ინფორმაცია კიბერდანაშაულის შესახებ

კიბერდანაშაულის არსი და რისკები

ინფორმაციული ტექნოლოგიების განვითარებამ და აღნიშნულთან დაკავშირებული რისკების მატებამ დღის წესრიგში საქართველოს სისხლის სამართლის კოდექსში შესაბამისი ცვლილებების საჭიროება დააყენა. 2000-2010 წლებში განხორციელებული ცვლილებების შედეგად კოდექსში ამოქმედდა კიბერდანაშაულის თავი, რომელიც სამ მუხლს მოიცავს. ესენია:

ა. კომპიუტერულ სისტემაში უნებართვო შეღწევა[1];

ბ. კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის უკანონოდ გამოყენება; [2]

გ. კომპიუტერული მონაცემის ან/და კომპიუტერული სისტემის ხელყოფა. [3]

აღნიშნული მუხლების პრაქტიკაში იმპლემენტაცია უკანასკნელ პერიოდამდე გარკვეულ სირთულეებთან იყო დაკავშირებული, თუმცა სათანადო საკანონმდებლო, მატერიალურ-ტექნიკური ბაზის შექმნამ, ასევე გამომძიებელთა და პროკურორთა მუდმივმა ტრენინგებმა უზრუნველყო აღნიშნული დანაშაულის ეფექტური პრევენცია და გამოძიება.

კიბერდანაშაულის კატეგორია

საერთაშორისო პრაქტიკაში გამოყოფენ კიბერდანაშაულის სამ კატეგორიას:

1. კომპიუტერის გამოყენება კრიმინალურ აქტივობასთან დაკავშირებული ქმედებების განსახორციელებლად (ნარკოდილერის შავი ბუღალტერიის გადმოწერა);

[1] მუხლი 284;
[2] მუხლი 285;
[3] მუხლი 286;

2. კომპიუტერის დანაშაულის ინსტრუმენტის სახით გამოყენება (არასრულწლოვანთა პორნოგრაფიის გავრცელება ინტერნეტის მეშვეობით);

3. კომპიუტერი, როგორც დანაშაულის იარაღი (ვირუსების გავრცელება).[4]

კიბერდანაშაულის შედეგად შეიძლება დაზარალდეს:

- **ინდივიდი** - აღნიშნული შეიძლება გამოიხატოს კიბერ გადაკიდებაში, დაჩაგვრაში, შეურაცხყოფის მიყენებაში, საბავშვო პორნოგრაფიის გავრცელებაში და სხვ.;

- **საკუთრება** - ინტერნეტ სივრცეშიც ხდება ისეთი დანაშაულები, როგორიცაა: ქურდობა და თაღლითობა. ელექტრონული შესყიდვებისა და ელექტრონული ბანკინგის მეშვეობით, კიბერ დამნაშავეებს წვდომა მისცეს სხვა პირთა ქონებისა და ფინანსებისადმი. მათ თავისუფლად შეუძლიათ მოიპარონ პირის საბანკო მონაცემები ან უბრალოდ დააზიანონ სხვა პირის ინფორმაცია ან პროგრამა;

- **სახელმწიფო** - აღნიშნული ტიპი ერთ-ერთი ყველაზე გავრცელებულია და მას სწორედ კიბერ ტერორიზმად მოიხსენიებენ. წარმატების შემთხვევაში დამნაშავეს შეუძლია დაანგრიოს სახელმწიფო სისტემა და გამოიწვიოს ქაოსი მოქალაქეებში.

კიბერ დანაშაულის გავრცელებული ტიპებია:

ჰაკეროზა: აღნიშნული ნიშნავს სხვისი კომპიუტერული უსაფრთხოების მექანიზმის დარღვევას, სხვის კომპიუტერში არსებული პირადი ინფორმაციის ხელმისაწვდომობას. ამერიკის შეერთებულ შტატებში ჰაკეროზა სისხლისსამართლებრივ დანაშაულადაა აღიარებული და ისჯება მისი სიმძიმიდან გამომდინარე. აღნიშნული უნდა განვასხვავოთ ეთიკური

[4] ინფორმაციის წყარო:
http://www.google.ge/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&ved=0CEsQFjAG&url=http%3A%2F%2Fopenjournals.gela.org.ge%2Findex.php%2FGRUNI_D%2Farticle%2Fdownload%2F155%2F189&ei=zrUEU5POD5Kd7gbR8YGgAw&usg=AFQjCNEO8jbkHmYa_sERQmNvCnetlM8cRQ;

ჰაკერობისაგან, რომელსაც ორგანიზაციები იყენებენ მათი ინტერნეტ უსაფრთხოებისათვის.

