კავკასიის საერთაშორისო უნივერსიტეტი

ხელნაწერის უფლებით

გიორგი ამაშუკელი

კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის პრობლემა.

სადოქტორო პროგრამა: სამართალი

სამეცნიერო ხელმძღვანელი: სერგო ჭელიძე, სამართლის დოქტორი,

ასოცირებული პროფესორი

სამართლის დოქტორის აკადემიური ხარისხის მოსაპოვებლად წარდგენილი

დისერტაციის

ავტორეფერატი

თბილისი 2022

სამეცნიერო ნაშრომი შესრულებულია კავკასიის საერთაშორისო უნივერსიტეტის სამართლის ფაკულტეტის სამართლის სადოქტორო პროგრამაზე.

სამეცნიერო ხელმძღვანელი: **სერგო ჭელიძე**

სამართლის დოქტორი, კსუ-ს ასოცირებული პროფესორი.

ოფიციალური რაცენზენტები: **ვლადიმერ მაჭარაშვილი**

სამართლის დოქტორი, კსუ-ს ასოცირებული პროფესორი.

ირაკლი იმერლიშვილი

სამართლის დოქტორი, გორის სახელმწიფო უნივერსიტეტის ასოცირებული პროფესორი

დისერტაციის დაცვა შედგება 2022 წლის 02 დეკემბერს, 15:00 საათზე, კავკასიის საერთაშორისო უნივერსიტეტის სამართლის ფაკულტეტის სადისერტაციო საბჭოს სხდომაზე.

მისამართი: 0141, თბილისი, ჩარგლის ქუჩა N-73; კავკასიის საერთაშორისო უნივერსიტეტის პირველი კორპუსი, 305-ე აუდიტორია.

დისერტაციის გაცნობა შეიძლება კავკასიის საერთაშორისო უნივერსიტეტის ბიბლიოთეკაში.

სადისერტაციო საბჭოს მდივანი: **ალექსანდრე გიორგიძე**

სამართლის დოქტორი,

ასოცირებული პროფესორი.

ნაშრომის ზოგადი დახასიათება

ადამიანთა მოდგმისთვის დამახასიათებელი ბუნებრივი ლტოლვა დესტრუქციული საქმიანობისკენ, ყველაზე აშკარად, ისე არსად არ მჟღავნდება, როგორც ეს კიბერსივრცეშია. საკითხი იმასთან დაკავშირებით, რომ კიბერტექნოლოგიების განვითარება, თავისთავად, პოზიტიური პროცესია და გაცილებით უფრო კომფორტულს ხდის ცხოვრებას, უდავოა. უდავოა ისიც, რომ ტექნოლოგიურმა რევოლუციამ უამრავი თავსატეხი გაუჩინა მსოფლიო თანამეგობრობას და მოგვევლინა ისეთ გამოწვევად, რომლის ტექნიკური და სამართლებრივი რეგულირება, ფაქტობრივად, შეუძლებელი აღმოჩნდა. განსაკუთრებული ყურადღება მიექცა ამ ვითარებას, XXI- ე საუკუნის დასაწყისში, როდესაც ტექნიკურ პროცესსა და მის სამართლებრივ რეგულირებას შორის გაჩნდა უაღრესად დიდი ნაპრალი და მისი შევსება დღემდე შეუძლებელია. მაგრამ, მთავარი მაინც ისაა, რომ თუ სამომავლო პერსპექტივაში, მსოფლიო თანამეგობრობის მიერ არ იქნება მიღებული ეფექტიან ღონისძიებათა მთელი კომპლექსი, კითხვის ნიშნის ქვეშ დადგება თავად ცივილიზაციის არსებობის საკითხი. ამიტომაა, რომ კიბერუსაფრთხოების საკითხს ექცევა, ზედმიწევნით, განსაკუთრებული ყურადღება და აყვანილია ეროვნული უსაფრთხოების რანგში. მის მოცულობით მნიშვნელობაზე მეტყველებს ისიც, რომ კიბერტექნოლოგიებმა კარდინალურად შეცვალა ომის წარმოების როგორც შინაარსი, ისე მისი არქიტექტურა. ამიტომ, საკითხი კიბერუსაფრთხოების აქტუალობასთან დაკავშირებით საყოველთაოდ ცნობილი ფაქტია და რაიმე განსაკუთრებული ამ მიმართულებით ვერ იქნება ნათქვამი.

როდესაც საუბარია კიბერუსაფრთხოების რეგულირებაზე, მხედველობაშია კომპლექსურ ღონისძიებათა მთელი კომპლექსი, რომელიც გულისხმობს ჰუმანიტარულ და ტექნიკურ მეცნიერებათა მონაცემებზე დაყრდნობით, ერთიანი, ზოგადსაკაცობრიო სტრატეგიის შემუშავებას და მისი განხორციელების ეფექტიან, მკაცრ სისტემათა შემუშავებას.

ამ მიმართულებით, მნიშვნელოვანი მისია აკისრია სისხლის სამართლის

მეცნიერებასაც, რომელმაც უნდა შეიმუშაოს სისხლისსამართლებრივი ზემოქმედების მექანიზმთა მოწესრიგებული სისტემა, სრულყოს და ხელი შეუწყოს საერთაშორისო კანონმდებლობასთან ჰარმონიზაციის პროცესს. ამ მიზნის მისაღწევად კი, უმნიშვნელოვანესია საკანონმდებლო საქმიანობის ისეთი არაპოპულარული, მაგრამ საჭირო მიმართულება, როგორიც კრიმინალიზაციაა.

შესაბამისად, **საკვლევი თემის აქტუალობა** უკავშირდება, სწორედ, კიბერსივრცეში წარმოშობილ სოციალურად საშიშ ქმედებათა კრიმინალიზაციის პრობლემებს, რაც, უპირველეს ყოვლისა, გულისხმობს კიბერდანაშაულებრივ ქმედებათა სისტემურ-სამართლებრივ მოწესრიგებას. ობიექტურობისთვის უნდა ითქვას, რომ თემის აქტუალობასთან დაკავშირებით, როგორც აღვნიშნეთ, არც ეროვნულ და არც საერთაშორისო სისხლის სამართლის მეცნიერებაში განსხვავებული მოსაზრება არ არსებობს. მეცნიერებაში აღიარებული შეხედულების თანახმად, ნებისმიერი საკითხი, რომელიც, ასე თუ ისე, უკავშირდება კიბერუსაფრთხოების საკითხებს, თავისთავად უკვე იძენს აქტუალობას. ამასთან, რაც ყველაზე მნიშვნელოვანია, ეს აქტუალობა განპირობებულია თავად საკითხის უკიდურესად კრიტიკული მდგომარეობით და საჭიროებს დროულ რეაგირებას. ზოგადად, მეცნიერებაში და, კერძოდ, სისხლისსამართლებრივ მეცნიერებაში არსებობს საკვლევ საკითხთა ისეთი კატეგორია, რომელთა გადაჭრას აქვს დიდი პრაქტიკული და მეცნიერული მნიშვნელობა. თუმცა, ამ პრობლემათა კვლევის დროში გაჭიანურებას არ მოჰყვება რაიმე არსებითი ზიანი სოციუმისთვის, რასაც ვერ ვიტყვით კიბერსივრცეთან მიმართებაში. აქ მდგომარეობა კარდინალურად განსხვავებულია და საჭიროებს დროულ რეაგირებას.

მხოლოდ ის ფაქტი, რომ ,,ჰაკერების'' მიერ უკვე მიტაცებული თანხები გაცილებით აღემატება, კაცობრიობის ისტორიაში, დანაშაულებრივი ქმედებით მთლიანად მიტაცებული მატერიალური სიკეთის ოდენობას, უკვე მეტყველებს მის მაღალ სოციალურ საშიშროებაზე, აღარაფერს ვამბობთ კიბერტექნოლოგიების სამხედრო-სტრატეგიულ სეგმენტზე.

ამგვარად, საკვლევი თემის აქტუალობის საკითხი, შეიძლება ითქვას, მოვლენათა

ზედაპირზე დევს და დავას არ იწვევს. ამასთან, იგი კიდევ უფრო წარმოჩინდება საკვლევი თემის კონკრეტულ პრობლემურ საკითხთა ჩამოყალიბებისას.

საკვლევი პრობლემის თვალსაჩინოებისთვის მიზანშეწონილია მეცნიერულად დასაბუთებულ კითხვათა დასმა, რომელიც საშუალებას მოგვცემს გარკვევით ჩამოვაყალიბოთ კვლევის საზრისი და განვსაზღვროთ თავად საკითხთა მეცნიერული ღირებულება.

ჩვენს მიერ შემოთავაზებულ კითხვათა არსი ასე გვესახება:

1. **რამ განაპირობა ,,კიბერდანაშაულებრივ" ქმედებათა კრიმინალიზაციის საჭიროება დამოუკიდებელ შემადგენლობებად?**
2. **ხომ არ შექმნა მსგავსმა პროცესმა სისხლისსამართლებრივ ნორმათა კონკურენციის ისეთი დონე, როდესაც მათი ინტერპრეტაცია სირთულესთანაა დაკავშირებული ან/და შეუძლებელი ხდება?**
3. **თუ ეს ასეა, ხომ არ იქონია ასეთმა საკანონმდებლო ხარვეზმა უარყოფითი ზეგავლენა საგამოძიებო და სასამართლო პრაქტიკაზე?**
4. **,,კიბერდანაშაული"- დამოუკიდებელი უმართლობა თუ დანაშაულის შემადგელობის ობიექტური მხარის ფაკულტატური ელემენტი?**
5. **,,კიბერდანაშაულის" ცნების პრობლემატურობა და მისი როლი დანაშაულის საკანონმდებლო და სასამართლო კვალიფიკაციაზე.**
6. **გაუფრთხილებლობა, როგორც ,,კიბერდანაშაულებრივ" ქმედებათა გამოვლინების შესაძლო და ბუნებრივი ფორმა.**

ამგვარად, წარმოდგენილი საკითხები, რომლებიც კრიმინალიზაციის ურთულეს

პროცესებთანაა დაკავშირებული, მიგვაჩნია, რომ პრობლემატურია, როგორც მეცნიერული, ისე პრაქტიკული თვალსაზრისით. გასაგებია ისიც, რომ სრულყოფილი და ამომწურავი პასუხების პრეტენზია არ უნდა გვქონდეს და იგი საჭიროებს შემდგომ მეცნიერულ კვლევებს. ამ ფონზე, შევეცდებით უფრო ცხადად და სრულყოფილად წარმოვაჩინოთ პრობლემათა აქტუალობა.

- ის გარემოება, რომ სოციუმის ტოტალური კომპიუტერიზაციის შედეგი

საინფორმაციო საზოგადოების ჩამოყალიბაა, ცხადია. ამასთან, კომპიუტერულ სისტემათა ინტერნეტიზაციამ იგი აქცია იმ საერთაშორისო არენად, სადაც ერთმანეთს დაუპირისპირდა ტრადიციულ და ლიბერალურ ღირებულებათა განსხვავებული შეხედულებები. როგორც აღმოჩნდა, ტექნოლოგიებმა შეუქცევადად დაიმკვიდრეს ადგილი სოციალური ცხოვრების აბსოლუტურად ყველა სფეროში და ხელი შეუწყვეს დანაშაულთა არა მარტო რაოდენობრივ, არამედ თვისებრივ სახეცვლილებასაც. ამასთან, არსებულმა და სამომავლო არასახარბიელო პერსპექტივებმა უბიძგა კანონმდებელს მკაცრი სისხლისსამართლებრივი პოლიტიკის გატარებისკენ და კრიმინალიზაციის პროცესის გააქტიურებისკენ.

არსებულმა ვითარებამ და კიბერსივრცეში წარმოშობილმა სოციალურად საშიშ ქმედებათა მრავალფეროვნებამ დაარწმუნა მსოფლიო თანამეგობრობა დაჩქარებულიყო მთელი რიგი საერთაშორისო თუ რეგიონული სამართლებრივი აქტების მიღების პროცედურა, ისევე, როგორც კანონმდებლობის ჰარმონიზაციის პროცესი. მაგრამ, როგორც რეალობამ გვიჩვენა, მიმდინარე პროცესში, როგორც ეროვნულ, ისე საერთაშორისო დონეზე, თავი იჩინა სამართლებრივმა ხარვეზებმა და შექმნა გარკვეული გაუგებრობა, ცალკეულ, სისხლისსამართლებრივ კონსტრუქციათა ჩამოყალიბებისას. მხედველობაში გვაქვს ,,კიბერდანაშაულებრივ'' ქმედებათა დამოუკიდებელ შემადგენლობათა კრიმინალიზაციის ტენდენცია. რა თქმა უნდა, კანონმდებელი ცდილობს ადექვატური პასუხი გასცეს სოციალურად საშიშ ქმედებათა მთელ წყებას და აწესებს სისხლისსამართლებრივ პასუხისმგებლობას. გასაგების ისიც, რომ კიბერდანაშაულებრივ ქმედებათა კრიმინალიზაცია ნაკარნახევია პრაქტიკული მოსაზრებებით. თუმცა, პრობლემურად გვესახება არა კრიმინალიზაციის პროცესი ან/და, თუნდაც, მკაცრი სისხლისსამართლებრივი პოლიტიკა, არამედ წმინდა სამართლებრივი საკითხები; ისეთი, როგორიცაა მსგავსი კატეგორიის ქმედებათა კრიმინალიზება დამოუკიდებელ შემადგენლობებად.

