შპს გურამ თავართქილაძის სახელობის თბილისის

სასწავლო უნივერსიტეტი

სამართლის ფაკულტეტი

სისხლი სამართლის სამაგისტრო პროგრამა

თემა: თანამედროვე ტექნოლოგიები და კიბერდანაშაული

ნაშრომი შერულებულია სამართლის მაგისტრის

აკადემიური ხარისხის მოსაპოვებლად

სტუდენტი: ბაჩუკი ჩხარტიშვილი

ნაშრომის ხელმძღვანელი

პროფესორი : გივი ლობჟანიძე

თბილისი

2020

შინაარსი

ანოტაცია

წინამდებარე ნაშრომში განხილულია თანამედროვე ტექნოლოგიებისა და კიბერდანაშაულის ცნება, ნაშრომში აღწერილი და განხილულია ზოგადად კიბერდანაშაულის განვითარების ეტაპები, კომპიუტეულ და ინტერნეტ ტექნოლოგიათა განვითარება, კიბერდანაშაულის სისხლისსამართლებრივი დახასიათება, კიბერდანაშაულთან დაკავშირებული ქართული საკანონმდებლო რეგულაციები, ევროპული კონვენციები კიბერდანაშაულთან დაკავშირებით და ჰაკერული თავდასხმის თავდიან აცილების თანამედროვე მეთოდები რაც თანამედროვე მიდგომებით უზრუნველყოფს კიბერდანაშაულის წინააღმდეგ ეფექტურ ბრძოლას.

ტექნოლოგიური განვითარების პარალელურად ვითარდება და იხვეწება კიბერდამნაშავეების დანაშაულებრივი მიდგომები, კიბერსივრცეში არსებულ წესწყობილებებთან. შესაბამისად, დიდი მნიშვნელობა უნდა მიენიჭოს კიბერდანაშაულში არა მხოლოდ საერთაშორისო თუ ეროვნულ რეზოლუციებს და რეკომენდაციებს, არამედ პიროვნულ ფაქტორს. რადგან კომპიუტერული ქსელისა და კომპიუტერული მოწყობილობის მომხმარებელი არის ფიზიკური პირი.

Annotation

This paper discusses the concept of modern technology and cybercrime, describes and discusses in general the stages of cybercrime development, computer technology development, criminal characterization of cybercrime, modern legislation on cybercrime related to cybercrime, and modern European conventions on cybercrime. To fight.

In parallel with the technological development, the criminal approaches of cybercriminals are developing and improving with the existing institutions in cyberspace. Therefore, not only international or national resolutions and recommendations, but also personal factors should be given great importance in cybercrime. Because the user of the computer network and computer device is a natural person.

შესავალი

არსებობს ტერმინის, „კიბერსივრცის“ განმარტების ბევრი ვარიანტი და ყველა მათგანი იძლევა თავისებურ განსაზღვრებას. კიბერსივრცეში უსაფრთხოების უზრუნველყოფის სირთულეებს საზღვრები არ გააჩნია. მაგრამ ქვეყანათა უმრავლესობა ცდილობს, 21 საუკუნის გამოწვევას დამოუკიდებლად საკუთარი ძალებით დაუპირისპირდეს რის გამოც, ყველა საჭირო ზომები და ღონისძიებები ხშირ შემთხვევაში არასაკმარისია. დღესდღეობით კიბერსივრცე, როგორც ეს ბევრ განმარტებაშია განსაზღვრული, გასცდა განმარტებულ ინფორმაციულ ტექნოლოგიური ინფრასტრუქტურის ურთიერთკავშირის კომპლექსს და იქცა უკვე ჩვენთვის კარგად ცნობილ კიბერდანაშაულად.არსებობს უამრავი სირთულე როგორც კიბერუსაფრთხოების სირთულეების ჩვენეულ გაგებაში, ისე სახელმწიფო პოლიტიკაში და ტექნოლოგიურ შესაძლებლობებში, რომლებიც სასიცოცხლოდ აუცილებელია მოცემული საკითხების გადასაჭრელად.

კაცობრიობის ჩამოყალიბებისთანავე ადამიანს გააჩნდა განვითარების წყურვილი, რამაც საბოლოოდ მიგვიყვანა დიდ პროგრესამდე. ყველა მნიშვნელოვან წინ გადადგმულ ნაბიჯს და გამოგონებას შორის ალბათ ყველაზე მნიშვნელოვანია ინტერნეტის შექმნა და განვითარება. რომელმაც თავის მხრივ ჩამოაყალიბა ადამიანების საერთო ენა და შექმნა კომპიუტერების გლობალური ქსელი.

21-ე საუკუნე ვირტუალური სამყაროს და ზოგადად ინტერნეტ კავშირის ეპოქაა. ამ ორი ელემენტის ერთობლიობა კი აყალიბებს ყოველდღიური ცხოვრების განუყოფელ ნაწილს. ანუ იმას რასაც კიბერ სივრცეს ვუწოდებთ. როგორც ზევით ავღიშნე მისი დახმარებით შეგვიძლია ფაქტიურად მომენტალურად მივიღოთ სასურველი ინფორმაცია, დავამყაროთ კავშირი მსოფლიოს ნებისმიერი წერტილიდან, გამოვიმუშაოთ ფული და მივიღოთ მნიშვნელოვანი გადაწყვეტილებები.მიუხედავად აღნიშნული სიკეთეებისა კიბერსივრცის დღევანდელი არქიტექტურა ვერ გვაძლევს ამ კავშირების უსაფრთხოების გარანტს.

კიბერდანაშაულის მზარდი სტატისტიკა განპირობებულია კიბერ საკითხებზე საზოგადოების დაბალი ცნობიერებით რაც მნიშვნელოვანი საფრთხის წინაშე აყენებს უბრალო მოქალაქეებს, სახელმწიფოს, მსოფლიო ეკონომიკას და რაოდენ გასაკვირიც არ უნდა იყოს გლობალურ ინფრასტრუქტურასაც. ამის ნათელი მაგალითები კი წარსულსა და აწმყოშიც მრავლად მოგვეპოვება.

მრავალი სახელმწიფო დარწმუნდა იმ რისკის არსებობაში, რომ კომპიუტერული ქსელები და ელექტრონული ინფორმაცია შეიძლება გამოყენებულ იქნას დანაშაულის ჩასადენად და ამგვარ დანაშაულთან დაკავშირებული მტკიცებულება შეიძლება ინახებოდეს ან გადაიცემოდეს ქსელების მიერ. მსოფლიოსთვის საერთოა ეს გამოწვევა. ყველა ქვეყანამ უნდა გადადგას ქმედითი ნაბიჯები, რათა კიბერკონფლიქტებმა და კიბერომებმა ინფორმაციული კატასტროფის წინაშე არ დაგვაყენოს. კიბერკრიმინალი, დანაშაული ინფორმატიკის სფეროში, სულ უფრო და უფრო გავრცელებული ხდება. კიბერკრიმინალი თანდათანობით ცინიკური, მასშტაბური და ორგანიზებული ხდება.

მალე ის მიაღწევს ორგანიზებული დანაშაულის ისეთი ტრადიციული სფეროების მასშტაბებს, როგორიცაა ნარკოტიკებითა და იარაღით ვაჭრობა, პროსტიტუცია. ექსპერტთა შეფასებით, ყოველწლიურად ხდება ინფორმაციის მოპარვა პლასტიკური ბარათებიდან და საბანკო ანგარიშებიდან, საიდანაც შეიძლება მოიხსნას 8-10მილიარდი დოლარი, ხოლო ინფორმაციის მიტაცების მცდელობა ყოველწლიურად აღწევს დაახლოებით 2 მილიონ შემთხვევას[1].

2008 წლის აგვისტოს ომის დროს განხორციელებულმა კიბერშეტევებმა ცხადყო, საქართველოში კიბერუსაფრხოების უზრუნველსაყოფად ეფექტური მექანიზმების არსებობის აუცილებლობა. ამასთან, ინფორმაციული ტექნოლოგიების მზარდ გამოყენებასთან ერთად ქვეყანაში თანდათანობით იზრდება კიბერდანაშაულის საფრთხე, სულ უფრო პრიორიტეტული ხდება ამ დანაშაულის წინააღმდეგ ბრძოლა მისი პრევენციისა და გამოძიების გზით[2].

ამ მიზეზებიდან გამომდინარე, კიბერ უსაფრთხოება წარმოადგენს თანამედროვე სამყაროს ნამდვილ გამოწვევას,რომელთან გამკლავებაც მხოლოდ სამართალმცოდნეების, უსაფრთხოების ექსპერტებისა და საზოგადოების აქტიური მონაწილეობით არის შესაძლებელი. იმისათვის, რომ უფრო ნათლად დაგანახოთ პრობლემის რეალურობა, წარმოგიდგენთ სტატისტიკურ მონაცემებს, არსებულ პრობლემებთან დაკავშირებით, ქვემოთ მოცემულ თავებში.აღნიშნული ინოფრომაცია დაფუძნებულია ისეთი გავლენიანი კომპანიების ანგარიშებზე როგორებიცაა: Symantec (სიმანტეკი),Blue Coat(ბლუ ქოათი), Mucap (მაქაფი),Interpol(ინტერპოლის ბიურო) და სხვა.

ნაშრომის აქტუალურობას განაპირობებს კიბერდანაშაული, როგორც სიახლე კაცობრიობისთვის. მასზე თითქმის არ მოიპოვება ნაშრომები და ლიტერატურა, რის გამოც წარმოდგენილი ნაშრომი კიდევ ერთი წინ გადადგმული ნაბიჯია თანამედროვე ტექნოლოგიებისა და კიბერდანაშაულის ირგვლივ ჩატარებულ კვლევაში. ამასთან მისი აქტუალურობა

[1]http://worldofhackers1.blogspot.com/

[2] ს. შენგელია, კიბერდანაშაული - XXI საუკუნის გამოწვევა, სტუდენტური სამართლებრივი ჟურნალი, თბ., 2011 გვ. 50.

გამომდინარეობს იქედან, რომ დღითი დღე იზრდება კიბერ შეტევები და ზოგადად კიბერდანაშაული, რასაც დამკვიდრებული საგამოძიებო მიმართულება ვერ ეწევა და შესაბამისად რჩება გაუხსნელი დანაშაული, რაც იმას ნიშნავს რომ მასზე მუშაობა აუცილებელია, რაც მისი სრულყოფილი შესწავლის შედეგად უნდა მოხდეს.

ჩვენი ნაშრომის მიზანია უკეთ გავაანალიზოთ კანონმდებლობა კიბერდანაშაულთან დაკავშირებით, გამოვკვეთოთ ხარვეზები და შევიმუშავოთ რეკომენდაციები. რამეთუ საქართველოში კომპიუტერული დანაშალის პრობლემის აქტუალობა ყოველწლიურად იზრდება. პროგრესს განაპირობებს კომპიტერლი დანაშაულის ჩადენისთვის ე.წ. ნოყიერი ნიადაგი. ამ ნიადაგს მიეკუთვნება: კომუნალური გადასახადების გადახდის შესაძლებლობა ინტერნეტით, ინტერნეტბანკინგის განვითარება[3], სხვადასხვა იტერნეტ მაღაზია, რომელშიც შინიდან გაუსვლელად შესაძლებელია სასურველი ნივთის შეძენა, სახელმწიფო დაწესებულებების მხრიდან ელექტრონულ დოკუემენტ ბრუნვაზე გადასვლა, ოფიციალური დოკუმენტების ელექტრონული წესით გაცემის შესაძლებლობა. გარდა ამისა მთელი რიგი სასიცოცხლო მნიშველობის ან/და სახელმწიფო დაწესებულება, იმართება სხვადასხვა კომპიუტერული პროგრამით და სისტემით. მაგალითად, აეროპორტები, საავადმყოფოები, სახელმწიფოს თავდაცვის ობიექტები და ა.შ.

ნაშრომის ამოცანაა სრულყოფილად გავეცნოთ თანამედროვე ტექნოლოგიებს და კიბერდანაშაულს, რათა შეგვეძლოს სრულყოფილად ვებრძოლოდ შესაბამის დანაშაულებს.

ნაშრომში გამოყენებულია კვლევის სხვადასხვა მეთოდები, მათ შორის შედარებით-სამართლებრივი მეთოდები, რითაც საქართველოს სამართლებრივი მდგომარეობა შევადარე საერთაშორისო სამართლის ნორმებს და აღნიშნულის საფუძველზე ნაშრომში გადმოცემულია შესაბამისი რეკომენდაციები. ნაშრომში ასევე გამოყენებულია სტატისტიკური მეთოდი და ასევე სიტემური მეთოდი რითაც გადმოცემულია ნაშრომში წარმოდგენილი ინფორმაცია.

[3]ინტერნეტ ბანკინგი არის, დისტანციური საბანკო მომსახურება რაც გულისხმობს მომხმარებლის მიერ საკუთარი ანგარიშების დისტანციურ მართვას. მომხმარებელი დამოუკიდებლად, ბანკში მიუსვლელად განკარგავს და აკონტროლებს თავის ანგარიშებს.

თავი I. ლიტერატურის მიმოხილვა

სამაგისტრო ნაშრომზე მუშაობისას გამოვიყენე ლიტერატურა, რომელიც დამეხმარა, რომ თემა შეხებოდა თანამედროვე ტექნოლოგიებს და კიბერდანაშაულის ყველა მნიშვნელოვან საკითხს. ასეთი იყო ავტორთა კოლექტივი, სისხლის სამართლის კერძო ნაწილი, წიგნი II, სადაც სამართლებრივად განხილული და გაშლილია საქართველოს სისხლის სამართლის კოდექსის XXXVთავით და XXXVIII თავის 324[1] მუხლით გათვალისწიენებული დანაშაულები. ასევე საინტერესო იყო პატარაია ლ., კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტებიში.

წიანამდებარე ნაშრომში გამოყენებულია როგორც ქართული ასევე უცხოური ლიტერატურა, ნორმატიული აქტები, სტატიები, ინტერვიუები და ა.შ. მაგ. საქართველოს კონსტიტუცია, საქართველოს სისხლის სამართლის კოდექსი, კიბერ უსაფრთხოების თემაზე სამაგისტრო და სადისერტაციო ნაშრომები, ევრო საბჭოს დებულებები რომლემბშიც განსაზღვრულია კიბერ უსაფრთხოების პოლიტიკა, საქართველოში ჩატარებული კიბერ უსაფრთხოების სტრატეგიების და მთავარი გამოწვევების შესახებ ინფორმაციები, კიბერ თავდამსხმელების მიერ ჩატარებული მასშტაბური შეტევების განხილვები და კიბერდანაშაულის თავიდან აცილების თანამედროვე მეთოდები. ასევე დიდი ინფორმაცია მომცა და გამომადგა, ინტერნეტ საიტებზე განთავსებული წყაროები თანამედროვე ტექნოლოგიებზე და კიბერ დანაშაულის შესახებ ძველ და თანამდეროვე გამოცდილებებზე.

თავი II. კიბერნეტიკის განვითარების ტენდენციები

კომპიუტერული დანაშაული დღეის მდგომარეობით მეტად მნიშვნელოვანია რადგან, როგორც ისტორია გვასწავლის კრიმინალები ხშირად ბოროტად იყენებენ ახალ ტექნოლოგიებს სარგებლის მისაღებად ან სხვებისთვის ზიანის მისაყენებლად. ავტომობილი ამის შესანიშნავი მაგალითია. ზოგადად ავტომობილი შეიქნა კანონმორჩილი ადამიანების ტრასპორტირებისთვის მაგრამ მალე ის გადაიქცა სხვადასხვა დანაშაულის საგნად (მაგ. მანქანის ქურდობა, მანქანის გაქურდვა), საშუალებად (მაგ. ბანკის ძარცვისას კართან მდგარი მანქანა ან სარგებლის მიღების მიზნით უკანონო ქუჩის რბოლების მოწყობა და მონაწილეობა) და იარაღად (მაგ. ავტო საგზაო შემთხვევა, როდესაც დამნაშავე მიიმალება)[4]. კომპიუტერების შემთხვევაშიც აშკარად იგივე მეორდება.

დღეისათვის, ადამიანების ცხოვრება ფაქტობრივად წარმოუდგენელი გახდა უინტერნეტოდ. ინტერნეტი გვხვდება ყველგან: ჩვენს სახლებში, სამსახურში, კაფეებში და სკვერებშიც კი. თუმცა, მიუხედავად ამისა, ცოტა ადამიანი თუ მოიძებნება ისეთი, ვინც იცის რეალურად საიდან წარმოიშვა ინტერნეტი და რა ევოლუციის ეტაპები განვლო მან დღემდე.

მას შემდეგ რაც 1957 წელს რუსეთმა კოსმოსში პირველი ხელოვნური თანამზავრი გაუშვა, ამერიკის მთავრობა სერიოზულად დაფიქრდა საკუთარ უსაფრთხოებაზე. ქვეყნის თავდაცვის უწყება მივიდა იმ დასკვნამდე, რომ საჭირო იყო შეექმნათ ახალი დეცენტრალიზირებული საკომუნიკაციო სისტემა. ისინი თვლიდნენ, რომ საჭირო იყო ინფორმაციის გადაცემის საიმედო სისტემა, რომლის გათიშვაც შეუძლებელი იქნებოდა მისი ერთერთი სეგმენტის მწყობრიდან გამოყვანის შემთხვევაშიც კი.

სწორედ ამისათვის შეიქმნა სპეციაულური მოწინავე პროექტების კვლევების სააგენტო, ცნობილი, როგორც ARPA (Advanced Research Projects Agency). აღნიშნული პროექტის ფარგლებში კი, 1969 წელს მიიღეს საბოლოო გადაწყვეტილება, რომ შეექმნათ კომპიუტერული ქსელი ARPANET. ეს პროექტი ამერიკელი სამხედროების მიერ იყო დაფინანსებული და აერთიანებდა 4 ამერიკულ სამეცნიერო ინსტიტუტს. აღსანიშნია, რომ იმ დროისათვის კომპიუტერს მონიტორიც კი არ ჰქონდა და ინფორმაციის მოწოდება პრინტის სახით ხდებოდა.

[4]Scott Charney, Kent Alexander, Types of computer crime, Computer Crime Research Center (6/04/2020) http://www.crime-research.org/articles/types-of-computer-crime

1969 წლის 29 ოქტომბერს, აპრა-ნეტში (APRA-net) ჩართულ ორ კომპიუტერს შორის პირველი კავშირი შედგა. ამ ორი კომპიუტერიდან ერთი ლოს–ანჯელესში , კალიფორნიის უნივერსიტეტში, ხოლო მეორე კი სტენფორდში, სტენფორდის კვლევით უნივერსიტეტში მდებარეობდა. მათ შორის მანძილი 649 კილომეტრი იყო. პირველი საკომუნიკაციო სიტყვა კი „LOG ON " უნდა ყოფილიყო თუმცა პირველ ჯერზე მხოლოდ „LOG"–ის გაგზავნა მოხერხდა, და შემდეგ სისტემა გაითიშა. თუმცა საათნახევრიანი მუშაობის შედეგად ცდა თავიდან ჩატარდა და კომუნიკაცია წარმატებით დასრულდა.

1973 წელს ტრანსატლანტიკური კაბელით ქსელს შეუერთდენ არაამერიკული ორგანიზაციები ნორვეგიიდან და დიდი ბრიტანეთიდან. თუმცა 1982 წლამდე ქსელებს შორის კომუნიკაცია მაინც გართულებული იყო, რადგანაც ზოგიერთი მათგანი განსხვავებული პრინციპებით იყო აგებული. ამიტომაც, 1982–83 წლებში შეიქმნა ერთიანი სტანდარტი ყველა ქსელებისათვის – TCP/IP რომელიც დღესაც გამოიყენება . ეს გულისხმობს რომ ქსელში ჩართულ ყველა კომპიუტერს საკუთარი უნიკალური ნომერი აქვს, და შესაბამისად მათ შორის კომუნიკაციაც მოწესრიგებულია. აღსანიშნია, რომ ამ პერიოდისათვის ინტერნეტით მხოლოდ მონაცემების გაცვლა იყო შესაძლებელი. არ არსებობდა არც ვებ გვერდების და არც ფაილების ჰოსტინგის სისტემა[5].

1983 წელს ARPANET ი უკვე საერთაშორისო ქსელი გახდა და შესაბამიდად წარმოიშვა ახალი ტერმინიც: INTERNET (International Net)

1989 წელს კი, კიდევ ერთი მნიშვნელვანი ფაქტი მოხდა: ევროპაში, ცერნის ლაბორატორიაში შემუშავდა WWW (World Wide Web) ის კონცეფცია, რომელიც ტიმ ბერნერს ლიმ წარმოადგინა. ტიმის მიზანი იყო ინტერნეტში შეექმნა ისეთი ვირტუალური სივრცე, სადაც შესაძლებელი გახდებოდა მონაცემებისა და ინფორმაციის ატვირთვა. ზუსტად ამ პერიოდით შეგვიძლია დავათარიღოთ ჩვენთვის აწ უკვე კარგად ნაცნობი ვებ გვერდებისკონცეფციის დაბადება[6].

კიბერდანაშაულის ორგვარი გაგება არსებობს. ფართო გაგებით კიბერდანაშაული არის ნებისმიერი დანაშაული, რომელიც კიბერსივრცეში ხდება, ხოლო ვიწროგაგებით კიბერდანაშაული არის შეტევა კიბერსაიტებზე, კომპიუტერული სისტემის ხელყოფა. კიბერდანაშაული – დანაშაული რომელიც ხდება ინტერნეტსივრცეში, სადაც კომპიუტერი ან მსხვერპლია ან დანაშაულის იარაღი. უზარმაზარი, უსაზღვრო ინტერნეტსივრცე, რომელიც მილიონობით ადამიანს აკავშირებს

[5] ფეისბუქ გვერდი, ისტორია - საინტერესო ფაქტები, 2015 წ. https://www.facebook.com/historyinterestingfacts/photos/A3/892572004128989/

[6] Iraklimk JUST ANOTHER WORDPRESS.COM SITE// https://iraklimk.wordpress.com

ერთმანეთთან, გამოიყენება არაკანონიერად, ფულის მოსაპარად, დეზინფორმაციის გასავრცელებლად და ა.შ.

რა შედის კიბერდანაშაულების რიცხვში? ა) ელექტრონული პროგრამისა და საკრედიტო ბარათების პაროლის გატეხვა, რაც ხშირ შემთხვევაში ხდება: მომხმარებლის დაუდევრობით (მარტივი ავტორიზაციის პაროლები, სესიის არასწორი დასრულება (Log Out); ბ) პერსონალური ინფორმაციის მოპოვება, შენახვა, რედაქტირება, გავრცელება, განადგურება; გ) სახელმწიფო დანიშნულების ინფორმაციის მოპოვება სადაზვერვო სამსახურების მიერ. (მაგალითად ოპერაცია ,,ენვერი“[7]); დ)ბავშვთა პორნოგრაფიის გავრცელება; ე)სპამი (ინგლ.სპამ) არის ელექტრონული წერილის ტიპი, რომელიც იგზავნება პიროვნების ან კომპანიის მიერ, მიმღების დაუკითხავად და სურვილის გარეშე. მსგავსი წერილები უმეტესწილად სარეკლამო ხასიათისაა. პიროვნებას, რომელიც მსგავს წერილებს გზავნის ეწოდება სპამერი. მათი ძირითადი მიზანია თავიანთი პროდუქტის პოპულარიზაცია. ვ) საავტორო უფლებების დარღვევა (ნებართვის, ან ლიცენზიის გარეშე, შემოსავლის მიღების მიზნით ინტელექტუალურ საკუთრების, არალიცენზირებული ფილმის, წიგნის, მუსიკის და ა.შ გავრცელება)[8].

კიბერდანაშაული პირველად ყურადღების ცენტრში XX საუკუნის 70-იან წლებში მოექცა. ამერიკელმა ალფონს კონფესორემ (პირველი კიბერ დამნაშავე) ელექტროგამომთვლელი მანქანის გამოყენებით 602 ათასი აშშ დოლარი მოიპარა და მსოფლიო კრიმინალისტიკის ისტორიაში პირველ კიბერდამნაშავედ იქცა. აღნიშნული ფაქტის შემდეგ ნაციონალურ და საერთაშორისო დონეზე დაიწყო ამ ფენომენის გამოკვლევა. ამერიკის შეერთებულ შტატებში ჯერ კიდევ 1977 წელს შეიმუშავეს კანონი ,,ფედერალური კომპიუტერული სისტემის დაცვის შესახებ“. გერმანიაში კომპიუტერული ინფორმაციის სფეროში ჩადენილ დანაშაულებზე სისხლისსამართლებრივი პასუხისმგებლობის საკითხი 1986 წლიდან დადგა. 1993 წელს მსგავსი ცვლილებები განიცადა ჰოლანდიის სისხლის სამართლის კოდექსმაც. დანაშაულის ეს სახეობა დღეს უკვე იმდენად

[7]2010 წლის 29 ოქტომბერსსააგენტო "როიტერმა" ანონიმურ წყაროზე დაყრდნობით მსოფლიოს აუწყა ინფორმაცია საქართველოს შსს-ს მიერ რუსეთის ჯაშუშების დაკავების შესახებ. შემდეგ კი უკვე ქართულმა მასმედიამ გაავრცელა ინფორმაცია, რომ საქართველოს შსს-ს კონტრდაზვერვის დეპარტამენტმა რუსეთის საგარეო დაზვერვის სამსახურის სასარგებლოდ მუშაობის ბრალდებით 13 პიროვნება დააკავა. ითქვა, რომ ისინი ცდილობდნენ ინფორმაციის მოპოვებას საქართველოს შსს-სა და თავდაცვის სამინისტროში განხორციელებულ შესყიდვებზე, ძალოვანი სტრუქტურების მაღალჩინოსნების პირადი მონაცემების შესახებ და ა.შ. შსს-ს ინფორმაციით, მათ გამოავლინეს რუსეთის ფედერაციის თავდაცვის სამინისტროს გენერალური შტაბის მთავარ სადაზვერვო სამმართველოსთან ფარულ კავშირში მყოფი ათეულობით ადამიანი https://www.myvideo.ge/v/1974947

[8] ს. შენგელია, კიბერდანაშაული - XXI საუკუნის გამოწვევა, სტუდენტური სამართლებრივი ჟურნალი, თბ., 2011, გვ. 51

”განვითარდა”, რომ ნარკოტიკებისა და იარაღით ვაჭრობის შემდეგ ყველაზე შემოსავლიანად ითვლება. მაგალითად, აშშ-ში ოფიციალური მონაცემებით, კომპიუტერული დანაშაულების შედეგად მიყენებული ზარალი წელიწადში საშუალოდ 5 მილიარდი დოლარია, საფრანგეთში-1 მილიარდი ევრო, გერმანიაში კი-4 მილიარდი ევრო. საგულისხმოა მათი ზრდის მაჩვენებელიც: ყოველწლიურად მსოფლიოში კიბერდანაშაულებათა რიცხვი 30-40%-ით იმატებს. კიბერდანაშაულებათა კუთხით პირველ პოზიციას 35%-იანი მაჩვენებლით აშშ იკავებს, მეორე ადგილზე ჩინეთია (30%), მესამეზე ბრაზილია (14,3%), სადაც განსაკუთრებით კომპიუტერული ვირუსებია გავრცელებული, მეოთხეზე რუსეთი (4,1%), ხოლო ”საპატიო ხუთეულს” შვედეთი (3,8%) ასრულებ[9] ისეთი განვითარებული სახელმწიფოები, როგორებიც არიან ამერიკის შეერთებული შტატები, იაპონია, დიდი ბრიტანეთი და ევროკავშირის სხვა ქვეყნები, ცდილობენ გააძლიერონ ცნობიერების ამაღლების კამპანია ინდივიდუალურ ინტერნეტ მომხმარებლებს შორის, თუ როგორ უნდა დაიცვან მათ თავი კიბერკრიმინალებისაგან. ორგანიზაციები, როგორებიცაა ფედერალური გამოძიების სააგენტო, ინტერპოლი და ევროპოლი, ოცდაოთხი საათის განმავლობაში აქტიურად მუშაობენ ინფორმაციის შეგროვების, შენახვის, ანალიზის და გაცვლის კუთხით. ისინი ორგანიზებას უკეთებენ კონფერენციებს, სემინარებს და ტრეინინგებს. ასევე აქვთ სპეციალური ცხელი ხაზები და განყოფილებები, რომელთა საშუალებით დახმარებას უწევენ მოქალაქეებს. აღსანიშნავია ის გარემოება, რომ ბოლო წლებში კომპიუტერული დანაშაული ფასდება სართაშორისო, ტრანსნაციონალურ დანაშაულად და მის წინააღმდეგ ბრძოლა მრავალი საერთაშორისო ორგანიზაციისთვის იქცა პრიორიტეტულ მიმართულებად. გაეროს მიერ მიღებულ იქნა ინფორმაციული ტექნოლოგიების გამოყენებით ჩადენილი დანაშაულების წინააღმდეგ ბრძოლის შესახებ რეზოლუციები[10].