საქართველოს სისხლის სამართლის კოდექსის 284-ე მუხლის თანახმად, დანაშაულია კომპიუტერულ სისტემაში უნებართვო შეღწევა და იგი ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით იმავე ვადით. თუ ქმედებამ გამოიწვია მნიშვნელოვანი ზიანი ან თუ იგი ჩადენილია წინასწარი შეთანხმებით ჯგუფის მიერ, სამსახურებრივი მდგომარეობის გამოყენებით ან ამგვარი ქმედებისათვის ნასამართლევი პირის მიერ, იგი ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით ვადით ორიდან ხუთ წლამდე.

საქართველოს სისხლის სამართლის კოდექსის 324[1] მუხლის თანახმად, დანაშაულია აგრეთვე კიბერტერორიზმი ესე იგი კანონით დაცული კომპიუტერული ინფორმაციის მართლსაწინააღმდეგო დაუფლება, მისი გამოყენება ან გამოყენების მუქარა, რაც ქმნის მძიმე შედეგის საშიშროებას, ჩადენილი მოსახლეობის დაშინების ან/და ხელისუფლების ორგანოზე ზემოქმედების მიზნით. ეს დანაშაულს ისჯება თავისუფლების აღკვეთით ვადით ათიდან თხუთმეტ წლამდე. თუ იგივე ქმედება გამოიწვევს ადამიანის სიცოცხლის მოსპობას ან სხვა მძიმე შედეგს, იგი ისჯება თავისუფლების აღკვეთით ვადით თორმეტიდან ოც წლამდე ან უვადო თავისუფლების აღკვეთით. ამ მუხლით გათვალისწინებული ქმედებისათვის სისხლისსამართლრივი პასუხისმგებლობა გათვალისწინებულია ასევე იურიდიული პირისათვის და იგი ისჯება ლიკვიდაციით ან საქმიანობის უფლების ჩამორთმევით და ჯარიმით.

კიბერ ქურდობა: აღნიშნული სახეზეა, როდესაც საავტორო უფლების დარღვევით ხდება ინტერნეტიდან სხვადასხვა ინფორმაციის გადმოწერა. უმეტეს შემთხვევაში ვებ-გვერდები თავად სთავაზობენ მომხმარებელს პირატულ მასალას.

საქართველოს სისხლის სამართლის კოდექსში კომპიუტერის საშუალებით საავტორო უფლების დარღვევის სპეციალური მუხლი არ არის გათვალისწინებული. ასეთი დანაშაულის ჩადენის შემთხვევაში პირის ქმედება კვალიფიცირდება ორი მუხლით: საქართველოს სისხლის სამართლის კოდექსის 284-ე (კომპიუტერულ სისტემაში უნებართვო შეღწევა) და 189-ე (საავტორო, მომიჯნავე უფლების მფლობელისა და მონაცემთა ბაზის დამამზადებლის უფლების ხელყოფა) მუხლებით. ეს უკანასკნელი (189-ე მუხლი), საავტორო, მომიჯნავე უფლების მფლობელის ან მონაცემთა ბაზის დამამზადებლის

უფლების ხელყოფა, ისჯება ჯარიმით ან თავისუფლების შეზღუდვით ვადით ორ წლამდე. იგივე ქმედება ჩადენილი განსაკუთრებით დიდი ოდენობით შემოსავლის მიღების მიზნით ან წინასწარი შეთანხმებით ჯგუფის მიერ, ისჯება თავისუფლების შეზღუდვით ვადით სამ წლამდე ან თავისუფლების აღკვეთით იმავე ვადით.