საქართველოს სისხლის სამართლის კოდექსის XXXV - ე თავი (კიბერდანაშაული) შედგება ხუთი შემადგენლობისგან:

< მუხლი 284. კომპიუტერულ სისტემაში უნებართვო შეღწევა

< მუხლი 285. კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის უკანონოდ გამოყენება

< მუხლი 286. კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა

< მუხლი 2861. კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა ფინანსური სარგებლის მიღების მიზნით

< მუხლი 2862. ყალბი ოფიციალური კომპიუტერული მონაცემის შექმნა

როგორც ვხედავთ, კანონმდებელმა მხედველობაში მიიღო კომპიუტერულ სისტემათა სფეროში დანაშაულებრივ ქმედებათა მაღალი სოციალური საშიშროების ფაქტორი და ცალკე თავი დაუთმო მას. ამასთან, ამ შემადგენლობათა სისხლისსამართლებრივი დაცვის ობიექტი კომპიუტერულ სისტემათა პარალელურად შეიძლება იყოს პირადი ცხოვრების საიდუმლოება, საკუთრება, პირადი მონაცემები თუ სხვა. როგორც არ უნდა იყოს საქმის ვითარება, ერთი რამ ცხადია: კანონმდებელი განსაკუთრებულ ყურადღებას უთმობს ტექნოლოგიურ კომპონენტს და თავისი შეხედულებისამებრ ახდენს ცალკეულ შემადგენლობათა კრიმინალიზებას. მაგრამ, ისევ პრაქტიკული საჭიროებიდან გამომდინარე, კვლავ დგება საკითხი ისეთ შემადგენლობათა კრიმინალიზებისა, რომელიც შინაარსობრივად კიბერდანაშაულია, მაგრამ ფორმალურად განთავსებულია სისხლის სამართლის კოდექსის სხვადასხვა თავებსა თუ კარში. აქაც, რა თქმა უნდა, კანონმდებელს ხელეწიფება მოახდინოს ამა თუ იმ სამართლებრივი კონსტრუქციის კრიმინალიზება საკუთარი მიხედულებით, მით უმეტეს, რომ საკითხი საყოველთაოდ აქტუალურია. ასე შეიქმნა კიბერტერორიზმის (324[1]-ე მუხლი), პირადი ცხოვრების ამსახველი ინფორმაციის ან პერსონალური მონაცემების ხელყოფა (157-ე მულის მე-2 ნაწილი), პირადი ცხოვრების საიდუმლოების ხელყოფა (157[1]-ე მუხლის მე-2 ნაწილი), კერძო კომუნიკაციის სადუმლოების დარღვევა (158-ე მუხლი), პირადი მიმოწერის, ტელეფონით საუბრის ან სხვაგვარი ხერხით შეტყობინების საიდუმლოების დარღვევა (159-ე მუხლი) და სხვა. მსგავსი ხასიათის შემადგენლობები სისხლის სამართლის

კოდექსში მრავლადაა და ეს ბუნებრივიცაა. ამასთან, გასათვალისწინებელია ის გარემოება, რომ კიბერტექნოლოგიების სულ უფრო მზარდი როლი სოციალური ცხოვრების ნებისმიერი სფეროში ბადებს ისეთ ურთიერთობებს, რომლებიც თავისი შინაარსით დანაშაულებრივია და საჭიროებს სისხლისსამართლებრივ რეაგირებას. თუ იმასაც გავითვალისწინებთ, რომ კიბერსივრცის ,,შესაძლებლობები'' ამოუწურავია, მაშინ გამოდის, რომ კანონმდებელს ყოველ ჯერზე მოუწევს ახალი შემადგენლობების კრიმინალიზება. ეს გარემოება რეალურია და ამის, არა თუ ნიშნები, არამედ პრაქტიკული წინააღმდეგობებიც სახეზეა. ამიტომ, კრიმინალიზაციის პროცესის ამ ფორმატით წარმართვა, უახლოვეს მომავალში, შექმნის, ერთი მხრივ, პრობლემებს საკანონმდებლო ტექნიკის თავალსაზრისით, როდესაც ჩვენ მივიღებთ მრავალტომიან სისხლის სამართლის კოდექსს და, მეორე მხრივ, გართულდება დანაშაულის საკანონმდებლო და სასამართლო კვალიფიკაცია.

უნდა ითქვას, რომ კიბერსივრცის უნივერსალური ბუნება, სრულად, თავსებადია ხელოვნურ ინტელექტთან და ამ ორი ფენომენის ტანდემი, რომლის გენეზისიც წარმატებით მიმდინარეობს, წარმოშობს ისეთ ურთიერთობათა წყებას, რომელსაც კაცობრიობა დღემდე არ იცნობდა. ამ შემთხვევაში, რა თქმა უნდა, ბუნებრივი იქნება დამოუკიდებელ დანაშაულებრივ შემადგენლობათა კრიმინალიზების საჭიროება და ამას ვერსად გავექცევით, მაგრამ მოცემულ ეტაპზე და, იმედია, უახლოვეს პერსპექტივაში, შესაძლებელია ერთგვარი სამართლებრივი კოლაფსის თავიდან აცილება, თუ შეძლებისდაგვარად, ,,კიბერტექნოლოგიური'' ელემენტები მოაზრებულ იქნება უკვე არსებულ, დანაშაულის ტრადიციულ შემადგენლობათა ფარგლებში.

- მიუხედავად იმისა, რომ კიბერდანაშაულებრივი შინაარსის ქმედებათა

კრიმინალიზაციის მსგავსი პროცესი ლეგიტიმურია და ნაკარნახევია პრაქტიკული, სისხლისსამართლებრივი მოთხოვნებით, იგი არამიზანშეწონილია სამართლებრივი თვალსაზრისით, რაშიც, უპირველეს ყოვლისა, იგულისხმება მისი სისტემურ-სამართლებრივი მოწესრიგება, როდესაც მსგავსი შემადგენლობები უსისტემოდაა გაბნეული სისხლის სამართლის კოდექსში და ქმნის ნორმათა კონკურენციის ისეთ

დონეს, რომლის დაძლევაც მისი ინტერპრეტაციის გზით გაძნელებულია თვით საკანონმდებლო დონეზე.

მაგალითად: სისხლის სამართლის კოდექსის მე-8 კარი დათმობილი აქვს ეკონომიკურ დანაშაულს და მასში ასახული ტრადიციული შემადგენლობები ითვალისწინებენ შესაბამის მაკვალიფიცირებელ ელემენტებს. კანონმდებელი, სისხლისსამართლებრივი პოლიტიკიდან გამომდინარე, თავად განსაზღვრავს შემადგელობის რომელ ნიშანს უნდა მიენიჭოს მაკვალიფიცირებელი გარემოების სტატუსი და აწესებს შესაბამის სასჯელს მისთვის. ამასთან, მაკვალიფიცირებელი გარემოებები გამომდინარეობენ მარტივი შემადგენლობებიდან და მოქცეულია ერთი მუხლის ფარგლებში. ასეა, სისხლის სამართლის კოდექსის 177-ე მუხლის(ქურდობა) მე-4 ნაწილის ,,დ'' ქვეპუნქტი, რომელიც ითვალისწინებს მაგისტრალურ მილსადენში ნავთობის ან გაზის ქურდობას, ისევე როგორც სხვა მაკვალიფიცირებელი გარემოებები. აღნიშნულთან დაკავშირებით, საინტერესოა სისხლის სამართლის კოდექსის 286^1 მუხლის შემადგენლობა, რომელიც ითვალისწინებს კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფას ფინანსური სარგებლის მიღების მიზნით. თუ სადავოდ არ გავხდით იმ გარემოებას, რომ ადგილი აქვს ერთი და იგივე შინაარსის მომწესრიგებელ ნორმებს (თუნდაც ნაწილობრივ), მაშინ უნდა გაირკვეს კანონმდებლის ნება იმასთან დაკავშირებით, თუ რომელი ნორმაა ზოგადი და რომელი სპეციალური. შესაძლებელია ისიც, რომ იგი საერთოდ უმართლობის დამოუკიდებელი სახე იყოს. აღნიშნული საკითხი საინტერესოა ქმედების საკანონმდებლო კვალიფიკაციის ეტაპზე, რადგანაც ნებისმიერი ბუნდოვანება უცილობლად გამოიწვევს სირთულეებს ქმედების სასამართლ კვალიფიკაციის დროს და გახდება არაერთგვაროვანი სასამართლო პრაქტიკის დამკვიდრების საფუძველი.

მოცემულ შემთხვევაში, 177-ე მუხლის შემადგენლობა, 286^1 მუხლთან მიმართებაში ზოგადია, ამიტომ პრიორიტეტი მიენიჭება უფრო ახალ და სპეციალურ ნორმას, მაგრამ 286^1 შინაარსი იძლევა იმის შესაძლებლობას, რომ იგი მივიჩნიოთ ზოგად ნორმად, რადგანაც ფინანსური სარგებლის მიღება, კომპიტერული მონაცემის ან სისტემის ხელყოფით, შესაძლებელია ქურდობის, გამოძალვის, თაღლითობის და სხვა მრავალი უმართლობის განხორციელებისას. ასეთ სიტუაციაში უნდა გაირკვეს კანონმდებლის

ნება იმასთან დაკავშირებით, უნდა დაკვალიფიცირდეს ასეთი ქმედება მხოლოდ სპეციალური ნორმის საფუძველზე, თუ ორივე ნორმის გამოყენებით, ანუ დანაშაულთა ერთობლიობით. სამართლებრივი კონსტრუქციის ანალიზი არ იძლევა იმის საშუალებას, რომ ქურდობა კომპიუტერული მონაცემის ან სისიტემის ხელყოფისას ან, თუნდაც, კომპიტერული მონაცემისა თუ სისტემის გამოყენებით, დაკვალიფიცირდეს სპეციალური მუხლით. ამდენად, შექმნილი სამართლებრივი კონსტრუქციების სტრუქტურული შინაარსი იძლევა მხოლოდ დანაშაულთა ერთობლიობით კვალიფიკაციის შესაძლებლობას.

როგორც აღვნიშნეთ, მოვლენათა ასეთი მდგომარეობა და კრიმინალიზაციის მსგავსი მიზანი, ფორმალურად ლეგიტიმურია, რადგანაც იგი დადგენილია საკანონმდებლო ხელისუფლების მიერ, მაგრამ პრობლემა იმაში მდგომარეობს, რომ ასეთი ტენდენცია აშკარად ხელყოფს სამართლიანობის პრინციპს. ასეთი კრიტერიუმებით, შესაძლებელი იქნებოდა ქურდობის, ძარცვის, თაღლითობისა თუ ნებისმიერი, სხვა, ტრადიციული შემადგენლობის განხორციელების ხერხისა და მეთოდების მეშვეობით, დამოუკიდებელ უმართლობათა კრიმინალიზება. მაგალითად:,, სხვისი მოძრავი ნივთის მართლსაწინააღმდეგო ხელყოფა, დაუფლება ან მისაკუთრება, ჩადენილი, სპეციალურად ამისთვის გაწრთვნილი ფრინველის ან ცხოველის მეშვეობით''. ამ შემთხვევაშიც, დანაშაულთა ერთობლიობით კვალიფიკაციას ალტერნატივა არ ექნებოდა.

ამით იმის თქმა გვინდა, რომ მართალია კანონმდებლის ექსკლუზიურ უფლებას განეკუთვნება კრიმინალიზაციის და, საერთოდ, კანონშემოქმედებითი საქმიანობის პროცესი, მაგრამ ეს უფლება არ არის აბსოლუტური და იზღუდება საყოველთაოდ აღიარებული სამართლებრივი პრინციპებითა და კრიტერიუმებით. კანონმდებელს შეუძლია მოახდინოს ცალკეულ უმართლობათა კრიმინალიზება ისევე, როგორც მაკვალიფიცირებელ გარემოებათა დადგენა, მაგრამ შეძლებისდაგვარად უნდა იქნას თავიდან აცილებული ისეთ შემადგენლობათა შექმნა და კრიმინალიზება, რომლებიც არ შეესაბამება განსაზღვრულობის სამართლებრივ პრინციპს. როგორც არ უნდა იყოს საქმის რეალური ვითარება, ნებისმიერი სახის, თუნდაც უმნიშვნელო ორაზროვნება, ქმნის ხელსაყრელ პირობებს მახინჯი სასამართლო პრაქტიკის დასამკვიდრებლად.

ამიტომ, განსახილველ საკითხთან დაკავშირებით, გაცილებით მიზანშეწონილი იქნებოდა ,,კიბერდანაშაულებრივ'' ქმედებათა კრიმინალიზება მომხდარიყო უკვე არსებულ, ტრადიციულ შემადგენლობათა ფარგლებში და არა ცალკეულ უმართლობათა ჩამოყალიბება-კონსტრუირებით. მსგავსი პროცესი საშუალებას მოგვცემდა თავიდან აგვეცილებინა დანაშაულთა ერთობლიობით კვალიფიკაციის ყოვლად გაუმართლებელი პრაქტიკა და, ამასთან, იგი საშუალებას მოგვცემდა მსგავსი კატეგორიის შემადგენლობათა სისტემურ-სამართლებრივ მოწესრიგებისთვის.

- თუ რეალობას თვალს გაუსწორებთ, უნდა ვაღიაროთ, რომ სისხლის

სამართლის იუსტიცია, ყველა ქვეყანაში და ნებისმიერ დროს, განსხვავებული დონით, მაგრამ მაინც ყოველთვის, მიმართული იყო სამართლის ნორმათა საკუთარი, ტენდენციური ინტერპრეტაციით, რაც აიხსნებოდა დამნაშავეობასთან ბრძოლის კეთილშობილური მიზნებით და, ზოგიერთ შემთხვევაში, კანონიდან ,,უმნიშვნელო'' გადახვევა, სწორედ ამ მოტივით აიხსნებოდა. ამიტომ, სისხლის სამართალში, სასიცოცხლოდ დიდი მნიშვნელობა აქვს როგორც განსაზღვრულობის, ისე სამართლიანობისა და სხვა საყოველთაოდ აღიარებული სამართლებრივი პრინციპების დაცვას. წინააღმდეგ შემთხვევაში, არასასურველ სასამართლო პრაქტიკას თავს ვერ დავაღწევთ.

