სისტემა“.[11] უ.ზაქაშვილი თავის სადისერტაციო ნაშრომში მიუთითებს, რომ ევროკავშირის გადაწყვეტილებით განსაზღვრული დეფინიცია საინფორმაციო სისტემის შესახებ წარმოადგენს, უფრო სრულყოფილ და ყოვლის მომცველს, კერძოდ, თუ „კომპიუტერული სისტემა“

[11] უ. ზაქაშვილი, კიბერდანაშაულის სისხლისამართლებრივი რეგულირების პრობლემები საქართველოში, დისერტაცია, თბ., 2013, გვ. 15

განიმარტება როგორც ნებისმიერი მექანიზმი, ან ერთმანეთან დაკავშირებული ან ურთიერთ დაკავშირებული მექანიზმთა ჯგუფი. რომელიც ერთი- ან მეტი პროგრამის მეშვეობით ასრულებას მონაცემთა ავტომატურ დამუშავებას, „საინფორმაციო სისტემის“დეფინიცია განისაზღვრება როგორც ნებისმიერი მექანიზმი,ან ერთმანეთან დაკავშირებული ან ურთიერთ დაკავშირებული მქანიზმთა ჯგუფი, რომელიც ერთი ან მეტი პროგრამის მეშვეობით ასრულებს მონაცემთა ავტომატურ დამუშავებას,ასევე მონაცემთა შენახავას, აღდგენას და გადაგზავნას სისტემის გამოყენების ,მუშაობის, დაცვისა და ტექნიკური მომსახურეობის მიზნების შესაბამისად.

ევროკავშირის საბჭოსადმი წარდგენილ იქნა მოხსენება რომლის მიზანიც იყო შეეფასებინა, რადენად სწორად იქნა განხორციელებული ევრო კავშირის ჩარჩო გადაწყვეტილება. [12]უ.ზაქაშვილი რამდენიმე ასპექტზე ამახვილებს ყურადღებას. ისევე როგორც კონვენცია „კიბერდანაშაულის შესახებ“, ჩარჩო გადაწყვეტილებითაც დანაშაულებრივ ქმედებას წარმოადგენს კომპიუტერულ სისტემაში უნებართვო შეხწევა და ამ ქმედების დანაშაულად კვალიფიკაცია არ უკავშირდება მის შედეგს. დანაშაული დამთავრებულად ითვლება უნებართვო შეხწევის განხორციელების მომენტიდან და არა იმ სისტემაში არსებული მონაცემების დაზიანების, ან მოპოვების ან სხვა მავნე შედეგის დადგომისას. მიუხედავად ამისა ავსტრია, ჩეხეთმა,ლატვიამ და ფინეთმა კომპოუტერულ სისტემაში უნებართვო შეხწევის გამო დასჯადობა დაუკავშირა დანაშაულებრივი შედეგის დადგომას, კერძოდ დამდგარ ზიანს ან ზიანის საფრთხეს.[13]

;კიბერდანაშაულის შესახებ“ კონვენციის მე-5 მუხლის მიხედვით დასჯადათ გამოცხადდა კომპიუტერული სისტემის ფუნქციონირებისათვი საფრთხის შექმნა, რომელიც ჩადენილია კომპიუტერულ მონაცემთა შეყვანის, გადაცემის, დაზიანების, წაშლის ან დაფარვის გზით, ხოლო ევროკავშირის ჩარჩო გადაწყვეტილების მე-3 მუხლის მიხედვით კი ყველა მონაწილე სახელმწიფო ვალდებულია მიიღოს საჭირო

[12] იქვე, გვ. 16

[13] Report from the Commission to the Council, Brussels, 17.07.2008. com (2008) 448 (Based on article 12 of the Council Framework Decision of 24.02.2005 on attaks against information systems).

ზომები , რათა უზრუნველყოს იგივე ქმედების კრიმინალიზაცია. თუმცა, ავსტრიაში დასჯადია ასეთი ქმედება მხოლოდ იმ შემთხვევაში , თუ ის ატარებს მძიმე დანაშულის ნიშნებს; ჩეხეთი, ესტონეთი და ლიტვა აუცილებელ პირობად მიჩნევენ ასეთი ქმედებით გამოწვეულ ზიანს.

მსოფლიოში კომპიუტერული დანაშაულის საკანომდებლო რეგულირების მცდელობის გარდა,იმუშავეს კომპიუტერული დანაშაულის ერთიანი დეფინიცის ჩამოსაყალიბებლად. 1983 წელს პარიზსში ექსპერტების ჯგუფმა ჩამოაყალიბა კომპიუტერული დანაშაულის ცნება: კომპიუტერული დანაშაული არის კანონით აგძაულილი არაეთიკური ქმედება, რომელიც აფერხებს მონაცემთა ბაზების ავტომატიზირებულ მუშაობას ან ინფორმაცის გადაცემას.[14]

[15]უ.ზაქაიძის აზრით აღნიშნიშნული დეფინიცია არასრულყოფილია: პირველ რიგში მიუღებელია ტერმინი „არაეთიკური ქმედება“ რადგან ბუნდოვანი და არაერთგვაროვანი შინარსის მატარებელია. მეორე ნაკლი კი გახლავთ, რომ კომპიუტერული დანაშაული მოქცეულია გარკვეულ ჩარჩოში. კერძოდ, დეფინიცის ავტორების აზრით, მან შესაძლებელია ხელყოს მხოლოდ მონაცემთა ბაზების ავტომატირიზებული მუშაობა და ინფორმაცის გადაცემა .შესაძლოა. 1983 წელს ექსპერტები კომპიუტერულ დანაშაულში მეტ საფრთხეს ვერ ხედავდნენ, თუმცა საეჭვოა არ სცოდნოდათ, რომ კომპიუტერული დანაშაულის მეშვეობით ხდება არა მარტო ინფორმაცის გადაცემის ხელყოფა, არამედ მისი განადგურება, შეცვლა და ასე აშ.აღნიშნულმა დეფინიცამ ვერ დაიმკვიდრა ადგილი მსოფლიოში.

1993 წელს ინტერპოლის მუშაობის ჩარჩოებში ორგანიზებული სემინაარის“კრიმინალისტიკა და კომპიუტერული დანაშაულის“ ფარგლებსში კომპიუტერული დანაშაულის ცნებამ შემდეგი სახე მიიღო: სისხლსი სამართლით

[14] Richard W. Aldrich, “CYBERTERRORISM AND COMPUTER CRIMES: ISSUES SURROUNDING THE ESTABLISHMENT OF AN INTERNATIONAL LEGAL REGIME”, USAF Institute for National Security Studies USAF Academy, Colorado, April 2000, gv.10

[15] უ.ზაქაშვილი,კიბერდანაშაულის სისხლისამართლებრივი რეგულირების პრობლემები საქართველოში, დისერტაცია, თბ, 2013, გვ 17

გათვალისწინებული საზოგადებრივად საშიში ქმედება რომლებშიც მანქანური ინფორმაცია წარმოადგენს დანაშალუებრივი ხელყოფის საშვალებას ან ობიექტს[16]

მოცემულ ცნების მთავარი ნაკლი ისაა, რომ ავტორებმა კომპიუტერული ინფორმაცია წარმოადგინეს როგორც დანაშაულის საშვალება და ობიექტი. თუმცა არ აღუნიშნავთ, რომ ის შეიძლება კომპიუტერული დანაშაულის საგანიც იყოს.

[17]2000 წლის აპრილის გაეროს X კონგრესზე განმარტეს, რომ კიბერ დანაშაულზე უნდა ემსჯელათ ვიწრო და ფართო გაგებით. პირველი მათგანი მოცავს კომპიუტერულ დანაშაულს, მერე კი კომპიუტერის გამოყენებასთან დაკავშირებულ დანაშაულს. ვიწრო გაგებით, კიბერდანაშაული ესაა: „ელექტრონული ოპერაციებით ჩადენილი განონით აკრძალული ქმედება, რომლის მიზანია კომპიუტერული სისტემის და მართი მონაცემების უსაფრთხოების ხელყოფა“. ფართო გაგებით კი კიბერდანაშაულია: „კანონით აკრძალული ნებისმიერი ქმედება, რომელიც დაკავშირებულია კომპიუტერების, მათი სისტემის და ქსელის გამოყენებასთან, მათ შორის კომპიუტერული სისტემის ან ქსელის გამოყენებით ინფორმაცის უკანონო შენახვა, შეთავაზება და გავრცელებასთან.

კიბერდანაშაულის ერთიანი ცნების შემოღება არაერთმა ქვეყანამ თუ საერთაშორისო ორგანიზაციამ სცადა, თუმცა მათი მცდელობა ბოლომე ვერ ასახავს კიბერდანაშაულის ცნების არსს.

2.2. კომპიუტერული დანაშაულის სამართლებრივი მოწესრიგება

2.2.1. კომპიუტერული დანაშაულის ობიექტური შემადგენლობა

2.2.1.1. საქართველოს სისხლის სამართლის კოდექსის 284-ე მუხლით გათვალისწინებული დანაშაულის ობიექტური შემადგენლობა

[16] ა.კაცმანი, „კომპიუტერული დანაშაულის სისხლისსამართლებრივი და კრიმინალისტიკური დახასიათება“,ჟურნ. „სამართალი“ 2000 წ N2 გვ. 58

[17] United Nations A/CONF.187/10, (ix. http://ebookuniverse.net/aconf18710-pdf-d8490066)

სისხლის სამართლის კოდექსის 284-მუხლის დისპოზიციის განსაზღვრება ჩამოყალიბებულია - „კომპიუტერულ სისტემაში უნებართვო შეხწევა“ დანაშაულის უშვალო ობექტს წარმოადგენს სისხლის სამართლის კანონით დაცული კონკრეტული საზოგადებრივი ურთიერთობა, რომლის წინაღმდეგაც მიმართულია დანაშაულებრივი ხელყოფა.

კომპიუტერული დანაშაულის უშვალო ობექტის განსაზღვრას ალ.კაცმანი უკავშირებს კომპიუტერული დანაშაულის შემადგენლობის შემცველ კონკრეტული მუხლების სახელწოდებას.[18] გ.მამულაშვილი 284 მუხლის ძველი რედაქციით, გათვალისწინებული დანაშაულის უშვალო ობექტად გამოყოფს კომპიუტერული, ინფორმაცის ხელშეუხებლობას, საკუთრების უფლებას კომპიუტერულ ინფორმაციას[19]. 284 მუხლის ახალი რედაქციით დაცვის უშვალო ობექტად გ.მამულაშვილი მიუთითებს:მონაცემის/ინფორმაციის მთლიანობას, ხელმისაწვდომობას და კომფიდეცალურობას, ასევე კომპიუტერული სისტემის ინტეგრირებულობას.

საინტერესოა კომპიუტერული ტექინიკა უნდა მივაკუთვნოთ თუ არა დანაშაულის ობექტს და საგანს.

უ. ზაქაშვილი მიიჩნევს კომპიუტერული ტექნიკა დანაშაულებრვი ხელყოფის, ობიექტი არ არის. იგი ეთანხმება ვ.ნ ჩერკასოვს, რომელიც მიიჩნევს რომ კომპიუტერული თაღლითბა, საპოტაჟი, ჯაშუშობა და სხვა რჩება ისევ თაღლითობად, საბოტაჟად და ჯაშუშობად რაც ჩადენილია კომპიუტერის, როგორც ტექნიკური საშვალების დახმარებით.

ალ.კაცმანი მიჩნევს, რომ კომპიუტერული დანაშაულის ხელყოფის საგანს წარმოადგნეს ინფორმაცია, რომლის დამუშავებაც ხდება კომპიუტერულ სისტემასში, ხოლო კომპიუტერი ითვლება ხელყოფის იარაღად, დანაშაულის საგანდ კომპიუტერის მითითებაში ალ.კაცმანი გულისხმობს კომპიუტერს როგორც ტეკნიკას თუ როგრც

[18] ა.კაცმანი, დისერტაცია „კომპიუტერული დანაშაული“, თბ, 2004წ გვ, 35.

[19] ავტორთა კოლექტივი, „სისხლის სამართლის კერძო ნაწილი“, გამომც „მერიდიანი“ თბ, 2012, გვ 46.

სისტემას. უ.ზაკაშვილი აღნიშნავს, რომ მხოლოდ კომპიუტერული ტექნიკით უშვალო კიბერდანშაულის საგანზე ზემოქმედების მოხდენა შეუძლებელია და თუ ალ.კაცმანს იმის თქმა სურდა, რომ კომპიუტერული ტექნიკა კიბერდანაშაულის იარაღია მაშინ იგი მას არ ეთანხმება.[20]

ამერიკელი ექსპერტები კენტ ალექსანდერი და სკოტ ჩარნი მიჩნევენ, რომ კომპიუტერი ან მასში შენახული ინფორმაცია შეიძლება იყოს დანაშაულის საგანი.[21]
ასეთ შემთხვევაში დამნაშავის მიზანია კომპიუტერიდან, ინფორმაცის მოპარვა ან მასზე ზიანის მიყენება. მეორე - კომპიუტერი შეიძლება იყოს დანაშაულის იარაღი. ასეთ შემთხვევას ადგილი აქვს მაშინ, როდესაც ადამინი იყენებს კომპიუტერს რომელიმე ისეთი ტრადიციული დანაშაულის ჩადენის ხელშეწყობისთვის, როგორიცაა თაღლითობა ან ქურდობა „მაგალითად, ბანკის თანმშრომელმა შეიძლება გამოყენოს კომპიუტერული პროგრამა თანხის მოსახსნელად ამავე ბანკში გახსნილი მოქალქეების ანგარიშიდან“. მესამე - ზოგჯერ კომპიუტერი მერე ხარისხოვანია დანაშაულის ჩასადენად, მაგრამ მნიშვნელოვანი სამართალდამცავებისთვის, რადგან იგი შეიცავს დანაშაულთან დაკავშირებულ მტკიცებულებას. მაგალითად, ნარკოტიკების მოვაჭრეება, ფურცლების და ჟურნალის ნაცვლად შეიძლება გმოიყენონ პერსონალური კომპიუტერი, ნარკოტიკებით ვაჭრობასთან დაკავშირებული ჩანაწერის შესანახად.

კიბერდანაშაულის ძირითად მახასიათებლად ალ.კაცმანი გამოყოფს[22]:

ა) დანაშულებრივი ხელყოფის ობექტის არაერთგვაროვნებას.

ბ) ერთი და იგივე კომპიტერული ინფორმაცია შეიძლება იყოს, ერთ შემთხვევაში ხელყოფის საგანი,ხოლო მერე შემთხვევაში დანაშაულის ჩადენის იარაღი ან საშვალება.

გ) დანაშაულებრივი ხელყოფის საგნისა და საშვალების მრავალფეროვნებას.

---

[20] ა.კაცმანი, დისერტაცია „კომპიუტერული დანაშაული“, თბ, 2004წ გვ, 30

[21] SCOTT CHARNEY, KENT ALEXANDER, Types of computer crime,25.11.2005 http://www.crimeresearch.org/articles/types-of-computer-crime/2

[22] ა.კაცმანი, დისერტაცია „კომპიუტერული დანაშაული“, თბ, 2004წ გვ, 58

ამ კლასიფიკაციიას სრულად იზიარებს უ.ზაქაშვილი, იმ განსხვავებით, რომ ხელყოფის საგანი, გარდა კომპიუტერული ინფორმაციისა, არის კომპიუტერული სისტემა და კომპიტერული მონაცემიც.[23]

284-ე მუხლით გათვალისწინებული დანაშაულის საგანი არის ის კომპიუტერული სისტემა და მონაცემი რომელშიც ხორციელდება უნებართვო შეხწევა.

284 მუხლის შენიშვნის პირველნ და მეორე ნაწილში განმარტებულია, როგორც კომპიუტერული სისტემის ასევე, კომპიუტერული მონაცემის ცნება: კომპიუტერული სისტემა არის ნებისმიერი მექანიზმი ან ერთმანეთან დაკავშირებულ მექანიზმთა ჯგუფი, რომელიც პროგრამის მეშვეობით, ავტომატურად ამუშავებს მონაცემებს „მათ შორის პერსონალური კომპიუტერი, ნებისმიერი მოწყობილობა მიკროფოცესორით, აგრეთვე მობილური ტელეფონი“, ხოლო კომპიუტერული მონაცემი არის კომპიტერულ სისტემაში დამუშავებისთვის ხელსაყრელი ნებისმიერი ფორმით ინფორმაცის გამოსახვა, მათ შორის პროგრამა, რომელიც უზრუნველყოფს ამ კომპიუტერული სისტემის ფუნქცინირებას.

ქართული კანომდებლობისგან, მიცირე განსხვავებით განმარტავენ [24]კომპიტერულლ სისტემას და კომპიტერულ მონაცემს ლ.ბოძაშვილი და ნ.კოხრეიძე სახელმძღვანელოში „კიბერცივრცის სამართალი“. მათი აზრით, კომპიუტერული სისტემა „ნებისმიერი მოწყობილობა ან ურთერთ და კავშირებულ ხელსაწყოთა ჯგუფი, რომელთაგან ერთ-ერთი მაინც ასრულებს მონაცემების ავტომატურ გადაცემას პროგრამის საშვალებით“, ხოლო კომპიუტერული მონაცემია ინფორმაციის, „ფაქტების ან საერთო წარმოდგენის გადმოცემა კომპიუტერული სისტემის თუ პროგრამისთვის გასაგებ ფორმაში, რომელმაც შეიძლება შეაასრულებინოს კომპიტერულ სისტემას გარკვეული ქმედება.

