NEW VISION UNIVERSITY

ევროპის კავშირის სამართლის
ჟან მონეს კათედრა

JEAN MONNET CHAIR
IN EU LAW

ევროპის კავშირის სამართლის
სამუშაო ფურცლები

WORKING PAPERS
ON EU LAW

01/2022

„ინფორმაციული უსაფრთხოების შესახებ" საქართველოს კანონში 2021 წლის 10 ივნისს განხორციელებული ცვლილებების მიმოხილვა ევროკავშირის ქსელისა და ინფორმაციული უსაფრთხოების (NIS) დირექტივასთან შესაბამისობის პერსპექტივის ჭრილში

OVERVIEW OF THE AMENDMENTS OF 10 JUNE 2021 TO LAW OF GEORGIA ON INFORMATION SECURITY IN THE CONTEXT OF COMPATIBILITY WITH THE NETWORK AND INFORMATION SECURITY DIRECTIVE (NIS) OF THE EUROPEAN UNION

ეკა გორდაძე
Eka Gordadze

With the support of the
Erasmus + Programme
of the european Union

წინამდებარე პუბლიკაციაზე მუშაობა განხორციელდა ჟან მონეს ევროპის კავშირის სამართლის კათედრის ფარგლებში, ევროპის კავშირის ერასმუს+ პროგრამის მხარდაჭერით. მასში გამოთქმული შეხედულებები და მოსაზრებები ეკუთვნის მხოლოდ ავტორს და შეიძლება არ ასახავდეს ევროპის კავშირის ან ევროპის განათლებისა და კულტურის აღმასრულებელი სააგენტოს (EACEA) შეხედულებებს. მათზე პასუხისმგებლობა არ შეიძლება დაეკისროს ევროპის კავშირს ან EACEA-ს.

The work on this publication took place within the framework of the Jean Monnet Chair in European Law, with the support of the Erasmus+ programme of the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

With the support of the
Erasmus+ Programme
of the European Union

2019 წელს, ნიუ ვიჟენ უნივერსიტეტში, ევროპის კავშირის ერასმუს+ პროგრამის მხარდაჭერით, დაარსდა ევროპის კავშირის სამართლის კათედრა, რომლის მიზანია, ხელი შეუწყოს საქართველოში ევროპის სამართლის საკითხებზე სწავლებისა და კვლევების განვითარებას. კათედრის ხელმძღვანელია ნიუ ვიჟენ უნივერსიტეტის სამართლის სკოლის პროფესორი გაგა გაბრიჩიძე.

კათედრის ფარგლებში წელიწადში ორჯერ გამოიცემა და ვრცელდება „ევროპის კავშირის სამართლის სამუშაო ფურცლები“, რომლის მიზანია კვლევის შუალედური შედეგების გავრცელების ხელშეწყობა და იდეების ურთიერთგაცვლისა და აკადემიური დისკუსიის მხარდაჭერა.

In 2019, with the support of the Erasmus+ Programme of the European Union the Jean Monnet Chair in EU Law was established at New Vision University. The Chair promotes teaching of and research on issues of EU law in Georgia. The holder of the Jean Monnet Chair is Professor of the Law School of New Vision University Gaga Gabrichidze.

The Chair publishes and disseminates a biannual electronic Working Papers on EU Law. The publication is aimed at supporting dissemination the research results of work in progress to encourage the exchange of ideas and academic debate.

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში 2021 წლის 10 ივნისს განხორციელებული ცვლილებების მიმოხილვა ევროპის კავშირის ქსელისა და ინფორმაციული უსაფრთხოების (NIS) დირექტივასთან შესაბამისობის პერსპექტივის ჭრილში

ეკა გორდაძე

ნიუ ვიჟენ უნივერსიტეტის სამართლის სკოლის დოქტორანტი

1. შესავალი

ინტერნეტის არსებობის დღიდან თანამედროვე სამყარო სულ უფრო მეტად ცდილობს გაუმკლავდეს კიბერსივრცეში წარმოშობილ საფრთხეებს. კიბერუსაფრთხოებასთან დაკავშირებული გამოწვევები თანაბრად აქტუალურია როგორც ინდივიდების, ისე - სამთავრობო და კერძო სექტორისათვის.[1]

2022 წლის 3 მარტს საქართველომ განაცხადი გააკეთა ევროპის კავშირში გაწევრიანების თაობაზე[2], რასაც, დაახლოებით 1 წლით ადრე, წინ უძღოდა ინფორმაციული უსაფრთხოების სფეროს მარეგულირებელ საკანონმდებლო აქტებში ძირეული ცვლილებების განხორციელება. ეჭვგარეშეა, ევროპული ინტეგრაციის გზაზე[3] საქართველომ უნდა უზრუნველყოს ევროპის კავშირისათვის მისაღები, იმგვარი სამართლებრივი გარემოს შექმნა, სადაც ტექნოლოგიური განვითარება და ციფრული სერვისების ხელმისაწვდომობა ადეკვატურად ერწყმის

[1] SolarWinds-ის კიბერშეტევა ერთ-ერთი ყველაზე ცნობილი და მასშტაბური შემთხვევაა ბოლო პერიოდის კიბერშეტევების ისტორიაში, უფრო მეტიც, მას 21-ე საუკუნის ყველაზე დიდ შეტევას უწოდებენ. 2020 წელს ჰაკერებმა მიზანში ამოიღეს კომპანია SolarWinds-ი და მავნე კოდი განათავსეს მის IT მონიტორინგისა და მართვის პროგრამულ უზრუნველყოფაში (Orion), რომელსაც უამრავი კომპანია და სამთავრობო უწყება იყენებს მთელს მსოფლიოში. აღნიშნული შეტევა დამაზიანებელი გამოდგა ათასობით ორგანიზაციისთვის, მათ შორის, აშშ-ს სამთავრობო წრეებისთვისაც. როგორც IT მონიტორინგის სისტემას, SolarWinds Orion-ს აქვს პრივილეგირებული წვდომა IT სისტემებზე „ლოგებისა“ და სისტემის მუშაობის მონაცემების მისაღებად. სწორედ ამ პრივილეგირებულმა წვდომამ და მისმა ფართო მასშტაბებმა აქცია SolarWinds-ი მიმზიდველ სამიზნედ. ჰაკერებმა მოიპოვეს წვდომა SolarWinds-ის ათასობით მომხმარებლის ქსელებზე, სისტემებსა და მონაცემებზე. ჰაკერებმა ჯერ კიდევ 2019 წელს მოიპოვეს არაავტორიზებული წვდომა SolarWinds-ის ქსელთან, ხოლო მავნე კოდის სისტემაში ჩანერგვის შემდეგ, 2020 წელს დაიწყო მომხმარებლებთან Orion-ის პროგრამული უზრუნველყოფის განახლებების (updates) დაგზავნა ისე, რომ თავად SolarWinds-მა არაფერი იცოდა. SolarWinds-ის 18 000-ზე მეტმა მომხმარებელმა გამოიყენა მავნე კოდის შემცველი განახლება.

[2] 2022 წლის 3 მარტს საქართველომ ოფიციალურად გააკეთა განაცხადი ევროპის კავშირში გაწევრიანების თაობაზე. იხ.: <https://www.gov.ge/index.php?lang_id=GEO&sec_id=573&info_id=81400> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 04.06.2022).

[3] ევროსაბჭოს გენერალური სამდივნოს 2022 წლის 24 ივნისის დასკვნის თანახმად, საბჭო აღიარებს საქართველოს ევროპულ პერსპექტივას და მზადაა ქვეყანას მიანჭოს კანდიდატის სტატუსი შესაბამისი პირობების დაკმაყოფილებისთანავე („...The European Council is ready to grant the status of candidate country to Georgia once the priorities specified in the Commission's opinion on Georgia's membership application have been addressed), იხ. ევროსაბჭოს გენერალური სამდივნოს 2022 წლის 24 ივნისის დასკვნა, მე-3 თავი: <https://www.consilium.europa.eu/media/57442/2022-06-2324-euco-conclusions-en.pdf> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 25.06.2022).

კიბერუსაფრთხოების მდგრადობის უზრუნველყოფას.[4] ამ ფონზე შეფასებას იმსახურებს ის გარემოება, რომ საქართველომ ასოცირების შეთანხმების დღის წესრიგის ფარგლებში[5] არ აიღო ევროპის კავშირის ქსელისა და ინფორმაციული უსაფრთხოების (NIS) დირექტივასთან დაახლოების თვალსაზრისით კონკრეტული ვალდებულება, არამედ - შემოიფარგლა ზოგადი მითითებით, რომ გააგრძელებს „მუშაობას საქართველოს კანონმდებლობის ქსელისა და ინფორმაციული უსაფრთხოების დირექტივასთან შემდგომ დაახლოებასთან დაკავშირებით.“ აქვე, ევროპის კავშირში საქართველოს წევრობის განაცხადთან დაკავშირებით ევროკომისიის დასკვნის თანახმად, კანდიდატი ქვეყნის სტატუსის მისაღებად საქართველოს ევალება, უზრუნველყოს ყველა სახელმწიფო ინსტიტუტის დამოუკიდებლობის ხარისხის ზრდა, ეფექტიანი ანგარიშვალდებულების მექანიზმის შექმნა და მათზე დემოკრატიული ზედამხედველობის განხორციელება.[6]

NIS დირექტივასთან საქართველოს კანონმდებლობის დაახლოების პერსპექტივის შესაფასებლად, წინამდებარე ნაშრომის ფარგლებში, ერთი მხრივ, განხილულია „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში 2021 წლის 10 ივნისს განხორციელებული საკანონმდებლო ცვლილებები, ხოლო, მეორე მხრივ, ევროპის კავშირის NIS დირექტივით დადგენილი კიბერუსაფრთხოების სტანდარტი. ნაშრომში განხილული საკითხები წარმოჩენილია შედარებით-სამართლებრივი ანალიზის გზით.

ნაშრომის მიზანია, შეფასოს, თუ რა დონეზე შეესაბამება „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის დღეს მოქმედი ვერსია ევროპის კავშირის NIS დირექტივით დადგენილ კიბერუსაფრთხოების სტანდარტს და რა ფორმით აისახება აღნიშნული საქართველოში კიბერუსაფრთხოების გარემოს ფორმირებაზე. ნაშრომში განზოგადებული დასკვნები ემსახურება კიბერუსაფრთხოების სფეროს მარეგულირებელი

[4] იხ. „ასოცირების შესახებ შეთანხმება ერთი მხრივ, საქართველოსა და მეორე მხრივ, ევროპის კავშირს და ევროპის ატომური ენერგიის გაერთიანებას და მათ წევრ სახელმწიფოებს შორის”, მე-14 მუხლი.

[5] იხ. საქართველოსა და ევროპის კავშირს შორის 2021 – 2027 წლების ასოცირების დღის წესრიგის ტექსტი, რომელიც საქართველოს საგარეო საქმეთა სამინისტრომ 2022 წელს გამოაქვეყნა. ხელმისაწვდომია შემდეგ ელექტრონულ რესურსზე: <https://mfa.gov.ge/getattachment/3ba81b82-36f8-4c7c-8ec3-53ddc292df1f/2021-2027-EU-Georgia-Association-Agenda-KA.pdf.aspx> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 14.06.2022).

[6] იხ. Communication from the Commission to the European Parliament, the European Council and the Council, Brussels, 17.6.2022 COM(2022) 405 final, §.4.

სამართლებრივი გარემოს გაუმჯობესებისა და უკეთესი პრაქტიკის ჩამოყალიბების ხელშეწყობას.