თუ დაუბრუნდებით განსახილველ საკითხს, უნდა ითქვას, რომ სასამართლო პრაქტიკა, აღარაფერს ვამბობთ საგამოძიებო პრაქტიკაზე, არაერთგვაროვანი და ტენდენციურია, რაც იმაში გამოიხატება, რომ ადგილი აქვს დანაშაულთა ერთობლიობით კვალიფიკაციის განსხვავებულ მიდგომებს. სტატისტიკური მონაცემები ცხადყოფს, რომ საკუთრების წინააღმდეგ მიმართული დანაშაული, რომელიც ჩადენილია კომპიუტერული ტექნოლოგიების გამოყენებით, ყველა შემთხვევაში დანაშაულთა ერთობლიობით კვალიფიცირდება. ამ მდგომარეობის საილუსტრაციოდ ნიშანდობლივია ,,კიბერთაღლითობის''ტერმინის დამკვიდრება, რომელსაც მხოლოდ არსებული რეალობის მნიშვნელობა გააჩნია და არა სამართლებრივი ფუნქცია. ამიტომაა, რომ თაღლითობის შემადგენლობა, თუ მასში კომპიუტერული ელემენტიც არსებობს, კვალიფიცირდება საქართველოს სისხლის

სამართლის კოდექსის 180-ე მუხლითა და XXXV- თავის შესაბამისი მუხლით. განსხვავებული ვითარებაა ევროპისა და რიგი ქვეყნების სისხლისსამართლებრივ კანონმდებლობაში, სადაც ,,კიბერთაღლითობა'' კრიმინალიზებულია დამოუკიდებელ შემადგენლობად და გააჩნია სპეციალური ნორმის სტატუსი, რაც გამორიცხავს დანაშაულთა ერთობლიობით კვალიფიკაციას.

ამდენად, შეიძლება კიდევ ერთხელ ითქვას, რომ კიბერტექნოლოგიური ელემენტის გათვალისწინება, როგორც მაკვალიფიცირებელი ნიშნისა, სრულიად შესაძლებელია უკვე არსებულ, ტრადიციულ შემადგენლობათა ფარგლებში.

- ის გარემოება, რომ კიბერდანაშაულებრივი კატეგორიის შემადგენლობები

უსისტემოდაა განლაგებული სისხლის სამართლის კოდექსში, სრულიად ნათელია, მაგრამ რა არის ის ნიშანი, რომელიც განსაზღვრავს ამა თუ იმ ქმედების კუთვნილებას კიბერდანაშაულისადმი.

კრიმინალიზებულ და პოტენციურად მოსალოდნელ კიბერდანაშაულებრივ შემადგენლობათა შინაარსს განსაზღვრას დანაშაულის შემადგენლობის ობიექტური მხარის ელემენტები, რომელიც სხვა არაფერია თუ არა ე.წ. ფაკულტატური ელემენტები (დანაშაულის ჩადენის საშუალება, დანაშაულის საგანი). ერთ შემთხვევაში, კანონმდებელი მიზანშეწონილად მიიჩნევს გარკვეული ქმედების კრიმინალიზებას სისხლისსამართლებრივი დაცვის ობიექტის მიხედვით (საქ. სსკ-ის 284-ე, 285-ე, 286-ე მუხლები), რომელიც ზოგადად კომპიუტერისა და კომპიუტერული სისტემების უსაფრთხოებაა, ხოლო მეორე შემთხვევაში, ცალკეულ შემადგენლობათა კრიმინალიზებას განაპირობებს დანაშაულის შემადგენლობის ობიექტური მხრის ელემენტები (დანაშაულის ჩადენის საშუალება, საგანი, ხერხი).

რა თქმა უნდა, საკითხისადმი მსგავსი მიდგომა სრულად შეესაბამება კრიმინალიზაციის პრინციპებსა და კრიტერიუმებს. კანონმდებელი, კონკრეტულ შემთხვევაში, ითვალისწინებს ამა თუ იმ ქმედების სოციალურ საშიშროებას, რომელიც შეიძლება დანაშაულის შემადგენლობის ნებისმიერი ელემენტი იყოს. პრობლემა კი მდგომარეობს არა ამ პროცესში, არამედ მის სისტემურ-სტრუქტურულ მოწესრიგებაში

ისევე, როგორც შემადგელობის სტრუქტურულ ჩამოყალიბებაში.

აქაც, შეიძლება იგივე ითქვას. ამ ელემენტების გათვალისწინება, სრულიად მიზანშეწონილია მოაზრებულ იქნას ტრადიციულ შემადგენლობათა ფარგლებში და არავითარი საჭიროება არ არსებობს მისი დამოუკიდებელ შემადგენლობად კონსტრუირებისა.

- ,,კიბერდანაშაულის'' ცნების საკითხი აქტუალურია იმდენად, რამდენადაც

პრობლემატური. უპირველეს ყოვლისა, არ არსებობს ამ ცნების საკანონმდებლო განმარტება, ხოლო დოქტრინაში არსებული ერთმანეთისგან განსხვავებულია. ამის მიზეზი ისაა, რომ არ არსებობს კიბერსივრცის სრულყოფილი განმარტება და, აქედან გამომდინარე, შეუძლებელია კიბერდანაშაულის სრულყოფილი დეფინიციაც. ამიტომაა, რომ ევროპისა და ამერიკის შეერთებული შტატების სისხლისსამართლებრივი კანონმდებლობა იყენებს არა კიბერდანაშაულის, არამედ კომპიუტერული დანაშაულის ცნებას, ხოლო ტერმინი-,,კიბერდანაშაული,, ძირითადათ, გამოიყენება დოქტრინაში. ისიც უნდა ითქვას, რომ სამეცნიერო ლიტერატურაში განსხვავებული მოსაზრებაა იმასთან დაკავშირებით თუ რომელი ცნებაა უფრო ფართო მნიშვნელობის. ეროვნული სისხლის სამართლის კანონმდებლობა კიბერდანაშაულს ცნებას მიიჩნევს უფრო ფართოდ და ამიტომაა, რომ საქართველოს სისხლის სამართლის კოდექსის XXXV- ე თავი დასათაურებულია კიბერდანაშაულად, ხოლო ამ თავში შემავალი დანაშაულთა შემადგენლობები მოიხსენებიან, როგორც კომპიუტერული დანაშაულები.

ამ სფეროში მოღვაწე კომპეტენტური ექსპერტი, ალექსანდრე ღლონტი, მართებულად აღნიშნავს, რომ,, კიბერუსაფრთხოებას არ გააჩნია ერთიანი, ყველასათვის მისაღები დეფინიცია. იქიდან გამომდინარე, თუ ვის შეეკითხებით, თქვენ მოისმენთ განსხვავებულ პასუხებს. ეს სულაც არ ნიშნას, რომ რომელიმე სპეციალისტის პასუხი არ არის სწორი. ეს ნიშნავს მხოლოდ იმას, რომ აღნიშნული სფერო არის ძალიან ფართო.''

ასევე, საინტერესოა პროფესორ ტ. ტროპინინას მოსაზრება იმასთან დაკავშირებით,

რომ ,, კიბერდამნაშავეობა, თავისი არსით, გაცილებით უფრო ყოვლის მომცველია, ვიდრე კომპიუტერული დანაშაული და შეიცავს მართლსაწინააღმდეგო ქმედებათა ფართო სპექტრს. შესაბამისად, კიბერდანაშაული-არის ისეთი ბრალეული ქმედება, რომელიც მიმართულია კომპიუტერის, კომპიუტერული სისტემების, კომპიუტერული მონაცემების წინააღმდეგ; არასანქცირებული მოდიფიკაცია, ასევე, ნებისმიერი არამართლზომიერი ქმედება, რომლის ჩადენაც შესაძლებელია კომპიუტერის უშუალო გამოყენებით ან მისი დახმარებით, ან/და ისეთი მოწყობილობით, რომელიც ხელმისაწვდომს ხდის ინფორმაციულ სივრცეს.''

ვფიქრობთ, რომ აღნიშნული დებულება უფრო შესაბამისობაშია რეალობასთან, რადგანაც კიბერსივრცეში წარმოშობილი რაიმე სახის მოვლენის წარმოშობის წყარო შეიძლება იყოს ნებისმიერი ელექტრო-მოწყობილობაც, რომელიც არ არის კომპიუტერი.

კიბერდანაშაულის პრობლემატურობის შესახებ თავის აზრს გამოთქვამს კიოლნის უნივერსიტეტის პროფესორი მარტინ პაულ ვასმერი, რომელიც აღნიშნავს, რომ კიბერდანაშაულის დეფინიციის განსაზღვრა რთულია. ფართო გაგების მიხედვით, კიბერდანაშაულში მოიაზრება ყველა სისხლისსამართლებრივი დანაშაული, რომელიც ჩადენილია საინფორმაციო ან საკომუნიკაციო ტექნოლოგიების გამოყენებით ან მათ მიმართ. ერთმანეთისაგან განასხვავებენ დანაშაულებს, რომლებიც ინტერნეტის, მონაცემთა ბაზის, საინფორმაციო ტექნოლოგიური სისტემების ან მათი მონაცემების წინააღმდეგ არის მიმართული (კიბერდანაშაული ვიწრო გაგებით) და დანაშაულებს, რომლებიც ამ ტექნიკის გამოყენებით ხორციელდება (კიბერდანაშაული ფართო გაგებით).

როგორც ვხედავთ, ერთიანი, ჩამოყალიბებული მოსაზრება კიბერდანაშაულის ცნებასთან მიმართებაში არ არის მეცნიერთა შორისაც, რაც შესაბამისად აისახება კრიმინალიზაციის პროცესზეც.

აქედან გამომდინარე, შეიძლება ითქვას, რომ ცნების პრობლემატურობა ხდება ერთ-ერთი დამაბრკოლებელი მიზეზი, კიბერდანაშაულებრივ ქმედებათა სამართლებრივ-სისტემური მოწესრიგებისა. ეს გარემოება, თავის მხრივ, აძნელებს, როგორც ქმედების საკანონმდებლო, ისე სასამართლო კვალიფიკაციას.

- ის გარემოება, რომ საქართველოს სისხლის სამართლის კანონმდებლობა არ

ითვალისწინებს ,,კიბერდანაშაულებრივ'' ქმედებათა გაუფრთხილებლობით ჩადენის შესაძლებლობას, ბადებს ლეგიტიმურ კითხვებს და მიანიშნებს კანონმდებლობის ხარვეზზე, მაშინ როდესაც რიგი ქვეყნების მიერ იგი კრიმინალიზებულია.

პირველ რიგში, უნდა აღინიშნოს, რომ **,,კიბერდანაშაული','** თავისი ბუნებით, არ წარმოადგენს რომელიმე გეოგრაფიულ-ტერიტორიული ერთეულისთვის დამახასიათებელ მოვლენას, ან სოციალური ცხოვრების რომელიმე სფეროს მახასიათებელ დესტრუქციას. რა თქმა უნდა არა და ამის შესახებ, ჩვენ უკვე გვქონდა მსჯელობა. იგი უნივერსალური მოვლენაა და არსებობს ყველგან და ყველაფერში, არ იზღუდება დროითა და სივრცით და გააჩნია უსაზღვრო შესაძლებლობები.

სამეცნიერო ლიტერატურაში არსებული აზრთა თანხვედრა ,,კიბერდანაშაულის'' უნივესალობის შესახებ, დასტურდება სოციალური ცხოვრების სინამდვილითაც. ამიტომაა, რომ მრავალი ქვეყნის სისხლისსამართლებრივი კანონმდებლობა კიბერდანაშაულის მახასიათებელ ნიშნად გაუფრთხილებლობას ბუნებრივად მიიჩნევს (აშშ, გერმანია, საფრანგეთი, იტალია და სხვ). მაშინ, რატომაა, რომ საქართველოს სისხლის სამართლის კოდექსის XXXV-ე თავით გათვალისწინებული შემადგენლობები განეკუთვნებიან განზრახ კატეგორიებს, მაშინ როდესაც კიბერდანაშაულის ,,უნივერსალობის'' ლოგიკით, გაუფრთხილებლობის ფორმის უარყოფა ყოვლად გაუმართლებელია.

შესაძლებელია, კანონმდებელი ფრთხილად ეკიდება ამ კატეგორიის ქმედებათა კრიმინალიზაციას, გაუფრთხილებლობის ინსტიტუტის პრობლემატურობიდან გამომდინარე. შესაძლებელია, ეს გამოწვეული იყოს სასამართლო პრაქტიკის სიმწირით და საკითხი საჭიროებდეს დამატებით კვლევებს. სწორედ, გაუფრთხილებლობის შეზღუდვაზე საუბრობს პროფესორი მ. უგრეხელიძე, როდესაც აღნიშნავს, რომ ,, დასჯადი გაუფრთხილებლობის სფეროს მოცულობა არ უნდა იყოს დამოკიდებული კანონმდებლის შეუზღუდავ ნებასა და მიხედულებაზე, როგორც ამას პოზიტივისტური ყაიდის მეცნიერები არც თუ იშვიათად ირწმუნებიან

იურიდიულ ლიტერატურაში...აქედან ლოგიკური თანმიმდევრობით გამომდინარეობს, რომ მხედველობაში არ მიიღება ობიექტური და სუბიექტური, რომლებიც ამა თუ იმ ქმედების ერთგვარ ,,შიგთავსს'' წარმოადგენენ. არადა, სწორედ მათ შორის ხასიათი, ბუნება და სიმტკიცე წარმოადგენს გადამწყვეტ ფაქტორს და კრიტერიუმს, რომლის მიხედვითაც განისაზღვრება, მხოლოდ განზრახ ქმედებებს განეკუთვნება მოცემული შემთხვევა, თუ კანონში მისი შეტანა და გათვალისწინება გაუფრთხილებლობის სტატუსითაც შესაძლებელია.''

აღნიშნული სისხლისსამართლებრივი პრინციპი, რომლის ძირითადი დებულებები უკვე განვიხილეთ ზევით, საშუალებას გვაძლევს ,,კიბერდანაშაულებრივ''ქმედებათა მიმართ გამოვიყენოთ და მიუსადაგოთ მათ ცალკეული ელემენტები, რომელიც საშუალებას მოგვცემს დავადგინოთ ა) კიბერდანაშაულებრივ ქმედაბათა მიმართ ,, დახშულია'' (მ. უგრეხელიძე) თუ არა გაუფრთხილებლობა და ბ) შესაძლებელია თუ არა გაუფრთხილებლობის სტატუსის გავრცელება მსგავსი კატეგორიის ქმედებებზე.

მოცემულ საკითხთა შემდეგი კვლევის ვექტორი დამოკიდებულია ერთ მნიშვნელოვან გარემოებაზე; კერძოდ: თუ ჩვენ ვიზიარებთ კიბერდანაშაულებრივ (კომპიუტერულ) ქმედებათა უნივერსალობას, რომელიც აუცილებლად ან პოტენციურად ახლავს თან, ფაქტობრივად, ყველა ტრადიციულ შემადგენლობას, მიუხედავად მათი შინაარსისა, მაშინ გამოდის, რომ ჩვენ უნდა მივდიოთ და ვიხელმძღვანელოთ უკვე არსებული, მეცნიერულად დადასტურებული შეხედულებებით დანაშაულთა ჩადენის ფორმების თაობაზე და საჭიროებას არ წარმოადგენს ცალკეულ შემადგენლობათა ანალიზი.

