საქართველოს ტექნიკური უნივერსიტეტი

ხელნაწერის უფლებით

ნიკა ასვანუა

პერსონალურ მონაცემთა დაცვის მექანიზმები და პრობლემატიკა საქართველოში

სადოქტორო პროგრამა – საჯარო მმართველობა

შიფრი – 1109

დოქტორის აკადემიური ხარისხის მოსაპოვებლად

წარდგენილი დისერტაციის

ა ვ ტ ო რ ე ფ ე რ ა ტ ი

თბილისი

2020 წელი

სამუშაო შესრულებულია საქართველოს ტექნიკურ უნივერსიტეტში
ბიზნესტექნოლოგიების ფაკულტეტი
საჯარო მმართველობისა და ელექტრონული ბიზნესის დეპარტამენტი

ხელმძღვანელი: ირაკლი გაბისონია

რეცენზენტები: ----------

დაცვა შედგება 2020 წლის ”_____” თებერვალს, _____ საათზე
საქართველოს ტექნიკური უნივერსიტეტის ბიზნესის ადმინისტრირების,
საჯარო მმართველობისა და მენეჯმენტის საუნივერსიტეტო სადისერტაციო
საბჭოს სხდომაზე.
კორპუსი VI, აუდიტორია ----------,
მისამართი: თბილისი, კოსტავას 77.

დისერტაციის გაცნობა შეიძლება სტუ-ს ბიბლიოთეკაში,
ხოლო ავტორეფერატისა ფაკულტეტის ვებგვერდზე

სადისერტაციო საბჭოს მდივანი
პროფესორი / ლ. კოჭლამაზაშვილი/

Abstract

Protecting human rights and ensuring the interests of the individual is the primary task of the state in the process of forming an information society in Georgia. Mechanisms for solving these tasks require constant change and refinement in the light of the development of information technology. In developed countries, the technology of "big data", artificial intelligence and others, is not only convenient and comfortable, but also poses new challenges and threats to society. The real danger is the uncontrolled processing of data about the individual, which can then be used potentially in a negative or undesirable way, as the probability of their modification and unauthorized use is quite high.

Therefore, the formation of adequate me chanisms for the protection of personal data and their perfection is the prerogative of the state, because the state is the main guarantor of human rights. The state is obliged to control the process of processing and dissemination of personal information by determining the rules and conditions of access to data.

The idea of the paper is to structure the governance model of personal data protection, which in combination with organizational, legal, technical mechanisms and new technologies of protection creates a certain balance between personal data as a category of protection of rights and economic category.

In order to refine the personal data management model, elements of data processing organization, analysis of collected information, legal and technical mechanisms of data protection have been proposed.

In order to establish these mechanisms, international practice and standards of personal data protection have been studied. The activities carried out by the Data Protection Inspector of Georgia during the implementation of the supervisory control function and the case law on the organization of data processing are analyzed. The following problems have been identified: non-compliance with data processing principles, lack of specific and clear purpose, or inadequate and disproportionate scope of the purpose; insecurity of data storage dates; illegal processing of personal data; violation of video surveillance rules and non-compliance with data security requirements; violation of the rules of informing the data subject; use of data in violation of the rules for the purposes of direct marketing, etc. Criteria for the adequacy and proportionality of the purpose of data processing have been developed.

Legislation on data protection is analyzed not in a static state, but in dynamic state, which implies the constant updating of legislation in the wake of new technologies.

There is a need for legal regulations related to the technological process of "big data", the improvement of the mechanisms for the protection of digital assets of human rights and freedoms on the basis of international agreements and constitutional regulations.

Active and passive aspects of technical mechanisms and modern standards of cryptography are discussed in the Resolution No. 274 of April 4, 2014 of the Government of Georgia on the Approval of the Procedure for Determining the Security of NATO Classified Information in Georgia and the Rules for Determining Their Activities. In parallel with this mechanism, the need for additional measures is justified. Such as joining the Cloud Security Alliance and focusing on the following areas: infrastructure security, data privacy, data management, response procedures.

The state of data processing on administrative offenses through "smart" cameras and contactless patrols has been studied; the processes of processing sensitive

personal information of individuals in the databases owned by law enforcement agencies are analyzed and the lack of organizational and technical measures taken by the agency for data protection, the unfounded need for access to databases are revealed.

In parallel with the confidentiality of information about the patient in medical institutions, the data protection features in the context of COVID-19 infection were analyzed. Some advantages of "big data" technology to solve various tasks in the fight against pandemics are substantiated; the dangers and risks of "big data" technology are highlighted. Therefore, the principle of independent regulation has been proposed to achieve the effectiveness of the introduction of this technology. A point modification of the Personal Data Protection Law in this regard will not be effective, as the protection of digital assets of human rights and freedoms must be based on international agreements and constitutional regulations. The effectiveness of the implementation of the big data processing project depends primarily on the development of security mechanisms, which in turn increases the timing of the project and the costs of implementing the protection system.

In order to ensure systematic prevention in the field of personal data protection and to ensure the interconnection of organizational-legal-technical mechanisms, a model of the government's strategic document has been developed, which serves the following tasks: security of infrastructure; ensuring data confidentiality - integration, classification, inventory; data access policy; data management; database key management; completion of protection mechanisms and response procedures; analysis of detection of harmful actions with databases, detection and response of threats, security of analytical results.

Such a strategic document defines the effectiveness of personal data protection mechanisms and state policy in this area.

ნაშრომის ზოგადი დახასიათება

საქართველოში ინფორმაციული საზოგადოების ფორმირების პროცესში ადამიანის უფლებათა დაცვა და ინდივიდის ინტერესების უზრუნველყოფა სახელმწიფოს უპირველესი ამოცანაა. ამ ამოცანების გადაწყვეტის მექანიზმები ინფორმაციული ტექნოლოგიების განვითარების ფონზე მუდმივ ცვლილებებსა და დახვეწას ითხოვს. კერძოდ: „მონაცემთა დიდი მასივების“ ტექნოლოგია, ხელოვნური ინტელექტი და სხვა, არა მარტო მოხერხებული და კომფორტულია, არამედ ახალი გამოწვევებისა და საფრთხეების წინაშე აყენებს საზოგადოებას. რეალურ საფრთხეს წარმოადგენს ინდივიდის შესახებ მონაცემთა არაკონტროლირებადი დამუშავება, რომელიც შემდგომ, პოტენციურად, შესაძლებელია გამოყენებულ იქნას ნეგატიური ან არასასურველი ფორმით. ამასთან, გლობალური ინფორმაციული საზოგადოების განვითარება და ინფორმაციისა და საკომუნიკაციო ტექნოლოგიების გაუმჯობესება ზრდის ამ პროცესის სიჩქარესა და მონაცემთა

მოცულობას. ასეთ დროს მათი მოდიფიკაციისა და არასანქციონირებული გამოყენების ალბათობა საკმაოდ დიდია. ასეთ პირობებში ინფორმაციული ტექნოლოგიების შემდგომი განვითარება საფრთხის ქვეშ აყენებს პირადი ცხოვრების არა მარტო ხელშეუხებლობას, არამედ თვით მისი არსებობის ფაქტსაც.