2. კრიტიკული ინფორმაციული სისტემების მიმართ NIS დირექტივით დადგენილი ძირითადი ვალდებულებები

ევროპის კავშირმა ღია, უსაფრთხო და დაცული კიბერსივრცის აუცილებლობის[7] შესახებ ხედვა მის კიბერუსაფრთხოების სტრატეგიაში[8] ასახა და მასთან ერთად, 2013 წელს გამოაქვეყნა NIS დირექტივის პროექტი.[9] მოგვიანებით, 2016 წელს მიღებული დირექტივა ევროპის კავშირისთვის კიბერუსაფრთხოების სფეროს მარეგულირებელი პირველი დოკუმენტი გახდა.[10]

აღნიშნული დირექტივა მიზნად ისახავს კავშირის შიგნით, თანაბრად და ერთგვაროვანი მიდგომებით ქსელისა და საინფორმაციო სისტემების უსაფრთხოების მაღალი დონის მიღწევას.[11] რამდენადაც დირექტივა შესასრულებლად სავალდებულოა დასახული მიზნის მიღწევის ფარგლებში,[12] წევრ სახელმწიფოებს, ამ შემთხვევაში, დაევალათ 2018 წლის

---

[7] ევროკომისიის მონაცემებით, 2014 – 2020 წწ. პერიოდში 600 მლნ. ევროზე მეტის ინვესტიცია გამოიყო კიბერუსაფრთხოების სფეროში კვლევითი და ინოვაციური ტიპის პროექტების დასაფინანსებლად. იხ. ელექტრონულ რესურსზე: <https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 04.06.2022).

[8] იხ. Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace, ხელმისაწვდომია ელექტრონულ რესურსზე: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 14.06.2022).

[9] იხ. ევროკომისიის მიერ გამოქვეყნებული ინფორმაცია შემდეგ ელექტრონულ რესურსზე: <https://ec.europa.eu/commission/presscorner/detail/en/IP_13_94> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 28.06.2022).

[10] იხ. ევროპის კიბერუსაფრთხოების სააგენტოს (ENISA) მიერ გამოქვეყნებული ინფორმაცია შემდეგ ელექტრონულ რესურსზე: <https://www.enisa.europa.eu/topics/nis-directive?tab=details> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 27.06.2022).

[11] იხ. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, მუხლი 1.

[12] იხ. „ევროპული კავშირის საქმიანობის წესის შესახებ“ ხელშეკრულება, 288-ე მუხლის მე-3 პუნქტი დირექტივას ახასიათებს როგორც სამართლებრივ აქტს. იგი ფორმისა და საშუალების არჩევის

9 მაისამდე ეროვნული კანონმდებლობის მასთან შესაბამისობაში მოყვანა.[13] დირექტივა წევრ სახელმწიფოებს უტოვებს რა გარკვეულ შესაძლებლობას, მხედველობაში მიიღონ ეროვნული თავისებურებები და გარემოებები, წევრმა სახელმწიფოებმა სხვადასხვა დროს დაასრულეს[14] დირექტივის ეროვნულ კანონმდებლობაში ტრანსპოზიციის პროცესი.

2.1 სასიცოცხლოდ მნიშვნელოვანი სერვისების გამწევი სუბიექტების იდენტიფიცირება

NIS დირექტივა წევრ სახელმწიფოებს, პირველ რიგში, ავალდებულებს, მოახდინოს სასიცოცხლოდ მნიშვნელოვანი სერვისების გამწევი სუბიექტების[15] იდენტიფიცირება.[16] ევროპის კავშირის წევრი სახელმწიფო ვალდებულია შექმნას ან/და დანიშნოს ეროვნული საზედამხედველო ორგანო ან ორგანოები უშუალოდ დირექტივის მიზნებისათვის, კერძოდ, დირექტივის ეროვნულ დონეზე გამოყენების საკითხების ზედამხედველობისათვის.[17] შესაბამისად, სწორედ საზედამხედველო ორგანო უწევს კრიტიკული სუბიექტების იდენტიფიცირებისა და მათი მხრიდან ვალდებულებების შესრულების პროცესს მონიტორინგს.

შესაძლებლობას თავად წევრ სახელმწიფოებს ანიჭებს. დამატებით იხ. *ოპერმანი, კლასენი, ნეთესჰაიმი,* ევროპული სამართალი, მე-8 განახლებული გამოცემა, 2018, 178.

[13] იხ. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, მუხლი 3.

[14] ევროკომისიის მიერ გამოქვეყნებული ინფორმაციის თანახმად, კავშირის წევრ 27-ვე ქვეყანაში დასრულდა დირექტივის ტრანსპოზიცია. იხ.: <https://digital-strategy.ec.europa.eu/en/policies/nis-transposition> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 10.06.2022).

[15] დირექტივა იყენებს ტერმინს: „operators of essential services“, რომელშიც მოიაზრება სუბიექტი: ა) რომელიც გასწევს საზოგადოების ნორმალური ფუნქციონირებისა და ეკონომიკური აქტივობისათვის კრიტიკულ მომსახურებას; ბ) გასწევს ამ მომსახურებას, რაც ასევე დამოკიდებულია ქსელსა და საინფორმაციო სისტემებზე და გ) რომლის ინციდენტსაც ექნება მნიშვნელოვანი დამღუპველი ეფექტი ამ სერვისის მიწოდებაზე. დირექტივის თანახმად, წევრ სახელმწიფოებს 2018 წლის 9 მაისის შემდეგ, რეგულარულად, თუმცა, სულ მცირე, 2 წელიწადში ერთხელ მაინც აქვთ ამ სიის გადახედვისა და საჭიროებისამებრ, განახლების ვალდებულება. იხ. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, მუხლი 5 (1).

[16] იხ. იქვე, მუხლი 4 (4), დანართი II.

[17] იხ. იქვე, მუხლი 8 (1), (2).

საამისოდ, დირექტივით განსაზღვრულია ის შვიდი სექტორი, რომლის ფარგლებში გაწეული მომსახურებაც, შესაბამისი კრიტერიუმების არსებობისას, შესაძლოა, მიჩნეულ იქნას საზოგადოებისათვის სასიცოცხლოდ მნიშვნელოვნად. პირველ სექტორს წარმოადგენს ენერგეტიკა, სადაც ერთიანდება ელექტროენერგიის, გაზის და ნავთობის მიწოდება. ამ სექტორს მოსდევს ტრანსპორტის სექტორი (საჰაერო, სახმელეთო, საზღვაო და სარკინიგზო ტრანსპორტი), საბანკო სფერო, საფინანსო ბაზრის ინფრასტრუქტურა, ჯანდაცვის სექტორი, სასმელი წყლის დისტრიბუცია და მიწოდება, ციფრული ინფრასტრუქტურა.[18]

გარდა სექტორული დაყოფისა, წევრი სახელმწიფოების მხრიდან ამგვარი კრიტიკული სერვისების მიმწოდებელი სუბიექტის იდენტიფიცირების პროცესში სავალდებულოდ გასათვალისწინებელია[19] შემდეგი კრიტერიუმები:

ა) ორგანიზაცია (როგორც კერძო, ისე - საჯარო სექტორში) გასწევს საზოგადოების ნორმალური ფუნქციონირებისა და ეკონომიკური აქტივობისათვის კრიტიკულ მომსახურებას;

ბ) ამ მომსახურების გაწევა დამოკიდებულია ქსელსა და ინფორმაციულ სისტემებზე;

გ) ინციდენტის შემთხვევაში, სერვისის მიწოდების შეფერხებას ექნება მნიშვნელოვანი დამაზიანებელი ეფექტი.[20]

თუ რომელიმე ზემოაღნიშნული კრიტერიუმის გათვალისწინებით, ორგანიზაცია იდენტიფიცირებულია, როგორც კრიტიკული სერვისების მიმწოდებელი, წევრი სახელმწიფო ვალდებულია, ის შესაბამის სიაში შეიყვანოს[21], რა დროიდანაც მას დირექტივით დადგენილი

---

[18] იხ. იქვე.

[19] იხ. *Markopoulou D., Papakonstantinou V., Hert P.,* The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, 2019, 3.

[20] იხ. იქვე, მუხლი 5 (1). ამასთან, „მნიშვნელოვანი დამაზიანებელი ეფექტის" (significant disruptive effect) განსაზღვრისას მხედველობაში მიიღება: ა) მომსახურების მომხმარებელთა რაოდენობა; ბ) სხვა სექტორის ამ სერვისზე დამოკიდებულება; გ) გავლენა, რომელსაც შეიძლება ჰქონდეს ინციდენტს, ხარისხისა და ხანგრძლივობის თვალსაზრისით, ეკონომიკურ და სოციალურ საქმიანობაზე ან საზოგადოებრივ უსაფრთხოებაზე; დ) ორგანიზაციის საბაზრო წილი; ე) ინციდენტით დაზარალების თვალსაზრისით გეოგრაფიული გავრცელების არეალი; ვ) სუბიექტის მნიშვნელობა მომსახურების საკმარისი დონის შესანარჩუნებლად, ამ სერვისის მიწოდების ალტერნატიული საშუალებების არსებობის გათვალისწინებით.

[21] იხ. *Markopoulou D., Papakonstantinou V., Hert P.,* The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, 2019, 3. ასევე, იხ. Directive (EU) 2016/1148, პრეამბულა, §. 25.

ცალკეული მოთხოვნების გათვალისწინების ვალდებულება წარმოეშობა. აღნიშნული გულისხმობს, ერთი მხრივ, პრევენციული ხასიათის ღონისძიებების გატარებას, როგორიცაა, მაგალითად, რისკების პროპორციული და შესაბამისი ტექნიკურ-ორგანიზაციული ზომების მიღება, ხოლო, მეორე მხრივ, ინციდენტების მართვასთან დაკავშირებული ღონისძიებები - ინციდენტის დამაზიანებელი შედეგების მინიმიზება და აღმოფხვრა. კრიტიკული სერვისების მიმწოდებელი ორგანიზაცია ვალდებულია, უზრუნველყოს საკუთარი ქსელისა და ინფორმაციული სისტემის უსაფრთხოება, მის წინაშე მდგარი გამოწვევებისა და რისკების პროპორციულად.[22] დირექტივა ხაზს უსვამს განსაკუთრებული გავლენის მქონე ინციდენტის[23] საზედამხედველო ორგანოს ან კომპიუტერული უსაფრთხოების ინციდენტებზე რეაგირების ჯგუფის (CSIRT) წინაშე დაუყოვნებლივი შეტყობინების ვალდებულებას, რათა თავიდან იქნას აცილებული არასასურველი შედეგები.[24] შესაბამისად, ნებისმიერი ინციდენტი, რომელიც უარყოფით გავლენას ახდენს არა მხოლოდ მონაცემთა ან მასთან დაკავშირებული სერვისების ხელმისაწვდომობაზე, არამედ მათ ავთენტურობაზე, მთლიანობასა თუ კონფიდენციალურობაზე[25], ექვემდებარება შეტყობინებას.

გარდა ზემოაღნიშნულისა, NIS დირექტივა ასევე ითვალისწინებს გარკვეულ ვალდებულებებს ციფრული სერვისის მიმწოდებლებისთვისაც.[26] დირექტივის მიზნებისათვის ციფრული მომსახურების მიმწოდებელს წარმოადგენენ ონლაინ საძიებო სისტემები, ე.წ. „ქლაუდ-კომპიუტინგის“ სერვისები და ონლაინ გაყიდვები.[27] სამივე სექტორის

[22] იხ. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, მუხლი 14 (1).