იდენტიფიკაციის ქურდობა: ბოლო რამოდენიმე წლის განმავლობაში სწორედ ასეთი ქმედება წარმოადგენს კიბერ დანაშაულებში მთავარ პრობლემას. დამნაშავე ნახულობს ბაზას პირის საბანკო ანგარიშის, საკრედიტო ინფორმაციის, დაზღვევის და სხვა მნიშვნელოვანი ინფორმაციის შესახებ, ხოლო შემდგომ იყენებს ამ ინფორმაციას მისი ნების გარეშე სხვადასხვა ფულადი ტრანზაქციებისა და საბანკო კრედიტებისათვის. აღნიშნულმა შესაძლოა გამოიწვიოს არა მხოლოდ მნიშვნელოვანი მატერიალური ზიანი, არამედ გააფუჭოს დაზარალებულის საბანკო ისტორიაც.

საქართველოს სისხლის სამართლის კოდექსში იდენტიფიკაციის ქურდობის სპეციალური მუხლი არ არის გათვალისწინებული. ასეთი დანაშაულის ჩადენის შემთხვევაში პირის ქმედება კვალიფიცირდება ორი მუხლით: საქართველოს სისხლის სამართლის კოდექსის 284-ე (კომპიუტერულ სისტემაში უნებართვო შეღწევა) და 177-ე (ქურდობა) მუხლებით. თუ დაუფლებული ქონების ღირებულება/ფულადი თანხის ოდენობა არ აღემატება 150 ლარს ქურდობა ისჯება ჯარიმით ან თავისუფლების შეზღუდვით ვადით ერთიდან სამ წლამდე ანდა თავისუფლების აღკვეთით იმავე ვადით. თუ დაუფლებული ქონების ღირებულება/ფულადი თანხის ოდენობა აღემატება 150 ლარს, მაგრამ არ აღემატება 10 000 ლარს, იგი ისჯება თავისუფლების აღკვეთით ვადით სამიდან ხუთ წლამდე, ხოლო თუ დაუფლებული ქონების ღირებულება/ფულადი თანხის ოდენობა აღემატება 10 000 ლარს ქურდობა ისჯება თავისუფლების აღკვეთით ვადით ექვსიდან ათ წლამდე.

ვირუსული პროგრამები: ეს გულისხმობს სპეციალური პროგრამების შექმნას, რომლებიც მიზნად ისახავს ქსელიდან კომპიუტერის გამოთიშვას. ამგვარი

პროგრამების საშუალებით დამნაშავეს ეძლევა საშუალება უპრობლემოდ ჰქონდეს წვდომა სხვა პირთა პირად ინფორმაციაზე.

საქართველოს სისხლის სამართლის კოდექსის 286-ე მუხლის თანახმად, დანაშაულია კომპიუტერული მონაცემის უნებართვო დაზიანება, წაშლა, შეცვლა ან დაფარვა და ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ან/და თავისუფლების აღკვეთით იმავე ვადით. თუ ქმედებამ გამოიწვია მნიშვნელოვანი ზიანი ან თუ იგი ჩადენილია წინასწარი შეთანხმებით ჯგუფის მიერ, სამსახურებრივი მდგომარეობის გამოყენებით ან ამგვარი ქმედებისათვის ნასამართლევი პირის მიერ ისჯება ისჯება ჯარიმით ან გამასწორებელი სამუშაოთი ვადით ორ წლამდე ანდა თავისუფლების აღკვეთით ვადით სამიდან ხუთ წლამდე.

კიბერ გადაკიდება: კიბერ გადაკიდების დროს დამნაშავის მიზანია მსხვერპლის საჯარო ან პირადი შეურაცხყოფა, რაც დაზარალებულის პირად ცხოვრებაზე ახდენს ძლიერ ფსიქოლოგიურ გავლენას. აღნიშნული ქმედება მას შემდეგ მოექცა ყურადღების ქვეშ, რაც მკვეთრად გაიზარდა ინტერნეტ შეურაცხყოფისა და აბუჩად აგდების საფუძველზე თვითმკვლელობისა შემთხვევები.

