საქართველოს ტექნიკური უნივერსიტეტი

გიორგი იაშვილი

უსაფრთხო დიზაინი კრიპტოგრაფიაში

წარმოდგენილია დოქტორის აკადემიური ხარისხის მოსაპოვებლად

სადოქტორო პროგრამა „ინფორმატიკა“

შიფრი 0613

საქართველოს ტექნიკური უნივერსიტეტი

თბილისი, 0160, საქართველო

საქართველოს ტექნიკური უნივერსიტეტი

ინფორმატიკისა და მართვის სისტემების ფაკულტეტი

ჩვენ, ქვემორე ხელისმომწერნი, ვადასტურებთ, რომ გავეცანით გიორგი იაშვილის მიერ შესრულებულ სადისერტაციო ნაშრომს: „უსაფრთხო დიზაინი კრიპტოგრაფიაში“ და ვაძლევთ მას რეკომენდაციას, წარმოდგენილი ნაშრომი განხილულ იქნეს საქართველოს ტექნიკური უნივერსიტეტის ინფორმატიკისა და მართვის სისტემების ფაკულტეტის სადისერტაციო საბჭოში დოქტორის აკადემიური ხარისხის მოსაპოვებლად.

----, ----- 2021 წელი

ხელმძღვანელი: პროფესორი მაქსიმ იავიჩი

რეცენზენტი: პროფესორი ვახტანგ კვარაცხელია

რეცენზენტი: ელზა ჯინჭარაძე

ავტორი: გიორგი იაშვილი

დასახელება: „უსაფრთხო დიზაინი კრიპტოგრაფიაში“
სადოქტორო პროგრამა: ინფორმატიკა
ფაკულტეტი: ინფორმატიკისა და მართვის სისტემების ფაკულტეტი

ხარისხი: დოქტორი
სხდომა ჩატარდა:

ავტორის ხელმოწერა

რეზიუმე

კრიპტოგრაფია დღეისთვის კიბერუსაფრთხოების ერთ-ერთი ყველაზე მნიშვნელოვანი მიმართულებაა. ამ მიმართულებას ეყრდნობა თანამედროვე უსაფრთხოების მექანიზმები. საინფორმაციო ტექნოლოგიების განვითარებასთან ერთად სულ უფრო და უფრო აქტუალური ხდება კიბერუსაფრთხოების საკითხი, რომლის პროცესების სწორად განაწილების გარეშე სისტემის მომხმარებელს სერიოზული პრობლემები შეექმნება და შედეგად მივიღებთ მნიშვნელოვანი დარღვევების მთელ რიგს.

კიბერუსაფრთხოების გამოყენებადობა განისაზღვრება უსაფრთხოების მექანიზმის გამოყენების საშუალებებით. რაც უფრო მარტივია სისტემის გამოყენების მექანიზმი, მით უფრო აქტიურად და ადვილად იყენებს მომხმარებელი სისტემას. გამოყენებადობის პრობლემები იწვევს, ასევე, უსაფრთხოების პრობლემებსაც ერთი მარტივი მიზეზის გამო: თუკი უსაფრთხოების მექანიზმი არ არის გამოყენებადი, მომხმარებელი შეეცდება, ამ უსაფრთხოების მექანიზმს აღარ მიმართოს.

ჩვენი კვლევის მიზანია შეიქმნას ისეთი სისტემა, რომლის გამოყენებისას, შესაბამისი რეკომენდაციების საფუძველზე, მომხმარებელი გაცილებით მარტივად შეძლებს საკუთარი კიბერუსაფრთხოების დონის გაზრდას. სისტემა ორიენტირებულია, საუკეთესო გამოყენებადობის მეთოდების ჩართვით, გაზარდოს უსაფრთხოების მაქსიმალურ დონე. დღეისთვის უსაფრთხოების მექანიზმების გამოყენება მომხმარებლისთვის, ხშირ შემთხვევაში, საკმაოდ რთულია. თუკი მომხმარებელს უწევს დამატებითი მოქმედებების შესრულება, თუნდაც მისი უსაფრთხოების დონის გასაზრდელად, იგი აუცილებლად შეეცდება, იპოვოს უფრო კომფორტული და მარტივი გამოსავალი, ან საერთოდ არ გამოიყენოს უსაფრთხოების წარმოდგენილი მექანიზმი. ნაშრომში განხილული და შესწავლილია დღეისთვის ისეთი აქტუალური საკითხი, როგორიცაა მომხმარებელზე მორგებული უსაფრთხოების მექანიზმები და კიბერუსაფრთხოებაში მანქანური სწავლების ელემენტები, რაც იმას ნიშნავს, რომ დაცვითი სისტემების გამართული მუშაობა და მათი გამოყენებადობის დონე დაკავშირებულია მომხმარებლის კომფორტულ მუშაობასთან. უსაფრთხოების მექანიზმების პრობლემა იმაში მდგომარეობს, რომ ეს მექანიზმები მომხმარებლისთვის გაუგებარია, შესაბამისად, არ არის გამოყენებადი და, თავისთავად, უსაფრთხოება, რომელსაც არ იყენებენ პრაქტიკაში, ვეღარ იარსებებს. ნაშრომში წარმოდგენილია უსაფრთხოების დონის გაზრდისთვის ახალი მეთოდი, რომელიც საგრძნობლად ამცირებს სისტემაში მომხმარებლის მოქმედებების რაოდენობას. ამის გამო მომხმარებლისთვის უსაფრთხოების მექანიზმი ბევრად უფრო გასაგები გახდება და, შედეგად, შესამჩნევად გაიზრდება მის მიერ უსაფრთხოების მექანიზმების გამოყენება. ასევე, გაიზრდება უსაფრთხოების სისტემების გამოყენებადობის ზოგადი დონე. კვლევის შედეგად ჩვენ მიერ შემუშავებულ სისტემაში გამოყენებულია ერთ-ერთი მძლავრი მანქანური სწავლების ალგორითმი, რომელიც გვხვდება ისეთ დარგებში, როგორებიცაა, მაგალითად, სოციალური ქსელები, ტურიზმი, ფილმების სარეკომენდაციო სისტემები და სხვა. ასეთი ტიპის მიდგომა კიბერუსაფრთხოების მიმართულებით აქამდე არ იყო გამოყენებული. ჩვენ გთავაზობთ არსებული მიდგომის ახალ მეთოდს, რომლის მეშვეობითაც შინაარსზე დაფუძნებული სისტემის (content-based filtering) გამოყენება შესაძლებელი გახდება კიბერუსაფრთხოების რეკომენდაციების შექმნისთვის.

აღნიშნული მეთოდი საგრძნობლად გაზრდის სისტემებში მომხმარებლის უსაფრთხოების დონეს.

აღსანიშნავია, რომ კვლევისას გამოვიყენეთ უსაფრთხო დიზაინის და გამოყენებითი უსაფრთხოების აპრობირებული გამოცდილებები, რათა სისტემა გამხდარიყო კიდევ უფრო მოქნილი და მომხმარებელზე ორიენტირებული. კვლევის პროცესში ნათელი გახდა, რომ მანქანური სწავლების ელემენტების გამოყენება შერეული სახითაც ყოფილა შესაძლებელი. ჩვენ სამომავლოდ ვაპირებთ უკვე არსებულ სისტემაში დამატებითი მანქანური სწავლების ალგორითმის დანერგვას, რაც შესძენს მას ახალ ფუნქციებს, გააუმჯობესებს პლატფორმის მოქნილობას და კიდევ უფრო დააკმაყოფილებს მომხმარებლის მოთხოვნებს. ნაშრომზე მუშაობის დროს, აგრეთვე, შევიმუშავეთ სარეკომენდაციო ალგორითმის ახალი მიდგომა, რომელიც გამოიყენება კიბერუსაფრთხოების რეკომენდაციების მიმართულებით. აქამდე ასეთი ტიპის ალგორითმები გვხვდებოდა სხვა დარგებში რეკომენდაციების გასაწევად; შევქმენით სარეკომენდაციო ალგორითმის ახალი მიმართულება, რომლის დახმარებით მომხმარებელს კომფორტული და გასაგები ფორმით მიეცემა შესაბამისი უსაფრთხოების რეკომენდაციები. ჩვენი კვლევის მიზანი იყო ისეთი სისტემის შექმნა, რომლის გამოყენებისას მომხმარებელი უფრო მარტივად შეძლებდა საკუთარი კიბერუსაფრთხოების დონის გაზრდას შესაბამისი რეკომენდაციების საფუძველზე. ჩვენ მიერ შემუშავებული სისტემა ორიენტირებულია უსაფრთხოების შესაძლო მაქსიმალურ დონეზე, საუკეთესო გამოყენებადობის მეთოდების ჩართვით. კვლევის მიზანი და ამოცანები, დღევანდელ რეალობაზე დაყრდნობით, არის შემდეგი: გამომდინარე იქიდან, რომ მრავალმომხმარებლიან სისტემებში, ისეთებში, როგორებიცაა, მაგალითად, ვებზე დაფუძნებული პროგრამები ან საიტები, უსაფრთხოების დონე ხშირად არის დამოკიდებული გამოყენებადობაზე. თუ სისტემა არაა გამოყენებადი, მომხმარებელი შეეცდება მისი ალტერნატივის პოვნას. ჩვენი კვლევის მიზანია უსაფრთხოების მექანიზმების და სისტემის გამოყენებადობის უკეთესი ბალანსის პოვნა, რადგან გამოყენებადი სისტემა ყოველთვის უნდა იყოს კომფორტული მომხმარებლისთვის და ის ყოველთვის იქნება ჩართული ამ სისტემებით განპირობებულ პროცესებში.

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 the 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 the research, we 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 the 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 we going to create hybrid system and add mechanisms of another machine learning algorithm to the system to make it even more flexible and user-friendly.

ცხრილების ნუსხა

ცხრილი 1. ტერმინების სიხშირე 55

ცხრილი 2. TF და WTF მნიშვნელობების შედარება 55

ცხრილი 3. ტერმინების სიხშირე 59

ცხრილი 4. შედეგი შეტანილი მონაცემების მიხედვით 59

ცხრილი 5. ინფორმაციული ბლოკების მნიშვნელობები 61

ნახატების და დიაგრამების ნუსხა

ნახ. 1. გამოყენებადობის და უსაფრთხოების დამოკიდებულება 34

ნახ. 2. სერტიფიკატების გამცემების ლოკალური ბაზა .....……....43

ნახ. 3. უსაფრთხოების სერტიფიკატი საიტის მხარეს ….....45

ნახ. 4. კონტენტზე დაფუძნებული სისტემის მუშაობის პრინციპი 52

ნახ. 5. საძიებო სისტემის შედეგების დემონსტრაცია 53

ნახ. 6. შედეგების დემონსტრაცია წიგნების მაგალითზე 54
ნახ. 7. TF-ის გამოთვლა 57
ნახ. 8. ვექტორის სივრცის მოდელი 58
ნახ. 9. შეწონილი ტერმინის სიხშირე ინფორმაციულ ბლოკში 59
ნახ. 10. IDF-ს გამოთვლა 60
ნახ. 11. IDF მომხმარებლის მიერ შეტანილი მონაცემების მიხედვით 60
ნახ. 12. სიგრძის ვექტორი პირველი საინფორმაციო ბლოკისთვის 60
ნახ. 13. ტერმინი პირველი საინფორმაციო ბლოკისთვის 60
ნახ. 14. სარეკომენდაციო სქემის კოდი 69
ნახ. 15. პლატფორმის ფორმის ინტერფეისი 71
ნახ. 16. ავტორიზაციის მოთხოვნის ფორმა 71
ნახ. 17. მომხმარებლის შედეგების გამოყვანა 72
ნახ. 18. რეკომენდაცია პარამეტრების მიხედვით 73
ნახ. 19. პოპულარული საძიებო მოთხოვნები 73
ნახ. 20. რეკომენდაციის ნახვები და ბმულები 74

შინაარსი

შესავალი 9
ლიტერატურის მიმოხილვა 15
თავი 1. თანამედროვე უსაფრთხოების მექანიზმები პრაქტიკაში 18
1.1. კრიპტოგრაფიული მექანიზმები.....18
1.2. კვანტური კომპიუტერები და მათი შესაძლებლობები.....20
1.3. თანამედროვე უსაფრთხოების მექანიზმები კრიპტოგრაფიაში.....21
1.4. თანამედროვე მექანიზმების პრობლემები.....22

1.5. ისტორიული ფაქტები და კიბერუსაფრთხოება.....23
თავი 2. გამოყენებადობა და მისი პრინციპები 31
2.1. უსაფრთხოების მექანიზმების გამოყენებადობა.....31
2.2. შიფრაციის მექანიზმების გამოყენებადობის შეფასება.....34
2.3. მომხმარებელზე ორიენტირებული უსაფრთხოების მექანიზმები...36
2.4. უსაფრთხოების სერტიფიკატების ტიპები.....37
2.5. უსაფრთხოების სერტიფიკატების გენერაცია.....39
2.6. გამოყენებადობის არსებული მდგომარეობის შეფასება.....43
თავი 3. შიგთავსზე დაფუძნებული ფილტრაციის სისტემები..... 45
3.1. შიგთავსზე დაფუძნებული ფილტრაცია.....45
3.2. შიგთავსზე დაფუძნებული ფილტრაციის პრინციპები.....46
3.3. შინაარსობრივი ტერმინები და მათი მნიშვნელობა.....49
3.4. ფილტრაციის პრინციპების გამოყენება კიბერუსაფრთხოებაში.....53
თავი 4. კვლევის ფარგლებში მიღებული შედეგები 57
4.1. შემუშავებული სისტემა.....57
4.2. მომხმარებელი და სისტემა.....68
4.3. სისტემის განვითარება.....77
4.4. სარეკომენდაციო მიდგომები.....80
4.5. განვითარების პერსპექტივები.....85
დასკვნა..... 90
გამოყენებული ლიტერატურა..... 91

შესავალი

თემის აქტუალურობა. კიბერუსაფრთხოება დღეისთვის ერთ-ერთი ყველაზე პოპულარული მიმართულებაა საინფორმაციო ტექნოლოგიების დარგში, რომელსაც თანამედროვე უსაფრთხოების მექანიზმები ეყრდნობა. საინფორმაციო ტექნოლოგიების განვითარებასთან ერთად კიბერუსაფრთხოების საკითხი სულ უფრო და უფრო აქტუალური გახდა. მისი პროცესების სწორად განაწილების გარეშე სისტემის მომხმარებელს სერიოზული პრობლემები შეექმნება და შედეგად მივიღებთ კრიტიკული დარღვევების მთელ რიგს. ნებისმიერი სისტემის მომხმარებელს კარგად უნდა ჰქონდეს გააზრებული ამ სისტემის სამუშაო მექანიზმები. მაგალითად, თუ ჩვენ ვიყენებთ რაიმე ტიპის ვებსაიტს და ამ პორტალზე გვჭირდება ავტორიზაციის გავლა, შეგვყავს ჩვენი (მომხმარებლის) მონაცემები, მაგალითად, მომხმარებლის სახელი და პაროლი. მომხმარებელმა იცის, რომ ეს ქმედება აუცილებელია მისი სისტემაში ავტორიზაციისთვის და მონაცემების უსაფრთხოებისთვის, რადგან 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 მისი ფინანსური მონაცემებიც, ისეთები, როგორებიცაა, მაგალითად, საბანკო ბარათის სრული ინფორმაცია. ასეთი ტიპის ინფორმაციის დაკარგვისას და მესამე პირის ხელში აღმოჩენისას, ხდება სერიოზული უსაფრთხოების პრობლემის საკითხი და ამ ვითარებამ შესაძლოა გამოიწვიოს მომხმარებლის როგორც ფინანსური, ასევე ინფორმაციული დანაკარგი. გამომდინარე იქიდან, რომ დღეისთვის მრავალმომხმარებლიანი სისტემები ძალიან გავრცელებულია და წარმოდგენილია, მაგალითად, სოციალური ქსელების სახით, მომხმარებლების უსაფრთხოების დონე ამ სისტემებში ერთ-ერთი პრიორიტეტია. უსაფრთხოების მექანიზმები ხდება კრიტიკულად მნიშვნელოვანი და აქტუალური, როცა მომხმარებლის მიერ გამოყენებადი სისტემა არ არის ბოლომდე კომფორტული და გასაგები. მომხმარებლის უსაფრთხოების ასპექტები ყოველთვის დაკავშირებულია მეორე კომპონენტთან და ეს არის გამოყენებადობა. ნებიესმიერ შემთხვევაში, როდესაც მუშაობენ 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 სურს შედეგის მისაღწევად ზედმეტი მოქმედებების შესრულება. ყოველი დამატებითი ქმედება მომხმარებლისთვის გარკვეული დისკომფორტია, შესაბამისად, ერთ-ერთი ყველაზე მნიშვნელოვანი საკითხი მომხმარებლის უსაფრთხოებაში კონკრეტულად გამოყენებადობის მაღალი დონის უზრუნველყოფაა.