[23] უ.ზაქაშვილი,კიბერდანაშაულის სისხლისამართლებრივი რეგულირების პრობლემები საქართველოში, დისერტაცია, თბ, 2013, გვ 28

[24] ლ.ბოძაშვილი, ნ.კოხრეიძე „კიბერსივრცის სამართალი, 2012 წ გვ 35

მოცემულ განმარტებაში კომპიუტერულ სისტემასთან დაკავშირებით დაკონკრეტებულია, რომ ურთერთ დაკავშირებულ ხელსაწყოთა შორის საკმარისია, თუნდაც ერთ-ერთი ასრულებდეს მონაცემთა ავტომატურ დამუშავებას. აღნიშნული პოზიციაზე შეიძლება ითქვას რომ იგი სავსებით მისაღებია და იმაზე ზუსტია ვიდრე ქართული კანომდებლობა.

284-ე მუხლის დისპოზიცია არ განსაზღვრავს კომპიუტერული სისტემაში შეღწევას კონკრეტულ სახეს, რადგან იგი ახალი ტექნოლოგიების განვითარებისა და აღმოჩენის პარლელურად ხშირად იცვლება. სწორედ ამიტომ დისპოზიციაში ტექნოლოგიებთან მიმართებაში ნეიტრალური ტერმნებია გამოყენებული, რაც ქმედების დანაშაულად კვალიფიკაცისას მეტი ინტეპრეტაციის საშვალებას იძლევა.[25]

ეს შეიძლება შეფასდეს დადებითად, რადგან საგამოძიებო ორგანოები და სასამრთლო არ იქნება შეზღუდული კომპიუტერულ სისტემაში უნვებართვო შეხწევის ხერხის დეტალური გამოკვლევის ვალდებულებით.[26] საკმარისი იქნება დადგინდეს უშვალოდ შეხწევის ფაქტი და ამ ქმედების უნებართვობა. თუმცა შესაძლებელია გამოვყოთ ის ხერხი, რომლის დახმარებითაც დამნაშავე ახერხებს კომპიუტერულ სისტემაში შეხწევას. კომპიტერულ სისტემაში შეხწევა შესაძლებელია ფიზიკურად და დისტანციურადაც. ფიზიკური გულისხმობს კომპიუტერულ სისტემაში შეღწევას, დისტანციურში კი იგულისხმება გლობალური ქსელის საშვალებით და სხვადასხვა პროგრამის დახამრებით კომპიუტერულ სისტემაში შეღწევა.

[27] შეხწევისთვის დამნაშავე იყენებს სხვადასხვა სახის კომპიტერულ პროგრამას მაგალითად ე.წ. „ტროას ცხენი“ ფაილების ხელმისაწდვომობის უზრუნველ საყოფად მის სამიზნე კომპიუტერულ სისტემაში დაისტალირების პროცეს ინფილტრაცია ეწოდება. იგი განსხვავებულ მეთოდებს მოიცავს: ერთი მათგანი მოითხოვს

[25] ავტორთა კოლექტივი, მოსამრთლეების ტრენინგი კომპიტერული დანაშაულის შესახებ:ტრენინგი სახემძღვანელო,ევრო საბჭო, სტრასბურგი, 2010 წ გვ. 47

[26] უ.ზაქაშვილი,კიბერდანაშაულის სისხლისამართლებრივი რეგულირების პრობლემები საქართველოში, დისერტაცია, თბ, 2013, გვ 40

[27] ნ.ცომაია, „სახელმწიფოს მხირდან კომპიუტერულ სისტემებში ფარული შეხწევა და ამ ღონისძიების კონსტიტუციურ სამართლებრივი საზღვრები“, ჟურ. „მართლმსაჯულება და კანონი“ 2008 წ N2, გვ. 81

მომხმარებლის მიერ მხარდაჭერას (გაუთვიცნობიერებელ), მერე კი, მომხმარებლის (გაუთვიცნობიერებელ) დახამრების გარეშე ხორციელდება.

„ტროას ცხენის“ მეშვეობით შესაძლებელია უცხო კომპიუტერულ სისტემაზე სრული კონტროლის მოპოვება. მისი ნაირსახეობაა ე.წ. „ლოგიკური ბომბი“ - პროგრამაში ბრძანების შეყვანა, რომელიც მხოლოდ განსაძღვრულ პირობებში მუშავდება, ან ე.წ. „დროზე დამოკიდებული ბომბი“ - იგი დროის გარკვეულ მომენტში აქტიურდება.

[28] უ.ზაქაშვილი იზიარებს აშშ-სა და უნგრეთის მიდგომას და მიაჩნია რომ 284-ე მუხლის შენიშვნაში მიეთითოს: „კომპიუტერულ სისტემაში უნებართვო შეღწევად განიხილება, კომპიტერულ სისტემაში შესვლის უფლებამოსილების ბოროტად გამოყენება“

შეიძლება ითქვას, რომ კომპიუტერულ სისტემაში უნებართვო შეხწევაა განძრახ განხორციელებული ისეთი მოქმედება, რომელიც ეწინაღმდეგება კომპიუტერული სისტემის ფლობელის ნებას და იწვევს კომპიუტერული სისტემის ინტეგრირებულობის და კომფიდეცალურობის დარღვევას.

2.2.1.2 საქართველოს სისხლის სამართლის კოდექსის 285-ე მუხლით გათვალისწინებული დანაშაულის ობიექტური შემადგენლობა

სისხლის სამართლის კოდექსის 285 მუხლით ჩამოყალიბებულია შემდეგგვარად: „კომპუტერული პროგრამის ან/და სხვა მოწყობილობის, აგრეთვე კომპიუტერულ სისტემაში შეხწევისთვის საჭირო პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის უნებართვო დამზადება, შენახვა, გაყიდვა, გავრცელება ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა ამ თავითა და ამკოდექსის 158-ე ან 159-ე მუხლით გათვალისწინებული დანაშაულის ჩადენის მიზნით“[29]

[28] უ.ზაქაშვილი,კიბერდანაშაულის სისხლისამართლებრივი რეგულირების პრობლემები საქართველოში, დისერტაცია, თბ, 2013, გვ 48

[29] სისხლის სამართლის კოდექსი,1999, 285-ე მუხლი

[30] გ.მამულაშვილის განმარტებით აღნიშნული ნორმით დაცულ ინტერეს ანუ ხელყოფის ობექტს წარმოადგენს კომპიუტერული სისტემის ან მისი მონაცემების კონფიდეციალობა , ინტეგრირებულობა, ხელმისაწვდომობა.

[31] თ.წერეთლის და გ.ტყეშელიაძის აზრით ზოგიერთ დანაშაულის შემადგენლობა გულისხმობს ხელყოფას ორ ან მეტ უშვალო ობექტზე. ამასთან ეს ობექტები შეიძლება სხვადასხვაგვაროვანნი იყვნენ.

[32]უ.ზაქაშვილი სვავს კითხვას 285-ე მუხლით გათვალისწინებული ქმედება ერთზე მეტ ობექტიანი დანაშაულია თუ არა?! კომპიუტერული სისტემის, მოწყობილობის და მონაცემების უსაფრთხოება, კონფიდენციალობა და ხელმისაწვდომობა უკვე აღინიშნა. განხილული ქმედებით შესაძლოა მოხდეს ინ კომპიუტერული სისტემის, პროგრამის ან სხვა მოწყობილობის მესაკუთრის ინტერესის ხელყოფა, რომლის კომპიუტერულ პროგრამაში, მოწყობილობაში ან კომპიუტერულ სისტემაში შეღწევისთვის საჭირო პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის უნებართვო დამზადება, შენახავა, გაყიდვა,გავრცელება ან ხელმისაწვდომობის უზრუნველყოფაც ხორციელდება, რადგან ამ ქმედებით იქნება რელური საფრთხე, რომ განხორციელდება კომპიუტერულ სისტემაში უნებართვო შეხწევა ან კერძო კომუნიკაციის საიდულოების დარღვევა და შეილახება ამ მონაცემის მესაკუთრის ინტერესები. ხელყოფის ობექტი, რიგშემთხვევაში შესაძლოა რეპუტაციაც .

საქართველოს სისხლის სამართლის კოდექსის 285-ე მუხლის პირველი ნაწილით [33]გათვალისწინებული დანაშაულის საგანია ის კომპიუტერული სისტემა და მონაცემი, რომლის ხელყოფის მიზნითაც იქმნება კომპიუტერული პროგრამა, მოწყობილობა და უნებართვო შეხწევისთვის საჭირო პაროლი დაშვების კოდი ან სხვა მსგავსი მონაცემი.

---

[30] ავტორთა კოლექტივი,"სისხლის სამართლის კერძო ნაწილი", წიგნი 2 გამომც, „მერიდიანი" თბ. 2012. გვ 40

[31] თ.წერეთელი გ.ტყეშელიაძე, „მოძღვრება დანაშაულზე" გამომც. „მეცნიერება" თბ. 1969 წ გვ. 156

[32] უ.ზაქაშვილი,კიბერდანაშაულის სისხლისამართლებრივი რეგულირების პრობლემები საქართველოში, დისერტაცია, თბ, 2013, გვ 49

[33] სისხლის სამართლის კოდექსი,1999, 285-ე მუხლი

285-ე მუხლით გათვალისწინებული ქმედების ობექტური მხარე, სხვადასხვა ასპექტებს მოიცავს: „კომპიუტერული პროგრამის ან და სხვა მოწყობილობის, აგრეთვე კომპიუტერულ სისტემაში შეხწევისთვის საჭირო პაროლის, დაშვების კოდის ან სხვა მსგავსი მონაცემის უნებართვო დამზადება, შენახვა, გაყიდვა, გავრცელება, ან ხელმისაწვდომობის სხვა გვარი უზრუნველყოფა ამ თავითა და ამ კოდექსის 158 მუხლით გათვალისწინებული დანაშაულის ჩადენის მიზნით“.

ევროპის ყველა ქვეყანამ რომელმაც განახორციელა ;კიბერდანაშაულის შესახებ“ კონვენციის რატიფიცირება , კანონმდებლობაში მოახდინა კონვენციის მე-6 მუხლის ინტეგრირება.აღნიშნული მუხლის მიხედვით დანაშაულია იმ მოწტყობილობის და კომპიუტრეული პროგრამის , კომპიუტრერული პაროლის , დაშვების კოდის ან მსგავსი მონაცემის წარმოება , გაყიდვა , გამოსაყენაბლად შეძენა/მიწოდება , გავრცელება , იმ პორტი ან ხელმისაწვდომიბის სხვგავარი უზრუნველყოფა , რომელთა გამოყენებითაც ხდება კონვეციის მე-2 , მე-3 , მე-4 და მე-5 მუხლით გათვალისწინებული დანაშაულების ჩადენა-განხორციელება. ამ მუხლებში მითითებულია კომპიუტერულ სისტემაში ან მის ნაწილში უნებართვო შეღწევა , კომპიუტერელი სისტემისთვის , სისტემიდან ან მის ფარგლებში მონაცემთა გადაცემის უნებართვოდ ხელში ჩაგდება , კომპიუტერულ მონაცემთა დაზიანება , წაშლა , გაუარესება , შეცვლა ან დაფარვა და ნებართვის გარეშე კომპიუტერული სისტემის ფუნქციონირების არსებითი შეფერხება კომპიუტერულ მონაცემთა შეყვანის , გადაცემის, დაზიანების , წაშლის , დაფარვის გზით.[34]

285-ე მუხლში კანონმდებელმა კონვეციდან არ გადმოიტანა დიდი ტერმინები . მაგალითად , კონვეციაში მითითებულია : წარმოება , გაყიდვა , გამოსაყენებლად , შეძენა/მიწოდება , გავცელება , იმპორტი და ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა. ქართულმა კანონმდებელმა კი მუხლში ჩაწერა შემდეგგვარად: დამზადება , შენახვა , გაყიდვა , გავცელება , და ხელმისაწვდომობის სხვაგვარი

[34] უ.ზაქაშვილი,კიბერდანაშაულის სისხლისამართლებრივი რეგულირების პრობლემები საქართველოში, დისერტაცია, თბ, 2013, გვ 51

უზრუნველყოფა . ქართულ ენაში ტერმინები ,, მიწოდება'' და ,,იმპორტი " ექცევიან ტერმინი ,, გავცელების " განმარტების ქვეშ . გარდა ამისა , ქართველმა კანონმდებელმა 285-ე მუხლის დისპოზიციას დაამატა ტერმინი ,, შენახვა " , რაც კონვეციაში საერთოდ არ წერია . აღსანიშნავია რომ შეტმინი ,, შეძენა " 285-ე მუხლში არ ჩაიწერა , უ.ზაქაშვილი აღნიშნულს არ ეთანხმება , რადგან ტერმინები მის შინაარს არ მოიცავენ .დანარჩენ ტერმინებთან დაკავშირებულ ქართული კანონმდებლობის მიდგომას ამ ნაწილში იგი სრულად იზიარებს .

მოცემულ კომპიუტერულ დანაშაულთან დაკავშირებით ძალიან მნიშვნელოვანია [35]ისითი ტექნიკური და პროგრამული ინსტრუმენტების ხელმისაწვდომობა , რომლებიც გამოიყენება დანაშაულის ჩადენის მიზნით . ასეთი მოწყობილობის უმეტესობა ხელმისაწვდომი , უფასო , და ადვილად დასამუშავებელია და მათი გამოყენება შეუძლიათ სპეციალური ცოდნის არ მქონე ადამიანებსაც. კომპიუტერული სისტემის სპეციუალური პროგრამის გამოყენებით შესაძლოა უკაბელო ქსელით კომუნიკაციის დაგაცემის ხელში ჩაგდება , ან ღია უკაბელო ქსელის აღმოჩენა , დაშიფრული ფაილების გაშიფვრა და კიბერ შეტევები . ასეთი დანაშაულის ჩადენისთვის , გარდა სპეციალური პროგრამისა , საჭიროა სათანადო მოწყობილობის შეძენაც . ამისთვის არსებობს შავი ბაზარი , სადაც ხდება მისი წარმოება და გასაღება .

კომპიუტერეული პროგრამა არის ბრძანებათა ერთობლიობა , რომელიც უზრუნველყოფს კომპიუტერში დავალების შესრულებისთვის საჭირო ოპერაციათა განხორციელების რიგს .[36]

კომპიუტერული პროგრამები ერთმანეთისგან განსხვავდებიან დანიშნულებით , ფუნქციით და სპეციფიკური მახასიათებლებით . კომპიუტერული პროგრამა უკავშირდება კომპიუტერული მონაცემის განმარტებასაც . ეს უკანასკნელი სწორედ კომპიუტერულ სისტემაში დამუშავებისთვის ხელსაყრელი ნებისმიერი ფორმით

[35] ავტორთა კოლექტივი, მოსამრთლეების ტრენინგი კომპიტერული დანაშაულის შესახებ:ტრენინგი სახემძღვანელო,ევრო საბჭო, სტრასბურგი, 2010 წ გვ. 57

[36] უ.ზაქაშვილი,კიბერდანაშაულის სისხლისამართლებრივი რეგულირების პრობლემები საქართველოში, დისერტაცია, თბ, 2013, გვ 55-56

ინფორმაციის გამოსახვას და მათ შორის იმ პროგრამას გულისხმობს , რომელიც უზრუნველყოფს კომპიუტერული სისტემის ფუნქციონირებას.

ყველა პერსონალურ კომპიუტერს აერთიანებს ე.წ პროგრამა ,, ბიოსი'' , იგი ენერგო დამოუკიდებელი მუდმივმახსოვრობის მოწყობილობა . მასში ჩაწერიალია მონაცემთა მიღების და გაცემის პროგრამა , კომპიუტერის ელექტრო ქსელში ჩართვის/გაშვების პროგრამა და სხვა პროგრამები , რომელიც იყენებს ინფორმაციას კომპიუტერის აპარატული კონფიგურაციის შესახებ . უნდა აღინიშნოს ოპერაციული სისტემა , რომელიც ასევე , კომპიუტერული პროგრამა და მართავს სხვადასხვა სამომსმარებლო პროგრამულ პაკეტებს , ასევე კომპიუტერის სისტემის შემადგენელ მოწყობილობებს და ამ სისტემის მომხმარებელს შორის ურთიერთბას. ოპერაციული სისტემა კომპიუტერული სისტემის შემადგენელი ნაწილია და 285-ე მუხლში მითითებული ,, კომპიუტერული პროგრამა " მასში არ იგულისხმება .

რაც შეეხება მოწყობილობას , მასში უნდა მოვიაზროთ ის დამატებითი დეტალები , რომლებიც არა კომპიუტერული სისტემის შემადგენელ მექანიზმთა განუყოფელი ნაწილი , მაგრამ აღჭურვილია მათში ინტეგრირების უნარით.

სხვა მოწყობილობაში უნდა ვიგულისხმოთ ისეთ ტიპის მექანიზმი რომელიც მონაცემს ელექტრონულად ამუშავებს, გადასცემს, ინახავს , იწერს და ასე შემდეგ , ასეთია : ტელეფონის ავტომოსასუხე , ციფრული ვიდეო კამერა , ფაქსის აფარატი , პრინტერი , სკანერი , პეიჯები , ჯპს , სატელიტური მოწყობილობა და სხვა .