საერთაშორისო მასშტაბით ელექტრონულ (კიბერნეტიკულ) დამნაშავეობასთან ბრძოლის საქმეში მნიშვნელოვან ნაბიჯს წარმოადგენ 2001 წლის 23 ნოემბერს ევროპის საბჭოს წევრი-ქვეყნების მიერ კონვენციის მიღება „კიბერდამნაშავეობასთან ბრძოლის შესახებ“. ეს კონვენცია განსაზღვრავს კიბერნეტიკულ დანაშაულთა სახეებს, რომლისთვისაც მონაწილე ქვეყნებმა სისხლისსამართლებრივი პასუხისმგებლობა უნდა დაადგინონ. ამ დოკუმენტით მსოფლიო თანამეგობრობის მიერ შემუშავებულია ერთნიანი პოზიცია იმის შესახებ, თუ რომელი ქმედებები უნდა იქნეს კრიმინალიზებული და რა ფორმით უნდა განხორციელდეს საერთაშორისო

[9]თ. კაციტაძე, გაზეთი “24 საათი”, კომპიუტერული დანაშაულები _ მსოფლიოს უდიდეს დანაშაულთა რიცხვში,

[10] ს. შენგელია, კიბერდანაშაული - XXI საუკუნის გამოწვევა, სტუდენტური სამართლებრივი ჟურნალი, თბ., 2011 გვ., 51

თანამშრომლობა კიბერნეტიკულ დანშაულთან საბრძოლველად. 2008 წლის 28 მარტს საქართველოს პრეზიდენტმა გამოსცა განკარგულება კიბერდამნაშავეობასთან ბრძოლის შესახებ კონვენციის ხელომოწერის თაობაზე, ხოლო საქართველოს 2010 წლის 24 სექტემბრის N 3619 კანონით ცვლილებები და დამატებები შევიდა სისხლის სამართლისა და სისხლის სამართლის საპროცესო კოდექსებში[11].

კიბერ დანაშაულის საკითხების მთავარ მარეგულირებელ საერთაშორისო დოკუმენტს წარმოადგენს ევროპის საბჭოს 2001 წლის ***კონვენცია კიბერდანაშაულის შესახებ***, რომლის რატიფიცირებაც საქართველომ 2012 წელს მოახდინა. აღნიშნული დოკუმენტი განსაზღვრავს კიბერ სივრცეში ჩადენილ იმ მართლსაწინააღმდეგო ქმედებებს, რომლის დასჯადად გამოცხადება ევალება კონვენციის ყველა წევრ სახელმწიფოს. ამასთანავე, კონვენცია წევრ ქვეყნებს ავალდებულებს შექმნან კიბერ დანაშაულთან ბრძოლის შიდა ეროვნული სპეციალიზირებული დანაყოფები, რომლებიც ასევე შეასრულებენ 24/7 საერთაშორისო საკონტაქტო პუნქტის უფლებამოსილებებს[12].

ამგვარად, საქართველოში განხორციელდა კიბერდანაშაულის შესახებ ევროკონვენციის ძირითადის პრინციპების ინტეგრაცია, ასევე ამ კონვენციის რაფიცირება და შესაბამისი საკანონმდებლო ცვლილებები.

2009 წლის 9 იანვარს ვაშინგტონში, სახელმწიფო დეპარტამენტში გაიმართა საქართველოსა და ამერიკის შეერთებულ შტატებს შორის სტრატეგიული პარტნიორობის ქარტიის ხელმწოწერის ცერემონიალი. დოკუმენტს ხელი მოაწერეს საქართველოს საგარეო საქმეთა მინისტრმა გრიგოლ ვაშაძემ და ამერიკის შეერთებული შტატების სახელწიფო მდივანმა კონდოლიზა რაისმა.

ქარტია ეფუძნება ორ სახელწიფოს შორის სტრატეგიული თანამშრომლობის პრინციპებს, სუვერენიტეტის, დამოუკიდებლობის, ტერიტორიული მთლიანობის, საძღვრების ურღვევობის მხარდაჭერას, კომპიუტერული დანაშაულის წიააღმდეგ ბრძოლას, დემოკრატიისა და სტაბილურობის განმტკიცებას. ევროატლანტიკურ სტრუქტურებში საქართველოს ინტეგრაციის გაღრმავების მიზნით, აშშ განახორციელებს გაძლიერებული უსაფრთხოების თანამშრომლობის პროგრამას, რაც გაზრდის საქართველოს პოტენციალს და გააძლიერებს ჩვენი ქვეყნის ნატო-ში გაწევრიანების შესაძლებლობებს.

[11] მ. ლეკვეიშვილი, ნ. თოდუა, გ. მამულაშვილი, სისხლის სამართლის კერძო ნაწილი, ნაწილი II, თბ., 2017 წ, გვ. 158

[12]http://police.ge/ge/projects/kiberdanashauli/kanonmdebloba-kiber-danashaulze-da-zogadi-politika

გლობალური მშვიდობისა და სტაბილურობის მიმართ საფრთხეების არსებობის გათვალისწინებით, საქართველოს და ამერიკის შეერთებული შტატები გააფართოვებენ თავდაცვისა და უსაფრთხოების სფეროებში თანამშრომლობის პროგრამებს, იბრძოლებენ მასობრივი განადგურების იარაღისა და სახიფათო ტექნოლოგიების გავრცელების წინააღმდეგ.

ეკონომიკისა და ვაჭრობისა სფეროებში თანამშრომლობის გაუმჯობესების მიზნით, საქართველო და აშშ განაახლებენ ხელშეკრულებას ორმხრივი ინვესტიციების შესახებ, გააფართოვებენ პრეფერენციათა განზოგადებულ სისტემაში საქართველოს ჩართულობას და განიხილავენ თავისუფალი სავაჭრო შეთანხმების შესაძლებლობას. შეერთებული შტატები დაეხმარება საქართველოს ომის შემდგომი რეკონსტრუქციისა და ფინანსური სტაბილურობის საქმეში.

საქართველო და აშშ ხელს შეუწყობენ ეკონომიკურ რეფორმებსა და ლიბერალიზაციის პროცესს, ახალი სამუშაო ადგილების შექმნას, ეკონომიკურ ზრდას და ბიზნეს-კლიმატის გაუმჯობესებას.[13]

დემოკრატიისა და პოლიტიკური პლურალიზმის განმტკიცების მიზნით, მხარეები ითანამშრომლებენ, რათა გაძლიერდეს მედიის თავისუფლება, პარლამენტი, სასამართლო რეფორმა, კანონის უზენაესობა, ანტიკორუფციული ღონისძიებები, ადამიანის უფლებები და ძირითადი თავისუფლებები.

კულტურის, განათლებისა და სამეცნიერო კვლევების სფეროებში გაიზრდება გაცვლითი პროგრამები, აგრეთვე აშშ გეგმავს სავიზო პროცედურების გამარტივებას აღნიშნულ პროგრამებში მონაწილეთათვის. ამერიკის შეერთებული შტატები საქართველოს დაეხმარება აგვისტოს ომის დროს დაზიანებული კულტურული მემკვიდრეობის ძეგლებისა და მედია გამოცემების აღდგენაში.[14]

თავდაპირველად, საქართველოს სისხლის სამართლის კოდექსში 2000 წლის 5 მაისის და 2000 წლის 30 ივნისის კანონების საფუძველზე შევიდა ცვლილება, რომლის თანახმადაც კოდექსმა განსაზღვრა სისხლისსამართლებრივი პასუხისმგებლობა კომპიუტერული დანაშაულისათვის. კერძოდ XXXV თავი „კომპიუტერული დანაშაული“ შედგება 284-ე, 285-ე, 286-ე მუხლებისაგან. ხოლო 2002 წლის 28 დეკემბერის ცვლილებით კოდექსის XXXVIII თავს (ტერორიზმი) დაემატა 324[1] მუხლი, რომელიც ითვალისწინებდა პასხისგებლობას კიბერტერორიზმისთვის. დღეს, ჩამოთვლილი მუხლების პირველადი რედაქციები აღარ არსებობს. აღსანიშნავია, რომ სისხლის

[13] https://mfa.gov.ge/News/-(1).aspx

[14] https://mfa.gov.ge/News/-(1).aspx

სამართლის კოდექსის ძველ რედაქციაში კომპიუტერული დანაშაულის განსაზღვრისას კანონმდებელი იყენებდა ისეთ ტერმინებს როგორებიც იყო ელექტრო გამომთვლელი მანქანა (ეგმ), ელექტრო გამომთვლელი მანქანის სისტემა და მისი ქსელი, მაშინ, როცა მსოფლიოს უმრავლეს ქვეყანაში, საკანონმდებლო დონეზე გამოიყენებოდა ტერმინი „კომპიუტერი“[15]. კომპიუტერი იგნლისური სიტყვაა და გამომთვლელს ნიშნავს. შინაარსობრივი განსხვავება კომპიუტერსა და ელექტრონულ გამომთვლელ მანქანას შორის არაა თუმცა, ალბათ, შესაბამისი იქნება გამოვიყენოთ ისეთი ტერმინები რომლებიც მსოფლიოში აღიარებულია.

2.1. კანონის ისტორია და საერთაშორისო პრაქტიკა

კომპიტერულმა დანაშაულმა პირველად თავი XX საუკუნის 70-იან ლწებში, ამერიკის შეერთებულ შტატებში იჩინა. არა მხოლოდ ნაციონალურ, არამედ საერთაშორისო დონეზეც კი დაიწყოამ ფენომენის გამოკვლევა. მიღებულიიქნა მისი მომწესრიგებელი სპეციალური რომები. 1977 წელს ამერიკისშეერთებულმა შტატებმა შეიმუშავა კანონპროექტი „ფედერალური კომპიუტერული სისტემისდაცვის შესახებ“, რომელიც სისხლისამმართლებრივ პასუხისმგებლობას კომპიუტერულიმოწყობილობის უკანონო გამოყენებისათვის, კომპიუტერულ სისტემაში ცრუ მონაცემების შეყვანისა და კომპიუტერული ტექნოლოგიების და კომპიუტერული ინფორმაციის მეშვეობითფულადი სახსრების მითვისებისათვის აწესებდა. სწორედ ხსენებულიკანონპროექტის საფუძველზე იქნა მიღებული (1984 წლის ოქტომბერში) კანონი „კომპიუტერული თაღლითობის და კომპიუტერისბოროტად გამოყენების შესახებ:. მიუხედავად იმისა, რომ ქმედებაკრიმინალიზეული გახდა და ამერიკელი გამომძიებლებიც წარმატებულად ახერხებდნენ დანაშაულთან გამკლავებას, ეს არ აღმონდა საკმარისი მასთან ბრძოლისათვის და აუცილებელი გახდა ახალი საკანონმდებლო ინიციატივის მომაზდება. 1991 წლის სექტემბერში, იუსტიციის დეპარტამენტის გენერალური სასარჩელო განყოფილებაში შეიქმნა ცალკე განყოფილება უშუალოდ კომპიუტერულ დანაშაულთან ბრძოლისათვის. აღნიშნულ საკანონმდებლო ინიციატივას დადებითად შეხვდა და მხარიც დაუჭირა ამერიკის გენერალური პროკურორის ეკონომიკური დანაშაულის საბჭომ. კომპიუტერულმადანაშაულმა ძალიან მალე მოიცვა მრავალი ძლიერი სახელმწიფო და კომპიუტერული ინფორმაციის სფეროში ჩადენილ დანაშაულებზე სისხლისამმართლებრივი პასუხისმგებლობის საკითხის დაყენების აუცილებლობა დადგა. საკანომდებლო ცვლილებები

[15]უ. ზაქაშვილი, კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, თბ., 2013. გვ. 115

განხორციელდა გერმანიაში (1986 წ.), ჰოლანდიაში (1993 წ.), დიდ ბრიტანეთში (1990 წ.) და კიდევ მრავალ ქვეყანაში. უსაფრთხოების სამსახურებს აქვთ შიში ელექტრონული 11 სექტემბრის განხორციელებისა. სწორედ ამიტომ, გერმანიაში ჯერ კიდევ 2011 წლის აპრილში შეიქმნა კიბერთავდასხმების თავიდან აცილების ეროვნული ცენტრი (NCAZ), რომელიც ფუნქციონირებს, როგორც უსაფრთხოების ორგანოების თანამშრომლობისათვის შექმნილი გაერთიანება საინფორმაციო და საკომუნიკაციო ტექნოლოგიების ინფრასტრუქტურებზე ელექტრონული თავდასხმების თავიდან ასაცილებლად. 2017 წლის აპრილში ფედერაციის თავდაცვის სამინისტრომ კიბერარმიასაც ჩაუყარა საფუძველი, რათა ინფრასტრუქტურები მომავალში უკეთ იქნას დაცული უცხო ქვეყნების ჰაკერული თავდასხმებისაგან და ძალებისაგან. არმიის, საზღვაო ფლოტის და საჰაერო ძალების გვერდით, კიბერარმია შექმნის ახალ შეიარაღებულ დანაყოფს, რომელიც თავდაპირველად 260 ჯარისკაცისაგან შედგება. 2021 წლისათვის საბრძოლო დანაყოფს 13.500 ჯარისკაცი და 1500 სამოქალაქო თანამშრომელი ეყოლება. ამით ასევე გათვალისწინებული იქნება ის ფაქტიც, რომ ნატომ კიბერსივრცე 2016 წლის ივნისში ოპერაციების დამოუკიდებელ სივრცედგამოაცხადა.მასშემდეგ შესაძლებელია ჰაკერულმა თავდასხმებმა ნატოს წევრ ქვეყანაზე ჩრდილოატლანტიკური ხელშეკრულების მე-5 მუხლის ამოქმედება გამოიწვიოს.[16]

[16] Scientific and Practical Cyber Security Journal (SPCSJ) 2(3): 98-107 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)// file:///C:/Users/admin/Downloads/RO2019040265787592K%20(1).pdf

თავი III. თანამედროვე ტექნოლოგიები როგორც კიბერსივრცის იარაღი

ინტერნეტის განვითარება და მისი სწრაფი ზრდა დიდ ზეგავლენას ახდენს მსოფლიო საზოგადოებაზე. განვითარებული, ისევე როგორც განვითარებადი ქვეყნების მოსახლეობა საინფორმაციო საზოგადოებად გარდაიქმნა. პროცესი ხასიათდება საინფორმაციო ყექნოლოგიების მზარდი გამოყენებით ინფორმაციის მიღებისა და მისი განვითარების მიზნით. აღნიშნული პროცესი უამრავ შესაძლებლობებს გვთავაზობს, დაწყებული ინფორმაციის ხელმისაწვდომობიდან, დამთავრებული კონტაქტით ყველა იმ ადამიანტან, ვისაც აქვს ინტერნეტი. მსოფლიო ბევრ რეგიონში, ინფორმაციის ხელმისაწვდომობამ და კომუნიკაციის შესაძლებლობამ გააძლიერა დემოკრატია, ადამიანების უფლებების დაცვა და სამართლებრივი სახელმწიფოს მშენებლობის პროცესი. აღნიშნული შესაძლებლობები ხელსუწყობს საინფორმაციო ტექნოლოგიების მუდმივ და ყოველდღიურ ინტეგრირებას ადამიანებისყოველდღიურ ცხოვრებაში მსოფლიო მასშტაბით. ინტერნეტს უკვე იყენებს მილიარდზე მეტი ადამიანი. ამ რიცხვში შედიან არა მხოლოდ ინდივიდები, არამედ ბიზნესებიც, რომელთაც, ასევე, სარგებელი აქვთ ინტერნეტისა და საინფორმაციო ტექნოლოგიებისგან, რადგან აღნიშნული ხელს უწყობს საქონლისა დამომსახურების შეთავაზებას მსოფლიო მასშტაბით და ნაკლები ფინანსური დანახარჯებით.[17] კომპიუტერული სისტემა და ინტერნეტმომსახურება ადამიანების პირად ცხოვრებაშიც სულ უფრო ხშირად ფიგურირებს. ადამიანები იყენებენ საინფორმაცი ტექნოლოგიებს საკუტარი აზრების განვიატრებისა და გაზიარების მიზნით, აკეთებენ ფილმებს, ინახავენ სურაებს, დოკუმენტებს და ამყარებენ კომუნიკაციას. საინფორმაციო ტექნოლოგიების განვითარებამ არა მხოლოდ კერძო მომხმარებლების და საწარმოების შესაძლებლობებო გააუმჯობესა. არამედ შესაძლებლობაც მისცა დამნაშავეებს, მიზანში ამოიღონ კონკრეტული კომპიუტერი ან მომსახურება. მსგავსი დანაშაული შეიძლება იყოს შეტევა ელექტრონულ-კომერციულ ობიექტებსა და მნიშვნელოვან ინფრასტრუქტურაზე. იგი ასევე, შეიძლება მოიცავდეს კერძო კომპიუტერებიდან ან კომპანიებისმონაცემთა ბაზიდან იდენტობასთან დაკავშირებული ინფორმაციის მოპოვებას. სწორედ ამიტომ, საინფორმაციო ტქნოლოგიების დაცვა, კომპიუტერული მონაცემებისა და სისტემის კონფიდენციალურობის, მთლიანობისა და მასში შეღწევისაგან დაცვა იმავდროულად

[17] მოსამართლეების ტრენინგი ქსელურ დანაშაულში, ტრენინგის სახელმძღვანელო, პროექტი, 2010 წ. გვ.11

ნიშნავს პირადი ცხოვრების, სიტყვის თავისუფლებისა და სხვა ფუნდამენტური უფლებების დაცვას.[18]

ზოგჯერ ინფორმაციულ უსაფრთხოებასა და კიბერ უსაფრთხოებას აიგივებენ და თვლიან თითქოსდა ეს ორი ცნება ანალოგიურია, თუმცა თავიდანვე უნდა აღინიშნოს, რომ ეს ორი ცნება რაღაც მხრივ ფარავს ერთმანეთს, კიბერ უსაფრთხოება სცდება თავად ინფორმაციული უსაფრთხოების საზღვრებს, იგი მოიცავს არა მხოლოდ საინფორმაციო რესურსების დაცვას არამედ სხვა აქტივობებსაც. როგორც ზემოთ აღინიშნა, რიგ შემთხვევებში ინფორმაციულ უსაფრთხოებასა და კიბერ უსაფრთხოებას ურთიერთ ჩანაცვლებად ტერმინებად იყენებენ. თუ ამ ორ ტერმინს ჩავთვლით სინონიმებად, მაშინ კიბერ უსაფრთხოების დასახასიათებლად დასაშვები იქნება თუ გამოვიყენებთ ინფორმაციული უსაფრთხოებისათვის განსაზღვრულ მახასიათებლებს. ამდენად, კიბერ შემთხვევის მაგალითი შეიძლება იყოს ინფორმაციის კონფიდენციალობის, მთლიანობის ან ხელმისაწვდომობის დარღვევა. კიბერ უსაფრთხოების უმრავლესობა დაკავშირებული შეიძლება იყოს მომხმარებელის ან / და ორგანიზაციის საფრთხეებთან. რაც შეეხება, კონკრეტულად კიბერ უსაფრთხოების განმარტებებს, Merriam Webster-ის ლექსიკონში კიბერუსაფრთხოება განსაზღვრულია, როგორც „ღონისძიებები, რომელიც იცავს კომპიუტერს ან კომპიუტერულ სისტემას არასანქცირებული წვდომისა და თავდასხმისაგან“.[19]

კომპიუტერული დანაშაულის რაობის შესახებ მოსაზრებები განსხვავებულია. მთავარი კითხვა აქ გახლავთ ის, არის ეს მხოლოდ კომპიუტერული მონაცემებისა და სისტემის წინააღმდეგ ჩადენილი დანაშაული (ვიწრო გაგება), თუ იგი, ასევე, მოიცავსიმ დანაშაულსაც, რომელიც ჩადენილია კომპიუტერული მონაცემებისა და სისტემის საშუალებით (ფართო გაგება). კომპიუტერული დანაშაულის კონვენციის ავტორებმა ამ ცნებაში ორივე განმარტება შეიტანეს და კომპიუტერული დანაშაული განსაზღვრეს ოთხი ტიპის დანაშაულად

1. კომპიუტერული მონაცემებისა და სისტემის კონფიდენციალურობის, ინტეგრირებულობისა და მასში შეღწევის წინააღმდეგ ჩადენილი დანაშაული.
2. კომპიუტერის საშუალებით ჩადენილი დანაშაული.

[18] მოსამართლეების ტრენინგი ქსელურ დანაშაულში, ტრენინგის სახელმძღვანელო, პროექტი, 2010 წ. გვ.11

[19] მ. მუსელიანი, საინფორმაციო უსაფრხოების ფენომენი 21-ე საუკუნეში-კიბერუსაფრთხოება დამისი განმსაზღვრელი ფაქტორები (ამერიკა საქართველო) გვ.12

3. შინაარსთან დაკავშირებული დანაშაული.
4. ინტელექტუალური საკუთრებისა დამსგავსი უფლებების წინააღმდეგ ჩადენილი დანაშაული.[20]

გარკვეული პერიოდის განმავლობაში, საზოგადოებრივი კეთილდღეობა და ეკონომიკური სტაბილურობა ეყრდნობოდა გადაცემის ქსელების მონაცემებისა და გამოთვლითი მომსახურების გამართულ მუშაობას, რომლის სანდოობის მაჩვენებელი საკმაოდ დიდი იყო. საერთო მოხმარების ინფორმაციული სისტემების ფუნქციონირებაზე დიდი გავლენა აქვს ისეთ ფაქტორებს, როგორებიც არის ინტერნეტზე შეტევა (attack), ფიზიკური ზემოქმედების შედეგად მიყენებული დარღვევები, პროგრამული და აპარატული უზრუნველყოფის მწყობრიდან გამოსვლა, ადამიანის როგორც მომხმარებლის მიერ მუშაობის პროცესში დაშვებული შეცდომები. ჩამოთვლილი ფაქტორები ნათლად აჩვენებს იმ გარემოებას, თუ რამდენად არის დამოკიდებული თანამედროვე საზოგადოება ინფორმაციული სისტემების სტაბილურ მუშაობაზე. მოცემულს ნათლად ასახავს კიბერუსაფრთხოების გერმანული სტრატეგია, კერძოდ: „კიბერსივრცეზე დაშვების უზრუნველყოფა, ასევე ინფორმაციის კონფიდენციალობა და სანდოობა კიბერსივრცეში გახდა ერთერთი მნიშვნელოვანი პრობლემა 21 - ე საუკუნეში. ამიტომ კიბერსივრცის დაცვა ხდება მთავარი ამოცანა სახელმწიფოს, ეკონომიკისა და საზოგადოების, როგორც ქვეყნის, ისე საერთაშორისო დონეზე“.

ევროკომისიის ზოგიერთ შეხვედრაზე არაერთხელ განიხილებოდა და ამჟამადაც აქტიურად განიხილება ქსელისა და ინფორმაციული უსაფრთხოების მნიშვნელობა. ამ მიზნით, ასევე აქტიური განხილვის საგანია ერთიანი ევროპული ინფორმაციული სივრცის შექმნა. [21]

ზემოაღნიშნულიდან გამომდინარე რაც უფრო მეტად ხდება საზოგადოება დამოკიდებული საინფორმაციო ტექნოლოგიებზე, მით მეტად იზრდება მისი დაუცველობა და საფრთხისათვისპასუხის გაცემის საჭიროება. აღნიშნული საფრთხის დასარეგულირებლად საჭირო სტრატეგია გახლავთ კომპიუტერული დანაშაულის წინააღმდეგ შესაბამისი საკანონმდებლო რეგულაციების შემუშავება და მისი განხორციელება. ამ პროცესში დიდია მოსამართლეების როლიც.

[20] მოსამართლეების ტრენინგი ქსელურ დანაშაულში, ტრენინგის სახელმძღვანელო, პროექტი, 2010 წ. გვ.12
[21] ვ. სვანაძე, კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები, კრებული, გვ.40

კომპიუტერიზაციის ნეგატიურ შედეგად შეიძლება ჩავთვალოთ კიბერდანაშაული. კიბერდანაშაული დანაშაულებს შორის დღესდღეობით მეორე ადგილზეა – ნარკოტიკითა და იარაღით ვაჭრობის შემდეგ. იგი გულისხმობს ნებისმიერ დანაშაულს, რომელიც კიბერსივრცეში ხდება. ამგვარ დანაშაულებში შეიძლება მოვიაზროთ სხვების კომპიუტერული სისტემის ხელყოფა, თავდასხმა კიბერ საიტებზე და შემდგომ მათი საშუალებით დეზინფორმაციის გავრცელება, საკრედიტო ბარათებისა და ელექტრონული პროგრამების პაროლების გატეხვა, პერსონალური ან სახელმწიფო დანიშნულების მქონე ინფორმაციის მოპოვება, რედაქტირება, გავრცელება.. ძირითად შემთხვევებში, გამოიყოფა რამდენიმე ისეთი ტიპის დანაშაული რაც კომპიუტერულიმოწყობილობით შეიძლება იქნას ჩადენილი:

კიბერშეურაცხყოფა: ბავშვთა პორნოგრაფიის გავრცელება, ვინმეს შეურაცხყოფა ან დამცირება ელ-ფოსტის ან სხვა მსგავსი საშუალების გამოყენებით. პირის სქესობრივი, რასობრივი, რელიგიური ან სხვა სახის პირადი ცხოვრების შეურაცხყოფა..