კიბერუსაფრთხოების გამოყენებადობა განისაზღვრება უსაფრთხოების მექანიზმის გამოყენების სიმარტივით. რაც უფრო მარტივია მექანიზმი გამოყენებისთვის, მით უფრო აქტიურადაა ჩართული სისტემურ პროცესებში მომხმარებელი. პრობლემები გამოყენებადობასთან იწვევს ასევე უსაფრთხოების პრობლემებსაც ერთი მარტივი მიზეზის გამო: თუკი უსაფრთხოების მექანიზმი არ არის გამოყენებადი, მომხმარებელი შეეცდება, ამ უსაფრთხოების მექანიზმს აარიდოს თავი.

უსაფრთხოების მექანიზმების უმრავლესობა მუშაობს, ე. წ. უკანა ფონზე, ისე, რომ სისტემაში მომხმარებელი ვერც კი ამჩნევს მათ მუშაობას. ზოგი მექანიზმი კი ითხოვს მომხმარებლის უსაფრთხოების პროცესებში ჩართულობას, მაგალითად, ზოგიერთ სისტემაში რეგისტრაციის დროს მომხმარებელს მოეთხოვება მოიფიქროს ე. წ. უსაფრთხოებისთვის განკუთვნილი კითხვა, რაც მისთვის დამატებითი ბერკეტია, როცა მომხმარებელს, მაგალითად, დაავიწყდა პაროლი და სჭირდება მისი აღდგენა.

შიფრაციის მექანიზმები ერთ-ერთი ყველაზე საჭირო და ზოგ შემთხვევაში აუცილებელი უსაფრთხოების ზომაა. კრიპტოგრაფიული ელემენტები გამოიყენება ძალიან ბევრ დარგში, დაწყებული სხვადასხვა ვებსისტემებით, დამთავრებული საბანკო ოპერაციებით ან ონლაინ თამაშებით. შიფრაციის მექანიზმები საჭიროა მომხმარებლის 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. ხშირ შემთხვევაში მომხმარებელს არ აქვს საკმარისი ცოდნა იმისთვის, რომ სრულყოფილად გამართოს ამა თუ იმ უსაფრთხოების მექანიზმი საჭირო დონეზე.

მთელი სისტემა და მისი მომხმარებლის უსაფრთხოება კითხვის ნიშნის ქვეშ დგება, რადგან უსაფრთხოების სისტემის სწორი გამართვა ერთ-ერთი ყველაზე მნიშვნელოვანია დაცვითი მექანიზმების ასამუშავებლად.

ჩვენს ნაშრომში განხილული და შესწავლილია დღეისთვის ისეთი აქტუალური საკითხი, როგორიცაა მომხმარებელზე მორგებული უსაფრთხოების მექანიზმები და მანქანური სწავლების ელემენტები კიბერუსაფრთხოებაში, რაც იმას ნიშნავს, რომ დაცვითი სისტემების გამართულობა და მათი გამოყენებადობის დონე პირდაპირ კავშირშია მომხმარებლის კომფორტულ მუშაობასთან. დღეისთვის ბევრი უსაფრთხოების მექანიზმის პრობლემა იმაში მდგომარეობს, რომ მომხმარებლისთვის ეს მექანიზმები გაუგებარია, შესაბამისად, არ არის გამოყენებადი. ამიტომ უსაფრთხოება, რომელსაც არ იყენებენ პრაქტიკაში, უბრალოდ ვერ იარსებებს. ნაშრომში შეთავაზებულია უსაფრთხოების დონის გაზრდისთვის ახალი მეთოდი, რომელიც საგრძნობლად ამცირებს მომხმარებლის მოქმედებების რაოდენობას და ხდის უსაფრთხოების მექანიზმს ბევრად უფრო გასაგებს, რაც მნიშვნელოვნად ზრდის მომხმარებლის მიერ უსაფრთხოების მექანიზმების გამოყენებას, შესაბამისად, გაიზრდება უსაფრთხოების სისტემების გამოყენებადობის ზოგადი დონეც.

კვლევის მიზანი და ამოცანები. ჩვენი მიზანია, შეიქმნას სისტემა, რომლის გამოყენებისას მომხმარებელი უფრო მარტივად შეძლებს საკუთარი კიბერუსაფრთხოების დონის გაზრდას შესაბამისი რეკომენდაციების საფუძველზე. სისტემა ორიენტირებულია უსაფრთხოების შესაძლო მაქსიმალურ დონეზე, საუკეთესო გამოყენებადობის მეთოდების ჩართვით. კვლევის მიზანი და ამოცანები, დღევანდელ რეალობაზე დაყრდნობით, შემდეგია: გამომდინარე იქიდან, რომ მრავალმომხმარებლიან სისტემებში, ისეთებში, როგორებიცაა, მაგალითად, ვებზე დაფუძნებული პროგრამები ან საიტები, უსაფრთხოების დონე ხშირად არის დამოკიდებული გამოყენებადობაზე. თუ სისტემა არაა გამოყენებადი, მომხმარებელი შეეცდება მისი ალტერნატივის პოვნას. კვლევის მიზანია უსაფრთხოების მექანიზმების და სისტემის გამოყენებადობის უკეთესი

ბალანსის პოვნა, რადგან გამოყენებადი სისტემა ყოველთვის იქნება უფრო კომფორტული მომხმარებლისთვის, ის იქნება ჩართული ამ სისტემებით განპირობებულ პროცესებში.

მიზნის მისაღწევად საჭიროა შემდეგი ამოცანების პოზიციონირება:

- განხილულ იქნეს 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 საგანია არსებული მომხმარებელზე ორიენტირებული უსაფრთხოების მექანიზმების შესწავლა და მათში გამოყენებადობის პრობლემების გამოვლენა. კვლევის საგანს წარმოადგენს გამოყენებადობის ახალი მექანიზმების რელევანტურობის შეფასება და კიბერუსაფრთხოებასა და გამოყენებადობას შორის უკეთესი ბალანსის შემუშავება.

კვლევის თეორიული და მეთოდოლოგიური საფუძვლები.

ნაშრომის სამეცნიერო სიახლე. სადისერტაციო ნაშრომის სამეცნიერო სიახლეს წარმოადგენს არსებული კიბერუსაფრთხოების მექანიზმების და მანქანური სწავლების ელემენტების ახალი მიდგომის შეთავაზება. დღეისთვის არსებული შიგთავსზე დაფუძნებული ფილტრაციის მექანიზმები მუშაობს ე. წ. რეკომენდაციების სისტემების ფარგლებში. ეს სისტემები გამოიყენება ისეთ სფეროებში, როგორებიცაა: სოციალური ქსელები, ფილმების ან სხვა კონტენტის შეთავაზების პლატფორმები.

მსგავსი ტიპის შიგთავსზე დაფუძნებული მექანიზმები არ გამოიყენება კიბერუსაფრთხოების მიმართულებით, კომპონენტების სპეციფიკიდან გამომდინარე. სადისერტაციო ნაშრომზე მუშაობისას შევისწავლეთ არსებული შიგთავსზე დაფუძნებული ფილტრაციის მექანიზმები და წარმოვადგინეთ ამ საკითხის ახალი

მიდგომა, რაც ეფუძნება მანქანური სწავლების ელემენტების, კერძოდ კი, შიგთავსზე დაფუძნებული ფილტრაციის მიდგომების კიბერუსაფრთხოების სარეკომენდაციო სისტემაში გამოყენებას. ის ინოვაციურია როგორც სამეცნიერო, ასევე პრაქტიკული კუთხით და საშუალებას გვაძლევს, გამოვიყენოთ მანქანური სწავლების ელემენტები მომხმარებლის მიერ გამოყენებად სისტემებში. ეს მიდგომა აგრეთვე საგრძნობლად გააუმჯობესებს მომხმარებლის უსაფრთხოების დონეს, იგი ახალია და მისი ანალოგი დღეისთვის არ მოიძებნება. შეთავაზებული მექანიზმის დახმარებით შეგვიძლია მივიღოთ სარეკომენდაციო შედეგი მანქანური სწავლების, კონკრეტულად კი შიგთავსზე დაფუძნებული ფილტრაციის ელემენტების საშუალებით, რაც კიბერუსაფრთხოების მიმართულებით ესეც ინოვაციურია.

აღსანიშნავია, რომ ჩვენი კვლევის ფარგლებში არსებული შიგთავსზე დაფუძნებული ფილტრაციის მანქანური სწავლების ალგორითმები შევცვალეთ და მოვარგეთ კიბერუსაფრთხოების მოთხოვნებსა და რეალურ გარემოს, რამაც მნიშვნელოვნად გაზარდა საბოლოო პროდუქტის მეცნიერული მნიშვნელობა.

დისერტაციის პრაქტიკული მნიშვნელობა. ნაშრომის მოცულობა და სტრუქტურა. სადოქტორო ნაშრომი შედგება შესავლისგან, ოთხი თავისგან, ოცი ქვეთავისგან, დასკვნისგან და გამოყენებული ლიტერატურის სიისგან. ნაშრომში წარმოდგენილია 24 გრაფიკული გამოსახულება.

ლიტერატურის მიმოხილვა

სადოქტორო ნაშრომზე მუშაობისას გავეცანით კიბერუსაფრთხოების და უსაფრთხო დიზაინის შესახებ არსებულ როგორც უცხოელ, ასევე ქართველი მეცნიერების პუბლიკაციებს, რომელთა ავტორებიც ამ დარგის წამყვანი სპეციალისტები არიან. მოძიებულ ლიტერატურაში ნათლად არის აღწერილი ჩვენთვის საინტერესო პრობლემების როგორც თეორიული, ასევე პრაქტიკული მხარეები. ნიმუშად განვიხილავთ რამდენიმე პუბლიკაციას:

K. Meena, R. Sivakumar (2014). Human Computer Interaction, PHI Learning Pvt. Ltd. – აღნიშნულ სტატიაში ნაჩვენებია მომხმარებლის და მანქანის ურთიერთქმედება, რაც საფუძვლად უდევს უსაფრთხო დიზაინის შემუშავების სისტემას. აღწერილია მომხმარებლის სისტემასთან კომუნიკაციის ძირითადი ასპექტები და მათი პრაქტიკული გამოყენება. გამოყენებადობა წარმოდგენილია როგორც მომხმარებლისთვის ერთ-ერთი მნიშვნელოვანი ასპექტი; J. Neilsen. Usability 101: Introduction to Usability – ამ სტატიაში

აღწერილია გამოყენებადობის ძირითადი დეტალები და მომხმარებლისთვის კომფორტული სისტემის პროტოტიპში გასათვალისწინებელი ფაქტორები. შემდგომი მნიშვნელოვანი ასპექტი არის უსაფრთხოება. გამოყენებადობას დაეკარგება ყველანაირი აზრი, თუ სისტემა არ იქნება შესაბამისად დაცული. არსებობს უსაფრთხოების მრავალი მექანიზმი, თითოეულ მექანიზმს გააჩნია თავისი დანიშნულება და გამოყენების სფერო; M. Iavich, G. Iashvili (2017). CAPTCHA analysis and its problems, Scientific and practical cyber security journal. Vol. 1 Issue 1. – ამ ნაშრომში განხილულია მომხმარებლის უსაფრთხოების ერთ-ერთი მექანიზმი CAPTCHA, რომელიც პრაქტიკაში წარმოადგენს ფილტრს ადამიანის რობოტისგან გასარჩევად; ანალოგიური მექანიზმის გამოყენებადობის პრობლემები და მათი ანალიზი აღწერილია ამ სტატიაში: M. Iavich, I. Pirtskhalava. Captcha development problems//Modern technics and technologies. 2015, №7. ამ მექანიზმების ანალიზი დაგვეხმარება უკეთ შევაფასოთ მიღებული სისტემის გამოყენებადობა, რამდენად კომფორტულია სისტემასთან მომხმარებლის მუშაობა; A. G. Gagnidze, M. P. Iavich, G. U. Iashvili (2016). Post-Quantum Cryptosystems. Modern scientific researches and innovations, 5. – ამ სტატიაში წარმოდგენილია პოსტკვანტური კრიპტოსისტემები, რისი ცოდნაც გააღრმავებს ანალიზის სიზუსტეს, რაც საშუალებას მოგვცემს უფრო სიღრმისეულად გავიაზროთ არსებული კრიპტოსისტემების გამოყენებადობის პრობლემები; M. P. Iavich, P. D. Isaev (2014). Problems Associated with The Creation of the Own Cryptosystems//Modern scientific researches and innovations, 4. – ამ სტატიაში აღწერილია ის პრობლემები, რომლებიც შეხვდათ აღნიშნული ნაშრომის ავტორებს კრიპტოსისტემის შემუშავების პროცესში. გასათვალისწინებელი ფაქტია, რომ უსაფრთხოების ნორმების დასაცავად რეკომენდირებულია მხოლოდ სტანდარტების გამოყენება, რადგან საკუთარი უსაფრთხოების მექანიზმი ხშირ შემთხვევაში დაუცველი და მოწყვლადია. მუშაობის პროცესში შესწავლილი და გაანალიზებული სამეცნიერო ნაშრომების რაოდენობა მუდმივად იზრდებოდა. ძირითადი აქცენტი კეთდებოდა კრიპტოგრაფიაში გამოყენებადობის პრობლემების გადაჭრასა და მომხმარებლისთვის უფრო მარტივი და გასაგები მექანიზმების შემუშავებაზე. ჩვენი კვლევის ფარგლებში საკმაოდ დიდი დრო დაეთმო მანქანური სწავლების შინაარსზე დამოკიდებული

ფილტრაციის მექანიზმების შესწავლას. შევისწავლეთ ლიტერატურა, რომელშიც აღწერილია როგორც ზოგადი მანქანური სწავლების მეთოდები, ასევე კონკრეტული მიმართულებები სარეკომენდაციო სისტემების შემუშავებისთვის. Frank Kane. „Building Recommender Systems with Machine Learning and AI: Help People Discover New Products and Content with Deep Learning, Neural Networks, and Mach“, 2018 – აღნიშნულ ნაშრომში აღწერილია, რამდენად მნიშვნელოვანია სარეკომენდაციო სისტემისთვის შესაბამისი მანქანური სწავლების ელემენტების ჩართვა; Ankit Jain, Armando Fandango, et al. „TensorFlow Machine Learning Projects: Build 13 real-world projects with advanced numerical computations using the Python ecosystem“, 2018 – ამ სტატიის ავტორები გვაცნობენ ერთ-ერთ ყველაზე გავრცელებულ ფრეიმვორკს მანქანაური სწავლებისთვის – TensorFlow-ს, რომელიც საკმაოდ მოქნილია და აქვს მდიდარი ფუნქციონალი ხელოვნური ინტელექტის განვითარების მხრივ. ამასთან ერთად, სტატიის ავტორები აღწერენ რეალური პროექტების მაგალითებს, რაც ნათელს ხდის TensorFlow-ის და, ზოგადად, მანქანური სწავლების მექანიზმების პოტენციალს და შესაძლებლობებს. Marco Gori. „Machine Learning: A Constraint-Based Approach“, 2017 – აღნიშნულ სტატიაში აღწერილია მანქანური სწავლების შინაარსზე დაფუძნებული მიმართულება. მეთოდები, რომლებსაც წარმოგვიდგენს ნაშრომის ავტორი, შეესაბამება მანქანური სწავლების ერთ-ერთ მნიშვნელოვან ასპექტს სარეკომენდაციო სისტემების შექმნისთვის – შინაარსზე დაფუძნებულ ფილტრაციას. Charu C. Aggarwal. „Recommender Systems: The Textbook“, 2006 – ეს ერთ-ერთი პირველი ნაშრომია, რომელშიც აღწერილია თანამედროვე სარეკომენდაციო სისტემების მიდგომა. ავტორი აღწერს სარეკომენდაციო სისტემების შექმნის ძირითად პრინციპებს და განიხილავს რამდენიმე მიდგომას გაცილებით ოპტიმალური შედეგის მისაღწევად.

