საქართველოს ტექნიკური უნივერსიტეტი

ხელნაწერის უფლებით

**გიორგი იაშვილი**

# უსაფრთხო დიზაინი კრიპტოგრაფიაში

დოქტორის აკადემიური ხარისხის მოსაპოვებლად

წარდგენილი დისერტაციის

**ა ვ ტ ო რ ე ფ ე რ ა ტ ი**

სადოქტორო პროგრამა: ინფორმატიკა

შიფრი: 0613

თბილისი

2021

სამუშაო შესრულებულია საქართველოს ტექნიკურ უნივერსიტეტში ინფორმატიკისა და მართვის სისტემების ფაკულტეტი

გამოთვლითი მათემატიკის დეპარტამენტი

ხელმძღვანელი: პროფესორი **მაქსიმ იავიჩი**

რეცენზენტები:

დაცვა შედგება 2021 წლის---------- საათზე საქართველოს ტექნიკური უნივერსიტეტის ინფორმატიკის, მართვის და ხელსაწყოთმშენებლობის საუნივერსიტეტო სადისერტაციო საბჭოს სხდომაზე, კორპუსი ----------, აუდიტორია ----------

მისამართი: 0175, თბილისი, კოსტავას 77.

დისერტაციის გაცნობა შეიძლება სტუ-ის ბიბლიოთეკაში,

ხოლო ავტორეფერატისა - ფაკულტეტის ვებგვერდზე

საუნივერსიტეტო სადისერტაციო საბჭოს
მდივანი, პროფესორი თ. კაიშაური

**თემის აქტუალობა.** კრიპტოგრაფია დღეისთვის არის კიბერ უსაფრთხოების ერთ-ერთი ყველაზე მნიშვნელოვანი მიმართულება. თანამედროვე უსაფრთხოების მექანიზმები ეყრდნობა ამ მიმართულებას. ტექნოლოგიების განვითარებასთან ერთად კიბერ უსაფრთხოების საკითხი ხდება სულ უფრო აქტუალური. კიბერ უსაფრთხოების პროცესების სწორი განაწილების გარეშე სისტემის მომხმარებლები შეიძლება აღმოჩდნენ სერიოზული პრობლემების წინაშე და შედეგად მივიღოთ კრიტიკული დარღვევების მთელი რიგი. ნებისმიერი სისტემის მომხმარებელს კარგად უნდა ჰქონდეს გააზრებული ამ სისტემის სამუშაო მექანიზმები, მაგალითად თუ ჩვენ ვიყენებთ რაიმე ტიპის ვებ საიტს და ამ პორტალზე გვჭირდება ავტორიზაციის გავლა - შეგვყავს ჩვენი მომხმარებლის მონაცემები მომხმარებლის სახელისა და პაროლის სახით. მომხმარებელმა იცის, რომ ეს ქმედება არის აუცილებელი მისი სისტემაში ავტორიზაციისთვის და მონაცემების უსაფრთხოებისთვის, რათა პროფილში ინახება მისი პირადი ან/და საკონტაქტო მონაცემები. ზოგ შემთხვევაში, თუკი მომხმარებელი მუშაობს მაგალითად ელექტრონული კომერციის სისტემებში ან ონლაინ მაღაზიებში, პირადი მონაცემების სიაში ასევე შედის ფინანსური მონაცემები, ისეთი როგორიცაა საბანკო ბარათის სრული ინფორმაცია. ასეთი ტიპის ინფორმაციის დაკარგვისას და მესამე პირის ხელში აღმოჩენისას, ხდება სერიოზული უსაფრთხობის პრობლემის საკითხი და ამ ვითარებამ შესაძლოა გამოიწვიოს მომხმარებლის როგორც ფინანსური ასევე ინფორმაციული დანაკარგი.

გამომდინარე იქიდან, რომ დღეისთვის მრავალ მომხმარებლიანი სისტემები არის ძალიან გავრცელებული, და წარმოდგენილია მაგალითად სოციალური ქსელების სახით, მომხმარებლების უსაფრთხოების დონე ამ სისტემებში არის ერთ-ერთი პრიორიტეტი. უსაფრთხოების მექანიზმები ხდება კრიტიკულად მნიშვნევანი და აქტუალური როცა მომხმარებლის მიეს გამოყენებადი სისტემა არ არის ბოლომდე კომფორტული და გასაგები. მომხმარებლის უსაფრთხოების ასპექტები ყოველთვის დაკავშირებულია მეორე კომპონენტთან და ეს არის გამოყენებადობა. ნებიესმიერ შემთხვევაში, როცა ხდება მუშაობა მომხმარებლის სისტემებზე, უსაფრთხოებასთან ერთად განიხილება ამ

სისტემის გამოყენებადობის დონე, რაც განპირობებულია დღევანდელი ტენდენციებით კომპიუტერულ სისტემებში. არაგამოყენებადი სისტემა ვერ იქნება წარმატებული ერთი აშკარა მიზეზის გამო - მომხმარებელს არ უნდა დამატებითი მოქმედებების გაკეთება შედეგის მისაღწევად. ყოველი დამატებითი ქმედება მომხმარებლისთვის არის გარკვეული დისკომფორტი, შესაბამისად ერთ-ერთი ყველაზე მნიშვნელოვანი საკითხი მომხმარებლის უსაფრთხოებაში არის კონკრეტულად გამოყენებადობის მაღალი დონის უზრუნველყოფა.

კიბერ უსაფრთხოების გამოყენებადობა განისაზღვრება უსაფრთხოების მექანიზმის გამოყენების სიმარტივით. რაც უფრო მარტივია მექანიზმი გამოყენებისთვის, მით უფრო აქტიურადაა ჩართული სისტემურ პროცესებში მომხმარებელი. პრობლემები გამოყენებადობასთან იწვევენ ასევე უსაფრთხოეიბს პრობლემებსაც ერთი მარტივი მიზეზიზ გამო - თუკი უსაფრთხოების მექანიზმი არ არის გამოყენებადი, მომხმარებელი გააკეთებს ყველაფერს, იმისათვის, რომ ამ უსაფრთხოების მექანიზმს აარიდოს თავი.

უსაფრთხოების მექანიზმების უმრავლესობა მუშაობს, ე.წ. უკანა ფონზე, ისე რომ მომხმარებელი ვერც კი ამჩნევს მათ მუშაობას სისტემაში. ზოგი მექანიზმი კი ითხოვს მომხამერბლის უსაფრთხოების პროცესებში ჩართულობას, მაგალითად ზოგიერთ სისტემაში რეგისტრაციის დროს მომხმარებელს მოეთხოვება ე.წ. უსაფრთხოების კითხვის მოფიქრება, რომელიც არის ერთგვარი დამატებითი ბერკეტი, როცა მომხმარებელს მაგალითად დაავიწყდა პაროლი და სჭირდება მისი აღდგენა.

შიფრაციის მექანიზმები წარმოადგენს ერთ-ერთ ყველაზე საჭირო და ზოგ შემთხვევაში აუცილებელ უსაფრთხოების ზომას. კრიპტოგრაფიული ელემენტები გამოიყენება ძალიან ბევრ დარგში, დაწყებული სხვა და სხვა ვებ სისტემებით, დამთავრებული საბანკო ოპერაციებით ან ონლაინ თამაშებით. შიფრაციის მეგანიზმები არის საჭიროა მომხმარებლების და სისტემების ინფორმაციის დაცვისთვის. დღეისთვის უსაფრთხოების მექანიზმების დიდი ნაწილი არ გამოირჩევა გამოყენებადობის მაღალი დონით, რაც იმას ნიშნავს, რომ მომხმარებელმა ამ უსაფრთხოების ელემენტების გამოყენებისთვის უნდა შეასრულოს ბევრი ქმედება და ხშირ შემთხვევაში მომხმარებელს არ აქვს საკმარისი ცოდნა იმისთვის, რომ სრულყოფილად მოახდინოს ამა თუ იმ

უსაფრთხოების მექანიზმის საჭირო დონეზე გამართვა. ეს ფაქტი იწვევს მთელი სისტემის და მისი მომხმარებლების უსაფრთხოების საკითხის ქვეშ აღმოჩენას, რათა უსაფრთხოების სისტემის სწორი გამართვა არის ერთ-ერთი ყველაზე მნიშვნელოვანი დაცვითი მექანიზმების ამუშავებისთვის.