[23] იხ. იქვე, მუხლი 14 (4). ინციდენტის განსაკუთრებული გავლენის შეფასებისას მხედველობაში მიიღება შემდეგი კრიტერიუმკები: ა) სასიცოცხლოდ მნიშვნელოვანი სერვისის შეწყვეტის შედეგად დაზარალებულ მომხმარებელთა რიცხვი; ბ) ინციდენტის ხანგრძლივობა და გ) ინციდენტის გავრცელების გეოგრაფიული არეალი.

[24] იხ. იქვე, მუხლი 14 (3).

[25] ავთენტურობა, მთლიანობა და კონფიდენციალურობა (Confidentiality, Integrity, & Availability, CIA) წარმოადგენენ კიბერუსაფრთხოების საჭიროებების მთავარ ელემენტებს.

[26] NIS დირექტივა იყენებს ტერმინს: „Digital Service Provider“.

[27] NIS დირექტივა (დანართი III) გამოყოფს 3 მათგანს: 1. online marketplace; 2. Online search engine და 3. Cloud computing service. „ტექნიკური რეგლამენტებისა და საინფორმაციო საზოგადოების მომსახურების წესების შესახებ ინფორმაციის მიწოდების პროცედურის (კოდიფიკაცია) დადგენის შესახებ“ დირექტივის (Directive (EU) 2015/1535) თანახმად, ციფრულ სერვისად მიიჩნევა ნებისმიერი

ფუნქციონირება მნიშვნელოვან როლს თამაშობს ევროპის შიდა ბაზრის განვითარების საქმეში.[28]

ერთი შეხედვით, ციფრული სერვისის მიმწოდებლები ამავე დროს სასიცოცხლოდ მნიშვნელოვანი სერვისების მიმწოდებლებსაც უწევენ მომსახურებას და ლოგიკურია, რომ ისინი არ უნდა ექცეოდნენ უფრო მკაცრი რეგულირების ქვეშ, ვიდრე - ეს უკანასკნელნი, თუმცა არაერთხელ გაჟღერდა საწინააღმდეგო მოსაზრებაც.[29] NIS დირექტივას შემოაქვს „მსუბუქი მიდგომის კონცეფცია“,[30] თუმცა მაინც ტოვებს გარკვეულ ადგილს სხვაგვარი ინტერპრეტაციისთვის - რამდენად არის უფლებამოსილი ევროპის კავშირის წევრი ქვეყნის საზედამხედველო ორგანო, ციფრული მომსახურების მიმწოდებლებსაც გაუწიოს ზედამხედველობა? ევროპის კიბერუსაფრთხოების სააგენტოს (ENISA) მოსაზრებით, საჭიროების შემთხვევაში, საზედამხედველო ორგანოს აქვს შესაძლებლობა, ციფრული მომსახურების მიმწოდებლებსაც გაუწიოს ზედამხედველობა, თუმცა მათ მიმართ შედარებით მსუბუქი ვალდებულებებია დადგენილი, რაც გამორიცხავს ოპერირებაში ხელის შეშლას.[31]

წევრ სახელმწიფოებს ევალებათ, უზრუნველყონ, რომ ციფრული სერვისის მიმწოდებლებმა აცნობონ საზედამხედველო ორგანოს ან CSIRT-ს ყოველგვარი ინციდენტის შესახებ, რომელიც არსებით გავლენას მოახდენს მათ მიერ კავშირის ფარგლებში მიწოდებულ სერვისზე.[32]

2.2 ევროპის კავშირის წევრი სახელმწიფოების კიბერშესაძლებლობების გაძლიერება

სერვისი, რომელიც ჩვეულებრივ უზრუნველყოფილია ანაზღაურებით, დისტანციურად, ელექტრონული საშუალებებითა და მომსახურების მიმღების ინდივიდუალური მოთხოვნით.

[28] ENISA, Incident Notification for DSPs in the context of NIS Directive: A comprehensive guideline on how to implement incident notification for Digital Service Providers, in the context of the NIS Directive, 2017, 11.

[29] იხ. იქვე, 9.

[30] გამოყენებულია ტერმინები: „light-touch and reactive ex post supervisory activities“. იხ. Directive (EU) 2016/1148, პრეამბულა, §. 60.

[31] იხ. ENISA, Incident Notification for DSPs in the context of NIS Directive: A comprehensive guideline on how to implement incident notification for Digital Service Providers, in the context of the NIS Directive, 2017, 10.

[32] იხ. Directive (EU) 2016/1148, მუხლი 16 (3), შეტყობინებები უნდა შეიცავდეს ინფორმაციას, რომელიც საშუალებას მისცემს კომპეტენტურ ორგანოს ან CSIRT-ს დაადგინოს ნებისმიერი ტრანსსასაზღვრო ზემოქმედების მნიშვნელობა.

დირექტივის თანახმად, წევრ სახელმწიფოებს აქვთ ვალდებულება, შემუშავებული ჰქონდეთ ეროვნული სტრატეგია კიბერუსაფრთხოების სფეროში,[33] რაც არ არის მარტივი ამოცანა განსხვავებული კულტურისა და მიდგომების მქონე ევროპული სახელმწიფოებისათვის.[34]

სტრატეგია უნდა მოიცავდეს შემდეგ საკითხებს:

ა) სტრატეგიული მიზნები, პრიორიტეტები და მმართველობითი ჩარჩო;

ბ) მზადყოფნის, რეაგირებისა და აღდგენის ღონისძიებები;

გ) საჯარო-კერძო პარტნიორობის მეთოდოლოგია;

დ) ცნობიერების ამაღლება, ტრენინგები და სწავლება;

ე) კვლევითი კომპონენტები;

ვ) რისკების შეფასების გეგმა;

ზ) სტრატეგიის იმპლემენტაციაში ჩართული აქტორების ჩამონათვალი.[35]

წევრი სახელმწიფოები ასევე განსაზღვრავენ „ერთიან საკონტაქტო პუნქტს“, რომელიც განახორციელებს მეკავშირის ფუნქციას სხვა წევრი სახელმწიფოების შესაბამის ორგანოებთან და თავად დირექტივით შექმნილ თანამშრომლობის მექანიზმებთან თანამშრომლობის უზრუნველსაყოფად.[36]

კიდევ ერთი ვალდებულება, შეიქმნას ინსტუტუციური ხასიათის ერთეული, შეეხება კომპიუტერული უსაფრთხოების ინციდენტებზე რეაგირების ჯგუფს (CSIRT). აღნიშნული რეაგირების ჯგუფი, პირველ რიგში, მონიტორინგს უწევს ეროვნულ დონეზე უსაფრთხოების ინციდენტებს და ახდენს მათზე რეაგირებას. ამ პროცესში დახმარების ჯგუფის მოვალეობაა,

[33] იხ. Directive (EU) 2016/1148, მუხლი 7.

[34] ევროპის კიბერუსაფრთხოების სააგენტოს (ENISA) გამოცდილება ცხადყოფს, რომ ეროვნულ-კულტურული განსხვავებები წარმოადგენენ დაბრკოლებას ამ თვალსაზრისით სახელმწიფოთა თანამშრომლობის საქმეში. დეტალებისათვის იხ. *OECD*, Roles and Responsibilities of Actors for Digital Security, OECD Digital Economy Papers, July 2019, №286, 19-20.

[35] იხ. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, მუხლი 7 (1).

[36] იხ. იქვე, მუხლი 8 (3), (4).

დროულად გააფრთხილოს ყველა ჩართული მხარე ინციდენტისა და მისგან გამოწვეული რისკების თაობაზე.[37]

დირექტივის საფუძველზე შეიქმნა თანაშრომლობის ჯგუფი,[38] რათა ჩამოყალიბდეს ნდობა, შედგეს სტარტეგიული თანამშრომლობა და ინფორმაციის გაცვლა წევრ სახელმწიფოებს შორის კიბერუსაფრთხოების საკითხებზე. თანამშრომლობის ჯგუფის შემადგენლობაში შედიან ევროკომისიისა და ევროპის ქსელისა და ინფორმაციული უსაფრთხოების სააგენტოს (ENISA) წარმომადგენლებიც. აღნიშნულ ჯგუფში წევრი ქვეყნები ცვლიან ინფორმაციას და თანხმდებიან იმაზე, დირექტივის იმპლემენტაციის საკითხებზე ევროპის კავშირის მასშტაბით.[39] როგორც წესი, თანამშრომლობის ჯგუფის წევრები არიან ეროვნული სამინისტროებისა და კიბერუსაფრთხოების ეროვნული სააგენტოების წარმომადგენლები.

ოპერაციულ დონეზე სწრაფი და ეფექტიანი თანამშრომლობის მიზნით, დირექტივამ ცალკე შექმნა ინციდენტებზე რეაგირების ჯგუფის (CSIRT) გაერთიანება,[40] რომელიც, ასევე, ნდობის ჩამოყალიბებას ისახავს მიზნად.

2.3 „NIS 2 დირექტივის“ პროექტი

დირექტივის მიმოხილვის ფონზე, მნიშვნელოვანია, აღინიშნოს, რომ 2020 წელს ევროკომისიამ წარადგინა ქსელისა და ინფორმაციული უსაფრთხოების დირექტივაში ცვლილების ამსახველი პროექტი, რომელიც NIS 2 დირექტივის სახელით[41] არის ცნობილი და მიზნად ისახავს მოქმედი დირექტივის ჩანაცვლებას.

---

[37] იხ. იქვე, მუხლი 9.

[38] NIS დირექტივა იყენებს ტერმინს „Cooperation Group“.

[39] იხ. დეტალური ინფორმაცია ჯგუფისა და მის მუშაობაში ENISA-ს ჩართულობის შესახებ ENISA-ს ოფიციალურ ვებგვერდზე: <ttps://www.enisa.europa.eu/topics/nis-directive> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 28.06.2022).

[40] NIS დირექტივა იყენებს ტერმინს „CSIRTs network“, მუხლი 12.

[41] იხ. ინფორმაცია NIS 2-ის შესახებ: <https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 28.06.2022).

2022 წლის მაისში მიღწეულ იქნა პოლიტიკური შეთანხმება ევროპულ პარლამენტსა და ევროპის კავშირის წევრ ქვეყნებს შორის NIS 2 დირექტივის თაობაზე.[42] წევრ სახელმწიფოებს NIS 2 დირექტივის ოფიციალურ ჟურნალში გამოქვეყნებიდან 21 თვე აქვთ დირექტივის ეროვნულ კანონმდებლობაში ტრანსპოზიციისათვის.

პირველ რიგში, აღნიშნული პროექტით ფართოვდება კრიტიკული სექტორების რაოდენობა და წევრ სახელმწიფოებს რჩებათ თავისუფლება, სასიცოცხლოდ მნიშვნელოვანი სერვისების გამწევი სუბიექტების სიაში შეიყვანონ მცირე ზომის, თუმცა მაღალი რისკების მქონე კომპანიები. ერთ-ერთი მნიშვნელოვანი განსხვავება მოქმედ დირექტივასთან მიმართებით სწორედ სექტორების არეალის გაფართოებაა, არსებულს ემატება კვების, წარმოების, საფოსტო და საკურიერო მომსახურების სფეროები, სახელმწიფო ელექტრონული კომუნიკაციების ქსელების ან სერვისების მიმწოდებლები, საჯარო დაწესებულებები, ციფრული სერვისები, თანამგზავრული სერვისები, ნარჩენი წყლისა და ნარჩენების მართვა. ასევე, მნიშვნელოვანია, რომ პროექტის ფარგლებში არ არსებობს რაიმე განსხვავება სასიცოცხლოდ მნიშვნელოვანი სერვისებისა და ციფრული სერვისების გამწევ სუბიექტებს შორის.[43]

NIS 2 დირექტივის პროექტი უფრო კომპლექსური ხასიათის უსაფრთხოების მოთხოვნებს ადგენს, მაგალითად, როგორიცაა ინციდენტებთან გამკლავებისა და კრიზისული სიტუაციის მართვის, შესყიდვებისა და მიწოდების ჯაჭვში კიბერუსართხოების მოთხოვნების გათვალისწინების ვალდებულება.