კიბერ-გადაკიდებას, როგორც დანაშაულის ცალკე სახეს, არ იცნობს საქართველოს კანონმდებლობა, თუმცა საქართველოს სისხლის სამართლის კოდექსი ითვალისწინებს სისხლისსამართლებრივ პასუხისმგებლობას თვითმკვლელობამდე მიყვანისათვის, რომელიც გამოიწვია მსხვერპლისადმი განხორციელებულმა მუქარამ, მისი პატივის ან ღირსების სისტემატურმა დამცირებამ. ეს დანაშაული ისჯება თავისუფლების შეზღუდვით ვადით სამ წლამდე ან თავისუფლების აღკვეთით ვადით ორიდან ოთხ წლამდე.

ბავშვთა დაყოლიება: დამნაშავეები მოცემულ შემთხვევაში ჩატის და პირადი მიმოწერის საფუძველზე ცდილობენ ბავშვები დაითანხმონ საბავშვო პორნოგრაფიაზე ან სხვა დანაშაულებრივ/ამორალურ საქციელზე.

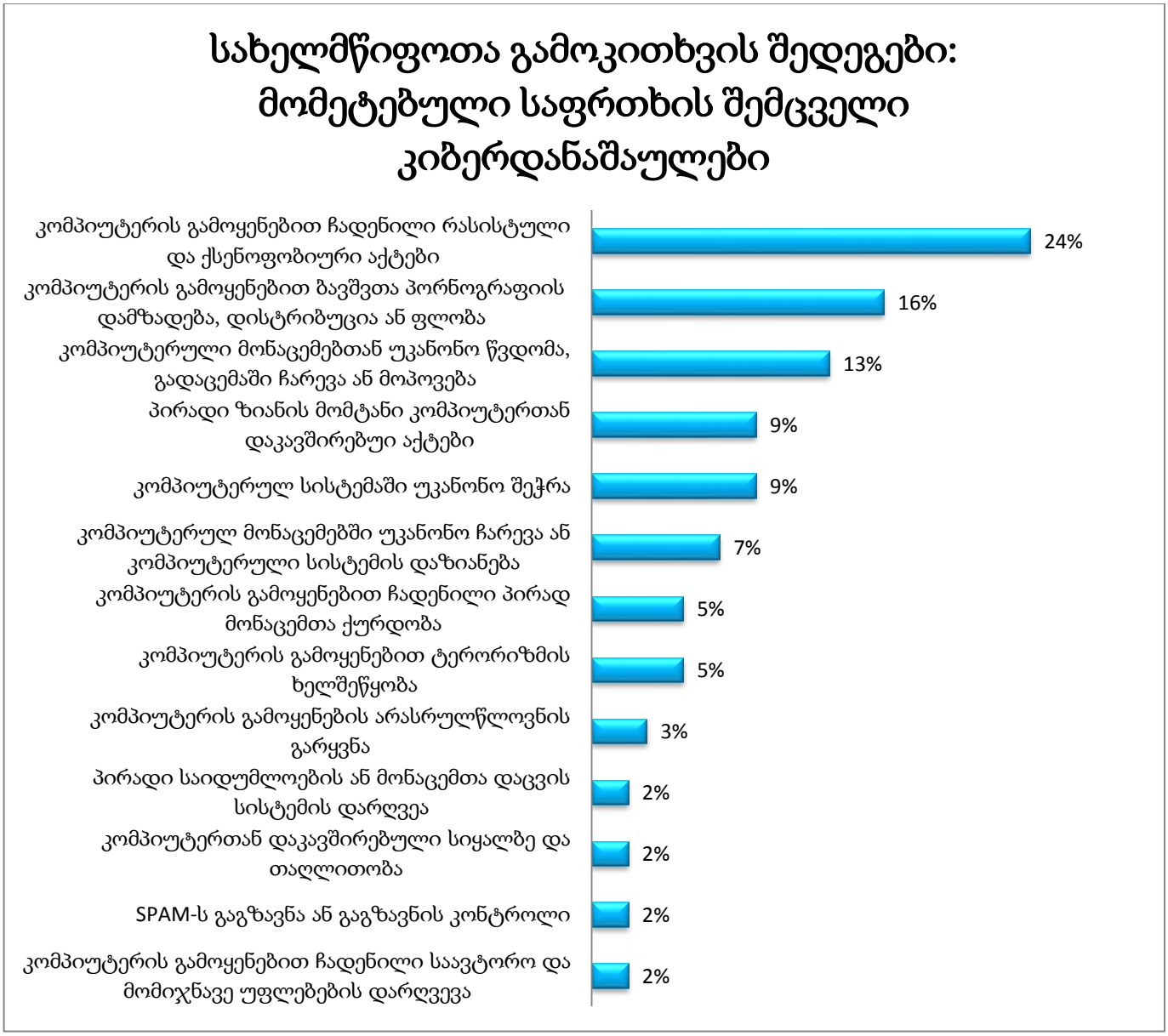
საქართველოს სისხლის სამართლის კოდექსი პირადი მიმოწერის/ჩატის გამოყენებით არასრულწლოვნის პორნოგრაფიაზე დათანხმების სპეციალურ მუხლს არ ითვალისწინებს. ასეთი დანაშაულის ჩადენის შემთხვევაში პირის ქმედება კვალიფიცირდება საქართველოს სისხლის სამართლის კოდექსის 255^1 მუხლით, რომელიც ითვალისწინებს სისხლისსამართლებრივ პასუხისმგებლობას