ჩემს ნაშრომში განხილულია და შესწავლილია ისეთი დღეისთვის აქტუალური საკითხი, როგორიცაა მომხმარებელზე მორგებული უსაფრთხოების მექანიზმები და მანქანური სწავლების ელემენტები კიბერ უსაფრთხოებაში, რაც იმას ნიშნავს, რომ დაცვითი სისტემების გამართულობა და მათი გამოყენებადობის დონე პირდაპირ არის კავშირში მომხმარებლის კომფორტულ მუშაობასთან. დღეისთვის ბევრი უსაფრთხოეიბს მექანიზმის პრობლემა არის იმაში, რომ მომხმარებლისთვის ეს მექანიზმები გაუგებარია, შესაბამისად, არ არის გამოყენებადი და უსაფრთხოება რომელსაც არ იყენებენ პრაქტიკაში უბრალოდ ვერ იარსებებს. ნაშრომში შეთავაზებულია უსაფრთხოეიბს დონის გაზრდისთვის სრულიად ახალი მეთოდი, რომელიც საგრძნობლად ამცირებს მომხმარებლის მხრიდან მოქმედებების რაოდენობას და ხდის უსაფრთხოეიბს მექანიზმს ბევრად უფრო გასაგებს, რაც მნიშვნელოვნად გაზრდის მომხმარებლების მიერ უსაფრთხოების მექანიზმების გამოყენებას, შესაბამისად გაიზრდება უსაფრთხოების სისტემების გამოყენებადობის ზოგად დონეს.

**მეცნიერული სიახლე.** სადისერტაციო ნაშრომის მეცნიერული სიახლეს წარმოადგენს არსებული კიბერ უსაფრთხოების მექანიზმების და მასში მანქანური სწავლების ელემენტების სრულიად ახალი მიდგომის შეთავაზებას. დღეისთვის არსებული შიგთავსზე დაფუძნებული ფილტრაციის მექანიზნები მუშაობს ე.წ. რეკომენდაციების სისტემების ფარგლებში, ეს სისტემები გამოიყენება ისეთ სფეროებში, როგორიცაა სოციალური ქსელები, ფილმების ან სხვა კონტენტის შეთავაზების პლატფორმები. მსგავსი ტიპის შიგთავსზე დაფუძნებული მექანიზმები არ გამოიყენება კიბერ უსაფრთხოების მიმართულებით, კომპონენტების სპეციფიკიდან გამომდინარე. კვლევის ფარგლებში მოვახდინე არსებული შიგთავზე დაფუძნებული ფილტრაციის მექანიზმების შესწავლა და სრულიად ახალი მიდგომის შეთავაზება. ეს მიდგომა ეფუძნება მანქანური

სწავლების ელემენტების, კერძოდ კი შიგთავზე დაფუძნებული ფილტრაციის მიდგომების კიბერ უსაფრთხოებს სარეკომენდაციო სისტემაში გამოყენებას. ასეთი მიდგომა არის ინოვაციური როგორც სამეცნიერო ასევე პრაქტიკული კუთხით და იძლევა საშუალებას გამოვიყენოთ მანქანური სწავლების ელემენტები მომხმარებლის მიერ გამოყენებად სისტემებში, რაც საგრძნობლად გააუმჯობესებს მომხმარებლების უსაფრთხოების დონეს. კვლევის ფარგლებში შემუშავებული მიდგომა არის სრულიად ახალი და მისი ანალოგი დღეისთვის არ არსებობს. შეთავაზებული მექანიზმი იძლევა საშუალებას მივიღოთ სარეკომენდაციო შედეგი მანქანური სწავლების, კონკრეტულად კი შიგთავსზე დაფუძნებული ფილტრაციის ელემენტების საშუალებით, რაც კიბერ უსაფრთხოების მიმართულებით არის ინოვაციური. აღსანიშნავია, რომ კვლევის ფარგლებში არსებული შიგთავსზე დაფუძნებული ფილტრაციის მანქანური სწავლების ალგორითმები იქნა შეცვლილი და მორგებული კიბერ უსაფრთხოების მოთხოვნებსა და რეალურ გარემოს, რამაც მნიშვნელოვნად გაზარდა საბოლოო პროდუქტის მეცნიერული მნიშვნელობა.

**კვლევის მიზანი.** კვლევის მიზანია შეიქმნას სისტემა, რომლის გამოყენებისას მომხმარებელი უფრო მარტივად შეძლებს საკუთარი კიბერ უსაფრთხოების დონის გაზრდას შესაბამისი რეკომენდაციების საფუძველზე. სისტემა ორიენტირებულია უსაფრთხოების შესაძლო მაქსიმალურ დონეზე, საუკეთესო გამოყენებადობის მეთოდების ჩართვით. კვლევის მიზანი და ამოცანები დღევანდელ რეალობაზე დაყრდნობით არის შემდეგი: გამომდინარე იქიდან რომ მრავალ მომხმარებლიან სისტემებში, ისეთებში, როგორიცაა მაგალითად ვებზე დაფუძნებული პროგრამები ან საიტები, უსაფრთხოების დონე ძალიან ხშირად არის დამოკიდებული გამოყენებადობაზე, თუ სისტემა არაა გამოყენებადი, მომხმარებელი შეეცდება მისი ალტერნატივის პოვნას. კვლევის მიზანი არის უსაფრთხოების მექანიზმებს და სისტემის გამოყენებადობის უკეთესი ბალანსის პოვნა, რათა გამოყენებადი სისტემა ყოველთვის იქნება უფრო კომფორტოლი მომხმარებლისთვის და ეს უკანასკნელი იქნება ჩართული ან სისტემებით განპირობებულ პროცესებში.

მიზნის მისაღწევად საჭიროა შემდეგი ამოცანების პოზიციონირება:

- იქნეს განხილული დღეისთვის არსებული მომხმარებელზე ორიენტირებული უსაფრთხოების მექანიზმები;
- გამოვლინდეს ამ უსაფრთხოების მექანიზმებში არსებული გამოყენებადობის პრობლემები;
- მიღებული ინფორმაციის საფუძველზე შემუშავდეს ახალი, უფრო დაბალანსებული და გამოყენებადი სქემები;
- მოხდეს მიღებული დაბალანსებული სქემების ინტეგრაცია პროგრამულ რეალიზაციაში;

**კვლევის ობიექტი და მეთოდები.** კვლევის ობიექტი არის არსებული მომხმარებელზე ორიენტირებული უსაფრთხოების მექანიზმების შესწავლა და მათში გამოყენებადობის პრობლემების გამოვლენა. კვლევის საგანს წარმოადგენს გამოყენებადობის ახალი მექანიზნების რეველანტურობის შეფასება და კიბერ უასფრთხოების და გამოყენებადობის შორის უკეთესი ბალანსის შემუშავება. არსებული უსაფრთხოების სისტემების გამოყენება ხშირ შემთხვევაში არის საკმაოდ რთული საბოლოო მომხმარებლისთვის, რადგან ამ სისტემებს არ გააჩნია გამოყენებადობის მაღალი დონე.
კვლევის თეორიული და მეთოდოლოგიური საფუძვლები წარმოდგენილია როგორც თეორიული მიდგომების და მეთოდების სიღრმისეული განხილვით ასევე პრაქტიკული შედეგების გაანალიზებით. კვლევის ფარგლებში იქნა განხილული როგორც ლოკალური, ასევე საერთაშორისო სამეცნიერო ნაშრომები, სტატიების, წიგნების და სხვადასხვა თემატურ კონფერენციებზე წარმოდგენილი პრაქტიკული შედეგების სახით. მოყვანილი ყწაროები წარმოადგენს კვლევის თეორიულ და მეთოდოლოგიურ საფუძვლებს. ამასთან ერთად კვლევის მეთოდოლოგიურ საფუძვლებზე გავლენა მოახდინა გლობალურ ქსელში სპეციალიზირებულ ინტერნეტ სერსურსებზე არსებულმა პრაქტიკებმა, რომლებშიც განიხილება სხვადასხვა უსაფრთხოების სისტემების გამოყენებადობის მაგალითები და არსებული პრობლემები.

სადოქტორო კვლევის ფარგლებში ასევე იყო განხილული და შესწავლილი კიბერ უსაფრთხოებაში არსებული გამოყენებადობის პრობლემები. კერძოდ, თანამედროვე უსაფრთხოების სისტემების მორგება მომხმარებლზე, რამაც გამოიწვია მომხმარებლების მიერ ამ აუცილებელი უსაფრთხოების მექანიზნების პრაქტიკაზე უფრო ხშირ გამოყენებას.

სადოქტორო კვლევის ფარგლებში იქნება შესწავლილი კიბერ უსაფრთხოების დარგის წამყვანი პრაქტიკოსი სპეციალისტების სამეცნიერო ლიტერატურა. არის ჩამოყალიბებული პრობლემა თანამედროვე უსაფრთხოების სისტემების გამოყენებაზე. კერძოდ კი პრობლემა ეხება უსაფრთხოების სისტემების გამოყენებადობას. თავისი სტრუქტურით დღევანდელი უსაფრთხოების მექანიზმები არის რთული და მომხმარებლების უმრავლესობისთვის გაუგებარიც კი.

