ვლადიმერ ნაფეტვარიძე*

კიბერ-დანაშაულების მეთოდების ზეგავლენა თანამედროვე სამყაროზე

აბსტრაქტი

21-ე საუკუნე სამართლიანად ითვლება ინფორმაციული ტექნოლოგიების ერად. მიუხედავად იმისა, რომ ინტერნეტიზაციის პროცესი გლობალური მასშტაბით სულ რაღაც სამი ათეული წელიწადია მიმდინარეობს, შესაძლებელია ითქვას, რომ ციფრულმა ტექნოლოგიებმა ადამიანური ცხოვრების ყველა სფერო რადიკალურად შეცვალა. სამყარო ყოველდღიურად სულ უფრო დამოკიდებული ხდება თანამედროვე ტექნოლოგებზე.

მიუხედავად იმისა, რომ ინტერნეტი 21-ე საუკუნის უმთავრესი მონაპოვარია, არ შეიძლება მისი თანმდევი საფრთხეების უგულვებელყოფა. ინტერნეტის განვითარებამ გააჩინა ახალი კიბერ განზომილებები და შესაბამისად კიბერ საფრთხეები. ციფრულმა სამყარომ შესაძლებლობათა ფართო ასპარეზი მისცა ყველას, მათ შორის კიბერ დამნაშავეებსაც, რომლებიც ცდილობენ თანამედროვე ტექნოლოგიების გამოყენებით, ზიანი მიაყენონ მოქალაქეებს, თუ სახელმწიფო ინსტიტუციებს.

მოცემული ნაშრომის მიზანი, არის იმ კიბერ დანაშაულების მეთოდების გამოვლენა, რომელიც თანამედროვე სამყაროში საფრთხეს უქმნის, როგორც ინდივიდებს, ასევე სახელმწიფოებს. თითოეული მათგანის განხილვა და კიბერ უსაფრთხოების პერსპექტივიდან ქართული რეალობის შეფასება.

საკვანძო სიტყვები: საქართველო; კიბერუსაფრთხოება; კიბერ კრიმინალი.

ინტერნეტის განვითარებამ მსოფლიოს უდიდესი პროგრესი მოუტანა, თუმცა არსებობს უარყოფითი მხარეებიც, რომელიც თანამედროვე ტექნოლოგიების დახვეწასთან ერთად სულ უფრო აქტუალური ხდება. მათ შორის არის კიბერდანაშაულიც. აღნიშნული ფენომენი მსოფლიოსთვის დიდ საფრთხეს წარმოადგენს, მის წინააღმდეგ საბრ-

* პოლიტიკის მეცნიერებათა დოქტორი, ილიას სახელმწიფო უნივერსიტეტის პოლიტოლოგიის ინსტიტუტის ასისტენტ-მკვლევარი

ძოლველად აუცილებელია თანამშრომლობა სხვადასხვა ქვეყნებსა და საერთაშორისო ორგანიზაციებს შორის. 2010 წლის გაეროს ასამბლეაზე კიბერდანაშაულის წინააღმდეგ ბრძოლა ერთ-ერთ მთავარ პრიორიტეტად გამოცხადდა. სახელმწიფოებში, სადაც განვითარებულია ელექტრონული მმართველობა და საზოგადოების უდიდესი ნაწილი სარგებლობს ონლაინ სერვისებით, კიბერ დანაშაული სერიოზულ პრობლემას წარმოადგენს.

ქვეყნაში ინფორმაციულ-კომუნიკაციური ტექნოლოგიების (ICT) დანერგვისა და განვითარებისთვის კიბერუსაფრთხოება მნიშვნელოვან როლს თამაშობს. აუცილებელია პარალელურ რეჟიმში ხდებოდეს ინტერნეტის უსაფრთხოებაზე მუშაობა, რადგან ყოველი ახალი ინოვაცია, ახალი საშუალებაა კიბერ–დამნაშავეებისთვის ინტერნეტ ქსელი არაკეთილსინდისიერად გამოიყენონ.