NIS 2 დირექტივის პროექტის პირობებში უმჯობესდება ფართომასშტაბიანი კიბერინციდენტების მართვა და პრევენცია.[44] ამგვარ ინციდენტებზე ეფექტიანი

[42] იხ. A proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive). დეტალური ინფორმაცია მოცემულია: <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 28.06.2022).

[43] იხ. European Parliament Briefing (EU Legislation in Progress), The NIS2 Directive - A high common level of cybersecurity in the EU, 7, ხელმისაწვდომია ევროპარლამენტის ოფიციალურ ვებგვერდზე: <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 25.06.2022).

[44] იხ. A proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive). დეტალური ინფორმაცია მოცემულია: <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 25.06.2022).

რეაგირებისათვის აუცილებელია სახელმწიფოთა მიერ ეროვნულ დონეზე მკაფიო პასუხისმგებლობების განსაზღვრა და ეფექტიანი თანამშრომლობა.

ევროპარლამენტის მიერ 2022 წლის ივნისში გამოქვეყნებული ინფორმაციის თანახმად, NIS დირექტივით გათვალისწინებული ზედამხედველობისა და აღსრულების რეჟიმი არცთუ ეფექტიანია. სახელმწიფოთა მიხედვით განსხვავებულია ის რესურსები, რომლებიც გამოყოფილია წევრი სახელმწიფოების მიერ დირექტივით გათვალისწინებული ამოცანების შესასრულებლად (როგორიცაა კრიტიკული სუბიექტების იდენტიფიცირება ან მათი ზედამხედველობა) და ცოდნის დონე კიბერუსაფრთხოების რისკებთან გამკლავების თვალსაზრისითაც. ცხადია, ეს ამძაფრებს წევრ სახელმწიფოების კიბერშესაძლებლობებს შორის სხვაობას.[45] ამდენად, პროექტი ყურადღებას ამახვილებს კიბერუსაფრთხოების რისკების მართვაზე[46] და ამავე დროს, მიზნად ისახავს კიბერუსაფრთხოების მოთხოვნების შესრულებისა და კიბერუსაფრთხოების ღონისძიებების განხორციელების კუთხით განსხვავებების აღმოფხვრას წევრ სახელმწიფოებში. პროექტი აყალიბებს მექანიზმებს თითოეულ წევრ სახელმწიფოში შესაბამის ორგანოებს შორის ეფექტური თანამშრომლობისთვის.[47] ის განაახლებს კიბერუსაფრთხოების ვალდებულებებს დაქვემდებარებული სექტორებისა და აქტივობების ჩამონათვალს და ითვალისწინებს დაცვის საშუალებებს და სანქციებს აღსრულების უზრუნველსაყოფად.

3. საქართველოს ინფორმაციული უსაფრთხოების სისტემის ცვლილება

3.1 ინფორმაციული უსაფრთხოების სფეროს რეფორმამდელი არქიტექტურა

2008 წლის რუსეთ-საქართველოს ომის[48] შემდეგ, ცხადი გახდა რა კიბერუსაფრთხოების სფეროს რეფორმის აუცილებლობა, 2011 წელს შეიქმნა კომპიუტერულ ინციდენტებზე

[45] იხ. European Parliament Briefing (EU Legislation in Progress), The NIS2 Directive - A high common level of cybersecurity in the EU, 6.

[46] პროექტში საუბარია კიბერუსაფრთხოების რისკების მართვის ღონისძიებებზე (cybersecurity risk management measures) და მათი გამოყენების აუცილებლობაზე.

[47] იხ. European Parliament Briefing (EU Legislation in Progress), The NIS2 Directive - A high common level of cybersecurity in the EU, 7.

[48] 2008 წლის აგვისტოში საქართველოს წინააღმდეგ რუსეთმა ფართომასშტაბიანი სამხედრო აგრესია წამოიწყო, რაც, ასევე მოიცავდა კრიტიკული სამთავრობო სისტემებისა და მედია

რეაგირების ჯგუფი საქართველოს იუსტიციის სამინისტროს საჯარო სამართლის იურიდიული პირის - მონაცემთა გაცვლის სააგენტოს ქვეშ.[49] ამავე წელს დაიწყო მუშაობა „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის შესაქმნელად.[50]

აღნიშნული კანონი საქართველოს პარლამენტმა 2012 წელს მიიღო[51] და ამ დროიდან დღემდე ის წარმოადგენს ინფორმაციული უსაფრთხოების სახელმწიფო პოლიტიკის განმსაზღვრელ ძირითად საკანონმდებლო ჩარჩოს.

2012 წლის 1 ივლიდიდან, როდესაც კანონი ამოქმედდა, მასში ძირეული ცვლილებების განხორციელებამდე - 2021 წლის 30 დეკემბრამდე - ინფორმაციული უსაფრთხოების სფეროს ზედამხედველ და სფეროს პოლიტიკის განმსაზღვრელ უწყებას წარმოადგენდა სსიპ - მონაცემთა გაცვლის სააგენტო (ამჟამად - სსიპ ციფრული მმართველობის სააგენტო). გამონაკლისის სახით, 2013 წელს შეიქმნა საქართველოს თავდაცვის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირი - კიბერუსაფრთხოების ბიურო, რომელსაც დაევალა თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემის სუბიექტების ზედამხედველობა.[52]

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მოქმედება ვრცელდება კრიტკული ინფორმაციული სისტემის სუბიექტებზე. აღნიშნულ სუბიექტებად

საშუალებების მიმართ კიბერშეტევების წარმოებას (სამეცნიერო წრეებსა და ლიტერატურაში აღნიშნული კვალიფიცირებულია, როგორც ერთ-ერთი პირველი კიბერ-ომი).

[49] „საჯარო სამართლის იურიდიული პირის - ციფრული მმართველობის სააგენტოს შექმნის შესახებ“ საქართველოს კანონის საფუძველზე, რეორგანიზებულ იქნა საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირი – მონაცემთა გაცვლის სააგენტო და საჯარო სამართლის იურიდიული პირი – „სმართ ლოჯიქი“ (SMART LOGIC) და მათი ერთმანეთთან შერწყმის შედეგად, 2020 წელს შეიქმნა საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირი – ციფრული მმართველობის სააგენტო. საჯარო სამართლის იურიდიული პირი – ციფრული მმართველობის სააგენტო არის საჯარო სამართლის იურიდიული პირების – მონაცემთა გაცვლის სააგენტოს და „სმართ ლოჯიქის“ (SMART LOGIC) უფლებამონაცვლე.

[50] იხ. *მალვენიშვილი მ., გალარჯიშვილი ნ.,* კიბერუსაფრთხოების რეფორმა საქართველოში: არსებული გამოწვევები, საერთაშორისო პრაქტიკა და რეკომენდაციები, თბილისი, 2020, 10.

[51] იხ. საქართველოს საკანონმდებლო მაცნე (www.matsne.gov.ge), 19/06/2012, სარეგისტრაციო კოდი: 140000000.05.001.016807.

[52] იხ. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ 2013 წლის 24 დეკემბრის კანონი, საქართველოს საკანონმდებლო მაცნე (www.matsne.gov.ge), 28/12/2013, სარეგისტრაციო კოდი: 140000000.05.001.017260.

2021 წელს განხორციელებულ საკანონმდებლო ცვლილებებამდე იდენტიფიცირებულნი იყვნენ მხოლოდ სახელმწიფო დაწესებულებები. სახელმწიფო ორგანო ან იურიდიული პირი, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანი იყო ქვეყნის თავდაცვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისათვის, საქართველოს მთავრობის გადაწყვეტილებით[53] ირიცხებოდა შესაბამის ნუსხაში. თავის მხრივ, ნუსხის შედგენისას მხედველობაში უნდა მიღებულიყო შემდეგი კრიტერიუმები:

ა) ინფორმაციული სისტემის შეფერხების ან მწყობრიდან გამოსვლის სავარაუდო შედეგების სიმძიმე და მასშტაბი;

ბ) სავარაუდო ეკონომიკური ზარალის სიმძიმე სუბიექტებისთვის ან/და სახელმწიფოსთვის;

გ) ინფორმაციული სისტემის მიერ გაწეული მომსახურების აუცილებლობა საზოგადოების ნორმალური ფუნქციონირებისათვის;

დ) ინფორმაციული სისტემის მომხმარებელთა რაოდენობა;

ე) სუბიექტის მატერიალური მდგომარეობა და სავარაუდო ხარჯების ოდენობა, რომლებიც მისთვის ამ კანონიდან გამომდინარე ვალდებულებების დაკისრებას მოჰყვებოდა.

„კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ“ საქართველოს მთავრობის 2014 წლის 29 აპრილის №312 დადგენილების[54] საფუძველზე, 39 ასეთი ორგანიზაცია იყო განსაზღვრული (მათ შორის, სხვადასხვა სამინისტრო და საჯარო სამართლის იურიდიული პირი).

კანონის საფუძველზე, 2013 წელს მაშინდელმა მონაცემთა გაცვლის სააგენტომ შეიმუშავა ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები,[55] რომელიც

[53] პროექტი საქართველოს მთავრობას დასამტკიცებლად წარედგინებოდა საქართველოს იუსტიციის სამინისტროს მიერ, საქართველოს თავდაცვისა და შინაგან საქმეთა სამინისტროებთან და საქართველოს სახელმწიფო უსაფრთხოების სამსახურთან შეთანხმებით.

[54] ძალადაკარგულად გამოცხადდა „პირველი, მეორე და მესამე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების ნუსხის დამტკიცების შესახებ“ საქართველოს მთავრობის 2021 წლის 31 დეკემბრის №646 დადგენილებით.

[55] „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ მონაცემთა გაცვლის სააგენტოს თავმჯდომარის 2013 წლის 4 თებერვლის №2 ბრძანება, რომელიც მოგვიანებით ძალადაკარგულად გამოცხადდა „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის 2020 წლის

ითვალისწინებდა სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO)[56] სტანდარტის (ISO 27000)[57] განხორციელების საუკეთესო პრაქტიკას. შესაბამისად, კრიტიკული ინფორმაციული სისტემის სუბიექტებს ევალებოდათ, ერთი მხრივ, შეემუშავებინათ ინფორმაციული უსაფრთხოების პოლიტიკა სწორედ მინიმალურ მოთხოვნებზე დაყრდნობით, ხოლო, მეორე მხრივ, ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესები განსახილველად წარედგენათ მონაცემთა გაცვლის სააგენტოსათვის.[58] ეს უკანასკნელი, მოწოდებული დოკუმენტების ზოგადი ანალიზის საფუძველზე, სუბიექტს წარუდგენდა რეკომენდაციებს მათში აღმოჩენილი ხარვეზების გამოსასწორებლად.[59] კრიტიკული ინფორმაციული სისტემის სუბიექტის სხვა ვალდებულებას წარმოადგენდა ინფორმაციული აქტივების აღწერა და მათი მართვა დადგენილი წესის შესაბამისად,[60] ინფორმაციული უსაფრთხოების აუდიტის ჩატარება[61] და ინფორმაციული უსაფრთხოების მენეჯერის დანიშვნა.[62]

რაც შეეხება კიბერუსაფრთხოების უზრუნველყოფას, მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის - CERT.GOV.GE - უმთავრეს მოვალეობას წარმოადგენდა საქართველოს კიბერსივრცეში ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვა.