ჩემი მიზანი კვლევის ფარგლებში იყო მაქსიმალურად გავამარტივო უსაფრთხოების მექნიზმების გამოყენება უბრალო მომხმარებლებისთვის, რაც საგრძნობლად გაზრდის ამ უკანასკნელების გამოყენებას. უსაფრთხოების მექანიზმების ხშირი გამოყენება კი გაზრდის ზოგად უსაფრთხოების დონეს. უნდა იყოს გათვალისწინებული კრიპტოგრაფიული მექნიზმების სირთულეები და გამოყენებადობის პრობლემები. ამის შემდეგ უნდა იყოს გაანალიზებული კრიპტოგრაფიული მექნიზმების მოხმარებისთვის რთული ასპექტები. ყველაზე რთული ასპექტების გამოვლენის შემდეგ იქნება შესაძლებელი აქცენტების განაწილება და სამუშაოს მიმართულების აღება. გამოყენებადობის პრობლემების ჩამოყალიბება მოხდება შესაბამისი სამეცნიერო ლიტერატურის გაანალიზებით. კვლევის ერთი ეტაპი დაეთმობა უკვე არსებული სისტემების გაანალიზებას და მათში გამოყენებადობის პრობლემების გამოვლენას.

ცნობილია, რომ დღეისთვის არსებული უსაფრთხოების მექანიზმები ხშირ შემთხვევაში არ არის მორგებული მომხმარებელზე და შედარებით რთულია გამოყენებისთვის. გამოვლენილი პრობლემების საფუძველზე, სადოქტორო კვლევის ფარგლებში შემუშავდება შესაბამისი პროტოტიპი, რომელიც შემოწმდება როგორც უბრალო მომხმარებლების მიერ, ასევე იქნება გაგზავნილი კიბერ უსაფრთხოების დარგის

ექსპერტებთან ანალიზისთვის და მისი პრაქტიკული ასპექტების გავლისათვის. მიღებული შედეგები იქნება შესწავლილი, ხოლო კიბერ უსაფრთხოების სპეციალისტების მითითებები იქნება გათვალისწინებული და დანერგილი სისტემის მექანიზმში.

**პრაქტიკული მნიშვნელობა.** ნაშრომ გააჩნია პრაქტიკული მნიშვნელობა კიბერ უსაფრთხოეიბს და გამოყენებადობის გამოუჯობესების კუთხით. კვლების ფარგლებში შემუშავდა სპეციალიზაირებული პლატფორმა, რომელზეც მომხმარებელს შეუძლია მოხმარების და მუშაობის სცენარის მიხედვით კონკრეტული მონაცემების შეყვანა. ამისთვის პლატფორმას გააჩნია სპეციალიზირებული ინტერაქტიული ფორმა. ამგვარად მომხმარებელი ახდენს მონაცემების შეყვანას, რის შემდეგაც სისტემა აყალიბებს შესაბამისი რეკომენდაციების ვარიანტს და მომხმარებელს შეუძლია საჭირო ინფორმაციის მიღება მარტივი და გასაგები ფორმით. უსაფრთხოების მექანიზმების უმრავლესობას გააჩნია გამოყენებადობის პრობლემები, შესაბამისად, მომხამერებლისთვის საკმაოდ რთულია მათი პრაქტიკაში გამოყენება. ეს არის განპირობებული მომხმარებლების სხვადასხვა დონით კომპიუტერული მეცნიერების და კიბერ უსაფრთხოების მიმართულებით. კვლევის ფარგლებში შექმნილი პლატფორმის მეშვეობით საგრძნობლად იზრდება უსაფრთხოების მექანიზმების გამოყენებადობის დონე, რადგან მიღებული მონაცემების საფუძველზე სისტემა ახდენს შესაბამისი რეკომენდაციების წარდგენას მომხმარებლისთვის მაქსმალურად მარტივი ფორმით. სადოქტორო კვლევის ფარგლებში შემუშავებული პლატფორმა და ინტერაქტიული ფორმა შეიძლება იყოს გამოყენებული პრაქტიკაზე ძალიან ბევრი დარგისთვის მიუხედავად მომხმარებლების სამუშაო მიმართულების ან გამოცდილებისა.

**კვლევის ძირითადი შედეგები.** სადოქტორო კვლევის შედეგად მიღებულია ინტერაქტიული სისტემა, რომელსაც საფუძვლად ჩაედო მანქანური სწავლების ერთ-ერთი რელევანტური პრინციპი - შინაარსე დაფუძნებული სარეკომენდაციო ალგორითმი, რომელიც ძალიან კარგად ახდენს სარეკომენდაციო პროცედურების განხორციელებას ისეთ დარგებში როგორიცაა მაგალითად სოციალური ქსელები, სხვადასხვა ფილმების ან

ტურიზმის პლატფორმები, საგანმათლებლო სისტემები და სხვა. ასეთი ტიპის ალგორითმი გამოიყენება მომხმარებლისთვის უკეთესი შინაარსის შეთავაზებისთვის და ეყრდნობა რამდენიმე ფაქტორს.

სადოქტორო კვლევის ფარგლებში იქნა შემუშავებული სარეკომენდაციო ალგორითმის სრულიად ახალი მიდგომა, რომელიც გამოიყენება კიბერ უსაფრთხოების რეკომენდაციების მიმართულებით. აქამდე ასეთი ტიპის ალგორითმები გამოიყენებოდა სხვა დარგებში რეკომენდაციების გასაწევად. ჩემი სადოქტორო კვლევის ფარლებში მოვახდინე სარეკომენდაციო ალგორითმის ახალი მიმართულებით შექმნა, რომელიც მიმართულია მომხმარებლისთვის კომფორტული და გასაგები ფორმით შესაბამისი უსაფრთხოების რეკომენდაციების გაცემაზე.

ამასთან ერთად, კვლევის ფარგლებში იყო გათვალისწინებული და საბოლოო პროდუქტში შეტანილი უსაფრთხო დიზაინის და გამოყენებადობის ძირითადი კონცეფციები, რათა სისტემა გამხდარიყო ბევრად უფრო მოსახერხებელი და გასაგები მომხმარებლისთვის. აქვე ავღნიშნავ, რომ ჩემი კვლევის ფარგლებში აღმოვაჩინე, რომ მანქანური სწავლების ალგორითმები დღეისთვის არის რამდენიმე მიმართულებით მომუშავე სქემები და შესაძლებელია რამდენიმე ალგორითმის პრინციპის გაერთიანება, რაც სამომავლოდ უფრო დახვეწილ და რელევანტურ შედეგს მოიტანს.

**დისერტაციის სტრუქტურა და მოცულობა.** სადოქტორო ნაშრომი შედგება შესავლისგან, ოთხი თავისგან ოცი ქვეთავისგან, დასკვნებისგან და გამოყენებული ლიტერატურის სიისგან. ნაშრომში წარმოდგენილია 24 გრაფიკული გამოსახულება.

## ნაშრომის ძირითადი შინაარსი

თავი 1. თანამედროვე უსაფრთხოების მექანიზმები პრაქტიკაში

პირველ თავში განხილულია დღეისთვის არსებული კიბერ უსაფრთხოების მექანიზმები პრაქტიკაზე. კრიპტოგრაფია თანამედროვე კომპიუტერულ სამყაროში არის ერთ-ერთი მნიშვნელოვანი უსაფრთხოების მექანიზმი, რომელიც გამოიყენება კიბერ სივრცის პრაქტიკულად ყველა მიმართულებაში დაწყებული უბრალო ვებ საიტებით

დამთავრებული სამხედრო და კრიტიკული ინფრასტრუქტურის ობიექტებით. კრიპტოგრაფიულ მექანიზმებს გააჩნია სერიოზული დატვრითვა უსაფრთხოების დონის უზრუნველყოფისთვის. ამ მექანიზმის პრინციპი წარმოადგენს მონაცემების შიფრაციას, ერთადერთი მიზნით - უსაფრთხოების უზრუნლვეყოფა. თუკი დაუშიფრავი მონაცემები აღმოჩნდება ბოროტმოქმედის ხელში, იგი შეძლებს მათ ბოროტად გამოყენებას და სერიოზული ზიანის მიყენებას როგორც მომხმარებლებისთვის ასევე იმ სისტემისთვის, რომელსაც იყენებენ ეს მომხმარებლები. უსაფრთხოების საკითხს ყოველთვის ეკავა უმნიშვნელოვანესი ადგილი საზოგადოებაში. უახლესი ტექნოლოგიების განვითარებასთან ერთად დგება ინფორმაციული ან კომპიუტერული უსაფრთხოების საკითხი, რადგან ჩვენი ცხოვრების უფრო და უფრი დიდი ნაწილი გადადის ციფრულ სამყაროში. თანხის ბრუნვა, სხვადასხვა ნივთების შეძენა, დოკუმენტების გადაცემა, პირის იდენტიფიცირება და მრავალი სხვა ჩვენი ცხოვრების ასპექტი უკავშირდება ელექტრონულ სამყაროს.  თითოეული ადამიანის მონაცემები და პირადი ინფორმაცია უნდა იყოს დაცული და მათზე წვდომა უნდა იყოს შეზღუდული. თუ კი რომელიმე მონაცემი ან/და მომხმარებლის პირადი ინფორმაცია ხდება ნათელი მესამე პირისთვის, ეს ნიშნავს იმას, რომ დაცვითმა მექნიზმმა შესაბამისად არ იმუშავა და გამოყენებულ კრიპტო სისტემაში არსებობს ხარვეზები. დღეისთვის არსებულ თანამედროვე კრიპტო სისტემებს გააჩნია გარკვეული ეფექტურობის პრობლემები და მათზე ფიქსირდება წარმატებული თავდასხმები. კრიპტოგრაფიული სისტემების გატეხვა შეიძლება იყოს გამოწვეული სხვადასხვა ფაქტორებით, როგორც არაეფექტური დაცვითი მექანიზმებით, ასევე კრიპტო სისტემების არასწორი გამოყენებით.