სავარაუდოთ, ეჭვს არ უნდა იწვევდეს კიბერტექნოლოგიების მონაწილეობით გაუფრთხილებლობით მკვლელობის ჩადენა, რადგანაც თანამედროვე ტრანსპორტის, საავიაციო თუ ენერგეტიკის სისტემური არქიტექტურა უმეტესწილად ეყრდნობა კიბერტექნოლოგიებს. შორს რომ არ წავიდეთ, ჩერნობილის ატომურ სადგურზე მომხდარი მსოფლიო მასშტაბის ტრაგედია ან, თუნდაც, კრუიზული გემის - კონკორდიას ჩაძირვა, სხვა არაფერია თუ არა გაუფრთხილებელი დანაშაული.

საინტერესოა ეროვნული სისხლისსამართლებრივი კანონმდებლობით გათვალისწინებული შემადგენლობა, რომელიც კულტურული და ბუნებრივი ობიექტების გაუფრთხილებლობით განადგურება-დაზიანებას ითვალისწინებს. (მუხლი 257. შემადგენლობის სამართლებრივი საჭიროება მეცნიერულად იქნა დასაბუთებული პროფესორ მ. უგრეხელიძის მიერ).

თუ იმას მივიღებთ მხედველობაში, რომ თანამედროვე რეალობაში, კულტურულ და ბუნების ობიექტთა დაცვა-შენახვის ტექნიკურ მექანიზმთა უმეტესი ნაწილი შედგება კომპიუტერული შემადგენლისგან, მაშინ ბუნებრივია ისიც, რომ ბუნების ძეგლის დაზიანება ან განადგურების დანაშაულებრივ გაუფრთხილებლობაში კიბერტექნოლოგიების როლი სულ უფრო მზარდი იქნება. რაც შეეხება, ამ სფეროში გაუფრთხილებლობის კრიმინალიზების მიზანშეწონილობას, მისი მეცნიერულად დასაბუთებული არგუმენტები მთლიანად გაზიარებულია კანონმდებლის მიერ და ადეკვატურია სოციალური მოთხოვნებისადმი.

ანალოგიურადაა შესაძლებელი მსგავსი თვალსაზრისის გავრცელება ტრადიციულ შემადგენლობათა ისეთი კატეგორიების მიმართ, სადაც გაუფრთხილებლობა ფიგურირებს. ამიტომ, ჩვენს მიერ განვითარებული მოსაზრების დასაბუთებისას, რაიმე სახის ძალისხმევა საჭირო არაა და არც სტატისტიკურ მონაცემთა ანალიზს მოითხოვს, რომელიც ისედაც არ არსებობს, იმ მარტივი მიზეზის გამო, რომ კიბერდანაშაულებრივ ქმედებათა გაუფრთხილებლობა არ არის კრიმინალიზებული.

ჩვენს მიერ ზევით განვითარებული მსჯელობა, რომელიც ,,კიბერდანაშაულის'' საკანონმდებლო დეფინიციის არარსებობის გამო წარმოშობილ სამართლებრივ წინააღმდეგობებს შეეხებოდა, კვლავ გვახსენებს თავს. ამჟამად, ცნების საჭიროება ვლინდება იმის დადგენაში, თუ რა მოიაზრება კიბერდანაშაულში; ეს კი, თავის მხრივ, დაგვეხმარება გავარკვიოთ, რეალურად და არა ფორმალურად, ,,კარხსნილია'' თუ არა გაუფრთხილებლობა კიბერდანაშაულისთვის.

მაშასადამე, თუ ჩვენ კიბერდანაშაულს მივაკუთვნებთ მხოლოდ XXXV-ე თავით გათვალისწინებულ შემადგენლობებს, მაშინ ისიც უნდა ვაღიაროთ, რომ საქმე გვაქვს განზრახი კატეგორიის დანაშაულთან, მაგრამ თუ კიბერდანაშაული შეიძლება განხილულ იქნას ამ თავის იქით არსებულ შემადგენლობებზეც, მაშინ, რეალურად, გაუფრთხილებლობა ისეთივე შესალო ფორმაა კიბერდანაშაულისთვის, როგორც ნებისმიერი შემადგენლობისთვის.

ასეთ შემადგენლობათა რიცხვს მიეკუთვნება საქ. სსკ 157-159 მუხლები, რომლებიც კოდესის XXIII-ე თავშია ასახული (ადამიანის უფლებებისა და თავისუფლებების წინააღმდეგ მიმართული დანაშაული).

საქ. სსკ 401-ე მუხლით გათვალისწინებულია საფრენი აპარატის ან ექსპლუატაციის წესების დარღვევა; ხოლო 402-ე მუხლი ივალისწინებს ხომალდის მართვის ან ექსპლუატაციის წესების დარღვევას; ისევე, როგორც 403-ე მუხლი: გარშემომყოფისათვის მომეტებული საშიშროების შემცველ იარაღთან მოპყრობის წესის დარღვევა.

თუ მხედველობაში მივიღებთ, რომ დღეს არსებული სამხედრო ტექნიკის სისტემური სტრუქტურა მთლიანად კომპიუტერიზებულია, მაშინ წესების დარღვევა სხვა არაფერია თუ არა კომპიუტერულ ტექნოლოგიათა არასწორი ექსპლუატაცია, ისევე, როგორც სატრანსპორტო დანაშაულთა ის შემადგენლობები, რომლებიც გაუფრთხილებლობას გულისხმობს.

გამოდის რომ ,ფაქტობრივად, ,,კიბერდანაშაულისთვის'' გაუფრთხილებლობა ,,კარხსნილია'' და არა ,,დახშული.''

როდესაც საუბარია კიბერდანაშაულის (კომპიუტერული) გაუფრთხილებლობით ჩადენის პრობლემატიკაზე, თავს იჩენს მისი, როგორც სოციალური საშიშროების, ისე ,,ტიპობრივი ვალენტობის პრინციპთან'' შესაბამისობის საკითხი. ამ მოცემულობაში, გაცილებით აქტუალურია სპეციალური სუბიექტის როლი. თუ სისხლის სამართლის სუბიექტის მიმართ შესაძლოა დავას იწვევდეს კრიმინალიზაციის პროცესთან დაკავშირებული მრავალი ნიუანსი, ამას ვერ ვიტყვით სპეციალური სუბიექტის მიმართ. მარტივად, ამ საკითხის ფორმულირება

შემდეგნაირად შეიძლება: ის რაც მისატევებელია რიგითი ადამიანისთვის, იგივეს ვერ ვიტყვით პასუხისმგებელ პირზე. ამ შემთხვევაში, ადგილი აქვს ამა თუ იმ პირის სამსახურებრივ ვალდებულებას, ჯეროვნად და სათანადოდ შეასრულოს მასზე დაკისრებული მოვალეობები. მაშინ, როდესაც გემის კაპიტანი ვალდებულია სრულყოფილად ფლობდეს სანავიგაციო და სხვა ტექნოლოგიურ კომპონენტებს, იგივეს ვერ ვიტყვით რიგით თანამშრომელზე და ა. შ. ამის დასტურია ,,საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ,'' სადაც დეტალურადაა განმარტებული კრიტიკული ინფორმაციის შენახვასა და კომპიუტერულ ინციდენტებზე რეაგირების შესაბამისი სუბიექტები.

ამიტომ, შეცდომა, რომელიც ადამიანის თანმდევი თვისებაა, ამ და მსგავს სფეროებში გარდაუვალი მოცემულობაა. ხოლო ის გარემოება, რომ მსგავსი ურთიერთობები რეგულირდება ადმინისტრაციული სამართლის ნორმებით, უკვე მიუთითებს მის სისხლისსამართლებრივი რეგულირების აუცილებლობაზეც. ფაქტობრივად, სისხლის სამართლის კოდექსი, მართლაც, ითვალისწინებს სპეციალურ შემადგენლობებს, რომლის მიხედვითაც დადგება სისხლისსამართლებრივი პასუხისმგებლობა, მაგრამ ეს სპეციალური მუხლებია (მაგალითად: საქ. სსკ 241. ატომური ენერგეტიკის ობიექტზე უსაფრთხოების წესების დარღვევა) და მისი ანალოგიით გამოყენება აკრძალულია, ამიტომ მსგავსი ხასიათის ქმედებათა არსებობისას კვალიფიკაცია შესაძლოა განისაზღვროს 342-ე მუხლით, თუნდაც, ადგილი ქონდეს გლობალურ ტრაგედიას (სამსახურებრივი გულგრილობა), თუ არ არსებობს შესაბამისი სპეციალური შემადგენლობა.

მხედველობაშია მისაღები ის გარემოებაც, რომ ,,კიბერდანაშაულებრივ'' შემადგენლობათა ისეთი კატეგორიის კრიმინალიზაცია, რომელიც შესაძლოა ჩადენილ იქნას გაუფრთხილებლობით, სამომავლო პერსპექტივაში გამოიწვევს შემადგენლობათა ისეთი რაოდენობის აკუმულირებას, რომელსაც სისხლის სამართლის კოდექსი ვერ დაიტევს. ამიტომ, ამ შემთხვევაშიც, მიზანშეწონილი იქნებოდა კიბერტექნოლოგიების, როგორც შემადგენლობის ობიექტური მხარის

ელემენტის გათავალისწინება უკვე არსებულ შემადგენლობათა ფარგლებში, როგორც მაკვალიფიცირებელი გარემოებისა. გამონაკლის შემთხვევებში, სოციალური საშიშროებისა და სხვა მახასიათებელი ნიშნების გათვალისწინებით, შესაძლებელია სპეციალური შემადგენლობების შექმნაც. ჩვენი აზრით, კრიმინალიზაციის პროცესისადმი მსგავსი მიდგომა თავიდან აგვაცილებდა მრავალ სამართლებრივ და საკანონმდებლო საქმიანობის ტექნიკურ საკითხებთან დაკავშირებულ სირთულეებს.

შესაბამისად, კვლევის მიზანს წარმოადგენს ,,კიბერდანაშაულებრივ'' (კომპიუტერული დანაშაულის) ქმედებათა კრიმინალიზაციის პროცესში, ისეთ სამართლებრივ და საკანონმდებლო საქმიანობის ტექნიკურ საკითხთა გადაწყვეტა, რომელიც ხელს შეუწყობს ამ კატეგორიის უმართლობათა სამართლებრივ - სისტემურ მოწესრიგებას, რომელსაც მოკლებულია ეროვნული და, არა მარტო ეროვნული, სისხლისსამართლებრივი კანონმდებლობა. ამასთან, განისაზღვრება იმ სპეციფიკურ ნიშან-თვისებათა ერთობლიობა, რომლის მიხედვითაც შესაძლებელი იქნება მსგავსი კატეგორიის ქმედებათა კლასიფიკაცია, ისევე, როგორც დადგენა იმისა, თუ უმართლობის რა სახესთან გვაქვს საქმე. პარალელურად, შესაბამის სამართლებრივ პრინციპებსა და კრიტერიუმებზე დაყრდნობით უნდა გაირკვეს ამ ქმედებათა შემადგენლობის ცალკეულ ელემენტთა თავსებადობის საკითხი, ისევე როგორც მისი გავრცელების ინტენსივობა. მეცნიერულ დასაბუთებას დაექვემდებარება გაუფრთხილებლობის ინსტიტუტის გავრცელების შესაძლებლობა ისეთ ქმედებათა მიმართ, რომელსაც კიბერდანაშაულად მოვიხსენიებთ. პასუხი გაეცემა კითხვას, თუ რატომ არ უშვებს ეროვნული სისხლისსამართლებრივი კანონმდებლობა მსგავს ქმედებათა გაუფრთხილებლობით ჩადენის შესაძლებლობას.

მეცნიერული სიახლე და თეორიულ-პრაქტიკული მნიშვნელობა - მეცნიერული კვლევის სიახლეს წარმოადგენს ,,კიბერდანაშაულებრივ'' ქმედებათა კრიმინალიზაციის პროცესის სრულყოფა, რომელიც მოაწესრიგებს ამ კატეგორიის დანაშაულის შემადგენლობათა სისტემურ-სამართლებრივ მოწესრიგებას. კერძოდ, სამართლებრივი კონსტრუქციები უსისტემოდაა გაბნეული სისხლის სამართლის კოდექსში და ქმნის ნორმათა ისეთ კონკურენციას, რომელიც ართულებს კანონის ინტერპრეტაციას. ამიტომ, მიზანშეწონილია, ტრადიციულ დანაშაულებრივ

შემადგენლობათა ფარგლებში, კიბერტექნოლოგიების ელემენტები მიჩნეულ იქნეს, როგორც მაკვალიფიცირებელი გარემოება. შესაძლებელია, ეს ელემენტი, როგორც დამამძიმებელი გარემოება, გათვალისწინებულ იქნას ამა თუ იმ თავის ან კარის ნაწილში ან/და სისხლის სამართლის კოდექსის ზოგად ნაწილში.

კრიმინალიზაციის ასეთი მიმართულებით წარმართვა თავიდან აგვაცილებს ქმედებათა, როგორც საკანონმდებლო, ისე სასამართლო კვალიფიკაციის პრობლემებს. მართლაც, კიბერტექნოლოგიებს, დანაშაულის შემადგენლობაში იმაზე მეტი ფუნქცია არ აკისრია, ვიდრე შემადგენლობის ობიექტური მხარის ელემენტების. ეს ელემენტები, მიუხედავად უმართლობათა სახესხვაობისა, პოტენციურად ახლავს თან ნებისმიერ დანაშაულს. კიბერსივრცე, რომელიც უკვე გვთავაზობს სოციალურად საშიშ ქმედებათა უამრავ ვარიანტს, მათი ყოველ ჯერზე კრიმინალიზება ფიზიკურად შეუძლებელი იქნება. ამიტომ, კვლევაში შემოთავაზებული ხედვა, ამ კუთხითაც სიახლეა და გააჩნია, როგორც თეორიული, ისე პრაქტიკული მნიშვნელობა.