არსებობს კიბერდანაშაულის სხვადასხვა სახე, მათ შორის ყველაზე დიდი ხნის ისტორია გააჩნია არალეგალურ შეღწევას, ე.წ „ჰაკერობას“. ეს მოვლენა წარმოადგენს კომპიუტერის სისტემაში არალეგალურად შესვლას. ინტერნეტის განვითარებასთან ერთად, გაიზარდა აღნიშნული კიბერდანაშაულის მასშტაბები. თანამედროვე ჰაკერების ყველაზე პოპულარული სამიზნე არის -“Nasa”, ამერიკის საჰაერო ძალები, პენტაგონი, Yahoo, Google.

არსებობს კიბერდანაშაულის განხორციელების სხვადასხვა მეთოდი:

- კონკრეტული პირის თუ მთლიანი საიტის პაროლის გატეხვა;

- კომპიუტერის პროგრამული ან სისტემური დაზიანება;

- ჰაკერული საიტების დამზადება (საიტის ჩანაცვლება ყალბი საიტით, რომელიც გავს ორიგინალს, მომხმარებელი მსგავსი საიტით სარგებლობისას, მთელ პირად ინფორმაციას გადაცემს კიბერ–დამნაშავეებს);

- „key logging” პროგრამა. რომელიც კლავიატურაზე აკრეფილ ნებისმიერ სიტყვას გადასცემს ჰაკერს.

ინტერნეტ დანაშაულის ჩადენის მოტივები სხვადასხვა შეიძლება იყოს:

- ზოგიერთი ჰაკერი უბრალოდ ერთობა სხვისი კომპიუტერის გატეხვით და ამით უმტკიცებს სხვა კიბერდამნაშავეებს თავის სიძლიერეს.

- პოლიტიკური მოტივები: ბევრი პოლიტიკოსის კომპიუტერში შესაძლოა აღმოჩნდეს მისი მაკომპრომიტირებელი მასალა, რასაც შეუძლია მისი კარიერის დანგრევა;

- მატერიალური მოტივები. მოპოვებული მასალის შედეგად მარტივია ადამიანის დაშანტაჟება და ფულის გამოძალვა;

- შპიონაჟი- საიდუმლო მასალების მოპოვება მათი სხვა ქვეყნისთვის გადაცემის მიზნით.

არსებობს სპეციალური პროგრამები, რომლის მეშვეობითაც შესაძლებელია განხორციელდეს კიბერდანაშაულები, ზოგი მათგანი უფასოდ მოიპოვება ინტერნეტში, ზოგი კი ათასობით დოლარი ღირს, ეს დამოკიდებულია მის მნიშვნელობასა და ხარისხზე;

ჰაკერები იყენებენ პროგრამა "Botnet"_ს , რომლის მეშვეობით მათ წვდომა აქვთ ერთდროულად უამრავ კომპიუტერთან, გაშვებული პროგრამა თავად პოულობს დაუცველ კომპიუტერებს და მის გამომყენებელს საშუალებას აძლევს იმოქმედოს საკუთარი სურვილის მიხედვით, გადმოიტანოს თუ უბრალოდ გაანადგუროს მსხვერპლ კომპიუტერებში არსებული მონაცემები;

გაცილებით მარტივი არის კერძო პირის კომპიუტერის გატეხვა, ვიდრე ოფიციალური სტრუქტურის, რადგან, ხშირ შემთხვევაში, მათ არ უყენიათ ოფიციალური პროგრამები და, შესაბამისად, დაცვის სისტემა ადვილად ხელმისაწვდომი ხდება, ხოლო ორგანიზაციების უმრავლესობას, გარდა იმისა, რომ უყენიათ ლიცენზირებული პროგრამები, ხშირად ჰყავთ საკუთარი "IT"- თანამშრომლები, რომლებიც ზრუნავენ ქსელსა და კომპიუტერულ ტექნიკაზე.

კომპიუტერის სისტემაში უკანონოდ შესვლა იგივე დონის დანაშაულია, როგორც კერძო პირის საცხოვრებელ სახლში შეღწევა. აუცილებელია არსებობდეს საკანონმდებლო ბაზა, რომელზე დაყრდნობითაც შესაბამის უწყებებს საშუალება ექნებათ ადეკვატური რეაგირება მოახდინონ.