## 1.1. კვანტური კომპიუტერები და მათი შესაძლებლობები

კვლევის ფარგლებში უნდა გავაანალიზოთ სხვადასხვა ტიპის თავდასხმები არსებულ კრიპტო სისტემებზე და განვიხილოთ თანამედროვე სისტემების სუსტი მხარეები, მათ გამოყენებას და არსებული კრიპტო სისტემების ალტერნატივებს კვანტური კომპიუტერების თავდასხმების წინააღმდეგ. ეს უკანასკნელი კლასიკურ კომპიუტერებთან შედარებით გამოირჩევა გამოთვლების უმაღლესი სიჩქარით.

კვანტური კომპიუტერების შესაქმნელად აქტიურად მუშაობენ მსოფლიოს წამყვანი მეცნიერები და კიბერ უსაფრთხოების ექსპერტები. გამოქვეყნდა პუბლიკაცია იმის თაობაზე, რომ კორპორაცია Google, NASA და კოსმოსური კვლევების უნივერსიტეტების ასოციაციამ (Universities Space Research Association) გააფორმეს ხელშეკრულება D-Wave პროცერორების მწარმოებელთან, რისი საგანაც არის კვანტური პროცესორის შექმნა.
არსებობს ორი ტიპის კრიპტოგრაფია: პირველი ტიპის კრიპტოგრაფია არ მისცემს საშუალებას შენს მეგობარს, რომ წაიკითხოს შენი წერილები და მეორე ტიპის კრიპტოგრაფია მთავრობას არ მისცემს საშუალებას წაიკითხოს შენი დოკუმეტები.

თუ ავიღებთ წერილს და შევინახავთ სხვა ქალაქში, ან ქვეყანაში, უცნობ სეიფში და გარკვეული პერიოდის შემდეგ დაგვჭირდა ამ წერილის წაკითხვა, ამ შემთხვევაში საქმე გვაქვს გაუგებრობასთან და არა უსაფრთხოებასთან. მეორეს მხრივ, თუ ავიღებთ წერილს, განვათავსებთ ისეთ სეიფში, რომლის ზომა, წონა, ჩამკეტის სპეციფიკა და სხვა ელემენტები არის ცნობილი, მათ შორის მსოფლიოს ყველაზე კვალიფიციურ სეიფების გამხსნელებს და ამის გათვალისწინებით ვერ ხერხდება ამ სეფიდან წერილის ამოღება, მაშინ შეიძლება ითქვას, რომ ეს სეიფი არის უსაფრთხო. წლების განმავლობაში მსგავსი კრიპტოგრაფია იყო სამხედრო სფეროს ნაწილი. აშშ-ს ნაციონალური უსაფრთხოების სააგენტო და მათი მოკავშირეები, ყოფილი საბჭოთა კავშირის ქვეყნების, ინგლისის, ისრაელის, და სხვა ქვეყნების სახით ხარჯავდნენ მილიარდობით დოლარს სხვისი უსაფრთხოების სისტემების გასატეხად. ქვეყნები რომლებსაც არ ჰქონდათ საკმარისი გამოცდილება და ფინანსური სახსრები თავიანთ სისტემებს ვერ იცავდნენ უფრო ძლიერი ქვეყნებისგან.
ამასთან ერთად პირველ თავში საუბარია კვანტურ კომპიუტერებზე და მათ სიმძლავრეზე. კვანტური კომპიუტერი კლასიკურ კომპიუტერებთან შედარებით გამოირჩევა გამოთვლების უმაღლესი სიჩქარით. კვანტური კომპიუტერების შესაქმნელად აქტიურად მუშაობენ მსოფლიოს წამყვანი მეცნიერები და კიბერ უსაფრთხოების ექსპერტები. გამოქვეყნდა პუბლიკაცია იმის თაობაზე, რომ კორპორაცია Google, NASA და კოსმოსური კვლევების უნივერსიტეტების ასოციაციამ (Universities Space

Research Association) გააფორმეს ხელშეკრულება D-Wave პროცერორების მწარმოებელთან, რისი საგანაც არის კვანტური პროცესორის შექმნა.

D-Wave 2X - უახლესი კვანტური პროცესორია, რომელიც შეიცავს 2048 ფიზიკურ კუბიტს (კვანტური განმუხტვები, ინფორმაციის შენახვის უმცირესი ერთეული კვანტურ კომპიუტერში). გამოთვლების შესასრულებლად კვანტური კომპიუტერის ამ მოდელში გამოიყენება 1152 კუბიტი. თითოეული დამატებითი კუბიტი აორმაგებს ძიების არეს, ამასთან ერთად იზრდება გამოთვლების სიჩქარეც. ზემოთ აღნიშნულიდან გამომდინარე ხდება ნათელი, რომ კვანტურ კომპიუტერს შესაძლებლობა ექნება დაანგრიოს უმეტესი ნაწილი, თუ არა აბსოლუტურად ყველა ტრადიციული კრიპტოსისტემა, რომელიც ფართოდ გამოიყენება პრაქტიკაში, და კონკრეტულად მთელი რიცხვების ფაქტორიზაციის ამოცანაზე დაფუძნებული სისტემები, როგორიც არის RSA სისტემა. ზოგიერთი კრიპტოგრაფიული სისტემა, როგორიც არის RSA, ოთხი ათას ბიტიანი გასაღებით ითვლება უსაფრთხოდ კლასიკური კომპიუტერების თავდასხმების წინაშე, მაგრამ უძლურია დიდი კვანტური კომპიუტერების თავდასხმების საწინააღმდეგოდ.
დღესდღეობით RSA კრიპტოსისტემა გამოიყენება უამრავ პროდუქტში, განსხვავებულ პლატფორმებზე სხვადასხვა დარგში. RSA კრიპტოსისტემა ინერგება ბევრ კომერციულ პროდუქტში და მათი რაოდენობაც დღითი დღე იზრდება. აგრეთვე იგი გამოიყენება Microsoft, Apple, Sun და Novell-ის ოპერაციულ სისტემებში. აპარატული მხრიდან RSA ალგორითმი გამოიყენება დაცულ ტელეფონებში, სხვადასხვა ქსელის პლატებში, სმარტ ბარათებში და აგრეთვე იგი გამოიყენება კრიპტოგრაფიულ აპარატულ უზრუნველყოფაში. ალგორითმი არის ინტერნეტ დაცული კომუნიკაციების ძირითადი პროტოკოლების ნაწილი, მათ შორის S/MIME, SSL და S/WAN. იგი გამოიყენება მრავალ დაწესებულებაში, მაგალითად სამთავრობო ორგანიზაციებში, ბანკებში, კორპორაციების უმრავლესობაში, სახელმწიფო ლაბორატორიებსა და სასწავლებელში. RSA BSAFE დაშიფრვის ტექნოლოგია მთელ მსოფლიოში გამოიყენება დაახლოებით 500 მილიონი მომხმარებლის მიერ. იმის გამო, რომ ხშირ შემთხვევაში ამ დაშიფრვის ტექნოლოგიებში გამოიყენება RSA ალგორითმი, იგი შეიძლება ჩაითვალოს მსოფლიოში საჯარო გასაღების ერთ-ერთ გავრცელებულ კრიპტოსისტემად, რომელსაც გააჩნია ზრდის ტენდენცია

ინტერნეტის განვითარებასთან ერთად. აქედან გამომდინარე RSA ალგორითმის დანგრევა ბევრ დარგში გამოიწვევს პროდუქტების უმეტესობის გატეხვას, რაც შესაძლოა იქცეს ქაოსად.