აქედან გამომდინარე, პერსონალურ მონაცემთა დაცვის ადექვატური მექანიზმების ფორმირება და მათი სრულყოფა სახელმწიფოს პრეროგატივაა, რადგან, სწორედ, სახელმწიფოა უფლებათა დაცვის მთავარი გარანტი. იგი ვალდებულია აკონტროლოს ინფორმაციის დამუშავებისა და გავრცელების პროცესი ამ ინფორმაციასთან დაშვების წესებისა და პირობების განსაზღვრით.

ამგვარად, პერსონალური მონაცემები პიროვნების სახელმწიფოსთან ურთიერთობის სტატუსის განმსაზღვრელი მნიშვნელოვანი რესურსია, რომლის უსაფრთხო მიმოქცევა სხვადასხვა დარგის მეცნიერთა კვლევის საგანი ხდება.

თუ ამ საკითხს სხვა კუთხით შევხედავთ, პერსონალურ მონაცემთა დაცვის პროცესის მართვას არსებითი მნიშვნელობა აქვს როგორც სახელმწიფოსთვის, ასევე კომერციული სტრუქტურებისთვის. ახალი ტექნოლოგიების დანერგვა ინფორმაციის დამუშავების პროცესში ქვეყნის ეკონომიკური და სოციალური განვითარების აუცილებელ ფაქტორს წარმოადგენს, რომლის შეჩერება პრაქტიკულად შეუძლებელია. ამასთან, ეს პროცესი მიმდინარეობს მონაცემთა ბაზების, მათ შორის პერსონალური მონაცემებისა და ინფორმაციული სისტემების სწრაფი ზრდის ფონზე.

ფაქტიურად ციფრული ეკონომიკისა და ელექტრონული მთავრობის განვითარება, რომლებიც სახელმწიფო პოლიტიკის პრიორიტეტულ მიმართულებებს წარმოადგენენ, ბევრადაა დამოკიდებული იმაზე, თუ როგორი იქნება პერსონალურ მონაცემთა დაცვის სფეროში სახელმწიფო სტრატეგია. ისიც გასათვალისწინებელია, რომ პერსონალურ მონაცემთა კონფიდენციურობის უზრუნველყოფის ჭარბი მოთხოვნების დაწესებას შესაძლებელია უკიდურესად ნეგატიური შედეგები მოჰყვეს ეკონომიკისა და სახელმწი-

ფოსთვის მთლიანად, განსაკუთრებით კი იმ სფეროებში, სადაც საქონლისა და მომსახურების მიწოდება პირდაპირ კავშირშია პერსონალურ მონაცემთა ავტომატიზებულ დამუშავებასთან (სახელმწიფო და მუნიციპალური მომსახურება, კავშირგაბმულობა, განათლება, ჯანდაცვა, ტრანსპორტი და სხვ.).

პერსონალურ მონაცემთა დაცვის პრობლემა და პიროვნების, სახელმწიფოსა და საზოგადოების ინტერესებს შორის ბალანსის საკითხი არაერთხელ მოხვედრილა მთავრობის საპროგრამო დოკუმენტებში. ასევე ფაქტია პირადი ცხოვრების ხელშეუხებლობისა და პერსონალურ მონაცემთა გავრცელებასთან დაკავშირებული დანაშაულებრივი ქმედებებისა და ამ მიმართულებით სასამართლო პრაქტიკის ზრდაც.

მიუხედავად იმისა, რომ პერსონალურ მონაცემთა დაცვის სფეროში საქართველო მრავალი საერთაშორისო კონვენციის მონაწილეა, მეტნაკლებად უკვე შექმნილია სამართლებრივი ბაზა, ფუნქციონირებს სახელმწიფო ინსპექტორის სამსახური, როგორც პერსონალურ მონაცემთა დაცვის მაკონტროლებელი ორგანო, დაცულობის ხარისხი რეალობაში მაინც დაბალია და ჩამორჩება საზოგადოების მოთხოვნებს.

ასეთ პირობებში პერსონალურ მონაცემთა დაცვის გარანტიების უზრუნველყოფის მექანიზმების არაეფექტურობა სერიოზულ პრობლემად რჩება. ეს გარემოება ითხოვს პერსონალურ მონაცემთა დამუშავების პროცესისა და ამ პროცესის მართვის მეცნიერულ დონეზე შესწავლას, რაც სადისერტაციო კვლევის **აქტუალობას** განსაზღვრავს.

ნაშრომის **მეცნიერულ სიახლეს** წარმოადგენს პერსონალურ მონაცემთა დაცვის მმართველობითი მოდელის სტრუქტურირება დაცვის პროცესის უზრუნველყოფის მექანიზმების მეშვეობით. ამ სფეროში სახელმწიფოს სტრატეგიული დაგეგმვის თეორიული და პრაქტიკული ამოცანის გადაწყვეტა.

პირველადაა მოცემული „მონაცემთა დიდი მასივების“ (Big data) ტექნოლოგიის პერსონალურ მონაცემთა დაცვის კანონმდებლობასთან შეუთავსებლობისა და მონაცემთა დამუშავებაზე მისი ზეგავლენის ანალიზი, დასაბუთებულია ამ ტექნოლოგიის უპირატესობა COVID-19 პანდემიასთან

ბრძოლის სხვადასხვა ამოცანის გადასაწყვეტად.

პერსონალურ მონაცემთა დაცვის სფეროში გამოვლენილი დარღვევების პრაქტიკის შესწავლისა და ანალიზის საფუძველზე შემუშავებულია ინფორმაციულ სისტემებში პერსონალურ მონაცემთა დაცვის სტრატეგიული დოკუმენტი.

კვლევის ობიექტია პერსონალურ მონაცემთა დაცვის მექანიზმები და ტექნოლოგიები.

კვლევის საგანია ნორმატიული აქტები, თეორიული მოდელები და პრაქტიკა, რომლებიც უზრუნველყოფენ პერსონალური მონაცემების დაცვის პროცესში მართვის მექანიზმების კონსტრუირებას.

კვლევის მიზანია პერსონალურ მონაცემთა დაცვის პროცესში პრობლემების გადაჭრის მექანიზმების სტრატეგიული წინადადებების შემუშავება.

კვლევის ამოცანებია:

- პერსონალური მონაცემების დაცვის მექანიზმების გამოვლენა და სისტემატიზაცია;
- საქართველოში პერსონალურ მონაცემთა დაცვის სისტემის ანალიზი;
- დაცვის მექანიზმების საერთაშორისო პრაქტიკის შესწავლა;
- პერსონალურ მონაცემთა დამუშავების პრაქტიკის გაანალიზება და პრობლემათა გამოვლენა;
- პერსონალურ მონაცემთა დარგობრივი პრინციპით დამუშავების თავისებურებათა გაანალიზება;
- ახალი ტექნოლოგიების ზეგავლენის განსაზღვრა პერსონალურ კანონმდებლობაზე;
- პერსონალურ მონაცემთა დაცვის სტრატეგიული წინადადებების შემუშავება.