არსებობს რამდენიმე მეთოდი, რომელსაც იყენებენ კიბერდამნაშავეები მონაცემთა მოსაპარად. ყველაზე მარტივია დაუცველი კომპიუტერის გატეხვა და იქიდან ნებისმიერი სახის მონაცემის თუ მასალის გადმოტანა, გარდა ამისა, შესაძლებელია დაცულ კომპიუტერშიც შეღწევა სპეციალური ჰაკერული პროგრამების მეშვეობით, ხოლო ხერხი, რომლითაც მომხმარებელი თავად უწყობს საკუთარი კომპიუტერის გატეხვას ხელს, ყველაზე კრეატიული და ეფექტურია. ამ მეთოდს-სოცი-

ალურ ინჟინერიას უწოდებენ, აქაც არსებობს რამდენიმე განსხვავებული გზა, რომლის მეშვეობით მომხმარებელი საკუთარ კომპიუტერს ხელმისაწვდომს ხდის კიბერდამნაშავეებისთვის; მათ შორის ყველაზე ცნობილი და ხშირად გამოყენებადი მეთოდია "Pishing", - აღნიშნული მეთოდის გამოყენებით, პიროვნება ელექტრონულ ფოსტაზე იღებს წერილს, სადაც მითითებულია მისი ბანკის მისამართი, იმისთვის, რომ მსხვერპლს ეჭვი ნაკლებად გაუჩნდეს მოსული გზავნილის ჭეშმარიტებაში, მისამართი საიდანაც გზავნიან მას, ძალიან ჰგავს ორიგინალის დასახელებას. იმ შემთხვევაში თუ მომხმარებელი ყურადღებით არ დააკვირდება წერილის ავტორს, ვერც შეამჩნევს, რომ რეალურად ორიგინალი მისამართისგან მხოლოდ ერთი ასოა განსხვავება, თუმცა სულ სხვა ორგანიზაციის საიტზე გადავა, რომელიც დიზაინით მსგავსი იქნება ორიგინალის, იმ შემთხვევაში კი თუ იგი შეიყვანს საიდენტიფიკაციო კოდს და პაროლს ცრუ-საიტზე, გახდება სოციალური ინჟინერიის მსხვერპლი და მისი საბანკო ანგარიშის პაროლები ცნობილი გახდება ჰაკერებისთვის.

არსებობს მეთოდი Pretexting, რომელიც ძირითადად ტელეფონის გამოყენებით ხორციელდება, ამ შემთხვევაში დამნაშავეები რეკავენ მსხვერპლთან სადაზღვევო აგენტის, თუ ბანკის თანამშრომლის სახელით და სხვადასხვა მიზეზების მოყვანით, სთხოვენ დაასახელონ საკუთარი საიდენტიფიკაციო კოდი და პაროლი, რის შემდეგაც მათი საბანკო ანგარიშის გატეხვა მხოლოდ დროის საკითხია;

Gimmers - არიან ადამიანები, რომლებიც ავრცელებენ Trojan ვირუსებს და მათი საშუალებით აკონტროლებენ კომპიუტერებს, თუმცა გავრცელების რამდენიმე მეთოდი გააჩნიათ, მაგალითად გავრცელებული ხერხი იყო კომპაქტ-დისკზე გარედან ცნობილი მომღერლის სურათის დახატვა და მისი დატოვება საზოგადოებრივ ადგილებში, მხვერპლს ჰგონია, რომ იპოვა ღირებული სიმღერების კრებული და დაუფიქრებლად მიაქვს სახლში და აინსტალირებს კომპიუტერში, რითაც იგი ღირებული სიმღერების, თუ პროგრამების ნაცვლად, იღებს Trojan ვირუსს. ისინი ასევე იყენებენ ინტერნეტს აღნიშნული ვირუსის გასავრცელებლად, სხვადასხვა ინტერნეტ საიტებს, სადაც მომხმარებელს სთავაზობენ საინტერესო პროგრამების, კინოების, თუ თამაშების გადმოწერას, რომელთა დაინსტალირების შემდგომ ხდებიან ვირუსის მსხვერპლები.

კიბერდანაშაულის წინააღმდეგ ბრძოლის ერთ-ერთი მეთოდია მოსახლეობის ცნობიერების დონის ამაღლება, იმ შემთხვევაში, თუ ინტერნეტ საზოგადოებას ეცოდინება, თუ რა მეთოდები არსებობს, კიბერდამნაშავეთა ხელში, გაცილებით რთული გახდება მათი შეცდომაში შეყვანა და კომპიუტერის თუ სისტემის გატეხვა სხვადასხვა მიზნებისთვის. გამომდინარე იქიდან, რომ ბიზნეს ორგანიზაციების კომპიუტერული სისტემის გატეხვა რთულია ხოლო კერძო პირისა ბევრად მარტივი, ჰაკერები, ხშირ შემთხვევაში ამჯობინებენ ინდივიდუალური მომხმარებლების სისტემის სხვადასხვა პროგრამებით გატეხვას, ვიდრე ორგანიზაციებისას.