## 1.2. თანამედროვე მექანიზმების პრობლემები

ასევე პირველ თავში აღწერილია თანამედროვე კრიპტოგრაფიული მექანიზმები. არსებობს RSA-ს განსხვავებული კვანტური თავდასხმებისადმი მდგრადი ალტერნატივები. დღესდღეობით ამ სისტემებზე ფიქსირდება ეფექტური თავდასხმების მთელი რიგი. პოსტ-კვანტური კრიპტოგრაფიის პრობლემის გადაჭრის ერთ-ერთი გზა არის McEliece კრიპტოსისტემა საჯარო გასაღებით. ეს სისტემა დაფუძნებულია ალგებრული კოდირების თეორიაზე, რომელიც რობერტ მაკ-ელისის მიერ 1978 წელს შეიქმნა. ეს გახლავთ რანდომიზაციის პროცესის გამოყენებით პირველი დაშიფრვის სისტემა. მიუხედავად იმისა, რომ ალგორითმმა კრიპტოგრაფიაში ვერ მიიღო ფართო აღიარება, ამავე დროს იგი წარმოადგენს პოსტ-კვანტური კრიპტოგრაფიის კანდიდატურას. დღეისათვის ამ კრიპტოსისტემაზე ფიქსირდება წარმატებული თავდასხმები. პროფესორმა მაიკლ სკოტმა და აგრეთვე დუბლინის უნივერსიტეტის დოქტორანტმა ნეილ კოსტიგანმა IRCSET-ის მხარდაჭერით, ამ ალგორითმზე შეძლეს წარმატებული თავდასხმის განხორციელება. ამისთვის დასჭირდათ პროცესორული დროის 8000 საათი. გატეხვაში მონაწილეობდა კიდევ ოთხი ქვეყნის წარმომადგენელი. მათ დასჭირდათ პროცესორული დროის 200000 საათი. გატეხვა იყო ერთობლივი. მეცნიერებმა დაადგინეს, რომ გასაღების საწყისი სიგრძე ამ ალგორითმში არასაკმარისია და უნდა გაიზარდოს. ამ მაგალითიდან ნათლად ჩანს, რომ დღისთვის კრიპტოსისტემების პოსტ-კვანტურ ეპოქაში გადაყვანისთვის არ ვართ მზად. ჩვენ ვერ ვიქნებით დარწმუნებულები ახლო მომავალში წარმოდგენილი სისტემების უსაფრთხოებაში. McEliece-ის გატეხვის მაგალითმა გვაჩვენა, რომ ალგორითმის გასაღების სიგრძე არ არის საკმარისი. მსგავსი პრობლემები ფიქსირდება სხვა არსებულ ალტერნატივებშიც. აღსანიშნავია ეფექტურობის ასპექტის მნიშვნელობაც. დღესდღეობით ექსპერტებმა მიაღწიეს საკმაოდ კარგ შედეგებს კრიპტო ალგორითმების შესრულების სისწრაფეში.

### 1.3. ისტორიული ფაქტები და კიბერ უსაფრთხოება

გარდა ამისა, პირველ თავში ასევე აღწერილია ისტორიული ფაქტები. კრიპტოგრაფიას გააჩნია საკმაოდ მდიდარი და საინტერესო ისტორია. იგი დაიწყო 4000 წლის წინ ეგვიპტეში. მე-20 საუკუნეში კრიპტოგრაფიამ შეასრულა ძალიან მნიშვნელოვანი როლი ორივე მსოფლიო ომის პერიოდში. მეორე მსოფლიო ომის დაწყებამდე მსოფლიოს წამყვანი ქვეყნების განკარგულებაში იყო ელექტრომექანიკური დაშიფრვის მოწყობილობები. არსებობდა ამ მოწყობილობების ორი ტიპი: როტორული და დისკური ტიპის მოწყობილობები. პირველ ტიპის წარმომადგენელია ენიგმა, რომელიც გამოიყენებოდა გერმანიის და მათი მოკავშირე ქვეყნების მიერ. მეორე ტიპის მოწყობილობა იყო ამერიკული M-209. ენიგმა-ს ისტორია იწყება პატენტით, რომელიც 1917 წელს მიიღო ჰიუგო კოხომ. შემდეგ წელს ეს პატენტი შეიძინა არტურ შერბიუსმა, რომელმაც დაიწყო კომერციული საქმიანობა. იგი ამ მანქანებს ყიდდა როგორც კერძო პირებზე, ასგრეთვე გერმანულ ჯარზეც და ფლოტზე. 1930-იანი წლების დასაწყისში გერმანელმა ჰანს ტილო-შმიდტმა გადასცა მანქანის ყველა მონაცემი ბრიტანულ და ფრანგულ დაზვერვას, ამან რეზონანსი არ გამოიწვია. იმ დროისთვის მათ ჩათვალეს, რომ ამ შიფრის ამოხსნა იყო შეუძლებელი.

მომხმარებლების ცხოვრებაში უსაფრთხოების მექანიზმები ოდიდგანვე მნიშვნელოვან პოზიციას იკავებდა. ტექნოლოგიების განვითარების რამდენიმე ეტაპზე მომხმარებლების განიცდიდნენ გარკვეულ პრობლემებს უსაფრთხოების მექანიზმების გამოყენებადობასთან, რამაც საგრძნობლად იმოქმედა საბოლოო მომხმარებლების ზოგად უსაფრთხოების დონეზე.

## თავი 2 გამოყენებადობა და მისი პრინციპები

### 2.1 უასფრთხოების მექანიზმების გამოყენებადობა

დღეისთვის კიბერ უსაფრთხოების მიმართულებით შექმუშავებულია საკმაოდ ბევრი მექანიზმი რომელიც ორიენტირებულია მომხმარებლის კომფორტულ და უსაფრთხო მუშაობაზე. მაგრამ თანამედროვე უსაფრთხოების მექანიზმების უმრავლესობა შეიძლება

იყოს საკმაოდ რთული გასაგები რიგითი მომხმარებლისთვის და ამ უკანასკნელზე უსაფრთხოების პასუხისმგებლობის გადაცემა ხშირ შემთხვევაში იწვევს უსაფრთხოების სერიოზულ პრობლემებს. როგორც ცნობილია, მომხმარებელი სისტემაში განისაზღვერა ორი ძირითადი კრიტერიუმით:

- ***უსაფრთხოება:*** რამდენად უსაფრთხოდ მიმდინარეობს მომხმარებლის და სისტემის ურთიერთქმედების მექანიზმები. რამდენად დაცულია მომხამრებლის ინფორმაცია მისი გადაცემის/მიღების და შენახვის სხვადასხვა ეტაპებზე;
- ***გამოყენებადობა:*** რამდენად კომფორტულია ამა თუ იმ სისტემასთან მუშაობა, და რამდენად გასაგებია სისტემაში არსებული სამართავი მექანიზმები საბოლოო მომხმარებლისთვის (end user);

## 2.2 შიფრაციის მექანიზმების გამოყენებადობის შეფასება

თანამედროვე სისტემებში პრაქტიკულად შეუძლია წარმოვიდგინოთ ბიზნესი, იდეა ან მიმართულება რომელზეც არ არის შექმნილი ვებ საიტი ან ვებ პლატფორმა. ეს მიმართულება მოითხოვს გარვეულ ცოდნასა და გამოცდილებას უსაფრთხოების და იდეების განვითარების კუთხით. ერთ-ერთი ყველაზე მნიშვნელოვანი და საჭირო უსაფრთხოების მექანიზმი ვებ უსაფრთხოების კუთხით არის გაგზავნილი / მიღებული მონაცემების უსაფრთხოება. ეს პროცესი ხდება რამდენიმე მეთოდით, მათ შორის სერვერსა და მომხმარებელს შორის მონაცემების მიმოცვლის შიფრაციით. ზუსტად მონაცემების შიფრაციაზე არის პასუხისმგებელი სპეციალური სერტიფიკატიები, რომლებიც ყენდება სერვერის მხარეს. მათ ასევე SSL (Secure Sockets Layer) ან უფრო ახალი თაობის TLS (Transport Layer Security) სერტიფიკატები ეწოდებათ. ზუსტად ეს უსაფრთხოეების მექზნიზმები პასუხისმგებელია მომხმარებლის და სერვერს შორის გადაცემული მონაცემების შიფრაციაზე. სერტიფიკატების მუშაობის მექანიზმში ჩართულია რამდენიმე შიფრაციის ალგორითმი, როგორც ასიმეტრიული (RSA ალგორითმი - ასიმეტრიული, უფრო დაცული, მაგრამ შედარებით ნელი) და ასევე სიმეტრიული (AES ალგორითმი, საკმაოდ სწრაფი). SSL / TLS სერტიფიკატების მოდელი არის ჰიბრიდული შიფრაციის სისტემის ერთ-ერთი კარგი მაგალითი. როცა გენერაციის

დროს პირველად გამოიყენება შედარებით მძიმე, მაგრამ უსაფრთხო RSA ალგორითმი ე.წ. სესიის გასაღების გადასაცემად, ხოლო ამ უკანასკნელის გადაცემის შემდეგ უკვე ერთვება უფრო სწრაფი და მჩატე AES ალგორითმი, რომლის მეშვეობითაც ხდება უკვე დამყარებული კავშირის ფარგლებში კომუნიკაციის შიფრაცია.

უსაფრთხო კომუნიკაცია კი ერთ-ერთი ყველაზე მნიშვნელოვანი ფაქტორია დღეის ციფრულ სამყაროში. ყოველდღე ინტერნეტის მომხმარებლები ახდენენ უზარმაზარი მონაცემების, ინფორმაციის გაგზავნასა და მიღებას. ამასთან ერთად ხდება გადაეცემა სპეციალური არხებით, აგრეთვე ცნობილი როგორც ოქმები. ინტერნეტისა და ქსელური სისტემების ზრდასთან ერთად, მომხმარებლები უფრო ხშირად აზიარებენ სხვადასხვა ტიპის მონაცემებს კომუნიკაციის დროს.