აქვე, აუცილებლად უნდა აღინიშნოს „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის აღსრულებასთან დაკავშირებული საკითხიც - 10 ივნისის საკანონმდებლო ცვლილებებამდე, კანონი არ შეიცავდა აღსრულების ეფექტიან მექანიზმებს,

---

16 ოქტომბრის №4 ბრძანებით. თავის მხრივ, ეს უკანასკნელი ძალადაკარგულად გამოცხადდა „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დადგენის შესახებ“ შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის 2021 წლის 14 დეკემბრის №1 ბრძანებით.

[56] იხ.: <https://www.iso.org/> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 10.06.2022).

[57] აღნიშნული წარმოადგენს სტანდარტების სერიას ინფორმაციული სისტემის მართვის სისტემისათვის. იხ. დეტალური ინფორმაცია შემდეგ ელექტრონულ რესურსზე: <https://www.iso.org/news/ref2266.html>.

[58] იხ. საქართველოს საკანონმდებლო მაცნე (www.matsne.gov.ge), 19/06/2012, სარეგისტრაციო კოდი: 140000000.05.001.016807, მე-4 მუხლი.

[59] იხ. იქვე.

[60] იხ. იქვე, მე-5 მუხლი.

[61] იხ. იქვე, მე-6 მუხლი.

[62] იხ. იქვე, მე-7 მუხლი.

კერძოდ, მონაცემთა გაცვლის სააგენტოს მხოლოდ წერილობითი ხასიათის რეკომენდაციებისა და მითითებების გაცემის უფლებამოსილება გააჩნდა.[63] აღნიშნულის გამო, ბუნებრივია, პრაქტიკაში კიბერუსაფრთხოების მოთხოვნების შესრულება გამოწვევის წინაშე დგებოდა და საბოლოო ჯამში, საფრთხეს უქმნიდა კიბერუსაფრთხოების გარემოს მდგრადობას,[64] ფართომასშტაბიანი ინციდენტების პრევენციასა და მათ მოგერიებას. ფაქტობრივად, საჭირო იყო ერთიანი სახელმწიფო პოლიტიკის შემუშავება, საკანონმდებლო ჩარჩოს დახვეწა და აღსრულების შესაბამისი მექანიზმების შექმნა გრძელვადიანი შედეგის მისაღწევად. ამ თვალსაზრისით, საინტერესოა გაეროს საერთაშორისო სატელეკომუნიკაციო ორგანიზაციის (ITU) მიერ წარმოებული გლობალური კიბერუსაფრთხოების ინდექსის (GCI)[65] გაანალიზება, სადაც 2017 წელს საქართველო წამყვან ქვეყნებს შორის დასახელდა, თუმცა მოგვიანებით, სწორედ სისტემური და ერთგვაროვანი მიდგომების არარსებობის გამო, მან ვერ უზრუნველყო მოწინავე პოზიციების შენარჩუნება.[66]

გარდა ციფრული მმართველობის სააგენტოსა, როგორც აღინიშნა, თავდაცვის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირი - კიბერუსაფრთხოების ბიურო თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემის

---

[63] საქართველოს სახელმწიფო აუდიტის სამსახურის რეკომენდაციით, მონაცემთა გაცვლის სააგენტოს (ამჟამად, ციფრული მმართველობის სააგენტოს) მიენიჭოს დამატებითი უფლებამოსილება ინფორმაციული უსაფრთხოების საკანონმდებლო მოთხოვნების შესრულების უზრუნველსაყოფად, მათ შორის, კრიტიკული ინფორმაციული სისტემის სუბიექტების მიმართ სანქციის გამოყენების შესაძლებლობა. დამატებით იხ. *მალვენიშვილი მ., ბალარჯიშვილი ნ.,* კიბერუსაფრთხოების რეფორმა საქართველოში: არსებული გამოწვევები, საერთაშორისო პრაქტიკა და რეკომენდაციები, თბილისი, 2020, 17.

[64] 2017 წლის ინდექსში საქართველო იკავებს მე-8 ადგილს მსოფლიოში და მოიაზრება ლიდერ ქვეყანად კიბერუსაფრთხოების სფეროში. იხ. GCI, 2017: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 28.06.2022).

[65] GCI-ს ფარგლებში ქვეყანა ფასდება ტექნიკური, ორგანიზაციული, სამართლებრივი, შესაძლებლობების განვითარებისა და თანამშრომლობის მიმართულებებში, შესაბამისი მეთოდოლოგიის გამოყენებით, იხ. დეტალურად მეთოდოლოგიის თაობაზე: <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 28.06.2022).

[66] იხ. გაეროს საერთაშორისო სატელეკომუნიკაციო ორგანიზაციის (ITU) მიერ წაროებული გლობალური კიბერუსაფრთხოების 2021 წლის ინდექსი, სადაც საქართველოს 55-ე ადგილი უჭირავს მსოფლიოში, ხოლო 30-ე - ევროპაში: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 28.06.2022).

სუბიექტების ზედამხედველობას ახორციელებს. ბიუროს ეს მანდატი 2021 წლის 10 ივნისის ცვლილებების შემდეგაც თავდაპირველი სახით შენარჩუნდა.

რაც შეეხება კიბერდანაშაულის გამოძიებას, საქართველოს შინაგან საქმეთა სამინისტროს ცენტრალური კრიმინალური პოლიციის დეპარტამენტში შეიქმნა კიბერდანაშაულთან ბრძოლის სამმართველო, რომელსაც ევალება კიბერ სივრცეში ჩადენილი მართლსაწინააღმდეგო ქმედებების გამოვლენა, აღკვეთა და პრევენცია.[67]

3.2 2021 წლის 10 ივნისის საკანონმდებლო ცვლილებების საპარლამენტო განხილვა

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის შესახებ“ საქართველოს კანონის პროექტი საქართველოს პარლამენტის წევრმა ჯერ კიდევ 2019 წლის ოქტომბერში დაარეგისტრირა[68] საქართველოს პარლამენტში. აღნიშნული პროექტის განმარტებითი ბარათის თანახმად, კანონპროექტის მიღება აუცილებელი იყო ინფორმაციული უსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განხორციელების შედეგად გამოვლენილი ხარვეზების აღმოფხვრისა და ასევე ინფორმაციული უსაფრთხოების და კიბერუსაფრთხოების სფეროში სახელმწიფო უსაფრთხოების სამსახურის მმართველობის სფეროში შემავალი საჯაროსამართლის იურიდიული პირის - საქართველოს ოპერატიულ-ტექნიკური სააგენტოს კომპეტენციის განსაზღვრის მიზნით.[69]

აღნიშნული საკანონმდებლო ცვლილებების მიერ საპარლამენტო მოსმენის რეჟიმში განვლილი გზა მნიშვნელოვანია ცვლილებების და მისით გამოწვეული გავლენის

[67] იხ. ინფორმაცია კიბერდანაშაულის შესახებ შსს-ს ოფიციალურ ვებგვერდზე: <https://police.ge/files/proeqtebi_reporma%20photos/organizebuli-danashauli/kiberdanashauli-informacia-moqalaqeebistvis.pdf> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 10.06.2022).

[68] იხ. საქართველოს პარლამენტის წევრ ირაკლი სესიაშვილის ინიციატივა, კანონპროექტი №07-3/401, ხელმისაწვდომია საქართველოს პარლამენტის ოფიციალურ ვებგვერდზე: <https://parliament.ge/legislation/18874> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 04.06.2022).

[69] იხ. საქართველოს პარლამენტის წევრ ირაკლი სესიაშვილის მიერ ინიცირებული კანონპროექტის განმარტებითი ბარათი, ხელმისაწვდომია საქართველოს პარლამენტის ოფიციალურ ვებგვერდზე: <https://info.parliament.ge/file/1/BillReviewContent/232432> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 04.06.2022).

შესაფასებლად. საქართველოს პარლამენტის 2020 წლის 18 მარტის №5819-IIს დადგენილების[70] თანახმად, „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის შესახებ“ საქართველოს კანონის პროექტი მიღებულ იქნა პირველი მოსმენით. მოგვიანებით, იურიდიულ საკითხთა კომიტეტის, რომელიც ამ შემთხვევაში წარმოადგენდა წამყვან კომიტეტს, პარლამენტის ბიუროსადმი 2020 წლის 6 აპრილს მიწერილ წერილში[71] ვკითხულობთ, რომ კანონპროექტის მეორე მოსმენით კომიტეტის სხდომაზე განხილვა, ობიექტური მიზეზებიდან გამომდინარე, ვერ ხერხდება რეგლამენტით დადგენილ ვადაში. შესაბამისად, კომიტეტმა მოითხოვა კანონპროექტის განხილვის ვადის 3 თვით გაგრძელება.

2020 წლის 29 მაისით დათარიღებულ კანონპროექტში ჯერ კიდევ არ არის ასახული ეროვნული ბანკის როლის თაობაზე.[72] ამ ვერსიაში დაკონკრეტდა კომპიუტერული ინციდენტისა და ქსელური სენსორის განმარტებები, ასევე ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებისადმი დადგენილი სტანდარტები, ჩამოყალიბდა ინფორმაციული უსაფრთხოების პირველადი და პერიოდული აუდიტისა და პენეტრაციის ტესტის ჩატარების ვალდებულების თაობაზე მითითებები და სხვა.[73] 2020 წლის 12 ივნისს ეყარა კენჭი კანონპორექტს II მოსმენით,[74] რასთან დაკავშირებითაც პარლამენტმა იმავე დღეს გამოსცა №6306-IIს დადგენილება.[75] საქართველოს პარლამენტის იურიდიულ საკითხთა კომიტეტმა

---

[70] ხელმისაწვდომია საქართველოს პარლამენტის ოფიციალურ ვებგვერდზე: <https://info.parliament.ge/file/1/BillReviewContent/248981> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 04.06.2022).

[71] იხ. იურიდიულ საკითხთა კომიტეტის 2020 წლის 6 აპრილის №2-4818/20 წერილი, ხელმისაწვდომია საქართველოს პარლამენტის ოფიციალურ ვებგვერდზე: <https://info.parliament.ge/file/1/BillReviewContent/246973> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 04.06.2022).

[72] იხ. II მოსმენაზე დაფიქსირებული კანონპროექტის ვერსია, ხელმისაწვდომია საქართველოს პარლამენტის ოფიციალურ ვებგვერდზე: <https://info.parliament.ge/file/1/BillReviewContent/249559>. აგრეთვე, დამატებით იხ. შენიშვნების ფურცელი, ხელმისაწვდომია საქართველოს პარლამენტის ოფიციალურ ვებგვერდზე: <https://info.parliament.ge/file/1/BillPackageContent/26967> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 04.06.2022).

[73] იხ. იქვე.

[74] იხ. კენჭისყრის ანგარიში, ხელმისაწვდომია საქართველოს პარლამენტის ოფიციალურ ვებგვერდზე: <https://info.parliament.ge/file/1/BillReviewContent/252490> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 04.06.2022).