რაც შეეხება დანაშაულის ობიექტური მხარის ნიშნებს , როგორიცა კომპიუტერული პროგრამის , მოწყობილობის, პაროლის , დაშვების კოდის ან სხვა მსგავსი მონაცემის უნებართვო დამზადება , შენახვა , გაყიდვა , გავრცელბა , ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფა უნდა აღინიშნოს , რომ ეს არ გულისხმობს მხოლოდ მათი თავიდან დამზადებას. მასში იგულისხმება უკვე არსებული მონაცემის გაშიფრაც . მაგალითად , თუ დამნაშავეს სპეციალური პაროლოს მოსაგები პროგრამის გამოყენებით მიიღებს კომპიუტერულ სისტემაში შეღწევისთვის საჭირო პაროლს , იგი

ამ ქმედებით დაამზადებს არა ახალ , არამედ უკვე არსებულ პაროლს . ამის შემდეგ , მას შეუძლია დაამზადოს ახალი პაროლი ძველის შეცვლის გზით .

285-ე მუხლით გათვალისწინებული დანაშაულის ჩადენის საშუალებაა ის ტექსნიკური და პროგრამული უზრუნველყოფა , რომლის დახმარებითაც ხორციელდება პროგრამის , მოწყობილობის , პაროლის , დაშვების კოდის , ან სხვა მსგავსი მონაცემის დამზადება ამავე დანაშაულის ჩადენის საშუალება ის კომპიურეული პროგრამა , რომლის დახმარებითაც შესაძლებელია სხვადასხვა მონაცემის შენახვა ასევე სოციალური ქსელი და საკომუნიკაცია პროგრამა , რომელებიც გამოიყენება ინფორმაციის გადაცემა-გავრცელებისთვის .

285-ე მუხლით გათვალისწინებული დანაშაული ფორმალური შემადგენლობისაა . ქმედების დანაშაულთა კვალიფკაციისთვის საკმარისია , კომპიუტერული პროგრამის ანდა სხვა მოწყობილობის აგრეთვე კომპიუტერულ სისტემაში შეღწევისთვის საჭირო პაროლის , დაშვების კოდის , ანდა სხვა მსგავსი მონაცემის უნებართვო დამზადების , შენახვის , გაყიდვის , გავცელების , ან ხელმისაწვდომობის სხვაგვარი უზრუნველყოფის ფაქტის დადგენა .

2.2.1.3 საქართველოს სისხლის სამართლის კოდექსის 286-ე მუხლით გათვალისწინებული დანაშაულის ობიექტური შემადგენლობა

საქართველოს სისხლის სამართლის კოდექსის 286-ე მუხლის დისპოზიცია ჩამოყალიბებულია შემდეგგვარად:

,, კომპიუტერული მონაცემის უნებართვი დაზიანება , წაშლა , შეცვლა ან დაფარვა “.

მე-2 ნაწილის განსაზღვრება შემდეგგვარია:

,, ამ მუხლის პირველი ნაწილით გათვალისწინებული ქმედება , აგრეთვე , კომპიუტერუელი მონაცემის უნებართვო ჩასმა ან გადაცემა , რამაც კომპიუტერული სისტემის ფუნქციონორების განძრახ მნიშვნელოვანი შეფერხება გამოიწვია “.

აღნიშნული დანაშაულის უშუალო ობიექტია იმ პომპიუტერული მონაცემის ინტერესი , რომელის უნებართვო დაზიანება , წაშლა , შეცვლა ან დაფარვა ხორციელდება . ასევე , ხელყოფის ობიექტი შეიძლება იყოს , კომპიუტერული სისტემის მთლიანობა და ნორმალური ფუნქციონირება . გ.მამულაშვილის აზრით , დანაშაულის ობიექტია კომპიუტერული სისტემის ინტეგრირებულობა და ნორამლური ფუნქციონირება , ასევე კომპიუტრეული სისტემის მფლობელის ინტერესი და მომხმარებელთა უფლებები .[37]

დანაშაულის საგანია ის კომპიუტერული მონაცემი , რომლის უნებართვო დაზიანება , წაშლა , შეცვლა ან დაფარვა ხორციელდება . ასევე , ის კომპიუტერული [38]სისტემა , რომლის ფუნქციონორებაც ფერხდება დანაშაულის შედეგად. კომპიუტერული სისტემის ფუნქციონირების შეფერხება არ გულისხმობს როგორც კომპიუტერული ტექნიკის მწყობრიდან გამოსვლას . ის გულისხმობს კომპიუტერული სისტემის ფუნცის მოშლას , არასათანადოდ შესრულებას . იმ შემთხვევაში თუ მოხდება კონკრეტულად კომპიუტერული ტექნიკის დაზიანება და დადგება 150 ლარზე მეტი ოდენობის ზიანი სახეზე გვექნება არა კიბერ დანაშაული , არამედ , სისხლის სამართლის კოდექსის 187-ე მუხლით აკრძალული სხვისი ნივთის დაზიანება ან განადგურება , რამაც მნიშვნელოვანი ზიანი გამოიწვია.

უ.ზაქაშვილის აზრით , ქართლი სისხლის სამართლის კიბერდანაშაულის მუხლები უნდა შეიცავდნენ დათქმას დანაშაულის ხელყოფის უბიექტთან დაკავშირებით. კერძოდ , კი განსაკითრებულად მნიშვნელოვანია დამამძიმებელი გარემოებებში სახელმშიფო ინტერესის და უსაბრთხოების ხაზგასმა .[39]

მისი აზრით, უმჯობესია რომ საქართველოს სისხლის სამართლის კოდექსის 284-ე , 285-ე და 286-ე მუხლების დისპოზიციას დაემატოს წინადადება , რომლის მიხედვითაც უფრო მძიმე სასჯელი იქნება გათვალისწინებული იმ კომპიუტერულ სისტემაზე

---

[37] ავტორთა კოლექტივი,"სისხლის სამართლის კერძო ნაწილი", წიგნი 2 გამომც, „მერიდიანი" თბ. 2012. გვ 43

[38] ავტორთა კოლექტივი,"სისხლის სამართლის კერძო ნაწილი", წიგნი 2 გამომც, „მერიდიანი" თბ. 2012. გვ 44

[39] უ.ზაქაშვილი,კიბერდანაშაულის სისხლისამართლებრივი რეგულირების პრობლემები საქართველოში, დისერტაცია, თბ, 2013 გვ 65

უკანონო ზემოქმედებისთვის , რომლის მესაკუთრე სახელმწიფოა და რომელიც ემსახურება ქვეყნის თავდაცვით და უშიშროების ინტერეს , რადგამ არ შეიძლებ გავაიგივოთ კერძო პირის კომპიუტერული სისტემა , რომელში შესაძლებელია კომპიუტრეული თამაშის და რამდენი ფოტოს გარდა არაფერი ინახებოდეს და კომპიუტრეული სისტემა, რომელიც შეიცავს სახელმწიფო მნიშვნელობის ინფორმაციას.

დანაშაულის ობიექტური მხარე შეიძლება გამოიხატოს უშუალოდ კომპიუტრეული მონაცემის უნებართო დაზიანებაში , წაშლაში , შეცვლასა ან დაფარვაში .

დანაშაულის ჩადენის საშუალება ის კომპიუტერული პროგრამა , რომლის გამოყენებითაც ხორციელდება კომპიუტრეული მონაცემის უნებართვო დაზიანება , წაშლა , შეცვლა ან დაფარვა . თუმცა შეიძლება ამ მოქმედების განხორციელებას არანაირი სპეციალური პროგრამა არ დასჭირდეს. მაგალითად , თუ პირი მოიპოვებს იმ სისტემაში შეღწევის პაროლს , რომელშიც ინახება აღნიშნული მონაცემი , ის ყოველგვარი დამხმარე პროგრამის გარეშე შეძლებს მის განადგურებას , დაზიანებას , და ასე შემდეგ.

ევროპის საბჭოს კონვენციის მე-4 მუხლი არამხოლოდ კომპიუტერული მონაცემების დაზიანებას და წაშლას გამოყოფს დასჯად ქმედებად, არამედ ისეთ ქმედებას, რომელმაც შესაძლოა გამოიწვიოს მსგავის დაიზიანება. ერთ-ერთი ასეთი ქმედება კომპიუტერულ მონაცემებში ცვლილებების შეტანა. თუ კომპიუტერული ვირუსი ცვლის მონაცემების შინაარს, ეს უთანაბრდება ფაილის წაშლას.[40] ევროსაბჭოს ექსპერტების აზრით, კომპიუტერული მონაცეემის შეცვლაში მოიაზრება მის შინაარსში ცვლილებების შეტანა და იგი უნდა გავუთანაბროთ კომპიუტერული მონაცემების წაშლას. აღნიშნულ მოსაზრებას უ.ზაქაშვილი [41] არ იზარებს იმ ნაწილიში, რომ მონაცემის შეცვლა უთანაბრდება მის წაშლას. შესაძლოა ვისაუბროთ ამ ორი ქმედების გამო დამდგარ მსგავს შედეგზე და ზინზე, მაგრამ შინარსით ისინი განსხვავდებიან ერთმანეთისგან.

[40] ავტორთა კოლექტივი, „სისხლის სამართლის კერძო ნაწილი“, წიგნი 2 გამოც. „მერიდიანი“, თბ. 2012, გვ. 42

[41] უ. ზაქაშვილი, კიბერდანაშაულის სისხლისამართლებრივი რეგულირების პრობლემები საქართველოში, დისერტაცია, თბ., 2013, გვ. 64

როგორც ევროპის საბჭოს კონვენციამ ისე ქართულმა კანომდებელმა კოდექსის 286-ე მუხლში ეს ტერმინები არ გაიგივა ერთმანეთს და ცალ-ცალკე გამოყო. ამ გვარად, კომპიუტერული მონაცემის წაშლაა, როცა ხდება მისი სრული განადგურება, ხოლო შეცვლაში უნდა ვიგულისხმოთ მის შინარსში ცვლილებების შეტანა.

კომპიუტერული მონაცეემის დაფვარვაა ამ მონაცემის ისეთი დამალვა, როცა მისი მფლობელისთვის უცნობია სად ინახება ის. გარდა ამისა, არსებობს ისეთი კომპიუტერული პროგრამა, რომელიც ახდენს კომპიუტერული მონაცემის უჩინარად გადაქცევას, ან ასეთ დროს კომპიტერული მონაცემი ვიზუალურად ვერ აღიქმება, თუმცა მყარ დისკზე ინახება.აღნიშნულ ხერხს ხშირად იყენებენ მსხვილი კომპანიები,როდესაც საგადასახადო სამსახურს უმალავენ ე.წ. „შავ ბუღალტერიას“.

ამავე ხერხს მიმართავენ ჰაკერები როდესაც სამრთალდამცავი ორგანოები ამოწმებენ მათ კომპიუტერს.

აღნიშნული მსჯელობიდან გამომდინარე, შეიძლება დავასკვნათ, რომ 286-ე მუხლით გათვალისწინებული დანაშაული მატერიალური შემადგენლობისაა, რადგან იგი უკავშირდება კონკრეტული შედეგის დადგომას.

286-ე მუხლის მერე ნაწილში მითითებულია:

„286 მუხლის პირველი ნაწილით გათვალისწინებული ქმედება, აგრეთვე კომპიუტერული მონაცემის უნებართვო ჩასმა ან გადაცემა, რამაც კომპიუტერული სისტემის ფუნქცინირების განძრახ მნიშვნელოვანი შეფერხება გამოიწვია“.

[42] კომპიუტერული სისტემის ფუნქციონირების განძრახ მნიშვნელოვან შეფერხებაში უნდა ვიგულისხმოთ კომპიუტერული სისტემის მუშაობის არსებითი შეფერხება. მაგალითად, თუ კიბერ შეტევის ობექტია ავიაკომპანია, რომელსაც შეტევის შედეგად ხელი შეშალა ფრენიების განხორციელებაში, მომხმარებლებს შეზღუდად ბილეთის შეძენის საშვალება ა.შ. ან მაგალითად, თუ სამეწარმეო რესტრის კომპიუტერულ სისტემაზე იერიშის გამო შეუძლებელი გახდა ახალი სამეწარმეო სუბექტების

[42] უ.ზაქაშვილი,კიბერდანაშაულის სისხლისამართლებრივი რეგულირების პრობლემები საქართველოში, დისერტაცია, თბ, 2013 გვ 66-67

რეგისტრაცია, ან უკვე რეგისტრირებულ სუბექტზე არსებული საჯარო ინფორმაციაზე შეიზღუდა ხელმისაწვდომობა ,რამაც გამოწვია კონკრეტული ხასაითის ზიანი,იქნება ეს ფინანსური ძარალი, სამეწარემო საქმინობის შეფერხება და ასე შემდეგ.

კომპიტერულ მონაცემების უნებართვო ჩასმა გულისხმობს, როგორც კომპიუტერული მონოცაემის არადანიშნულებისამებრ და არამიზრობრიავად ჩაწერა.
მაგალითად, როდესაც დამნაშავე სამიზნე კომპიუტერში უნებართვოდ ჩაწერს სპეციალურ პროგრამას,რომლის გააქტიურებაც შეაფერხებს კომპიუტერული სისტემის ფუნქციონირებას.

კომპიუტერული მონაცემის გადაცემის ყველაზე თვალსაჩინო მაგალითია ეგრედწოდებული „დოს“ შეტევა, ანუ როდესაც საიტის სერვერის მიმართ გადიცემა ერთდროულად 1000-ობით მოთხოვნა, რასაც სერვერი ვერ უძლებს და ხდება კომპიუტერული სისტემის ფუნქცინირების შეფერხება.

[43]286-ე მუხლის მერე ნაწილით გათვალისწინებული დანაშუალის ობექტური მხარე გამოიხატება, კომპიუტერული მონაცემების ისეთ მიზანმიმართულ გადაცემაში, რომელიც მიმართულა კომპიუტერული სისტემის ნორმალური ფუნქციონირებისთვის ხელის შეშლისკენ

აღსანიშნავია, რომ მოცემული დანაშაული მატერიალური შემადგენლობისა, რადგან სისხლის სამართლებრვი პასუხისმგებლობა უკავშირდება კონკრეტული შედეგის დადგომას, ანუ კომპიუტერული სისტემის განძრახ მნიშვნელოვან შეფერხებას.

კიბერშეტევის მავნე შედეგებზე შესაძლებელია დაუსრულებლად საუბარი აღსანიშნავია იმის განსაზღვრა თუ რაში შეიძლება გამოიხატოს 286-ე მუხლის 2 ნაწილით გათვალისწიინებული ქმედების ობექტური მხარე. აღნიშნულის განსახილველად ცოცხალი მაგალითია საქართველოს უახლესი ისტორიიდან 2008წ რუსეთ საქართველოს ომი. [44] ინფორმაციულ ტექნოლოგიებზე სახელმწიფოს

[43] ავტორთა კოლექტივი, მოსამრთლეების ტრენინგი კომპიტერული დანაშაულის შესახებ:ტრენინგი სახემძღვანელო,ევრო საბჭო, სტრასბურგი, 2010 წ გვ. 55
[44] ბ,კვირკველია. „კომპიუტერული დანაშაული“

კრიტიკული ინფრასტრუქტურის დამოკიდებულებასთან ერთად იზრდება ის გამოწვევები, რომლებიც საქართველოს ინფორმაციული სივრცის დაცვასთანაა დაკავშირებული. 2008 წლის რუსეთ - საქართველოს ომის დროს რუსეთის ფედერაციამ საქართველოს წინააღმდეგ, სახმელეთო, საჰაერო და საზღვაო შეტევების პარალელურად, მიზანმიმართული და მასობრივი კიბერთავდასხმები განახორციელა. ამ კიბერშეტევებმა აჩვენა, რომ კიბერსივრცის დაცვა ეროვნული უსაფრთხოებისთვის ისევე მნიშვნელოვანია, როგორც სახმელეთო, საჰაერო და საზღვაო სივრცეების დაცვა.

იმ დროს როდესაც ეს კიბერშეტევა განხორციელდა, საქართველოს სისხლის სამართლის კოდექსი არ შეიცავდა 286-ე მუხლს არსებული რედააქციით, ის კომპიუტერული დანაშაულებრივი, რომელსაც კოდექსი ითვალისწინებდა, არ მოიცავდა მსგავსი შინაარსის ქმედებას. კერძოდ 284 მუხლი ითვალისწინებდა კანონით დაცულ ინფორმაციაში არამართლზომიერ შეხწევას, 285 -ე მუხლი ეგმს დამაზიანებელი პროგრამის შექმანს ან არსებულ პროგრამაში ცვლილებების შეტანას, რამაც გამოიწვია ინფორმაციის განძრახ განადგურება, ბლოკირება და ა.შ. 286-ე მუხლით აგრძალული იყო ეგმს და მისი ქსელის ექსპლუატაციის წესების დარღვევა.

ეგრედ წოდებული დოს შეტევა არ მოიცავს არც კომპიუტერულ სისტემაში შეხწევის და არც მისი დამაზიანებელი პროგრამის შექმნის, გავრცელების და ასე შემდეგ ფაქტს. აქედან გამომდინარე, 208 წელს სამრთალდამცევი ორგანოეები კომპიტერული დანაშაულის ჩადენის ფაქტზე გამოძიებას ვერ ჩატარებდნენ. თუმცა ისევე, როგორც დღეს, მაშინაც არსებობდა კოდექსის 318-ე მუხლი, კერძოდ საბოტაჟი: „საქართველოს დასუსტების მიზნით სახელმწიფო ან სხვა საწარმოს, დაწესებუელბის, ორგანიზაციის ან სამსახურის ნორმალური ფუნქციონირებისთვის ხელის შეშლა“. საბოტაჟი ამ ფორმით ფორმალურ დანაშაულს წარმოადგენს და იგი დამთავრებულად ჩაითვლება საქართველოს დასუსტების მიზნით ხელის შემშლელი ნებისმიერი ქმედების ჩადენის მომენტიდან, იმისგან დამოუკიდებლად, მოყვა თუ არა მას ქვეყნისთვის საზიანო შედეგი.