### 2.3 მომხმარებელზე ორიენტირებული უსაფრთხოების მექანიზმები

სერიოზული კვლევები ჩატარდა მომხმარებელზე ორიენტირებული სისტემის შექმნის თაობაზე. ასეთი სისტემა უნდა იყოს უფრო კომფორტული და გასაგები საბოლოო მომხმარებლისთვის. ამგვარი კვლევების მიზანია მომხმარებელთა უსაფრთხოების დონის ამაღლება სხვადასხვა სისტემები. სპეციალური კვლევითი სფერო, რომელიც აანალიზებს მომხმარებლის ქცევას ტექნოლოგიურ სისტემებსა და კომპიუტერში უსაფრთხოების სამყარო ადამიანის კომპიუტერულ ურთიერთქმედება (HCI) ეწოდება. ეს მიმართულება ასევე ცნობილია როგორც გამოყენებადი უსაფრთხოება.

ამ მიმართულებით ჩატარებული კვლევები მომხმარებელზეა ორიენტირებული და მიზნად მომხმარებლის მხრიდან სისტემის გაგებას ისახავს. ყველაზე მნიშვნელოვანი ნაწილი HCI-ში არის მომხმარებლის პარამეტრების, შესაძლებლობებისა და შეზღუდვების შესწავლა ტექნოლოგიაში გამოყენებისთვის. ამ მონაცემების საფუძველზე ხდება უფრო მეგობრული და სხვა მომხმარებლისთვის უფრო გასაგები მექანიზმების დანერგვა. ამგვარი მოდელი შეიძლება სხვადასხვა ვებსაიტზე ან მრავალ მომხმარებელზე გათვლილ სისტემებში იყოს დანერგილი.

## 2.4 უსაფრთხოების სერტიფიკატების ტიპები

იმისათვის, რომ მიიღოთ ვებსაიტის ტრანსპორტირების ფენის უსაფრთხოება (Transport layer security – TLS), მომხმარებელმა უნდა აირჩიოს TLS სერთიფიკატის სწორი ტიპი. დღეისთვის არსებობს სხვადასხვა ტიპის სერთიფიკატები, რომელთა არჩევა უნდა მოხდეს ვებსაიტის კატეგორიის მიხედვით. ყველაზე ფართოდ გამოიყენება წარმომადგენლები TLS სერთიფიკატებისა:

***ზოგადი დანიშნულების TLS სერთიფიკატები*** - მცირე და საშუალო ბიზნესის ვებსაიტებისთვის გამოყენებული სერთიფიკატები;

***გაფართოებული ვალიდაციის (EV) TLS სერთიფიკატები*** - გამოიყენება უფრო დიდი პროექტებისთვის, რომლებზეც საჭიროა ორგანიზაციების და სპეციალური დოკუმენტაციის შემოწმება;

***მრავალი დომენის EV TLS სერთიფიკატები*** - ერთი სერტიფიკატი შეიძლება გამოყენებულ იქნას მრავალი ვებ – გვერდის დომენისთვის;

***Wildcard TLS სერთიფიკატები*** - გამოიყენება ვებ საიტების ქვედომეინებისთვის;***პირადი ავთენტიფიკაციის / ელ.ფოსტის სერთიფიკატები*** - გამოიყენება პირადი ან ელ.ფოსტის კლიენტების დაშიფვრისთვის.

## 2.5 უსაფრთხოების სერტიფიკატების გენერაცია

ტრანსპორტის ფენის უსაფრთხოების (Transport layer security – TLS) ყველა ტიპი უნდა იყოს დაინსტალირებული და კარგად კონფიგურირებული სერვერის მხარეს. ჩვეულებრივ კლიენტები იყენებენ ნაგულისხმევ პარამეტრებს TLS სერთიფიკატების კონფიგურაციისთვის, რაც ნორმალურია დამწყებთათვის. უფრო დეტალური კვლევის შემდეგ შეგვიძლია ვთქვათ, რომ ზოგიერთ შემთხვევაში, კლიენტები იყენებენ ნაგულისხმევ პარამეტრებს TLS სერთიფიკატის შექმნის დროს, რადგან მათ საკმარისი ცოდნა არ აქვთ და არ შეუძლიათ იმის გაგება, თუ რა ხდება სინამდვილეში და რატომ უნდა მოხდეს ამ პროცესის კარგად გამართვა. როგორც უკვე ვიცით, ტრანსპორტის ფენის უსაფრთხოების სერტიფიკატის ტექნოლოგიაში გამოიყენება სიმეტრიული და ასიმეტრიული კრიპტოგრაფია. ასიმეტრიული კრიპტოგრაფია გამოიყენება ყოველთვის,

როდესაც ხდება კლიენტის მიერ სერვერთან კავშირის დამყარება. პირველ ეტაპზე გამოიყენება RSA კრიპტოგრაფიული ალგორითმი. მას შემდეგ, რაც კავშირი არის დამყარებული გადაეცემა სპეციალური გასაღები, რომელსაც ეწოდება სესიის გასაღები (session key) და სიმეტრიული კრიპტოგრაფია იწყებს მუშაობას. TLS სამუშაო პროცესში გამოიყენება ჰიბრიდული დაშიფვრის მეთოდები და ეს გამოწვეული ორი მთავარი მიზეზით - უსაფრთხოება და ეფექტურობა.

## 2.6 გამოყენებადობის არსებული მდგომარეობის შეფასება

ჩემი სადოქტორო ნაშრომის ფარგლებში შესწავლის პროცესშია დღეისთვის არსებული კრიპტო სისტემები. უნდა განვიხილოთ წარმატებით განხორციელებული თავდასხმები არსებულ კრიპტო სისტემებზე. თანამედროვე კრიპტო სისტემების სუსტი მხარეების გამოვლენის ანალიზი კვლევის ერთ-ერთი ნაწილია. მიმდინარეობს არსებულ კრიპტო სისტემებზე პრაქტიკული და თეორილიული ნამუშევრების განხილვა. შესწავლილია არსებული გაუმჯობესების მეთოდების ეფექტურობა და მათი პრაკტიკაზე გამოყენების პერსპექტივა. მიღებული შედეგები იქნება გავრცელებული კიბერ უსაფრთხოების ექსპერტებში, როგორც პირადი მიმოწერის, აგრეთვე სოციალური ჯგუფების და ფორუმების საშუალებით. მიღებული რჩევების და მათი ღრმა ანალიზის საფუძველზე შესაძლებელი იქნება სისტემის გაუმჯობესების და ეფექტურობის გაზრდის გაგრძელება. ძირითად კვლევის საკითხებს კი წარმოადგენენ; არსებული უსაფრთხოების მექანიზმების გამოყენებადობის სუსტი წერტილების გამოვლინება და მათზე წარმატებულად განხორციელებული თავდასხმების გარჩევა. იმის გაანალიზება, თუ რითი არის გამოწვეული ეს გამოყენებადობის პრობლემები, დაცვითი სისტემების რა ელემენტებზე ხდებოდა ძირითადი აქცენტი და როგორი გაუმჯობესების გზების შეთავაზება არის საჭირო ამ პრობლემების გადაჭრისათვის.

უსაფრთხოების მექანიზმებთან ერთად, გამოყენებადობა არის ერთ-ერთი მნიშვნელოვანი კომპონენტი მომხმარებლის სისტემასთან ურთიერთქედებაში. გამოყენებადობის კარგი დონით ბევრად მარტივია საბოლოო მომხმარებლის უსაფთხოების დონიზ გაზრდაც.