თავი 1. თანამედროვე უსაფრთხოების მექანიზმები პრაქტიკაში

1.1. კრიპტოგრაფიული მექანიზმები

კრიპტოგრაფია თანამედროვე კომპიუტერულ სამყაროში ერთ-ერთი მნიშვნელოვანი უსაფრთხოების მექანიზმია, რომელიც გამოიყენება კიბერსივრცის თითქმის ყველა მიმართულებაში, დაწყებული უბრალო ვებსაიტებით, დამთავრებული სამხედრო და კრიტიკული ინფრასტრუქტურის ობიექტებით. კრიპტოგრაფიულ მექანიზმებს გააჩნია სერიოზული დატვირთვა უსაფრთხოების დონის უზრუნველყოფისთვის. ამ მექანიზმის პრინციპია მონაცემების შიფრაცია, ერთადერთი მიზნით – უსაფრთხოების უზრუნველყოფა. თუკი დაუშიფრავი მონაცემები აღმოჩნდება დამნაშავის ხელში, იგი მათ ბოროტად გამოიყენებს და სერიოზულ ზიანს მიაყენებს როგორც მომხმარებელს, ასევე იმ სისტემას, რომელსაც იყენებს ეს მომხმარებელი. უსაფრთხოების საკითხს ყოველთვის ეკავა უმნიშვნელოვანესი ადგილი საზოგადოებაში. უახლესი ტექნოლოგიების განვითარებასთან ერთად დადგა ინფორმაციული ან კომპიუტერული უსაფრთხოების საკითხი, რადგან დედამიწის მოსახლეობის უდიდესი ნაწილი გადადის ციფრულ სამყაროში: თანხის ბრუნვა, სხვადასხვა ნივთების შეძენა, დოკუმენტების გადაცემა, პირის იდენტიფიცირება და ჩვენი ცხოვრების მრავალი სხვა ასპექტი უკავშირდება ელექტრონულ სამყაროს. თითოეული ადამიანის მონაცემები და პირადი ინფორმაცია უნდა იყოს დაცული და მათზე წვდომა – შეზღუდული. თუკი რომელიმე მონაცემი ან/და მომხმარებლის პირადი ინფორმაცია ცნობილი გახდება მესამე პირისთვის, ეს ნიშნავს იმას, რომ დაცვითმა მექანიზმმა შესაბამისად ვერ იმუშავა და გამოყენებულ კრიპტოსისტემაში ხარვეზებია საძიებელი. დღეისთვის არსებულ თანამედროვე კრიპტოსისტემებს გააჩნია გარკვეული პრობლემები, ეფექტურად ვერ მუშაობენ, ამიტომ, სამწუხაროდ, მათზე თავდასხმები ჰაკერისთვის წარმატებით სრულდება. კრიპტოგრაფიული სისტემების „გატეხვა“ შეიძლება გამოწვეული იყოს სხვადასხვა ფაქტორებით, როგორც არაეფექტური დაცვითი მექანიზმების, ასევე კრიპტოსისტემების არასწორი გამოყენების გამო. ჩვენს ნაშრომში გავაანალიზებთ სხვადასხვა ტიპის თავდასხმებს არსებულ კრიპტოსისტემებზე და განვიხილავთ

თანამედროვე სისტემების სუსტ მხარეებს, მათ გამოყენებას და არსებული კრიპტოსისტემების ალტერნატივებს კვანტური კომპიუტერების თავდასხმების წინააღმდეგ. ეს უკანასკნელი კლასიკურ კომპიუტერებთან შედარებით გამოირჩევა გამოთვლების უმაღლესი სიჩქარით. კვანტური კომპიუტერების შესაქმნელად აქტიურად მუშაობენ მსოფლიოს წამყვანი მეცნიერები და კიბერუსაფრთხოების ექსპერტები. არსებობს პუბლიკაცია იმის თაობაზე, რომ კორპორაცია Google, NASA და კოსმოსური კვლევების უნივერსიტეტების ასოციაციამ (Universities Space Research Association) გააფორმეს ხელშეკრულება D-Wave პროცესორების მწარმოებელთან, რომელიც კვანტურ პროცესორებს ამზადებს.

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 საძიებო არეს, ამასთან ერთად იზრდება გამოთვლების სიჩქარეც. ზემოთ აღნიშნულიდან გამომდინარე ნათელი ხდება, რომ კვანტურ კომპიუტერს შესაძლებლობა ექნება დაშალოს უმეტესი ნაწილი თუ არა, აბსოლუტურად ყველა ტრადიციული კრიპტოსისტემა, რომელიც ფართოდ გამოიყენება პრაქტიკაში, აგრეთვე კონკრეტულად მთელი რიცხვების ფაქტორიზაციის ამოცანაზე დაფუძნებული სისტემები, როგორიცაა RSA სისტემა. ზოგიერთ კრიპტოგრაფიულ სისტემაზე, მაგალითად RSA-ზე, ოთხი ათასბიტიანი გასაღებით, კლასიკური კომპიუტერების მხრიდან მასზე თავდასხმა გამორიცხულია, მაშინ როდესაც ის უძლურია დიდი კვანტური კომპიუტერების წინაშე.

არსებობს ორი ტიპის კრიპტოგრაფია: პირველი ტიპის კრიპტოგრაფია არ მისცემს საშუალებას ცალკეულ პირს, წაიკითხოს სხვისი წერილები; მეორე ტიპის კრიპტოგრაფია მთავრობას არ მისცემს საშუალებას, წაიკითხოს რომელიმე პირის დოკუმენტები.

თუ ავიღებთ წერილს და შევინახავთ სხვა ქალაქის ან ქვეყნის სეიფში და გარკვეული პერიოდის შემდეგ დაგვჭირდება ამ წერილის წაკითხვა, ამ შემთხვევაში საქმე გვაქვს გაუგებრობასთან და არა უსაფრთხოებასთან. მეორე მხრივ, თუ ავიღებთ წერილს, განვათავსებთ ისეთ სეიფში, რომლის ზომა, წონა, ჩამკეტის სპეციფიკა და სხვა

ელემენტები ცნობილია, მათ შორის მსოფლიოს ყველაზე კვალიფიციური სეიფების გამხსნელებისთვისაც კი და ამის გათვალისწინებით მაინც ვერ ხერხდება ამ სეიფიდან წერილის ამოღება, შეიძლება ითქვას, რომ ეს სეიფი უსაფრთხოა. წლების განმავლობაში მსგავსი კრიპტოგრაფია სამხედრო სფეროს ნაწილი იყო. აშშ-ის ნაციონალური უსაფრთხოების სააგენტო და მათი მოკავშირეები, ყოფილი საბჭოთა კავშირის ქვეყნები, ინგლისი, ისრაელი და სხვა ქვეყნებიც ხარჯავდნენ მილიარდობით დოლარს სხვისი უსაფრთხოების სისტემების „გასატეხად“. ქვეყნები, რომლებსაც არ ჰქონდათ საკმარისი გამოცდილება და ფინანსური სახსრები, თავიანთ სისტემებს ვერ იცავდნენ უფრო ძლიერი ქვეყნების თავდასხმებისგან.

1.2. კვანტური კომპიუტერები და მათი შესაძლებლობები

კვანტური კომპიუტერი კლასიკურ კომპიუტერებთან შედარებით გამოირჩევა გამოთვლების უმაღლესი სიჩქარით. კვანტური კომპიუტერების შესაქმნელად აქტიურად მუშაობენ მსოფლიოს წამყვანი მეცნიერები და კიბერუსაფრთხოების ექსპერტები. არსებობს პუბლიკაცია იმის თაობაზე, რომ კორპორაცია Google, NASA და კოსმოსური კვლევების უნივერსიტეტების ასოციაციამ (Universities Space Research Association) გააფორმეს ხელშეკრულება D-Wave პროცესორების მწარმოებელთან, რომელიც კვანტურ პროცესორებს აწარმოებს.

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 საძიებო არეს, ამასთან ერთად იზრდება გამოთვლების სიჩქარეც. ზემოთ აღნიშნულიდან გამომდინარე ნათელი ხდება, რომ კვანტურ კომპიუტერს შესაძლებლობა ექნება დაშალოს უმეტესი ნაწილი თუ არა, აბსოლუტურად ყველა ტრადიციული კრიპტოსისტემა, რომელიც ფართოდ გამოიყენება პრაქტიკაში, აგრეთვე კონკრეტულად მთელი რიცხვების ფაქტორიზაციის ამოცანაზე დაფუძნებული სისტემები, როგორიცაა RSA სისტემა.

ზოგიერთ კრიპტოგრაფიულ სისტემაზე, მაგალითად RSA-ზე, ოთხი ათასბიტიანი გასაღებით, კლასიკური კომპიუტერების მხრიდან მასზე თავდასხმა გამორიცხულია, მაშინ როდესაც ის უძლურია დიდი კვანტური კომპიუტერების წინაშე.

დღესდღეობით RSA კრიპტოსისტემა გამოიყენება უამრავ პროდუქტში, განსხვავებულ პლატფორმებზე სხვადასხვა დარგში. RSA კრიპტოსისტემა ინერგება ბევრ კომერციულ პროდუქტში და მათი რაოდენობაც დღითიდღე იზრდება. აგრეთვე იგი გამოიყენება Microsoft, Apple, Sun და Novell-ის ოპერაციულ სისტემებში. აპარატული მხრიდან RSA ალგორითმი გამოიყენება დაცულ ტელეფონებში, სხვადასხვა ქსელის პლატებში, სმარტბარათებში და აგრეთვე კრიპტოგრაფიულ აპარატულ უზრუნველყოფაში. ალგორითმი ინტერნეტდაცული კომუნიკაციების ძირითადი პროტოკოლების ნაწილია, მათ შორის S/MIME, SSL და S/WAN. იგი გამოიყენება მრავალ დაწესებულებაში, მაგალითად: სამთავრობო ორგანიზაციებში, ბანკებში, კორპორაციების უმრავლესობაში, სახელმწიფო ლაბორატორიებსა და სასწავლებლებში.

დღეისთვის RSA BSAFE დაშიფრვის ტექნოლოგიის მომხმარებელი დაახლოებით 500 მილიონი ადამიანია. 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, ქაოსად იქცეს [1,2].

1.3. თანამედროვე უსაფრთხოების მექანიზმები კრიპტოგრაფიაში

არსებობს RSA-გან განსხვავებული კვანტური თავდასხმებისადმი მდგრადი ალტერნატივები. დღესდღეობით ამ სისტემებზე თავდასხმები ხშირად ეფექტურია. პოსტკვანტური კრიპტოგრაფიის პრობლემის გადაჭრის ერთ-ერთი გზა არის McEliece, კრიპტოსისტემა საჯარო გასაღებით. ეს სისტემა დაფუძნებულია ალგებრული კოდირების თეორიაზე, რომელიც რობერტ მაკელისის 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 პოსტკვანტური კრიპტოგრაფიის კანდიდატურას. დღეისათვის ამ კრიპტოსისტემაზე თავდასხმები წარმატებით სრულდება. პროფესორმა მაიკლ სკოტმა და დუბლინის უნივერსიტეტის დოქტორანტმა ნეილ კოსტიგანმა, IRCSET-ის მხარდაჭერით, ამ ალგორითმზე დაყრდნობით, თავდასხმა შეძლეს. ამისთვის მათ დასჭირდათ პროცესორული დროის 8000 საათი. „გატეხვაში“ მონაწილეობდა კიდევ ოთხი ქვეყნის წარმომადგენელი. მათ ამ საქმეში დასჭირდათ პროცესორული დროის 200 000 საათი. მეცნიერებმა დაადგინეს, რომ ამ ალგორითმში გასაღების საწყისი სიგრძე არ არის საკმარისი და იგი უნდა გაიზარდოს. ამ მაგალითიდან ნათლად ჩანს, რომ დღეისთვის კრიპტოსისტემების პოსტკვანტურ ეპოქაში გადაყვანისთვის არ ვართ მზად. ჩვენ ასევე 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 კრიპტოალგორითმების შესრულების სისწრაფეში [3].

1.4. თანამედროვე მექანიზმების პრობლემები

ჩვენ მიერ ჩატარებული კვლევის შედეგად ცნობილი გახდა, რომ წარმოდგენილი პოსტკვანტური კრიპტოსისტემები ნაკლებად ეფექტურია, მათი რეალიზაციის ალგორითმები მოითხოვს დიდ დროს მათი შესრულების და დადასტურებისთვის. არაეფექტური კრიპტოგრაფია შეიძლება იყოს მისაღები რიგითი მომხმარებლისთვის, მაგრამ ვერანაირად ვერ იქნება მისაღები ინტერნეტ სერვერებისთვის, რომლებიც წამში ათასობით კლიენტს ამუშავებენ. Google-ს დღეს უკვე გააჩნია გარკვეული პრობლემები არსებულ კრიპტოგრაფიასთან. არ არის რთული წარმოსადგენი, რა შეიძლება მოხდეს, თუ კრიპტოალგორითმების შესრულებას უფრო მეტი დრო დასჭირდება. იმისათვის, რომ

თანამედროვე კრიპტოსისტემები განვითარდნენ და გაუმჯობესდნენ, დიდი დროა საჭირო. ამასთან ერთად ამ სისტემებზე მუდმივად ხდებოდა თავდასხმები. როდესაც ისაზღვრება დაშიფრვის უსაფრთხო ფუნქცია და იგი სტანდარტად იქცევა, მას ესაჭიროება შესაბამისი პროგრამული და, ხშირ შემთხვევაში, აპარატული უზრუნველყოფის რეალიზაცია. რეალიზაციის დროს უნდა იყოს უზრუნველყოფილი არა მხოლოდ ფუნქციის მუშაობის გამართულობა და მისი ეფექტური სიჩქარე, არამედ სხვადასხვა ტიპის გაჟონვების თავიდან აცილება. ახლახან დაფიქსირდა RSA და AES რეალიზაციებზე წარმატებული cache-timing თავდასხმები, რის შემდეგაც კომპანია Intel-მა თავის მიერ წარმოებულ პროცესორებში დაამატა AES ინსტრუქციები. როგორც ვხედავთ, უსაფრთხო და ეფექტური პოსტკვანტური კრიპტოსისტემების შექმნისთვის და რეალიზაციისთვის საკმაოდ დიდი სამუშაოა ჩასატარებელი. უნდა იყოს განხილული შემოთავაზებული პოსტკვანტური კრიპტოსისტემები; უნდა იქნეს შესწავლილი მათზე ეფექტური თავდასხმები, გამოვლინდეს მათი სუსტი მხარეები და ამ სისტემებზე დამატებითი თავდასხმები განხორციელდეს; უნდა შემოწმდეს მათი ეფექტურობა, განისაზღვროს ამ სისტემების რეალიზაციის ალგორითმების შესრულების დრო, პირადი და სხვების მიერ ჩატარებული კვლევის საფუძველზე; უნდა დადგინდეს სისტემების არასაკმარისი ეფექტურობის გამომწვევი მიზეზები; უნდა შემუშავდეს უსაფრთხო ჰიბრიდული კრიპტოსისტემები პოსტკვანტური ეპოქისთვის.