კვლევის მეთოდოლოგია. უცხოელ და ქართველ მკვლევართა ნაშრომების გაცნობისა და პერსონალურ მონაცემთა დაცვის სფეროში არსებულ დარღვევებზე დაკვირვების საფუძველზე ისმება კითხვა:

რომელი მექანიზმებით და რა ტექნოლოგიების გამოყენებით იქნება

შესაძლებელი პერსონალურ მონაცემთა დაცვის პროცესის ეფექტური მართვა?

ეს კითხვა განსაზღვრავს ჩვენი კვლევის პრობლემას, რომელზე მუშაობის პროცესში:

გამოყენებულია ინდუქციური (კერძოდან ზოგადისკენ), ფორმალურ-ლოგიკური, შედარებითი **მეთოდები**; სიმრავლის თეორია, სახელმწიფო მართვის თეორია, პროექტირების ტექნოლოგია.

კვლევის ემპირიულ საფუძველს წარმოადგენს საერთაშორისო აქტები, საქართველოს კანონმდებლობა პერსონალურ მონაცემთა დაცვის სფეროში, პერსონალურ მონაცემთა დაცვის ინსპექტორის ანგარიშები და ამ სფეროში მოქმედი საერთაშორისო სტანდარტები.

ჰიპოთეზა - თუ მხედველობაში მივიღებთ, რომ ორგანიზაციულ-სამართლებრივი და ტექნიკური მექანიზმების კონსტრუირება პერსონალურ მონაცემთა დაცვის კარგი საშუალებაა, მაშინ ახალი ტექნოლოგიების პირობებში მექანიზმთა ასეთი კონსტრუირება სისტემურ მოდერნიზებას მოითხოვს.

კვლევის თეორიული და პრაქტიკული მნიშვნელობა. კვლევით თემასთან დაკავშირებული სამეცნიერო ცოდნის სისტემატიზაცია და მიღებული კვლევის შედეგებით დასტურდება, რომ ჩვენს მიერ ფორმულირებული თეორიული დებულებები და პრაქტიკული წინადადებები გარკვეულ წვლილს შეიტანს მონაცემთა დაცვის მართვის თეორიასა და ინფორმაციული სამართლის მეცნიერებაში. ამასთან, ისინი შესაძლებელია გამოყენებულ იქნას როგორც მართვის პროცესის სრულყოფაში, ასევე კანონშემოქმედებით საქმიანობაში.

ნაშრომის ძირითადი დებულებები: პერსონალურ მონაცემთა მართვის მოდელის დახვეწის აუცილებელი პირობაა მონაცემთა დამუშავების ორგანიზების, შეგროვილი ინფორმაციის ანალიზის, მონაცემთა დაცვის სამართლებრივი და ტექნიკური მექანიზმების ელემენტების ერთობლიობა.

მონაცემთა დაცვის ინსპექტორის საზედამხედველო მაკონტროლებელი ფუნქციის განხორციელების პროცესში გაწეული საქმიანობა, აგრეთვე

სასამართლო პრაქტიკა მონაცემთა დამუშავების ორგანიზების სფეროში ითხოვს უკუკავშირის სისტემას.

დამუშავების მიზნის ადეკვატურობა და პროპორციული მოცულობის მონაცემთა შენახვის ვადები დაკავშირებულია ბალანსის კრიტერიუმების შემუშავებასთან;

პერსონალურ მონაცემთა დაცვის შესახებ კანონმდებლობა ტექნოლოგიების განვითარების კვალდაკვალ მუდმივ განახლებას ექვემდებარება, რაც გულისხმობს არა სტატიკურ მდგომარეობაში მის არსებობას, არამედ დინამიკაში ფუნქციონირებას.

„მონაცემთა დიდი მასივების“ (Big data) ტექნოლოგიური პროცესი დაკავშირებულია ახალი სამართლებრივი რეგულაციების აუცილებლობასთან.

ადამიანის უფლებათა ციფრული აქტივების დაცვის ახალი მექანიზმების სრულყოფა საერთაშორისო შეთანხმებების საფუძველზეა შესაძლებელი და კონსტიტუციური რეგლამენტაციის შემთხვევაში საგნობრივ სფეროს სტრატეგიულ ხასიათს სძენს.

ტექნიკური მექანიზმები აქტიური და პასიური მხარეებით ხასიათდება, რომელთა სტატუსი ტექნოლოგიის შინაარსზეა დამოკიდებული;

„საქართველოში ნატოს კლასიფიცირებული ინფორმაციის უსაფრთხოების უზრუნველმყოფი პასუხისმგებელი ორგანოებისა და მათი საქმიანობის განსაზღვრის წესის დამტკიცების შესახებ“ საქართველოს მთავრობის 2014 წლის 4 აპრილი №274 დადგენილების უზრუნველყოფის საქმეში. განმსაზღვრელი როლი კრიპტოგრაფიის თანამედროვე სტანდარტებს ენიჭებათ;

სამართალდამცავი ორგანოების მფლობელობაში არსებულ მონაცემთა ბაზებში ფიზიკურ პირთა სენსიტიური პერსონალური ინფორმაციის დამუშავების პროცესები აჩვენებს უწყების მიერ მონაცემთა დაცვისათვის მიღებული ორგანიზაციულ-ტექნიკური ზომების არასაკმარისობას, მონაცემთა ბაზებზე წვდომის საჭიროების დაუსაბუთებლობას.

„ჭკვიანი“ კამერებისა და უკონტაქტო პატრულირების საშუალებით

ადმინისტრაციულ სამართალდარღვევებზე მონაცემთა დამუშავების მდგომარეობა არ შეესაბამება სტანდარტებს;

არასრულწლოვანთა პერსონალური მონაცემების დამუშავების, შრომითი ურთიერთობებისას მონაცემთა შეგროვების პროცესი, ადვოკატის მიერ სხვისი მონაცემების გასაჯაროების ფაქტები პროფესიული საქმიანობის ფარგლებში ითხოვს პროფილაქტიკური ღონისძიებების გაძლიერებას;

სამედიცინო დაწესებულებებში პაციენტზე ინფორმაციის კონფიდენციალობის პარალელურად COVID-19 ინფექციის პირობებში, „მონაცემთა დიდი მასივების“ ტექნოლოგიის გამოყენებას აქვს გარკვეული უპირატესობები პანდემიასთან ბრძოლის სხვადასხვა ამოცანის გადასაწყვეტად;

პერსონალურ მონაცემთა დაცვის სფეროში ორგანიზაციული მართვის უზრუნველსაყოფად აუცილებელია პერსონალურ მონაცემთა დაცვის სტრატეგიის არსებობა, როგორც ამ სფეროში უმნიშვნელოვანესი სახელმწიფო რესურსის დაცვის ვექტორ;.

ნაშრომის თეორიული და პრაქტიკული მნიშვნელობა. ნაშრომში ფორმირებულია თეორიული დებულებები, რომლებიც განსაზღვრავენ მექანიზმების არსსა და მნიშვნელობას პერსონალურ მონაცემთა დაცვის პროცესში, აგრეთვე ახალი ტექნოლოგიების განვითარების პირობებში უფლებათა დაცვასა და ეკონომიკურ კატეგორიას შორის ბალანსს. ყურადღება ეთმობა ცნებათა აპარატის დახვეწას.