# თავი 3. შიგთავსზე დაფუძნებული ფილტრაციის სისტემები

## 3.1 შიგთავსზე დაფუძნებული ფილტრაცია

თანამედროვე კიბერ სამყაროში სარეკომენდაციო სისტემები ხელოვნური ინტელექტის მექანიზმების ყველაზე თვალსაჩინო მაგალითია. ჩვეულებრივ, ასეთი პროგრამები იქმნება მომხმარებლისთვის უკეთესი გამოცდილებისთვის სხვადასხვა სისტემებში. მაგალითად Facebook, რომელიც შეიცავს „ადამიანები, რომელბსაც შეიძლება იცნობდეთ" მოდული და YouTube, რომელიც გთავაზობთ შესაბამის ვიდეოს ინტერესების მიხედვით, რაც დგინდება დათვალიერების წინა ისტორიის საფუძველზე. ეს ყველაფერი შეიძლება ჩაითვალოს მომხმარებელზე ორიენტირებული სარეკომენდაციო სისტემების საკმაოდ კარგ მაგალითებად. ვებ პლატფორმები მომხმარებლებს საშუალებას აძლევს მიიღოს რეკომენდაციები სხვადასხვა კრიტერიუმების საფუძველზე. ალგორითმებს, რომლებიც გამოიყენება ასეთი პროგრამებს მიერ უწოდებენ სარეკომენდაციო სისტემებს. დღეს ალგორითმები გამოიყენება სხვადასხვა სარეკომენდაციო სისტემა, მაგრამ შინაარსზე დაფუძნებული შემოთავაზებების მეთოდი ერთ-ერთი ყველაზე ორიენტირებულია მომხმარებელზე. სარეკომენდაციო სისტემები ფართოდ გამოიყენება შინაარსის ფილტრაციისთვის სხვადასხვა ვებ პლატფორმებში, როგორიცაა ონლაინ მაღაზიები, ფილმების ან მოგზაურობის მონაცემთა ბაზა, საგანმანათლებლო მიმართულებები და მრავალი სხვა. შინაარსის ფილტრაციის სისტემები (content filtering systems) მომხმარებლებს ეხმარება მაქსიმალურად კარგად იპოვონ შესაბამისი შინაარსი, მათი საჭიროებებიდან და ინტერესებიდან გამომდინარე. დღეს ნებისმიერი თანამედროვე სისტემისთვის მომხმარებლის უსაფრთხოებაა უაღრესად მნიშვნელოვანია. ჰაკერები ასრულებენ შეტევას სხვადასხვა ტექნიკისა და მიდგომის გამოყენებით. აპარატურულ უზრუნველყოფაზე დაფუძნებული სისტემები ხშირად ხდება სხვადასხვა თავდასხმების სამიზნეები. გვერდითი არხი (side-channel), ცენტრალურ პროცესორზე ორიენტირებული (central processor unit) და ფიზიკური შეტევები გარჩევის ან კრიტიკული ინფორმაციის მიღების დღეს თავდასხმის მოდელის ერთ-ერთი ყველაზე პოპულარული მეთოდია. აღსანიშნავია, რომ სხვადასხვა პროგრამული მექანიზმები სამუშაოდ დღეს იყენებენ აპარატურულ სისტემას.

## 3.2 შიგთავსზე დაფუძნებული ფილტრაციის პრინციპები

უსაფრთხოების სცენარის ანალიზისთვის შინაარსზე (content-based) დაფუძნებული რეკომენდაციების სისტემას სჭირდება მომხმარებლის მიერ მოწოდებული მონაცემები და სპეციალური ჩარჩოები, რომელიც ინახება მონაცემთა ბაზაში, მაგალითად შინაარსზე დაფუძნებული პარამეტრები, შეფასება, უკუკავშირი და მომხმარებლის სხვა აქტივობები. ამ შემთხვევაში კიბერ უსაფრთხოებაზე და ტექნიკაზე დაფუძნებულ სისტემებში, მონაცემები კონკრეტული რეკომენდაციით გაანალიზებულია სისტემის მიერ. მონაცემების შეყვანა ხდება სპეციალური ინტერაქტიული ჩაშენებული ფორმის გამოყენებით.

## 3.3 შინაარსობრივი ტერმინები და მათი მნიშვნელობა

დღეისთვის სარეკომენდაციო სისტემებში არის გამოყენებადი ორი ძირითადი მექანიზმი. ეს არის ტერმინი სიხშირის (TF – term frequency) და ინვერსიული დოკუმენტის სიხშირის (IDF – inverse document frequency) მექანიზმები. შეგვიძლია განვსაზღვროთ სხვადასხვა შინაარსის ვებსაიტებისთვის გამოყენებული სიტყვების სიხშირე. ჩემი კვლევის ფარგლებში დამუშავდა შემდეგი ორგანიზაციების ვებ – გვერდები:

1. სამეცნიერო კიბერ უსაფრთხოების ასოციაციის ოფიციალური ვებგვერდი;
2. Utoweb სტუდიის ოფიციალური ვებ – გვერდი;
3. საბავშვო კიბერ უსაფრთხოების უნივერსიტეტის ოფიციალური ვებ – გვერდი.

## 3.4 ფილტრაციის პრინციპების გამოყენება კიბერ უსაფრთხოებაში

შინაარსზე დაფუძნებული რეკომენდაციების სისტემის მოდელი შეგვიძლია გამოვიყენოთ უსაფრთხოების მექანიზმებში. ჩემი კვლევის ფარგლებში შემუშავებული ვებ სისტემა იყენებს ჩაშენებულ ფილტრაციის მექანიზმს მომხმარებლის მიერ შეყვანილი მონაცემების სიხშირის გამოსათვლელად და უქვეყნებს საბოლოო მომხმარებელს შესაბამის რეკომენდაციებს.

სისტემა ორიენტირებულია მომხმარებლის მიერ შეყვანილი მონაცემების ანალისზე. მომხმარებლის მიერ შეყვანილი მონაცემების საშუალებით, სისტემა აწარმოებს გამოთვლებს TF-IDF ფორმულის მიხედვით, რათა აღმოაჩინოს მსგავსება სხვა მომხმარებლების მიერ ადრე შეყვანილ მონაცემებთან.

შიგთავსზე დაფუძნებული ფილტრაციის მექანიზმები არის მანქანური სწავლების ერთ-ერთი გავრცელებული მეთოდი, რომელიც ძირითადად გამოიყენება სარეკომენდაციო სისტემებში, მისი ინტეგრაცია უსაფრთხოების პრინციპებში იძლევა დიდ შესაძლებლობებს როგორც გამოყენებადობის ასევე უსაფრთხოების დონის გაზრდისთვის.

## თავი 4. კვლევის ფარგლებში მიღებული შედეგები

### 4.1 შემუშავებული სისტემა

სადოქტორო ნაშრომის ფარგლებში იყო განხილული და შესწავლილი არსებული უსაფრთხოების სისტემები და აგრეთვე იყო გაანალიზებული მათი სუსტი მხარეები გამოყენებადობის კუთხით. იყო გაანალიზებული არსებული უსაფრთხოების სისტემების სისუსტეების გამოსწორების შეთავაზებული გზები და ასევე შესრულდა გამოყენებადობის მოდელებით გაუმჯობესებული სისტემის პროგრამულ რეალიზაცია. კვლევის ფარგლებში მიღებულია გამოყენებადობის გაუმჯობესებისთვის შედეგები და შემუშავდა რამოდენიმე იდეა იმის თაობაზე, თუ როგორ უნდა განხორციელდეს პროგრამული ალგორითმი. და მისი ვიზუალური მხარე. იყო შესწავლილი საერთაშორისო ლიტერატურა და ნაშრომში ვითვალისწინებ საკვანძო პრინციპებს, რომელიც იყო აღწერილი და დადგენილი კიბერ უსაფრთხოების ექსპერტების მიერ. უკვე მიღებული იდეები და კონცეფციები იყო განხილული თემატურ ჯგუფებსა და ფორუმებში როგორც ინტერნეტის აგრეთვე პირადი შეხვედრების მეშვეობით. მიღებული პასუხების/რჩევების საფუძველზე განხორციელდა პროტოტიპების გაუმჯობესება და მცირე კორექტირების შეტანა საერთო დიზაინში. სადოქტორო ნაშრომზე მუშაობის პროცესში იყო რამოდენიმე რთულად ამოსახსნელი ამოცანა, რომლის გადაჭრაშიც მეხმარებოდა ჩემი პროექტის ხელმძღვანელი.

## 4.2 მომხმარებელი და სისტემა

მომხმარებელზე ორიენტირებული სისტემის ერთ-ერთ ყველაზე მნიშვნელოვან ფაქტორს წარმოადგენს მომხმარებლის და სისტემის ურთიერთქმედება. შეუძლებელია გამოყენებადი სისტემის შექმნა ამ კონფეფციის გათვალისინების გარეშე. HCI (Human Computer Interaction) - შეისწავლის თუ როგორ ურთიერთქმედებს მომხმარებელი ტექნოლოგიასთან. ეს შეიძლება იყოს სტაციონალურ კომპიუტერზე, ლეპტოპზე მომუშავე ადამიანი ან მობილური ტელეფონის და პლანშეტური კომპიუტერის მომხმარებელი. უფრო მეტიც, შესაძლოა მომხმარებელმა გამოიყენოს სხვადასხვა პორტატული მოწყობილობა, როგორიც არის ჭკვიანი საათი, სამაჯურები და სხვა.

## 4.3 სისტემის განვითარება

სადოქტორო კვლევის ფარგლებში მიღებულია თანამედროვე და რაც მთავარია მომხმარებლების და დღვანდალი ბაზრის მოთხოვნებზე მორგებული სისტემა. როგორც აღინიშნა, კვლევის ფარგლებში შემუშავებული სისტემის ერთ-ერთი მთავარი მიზანია კიბერ უსაფრთხოების მექანიზმებისთვის უკეთესი გამოყენებადობის დონის შექმნა, რაც მიიღწევა შექმნილ სისტემაში გამოყენებადობის მთავარი პრინციპების დანერგვით. მომხმარებლისთვის უფრო გასაგები და მარტივი ქმედებების შესრულების საფუძველზე სისტემა ახდენს შესაბამისი რეკომენდაციების გაცემას. ამ ეტაპისთვის სადოქტორო კვლევაში აქცენტი გაკეთდა კონკრეტულად მანქანური სწავლების ელემენტებზე, კერძოდ კი შინაარსე დაფუძნებული ფილტრაციის კონცეფციაზე, რაც თანამედროვე სარეკომენდაციო სისტემებს უდევს საფუძვლად.