კიბერვანდალიზმი: ნებისმიერი ტიპის საინფორმაციო ბაზების დაზიანება/განადგურება. ამის კარგი მაგალითია: კონკურენტი კომპანიების მიერ კორპორაციული კიბერჯაშუშის შეგზავნა მეტოქე დაწესებულებაში, რათა მან მოიპაროს გარკვეული ინფორმაცია, რითაც შეიძლება ქონებრივი ზიანი მიადგენს კომპანიას ან საერთოდ გაკოტრდეს.

კიბერგათეთრება: უკანონოდ მოპოვებული ფულის ინტერნეტ გადარიცხვა, წყაროსა და მიმღების ვინაობის დაფარვის მიზნით. აღნიშნული დანაშაულის თვალსაჩინომაგალითია “BICOIN”-ი.

კიბერქურდობა: ქურდობა ინტერნეტსივრცის დახმარებით.

კიბერტერორიზმი: ამ შემთხვევაში დანაშაული სახეზეა, როდესაც პიროვნება ტეხავს სამთავრობო ან სამხედრო ვებ-გვერდს. ან, თუნდაც ინტერნეტსივრცეში იდეოლოგიურად მოტივირებული ძალადობა მოქალაქეთა წინააღმდეგ.

იმის მიხედვით, თუ ვის ან რის წინააღმდეგ შეიძლება იყოს მიმართული კიბერდანაშაული, 3 კატეგორია გამოიყოფა:

1. პიროვნების წინააღმდეგ მიმართული დანაშაული.
2. საკუთრების წინააღმდეგ მიმართული დანაშაული.

3. სახელმწიფოს წინააღმდეგ მიმართული დანაშაული.[22]

გამომდინარე იქიდან, რომ დროის სვლასთან ერთად იცვლება მოქმედების საშუალებები, კიბერდანაშაული დღესდღეობით ის ხერხია, რომლითაც დამნაშავეებს არ უწევთ ფიზიკური დაპირისპირება სხვებთან. ზოგავენ დროს და ენერგიას და საჭირო ოპერაციებს ინტერნეტის საშუალებით აკეთებენ. დღესდღეობით კიბერდანაშაული, უფრო სწორედ კი, კიბერტერორიზმია ის, რითიც სახელმწიფოები ერთმანეთს ებრძვიან. სამხედრო დაპირისპირების მაგივრად სულ უფრო პოპულარული ხდება ეს ხერხი და იგი თანამედროვე ომის ერთ-ერთ ნაირსახეობადაც შეიძლება, მოვიაზროთ. აქვე გავიხსენოთ 2008 წლის რუსეთ-საქართველოს ომიც, რომელშიც რუსეთმა საქართველოს წინააღმდეგ სამხედრო დაპირისპირების გარდა, ეს ხერხიც გამოიყენა. ყველაფერ ამის შედეგად კი, ქვეყნის ეკონომიკა მნიშვნელოვნად დაზიანდა.[23]

3.1. კომპიუტერი და მისი შემადგენელი ნაწილები, როგორ მუშაობს იგი

კომპიუტერი (ინგლ. computer) - მოწყობილობა, რომლის დაპროგრამების მეშვეობით ხდება არითმეტიკული ან ლოგიკური ოპერაციის ავტომატური შესრულება. ვინაიდან ოპერაციების თანმიმდევრობა შეიძლება შეიცვალოს, კომპიუტერს შეუძლია ერთდროულად რამდენიმე მათგანის შესრულება.

როგორც წესი, კომპიუტერი შედგება სულ ცოტა, ერთი პასუხისმგებელი მოწყობილობისგან, რომელი, პროცესორისგან და კომპიუტერული მეხსიერების რამე სახის ფორმისგან. პროცესორი აწარმოებს არითმეტიკული და ლოგიკური ოპერაციების შესრულებას.მიმდინარეობების და კონტროლის მოწყობილობა ცვლის ოპერაციების თანმიმდევრობას შენახული ინფორმაციის თანახმად. პერიფერიული მოწყობილობებით ხდება ინფორმაციის მოპოვება გარე წყაროდან, შემდეგ კი - ოპერაციების შედეგების შენახვა და შემდგომი მოძიება.

მეორე მსოფლიო ომის პერიოდში საომარი ოპერაციებისთვის გამოიყენებოდა მექანიკური ანალოგური კომპიუტერი. ამ პერიოდში შეიქმნა პირველი ელექტრონული ციფრული კომპიუტერები. თავდაპირველად ასეთი კომპიუტერი დიდი ოთახის ზომის იყო და მოიხმარდა

[22] თ. უგრეხელიძე, კიბერდანაშაული,როგორც XXI საუკუნის გლობალური გამოწვევა, 2019 წ.
[23] თ. უგრეხელიძე, კიბერდანაშაული,როგორც XXI საუკუნის გლობალური გამოწვევა, 2019 წ.

ელექტროენერგიას, რომლის რაოდენობა უდრის დღევანდელი რამდენიმე ასეული პერსონალური კომპიუტერის მიერ მოხმარებულ ენერგიას.[24]

თანამედროვე კომპიუტერები, რომლებიც ეფუძნება ინტეგრირებულ წრედებს, მილიონიდან მილიარდამდე უფრო მეტად უნარიანია, ვიდრე ადრეული მანქანები და იკავებენ მცირე სივრცეს. მარტივი კომპიუტერები თავსდება მობილურ მოწყობილობებში. მობილური კომპიუტერები იკვებება მცირე ზომის ბატარეებით. პერსონალური კომპიუტერები, სხვადასხვა სახით, წარმოადგენენ საინფორმაციო ეპოქის სიმბოლოს და იმას, თუ რას წარმოიდგენენ ადამიანები სიტყვა კომპიუტერის ხსენებისას. თუმცა, რაოდენობით ინტეგრირებული კომპიუტერები უფრო მეტია - ციფრული აუდიო პლეერებიდან საბრძოლო საფრენ ტექნიკამდე და სათამაშოებიდან ინდუსტრიულ რობოტებამდე[25].

მოგეხსენებათ კომპიტერი რთული მექანიზმია, შესაბამისად საინტერესოა ის თუ რა კომპონენტებისაგან შედგება იგი. აქედან გამომოდინარე მივყვეთ დეტალურად და განვიხილოთ თუ რა ნაწილებისგან შედგება იგი.

- **სისტემური პლატა (Motherboard)** - ეს არის კომპიუტერის ძირითადი ნაწილი. ყველა დანაფჩენი კომპონენტი სწორედ მასთან არის მიერთებული. სისტემურიპლატის დანიშნულება არის მათ შორისინფორმაციის გაცვლა. აქმოთავსებულია ძირითადი შემავალ გამავალი სისტემა, რომელიც არის პროგრამა, რომელიც იწყებს მუშაობას კომპიუტერის ჩართვისას. მასთანვეა დაკავშირებული მეხსიერება, პროცესორი, გრაფიკული კარტა, მყარი დისკი, დისკის დრაივერი და სხვა.
- **ელექტროენერგიის წყარო** - ეს კომპონენტი არეგულირებს და ელექტროენერგიას აწოდებს კომპიუტერის სხვადასხვა კომპონენტებს. სტანდარტულად, შემავალ 110 ან 220 ვოლტს გარდაქმნის კომპონენტებისათვის საჭირო ვოლტაჟად. ელექტროენერგიის წყაროობს აქვთ კონკრეტული გამომავალი სიმძლავრეები ვატებში, როგორც წესი სტანდარტულადხდება

[24] In 1946, ENIAC required an estimated 174 kW. By comparison, a modern laptop computer may use around 30 W; nearly six thousand times less. Approximate Desktop & Notebook Power Usage. University of Pennsylvania

[25] Early computers such as Colossus and ENIAC were able to process between 5 and 100 operations per second. A modern "commodity" microprocessor (as of 2007) can process billions of operations per second, and many of these operations are more complicated and useful than early computer operations. Intel Core2 Duo Mobile Processor: Features. Intel Corporation.

350 ვატის მიწოდება. რაც უფრო მეტია კომპონენტები, მით მეტი ენერგია სჭირდება კომპიუტერს.

- **CMOS დაBIOS** - ეს აბრევიატურები ერთმანეთის შემცვლელებად გამოიყენება. შეიძლება ასეც განვიხილოთ: BIOS არის პროგრამა ხოლო CMOS კი კომპონენტი, რომელიც მას ამუშავებს და რომელიც ასრულებს დაბალი დონის ფუნქციებს, ამუშავებს კომპიუტერის საათს, უზრუნველყოფს ინტერფეისს, რომ BIOS-მა შეასრულოს თავისი ფუნქციები. მას ჭირდება ძალზედ ცოტა ელექტროენერგია. BIOS, არის ინტერფეისი, რომელიც საშუალებას აძლევს მომხმარებელს, შეიტანოს ცოტაოდენი ცვლილებები კომპიუტერის სისტემურ პლატაში, მეხსიერებასა და სხვა კომპონენტებში. ერთ-ერთი ყველაზე მნიშვნელოვანი ცვლილება, რაც გაუკეთდა ბაისოსს არის იმ თანამიმდევრობის შეცვლა, რომელსაც კომპიუტერი ეძებს, რომ დაიწყოს ფუნქციონირება. როგორც წესი, კომპიუტერული ექსპერტიზის დროს იყენებს კომპაქტ დისკზე არსებულ პროგრამას და ცვლის ბაიოსს ისე, რომ კომპიუტერმა დაიწყოს კომპაქტ დისკიდან და არა მყარი დისკიდან, რადგან ეს გამოიწვევდა მონაცემების შეცვლას.
- **პლატის გაფართოვებული ბუდე** - კომპიტერის უკანა ნაწილში არსებულიბუდე, სადაც შეგიძლიათ მიუერთოთ ხმის კარტა, ვიდეო კარტა, უკაბელო ადაპტორიდა სხვა.
- **ცენტრალური პროცესორი** - ხშიად ურევენ მას კომპიუტერის ტანში. პროცესორი კომპიუტერის შიდა ნაწილია, რომელიც გარედან არ ჩანს. პირველად გამოიყენეს 1960-იან წლებში. ა970-იანი წლებიდან მისი ზომები კიდევ უფრო შემცირდა, რამაც ხელიშეუწყო კომპიუტერის ზომების შემცირებას. მიუხედავად იმისა, თუ რა სახის არის კომპიუტერი, პროცესორი მუშაობს და ასრლებს უამრავ ინსტრუქციას, რომელიც ცნობილია პროგრამის სახელით. პროცესორების უმეტესობა შეესაბამება, ვონ ნიუმანის არქიტექტურას, რომლის მიხედვითაც პროცესორმა სწრაფად უნდა მიიღოს, გაშიფროს, გაანალიზოს და უკან გაუგზავნოს მონაცემები. მოკლედ იგი არის კომპიუტერის ტვინი.
- **მეხსიერება** - არისმონაცემების ელექტრონული შენახვა, რომელთან შეღწევაც სწრაფად არის შესაძლებელი. ინფორმაციის მიღება იქნებოდა ძალიან ხანგრძლივი პროცესი, ესრომ ხდებოდეს პროცესორის მიერ ინფორმაციის მყარი დისკიდან მიღების გზით. ამიტომ, მონაცემები ინახება დროებით მეხსიერებაში, რაც ინფორმაციის მიღების პროცესს აჩქარებს. ეს მეხსიერება ცნობილია, როგორც რამი. პროცესორიინფორმაციას ითხოვს რამიდან, გადაამუშავებს და აგზავნის უკან. ეს ხდება წამში მილიონჯერ. დროებით მეხსიერების ცოდნა მნიშვნელოვანია ექსპერტიზის დროს მონაცემთა ამოღებისმიზნით, რადგან მისი შენახვა არ ხდება თუ კომპიუტერი დენის წყაროსთან არ არის მიერთებული, რასაც ხშირად

ქონია ადგილი. ამიტომ, ახლა სამართალდამცავი ორგანოები, ცდილობენ მონაცემების რამიდან ამოღებას მანამ, სანამ კომპიუტერს გამორთავენ დენის წყაროდან. ამას ეწოდება „მონაცემების ექსპერტიზა ეთერში/ლაივში“. ეს საქმიანობა სულ უფრო გახშირდა, რადგან შესაძლოა დასაკარგი მონაცემების მოცულობა უფრო დიდია, ვიდრე რამდენიმე წლის წინ ყველაზე დიდი მყარი დისკის შესაძლებლობა იყო.[26]

- **მყარი დისკი** - კომპიუტერს აქვს, სულმცირე, ერთი ან მეტი მყარი დისკი. დიდ კომპიუტერებს ბევრი მყარი დისკი აქვთ.მყარი დისკი ასევე აქვთ, მუსიკალურ ცენტრებს, რაც საშუალებას იძლევა დაიტიოს უამრავი ინფორმაცია. აქედან გამომდინარე ადვილია ინფორმაციის ცაწერა და წაშლა, რაცხელს არ უშლის და არ აფუჭებს თავად დისკს. ინფორმაცია ინახება სექტორებში და ცალკებილიკებში/ტრეკებში. ბილიკები არის კონცენტრულიწრეები, ხოლო სეტორები - ჩანართიამ ბილიკების. მონაცემებიმყარ დისკზეინახება ფაილების სახით, რაც წარმოადგენს ბაიტებისჯგუფს. პროგრამებიც ასევე წარმოადგენს ფაილებს.
- **სიდი/დივიდი/ბლურეიდისკები** - მათ შეუძლიათ სხვადასხვა მოცულობის ინფორმაციის დატევა და როგორც წესი, გამოიყენება მუსიკის, ვიდეოს და სხვა ინფორმაციის გავრცელების მიზნით. დივიდი იგივე ზომისაა რაც სიდი, მაგრამ იტევს შვიდჯერ მეტინფორმაციას. ბრუ რეი დისკი, რომელიც გამოიყენება მაღალი გამოსახულებისმქონე ინფორმაციისათვის დივიდიზე ათჯერ მეტ ინფორმაციას იტევს. მოკლედ, იტევენ უფრომეტ ინფორმაციას ვიდრე ეს შეეძლომყარ დისკებს რამოდენიმე წლის წინ. ისინი ინახავენ ინფორმაციასსხვადასხვა გზით და ამიტომ მათზე შენახული ინფორმაცია უფრო ხანგრძლივია და ნაკლებად არის დამოკიდებული ელექტროენერგიაზე, ვიდრე მყარ დისკზე შენახული ინფორმაცია.[27]
- **იუ-ეს-ბიდამაკავშირებელი** - მას ბევრკომპიუტერზე ნახავთ. იგიკომპიუტერთან აერთებს სხვადასხვა ნაწილებს: მაუსს, პრინტერს, მობილურ ტელეფონს და სხვა. ეს ყველაზე ფართოდ გავრცელებული მეთოდია. ადრე არსებობდამიერთების პარალელური ან სერიული პორტები, რაც პრობლემატური იყომისაერთებელი კომპონენტების

[26] მოსამართლეების ტრენინგი ქსელურ დანაშაულში, ტრენინგის სახელმძღვანელო, პროექტი, 2010 წ. გვ.35

[27] მოსამართლეების ტრენინგი ქსელურ დანაშაულში, ტრენინგის სახელმძღვანელო, პროექტი, 2010 წ. გვ.35

რაოდენობასთან დაკავშირებით. ასევე, ინფორმაციის გადაცემის სიჩქარეც ნაკლები იყო. იუ-ეს-ბი ძალიან მნიშვნელოვანია ციფრული ექსპერტიზის დროს.[28]

3.2. მძლავრი ინტერნეტი ინფორმაციაზე სწრაფი წვდომა თუ მასიური დანაშაულისა და კონტროლის იარაღი

ინტერნეტმა თავისი არსებობა სამოციან წლებში აპრანეტით დაიწყო. მიუხედავად იმისა, რომ ქვემოთმოყვანილი ინფორმაცია არ არის პირდაპირ დაკავშირებული საკითხთან, ის ფაქტი, რომ ინტერნეტი არასოდეს ითვალისწინებდა უსაფთხოებას, ხსნის იმას, თუ რატომუადვილდებოდათ დამნაშავეებს მისი გამოყენება. პირველი პიზიკური კავშირი დამარდა1969 წელს, ოთხ საუნივერსიტეტო კვანძს/ადგილს შორის. პირველიიმეილი გაიგზავნა 1972 წელს. შემდეგ წელს შეიქმნაახალი საკომუნიკაციო პროტოკოლიTCP/IP, რომელიც დღეს ინტერნეტის საფუძველს წარმოადგენს. თავიდან არსებობდა ერთმანეთთან დაუკავშირებელი ქსელები. შემდეგ შემუშავდა პაკეტი, რომელიც ითვალისწინებდა ამ ქსელების დაკავშირებას.

აღნიშნულმა მომავალში გააძლიერა ქსელების დაკავშირება, რაც სწრაფად განვითარდა დასავლეთში და შემდეგ უკვე მთელს მსოფლიოში. დრესაცშესამჩნევია ციფრული ტექნიკისგამოყენების განსხვავებები მეტად და ნაკლებად განვითარებული ქვეყნების მიერ. ამაშ შემდგომ მოყვა ინტერნეტის კომერციალიზაცია და ინტერნეტ პროვაიდერების გამოჩენა 1980-იან წლებში. ამან ხელი შეუწყო ინტერნეტის პოპულარიზაციას რაც კიდევ უფრო გაიზარდა 90-იან წლებში. ინტერნეტს დიდი გავლენა აქვს, როგორც ბიზნესზე, ისე კულტურაზე. დღეისათვის არსებობს იმეილი, სოციალური ქსელები, ფორუმები და სხვა. იგი იზრდება, ვითარდება და აგროვებს სულ უფრომეტ ინფორმაციას და ცოდნას[29].

საბჭოთა კავშირის მიერ გაშვებულმა თანამგზავრმა, 1958 წელს, ტექნოლოგიური ლიდერობის დასაბრუნებლად, ამერიკის შეერთებულ შტატებს შთააგონა შეექმნა მოწინავე პროექტების კვლევის სააგენტო(ADVANCED RECEARCH PROJETS AGENCY), ცნობილი, როგორც ARPA. ARPA -მ, ნახევრად ავტომატური მიწის გარემოს (SEMI AUTOMATIC GROUND ENRVINOMENT (SAGE)) პროგრამის წინსვლიOFFICE), ცნობილი, როგორც IPTO, რომელიც მიერთებული იყო ქვეყნის სარადარო სისტემის ქსელში. J. C. R. LICKLIDER არჩეულ იქნა ITPO-ს მეთაურად.

[28] www. computer.howstuffworks.com/computer-hardware-channel.html.

[29] მოსამართლეების ტრენინგი ქსელურ დანაშაულში, ტრენინგის სახელმძღვანელო, პროექტი, 2010 წ., გვ. 38

LICKLIDER 1950 წელს, ჰარვარდის უნივერსიტეტში არსებული ფსიქო-აკუსტიკური ლაბორატორიიდან გადავიდა, მასაჩუსეტსის ტექნოლოგიის ინსტიტუტში(MIT), რის შემდეგადაც ის დაინტერესდა ინფორმაციული ტექნოლოგიებით. 1957 წელს ის გახდა BOLT BERANEK and Newman(BBN)-ის ვიცე-პრეზიდენტი. სადაც მან შეიძინა PDP-1 კომპიუტერის პირველი პროდუქცია და გაუძღვა, მრავალ მომხმარებელს შორის რესურსების გამოთვლის განაწილების(Time-Sharing) დემონსტრაციას.

IPTO-ში, Lიცკლიდერ -მა ქსელის განვითარების პროექტის მეთაურობა გადააბარა Lawrence Roberts-ს. ამის შემდეგ რობერტსი დაეყრდნო Paul Baranis-ის ტექნოლოგის, რომელმაც ამერიკის საჰაერო ძალებისთვის(U.S. A. FORCE) დაწერა ამომწურავი ინფორმაციის მქონე წიგნი, რომელსაც რეკომენდაციას უწევდა Packet Switching. ხანგრძილი მუშაობის შემდეგ, Menlo Park-ში, კალიფორნიაში, 29 ოქტომბერს, 1969 წელს, შეერთდა პირველი კვანძი, რომელიც ცნობილია, როგორც ARPANET, კალიფორნიის უნივერსიტეტსა და სტენფორდის კვლევით ინსტიტუტს შორის. ARPANET გახდა დღევანდელი ინტერნეტის ერთ-ერთი "მშობელი". დემონსტრაციის მიხედვით, რომელსაც აწარმოებდა Packet Switching, British Post Office, Telenet, DATAPAC da TRANSPAC ითანამშრომლეს, რათა შეექმნათ პირველი საერთაშორისო Packet-Switching ქსელის სერვისი. გაერთიანებულ სამეფოში 1978 წელს, ეს პროექტი ცნობილი იყო, როგორც საერთაშორისო პაკეტის დინების სერვისი(International Packet Stream Service (IPSS)). X.25 კოლექციის ბაზირებული ქსელი გაიზარდა ევროპიდან და ამერიკიდან, კანადაში, ჰონგ კონგში და ავსტრალიაში. X.25 პაკეტის სტანდარტი შეიქმნა ჩჩIთთ-ში 1976 წელს(ახლა მას ქვია საერთაშორის ტელეკომუნიკაციების კავშირი(ITU-T)). X.25 იყო დამოუკიდებელი TCP/IP პროტოკოლი, რომელიც შეიქმნა 1974 წლის, დეკემბრის დაცვის მოწინავე პროექტების კვლევის სააგენტოს(Defense Advanced Research Projects Agency(DARPA)) მიერ წარმოებულ APANET, Packet Radio Net da Packet Satellite Net-ზე ექსპერიმენტის შედეგად. Vinton Cerf da Robert Kahn-მა 1973 წელს შექმნეს TCP პროტოკოლის პირველი განსაზღვრება, რომელიცს გამოქვეყნდა 1974 წლის მაისში. TCP-ს პირველი სრული სპეციფიკაცია დაიწერა Vinton Cerf, Yogen Dalal da Carl Sunshin-ის მიერ, შემდეგ კი სტენფორდის უნივერსიტეტში. შემდეგი ცხრა წლის განმავლობაში, მუშაობა მიმდინარეობდა პროტოკოლების გაუმჯობესებასა და მათ გამოყენებაზე ოპერაციული სისტემების ქსელის რანგში.

პირველი TCP/IP ფართო მასშტაბის ქსელი შექიმნა 1983 წლის, 1 იანვარს, როდესაც ARPANET-ში არსებული ყველა ჰოსტი ძველი NCP პროტოკოლიდან შეერთდა ახალ TCP/IP პროტოკოლში. David L. Mills-ის ინვესტიციით, 1985 წელს, ამერიკის შეერთებული შტატების ნაციონალური მეცნიერების

ორგანიზაციამ(National Science Foundation (NSF)) შექმნა 56 კილობიტი/წამში სიჩქარის მქონე ქსელი, რომელსაც იყენებდნენ კომპიუტერები სახელად "ფუზზბალლს". მიმდინარე წელში NშF-მა დაასპონსორა მაღალ სიჩქარიანი 1.5 მეგაბიტი/წამში სიჩქარის ქსელი, რომელიც შემდგომ გახდა NSFNET. [30]

ინტერნეტი შეიძლება განვიხილოთ, როგორც ინფრასთრუქტურა, რომელიც ერთდროულად ბევრი მიზნით გამოიყენება. თუ ინტერნეტის ერთი ნაწილი არ მუშაობს, კომუნიკაცია მაინც გრძელდება. ინტერნეტს არავინ ფლობს. იგი თვითრეგულირებადია. ყველაზე თანამედროვე ქსელები, განსაზღვრულია, როგორც „კავშირგარეშე“ ანუ „პაკეტური ჩართვა“. ინტერნეტ ტრაფიკი იყოფა პატარა პაკეტებად, რომლებიც მოძრაობენ გამგზავნსა და მიმღებს შორის. ისინი არ მოძრაობენ ერთი მარშრუტით და კვლავ ერთდებიან, როცა მიაღწევენ დანიშნულების ადგილს.

ადამიანები ინტერნეტში შედიან პროვაიდერების საშუალებით. ესენი არიანკომერციული ორგანიზაციები, რომლებიც ქირაობენ სივრცეს. ისინი აწარმოებენ აღრიცხვას, მაგრამ რამდენი ხნით? არსებობს ეროვნული და საერთაშორისო მონაცემთა დაცვისა და კონფიდენციალურობის საკითხები, რომლებიც უკავშირდება ინფორმაციის შენახვის ვადებს. ეს რა თქმა უნდა, პირდაპირ კავშირშია ციფრული ინფორმაციის მოპოვებასთან. კავშირი ინტერნეტთან ხორციელდება Dial Up, Broadband, ISDN, საკაბელო, უკაბელო და სატელიტის გზით.

ინტერნეტის არსისი გასაგებად მშვენიერი ფილმია ქსელური მეომრები. იგი კარგად უხსნის ინტერნეტის რაობას მათ, ვინც ეს არ იცის. ფილმი 12 წუთიანია და ეხება ინტერნეტის რაობას და მის სტრუქტურას, ტრანსატლანტიკური კაბელების ჩართვით. შესაძლებელია მისი ჩამოტვირთვა: www.warriorsofthe.net გერმანულ, ინგლისურ, ესპანურ, ებრაულ და სხვა ენებზე. რეკომენდირებულია სტატისტიკური ინფორმაციის მიწოდება მსმენელებისათვის, რაც უზრუნველყოფს მათ ქვეყანაზე გავლენის გააზრებას.

აქვე მოგვყავს რამდენიმე ტერმინი, დაკავშირებული ქსელებთან და ინტერნეტთან:

- Network Internet Card - პლატა, ან კარტა, რომელიც ჯდება კომპიუტერში ინტერნეტთან კავშირის დამყარების მიზნით.
- MAC address - კვაზი-უნიკალური იდენტიფიკატორი ქსელების ადაპტირებისათვის იდენტიფიკაციის მიზნით.

[30] https://sites.google.com/site/chemiproekti/internetis-ganvitarebis-istoria

- Network Hub - ანუ კონცენტრატორი, რომელიც აერთებს ოპტიკო ბოჭკოვან ეთერნეტის მოწყობილობებს და ხელს უწყობს მათ ფუნქციონირებას, როგორც ერთი ქსელისას. ჰაბები მუშაობს ფიზიკურ შრეზე ტერმინი „შრე 1 ჩართვა“ არის ჰაბის სინონიმი. ამგვარად ეს ხელსაწყო არის მრავალპორტიანი რეპეტორი. ქსელების ჰაბები, ასევე, გადასცემენ გადატვირთვის სიგნალს ყველა პორტს.[31]
- Network Switch - ქსელის მოწყობილობა რომელიც აკავშირებს ქსელის სეგმენტებს. წარსულში გამოიყენებოდა შრე 2, რაც უფრო სწრაფი იყო. შემდეგში, იგივე იგივე სისწრაფით ხდებოდა ძებნა IP და MAC მისამართებზე.[32]

სერ ტიმოთი ბერნერს-ლი (ინგლ. Tim Berners-Lee; დ. 8 ივნისი, 1955, ლონდონი) — ინგლისელი კომპიუტერული მეცნიერი, რომელმაც გამოიგონა ინტერნეტ-რესურსების ადრესაციის სისტემა. იგი არის შესული ცოცხალ 100 ყველაზე გენიოს ადამიანს შორის. ბერნერს-ლი დღესდღეობით არის World Wide Web Consortium-ის (W3C) დირექტორი, რომელიც ადევნებს თვალს World Wide Web-ის განვითარებას.[33]

World Wide Web დაიბადა 1991 წელს, როცა ტიმ ბერნლელ-ლიმ გამოიგონა ჰიპერტექსტური ენა HTML, რაც საშუალებას იძლეოდა გაერთიანებულიყო სიტყვები, სურათები და ბგერები. სტანდარტები შეიმუშავა World Wide Web კონსორციუმმა. WWWშედგება დოკუმენტებისაგან, რომლებიც ერთმანეთს ლინკებით უკავშირდებიან, რაც ობობას ქსელს წააგავს. ამიტომაც ეწოდება ვები-ქსელი.