უკანონო ინტერაქცია - ამ მეთოდის გამოყენებით, ჰაკერს შეუძლია ჩაერთოს მომხმარებლის ინტერნეტ ქსელში, არსებობს სხვადასხვა საშუალებები ამის განსახორციელებლად; მაგალითად WiFi-ის გამოყენებით. საზოგადოებრივ ადგილებში არსებული უსადენო ინტერნეტი, სადაც ნებისმიერ მსურველს შეუძლია შესვლა, წარმოადგენს საფრთხეს, რადგან ზოგიერთი მათგანი არ არის დაცული და შესაბამისი პროგრამული აღჭურვილობის არსებობის შემთხვევაში, აღნიშნული საერთო ქსელის გამოყენებით შესაძლებელი გახდება მასში ჩართული ყველა კომპიუტერის სისტემაში შეღწევა.

მონაცემთა დაზიანება - არსებობს კიბერდანაშაული, რომლის მიხედვით ჰაკერი, არათუ იპარავს ინფორმაციას, არამედ აზიანებს ან შლის მას. ძირითადად ასეთი თავდასხმის მსხვერპლი ხდებიან ორგანიზაციები და სახელმწიფო სტრუქტურები, თუმცა ასეთი დანაშაულის ჩადენის მოტივაცია, პირად ინტერესებზე მაღლა დგას, ამ შემთხვევაში საქმეში ერევიან სხვადასხვა აქტორები, რომელთა ინტერესს წარმოადგენს მოახდინოს დესტაბილიზაცია, მაგალითად თუ მოხდება სატრანსპორტო, თუ კომუნალურ სისტემაზე თავდასხმა, ეს იქნება სახელმწიფოს წინააღმდეგ მიმართული ქმედება, რამაც შესაძლებელია მძიმე შედეგები მოიტანოს. 2000 წელს გავრცელდა ვირუსი სახელწოდებით “The Computer Worm", რომელმაც გააქტიურებიდან 10 წუთში დააზიანა 70 ათასი კომპიუტერი, რაც იმ პერიოდისთვის არსებული კომპიუტერების რაოდენობასთან მიმართებაში საკმაოდ დიდ პროცენტს წარმოადგენდა.

სისტემის დაზიანება - ეს არის კიბერდანაშაულის ერთ-ერთი სახეობა, რომელიც მიზნად ისახავს არათუ მონაცემის ან სხვადასხვა ფაილების დაზიანებას, არამედ მთლიანი კომპიუტერის მწყობრიდან გა-

მოყვანას, რაც თავისთავად იწვევს იმ სისტემის დაზიანებას, რომელშიც აღნიშნული მოწყობილობაა ჩართული, გამომდინარე იქიდან, რომ დიდი მნიშვნელობის დაწესებულებების წინააღმდეგ ხდება მსგავსი თავდასხმების განხორციელება, მათი უმრავლესობა წარუმატებლად სრულდება. სახელმწიფო მნიშვნელობის მქონე კომპიუტერების დაცვის მექანიზმი საკმაოდ ძლიერი და რთულად შესაღწევია, გარდა ამისა, არსებობს საფრთხე კიბერდამნაშავეებისთვის, რომ მათ წინააღმდეგ განხროციელდება სერიოზული საგამოძიებო სამუშაოები, რადგან სამართლებრივად დიდი განსხვავებაა კერძო პირის კომპიუტერის გატეხვასა და სახელწმიფო დაწესებულებების კომპიუტერული ინფრასტრუქტურის დაზიანებას შორის;