დისერტაციის მასალები პერსპექტივებისა და ტენდენციების განვითარების კონტექსტში შესაძლებელია გამოყენებულ იქნას პერსონალურ მონაცემთა დაცვის პროცესის მართვის თეორიულ საფუძვლად, აგრეთვე იქცეს დარგთაშორისი კვლევის საგნად.

დასკვნები და რეკომენდაციები შეიძლება გამოყენებულ იქნას აღმასრულებელი ხელისუფლების მიერ კავშირგაბმულობის, ინფორმაციული ტექნო-ლოგიებისა და კომუნიკაციების სფეროში ეფექტური მართვის უზრუნველსაყოფად.

სადისერტაციო მასალები ხელს შეუწყობს უმაღლესი განათლების პროფილური პროგრამების მოდერნიზებას, საჯარო ლექციებისა და სემინა-

რების ორგანიზებას.

კვლევის შედეგების აპრობაცია. კვლევის პროცესში ფორმულირებული დებულებები, დასკვნები და რეკომენდაციები აისახა ავტორის მიერ გამოქვეყნებულ სტატიებში. აქტუალური პრობლემები განხილულია კონფერენციებსა და დარგობრივ სემინარებზე.

ნაშრომი არაერთხელ იქნა განხილული სტუ საჯარო მმართველობის პრობლემათა კვლევების ინსტიტუტში მეთოდური მხარდაჭერისა და მისი გამოყენებითი მნიშვნელობის დებულებების უზრუნველსაყოფად.

ნაშრომის სტრუქტურა. ნაშრომი შედგება შესავლის, ხუთი თავის და 17 პარაგრაფისგან, დასკვნისა და რეკომენდაციებისგან.

ნაშრომის სტრუქტურა:

შესავალი

ლიტერატურის მიმოხილვა

თავი 1. პერსონალურ მონაცემთა დაცვის მექანიზმების თეორიული საფუძვლები

1.1. პერსონალურ მონაცემთა დაცვის არსი და მნიშვნელობა ავტომატიზირებული დამუშავების პროცესში

1.2. პერსონალურ მონაცემთა დაცვის ორგანიზაციული მექანიზმები

1.3. პერსონალურ მონაცემთა სამართლებრივი დაცვის მექანიზმები

1.4. პერსონალურ მონაცემთა დაცვის ტექნიკური მექანიზმები

თავი 2. პერსონალურ მონაცემთა დამუშავების ორგანიზაციულ-სამართლებრივი და ტექნიკური პრობლემები

2.1. პერსონაურ მონაცემთა დამუშავების თავისებურებები ტექნოლოგიური განვითარების პროცესში

2.2. საერთაშორისო სტანდარტები და მათი მნიშვნელობა პერსონალურ მონაცემთა დამუშავების დროს

2.3. პერსონალურ მონაცემთა დამუშავების შესაბამისობა საერთაშორისო სტანდარტებთან

2.4. პერსონალურ მონაცემთა დამუშავების შიდაორგანიზაციული

პრობლემები

თავი 3. პერსონალურ მონაცემთა დაცვის სისტემის ეფექტურობის კონტროლის მექანიზმები საქართველოში

3.1. პერსონალურ მონაცემთა დაცვის საფუძვლები

3.2. პერსონალურ მონაცემთა დაცვის კონტროლი ელექტრონულ სისტემებში მონაცემთა დამუშავების დროს

3.3. ვიდეოთვალთვალის სისტემის კონტროლი

3.4. საქართველოში მონაცემთა გამჟღავნებისა და გასაჯაროების კონტროლის პრაქტიკის ანალიზი

თავი 4. პერსონალურ მონაცემთა დაცვის უზრუნველყოფის მექანიზმები დარგობრივი დამუშავების პროცესში

4.1.პერსონალურ მონაცემთა დაცვის ღონისძიებები ჯანდაცვის სფეროში და მათი თავისებურებები COVID-19 პანდემიის პირობებში

4.2. არასრულწლოვანთა პერსონალური მონაცემების დაცვის ღონისძიებები

4.3. პერსონალურ მონაცემთა დაცვის ღონისძიებები შრომითი ურთიერთობების პროცესში

4.4. პერსონალურ მონაცემთა დაცვა მიზნობრივი და პირდაპირი მარკეტინგის პროცესში

4.5. ბიომეტრული პერსონალური მონაცემების დაცვის ღონისძიებები

თავი 5. პერსონალურ მონაცემთა დაცვის სტრატეგია საერთაშორისო ინფორმაციულ სისტემებში მონაცემთა გადაცემის პროცესში

დასკვნები, რეკომენდაციები და გამოყენებული ლიტერატურა.

ნაშრომის ძირითადი შინაარსი

ნაშრომის შესავალში მიმოხილულია საკვლევი თემის ძირითადი ასპექტები, გამოწვევები, რომელიც ჩვენი ქვეყნის წინაშე დგას პერსონალურ მონაცემთა დაცვისას, მოცემულია თემის აქტუალობის შესახებ შესაბამისი არგუმენტები, კვლევის მიზანი, სიახლე, თეორიული და პრაქტიკული მნიშვნელობა და სხვა.

ლიტერატურის მიმოხილვა მოიცავს სადისერტაციო თემის კვლევის პროცესში გამოყენებული იმ ძირითადი სახელმძღვანელოების, სამეცნიერო თუ საინფორმაციო სტატიების, საერთაშორისო და ადგილობრივი ორგანიზაციის ანგარიშების, რეკომენდაციების, ღია ინტერნეტ სივრცეში განთავსებული მასალების ანალიზს. სადისერტაციო ნაშრომის ძირითადი მიგნებები, შეფასებები და აქცენტები ემყარება სხვადასხვა კვლევებს, სტატისტიკურ მონაცემებს, პრაქტიკულ-სამეცნიერო მასალებს. მნიშვნელოვანი ყურადღება დაეთმო როგორც ადგილობრივი, ისე უცხოელი მეცნიერებისა და პრაქტიკოსი სახელმწიფო მოხელეებისა და იურისტების შეხედულებებს, რომლებიც ასახულია სამეცნიერო თუ პრაქტიკულ ჟურნალებში, მონოგრაფიებსა და სხვადასხვა ტიპის შრომებში.

ნაშრომზე მუშაობისას ასევე განხილულ იქნა სხვადასხვა ქვეყნის საუკეთესო პრაქტიკა, რამაც საშუალება მოგვცა დაგვესკვნა ქვეყნებს შორის არსებული სხვაობების გავლენა, როგორც საკვლევ საკითხებზე, ასევე მარეგულირებელი ნორმების თავისებურებებზე.

საკვლევი თემისათვის აგრეთვე მნიშვნელოვანი აღმოჩნდა სხვადასხვა საერთაშორისო და ადგილობრივი ორგანიზაციების მიერ მომზადებული გზამკვლევები და ანგარიშები, რადგან ისინი ემყარება სახელმწიფოთა გამოცდილებას, პრაქტიკოსი და თეორიტიკოსი საჯარო მოხეელების რეკომენდაციებს და ხშირად ობიექტურად ასახავს არსებულ აქტუალურ პრობლემებსა და არსებულ საჭიროებებს.