ბრაუზერის სასუალებით შედიხართ ვებში:ინტერნეტ ექსპლორერი, მოზილა ფაიერფოქსი, გუგლი, საფარა, და ოპერა. HTML ის ენაა, რომელსაც კავშირის მიზნით იყენებენ ბრაუზერები და მომცახურებები. მიუხედავად იმის არომ ბრაუზერის საშუალებით ხდება ბევრ პროტოკოლში შესვლა, HTTP ყველაზე ხშირად გამოყენებადი პროტოკოლია. ბევრი ფიქრობს, რომ WWW არის ინტერნეტი. ამასვე იყენებენ კრიმინალები[34].

გლობალურ ქსელს - ინტერნეტს ბევრ სიკეთესთან ერთად გააჩნია უარყოფითი მხარეები, რომლებსაც ინტერნეტ მომხმარებლები ნაკლებ ყურადღებას უთმობენ. თუმცა ინტერნეტ

[31] მოსამართლეების ტრენინგი ქსელურ დანაშაულში, ტრენინგის სახელმძღვანელო, პროექტი, 2010 წ. გვ.38
[32] მოსამართლეების ტრენინგი ქსელურ დანაშაულში, ტრენინგის სახელმძღვანელო, პროექტი, 2010 წ. გვ.39
[33] Quittner, Joshua. “Tim Berners Lee—Time 100 People of the Century“, Time Magazine, 29 March 1999. „He wove the World Wide Web and created a mass medium for the 21st century. The World Wide Web is Berners-Lee's alone. He designed it. He loosed it on the world. And he more than anyone else has fought to keep it open, nonproprietary and free“
[34] მოსამართლეების ტრენინგი ქსელურ დანაშაულში, ტრენინგის სახელმძღვანელო, პროექტი, 2010 წ. გვ.40

საფრთხეებს შეუძლია სერიოზული ზიანი მიაყენოს როგორც კონკრეტულ პიროვნებას, ასევე ადამიანთა ჯგუფს, ორგანიზაციას, დაწესებულებას ან მთლიანად ქვეყანას.

ინტერნეტის დადებითი მხარეებია:

1. **ახალი ტიპის კომუნიკაცია.** ადამიანები კომუნიკაციისათვის ყოველთვის იყენებდნენ სხვადასხვა საშუალებებს, როგორებიცაა ზეპირი გადაცემა, წერილობითი სახის ინფორმაციის მიმოცვლა, ფოსტა, სატელეფონი კავშირი, ტელეგრაფი და ა.შ. ინტერნეტის შექმნამ საგრძნობლად გაამარტივა კომუნიკაცია. ისეთი სერვისები როგორებიცაა ელექტრონული ფოსტა, ხმოვანი და ვიდეო კავშირი რეალურ დროში, სწრაფი მესიჯების სისტემები, სოციალური ქსელები - ადამიანს საშუალებას აძლევს დროის უმოკლეს მონაკვეთში მიიღოს ან გაცვალოს სხვადასხვა სახის ინფორმაცია მეგობრებთან, ოჯახის წევრებთან, ბიზნეს პარტნიორებთან - დაამყაროს კომუნიკაცია მისთვის მოსახერხებელი ფორმით, სასურველ დროს და რაც მთავარია მსოფლიოს ნებისმიერი წერტილიდან.
2. **ინფორმაციის წყარო.** ინტერნეტის ერთერთი ყველაზე მნიშვნელოვანი თვისებაა უამრავი სახის ინფორმაციის არსებობა ერთ სივრცეში. მომხამარებელს შეუძლია მოიძიოს თითქმის ნებისმიერი თემის, შინაარსის ინფორმაცია სხვადასხვა ენაზე, მათი გამოქვეყნების თარიღის, ავტორის, ორგანიზაციის და სხვა მრავალი პარამეტრის მიხედვით. რასაკვირველია ინფორმაციის სანდოობა და საიმედოობა განისაზღვრება იმით, თუ რომელი წყაროა მისი შემქმნელი და განმათავსებელი ინტერნეტ სივრცეში.
3. **ონლაინ ბანკინგი.** ინტერნეტი საგრძნობლად ამარტივებს საბანკო-საფინანსო საქმიანობას. ინტერნეტმომხმარებელს სახლიდან გაუსვლელად, ნებისმიერ დროს შეუძლია ისეთი ოპერაციების ჩატარება როგორიცაა: ონლაინ კომერცია, ფულადი გადარიცხვები, ინტერნეტ-მაღაზიებში ვაჭრობა, კომუნალური გადასახადების დაფარვა, ანგარიშების მართვა და ა.შ. სპეციალური საიტები ინტერნეტ მომხმარებელს უმარტივებს ყოველდღიურ საქმიანობას და სხვადასხვა სახის მომსახურეობას სთავაზობს. შეკვეთები და გადაზიდვები, საკონცერტო თუ სატრანსპორტო ბილეთების, სასტუმროების დაჯავშნა, ჟურნალ-გაზეთების გამოწერა და ა.შ.
4. **ონლაინ ტრენინგები, სემინარები, უნივერსიტეტები.** ინტერნეტში განთავსებულია მრავალი საგანმანათლებლო დაწესებულების რესურსები. ნებისმიერ მსურველს შეუძლია გაიაროს ონლაინ ტრენინგები, დაესწროს სემინარებს, მოიძიოს და გადმოწეროს საკუთარ კომპიუტერში სხვადასხვა სასწავლო მასალა შემდგომი გამოყენებისათვის. მრავალ

უნივერსიტეტს შექმნილი აქვს ონლაინ სწავლის, დისტანციური განათლების სისტემები, ისე რომ ინტერნეტ მომხმარებელს შესაძლებლობა ეძლევა ნებისმიერი ქვეყნიდან, სახლიდან გაუსვლელად გაიაროს მისთვის სასურველი კურსი და მოიპოვოს შესამაბისი ატესტატი, სერტიფიკატი ან უნივერსიტეტის ხარისხი.[35]

5. **კომუნიკაციები, ფორუმები, ბლოგები.** საერთო ინტერესის მქონე ინტერნეტ მომხმარებლები ქმნიან ე.წ. საზოგადოებებს ქომუნითიებს, ფორუმებს, სადაც მიმდინარეობს ინტერესის სფეროს მიხედვით სხვადასხვა აქტუალური თემის განხილვა. შესაძლებელია ინფორმაციის მიმოცვლა, აზრის დაფიქსირება, დისკუსიები ნებისმიერ საკითხზე. ფორუმებზე იქმნება თემები და კატეგორიები, შესაბამისად ინტერნეტ მომხმარებელმა ზუსტად იცის სად უნდა მოიძიოს მისთვის საინტერესო ინფორმაცია, დაინტერესებულ და კომპეტენტურ ადამიანთა ჯგუფი ან უბრალოდ გაეცნოს სხვა ადამიანთა აზრს კონკრეტულ საკითხთან დაკავშირებით. ბლოგი - პერსონალური საიტია. ნებისმიერ მსურველს შეუძლია შექმნას საკუთარი ბლოგი და ნებისმიერ თემაზე გამოაქვეყნოს თავისი შეხედულება, ნააზრევი, ნაშრომი ან უბრალოდ საინტერესო ინფორმაცია. საინტერესო ადამიანების მიერ მნიშვნელოვან თემებზე შექმნილი ბლოგები, განსაკუთრებული ყურადღებით სარგებლობს და ვიზიტორების დიდი რაოდენობით გამოირჩევა.
6. **გართობა.** ინტერნეტ სივრცეში არსებობს უამრავი ვებ გვერდი და რესურსი, რომელსაც ინტერნეტ მომხმარებელი, შეიძლება ეწვიოს უბრალოდ დროის სახალისოდ გატარების ან გართობის მიზნით. სხვადასხვა ჟანრის თამაშები ნებისმიერი ასაკის და ინტერესის ადამიანისთვის, ასევე ვიდეო და აუდიო პორტალები, ფილმები, გასართობი საიტები, ინტერნეტ მომხმარებელს გართობის და დროის საინტერესოდ გატარების უდიდეს არჩევანს სთავაზობს.

ინტერნეტის უარყოფითი მხარეები, საფრთხეები:

1. **პერსონალური მონაცემები, პრივატულობის დაცვა.** ინტერნეტის გამოყენებისას მომხმარებელი ზოგიერთ საიტზე განათავსებს პირად მონაცემებს: სახელი, გვარი, მისამართი, ტელეფონის ნომრები, ინტერესის სფეროები, მეგობართა წრე, ფოტოები და ა.შ. ასევე ონლაინ შესყიდვების დროს პირადი ინფორმაცია საბანკო ბარათების და საიდუმლო სიტყვის, პაროლების შესახებ გადაეცემა ინტერნეტ-მაღაზიების საიტებს. ეს ინფორმაცია

[35] ინტერნეტის დადებითი და უარყოფითი მხარეები - http://elearning.grena.ge/pluginfile.php/901/mod_resource/content/2/chapter1.pdf

შეიძლება მოიპოვოს არაკეთილმოსურნე პიროვნებამ რომელიც შემდგომ აღნიშნულ ინფორმაციას გამოიყენებს ბოროტი მიზნებით: ფინანსების ხელში ჩაგდება, შანტაჟი, უცხო პიროვნების რეკვიზიტებით ინტერნეტ თაღლითობის ან სხვა ტიპის კიბერდანაშაულის ჩადენა. ამიტომ საჭიროა ინტერნეტ მომხმარებელი სიფრთხილით მოეკიდოს საკუთარი პრივატულობის დაცვას და პირადი ინფორმაცია მხოლოდ სანდო და სერიოზული რეპუტაციის მქონე საიტებს ანდოს ან მაქსიმალურად შეზღუდოს ასეთი ინფორმაციის გასაჯაროება. ზოგ შემთხვევებში ინტერნეტში თუნდაც პრივატულად განთავსებული ინფორმაცია, შესაძლებელია ხელში ჩაიგდოს სხვა, მესამე პირმა, არასანქცირებული წვდომის მოპოვების (Hacking) ან კიბერდანაშაულის სხვადასხვა მეთოდების გამოყენების გზით.[36]

2. **არასანქცირებული მონიტორინგი.** ვინაიდან ინტერნეტი, ისევე როგორც მობილური და რადიო კავშირგაბმულობა სხვადასხვა ტექნიკური საშუალებებით იმართება, შესაძლებელია ინტერნეტ აქტივობის მონიტორინგი, ჩაწერა, გაანალიზება, როგორც საჭირო და აუცილებელი, ასევე არასასურველი ბოროტი მიზნებით. იმისათვის რომ ინტერნეტ მომხმარებლის კომუნიკაცია და აქტივობა მაქსიმალურად პრივატული იყოს, საჭიროა ინტერნეტ მომხმარებელმა დაიცვას ინტერნეტ უსაფრთხოების ნორმები, წესები და შეძლებისდაგვარად გამოიყენოს უსაფრთხო კავშირის საშუალებები და ინტერნეტ გადაწყვეტილებები. მაგ: Antivirus, Firewall პროდუქტები, სანდო და მაღალი რეპუტაციის მქონე პროგრამების და საიტების გამოყენება, პაროლით დაცული უსაფრთხო კავშირის პროტოკოლები და ა.შ.
3. **ფინანსური ზიანი.** მრავალი ქვეყნის და ორგანიზაციის მუშაობაში განსაკუთრებული ადგილი უკავია კომპიუტერულ სისტემების და ინტერნეტის გამოყენებას, შესაბამისად მათი მუშაობის შეფერხება ან რაიმე სახის დაზიანება, სერიოზულად იმოქმედებს ნებისმიერ პროცესზე, რასაც აღნიშნული ორგანიზაცია, კომპანია თუ სახელმწიფო სტრუქტურა ახორციელებს. აღწერილია მრავალი შემთხვევა როდესაც კომპიუტერული სისტემების დაზიანებამ, სერიოზული ეკონომიკური ზიანი და ზოგჯერ მუშაობის სრული შეფერხება გამოიწვია.
4. **ინფრასტრუქტურების დაზიანება.** ინტერნეტი და კომპიუტერული სისტემები გამოიყენება მრავალი ინფრასტრუქტურის სამართავად. სამხედრო და სატელიტური სისტემები,

[36] ინტერნეტის დადებითი და უარყოფითი მხარეები - http://elearning.grena.ge/pluginfile.php/901/mod_resource/content/2/chapter1.pdf გვ.4

კომუნიკაციის არხები, წყლის, გაზის, ელექტრო და ატომური ენერგიის, ნავთობ მომპოვებელი და გადამამუშავებელი ინფრასტრუქტურის ელემენტები. რომელიმე მათგანის დაზიანება ან მწყობრიდან გამოსვლა სერიოზული ზიანის მომტანია როგორც კომპანიის ასევე სახელმწიფოსათვის. 2010-2012 წლის განმავლობაში დაფიქსირდა მრავალი შემთხვევა, როდესაც ინტერნეტის და კომპიუტერული ვირუსების გამოყენებით მიზანმიმართულად დაზიანდა სხვადასხვა ქვეყნის და კომპანიის კრიტიკული, მნიშვნელოვანი ინფრასტრუქტურა.

5. **მავნე კოდი, ვირუსები.** ინტერნეტში გავრცელებულია მილიონობით ვირუსული, მავნე კოდი, რომელიც შექმნილია კომპიუტერული სისტემების დასაზიანებლად. არსებობს მრავალი ფუნქციის მქონე ვირუსი: ზოგიერთ ვირუსს შეუძლია კომპიუტერის მართვა და არასანქცირებული მონიტორინგი, თვალთვალი ინტერნეტ მომხმარებლის საქმიანობაზე, ასევე საიდუმლო დოკუმენტაციის, ფინანსური მასალების, საბანკო ბარათების ინფორმაციის ხელში ჩაგდება და გადაგზავნა ვირუსის ავტორისთვის, სხვადასხვა კრიტიკული ინფორმაციული სისტემების წინააღმდეგ ინტერნეტ მომხარებლის კომპიუტერიდან შეტევის განხორციელება. ვირუსები ვრცელდება ელექტრონული ფოსტით (Spam, Phishing), ასევე USB მოწყობილობებით, დისკებით, სხვადასხვა საიტზე განთავსებული უფასო პროგრამული პროდუქტების სახით და ა.შ.[37]
6. **არასასურველი შინაარსი.** ინტერნეტში, მრავალ საინტერესო და მნიშვნელოვან საიტთან ერთად, განთავსებულია არასასურველი შინაარსის მქონე საიტები. ზოგიერთ მათგანზე აქვეყნებენ კომპრომატებს, ორგანიზაციის ან პიროვნების დამამცირებელ განცხადებებს და მასალებს. ასევე მრავლადაა პორნოგრაფიული, რასიზმის და ძალადობის შინაარსის მქონე საიტები. სასურველია ინტერნეტ მომხმარებელმა მაქსიმალური სიფრთხილე გამოიჩინოს და არ ეწვიოს მსგავსი შინაარსის საიტებს. მრავალი მათგანი გამოიყენება ინტერნეტ შეტევებისთვის და ვიზიტორების ვირუსული პროგრამებით დასაინფიცირებლად. მნიშვნელოვანია სპეციალური პროგრამების გამოყენება, რომლებიც ყოველდღიურად ქმნიან „ცუდი რეპუტაციის“ საიტების სიას, ბლოკავენ მასზე შესვლის და მონახულების მცდელობებს და ამ გზით იცავენ ინტერნეტ მომხმარებელს.[38]

[37] ინტერნეტის დადებითი და უარყოფითი მხარეები - http://elearning.grena.ge/pluginfile.php/901/mod_resource/content/2/chapter1.pdf

[38] ინტერნეტის დადებითი და უარყოფითი მხარეები - http://elearning.grena.ge/pluginfile.php/901/mod_resource/content/2/chapter1.pdf

თავი IV. კიბერდანაშაულის სისხლისსამართლებრივი დახასიათება და საერთაშორისო სტანდარტები

კიბერდანაშაული 21-ე საუკუნის ერთ-ერთი მთავარი გამოწვევაა და მისი მასშტაბების გათვალისწინებით, განსაკუთრებულ მიდგომას საჭიროებს. ეს, თავის მხრივ, სახელმწიფო, კერძო თუ არასამთავრობო სექტორებს შორის აქტიურ თანამშრომლობას მოითხოვს. ამ მიმართულებით მნიშვნელოვანია სწორი სახელმწიფო პოლიტიკის გატარება, რასაც თან უნდა ერთვოდეს სწორი კრიმინალური პოლიტიკის არსებობა. რაც საგრძნობლად შეამცირებს კიბერდანაშაულით გამოწვეულ ეკონომიკური, პოლიტიკური და სოციალური ხასიათის საფრთხეებს და შექმნის მეტად უსაფრთხო გარემოს სახელმწიფოებრივი და საზოგადოებრივი განვითარებისათვის.

იმისათვის, რომ ქვეყანაში დანაშაული შემცირდეს საჭიროა სწორი კრიმინალური პოლიტიკის არსებობა. აღნიშნული პოლიტიკა საკუთარ თავში არ უნდა გულისხმობდეს და მოიცავდეს მხოლოდ რეპრესიული ქმედებების განხორციელებას. იგი საკუთარ თავში უნდა მოიაზრებდეს სისხლის სამართლებრივი სასჯელის გარდა სხვა პრევენციული ღონისძიებების განხორციელებასაც.[39] ამასთანავე უნდა ღინიშნოს ისიც, რომ კრიმინოლოგია როგორ მეცნიერება მნიშვნელოვან როლს თამაშობს ქვეყნის კრიმინალური პოლიტიკის ჩამოყალიბებაში. იმდენად რამდენადაც კრიმინოლოგია იკვლევს დანაშაულს და მის გამომწვევ მიზეზებს, საუკეთესო გარანტიაა იმისა, რომ არსებული ვითარების, მდგომარეობის, რაციონალური და ჯეროვანი შეფასება მოხდეს, რაც ჩემი აზრით მნიშვნელოვანია იმ არსისა და მორალისთვის რასაც დანაშაულის პრევენცია ეწოდება.

2008 წლიდან მოყოლებული, დაიწყო კონკრეტული ნაბიჯების გადადგმა კიბერდანაშაულის წინააღმდეგ ბრძოლის კუთხით. 2012 წლიდან მოქმედებს ,,საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ“. საქართველოს მიერ რატიფიცირებულია ევროპის საბჭოს კონვენცია „კიბერდანაშაულის შესახებ“. სრულად განახლდა სისხლის სამართლის კოდექსის XXXV თავი. ცვლილებები შეეხო საპროცესო კანონმდებლობასაც. დაემატა სპეციფიური საგამოძიებო მოქმედებები, კერძოდ, სსსკ-ის XVI თავი კომპიუტერულ მონაცემთან დაკავშირებული საგამოძიებო მოქმედებები, ტერმინთა განმარტება და სხვა. **შემოღებულ იქნა იურიდიული პირის სისხლისსამართლებრივი პასუხისმგებლობა კიბერდანაშაულის ჩადენისათვის.** დაიხვეწა ინტელექტუალური საკუთრების შესახებ მუხლი (საავტორო, მომიჯნავე უფლების მფლობელისა და მონაცემთა ბაზის დამამზადებლის უფლების ხელყოფა). დაიხვეწა ბავშვთა პორნოგრაფიის

[39] მ. შალიკაშვილი, კრიმინოლოგია, II გამოცემა, თბ., 2011, გვ. 45

მუხლი. ცვლილებები შევიდა ასევე საქართველოს კანონებში „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ და „ელექტრონული კომუნიკაციების შესახებ.“ ასევე შეიქმნა კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი (CERT)[40], რომელიც უფლებამოსილია, განახორციელოს კიბერსივრცის მონიტორინგი, კომპიუტერული ინციდენტების გამოვლენისა და მართვის მიზნით, განსაზღვროს და გაატაროს კიბერუსაფრთხოების პოლიტიკა, ასევე განახორციელოს საქართველოს კანონმდებლობით მინიჭებული სხვა უფლებები. კიბერდანაშაულის წინააღმდეგ ბრძოლა შინაგან საქმეთა სამინისტროს კომპეტენციას წარმოადგენს. ცენტრალური კრიმინალური პოლიციის დეპარტამენტში შექმნილია კიბერდანაშაულის წინააღმდეგ ბრძოლის სამმართველო, რომელიც მოიცავს კიბერდანაშაულის საერთაშორისო საკონტაქტო პუნქტს 24/7. შსს-ში ასევე ფუნქციონირებს საექსპერტო-კრიმინალისტიკური მთავარი სამმართველოს კომპიუტერულ-ციფრული ექსპერტიზის ქვეგანყოფილება, რომელიც ახორციელებს საგამოძიებო მოქმედებების შედეგად მიღებული ციფრული მტკიცებულებების ექსპერტიზას.

კიბერდამნაშავეები არამარტო აზიანებენ კრიტიკულ ინფორმაციულ სისტემებს, აგრეთვე იყენებენ კიბერსივრცეს სხვადასხვა დანაშაულის ჩასადენად. კიბერდანაშაულის წინააღმდეგ ბრძოლის ეფექტიანობის მიზნით, აუცილებელია საინფორმაციო კამპანიების წარმოება (სოციალური ქსელები, შესაბამისი უწყებების ვებგვერდები და სხვა) კიბერდანაშაულისა და მისგან გამოწვეული ზიანის შესახებ. ასევე მნიშვნელოვანია აღნიშნულის შესახებ სკოლებში სამართალდამცავი უწყებებისა და განათლებისა და მეცნიერების სამინისტროს წარმომადგენელთა მიერ მოსწავლეების ინფორმირება. საზოგადოებამ უნდა იცოდეს, თუ როგორ დაიცვას თავი კიბერდანაშაულისგან, უნდა გააჩნდეს ინფორმაცია პოტენციური საფრთხეების, მათი იდენტიფიცირებისა და მათზე რეაგირების შესახებ.[41]

ჩემს თემაში არა ერთხელ იქნა აღნიშნული, რომ საქართველოში კიბერდანაშაულის დასჯადობის საკითხებს არეგულირებს სისხლის სამართლის კოდექსის (სსკ) XXXV თავი, რომლის თანახმადაც, სისხლის სამართლის პასუხისმგებლობას იწვევს კიბერსივრცეში ჩადენილი შემდეგი ქმედებები: კომპიუტერულ სისტემაში უნებართვო შეღწევა, კომპიუტერული მონაცემის ან/და

[40] CERT.GOV.GE საქართველოს იუსტიციის სამინისტროს მონაცემთა გაცვლის სააგენტოს ფარგლებში ფუნქციონირებს. CERT.GOV.GE-ს პასუხიმგებლობაა რეაგირება მოახდინოს საქართველოს სამთავრობო ქსელში და კრიტიკულ ინფრასტრუქტურაში დაფიქსირებულ კომპიუტერულ ინციდენტებზე. CERT.GOV.GE-მ ოპერირება დაიწყო 2011 წ. იანვარში. ვინაიდან ამ ეტაპზე საქართველოში არ ფუნქციონირებს ნაციონალური კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი, CERT.GOV.GE ქვეყანაში მომხდარ ყველა კრიტიკულ კომპიუტერულ ინციდენტს იკვლევს. CERT.GOV.GE-ს მთავარი მისიაა ქვეყანაში მომხდარ კომპიუტერულ ინციდენტებზე სწრაფი რეაგირების მოხდენა, მათი გაანალიზება და რეკომენდაციების გაცემა.

[41] http://police.ge/ GEO

კომპიუტერული სისტემის უკანონოდ გამოყენება და კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა.

კიბერდანაშაულთან დაკავშირებით მნიშვნელოვანია დადებითად შეფასდეს საქართველოს მიერ გატარებული შემდეგი საკანონმდებლო რეგულაციები:

- მიღებულ იქნა კანონი „ინფორმაციული უსაფრთხოების შესახებ“, რომელიც აწესებს ინფორმაციული უსაფრთხოების ზოგად სტანდარტებს საჯარო და კერძო სექტორისთვის.
- შინაგან საქმეთა სამინისტროს ცენტრალური კრიმინალური პოლიციის დეპარტამენტში შეიქმნა კიბერდანაშაულთან ბრძოლის სამმართველო, რომელსაც ევალება კიბერ სივრცეში ჩადენილი მართლსაწინააღმდეგო ქმედებების გამოვლენა, აღკვეთა და პრევენცია.
- შსს საექსპერტო-კრიმინალისტიკური მთავარი სამმართველოს შემადგენლობაში ჩამოყალიბდა კომპიუტერულ-ციფრული ექსპერტიზის ქვეგანყოფილება.
- საქართველოს კიბერ უსაფრთხოების სტრატეგია 2013-2015 წარმოადგენს კიბერ უსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელ მთავარ დოკუმენტს.
- შემუშავდა სტანდარტული ოპერაციული პროცედურები ციფრული მტკიცებულებების პირველადი მოპყრობის შესახებ. დოკუმენტები განსაზღვრავს იმ პროგრამულ უზრუნველყოფის სახეებსა და ტექნიკურ წესებს, რომლის მიხედვითაც უნდა განხორციელდეს ციფრული მტკიცებულებების დამუშავება.
- შსს აკადემიაში შემუშავდა სპეციალური ტრენინგ მოდულები, რომელიც ფარავს კიბერ დანაშაულთან დაკავშირებულ შემდეგ საკითხებს: ელექტრონული მტკიცებულებების ჩხრეკა ამოღება, კიბერ დანაშაულის საგამოძიებო ტექნიკა, კიბერ დანაშაულის სამართლებრივი ასპექტები და ა.შ.[42]

4.1 სისხლის სამართლის ეროვნული კანონმდებლობა

საქართველოს ახალ სისხლის სამართლის კოდექსში ცალკე თავი აქვს დათმობილი კომპიუტერულ დანაშაულს. ახალი რედაქციით სისხლის სამართლის კოდექსის XXXV თავი შეიცავს სამ მუხლს, კერძოდ კი: 284-ე (კომპიუტერულ სუსტემაში უნებართვო შეღწევა), 285-ე (კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის უკანონოდ გამოყენება), და 286-ე (კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა) მუხლებს.[43]

[42] http://police.ge

[43] საქართველოს სისხლის სამართლის კოდექსი, 1999, 2020 წლის 10 ივნისის მდგომარეობით

საქართველოს სსკ-ის 35-ე თავით გათვალისწინებული სამივე შემადგენლობა მიეკუთვნება ნაკლებად მძიმე დანაშაულთა კატეგორიას. მათი ობიექტური შემადგენლობები ჩამოყალიბებულია როგორც ფორმალური და განხორციელება მოქმედებით ხდება.