პორნოგრაფიული ნაწარმოების ან პორნოგრაფიული ხასიათის სხვა საგნის უკანონოდ დამზადებასა და გასაღებაში არასრულწლოვნის ჩაბმისათვის. ეს დანაშაული ისჯება თავისუფლების აღკვეთით ვადით ორიდან ხუთ წლამდე.

იმ შემთხვევაშ თუ ეს გადაბირება მიზნად ისახავს არასრუწლოვნის ექსპლოატაციას, ასეთ შემთხვევასი ქმედება კვალიფიცირდება 143[2] მუხლით - არასრულწლოვნით ვაჭრობა (ტრეფიკინგი), რომლის ყველაზე მსუბუქი შემთხვევა ისჯება თავისუფლების აღკვეთით ვადით რვიდან თორმეტ წლამდე, ხოლო დამამძიმებელ გარემოებებში ჩადენის შემთხვევაში სასჯელად გათვალისწინებულია თავისუფლების აღკვეთა ოც წლამდე ან უვადო თავისუფლების აღკვეთა.

გაეროს მონაცემები კიბერდანაშაულთან დაკავშირებით

გაეროს მონაცემების თანახმად, ეკონომიკური მოგების მიზნით ჩადენილ კომპიუტერულ დანაშაულთა რიცხვი (კომპიუტერული სიყალბე, კომპიუტერული თაღლითობა) მსოფლიოს თითქმის ყველა რეგიონში კიბერდანაშაულთა საერთო რაოდენობის ერთ მესამედს შეადგენს. ქვეყნების გარკვეული ნაწილის ანგარიშებში ჭარბობს ისეთი დანაშაულები, როგორებიცაა: „თაღლითობა ელექტრონულ ვაჭრობასა და გადახდების დარგში“, „თაღლითობა ინტერნეტ აუქციონებზე - როგორებიცაა ebay“, „ფინანსური და პერსონალური ინფორმაციის წინააღმდეგ ჩადენილი კიბერდანაშაული“, „თაღლითობის სქემა ელექტრონული ფოსტისა და სოციალური ვებ-გვერდების მეშვეობით“.



ევროსაბჭოს აქტივობა კიბერდანაშაულის სფეროში

ევროსაბჭოს მიერ, კანადისა და იაპონიის აქტიური მონაწილეობით, 2001 წელს შემუშავებულ იქნა კონვენცია კიბერდანაშაულის შესახებ. ხსენებული კონვენცია ძალაში შევიდა 2004 წელს, ხოლო საქართველომ მისი რატიფიცირება მოახდინა 2012 წელს. კიბერდანაშაულის შესახებ ევროსაბჭოს კონვენცია (ე.წ. ბუდაპეშტის კონვენცია) ერთადერთი შესასრულებლად სავალდებულო დოკუმენტია აღნიშნულ საკითხთან დაკავშირებით. იმის მიუხედავად, რომ კონვენცია მიიღეს ევროსაბჭოს ეგიდით, შესაძლებელი იყო მას შეერთებოდნენ არაევროპული