1.5. ისტორიული ფაქტები და კიბერუსაფრთხოება

კრიპტოგრაფიას გააჩნია საკმაოდ მდიდარი და საინტერესო ისტორია. იგი სათავეს იღებს 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 ტიპს მიეკუთვნება „ენიგმა“, რომელსაც იყენებდნენ გერმანია და მისი მოკავშირე ქვეყნები. მეორე ტიპის მოწყობილობა ამერიკული იყო – M-209. 1917 წელს ჰიუგო კოხომ მიიღო „ენიგმას“ გამოყენების პატენტი.

მომდევნო წელს ეს პატენტი, კომერციული საქმიანობის მიზნით, შეიძინა არტურ შერბიუსმა. იგი ამ მანქანებს ყიდდა როგორც კერძო პირებზე, აგრეთვე გერმანიის ჯარსა და ფლოტზე. 1930-იანი წლების დასაწყისში გერმანელმა ჰანს ტილო-შმიდტმა გადასცა მანქანის ყველა მონაცემი ბრიტანულ და ფრანგულ დაზვერვას. ამას რეზონანსი არ გამოუწვევია. იმ დროისთვის ჩათვალეს, რომ ამ შიფრის ამოხსნა შეუძლებელი იყო. 1939 წელს სამი პოლონელი მათემატიკოსისგან შემდგარმა ჯგუფმა შეძლო ენიგმას მიერ დაშიფრული შეტყობინებების წაკითხვა. იმავე წელს ჯგუფის წევრს, მარიან რეევსკის გაუჩნდა სხვა ელექტრომექანიკური მანქანის შექმნის იდეა. ახალ მანქანას ნამცხვრის სახელი – „ბომბა“ დაარქვეს, რადგან ეს აზრი მათემატიკოსს კაფეში დაებადა. გერმანიის მიერ პოლონეთის დაპყრობამდე, პოლონელებმა ინგლისელებს გადასცეს რამდენიმე ენიგმა, ელექტრომექანიკური მანქანა „ბომბა“, რომელიც შედგებოდა ექვსი ენიგმასგან და ეხმარებოდა მათ შეტყობინებების გაშიფრვაში. ელექტრომექანიკურ მანქანებთან ერთად პოლონელებმა ინგლისელებს კრიპტოანალიზის მეთოდებიც მიაწოდეს. გაშიფრვის შემდგომი სამუშაოები იმართებოდა ბლეტჩლი პარკში, რომელიც დიდი ბრიტანეთისთვის ღირშესანიშნაობას წარმოადგენს. Station X-ის საქმიანობის პიკზე მას 12000 ადამიანი ემსახურებოდა. გერმანიისთვის ამ ცენტრის შესახებ არაფერი იყო ცნობილი. Station X-ის დაშიფრულ ინფორმაციას გააჩნდა გრიფი Ultra, რომელიც უფრო საიდუმლო იყო, ვიდრე Top Secret-ის გრიფი. ინგლისური მხარე უსაფრთხოების სპეციალურ ზომებს იღებდა, რომ გერმანელებს შიფრის გაგება ვერ მოეხერხებინათ. 1940 წლის 14 ნოემბერს, ქალაქ კოვენტრიზე თავდასხმა ყველაზე თვალსაჩინო ფაქტია, რომლის შესახებაც, შეტყობინების გაშიფრვის დახმარებით, დიდი ბრიტანეთის პრემიერ-მინისტრისთვის, უინსტონ ჩერჩილისთვის წინასწარ იყო ცნობილი. მიუხედავად ამისა, უ. ჩერჩილს არანაირი ზომები არ მიუღია არც ქალაქის დაცვისთვის და არც ქალაქის მცხოვრებთა ევაკუაციისთვის. იგი იზიარებდა ანალიტიკოსთა აზრს, რის თანახმადაც გერმანიას არ უნდა გაეგო ოპერაცია Ultra-ს შესახებ. Station X-ის არსებობა და მისი მუშაობის შედეგები ცნობილი იყო საბჭოთა კავშირისთვის. სწორედ Station X-ის მეშვეობით საბჭოთა კავშირმა შეიტყო, რომ ადოლფ ჰიტლერი რევანშისთვის ემზადებოდა მისი ჯარების სტალინგრადთან დამარცხების გამო და დროულად

მოემზადა ოპერაციისთვის კურსკის მიმართულებით. ამ ოპერაციას „კურსკის რკალი“ დაარქვეს.

საბანკო სფეროში კომპიუტერული დანაშაულების მსოფლიო სტატისტიკა გვიჩვენებს, რომ ამ დანაშაულების დაახლოებით 70% არის ფულის მიტაცება და დაახლოებით 20% – მონაცემების მოპარვა და მათი ფალსიფიცირება. კრიპტოგრაფიის ამოცანა და მისი გამოყენება საბანკო საქმეში იმ საშიშროების აღმოფხვრაა, რომელიც დამახასიათებელია საბანკო სისტემისთვის.

ეს არის:

- იმ პირთა არასანქცირებული წვდომა და კონფიდენციალური ინფორმაციის გაცნობა, რომლებიც არ მიეკუთვნებიან საბანკო პერსონალს;
- საბანკო პერსონალისთვის ისეთი ინფორმაციის გაცნობა, რომელთანაც მათ არ უნდა ჰქონდეთ წვდომა;
- პროგრამების და მონაცემების არასანქცირებული კოპირება;
- ინფორმაციის, რომელიც გადაეცემა სპეციალური საკომუნიკაციო არხებით, მოსმენა და შემდეგ კონფიდენციალური ინფორმაციის გასაჯაროება;
- მყარი დისკების მოპარვა, სადაც ჩაწერილია კონფიდენციალური ინფორმაცია;
- ამობეჭდილი საბანკო დოკუმენტების მოპარვა;
- ინფორმაციის შემთხვევითი ან მიზანმიმართული განადგურება;
- საბანკო პერსონალის მიერ ფინანსური დოკუმენტების, ანგარიშების და მონაცემთა ბაზების არასანქცირებული მოდიფიცირება;
- საკომუნიკაციო არხების საშუალებით გადაცემული შეტყობინებების ფალსიფიცირება;
- უარის თქმა შეტყობინების ავტორობაზე, რომელიც გადაეცემა საკომუნიკაციო არხების საშუალებით;
- ინფორმაციის მიღების ფაქტის უარყოფა;
- მომსახურე პერსონალის მუშაობისას დაშვებული შეცდომები;

- პროგრამების და აპარატურული მოწყობილობების არასწორი მუშაობის გამო ფაილური სისტემის ნგრევა;
- ვირუსული პროგრამების ზემოქმედების გამო ინფორმაციის განადგურება;
- მყარ დისკზე შენახული საბანკო არქივების განადგურება;
- შეცდომები პროგრამულ უზრუნველყოფაში;
- მოწყობილობების შეფერხებით მუშაობა. მაგალითად, ელექტროენერგიის გათიშვის ან სხვა ფაქტორების გამო მუშაობის შეფერხება. ამ შეფერხებებს შეიძლება ჰქონდეთ გამოჩენის სხვადასხვა ალბათობები, რომლებიც ბანკში არსებულ კონკრეტულ ფაქტორებზე არიან დამოკიდებულები.

დღევანდელ დღეს შეგვიძლია თვალყური ვადევნოთ ფარულ ბრძოლას ბანკებს შორის, რათა შეინარჩუნონ წამყვანი პოზიციები და მიიზიდონ ახალი კლიენტები. ამ ყველაფრის მიღწევა შესაძლებელია ახალი სერვისების შეთავაზებით და მომსახურებისთვის საჭირო დროის შემცირებით. ეს, თავის მხრივ, მიიღწევა ყველა საბანკო ოპერაციის შესაბამისი დონის ავტომატიზაციით. ზემოთ ჩამოთვლილია საფრთხეები, რომლებიც დამახასიათებელია გადახდების სისტემებისთვის. აქედან გამომდინარე, საბანკო სისტემაში გამოთვლითი ტექნიკის გამოყენება იწვევს როგორც პროცესების გაადვილებას, ასევე აჩენს ბანკისთვის არატრადიციულ საფრთხეებს. ეს ახალი საფრთხეები დაკავშირებული არიან: ინფორმაციის ფიზიკურ დაზიანებასთან ან განადგურებასთან, ინფორმაციის შემთხვევით ან მიზანმიმართულ მოდიფიცირებასთან და, ასევე, ინფორმაციის მიღებასთან არასანქცირებული პირების მიერ, რომელთათვისაც ის განკუთვნილი არ არის. თუმცა, საბანკო ინფორმაციის დაცვისთვის მთავარი ამოცანაა კრიპტოგრაფიული გადაწყვეტილებების დანერგვა. ბუნებრივია, რომ კრიპტოგრაფიული მეთოდების დახმარებით ინფორმაციის დაცვისთვის გატარებული ღონისძიებების დონე, როგორც წესი, ყოველთვის ჩამორჩება ავტომატიზაციის ღონისძიებებს. პრინციპში, ასეთმა ჩამორჩენამ შეიძლება გამოიწვიოს სერიოზული პრობლემები. ამ პრობლემების ერთ-ერთი მიზეზია ის, რომ კრიპტოგრაფიული პროდუქტთა ბაზარი არ არის განვითარებული. ავტომატიზებულ კომპლექსებში, ინფორმაციის დაუცველობის პირობებში, აუცილებელია უსაფრთხოების ზომების მიღება, თუმცა არსებობს

გარკვეული სირთულეები: 1. უსაფრთხოების საშუალებების მწარმოებლების მიერ არის შეთავაზებული ცალკეული კომპონენტები კონკრეტული ამოცანების გადასაწყვეტად. შესაბამისად, მომხმარებელს უწევს უსაფრთხოების საშუალებების თავსებადობის პრობლემის მოგვარება; 2. საიმედო დაცვის უზრუნველყოფისთვის საჭიროა ტექნიკურ და ორგანიზაციულ საკითხთა კომპლექსის მოგვარება და შესაბამისი დოკუმენტაციის შემუშავება;

3. კვალიფიციურ ჰაკერს, რეალურ რთულ სისტემაში, ყოველთვის ძალუძს „მოატყუოს“ მწარმოებლის უსაფრთხოების საშუალებას. შესაბამისად, დაცვის დახვეწა უნდა ხდებოდეს ყოველთვის, როგორც კი ახალ ცოდნასა და გამოცდილებას მივიღებთ. დაცვის სისტემის მუშაობა დაყოფილია სამ ეტაპად: რისკის ანალიზი, უსაფრთხოების პოლიტიკის რეალიზაცია და უსაფრთხოების პოლიტიკის მხარდაჭერა. უსაფრთხოების პოლიტიკა მიმართულია: კონფიდენციალობის, მონაცემთა ერთიანობის და მზადყოფნის მიღწევაზე. გადახდების სისტემაში პრიორიტეტი ენიჭება სისტემის მზადყოფნას, მოემსახუროს მომხმარებელს, რადგან შეფერხებები მის ფუნქციონირებაში იწვევს ყველა მომხმარებლის შესამჩნევ ზარალს. გადახდების სისტემის პრიორიტეტებს შორის შემდეგი ეტაპი მონაცემთა ერთიანობის დაცვაა, შემდეგ მოდის პრიორიტეტებს შორის კონფიდენციალობის უზრუნველყოფა. მისი დარღვევით პროცესის მონაწილეები არ ზარალდებიან და, როგორც წესი, კატასტროფული შედეგების მატარებელიც არ არის, თუმცა ეს იმისთვის არის საჭირო, რომ პროცესის მონაწილეები დაიცვას კრიმინალებისაგან. გადახდების სისტემის ერთ-ერთი უმთავრესი ელემენტი გადახდების დოკუმენტების იურიდიული დაცვაა, რათა ყველა სახის დავა ადვილად გადაწყდეს. თუ დოკუმენტები იურიდიულად დაცულია, მაშინ მომხმარებელი ენდობა ამ გადახდების სისტემას. სწორედ ეს არის არგუმენტი იმის სასარგებლოდ, რომ გადახდების სისტემაში უფრო პრიორიტეტულია დოკუმენტების ავთენტურობის და ერთიანობის უზრუნველყოფა კრიპტოგრაფიული მეთოდების გამოყენებით და არა კონფიდენციალურობის მეთოდების უზრუნველყოფა. საკომუნიკაციო არხების გამოყენებით საბანკო ინფორმაციის გადაცემისას დაცვა ძირითადად ხდება კრიპტოგრაფიული საშუალებებით. ეს საშუალებები გახლავთ დასადასტურებელი

კოდების სისტემა. კრიპტოგრაფიული მეთოდები, რომლებიც იცავენ სისტემას იმისგან, რომ მასში სანქციის გარეშე არავინ შევიდეს, თითქმის არ არის გამოყენებული საბანკო ინფორმაციის დამუშავების და შენახვის დროს. ასევე არ ხდება ინფორმაციის კომპლექსური დაცვა ყველა ეტაპზე, მაგალითად, დამუშავების, შენახვის და გადაცემის ეტაპებზე. გადახდების სისტემების კრიპტოგრაფიული დაცვა უნდა აკმაყოფილებდეს ზოგ სტანდარტს, მაგალითად, უნდა ჰქონდეს მდგრადი კრიპტოალგორითმები. ასევე გადახდების სისტემას აქვს სპეციფიკური თვისებები, რომლებიც მოითხოვენ დამატებით კრიპტოგრაფიული დაცვის საშუალებებს. მაგალითად, გადახდების სისტემა უნდა იყოს საიმედო და ოპერატიული მომხმარებლებს შორის თანხების გადარიცხვის დროს. მაგალითად, განვითარებულ ქვეყნებში თანხის გადაგზავნა და გადახდები 24 საათის განმავლობაში სრულდება. არსებობს კიდევ ერთი ფაქტორი, რომელიც მოქმედებს გადახდების სისტემის კრიპტოგრაფიულ დაცვაზე: ცენტრალური ბანკი დაკავშირებულია კომერციულ ბანკებთან, რომლებსაც, თავის მხრივ, საკუთარ მომხმარებელთან აქვს ვალდებულება. მათ, აგრეთვე, ეკისრებათ პასუხისმგებლობა ვადების დარღვევასა და გადახდების განხორციელების კორექტულობაზე. ისიც გასათვალისწინებელია, რომ გადახდების სისტემა იქცევა ბოროტმოქმედის შეტევის ობიექტი. ბოროტმოქმედი შეიძლება იყოს როგორც უცხო ადამიანი, ასევე თვით ამ სისტემის მომხმარებელი. გადახდების სისტემის მომხმარებელთა რიცხვი ძალიან დიდია. აგრეთვე დიდი როლი უკავია საკვანძო სისტემის მოწყობას საბანკო გადახდების კრიპტოსისტემების გამოყენებით. გადახდების სისტემის ძალიან ბევრი ასპექტი მოქმედებს სისტემის არჩევაში, მაგალითად: გადახდების სისტემის საიმედოობა, ოპერატიულობა და კეთილსინდისიერების მაღალი ხარისხი და ა. შ. კრიპტოგრაფიის თეორიაში კვლევების ორი მიმართულებაა, რომლებიც მუშაობენ საბანკო სისტემებში. ესენია: საბანკო ბარათების კრიპტოგრაფიული უზრუნველყოფა და საბანკო კრიპტოგრაფიული პროტოკოლები. საბანკო ბარათებს ასევე უწოდებენ ინტელექტუალურ ბარათებს. პლასტიკური საბანკო ბარათი არის ბარათი, რომლის ზომებია 85.6 მმ და 53.9 მმ. ის დამზადებულია ისეთი პლასტმასისგან, რომელიც მდგრადია თერმული და მექანიკური ზემოქმედების მიმართ. პლასტიკური ბარათის