318-ე მუხლის მერე ნაწილი სრულად შესაბამება საქართველოს წინაღმდეგ განხორციელებული კიბერშეტების არსს. კერძოდ, „დოს“ შეტევის შინაარს ამა თუ იმ საიტის მუშაობისთვის ხელის შეშლა წარმოადგენს, მაშინ როცა შეტევის მიზანი ხდება სამთავრობო და მასობრივი ინფორმაციის საშვალება, მტკიცება რომ ესაა საქართველოს წინაღმდეგ განხორციელებული საბოტაჟი, დასაბუთებული ხდება. გარდა ამისა, მოხდა მოსახლეობისთვის სასიცოცხლო მნიშნველობის დაწესებულების და ორგანიზაციების ნორმალური ფუნქცინირებისთვის აუცილებელი, საზოგადოებრივი უშიშროების და წესრიგის დაცვისთვის განკუთვნილი ობექტის დაიზნება და მწყობრიდან გამოყვანა, რადგან ყველა სამთავრობო საიიტი, მით უფრო შინაგან საქმეთა , თავდაცვის სამინისტროს და პრეზიდენტის საიტები, განსაკუთრებით ომის პერიოდში წარმოადგენენ სასიცოცხლო ობიექტებს და ემსახურებიან მოსახლეობის სწორი ინფორმაციით აღჭურვას, რათა არ შეიქმნას პანიკა, შესაძლებელი გახდეს ქვეყნის მაშტაბით გადადგილება და სხვა. სისხლის სამართლის 284 -ე მუხლის შენიშვნის 3 ამე ნაწილის შესაბამისად ტერმინი „უნებართვო“ განმარტებულია, რომ უნებართვო გულისხმობს უკანონოს, აგრეთვე იმ შემთხვევას, როდესაც უფლების მფლობელს პირდაპირ ან არაპირდაპირ არ გადაუცია უფლება ქმედების ჩამდენი პირისთვის.

2.3 კიბერსივრცის საერთაშორისო და რეგიონალური დაცვითი ღონისძიებები

კიბერდანაშაულთან ბრძოლისა და კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის პროცესში დიდი მნიშვნელობა ენიჭება არამარტო ეროვნულ პოლიტიკას, სტრატეგიასა თუ სხვა სახის ქმედით ზომებს, არამედ ასევე თანამშრომლობას საერთაშორისო და რეგიონალურ დონეზე. მსგავსი თანამშრომლობა კიბერსივრცის

დაცვის სფეროში ითვალისწინებს და მოიცავს საერთაშორისო და რეგიონალურ კონვენციებს, ფორუმებს, ორგანიზაციებსა და ალიანსებს, შეხვედრებსა და დისკუსიებს, ერთობლივ რეზოლუციებს, გადაწყვეტილებებსა და რეკომენდაციებს, დირექტივებს.

2001 წლის 23 ნოემბერს ბუდაპეშტში ხელი მოეწერა კიბერდანაშაულთან ბრძოლის [45]ევროპულ კონვენციას (CETS 185) 1 , რომელიც ძალაში შევიდა 2004 წლის 1 ივლისს. კონვენცია მომზადდა ევროპის საბჭოს ფარგლებში კანადის, შეერთებული შტატების, იაპონიისა და სამხრეთ აფრიკის რესპუბლიკის მონაწილეობით. დღესდღეისობით ეს კონვენცია არის მოცემულ სფეროში ერთადერთი აღიარებული იურიდიული დოკუმენტი, რომელიც მიღებულია საერთაშორისო დონეზე და ის არის ღია ყველა დაინტერესებული ქვეყნისთვის. ასევე საინტერესოა კონვენციაზე დამატებით მიღებული პროტოკოლი (CETS 189)2 კომპიუტერულ ქსელებში ქსენოფობიისა და რასიზმის ნიადაგზე ჩადენილი დანაშაულების შესახებ, რომელსაც ხელი მოეწერა 2003 წლის იანვარში და ძალაში შევიდა 2006 წლის მარტის თვეში.

კონვენცია ხელმომწერ ქვეყნებს ავალდებულებს შექმნან სამართლებრივ - ნორმატიული ბაზა აუცილებელი კიბერდანაშაულის პრობლემის ეფექტური გადაწყვეტისთვის. ასევე ყველა ხელმომწერი ქვეყანა თავის თავზე იღებს ერთმანეთისთვის დახმარების აღმოჩენას კიბერდამნაშავეთა სამართლებრივი დევნისა და ინციდენტების გამოძიების საკითხში. ევროპული კონვენცია არის ერთერთი პირველი საერთაშორისო დოკუმენტი, სადაც განსაზღვრულია და კლასიფიცირებულია კიბერდანაშაული. კერძოდ, შემოსულია ინტერნეტ სივრცეში არასანქცირებული შეღწევისა და რესურსების არაკანონიერი გადაჭერის განსაზღვრება, კომპიუტერულ სისტემებსა და ინფორმაციის მატარებელზე არაკანონიერი ჩარევა, მოწყობილობის არასამართლებრივი გამოყენება, კომპიუტერული მაქინაციები. კონვენციის მოქმედება ასევე ვრცელდება საბავშვო პორნოგრაფიასა და საავტორო უფლებების დარღვევაზე. დოკუმენტში განსაზღვრულია კომპიუტერული დანაშაულების ეფექტური გამოძიების

[45] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

ინსტრუმენტები და მათთან ბრძოლა. კონვენციის მოქმედფება ვდრცელდება ყველა დანაშაულზე, რომელიც ჩადენილია კომპიუტერულ სისტემებში, ასევე ელექტრონული საშუალებებით შეგროვილი ნებისმიერი მტკიცებულებები.

ამ ეტაპზე კონვენცია რატიფიცირებულია ევროკავშირის ყველა ქვეყნისა და შეერთებული შტატების მიერ, და ხელმოწერილია ორმოცდაექვსი ქვეყნის მიერ[46] . ხუთ ქვეყანას მიეცა რეკომენდაცია და გაუკეთდა შეთავაზება მიუერთდეს კონვენციას . ისეთმა დიდმა ქვეყნებმა, როგორებიცაა ჩინეთი და რუსეთი უარი თქვეს ხელი მოეწერათ კონვენციაზე და მიერთებოდნენ მას [47]. ევროპული კონვენცია გამოიყენება როგორც სახელმძღვანელო და ცნობარი მსოფლიოს ასზე მეტი ქვეყნის სტანდარტული ან ტიპიური საკანონმდებლო ბაზისათვის. გარდა ამისა, კონვენცია მხარს უჭერს ყველა სხვა ორგანიზაციას, რომლებიც იყენებენ მას თავიანთი გადაწყვეტილების მიღებაში. ეს ორგანიზაციებია ევროპის კავშირი, ამერიკის სახელმწიფოთა ორგანიზაცია (OAS) [48] , ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაცია (OECD)[49] , აზია - წყნარი ოკეანის ეკონომიკური თანამშრომლობის ორგანიზაცია (APEC) [50] , ინტერპოლი , ასევე კერძო სექტორის წარმომადგენლები.

მიუხედავად იმისა, რომ მოცემულ კონვენციას აქვს ფართო საერთაშორისო აღიარება, ზოგიერთი ქვეყანა მაინც ამტკიცებს, რომ კონვენცია ითვალისწინებს კიბერდანაშაულის აღსაკვეთად საჭირო არასაკმარის ზომებს, და რამაც შეიძლება დიდი.ზიანი მიაყენოს ეროვნულ უსაფრთხოებას. პირველ რიგში, კონვენცია კომპიუტერულ ქსელზე განხორციელებულ შეტევას განიხილავს როგორც კერძო და სახელმწიფო საკუთრების წინააღმდეგ ჩადენილ დანაშაულს, და არა როგორც ეროვნული უსაფრთხოების საფრთხეს. მეორე, კონვენცია ერთმანეთისგან არ

[46] ევროკავშირის წევრი ქვეყნები, კანადა, იაპონიია, სამხრეთ აფრიკის რესპუბლიკა და ნატო - ს ყველა წევრი ქვეყანა

[47] აღნიშნული კონვენცია საქართველოსთან მიმართებაში ძალაში შევიდა 2012 წლის პირველი ოქტომბრიდან. შედეგად, საქართველო გახდა კონვენციის 34-ე წევრი სახელმწიფო

[48] Organization of American States http://www.oas.org/en/

[49] Organization for Economic Co-operation and Development http://www.oecd.org/

[50] Azia – Pacific Economic Cooperation http://www.apec.org/

ანსხვავებს შეტევებს ჩვეულებრივი კომპიუტერული ქსელებსა და კრიტიკული ინფორმაციული ინფრასტრუქტურის ობიექტებს შორის, ისევე როგორც ფართომასშტაბიან და ლოკალურ შეტევებს შორის.

თუმცა კონვენცია წარმოადგენს სტანდარტულ დოკუმენტს, რომელიც წარმოადგენს საერთაშორისო კანონმდებლობის ძალზედ მნიშვნელოვან შემადგენელ ნაწილს. მასში მოცემულია იურიდიული და ტექნიკური ნორმების ოპტიმალური კომპლექსი, რომელიც შეიძლება გამოყენებულ იქნას ამ სფეროში საერთაშორისო თანამშრომლობის გაფართოებაზე დამატებითი შეთანხმებების დამუშავების მიზნით. გამომდინარე, რომ კიბერდანაშაულს, კიბერტერორიზმსა და კიბერომს გააჩნიათ ბევრი საერთო ნიშანი და მახასიათებელი, კონვენცია ნებისმიერ კიბერშეტევაზე, მიუხედავად მათი მოტივაციისა, ითვალისწინებს, რომ მასზე ხელმომწერმა ქვეყნებმა პასუხისმგებელი უწყებების მოთხოვნაზე უნდა დააკავონ და გადასცენ ყველა კიბერდამნაშავე სამართალდამცავ ორგანოებს, მიუხედავად იმისა, განიხილებიან თუ არა ისინი საკუთარ ქვეყნებში როგორც დამნაშავეები, ტერორისტები ან კიდევ პატრიოტები.

ევროკავშირი წარმოადგენს ინფორმაციული უსაფრთხოების სფეროში საერთაშორისო დონეზე არსებულ მთავარ სუბიექტს. ამავდროულად, ევროკავშირი დიდ ყურადღებას უთმობს ისეთ საკითხებს, როგორიც არის კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვა, ინფორმაციული საზოგადოების ფორმირება და ინფორმაციული დაცვა. ევროკავშირმა დაიწყო სამეცნიერო - კვლევითი და სხვა სახის პროგრამების რეალიზება, რომელიც უკავშირდება ინფორმაციული რევოლუციის ასპექტებსა და განათლებაზე, ბიზნესზე, ჯანდაცვასა და კავშირგაბმულობაზე მათ გავლენას.

2004 წლის 20 ოქტომბერს [51] ევროკავშირის კომისიის მიერ მიღებული კომუნიკე კრიტიკული ინფრასტრუქტურის დაცვაზე იძლევა კრიტიკული ინფრასტრუქტურისა და მისი ობიექტების განსაზღვრებას, ასევე ადგენს კრიტერიუმებს იმ ობიექტების მიმართ,

[51] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm

რომლებიც შეიძლება წარმოიშვას მომავალში. 2005 წლის ნოემბერში [52]ევროკავშირის კომისიის მიერ მიღებულია კრიტიკული ინფრასტრუქტურის დაცვის ევროპული პროგრამა „მწვანე წიგნი“, სადაც განსაზღვრულია ევროკავშირის მოქმედების მიმართულებები მოცემულ სფეროში. 2008 წელს ევროკავშირის კომისია შეუდგა პროექტის რეალიზებას, რომელიც მიმართულია კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის საერთო სტრატეგიის გამომუშავებაზე.

ქვემოთ მოცემულია ევროკავშირის კომისიის სხვა პროექტები და სტრატეგიები:

ევროკავშირის კომისიის დაკვეთით, ელექტრონული კავშირის ინფრასტრუქტურის შეღწევადობისა და საიმედოობის პრობლემების კვლევების ჩატარება (ARECI),[53]

პროექტი „კრიტიკული ინფრასტრუქტურის საფრთხეების შეტყობინების ინფორმაციული ქსელი“ (CIWIN),[54]

2004 წლის მარტში შეიქმნა და 2005 წლის სექტემბერში, კუნძულ კრეტაზე დაიწყო ფუნქციონირება ქსელური და ინფორმაციული უსაფრთხოების ევროპულმა სააგენტომ (ENISA) [55] სააგენტოს მიზანია ევროკავშირის ფარგლებში ელექტრონული ქსელების უსაფრთხოების მაღალი დონის მიღწევა;

ტელემეტრიის ტრანსევროპული სამთავრობოთაშორისო სამსახური (TESTA)[56] . ეს არის სამთავრობოთაშორისო კავშირის ქსელი, რომელიც მოქმედებს მხოლოდ ევროკავშირის ფარგლებში. ის არ არის ჩართული ინტერნეტ - სივრცეში და სხვადასხვა უწყების თანამდებობის პირებს ერთმანეთთან ურთიერთობისას, ინფორმაციის დაზიანებისა და გადინების თავიდან აცილების საშუალებას აძლევს.

დიდი რვიანი 1995 წლიდან მოყოლებული სულ უფრო მეტ აქტიურ მონაწილეობას იღებს იმ საკითხების გადაწყვეტაში, რომლებიც უკავშირდება კიბერდანაშაულს,ინფორმაციულ საზოგადოებას, კრიტიკული ინფორმაციული

[52] იქვე

[53] The Availability and Robustness of Electronic Communications Infrastructures

[54] The Critical Infrastructure Warning Information Network https://ciwin.europa.eu/Pages/Home.aspx

[55] The European Union Agency for Network and Information Security https://www.enisa.europa.eu/

[56] The European Software Testing Awards http://www.softwaretestingawards.com/

ინფრასტრუქტურის დაცვას. 1995 წელს ჰალიფაქსის სამიტზე [57] შეიქმნა უფროს ექსპერტთა ჯგუფი, რომელსაც დაევალა შეეფასებინა და გაანალიზებინა არსებული საერთაშორისო შეთანხმებები, ასევე ორგანიზებულ დანაშაულთან ბრძოლის მექანიზმები. მოცემულმა ჯგუფის მიერ ჩატარებული სამუშაოს შედეგად, შემუშავდა ორმოცი ოპერატიული რეკომენდაცია, რომლებიც დამტკიცებულ იქნა 1996 წელს დიდი რვიანის ლიონის სამიტზე. ამ დროდან მოყოლებული ლიონის ჯგუფი გახდა მუდმივმოქმედი მრავალფუნქციური ორგანო, რომლის შემადგენლობაში შევიდა მთელი რიგი სპეციალური სამუშაო ჯგუფები. 2001 წლიდან, ტერორიზმთან დაკავშირებულ საკითხებზე, ლიონის ჯგუფის სხდომები მიმდინარეობს ერთობლივად რომის ჯგუფთან.

კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის სფეროში დიდი რვიანის მუშაობის მიღწევად შეიძლება ჩაითვალოს, პარიზში 2000 წელს [58] ჩატარებული კონფერენცია, სადაც მონაწილეობას იღებდა როგორც სახელმწიფო ისე კერძო სექტორი. კონფერენცია მიეძღვნა სახელმწიფოსა და კერძო სექტორს შორის უსაფრთხოებისა და კიბერსივრცის სფეროში სანდოობის ამაღლების განვითარება. კონფერენციის მიზანი იყო მარალტექნოლოგიური დანაშაულისა და ინტერნეტ - სივრცის არაკანონიერი გამოყენების ირგვლივ მსჯელობა და გადაწყვეტილების მიღება. დიდი რვიანის წევრი ქვეყნები პარიზის კონფერენციაზე შეთანხმდნენ კიბერდანაშაულთან ბრძოლის კონკრეტულ და გამჭვირვალე პრინციპებზე, რომლებიც მიმართულია ახალი „უსაფრთხოების კულტურის“ შექმნაზე, საერთაშორისო თანამშრომლობის გააქტიურებაზე, ასევე მონიტორინგისა და კომპიუტერულ ქსელებში საფრთხის შეტყობინების სფეროში არსებული მოწინავე გამოცდილების გაზიარებაზე. კონფერენციაზე ასევე მიღწეული იყო შეთანხმება ერთობლივი სასწავლო კურსების ჩატარებაზე, რომელმაც უნდა გამოავლინოს ქსელებში საგანგებო ინციდენტებზე რეაგირების სამსახურების მომზადების მზადყოფნა, აგრეთვე საფრთხეების შესახებ

[57] http://www.chebucto.ns.ca/Current/HalifaxSummitG7/

[58] https://www.ciret.org/conferences/paris-2000/

შეატყობინოს სხვა ქვეყნების მთავრობებს. კონფერენციაზე სულ მიღებული იქნა თერთმეტი პრინციპი, რომლებიც დახმარებას გაუწევს სახელმწიფოებს კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის სფეროში შექმნას და გაატაროს ეფექტური ეროვნული პოლიტიკა.

კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის პრინციპების ძირითადი ელემენტები აისახა, 2004 წელს გაეროს 78 - ე ასამბლეაზე მიღებულ №58/199 რეზოლუციაში [59] „კიბერუსაფრთხოებისა და კრიტიკული ინფორმაციული ინფრასტრუქტურის დაცვის გლობალური კულტურის შექმნაზე“.

2002 წელს, მას შემდეგ რაც 1990 წლების ბოლოს ბალკანებზე სამხედრო ოპერაციის დროს განხორციელდა ქსელური შეტევები, ალიანსმა შეიმუშავა და გაუშვა კიბერ - დაცვის საკუთარი პროგრამა. ალიანსის ხელმძღვანელობამ გაითვალისწინა „ბალკანეთის გაკვეთილები“, და 2002 წელს პრაღის სამიტზე[60] ნატო - ს წევრი ქვეყნების ლიდერები შეთანხმდნენ კიბერნეტიკული თავდაცვის პროგრამის შემუშავებასა და ინფორმაციულ ქსელებში ინციდენტებზე რეაგირების საკუთარი ჯგუფის (NCIRC) [61] შექმნაზე. ჯგუფის საკოორდინაციო ცენტრი განთავსებულია ბრუსელში, ნატო - ს შტაბ - ბინაში, ხოლო ალიანსის სამეთაურო ოპერაციების მართვის შტაბში[62] ორგანიზებულ იქნა NCIRC - ს ტექნიკური ცენტრი. მოცემული სტრუქტურის შექმნით, ალიანსმა გადაწყვიტა მთელი რიგი სირთულეები დაკავშირებული კიბერუსაფრთხოების საკითხებთან. კერძოდ, ნატო - ს კომპიუტერულ ქსელებში არასანქცირებული შეღწევისა და სხვა მავნებლობების აღმოჩენა და განეიტრალება, ასევე ქსელების კრიპტოგრაფიული დაცვის ეფექტური მართვის უზრუნველყოფა.

გარდა ამისა, ალიანსის ექსპერტები უზრუნველყოფენ კომპიუტერულ ქსელებში საფრთხის წარმოქმნის საწინააღმდეგო ტექნიკურ ღონისძიებების, ასევე შეიმუშავებენ

[59] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf

[60] Cooperative Cyber Defense Centre of Exelllence https://ccdcoe.org/tallinn-manual.html

[61] 1 Computer Incident Response Capability https://www.terena.org/activities/tf-csirt/meeting11/NCIRC-Anil.pdf

უსაფრთხოების უზრუნველყოფის რეჟიმსა და კომპიუტერულ დანაშაულებების გამოძიების მეთოდოლოგიას. ამის პარალელურად, ტალინში შეიქმნა ალიანსის კომპიუტერული თავდაცვის სფეროში მოწინავე გამოცდილების გაცვლის ცენტრი (CCDCOE), ნატო-მ ასევე დააფუძნა კიბერ - თავდაცვის ღონისძიებების მართვის სპეციალური ორგანო (CDMA) [63] , რომელმაც ფუნქციონირება დაიწყო 2008 წელს. ამ უკანასკნელის ფუნქციებში შედის ალიანსის კომპიუტერულ ქსელზე შეტევის შემთხვევაში „კიბერ - თავდაცვის ოპერატიული და ეფექტური ღონისძიებების“ ორგანიზება და კოორდინაცია. 2009 წელს სტრასბურგის სამიტზე ნატო-ს წევრმა ქვეყნებმა ვალდებულება აიღეს დააჩქარონ კიბერ-თავდაცის თანამედროვე საშუალებების შეძენა, გახადონ კიბერდაცვა ალიანსის განუყოფელ ნაწილად, განავითარონ საერთაშორისო თანამშრომლობა არამარტო ნატო - ს წევრ - ქვეყნებს შორის. არამედ ასევე პარტნიორ ქვეყნებთან. ალიანსი ასევე ახორციელებს მხარდამჭერ პროგრამებს მიმართულს წევრი და პარტნიორი ქვეყნების კიბერუსაფრთხოების ეროვნული პოლიტიკის განვითარებისა და კიბერ - საფრთხეებზე ექსტრემალური რეაგირების ჯგუფის შექმნისკენ.

კრიტიკული ინფრასტრუქტურის დაცვა არის ალიანსის ძირითადი მიმართულება ასევე სამოქალაქო თავდაცვის დაგეგმვის სფეროში. ამ სფეროში ღონისძიებების გატარების აუცილებლობაზე ნატო - ს ფარგლებში არაერთი დოკუმენტია მიღებული, სადაც ასახულია სამოქალაქო თავდაცვის დაგეგმვის პრინციპები, რომლებიც შემუშავდა წევრი ქვეყნების შესაბამისი უწყებებისთვის. გარდა ამისა, გეგმის ახალ რედაქციაში კიბერ - საფრთხეების ჭრილში, მოცემულია სამოქალაქო თავდაცვის საგანგებო სიტუაციების ისეთი მიმართულებები როგორიცაა ქიმიური, ბიოლოგიური და ატომური იარაღის გამოყენების წინააღმდეგ. ნატო - ს სამოქალაქო თავდაცვის

[63] The Cyber Defense Management Authority (CDMA): The Authority was called upon to initiate and coordinate response to cyber attacks against allied member states, and NATO itself. CDMA was Created and was operational in mid-2008. It was a big step in NATO Cyber Defense because it helps member states improve their own cyber security. Rapid-Reaction Teams (RRT's) are also being created and will be available to member states in order to help them counter cyber attacks and will be available for immediate deployment http://csis.org/blog/nato-and-cyber-defensebrief-overview-and-recent-events

დაგეგმვის მთავარი კომიტეტი და მისი რვა განყოფილება და კომიტეტი აგრძელებს კრიტიკული ინფრასტრუქტურის დაცვის ფუნქციონალური ასპექტების შესწავლას. ამის შედეგად, მუშავდება შესაბამისი რეკომენდაციები დაგეგმვის ყველა სახეობის მიმართულებით, რასაც ახორციელებს სათანადო განყოფილებები და კომიტეტები.

გაერომ 80 - იანი წლების ბოლოს დაიწყო კრიტიკული ინფორმაციული ინფრასტრუქტურის საკითხების განხილვა, თუმცა ფორმალური ზომების დანერგვა დაიწყო მხოლოდ ბოლო პერიოდში. ორგანიზაციის მიერ მის ფარგლებში მიღებულია მთელი რიგი ინიციატივები მიმართული კოორდინირებული მოქმედების გასაუმჯობესებლად. კერძოდ, ეს არის რამოდენიმე რეზოლუცია, მსოფლიო სამიტები ინფორმაციული საზოგადოების საკითხებზე (WSIS), გაეროს ზოგიერთი სტრუქტურის პროექტები.

გლობალურ ციფრულ სივრცეში საერთაშორისო ინფორმაციული უსაფრთხოების გაძლიერების მიზნით, გაეროს განიარაღების კვლევითმა ინსტიტუტმა (UNIDIR) ჩაატარა მთელი რიგი სემინარები. თავის მხრივ, გაეროს ნარკომანიასთან და დანაშაულთან ბრძოლის სამმართველო სისტემატურად ატარებს სწავლებებს, რომლის მიზანია შეთანხმებული და კოორდინირებული მიდგომა კიბერდანაშაულის პრობლემებთან.

სერიოზული და მნიშვნელოვანი მოვლენა იყო, 2001 წელს გაეროს ეკონომიკური და სოციალური საბჭოს თხოვნის საფუძველზე ინფორმაციული და საკომუნიკაციო ტექნოლოგიების საკითხებზე გაეროს მიზნობრივი ჯგუფის შექმნა. ამ ჯგუფმა მიიღო უფლებამოსილება გაუწიოს საერთაშორისო საზოგადოების ძალისხმევას მობილიზება დეკლარაციის „ათასწლეულის განვითარების მიზნებზე“ იმ ნაწილს რეალიზაცია, რომელიც ეხება ინფორმაციული და საკომუნიკაციო ტექნოლოგიების განვითარებას. 2004 წლის აპრილში ნატო - ს შტაბ - ბინაში, სამიზნე ჯგუფის მიერ ორგანიზებული იყო სემინარი თემაზე „ინფორმაციული უსაფრთხოების სფეროში უსაფრთხოების საკითხები და პოლიტიკა“. 2005 წელს სამიზნე ჯგუფმა გამოაქვეყნა პრაქტიკული

სახელმძღვანელო თემაზე „ინფორმაციის დაუცველობა - კიბერსაფრთხეებისა და კიბერუსაფრთხოების „გამოუკვლევი ტერიტორიების“ ათვისების გაკვეთილები“. მოცემულ პრაქტიკულ სახელმძღვანელოში ნაჩვენებია ისეთი ახალი და სერიოზული საერთაშორისო კიბერსაფრთხეები, როგორებიც არის კიბერჰულიგნობა, კიბერტერორიზმი, კიბერომი და კიბერდანაშაული.

ინფორმაციული საზოგადოების საკითხებზე გაეროს მსოფლიო სამიტის მსვლელობისას მონაწილე ქვეყნების ლიდერებმა დაავალეს ელექტროკავშირების საერთაშორისო გაერთიანებას კიბერუსაფრთხოების სფეროში კოორდინაცია გაუწიოს საერთაშორისო მოქმედებებს. თავის მხრივ, 2007 წლის მაისში ელექტროკავშირების საერთაშორისო გაერთიანების ინიციატივით შეიქმნა კიბერუსაფრთხოების გლობალური პროგრამა (GCA), რომელმაც უნდა გამოიმუშავოს გაზრდილი კიბერსაფრთხეების წინააღმდეგ მიმართული ღონისძიებების, პრინციპებისა და მექანიზმების კოორდინირებული მოქმედების საერთო კომპლექსი. პროგრამის რეალიზების მიზნით შეიქმნა უმაღლესი დონის ექსპერტთა ჯგუფი, სადაც შედიან კიბერუსაფრთხოების სფეროში მსოფლიოში აღიარებული ასამდე სპეციალისტი, რომლებიც წარმოადგენენ კვლევით ინსტიტუტებსა და სამეცნიერო წრეებს, სახელმწიფო და კერძო სექტორს, სამრეწველო საზოგადოებებს, საერთაშორისო ორგანიზაციებს. 2007 და 2008 წლების განმავლობაში, ელექტროკავშირების საერთაშორისო გაერთიანების მიერ ჩატარდა დიდი სამუშაოები უსაფრთხოების არქიტექტურის სტანდარტიზაციაზე, კავშირის არხების კოდირების მეთოდოლოგიის შემუსავებაზე, ინფორმაციული სისტემების უსაფრთხოების მართვასა და ქსელების მომხმარებლის ავტორიზაციაზე. გარდა ამისა, მომზადდა ინფორმაციული და საკომუნიკაციო ტექნოლოგიების უსაფრთხოების სტანდარტების „გზამკვლევი“, რომელიც წარმოადგენს მონაცემთა ელექტრონულ ბაზას, რომელიც შეიცავს ინფორმაციული და საკომუნიკაციო ტექნოლოგიების უსაფრთხოების უკვე არსებულ

სტანდარტებს, ასევე საერთაშორისო ნორმებსა და სტანდარტებზე მომუშავე ძირითადი ორგანიზაციების პროექტების ჩამონათვალს.

კომპიუტერული დანაშაულებები და ელექტრონულ ქსელებში არასანქცირებული შეღწევა დიდ ზიანს აყენებს ფინანსურ სექტორს. იმის გათვალისწინებით, რომ სულ უფრო იზრდება ფინანსური ინფორმაციის შენახვისა და გადაცემის მოცულობა, კომპიუტერული დამნაშავეებისთვის ასევე ადვილი ხდება ქსელებში არასანქცირებული შეღწევა და თავიანთი მავნებლური ქმედებების განხორციელება. ამიტომ მსოფლიო ბანკის ჯგუფმა ბოლო პერიოდში განახორციელა მთელი რიგი ღონისძიებები მიმართული ინფორმაციული უსაფრთხოების უზრუნველსაყოფად, განსაკუთრებით ეს ეხება განვითარებად ქვეყნებს.

გლობალური ინფორმაციული - საკომუნიკაციო ტექნოლოგიების დეპარტამენტი38 უწევს დახმარებას განვითარებად ქვეყნებს ინფომაციული და საკომუნიკაციო ტექნოლოგიების განვითარებაში, ასევე უზრუნველყოფას მსოფლიო ბანკის ჯგუფის ძირითადი დეპარტამენტების საქმიანობას, რომელიც ეხება ინფორმაციული - საკომუნიკაციო ტექნოლოგიების სფეროში კვლევების ჩატარებას, პოლიტიკის განსაზღვრას, ინვესტიციებსა და სხვადასხვა პროგრამების განხორციელებას.

2003 წელს გამოიცა „კომპიუტერული უსაფრთხოების ცნობარი“,[64] სადაც განხილულია მოწინავე გამოცდილება და რეკომენდაციები ინფორმაციული უსაფრთხოების უზრუნველყოფაში, რომელიც გამოადგება ყველა ქვეყანას, მიუხედავად მათი ტექნიკური შესაძლებლობების დონისა. ეს რეკომენდიციები მოცემულია შესაბამის ვებ - გვერდზე და ახალი ტექნოლოგიებისა და მეთოდიკის გამოჩენასთან ერთად, მუდმივად ხდება მისი განახლება.

2004 წლის იანვარსა და მაისში გამოვიდა შემდეგი პუბლიკაცია სახელწოდებით „ტექნოლოგიური რისკების საკონტროლო სია“ [65], სადაც მოცემულია ელექტრონული უსაფრთხოების ოცდაათამდე დონის აღწერა, ასევე განხილულია ის რისკები,

[64] Information Technology Security Handbook

[65] Technology Risk Checklist http://archive.rdec.gov.tw/public/Data/851413535571.pdf

რომლებიც უკავშირდება ქსელების ინფრასტრუქტურის პროგრამულ უზრუნველყოფას. ყოველი მოცემული დონისთვის გათვალისწინებულია რისკების მართვის, კიბერდაზვერვისა და ინტელექტუალური ცენტრალიზებული მართვის ღონისძიებები; დაშვებისა და ავტორიზაციის კონტროლი; ქსელთაშორისი დაცვა და კონტენტის ფილტრაცია; შეღწევის აღმოჩენისა და ანტივირუსული სისტემები; კოდირების საშუალებები და მოწყვლადობის ტესტირება; სისტემური ადმინისტრირების ღონისძიებები; შეღწევის შემთხვევაში ექსტრემალური ღონისძიებების გეგმები. 2005 წელს გამოვიდა კიდევ ორი დოკუმენტი42 დაკავშირებული ელექტრონული გადახდების სისტემების უსაფრთხოებასთან, სადაც განხილულია საფრთხეები, რომლებიც მოდის ბოტ - ქსელებისგან, აგრეთვე კიბერსივრცეში ფულის გათეთრების პრობლემები.

2007 წელს ინსტიტუტის „აღმოსავლეთი - დასავლეთი“ ამერიკულმა ჯგუფმა „სტრატეგიული დიალოგები“, გენერალ ჯეიმს ჯონსონის [66] ხელმძღვანელობით, კიბერუსაფრთხოების სფეროში საერთაშორისო თანამშრომლობის თაობაზე ჩაატარა შეხვედრების სერია ჩინეთისა და რუსეთის ხელმძღვანელ პირებთან. ეს შეხვედრები გაგრძელდა კიდევ უფრო მაღალ დონეზე, რომლის დროს გამართულმა დისკუსიებმა გამოავლინა შეერთებული შტატების, ჩინეთისა და რუსეთის საერთო აღშფოთება არასახელმწიფო სუბიექტების სწრაფად მზარდი შესაძლებლობები, რომლებსაც შესწევთ უნარი დიდი ზიანი მიაყენოს მსოფლიო ეკონომიკას და საფრთხის ქვეშ დააყენოს როგორც თითოეული ქვეყნის ეროვნული უსაფრთხოება ისე დიდი საფრთხე შეუქმნას საერთაშორისო და რეგიონალურ უსაფრთხოებას. შეხვედრების შედეგად, თითოეულმა ქვეყანამ გადახედა კიბერუსაფრთხოების საკითხების შეფასებას, ხოლო შეერთებულმა შტატებმა კიბერსაფრთხეებს მისცა ატომური საფრთხის ტოლფასი შეფასება.

[66] ევროპაში ნატო - ს გაერთიანებული შეიარაღებული ძალების ყოფილი უმაღლესი მთავარსადრდალი, ამჟამად შეერთებული შტატების ეროვნული უსაფრთხოების მრჩეველი

გლობალური კიბერუსაფრთხოების ინიციატივის საკონსულტაციო ჯგუფს სათავეში ჩაუდგა “Deloitte” კიბერინოვაციების ცენტრის დირექტორი გენერალი ჰარრი რეიდუუედჯი. ეს ჯგუფი სთავაზობს პრობლემის გადაჭრას შემდეგ ორ დონეზე: (1) სანდოობის ამაღლება კიბერუსაფრთხოების კონკრეტული პრობლემის ერთობლივი თანამშრომლობისა და გადაწტვეტილების მიღების გზით, სადაც ჩართული არიან ორი ან ორზე მეტი ქვეყნის ექსპერტთა ჯგუფები; და (2) საზოგადოებრივი პროცესის ინიცირება, რომელიც საშუალებას იძლევა გადაიდგას პირველი ნაბიჯები კიბერსივრცეში საერთაშორისო უსაფრთხოების პოლიტიკის რეალიზების მიმართულებით, როგორც ეს უკვე არსებობს საზღვაო, საჰაერო და კოსმოსური სივრცისთვის. მეორე მიმართულებით საქმიანობა, ინსტიტუტის „აღმოსავლეთ - დასავლეთი“ ეგიდით, დაიწყო 2010 წლის მაისში, როცა კიბერუსაფრთხოების საკითხების მსოფლიო პირველი სამიტის ფარგლებში „კიბერ - 40“45 - ის 200 - მდე ლიდერი შეიკრიბა დალასში (აშშ). ეს სამიტი გახდა უმაღლეს დონეზე სახელმწიფოსა და კერძო სექტორს შორის საპარტნიორო მოძრაობის შექმნის პირველი მცდელობა, რომელიც ეძღვნება კრიტიკული ინფრასტრუქტურის კიბერდაცვის საკითხებს.