[75] იხ. საქართველოს პარლამენტის 2020 წლის 12 ივნისის №6306-IIს დადგენილება, ხელმისაწვდომია საქართველოს პარლამენტის ოფიციალურ ვებგვერდზე:

2020 წლის 22 ივნისის კომიტეტის სხდომაზე მესამე მოსმენით განიხილა კანონპროექტი, თუმცა აქ ყურადღებას იქცევს ერთი გარემოება - კომიტეტის დასკვნაში აღნიშნულია, რომ კომიტეტი, ერთი მხრივ, დადებითად აფასებს კანონის პროექტით გათვალისწინებულ საკანონმდებლო ცვლილებებს, თუმცა, მეორე მხრივ, კომიტეტის სხდომაზე მომხსენებლმა აღნიშნა, რომ მიზანშეწონილია მასში ისეთი შინაარსის ცვლილებების შეტანა, რომლებიც კანონის პროექტის მესამე მოსმენით დროს ვერ განხორციელდება. კომიტეტის დასკვნაში მითითებული არ არის, რა სახის ცვლილებაზეა საუბარი, თუმცა მან აუცილებელად მიიჩნია კანონის პროექტის მესამე მოსმენიდან მეორე მოსმენით განხილვისთვის დაბრუნება.[76] 2020 წლის 23 ივნისს პარლამენტმა კენჭი უყარა ამ კანონპროექტის მესამე მოსმენიდან მეორე მოსმენაზე დაბრუნების საკითხს,[77] მომხსენებელმა კენჭისყრამდე განმარტა, რომ თავად ჰქონდა მოტივირებული შენიშვნები, რასაც მხარს უჭერდა იურიდიულ საკითხთა კომიტეტი და სწორედ ამის გამო ითხოვდა პროექტის მეორე მოსმენის ეტაპზე დაბრუნებას.[78]ამ შემთხვევაშიც არ ყოფილა მომხსენებლის მიერ დაკონკრეტებული, თუ რა სახის შენიშვნების გამო მიიჩნიეს მიზანშეწონილად პროექტის დაბრუნება.[79]

<https://info.parliament.ge/file/1/BillReviewContent/256153> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 04.06.2022).

[76] იხ. იურიდიულ საკითხთა კომიტეტის 2020 წლის 23 ივნისის №2-6666/20 დასკვნა „საქართველოს კანონის პროექტზე „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ (N07-3/401; 02.10.2019)“, ხელმისაწვდომია საქართველოს პარლამენტის ოფიციალურ ვებგვერდზე: <https://info.parliament.ge/file/1/BillReviewContent/263128> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 04.06.2022).

[77] იხ. კენჭისყრის ანგარიში, ხელმისაწვდომია საქართველოს პარლამენტის ოფიციალურ ვებგვერდზე: <https://info.parliament.ge/file/1/BillReviewContent/254442> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 04.06.2022).

[78] იხ. პროექტის განხილვის აუდიოჩანაწერი, ხელმისაწვდომია საქართველოს პარლამენტის ოფიციალურ ვებგვერდზე: <https://info.parliament.ge/file/1/BillReviewContent/254712> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 04.06.2022).

[79] იხ. საქართველოს პარლამენტის 2020 წლის 23 ივნისის №6365-IIს დადგენილება „საქართველოს პარლამენტის წევრის, ირაკლი სესიაშვილის, მიერ საკანონმდებლო ინიციატივის წესით წარმოდგენილი (N07-3/401; 02.10.2019) „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ საქართველოს კანონის პროექტის მესამე მოსმენიდან მეორე მოსმენით პლენარულ სხდომაზე განხილვისათვის დაბრუნების შესახებ“, ანგარიში, ხელმისაწვდომია საქართველოს პარლამენტის ოფიციალურ ვებგვერდზე:

ინფორმაციული უსაფრთხოების სფეროში ეროვნული ბანკის მანდატის თაობაზე მითითება აისახა კანონპროექტის 2020 წლის 1 სექტემბრის ვერსიაში.[80] იურიდიულ საკითხთა კომიტეტის დასკვნაში,[81] ყოველგვარი დასაბუთების გარეშე, აღნიშნულია მხოლოდ ის, რომ კომიტეტი დადებითად აფასებს კომერციულ ბანკებთან მიმართებით, ინფორმაციული უსაფრთხოების უზრუნველყოფის თვალსაზრისით, გარკვეული უფლებამოსილებების საქართველოს ეროვნული ბანკისთვის მინიჭებას.

საბოლოო ჯამში, 2021 წლის 15 თებერვალს გამოიცა პარლამენტის ბიუროს გადაწყვეტილება,[82] ხოლო 18 თებერვალს - საქართველოს პარლამენტის დადგენილება[83] კანონპროექტის განხილვის პროცედურის დაწყების შესახებ და ამგვარად, ახალი მოწვევის პარლამენტმა დაიწყო წინა მოწვევის პარლამენტის მიერ დაწყებული კანონპროექტის განხილვა. საბოლოო რედაქტირებულ ვარიანტს საქართველოს პარლამენტმა 2021 წლის 10 ივნისს უყარა კენჭი.[84]

<https://info.parliament.ge/file/1/BillReviewContent/255948> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 04.06.2022).

[80] იხ. მეორე მოსმენის ეტაპზე დაბრუნებული პროექტის პირველი მუხლი, ხელმისაწვდომია საქართველოს პარლამენტის ოფიციალურ ვებგვერდზე: <https://info.parliament.ge/file/1/BillReviewContent/262039> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 04.06.2022).

[81] იხ. იურიდიულ საკითხთა კომიტეტის 2020 წლის 31 აგვისტოს №2-8902/20 დასკვნა „საქართველოს კანონის პროექტზე „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ (N07-3/401; 02.10.2019), ხელმისაწვდომია საქართველოს პარლამენტის ოფიციალურ ვებგვერდზე: <https://info.parliament.ge/file/1/BillReviewContent/262034> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 04.06.2022).

[82] იხ. საქართველოს პარლამენტის ბიუროს 2021 წლის 15 თებერვლის №23/6 გადაწყვეტილება „ნორმატიული აქტის პროექტის განხილვის პროცედურის დაწყების შესახებ“, ხელმისაწვდომია საქართველოს პარლამენტის ოფიციალურ ვებგვერდზე: <https://info.parliament.ge/file/1/BillReviewContent/268827> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 04.06.2022).

[83] ხელმისაწვდომია საქართველოს პარლამენტის ოფიციალურ ვებგვერდზე: <https://info.parliament.ge/file/1/BillReviewContent/269686> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 04.06.2022).

[84] იხ. კენჭისყრის ანგარიში, ხელმისაწვდომია საქართველოს პარლამენტის ოფიციალურ ვებგვერდზე: <https://info.parliament.ge/file/1/BillReviewContent/275887> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 04.06.2022).

3.3 2021 წლის 10 ივნისის საკანონმდებლო ცვლილებების ძირითადი ასპექტები

ცვლილებები, პირველ რიგში, შეეხო კიბერ და ინფორმაციული უსაფრთხოების მმართველობით მოდელს. ნაცვლად სსიპ ციფრული მმართველობის სააგენტოსა, რომელიც საჯარო სექტორში არსებულ კრიტიკული ინფორმაციული სისტემის სუბიექტებს უწევდა ზედამხედველობას, კანონპროექტის შედეგად, გაჩნდა კიდევ ერთი ზედამხედველი უწყება - საქართველოს ოპერატიულ-ტექნიკური სააგენტოს სახით.

ბუნებრივია, მხოლოდ ფაქტი, რომ კიბერუსაფრთხოების სფეროში ახალი სახელმწიფო აქტორი გამოჩნდა, არ გვაძლევს საკმარის საფუძველს დასკვნებისათვის მაშინ, როდესაც ეროპული დირექტივაც შესაძლებლად მიიჩნევს ერთდროულად რამდენიმე საზედამხედველო ორგანოს არსებობას. ამ შემთხვევაში, უფრო მნიშვნელოვანია საქართველოს ოპერატიულ-ტექნიკური სააგენტოს სხვა უფლებამოსილების განხილვა-შეფასება და მათში შესაძლო კონფლიქტის ძიება. აღნიშნული სააგენტო შედის საქართველოს სახელმწიფო უსაფრთხოების სამსახურის მმართველობის სფეროში და მას მთელი რიგი ფარული საგამოძიებო მოქმედებების ჩატარების ქსკლუზიური უფლებამოსილება გააჩნია.[85] სააგენტოს ამოცანას წარმოადგენს სპეციალური ტექნოლოგიური საშუალებებით, ფარული მეთოდებით ქვეყნის კონსტიტუციური წყობილების, სუვერენიტეტის, თავდაცვისუნარიანობის, ტერიტორიული მთლიანობის, მართლწესრიგისა და სამხედრო პოტენციალის წინააღმდეგ მიმართულ ქმედებათა შესახებ ინფორმაციის მოპოვება, აგრეთვე სისხლის სამართლის საქმეზე ფაქტობრივი მონაცემების მოპოვება და ამ მიზნით ისეთ ღონისძიებათა განხორციელება, როგორიცაა ფარული მიყურადებაი და ჩაწერა, კომპიუტერული სისტემიდან ინფორმაციის მოპოვება[86] და სხვა. 2016 წელს საქართველოს საკონსტიტუციო სასამართლომ სწორედ სახელმწიფო უსაფრთხოების სამსახურთან მიმართებით დაადგინა კონსტიტუციით გარანტირებული პიროვნების თავისუფალი განვითარებისა და პირადი ცხოვრების ხელშეუხებლობის უფლებების დარღვევა, რადგანაც სახელმწიფო უსაფრთხოების სამსახური

[85] *კუკავა ქ., ახალაძე ნ., ჩხაიძე ს.,* ფარული მიყურადება საქართველოში - კანონმდებლობისა და პრაქტიკის ანალიზი, თბილისი, 2020, 8.

[86] იხ. „საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონი, საქართველოს საკანონმდებლო მაცნე (www.matsne.gov.ge), 27/03/2017, სარეგისტრაციო კოდი: 040030000.05.001.018374.

მიიჩნია „გამოძიებაზე პასუხისმგებელ და პროფესიულად დაინტერესებულ ორგანოდ“, რომლის მიერ დიდი ოდენობით ინფორმაციის ფლობა, „...ასეთი ინფორმაციის კონფიდენციალურობის და ხელშეუხებლობის მყარი, საკმარისი და ეფექტური გარანტიების არარსებობის პირობებში წარმოადგენს ... გაუმართლებლად ინტენსიურ ჩარევას...“.[87] 2021 წლის 10 ივნისის ცვლილებების შედეგად, ოპერატიულ-ტექნიკურ სააგენტოს აქვს სახელმწიფო სექტორში არსებული კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების პირველადი აუდიტისა და პენეტრაციის (შეღწევადობის) ტესტის ჩატარების უფლებამოსილება. მისი ეს უფლებამოსილება, შესაძლოა, გავრცელდეს ელექტრონული კომუნიკაციის კომპანიებზეც, ამ უკანასკნელთა გადაწყვეტილებით.[88] კრიტიკული ინფორმაციული სისტემის სუბიექტი კომპიუტერული ინციდენტის იდენტიფიცირების მიზნით იყენებს ქსელურ სენსორს - აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებების ერთობლიობას, რომელიც გამიზნულია ქსელური ნაკადის მონიტორინგისთვის, ინფორმაციული სისტემის წინააღმდეგ მიმართული კომპიუტერული ინციდენტის გამოსავლენად.[89] ოპერატიულ-ტექნიკური სააგენტო ასევე, განსაზღვრავს ქსელური სენსორის კონფიგურირების წესებს. აქვე, კანონში ხაზგასმულია, რომ ამ შემთხვევაში ოპერატიულ-ტექნიკური სააგენტოს მიერ კომუნიკაციის შინაარსობრივი მონაცემის ხელმისაწვდომობის შესაძლებლობა უნდა გამოირიცხოს. სამწუხაროდ, ქსელური სენსორის კონფიგურირების წესები ამ დრომდე არ არის გამოქვეყნებული საქართველოს

[87] იხ. საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის №1/1/625,640 გადაწყვეტილება საქმეზე საქართველოს სახალხო დამცველი, საქართველოს მოქალაქეები – გიორგი ბურჯანაძე, ლიკა საჯაია, გიორგი გოცირიძე, თათია ქინქლაძე, გიორგი ჩიტიძე, ლაშა ტუღუში, ზვიად ქორიძე, ააიპ „ფონდი ღია საზოგადოება საქართველო“, ააიპ „საერთაშორისო გამჭვირვალობა – საქართველო“, ააიპ „საქართველოს ახალგაზრდა იურისტთა ასოციაცია“, ააიპ „სამართლიანი არჩევნებისა და დემოკრატიის საერთაშორისო საზოგადოება“ და ააიპ „ადამიანის უფლებათა ცენტრი“ საქართველოს პარლამენტის წინააღმდეგ, II, §. 115. დამატებით, ასევე იხ. §. 31.