ერთ-ერთი უმთავრესი ფუნქცია არის გადახდების სისტემაში მონაწილე პირის იდენტიფიცირების უზრუნველყოფა. ამიტომაც ბარათზე მოცემულია: შესაბამისი ბანკის სახელი და გადახდის სისტემა, რომელიც ემსახურება ამ ბარათს, ასევე მფლობელის სახელი და გვარი, მოქმედების ვადა და ა. შ. საბანკო ბარათის კრიპტოგრაფიული ნაწილი შეიძლება შეიცავდეს ბანკისთვის სპეციფიკურ კრიპტოალგორითმებს, აუტენტიფიკაციის სქემებს, ელექტრონულ ხელმოწერებს და ა. შ. ახალი თაობის პლასტიკური ბარათები განსხვავდებიან ძველი თაობის პლასტიკური ბარათებისგან იმით, რომ მათში უფრო მეტი საშუალებაა ახალი დაცვითი სისტემების დანერგვისთვის. ახალი თაობის ბარათებში არსებული გამოთვლითი რესურსი აძლევს იმის საშუალებას, რომ მოხდეს რთული კრიპტოგრაფიული სქემების რეალიზება. თუმცა, კომპრომისი ეფექტურობას და კრიპტოგრაფიული სქემების მდგრადობას შორის, საბანკო სისტემებისთვის, რომლებიც იყენებენ ინტელექტუალურ ბარათებს, მწვავე საკითხად რჩება. კიდევ ერთი მიმართულება, რომელიც შემუშავებულია საბანკო აპლიკაციებისთვის, საბანკო კრიპტოგრაფიული პროტოკოლებია. მათი ამოცანაა, უზრუნველყონ ელექტრონული გადახდების სისტემების უსაფრთხოება. ციფრული ხელმოწერა არის კრიპტოგრაფიული პროტოკოლის ერთ-ერთი ელემენტი, რომლის დახმარებით ორივე მხარე აღწევს მათთვის სასურველ მიზნებს. თავის მხრივ, მხარეების მიზნებია მონაცემთა ერთიანობა და კონფიდენციალობა. სწორედ კრიპტოგრაფიული ალგორითმების სანდოობით მიიღწევა ზემოთ აღნიშნული მიზნები. კრიპტოგრაფიული გარდაქმნების სტანდარტების პარამეტრები და გასაღებების ზომები ისეთნაირად შეირჩევა, რომ მათი „გატეხვა“ (გარდა იმ შემთხვევებისა, როდესაც გასაღები მოპარულია) რამდენიმე ათეული წლის განმავლობაში ვერ მოხერხდეს. რაც შეეხება ბოროტმოქმედს, ის იმ შემთხვევაში მიაღწევს წარმატებას, თუ გამოვიყენებთ სუსტ ან არასტანდარტულ პროტოკოლებს. საიმედო კრიპტოპროტოკოლებს (მათი შესაბამისი დაშიფრვის საშუალებებით) იყენებს ბევრი ქვეყანა დიპლომატიური, სამხედრო ან სხვა მსგავსი ხასიათის მიმოწერების დასაცავად. მიუხედავად ზოგი ადამიანის მიერ გავრცელებული მცდარი მოსაზრებისა, ასეთი სისტემების კრიპტოგრაფიული მდგრადობა შეიძლება შენარჩუნდეს რამდენიმე ათეული წლის განმავლობაში. ასეთი სისტემის „გასატეხად“, ბოროტმოქმედმა უნდა ამოხსნას

მათემატიკური ამოცანები, რაც ძალიან იშვიათად ხდება. ავტომატიზებულ საბანკო სისტემებს ასევე უწოდებენ ელექტრონული გადახდების სისტემებს, რომლებიც წარმოადგენს უნაღდო გადახდების სისტემას. ისინი იყენებენ უახლეს საკომუნიკაციო საშუალებებს. დღეისთვის, ელექტრონულ საგადასახადო სისტემებში ქაღალდის ფული მთლიანად ჩანაცვლებულია ელექტრონული ფულით, რომელსაც მომხმარებელი იყენებს გადახდების დროს როგორც ერთმანეთთან, ასევე, თუნდაც, ბანკებს შორის. ელექტრონული გადახდების სისტემების კიდევ ერთი თავისებურებაა, რომ მომხმარებლის ქმედებები არ იყოს დათვლილი. უცხოელმა სპეციალისტებმა მომხმარებლის ქმედებების დათვლის საჭიროება ახსნეს ქვემოთ მოყვანილ და მის მსგავს მაგალითებზე დაყრდნობით: ყოველ გადახდაზე საკრედიტო ბარათი ახდენს მისი მფლობელის იდენტიფიცირებას. მაგალითად, თუ საკრედიტო ბარათის მფლობელი იყენებს მას ავტობუსის ბილეთის საყიდლად, მაშინ სატრანსპორტო კომპანიას ექნება ინფორმაცია მისი ყველა გადაადგილების შესახებ. რასაკვირველია, ეს არ არის სერიოზული პრობლემა, მაგრამ თუ განვიხილავთ ამ პრობლემას ისეთ მაგალითზე, როდესაც ხდება დიდი თანხების გადარიცხვა, ამ შემთხვევაში უსაფრთხოება მაღალ დონეზე უნდა იყოს უზრუნველყოფილი. ამიტომ დეველოპერებს კარგად აქვთ გათვითცნობიერებული ის ფაქტი, რომ უნდა მოხდეს საბანკო სისტემების დაცვა ბოროტმოქმედისგან. მომხმარებლის ქმედებების დათვლის მოწინააღმდეგეები ამბობენ, რომ ის საჭირო არ არის, რადგან მომხმარებელი თუ არ ენდობა ბანკს, მაშინ ის იქ არასდროს გახსნის ანგარიშს. ასეთ შემთხვევაში, მომხმარებელი არ ენდობა ბანკში მომუშავე პერსონალს და მესამე პირს, რომელსაც შეიძლება იმ ინფორმაციის მიტაცების საშუალება ჰქონდეს, რომელიც გადის საინფორმაციო არხებში. მეორე მხრივ, ბანკების უმეტესობა ცდილობს მოიპოვოს მომხმარებლის ნდობა, საბანკო გადარიცხვების სტანდარტის ამაღლებით [4].

თავი 2. გამოყენებადობა და მისი პრინციპები

2.1 უსაფრთხოების მექანიზმების გამოყენებადობა

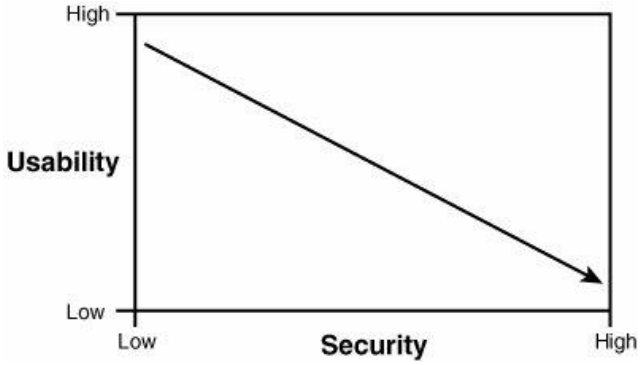
დღეისთვის კიბერუსაფრთხოების მიმართულებით შემუშავებულია საკმაოდ ბევრი მექანიზმი, რომელიც ორიენტირებულია მომხმარებლის კომფორტულ და უსაფრთხო მუშაობაზე. მაგრამ თანამედროვე უსაფრთხოების მექანიზმების უმრავლესობა საკმაოდ რთულად გასაგებია რიგითი მომხმარებლისთვის და მასზე უსაფრთხოების პასუხისმგებლობის გადაცემა, ხშირ შემთხვევაში, იწვევს უსაფრთხოების სერიოზულ პრობლემებს. როგორც ცნობილია, მომხმარებელი სისტემაში განისაზღვრა ორი ძირითადი კრიტერიუმით:

– ***უსაფრთხოება:*** რამდენად უსაფრთხოდ მიმდინარეობს მომხმარებლის და სისტემის ურთიერთქმედების მექანიზმები; რამდენად დაცულია მომხმარებლის ინფორმაცია მისი გადაცემის/მიღების და შენახვის სხვადასხვა ეტაპზე;

– ***გამოყენებადობა:*** რამდენად კომფორტულია ამა თუ იმ სისტემასთან მუშაობა, რამდენად გასაგებია სისტემაში არსებული სამართავი მექანიზმები საბოლოო მომხმარებლისთვის (end user).

გამომდინარე ამ ორი კრიტერიუმიდან, შეიძლება დავასკვნათ, რომ მომხმარებლის უსაფრთხოების დონე შემდეგნაირად არის დაკავშირებული გამოყენებადობასთან:

სურ 1. *გამოყენებადობის და უსაფრთხოების დამოკიდებულება*



უსაფრთხოების დონის გაზრდა, თუკი ეს დამოკიდებულია მომხმარებელზე, აუცილებლად აისახება გამოყენებადობის დონეზე. რაც უფრო მკაცრად არის დაცული

უსაფრთხოების ნორმები, მით უფრო რთულია საბოლოო მომხმარებლისთვის ამ სისტემასთან მუშაობა გამოყენებადობის მხრივ. აღსანიშნავია, რომ გამოყენებადობის დონის გაზრდასთან ერთად აუცილებლად უნდა იყოს შემოტანილი გარკვეული კომპრომისი უსაფრთხოების კუთხით. თუ სისტემასთან მუშაობას გავამარტივებთ, ამით უსაფრთხოება მოისუსტებს. ამისი თვალსაჩინო მაგალითია ორფაქტორიანი ავთენტიფიკაცია, რომელიც დღეისთვის გამოიყენება მრავალ ცნობილ სისტემაში. ასეთი უსაფრთხოების მიდგომას უკვე დიდი ხანია იყენებენ ისეთ სისტემებში, როგორებიცაა, მაგალითად, Facebook ან Google. მისი არსი მდგომარეობს შემდეგში: ადამიანი ვერ ისარგებლებს პირადი პროფილით (იქნება ეს ელ-ფოსტა ან პროფილი სოციალურ ქსელში) მანამდე, სანამ არ დაადასტურებს შესვლას „დამატებითი“ წყაროდან. ეს ხშირ შემთხვევაში ხდება მომხმარებლის პროფილზე წინასწარ მიბმული სმარტფონის გამოყენებით. პროფილზე შესვლის მცდელობისთანავე, მოწყობილობას ეგზავნება შესაბამისი შეტყობინება ან დამადასტურებელი კოდი, რომელიც უნდა შეიტანოს მომხმარებელმა სისტემაში შესასვლელად.

ასეთი ტიპის მიდგომებს, რა თქმა უნდა, გააჩნია, უსაფრთხოების მხრივ, დადებითი მხარეები. ბოროტმოქმედისთვის ბევრად რთულია ასეთ პირობებში მუშაობა, რადგან მომხმარებლის პროფილზე წვდომისთვის, პირადი ხასიათის მონაცემებთან ერთად (როგორიცაა მომხმარებლის სახელი/ელ-ფოსტა/ტელეფონი და პაროლი), საჭიროა დამატებითი კომპონენტი – მოწყობილობა, საიდანაც პროფილში უნდა შევიდეს.

ამავდროულად, ასეთ უსაფრთხოების მიდგომას გააჩნია უარყოფითი მხარე გამოყენებადობის მხრივ: მომხმარებლის პროფილზე წვდომისთვის საჭიროა დამატებითი ქმედებების განხორციელება. ხშირ შემთხვევაში საბოლოო მომხმარებლისთვის ეს არაკომფორტული, დამღლელი და ზოგჯერ გამაღიზიანებელიც კი არის. ამიტომაც ასეთი ტიპის უსაფრთხოების მექანიზმები გავრცელებულ სისტემებში მხოლოდ ნებაყოფლობითია და არა – სავალდებულო. მომხმარებელს ნებისმიერ დროს შეუძლია ამ მექანიზმების გათიშვა და სტანდარტულ შესვლის რეჟიმზე გადასვლა.

მომხმარებლის პროფილში შესვლის გარდა, მნიშვნელოვან როლს თამაშობს, ასევე, პირველადი და ყველაზე, ერთი მხრივ, ხელმისაწვდომი უსაფრთხოების ზომა – პაროლი, მაგრამ აქაც არ არის ყველაფერი ასე ცალსახად. რაც უფრო მარტივად დასამახსოვრებელ პაროლს ვიყენებთ, მით უფრო მარტივია მისი აღდგენა, ხოლო რაც უფრო რთულს აღსადგენად – მით უფრო რთულია ასეთი პაროლის დამახსოვრება და მისი შემდგომი გამოყენება.

დღეისთვის არსებული პოპულარული პლატფორმები და აპლიკაციები იყენებენ ე. წ. უსაფრთხო პაროლების მოდელს, რომელიც ითვალისწინებს მხოლოდ „რთული“ პაროლების გამოყენებას. „რთული“ პაროლის მოდელი ითვალისწინებს პაროლში შემავალი სიმბოლოების გარკვეულ რაოდენობას, ზედა და ქვედა რეგისტრის სიმბოლოების გამოყენებას და, ამასთან ერთად, დამატებითი სიმბოლოების და რიცხვების გამოყენებას.

ამგვარად, ცნობილი ხდება, რომ უსაფრთხოების მექანიზმების გამოყენება, თუკი ეს მექანიზმები გაუგებარია მომხმარებლისთვის, ხშირად იწვევს ნეგატიურ განწყობას და მის გამოყენებაზე უარის თქმას. ეს ფაქტი, ცხადია, უარყოფითად მოქმედებს ზოგადად მომხმარებლის ქცევასა და უსაფრთხოების დონეზე. ამ სიტუაციამ, შესაძლოა, გამოიწვიოს სერიოზული უსაფრთხოების პრობლემები. შესაბამისად, ერთ-ერთი მნიშვნელოვანი და აქტუალური საკითხი უსაფრთხოების დონის გაზრდისთვის არის ერთგვარი ბალანსის შექმნა, რომელიც იმუშავებს უსაფრთხოების ზოგად დონესა და გამოყენებადობის დონეს შორის. სისტემა ისე უნდა იყოს დაცული, რომ არ გაატაროს სხვადასხვა ტიპის მომხმარებელზე ორიენტირებული თავდასხმები, მაგრამ, ამავდროულად, ეს უსაფრთხოების პროცესები და მათი პრაქტიკული გამოყენება არ უნდა იყოს რთულად გასაგები საბოლოო მომხმარებლისთვის, წინააღმდეგ შემთხვევაში მომხმარებელი მათ უბრალოდ აღარ გამოიყენებს. ამიტომაც საჭიროა სპეციალური, უფრო ხელმისაწვდომი უსაფრთხოების მექანიზმების შექმნა, რომელთა გამოყენება იქნება უფრო მარტივი და გასაგები სხვადასხვა პლატფორმის მომხმარებლისთვის. მაგალითად, დღეისთვის ვებსაიტები და ვებაპლიკაციები მთელ მსოფლიოში ინფორმაციის ყველაზე მსხვილი წყაროა. ლოგიკურია, რომ ეს მიმართულება საკმაოდ

მიმზიდველია ბოროტმოქმედისთვის, არსებობს ვებორიენტირებული თავდასხმების მთელი რიგი.