პირველი თავში განხილულია პერსონალურ მონაცემთა დაცვის მექანიზმების თეორიული საფუძვლები. კერძოდ, გააზრებულია ისეთი საკითხები როგორიცაა: პერსონალურ მონაცემთა დაცვის არსი და მნიშვნელობა ავტომატიზირებული დამუშავების პროცესში; პერსონალურ მონაცემთა დაცვის ორგანიზაციული მექანიზმები; პერსონალურ მონაცემთა სამართლებრივი დაცვის მექანიზმები და ასევე პერსონალურ მონაცემთა დაცვის ტექნიკური მექანიზმები.

ამ თავში მოცემულია როგორც სახელმწიფო ინსპექტორის სამსახურის მისია ისე ის ღირებულებები, რომლითაც იგი ხელმძღვანელობს საქმიანო-

ბის პროცესში.

მეორე თავში განხილულია პერსონალურ მონაცემთა დამუშავების ორგანიზაციულ-სამართლებრივი და ტექნიკური პრობლემები. თუ რა თავისებურებები ახასიათებს მონაცემთა დამუშავებას ტექნოლოგიური განვითარების პროცესში. ასევე წარმოდგენილია საერთაშორისო სტანდარტები და გააზრებულია მათი მნიშვნელობა პერსონალურ მონაცემთა დამუშავების დროს.

ამ თავში მოცემულია პერსონალურ მონაცემთა დამუშავების შიდაორგანიზაციული პრობლემები და პერსონალურ მონაცემთა დამუშავების არსებული პრაქტიკის შესაბამისობა საერთაშორისო სტანდარტებთან.

მესამე თავი ეძღვნება პერსონალურ მონაცემთა დაცვის სისტემის ეფექტურობის კონტროლის მექნიზმებს საქართველოში. გაანალიზებულია ისეთი საკითხები როგორიცაა: პერსონალურ მონაცემთა დაცვის საფუძვლები; პერსონალურ მონაცემთა დაცვის კონტროლი ელექტრონულ სისტემებში მონაცემთა დამუშავების დროს.

ასევე საუბარია ვიდეოთვალთვალის სისტემათა კონტროლის თავისებურებებსა და არსებულ პრობლემებზე.

ამ თავში სიღრმისეულად არის წარმოდგენილი საქართველოში მონაცემთა გამჟღავნებისა და გასაჯაროების კონტროლის პრაქტიკის ანალიზი.

მეოთხე თავში განხილულია პერსონალურ მონაცემთა დაცვის უზრუნველყოფის მექანიზმები დარგობრივი დამუშავების პროცესში, კერძოდ: პერსონალურ მონაცემთა დაცვის ღონისძიებები ჯანდაცვის სფეროში და მათი თავისებურებები COVID-19 პანდემიის პირობებში, არასრულწლოვანთა პერსონალური მონაცემების დაცვის ღონისძიებები, პერსონალურ მონაცემთა დაცვის ღონისძიებები შრომითი ურთიერთობების პროცესში, პერსონალურ მონაცემთა დაცვა მიზნობრივი და პირდაპირი მარკეტინგის პროცესში და ბიომეტრული პერსონალური მონაცემების დაცვის ღონისძიებები.

მეხუთე თავში მოცემულია პერსონალურ მონაცემთა დაცვის სტრატეგია საერთაშორისო ინფორმაციულ სისტემებში მონაცემთა გადაცემის პროცესში. ასევე დეტალურად არის წარმოდგენილი ის ორგანიზაციული, სამარ-

თლებრივი და ტექნიკური მექანიზმების გამოყენების თვალსაზრისით არსებული ხარვეზები, რომლებიც კვლევის შედეგად გამოვლინდა ამ მიმართულებით.

დასკვნა

პერსონალურ მონაცემთა დაცვის მექანიზმების კვლევა ინფორმაციული საზოგადოების განვითარების პროცესში ინტერნეტის ხელმისაწვდომობისა და ინფორმაციული ტექნოლოგიების სწრაფი ზრდის ტენდენციის გათვალისწინებითაა წარმოებული. შესაბამისად, პერსონალურ მონაცემთა დაცვის მექანიზმების ფუნქციონირება გათვლილია არა სტატიკურ მდგომარეობაზე, არამედ დინამიკურ ურთიერთობებზე. ამ საქმეში დიდ როლს ასრულებს პროგნოზირება და არსებული მექანიზმების ხშირი, სისტემური რედაქტირება. ამას ისიც ემატება, რომ უფლებათა დაცვასა და პერსონალურ მონაცემთა ეკონომიკურ კატეგორიას შორის ბალანსის დაცვა აუცილებელი პირობაა. ამიტომ ერთიანი სტრატეგიული დოკუმენტი პერსონალურ მონაცემთა დაცვის მექანიზმების ფორმირებაში სახელმწიფო პოლიტიკას უფრო მოქნილს ხდის.

სტრატეგიული დოკუმენტის შექმნის აუცილებლობა ეფუძნება პერსონალური მონაცემების დაცვის სფეროში არსებული პრობლემების შესწავლას და დაცვის მექანიზმების სისტემურ ანალიზს. კვლევის პროცესში ინდუქციური შემეცნების მეთოდმა საშუალება მოგვცა კონკრეტული ფაქტების განზოგადების საფუძველზე შეგვესწავლა პერსონალურ მონაცემთა დაცვის მექანიზმები. ონტოლოგიის საფუძველზე კი გვეწარმოებინა საგნობრივი სფეროს სისტემური ანალიზი, რაც, თავის მხრივ, სემანტურად ორიენტირებული გლობალური ქსელის საინფორმაციო წყაროებთან დაშვების პროცესს უკავშირდება. ამ თეორიისა და მეთოდის საფუძველზე შემუშავებულია პერსონალურ მონაცემთა დაცვის მექანიზმების კონკრეტული მოდელი.

მოდელის ახსნა გულისხმობს მონაცემთა დამუშავების ორგანიზების არსის ფორმირებას, ანუ მონაცემთა ბაზებიდან ყველა იმ ინფორმაციის

გამორიცხვას, რომლის დამუშავებაც აკრძალულია კანონმდებლობით; პირველადი ინფორმაციის სრული ანალიზი შესაძლებელია მხოლოდ მისი შეკრების შემდეგ, ე. ი. მონაცემთა იმ მდგომარეობაში მოყვანა, რომლის მიხედვით მოსახერხებელია შედარება, ინტერპრეტირება, განზოგადება.

ამ პროცესში პერსონალურ მონაცემთა დაცვის მექანიზმები სამი მიმართულებითაა დაჯგუფებული: ორგანიზაციული, სამართლებრივი, ტექნიკური.

ორგანიზაციული მექანიზმები გულისხმობს: შიდაორგანიზაციული მართვის სტრუქტურას, პროცესზე კონტროლის საშუალებებს, სახელმწიფო ზედამხედველობის სტრუქტურასა და პროცედურებს.