[88] იხ. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი, მუხლი 6, საქართველოს საკანონმდებლო მაცნე (www.matsne.gov.ge), 19/06/2012, სარეგისტრაციო კოდი: 140000000.05.001.016807. პენეტრაციის ანუ შეღწევადობის ტესტი არის სიმულირებული კიბერშეტევა კომპიუტერულ სისტემაზე, რათა შეამოწმოს მისი მოწყვლადობა. რაც შეეხება ინფორმაციული უსაფრთხოების აუდიტს, ამავე კანონის თანახმად, ის წარმოადგენს ინფორმაციული უსაფრთხოების მართვის სისტემის ინფორმაციული უსაფრთხოების მინიმალურ სტანდარტებთან შესაბამისობის შეფასებას.

[89] იხ. იქვე, მუხლი 2.

საკანონმდებლო მაცნეს ვებგვერდზე (სააგენტოს მისი გამოქვეყნება ევალებოდა კანონის ამოქმედებიდან 6 თვის ვადაში) და ამდენად, შეუძლებელია მისი შეფასება.

კიდევ ერთი საკითხი საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმებას უკავშირდება - საჯარო სექტორის კრიტიკული ინფორმაციული სისტემის სუბიექტის საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის უსაფრთხოების შემოწმების მიზნით, ოპერატიულ-ტექნიკური სააგენტო უფლებამოსილია მიიღოს გადაწყვეტილება ამ სუბიექტის საინფორმაციო-ტექნოლოგიური ინფრასტრუქტურის შემოწმების ჩატარების შესახებ.[90] შემოწმების ფარგლები არცთუ ვიწროა, კერძოდ, მოწმდება აპარატული და პროგრამული უზრუნველყოფის საშუალებები, ქსელური ინფრასტრუქტურა და მათთან დაკავშირებული ყველა დოკუმენტი თუ პროცესი. აქვე, პირველი კატეგორიის სუბიექტი ვალდებულია, ამ სააგენტოს შეუთანხმოს წინასწარ დაგეგმილი ცვლილებები, რათა არ შეფერხდეს შემოწმება. თავის მხრივ, თუ შემოწმების ჩატარების შედეგად გამოიკვეთება საქართველოს სისხლის სამართლის კანონმდებლობით განსაზღვრული დანაშაულის ნიშნები, სააგენტო ამ შემოწმების მასალებს დაუყოვნებლივ წარუდგენს საგამოძიებო ორგანოს. აღნიშნული ნაკლებად შეიძლება მივიჩნიოთ იმ პროპორციულ და შესაბამის ღონისძიებად[91], რომლის განხორციელების უფლებამოსილებასაც NIS დირექტივა საზედამხედველო ორგანოებს ანიჭებს.

ოპერატიულ-ტექნიკური სააგენტო ფლობს ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკს, რომელშიც თავს იყრის სხვადასხვა ელექტრონული კომუნიკაციის კომპანიიდან მოპოვებული ელექტრონული კომუნიკაციის მაიდენტიფიცირებელი მონაცემები[92] და ამავე დროს, ზედამხედველობს მათი მხრიდან კიბერუსაფრთხოების სფეროს მოთხოვნების შესრულებას.

---

[90] იხ. იქვე, მუხლი 9[1].

[91] Freedom House-ის 2018 წლის ანგარიშში ეჭვქვეშ არის დაყენებული სსიპ საქართველოს ოპერატიულ-ტექნიკური სააგენტოს დამოუკიდებლობა და მასზე ზედამხედველობის მექანიზმების ეფექტიანობა. ანგარიში ხელმისაწვდომია ელექტრონულად: <https://freedomhouse.org/country/georgia/freedom-world/2018> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 28.06.2022). მითითებულია: *კუკავა ქ., ახალაძე ნ., ჩხაიძე ს.,* ფარული მიყურადება საქართველოში - კანონმდებლობისა და პრაქტიკის ანალიზი, თბილისი, 2020, 17.

[92] იხ. სახელმწიფო ინსპექტორის სამსახურის საქმიანობის ანგარიში, თბილისი, 2019, 93.

შესაბამისად, საკანონმდებლო ცვლილებების შედეგად, არცთუ ნათლად წარმოჩინდა ის ზღვარი, რომელიც გადის, ერთი მხრივ, ფარული მიყურადებისა და კომპიუტერული სისტემიდან ინფორმაციის მოპოვების უფლებამოსილებასა და, მეორე მხრივ, კიბერუსაფრთხოების სფეროში კრიტიკული ინფორმაციული სისტემის სუბიექტების ზედამხედველობასა და მათ ინფორმაციასთან წვდომას შორის.

გარდა საზედამხედველო მანდატში ცვლილებისა, აღსანიშნავია, რომ კრიტიკული ინფორმაციული სისტემის სუბიექტები დაიყვნენ სამ კატეგორიად: პირველ კატეგორიაში გაერთიანდნენ სახელმწიფო და მუნიციპალიტეტის ორგანოები და დაწესებულებები, საჯარო სამართლის იურიდიული პირები და სახელმწიფო საწარმოები, ხოლო მეორე კატეგორიის ქვეშ მოექცნენ ელექტრონული კომუნიკაციის კომპანიები, რომელთა ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისთვის ან/და ეკონომიკური უსაფრთხოებისთვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი ცხოვრების შენარჩუნებისთვის.[93] ორივე კატეგორიის ქვეშ შემავალი სუბიექტების მიერ ამავე კანონის მოთხოვნათა შესრულებას ზედამხედველობს სწორედ ოპერატიულ-ტექნიკური სააგენტო. რაც შეეხება ციფრული მმართველობის სააგენტოს, ეს უკანასკნელი მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემების, ანუ კერძო სექტორში არსებული სუბიექტების ზედამხედველი უწყება გახდა.[94] თავის მხრიც, ცალკე აღნიშნულია თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემის სუბიექტთა ზედამხედველობის საკითხი, რომელსაც საქართველოს თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიურო ახორციელებს.[95] გარდა ამ უწყებებისა, საქართველოს ეროვნული უსაფრთხოების საბჭოც ასრულებს ცალკეულ როლს კიბერუსაფრთხოების სფეროს კოორდინაციის მიზნით, როგორიცაა ამ სფეროს ეროვნული სტრატეგიის შემუშავებასა და კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცებაში მონაწილეობა.[96]

კრიტიკული ინფორმაციული სისტემის სუბიექტთა კატეგორიზაციის ამ მიდგომასთან დაკავშირებით, რომელიც უცხოა ევროპის კავშირის NIS დირექტივისათვის,

---

[93] იხ. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი (საქართველოს საკანონმდებლო მაცნე (www.matsne.gov.ge), 19.06.2012, სარეგისტრაციო კოდი: 140000000.05.001.016807), მე-2 მუხლი.

[94] იხ. იქვე, მე-4 და მე-6 მუხლები, III[2] თავი.

[95] იხ. იქვე.

[96] იხ. იქვე, მე-3, 8[1] და 10[1] მუხლები.

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის შესახებ“ საქართველოს კანონის პროექტის განმარტებითი ბარათში აღნიშნულია, რომ „...ამგვარად კონტროლის და ადმინისტრაციულ-სამართლებრივი პასუხისმგებლობის დიფერენცირებული მიდგომების გამოყენება ხდება შესაძლებელი“.[97] გარდა ამ ზოგადი ჩანაწერისა, განმარტებით ბარათში არ არის დასახელებული ის მიზეზები ან გარემოებები, რომელიც შესაძლოა იწვევდეს ამგვარი, განსხვავებული რეჟიმის დაწესების აუცილებლობას თითოეული კატეგორიისთვის. NIS დირექტივა არ იცნობს სახელმწიფო და კერძო სექტორების მიხედვით კრიტიკული ინფორმაციული სისტემების დაყოფას.

საბოლოო ჯამში, საქართველოს მთავრობამ 2021 წლის მიწურულს დაამტკიცა პირველი, მეორე და მესამე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების ნუსხა.[98] აღნიშნული ნუსხა აერთიანებს 61 პირველი კატეგორიის, 8 მეორე კატეგორიისა და 29 მესამე კატეგორიის სუბიექტს.

რაც შეეხება ეროვნული ბანკის, როგორც საბანკო სექტორის მარეგულირებლის როლს, ის თანაკვეთაშია სსიპ ციფრული მმართველობის სააგენტოს მანდატთან და ბადებს გარკვეულ კითხვის ნიშნებს, თუ რომელმა უწყებამ უნდა განახორციელოს საზედამხედველო უფლებამოსილება იმ კომერციული ბანკების მიმართ, რომლებიც ექცევიან მესამე კატეგორიის ქვეშ. კრიტიკული კომერციული ბანკი ეროვნული ბანკის წინაშე ასრულებს „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით ნაკისრ ისეთ ვალდებულებებს, როგორიცაა ინფორმაციული უსაფრთხოების აუდიტის ან პენეტრაციის ტესტის შედეგების გაზიარება[99], შეუსაბამობის/სისუსტეების აღმოსაფხვრელად განსაზღვრული სამოქმედო გეგმის წარდგენა[100] და სხვა. მნიშვნელოვანია, რომ მესამე კატეგორიის კრიტიკული ინფორმაციული

[97] იხ. განმარტებითი ბარათი საქართველოს კანონის პროექტზე „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე, ხელმისაწვდომია საქართველოს პარლამენტის ოფიციალურ ვებგვერდზე: <https://info.parliament.ge/file/1/BillReviewContent/232432> (ვებგვერდზე ბოლო ვიზიტის თარიღი: 04.06.2022).

[98] იხ. „პირველი, მეორე და მესამე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტების ნუსხის დამტკიცების შესახებ“ საქართველოს მთავრობის 2021 წლის 31 დეკემბრის №646 დადგენილება.

[99] იხ. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი (საქართველოს საკანონმდებლო მაცნე (www.matsne.gov.ge), 19.06.2012, სარეგისტრაციო კოდი: 140000000.05.001.016807), მე-6 მუხლის მე-13 პუნქტი.

[100] იხ. იქვე, მე-6 მუხლის მე-17 პუნქტი.

სისტემის სუბიექტი კომერციული ბანკის მიმართ ადმინისტრაციული სამართალდარღვევის საქმის განხილვისა და ადმინისტრაციული სახდელის დადების უფლება აქვს ეროვნულ ბანკს.[101]

როგორც ვხედავთ, ეროვნული ბანკი მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტ კომერციულ ბანკებს შესასრულებლად სავალდებულო მითითებებს ან/და რეკომენდაციებს აძლევს ინფორმაციული უსაფრთხოების სფეროში და განიხილავს ადმინისტრაციული სამართალდარღვევის საქმეებს. ეროვნულ ბანკს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი კომერციული ბანკების მიმართ ინფორმაციული უსაფრთხოების პოლიტიკისა და ინფორმაციული უსაფრთხოების შინასამსახურებრივი გამოყენების წესების დამატებით სტანდარტებისა და მოთხოვნების დადგენის შესაძლებლობაც გააჩნია. აღნიშნული საკმაოდ მძიმე ტვირთად შეიძლება დააწვეს კომერციულ ბანკს, რომელსაც, ერთი მხრივ, მოუწევს სსიპ ციფრული მმართველობის სააგენტოს მიერ დადგენილი ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების, ხოლო, მეორე მხრივ, ამავე სფეროში ეროვნული ბანკის დამატებითი მოთხოვნების შესრულება.