2.2 . შიფრაციის მექანიზმების გამოყენებადობის შეფასება

თანამედროვე სისტემებში პრაქტიკულად შეუძლებელია წარმოვიდგინოთ ბიზნესი, იდეა ან მიმართულება, რომელის ირგვლივ არ არის შექმნილი ვებსაიტი ან ვებპლატფორმა. ეს მიმართულება მოითხოვს გარკვეულ ცოდნასა და გამოცდილებას უსაფრთხოების და იდეების განვითარების მხრივ. ერთ-ერთი ყველაზე მნიშვნელოვანი და საჭირო უსაფრთხოების მექანიზმი ვებუსაფრთხოების კუთხით გაგზავნილი/მიღებული მონაცემების უსაფრთხოებაა. ეს პროცესი წარმოებს რამდენიმე მეთოდით, მათ შორის, სერვერსა და მომხმარებელს შორის მონაცემების გაცვლის შიფრაციით. ზუსტად მონაცემების შიფრაციაზე პასუხისმგებელია სპეციალური სერტიფიკატები, რომლებიც დგება სერვერის მხარეს. მათ, ასევე, SSL (Secure Sockets Layer), ან უფრო ახალი თაობის TLS (Transport Layer Security) სერტიფიკატები ეწოდებათ. სწორედ ეს უსაფრთხოების მექანიზმები პასუხისმგებელია მომხმარებელსა და სერვერს შორის გადაცემული მონაცემების შიფრაციაზე. სერტიფიკატების მუშაობის მექანიზმში ჩართულია რამდენიმე შიფრაციის ალგორითმი როგორც ასიმეტრიული (RSA ალგორითმი – ასიმეტრიული, უფრო დაცული, მაგრამ შედარებით ნელი), ასევე სიმეტრიული (AES ალგორითმი, საკმაოდ სწრაფი). SSL/TLS სერტიფიკატების მოდელი ჰიბრიდული შიფრაციის სისტემის ერთ-ერთი ნათელი მაგალითია. 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 დღეისთვის ციფრულ სამყაროში ერთ-ერთი ყველაზე მნიშვნელოვანი ფაქტორია. ყოველდღიურად ინტერნეტის მომხმარებლები იღებენ და

აგზავნიან უზარმაზარ მონაცემებსა და ინფორმაციას. ამასთან ერთად, ის გადაიცემა სპეციალური არხებით, ცნობილია, როგორც ოქმები. ინტერნეტისა და ქსელური სისტემების გამუდმებული ზრდა მომხმარებლებს საშუალებას აძლევს, უფრო ხშირად გაცვალონ ერთმანეთთან სხვადასხვა ტიპის მონაცემები. დღესდღეობით, მონაცემთა გადაცემა მრავალფეროვანია სხვადასხვა დანიშნულების პროტოკოლებით. უსაფრთხოების უკეთესი დონისთვის კომუნიკაცია კლიენტს (ინტერნეტ ბრაუზერი) და სერვერს შორის უნდა შესრულდეს დაშიფრული პროტოკოლის – უსაფრთხო ჰიპერტექსტის საშუალებით (HTTPS). უმეტეს შემთხვევაში სისტემების მომხმარებლები საკმარისად არ აქცევენ ყურადღება მათ უსაფრთხოებას. კვლევების საფუძველზე ირკვევა, რომ რიგითი მომხმარებელი არ იცნობს სისტემების უსაფრთხოების სხვადასხვა მექანიზმს და არ ესმის მათი გამოყენების მნიშვნელობა. ეს ფაქტი საგრძნობლად ამცირებს მომხმარებელთა უსაფთხოების დონეს სხვადასხვა სისტემაში, განსაკუთრებით ვებსაიტებზე ან სხვადასხვა მრავალ მომხმარებელზე გათვლილ სისტემებში. პირადი ინფორმაციის და მონაცემთა დარღვევა, ფიშინგი და სხვადასხვა სოციალური საინჟინრო მეთოდები –მომხმარებელზე ორიენტირებული შეტევები – დღეს ძალიან პოპულარულია მომხმარებელთა არასაკმარისი ცოდნის გამო.

ეს ვითარება, ასევე, გამოწვეულია ზოგიერთი გამოყენებადობის პრობლემით უსაფრთხოების მექანიზმში. მომხმარებელს არ შეუძლია გაიგოს, რატომ და როგორ უნდა გამოიყენოს უსაფრთხოების მოდელები პრაქტიკაში. ამ ნაშრომში შეთავაზებული იქნება დაბალანსებული, მომხმარებელზე მორგებული (user-friendly) პროცესის ერთ-ერთი ყველაზე ხშირად გამოყენებული უსაფრთხოების მექანიზმი – Transport Layer Security (TLS) სერთიფიკატის HTTPS კავშირის დამყარებისთვის კლიენტსა და სერვერს შორის. ეს მიდგომა გაზრდის TLS-ის სერთიფიკატების გამოყენებას ვებსაიტების მფლობელების მიერ, შესაბამისად, ვებგვერდებზე მომხმარებლის უსაფრთხოების დონე ასევე გაუმჯობესდება.

ამასთან ერთად, მნიშვნელოვანი ფაქტორია გამოყენებადობის დონე და ზოგადად გამოყენებადობა, რაზეც დიდწილად დამოკიდებულია თავად უსაფრთხოების პროცესი

და მისი პრაქტიკული გამოყენება. ამ პროცესის გამართვისთვის საჭიროა სისტემაში მომხმარებლის ინტერესების გათვალისწინება [5,6].

2.3 მომხმარებელზე ორიენტირებული უსაფრთხოების მექანიზმები

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

ამ მიმართულებით ჩატარებული კვლევები მომხმარებელზეა ორიენტირებული და მიზნად ისახავს, რომ მომხმარებელმა კარგად გაიგოს სისტემის პროცესები. ყველაზე მნიშვნელოვანი ნაწილი HCI-ში არის მომხმარებლის პარამეტრების, შესაძლებლობებისა და შეზღუდვების შესწავლა მათი ტექნოლოგიაში დასანერგად. ამ მონაცემების საფუძველზე ხდება უფრო მეგობრული და სხვა მომხმარებლისთვის უფრო გასაგები მექანიზმების გამოყენება. ამგვარი მოდელი შეიძლება დანერგილი იყოს სხვადასხვა ვებსაიტსა ან მრავალ მომხმარებელზე გათვლილ სისტემებში.

გამოყენებადობის კუთხით არსებობს შემდეგი პარამეტრები:

სიჩქარე – საზომი, თუ რამდენად სწრაფად შეუძლია მომხმარებელს სისტემაში ამოცანის შესრულება.

ეფექტურობა – იზომება რამდენი შეცდომაა დაშვებული ამოცანის შესრულებისას.

სწავლის უნარი – ზომავს რამდენად სწრაფად შეუძლია მომხმარებელს შეისწავლოს სისტემის პროცესები.

დამახსოვრებადობა – რამდენად დასამახსოვრებელია სისტემა მომხმარებლისთვის.

მომხმარებლის გამოხმაურება – მომხმარებლის გამოხმაურების საფუძველზე შეგვიძლია დავადგინოთ ჩვენი სისტემის სუსტი წერტილები და ნაკლებად გამოსადეგი სეგმენტები.

სისტემის უკეთესი გამოყენებადობა ნიშნავს სისტემაში მომხმარებლის უფრო კომფორტულ მუშაობას. ამ მიდგომას, ცხადია, საკმაოდ დადებითი გავლენა ექნება მრავალმომხმარებლიანი სისტემების უსაფრთხოების დონეზე.

2.4 უსაფრთხოების სერტიფიკატების ტიპები

იმისათვის, რომ მივიღოთ 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 TLS სერთიფიკატების წარმომადგენლები:

ზოგადი დანიშნულების TLS სერთიფიკატები – მცირე და საშუალო ბიზნესის ვებსაიტებისთვის გამოყენებული სერთიფიკატები;

გაფართოებული ვალიდაციის (EV) TLS სერთიფიკატები – გამოიყენება უფრო დიდი პროექტებისთვის, რომლებისთვისაც საჭიროა ორგანიზაციების და სპეციალური დოკუმენტაციის შემოწმება;

მრავალი დომენის EV TLS სერთიფიკატები – ერთი სერტიფიკატი შეიძლება გამოყენებულ იქნეს მრავალი ვებგვერდის დომენისთვის;

Wildcard TLS სერთიფიკატები – გამოიყენება ვებსაიტების ქვედომენებისთვის;

პირადი ავთენტიფიკაციის/ელ-ფოსტის სერთიფიკატები – გამოიყენება პირადი ან ელ-ფოსტის კლიენტების დაშიფვრისთვის.

თითოეულ სერთიფიკატს აქვს თავისი დანიშნულება და განსაკუთრებული მახასიათებლები, რომლებიც დამოკიდებულია ვებგვერდის ტიპზე, ინდუსტრიასა და გლობალიზაციაზე. მფლობელებმა უნდა გაიგონ, რომელი ტიპის TLS სერთიფიკატი უნდა ჰქონდეთ და რომელი უნდა გამოიყენონ კონკრეტულ შემთხვევაში.

ფასიანი და უფასო სერტიფიკატები:

არსებობს, ასევე, სერტიფიკატების ორი ტიპი: ფასიანი და უფასო. თვისობრივად, ისინი, როგორც წესი, ერთმანეთისგან არ განსხვავდება, თუმცა ფასიან სერტიფიკატებს აქვთ გარკვეული პირობები, რომელიც მომხმარებლისთვის უფრო კომფორტულია. მაგალითად, უფასო სერტიფიკატს გააჩნია ვალიდაციის უფრო ნაკლები ვადა, როგორც წესი 3-6 თვე, როდესაც ფასიანი სერტიფიკატების ვადა განისაზღვრება 1-2 წლამდეც კი. ვადის გასვლის შემდეგ საჭიროა სერტიფიკატის ხელახალი გენერაცია, რომ შესაძლებელი იყოს მისი გამოყენება, მაგრამ აქაც არის რამდენიმე ნიუანსი: კვლევის შედეგად დადგინა, რომ ზოგიერთი სერვერის შემთხვევაში (განსაკუთრებით ეს მუშაობს ე. წ. საზიარო ჰოსტინგზე (shared hosting)) შესაძლებელია უფასო სერტიფიკატის განახლება ავტომატურად, სერვერზე სპეციალური ბრძანების გაწერით.

ამასთან ერთად, ფასიანი სერტიფიკატი მომხმარებელს სთავაზობს ტექნიკურ მხარდაჭერას სერტიფიკატის გენერაციის, გამართვის და დაყენების საკითხებში, როცა უფასო სერტიფიკატების გენერაციის და კონფიგურაციის პროცესი სრულიად დამოკიდებულია მომხმარებელზე (საიტის მფლობელზე).

სერთიფიკატების გამცემები:

დღეისთვის არსებობს საკმაოდ ბევრი სერთიფიკატების გამცემი ორგანიზაცია, რომელიც დაკავებულია სხვადასხვა ტიპის სერტიფიკატების შექმნით და გავრცელებით, ზოგიერთი – კონკრეტულად, უსაფრთხოების საკითხებითაც. მათ ეწოდებათ Trusted authorities – სანდო ორგანიზაციები, რომელთა სერტიფიკატებიც ლეგიტიმურია და აღიარებულია სხვადასხვა ინტერნეტ ბრაუზერის მიერ. ნებისმიერ თანამედროვე ბრაუზერში არსებობს სპეციალური სერტიფიკატების გამცემების მონაცემთა ბაზა, სადაც

განთავსებულია აღნიშნული სანდო ორგანიზაციები. საიტზე შესვლისას სერტიფიკატი მოწმდება, თუ ის გაცემულია სანდო ორგანიზაციის მიერ, მაშინ ბრაუზერი მას უპრობლემოდ ატარებს. მისი შემოწმება ხდება საიტზე გაშვებული სერტიფიკატის ბრაუზერში ჩაშენებულ ბაზასთან შედარებით.

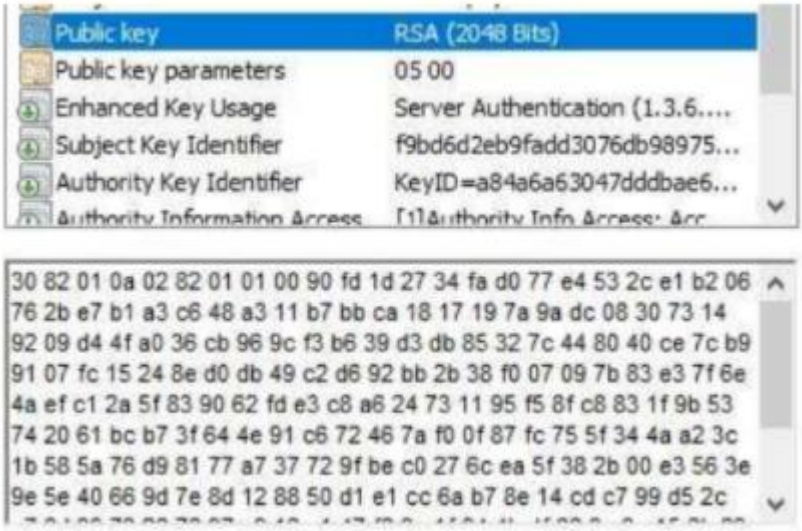
ნახ. 2. *სერტიფიკატების გამცემების ლოკალური ბაზა*

2.5 უსაფრთხოების სერტიფიკატების გენერაცია

ტრანსპორტის ფენის უსაფრთხოების (Transport layer security – TLS) ყველა ტიპი უნდა იყოს დაინსტალირებული და კარგად კონფიგურირებული სერვერის მხარეს. კლიენტები იყენებენ ნაგულისხმევ პარამეტრებს TLS სერთიფიკატების კონფიგურაციისთვის, რაც დამწყებთათვის სავსებით ნორმალურია. 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 კლიენტი სერვერთან კავშირს ამყარებს. პირველ ეტაპზე გამოიყენება RSA კრიპტოგრაფიული ალგორითმი. კავშირის დამყარების შემდეგ მას გადაეცემა სპეციალური გასაღები, რომელსაც ეწოდება სესიის გასაღები (session key) და სიმეტრიული კრიპტოგრაფია იწყებს მუშაობას. TLS სამუშაო პროცესში გამოიყენება ჰიბრიდული დაშიფვრის მეთოდები, რაც გამოწვეულია ორი მთავარი მიზეზით: უსაფრთხოებითა და ეფექტურობით.

ასიმეტრიული კრიპტოგრაფია უფრო უსაფრთხოა და ამიტომ ეს მეთოდი გამოიყენება სესიის გასაღების დაშიფვრისთვის, მაგრამ მას დაბალი სიჩქარე აქვს. უფრო მაღალი სიჩქარის უზრუნველსაყოფად, მეორე ეტაპზე, როცა სესიის გასაღები უკვე გადაცემულია, ამ დროს TLS-ში გამოიყენება AES ალგორითმი. სიმეტრიული შიფრაცია გამოიყენება ყოველჯერზე იმის ნაცვლად, რომ გამოვიყენოთ მძიმე ასიმეტრიული კრიპტოგრაფია მონაცემთა მიმოცვლისთვის.



ნახ. 3. *უსაფრთხოების სერტიფიკატი საიტის მხარეს*

გრაფიკულ გამოსახულებაზე (ნახ. 3) ვხედავთ, რომ ვებსაიტი იყენებს RSA დაშიფვრას.

