Scientific and Practical Cyber Security Journal (SPCSJ) 6(4): 12-19 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

DIGITAL TECHNOLOGIES AND THEIR CYBER SECURITY IN LIGHT OF RECENT CHANGES IN ELECTORAL LAW

ციფრული ტექნოლოგიები და მათი კიბერუსაფრთხოება საარჩევნო კანონმდებლობაში შეტანილი ბოლო ცვლილებების ფონზე

Andro Gotsiridze – professor Business & Technology University of Georgia, Cybersecurity Consultant, Founder of CYSEC - Cyber Security Educational Research Center, Director of Cyber Security Bureau of Ministry of Defence of Georgia in 2014 -2017

ანდრო გოცირიძე, საქართველოს ბიზნესისა და ტექნოლოგიების უნივერსიტეტის პროფესორი, კიბერუსაფრთხოების კონსულტანტი. კიბერუსაფრთხოების საგანმანათლებლო კვლევითი ცენტრის CYSEC დამფუძნებელი, თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიუროს დირექტორი 2014-2017 წლებში.

ABSTRACT:The democratic approach considers that all elections are expected to be free, open and fair, and based on secret ballot; Digital Solutions, IC Technologies are integral parts of the modern electoral process. Their usage increases confidence, the degree of freedom and impartiality of elections, but from a cybersecurity perspective, any process involving the use of electronic devices or digitized data contains risks. Technology cannot be introduced at the cost of compromising mentioned requirements.

Depending on the motives of the attacker, cyber threats can lead to a decrease in confidence in the democratic process. Due to the growing trend of using cyber and information operations to interfere in elections, the cybersecurity of electoral processes is definitely one of the most important tasks of the state. The article gives a short overview of the cyber threats to election and discusses some cybersecurity aspects of integration of digital solutions into elections processes.

KEYWORDS: *cybersecurity, digital solution*

აბსტრაქტი: დემოკრატიული საზოგადოება მოელის, რომ ნებისმიერი არჩევნები იქნება თავისუფალი, ღია, სამართლიანი და უზრუნველყოფს მოქალაქის არჩევანის ფარულობას.ციფრული ტექნოლოგიები, კომპიუტერული სისტემები და პროგრამული უზრუნველყოფა საარჩევნო პროცესის თითოეული კომპონენტის შემადგენელი ნაწილია. მათი გამოყენება არჩევნების სანდოობას, თავისუფლების ხარისხსა და მიუკერძოებლობას ზრდის, თუმცა, კიბერუსაფრთხოების პერსპექტივიდან, ნებისმიერი პროცესი, რომელიც მოიცავს ელექტრონული მოწყობილობის ან გაციფრულებული მონაცემების გამოყენებას, გარკვეულწილად, რისკის შემცველია. ცხადია, ტექნოლოგიების დანერგვა არ უნდა მოხდეს ზემოჩამოთვლილი მოთხოვნების ხარჯზე.თავდამსხმელის მოტივიდან გამომდინარე, კიბერსაფრთხეებმა შესაძლოა შეზღუდოს არჩევნების თავისუფლება, განაპირობოს

დემოკრატიული პროცესისადმი ნდობის შემცირება.ბუნებრივია, კიბერდანაშაულის ზრდის ტენდენციის პირობებში, საარჩევნო პროცესების კიბერუსაფრთხოება თანამედროვე სახელმწიფოსათვის ერთ ერთი უმნიშვნელოვანესი ამოცანაა. სტატიაში განვიხილავთ არჩევნებში გამოყენებული ციფრული ტექნოლოგიების გამოყენებისას წარმოქმნილ კიბერსაფრთხეებს და კიბერუსაფრთხოების ზოგიერთ ასპექტს.