ლიტერატურის მიმოხილვისას შევნიშნავთ, რომ კიბერდანაშაულს, როგორც ადამიანთა დესტრუქციული საქმიანობის მეტად სპეციფიკურ სახეს, განსაკუთრებული ყურადღება მიექცა XX-ე საუკუნის მიწურულსა და XXI-ე საუკუნის დასაწყისში, როდესაც აშკარად გამოიკვეთა ამ მოვლენის მაღალი სოციალური საშიშროების დონე და როდესაც ინტენსიურად იწყება ასეთი კატეგორიის ქმედებათა კრიმინალიზაციის პროცესი.

ამ კუთხით მნიშვნელოვანია პროფესორ მინდია უგრეხელიძის მიერ დაფუძნებული და განვითარებული ,, ტიპობრივი ვალენტობის პრინციპი სისხლის სამართალში''. აღნიშნული პრინციპი, კვლევის ფარგლებში, ისევე როგორც, საერთოდ, კრიმინალიზაციის პროცესში, წარმოადგენს ერთგვარ სამართლებრივ ორიენტირს, რომელიც ბოლომდე გასდევს სადისერტაციო ნაშრომს და ასრულებს გზამკვლევის ფუნქციას.

უმნიშვნელოვანესია დებულება იმის შესახებ, რომ დანაშაულის შემადგენლობის კონსტრუირებისას, არა მარტო შემადგენლობის ობიექტური მხარის ელემენტთა თავსებადობის საკითხი კი არ მიიღება მხედველობაში, არამედ ისიც თუ რამდენად

ტიპურია, დამახასიათებელია იგი საზოგადოებისთვის. თუ ამ დებულებას მიუსადაგებთ კრიმინალიზაციის პროცესში მოპოვებულ მონაცემებს, აღმოჩნდება, რომ კიბერტექნოლოგიების ჩართულობით განხორციელებულ, სოციალურად საშიშ ქმედებათა ინტენსივობა და სიხშირე, უკიდურესად დიდია, არა მარტო ქვეყნის, არამედ მსოფლოს მასშტაბით. ამდენად, კიბერდანაშაულებრივ ქმედებათა კრიმინალიზაციის პროცესი, შეიძლება ითქვას, რომ სრულად აკმაყოფილებს ,,ტიპობრივი ვალენტობის პრინციპს.''

დისერტაციის კვლევის პროცესში გამოყენებულია პროფესორ გურამ ნაჭყებიას მეცნიერული შრომები:,,სისხლის სამართლის მეცნიერების საგანი,'' ,,სისხლისსამართლებრივი ურთიერთობა და დანაშაულის ცნება,'' და ,,სისხლის სამართლის მეცნიერების მეთოდოლოგიური ანბანი.'' აღნიშნულ მონოგრაფიებში განვითარებული მსჯელობა და მეცნიერულად დასაბუთებული დებულებები, ფასდაუდებელ დახმარებას გვიწევს კრიმინალიზაციის პროცესთან დაკავშირებული საკითხების გადაწყვეტაში.

საყოველთაოდ აღიარებული თვალსაზრისი, რომელიც კიბერსივრცის უნივერსალობას ეხება, კარგადაა ნაჩვენები პროფესორ ზვიად გაბისონიას უახლეს სახელმძღვანელოში:,, ინტერნეტ სამართალი და ხელოვნური ინტელექტი.'' სწორედ, ეს ნაშრომი წარმოაჩენს კიბერსივრცეში მიმდინარე პროცესების, როგორც დადებით მხარეებს, ისე უკვე არსებულ და პოტენციურად საშიშ ქმედებათა წარმოშობის ნეგატიურ პერსპექტივას. ამიტომ, ჩვენს მიერ განვითარებული მსჯელობა, რომელიც საინფორმაციო სივრცეში ადამიანის დესტრუქციულ საქმიანობას ეხება, სრულ შესაბამისობაშია სახელმძღვანელოში არსებულ ნააზრევთან.

გამოჩენილი სოციოლოგების: ე. ფრომის, მასუდას, ბელის, ფრიმენის და სხვათა ფუნდამენტური ნაშრომები და მათში განვითარებული მოსაზრებები ადამიანის დესტრუქციული საქმიანობის შესახებ საინფორმაციო საზოგადოებაში, სრულად ემთხვევა კვლევის პროცესში გამოთქმულ მოსაზრებას, კიბერდანაშაულის, როგორც დესტრუქციული საქმიანობის სპეციპიკურ სახეზე.

მნიშვნელოვანია ქართველ ექსპერტთა: ა. ღლონტის, უ. ზაქაშვილის, ლ. ბოძაშვილისა და ნ. კოხრეიძის სამეცნიერო ნაშრომები კიბერუსაფრთხოებისა და კიბერდანაშაულის პრობლემატიკაზე, ისევე როგორც უცხოელ მეცნიერთა ნაშრომები.

კვლევის თეორიული საფუძვლები - კიბერსივრცესთან დაკავშირებული საკითხები და მისი სამართლებრივი რეგულირების სპეციფიკა, განსაკუთრებით, ახალი სისხლისსამართლებრივი კონსტრუქციების შექმნა, ანუ კრიმინალზაცია, რომელიც რთული და კომპლექსური ხასიათის სამართალშემოქმედებითი პროცესია, მოითხოვს არა მარტო სამართლებრივი, არამედ მომიჯნავე და სხვა, ტექნიკურ და ჰუმანიტარულ მეცნიერებათა, როგორც მეთოდების, ისე მონაცემთა გათვალისწინებას. ეს, სწორად ისეთი სფეროა, სადაც ყველაზე აშკარად იკვეთება ტექნიკურ და ჰუმანიტარულ მეცნიერებათა დაახლოვებისა და შერწყმის კონტურები, რომელიც დიმენსიოლოგიის სფეროა. რა თქმა უნდა, საკითხის კვლევისას გამოყენებულია ტრადიციული სამართლებრივი მეთოდები: სამართალმზომელობის ანუ ლეგიმეტრიის, შედარებით-სამართლებრივი, ლოგიკური, ისტორიული, დედუქციური, ინდუქციური, ფიქციის და მრავალი სხვა, რადგანაც კვლევის სპეციფიკიდან გამომდინარე, სახეზეა სამართლებრივი კვლევის მეთოდთა საჭიროების მრავალფეროვნება.

განსაკუთრებული აღნიშვნის ღირსია პროფესორ მ.უგრეხელიძის მიერ დაფუძნებული და განვითარებული ,,ტიპობრივი ვალენტობის პრინციპი სისხლის სამართალში,'' რომელიც ერთგვარი ორიენტირის ფუნქციას ასრულებს კვლევისას და ქმნის მყარ სამართლებრივ კარკასს. ამასთან, სტატისტიკურ მეთოდთან ერთად, ხდება ამ პრინციპის რეალიზაცია და ხორცშესხმა, ცალკეულ სისხლისსამართლებრივ კონსტრუქციათა ჩამოყალიბებისას. ამიტომ, დანაშაულის შემადგენლობათა ელემენტების ანალიზისას, მათ შორის არა მარტო თავსებადობის საკითხს მიექცევა ყურადღება, არამედ იმასაც, თუ რამდენად დამახასიათებელი და ტიპურია იგი სოციალური ურთიერობებისთვის.

კვლევის სპეციფიკიდან გამომდინარე, სტატისტიკურ მონაცემთა შეგროვება-ანალიზისას, ოფიციალურ სტატისტიკურ მონაცემებზე დაყრდნობა ერთობ

არაეფექტიანია და რეალურად ვერ ასახავს ფაქტობრივ მდგომარეობას, ამიტომ კვლევის პროცესში გამოყენებულ იქნა ანონიმური ინტერვიუს მეთოდი.

ნაშრომის მოცულობა და სტრუქტურა - სადისერტაციო ნაშრომი შედგება შესავლის, 3 თავის, 5 ქვეთავის, დასკვნის, ბიბლიოგრაფიისა და სოციოლოგიური კვლევის შედეგებისგან. (სულ 163 ერთეული).

პირველი თავი ეძღვნება კიბერდანაშაულის გენეზისს, რომელიც ტექნოლოგიური რევოლუციის შედეგია და სწორედ მის წიაღში წარმოიშვა. განხილულია კომპიუტერის, კომპიუტერული სისტემებისა და სოციუმის ინტერნეტიზაციის განვითარების ეტაპები.

მეორე თავი დათმობილი აქვს კიბერსივრცეში წარმოშობილ ქმედებათა კრიმინალიზაციის თეორიულ საფუძვლებს, განხილულია საინფორმაციო საზოგადოებაში ადამიანის დესტრუქციული საქმიანობის სამართლებრივ-კრიმინოლოგიური ასპექტები და ნაჩვენებია კრიმინალიზაციის უკიდურესი აუცილებლობა.

მესამე თავი მოიცავს კიბერდანაშაულის სამართლებრივი რეგულირების პრობლემებს; ეროვნული და საერთაშორისო სისხლისსამართლებრივი კანონმდებლობის შედარებითი ანალიზის საფუძველზე განხილულია კიბერდანაშაულის, როგორც დანაშაულებრივი გამოვლინების უნივერსალური ფორმის თავისებურებანი და გამოთქმულია მოსაზრება, ეროვნულ სისხლისსამართლებრივ კანონმდებლობაში, კიბერდანაშაულებრივ ქმედებათა მიმართ გაუფრთხილებლობის გავრცელების თაობაზე.

ნაშრომის ძირითადი შინაარსი

თავი 1. . კიბერდანაშაულის გენეზისი.

დისერტაციის აღნიშნულ თავში განხილულია ტექნოლოგიური პროგრესისა და მის წიაღში სოციალურად საშიშ ქმედებათა მთელი წყების წარმოშობა.

სწორედ, საინფორმაციო საშუალებების განვითარებასა და გლობალიზაციას უკავშირდება სოციალურად საშიშ ქმედებათა მრავალფეროვნების წარმოშობა, რომლის მასშტაბების არა თუ ზუსტი, არამედ მიახლოვებით დადგენაც შეუძლებელი აღმოჩნდა. საქმე იმაში გახლავთ, რომ ტექნოლოგიურმა რევოლუციამ არსებითად შეცვალა დანაშაულის შესახებ მანამდე არსებული ტრადიციული წარმოდგენები და გადაიყვანა იგი ისეთ განზომილებაში, სადაც რაიმე საიმედო პროგნოზირებაზე საუბარი რთულია.

განსაკუთრებული ზემოქმედება იქონია კიბერტექნოლოგიების განვითარების ტენდენციებმა მსოფლიო უსაფრთხოების მდგომარეობაზე. მართლაც, ცივი ომიდან მოყოლებული, დღევანდელ დრომდე, თუ მსოფლიო უსაფრთხოების ბალანსს უზრუნველყოფდა სახელმწიფოთა გამგებლობაში არსებული ბირთვული შეიარაღების იმ არსენალის არსებობა, რომელიც იმთავითვე ქმნიდა ურთიერთგანადგურების უპირობო გარანტიას და ამით სახეზე იყო შემაკავებელი მექანიზმების ერთგვარი ფსიქოლოგიური განცდა, ამას ვერ ვიტყვით უკვე არსებულ რეალობაზე. კიბერტექნოლოგიები მოგვევლინა იმ კატეგორიად, რომლის განუსაზღვრელი შესაძლებლობების კონტროლი და, მით უმეტეს, სრულყოფილი მართვა შეუძლებელი აღმოჩნდა. თუ იმასაც მივიღებთ მხედველობაში, რომ სამხედრო შეიარაღების სრული კომპლექტაციის ფუნქციონირებას კიბერტექნოლოგიები განსაზღვრავენ, მაშინ ძნელი მისახვედრი არ უნდა იყოს კაცობრიობის მოსალოდნელი, არაპროგნოზირებადი მომავალი. ამასთან, თუ ტრადიციული სამხედრო-სამრეწველო კომპლექსი მოითხოვდა ასტრონომიულ ფინანსებს, ადამიანურ და მატერიალურ რესურსებს და, ყველაფერთან ერთად, იგი მკაცრად სახელმწიფოს ექსკლუზიურ უფლებას წარმოადგენდა, კიბერსივრცის სოციალიზაციამ ისეთი გარემო შექმნა, როდესაც არა თუ სახელმწიფოებს, არამედ

ცალკეულ ჯგუფებსა და ფიზიკურ პირებსაც ხელეწიფებათ ნებისმიერი კანონით დაცული სიკეთის დანაშაულებრივი ხელყოფა.

რეიტინგული ,, Wall Street Journal''- ის მიერ ჩატარებული გამოკვლევებით, ჯერ კიდევ 2015 წლისთვის, 60 ქვეყანა უკვე ინტენსიურად ატარებდა ფუნდამენტურ სამეცნიერო კვლევებს კომპიუტერული სადაზვერვო პროგრამების შექმნის მიზნით. 29 ქვეყანას გააჩნია სპეციალური სახელმწიფო უსაფრთხოების სისტემაში შემავალი დანაყოფები, რომელთა უშუალო მიზანია კიბერშეტევათა სისტემების უზრუნველყოფა და განვითარება.