ალგორითმი და საჯარო გასაღების სიგრძე არის 2048 ბიტი, რომელიც მიღებულია სტანდარტების ეროვნული ინსტიტუტის (NIST) მიერ. ჰოსტინგის ზოგიერთი კომპანია

უზრუნველყოფს უფასო სერტიფიკატების მიწოდებას და ასევე მართვის სისტემას TLS სერტიფიკატების ხელით კონფიგურაციისთვის. მაგალითად, ერთ-ერთ ჩვენს კვლევაში განხილულია გერმანიაში მყოფი Hetzner Online GmbH პროვაიდერი, რომელსაც გააჩნია მონაცემთა სხვადასხვა ცენტრი. ეს პროვაიდერი მომხმარებელს სთავაზობს უფასო TLS სერტიფიკატის წარმოების მოდელებს ზოგიერთი პაკეტისთვის პირდაპირ ჰოსტინგის მმართველ პანელში. მომხმარებელს შეუძლია ხელით აწარმოოს სერტიფიკატის შექმნის და გამართვის პროცედურა.

ტრანსპორტის შრის უსაფრთხოების სერტიფიკატის წარმოების პროცესი

ასეთ სერთიფიკატებს აქვს ორი ეტაპი – გაცემის პროცედურა და DNS ვალიდაციის პროცესი. პირველ ეტაპზე, სერთიფიკატის გენერაციის პროცესის გასაშვებად, მომხმარებელმა უნდა განსაზღვროს შემდეგი:

- დომენური სახელი;
- DNS დადასტურება;
- TLS სერთიფიკატის სახელი;
- საერთო სახელი (common name);
- გასაღების სიგრძე (ბიტებში).

ასეთი სერთიფიკატები მუშაობს დომენის სახელის ან DNS სერვერზე, ხოლო დაფუძნებული ვალიდაცია მოითხოვს სპეციალურ TXT ჩანაწერებს ჰოსტინგის კონფიგურაციაში. ინფორმაციის შეტანის შემდეგ იწყება TLS სერტიფიკატის მიღების პროცედურა. სისტემა ავტომატურად ქმნის თვითნებურად დამოწმებულ სერთიფიკატს პირველი ეტაპის განმავლობაში მომხმარებლის მიერ შეტანილი პარამეტრებით. ყოველ ხუთ წუთში ერთხელ სისტემა ცდილობს, მიიღოს სერთიფიკატი.

მომხმარებლის გამოყენებადობის პრობლემები

ზოგჯერ TLS სერთიფიკატის გენერაციის და კონფიგურაციის პროცესი ხორციელდება ვებსაიტის მფლობელების მიერ. სერთიფიკატის არასწორი კონფიგურაცია ახდენს

ნეგატიურ გავლენას მთელი საიტის ეფექტურობასა და უსაფრთხოებაზე. სერტიფიკატის სწორი კონფიგურაციისთვის მომხმარებელმა უნდა იცოდეს სერტიფიკატის გენერაციის თითოეული პარამეტრი, რათა შეძლოს მისი სწორი გამართვა და დაყენება.

თუ ვებსაიტი გამოიყენება მხოლოდ ინფორმაციული მიზნებისთვის, ჩვენ გვჭირდება ერთი დაბალანსებული უსაფრთხოების მექანიზმი, მაგრამ თუ ვებსაიტი შეიცავს სხვადასხვა მგრძნობიარე ინფორმაციას, მაგალითად, მომხმარებლის პერსონალურ მონაცემებს, ეს სულ სხვა სიტუაციაა და ამ შემთხვევაში უსაფრთხოების დონე უნდა გაიზარდოს. ჩვენ უკვე ვიცით, რომ უსაფრთხოების დონის მატებასთან ერთად, სისტემის გამოყენებადობა აუცილებლად იკლებს. შემოთავაზებულია TLS სერტიფიკატის წარმოების ზოგიერთი მოსახერხებელი მექანიზმი, მაგრამ მათ ჯერ კიდევ აქვთ ეფექტურობის პრობლემები. განხილულია დაშიფვრა TLS სერთიფიკატების წარმოების პროცესის მაგალითზე, რომელიც მოწოდებულია Hetzner Online GmbH-ის მიერ. შეგვიძლია გავიგოთ, რომ სერტიფიკატის კონფიგურაციის ძირითადი პარამეტრები უნდა დაადგინოს მომხმარებელმა, რამაც შეიძლება გამოიწვიოს ვებგვერდზე უსაფრთხოების პრობლემა, განსაკუთრებით მაშინ, თუ ვებგვერდი შექმნილია, მაგალითად, ონლაინ მაღაზიის განსათავსებლად. ამ შემთხვევაში საიტი წარმოადგენს როგორც სავაჭრო ან მონაცემთა გაცვლის პლატფორმას, სადაც მომხმარებელი აგზავნის და იღებს პერსონალურ მონაცემებს.

უსაფრთხოების პრობლემები

მიუხედავად იმისა, რომ მომხმარებელს პრობლემები აქვს უსაფრთხოების მექანიზმების გაგებასთან დაკავშირებით, ის შეეცდება არ გამოიყენოს რთული სისტემები, მათი საჭიროების მიუხედავად. მრავალმომხმარებლიან სისტემებში უსაფრთხოების პრობლემების უმეტესობა იმის გამოა, რომ კლიენტს არ აქვს შესაფერისი ცოდნა. კარგად ფორმირებული და ადვილად გამოსაყენებელი უსაფრთხოების მექანიზმები გადაჭრის კიბერუსაფრთხოების უამრავ პრობლემას და ხელს შეუშლის მომხმარებელზე თავდასხმებს.

უსაფრთხო დიზაინის მეთოდების რეალიზაცია

კიბერუსაფრთხოების სფეროში ჩატარებული კვლევების საფუძველზე, მომხმარებელზე ორიენტირებული უსაფრთხოების ყველაზე ეფექტური სისტემები აგებულია მაღალი დონის გამოყენებადობის გათვალისწინებით. მიუხედავად იმისა, რომ უსაფრთხოების სისტემა ნაწილობრივ იმართება ადამიანის მიერ, უსაფრთხო დიზაინის კონცეფციებისა და მეთოდების სრულად მართვა დიდ გავლენას მოახდენს სისტემის მთლიან უსაფრთხოების დონეზე. უსაფრთხო დიზაინი მიზნად ისახავს ძლიერი უსაფრთხოების მექანიზმის შემუშავებას მომხმარებლისთვის მოსახერხებელი და გასაგები ინტერფეისით და ფუნქციონირებით. დიზაინის აგების ციკლი შედგება ძირითადი სტრუქტურის მშენებლობის სხვადასხვა ეტაპისგან:

მოთხოვნები – განსაზღვრავს სისტემასთან ურთიერთქმედების მოთხოვნებს. სისტემის შიგნით ძირითადი მიმართულება, ამოცანები და წესები.

ანალიზი - მთელი სისტემის კონცეპტუალური მოდელის აგება, რომელიც ემყარება მოთხოვნების კვლევას და პრაქტიკულ ანალიზს. დიზაინი – სისტემის ძირითადი სტრუქტურა, რომელიც ყველაზე მნიშვნელოვანი ნაწილია ადამიანის და სისტემის ურთიერთქმედების პროცესში. აგრეთვე გასათვალისწინებელია სხვადასხვა ფაქტორიც. ინტერფეისი უნდა შეესაბამებოდეს შემთხვევის გამოყენებას.

დანერგვა – ამ ეტაპზე სისტემის ტექნიკური ნაწილი უნდა იყოს ინტეგრირებული. გათვალისწინებული უნდა იყოს უსაფრთხოების ყველა ზომა და გაანალიზდეს სხვადასხვა სცენარი [7-9].

2.6 გამოყენებადობის არსებული მდგომარეობის შეფასება

სადოქტორო ნაშრომზე მუშაობისას შევისწავლეთ დღეისთვის არსებული კრიპტოსისტემები, უნდა განვიხილოთ შედეგიანად განხორციელებული თავდასხმები არსებულ კრიპტოსისტემებზე. თანამედროვე კრიპტოსისტემების სუსტი მხარეების გამოვლენა და მისი ანალიზი ჩვენი კვლევის ერთ-ერთი ნაწილია. მიმდინარეობს

არსებულ კრიპტოსისტემებზე პრაქტიკული და თეორიული ნამუშევრების განხილვა. შესწავლილია არსებულის გაუმჯობესების მეთოდების ეფექტურობა და მათი პრაქტიკაში გამოყენების პერსპექტივა. მიღებული შედეგები ცნობილი გახდება კიბერუსაფრთხოების ექსპერტებისთვის, როგორც პირადი მიმოწერის, აგრეთვე სოციალური ჯგუფების და ფორუმების საშუალებით. მიღებული რჩევების და მათი ღრმა ანალიზის საფუძველზე შესაძლებელი იქნება სისტემის გაუმჯობესება და მისი ეფექტურობის გაზრდა. ძირითადი კვლევის საკითხებს კი წარმოადგენს: არსებული უსაფრთხოების მექანიზმების გამოყენებადობის სუსტი წერტილების გამოვლენა და მათზე წარმატებულად განხორციელებული თავდასხმების განხილვა, იმის გაანალიზება, თუ რითი არის გამოწვეული ეს გამოყენებადობის პრობლემები, დაცვითი სისტემების რა ელემენტებზე კეთდებოდა ძირითადი აქცენტი და როგორი სახის გაუმჯობესების გზების შეთავაზება არის საჭირო ამ პრობლემების გადაჭრისთვის.

გაანალიზებულია არსებული უსაფრთხოების სისტემების გამოყენებადობა და გამოვლენილია სუსტი წერტილები, შესწავლილია თავდასხმების მაგალითები არსებულ სისტემებზე. ასევე იქნა განხილული RSA-ს არსებული ალტერნატივა და კეთდება მათი გამოყენებადობის და პრობლემების ანალიზი. სადოქტორო ნაშრომზე მუშაობისას შევისწავლეთ და გამოვიყენეთ მსოფლიოში წამყვანი კიბერუსაფრთხოების ექსპერტების ნაშრომები, ისეთების, როგორებიც გახლავთ: Dan Boneh და Jonathan Katz; გავეცანით სამეცნიერო პუბლიკაციებს კრიპტოგრაფიის დარგში, გავაანალიზეთ მიღებული შედეგები. პრაქტიკული ნაშრომების განხილვის შემდეგ გამოიკვეთება კიბერუსაფრთხოების ძირითადი პრობლემები და მათი გადაჭრის გზები უფრო ნათელი გახდება.

თავი 3. შიგთავსზე დაფუძნებული ფილტრაციის სისტემები

3.1 შიგთავსზე დაფუძნებული ფილტრაცია

თანამედროვე კიბერსამყაროში სარეკომენდაციო სისტემები ხელოვნური ინტელექტის მექანიზმების ყველაზე თვალსაჩინო მაგალითია. ჩვეულებრივ, ასეთი პროგრამები იქმნება მომხმარებლის უკეთესი გამოცდილებისთვის სხვადასხვა სისტემებში. მაგალითად, Facebook, რომელიც შეიცავს – „ადამიანები, რომლებსაც შეიძლება იცნობდეთ“ – მოდულს და YouTube, რომელიც გთავაზობთ შესაბამის ვიდეოს თქვენი ინტერესის მიხედვით, რაც დგინდება დათვალიერების წინა ისტორიის საფუძველზე. ეს ყველაფერი შეიძლება ჩაითვალოს მომხმარებელზე ორიენტირებული სარეკომენდაციო სისტემების საკმაოდ კარგ მაგალითებად. ვებპლატფორმები მომხმარებელს საშუალებას აძლევს, მიიღოს რეკომენდაციები სხვადასხვა კრიტერიუმის საფუძველზე. ალგორითმებს, რომლებიც გამოიყენება ასეთი პროგრამების მიერ, სარეკომენდაციო სისტემებს უწოდებენ. დღეს ალგორითმები გამოიყენება სხვადასხვა სარეკომენდაციო სისტემაში, მაგრამ ყველაზე ხშირად შინაარსზე დაფუძნებულ შემოთავაზებების მეთოდს იყენებენ, რომელიც ორიენტირებულია მომხმარებელზე.

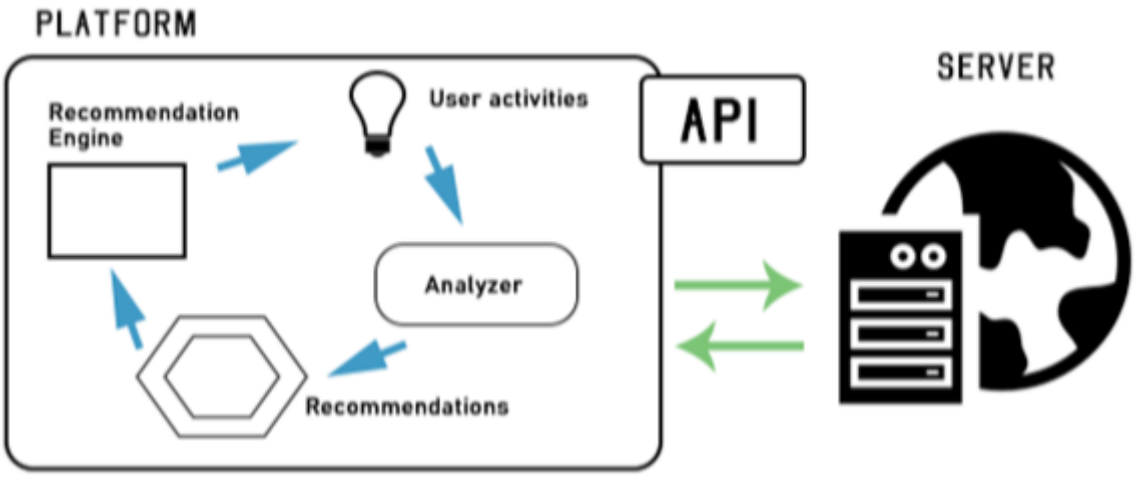
სარეკომენდაციო სისტემები ფართოდ გამოიყენება შინაარსის ფილტრაციისთვის სხვადასხვა ვებპლატფორმაში, ისეთებში, როგორებიცაა: ონლაინ მაღაზიები, ფილმების ან მოგზაურობის მონაცემთა ბაზა, საგანმანათლებლო მიმართულებები და მრავალი სხვა. მსგავსი შინაარსის ფილტრაციის სისტემები (content filtering systems) მომხმარებელს ეხმარება მაქსიმალურად ადვილად იპოვოს შესაბამისი შინაარსი, მისი საჭიროებიდან და ინტერესიდან გამომდინარე. დღეს ნებისმიერი თანამედროვე სისტემისთვის მომხმარებლის უსაფრთხოება უაღრესად მნიშვნელოვანია.

ჰაკერების შეტევისთვის იყენებენ სხვადასხვა ტექნიკასა და მიდგომებს. აპარატურულ უზრუნველყოფაზე დაფუძნებული სისტემები ხშირად ხდება სხვადასხვა თავდასხმის სამიზნეები. გარჩევის ან კრიტიკული ინფორმაციის მიღებისთვის თავდასხმის მოდელის ერთ-ერთი ყველაზე პოპულარული მეთოდია გვერდითი არხი (side-channel),

ცენტრალურ პროცესორზე ორიენტირებული (central processor unit) და, აგრეთვე, ფიზიკური შეტევები. აღსანიშნავია, რომ სხვადასხვა პროგრამული მექანიზმი სამუშაოდ იყენებს აპარატურულ სისტემას, რომლის უსაფრთხოების ხარვეზებმა შეიძლება მათ სერიოზული პრობლემები შეუქმნას. სისტემა უზრუნველყოფს მომხმარებელს რეკომენდაციებით შესაბამის ინტერესებსა და პარამეტრებზე დაყრდნობით. სარეკომენდაციო სისტემის პირველი ვერსია ეყრდნობა ცნობილ ღია წყაროებს, მოწყვლად მონაცემთა ბაზებს და მუშაობს თითოეული მომხმარებლის შეტანისთვის ინდივიდუალურად. მანქანური სწავლების მექანიზმების გამოყენებით, რომლებიც ჩაწერილია არსებულ რეკომენდაციების სისტემაში უკეთესი შედეგების მისაღწევად. ასეთი მიდგომა მნიშვნელოვნად გაზრდის უსაფრთხოების დონეს აპარატურულ სისტემებში [10].