საკვანძო სიტყვები: *ციფრული ტექნოლოგიები, კიბერუსაფრთხოება, თანამედროვე ტექნოლოგოები*

ციფრული ტექნოლოგიები, კომპიუტერული სისტემები და პროგრამული უზრუნველყოფა საარჩევნო პროცესის თითოეული კომპონენტის შემადგენელი ნაწილია. მათი გამოყენება არჩევნების სანდოობას, თავისუფლების ხარისხსა და მიუკერძოებლობას ზრდის, თუმცა, კიბერუსაფრთხოების პერსპექტივიდან, ნებისმიერი პროცესი, რომელიც მოიცავს ელექტრონული მოწყობილობის ან გაციფრულებული მონაცემების გამოყენებას, გარკვეულწილად, რისკის შემცველია.

ბუნებრივია, კიბერდანაშაულის ზრდის ტენდენციის პირობებში, საარჩევნო პროცესების კიბერუსაფრთხოება თანამედროვე სახელმწიფოსათვის ერთ ერთი უმნიშვნელოვანესი ამოცანაა.

ზოგადად, კიბერთავდასხმის ტექნიკური თუ ადამიანური ვექტორი მოიცავს თავად საინფორმაციო ტექნოლოგიური სისტემებს, ასევე მათი შექმნისა და მართვის პროცესებს. ნებისმიერ სფეროსა თუ ინდუსტრაში სისტემის ან პროგრამული უზრუნველყოფის ტექნიკური სიუსტის კვალდაკვალ, ხშირად, კიბერშეტევების განსახორციელებლად ადამაინური ფაქტორი გამოიყენება. ბუნებრივია, ეს ტენდენცია ვრცელდება საარჩევნო სისტემების კიბერუსაფრთხოებაზეც. თავდამსხმელის მოტივიდან გამომდინარე, კიბერსაფრთხეებმა შესაძლოა შეზღუდოს არჩევნების თავისუფლება, განაპირობოს დემოკრატიული პროცესისადმი ნდობის შემცირება.

როგორც აღინიშნა, თანამედროვე არჩევნების თითქმის ყველა კომპონენტიამა თუ იმ ფორმით დაკავშირებულია ციფრულ ტექნოლოგიებთან და პროცესებთან. საარჩევნო რეესტრებს წარმოება, ამომრჩეველთა, პარტიებისა და კანდიდატების რეგისტრაცია, პარტიებისა და კანდიდატების რეგისტრაცია, დამკვირვებელთა, საარჩევნო ადმინისტრაციის და ამომრჩეველთა ცნობიერების ამაღლების ღონისძიებები, კენჭისყრა, ხმების დათვლა და შედეგების მართვა, ინფორმაციის მიმოცვლა და ანალიზი, საჩივრებისა და დავების მართვის სისტემები და სხვა მნიშვნელოვანი პროცესები ძალიან ხშირადკომპიუტერული ტექნოლოგიების საშუალებით ხდება. ეს ტენდენცია მეტწილად საარჩევნო პროცესების

გაუმჯობესებას, არჩევნების სამართლიანობის და სანდოობის ამაღლებას იწვევს, თუმცა მზარდი კიბერრისკების პირობებში, მოუმზადებელი ნორმატიული ბაზის, კიბერრისკების მართვის არასრულყოფილი სისტემისა და არასკმარისი ცნობიერების პირობებში, სახელმწიფოსათვის უმნიშვნელოვანესი პროცესი- არჩევნები, არცთუ იშვიათად, მოწყვლადი ხდება ხოლმე.

საარჩევნო სისტემების გაციფრულება, რაც ერთის მხრივ, სათანადო ნორმატიული ბაზის შექმნას, პროცესების გამართვას, მეორეს მხრივ კი არჩევნების კიბერუსაფრთხოების უზრუნველყოფას გულისხმობს, საქართველოშიც არაერთხელ დამდგარა დღის წესრიგში.