კომპიუტერული დანაშაულის სუბიექტი შეიძლება იყოს როგორც ფიზიკური ისე იურიდიული პირი[44]. აღნიშნულთან დაკავშირებით ვთვლი რომ კომპიუტერული დანაშაულის სუბიექტი შეიძლება იყოს მხოლოდ და მხოლოდ ფიზიკური პირი, ხოლო იურიდიული პირი უბრალოდ საშუალებად გამოიყენოს ისევ ფიზიკურმა პირმა რათა მიაღწიოს სასურველ მიზანს. იურიდიული პირი მთელი მისი არსით დამოუკიდებლად ვერ შეძლებს განახორციელოს რაიმე მოქმედება ფიზიკური პირის გარეშე. შესაძლოა ფიზიკური პირის გარეშე იურიდიული პირი არსებობდეს თუმცა იგი უფუნქციო და სრულიად უსაფრთხო იქნება, იმ შემთხვევაში თუ კი მას ფიზიკური პირი არ გამოიყენებს. მაგალითისთვის, შესაძლოა ისევ ავტომობილი გამოვიყენოთ. წარმოიდგინეთ მძღოლის გარეშე იგი რას შეძლებდა? ვერაფერს უბრალოდ იარსებებდა და იქნებოდა სრულიად უსაფრთხო. ხოლო, თუ კი მას ადამიანი მართავს შესაძლოა ავტომობილი ნამდვილ მკვლელ იარაღად გარდაიქმნას. ამ კონკრეტულ შემთხვევაში ადამიანი ჩადის დანაშაულს და არა მანქანა, მანქანა უბრალო იარაღია ფიზიკური პირის ხელში. შესაძლოა ჩემს მიერ მოყვანილი მაგალითი უხეში შედარებაა თუმცა იურიდიულ პირსაც და ხალხის მკვლელ მანქანასაც საბოლოო ჯამში, მას შემდგე რაც ფიზიკური პირი მათ დანაშაულის ჩადენის საშუაებად გამოიყენებს მხოლოდ ერთი რამ ემუქრებათ, განადგურება.

თ. წერეთელი თვლის, რომ „ადამიანის ქცევა მაშინ უნდა ჩაითვალოს საზოგადოებრივად საშიში შედეგის პირობად, როდესაც ქმედების გარეშე შედეგი არ განხორციელდებოდა, ხოლო იმის დასადგენად, განხორციელდებოდა თუ არა საზოგადოებრივად საშიში შედეგი მოქმედების გარეშე, შეიძლება გამოვიყენოთ ქმედების აზრობრივი გამორიცხვის მეთოდი, ე.ი. ჩვენს წარმოდგენაში დავუშვათ, რომ შედეგი მაინც დადგებოდა, თანაც დადგებოდა სწორედ ამ დროს და ამ სახით, რგორც იგი სინამდვილეში განხორციელდა, ეს იმას ნიშნავს, რომ ადამიანის ქმედება არ ყოფილა მიზეზშედეგობრივ კავშირში შედეგთან“[45]. რა შეგვიძლია გავიგოთ ქალბატონი თ. წერეთლის სიტყვებიდან თუ კი აქ ნათქვამ სიტყვებს დავუკავშირებთ კომპიუტერული დანაშაულის სუბიექტებს?! მოკლედ თუ დავუშვებთ იმას რომ კომპიუტერს შეუძლია საკუთარი „ნებით“ განახორციელოს რაიმე ქმედება მაშინ შეგვიძლია ვთქვათ რომ კომპიუტერული დანაშაულის

[44] მ. ლეკვეიშვილი, ნ. თოდუა, გ. მამულაშვილი. სისხლის სამართლის კერძო ნაწილი, წიგნი მეხუთე, ნაწილი II, თბ., 2017, გვ. 159

[45] თ. წერეთელი, სისხლის სამართლის პრობლემები, ტომი I, თბ., 2007, გვ. 241

ჩადენა შეუძლია იურიდიულ პირს ადამიანის გარეშე. როგორ? მარტივად იურიდიულმა პირმა თუ ჩაიდინა კომპიუტერული დანაშაული საამისოდ საჭიროა ადამიანი, ხოლო იურიდიული პირის სახელით ადამიანმა, რომ ჩაიდინოს კომპიუტერული დანაშაული საამისოდ საჭიროა კომპიუტერი. თუ კი დავუშვებთ იმას, რომ კომპიუტერული დანაშაულის ჩადენა შეუძლია კომპიუტერს ადამიანის და იურიდიული პირის გარეშე მივალთ დასკვნამდე რომ თურმე კომპიუტერული დანაშაულის სუბიექტი არა ფიზიკური ან იურიდიული პირი არამედ კომპიუტერი ყოფილა. აღნიშნული კი საღ აზრს მანამ ვერ მიუახლოვდება სანამ კომპიუტერს ხელოვნურ ინტელექტთან ერთად საკუთარი ნებაც არ ექნება.

ამრიგად მიმაჩნია რომ კომპიუტერული დანაშაულის სუბიექტი შეიძლება იყოს მხოლოდ ფიზიკური პირი ხოლო იურიდიული პირი კი უბრალო საშუალება ადამიანისთვის რათა მან მიაღწიოს მის დანაშაულებრივ მიზანს და თუ მაინც და მაინც სუბიექტად მიაჩნიათ იურიდიული პირი მიზანშეწონილად მიმაჩნია ასევე სუბიექტად მიიჩნიონ კომპიუტერიც. აქვე არ დაგვავიწყდეს ის ფაქტი, რომ ისევ და ისევ ფიზიკურ პირს ანუ მოაზროვნე ადამიანს შეუძლია შექმნას იურიდიული პირიც და კომპიუტერიც იმისათვის, რომ მისი გეგმა, არ აქვს მნიშვნელობა ეს დანაშაულებრივი იქნება თუ არა მოიყვანოს მოქმედებაში და საბოლოოდ მიიღოს შედეგი ანუ მიაღწიოს მიზანს.

4.2 კიბერდანაშაულის სამართლებრივი რეგულირება სხვადასხვა ქვეყნებში და ევროპული კონვენცია „კიბერდანაშაულის შესახებ“

ამერიკაში კომპიუტერულ დანაშაულთან დაკავშირებით საკანონმდებლო ცვლილებები მუდმივად მიმდინარეობდა. მისი ახალი ტალრა კი XXI საუკუნის დასაწყისიდანვე აგორდა. 2001 წლის ოქტომბერში მიღებულ იქნა ფედერალური კანონი, ე.წ. „პატრიოტთა აქტი“. მისი შემუშავება 2001 წლის 11 სექტემბრის ტერაქტმა განაპირობა. არნიშნულმა აქტმა გააფართოვა ფედერალური გამოძიების ბიუროს უფლბამოსილება ელექტრონული თვალთვალისა და მოსმენის სფეროში. ამავე აქტის 814-ე მუხლით ცვლილება შევიდა კანონთა კრებულის მე-18 ტიტულის 1030-ე მუხლში, რომელიც ეხება ცალკეულ კომპიუტერულ დანაშაულს. ამ ცვლილების შედეგად კომპიუტერული დანაშაულისთვის გახდა თავისუფლების აღკვეთა 10 წელი, განმეორებითისთვის კი 20 წელი. აღნიშნული ცვლილების შემდეგ ამერიკის შეერთებულ შტატებში ქმედების დანაშაულად კვალიფიკაციისთვის აუცილებელი გახდა დამნაშავის მიზნის დადგენა.

მასში ზიანის ცნება და იგი ჩამოყალიბდა, როგორც „მონაცემთა, სისტემის პროგრამის ან ინფორმაციის მთლიანობის ნებისმიერი დაზიანება“.

ამერიკელი კანონმდებლები დასჯადად აცხადებს კომპიუტერულ სისტემაში არასანქცირებულშეღწევას, მასში უნდა ვიგულისხმოთ, სანქცირებული შესვლის ფარგლების გადამეტებაც.[46]

კანონმდებელმა განსაზღვრა კომპიუტერული ჯაშუშობის ცნება, რომელიც გულისხმობს პირის მიერ კომპიუტერულ სისტემაში, არასანქცირებულ შეღწევას ან სანქცირებული შესვლის ფარგლების გადამეტებას, ასევე ისეი ინფორმაციის მოპოვებას, რომელსაც კავშირი აქვს სახელმწიფო უსაფრთხოების, საერტაშორისო ირთიერთობის და ატომური ენერგიის საკითხთან.

გარდა ზემოაღნიშნულისა, დასჯადია კომპიუტერული თაღლითობა, ესე იგი თაღლითური განზრახვიტ და უკანონო სარგებლის მიღების მიზეზით კომპიუტერულ სისტემაში შეღწევა.

ასევე საინტერესოა ის ფაქტი, რომ იუტას შტატში დასაშვებია ორგანიზაციის მიერ კომპიუტერული თავდასხმა იმ კომპიიუტერულ ქსელზე ან სისტემაზე, რომლიდანაც ცდილობდნენ არასანცირებული შეღწევის განხორციელებას მათ კომპიუტერში ან სისტემაში.[47]

გერმანიამ საკანონმდებლო ცვლილებებზე მსჯელობა 2007-ი წლიდან დაიწყო. ევროსაბჭოს ექსპერტი მარკო გერკე, რომელიც მონაწილე იყო გერმანიის საკანონმდებლო ორგანოში ცვლილების მომზადების პროცესში, ჯერ კიდევ 2007 წლის ივლისში, აცხადებდა, რომ გერმანიის კანონმდებლობა განსხვავებით ბევრი სხვა ქვეყნისაგან არ აწესებდა სისხლისსამართლებრივ პასუხისმგებლობას კომპიუტერში ან მის ქსელში უნებართვო შეღწევისთვის. ეს ქმედება დასჯადი იყო მხოლოდ მაშინ თუ კი უნებართვო შეღწევა გამოიწვევდა ინფორმაციის მოპოვებას. მ. გერკეს დასაბუთებულად მიაჩნდა, რომ აღნიშნული ხარვეზი საჭიროებდა აღმოფხვრას და კომპიუტერულ სისტემაში უნებართვო შეღწევა უნდა ყოფილიყო დასჯადი, მიუხედავად იმისა დადგა თუ არა რაიმე შედეგი. მ. გერკეს აუცილებლად მიაჩნდა კიბერდანაშაულის შესახებ კონვენციის მე-6 მუხლით გათვალისწინებული ქმედების კრიმინალიზაცია. მისი აზრით, ცვლილება უნდა შეხებოდა გერმანიის სისხლის სამართლის 303-ბ მუხლსაც, რომელის მიხედვითაც, ძველი რედაქციით დასჯადი იყო ინფორმაციის დამუშავების პროცესის ხელყოფა, იგი განსაკუთრებული მნიშვნელობის იყო ბიზნესის, საწარმოს ან ადმინისტრაციულ ორგანოსათვის. მ. გერკეს აზრით, ცვლილების შედეგად ქმედება დასჯადი უნდა ყოფილიყო იმ შემთხევაშიც თუ მოხდებოდა იმ ინფორმაციის დამუშავების პროცესის ხელყოფა, რომელიც ინახებოდა კერძო პირის საკუთრებაში.

[46] უ. ზაქაშვილი, კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, თბ., 2013 წ. გვ. 118

[47]უ. ზაქაშვილი, კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, თბ., 2013 წ. გვ.119

მ. გერკეს პოზიცია 2007 წელს გაზიარებული არ იქნა, მაგრამ გერმანიამ კიბერდანაშაულის შესახებ კონვენციის რატიფიცირება 2009 წლის მარტში მოახდინა. რის შემდეგაც გათვალისწინებულ იქნა მ. გერკეს პოზცია და აზრი კიბერ დანაშაულთან დაკავშირებით.[48]

იტალიაში კიბერდანაშაულის შესახებ კონვენცია ძალაში შევიდა 2008 წლის 1 ოქტომბრიდან. უნდა აღინიშნოს, რომ იტალიური კანონმდებლობა ჯერ კიდევ 1993 წლიდან იცნობდა და ითვალისწიებდა კომპიტერულ სისტემაში უნებართვო შეღწევას, კომპიუტერული თაღლითობისთვის, კომპიუტერული მონაცემების გადაცემისთვის და ა.შ.

იტალია კონვენციას სრულად შეუერთდა, ანუ კანონმდებლობაში გადაიტანა ყველა ის პრინციპი და ტერმინი, რაც კონვენციით განისაზღვრა. იტალიელი მეცნიერი ჯუზეპე კორასანიტის აზრით, ევროპის საბჭოს კონვენცია აბსტრაქტულ კანონმდებლობას არ წარმოადგენს, ის კიდევ უფრო ეფექტური გახდება მას შემდეგ, როცა წაიშლება ზღვარი და ყველა ქვეყანა მოახდენს მის რატიფიცირებას. [49]

იტალიური კანონმდებლობით ასევე დასჯადი ქმედებაა კომპიუტერული თაღლითობა, რაც იცავს ელექტრონული ხელმოწერის გაყალბებას და მის გამოყენებას. აღნიშნული საინტერესო იმითაა, რომ დანაშაულის სუბიექტი შეიძლება იყოს მხოლოდ ის პირი ვისაც ელექტრონულ ხელმოწერაზე ხელი მიუწვდება. ეს განსაკუთრებული სიახლეა, რადგან მსოფლიოს მასშტაბით ხშირად გამოიყენება ელექტრონული ხელმოწერა. შესაბამისად გაზრდილია მისი გაყალბების საფრთხეც და ამიტომ იტალიელმა კანონმდებლებმა აღნიშნულის გათვალისწინებით დანაშაულებრივ ქმედებად მიიჩნიეს კომპიუტერული თაღლითობა, რაც სხვისი ელექტრონული ხელმოწერის გაყალბებას გულისხმობს. (იტალიის სისხლის სამართლის 640-ე მუხლი).[50]

აქვე უნდა აღინიშნოს, რომ მსგავსი დანაშაულის ჩადენის წინაშე საქართველო ჯერ არ დგას, რადგან ჩვენს ქვეყანაში მსგავსი ხელმოწერები ფართოდ არ არის გავრცელებული და ისინი ჯერ არ გამოიყენება ოფიციალური იურიდული საბუთების მოსაწესრიგებლად. თუმცა რათქმაუნდა აღნიშნულის განვითარებასთან ერთად საჭირო იქნება ისეთივე რეგულაციებისა და ნორმების მიღება, როგორც ეს იტალიამ გააკეთა.

---

[48] უ. ზაქაშვილი, კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, თბ., 2013. გვ. 120

[49] უ. ზაქაშვილი, კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, თბ., 2013 წ. გვ. 123

[50] უ. ზაქაშვილი, კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, თბ., 2013. გვ. 123

გაერთიანებული სამეფო (ინგლისი, უელსი) დიდი ხნის განმავლობაში არ ახდენდა „კიბერდანაშაულის შესახებ“ კონვენციის რატიფიცირებას. რის გამოც ის კრიტიკის ობიექტი ხდებოდა. დიდი კრიტიკის აჟიოტაჟისა და განხილვების შემდეგ დიდმა ბრიტანეთმა აღნიშნული კონვენციის რატიფიცირება მოახდინა საკმაოდ გვიან 2011 წლის 25 მაისს.

პროფესორი პიტერ სომერი „კიბერდანაშაულის შესახებ“კონვენციას დადებითად აფასებს, თუმცა სკეპტიკურად უდგება სხვადასხვა საერთაშორისო ორგანიზაციის ძალისხმევას მოაგვაროს კომპიუტერული დანაშაულის პრობლემა მხოლოდ ცოდნის გაზიარების გზიოტ და რეკომენდაციების გაცემით. გარდა ზემოაღნშნულისა პ. სომერი მიუთითებს რომ ევროპილი ქვეყნების სამართალი, დაფუძნებულია კოდექსებზე, ინგლისში, კი „საერთაშორისო სამართალია“, რომლის მიხედვითაც სამართლის უფრო მნიშნელოვანი ნაწილი თავმოყრილია სასამართლო პრეცედენტებში. მისი აზრით, სწორედ ეს გარემოება აბრკოლებს დიდ ბრიტანეთში კონვენციის რატიფიცირებას.[51]

2001 წლის 23 ნოემბერს ქ. ბუდაპეშტში ევროსაბჭოს 41 წევრი სახელმწიფოს მიერ მიღებულ იქნა კონვენცია ,,კიბერდანაშაულის შესახებ“. (Council of Europe-ETS N 185 Con-venton on cybercrime 23.11.2001. Budapest), რომელიც ძალაში შევიდა 2004 წლის 1 ივლისიდან. აღნიშნული დოკუმენტი წარმოადგენს მსოფლიოს მასშტაბით ერთ-ერთ პირველ სერიოზულ მცდელობას ნაციონალური უსაფრთხოების დასაცავად კიბერდანაშაულის წინააღმდეგ ბრძოლაში ერთიანი სტრატეგიის დასახვისა და ურთიერთთანამშრომლობისათვის. 2009 წლის მდგომარეობით კონვენციაზე ხელი მოაწერა 46 ქვეყანამ, ხოლო მისი რატიფიცირება განხორციელდა მხოლოდ 26 მათგანში.

ეს კონვენცია პირველი საერთაშორისო ხელშეკრულებაა ინტერნეტით და სხვა კომპიუტერული ქსელებით ჩადენილი დანაშაულების შესახებ. მისი მთავარი მიზანი არის საერთო კრიმინალური პოლიტიკის გატარება, რომელიც მიზნად ისახავს საზოგადოების დაცვას კიბერკრიმინალისაგან. განსაკუთრებით სათანადო კანონმდებლობის შექმნის და საერთაშორისო თანამშრომლობის გაძლიერების გზით.

ამერიკელი და ევროპელი ექსპერტების ნაწილი კონვენციის ძირითად ნაკლად იმ თეორიულ საფრთხეს მიიჩნევენ, რომელსაც ეს დოკუმენტი პირადი ინფორმაციის ანონიმურობას უქმნის. კონვენციის მიხედვით, თუ არის ეჭვი, რომ კონკრეტული ინტერნეტ მომხმარებელი დაკავშირებულია კრიმინალურ საქმიანობასთან, გამოძიებას უფლება აქვს, მოსამართლის

[51] უ. ზაქაშვილი, კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, თბ., 2013. გვ. 120-121.

ნებართვით, მისი პერსონალური ინფორმაცია მოიპოვოს და თვალი ადევნოს მის პირად კომუნიკაციას. ამ ადამიანმა, შესაძლოა, ვერასოდეს გაიგოს, რომ მას ოდესმე უთვალთვალებდნენ. საქართველოს პარლამენტის იურიდიულ საკითხთა კომიტეტში განმარტავენ, რომ საზოგადოებრივი ინტერესი პირადი საუბრის ყველა სახის შელახვას ამართლებს.

კონვენციის რატიფიკაციაზე უარი განაცხადა რუსეთმაც. რაც იმას ნიშნავს, რომ 2008 წელს საქართველო კონვენციის ხელმომწერი რომც ყოფილიყო, ეს მას კიბერომს თავიდან ვერ აცილებდა. რუსი სამართალდამცავი ორგანოები არასდროს იქნებიან ევროსაბჭოს წინაშე ანგარიშვალდებულნი, დააკავონ და დასაჯონ კიბერშეტევებში დამნაშავეები[52].

კიბერ დანაშაულის შესახებ კონვენცია განსაზღვრავს კიბერნეტიკულ დანაშაულთა სახეებს, რომლისთვისაც მონაწილე ქვეყნებმა სისხლისსამართლებრივი პასუხისმგებლობა უნდა დაადგინონ. ამ დოკუმენტით მსოფლიო თანამეგობრობის მიერ შემუშავებულია ერთნიანი პოზიცია იმის შესახებ, თუ რომელი ქმედებები უნდა იქნეს კრიმინალიზებული და რა ფორმით უნდა განხორციელდეს საერთაშორისო თანამშრომლობა კიბერნეტიკულ დანშაულთან საბრძოლველად. 2008 წლის 28 მარტს საქართველოს პრეზიდენტმა გამოსცა განკარგულება კიბერდამნაშავეობასთან ბრძოლის შესახებ კონვენციის ხელომოწერის თაობაზე. ხოლო იგი რატიფიცირებულ იქნა 2012 წელს.

ამასთანვე, კონვენცია წევრ ქვეყნებს ავალდებულებს შექმნან კიბერ დანაშაულთან ბრძოლის შიდა ეროვნული სპეციალიზირებული დანაყოფები, რომლებიც ასევე შეასრულებენ 24/7 საერთაშორისო საკონტაქტო პუნქტის უფლებამოსილებებს.[53]

[52] ს. შენგელია, კიბერდანაშაული - XXI საუკუნის გამოწვევა, სტუდენტური სამართლებრივი ჟურნალი, თბ., 2011, გვ. 54

[53] http://police.ge/ge/projects/kiberdanashauli/kanonmdebloba-kiber-danashaulze-da-zogadi-politika

თავი V.კიბერდანაშაულთან დაკავშირებული ქართული საკანონმდებლო რეგულაციები

კიბერდანაშაული 21-ე საუკუნის ერთ-ერთი მთავარი გამოწვევაა და მისი მასშტაბების გათვალისწინებით, განსაკუთრებულ მიდგომას საჭიროებს. ეს, თავის მხრივ, სახელმწიფო, კერძო თუ არასამთავრობო სექტორებს შორის აქტიურ თანამშრომლობას მოითხოვს. ამ მიმართულებით მნიშვნელოვანია სწორი სახელმწიფო პოლიტიკის გატარება, რასაც თან უნდა ერთვოდეს სწორი კრიმინალური პოლიტიკის არსებობა. რაც საგრძნობლად შეამცირებს კიბერდანაშაულით გამოწვეულ ეკონომიკური, პოლიტიკური და სოციალური ხასიათის საფრთხეებს და შექმნის მეტად უსაფრთხო გარემოს სახელმწიფოებრივი და საზოგადოებრივი განვითარებისათვის. [54]

იმისათვის, რომ ქვეყანაში დანაშაული შემცირდეს საჭიროა სწორი კრიმინალური პოლიტიკის არსებობა. აღნიშნული პოლიტიკა საკუთარ თავში არ უნდა გულისხმობდეს და მოიცავდეს მხოლოდ რეპრესიული ქმედებების განხორციელებას. იგი საკუთარ თავში უნდა მოიაზრებდეს სისხლის სამართლებრივი სასჯელის გარდა სხვა პრევენციული ღონისძიებების განხორციელებასაც.[55] ამასთანავე უნდა ღინიშნოს ისიც, რომ კრიმინოლოგია როგორ მეცნიერება მნიშვნელოვან როლს თამაშობს ქვეყნის კრიმინალური პოლიტიკის ჩამოყალიბებაში. იმდენად რამდენადაც კრიმინოლოგია იკვლევს დანაშაულს და მის გამომწვევ მიზეზებს, იგი საუკეთესო გარანტიაა იმისა, რომ არსებული ვითარების, მდგომარეობის, რაციონალური და ჯეროვანი შეფასება მოხდეს, რაც ჩემი აზრით მნიშვნელოვანია იმ არსისა და მორალისთვის რასაც დანაშაულის პრევენცია ეწოდება.

2008 წლიდან მოყოლებული, დაიწყო კონკრეტული ნაბიჯების გადადგმა კიბერდანაშაულის წინააღმდეგ ბრძოლის კუთხით. 2012 წლიდან მოქმედებს ,,საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ“. საქართველოს მიერ რატიფიცირებულია ევროპის საბჭოს კონვენცია „კიბერდანაშაულის შესახებ“. სრულად განახლდა სისხლის სამართლის კოდექსის XXXV თავი. ცვლილებები შეეხო საპროცესო კანონმდებლობასაც. დაემატა სპეციფიური საგამოძიებო მოქმედებები, კერძოდ, სსსკ-ის XVI თავი კომპიუტერულ მონაცემთან დაკავშირებული საგამოძიებო მოქმედებები, ტერმინთა განმარტება და სხვა. **შემოღებულ იქნა იურიდიული პირის სისხლისსამართლებრივი პასუხისმგებლობა კიბერდანაშაულის ჩადენისათვის.** დაიხვეწა ინტელექტუალური საკუთრების შესახებ მუხლი (საავტორო, მომიჯნავე უფლების მფლობელისა

[54] საქართველოს მთავრობის დადგენილება N 252, საქართველოს ორგანიზებული დანაშაულის წინააღმდეგ ბრძოლის ეროვნული სტრატეგიის დამტკიცების შესახებ, 2013 წ.

[55] მ. შალიკაშვილი, კრიმინოლოგია, II გამოცემა, თბ., 2011, გვ. 45

და მონაცემთა ბაზის დამამზადებლის უფლების ხელყოფა). დაიხვეწა ბავშვთა პორნოგრაფიის მუხლი. ცვლილებები შევიდა ასევე საქართველოს კანონებში „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ და „ელექტრონული კომუნიკაციების შესახებ.“ ასევე შეიქმნა კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი (CERT)[56], რომელიც უფლებამოსილია, განახორციელოს კიბერსივრცის მონიტორინგი, კომპიუტერული ინციდენტების გამოვლენისა და მართვის მიზნით, განსაზღვროს და გაატაროს კიბერუსაფრთხოების პოლიტიკა, ასევე განახორციელოს საქართველოს კანონმდებლობით მინიჭებული სხვა უფლებები. კიბერდანაშაულის წინააღმდეგ ბრძოლა შინაგან საქმეთა სამინისტროს კომპეტენციას წარმოადგენს. ცენტრალური კრიმინალური პოლიციის დეპარტამენტში შექმნილია კიბერდანაშაულის წინააღმდეგ ბრძოლის სამმართველო, რომელიც მოიცავს კიბერდანაშაულის საერთაშორისო საკონტაქტო პუნქტს 24/7. შსს-ში ასევე ფუნქციონირებს საექსპერტო-კრიმინალისტიკური მთავარი სამმართველოს კომპიუტერულ-ციფრული ექსპერტიზის ქვეგანყოფილება, რომელიც ახორციელებს საგამოძიებო მოქმედებების შედეგად მიღებული ციფრული მტკიცებულებების ექსპერტიზას.