ორგანიზაციული მექანიზმების ანალიზი ცხადჰყოფს, რომ გაიზარდა პერსონალურ მონაცემთა დაცვის ინსპექტორისადმი მიმართვიანობა. ინსპექტორის საქმიანობის შესწავლით გამოვლენილია შემდეგი პრობლემები: მონაცემთა დამუშავების პრინციპების დაუცველობა; მონაცემთა დამუშავების პროცესში კონკრეტული და მკაფიო მიზნის არარსებობა, რომლის შედეგია ინფორმაციის დამუშავება მიზნის არაადეკვატური და არაპროპორციული მოცულობით; მონაცემთა შენახვის ვადების დაუცველობა; პერსონალურ მონაცემთა არაკანონიერი დამუშავების გაზრდილი რაოდენობა; ვიდეოთვალთვალის წესების დარღვევა და მონაცემთა უსაფრთხოების დაცვის მოთხოვნების შეუსრუ-ლებლობა; მონაცემთა სუბიექტის ინფორმირების წესების დარღვევა; პირდაპირი მარკეტინგის მიზნებისათვის წესების დარღვევით მონაცემთა გამოყენება; განსაკუთრებული კატეგორიის მონაცემთა დამუშავება კანონიერი საფუძვლების გარეშე და სხვ.

მართალია, მოქალაქეთა და იურიდიულ პირთა მხრიდან ინსპექტორისადმი მიმართვის რაოდენობის ზრდა მიუთითებს პერსონალურ მონაცემთა დაცვის სფეროში ამ მექანიზმის მნიშვნელობაზე, მაგრამ გამოვლენილი ხარვეზები პრობლემად რჩება სახელმწიფოსთვის.

ამას ისიც ემატება, რომ სამართალდამცავ ორგანოებში ფიზიკურ პირთა შესახებ პერსონალური ინფორმაციის შემცველი მონაცემთა ბაზების დაცვისათვის მიღებული ორგანიზაციულ-ტექნიკური ღონისძიებები არ

არის შესაბამისობაში საერთაშორისო სტანდარტებთან. მაგალითად: ელექტრონული მონაცემების მიმართ შესრულებულ მოქმედებათა აღურიცხაობა; მონაცემთა შენახვის ვადების განუსაზღვრელობა; დანერგილ მონაცემთა ავტომატური წაშლის ან დეპერსონალიზაციის მექანიზმების არარსებობა; სხვა სახელმწიფო ორგანოების წარმომადგენლების წვდომის შესაძლებლობა დაცვის ობიექტთან. მონაცემთა დამუშავების მიზნისა და საფუძვლების არარსებობა; რადარისა და „ჭკვიანი“ კამერების საშუალებით ადმინისტრაციულ სამართალდარღვევების ფაქტის დაფიქსირება და ადმინისტრაციული სახდელის შეფარდების სხვადასხვა ეტაპზე შეგროვილი მონაცემების ჩაწერა, შენახვისა და გამოყენების პროცესის განსაზღვრა. სამინისტროს მხრიდან ამ მონაცემების დამუშავების პროცესში არ არის უზრუნველყოფილი კანონით გათვალისწინებული მონაცემთა უსაფრთხოების მოთხოვნები, არ აღირიცხება ელექტრონული მონაცემების მიმართ შესრულებული ყველა მოქმედება; თუ ამას იმასაც დავუმატებთ, რომ არსებობს ადვოკატის მიერ სხვისი მონაცემების გასაჯაროების ფაქტები პროფესიული საქმიანობის ფარგლებში. ნათელი ხდება რომ ორგანიზაციული ხასიათის მექანიზმები შევსებას ითხოვს უკუკავშირის ელემენტებით.

ასეთივე პრობლემაა ჯანდაცვის სფეროში მონაცემთა დამუშავების ორგანიზების საკითხებზე როგორც კერძო, ასევე საჯარო სფეროში. ჯანდაცვის სფეროში მონაცემების დამუშავების პროცესში არის დოკუმენტების ელექტრონული ასლების არასრული სახით აღრიცხვის შემთხვევები, რაც მონაცემთა გამჟღავნების რისკს წარმოშობს, ამასთან, შეუძლებელია სამართალდამრღვევი პირის იდენტიფიცირება. პაციენტზე ინფორმაციის კონფიდენციალობის დაცვის მკაცრი ნორმატიული რეგულირების მიუხედავად, ჯანდაცვის სფეროს უფლებამოსილი პირები ნაკლებად აქცევენ ყურადღებას იმ შედეგებს, რომლებიც შესაძლოა პერსონალური მონაცემების არაუფლებამოსილი პირისთვის გადაცემას მოჰყვეს.

აქედან გამომდინარე, ორგანიზაციული მექანიზმების სრულყოფის მიზნით, ჯანდაცვის სტრუქტურებმა უნდა შეიმუშაონ ინსტრუქციული დოკუმენტი, პაციენტის შესახებ ინფორმაციის მესამე პირისთვის გადაცემის

შესახებ, რომელშიც მოცემული იქნება ინფორმაციის გაცემის პირობები, ადვოკატირება; უსაფრთხოების წესები და ამ რეგულაციის შესრულებაზე მონიტორინგის მექანიზმები; ელექტრონული სისტემების გამოყენებით მონაცემთა დამუშავების შემთხვევები და სხვ.

ხშირია პირდაპირი მარკეტინგის მიზნებისთვის პერსონალური მონაცემების დამუშავების პროცესში დარღვევები. ესენია: სუბიექტის წერილობითი თანხმობის არარსებობა, სარეკლამო ტექსტებზე არ არის უარის თქმის მექანიზმი ან სხვა ადეკვატური საშუალებები; რაც შეეხება ბიომეტრიულ მონაცემების შეგროვებას, კომპანიები მას იყენებენ ისეთ შემთხვევებში, როცა შესაძლებელია მიზნის მიღწევა უფრო ნაკლები მოცულობის პერსონალური მონაცემების დამუშავებით.

ორგანიზაციულ მექანიზმებთან მჭიდრო კავშირშია სამართლებრივი მექანიზმები, რომელიც გულისხმობს კონსტიტუციურად აღიარებული უფლების დაცვის საკანონმდებლო გარანტიათა სისტემას. სამართლებრივ მექანიზმებში „პერსონალურ მონაცემთა დაცვის შესახებ“ და „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონების გარდა მოიაზრება სხვა დარგობ-რივი კანონები. როგოროცაა: ,,კომერციული ბანკების შესახებ“; ,,პაციენტის უფლების შესახებ“; ,,ზოგადი განათლების შესახებ“ და სხვა. აგრეთვე ინსტრუქციები და თვითრეგულირების აქტები, რომლებიც კერძო სექტორში არსებული მონაცემების დაცვას ისახავს მიზნად. საქმე ისაა, რომ კანონი ერთმანეთისგან არ მიჯნავს კერძო და საჯარო პირების პერსონალური მონაცემების დაცვის რეჟიმებს. საჯარო მოხელეების სამსახურებრივი უფლებამოსილების განხორციელებასთან დაკავშირებული ინფორმაცია, მოქალაქეებისათვის საჯარო უნდა იყოს დემოკრატიულ სახელმწიფოში არსებული გამჭვირვალობის მაღალი სტანდარტებიდან გამომდინარე. შესაბამისად, ამ კატეგორიის მონაცემებზე კონფიდენციალურობის რეჟიმის ნაცვლად მონაცემთა გავრცელების ლეგიტიმურობის რეჟიმი უნდა დაწესდეს.