ამდენად, კიბერსივრცე იქცა ერთგვარ ბრძოლის ველად, რომლის შემადგენელ ნაწილებს წარმოადგენენ კომპიუტერული სისტემები და ინტერნეტი. ინტერნეტი წარმოადგენს არა უბრალოდ ინტერნეტს, არამედ იგი გვევლინება ქსელების ქსელად, რომლის მასშტაბების დადგენა ფაქტობრივად შეუძლებელია. კიბერსივრცის კომპონენტს უნდა მივაკუთვნოთ ტრანსნაციონალური, კერძო ტიპის ქსელები, რომლებიც ამუშავებენ, ინახავენ და გადასცემენ ფულადი თანხების მოძრაობას მსოფლიო მასშტაბით; ასევე, ვაჭრობისა და საფონდო ბირჟების ფინანსურ მონაცემებს. გარდა ამისა, არსებობს კონტროლის ისეთი სისტემები, რომლებიც ადამიანთა უშუალო მონაწილეობის გარეშე უზრუნველყოფენ სხვადასხვა ობიექტების ერთმანეთთან კომუნიკაციას, ინფორმაციის გაცვლა-გამოცვლას და მის პროგრამულ დამუშავებას. ასეთ მოცემულობაში, კიბერდამნაშავეებს ხელეწიფებათ უნებართვოდ შეაღწიონ დაცულ სისტემაში და დაეუფლონ კონფიდენციალურ ინფორმაციას ან ჩანერგონ ისეთი ხასიათის პროგრამა, რომელიც უზრუნველყოფს ფულადი თანხების არამართლზომიერ გადინებას. უფრო მეტიც, მსგავსი პროგრამული უზრუნველყოფის მეშვეობით შესაძლებელია არა მარტო სოციალურ სფეროში ნებისმიერი თვითნებობის განხორციელება, არამედ თავდაცვითი სისტემების მანიპულირებაც. ერთი სიტყვით, კიბერსივრცეში შესაძლო, სოციალურად საშიშ ქმედებათა განხორციელების პოტენციალი იმდენად უსაზღვროა, რამდენადაც უსაზღვროა თავად კიბერსივრცე. ეს თვისება გვევლინება უნივერსალურად და ქსელების ბუნებრივი მახასიათებელია: ურთიერთკავშირი, მასშტაბები, სისწრაფე, ლატენტობა და პროცესების სირთულე. ესაა კიბერდანაშაულის სპეციფიკა, რომელიც უდავოდ ზრდის მსგავს ქმედებათა

სოციალურ საშიშროებას. მართლაც, ინტერნეტის უნივერსალურმა ხასიათმა განაპირობა კიბერშეტევის ისეთი სისწრაფით განხორციელება, რომლის არა თუ აღკვეთა, არამედ ინფორმაციის მიღებაც დროში გაჭიანურებული პროცესია. ამიტომ, როგორც რეალობა გვიჩვენებს, კიბერშეტევის ანონიმურად განხორციელება სულ უფრო მარტივდება, ხოლო მისი პრევენცია კი რთულდება. ასეთი სახის ასიმეტრიულობა კი თვისებრივად ცვლის სიტუაციას, რომლის დროსაც თანამედროვე ქურდს, კიბერტექნოლოგიების გამოყენებით შეუძლია მოიპაროს გაცილებით დიდი თანხა, მისთვის გაცილებით უფრო ნაკლები რისკის გაწევით, ვიდრე ცეცხლსასროლი იარაღის გამოყენებით. ისევე, როგორც ტერორისტს, კომპიუტერის გამოყენებით შეუძლია ისეთი ტრაგედიის დატრიალება, რომელსაც ვერ მოახერხებს ბომბის აფეთქებით.

ამდენად, კიბერდანაშაული დღეის მდგომარეობით გვევლინება, როგორც ციფრული ეპიდემია, რომელიც კაცობრიობას აიძულებს იმოქმედონ სინქრონულად და კომპლექსურად. წინააღმდეგ შემთხვევაში, რაიმე სახის პოზიტიურ ცვლილებაზე საუბარიც კი ზედმეტია.

არსებული მძიმე მდგომარეობის ნათელი მაგალითია სიხშირეთა დიაპაზონის გაზრდა და ავტომატური სისტემების სრულყოფა, რაც საშუალებას იძლევა მილიონობით სპამის გასაგზავნად მსოფლიოს ნებისმიერ გეოგრაფიულ რეგიონში. ჰაკერული შეტევების ავტომატურ რეჟიმში განხორციელება შესძლებელს ხდის ზიანის არეალის უთანაზომოდ გაზრდას, რა დროსაც, ყოველდღიურად ადგილი აქვს ათეულობით მილიონი კიბერშეტევის განხორციელებას პროგრამული მექანიზმების განხორციელებით. ასეთი პროგრამა იქნა აღმოჩენილი ახლახან, რომელიც აკონტროლებდა თხუთმეტ მილიონ კომპიუტერს, რომელთაგან უმეტესი ნაწილი ეკუთვნოდა მსხვილ კერძო კომპანიებს.

ზემოაღნიშნულიდან გამომდინარე, შეიძლება ითქვას, რომ კრიმინალიზაციის პროცესს, მოცემულ შემთხვევაში ალტერნატივა არ აქვს. რა თქმა უნდა, მხედველობაში გვაქვს კრიმინალიზაციის ისეთი პროცესი, რომელიც სრულად შეესაბამება საყოველთაოდ აღიარებულ სამართლებრივ პრინციპებსა და კრიტერიუმებს.

თავი 2. კიბერსივრცეში წარმოშობილ ქმედებათა კრიმინალიზაციის თეორიული საფუძვლები. (ქვეთავები:2.1. კიბერსივრცეში ადამიანის დესტრუქციული საქმიანობი ზოგად-სოციოლოგიური ანალიზი, 2.2 კიბერდაშაულებრივ ქმედებათა კრიმინალიზაციის თავისებურებანი).

ნაშრომის მოცემულ თავში განხილულია, ზოგადად, კრიმინალიზაციის და კიბერსივრცეში წარმოშობილ ქმედებათა კრიმინალიზაციის თავისებურებანი. ანალიზსა და სამართლებრივ შეფასებას დაექვემდებარება ის სამართლებრივი მეთოდები, პრინციპები და კრიტერიუმები, რომლებიც გამოიყენება კრიმინალიზაციის პროცესში. ამასთან ნაჩვენებია ადამიანის დესტრუქციული საქმიანობის მასშტაბები საინფორმაციო სფეროში.

შეუძლებლად მიგვაჩნია დესტრუქციის, როგორც ადამიანური საქმიანობის ანალიზის გარეშე ჩვენს მიერ დასახული კვლევის მიზნის მიღწევა. სწორედ კიბერსივრცეა ის განზომილება, რომელშიც ყველაზე მკაფიოდ, აგრესიულად და დამანგრეველი შედეგებით ვლინდება ეს ფენომენი. ამიტომ, თუ არ მოხდა ამ ფენომენის სათანადოდ წარმოჩენა, ჩვენი კვლევის პროცესი ჩაიკარგება ცალკეულ დანაშაულებრივ შემადგენლობათა კონსტრუქციების ჩამოყალიბება - დასაბუთების უსასრულო კაზუისტიკაში და სრულყოფილი პასუხი ვერ გაეცემა მთავარ კითხვებს: რას წარმოადგენს კიბერდანაშაული? არის იგი დამოუკიდებელი სამართლებრივი უმართლობა თუ იგი უნდა მოვიაზროთ უკვე არსებულ დანაშაულებრივ შემადგენლობათა ფარგლებში, როგორც ამ შემადგენლობათა ობიექტური მხარის ელემენტები. ამ პრობლემის გარკვეული დოზით ანალიზს აქვს გადამწყვეტი მეცნიერული და პრაქტიკული მნიშვნელობა და მასზეა დამოკიდებული თავად კიბერდანაშაულის ცნების მიზანშეწონილობის საკითხიც.

როდესაც საუბარია ადამიანის დესტრუქციულ საქმიანობაზე საინფორმაციო სფეროში, მხედველობიდან არ უნდა გამოგვრჩეს მისი სოციუმზე ზემოქმედების როგორც სამართლებრივი, ისე ტექნიკური, ეთიკური, სოციალური, ფსიქოლოგიური, კრიმინოლოგიური თუ სხვა ასპექტები.

სიახლეს არ წარმოადგენს ის გარემოება, რომ ტექნოლოგიურმა რევოლუციამ, გარკვეულწილად, გააუფერულა სოციუმში საუკუნეების განმავლობაში დამკვიდრებულ ეთიკურ ნორმათა პრიორიტეტულობა და გზა გაუხსნა ადამიანის პრაგმატულად აზროვნების ტენდენციას. ამის მიზეზი, გარდა გლობალიზაციის უარყოფითი, თანმდევი პროცესებისა, იმის დამსახურებაცაა, რომ კიბერტექნოლოგიბი ორგანულად შეეზარდა სოციალური ცხოვრების ყველა სფეროს, იქცა ადამიანთა ყოფის ორგანულ ნაწილად და უკვე აშკარად კარნახობს მას თავის დღის წესრიგს. ბუნებრივია ის გარემოებაც, რომ ადამიანური ცხოვრების ახალმა სტილმა,რომელიც, მართალია, უფრო კომფორტულს ხდის მას, დასაბამი დაუდო თვისებრივად ახალი, სოციალურად საშიშ ისეთ ქმედებათა აღმოცენებას, რომელსაც კაცთა მოდგმა დღემდე არ იცნობდა. შესაბამისად, დღის წესრიგში დადგა გარკვეულ დესტრუქციულ ქმედებათა კრიმინალიზაციის აუცილებლობა. კრიმინალიზაციის პროცესი კი სამართალშემოქმედებითი საქმიანობის ყველაზე რთული და მრავალგანზომილებიანი მიმართულებაა; კიბერტექნოლოგიების მზარდმა სოციალიზაციამ და კომპიუტერიზაციის შეუქცევადმა პროცესმა კი იგი უფრო დაამძიმა. სწორედ, კიბერსივრცე აღმოჩნდა ინდივიდებს, პირთა ცალკეულ ჯგუფებსა და სახელმწიფოებს შორის დაპირისპირების არენა. ამასთან, ეს დაპირისპირება მოიცავს სოციალური ცხოვრების ყველა მიმართულებას. ამიტომ, საკითხი კრიმინალიზაციის პროცესის მიზანშეწონილობაზე, კონკრეტულად ამ კუთხით, არავითარ ეჭვს არ იწვევს.

ამასთან, კრიმინალიზაცია, როგორც სოციალური კონტროლის არასასურველი მაგრამ აუცილებელი მექანიზმი აუცილებლად ექვემდებარება შესაბამის პრინციპებს. ამიტომაა, რომ სოციალური სტრუქტურა წინასწარ განსაზღვრავს ქმედებათა შეფასების კრიტერიუმებს, რაც მიუთითებს საზოგადოებაში გაბატონებულ ღირებულებებზე და მის სოციალურ შინაარსზე.

თავი 3. კიბერდანაშაულის სისხლისსამართლებრივი რეგულირების პრობლემა. (ქვეთავები:3.1.ცალკეული ქვეყნების სისხლისსამართლებრივი კანონმდებლობა. 3.2. ,,კიბერდანაშაულის,, სამართლებრივ-სისტემური მოწესრიგება.3.3 3.3 .გაუფრთხილებლობა, როგორც ,,კიბერდანაშაულებრივ'' ქმედებათა გამოვლინების შესაძლო ფორმა).

ეროვნული და საზღვარგარეთის სისხლისსამართლებრივი კანონმდებლობის შედარებით-სამართლებრივი ანალიზის საფუძველზე განხილულია კიბერდანაშაულებრივ ქმედებათა კრიმინალიზაციის თავისებურებანი და გამოთქმულია მოსაზრებები მათი სისტემურ-სამართლებრივი მოწესრიგების კუთხით.

იმთავითვე უნდა შევთანხმდეთ, რომ კიბერუსაფრთხოებისა და მისი შემადგენელი ნაწილის - კიბერდამნაშავეობის საკითხი, აშკარად სცილდება ცალკე აღებული ქვეყნისა და ეროვნული კანონმდებლობის ფარგლებს. ამის მიზეზი კი მისი ტრანსნაციონალური და გლობალური ხასიათია.

სამეცნიერო ლიტერატურაში დავას არ იწვევს კიბერდანაშაულის, როგორც მომეტებული საშიშროების საკითხი, ისე სისხლისსამართლებრივი კანონმდებლობის ჰარმონიზაციის აუცილებლობა. სწორედ, კანონმდებლობის ჰარმონიზაცია და მჭიდრო საერთაშორისო თანამშრომლობითაა შესაძლებელი კიბერუსაფრთხოების გარკვეულწილად უზრუნველყოფა და შესაბამის ჩარჩოებში მოქცევა.

დღემდე ჩატარებული სამეცნიერო კვლევების უმეტესი ნაწილი, არსებული მონოგრაფიები, სადისერტაციო ნამუშევრები თუ ცალკეული სტატიები, ეძღვნება კიბერდანაშაულის წარმოშობის ისტორიულ ასპექტებს, ცალკეული ქვეყნების გამოცდილებას, კიბერუსაფრთხოების ტექნიკურ მხარეებს და დანაშაულის შემადგენლობის ცალკეული კონსტრუქციების მიზანშეწონილობის დასაბუთებას, ისევე როგორც ცალკეულ სახელმწიფოთა სისხლისსამართლებრივი კანონმდებლობის

შედარებით-სამართლებრივ ანალიზს. ამ კუთხით, რაიმე არსებითი და აქტუალური პრობლემა ვერ იქნება წინ წამოწეული და განხილული, ხოლო იგივე საკითხთა განმეორებით კვლევა, საკითხისადმი მხოლოდ ფორმალური მიდგომა იქნებოდა და არავითარ მეცნიერულ ღირებულებას ვერ შეიძენდა. ამიტომ, ჩვენს მიერ, საზღვარგარეთის ქვეყნების სისხლისსამართლებრივი კანონმდებლობის ანალიზისას გამოვყოფთ მხოლოდ ძირითად და, კვლევისთვის არსებულ მინიმუმს, რომელიც საშუალებას მოგვცემს ფოკუსირება მოვახდინოთ ჩვენს მიერ დასმული საკითხების ირგვლივ, რომლის არსიც იმის გარკვევაში მდგომარეობს - **თუ რამდენადაა შესაძლებელი კიბერდანაშაულებრივი ხასიათის ქმედებები მივაკუთვნოთ დამოუკიდებელ უმართლობათა კატეგორიას და მეორე - მსგავსი კატეგორიის ქმედებათათვის, რამდენადაა ,, კარხსნილი"(მ. უგრეხელიძე) გაუფრთხილებლობა.**

პრობლემის არსი მდგომარეობს, არა იმდენად, კიბერდანაშაულებრივ ქმედებათა კრიმინალიზაციის აუცილებლობის დასაბუთებაში (რაც თავისთავად ასევე კომპლექსურ მიდგომას საჭიროებს), არამედ იმის დადგენაში, სავარაუდოთ, თუ სად გადის უამრავ კიბერდანაშაულებრივ შემადგენლობათა კრიმინალიზაციის ზღვარი.