კიბერდამნაშავეები არამარტო აზიანებენ კრიტიკულ ინფორმაციულ სისტემებს, აგრეთვე იყენებენ კიბერსივრცეს სხვადასხვა დანაშაულის ჩასადენად. კიბერდანაშაულის წინააღმდეგ ბრძოლის ეფექტიანობის მიზნით, აუცილებელია საინფორმაციო კამპანიების წარმოება (სოციალური ქსელები, შესაბამისი უწყებების ვებგვერდები და სხვა) კიბერდანაშაულისა და მისგან გამოწვეული ზიანის შესახებ. ასევე მნიშვნელოვანია აღნიშნულის შესახებ სკოლებში სამართალდამცავი უწყებებისა და განათლებისა და მეცნიერების სამინისტროს წარმომადგენელთა მიერ მოსწავლეების ინფორმირება. საზოგადოებამ უნდა იცოდეს, თუ როგორ დაიცვას თავი კიბერდანაშაულისგან, უნდა გააჩნდეს ინფორმაცია პოტენციური საფრთხეების, მათი იდენტიფიცირებისა და მათზე რეაგირების შესახებ.[57]

ჩემს თემაში არა ერთხელ იქნა აღნიშნული, რომ საქართველოში კიბერდანაშაულის დასჯადობის საკითხებს არეგულირებს სისხლის სამართლის კოდექსის (სსკ) XXXV თავი, რომლის თანახმადაც, სისხლის სამართლის პასუხისმგებლობას იწვევს კიბერსივრცეში ჩადენილი შემდეგი ქმედებები: კომპიუტერულ სისტემაში უნებართვო შეღწევა, კომპიუტერული მონაცემის ან/და

[56] CERT.GOV.GE საქართველოს იუსტიციის სამინისტროს მონაცემთა გაცვლის სააგენტოს ფარგლებში ფუნქციონირებს. CERT.GOV.GE-ს პასუხიმგებლობაა რეაგირება მოახდინოს საქართველოს სამთავრობო ქსელში და კრიტიკულ ინფრასტრუქტურაში დაფიქსირებულ კომპიუტერულ ინციდენტებზე. CERT.GOV.GE

[57] საქართველოს მთავრობის დადგენილება N 252, საქართველოს ორგანიზებული დანაშაულის წინააღმდეგ ბრძოლის ეროვნული სტრატეგიის დამტკიცების შესახებ, 2013 წ.

კომპიუტერული სისტემის უკანონოდ გამოყენება და კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა.

კიბერდანაშაულთან დაკავშირებით მნიშვნელოვანია დადებითად შეფასდეს საქართველოს მიერ გატარებული შემდეგი საკანონმდებლო რეგულაციები:

- მიღებულ იქნა კანონი „ინფორმაციული უსაფრთხოების შესახებ“, რომელიც აწესებს ინფორმაციული უსაფრთხოების ზოგად სტანდარტებს საჯარო და კერძო სექტორისთვის.
- შინაგან საქმეთა სამინისტროს ცენტრალური კრიმინალური პოლიციის დეპარტამენტში შეიქმნა კიბერდანაშაულთან ბრძოლის სამმართველო, რომელსაც ევალება კიბერ სივრცეში ჩადენილი მართლსაწინააღმდეგო ქმედებების გამოვლენა, აღკვეთა და პრევენცია.
- შსს საექსპერტო-კრიმინალისტიკური მთავარი საამმართველოს შემადგენლობაში ჩამოყალიბდა კომპიუტერულ-ციფრული ექსპერტიზის ქვეგანყოფილება.
- საქართველოს კიბერ უსაფრთხოების სტრატეგია 2013-2015 წარმოადგენს კიბერ უსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელ მთავარ დოკუმენტს.
- შემუშავდა სტანდარტული ოპერაციული პროცედურები ციფრული მტკიცებულებების პირველადი მოპყრობის შესახებ. დოკუმენტები განსაზღვრავს იმ პროგრამულ უზრუნველყოფის სახეებსა და ტექნიკურ წესებს, რომლის მიხედვითაც უნდა განხორციელდეს ციფრული მტკიცებულებების დამუშავება.
- შსს აკადემიაში შემუშავდა სპეციალური ტრენინგ მოდულები, რომელიც ფარავს კიბერ დანაშაულთან დაკავშირებულ შემდეგ საკითხებს: ელექტრონული მტკიცებულებების ჩხრეკა ამოღება, კიბერ დანაშაულის საგამოძიებო ტექნიკა, კიბერ დანაშაულის სამართლებრივი ასპექტები და ა.შ.[58]

5.1. კიბერდანაშაულის სახეები და მისი სუბიექტები

კიბერდამნაშავეები საზოგადოებაში ჰაკერების სახელითაც არიან ცნობილნი. ჰაკერი ინგლისური სიტყვაა და სიტყვასიტყვით ჭრილობას, გაპობას, გაჭრას ნიშნავს. პირველად ეს ტერმინი 1960-იან წლებში გაჩნდა და ამის შემდეგ მას მრავალი მნიშვნელობა გაუჩნდა. ჰაკერი აუცილებლად, სულ ცოტა, 2 პროგრამირების ენას უნდა ფლობდეს, ერკვეოდეს ქსელში და იყენებდეს ძლიერ ოპერაციულ სისტემებს (*nix - UNIX, BSD, Linux და ა.შ.). არსებობს ისეთი მოსაზრებაც, რომ ”ჰაკერი” ”ყველაფრის მცოდნეა”.[59] ჰაკერებს უწოდებენ საინფორმაციო

[58] საქართველოს მთავრობის დადგენილება N 252, საქართველოს ორგანიზებული დანაშაულის წინააღმდეგ ბრძოლის ეროვნული სტრატეგიის დამტკიცების შესახებ, 2013 წ.
[59] რ. ტეტუნაშვილი, ვინ არის ჰაკერი?, 2019 წ.

ტექნოლოგიების სპეციალისტებს, რომლებიც განსაკუთრებული პროფესიონალიზმით გამოირჩევიან ამ სფეროში და უბადლოდ ფლობენ კომპიუტერული პროგრამების შექმნის უნარ-ჩვევებს. როგორც წესი, ჰაკერები საკუთარ კვალს ან შლიან, ან ცვლიან, რის შედეგადაც თითქმის შეუძლებელი ხდება მათი პოვნა და ვინაობის დადგენა.[60]

აღნიშნულიდან გამოდინარე შეგვიძლია ვთქვათ, რომ კიბერდანაშაულის სუბიექტი არის პირი, რომელიც უშუალო მოქმედებით ახორციელებს კიბერ შეტევას. ასეთ სუბიექტებს ჩვენ შეგვიძლია ვუწოდოთ ჰაკერები.

ისინი დანაშაულის ჩადენის ისეთ ხერხებს იყენებენ როგორებიც არის:

SPAM-სპამი არის ელექტრონული წერილის ტიპი, რომელიც მასობრივად და ანონიმურად იგზავნება მიმღების ელექტრონული ფოსტის მისამართზე, მის დაუკითხავად და სურვილის გარეშე. მსგავსი წერილები უმეტესწილად სარეკლამო ხასიათისაა და განკუთვნილია რაიმე მომსახურების ან საქონლის რეკლამირებისათვის (პოტენციის ასამაღლებელი აბების რეკლამა, ფიქტიური კომპანიებისგან საფონდო ბირჟებზე მომხიბვლელი გარიგებების შესახებ მოწვევები და უამრავი სხვა დამაინტრიგებელი წინადადება). სპამი (ინგლ. Spam, Bulk ან Junk) არის ელექტრონული წერილის ტიპი, რომელიც იგზავნება პიროვნების ან კომპანიის მიერ, მიმღების დაუკითხავად და სურვილის გარეშე. მსგავსი წერილები უმეტესწილად სარეკლამო ხასიათისაა. პიროვნებას, რომელიც მსგავს წერილებს გზავნის ეწოდება სპამერი. მათი ძირითადი მიზანია თავიანთი პროდუქტის პოპულარიზაცია.[61]

2. FISHING-ფიშინგი (ინგლისურად phishing:fishing - თევზაობა) — ინტერნეტ თაღლითობის დანაშაულებრივი ფორმა, რომლის მიზანია თაღლითური გზით მომხმარებელს გამოსძალოს პირადი საიდენტიფიკაციო მონაცემები, მაგალითად: პაროლი, საკრედიტო ბარათის ან საბანკო ანაგარიშის ნომერი და სხვა კონფიდენციალური ინფორმაცია. ფიშინგისას შენიღბული ინტერნეტ კომუნიკაციის საშუალებით ხდება მომხმარებლის შესახებ ისეთი ინფორმაციის მოპოვება, როგორიცაა: მომხმარებლის სახელი, პაროლი, საკრედიტო ბარათის ან საბანკო ანგარიშის ნომერი. ეს მიიღწევა შემდეგი მეთოდებით: მასიური ელექტრონული წერილების დაგზავნით (წერილის ავტორებად იყენებენ ცნობილ ორგანიზაციებს და ბრენდებს), ასევე პირადი შეტყობინებებით სადაც იყენებენ ბანკის სახელს, მეილ სერვერების გამოყენებით და სოციალური ქსელების საშუალებებით. წერილში ხშირად არის ვებ გვერდის ბმული, რომლის ვიზუალური მხარე არ განსხვავდება ნამდვილისგან. შესაბამისად გაყალბებულ ვებ გვერდზე შეტანილი ინფორმაცია:

[60]https://sites.google.com/site/chemiproekti/hakerebi

[61] SPAM-სპამი https://cert.gov.ge/uploads/Articles/SPAM1.pdf

მომხმარებლის სახელი, პაროლი, საკრედიტო ბარათის ან საბანკო ანგარიშის ნომერი ავტომატურად ხვდება ეგრედ წოდებული "ფიშერი"-ს ხელში.[62]

3. MALWARE- ზიანის მომტანი "მავნე", „ბოროტი“ პროგრამა - ეს არის კრებსითი სახელწოდება ყველა ტიპის მავნე ფუნქციის მქონე პროგრამისთვის. მავნე ფუქნციების მქონე პროგრამა შეიცავს ვირუსებს, ე.წ. „Trojans“, „Worms“ და „Spyware“, თუმცა უნდა ითქვას, რომ მხოლოდ ამით არ შემოიფარგლება მისი მავნე ფუნქციონალი. მავნე ფუნქციონალის მქონე პროგრამის მიზანი უპირველეს ყოვლისა არის სისტემებში შეღწევა და ამდენად, იქ შენახული ინფორმაციის კრიმინალური, კომერციული ან გამანადგურებელი მიზნებისთვის გამოყენება. ამგვარი „ბოროტი“ პროგრამები ხშირად ელ-ფოსტით თანდართულ ფაილშია წარმოდგენილი ან ავტომატურად ხდება მისი ჩამოტვირთვა და დაინსტალირება თქვენს კომპიუტერზე, როდესაც თქვენს ელ-ფოსტაში მოცემულ ბმულზე დააწკაპუნებთ. „ბოროტი“ პროგრამები შეიძლება უყურადღებობის გამო ჩამოიტვირთოს ვებგვერდებიდან, ან ავტომატურად მოხდეს მისი ჩამოტვირთვა თქვენს კომპიუტერზე როგორც კი შეხვალთ ამ მიზნით შექმნილ ვებგვერდზე. სრულიად ახალი და კარგად მოფიქრებული გავრცელების საშუალება გახლავთ „მოციმციმე“ სარეკლამო ფანჯრები (Pop-Ups) , რომელთა ლეგალურობაშიც ეჭვს ვერ შეიტანთ ერთი შეხედვით, რადგანაც ნამდვილად შეიცავენ სარეკლამო შეტყობინებებს.[63]

4. BOTNET-ბოტნეტი "ბოტი" შემოკლებული ვარიანტია სიტყვისა რობოტი და ჩვენს შემთხვევაში იგი წარმოადგენს მავნე პროგრამას, რომელიც ინსტალირდება მსხვერპლის კომპიუტერში და გარკვეული ადამიანის, ან ადამიანების ეგრეთ წოდებული BOT MASTER-ის მიერ კონტროლირდება. ბოტებს ხშირად იყენებენ სხვადასხვა მავნე ქმედებების ჩასადენად, მაგალითად DDoS შეტევების განსახორციელებლად და Spam-ის გასაგზავნად. DDoS - გახლავთ შემოკლებული ფორმა Distributed Denial of Service-ის, რაც ნიშნავს სერვერის ან რაიმე სერვისის მიერ უარის თქმას მომსახურებაზე. DDoS ის შემთხვევაში ძირითადად შეტევა ხორციელდება ბევრი დავირუსებული კომპიუტერის მეშვეობით (სხვადასხვა IP მისამართებიდან ერთდროულად), ანუ ეგრეთწოდებული ზომბირებული კომპიუტერების ჯგუფიდან, რომლებიც ერთდროულად ახორციელებენ შეტევას. ეს მეთოდი გამოიყენება სერვერის ან რაიმე სერვისის ფუნქციონალის შეფერხებისთვის, გათიშვისთვის. "ბოტნეტი" - იგივე ზომბების არმია, წარმოადგენს ზემოდ მოყვანილ ბოტების ორგანიზებულ ჯგუფს, რომელიც ერთი ან რამოდენიმე ადამიანის მიერ კონტროლირდება. ბოტნეტის მფლობელი ცდილობს მაქსიმალურად გაავრცელოს ბოტი, რათა უფრო მძლავრი გახდეს

[62] https://dea.gov.ge/?action=article&article_id=8&lang=geo
[63] https://dea.gov.ge/?action=article&article_id=5&lang=geo

მისი რესურსი. გასავრცელებლად მრავალი ხერხი გამოიყენება, სპამი IRC სერვერებზე და იმეილზე.[64]

საქართველო პირველ ადგილზეა არალიცენზირებული პროდუქციის გავრცელების თვალსაზრისით. ქართულ საიტებზე ატვირთული თითქმის არც ერთი პროდუქცია ფილმები, მუსიკა, პროგრამები-ლიცენზირებული არაა. შეხვდებით არასრულწლოვანთა პორნოგრაფიის განყოფილებებს და სპეციალურ საიტებსაც კი, სადაც შეგიძლიათ, ჰაკეროზა ისწავლოთ. ასეთ ვებ-გვერდებზე შეგიძლიათ, კიბერკრიმინალი დაუკვეთოთ კიდეც 50 ლარად თქვენთვის სასურველ ელფოსტას, სკაიპს ან სხვა პროგრამას გაგიტეხენ და კერძო პირის პერსონალურ ინფორმაციას მოგაწვდიან.[65]

5.2. არასრულწლოვნების გამოწვევა კიბერსივრცეში, „ლურჯი ვეშაპი“ და „მარიამ გეიმი“

ბავშვი ყველაზე კარგ პირობებშიც რომ იზრდებოდეს, მოზარდობის წლები მაინც მშფოთვარე პერიოდად ითვლება. სქესობრივი მომწიფების პერიოდში მოზარდებში სრულიად უცხო გრძნობები და ემოციებია მოზღვავებული. მოზარდებზე მასწავლებლები თუ თანატოლები ყოველდღე ახდენენ გავლენას. ისინი ტელევიზორის, კინოფილმების, მუსიკისა და ინტერნეტის ძლიერი ზეგავლენის ქვეშაც ექცევიან. კომპიუტერული ტექნიკისა და ინტერნეტის დამკვიდრებასთან ერთად, გამოიკვეთა ახალი პრობლემა – კომპიუტერული თამაშები, სადაც უმეტესად ძალადობის ფაქტები მძაფრად და უხვადაა. გაერთიანებული ერების ორგანიზაციის ანგარიშში ნათქვამია, რომ „მოზარდობის წლები გარდატეხის პერიოდია, რომელსაც თან ახლავს სტრესი და მღელვარება“[66].

სამწუხაროდ, მოზარდებს ხშირად საკმარისი გამოცდილება არა აქვთ სტრესისა და მღელვარების დასაძლევად. სათანადო ხელმძღვანელობის გარეშე ისინი ადვილად შეიძლება მოექცნენ დამღუპველი ზეგავლენის ქვეშ. მაგალითად, გაეროს ანგარიშში ნათქვამია: „გამოკვლევები ცხადყოფს, რომ ხშირად ნარკოტიკების მოხმარებას მოზარდობის წლებში ან მის შემდგომ პერიოდში იწყებენ“. იმავეს თქმა შეიძლება ძალადობაზე და ნებისმიერ შემხვედრთან სქესობრივ კავშირზე.[67]

---

[64] Iberia Gaming Roleplay BOTNET-ბოტნეტი https://igrp.proboards.com/thread/28/

[65] ს. შენგელია, კიბერდანაშაული - XXI საუკუნის გამოწვევა, სტუდენტური სამართლებრივი ჟურნალი, თბ., 2011, გვ. 52

[66] https://wol.jw.org/ka/wol/d/r20/lp-ge/102005242

[67] https://wol.jw.org/ka/wol/d/r20/lp-ge/102005242

კომპიუტერული თამაშები ახალგაზრდებში საკმაოდ დიდი პოპულარობით სარგებლობს. ფაქტობრივად, ძნელია მოზარდის პოვნა, რომელიც ამით არ არის დაკავებული. ასევე ძნელი და თითქმის შეუძლებელია ისეთი თამაშის პოვნა, რომელიც ძალადობაზე არაა დაფუძნებული. თუ, რა თქმა უნდა, სპორტულ თამაშებს არ ჩავთვლით. აქვე აღსანიშნავია ისიც, რომ თამაშებს, ისევე როგორც მაგალითად ფილმებს, ასაკობრივი დაყოფა აქვთ. ანუ, მათაც აქვთ მითითებული +18 ნიშანი, მაგრამ ვინაიდან თამაშები ინტერნეტში უპრობლემოდ იძებნება და მისი ჩამოტვირთვაც საკმაოდ მარტივია, აღნიშნული ამკრძალავი ნიშანი აზრს კარგავს, რადგან მშობლის კონტროლის გარეშე დარჩენილი ბავშვი ნებისმიერ სასურველ თამაშს მარტივად მონახავს[68].

რამდენიმე სახის თამაში არსებობს – არის სტრატეგიული ხასიათის თამაშები; თამაშები, სადაც ტურებს გადიხარ და ყოველი ტურის დაძლევის შემდეგ ახალ დავალებებს იღებ და ე.წ. „შუთერები“, რომლის ძირითადი თემა სროლა და მკვლელობაა – ან ზომბებს დასდევ, ან ერთი კონკრეტული მოწინააღმდეგე გყავს და იმას ესვრი და ა.შ

ზოგიერთი თამაშის აზრი მხოლოდ დახოცვაა. რაც მეტს მოკლავ – მით უკეთესი. თუმცა არის თამაშები, რომელთაც კონკრეტული მიზანი გააჩნიათ. მარტივი მაგალითის სახით რომ გითხრათ – სამყაროს გადარჩენა ან რაიმე მსგავსი. თუმცა ესენიც ძალადობას მოიაზრებს, რადგან გზადაგზა აუცილებლად გიწევს ხალხის ხოცვა. ზოგიერთ თამაშში ყურადღება ექცევა არა უბრალოდ მოკვლას, არამედ იმას, თუ როგორ კლავ. ანუ, რაც უფრო სასტიკია მეთოდი, მით უფრო მაგარ მოთამაშედ ითვლები. ეს თამაშები მოთამაშეს ასწავლის კიდეც „საჭირო წერტილებს“ ადამიანის ორგანიზმში, რათა ერთი სროლით, ან ერთი ჭრილობით მაქსიმალურად სწრაფი ეფექტის მიღება შეგეძლოს. ზოგიერთ თამაშში ტურს, რომ გადიხარ შენი პერსონაჟი ვითარდება და მეტი რამის კეთება შეუძლია. ანუ, უფრო მრავალფეროვანი ხერხებით მოკვლა. თავში მორტყმით რომ კლავ მაგას headshoot ქვია და ყველაზე მაგარ რამედ ითვლება. არის ერთი თამაში, SNIPER-ი რომელშიც როცა ესვრი, გიჩვენებს როგორ შედის სხეულში ტყვია. თამაშების ბოლოს კი, თუკი სწრაფად გაიმარჯვებ, ე.წ. ფატალითით „დაჯილდოვდები“. ეს იმას ნიშნავს, რომ თამაში საშუალებას გაძლევს დამარცხებულ მოწინააღმდეგეს უსასტიკესად გაუსწორდე. მაგალითად, შუაზე გადახერხო, კიდურები მოაგლიჯო, ტყავი გააძრო, თავი მოაჭრა და სიგარეტი არტერიაში

[68] ნ. თაბუკაშვილი, გართობიდან სადიზმამდე - კომპიუტერული თამაშების ბეწვის ხიდი და აგრესია მოზარდებში, 2017 წ.

ჩააქრო, მოჭრილ თავს კი სკალპი კანი ააძრო და თავის ქალით ითამაშო, მოწინააღმდეგეს სახიდან და სხეულიდან ხორცი აათალო, გული ამოაგლიჯო და ჩაკბიჩო და ა.შ. [69]

მოკლედ ამ ყოველივეს გათვალისწინებით და საკუთარი გამოცდილებით შემიძლია გითხრათ, რომ კომპიუტერული თამაში რამდენად საინტერესოა ორი იმდენად საშიშიცაა. რამეთუ მაქვს გამოცდილება და ხშირ შემთხვევაში მიოცნებია კიდეც ვირტუალური რეალური ყოფილიყო და რეალურ დროში შემძლებოდა იმის კეთება რასაც ჩემი თამაშის პერსონაჟი კომპიუტერულ თამაშში აკეთებდა. აქვე მინდა ავღნიშნო ის ფაქტიც, რომ ძალადობრივი თამაშები იწვევენ ფსიქიკურ დარღვევებს. რაც საბოლოოდ დიდ აგრესიაში გამოიხატება.

ბოლო პერიოდში საზოგადოება აღაშფოთა ერთ-ერთმა ინტერნეტ თამაშმა რასაც ქართულად ლურჯი ვეშაპი, რუსულად Синий кит, ინგლისურად Blue Whale Challenge, ბერძნულად Μπλε φάλαινα ეწოდება.

ლურჯი ვეშაპი სოციალური ქსელის ფენომენი, რომელიც როგორც ამტკიცებენ 2016 წლის დასაწყისიდან არსებობს რამდენიმე ქვეყანაში. პირველად მოხსენიებული იყო რუსეთში 2013 წელს. ტერმინი „ლურჯი ვეშაპი“ მომდინარეობს ნაპირზე გამორიყული ვეშაპების ფენომენისაგან, რომელიც თვითმკვლელობასთანაა მიმსგავსებული. მიუხედავად იმისა, რომ ამ თამაშმა მასობრივი საინფორმაციო საშუალებების მნიშვნელოვანი ყურადღება დაიმსახურა, ამ დრომდე ძალიან ცოტა სანდო დამამტკიცებელი საბუთი მოიპოვება საერთოდ თამაშის არსებობის ან მისი როლის ბავშვებისა და მოზარდთა თვითმკვლელობამდე მიყვანისა და თვითდაზიანებების მიყენების შესახებ. [70]

სოციალურ ქსელებში გავრცელებული იყო თვითმიყენებული ჭრილობების ფოტოსურათები და თამაშის ჰეშტეგები(ონლაინ მისამართები)[71]. როგორც იუწყებიან, თამაში დაფუძნებულია მოწინააღმდეგეებსა და კურატორთა შორის არსებულ ურთიერთობაზე. იგი შეიცავს დავალებების სერიას, რომლებსაც კურატორები იძლევიან და რომლებიც ჩვეულებრივ, მოთამაშეებმა დღეში ერთხელ უნდა შეასრულონ. ზოგიერთი დავალება მოთამაშის თვითდაზიანებამდე მიყვანას გულისხმობს[72]. თვით დაზიანების ამსახველ ფოტოს ან ვიდეოს კი მოთამაშე კურატორს უგზავნის. კურატორები ზოგიერთ დავალებას მოთამაშეებს წინასწარ აძლევენ, ზოგიერთს კი იმავე დღეს. უკანასკნელი დავალებაა თვითმკვლელობა. დავალებების სია,

[69] ნ. თაბუკაშვილი, გართობიდან სადიზმამდე - კომპიუტერული თამაშების ბეწვის ხიდი და აგრესია მოზარდებში, 2017 წ.

[70] Evon, Dan. (February 27, 2017) Was a Game Called 'Blue Whale' Responsible for Dozens of Suicides in Russia?

[71] Parents Warned about new suicide game 'The Blue Whale Game' – Police Hour. Policehour.

[72] Baleia Azul, o jogo suicida que preocupa o Brasil e o mundo. Terra.

რომლებიც 50-დღეში უნდა იყოს დასრულებული, მოიცავს დილის 4:20 სთ-ზე გაღვიძებასა და ამწეზე ასვლას, ამავდროულად, სხვადასხვა ტიპის დავალებების შესრულებას. ლურჯი ვეშაპის მონაწილეები ვალდებულნი არიან მოუსმინონ მუსიკასა და უყურონ ვიდეოს, რომლებსაც მათ კურატორები უგზავნიან.[73]

დავალებები, თავიდან, არცთუ ისე რთულია მაგალითად, ღამის 4:20 სთ.-ზე (დრო, სასწაული სიზუსტით შერჩეული, ფსიქოლოგიური ზემოქმედებისათვის) გამოღვიძება და რაიმე საშინელებათა ვიდეოს ყურება (რაც, ბევრი თინეიჯერისთვის არაა რთული და უჩვეულო ამბავი, მეტწილს არც კი სძინავს, ამ დროს) ან უცნაური, ელექტრონული მუსიკის მოსმენა, ასევე, იგივე საათზე ახალ დავალებათა მიღება და შესრულებულთა ჩვენება – აქედან თამაშის კიდევ ერთი სახელწოდება – „4:20“, რომელსაც ასევე Я в игре, f 57 და f 58 სახელითაც იცნობენ.[74]

ძველი, „კლასიკური გამოცემა“ თამაშისა, 50 დღეს მოიცავდა, სადღაც 30-ე დღიდან კურატორის მიერ ფარული ბმულის მიცემით, რომელზე გადასვლის შემდეგ მოთამაშე, თავისდაუნებურად, საკუთარ კომპიუტერულ საიდენტიფიკაციო IP მისამართს (IP address), მისგან გამომდინარე კი მოთამაშე რეალურ საცხოვრებელ მისამართს ამჟღავნებდა და შემგომში უკვე, უფრო იოლ მსხვერპლად იქცეოდა, ვინაიდან, ბოლო დავალებამდე მისულს, უკან დახევის შემთხვევაში, კურატორი მას დაწვრილებით აღუწერდა მის საცხოვრებელ გარემოს, ეუბნებოდა, რომ მას აკვირდებიან და თუ „ლურჯ ვეშაპს“ არ შეასრულებს, მაინც მოაკვდინებენ ან ამოუწყვეტენ ოჯახის წევრებს. ამჟამად, კრიმინალისტებისგან დევნის გამო, ეს ვადა – 50 დღე, მნიშვნელოვნად „დაჩქარებულია“ – კიდევ ერთი შემაშფოთებელი ფაქტი.[75]

ერთ-ერთმა ჟურნალისტმა 15 წლის გოგონას როლი გაითამაშა. მისი დიალოგი კურატორთან შემდეგნაირად წარიმართა:

ჟურნალისტი : „ლურჯი ვეშაპის“ გამოწვევის მიღება მსურს.

კურატორი: დარწმუნებული ხარ? თუ დაიწყებ, უკან დასაბრუნებელი გზა აღარ იარსებებს.

ჟურნალისტი: რას ნიშნავს ეს? რას ნიშნავს – უკანადასბრუნელი გზა არ იარსებებს?

კურატორი: აღარ შეგიძლია თამაშის დატოვება, როდესაც დაიწყებ მას.

ჟურნალისტი: მზად ვარ.

[73] Evon, Dan,Was a Game Called 'Blue Whale' Responsible for Dozens of Suicides in Russia, 2017

[74] ინტერნეტ თამაშმა, რომელიც თვითმკვლელობით სრულდება, საქართველოშიც შემოაღწია, ჟურნალი ტაბულა, 27/05/2017 წ.