მიმდინარე წელს საქართველოს კანონმდებლობაში შეტანილი ცვლილებები ცესკო -ს მომდევნო მუნიციპალურ არჩევნებზე ამომრჩეველთა ელექტრონული რეგისტრაციის, ელექტრონული კენჭისყრის, ხმათა ელექტრონული დათვლისა და არჩევნების შედეგების შემაჯამებელი ოქმის ელექტრონულად შედგენის უფლებამოსილებას ანიჭებს.ამასთან, ელექტრონული რეგისტრაცია ყველა საარჩევნო უბანზე უნდა იყოს დანერგილი, ხოლო ქაღალდის ბიულეტენების ელექტრონული დათვლის სისტემა კი, საჭიროებისამებრ, სოციოლოგიურად ვალიდური შედეგებისათვის საჭირო რაოდენობის უბნებში. რაც შეეხება ელექტრონულ კენჭისყრის სახეს, ის არ არის განსაზღვრული.

ამჟამად საქართველოში არსებობს გარკვეული მონაცემთა ბაზები, როგორიცაა ამომრჩეველთა ერთიანი სია, დამკვირვებელთა რეესტრი, პრესის, მედიისადა პარტიების რეგისტრაცია, ასევე, საქართველოს საარჩევნო კოდექსის მიხედვით, შესაძლებელია, საარჩევნო სუბიექტების, დამკვირვებლების, მედიის მიერ ელექტრონული საშუალებებით განაცხადების წარდგენას.

ზოგადად, სხვადასხვა ეტაპზე, ციფრული ტექნოლოგიები სხვადასხვა სახით გამოიყენება და მათ მიმართ არსებული კიბერსაფრთხეებიც, ისევე, როგორც მათი პრევენციის ან მიტიგაციის გზაც სხვადასხვა.

ქვემოთ განვიხილავთ არჩევნებში გამოყენებული ციფრული ტექნოლოგიების გამოყენებისას წარმოქმნილ კიბერსაფრთხეებს და კიბერუსაფრთხოების ზოგიერთ ასპექტს.

როგორც უკვე აღინიშნა, საქართველოში რამდენიმე ელექტრონული რეესტრი არსებობს და ინერგება ტექნოლოგიები საარჩევნო პროცესის სამართავად. ინტეგრირებული სისტემები და სერვისები, რომლებიც გაციფრულებული საარჩევნო მონაცემების სამართავად გამოიყენება **არჩევნების მართვის სისტემის** სახელითაა ცნობილი და იგი რამდენიმე სერვისს მოიცავს. სისტემის ზოგიერთი შემადგენელი ადგილობრივ დონეზეა ბაზირებული თუმცა კავშირი და ინფორმაციის მიმოცვლა აქვს ცენტრალურ ბაზასთან. არჩევნების მართვის სისტემის

შემადგენელი ნაწილია, ასევე სხვადასხვა მონაცემთა ბაზა, აპლიკაციები და სხვა პროგრამები, რომელთა მიმართ არსებული კიბერრისკები მთლიანი სისტემისთვისაც საფრთხის შემცველია.

საარჩევნო პროცესებში მოწყვლადი კომპონენტებია ამომრჩევლის ონლაინ-რეგისტრაცია, ხმის მიცემის ელექტრონული პროცესი, შედეგების შეჯამება და გამოცხადება, კომუნიკაცია, საარჩევნო კამპანიის წარმოების ელექტრონული საშუალებები და სხვა უამრავი პროცესი, რომელთა ოპტიმალური მართვა სწორედ ციფრული ტექნოლოგიების გამოყენებით მიიღწევა . თუმცა, ამგვარ მრავალფეროვან პროცესებს სათანადო კიბერრისკებიც ახლავს თან, რომელთა არასრული ჩამონათვალი შესაძლოა შემდეგნაირად წამოვიდგინოთ:

- **არაავტორიზებული წვდომა:** ინტერნეტთან კავშირის მქონე მონაცემთა ბაზები მოწყვლადია. თავდამსხმელს, წვდომის მოპოვების შემდგომ, შეუძლია დაამატოს, შეცვალოს, ამოშალოს ამომრჩეველი, გააყალბოს ხმა არჩევნების დღეს. იმ შემთხვევაშიც კი, თუ ამგვარი ქმედება მნიშვნელოვან გავლენას ვერ ახდენს არჩევნების შედეგზე, პროცესში ჩარევის აღქმა სერიოზულ საფრთხეს უქმნის არჩევნების სანდოობას
- **არასათანადო ტექნიკური მომსახურება ან ავტომატიზირებული განახლებების დაგვიანებული პროცესი** ხშირად განაპირობებს თავდამსხმელის მხრიდან მავნე პროგრამული უზრუნველყოფის იმპლანტაციას
- **ავტორიზებული პირის ანგარიშის კომპრომეტაცია.**თავდამსხმელმა შეიძლება მოახდინოს საარჩევნო ადმინისტრაციის წევრის ან სხვა ინსაიდერის ანგარიშის კომპრომეტაცია. არასათანადო კონტროლის პირობებში, მას საშუალება მიეცემა ამომრჩევლის შესახებ ჩანაწერები მისი შეხედულებისამებრ შეცვალოს. ლოგირებისა და მონიტორინგის სისტემის არარსებობის პირობებში ეს ხარვეზი აისახება არჩევნების შედეგზე.
- **დაკავშირებული სისტემების და მონაცემთა ბაზების კომპრომეტაცია.** როგორც აღინიშნა, არჩევნების მართვის სისტემასთან დაკავშირებულია სხვადასხვა აპლიკაცია, პროგრამა ან მონაცემთა ბაზა, რომელთაგან ზოგიერთი, შესაძლოა, არ იყოს სათანადოდ დაცული და მოხდეს მისი კომპრომეტაცია ან მონაცემების მანიპულაცია მათი გადაგზავნისას. გარკვეულ რისკს წარმოადგენს ასევე ის ფაქტორი, რომ ზოგჯერ

გარე ბაზებიდან მონაცემები პირდაპირ ხვდება არჩევნების მართვის სისტემებში, დამატებითი გადამოწმებისა და დადასტურების გარეშე. ასეთ შემთხვევაში შესაძლებელია ამომრჩევლის სტატუსის მანიპულირება მავნე აქტორის მხრიდან.

- **ვებგვერდის გაყალბება:** თავდამსხმელი შესაძლოა ახდენდეს პოზიციონირებას, როგორც ოფიციალური საიტი, სინამდვილეში კი ცდილობდეს ამომრჩეველთა პერსონალური ინფორმაციის მოპარვას მიმსგავსებული გვერდის მეშვეობით
- DDoS შეტევა, რომლის მეშვეობითაც, თავდამსხმელი, აფერხებს რა სერვისის ხელმისაწვდომობას, ცდილობს შეზღუდოს ამომრჩევლის რეგისტრაციის შესაძლებლობა. საბოლოო ჯამში მსგავსმა ზემოქმედებამ შესაძლოა გამოიწვიოს არცევნებში მონაწილეობის დაბალი პროცენტი
- **არასათანადოდ დაცული ვებგვერდი**შესაძლოა გახდეს ამომრჩევლების მონაცემთა ბაზაში შეღწევის ვექტორი, რასაც თან სდევს ამომრჩეველთა შესახებ ჩანაწერის გაყალბება
- **ხმის მიცემის ელექტრონული მოწყობილობა** შესაძლოა კომპრომეტირებულ იქნას ფიზიკური ჩარევის, (მაგ. USB ან სხვა სახის მედიამატარებელი) ან გარე კავშირის (მაგ. უსადენო ინტერნეტი) გზით, რამაც, შესაძლოა შეცვალოს ინფორმაცია ხმის მიცემის შესახებ
- ოფიციალურ პირთა **ელფოსტის ანგარიშის კომპრომეტაცია**ფიშინგის ან სოციალური ინჟინერიის სხვა ტექნიკით, შესაძლოა გამოყენებულ იქნას თავდამსხმელის მიერ ყალბი ინფორმაციის გასავრცელებლად, არაკეთილსინდისიერი განკარგულების გასაცემად. კომპრომეტირებული ანგარიში ასევე გამოიყენება მავნე პროგრამული უზრუნველყოფის ქსელში გასავრცელებლად
- საარჩევნო ადმინისტრაციის **ვებგვერდის მანიპულაცია** - ხშირია Defacement ტიპის შეტევის განხორციელება ამომრჩევლის დაბნევის, დაშინების, შეცდომაში შეყვანის მიზნით. ასევე, შესაძლებელია ონლაინ ხმის მიცემის საიტის ლოკაციის შეცვლა, ამომრჩეველთა წვდომის გართულების მიზნით.
- **სოციალური ქსელის რისკებიდან** ყურადსაღებია ყალბი ანგარიშები ან ოფიციალური გვერდების კომპრომეტაცია. ეს ტექნიკა შესაძლებელია გამოყენებულ იქნას