თავი 2..4 საქართველოში არსებული კიბერ გამოწვევები

კიბერდანაშაული 21-ე საუკუნეში ერთ-ერთი მთავარი გამოწვევაა საზოგადოებისთვის და ეკონომიკური დანაკარგები სულ უფრო გაიზრდება, რაც სხვა მხრივ ხელს შეუწყობს სახელმწიფოსა და კერძო სექტორს შორის თანამშრომლობის განვითარებას[67]. კიბერ შესაძლებლობების კონცეფციას გავლენა ექნება საერთაშორისო პოლიტიკაზე და ძალაუფლებისთვის გლობალურ ბრძოლაზე, რაც ასევე შეუწყობს ხელს კიბერ სივრცეში გამალებული შეიარაღების პროცესის გაზრდის ტენდენციას. სავსებით

[67] ლ. პატარაია, კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, თბ., 2012, გვ 49

შესაძლებელია, რომ ახლო მომავალში მოხდება გლობალური კიბერ კატასტროფა, რაც მთლიანად შეცვლის ჩვენს მიდგომას არამარტო კიბერუსაფრთხოების, არამედ მთლიანად კიბერსივრცეში.

საერთაშორისო თანამშრომლობის მიმართ. კიბერის ახალ ეპოქაში გამარჯვებული იქნება ის, ვინც შეძლებს საბაზრო ეკონომიკის გათვალისწინებით უსაფრთხოების საკითხების კომპლექსურ გადაწყვეტას; გააჩნიათ საუკეთესო ტალანტების მობილიზების შესაძლებლობა; და შესწევთ ადაპტაციის უნარი და ყოველგვარი ძალისხმევის გარეშე იმუშაონ მრავალეროვან გარემოში. ფაქტიურად, კიბერუსაფრთხოება გახდა საგარეო პოლიტიკის შემადგენელი ნაწილი და ის სულ უფრო აქტიურ როლს თამაშობს საერთაშორისო ურთიერთობების საკითხში. საინტერესოა ამ მხრივ რა მდგომარეობაა საქართველოში.[68]

2008 წლის აგვისტოს ომის შემდეგ, როცა რუსეთის მხრიდან მოხდა მასირებული კიბერ შეტევა ქვეყნის ინფრასტრუქტურაზე, სამთავრობო ვებგვერდებზე. ქვეყანა დადგა სერიოზული პრობლემის წინაშე, იყო საფრთხე, რომ საქართველო მოქცეულიყო ინფორმაციულ ვაკუუმში. მიღებული ცუდი გამოცდილების გათვალისწინებით, ხელისუფლებამ დაიწყო კიბერუსაფრთხოების სფეროს განვითარებაზე ფიქრი. კერძოდ, იუსტიციის სამინისტროში შეიქმნა სსიპ - მონაცემთა დაცვის სააგენტო, განისაზღვრა კრიტიკული ინფორმაციული ინფრასტრუქტურის სუბიექტები, რომელთა დაცვა დაევალა მონაცემთა გაცვლის სააგენტოს, შეიქმნა კანონი „ინფორმაციული უსაფრთხოების შესახებ“ და „კიბერუსაფრთხოების სტრატეგია“, ასევე თავდაცვის სამინისტროში ახალი შექმნილია სსიპ - კიბერუსაფრთხოების ბიურო, რომელიც პასუხისმგებელია თავდაცვის სფეროში კიბერუსაფრთხოებითი ღონისძიებების გატარებაზე. ასევე შინაგან საქმეთა სამინისტროს ცენტრალური კრიმინალური პოლიციის დეპარტამენტში არსებობს კიბერდანაშაულთან ბრძოლის სამმართველო, და ბოლოს რაც ასევე მნიშვნელოვანია შეიქმნა კიბერუსაფრთხოების სფეროში

[68] კაცმანი ა., კომპიუტერული დანაშაული, ავტორეფერატი იურიდიულ მეცნიერებათა კანდიდატის სამეცნიერო ხარისხის მოსაპოვებლად, თბ., 2004, გვ 77-81

სახელმწიფო პოლიტიკის განმსაზღვრელი მთავარი დოკუმენტი – საქართველოს კიბერუსაფრთხოების 2013-2015 წლების სტრატეგია. აქვე შეიძლება ავღნიშნოთ ორგანიზაცია „გრენას“ დადებითი როლი და საქმიანობა ამ მიმართულებით[69].

ასევე კიბერდანშაულთან ბრძოლისთვის დიდი მნიშვნელობა აქვს საზოგადობის ცნობიერების ამაღლებას, რაც ჩვენთან ფაქტიურად არ ხორციელდება. საზოგადოების ცნობადობის ამაღლება და დარგის აკადემიურ დონეზე განვითარება, რაც ასევე გულისხმობს სამეცნიერო-კვლევითი და ანალიტიკური საქმიანობის წარმოებას, გაცილებით ამცირებს კიბერსივრციდან მომდინარე საფრთხეებს. აქვე ცალკე გამოვყოფდი საჭირო პროფესიული კადრებისა და სპეციალისტების არარსებობას. მაგალითად, ქვეყანას არ ჰყავს კიბერ-ანალიტიკოსები, არ არის კიბერ სამართლის დარგის სპეციალისტები, არ გვყავს კრიპტოგრაფები, რაც კიბერ თავდაცვითი საქმიანობის განვითარებისთვის აუცილებელ პირობას წარმოადგენს[70]

დასავლეთის პრესა და ექსპერტები სულ უფრო ხშირად წერენ, რომ რუსეთი "ჰიბრიდული ომების" შემადგენელი ელემენტების გამოყენებას, უკრაინის შემდეგ იწყებს ბალტიისპირეთის ქვეყნებისა და პოლონეთის წინააღმდეგ. აქ საუბარია მიზანმიმართულ კიბერ შეტევებსა და "საინფორმაციო ომზე". არ უნდა გამოვრიცხოთ ასევე ახლო მომავალში მსგავსი ქმედებები საქართველოს წინააღმდეგ, თუმცა მანამდე ჩვენი ქვეყნის მიმართ განხორციელდა სხვა კიბერ შეტევები. [71] მაგალითისთვის, ამერიკული ავტორიტეტული ორგანიზაცია "FireEye"-ს კვლევისა და ანალიზის მიხედვით, 2008 – 2014 წლებში რუსეთის მხრიდან მუდმივად ხორციელდებოდა კიბერ შეტევები, რომელთა ობიექტები იყო საქართველოს საგარეო და შინაგან საქმეთა და თავდაცვის სამინისტროები, ასევე სხვადასხვა საინფორმაციო სააგენტოები. კიბერ

[69] მშვიდობაძე ხ., გლობალური მნიშვნელობის კიბერდომეინი და ახალი გამოწვევები, ექსპერტის აზრი, №11, 2013, გვ 26;

[70] http://www.oecd.org/sti/whatistheoecdworkingpartyoninformationsecurityandprivacywpisp.htm

[71] პატარაია ლ., კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, თბ., 2012, გვ 49;

შეტევების. ხასიათი იყო ჯაშუშური და მიზნად ისახავდა დასავლურ ინსტიტუტებთან დაკავშირებით ქვეყნის მიზნებისა და ამოცანების შესახებ ინფორმაციის მოპარვას.

კიბერუსაფრთხოების ელემენტების განხილვა უნდა მოხდეს ეროვნული უსაფრთხოების დონეზე, მიმდინარე და ახალი საფრთხეები აუცილებლად გათვალისწინებული და ასახული უნდა იყოს ეროვნული უსაფრთხოების კონცეფციაში.[72]

თავი 2.4.1 ფარული მოსმენების რეგულირების საკანონმდებლო გამოწვევები საქართველოში

სახელმწიფოს როგორც ქვეყნის უშიშროების და უსაფრთხოების დაცვის გარანტს ექსკლუზიური უფლებამოსილება აქვს რომ განახორციელოს ფარული მიყურადება აღნიშნული მიზნების მისახწევად ის იყენებს სხვადასხვა ტექნიკურ საშვალებეს. მნიშვნელოვანია რომ სახლმწიფოს ქონდეს აღნიშნული მიზნის მისახწევად მკაფიოდ ჩამოყალიბებული წესები რომ არ მოხდეს ადამინის კოსტიტუციით გარანტირებული პირადი ცხოვრების ხელყოფა, აუცლებელია რომ სახლმწიფომ დაიცვას ზღვარი საჯარო ინტერესა და კერძო ინტერეს შორის რომელიც გაჩნია მოქალაქეს.

აღნიშნული ზღვარის დასაცავად მკაფიოდ უნდა იყოს ჩამოყალიბებული ლეგიტმური მიზანი რომ აღნიშნული ბალანსი არ დაირღვეს, ასევე მნიშვნელოვანია რომ სახელმწიფოს არ გაჩნდეს განუსაზღვრელი ბერკეტი მოქალაქეების პირადი ცხოვრებაში ჩარევის განსახორციელებლად, წინაღმდეგ შემთხვევაში არსებობს ალბათობა იმისა რომ მოხდება სახელმწიფოს მხირდან არალეგიტმური ჩარევა,რაც თავის მხრივ დანაშაულია და ითვალისწინებს სისხლის სამართლებრვი პასუხისმგებლობას. ზემოაღნიშნულიადნ გამომდიანრე, თუ სახელმწიფო

[72] კაცმანი ა., კომპიუტერული დანაშაული, ავტორეფერატი იურიდიულ მეცნიერებათა კანდიდატის სამეცნიერო ხარისხის მოსაპოვებლად, თბ., 2004, გვ 77-81;

არალეგიტიმურად ჩაერევა მოქალქის პირად ცხოვრებაში შეიძლება ითქვას რომ, სახელმწიფო ხდება კიბერ დანაშაულის ჩამდენი რომელიც გათვალისწინებულია საქართველოს სისხლის სამართლის კოდექსით.[73]

2014 წლის 14 აპრილს საქართველოს საკონსტიტუციო სასამართლომ დააკმაყოფილა არასამთავრობო ორგანიზაციების გაერთიანებული სარჩელი პარლამენტის წინააღმდეგ.

კონსტიტუციური სარჩელებით სადავოდ იყო გამხდარი საკანონმდებლო ნორმები, რომლებიც ფარული საგამოძიებო მოქმედებების განხორციელებაზე უფლებამოსილ ორგანოს (სახელმწიფო უსაფრთხოების სამსახურს) ანიჭებდა უფლებამოსილებას, ჰქონოდა კავშირგაბმულობის და კომუნიკაციის ფიზიკური ხაზებიდან ინფორმაციის რეალურ დროში მოპოვების და ამ მიზნით სათანადო აპარატურის და პროგრამული უზრუნველყოფის საშუალებების განთავსების შესაძლებლობა. ამავე დროს, სახელმწიფო უსაფრთხოების სამსახური აღჭურვილი იყო უფლებამოსილებით, განეხორციელებინა კავშირგაბმულობის არხში არსებული მაიდენტიფიცირებელი მონაცემების კოპირება და მათი 2 წლის ვადით შენახვა.

საკონსტიტუციო სასამართლომ მიიჩნია, რომ სადავო ნორმები, მართალია, ემსახურება ლეგიტიმურ მიზნებს, მაგრამ არ წარმოადგენს ამ მიზნების მიღწევის ნაკლებად მზღუდავ, პროპორციულ საშუალებას. სადავო ნორმები შესაძლებლობას აძლევს სახელმწიფო უსაფრთხოების სამსახურს, თანამედროვე ტექნოლოგიების გამოყენებით, მოიპოვოს პირადი ხასიათის ინფორმაცია განუსაზღვრელ პირთა წრის შესახებ. მართალია, არსებობს პრეზუმფცია, რომ შესაბამისი უფლებამოსილების მქონე ორგანო ბოროტად არ ისარგებლებს ამ ტექნიკური საშუალებებით, თუმცა რეალურ დროში პირადი ხასიათის ინფორმაციის მოპოვების ტექნიკური შესაძლებლობის (მათ შორის პროგრამული უზრუნველყოფის) ფლობა, ადმინისტრირება და ამ საშუალებების გამოყენებით პირადი ხასიათის ინფორმაციაზე პირდაპირი წვდომის შესაძლებლობა,

[73] სისხლის სამართლის კოდექსი,1999წ

ასევე მაიდენტიფიცირებელი მონაცემების (მეტადატის) კოპირება და შენახვა ისეთი უწყების მიერ, რომელსაც მინიჭებული აქვს გამოძიების ფუნქცია ან არის პროფესიულად დაინტერესებული ამ ინფორმაციის გაცნობით, ქმნის პირად ცხოვრებაში ჩარევის მომეტებულ საფრთხეს.

საკონსტიტუციო სასამართლომ არაკონსტიტუციურად ცნო სახელმწიფო უსაფრთხოების სამსახურის მიერ სატელეფონო მოსმენების განსახორციელებლად ორეტაპიანი ელექტრტონული სისტემის ფლობის, განთავსებისა და მისი უშუალოდ გამოყენების გზით ინფორმაციის რეალურ დროში მოპოვების შესაძლებლობა, ასევე კავშირგაბმულობის ხაზებიდან და მათი შემაერთებლებიდან, მეილსერვერებიდან, ბაზებიდან, კავშირგაბმულობის ქსელებიდან და კავშირგაბმულობის სხვა შემაერთებლებიდან ინფორმაციის რეალურ დროში მოსაპოვებლად სხვა ტექნიკური საშუალებების გამოყენება. საკონსტიტუციო სასამართლომ მიიჩნია, რომ სადავო ნორმის არაკონსტიტუციურობას განაპირობებს შემდეგი გარემოებები: სახელმწიფო უსაფრთხოების სამსახური ფლობს ფარული მოსმენების განსახორციელებლად და ინტერნეტურთიერთობის მონიტორინგის საჭირო ტექნიკურ საშუალებებს, რომლებიც რეალურ დროში პირადი ხასიათის ინფორმაციის მოპოვების „მასიურ“ (პრაქტიკულად შეუზღუდავ) შესაძლებლობას იძლევა. ეს შესაძლებლობა მხოლოდ უსაფრთხოების სამსახურის ამჟამადხელთ არსებული ტექნიკური საშუალებების სიმძლავრით არის შეზღუდული, ამასთან, სახელმწიფო უსაფრთხოების სამსახური უზრუნველყოფს ამ სისტემის ადმინისტრირებას, ფლობს და კომუნიკაციის წყაროებთან განათავსებს ტექნიკურ საშუალებებს. ამ პირობებში პერსონალურ მონაცემთა ინსპექტორისთვის მინიჭებული უფლებამოსილება, გასცეს თანხმობა „ობიექტის აქტივაციაზე“ (მოსმენებზე) და განახორციელოს აღნიშნული სისტემის შემოწმება, მართალია, ემსახურება პირად ცხოვრებაში გაუმართლებელი ჩარევის საფრთხის შემცირებას, მაგრამ მოცემულ შემთხვევაში, ვერ ჩაითვლება ამ პროცესზე გარე კონტროლის საკმარის და ეფექტურ შესაძლებლობად. მით უფრო, რომ მომეტებულია პირად ცხოვრებაში

გაუმართლებელი ჩარევის რისკი ინფორმაციის ფარულად ისეთი ტექნიკური საშულებებით მოპოვების შემთხვევებში, რომლებიც არ ითვალისწინებენ ზედამხედველობის (კონტროლის) ეფექტიან მექანიზმებს.[74]

თავი 2.4.1.1 უკანონო ფარული მიყურადების სასამართლო პრაქტიკა

2017 წლის იანვრიდან ივლისამდე ფარული მიყურადების შემთხვევებთან დაკავშირებით მოვლენები შემდეგნაირად განვითარდა:

საქართველოს მთავარი პროკურორის ყოფილი მოადგილის დავით საყვარელიძის [75] განცხადებით, ბიძინა ივანიშვილის პრემიერობის დროს მოქმედი მთავარი პროკურორის მოადგილე ლაშა ნაცვლიშვილი მას სთავაზობდა ბიძინა ივანიშვილის სატელეფონო ფარული ჩანაწერების ამსახველი აუდიომასალის ყიდვას რამდენიმე მილიონის სანაცვლოდ. ეს ინფორმაცია დაადასტურა რუსთავი 2-ის გენერალურმა დირექტორმა ნიკა გვარამიამ.

2017 წლის 20 აპრილს, თბილისის სააპელაციო სასამართლომ ძალაში დატოვა შსს-ს მინისტრის ყოფილი მოადგილის შოთა ხიზანიშვილის, კონსტიტუციური უსაფრთხოების დეპარტამენტის ყოფილი უფროსის ლევან ქარდავასა და ამავე უწყების დეპარტამენტის უფროსის ყოფილი უფროსის ლევან ქარდავასა და ამავე უწყების დეპარტამენტის უფროსის ყოფილი მოადგილის ვასილ ლელუაშვილის განაჩენი, თანამდებობრივი უფლებამოსილების გადამეტების შესახებ.