[75] ემიგრანტისგან ემიგრანტებისთვის https://georgians.gr/author/david-shannow/feed/

კურატორი: გამოწვევა, ყველა დავალება წარმატებით უნდა შეასრულო. და არავინ არ უნდა გაიგოს ამის შესახებ. როდესაც შეასრულებ დავალებას, მიგზავნი ფოტოსურათს. თამაშის ბოლოს კვდები. თანახმა ხარ?

ჟურნალისტი: თუ შეჩერება მომინდება?

კურატორი: გამორიცხულია. ყველა შენი მონაცემი ხელთ გვექნება უკვე. არ გაგახარებთ.

პირველი დავალება, რომელიც მიიღო იყო: „ამოიკვეთე f 58 მხარზე“. ჟურნალისტმა სცადა, გაეგზავნა ყალბი ფოტოგრაფია, დამუშავებული ფოტოშოპის მეშვეობით, მაგრამ კურატორი მიუხვდა და აღარ დაეკონტაქტა[76].

ადამიანი, რომელიც ამ „თვითმკვლელთა თამაშის“ უკან დგას სანკტ-პეტერგბურგელი ფილიპ ბუდეიკინი, სტუდენტი-ფსიქოლოგი, რომელიც გარიცხული იყო უნივერსიტეტიდან მეტსახელად ფილიპ ლისი-ა და იგი მხოლოდ 21 წლისაა. მეტიც, 2013 წელს, როდესაც ამ თამაშის „აწყობა“ დაიწყო, მხლოდ 17 წლის იყო. ამჟამად, ბრალი ედება, სულ მცირე 16 თვითმკვლელობის ინსპირირებაში. გასული წლის დეკემბრის თვიდან თავისულფებააღკვეთილია, რუსი სამართლდამცავების მიერ. შეკითხვაზე თუ რა იყო საბაბი ამ თამაშის წამოწყებისა ფილიპის სიტყვები იყო „თვითგამოხატვა, პოპულაროზისა და ლაიქების მოპოვება“. აღსანიშნავია კიდევ ერთი შემაძრწუნებელი ფაქტი: რუსეთის სასჯელთაღმსრულებელი კომიტეტის პრეს-სამსახურის ინფორმაციით, სანკტ-პეტერბურგის „კრესტი“-ში დატუსაღებული ბუდეიკინი ყოველდღიურად ათობით, ინტიმური ხასიათის წერილს ღებულობს თაყვანისმცემელი გოგონებისგან, რაც იმას ამტკიცებს, რომ მოთამაშეები ემოციურ კონტაქტშიც შედიან კურატორებთან[77].

ამრიგად შეგვიძლია ვთქვათ, რომ საქმე გვაქვს ჩვეულებრივ სოციოპათთან რომელსაც არანაირი სინანულის გრძნობა არ გააჩნია მის მიერ ჩადენილ ქმედებასთან დაკავშირებით.

2017 წლის 27 მაისს ტელეკომპანია „რუსთავი 2“-მა გაავრცელა ინფორმაცია, რომ თბილისში 12 წლის გოგონამ მეხუთე სართულიდან გადმოხტომით თვითმკვლელობა სცადა, ის საავადმყოფოში სხეულის მრავლობითი დაზიანებებით გადაიყვანეს. „რუსთავი 2“-ის ინფორმაციით, მან საავადმყოფოში მიყვანის შემდეგ თქვა, რომ ის მიცემულ დავალებებს ასრულებდა. როგორც ირკვევა მოზარდს გადახტომამდე დაუდგენელი პირები ინტერნეტით უკავშირდებოდნენ.[78]

---

[76] ემიგრანტისგან ემიგრანტებისთვის https://georgians.gr/author/david-shannow/feed/

[77] ემიგრანტისგან ემიგრანტებისთვის https://georgians.gr/author/david-shannow/feed/

[78] ინტერნეტ თამაშმა, რომელიც თვითმკვლელობით სრულდება, საქართველოშიც შემოაღწია, ჟურნალი ტაბულა, 27/05/2017 წ.

თითქმის ხუთთვიანი გამოძიების შემდეგ, შინაგან საქმეთა სამინისტრო სრული პასუხისმგებლობით აცხადებს, რომ ე.წ. ონლაინ თამაში "ლურჯი ვეშაპი", რასაც არასრულწლოვნების სუიციდის მცდელობებს უკავშირებდნენ, ქართულ ინტერნეტ სივრცეში არ არსებობს. ამის შესახებ შსს-მ განცხადება დღეს გაავრცელა.

ცენტრალური კრიმინალური პოლიციის დეპარტამენტის ორგანიზებულ დანაშაულთან ბრძოლის მთავარი სამმართველოს კიბერდანაშაულთან ბრძოლის სამმართველოში მიმდინარე წლის 30 მაისს დაიწყო გამოძიება ონლაინ თამაშის „ლურჯი ვეშაპის" შემქმნელების მიერ არასრულწლოვანთა თვითმკვლელობამდე და თვითმკვლელობის ცდამდე მიყვანის, ასევე, კომპიუტერული მონაცემის ან კომპიუტერული სისტემის უკანონოდ გამოყენების ფაქტზე, საქართველოს სსკ-ს 115-ე მუხლით და სსკ-ს 285-ე მუხლის 1-ლი ნაწილით. შსს-ს ცნობით, მიმდინარე გამოძიების პროცესში, პოლიციამ დეტალურად შეისწავლა უკლებლივ ყველა შეტყობინება, რომელიც შეეხებოდა სკოლის მოსწავლეების მიერ „ლურჯი ვეშაპის" შესაძლო თამაშის ფაქტებს: "ამასთან, საგანმანათლებლო დაწესებულებების მანდატურის სამსახურს მიეცა მითითება, თუკი რომელიმე მოსწავლეს სხეულზე რაიმე სახის დაზიანებას, მათ შორის, ნაკაწრის სახით, შეამჩნევდნენ, პოლიციისთვის ეცნობებინათ." როგორც შსს აცხადებს, სამართალდამცველებმა, მიღებული შეტყობინებების საფუძველზე, რამდენიმე ათეული არასრულწლოვანი გამოკითხეს. უწყების განცხადებით, გამოძიება თითოეული შეტყობინების თუ განცხადების საფუძვლიანად და სიღრმისეულად გამოძიების მიზნით, გარდა არასრულწლოვანთა გამოკითხვისა, აქტიურად იყენებდა კვალიფიციური ფსიქოლოგების დახმარებას. მათი ცნობით, ასევე განხორციელდა არასრულწლოვნების სოციალური ქსელის პირადი პროფილების, კომპიუტერული ტექნიკისა და მობილური ტელეფონების დათვალიერება. ამასთან, შინაგან საქმეთა სამინისტროს განცხადებით, მიმდინარე გამოძიების პროცესში, არაერთი სხვა კომპლექსური საგამოძიებო მოქმედება ჩატარდა:"სრული პასუხისმგებლობით ვაცხადებთ, რომ დღეის მდგომარეობით, საქმეში არსებული მასალებიდან გამომდინარე, ქართულ ინტერნეტ სივრცეში ე.წ. ონლაინ თამაში "ლურჯი ვეშაპის" არსებობის რეალური ფაქტი არ დადასტურებულა."[79]

ქართულ ინტერნეთ სივრცეში გამოჩნდა, ახალი საშიში თამაში რომელიც მსოფლიოშია ცნობილი. იგი ლურჯი ვეშაპის შემდეგ საქართველოშიც პოპულარული ხდება. სქემა იგივეა ჯგუფში აწევრიანებენ მოზარდებს, შემდეგ შედიან ნდობაში, იწყებენ საფრთხის შემცველი

[79]გ. დიასამიძე, ჟურნალი ნეტგაზეთი, „ლურჯი ვეშაპი" ქართულ ინტერნეტში არ არსებობს - ხუთთვიანი გამოძიების შედეგები, 14/10/2017 წ.

დავალებების მიცემას. საბოლოო მიზანი კი მათი სრული დამორჩილებაა. ერთ-ერთი ბავშვის მშობელი აცხადებს, რომ თამაშით მისი მცირეწლოვანი შვილიც დაინტერესებული იყო, თუმცა მან დროულად მოახდინა რეაგირება და შვილის დაცვა დროულად შეძლო. ახალი საშიში ინტერნეტ თამაში არაბული წარმოშობისაა ეს თამაში გოგონაზეა, რომელიც ახლო აღმოსავლეთში ცხოვრობდა XVIII საუკუნეში და კავშირი ჰქონდა სულებთან. თამაშიდან შიში მოდის მშვიდად, სიუჟეტურად, შინაარსობრივად და არა ყვირილით ან სხვა ეფექტებით. ამ ეტაპზე, თამაში 9,407,698 მომხმარებელს აქვს გადმოწერილი[80]. თამაშში ძირითადად კითხვა პასუხებია, ვირტუალური მარიამი მოთამაშეს კონკრეტულ დავალებებს აძლევს. ეს შეიძლება იყოს ბნელ ოთახში გასვლა, საშინელებათა ფილმის ნახვა და ა.შ. დავალებები თანდათან რთულდება, ბოლო მისია რომელსაც მსხვერპლი ასრულებს სასაფლაოზე გასვლაა. საქართველოში „მარიამ გეიმმა“ უკვე არაერთი მოზარდი დააინტერესა. ამის შესახებ სამოქალაქო აქტივისტი საუბრობს, რომელიც ამ მიმართულებიტ უკვე წლებია მუშაობს. ნანა ბერძენიშვილმა თამაშის პრინციპი შეისწავლა, იგი ყვება, რომ გართობის მიზანი არასრულწლოვანის სრულად დამორჩილება და მის ფსიქიკის სრული შერყევაა რაც შესაძლებელია სუიციდით დამთავრდეს.

მიუხედავად იმისა რომ არსებობს +18 ნიშნები კომპიუტერულ თამშებზე ეს არ იძლევა იმის შესაძლებლობას, რომ ინტერნეტით მოსარგებლე არასრულწლოვნები დავიცვათ იმ კომპიუტერული თამაშებისაგან, რომელთა უკან მომაკვდინებელი საფრთხეები იმალება. ამის გათვალისწინებით სახელმწიფომ უნდა უზრუნველყოს ინტერნეტ პროვაიდერების გაკონტროლება საიმისოდ, რომ ყველა ასაკის მომხმარებელს არ მიეცეს შესაძლებლობა ისარგებლოს კონკრეტული ვებგვერდებით. მართალია აღნიშნული რთული და შრომატევადი პროცესია თუმცა ვფიქრობ მონდომების შემთხვევაში შესაძლებელი.

[80] თ. უთურგაშვილი, ფორტუნა, მშობლებო გთხოვთ გააკონტროლოთ! - ახალი სახიფათო თამაში ქართულ ინტერნეტსივრცეში, 12/06/2020 წ.

თავიVI.კიბერტერორიზმი

დღევანდელ დღემდე ცივილიზებული სამყარო მეტნაკლებად მშვიდად ცხოვრობდა, არსებობდა საფრთხეები, თუმცა არსებობდა მათი შეკავების მექანიზმებიც. დღეს ახალი გამოწვევების წინაშე ვართ და ეს წესრიგი მთლიანად მოიშალა. სწორედ ასეთ გამოწვევებს ეწოდებათ ჰიბრიდული გამოწვევები, სადაც კონვენციური, ბირთვული, ეკონომიკური საფრთხე და საინფორმაციო სივრცე ერთიანობაშია მოქცეული იმისთვის, რომ პოლიტიკური ინტერესები გატარდეს. ხშირად ვამბობ ხოლმე, რომ ვირტუალურ სივრცეში უკვე მიმდინარეობს მესამე მსოფლიო ომი. ფრონტის ხაზი კი თითოეული ადამიანის გონებაში გადის. რაც უფრო მეტად დაიპყრობს ადამიანის გონებას, მით უფრო გავლენიანი იქნება ის. ამას აკეთებენ ტერორისტები ამას აკეთებს რუსეთიც და ბუნებრივია, რომ საინფორმაციო ველს ამ საკითხში ძალიან დიდი მნიშვნელობა აქვს.[81]

დღეს მეწარმეობა, ხელისუფლება, ინდუსტრია და საზოგადოება მიჯაჭვულია ინფორმაციასთან, ეს კი ახალ შესაძლებლობებს უხსნის ტერორიზმს. კიბერ ტერორიზმი არის კომპიუტერზე, ქსელზე და მათში არსებულ ინფორმაციაზე შეტევის ან შეტევის განხორციელების მუქარა, სახელმწიფოს ან მისი ხალხის პოლიტიკურად, სოციალურად, რელიგიურად ან იდეოლოგიურად დაშინების მიზნით. თუმცა ეს განმარტებაც არაა ზუსტი, რადგან კიბერ ტერორიზმი ასევე მოიცავს, სახელმწიფო ფინანსებზე ან ეროვნულ კომპანიებზე თავდასხმას და მათი მონაცემების გამოყენებას სხვადასხა ფულადი თუ სხვა სახის მაქინაციებისთვის, რომელიც მიმართულია ქვეყნის წინააღმდეგ[82].

კიბერტერორისტად შეგვიძლია მივიჩნიოთ პირი/ჯგუფი, რომელიც ზემოთ დასახელებულ ქმედებებს განახორციელებს, ან კიბერ ტერორიზმის ფაქტად შევრაცხოთ ქმედება, რომელსაც განახორციელებს ტერორისტული დაჯგუფება საკუთარი ინტერესებისათვის, რომელიც იმავდროულად ან მომავალში სახელმწიფოებისა და მმართველობების წინააღმდეგ იქნება გამოყენებული. კიბერტერორისტები იჭრებიან სახელმწიფო სტუქტურების კომპიუტერულ ქსელებში და იპარავენ სახელმწიფო დონის უსაფრთხოების ინფორმაციებს. ასევე ავრცელებენ ცრუ ინფორმაციას, რათა საზოგადოებაში დათესონ პანიკა და წარმოშვან დესტაბილიზაცია. შესაძლოა გაუკეთონ პროვოცირება სხვადასხვა ანტისამთავრობო მოძრაობებს და სხვა. კიბერტერორისტების მიზანს, არა მხოლოდ სახელმწიფო სტურქტურები და ეროვნული თუ ტრანსნაციონალური კომპანიები წარმოადგენს, არამედ უბრალო მოსახლეობაც. ისინი იყენებ ფიზიკური პირის

[81] კიბერ უსაფრთხოების სტრატეგია და მთავარი გამოწვევები, 20/05/2017 წ.
[82] ნ. კოხრეიძე, CYBERLOW- კიბერსივრცის სამართალი:კიბერტერორიზმი, 15/05/2012 წ.

მონაცემებს სხვადასხვა მაქინაციების ჩასატარებლად და კვალის დასაფარავად. კიბერტერორისტებმა შესაძლოა საზოგადოებას მიაყენონ სერიოზული ფსიქოლოგიური ზიანი, ინტერნეტ სივრცეში სხვადასხვა აკრძალული მასალის გავრცლებით, ან ტყუილი ე.წ „ფეიქი“ მასალის შემქნითა და მიწოდებით. კიბერტერორისტული ქმედებები ხშირად იჩენს თავს ომისა და კონფლიქტების დროს. შესაძლოა კიბერ თავდასხმა ერთმა ქვეყანამ განახორციელოს მეორეზე. მაგალითად 2008 წლის რუსეთ-საქართველოს ომის დროს, რუსეთი თავს დაესხა ქართულ საიტებს, შექმნა ინფორმაციული ვაკუუმი, რაც კიბერ ტერორიზმის ერთ-ერთი საშუალებაა საზოგადოებაში პანიკის გამოსაწვევად[83].

კიბერ ტერორისტული შეტევის განხორციელებების განზრახვა შეიძლება მრავალი სახის იყოს, ეკონომიკური ზიანის მიყენებიდან დაწყებული, ფიზიკური ზიანით დამთავრებული. მიუხედავად იმისა, რომ კიბერ შეტევებმა გამოიწვიეს მილიარდობით დოლარის ზიანი და მილიონობით ადამიანის ცხოვრებას შეეხენ, ჩვენ მაინც არ გვინახავს ნამდვილი კატასტროფული კიბერ ტერორიზმი. რა იქნება მისი მთავარი მახასიათებლები?

პირდაპირი ფინანსური ზიანი:

- გაყიდვების ჩავარდნა
- ქსელის შეფერხებები, წყვეტილი კავშირი მომხმარებლებისათვის
- სადაზღვევო ზიანის ანაზღაურობა გასაჩივრებიდან გამომდინარე
- ინტელექტუალური საკუთრების დაკარგვა
- გამოძიების ხარჯები
- კრიტიკული კომუნიკაციების დაკარგვაარ აპირდაპირი ფინანსური ზიანი
- არსებული ფინანსური სისტემების მიმართ უნდობლობის ზრდა
- გლობალურად გამქრალი რეპუტაცია
- დაძაბული სამეწარმეო ურთიერთობა, შიდა და საერთაშორისო
- მომავალი კლიენტებისგან მიღებული შემოსავლის დაკარგვა
- სახელმწიფოსა და კომპიუტერული ინდუსტრიის მიმართ ნდობის გაქრობა[84]

დღემდე არსებულმა კვლევებმა აჩვენა, რომ კრიტიკული ინფრმაციული ინფრასტრუქტურა პოტენციურად ღიაა კიბერ ტერორისტული შეტევებისათვის. ინფორმაციული სისტემების მზარდი გართულება ქმნის ახალ საფრთხეებსა და გამოწვევებს IT მენეჯმენტისათვის. იმ შეთხვევაშიც კი, თუ ტექნოლოგიები მთლიანად "ჯავშანში მოთავსდებიან", ამა თუ იმ ორგანიზაციის წევრები ე.წ.

[83] ნ. ჩერქეზიშვილი, კიბერ ტერორიზმი (სტუდენტური კონფერენცია) ავტორი, 03/10/2015 წ.
[84] CYBERLOW- კიბერსივრცის სამართალი:კიბერტერორიზმი http://ilawge.blogspot.com/2012/05/21.html

ინსაიდერები მაინც შეძლებენ მასში უნებართვოდ შეღწევის განხორციელებას, დამოუკიდებლად ან ტერორისტების დახმარებით[85].

თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიუროს ყოფილი ხელმძღვანელის, ანდრია გოცირიძის თქმით, კიბერუსაფრთხოების კუთხით, ერთადერთი რეალური საფრთხის შემცველი რუსეთია: "იმისათვის, რომ სახელმწიფომ ადეკვატური რეაგირება მოახდინოს, გაცნობიერებული უნდა ჰქონდეს კიბერ საფრთხის შემცველი ფაქტორები. ეს კლასიკაა და ახალს ვერაფერს ვამბობ. ისევე როგორც მსოფლიოს სხვა ქვეყნებისთვისაც ჩვენთვისაც კიბერ საფრთხეების შემცველი ფაქტორები არიან მაღალ განვითარებული კიბერ პოტენციალის მქონე ქვეყნები. თუ ავიღებთ საფრთხის მნიშვნელობას ჩვენი ჩრდილო მეზობელი ერთადერთი ფაქტორია, რომელსაც აქვს იმის შესაძლებლობა, რომ მასობრივი ზარალი და მსხვერპლი მოიტანოს. მხვედველობაში ის მაქვს, რომ რუსეთის შემტევ კიბერ პოტენციალში არსებობს შესაძლებლობა, წვდომა მოიპოვოს ინფრასტრუქტურის მაკონტროლებელ სისტემებზე და განახორციელოს დარტყმა. გასაგები რომ იყოს, შემიძლია გავიხსენო უკრაინაში მომხდარი ფაქტი, როდესაც მთელი დასავლეთ უკრაინა ელექტროენერგიის გარეშე დარჩა - ადვილი წარმოსადგენია თუ რა საფრთხის შემცველი შეიძლება იყოს ის საქართველოსთვის"[86].

ერთ-ერთი საერთაშორისო ანალიტიკური ფონდის მონაცემებით (SHADOWSERVER) DoS შეტევა ჯერ კიდევ 2008 წლის 18 ივლისს დაფიქსირდა. ხოლო 8 აგვისტოდან ფართო მასშტაბიანი ინტერნეტშეტევები განხორციელდა სამხრეთ ოსეთის სახელისუფლებო და მედია საიტებზე. როგორც (SHADOWSERVER)-ის მოხსენებებიდან ჩანს ამ კიბერშეტევების უკან "პატრიოტი" რუსი ოპერატორები იდგნენ, რომლებიც ფორუმებზე და უცხოურ საიტებზე მითითებებს იძლეოდნენ მომავალი დაბომბვის შესახებ: ,,გაიმარჯვე+მიყვარხარ+რუსეთი" (1 win+love+in+Rusia 807). დამკვირვებლების მონაცემებით საქართველოს საიტები ბიზუს კოკოვს სერვერიდან იბომბებოდა, ეს საიტი მოგვიანებით "JULY SERVER"-მა ჩაანაცვლა[87].

2009 წელს, რუსეთ-საქართველოს ომის წლისთავზე, ინტერნეტში ნამდვილი ბრძოლა გაჩაღდა. დაპირისპირება იმდენად მასშტაბური იყო, რომ მსოფლიოს სხვადასხვა კუთხეში მცხოვრებ უამრავ ადამიანს შეეხო. ამის შესახებ წამყვანი უცხოური მედია საშუალებებიც წერდნენ – New York Times, CNET, The Register და… ცდილობდნენ გაერკვიათ რაში იყო საქმე, რატომ დაიბლოკა ინტერნეტ სერვისები, რომლებსაც მილიონობით ადამიანი იყენებს. უბრალოდ, ერთ

[85] CYBERLOW- კიბერსივრცის სამართალი:კიბერტერორიზმი http://ilawge.blogspot.com/2012/05/21.html
[86] კიბერ უსაფრთხოების სტრატეგია და მთავარი გამოწვევები, 20/05/2017 წ.
[87] მ. ცაცანაშვილი, ფეისბუქ გვერდი, აგვისტოს მოვლენების არასტანდარტული შეფასება, რომლის მიხედვით საქართველო მსხვერპლია და არა თავდამსხმელი, მარიამ ცაცანაშვილი, 08/06/2018 წ.

დღეს, რუსეთ – საქართველოს ომის წლისთავზე Twitter, Facebook, YouTube, Blogger, Livejournal-ი ჰაკერების სამიზნედ გადაიქცნენ, მათი მუშაობა შეფერხებული აღმოჩნდა. ყველაფრის მიზეზი კი, ამ სერვისების ერთი რიგითი ქართველი მომხმარებელი იყო, რომელიც ცნობილია მეტსახელით „Cyxymu“. იგი ცდილობდა სხვადასხვა ინტერნეტ სერვისების საშუალებით დაპირისპირებოდა რუსეთის პროპაგანდისტულ მანქანას და საქართველოდან დანახული რეალობა გაეცნო ინტერნეტ მკითხველისთვის. მაგალითად, მას მოჰყავდა ინფორმაცია იმის შესახებ, რომ რუსულმა ტანკებმა კონფლიქტის დაწყებამდე გადმოლახეს როკის გვირაბი. როგორც ჩანს, ვიღაც ვიღაცებმა მისი გაჩუმება გადაწყვიტეს. მაგრამ ზემოთ მოყვანილი სერვისების თავისებურებებიდან გამომდინარე, შეუძლებელია რომელიმე ერთი კონკრეტული მომხმარებლის დაბლოკვა და შესაბამისად, ამ სერვისების ყველა – მილიონობით მომხმარებელი დაიბლოკა. „Cyxymu“ კი ინტერნეტ სივრცის „ვარსკვლავი“ გახდა.[88]

როგორც The New York Times-ი თვლის, რუსული სამართალდამცავები თავისი არაკომპეტენტურობისა ან კორუმპირებულობის გამო არ ებრძვიან ჰაკერებს . ან კიდევ შეიძლება მიზეზი იმაშია, რომ რუსები ჰაკერების საქმიანობის გამო სიამაყეს გრძნობენ, ისინი ხომ მრავალმილიონიან კიბერ აფიორებს ახორციელებენ და მათი მსხვერპლი კი, ძირითადად, ამერიკის და ევროპის მოქალაქეები არიან[89].

6.1 კიბერტერორიზმის სისხლისსამართლებრივი დახასიათება

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 სხვა[90].

„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[91].

[88] ს. ასათიანი, კიბერ-ომი, 13/09/2019 წ.
[89] ს. ასათიანი, კიბერ-ომი, 13/09/2019 წ.
[90] ავტორთა კოლექტივი, სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეხუთე გამოცემა, გამომც. „მერიდიანი“,2017, გვ 281
[91] კ. ჩიხლაძე, კიბერტერორიზმი (ინფორმაციული ესე), ინფორმაციული ტექნოლოგიები, ყოველკვარტალური სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი“ №3 , 2012, გვ122

„ტერორიზმის გარშემო ერთგვარი აზრთა 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[92].

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[93].

ფაქტობრივად, ტერორისტულ ორგანიზაციებმა უახლოესი კომპიუტერული ტექნოლოგიები ტერორისტულმა აქტის ჩდენის საშუალებად აქციეს და ამით აღნიშნული დანაშაული უფრო საშიშ მოვლენად ექცა მსოფლიოს. კიბერტერორიზმი 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[94].

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,

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

[93] 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)

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

ნივთების შესახებ მათემატიკური, სიმბოლური ან ნებისმიერი სხვა სახით და მოძრაობის პროცესშია ლოკალური ან გლობალური კომპიუტერული ქსელით[95].

„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“[96].

ტერმინი „კიბერტერორიზმი“ პირველად 1980 წელს კალიფორნიის უსაფრთხოები სადადაზვერვის ინსტიტუტის მეცნიერ თანამშრომელმა ბარი კოლინმა გამოიყენა. 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[97].

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

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

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

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

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 გამოყენებულ იქნება ვაშინგტონის შეთანხმების მეხუთე პუნქტი, რომლის მიხედვითაც წევრი სახელმწიფოს მიმართ განხორციელებული შეტევა ითვლება შეტევად ალიანსის წევრ-სახელმწიფოებზე[98].

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"[99]. მავნე ფუნქციის მქონე პროგრამის მიზანი, უპირველეს ყოვლისა, არის სისტემებში შეღწევა და ამდენად, იქ შენახული ინფორმაციის კრიმინალური, კომერციული ან გამანადგურებელი მიზნებისთვის გამოყენება. ე.წ. „ბოროტი" პროგრამისაგან დასაცავად:

- ✓ გამოიყენეთ ანტი-ვირუსული პროგრამული უზრუნველყოფა
- ✓ გამოიყნებეთ დამცავი ბარიერი (Firewall)
- ✓ გააქტიურეთ „სპამის" და „ფიშინგის" ფილტრები
- ✓ გააქტიურეთ „მოციმციმე" სარეკლამო ფანჯრების (Pop-Up) ბლოკირება

აქვე გახსოვდეთ!

- მუდმივად განაახლეთ თქვენი კომპიუტერი უახლესი პროგრამული უზრუნველყოფით.