მხედველობაში გვაქვს საკანონმდებლო საქმიანობის ისეთი ტენდენცია, როდესაც სისტემატიურად წარმოიშობა ,,კიბერდანაშაულებრივ" ქმედებათა ისეთი სახეობები, რომლებიც დაუყოვნებლივ საჭიროებენ კრიმინალიზაციას და კანონმდებელიც იძულებულია შეიმუშაოს დანაშაულის შემადგენლობის შესაბამისი კონსტრუქცია და დააწესოს სიხლისსამართლებრივი პასუხისმგებლობა. მსგავსი ტენდენცია, ადრე თუ გვიან, აუცილებლად მიგვიყვანს ისეთ მდგომარეობამდე, როდესაც, ერთი მხრივ, პარალელურად, სახეზე გვექნება ტრადიციულ შემადგენლობათა ანალოგიური შემადგენლობები. ე. ი. გვექნება თაღლითობის ტრადიციული შემადგენლობა და კიბერთაღლითობა (აღნიშნულ შემადგენლობებს მრავალი ქვეყნის კანონმდებლობა იცნობს); ქურდობა და კიბერქურდობა; ტერორიზმი და კიბერტერორიზმი, ან ტექნოლოგიური ტერორიზმი; მუქარა და კიბერმუქარა და სხვა. ამასთან, დასახელებულ ქმედებათა ზოგიერთი კონსტრუქცია რეგლამენტირებულია ეროვნულ სისხლის სამართლის კოდექსში. მთავარი მაინც ისაა, რომ კიბერსივრცე

პერმანენტულად გვთავაზობს რაოდენობრივად და თვისებრივად ახალ, სოციალურად საშიშ ქმედებათა მრავალფეროვნებას, ხოლო ყოველ ჯერზე, მათი კრიმინალიზება და ცალკეულ შემადგენლობათა ჩამოყალიბება უთანაზომოდ გაზრდის სისხლის სამართლის კოდექსის მოცულობას, რაც ყველაფერთან ერთად, გააძნელებს სამართალგამოყენებით სფეროს. ამ შემთხვევაში, აშშ-ს სისხლის სამართლის კოდექსი მაგალითად არ გამოგვადგება, რადგანაც იქ არსებულ დანაშაულებრივი ქმედებათა რეგლამენტაცია ხდება არა სისტემურად, არამედ ალფავიტის მიხედვით, რაც ამ ქვეყნის სამართლის სისტემის თავისებურებითა და სამართალგამოყენების გაადვილების მოტივითაა განპირობებული.

შორს რომ არ წავიდეთ, უკრაინის სისხლის სამართლის კოდექსში უკვე შეინიშნება კიბერდანაშაულის შემადგენლობათა სიმრავლე, რომლებიც მიმობნეულია კოდექსის სხვადასხა თავებში და უსისტემოდ ხდება მათი რეგლამენტაცია. ასეთი მდგომარეობაა ყველა ქვეყნის სისხლისსამართლებრივ კანონმდებლობაში.

ზემოთ აღვნიშნეთ, რომ მსოფლიო ქვეყნების უმრავლესობა ერიდება კიბერდანაშაულის საკანონმდებლო განმარტებას და, შესაბამისად, ამ ტერმინის გამოყენებაც უარყოფილია მოქმედ სისხლისსამართლებრივ კანონმდებლობაში. იგი ჩანაცვლებულია ,,კომპიუტერული დანაშაულის'' ცნებით, რაც სრულად აკმაყოფილებს სისხლისსამართლებრივ მოთხოვნებს.

ამჯერად, გამოვყოფთ პრობლემებს, რომლებიც, ერთის მხრივ, შეიძლება განზოგადებულ იქნეს ქმედებათა დიდი წრისთვის, ხოლო, მეორე მხრივ, შეეხება კონკრეტულ საკითხებს.

ეროვნულ სისხლისსამართლებრივ კანონმდებლობაში, კიბერდანაშაულებრივ ქმედებათა კრიმინალიზების პროცესი განაპირობა საერთაშორისო გამოცდილებამ და თავად საკითხის აქტუალობამ. დღეის მდგობარეობით, საქ.სსკ XXXV-ე თავი ეძღვნება ,,კიბერდანაშაულს'' და შედგება ხუთი შემადგენლობისგან (284-286[2].). აღნიშნული შემადგენლობები ჩვენ ზოგადად განვიხილეთ და მისი შემდგომი განხილვა მიზანშეწონილად არ მიგვაჩნია.

პასუხი უნდა გაეცეს შეკითხვებს: 1) რამ განაპირობა „კიბერდანაშაულებრივ" ქმედებათა კრიმინალიზაციის საჭიროება დამოუკიდებელ შემადგენლობებად? 2) ხომ არ შექმნა მსგავსმა პროცესმა სისხლისსამართლებრივ ნორმათა კონკურენციის ისეთი დონე, როდესაც მათი გამიჯვნა სირთულესთანაა დაკავშირებული ან/და შეუძლებელი ხდება? 3)თუ ეს ასეა, მაშინ რა სახის საკანონმდებლო ცვლილებებია მიზანშეწონილი საკითხის ნორმალიზებისთვის?

საკვლევი თემის ფარგლებში განვითარებული მსჯელობის საფუძველზე, ვფიქრობთ, რომ შემდეგი სახის პასუხები ნაწილობრივ მაინც იქნება შესაბამისობაში, როგორც პრობლემის არსთან, ისე მათი რაციონალური გადაწყვეტის გზებთან:

1. ეროვნულ და საზღვარგარეთის სისხლისსამართლებრივ კანონმდებლობაში ასახულ კიბერდანაშაულებრივ ქმედებათა დამოუკიდებელ შემადგენლობად ფორმირებას საფუძვლად დაედო შემადგენლობის ობიექტური მხარის ისეთი ელემენტები (ფაკულტატური), როგორიცაა -დანაშაულის ჩადენის ხერხი, საშუალება, საგანი. (კომპიუტერული ტექნოლოგიები). კანონმდებელმა, მომეტებული სოციალური საშიშროების შემცველად მიიჩნია ნებისმიერი დანაშაულის სტრუქტურაში კომპიუტერულ ტექნოლოგიათა ნიშანი. (კიბერტერორიზმი, ტექნოლოგიური ტერორიზმი და სხვ). ამასთან, რიგ შემადგენლობებში კიბერტექნოლოგიების როლი და მისი ადგილი განისაზღვრა, როგორც მაკვალიფიცირებელი გარემოება, რაც გამართლებულია სამართლებრივი და საკანონმდებლო ტექნიკის თვალსაზრისით. რაც შეეხება, ქმედებათა დამოუკიდებელ შემადგენლობებად ფორმირებას, ამის არც სამართლებრივი, არც კრიმინოლოგიური და არც სოციალური საჭიროება არ არსებობდა. სავარაუდოთ, იგი განპირობებულია „ბუდაპეშტისა" და სხვა საერთაშორისო კონვენციების რეკომენდაციებით, ისევე, როგორც საზღვარგარეთის ქვეყნების საკანონმდებლო საქმიანობის მექანიკური კოპირებით.კიბერდანაშაულებრივ შემადგენლობათა დამოუკიდებელ უმართლობად ფორმირებამ იმ ფორმით, როგორც ეს სისხლის სამართლის კოდექსშია ასახული, შექმნა არა სპეციალური ნორმის ტიპური კონსტრუქცია, არამედ ფიქციის ისეთი მოდელი, რომელიც იძულებულს ხდის

სამართალგამოყენებით პრაქტიკას მოახდინოს ქმედების კვალიფიკაცია დანაშაულთა ერთობლიობით. მსგავსი პრაქტიკა ეწინააღმდეგება, კრიმინალიზაციის საყოველთაოდ აღიარებულ პრინციპებსა და კრიტერიუმებს; ხელს უწყობს მახინჯი საგამოძიებო და სასამართლო პრაქტიკის დამკვიდრებას და ქმნის უსამართლობის განცდას.

2. მიუხედავად იმისა, რომ კიბერდანაშაულთან მიმართებაში არსებული საგამოძიებო და სასამართლო პრაქტიკა მწირია და ხშირად ხელმიუწვდომელი, ცალკეულ სისხლის სამართლის საქმეთა ანალიზი ცხადყოფს, რომ პრობლემის სათავე, პირველ რიგში, კრიმინალიზაციის პროცესშია. კერძოდ, როგორც უკვე არაერთხელ აღინიშნა, კიბერდანაშაულებრივ ქმედებათა დამოუკიდებელ სამართლებრივ კონსტრუქციად კრიმინალიზება იმთავითვე გულისხმობს სისხლისსამართლებრივ ნორმათა კონკურენციას, ამ სიტყვის ყველაზე უარყოფითი გაგებით. უმეტეს შემთხვევაში, კრიმინალიზებას დაექვემდებარა იდენტური შინაარსისა და სამართლებრივი სტრუქტურის ნორმები, რაც დაუშვებელია.

   ამ მიზნით, მიზანშეწონილად მიგვაჩნია, გატარდეს შესაბამისი საკანონმდებლო ცვლილებები სისხლის სამართლის კოდექსში, რომლის მიზანი იქნება ,,კიბერდანაშაულებრივ" ხასიათის ქმედებათა არა დამოუკიდებელ უმართლობად კრიმინალიზება, არამედ მისი გათვალისწინება უკვე არსებულ, ტრადიციულ შემადგენლობათა ფარგლებში. დანაშაულის შემადგენლობის ობიექტური მხარის ფაკულტატური ელემენტების (დანაშაულის ჩადენის საშუალება, საგანი, ხერხი) გათვალისწინება მსგავსი სქემით სრულად აგვაცილებდა არსებულ და სამომავლო პერსექტივაში მოსალოდნელ სამართლებრივ სირთულეებს. ამასთან, ამ ელემენტების გათვალისწინება, როგორც მაკვალიფიცირებელი გარემოებისა, შესაძლებელია, როგორც ცალკეული თავების მიხედვით, ისე კოდექსის ზოგადი ნაწილის ნორმებში.

ამდენად, ჩვენს მიერ დაყენებული საკითხები, შეიძლება ითქვს, რომ მხოლოდ პრობლემის დაყენების, დემონსტრირებისა და მისი აქტუალობის წამოჩინების მცდელობაა, რადგან თავად პრობლემის სიღრმისეული კვლევა საჭიროებს გაცილებით განსხვავებულ მიდგომებს. ჩვენის მხრიდან კი ადგილი ქონდა მხოლოდ ამ პრობლემის აქტუალობის დასაბუთებისა და გადაწყვეტის მოკრძალებულ მცდელობას.

დასკვნა

სადისერტაციო ნაშრომის ფარგლებში დასმულ საკითხთა იურიდიული აქტუალობა, შეიძლება განხილულ იქნას, როგორც ,,კიბერდანაშაულებრივ'' ქმედებათა კრიმინალიზაციის პროცესში არსებულ სამართლებრივ, კრიმინოლოგიურ და საკანონმდებლო საქმიანობის ტექნიკურ მხარეთა პრობლემატიკის წარმოჩინების მეცნიერული ინტერესი, რომელიც, თავის მხრივ, ნასაზრდოებია პრაქტიკული მოსაზრებებითაც.

პირველი და უმთავრესი პრობლემა, რომელიც უწყვეტ ხაზად გასდევს კრიმინალიზაციის პროცესს, მდგომარეობს ისეთ ცნებათა ჩამოყალიბებასა და მეცნიერულ დასაბუთებაში, რომელიც საშუალებას მისცემს კანონმდებელს სრულყოფილად განახორციელოს საკანონმდებლო საქმიანობა.

ის გარემოება, რომ დღეის მდგომარეობით არ გაგვაჩნია ,,კიბერდანაშაულის'' საკანონმდებლო დეფინიცია, სისხლის სამართლის მეცნიერებასა და სამართალგამოყენებით სფეროში ქმნის მრავალ გაუგებრობას და სიძნელეს. მართლაც, რთულია იმსჯელო დანაშაულთა ისეთ კატეგორიაზე, როგორიც ,,კიბერდანაშაულია'' და ხელთ არ გაგაჩნდეს მისი ლეგალური განმარტება. ამ შემთხვევაში, დოქტრინაში არსებული დეფინიციები, რომელიც არაერთგვაროვანი და განსხვავებულია, ვერ გამოდგება სისხლისსამართლებრივი მიზნებისთვის. მოქმედი კანონმდებლობის მიხედვით, ,,კიბერდანაშაული'' დაყვანილია კომპიუტერულ დანაშაულამდე

და, ერთი შეხედვით, რაიმე სახის სამართლებრივ პრობლემას არ ქმნის, მაგრამ თუ საკითხს სხვა კუთხით შევხედავთ, აღმოჩნდება, რომ ცნების არარსებობა მიზეზი ხდება ამ სახის უმართლობათა სისტემური მოუწესრიგებლობისა, რაც იმაში გამოიხატება, რომ სისხლის სამართლის კოდექსში მსგავსი შინაარსის დანაშაულთა შემადგენლობები გაბნეულია აბსოლუტურად უსისტემოდ და ქმედების საკანონმდებლო და სასამართლო კვალიფიკაციისას, პრაქტიკაში ქმნის სერიოზულ სიძნელეებს. მხედველობაში გვაქვს სამართლებრივ ნორმათა ისეთი კონკურენციის დონე, როდესაც კანონის ინტერპრეტაციის სამართლებრივი მეთოდი ერთობ არაეფექტიანია.

სავარაუდოთ, ეს გარემოებაა იმის მიზეზი, რომ მთელი რიგი ქვეყნების კანონმდებლობა იყენებს არა კიბერდანაშაულის, არამედ კომპიუტერული დანაშაულის ცნებას, რაც უფრო შეესაბამება სამართლებრივ წესრიგს. რა თქმა უნდა, სისხლისსამართლებრივი ცნების განმარტება არ უნდა ხდებოდეს მხოლოდ ინტუიციური გააზრებისა და სუბიექტური შეხედულებების საფუძველზე, არამედ მას საფუძვლად უნდა დაედოს მკაცრად განსაზღვრული, მეცნიერულად დასაბუთებული კრიტერიუმები. წინააღმდეგ შემთხვევაში, ცნების ზოგადი სახით გაგება, აუცილებლად მიგვიყვანს კრიმინალიზაციის პროცესში უკიდურეს სუბიექტივიზმამდე. კრიმინალიზაციის პროცესის ასეთი სახით წარმართვა კი, გარანტირებულად დაამკვიდრებს არაერთგვაროვან სამამართლო პრაქტიკას.