ქვეყნებიც. ხსენებული დოკუმენტი წევრი სახელმწიფოებისთვის სახელმძღვანელო პრინციპების ერთობლიობას წარმოადგენს და მიზნად ისახავს ეროვნულ დონეზე ყოვლისმომცველი საკანონმდებლო ბაზის შექმნასა და საერთაშორისო თანამშრომლობის გაძლიერებას. კონვენციის დამატებითი პროტოკოლი ეხება ქსენოფობიისა და რასიზმის გამოვლენას კომპიუტერული სისტემის გამოყენებით.[5]

აღნიშნული კონვენცია კიბერდანაშაულის სხვადასხვა სახეებს უსვამს ხაზს. მათ შორისაა:

კიბერდანაშაულის ტიპი ბუდაპეშტის კონვენციის მიხედვით	*კონკრეტული კიბერდანაშაული*
კომპიუტერული მონაცემებისა და სისტემების კონფიდენციალობისა და მთლიანობის წინააღმდეგ მიმართული დანაშაულები	კომპიუტერულ სისტემაში უნებართვო შეღწევა
	ტექნიკური ღონისძიებების გამოყენებით კომპიუტერული მონაცემების არასაჯარო გზით გადაცემის პროცესში უკანონო ჩარევა (interception)
	სხვისი კომპიუტერული მონაცემების დაზიანება, განადგურება, წაშლა, შეცვლა და ჩახშობა

[5] ე.წ. internet bullying;

		კომპიუტერული მონაცემების დაზიანების, განადგურების, წაშლის, შეცვლისა და ჩახშობის გზით კომპიუტერის სისტემის გამართული მუშაობისათვის უკანონოდ ხელის შეშლა
		კომპიუტერულ სისტემაში ან მონაცემებში უკანონო წვდომის მოპოვების მიზნით, მოწყობილობის, მათ შორის, კომპიუტერული პროგრამის, პაროლის, სხვა მონაცემის წარმოება, გაყიდვა, უკანონოდ და განზრახ შეძენა, იმპორტი, დისტრიბუცია ან სხვაგვარად ხელმისაწვდომად გახდა
კომპიუტერთან დანაშაულები	**დაკავშირებული**	კომპიუტერული სიყალბე - კომპიუტერული მონაცემების განზრახ და უკანონოდ შეცვლა, წაშლა ან სხვა ქმედების განხორციელება არაავთენტური მონაცემების ავთენტურ მონაცემებად გასაღების მიზნით

	კომპიუტერული თაღლითობა - თაღლითობის გზით კომპიუტერული მონაცემების განზრახ და უკანონოდ შეცვლა, წაშლა ან სხვა ქმედების განხორციელება არაავთენტური მონაცემების ავთენტურ მონაცემებად გასასაღებლად ეკონომიკური მოგების მიღების მიზნით
ქონთენთთან დაკავშირებული დანაშაულები	ბავშვთა პორნოგრაფიასთან დაკავშირებული დანაშაულები
საავტორო და მომიჯნავე უფლებებთან დაკავშირებით ჩადენილი დანაშაულები	საავტორო და მომიჯნავე უფლებებთან დაკავშირებული კიბერდანაშაულები

კიბერდანაშაულის მზარდი სტატისტიკა ძირითადად განპირობებულია კიბერ საკითხებზე საზოგადოების დაბალი ცნობიერებით. კიბერ დამნაშავეები ძირითადად იყენებენ ფიშინგის, სპამის მეთოდებსა და სხვადასხვა მავნე პროგრამებს.