2021 წლის 10 ივნისის ცვლილებების მიხედვით, პრინციპულად შეიცვალა ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნების დადგენის წესი. ცვლილებებამდე საზედამხედველო ორგანო ვალდებული იყო ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების ჩამოყალიბებისას მხედველობაში მიეღო სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO) და ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ დადგენილი სტანდარტები და მოთხოვნები.[102] ამ ეტაპზე, თითოეულ საზედამხედველო ორგანოს აქვს შესაძლებლობა, გადაუხვიოს ნაცად გზას და დაეყრდნოს აშშ-

[101] იხ. იქვე, 10[18] მუხლი.

[102] სსიპ მონაცემთა გაცვლის სააგენტოს, ხოლო მოგვიანებით - სსიპ ციფრული მმართველობის სააგენტოს მიერ დადგენილი ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნები ეფუძნებოდა და თანხვედრაში იყო ISO 27000 სტანდარტის განხორციელების საუკეთესო პრაქტიკასთან. იხ. „ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დამტკიცების შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის 2020 წლის 16 ოქტომბრის №4 ბრძანება, ძალადაკარგულად გამოცხადდა „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დადგენის შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის 2021 წლის 14 დეკემბრის №1 ბრძანებით.

ის სტანდარტებისა და ტექნოლოგიების ეროვნული ინსტიტუტის (NIST) მეთოდოლოგიას.[103] თავისთავად, აღნიშნული ქმნის არაერთგვაროვანი პრაქტიკის ჩამოყალიბების რისკს[104] სამი განსხვავებული სექტორისა და რამდენიმე მარეგულირებლის არსებობის პირობებში.

4. დასკვნა

უდაოდ წინგადადგმულ ნაბიჯად უნდა შეფასდეს ის გარემოება, რომ „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილებების შედეგად ეროვნული უსაფრთხოების საბჭო წარმართავს და კოორდინაციას უწევს კიბერუსაფრთხოების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის პროექტის საქართველოს მთავრობის მიერ დამტკიცების პროცესს. ასევე, საბჭოს აქვს გარკვეული როლი კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების პროცესშიც და ეს ფუნქცია სრულად ზედამხედველი უწყებების ხელში არ არის მოქცეული. მიუხედავად ამისა, კიბერუსაფრთხოების არქიტექტურაში საბჭოს ეს როლი ამომწურავად და ცხადად მაინც არ არის წარმოდგენილი. მნიშვნელოვანია, უფრო მეტად დაკონკრეტდეს, რა ფუნქცია - მოვალეობებში უნდა გამოიხატოს საბჭოს მაკოორდინირებელი საქმიანობა.

ამას გარდა, საკმაოდ დიდ ბუნდოვანებას იწვევს ინფორმაციული უსაფრთხოების არქიტექტურაში საქართველოს ეროვნული ბანკის როლი. სსიპ ციფრული მმართველობის

[103] იხ. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი (საქართველოს საკანონმდებლო მაცნე (www.matsne.gov.ge), 19.06.2012, სარეგისტრაციო კოდი: 140000000.05.001.016807), მე-4 მუხლის მე-2 პუნქტი.

[104] ამ ეტაპზე „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დადგენის შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის 2021 წლის 14 დეკემბრის №1 ბრძანების თანახმად, მოთხოვნები ითვალისწინებს სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO) სტანდარტის (ISO 27000) განხორციელების საუკეთესო პრაქტიკას. ანალოგიურად, „პირველი და მეორე კატეგორიების კრიტიკული ინფორმაციული სისტემების სუბიექტებისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დადგენის შესახებ“ საქართველოს სახელმწიფო უსაფრთხოების სამსახურის სსიპ – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს უფროსის 2021 წლის 21 დეკემბრის №35 ბრძანებით დამტკიცებულ „პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემების სუბიექტებისთვის ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებში“ აღნიშნულია, რომ ეს მინიმალური მოთხოვნები ეფუძნება ISO 27000:2018, ISO 27001:2013, ISO 27002:2013 და ISO 27005:2018 სტანდარტებს.

სააგენტოს ფაქტობრივად კომერციულ ბანკებთან მიმართებით არ ეძლევა მისი საზედამხედველო მანდატის სრულად გამოყენების საშუალება, როგორც ეს განსაზღვრულია სხვა, კერძო სამართლის იურიდიული პირების შემთხვევაში. საპარლემენტო განხილვის მასალებისა და განმარტებითი ბარათის შესწავლის შემდეგაც რთულია არგუმენტირებული პასუხის ძიება კითხვაზე, თუ რატომ არის ამგვარი გამონაკლისი საბანკო სექტორის სახით „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში. ამის საპირისპიროდ, NIS დირექტივა წევრ სახელმწიფოებს მოუწოდებს, მკაფიოდ განსაზღვრონ როლები და პასუხისმგებლობები საზედამხედველო ორგანოებს შორის.

ამასთან, NIS დირექტივა იცნობს „ერთიანი საკონტაქტო პუნქტის“ ცნებას, რომელიც ერთგვარად მეკავშირე ფუნქციას ასრულებს, მათ შორის ინსტიტუციური და ტრანსსასაზღვრო თანამშრომლობის თვალსაზრისითაც. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი, ერთი მხრივ, სსიპ ციფრული მმართველობის სააგენტოს, ხოლო, მეორე მხრივ, ოპერატიულ-ტექნიკურ სააგენტოს ანიჭებს, კომპეტენციის ფარგლებში, საერთაშორისო დონეზე წარმომადგენლობის უფლებამოსილებას, თუმცა არ არის დაკონკრეტებული, რომელი მათგანი შეასრულებს ეროვნულ დონეზე ერთიანი საკონტაქტო პუნქტის ფუნქციას.

აუცილებლად უნდა აღინიშნოს CSIRT-ებისთვის ინციდენტების დაუყოვნებლივ/რეალურ დროში შეტყობინების თაობაზე. დღეს მოქმედ კანონში კიბერ ინციდენტების შეტყობინების არეალი ვიწროა და საჭიროებს გაფართოებას ქსელური სენსორების გამოყენების მიღმა (მაგალითად, ინციდენტის შესახებ ინფორმაციის მიღება ფიზიკური პირებისა და ბიზნეს სუბიექტებისგან, ასევე, საერთაშორისო ქსელების მეშვეობით).

გარდა ზემოაღნიშნულისა, პრობლემურად წარმოჩინდა ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების განსაზღვრის საკითხიც. თითოეული საზედამხედველო ორგანო, დისკრეციული უფლებამოსილების ფარგლებში, თავად განსაზღვრავს ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებს და შესაბამისად, წყვეტს სამი ალტერნატივიდან რომელს - სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO), აშშ-ის სტანდარტებისა და ტექნოლოგიების ეროვნული ინსტიტუტის (NIST) თუ ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ დადგენილ სტანდარტებსა და მოთხოვნებს - მიიღებს მხედველობაში. აღნიშნული, ცხადია, ქმნის

ინფორმაციული უსაფრთხოების სფეროში სახელმწიფო პოლიტიკის არაერთგვაროვნებისა და ცალკეული სუბიექტების არათანაბარ პირობებში ჩაყენების საფრთხეებს.

ერთ-ერთი ყველაზე დიდი შეუსაბამობა „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონსა და NIS დირექტივას შორის უკავშირდება კრიტიკული ინფორმაციული სისტემის სუბიექტების იდენტიფიცირებას და მათ კატეგორიზაციას. როგორც უკვე იყო განხილული, „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი განსხვავებულ ლოგიკას იყენებს და ერთი მხრივ, ასხვავებს საჯარო და კერძო სექტორის კრიტიკული ინფორმაციული სისტემის სუბიექტებს, ხოლო, მეორე მხრივ, ცალკე გამოყოფს ელექტრონული კომუნიკაციის კომპანიებს. ასევე, სრულიად განსხვავებულ საზედამხედველო რეჟიმს უქვემდებარებს კომერციულ ბანკებს. გაუგებარია, რატომ მოხდა ელექტრონული კომუნიკაციის სექტორის ცალკე გამოყოფა და არ მოხდა მისი სხვა, კერძო სექტორის კრიტიკული ინფორმაციული სისტემის სუბიექტებთან გაერთიანება. ელექტრონული კომუნიკაციის კომპანიები ექცევიან ოპერატიულ-ტექნიკური სააგენტოს ზედამხედველობის ქვეშ. ამ ფონზე, კიდევ ერთხელ აღნიშვნის ღირსია საქართველოს საკონსტიტუციო სასამართლოს 2016 წლის 14 აპრილის გადაწყვეტილება, სადაც მან სახელმწიფო უსაფრთხოების სამსახურის მიერ პერსონალური მონაცემების კოპირება/შენახვის თავად ფაქტს „ერთგვარად მსუსხავი ეფექტის მქონე“ უწოდა და დაინახა უსაფრთხოების სამსახურის მხრიდან ადამიანის ძირითად უფლებაში ჩარევის მომეტებული საფრთხე. ამ შემთხვევაში ოპერატიულ-ტექნიკური სააგენტოს ერთდროულად გააჩნია ფარული მიყურადებისა და კომპიუტერული სისტემიდან ინფორმაციის მოპოვების უფლებამოსილება და ტექნიკური შესაძლებლობა და ასევე, ელექტრონული კომუნიკაციის კომპანიების (რომლებიც ერთ-ერთი ყველაზე მსხვილი პერსონალურ მონაცემთა დამმუშავებლები არიან) ზედამხედველობის მანდატი.

ამ მხრივ ნაკლებად იმედისმომცემად გამოიყურება 2022 წელს გამოქვეყნებული ასოცირების დღის წესრიგი, სადაც კონკრეტული ვალდებულებების ნაცვლად აღნიშნულია, რომ საქართველო და ევროპის კავშირი გააგრძელებენ ერთობლივ მუშაობას NIS დირექტივასთან შემდგომი დაახლოებისათვის. აქვე, ევროპის კავშირში საქართველოს წევრობის განაცხადთან დაკავშირებით ევროკომისიის დასკვნის თანახმად კი, საქართველოს დაევალა სახელმწიფო ინსტიტუტების ანგარიშვალდებულების და მათზე დემოკრატიული კონტროლის განხორციელების ეფექტიანი მექანიზმების შექმნა.

და ბოლოს, ამ ფონზე, სასურველია, კანონში მითითება გაკეთდეს პერსონალური მონაცემების დამუშავების კანონიერების საკითხზე. აღნიშნული განსაკუთრებით დიდ ინტერესს იწვევს ოპერატიულ-ტექნიკური სააგენტოს მიერ ელექტრონული კომუნიკაციის კომპანიების ზედამხედველობასა და ქსელური სენსორების ფუნქციონირებასთან დაკავშირებით. რამდენადაც ელექტრონული კომუნიკაციის კომპანიებსა და საბანკო სექტორში თავს იყრის დიდი რაოდენობით პერსონალური მონაცემების შემცველი ინფორმაცია, მნიშვნელოვანია, არსებობდეს ჩანაწერი მაიდენტიფიცირებელი მონაცემების დამუშავების ფარგლებთან დაკავშირებით.