გამომდინარე იქიდან, რომ პერსონალური მონაცემები სახელმწიფოს სტრატეგიული ობიექტია, იგი კონსტიტუციურ რეგლამენტაციაში უნდა მოექცეს. კერძოდ: საქართველოს კონსტიტუციის მე-7 მუხლის „დ“ ქვე-

პუნქტს, რომელიც ეხება საქართველოს უმაღლეს სახელმწიფო ორგანოთა განსაკუთრებულ გამგებლობას მიკუთვნებულ საკითხებს: სახელმწიფოს თავდაცვა, სამხედრო მრეწველობა და იარაღით ვაჭრობა; ომისა და ზავის საკითხები; საგანგებო და საომარ მდგომარეობათა სამართლებრივი რეჟიმის დადგენა და შემოღება; - უნდა დაემატოს სიტყვები „ინფორმაციული ტექნოლოგიები და პერსონალურ მონაცემთა მიმოქცევა“.

რაც შეეხება პერსონალურ მონაცემთა დაცვის ტექნიკურ მექანიზმებს, მათი როლი წამყვანია პერსონალურ მონაცემთა დაცვის სფეროში, რომელსაც სპეციალური ცოდნა სჭირდება. ორგანიზაციულ-სამართლებრივი მექანიზმების ეფექტურობა სწორად შერჩეული ტექნიკური საშუალებების ფონზეა შესაძლებელი.

ტექნიკური მექანიზმების მნიშვნელობა განაპირობებს პერსონალურ მონაცემთა სფეროში ორგანიზაციული და სამართლებრივი მექანიზმების ფორმირების დინამიკას. ტექნიკური მექანიზმები განაპირობებენ ტექნოლოგიური განვითარების პროცესში მონაცემთა დაცვის მაღალი სტანდარტის დამკვიდ-რების აუცილებლობას.

ამ მიმართულებით დისერტაციაში შესწავლილია „მონაცემთა დიდი მასივების“ (Big data) ტერმინოლოგიური და სამართლებრივი რეგულაციების თავისებურები, დასაბუთებულია მისი გამოყენების არეალი.

აღსანიშნავია, რომ ამ ტექნოლოგიას გარკვეული უპირატესობები აქვს საქართველოში იუსტიციის სისტემაში საჯარო რეესტრის უძრავი ქონების რეგისტრაციის „ბლოკჩეინ“ ტექნოლოგიის პროექტთან მიმართებაში. მონაცემები, რომლებიც ბლოკჩეინში მოხვდება სამუდამოდ რჩება იქ. ამიტომ ამ ტექნოლოგიის გამოყენებას აზრი იმ ამოცანების გადასაწყვეტად აქვს, როცა მონაცემები მოძველდა და ისინი გამოყენებისთვის უსარგებლოა. ბლოკჩეინთან დაკავშირებული ურთიერთობები არ რეგულირდება არც ერთი კანონმდებლობით, ამიტომ საკუთრების უფლებასთან დაკავშირებული ამოცანების გადასაწყვეტად არსებობს ამ უფლების დაუცველობის დიდი რისკი. შესაბამისად, ეს ტექნოლოგია მსოფლიოში მხოლოდ კრიპტოვალუტის სფეროში გამოიყენება.

„მონაცემთა დიდი მასივების“ ტექნოლოგიას ასევე გააჩნია გარკვეული საფრთხეები და რისკები. მისი დანერგვის ეფექტურობა დამოუკიდებელი რეგულაციის პრინციპს უკავშირდება. პერსონალურ მონაცემთა დაცვის კანონის წერტილოვანი მოდიფიცირება ამ სფეროში ეფექტური არ იქნება. ეს არის ადამიანის უფლებათა და თავისუფლებათა ციფრული აქტივების დაცვა საერთაშორისო შეთანხმებებისა და კონსტიტუციური რეგლამენტაციის საფუძველზე. მონაცემთა დიდი მასივების დამუშავების პროექტის რეალიზების ეფექტურობა, უპირველეს ყოვლისა, დამოკიდებულია უსაფრთხოების მექანიზმების შემუშავებაზე, რაც, თავის მხრივ, პროექტის ვადებსა და დაცვის სისტემის რეალიზაციის ხარჯებს ზრდის.

ტექნიკურ მექანიზმებს შორის ხაზი უნდა გაესვას კრიპტოგრაფიას, როგორც ინფორმაციის კონფიდენციალურობის უზრუნველყოფის საშუალებას. იგი შექმნილია თანამედროვე მათემატიკის, ფიზიკის, რადიო ელექტრონიკის, ინჟინერიისა და სხვა დარგების დარგთაშორისი კვლევის შედეგად და, როგორც ტექნოლოგია წარმოადგენს მონაცემთა შიფრაციის სტანდარტისა (Data Encryption Standard — DES) და გაუმჯობესებული (Advanced Encryption Standard — AES) სტანდარტის ერთ ბლოკს (3DES).

ამ მიმართულებით წინგადადგმული ნაბიჯია საქართველოს მთავრობის 2014 წლის 4 აპრილის №274 დადგენილებით საქართველოში ნატო-ს კლასიფიცირებული ინფორმაციის უსაფრთხოების უზრუნველმყოფი პასუხისმგებელი ორგანოებისა და მათი საქმიანობის განსაზღვრის წესის დამტკიცების შესახებ. თუმცა, უნდა ითქვას, რომ ეს საკმარისი არაა. აუცილებელია დამატებითი ღონისძიებების განხორციელება. როგორიცაა უსაფრთხოების ალიანსში გაერთიანება (Cloud Security Alliance) და შემდეგ ოთხ მიმართულებაზე ორიენტირება: ინფრასტრუქტურის უსაფრთხოება, მონაცემთა კონფიდენციურობა, მონაცემთა მართვა, რეაგირების პროცედურები.

მონაცემთა დიდი მასივების ტექნოლოგია მსოფლიოში დამკვიდრდა მას შემდეგ, რაც ინფორმაციამ ღირებული აქტივის სტატუსი შეიძინა, იგი შეიძლება „ახალ ნავთობსაც“ კი შევადაროთ, რადგან ინფორმაციული საზოგადოების მამოძრავებელი ძალაა, ტრადიციული ნავთობი კი - ინდუს-

ტრიული საზოგადოების მთავარი რესურსი. ამ ტექნოლოგიის უპირატესობები უკვე აპრობირებულია კლიენტთან ურთიერთობის ახალ ბიზნეს-მოდელებში, საჯარო სექტორში გამოიყენება კრიმინოგენულ სიტუაციასთან ბრძოლაში; აგრეთვე ჯანდაცვის სისტემის სრულყოფისათვის.

ჯანდაცვის სფეროში COVID-19 ინფექციის პირობებში პერსონალურ მონაცემთა დაცვის საკითხი კიდევ უფრო მეტი თავისებურებებით ხასიათდება.