სააპელაციო სასამართლოს გადაწყვეტილებით, 2009 წელს, ვასილ ლელუაშვილის დავალებით, კონსტიტუციური უსაფრთხოების დეპარტამენტმა უკანონოდ შექმნა ისეთი კომპიუტერული პროგრამა, რომლის დახმარებითაც, შესაძლებელი იქნებოდა

[74] საქართველოს საკოსტიტუციო სასამართლოს გადაწყვეტილება, №1/1/625, 640

[75] ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, ფარული რეგულირების მიყურადება საქართველოში, გვ 14

ნებისმიერ კომპიუტერულ სისტემაში შეღწევა, მათ შორის კომპიუტერთან ახლოს გამართული საუბრების უკანონო მიყურადება ჩაწერა. აღნიშნული პროგრამა შეიქმნა 2011 წელს და გამოიყენებოდა პირადი ინფორმაციის უკანონოდ მოსაპოვებლად.

2017 წლის 3 ივლისს პირადი ცხოვრების ამსახველი ფარული კადრების მოპოვება-შენახვაში ბრალდებული კუდ-ისა და პოლიციის ყოფილი მაღალჩინოსნები სასამართლომ დამნაშავედ ცნო. საქმეზე ბრალდებული 6 პირიდან ერთი გამართლდა მასზე არასაკმარისი მტკიცებულებების არსებობის გამო, დანარჩენებს კი თავისუფლების აღკვეთა შეეფარდათ. თუმცა, ბრალდებული ხუთი პიროვნებიდან ორი ამჟამად მიმალვაშია.

თავი 2.5 კიბერტერორიზმი

2.5.1. კიბერტერორიზმის სისხლისსამართლებრივი დაასიათება

მრავალი რევოლუციური ტექნოლოგიის მსგავსად, კომპიუტერული ტექნოლოგიები თავის თავსში უზარმაზარ პოტენციალს ატარებენ როგორც პროგრესისთვის, ისე ბოროტად გამოყენებისთვის - ქსელური ინფორმაციის ხელყოფა, კომპიუტერული მეკობრეობა, ელექტრონული ჯაშუშობა, პორნოგრაფიის გავრცელება და სხვ“. [76] „საბრძოლო იარაღმა დროთა განმავლობაში უდიდესი ევოლუცია განიცადა. სატევარი, შუბისპირი, მშვილდი, ისარი, ხმალი, ფარი, მუზარადი, ზარბაზანი... მერე ტანკი, ავტომატი, ტყვიამფრქვევი და ბირთვული იარაღიც. გაუმჯობესდა იმდენად, რომ კომპიუტერის კლავიატურითაც შესაძლებელი გახდა არანაკლები ზიანის მიყენება მოწინააღმდეგისათვის. გაჩნდა ახალი ტერმინები, როგორიცაა: კიბერტერორიზმი, კიბერ ომი, კიბერ თავდასხმა“. [77] „ტერორიზმის გარშემო ერთგვარი აზრთა

[76] ავტორთა კოლექტივი, სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეხუთე გამოცემა, გამომც. „მერიდიანი“, 2017, გვ 281

[77] ჩიხლაძე კ., კიბერტერორიზმი (ინფორმაციული ესე), ინფორმაციული ტექნოლოგიები, ყოველკვარტალური სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი“ №3 , 2012, გვ122;

სხვადასხვაობა არის, რის გამოც რთულია იგი კონკრეტული დეფინიციით განვსაზღვროთ. თავად ტერორისტებზე ამგვარი გამონათქვამიც კი არსებობს: „ერთისთვის ტერორისტი, სხვისთვის თავისუფლებისათვის მებრძოლია.“ ეს სიტყვები ჟერარდ სეიმურმა 1975 წელს, თავის წიგნში „ჰარის თამაშში“ მოიხსენია.

მერიკის შეერთებული შტატების მთავრობის დეპარტამენტის პოზიცია ტერორიზმის შესახებ შემდეგნაირად არის ჩამოყალიბებული: “წინასწარ დაგეგმილი, პოლიტიკურად მოტივირებული სისასტიკე, ჩადენილი სამოქალაქო სამიზნეებზე, ქვენაციონალური ჯგუფის ან საიდუმლო აგენტების მიერ, რომელიც საზოგადოების დაშინებას ემსახურება.[78]

ყოველდღიურად ხდება კიბერდანაშაული ინდივიდების, სხვადასხვა ბიზნესისა თუ მთავრობის წინააღმდეგ. კიბერომი უკვე წარმოადგენს საფრთხეს, რომლის წინააღმდეგაც ეროვნული უსაფრთხოების ექსპერტები ეძიებენ უფრო ეფექტურ, თანმიმდევრულ სტარტეგიებსა და საერთაშორისო შეთანხმებებს.[79]

კიბერთავდასხმები შესაძლოა იყოს სპეცოპერაციებისა და საჰაერო თავდასხმების ეკვივალენტური. სპეციალური დანიშნულების რაზმების ან საჰაერო ძალების გაწვრთნისა და აღჭურვისათვის საჭირო ფინანსურ და ადამიანურ რესურსებთან შედარებით ჰაკერები, კომპიუტერები და ბოტნეტები თუ სხვა სახის კიბერ და ინფორმაციული იარაღის შექმნა გაცილებით მცირე დროსა და სახსრებს მოითხოვს. ამან შესაძლოა საფრთხე შეუქმნას ქვეყნის კრიტიკულ ინფრასტრუქტურას, ეკონომიკას და მოსახლეობის ფსიქოლოგიურ მდგომარეობას.[80]

ფაქტობრივად, ტერორისტულ ორგანიზაციებმა უახლოესი კომპიუტერული ტექნოლოგიები ტერორისტულმა აქტის ჩდენის საშუალებად აქციეს და ამით აღნიშნული დანაშაული უფრო საშიშ მოვლენად ექცა მსოფლიოს. კიბერტერორიზმი

[78] პატარაია ლ., კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, 2012, 45

[79] http://www.chebucto.ns.ca/Current/HalifaxSummitG7/

[80] Report from the Commission to the Council, Brussels, 17.07.2008. com (2008) 448 (Based on article 12 of the Council Framework Decision of 24.02.2005 on attaks against information systems);

არის თანამედროვე ეპოქის სწრაფი ტექნოლოგიური განვითარებისა და წინსვლის შედეგი. მოგეხსენებათ, ტექნოლოგიის განვითარებას ყოველთვის თან ახლავს ჰაკერების დიდი ინტერესი, მოახდინონ ჰაკერული ცოდნის დემონსტრირება ანუ კიბერტერორის განხორციელება. მოქმედების მექანიზმი კი შემდეგშია: დათქმულ დროს, ასეულ ათასობით კომპიუტერიდან ხდება გასატეხი სერვერიდან ინფორმაციის ერთდროული მოთხოვნა. სერვერი ვერ ძლებს და იჭედება.[81]

ეტიმოლოგიურად „კიბერტერორიზმი“ ორი სიტყვისაგან - „კიბერ“ და „ტერორიზმისაგან“ შედგება. წინსართი „კიბერ“ ნიშნავს კიბერნეტიკულ სივრცეს, ვირტუალურ სივრცეს, ანუ კომპიუტერის მეშვეობით, მოდელირებულ სინივთების შესახებ მათემატიკური, სიმბოლური ან ნებისმიერი სხვა სახით და მოძრაობის პროცესშია ლოკალური ან გლობალური კომპიუტერული ქსელითვრცეს, რომელშიც ინახება ინფორმაცია პირების, ფაქტების, მოვლენების, პროცესების, ნივთების შესახებ მათემატიკური, სიმბოლური ან ნებისმიერი სხვა სახით და მოძრაობის პროცესშია ლოკალური ან გლობალური კომპიუტერული ქსელით.[82]

„ტერმინი - „კიბერტერორიზმი“, ინფორმაციული ტექნოლოგიების ლექსიკონში 1997 წელს გაჩნდა, როდესაც ფედერალური გამოძიების ბიუროს აგენტმა მარკ პოლიტმა განსაზღვრა ტერორიზმის აღნიშნული სახეობა როგორც „სამოქალაქო მიზნების მიმართ, წინასწარ განსაზღვრული პოლიტიკურად მოტივირებული შეტევები ინფორმაციულ, კომპიუტერულ სისტემებზე, კომპიუტერულ პროგრამებსა და მონაცემებზე, სუბნაციონალური დაჯგუფებების ან საიდუმლო აგენტების მხრიდან, გამოხატული ძალადობით“.[83]

„ტერმინი „კიბერტერორიზმი“ პირველად 1980 წელს კალიფორნიის უსაფრთხოები სადადაზვერვის ინსტიტუტის მეცნიერ თანამშრომელმა ბარი კოლინმა გამოიყენა

[81] ჩიხლაძე კ., კიბერტერორიზმი (ინფორმაციული ესე), ინფორმაციული ტექნოლოგიები, ყოველკვარტალური სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი“ №3 თბ., 2012, 123

[82] ავტორთა კოლექტივი, სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეხუთე გამოცემა, გამომც. „მერიდიანი“ , 2017, გვ 281

[83] Larry J. Siegel (2008) Criminology- Cyber crime and technology - Cyber terrorism: Cyber Crime With Political Motives . pp № 449

ტერორისტული ორგანიზაციების მიერ კიბერსივრცის აქტიურად გამოყენების აღსანიშნავად. მოგვიანებით,აშშ-ის კიბერტერორიზმის ერთ-ერთი წამყვანი ექსპერტი, ჯორჯთაუნის უნივერსიტეტის პროფესორი დოროთი დენინგი ინტერნეტში საქმიანობის კლასიფიკაციის შემდეგ ასპექტებს გამოყოფს: „აქტივიზმი“ და „კიბერტერორი“. კიბერტერორიზმი წარმოადგენს ტერორიზმისა და კიბერსივრცის შერწყმას. ის მოიცავს პოლიტიკურად მოტივირებულ ჰაკერულ ოპერაციებს,რომელთა მიზანია პოლიტიკური თუ ეკონომიკური ხასიათის დამანგრეველი შედეგების მიღწევა. დენინგის ამგვარი კლასიფიკაცია გამყარებულია „Computer Emergency“ ჯგუფის სტატისტიკური კვლევითი მონაცემებით. ამ მონაცემების მიხედვით, 2001 წელს დაფიქსირებულია ქსელებზე შეტევის 52 685 შემთხვევა, რომელსაც შეეძლო აშშ-ის ინფრასტრუქტურის პარალიზება. ეს ციფრი ორჯერ მეტია 2000 წლის მონაცემებთან შედარებით. მას შემდეგ ინციდენტების რაოდენობა კატასტროფულად მატულობს, საკრედიტო ბარათების სკანირებით დაწყებული და სხვა სახის კომპიუტერული შეტევით დამთავრებული.[84]

სად გადის ზღვარი ჰაკერის მიერ ჩადენილ მარტივ ხულიგნობასა, სამთავრობო დაფინანსების კიბერ ოპერაციებსა და კიბერ ომებს შორის? ეს დღესდღეობით კიბერ სივრცის ერთ-ერთი ყველაზე აქტუალური კითხვაა, რადგან კიბერ შეტევა შეიძლება გახდეს საპასუხო სამხედრო აგრესიის მიზეზი. დღეს ამერიკის შეერთებული შტატების თავდაცვის დეპრატამენტმა უკვე მიიღო ინიციატივა, რომლის მიხედვითაც იგი სახელმწიფოს წინააღმდეგ განხორციელებულ სამთავრობო კიბერ შეტევას, კონვენციური სამხედრო მოქმედებებით უპასუხებს. ასევე გასათვალისწინებელია ჩრდილოატლანტიკური ალიანსის პოტენციალიც, რომელიც მსგავსი სცენარებით ყოველწლიურ სამხედრო სწავლებებსაც მართავს – Nato Cyber Coalition. ამ რეალობაში კიბერ აქტივობები განსაკუთრებულ საფრთხეს ატარებს, რომელმაც შეიძლება კოლოსალური მასშტაბების სამხედრო მოქმედებები გამოიწვიოს. მაგალითად, თუ შეტევა განხორციელდა ალიანსის წევრი სახელმწიფოს მიმართ, მოსალოდნელია რომ

[84] გურეშიძე ს., სტატია, „ტერორიზმი ინტერნეტში“, ახლო აღმოსავლეთი და საქართველო, V, თბ., 2008, 67

გამოყენებულ იქნება ვაშინგტონის შეთანხმების მეხუთე პუნქტი, რომლის მიხედვითაც წევრი სახელმწიფოს მიმართ განხორციელებული შეტევა ითვლება შეტევად ალიანსის წევრ-სახელმწიფოებზე.[85]

აგრეთვე, საყურადღებოა სამომავლო ტერორისტული ოპერაციების დაგეგმვის და [86] მათი განხორციელების მიზნით, ტერორისტული ორგანიზაციების და კიბერდამნაშავეთა დაჯგუფებებს შორის აქტიური თანამშრომლობა. კიბერდამნაშავეებს გააჩნიათ ის ტექნიკური უნარჩვევები და პოტენციური შესაძლებლობები, რაც საჭიროა კიბერსივრცეში ტერორისტული ოპერაციების ჩასატარებლად და კინეტიკურ სფეროში ჩასატარებელი ტერორისტული ოპერაციების ტექნიკური მხარდაჭერისთვის. ამიტომაც, ტერორისტული დაჯგუფებების მხრიდან არსებობს დაინტერესება გამოიყენონ კიბერდამნაშავეები ტერორისტული საქმიანობისთვის. მრავალი ტერორისტული დაჯგუფება თუ ორგანიზაცია დღეს უფრო მეტად ორიენტირებულია კიბერსივრცეში ტერორისტული აქტების განხორციელებისკენ. აღნიშნულს განსაზღვრავს რამდენიმე მნიშვნელოვანი ფაქტორი, მათ შორის: კიბერსივრცეში ჩატარებული ოპერაციების დაბალი ბარიერი, ადამიანური რესურსების ეფექტიანი გამოყენება ოპერაციის ფარულობა. და მობილობა“.

2.5.1.1 კიბერტერორიზმის განსაზღვრება საქართველოს სისხლის სამართლის კოდექსით

[85] პატარაია ლ., კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, გამომცემლობა ,,სანი“, თბ., 2012, 46;

[86] ნაკაშიძე გ., სტატია, „კიბერტერორიზმი - XXI საუკუნის მწვავე გამოწვევა“, ჟურნალი ეკონომიკა და ბიზნესი, №4 ივლისი-აგვისტო, 2012, 172

საქართველოს კანონდებლობით კიბერტერორიზმი განმარტებულია, როგორც კანონით დაცული კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლება, მისი გამოყენება ან გამოყენების მუქარა, რაც ქმნის მძიმე შედეგის საშიშროებას, ჩადენილი მოსახლეობის დაშინების ან ხელისუფლების ორგანოებზე ზემოქმედების მიზნით. კიბერტერორიზმის კლასიკური დეფინიციის მიხედვით ის წარმოადგენს კრიმინალურ ქმედებას, რომლის დროსაც გამოიყენება კომპიუტერული და ტელესაკომუნიკაციო საშუალებები და მიზანი კრიტიკული ინფრასტრუქტურის მწყობრიდან გამოყვანაა. კიბერტერორირზმს შედეგად შეიძლება მოჰყვეს ადამიანთა მსხვერპლი, მატერიალური დანაკარგი და მრავალი სხვა პრობლემა.

„საქართველოს სისხლის სამართლის კოდექსის 3241 -ე მუხლის მიხედვით, კიბერტერორიზმისაგან სისხლისსამართლებრივი დაცვის უშუალო ობიექტია სახელმწიფოს ინტერესი (სტრატეიული, პოლიტიკური ან ეკონომიკური), დამატებითი ობიექტი შეიძლება იყოს ადამიანის სიცოცხლე, ჯანმრთელობა, ქონება“.

კიბერტერორიზმის ობიექტური მხარე გამოიხატება კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლებაში, მის გამოყენებაში ან გამოყენების მუქარაში, რაც ქმნის მძიმე შედეგის განხორციელების საშიშროებას.

3241 -ე მუხლის დისპოზიციაში საუბარია კომპიუტერული ინფორმაციის დაუფლებაზე, მის გამოყებნებაზე ან გამოყენების მუქარაზე. საფრთხე - „მძიმე შედეგის განხორციელების საშიშროება“ - რაც შეიძლება შეიქმნას აღნიშნული მოქმედების განხორციელებით სხვდასხვა ხასიათის შიძლება იყოს, მაგალითად, ტრანსპორტის მუშაობის ბლოკირება, შფერხება ენერგომომარაგეაში, მასობრივი განადგურების იარაღის დამზაების ტექნოლოგიის ხელში ჩაგდება, სხვადასხვა სტრატეგიული დანიშნულების ობიექტების მუშაობის დეზორგანიზაცია და სხვა.[87]

324 1 -ე მუხლის პირველი ნაწილით გათვალისწინებული შმადგენლობა კონკრეტული საფრთხის შემქმნელი დელიქტის სახით არის ჩამოყალიბებული. ისჯება

[87] ჩიხლაძე კ., კიბერტერორიზმი (ინფორმაციული ესე), ინფორმაციული ტექნოლოგიები, ყოველკვარტალური სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი“ №3 თბ., 2012 გვ 23;

თავისთავად კანონში მითითებული მოქმედების ჩადენა - კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლება, მისი გამოყენება ან გამოყენების მუქარა, რაც ქმნის მძიმე შედეგის განხორციელების საშიშროებას.