მოცემული ტექნიკები და მეთოდები, კიბერდამნაშავეებს აძლევს საშუალებას შეაღწიონ დაუცველ კომპიუტერულ ქსელში და დააზიანონ, მიითვისონ, ან წაშალონ მონაცემები. ელექტრონული მმართველობის განვითარებისთვის, ერთ–ერთ უმნიშვნელოვანეს ფაქტორს წარმოადგენს საზოგადოების დამოკიდებულება ონლაინ სისტემის მიმართ, რადგან იმ შემთხვევაში თუ მოქალაქეებს არ ექნებათ შეგრძნება, რომ მათი ელექტრონული ოპერაციები დაცულია და არავის მიუწვდება ხელი, ნდობა ონლაინ სერვისებისადმი და შესაბამისად, ელექტრონული მმართველობისადმი საგრძნობლად შემცირდება. მოქალაქეები მთავარი წყაროა ელექტრონული ხელისუფლების მუშაობისთვის, რადგან ცალმხრივად შეუძლებელია განხორციელდეს ციფრული მმართველობა. გამომდინარე აქედან, უმნიშვნელოვანესია სახელმწიფომ იზრუნოს ელექტრონული ბაზების დაცვაზე და ბრძოლა გამოუცხადოს კიბერ–დანაშაულს, რადგან 21 –ე საუკუნეში, სადაც მოქალაქეთა უდიდესი ნაწილი სულ უფრო დამოკიდებული ხდება ინტერნეტ სივრცეზე, კიბერ დანაშაული დიდ საფრთხეს წარმოადგენს, როგორც კონკრეტული ინდივიდებისთვის, ასევე სახელმწიფოებისთვისაც. მსოფლიოს ბევრ ქვეყანას გააჩნია სპეციალური სტრატეგია ამ პრობლემის წინააღმდეგ საბრძოლველად. არსებობს საკანონმდებლო ბაზები, რომლის მიხედვით ინტერნეტში განხორციელებული დანაშაული, ისეთივე კრიმინალად ითვლება, როგორ რეალურ ცხოვრებაში ჩადენილი მსგავსი ფაქტი. შესაბამისად არსებობენ სტრუქტურები, რომელთაც ევალებათ აღკვეთონ კანონის დარღვევის ფაქტები ინტერნეტში. საქართველოშიც არსებობს საკანონმდებლო ბაზა, რომელიც განსაზღვრავს ელექტრონულ სივრცეში მიმდინარე პროცესების კანონიერებას, თუ უკანონობას.

21-ე საუკუნეში კიბერ კრიმინალთან ბრძოლა სამყაროს ერთ-ერთ უმნიშვნელოვანეს გამოწვევად იქცა. კიბერ კრიმინალება სააფრთხეს წარმოადგენენ არამხოლოდ ინდივიდუალური მოქალაქეებისთვის, არამედ სახელმწიფოებრივ დონეზეც კი. არსებობს მთელი რიგი მეთოდები, რომლის გამოყენებითაც შესაძლებელია ქვეყნის კიბერ სივრცეს სერიოზული ზიანი მიადგეს. საქართველო ერთ-ერთი პირველი სახელმწიფოთაგანია, რომელმაც საკუთარ თავზე გამოსცადა სახელმწიფო მასშტაბის კიბერ შეტევა.

2008 წელს საქართველოს წინააღმდეგ კიბერ შეტევის არაერთგვაროვანი მეთოდები იქნა გამოყენებული. DDOS-ს შეტევების შედეგად, ქართული ვებ გვერდები დატვირთვას ვერ უძლებდნენ და სერვერი ითიშებოდა. DDOS-ს შეტევის დროს, ჰაკერები სხვადასხვა მეთოდით ამისამართებენ ასეულობით, ზოგჯერ კი ათასეულობით მომხმარებელს კონკრეტულ ვებ-გვერდებზე, რის შედეგადაც საიტის სერვერი გამოდის მწყობრიდან. 2008 წელს მსგავსი მეთოდის გამოყენების შედეგად, 300-400 უნიკალური ვიზიტორი ერთდროულად სტუმრობდა ქართულ ვებ-გვერდებს რამაც გამოიწვია სერვერების გათიშვა და მწყობრიდან გამოსვლა.