საქართველოს შინაგან საქმეთა სამინისტროს აქტივობა კიბერდანაშაულთან ბრძოლის სფეროში

აღნიშნულთან საბრძოლველად საქართველოს შინაგან საქმეთა სამინისტროს მიერ გაწეული საქმიანობის შედეგად შემუშავებულ იქნა პროექტი. კერძოდ, კიბერსივრცეში ჩადენილი მართლსაწინააღმდეგო ქმედებების გამოვლენის, აღკვეთისა და პრევენციის უზრუნველსაყოფად, 2012 წლის დეკემბერში შინაგან საქმეთა სამინისტროს ცენტრალური კრიმინალური პოლიციის დეპარტამენტში შეიქმნა კიბერდანაშაულთან ბრძოლის სამმართველო. ამასთან, შსს საექსპერტო–კრიმინალისტიკური მთავარი სამმართველოს შემადგენლობაში ჩამოყალიბდა

კომპიუტერულ–ციფრული ექსპერტიზის ქვეგანყოფილება, რომელიც ახორციელებს უშუალოდ ციფრული მტკიცებულებების პირველად მოპყრობასა და მათ შემდგომ ექსპერტიზას.

შინაგან საქმეთა სამინისტროს ორგანიზებული დანაშაულის სტრატეგიაში ცალკე თავად არის წარმოდგენილი კიბერ დანაშაულის წინააღმდეგ ბრძოლის საკითხები.

გარდა ამისა, შემუშავდა სტანდარტული ოპერაციული პროცედურები ციფრული მტკიცებულებების პირველადი მოპყრობის შესახებ.[6]

კიბერდანაშაულის კონვენციასთან ქართული კანონმდებლობის ჰარმონიზაციის უზრუნველსაყოფად ევროპის საბჭოსა და ევროპული კომისიის ერთობლივი პროექტის ფარგლებში ცვლილებები შევიდა სისხლის სამართლის კოდექსში, სისხლის სამართლის საპროცესო კოდექსში, „ოპერატიული–სამძებრო საქმიანობის შესახებ“ და „ელექტრონული კომუნიკაციების შესახებ“ კანონებში.[7]

კიბერდანაშაულის გავრცელებული სახეები და მათი პრევენცია

პრევენციულ ღონისძიებებზე საუბრისას აუცილებელია განვიხილოთ აქტივობები, რომლებიც განსაკუთრებული საფრთხის შემცველია. ესენია:

1. ინტერნეტ თაღლითობა;
2. ბავშვების პორნოგრაფია, მათი სქესობრივი დევნა და/ან დაყოლიება სქესობრივ კავშირზე ინტერნეტის გამოყენებით;
3. ინტერნეტ დაშინება (ბულინგი) - ინტერნეტის საშუალებით კონკრეტულ პირთა წინაღმდეგ დამაშინებელი, შეურაცხმყოფელი და/ან დამამცირებელი ინფორმაციის გავრცელება/კომენტარების ან სურათების გამოქვეყნება;

[6] ინფორმაციის წყარო: http://police.ge/ge/projects/kiberdanashauli/shinagan-saqmeta-saministros-mier-gankhortsielebuli-ghonisdziebebi;
[7] ინფორმაციის წყარო: http://police.ge/ge/projects/kiberdanashauli/saertashoriso-tanamshromloba-kiber-danashaultan-brdzolashi

4. მოგების მიღების და/ან სხვა მიზნით ინტერნეტის მეშვეობით პირადი მონაცემების (საბანკო ანგარიშის მონაცემები, სატელეფონო მონაცემები, პირადობის მოწმობის მონაცემები) ქურდობა;

აღნიშნული დანაშაულებისაგან თავის დასაცავად კონკრეტულმა პირებმა მიმართეთ შემდეგ ღონისძიებებს:

- ყოველთვის განაახლეთ თქვენი კომპიუტერი უახლესი პროგრამების მიხედვით - ეცადეთ „დააფდეითოთ“ თქვენი იგი. აღნიშნული ქმედებით, თქვენ ხელს შეუშლით დამნაშავეს ისარგებლოს პროგრამის სისუსტეებითა და სიძველით. თუმცა ეს იმას არ ნიშნავს, რომ თქვენ გექნებათ აბსოლუტური დაცვა ჰაკერებისაგან, აღნიშნული მხოლოდ ართულებს მათ საქმეს და შესაძლოა თავიდან აიცილოთ ნაკლებად გამოცდილი დამნაშავის მცდელობა;