324 1 -ე მუხლის პირველი ნაწილით გათვალისწინებული შმადგენლობა კონკრეტული საფრთხის შემქმნელი დელიქტის სახით არის ჩამოყალიბებული. ისჯება თავისთავად კანონში მითითებული მოქმედების ჩადენა - კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლება, მისი გამოყენება ან გამოყენების მუქარა, რაც ქმნის მძიმე შედეგის განხორციელების საშიშროებას.

3241 -ე მუხლის მე-2 ნაწილი პასუხისმგებლობის დამამძიმებელ გარემოებად ითვალისწინებს ადამიანის ადამიანის სიკვდილს ან სხვა მძიმე შედეგს, პირველი ნაწილით გათვალისწინებული ქმედების ჩადენის შედეგად.

324 1 -ე მუხლის მე-2 ნაწილი პასუხისმგებლობის დამამძიმებელ გარემოებად ითვალისწინებს ადამიანის ადამიანის სიკვდილს ან სხვა მძიმე შედეგს, პირველი ნაწილით გათვალისწინებული ქმედების ჩადენის შედეგად.[88]

მძიმე შედეგი შეფასებითი ნიშანია და საქმის კონკრეტული გრემოების მხედველობაში მიღებით უნდა შეაფასოს სასამართლომ. მძიმე შედეგი შეიძლება გამოიხატოს სტრატეგიული ობიექტის მუშაობის პარალიზებაში, ხელისუფლების ორგანოთა მუშაობის დეზორგანიზაციაში, დიდ ქონებრივზიანში და ა.შ.

კიბერტერორიზმის ამსრულებელი შეიძლება იყოს ნებისმიერი შერაცხადი ფიზიკური პირი 14 წლის ასაკიდან, ასევე იურიიული პირი.

სუბიექტური მხრივ კვალიფიკაციისათვის განმსაზღვრელი მნიშვნელობა აქვს მიზანს - მოსახლეობის დაშინება ან/და ხელისუფლების ორგანოზე ზემოქმედება. კიბერტერორიზმის მოტივი სხვადასხვა შეიძლება იყოს, პოლიტიკურით დაწყებული და

[88] სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეოთხე გამოცემა, ავტორთა კოლექტივი, გამომც. „მერიდიანი“ თბ., 2012 გვ 24;

რელიგიური ფანატიზმით დამთავრებული. ის კვალიფიკაციაზე გავლენას არ მოახდენს. სახეზეა პირდაპირი განზრახვით ჩადენილი დანშაული.[89]

„თანამედროვე მსოფლიოში კიბერდანაშაულის წინააღმდეგ ბრძოლა უკვე საერთაშორისო პრობლემად იქცა და თავისი მნიშვნელობით საერთაშორისო ტერორიზმსაც გაუტოლდა. ტრანსნაციონალური კომპიუტერული დანაშაულის და კიბერტერორიზმის წინააღმდეგ ბრძოლის ეფექტიანი მეთოდების შემუშავება წარმოადგენს მსოფლიო კიბერსივრცის უსაფრთხოების უზრუნველყოფის ძირითადი ელემენტია. სწორედ ამიტომ, კიბერსივრცის უსაფრთხოების კვლევა მსოფლიოში მრავალი ქვეყნის მუშაობის პრიოტეტულ მიმართულებად იქცა.

დასკვნა

თუ გადავხედავთ ტექნოლოგიების განვითარების ისტორიას, შევამჩნევთ , რომ იზდება იმ დანაშაულთა ჩადენის მაჩვენებლები რომელებიც ტექნოლოგიური საშვალებით ხორციელდება.

მიხედავათ იმასა რომ გაერომ და ევროკაავშირმა შეიმუშავეს კიბერდანაშაულთან ბრძოლის ერთიანი სტრატეგია დღემდე, მაინც ერთ-ერთ მნიშვნელოვან გამოწვევად რჩება მსოფლიოსთვის, რადგან აღნიშნული დანაშაული თავის ბუნებით სეპციფიური ხასიათიასაა და ის ხორციელდება, დანაშაულისელყოფის ადგილიდან მოშორებით. საზღვრების გახსნისა და ფართო გლობალიზაციის პირობებში, დამნაშვეს აქვს საშვალება ერთი ქვეყნიდან მერე ქვეყანაში განახორციელოს კიბერდანაშაულით გათვალისწინებული ქმედება, ამიტომ მნიშვნელოვანი უფრო მეტი სახელმწიფო

[89] სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეხუთე გამოცემა, ავტორთა კოლექტივი, გამომც. „მერიდიანი“ თბ., 2017, 282-283;

გაერთიანდნენ აღნიშნულ დანაშალთან ბრძოლაში, შექმნან ერთიანი სამოქმედო სტრატეგია და ითანამშრომლონ ეფექტურად კიბერდანაშაულის წინაღმდეგ ბრძოლაში.

საქართველო შეუერთდა ევროპული ქვეყნების სულის კვეთებას კიბერდანაშაულის წინაღმდეგ ბრძოლაში და მოახდინა კრიმინალიზაცია კიბერდანაშაულით გათვალისწინებული ქმედებების, ჩვენ დღესდღეობით რამოდენიმე მუხლი გვხვდება კანომდებლობაში რომლითც ხდება კიბერ დანაშაულთან ბრძოლა.

კანომდებლობის არსებობასთან ერთად მნიშვნელოვანია რომ გვქონეს ეფექტური გეგმა და მისი შესრულების ტექნიკური საშვალებები კიბერ დანაშაულის წინაღმდეგ ბრძოლისთვის, რადგან მომზადებული შევხვდეთ ფართო მაშტავიან კიბერ თავდასხვმას, რომელიც მოხდა 2008 წელს რუსეთ - საქართველოს ომის პერიოდში, რუსეთის სახელმწიფომ ფართო მაშტაბიანი კიბერ შეტევა განახორციელა ქართულ სახელმწიფოზე, საქართველო ამისთვის მზად არ აღმოჩნდა, სამომავლოდ იგვე რომ არ გამორდეს აუცილებელაი ეფექტური სტრატეგის ჩამოყლიებება და პრაკტიკაში დანერგვა.

მნიშვნელოვანია სახლმწიფოს ქონდეს მკვეთრად განსაზღვრული კანომდებლობა რომლითაც მოხდება სახელმწიფო უსაფრთოებისა და უშიშროების ლეგიტმური მიზნის მისახწევად ადამიანის პირად ცხოვრებაში ჩარევა, აუცილებელია რომ სახელმწიფომ ზღვარი დაიცვას ლეგიტიმურ მიზნის მიხწევასა და პირადი ცხოვრების ხელშეუხებლობის დაცვას შორის. სახელმწფოს შეზღუდული უნდა ქონდეს მართვითი ბერკეტები რომ უკანონოდ და არაპროპორციულად არ ჩაერიოს ადამინის პირად ცხოვრებაში და არ დადაიქცეს კიბერ დანაშაულის ჩამდენ სუბექტად.

გამოყენებული ლიტერატურა

1. ავტორთა კოლექტივი, „სისხლის სამართლის კერძო ნაწილი“, წიგნი 2, გამომც. „მერიდიანი“, თბ., 2012;
2. [1] Cooperative Cyber Defense Centre of Exelllence https://ccdcoe.org/tallinn-manual.html
3. www.conventions.coe.int
4. [1] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm
5. [1] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm
6. [1] http://www.chebucto.ns.ca/Current/HalifaxSummitG7/
7. [1] http://www.oecd.org/sti/whatistheoecdworkingpartyoninformationsecurityandprivacywpisp.htm
8. [1] Organization of American States http://www.oas.org/en/
9. [1] SCOTT CHARNEY, KENT ALEXANDER, Types of computer crime,25.11.2005 http://www.crimeresearch.org/articles/types-of-computer-crime/2
10. [1] Technology Risk Checklist http://archive.rdec.gov.tw/public/Data/851413535571.pdf
11. [1] ა. კაცმანი, დისერტაცია „კომპიუტერული დანაშაული“, თბ, 2004წ გვ, 35.

12. [1] ავტორთა კოლექტივი, „სისხლის სამართლის კერძო ნაწილი“, გამომც „მერიდიანი“ თბ, 2012, გვ 46.

13. [1] ავტორთა კოლექტივი, მოსამრთლეების ტრენინგი კომპიტერული დანაშაულის შესახებ:ტრენინგი სახემძღვანელო,ევრო საბჭო, სტრასბურგი, 2010 წ გვ. 57

14. [1] ავტორთა კოლექტივი, მოსამრთლეების ტრენინგი კომპიტერული დანაშაულის შესახებ:ტრენინგი სახემძღვანელო,ევრო საბჭო, სტრასბურგი, 2010 წ გვ. 55

15. [1] ავტორთა კოლექტივი, “სისხლის სამართლის კერძო ნაწილი“, წიგნი 2 გამომც, „მერიდიანი“ თბ. 2012. გვ 40

16. [1] ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, ფარული რეგულირების მიყურადება საქართველოში, გვ 14

17. [1] კაცმანი ა., კომპიუტერული დანაშაული, ავტორეფერატი იურიდიულ მეცნიერებათა კანდიდატის სამეცნიერო ხარისხის მოსაპოვებლად, თბ., 2004, გვ 77-81

18. [1] კაცმანი ა., კომპიუტერული დანაშაული, ავტორეფერატი იურიდიულ მეცნიერებათა კანდიდატის სამეცნიერო ხარისხის მოსაპოვებლად, თბ., 2004, გვ 77-81;

19. [1] ლ.ბოძაშვილი, ნ.კოხრეიძე „კიბერსივრცის სამართალი, 2012 წ გვ 35

20. [1] ლ.ბოძაშვილი, ნ.კოხრეიძე, კიბერსივრცის სამართალი, თბ, 2012, გვ 5

21. [1] მშვიდობაძე ხ., გლობალური მნიშვნელობის კიბერდომეინი და ახალი გამოწვევები, ექსპერტის აზრი, №11, 2013, გვ 26;

22. [1] ნ.ცომაია, „სახელმწიფოს მხირდან კომპიუტერულ სისტემებში ფარული შეხწევა და ამ ღონისძიების კონსტიტუციურ სამართლებრივი საზღვრები“, ჟურ. „მართლმსაჯულება და კანონი“ 2008 წ N2, გვ. 81

23. [1] საქართველოს საკოსტიტუციო სასამართლოს გადაწყვეტილება, №1/1/625, 640

24. სისხლის სამართლის კოდექსი,1999წ
25. უ. ზაქაშვილი, კიბერდანაშაულის სისხლისამართლებრივი რეგულირების პრობლემები საქართველოში, დისერტაცია, თბ., 2013, გვ. 64
26. [1] 1 Computer Incident Response Capability https://www.terena.org/activities/tf-csirt/meeting11/NCIRC-Anil.pdf
27. [1] Azia – Pacific Economic Cooperation http://www.apec.org/
28. [1] http://en.wikipedia.org/wiki/Convention_on_Cybercrime
29. [1] http://www.interpol.int/Public/ICPO/FactSheets/FHT02.pdf
30. [1] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf
31. [1] http://www.today.az/news/society/46054.html
32. [1] https://www.ciret.org/conferences/paris-2000/
33. [1] Information Technology Security Handbook
34. [1] Larry J. Siegel (2008) Criminology- Cyber crime and technology - Cyber terrorism: Cyber Crime With Political Motives . pp № 449
35. [1] Organization for Economic Co-operation and Development http://www.oecd.org/
36. [1] Pedro Verdelho,Cybercrime and Electronic Evidence, E-Newsletter "Electronic Newsletter on the Fight Against Cybercrime"(ENAC)" #1, jule, 2009, p2
37. [1] Report from the Commission to the Council, Brussels, 17.07.2008. com (2008) 448 (Based on article 12 of the Council Framework Decision of 24.02.2005 on attaks against information systems).
38. [1] Report from the Commission to the Council, Brussels, 17.07.2008. com (2008) 448 (Based on article 12 of the Council Framework Decision of 24.02.2005 on attaks against information systems);
39. [1] Richard W. Aldrich, "CYBERTERRORISM AND COMPUTER CRIMES: ISSUES SURROUNDING THE ESTABLISHMENT OF AN INTERNATIONAL LEGAL

REGIME", USAF Institute for National Security Studies USAF Academy, Colorado, April 2000, gv.10

40. [1] SCOTT CHARNEY, KENT ALEXANDER, Types of computer crime,25.11.2005 http://www.crimeresearch.org/articles/types-of-computer-crime/2
41. [1] The Availability and Robustness of Electronic Communications Infrastructures
42. [1] The Critical Infrastructure Warning Information Network https://ciwin.europa.eu/Pages/Home.aspx
43. [1] The Cyber Defense Management Authority (CDMA): The Authority was called upon to initiate and coordinate response to cyber attacks against allied member states, and NATO itself. CDMA was Created and was operational in mid-2008. It was a big step in NATO Cyber Defense because it helps member states improve their own cyber security. Rapid-Reaction Teams (RRT's) are also being created and will be available to member states in order to help them counter cyber attacks and will be available for immediate deployment http://csis.org/blog/nato-and-cyber-defensebrief-overview-and-recent-events
44. [1] The European Software Testing Awards http://www.softwaretestingawards.com/
45. [1] The European Union Agency for Network and Information Security https://www.enisa.europa.eu/
46. [1] United Nations A/CONF.187/10, (ix. http://ebookuniverse.net/aconf18710-pdf-d8490066)
47. [1] ა.კაცმანი, „კომპიუტერული დანაშაულის სისხლისსამართლებრივი და კრიმინალისტიკური დახასიათება",ჟურნ. „სამართალი" 2000 წ N2 გვ. 58
48. [1] ავტორთა კოლექტივი, „სისხლის სამართლის კერძო ნაწილი", წიგნი 2 გამოც. „მერიდიანი", თბ. 2012, გვ. 42
49. [1] ავტორთა კოლექტივი, მოსამრთლეების ტრენინგი კომპიტერული დანაშაულის შესახებ:ტრენინგი სახემძღვანელო,ევრო საბჭო, სტრასბურგი, 2010 წ გვ. 47

50. [1] ავტორთა კოლექტივი, სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეხუთე გამოცემა, გამომც. „მერიდიანი“, 2017, გვ 281
51. [1] ავტორთა კოლექტივი, სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეხუთე გამოცემა, გამომც. „მერიდიანი“ , 2017, გვ 281
52. [1] აღნიშნული კონვენცია საქართველოსთან მიმართებაში ძალაში შევიდა 2012 წლის პირველი ოქტომბრიდან. შედეგად, საქართველო გახდა კონვენციის 34-ე წევრი სახელმწიფო
53. [1] ბ,კვირკველია. „კომპიუტერული დანაშაული“
54. გურეშიძე ს., სტატია, „ტერორიზმი ინტერნეტში“, ახლო აღმოსავლეთი და საქართველო, V, თბ., 2008, 67
55. [1] ევროკავშირის წევრი ქვეყნები, კანადა, იაპონიია, სამხრეთ აფრიკის რესპუბლიკა და ნატო - ს ყველა წევრი ქვეყანა
56. [1] ევროპაში ნატო - ს გაერთიანებული შეიარაღებული ძალების ყოფილი უმაღლესი მთავარსადრდალი, ამჟამად შეერთებული შტატების ეროვნული უსაფრთხოების მრჩეველი
57. [1] თ.წერეთელი გ.ტყეშელიაძე, „მოძღვრება დანაშაულზე“ გამომც. „მეცნიერება“ თბ. 1969 წ გვ. 156
58. [1] ლ. პატარაია, კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, თბ., 2012, გვ 49
59. [1] მ.პ.ვასმერი, კიბერდანაშაული - აწყმყო და მომოვალი, გვ, 13
60. [1] ნაკაშიძე გ., სტატია, „კიბერტერორიზმი - XXI საუკუნის მწვავე გამოწვევა“, ჟურნალი ეკონომიკა და ბიზნესი, №4 ივლისი-აგვისტო, 2012, 172
61. [1] პატარაია ლ., კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, თბ., 2012, გვ 49;
62. [1] პატარაია ლ., კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, 2012, 45

63. [1] პატარაია ლ., კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, გამომცემლობა ,,სანი“, თბ., 2012, 46;
64. [1] სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეოთხე გამოცემა, ავტორთა კოლექტივი, გამომც. „მერიდიანი“ თბ., 2012 გვ 24;
65. [1] სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეხუთე გამოცემა, ავტორთა კოლექტივი, გამომც. „მერიდიანი“ თბ., 2017, 282-283;
66. [1] სისხლის სამართლის კოდექსი,1999, 285-ე მუხლი
67. [1] უ.ზაქაშვილი,კიბერდანაშაულის სისხლისამართლებრივი რეგულირების პრობლემები საქართველოში, დისერტაცია, თბ, 2013, გვ, 7
68. [1] ჩიხლაძე კ., კიბერტერორიზმი (ინფორმაციული ესე), ინფორმაციული ტექნოლოგიები, ყოველკვარტალური სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი“ №3 , 2012, გვ122;
69. [1] ჩიხლაძე კ., კიბერტერორიზმი (ინფორმაციული ესე), ინფორმაციული ტექნოლოგიები, ყოველკვარტალური სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი“ №3 თბ., 2012, 123
70. [1] ჩიხლაძე კ., კიბერტერორიზმი (ინფორმაციული ესე), ინფორმაციული ტექნოლოგიები, ყოველკვარტალური სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი“ №3 თბ., 2012 გვ 23;
71. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_in_georgia/projectcyber_e n.asp).