[98] ლ. პატარაია, კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, გამომცემლობა ,,სანი", თბ., 2012, გვ. 46

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

- დარწმუნდით, რომ კომპიუტერი სწორად არის კონფიგურირებული. ახლად შეძენილ კომპიუტერებს შესაძლოა არ ჰქონდეთ გააქტიურებული დაცვის პროგრამა, რაც დამნაშავის სასარგებლოდ იმუშავებს.
- აირჩიეთ ძლიერი კოდი და არ გამოააშკარაოთ იგი- პაროლები ინტერნეტ სარგებლობისგანუყოფელ ნაწილს წარმოადგენს, ინტერნეტ შესყიდვები და ინტერნეტ ბანკინგი შეუძლებელია მის გარეშე.
- დაიცავით თქვენი კომპიუტერი სპეციალური ანტი-ვირუსული პროგრამებით. პირველადი დამცავი მექანიზმი არის თქვენი კომპიუტერის „ფაიერვოლი“. სწორედ იგი უზრუნველყოფს შემავალი და გამავალი ინფორმაციის კონტროლს.
- ონლაინ შემოთავაზებები - ნუ აყვებით ემოციებს და ნუ მიიღებთ არარეალურად მომგებიან შემოთავაზებებს უცხო პირებისგან.
- რეგულარულად შეამოწმეთ საკრედიტო ბარათისა და ინტერნეტ ბანკინგის პირადი მონაცემები. ე.წ. ,,ტერმინალი''-თ მომსახურების ან ნივთის საფასურის გადახდის დროს, ყურდღება მიაქციეთ საკრედიტო ბარათის მიმღები პირის ქმედებას და არ დაუშვათ ბარათის ფიზიკური გასვლა თქვენი ვიზუალური მეთვალყურეობის არედან[100].
- თავი შეიკავეთ საეჭვო ინტერნეტ საიტებზე ონლაინ გადახდებისა და საკრედიტო ბარათის მონაცემების დაფიქსირებისგან.
- ბანკომატიდან თანხის განაღდების დროს, ყურადღება მიაქციეთ ხომ არ არის მასზე განთავსებული რაიმე ისეთი მოწყობილობა, რომელიც ადრე არ შეგინიშნავთ. ასეთის აღმოჩენის შემთხვევაში შეატყობინეთ შესაბამის საბანკო დაწესებულებას და პოლიციას.
- ყურადღება მიაქციეთ ბავშვების ინტერნეტში შესვლას, თვალყური ადევნეთ ვებ-გვერდებს, რომლებსაც ისინი ხშირად სტუმრობენ. აკონტროლეთ უცხო პირთა მიერ მათთან სოციალური ქსელების ან ელექტრონული ფოსტის მეშვეობით დაკავშირების მცდელობები.
- დაიცავით თქვენი პერსონალური ინფორმაცია - გამოიჩინეთ განსაკუთრებული სიფრთხილე, როდესაც აზიარებთ თქვენს პირად მონაცემებს.
- არ უპასუხოთ სპამ წერილებს - პასუხის გაცემით თქვენ ადასტურებთ, რომ თქვენი ელ-ფოსტის მისამართი არის აქტიური და ამის შემდეგ უფრო მეტი არასასურველი წერილი მოგივათ.

[100] https://police.ge/files/proeqtebi_reporma%20photos/organizebuli-danashauli/kiberdanashauli-informacia-biznesistvis.pdf

- არ გახსნათ სპამ წერილში მითითებული არცერთი ლინკი (ბმული) რა შინაარსისაც არ უნდა იყოს ის, ლინკზე დაჭერით შესაძლოა გადახვიდეთ სახიფათო ვებ-გვერდზე.
- არ გახსნათ სპამ წერილში თანდართული ფაილი (attachment) , რადგან შეიძლება შეიცავდეს ვირუსს ან მავნე პროგრამას.
- არ გამოაქვეყნოთ თქვენი ელ-ფოსტის მისამართი ვებ-გვერდზე ან ფორუმზე, რადგან სპამ-ბოტები ათვალიერებენ ვებ გვერდებს და ელ-ფოსტის მისამართის პოვნისას ავტომატურად შეაქვთ სპამ სიაში.
- შექმენით დამატებითი ელ-ფოსტის მისამართი - თუ თქვენ ხშირად რეგისტრირდებით სხვადასხვა ვებ გვერდზე, ონლაინ სერვისებზე ან რაიმეს ყიდულობთ ინტერნეტის მეშვეობით, ამისათვის შექმენით სხვა ელ-ფოსტის მისამართი(ები), ეს მოგცემთ საშუალებას თქვენს ძირითად მისამართზე ნაკლები არასასურველი გზავნილი მოვიდეს[101].
- არ გადაამისამართოთ უცნობი წერილები - თუ თქვენ უცნობისაგან მოგივიდათ წერილი, სადაც გთხოვენ გაავრცელოთ რაიმე ინფორმაცია და გადაუგზავნოთ თქვენს მეგობრებს, არ გააგზავნოთ ის, რადგან ამ გზით სპამერს შეუძლია უფრო მეტი ელ-ფოსტის მისამართის გაგება.
- გამოიყენეთ თქვენი ელ-ფოსტის პროგრამის ფილტრი (Outlook, Thunderbird,The Bat, Live Mail), თქვენი სურვილის მიხედვით შეგიძლია შექმნათ წესები (rule), სადაც მიუთითებთ რის მიხედვით (From, Subject, Text) დაიბლოკოს არასასურველი წერილები ან გადაამისამართოთ სხვა ყუთში.
- გამოიყენეთ ანტივირუსი - ბევრ თანამედროვე ანტივირუსულ პროგრამას აქვს ანტი-სპამ ფუქნცია.

თუ თქვენ გახდით კიბერ თავდასხმის მსხვერპლი ან ფლობთ ინფორმაციას კიბერდანაშაულის თაობაზე, შეგიძლიათ დაუკავშირდეთ კიბერ დანაშაულთან ბრძოლის სამსახურს შემდეგ საკონტაქტო მონაცემებზე:

24 საათიანი უფასო ცხელი ხაზი - 112

ტელ: 2 41 12 96, 2 41 17 67;

ელ–ფოსტა: cybercrime@mia.gov[102].

[101] https://police.ge/files/proeqtebi_reporma%20photos/organizebuli-danashauli/kiberdanashauli-informacia-biznesistvis.pdf

[102] https://police.ge/files/proeqtebi_reporma%20photos/organizebuli-danashauli/kiberdanashauli-informacia-biznesistvis.pdf

თავი VII. კვლევის შედეგები

კვლევის ყოველი თავი დაწერილია თეორიული მასალის მეშვეობით, რომელთა საბოლოო ანალიზითაც მივედით შედეგებამდე. დასაწყისში სწორედ ამ გამოყენებულ ლიტერატურას მიმოვიხილავთ. შემდეგი თავი ეხება კიბერნეტიკის განვითარების ტენდენციებს და კიბერდანაშაულთან დაკავშირებული კანონის ისტორიის შექმნას და საერთაშორისო პრაქტიკას, შემდეგ კი განხილულია თანამედროვე ტექნოლოგიები როგორც კიბერსივრცის იარაღი, კომპიუტერული სისტემის აგებულება და ინტერნეტ სამყაროს მოკლე მიმოხილვა.

მომდევნო თავში განხილულია, კიბერდანაშაულის სისხლისამართლებრივი დახასიათება ქართულ კანონმდებლობაში და საერთაშორისო სტანდარტები. აღნიშნულთან დაკავშირებით ვხედავთ თუ რამდენად სწორად არის გაგებული ცნების მნიშვნელობა და რამდენად სწორად არის ჩამოყალიბებული ის ქართულ კანონმდებლობაში. ასევე ნათლადაა გამოკვეთილი ის მიმართულებები და რეკომენდაციები რასაც ევროპული კონვენცია „კიბერდანაშაულის შესახებ“ გვთავაზობს და გვიზიარებს.

მნიშვნელოვანი არის წინამდებარე ნაშრომის სრულყოფილი გამოკვლევისთვის კიბერდანაშაულთან დაკავშირებული ქართული საკანონმდებლო რეგულაციები, რომელთან ერთადაც განვიხილავ, კიბერდანაშაულის სახეებსა და მისი სუბიექტებს ასევე ინტერნეტ სივრცეში არსებულ მომაკვდინებელ თამაშებს. ზემოაღნიშნულ, კიბერდანაშაულთან დაკავშირებულ საკანონმდებლო რეგულაციებთან მიმართებაში მნიშვნელოვანია გვახსოვდეს, იმისათვის, რომ ქვეყანაში კიბერდანაშაული შემცირდეს საჭიროა სწორი კრიმინალური პოლიტიკის არსებობა. აღნიშნული პოლიტიკა საკუთარ თავში არ უნდა გულისხმობდეს და მოიცავდეს მხოლოდ რეპრესიული ქმედებების განხორციელებას. იგი საკუთარ თავში უნდა მოიაზრებდეს სისხლის სამართლებრივი სასჯელის გარდა სხვა პრევენციული ღონისძიებების განხორციელებასაც.[103] ამასთანავე უნდა ღინიშნოს ისიც, რომ კრიმინოლოგია როგორ მეცნიერება მნიშვნელოვან როლს თამაშობს ქვეყნის კრიმინალური პოლიტიკის ჩამოყალიბებაში. იმდენად რამდენადაც კრიმინოლოგია იკვლევს დანაშაულს და მის გამომწვევ მიზეზებს, იგი საუკეთესო გარანტიაა იმისა, რომ არსებული ვითარების, მდგომარეობის, რაციონალური და ჯეროვანი შეფასება მოხდეს, რაც ჩემი აზრით მნიშვნელოვანია იმ არსისა და მორალისთვის რასაც დანაშაულის პრევენცია ეწოდება.

[103] მ. შალიკაშვილი, კრიმინოლოგია, II გამოცემა, თბ., 2011, გვ. 45

დასკვნა

ნაშრომის დასასრულს, განხილული კომპიუტერული დანაშაულის სისხლისამართლებრივი დახასითება და მასთან დაკავშირებული პრობლემები, შედეგია მრავალი წლის განმავლობაში, საქართველოში ჩამოყალიბებული არასწორი მიდგომის კიბერდანაშაულთან დაკავშირებით და ხსენებული დნაშაულის აქტუალობის. კიბერდანაშაული არასოდეს ყოფილა ქართველი მეცნიერების ღრმა კვლევის ობიექტი. შესაბამისად ამ თემაზე ქართული სამეცნიერო ნაშრომები არ მოგვეპოვება. აღნიშნულ თემასთან დაკავშირებით იწერება მხოლოდ ინტერნეტ სივრცეში: ბლოგები, პოსტები. იშვიათ შემხვევებში ჟურნალ-გაზეთებში სტატიები, თუმცა ესეც არ არის იმ სიღრმის კვლევებზე დამყარებული, რომ შეგვეძლოს მხოლოდ მათ დავეყრდნოთ რეალური პრობლემის შესაფასებლად.

ჩემს მიერ წარმოდგენილ ნაშრომში განვიხილე, ევროპის საბჭოს კონვენცია იმდენად რამდენადაც იგი შემხებლობაშია საქართველოს სისხლის სამართლის კოდექსთან. ასევე ნაშრომში განხილული მაქვს, ქართული კანონმდებლობა და სასამართლო პრაქტიკა.

რაც შეეხება იმ ცვლილებებსა და რეფორმებს რაც კონკრეტულად შეეხო სისხლის სამართლის კოდექსში კიბერდანაშაულის თავს, 2000 წლის 30 ივნისს და არა მხოლოდ ამ რეფორმებს, შეიძლება ითქვას, რომ მის ეფექტურობას დრო გვიჩვენებს. ხოლო რაც შეეხება საზოგადოებაში არსებული წესრიგის ურყეოფას, მას თავის მხრივ განაპირობებს ისიც, თუ რამდენად მზად დახვდება ან/და ინფორმირდება საზოგადოება, დაუპირისპირდეს კიბერთავდამსხმელებს.

აქედან გამომდინარე კიბერ უსაფრთხოება XXI საუკუნის ნამდვილი გამოწვევაა, რასთან გამკლავებაც

მხოლოდ სამართალმცოდნეების, საზოგადოების და უსაფრთხოების ექსპერტების აქტიური მონაწილეობით არის შესაძლებელი. ასევე უაღრესად მნიშვნელოვანია მოხდეს საზოგადოების ფართო მასების ინფორმირება იმასთან დაკავშირებით, თუ როგორ შეიძლება თავი აარიდოს იმ არასასურველ მოქმედებებს, რასაც ჰაკერები ჩადიან თავიანთი მართლსაწინააღმდეგო ქმედებებით. მართალია შინაგან საქმეთა სამინისტრო ყოველდღიურად მუშაობს იმაზე, რომ დაიცვას მოქალაქეები კიბერთავდასხმისგან, თუმცა

იმისთვის, რომ ხსენებული ორგანოს საქმიანობა მაქსიმალურად ეფექტური იყოს მნიშვნელოვანია თითოეულმა მოქალაქემ, თითოეულმა ჩვენგანმა ხელი შევუწყოთ მათ.

მიზანშეწონილად მიმაჩნია, რომ ე.წ. „DoS“ შეტევა განხილული იქნას როგორც დამოუკიდებელი კომპიუტერული დანაშაული, და კიბერდანაშაულის თავს დაემატოს ცალკე მუხლად. აღნიშნულ, “DoS“ შეტევაზე საუბარი მქონდა II-ე თავის 2.2 ქვეთავში. ასევე სასურველია, მასში არ მიეთითოს დათქმა „მნიშვნელოვან შეფერხებაზე“, რადგან საკმარისია მიეთითოს „კომპიუტერული სისტემის ფუნქციონირების შეფერხება“, ხოლო თუ კანონმდებელი აუცილებლად მიიჩნევს ზემო აღნიშნული ტერმინის გამოყენებას, მაშინ შეიტანოს მეტი სიცხადე მის განმარტებაში და მუხლს დაურთოს შესაბამისი შენიშვნა.

საქართველოს სსკ-ი სხვა ტიპის დანაშაულებზეც ითვალისწინებს იურიდიული პირის სისხლისამართლებრივ პასუხისმგებლობას, თუმცა კიბერდანაშაულთან დაკავშირებით, მიმაჩნია, რომ აღნიშნული საკითხი მოითხოვს სიღრმისეულ გააზრებას. განსაკუთრებით ორაზროვნებას იწვევს კოდექსის 107[1]-ე მუხლის მე-4 ნაწილი, რომლის მიხედვითაც იურიდიული პირი პასუხს აგებს იმ შემთხვევაშიც, დადგინდება თუ არა დანაშაულის ჩამდენი ფიზიკური პირი. ეს გარემოება, კი იმ პირობებში, როდესაც კომპიუტერული დანაშაულის მასშტაბები სცილდება ყოველგვარ ფიზიკურ და წარმოსახვით საზღვრებს, ბადებს შესაძლებლობას ზიანი მიადგეთ სრულიად უდანაშაულო იურიდიულ პირებს. აღნიშნულ საკითხთან დაკავშირებით, ჩემი პოზიცია, შეგიძლიათ ნახოთ ამ ნაშრომის II-ე თავში.

ასევე მიზანშეწონილად მიმაჩნია, ყველა ის დანაშაული, რომლის ჩადენის იარაღად შეიძლება გამოყენებული იყოს კომპიუტერი ან კომპიუტერული მოწყობილობა გაერთიანდეს სისხლის სამართლის კოდექსის ერთ თავში. მაგალითისთვის, შეგვიძლია გავიხსენოთ კიბერტერორიზმი, მუხლი 324[1], რომელიც საქართველოს სსკ-ის XXXVIII თავშია მოცემული. აღნიშნული დანაშაულის ჩადენისთვის საჭიროა როგორც ვიცით კომპიუტერი, ამიტომ მიმაჩნია, აღნიშნული დანაშაული გადატანილ იყოს სისხლის სამართლის კოდექსის XXXV თავში რაც კიბერდანაშაულს გულისხმობს.

მიუხედავად იმისა, რომ კიბერდანაშაული საქართველოში გავრცელებულ დანაშაულთა კატეგორიას არ განეკუთვნება, საშიშროება მაინც დიდია ვინაიდან ჩვენს ქვეყანაში დაცული კომპიუტერული სისტემები თითქმის არ არსებობს. შესაძლოა, კიბერდანაშაულის დაბალი მაჩვენებელი, საქართველოში დაკავშირებული იყოს მის ლატენტურ ხასიათთან. მაგალითად: ხშირია შემთხვევა როცა პიროვნებას უტეხენ მეილს თუმცა იგი ამას არაფრად აგდებს, მეტიც ამის შესახებ ის არავის ეუბნება გარდა მეგობრებისა მაშინ როცა ეს წმინდა წყლის დანაშაულია.

კიბერდანაშაულის ლატენტურ ხასითთან დაკავშირებით აშშ- ში ს. კარნის და კ. ალექსანდერის მიერ ჩატარდა კვლევა, სადაც ისინი ამბობენ: "იმ ფონზე, როდესაც ეს გამოკითხვა ასეთ საგანგაშო სურათს ქმნის, უსაფრთხოების ექსპერტები მიიჩნევენ, რომ კომპიუტერული დანაშაულის უმეტესობა არც დაფიქსირებულია და არც გამოვლენილი. ამ დასკვნას აშშ-ს მთავრობის ერთ-ერთი სააგენტოს მიერ გაკეთებული სტატისტიკა ამყარებს. ამ სააგენტოს კომპიუტერების უსაფრთხოების შესამოწმებლად მანქანებზე განზრახ განხორციელდა თავდასხმა. 38 000 სამიზნეზე, კომპიუტერიდან დაზარალებულ მანქანებში, შეღწევა წარმატებით განხორციელდა 65%-ში. წარმატებით დაზიანებული საიტების სისტემურმა ადმინისტრატორებმა დააფიქსირეს შეღწევის მხოლოდ 40%. ამ 40%-დან მხოლოდ 27%-მა განახორციელა გადაცემა. სხვა სიტყვებით, რომ ვთქვათ 38 000 დაზარალებული მანქანიდან 24 700-ში განხორციელდა შეღწევა, რაც აღიქვა მხოლოდ 988-ა მათგანმა და თავდასხმის შესახებ ინფორმაციის გადაცემა მოახერხა მხოლოდ 267-მა"[104].

როგორც ვხედავთ საკითხის აქტუალობა სულაც არაა დამოკიდებული ოფიციალური სტატისტიკის შედეგზე, რადგან კიბერდანაშაულის მაღალი ლატენტური ხასიათიდან გამომდინარე შეუძლებელია სრულად მისი გამოვლენა, შესაბამისად თუ კი დანაშაული არ გამოვლინდება შეუძლებელია მისი გამოძიება.

[104] უ. ზაქაშვილი, კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, თბ., 2013. გვ. 6.

გამოყენებული ლიტერატურა

1. საქართველოს კონსტიტუცია, თბ., 1995 წ;
2. საქართველოს სისხლის სამართლის კოდექსი, თბ., 1999, 2020 წლის 10 ივნისის მდგომარეობით;
3. საქართველოს მთავრობის დადგენილება N 252, საქართველოს ორგანიზებული დანაშაულის წინააღმდეგ ბრძოლის ეროვნული სტრატეგიის დამტკიცების შესახებ, 2013
4. ავტორთა კოლექტივი, სისხლის სამართლის კერძო ნაწილი, წიგნი II, თბ., 2012 წ;
5. ავტორთა კოლექტივი, სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეხუთე გამოცემა, გამომც. „მერიდიანი“ , 2017, გვ 281
6. მ. ლეკვეიშვილი, ნ. თოდუა, გ. მამულაშვილი. სისხლის სამართლის კერძო ნაწილი, წიგნი მეხუთე, ნაწილი II, თბ., 2017 წ.
7. უ. ზაქაშვილი, კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემები საქართველოში, თბ., 2013
8. მ. შალიკაშვილი, კრიმინოლოგია, II გამოცემა, თბ., 2011 წ.
9. თ. წერეთელი, სისხლის სამართლის პრობლემები, ტომი I, თბ., 2007 წ.
10. მ. ლეკვეიშვილი, ნ. თოდუა, გ. მამულაშვილი, სისხლის სამართლის კერძო ნაწილი, ნაწილი II, თბ., 2017 წ;
11. ავტორთა კოლექტივი, სისხლის სამართლის კერძო ნაწილი, წიგნი II, მეხუთე გამოცემა, გამომც. „მერიდიანი“,2017.
12. ვ. სვანაძე, კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები, კრებული 2016 წ.
13. ს. გურეშიძე, სტატია, „ტერორიზმი ინტერნეტში“, ახლო აღმოსავლეთი და საქართველო, თბ., 2008
14. ლ. პატარაია, კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, გამომცემლობა ,,სანი“, თბ., 2012.
15. ლ. პატარაია, კიბერ ტერორიზმი და კიბერ ომები, კიბერ კრიმინალი - ლეგალური და სადაზვერვო ასპექტები, 2012
16. თ. უგრეხელიძე, კიბერდანაშაული,როგორც XXI საუკუნის გლობალური გამოწვევა, 2019 წ.
17. რ. ტეტუნაშვილი, ვინ არის ჰაკერი?, 2019 წ.ჰაკერი

18. ნ. თაბუკაშვილი, გართობიდან სადიზმამდე - კომპიუტერული თამაშების ბეწვის ხიდი და აგრესია მოზარდებში, 2017 წ.
19. მოსამართლეების ტრენინგი ქსელურ დანაშაულში, ტრენინგის სახელმძღვანელო, პროექტი, 2010 წ.
20. კიბერ უსაფრთხოების სტრატეგია და მთავარი გამოწვევები, 20/05/2017 წ.
21. ნ. კოხრეიძე, CYBERLOW- კიბერსივრცის სამართალი:კიბერტერორიზმი, 15/05/2012 წ.
22. ნ. ჩერქეზიშვილი, კიბერ ტერორიზმი (სტუდენტური კონფერენცია) , 03/10/2015 წ.
23. მ. ცაცანაშვილი, ფეისბუქ გვერდი, აგვისტოს მოვლენების არასტანდარტული შეფასება, რომლის მიხედვით საქართველო მსხვერპლია და არა თავდამსხმელი, 08/06/2018 წ.
24. ს. ასათიანი, კიბერ-ომი, 13/09/2019 წ.
25. ჩიხლაძე კ., კიბერტერორიზმი (ინფორმაციული ესე), ინფორმაციული ტექნოლოგიები, ყოველკვარტალური სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი“ №3 , 2012.
26. ჩიხლაძე კ., კიბერტერორიზმი (ინფორმაციული ესე), ინფორმაციული ტექნოლოგიები, ყოველკვარტალური სამეცნიერო ჟურნალი „ბიზნეს-ინჟინერინგი“ №3 თბ., 2012,
27. ს. შენგელია, კიბერდანაშაული - XXI საუკუნის გამოწვევა, სტუდენტური სამართლებრივი ჟურნალი, თბ., 2011.
28. ინტერნეტ თამაშმა, რომელიც თვითმკვლელობით სრულდება, საქართველოშიც შემოაღწია, ჟურნალი ტაბულა, 27/05/2017 წ.
29. გ. დიასამიძე, ჟურნალი ნეტგაზეთი, „ლურჯი ვეშაპი“ ქართულ ინტერნეტში არ არსებობს - ხუთთვიანი გამოძიების შედეგები, 14/10/2017 წ.
30. თ. უთურგაშვილი, ფორტუნა, მშობლებო გთხოვთ გააკონტროლოთ! - ახალი სახიფათო თამაში ქართულ ინტერნეტსივრცეში, 12/06/2020 წ.
31. ინტერნეტ თამაშმა, რომელიც თვითმკვლელობით სრულდება, საქართველოშიც შემოაღწია, ჟურნალი ტაბულა, 27/05/2017 წ.
32. თ. კაციტაძე, გაზეთი “24 საათი”, კომპიუტერული დანაშაულები _ მსოფლიოს უდიდეს დანაშაულთა რიცხვში,
33. გ. ნაკაშიძე, სტატია, „კიბერტერორიზმი - XXI საუკუნის მწვავე გამოწვევა“, ჟურნალი ეკონომიკა და ბიზნესი, №4 ივლისი-აგვისტო, 2012
34. ფეისბუქ გვერდი, ისტორია - საინტერესო ფაქტები, 2015 წ.

35. მ. მუსელიანი, საინფორმაციო უსაფრხოების ფენომენი 21-ე საუკუნეში- კიბერუსაფრთხოება და მისი განმსაზღვრელი ფაქტორები (ამერიკა საქართველო)
36. Scientific and Practical Cyber Security Journal (SPCSJ) 2(3): 98-107 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)// file:///C:/Users/admin/Downloads/RO201904026578759ZK%20(1).pdf
37. In 1946, ENIAC required an estimated 174 kW. By comparison, a modern laptop computer may use around 30 W; nearly six thousand times less. Approximate Desktop & Notebook Power Usage. University of Pennsylvania.
38. Early computers such as Colossus and ENIAC were able to process between 5 and 100 operations per second. A modern "commodity" microprocessor (as of 2007) can process billions of operations per second, and many of these operations are more complicated and useful than early computer operations. Intel Core2 Duo Mobile Processor: Features. Intel Corporation.
39. Quittner, Joshua. "Tim Berners Lee—Time 100 People of the Century", Time Magazine, 29 March 1999. „He wove the World Wide Web and created a mass medium for the 21st century. The World Wide Web is Berners-Lee's alone. He designed it. He loosed it on the world. And he more than anyone else has fought to keep it open, nonproprietary and free
40. Evon, Dan. (February 27, 2017) Was a Game Called 'Blue Whale' Responsible for Dozens of Suicides in Russia?
41. Parents Warned about new suicide game 'The Blue Whale Game' – Police Hour. Policehour.
42. Baleia Azul, o jogo suicida que preocupa o Brasil e o mundo. Terra.
43. Evon, Dan,Was a Game Called 'Blue Whale' Responsible for Dozens of Suicides in Russia, 2017
44. 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).
45. Larry J. Siegel (2008) Criminology- Cyber crime and technology - Cyber terrorism: Cyber Crime With Political Motives . pp № 449
46. ფეისბუქ გვერდი, ისტორია - საინტერესო ფაქტები, 2015 წ. https://www.facebook.com/historyinterestingfacts/photos/A3/892572004128989/
47. ინტერნეტის დადებითი და უარყოფითი მხარეები - http://elearning.grena.ge/pluginfile.php/901/mod_resource/content/2/chapter1.pdf

48. http://police.ge
49. http://www.crime-research.org
50. https://police.ge/files/proeqtebi_reporma%20photos/organizebulidanashauli/kiberdanashauli-informacia-biznesistvis.pdf
51. https://iraklimk.wordpress.com
52. https://www.myvideo.ge/v/1974947
53. http://lawlibrary.info
54. http://worldofhackers1.blogspot.com/
55. https://mfa.gov.ge/News/-(1).aspx
56. http://police.ge/ge/projects/kiberdanashauli/kanonmdebloba-kiber-danashaulze-da-zogadi-politika
57. www. computer.howstuffworks.com/computer-hardware-channel.html.
58. https://sites.google.com/site/chemiproekti/internetis-ganvitarebis-istoria
59. SPAM-სპამი https://cert.gov.ge/uploads/Articles/SPAM1.pdf
60. ფიშინგი https://dea.gov.ge/?action=article&article_id=8&lang=geo
61. Malware – „ბოროტი პროგრამა“ https://dea.gov.ge/?action=article&article_id=5&lang=geo
62. Iberia Gaming Roleplay BOTNET-ბოტნეტი https://igrp.proboards.com/thread/28/
63. https://wol.jw.org/ka/wol/d/r20/lp-ge/102005242