- დარწმუნდით, რომ კომპიუტერი სწორად არის კონფიგურირებული - ახლად შეძენილ კომპიუტერებს შესაძლოა არ ჰქონდეთ გააქტიურებული დაცვის პროგრამა, რაც დამნაშავის სასარგებლოდ იმუშავებს. ახალი კომპიუტერის დაყენებისას დარწმუნდით, რომ იგი არა მხოლოდ მუშაობს, არამედ მუშაობს დაცულ რეჟიმში. განსაკუთრებით საშიში და ადვილად შეღწევადი იქნება კომპიუტერი, თუკი მასში არალიცენზირებული პროგრამებია ჩატვირთული;

- აირჩიეთ ძლიერი კოდი და არ გამოააშკარაოთ იგი - პაროლები ინტერნეტ სარგებლობის განუყოფელ ნაწილს წარმოადგენს, ინტერნეტ შესყიდვები და ინტერნეტ ბანკინგი შეუძლებელია მის გარეშე. სწორედ ამიტომ უზრუნველყავით მტკიცე და რთული კოდის დაყენება, რომელიც მხოლოდ თქვენ გეცოდინებათ;

- დაიცავით თქვენი კომპიუტერი სპეციალური ანტი-ვირუსული პროგრამებით. პირველადი დამცავი მექანიზმი არის თქვენი კომპიუტერის „ფაიერვოლი“. სწორედ იგი უზრუნველყოფს შემავალი და გამავალი

ინფორმაციის კონტროლს, ასევე იგი უზრუნველყოფს ცუდი ვებ-გვერდებიდან და კავშირებიდან დაბლოკვას. დამატებით საჭიროა სპეციალური ანტი-ვირუსული პროგრამის დაინსტალება კომპიუტერში, მაგრამ გახსოვდეთ, რომ პროგრამის ვერსია აუცილებლად უნდა იყოს ლიცენზირებული;

- დაიცავით თქვენი პერსონალური ინფორმაცია - გამოიჩინეთ მომეტებული ყურადღება, როდესაც აზიარებთ თქვენს პირად მონაცემებს. იმისათვის, რომ მიიღოთ სხვადასხვა ონლაინ მომსახურება, თქვენ მოგეთხოვებათ პერსონალური ინფორმაციის მიწოდება. გაითვალისწინეთ, რომ ბევრი მომწოდებელი არის თაღლითი და ინფორმაციას ბოროტად გამოიყენებს:
  - დააკვირდით მეილის შემადგენლობას - როგორც წესი, დავირუსებული ან სხვა თაღლითური მეილები შედგენილია უბრალო და გაუმართავი ენით, ისინი შეიცავენ ზოგად და არაფრისმთქმელ ინფორმაციას;
  - თუ არ ხართ წყაროში დარწმუნებული ნუ უპასუხებთ ისეთ მეილს, რომელიც ითხოვს თქვენს პერსონალურ ინფორმაციას;
  - ყოველთვის ეცადეთ, რომ მეილში მითითებული ვებ-მისამართები ჩააკოპიროთ სპეციალური ბრაუზერის URL საძიებო სისტემაში ვიდრე შეხვალთ მასში უბრალოდ დაკლიკებით მეილის მეშვეობით. აღნიშნული უადვილებს დამნაშავეს თქვენს კომპიუტერში შეღწევას;
  - ყურადღებით წაიკითხეთ პირადი ინფორმაციის გამოყენების პირობები ვებ-გვერდებსა და სხვა აპლიკაციებში;
- ონლაინ შემოთავაზებები - ეცადეთ არ აყვეთ ემოციებს და არ მიიღოთ არარეალურად მომგებიანი შემოთავაზებები უცხო პირებისგან;
- რეგულარულად შეამოწმეთ საკრედიტო ბარათისა და ინტერნეტ ბანკინგის პირადი მონაცემები. აღნიშნული მოგცემთ საშუალებას დაბლოკოთ თქვენი ანგარიში ოდნავი ეჭვის შემთხვევაშიც;

- ყურადღება მიაქციეთ ბავშვებს ინტერნეტში ყოფნისას, თვალყური ადევნეთ ვებ-გვერდებს, რომელეთაც ისინი ხშირად სტუმრობენ. აკონტროლეთ უცხო პირთა მიერ მათთან სოციალური ქსელების ან ელექტრონული ფოსტის მეშვეობით დაკავშირების მცდელობები.