ამ მიმართულებით გაწეული ღონისძიებები გარკვეულწილად პერსონალურ მონაცემთა დაცვის უფლების შეზღუდვასთანაა დაკავშირებული, ამიტომ სახელმწიფოთა მიერ რა გადაწყვეტილებაც არ უნდა იქნას მიღებული აუცილებელია მოქმედებაში მოვიდეს უფლებათა დაცვის მკაცრი სამართლებრივი და ტექნიკური გარანტიები. ერთი მხრივ, სახეზეა ადამიანის ჯანმრთელობისთვის მსოფლიო სამედიცინო სამყაროს გაერთიანება, რომელსაც კვლევისთვის სჭირდება დაავადების შესახებ მონაცემები, მეორე მხრივ, პერსონალური მონაცემების დაცვა რისკის ქვეშ დგება.

ამ შემთხვევაში „მონაცემთა დიდი მასივების“ ტექნოლოგიას აქვს გარკვეული უპირატესობები პანდემიასთან ბრძოლის სხვადასხვა ამოცანის გადასაწყვეტად;

ეს ის შემთხვევაა, როცა კანონმდებლობამ უნდა განსაზღვროს პაციენტის თანხმობის გარეშე პერსონალურ მონაცემთა დამუშავება ნორმის საკარანტინო ვადით არსებობის შესახებ. ვადის გასვლის შემდეგ კი ეს მონაცემები უნდა განადგურდეს, ან ისე დამუშავდეს, რომ პერსონალურ მონაცემთა სუბიექტის იდენტიფიცირების გარეშე შესაძლებელი იყოს მისი სამედიცინო კვლევითი მიზნებისთვის გამოყენება.

„მონაცემთა დიდი მასივების“ ტექნოლოგია რისკის შემცველია არასრულწლოვანთა პერსონალური მონაცემების დამუშავებისა და შრომითი ურთიერთობების მონაცემთა დამუშავების პროცესში.

პერსონალურ მონაცემთა დაცვის სფეროში სისტემური პრევენციისა და ორგანიზაციულ-სამართლებრივ-ტექნიკური მექანიზმების ურთიერთკავშირის უზრუნველყოფის მიზნით, მნიშვნელოვანია არსებობდეს მთავრობის მიერ დამტკიცებული სტრატეგია, რომელიც უნდა ჩამოყალიბდეს

შემდეგი ამოცანების მიხედვით: სტრატეგიის რეალიზაციის პრიორიტეტული ამოცანები და მიმართულებები, ინფრასტრუქტურის უსაფრთხოება; მონაცემთა კონფიდენციალურობის უზრუნველყოფა - ინტეგრაცია, კლასიფიკაცია, ინვენტარიზაცია, მონაცემებთან დაშვების პოლიტიკა; მონაცემების მართვა. მონაცემთა საცავების დაცვა, მონაცემთა ბაზის გასაღების მართვა; მონაცემთა სისრულე და რეაგირების პროცედურები. ბაზებთან მავნე ქმედების გამოვლენის ანალიტიკა, საფრთხეების გამოვლენა და რეაგირება, ანალიტიკის შედეგების უსაფრთხოება;

და, ბოლოს, ორგანიზაციულ-სამართლებრივი და ტექნიკური მექანიზმების კონსტრუირება პერსონალურ მონაცემთა დაცვის კარგი საშუალებაა. თუმცა, მათი არსებობა სტატიკურ გარემოში შეუძლებელია და ამიტომ, ახალი ტექნოლოგიების დანერგვის პირობებში მექანიზმთა ასეთი კონსტრუირება ითხოვს მათ სისტემურ მოდერნიზებას.

რეკომენდაციები

კვლევის შედეგად ორგანიზაციულ-სამართლებრივი და ტექნიკური მექანიზმების სრულყოფის მიზნით, გამოიკვეთა რამდენიმე რეკომენდაცია:

1. საქართველოს მთავრობის დონეზე დასამტკიცებელია პერსონალურ მონაცემთა დაცვის სტრატეგია, ნაშრომში მოცემული საკითხებისა და ამოცანების მიხედვით;
2. საქართველოს კონსტიტუციის მე-7 მუხლის „დ“ ქვეპუნქტს დაემატოს სიტყვები „ინფორმაციული ტექნოლოგიები და პერსონალურ მონაცემთა მიმოქცევა“;
3. COVID-19-სა და სხვა ინფექციური დაავადებების შესწავლისა და პროფილაქტიკის მიზნით, დაინერგოს „მონაცემთა დიდი მასივების“ ტექნოლოგია. ხოლო პაციენტთა უფლებების შესახებ საქართველოს კანონში გაკეთდეს შესაბამისი დათქმა: პანდემიის პირობებში პაციენტის თანხმობის გარეშე პერსონალურ მონაცემთა დამუშავება ნორმის საკარანტინო ვადით არსებობის შესახებ. ვადის გასვლის შემდეგ ეს მონაცემები უნდა განადგურდეს.

ნაშრომის აპრობაცია

სადისერტაციო ნაშრომის ძირითადი დებულებები გამოქვეყნებულია ავტორის შრომებში, სტატიებში, კოფერენციაზე და გადმოცემულია ინფორმაციის სახით დისერტანტის მიერ შესრულებულ კოლოქვიუმებში:

თემატური კოლოქვიუმები:

1. ,,პერსონალურ მონაცემთა დაცვის კანონმდებლობა საქართველოში“ - პირველი თემატური კოლოქვიუმი. 15 თებერვალი 2017 წელი;
2. ,,შრომით ურთიერთობებში პერსონალური მონაცემების დაცვის პრობლემატიკა საქართველოში“ - მეორე თემატური კოლოქვიუმი. 7 ივლისი 2017 წელი.
3. ,,პერსონალურ მონაცემთა დაცვის მდგომარეობა საქართველოში და მისი კვლევითი ანალიზი“ - მესამე თემატური კოლოქვიუმი. 6 თებერვალი 2018 წელი.

სადისერტაციო ნაშრომის ძირითადი დებულებები გამოქვეყნებულია ფაკულტეტის სადისერტაციო საბჭოს მიერ რეკომენდებულ საერთაშორისო რეფერირებად ჟურნალებში:

სტატიები:

1. პრივატულობა თანამედროვე ეპოქაში. სამეცნიერო ჟურნალი ,,ხელისუფლება და საზოგადოება (ისტორია, თეორია, პრაქტიკა)”. ISSN 1512-374X. №1(53) 2020, გვ. 99-105.
2. პირადი ცხოვრების დაცვა თანამედროვე ეპოქაში. საერთაშორისო რეფერირებადი სამეცნიერო-პრაქტიკული ჟურნალი „იურისტი“. ISSN 9772449270009. №9, 2020, გვ. 107-112.
3. პერსონალურ მონაცემთა დაცვის ისტორია 1918-1921 წლების საქართველოში. სამეცნიერო ჟურნალი ,,ხელისუფლება და საზოგადოება (ისტორია, თეორია, პრაქტიკა)”. ISSN 1512-374X. №2 (54) 2020, გვ. 55-60.

კონფერენციები:

1. შრომით ურთიერთობებში პერსონალური მონაცემების დაცვის პრობლემატიკა საქართველოში. საქართველოს ტექნიკური უნივერსიტეტის II საერთაშორისო სამეცნიერო კონფერენცია „გლობალიზაცია და ბიზნესის თანამედროვე გამოწვევები“. საქართველო, თბილისი, 2018 წელი.