სოციალური ქსელით შეცდომაში შემყვანი ინფრომაციის, არასწორი ლოკაციების, გაყალბებული შედეგების გასავრცელებლად.

ზოგადად, თუკი არჩევნების თანმდევ კიბერშეტევებს გავაანალიზებთ, ცხადი ხდება კანონზომიერება, რომ თავდამსხმელები კიბერშეტევების იაფ მეთოდებს ანიჭებენ უპირატესობას. ასე მაგალითად, დაბალტექნოლოგიური და ეკონომიკურად ეფექტური DDoS და Defacement სჭარბობს დახვეწილ APT შეტევებს. ეს უკანასკნელი ტიპი შეტევისა მეტად იშვიათად გამოიყენება და ისიც, მხოლოდ მაღალგანვიტარებული კიბერპოტენციალის მქონე სახელმწიფოთა საარჩევნო სისტემების წინააღმდეგ.

კიბერსაფრთხეებისაგან თავდასაცავად მნიშვნელოვანია ღონისძიებათა კომპლექსის გატარება:

- **ძლიერი პასვორდისა და მრავალფაქტორიანი ავთენტიფიკაციის პოლიტიკის** გატარება ნებისმიერი ავტორიზებული მომხმარებლისათვის. განსაკუთრებული ყურადღება უნდა დაეთმოს ადმინისტრირების უფლების მქონე მომხმარებლის ანგარიშების უსაფრთხოებას.
- **შეღწევადობის ტესტის, პროგრამის კოდის აუდიტის ჩატარება,** მიუხედავად იმისა, გამოყენებული პროგრამული უზრუნველყოფები ადმინისტრაციის მიერაა შექმნილი თუ ვენდორების მოწოდებულია. აუდიტისა და ტესტის შედეგები კარგ წარმოდგენას იძლევა სისტემის სისუსტეებზე. ასევე, მნიშვნელოვანია ფიშინგის და სოციალური ინჟინერიის სხვადასხვა სახეობების მიმართ ორგანიზაციის მდგრადობის ტესტები და რეგულარული სავარჯიშოები.
- პროგრამული უზრუნველყოფის **განახლებების პროცესის წარმოება ავტომატურ რეჟიმში** ყველა მოწყობილობასა თუ სისტემაზე, რომელიც კავშირშია არჩევნების მართვის სისტემასთან.
- მონაცემთა ბაზის სერვერების **ინტერნეტით ხელმისაწვდომობის** შეზღუდვა
- გარე სისტემებიდან შემოსული **მონაცემების ვალიდაციის მექანიზმის** გამართვა
- **მიმდინარე პროცესების ლოგირება და დაშვებების სწორი მენეჯმენტი.** როგორც წესი, უნდა ინახებოდეს მონაცემტა ბაზებში განხორციელებული ნებისმიერი ცვლილების სესახებ ჩანაწერი და უნდა ხდებოდეს მათი ანალიზი, ასევე,

ანომალიური აქტივობების კვლევა. წასული თანამშრომლების ან სხვა ინსაიდერების (მაგ. ვენდორის, კონტრაქტორის) სისტემასთან წვდომა ავტომატურად უნდა იზღუდებოდეს მისი საჭიროების გაქრობის მომენტიდან.