## 4.4 სარეკომენდაციო მიდგომები

სარეკომენდაციო სისტემისთვის, განსაკუთრებით როცა საუბარი მიდის მომხმარებელზე და მის უსაფრთხოებაზე, ერთ-ერთი ყველაზე მნიშვნელოვანი ფაქტორი არის სწორი მიდგომის შერჩევა, რაც გამოიხატება სარეკომენდაციო ალგორითმის შერჩევაში.

დღეისთვის არსებობს რამდენიმე სარეკომენდაციო ალგორითმი და თითეულ მათგანს გააჩნია საკუთარი დატვირთვა. ჩემთვის სადოქტორო კვლევის ფარგლებში იყო ძალიან მნიშვნელოვანი სწორი ალგორითმის გამოყენება და ამის შემდეგ მისი ახალი ვარიანტის შეთავაზება, რომელიც მორგებულია კიბერ უსაფრთხოების რეალობას.

როდესაც ხდება სარეკომენდაციო ალგორითმების გარჩევა, დგინდება, რომ თითეულ მიდგომას გააჩნია თავისი დადებითი და უარყოფითი მხარეები და სწორი ალგორითმის შერჩევა ჩემთვის იყო ერთ-ერთი პრიორიტეტი, რადგან მთელი სისტემის მუშაობის სისწორე და სისწრაფე ეფუძნება შერჩეული ალგორითმის სამუშაო პრინციპებს.

## 4.5 განვითარების პერსპექტივები

სადოქტორო კვლევის ფარგლებში გამოიკვეთა დღეისთვის არსებული მანქანური სწავლების რამდენიმე მიდგომა და ალგორითმი. აღსანიშნავია, რომ თითოეული ალგორითმი წარმოადგენს კონკრეტულ მიმართულებას და გააჩნია საკუთარი სამუშაო დარგი. ჩვენ შემთხვევაში იყო შერჩეული შინაარსზე დაფუძნებული მიდგომა, რადგან კვლევის ფარგლებში გამოიკვეთა რამდენიმე პრინციპი რაც აუცილებლად უნდა იყოს კიბერ უსაფრთხოების სარეკომენდაციო სისტემაში. ერთ-ერთი მნიშვნელოვანი პრინციპი არის ის, რომ რეკომენდაციები კონკრეტული სცენარის მიხედვით უნდა იყოს გაცემული უკვე არსებული გამოცდილების საფუძველზე, ანუ ასეთი ტიპის მიდგომა მოითხოვს რაც შეიძლება მეტ შეყვანილ მონაცემს, რითიც სამომავლოდ არის განპირობებული რეკომენდაციის სიზუსტე და რელევანტურობა.

შინაარსზე დაფუძნებული ფილტრაციის მექანიზმების ინტეგრაცია კიბერ უსაფრთხოების გამოყენებად მექანიზმებში არის ამ სფეროსთვის სრულიად ახალი მიდგომა, რაც საგრძნობლად გაზრდის სისტემების გამოყენებადობის დონეს და შესაბამისად უსაფრთხოებასაც.

## დასკვნები

სადოქტორო კვლევის შედეგად მიღებულია ინტერაქტიული სისტემა, რომელსაც საფუძვლად ჩაედო მანქანური სწავლების ერთ-ერთი რელევანტური პრინციპი - შინაარსე დაფუძნებული სარეკომენდაციო ალგორითმი, რომელიც ძალიან კარგად ახდენს სარეკომენდაციო პროცედურების განხორციელებას ისეთ დარგებში როგორიცაა მაგალითად სოციალური ქსელები, სხვადასხვა ფილმების ან ტურიზმის პლატფორმები, საგანმათლებლო სისტემები და სხვა. ასეთი ტიპის ალგორითმი გამოიყენება მომხმარებლისთვის უკეთესი შინაარსის შეთავაზებისთვის და ეყრდნობა რამდენიმე ფაქტორს.

## გამოქვეყნებული შრომები


1. **G.Iashvili**, "Novel System For Hardware-Based Vulnerabilities Recognition" Scientific and Practical Cyber Security Journal (SPCSJ) 5(2), ISSN 2587-4667, 2021, 1-11pp
2. **G. Iashvili**, M. Iavich, A. Gagnidze, S. Gnatyuk, "Increasing Usability of TLS Certificate Generation Process Using Secure Design", *CEUR-ws.org, Vol-2698*, 2020.
3. A. Gagnidze, M. Iavich, **G. Iashvili**, Post-Quantum Cryptosystems. *Modern scientific researches and innovations*, 5, 2016.
4. M. Iavich., S. Gnatyuk, A. Arakelian, **G. Iashvili**, Y. Polishchuk, D. Prysiazhnyy, "Improved Post-quantum Merkle Algorithm Based on Threads",. *Advances in Intelligent Systems and Computing, vol 1247*, 2020. Springer, Cham. https://doi.org/10.1007/978-3-030-55506-1_41
5. M. Iavich, **G. Iashvili**, S. Gnatyuk, A. Fesenko, "Security methods against modern cyber attack vectors in countries of Europe", *Scientific and Practical Cyber Security Journal (SPCSJ) 3(2):* pp. 49- 53, 2019.
6. A.Gagnidze, M.Iavich, **G.Iashvili**, Analysis of Post Quantum Cryptography use in Practice, *Bulletin of the Georgian National Academy of Sciences,* 2017.
7. M. Iavich, R. Bocu, **G. Iashvili** and S. Gnatyuk, "Novel Method of Hardware Security Problems Identification," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 427-431, doi: 10.1109/PICST51311.2020.9467966.

მოხსენებები კონფერენციებზე

1. Attacks on post-quantum cryptosystems, 17-th International Young Scientists Conference" Optics & High Technology Material Science", Kiev, Ukraine, 2017.
2. Hash Based Digital Signature Scheme with Integrated TRNG, The 23rd conference „Information Society and University Studies" (IVUS 2018), 2018.
3. HCI and Computer security, International Scientific and Practical Conference "Problems of Cyber Security and Telecommunication Systems", Kiev, Ukraine, 2018.
4. Modern security problems of hardware-based systems, Caucasus University 6th Annual Conference, Tbilis, Georgia, 2020.
5. Increasing Usability of TLS Certificate Generation Process Using Secure Design, Information Society and University Studies 2020, Kaunas, Lithuania, 2020.
6. International Symposium on Network Security and Communications - ISNSC2021, Novel Quantum Random Number Generator with the Improved Certification Method, 2021, Kiev, Ukraine.

კვლევა განხოციელდა „შოთა რუსთაველის ეროვნული სამეცნიერო ფონდის ფინანსური მხარდაჭერით (გრანტი # PHD-19-519)

## Secure design in cryptography

### Abstract

Cryptography is one of the most important fields of cyber security today. Very frequently the modern security mechanisms rely on this direction. With the development of technology, the issue of cyber security is becoming more and more relevant today. Without the proper distribution of cyber security processes, system users can face serious problems. The usability of cyber security system is determined by the ease of use of the security mechanism. The simpler the mechanism to use, the more actively the user is involved in system processes. Problems with

usability also lead to security problems for one simple reason - if the security mechanism is not usable, the user will do everything in his power to avoid this security mechanism. The aim of the research is to create a system that will help the users to increase their cyber security level by means of corresponding security recommendations. The system is focused on the highest possible level of security, including the best usability methods. One of the most relevant areas in cyber security today is user-oriented attacks approaches. Every day new vectors are created to break the systems managed by the users. And very important aspect here is to protect users with their minimal involvement. The system offered in the frame of the research relies on machine learning algorithms, concretely on content-based filtering mechanisms, that are made for better optimization of user-entered information and provide the users with relevant security recommendations. The innovative approach offered in the frame of the research is content-based filtering algorithm built specially for cyber security recommendations. Before that, concretely content-based filtering approach was used for another directions like social networks, movie recommendation systems etc. Another area of work is usability that is very important aspect for user security. If the user cannot understand the security mechanisms, or this mechanism is too complicated, the user will try to not use it at all. Than fact may make serious security problems for both, the system and the user of this system at the time. Content-based filtering algorithm is used to offer better content to the user and relies on several factors. As part of my research, a completely new approach to the recommendation algorithm was developed, which is used in the direction of cyber security recommendations. Until now, this type of algorithm has been used to make recommendations in other fields. In the frame of my research, I have created a new direction of the recommendation algorithm, which is aimed at providing appropriate safety recommendations in a user-friendly and understandable way. As security mechanism mainly are complicated and not understandable for the end users, the system build in the frame of my work will significantly increase the usability of the system used by the end-user and will help in providing better security of the systems by means of appropriate recommendations. This fact makes the developed system unique and very modern based on the market requirements. For the future I am going to create hybrid system and add mechanisms of another machine learning algorithm to my system to make it even more flexible and user-friendly.