ამიტომ, სანამ არ მომხდარა ,,კიბერდანაშაულის''ცნების, ერთიანი, მეცნიერულად დასაბუთებული გაგება და ამის საფუძველზე, მისი ლეგალური განმარტება, მიზანშეწონილია დროებით უარი ითქვას მისი საკანონმდებლო დანიშნულებით გამოყენებაზე, რადგანაც ,,კომპიუტერული დანაშაულის'' ცნება, მოცემულ სამართლებრივ რეალობაში, სრულად შეესაბამება სამართლებრივ მოთხოვნებს. აღნიშნული, ისე არ უნდა იქნას გაგებული, თითქოსდა, საერთოდ უარი უნდა ითქვას ამ ტერმინის გამოყენებაზე. რა თქმა უნდა არა. ეს ტერმინი, როგორც უნივერსალობის აღმნიშვნელი ერთგვარი სიმბოლო, ხელსაყრელია კიბერსივრცის წიაღში წარმოშობილი და მაღალი ტექნოლოგიების სისტემებთან გენერირებული ისეთი ფენომენების აღსანიშნავად, როგორიცაა ხელოვნური ინტელექტი,

კრიპტოვალუტა და სხვა. ამიტომ, მეცნიერული კვლევების თვალსაზრისით, მისი ტერმინოლოგიური დანიშნულებით გამოყენების საჭიროება ეჭვს არ იწვევს.

ჩვენს მიერ გამოთქმული თვალსაზრისი, რომ სისხლის სამართლის კოდექსში რეგლამენტირებული კიბერდანაშაულებრივი (კომპიუტერული) შემადგენლობები, მათი სისტემური წყობის თვალსაზრისით, არ ექვემდებარება ლოგიკურ-სამართლებრივ წესრიგს, არ არის გამოწვეული მხოლოდ ,,კიბერდანაშაულის'' ცნებასთან დაკავშირებული გაუგებრობით. საქმე იმაში გახლავთ, რომ ეროვნულ და უცხო ქვეყნების სისხლისსამართლებრივ კანონმდებლობაში, კომპიუტერული შინაარსის დანაშაულებრივი შემადგენლობები მოქცეულია, როგორც სპეციალურად ამისთვის განკუთვნილ (კიბერდანაშაული ან კომპიუტერული დანაშაული), ისე სხვა კატეგორიისა და ტიპობრივი ჯგუფის შემადგენლობათა მარეგულირებელ საკანონმდებლო თავებში. როგორც უკვე აღვნიშნეთ, ეს იწვევს ნორმათა ისეთ კონკურენციას, რომლის დროსაც ვერ ხერხდება ზოგადი და სპეციალური ნორმების ურთიერთგამიჯვნა, რის შედეგადაც ადგილი აქვს ქმედების დანაშაულთა ერთობლიობით კვალიფიკაციის უსამართლო შემთხვევებს (უმართლობის ერთი და იგივე შინაარსისა და სტრუქტურის ქმედებათა კვალიფიკაცია ორი შემადგენლობით).

თუ ეს ასეა, მაშინ იმის გამომწვევი მიზეზიც უნდა დადგინდეს, რამაც მსგავსი ვითარება შექმნა.

ამ საკითხის გარკვევა კრიმინალიზაციის პროცესის კვალობაზე უნდა მოხდეს. უპირველეს ყოვლისა, უნდა დადგინდეს კანონმდებლის ნება და ის მახასიათებელი ნიშნები, რომლებიც განაპირობებენ ამა თუ იმ ქმედების კუთვნილებას კომპიუტერული დანაშაულისადმი.

ამა თუ იმ უმართლობათა კრიმინალიზაციისა და სისტემურ-სამართლებრივი მოწესრიგების დროს კანონმდებელი ხელმძღვანელობს საყოველთაოდ აღიარებული სამართლებრივი პრინციპებითა და კრიტერიუმებით, რის შესახებაც ჩვენ გარკვეულწილად ვიმსჯელეთ ნაშრომის ძირითად ნაწილში, ისევე როგორც კრიმინალიზაციის პროცესში, კანონმდებლის ექსკლუზიურ უფლებაზე. აღინიშნა ისიც, რომ კანონმდებლის ეს უფლება არ არის აბსოლუტური და ზღვარდაუდებელი,

სწორედ, ამ პრინციპების ბოჭვით. მაგრამ, პრინციპები და კრიტერიუმები ყოველთვის ზოგადი ხასიათისაა და ხშირ შემთხვევაში მოკლებულ არიან ნიუანსებში წვდომის შესაძლებლობას. ამიტომ, მოცემულ შემთხვევაში, პასუხი, თუ რა სამართლებრივი კრიტერიუმებით და მექანიზმებით ხელმძღვანელობდა კანონმდებელი კომპიუტერულ დანაშაულთა კლასიფიკაციისა და მათი სისტემურ- სამართლებრივი მოწესრიგებისას, ვერ იქნება მიღებული სამართლებრივ პრინციპებზე დაყრდნობით. ამიტომ, საჭიროა თვით დანაშაულის შემადგენლობათა ელემენტების სტრუქტურული ანალიზი.

რა სამართლებრივი დასკვნაც არ უნდა გაკეთდეს კიბერდანაშაულებრივ (კომპიუტერულ) ქმედებათა სტრუქტურული მახასიათებლების მიმართ, ერთი რამ უდავოა: მისი გენეზისი და შემდგომ კრიმინალიზაციის პროცესი, უალტერნატივოდ განპირობებულია ამ ტიპის შემადგენლობათა ელემენტების აქტუალიზაციით. ამასთან, საუბარი მიდის და არა ძირითად, არამედ ობიექტური მხარის ელემენტებზე (ე.წ. ფაკულტატური ელემენტები-ხერხი, საგანი, საშუალება). სწორედ, ეს ელემენტები დაედო საფუძვლად ზემოხსენებულ შემადგენლობათა კრიმინალიზაციას და არა, სუბიექტური მხარის ნიშნები.

გამოდის, რომ სწორედ ეს ნიშნები განსაზღვრავენ ქმედების სპეციფიურობასა და კუთვნილებას ამ ტიპის უმართლობებისადმი. შესაბამისად, ეს ნიშნები უნდა დაედოს საფუძვლად ამ ქმედებათა კლასიფიკაციას, მათი კოდექსში შემდგომი რეგლამენტაციის მიზნით, მაგრამ როგორც ვნახეთ, კიბერდანაშაულებრივ შემადგენლობებს ვხვდებით სისხლის სამართლის კოდექსის სხვადასხვა კატეგორიის უმართლობათა ჯგუფში. (კიბერტერორიზმი, ტექნოლოგიური ტერორიზმი, პირადი ცხოვრების საიდუმლოს ხელყოფა და სხვ). ამასთან, ზოგიერთ შემადგენლობაში პირდაპირაა მითითებული კიბერტექნოლოგიებზე, როგორც შემადგენლობის ძირითად ან მაკვალიფიცირებელ გარემოებებზე. ამასაც რომ თავი დავანებოთ, ტრადიციულ შემადგენლობათა უმეტესობის ობიექტურ მხარეში, იმთავითვე, მოიაზრება კომპიუტერულ სისტემათა და ინტერნეტის როლი. (სატრანსპორტო, საავიაციო, ენერგეტიკის და სხვა სფეროების მუშაობის პრინციპს, უმეტესწილად, განსაზღვრავს კიბერტექნოლოგიები).

კიბერსივრცის ფენომენიდან გამომდინარე, უკვე არსებული და პოტენციურად სამომავლო პერსპექტივა იმის მყარ საფუძველს იძლევა, რომ მსგავსი კონსტრუქციის შემადგენლობების კრიმინალიზების საჭიროება ყოველთვის იქნება დაუსრულებლად. ასეთი ვითარებაში, სისხლისსამართლებრივი კანონმდებლობა ფიზიკურად ვერ დაიტევს და ,,გადახარშავს'' მას.

ამიტომ, სამართლებრივი და, არა მარტო სამართლებრივი, თვალსაზრისით, მიზანშეწონილია ,,კიბერდანაშაულის'' ელემენტთა გათვალისწინება უკვე არსებულ ტრადიციულ შემადგენლობათა ფარგლებში, როგორც ამა თუ იმ დანაშაულის მაკვალიფიცირებელი გარემოება. კრიმინალიზაციის ასეთი კონფიგურაცია ერთი მხრივ, გამართლებულია იმითაც, რომ თავიდან ავიცილებთ სისხლისსამართლებრივ ნორმათა არასასურველ კონკურენციას, რომ არაფერი ვთქვათ საკანონმდებლო საქმიანობის ტექნიკურ მხარეზე. მეორე მხრივ, იგი ხელს შეუწყობს კვალიფიკაციის პროცესს და ერთგვაროვანი სასამართლო პრაქტიკის დამკვიდრებას.

თუ შევთანხმდებით აღნიშნული მსჯელობის მართებულობაზე, მაშინ თავიდან ავიცილებთ ,,კიბერდანაშაულის'' გაუფრთხილებლობით კრიმინალიზაციის პროცესთან დაკავშირებული არგუმენტაციის აუცილებლობას, რადგანაც ეს საკითხი გადაწყდება უკვე არსებული დანაშაულის შემადგენლობის შინაარსის მიხედვით. მაგალითად: თუ კიბერტერორიზმი, ტერორიზმის შემადგენლობის მაკვალიფიცირებელი გარემოება იქნება, ამ შემთხვევაში გასაგები იქნება ისიც, რომ საქმე გვაქვს განზრახ დანაშაულთან; თუ საფრენი აპარატის მართვის ან ექსპლუატაციის წესების დარღვევა, კიბერტექნოლოგიებისადმი გაუფრთხილებლობით დამოკიდებულებამ გამოიწვია, ადგილი აქვს გაუფრთხილებელ დანაშაულს; ატომური ენერგეტიკის ობიექტებზე უსაფრთხოების წესების დარღვევა თუ კომპიუტერული ტექნოლოგიების გაფრთხილებელმა გამოიწვია, აქაც ყველაფერი სრულიად ნათელი იქნება.

ამრიგად, კვლევის პროცესში დასმული პრობლემატური საკითხები, რომელიც უკავშირდება კიბერსივრცის წიაღში წარმოშობილ ქმედებათა კრიმინალიზაციის სპეციფიკას, კომპლექსური და მრავალასპექტიანი შინაარსის საქმიანობაა და საჭიროებს

სიღრმისეულ კვლევას. მით უმეტეს, რომ სოციუმის ტოტალური კომპიუტერიზაცია და ხელოვნური ინტელექტის ტანდემი კიბერტექნოლოგიებთან, უახლოვეს მომავალში წარმოშობს მრავალ სამართლებრივ დილემას.

სადისერტაციო ნაშრომის ძირითადი შინაარსი გამოქვეყნებულია შემდეგ პუბლიკაციებში

სტატიები:

1.ამაშუკელი გიორგი. ,,კიბერსივრცეში განხორციელებულ ქმედებათა კრიმინალიზაციის აუცილებლობა.'' შედარებითი სამართლის ქართულ-გერმანული ჟურნალი 10/2021 ქ. თბილისი

2. ამაშუკელი გიორგი. ,,კიბერდანაშაული, როგორც დანაშაულის გამოვლინების უნივერსალური ფორმა.'' შედარებითი სამართლის ქართულ-გერმანული ჟურნალი 11/2021 ქ. თბილისი.

3. ამაშუკელი გიორგი. ,, კიბერსივრცეში ადამიანის დესტრუქციული საქმიანობის სამართლებრივ-კრიმინოლოგიური ანალიზი.'' შედარებითი სამართლის ქართულ - გერმანული ჟურნალი. 4/2022. ქ. თბილისი.

საერთაშორისო სამეცნიერო კონფერენციები:

1. ამაშუკელი გიორგი. ,, კიბერდანაშაული, როგორც დანაშაულის გამოვლინების უნივერსალური ფორმა.'' საერთაშორისო სამეცნიერო კონფერენცია - ,,თანამედროვე სამართლის გამოწვევები.'' კავკასიის საერთაშორისო უნივერსიტეტი. . თბილისი 2022.

Caucasus International University

Right of Authorship

George Amashukeli

The problem of criminalization of actions carried out in cyberspace

PhD Program: Law

Scientific Supervisor: Sergo chelidze, Doctor of Laws, Associate Professor

Abstract dissertation Presented for the academic degree of Doctor of Laws

Tbilisi

2022

Scientific supervisor: **Sergo Chelidze,**

Doctor of Low, Associate Professor

Official reviewers: **Irakli Imerlishvili,**

Doctor of Low, Associate Professor

Vladimer Macharashvili

Doctor of Low, Associate Professor

Defence of the dissertation shall take place on December 02, 2022, 15:00 PM, at the Dissertation Council of the Faculty of Law of Caucasus International University

Address: Room 305, Building 1 of Caucasus International University, Chargali Str. N73, 0141, Tbilisi

Dissertation is accessible at the library of the Caucasus international University

Secretary of the Dissertation Board: **Aleksandre Giorgidze**

Doctor of Low, Associate Professor

Annotation

The presented paper deals with such an undesirable but necessary process of social control as criminalization. The complexity and problematic nature of this process is particularly acute in relation to the actions that take place within the cyberspace. Presumably, no field of human activity reveals the contradiction of political, religious, cultural or other values and differences of opinion as it does in the process of criminalization. If a society has developed a certain degree of immunity and tolerance for the existing, traditional offenses, the same cannot be said of newly emerging socially dangerous acts, the criminalization of which is always a matter of passion and time-consuming discussion.

The contours of the issue lie on the surface of events and are related to the concept of "cybercrime" (Chapter XXXV of the Criminal Code "Cybercrime"). The legislature criminalizes cybercrime, but does not formulate its definition.

Bringing the concept of cybercrime to an understanding of the content of cybercrime is unacceptable. It is true that the latter is considered within the framework of cybercrime, but the lack of a legislative definition of cybercrime itself complicates the systematic legal regulation of this category of injustices; This circumstance, in turn, creates a competition of norms, during which it is substantially difficult to qualify the action and is based on heterogeneous case law.

In the course of the research, opinions are presented on the expediency of legalizing this problem and negligence as a possible form of criminalization of the manifestation of cybercrime.