DDOS შეტევის გარდა, ჰაკერების მხრიდან ხდებოდა ე.წ. SQL INJECTION-ის მეთოდის გამოყენება, ეს არის ვებ-გვერდების სკანირების მეთოდი, რომლის შედეგადაც გამოვლინდება საიტის სუსტი წერტილი. ამ ინფორმაციის მიღების შემდგომ კი ჰაკერები მარტივად ახერხებდნენ სისტემაში შეღწევას. ფაქტი, რომ დაახლოებით 100 ქართული ვებ-გვერდი ამ მეთოდით იქნა გატეხილი, მიუთითებს იმაზე, რომ ბოროტმოქმედებმა რამდენიმე თვით ადრე დაიწყეს ამ ოპერაციისთვის მზადება და ზუსტად იმ დროს განახორციელეს, როცა რუსეთის ფედერაცია მიმართავდა აგრესიულ სამხედრო ინტერვენციას.

აღნიშნული მეთოდების გარდა, ჰაკერები იყენებდნენ ე.წ. BGP hijacking და ცდილობდნენ ეკონტროლებინათ ქართული IP მისამართები. ეს იყო მსოფლიოში პირველი შემთხვევა, როდესაც ფართომასშტაბიან საომარ ქმედებებს თან ახლდა ფართომაშტაბიანი კიბერ თავდასხმები. 2008 წელს საქართველოში არ ხორციელდებოდა ელექტრონული მმართველობის დანერგვის სახელმწიფო პოლიტიკა. არსებობდა ცალკეული ინიციატივები გარკვეული სამინისტროების ციფრული ბაზების შექმნასთან დაკავშირებით, თუმცა სახელმწიფო არ ახორციელებდა კოორდინირებულ სამოქმედო გეგმას. აქედან გამომდინარე, არ

არსებობდა სპეციალური სააგენტოები, რომლებიც იქნებოდნენ პასუხისმგებლები ელექტრონული სისტემების დანერგვასა, თუ მათ უსაფრთხოებაზე. 2008 წლის კიბერ თავდასხმას, საქართველო მოუმზადებელი შეხვდა, თუმცა აღსანიშნავია ის ფაქტი, რომ ესტონურმა და პოლონურმა CERT ჯგუფებმა (Computer Emergency Response Team) საქართველოს სამეცნიერო–საგანმანათლებლო კომპიუტერული ქსელების ასოციაცია -„გრენა"-სთან ერთად, შეძლეს და გარკვეულწილად მოახერხეს ჰაკერული თავდასხმის თავიდან არიდება. კერძოდ კი რამდენიმე ქართლი ვებ-გვერდი გადაიტანეს ესტონურ სერვერებზე და ამით თავიდან აიცილეს DDOS-ს შეტევის შედეგად გამოწვეული ზიანი.

გამოყენებული ლიტერატურის სია

- BBC News, Virus-like attack hits web traffic, ხელმისაწვდომია: http://news.bbc.co.uk/2/hi/technology/2693925.stm;
- Development of surveillance technology and risk of abuse of economic information, 2.4, ხელმისაწვდომია: http://cryptome.org/stoa-r3-5.htm.
- Granger, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus; ხელმისაწვდომია: www.securityfocus.com/infocus/1527.
- Netadmintools Keylogging, available at: www.netadmintools.com/part215.html
- Anderson, Hacktivism and Politically Motivated Computer Crime, 2005, ხელმისაწვდომია: www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.
- O'Connell, M. E. (2012). Cyber security without cyber war. Journal of Conflict and Security Law, 17(2), 187-209.
- Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10).
- Svanadze, V. (2018). 2017 Cyber Security Challenges and Georgia. Scientific and practical cyber security journal.
- Silcock, R. (2001). What is e-government. Parliamentary affairs, 54(1), 88-101.

Vladimeri Napetvaridze

The Influence of Cyber Cryme Methods on the Contemporary World

Abstract

The 21st century is fairly considered the age of information technology. Although the process of internetization has been going on globally for just three decades, it can be said that digital technologies have radically changed all areas of human life. The world is becoming more and more dependent on modern technologies, which play a big role in the development of humanity.

Although the Internet is one of the major achievements of the 21st century, the dangers that accompany this phenomenon cannot be ignored. The development of the Internet has given rise to new cyber dimensions and consequently cyber threats. The digital world has given a wide range of opportunities to everyone, including cybercriminals who are trying to use modern technology to harm citizens or state institutions.

The aim of this paper is to identify the methods of cybercrime that pose a threat to both individuals and states in the modern world. Discussion each of them, and assessment the Georgian reality from the perspective of cyber security.

Keywords: Georgia; Cyber security; Cyber criminal.