- საარჩევნო ადმინისტრაციის, ასევე არჩევნებში მონაწილე პირთა**ცნობიერების ამაღლება,**გასაკუთრებით, სოციალური მედიის რისკების თემატიკაზე. სოციალური მედიის როგორც ოფიციალური, ასევე პირადი ანგარიშები აუცილებელია დაცულ იქნეს ორმაგი ავტენტიფიკაციით. ძლიერი პასვორდის პოლიტიკასთან ერთად, ეს საუკეთესო ნაბიჯია ანგარიშის კომპრომეტაციის თავიდან ასაცილებლად.

ამრიგად, სახელმწიფოთა მიერ მხარდაჭერილი კიბერშეტევები ხშირად მიმართულია უნდობლობის გაღვივების, საზოგადოების პოლარიზაციისკენ და მიზნად ისახავს დემოკრატიული პროცესების შეფერხებასა და მოშლას. ნებისმიერი სისტემით ჩატარებული არჩევნები უნდა იყოს ღია, სამართლიანი, თავისუფალი და ემყარებოდეს ხმის მიცემის ფარულობას. ციფრული ტექნოლოგიების დანერგვა არ უნდა ახდენდეს რომელიმე ამ მახასიათებლის კომპრომეტაციას. ციფრული გადაწყვეტები ან საარჩევნო ტექნოლოგიები თავისთავად არ შეიცავენ უფრო მეტ ან ნაკლებ საფრთხეს, მაგრამ მათი დანერგვისას აუცილებელია გარკვეული სიფრთხილის დაცვა ციფრული პროცესების მოქმედ კანონმდებლობასთან შესაბამისობაში მოსაყვანად. ხშირად, კიბერუსაფრთხოების შესაბამისი მოთხოვნების დაცვით ციფრული ტექნოლოგიების დანერგვა ხელსუწყობს არჩევნების პროცესისადმი წაყენებული მოთხოვნების შესრულებას და მათ მაღალ ლეგიტიმაციას.

სტატიაში შევეცადეთ ფოკუსირება მოგვეხდინა კიბერშეტევებთან და ქსელის უსაფრთხოებასთან დაკავშირებულ საფრთხეებზე და მათთან გამკლავების გზებზე. საარჩევნო პროცესებში ჩარევაში მნიშვნელოვან როლს თამაშობს დეზინფორმაცია, სოციალური მედია და საინფორმაციო ოპერაციები, რომელთა გავლენა არჩევნების ძირითად მახასიათებლებსა და მის ლეგიტიმურობაზე ცალკე განხილვის თემაა და ამდენად, ეს მიმართულება წინამდებარე ნაშრომში ვერ მოხვდა.

ბიბლიოგრაფია

1. Sebastian Bay, Guna Šnore, Protecting Elections: a strategic communications approach. NATO Strategic Communications Centre of Excellence, 2019
2. Defence Intelligence Agency. Russia Military Power - Building a Military to Support Great Power Aspirations. Report, 2017. ხელმისაწვდომია www.dia.mil/Military-Power-Publications

3. Laura Galante, Shaun Eee. Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents. Atlantic Councis Issue Brief. September, 2018
4. Intelligence Community Assesment. Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution. ICA 2017-01D, 6 January 2017
5. ა.გოცირიძე. კიბერსაფრთხეები და მათთან ბრძოლის სტრატეგიული მიმართულებები საქართველოს პერსპექტივიდან. თ.ხიდაშელი "ჰიბრიდული ომების ანატომია"-ში. გვ. 365-395. გამომცემლობა პალიტრა L.
6. Defending Digital Democracy Project**.** Belfer Center for Science and International Affairs**.** Harvard Kennedy School**.** The State and Local Election Cybersecurity Playbook. 2018.
7. Office of the Director of National Intelligence, Cyber Threat Intelligence Integration Center. Cyber Threats to Elections – a Lexicon. 2018