3.2 შიგთავსზე დაფუძნებული ფილტრაციის პრინციპები

უსაფრთხოების სცენარის ანალიზისთვის შინაარსზე (content-based) დაფუძნებულ რეკომენდაციების სისტემას სჭირდება მომხმარებლის მიერ მიწოდებული მონაცემები და სპეციალური ჩარჩოები, რომლებიც ინახება მონაცემთა ბაზაში. მაგალითად, შინაარსზე დაფუძნებული პარამეტრები, შეფასება, უკუკავშირი და მომხმარებლის სხვა აქტივობები. ამ შემთხვევაში კიბერუსაფრთხოებასა და ტექნიკაზე დაფუძნებულ სისტემებში მონაცემები, კონკრეტული რეკომენდაციით, გაანალიზებულია სისტემის მიერ. სისტემაში მონაცემების შედის სპეციალური ინტერაქტიული ჩაშენებული ფორმის გამოყენებით. ამ მონაცემებზე დაყრდნობით, სისტემა ქმნის მომხმარებლის პროფილს, რომელიც გამოიყენება შესაბამისი უსაფრთხოების რეკომენდაციების შესაქმნელად. ეს პროცესი მიმდინარეობს მომხმარებლის მხრიდან დამატებითი ინფორმაციის შეტანის საშუალებით. სისტემას შეუძლია ამ დამატებითი ინფორმაციის დამუშავება, რის შედეგადაც ეს მექანიზმი ხდება უფრო ზუსტი [11].



ნახ. 4. *კონტენტზე დაფუძნებული სისტემის მუშაობის პრინციპი*

როგორც ნაჩვენებია გრაფიკულ გამოსახულებაზე (ნახ. 4.), პლატფორმის შიგნით სისტემას შეუძლია გვიჩვენოს მომხმარებლის საქმიანობა – მისი მონაცემები და პრეფერენციები, ის მათ აანალიზებს და გარდაქმნის რეკომენდაციებად. მიღებული რეკომენდაციები კი იგზავნება სარეკომენდაციო ძრავასთან. პლატფორმა ქმნის კავშირს სერვერთან, რის შემდეგაც გაცვლის მონაცემებს სპეციალური არხით ან სპეციალური API-თ.

ყოველი ახალი იტერაცია გვაძლევს უფრო ზუსტ და მომხმარებელზე მორგებულ შედეგს, გამომდინარე იქიდან, რომ ხდება მომხმარებლის უფრო მეტი მონაცემების დაგროვება და გამოიკვეთება მისი პრეფერენციები და სხვა აქტივობა სისტემასთან მიმართებით.

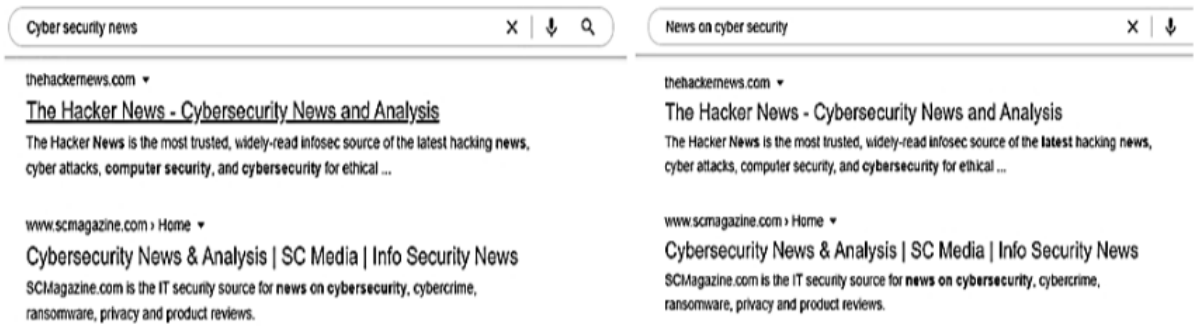
შინაარსზე დაყრდნობილ სისტემებში გამოყენებული კონცეფცია

შინაარსზე დაფუძნებულ მექანიზმებში გამოყენებული ცნებები ხშირად ეყრდნობა ინფორმაციის აღდგენის სისტემებს. ინფორმაციის მოძიების ეს სისტემები მომხმარებელს უზრუნველყოფს შესაბამისი ძიების შედეგებით. ამავე დროს ის აანალიზებს მომხმარებლის ქცევას. ეს აძლევს ამ სისტემებს შესაძლებლობას, დაადგინოს, არის თუ არა სასარგებლო მომხმარებლის ძებნის მოთხოვნა. ეს პროცესი ემყარება განსხვავებული კომბინაციის ალგორითმებს, რომლებიც ხელს უწყობს თითოეული მომხმარებლის მოთხოვნის ძიების პროცესს. ჩვენ ვხედავთ აღნიშნული ალგორითმების პრაქტიკულ

მუშაობას, როდესაც ვიყენებთ ძებნას ისეთი ძრავების დახმარებით, როგორებიცაა Google ან Yahoo.

ასეთი ტიპის საძიებო სისტემებში ინფორმაციის აღდგენის სისტემები უფრო რთულია, რადგან ის მუშაობს უზარმაზარ მონაცემებთან და ეყრდნობა ინტერნეტის მომხმარებლის მოთხოვნებს. საძიებო სისტემების მუშაობა ნათლად გამოჩნდება, თუ შევადარებთ სხვადასხვა ძიების შედეგებს (ნახ. 5):

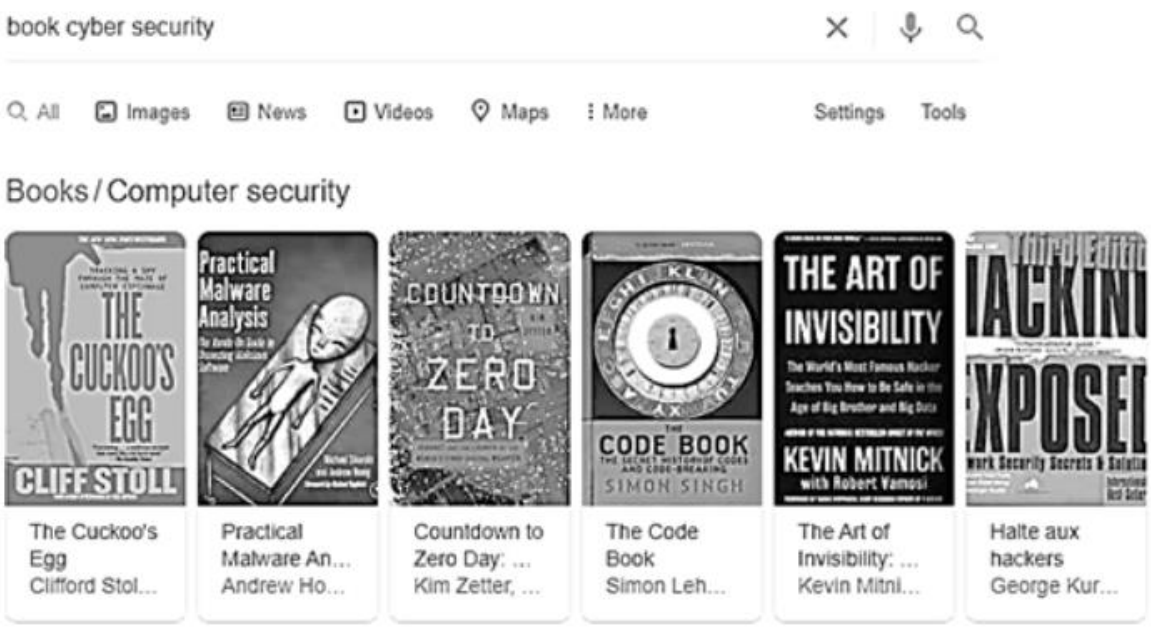
- Cyber security news;
- News on cyber security;



ნახ. 5. *საძიებო სისტემის შედეგების დემონსტრაცია*

როგორც ვხედავთ, ორივე საძიებო მოთხოვნის (ნახ. 5) შედეგები ძალიან ჰგავს ერთმანეთს. ასევე უნდა აღინიშნოს ისიც, რომ თუ ჩვენ შევასრულებთ ისეთ საძიებო მოთხოვნას, როგორიცაა, მაგალითად, „წიგნები კიბერუსაფრთხოება“, ჩვენ სულ სხვა შედეგს მივიღებთ. საძიებო სისტემა გვთავაზობს უსაფრთხოებასთან დაკავშირებულ სხვადასხვა წიგნებს, რომლებიც ინტერნეტში იძებნება. მართალია, შედეგი განსხვავებულია, მაგრამ საინტერესო ისაა, თუ როგორ შეუძლია საძიებო სისტემას ამოიცნოს საძიებო მოთხოვნა და მიაწოდოს მომხმარებელს შესაბამისი ინფორმაცია. საძიებო ძრავები აგროვებენ ინფორმაციას, რომელსაც მომხმარებლები აწვდიან მოთხოვნების დროს და ამ შედეგის საშუალებით საძიებო სისტემას შეუძლია გააანალიზოს და შესატყვის შინაარსში სხვადასხვა საძიებო ობიექტები მოძებნოს. შედეგი მიიღწევა ტექსტის მოპოვების ტექნიკის გამოყენებით. თანამედროვე საძიებო სისტემები განსხვავებული ტექსტის მოპოვების ტექნიკას იყენებენ. ყველაზე თვალსაჩინო ტექნიკა

ტექსტის მოპოვებისთვის არის TF მატრიცა (ტერმინის სიხშირის მატრიცა). ამ ტექნიკის საფუძველზე კონტექსტში ყველაზე ხშირად გავრცელებულ სიტყვას უფრო მეტი აქტუალურობა აქვს. საძიებო სისტემა იყენებს TF-ის მატრიცას, რათა გააანალიზოს თითოეული სიტყვის სიხშირე საძიებო სისტემაში, რომელსაც ითხოვს მომხმარებელი [12-13].



ნახ. 6. *შედეგების დემონსტრაცია წიგნების მაგალითზე*

3.3 შინაარსობრივი ტერმინები და მათი მნიშვნელობა

დღეისთვის სარეკომენდაციო სისტემებში გამოიყენება ორი ძირითადი მექანიზმი: სიხშირის ტერმინი (TF – term frequency) და ინვერსიული დოკუმენტის სიხშირე (IDF – inverse document frequency). აქედან გამომდინარე, შეგვიძლია განვსაზღვროთ სხვადასხვა

შინაარსის ვებსაიტებისთვის გამოყენებული სიტყვების სიხშირე. სადოქტორო ნაშრომზე მუშაობისას ჩვენ დავამუშავეთ შემდეგი ორგანიზაციების ვებგვერდები:

1. სამეცნიერო კიბერუსაფრთხოების ასოციაციის ოფიციალური ვებგვერდი;
2. Utoweb სტუდიის ოფიციალური ვებგვერდი;
3. საბავშვო კიბერუსაფრთხოების უნივერსიტეტის ოფიციალური ვებგვერდი.

ცხრილი 1. ასახულია თითოეული სიტყვის სხვადასხვა სიხშირის დათვლის შედეგები ვებსაიტის შინაარსში:

	სიტყვების სიხშირე					
საიტი	security	wesite	student	team	university	design
1	120	28	15	17	9	1
2	25	85	0	5	0	75
3	85	105	55	0	1	1

ცხრილი 1*. ტერმინების სიხშირე*

ტერმინების სიხშირის შესამოწმებლად ზემოთ აღნიშნულ ვებგვერდებზე უნდა დაითვალოს სიტყვების წარმოქმნის რაოდენობა. მაგალითად, ის ფაქტი, რომ კონკრეტული სიტყვა "X" პირველ ვებგვერდზე გვხვდება 20-ჯერ, ხოლო მეორე ვებგვერდზე – 4-ჯერ, არ ნიშნავს რომ სიტყვა „X“ პირველ ვებგვერდზე 5-ჯერ უფრო აქტუალურია, ვიდრე მეორეში. სხვაობა ამ შემთხვევაში გაცილებით ნაკლებია. „ტერმინი სიხშირე“-თან ერთად უნდა გავითვალისწინოთ „ინვერსიული დოკუმენტის სიხშირე“ (IDF), რომელიც ზომავს, რამდენად მნიშვნელოვანია კონკრეტული ტერმინი დოკუმენტში. ტერმინის სიხშირე (TF) ჩვეულებრივ იყოფა დოკუმენტის ზომაზე და გვიჩვენებს შინაარსის კონკრეტული პირობების საერთო რაოდენობას:

TF (A) = რამდენჯერ გამოჩნდება ტერმინი A დოკუმენტში და იყოფა ჯამზე ამ დოკუმენტის ტერმინების რაოდენობა. რადგან ინვერსიული დოკუმენტის სიხშირე (IDF) ზომავს ტერმინის მნიშვნელობას, გასათვალისწინებელია, რომ ისეთი შემთხვევები,

როგორებიცაა "the", "of", "or", "is" შეიძლება ბევრი აღმოჩნდეს შინაარსში, მაგრამ ნაკლები წონა ექნება.

ბალანსის მიღება შესაძლებელია შემდეგი ფორმულით:

IDF (A)= log_e (ყველა დოკუმენტის რიცხვი გაყოფილი დოკუმენტების რაოდენობაზე, შინაარსით A). მაგალითად, ჩვენ გვაქვს ტერმინი A, რომელიც 3-ჯერ გვხვდება D დოკუმენტში, რომელიც, ჯამში, შეიცავს 100 სიტყვას, TF ტერმინისთვის გამოითვლება (3/100) = 0,03.

მაგალითად, თუ ჩვენ გვაქვს ათი მილიონი დოკუმენტი და A ტერმინი გვხვდება 1000 დოკუმენტში და არ გვჭირდება დოკუმენტის სიხშირის გამოთვლა, ეს შეიძლება გაკეთდეს შემდეგნაირად:

$$\log (10\,000\,000/1\,000) = 4$$

ამიტომ A შემთხვევაში TF-IDF წონა არის ზემოთ ნახსენები სიდიდეების ნამრავლი, 0,03 * 4 = 0,12.

TF-IDF გაანგარიშების log გამოიყენება უფრო მაღალი სიხშირის სიტყვების ეფექტის შესუსტებისთვის.

წონის საფუძველზე შეგვიძლია გამოვთვალოთ მნიშვნელობა ტერმინსა და თავად დოკუმენტს შორის. ამისათვის ჩვენ მივცემთ წონას, რომ ტოლი იყოს კონკრეტული ტერმინის დადგომის რაოდენობის შეწონილი TF-ის. გამოსათვლელად გამოვიყენოთ ფორმულას:

$$w_{t,d} = \begin{cases} 1+log_{10}tf_{t,d}, & if\ tf_{t,d} > 0 \\ 0, & otherwise \end{cases}$$

ნახ. 7*. TF-ის გამოთვლა*

ამ ფორმულის გამოყენებით, არსებული ტერმინების სიხშირის შედეგების გარდაქმნის მიზნით, ვხედავთ, რომ შეწონილ TF-ში ტერმინების სიხშირე კლებულობს.

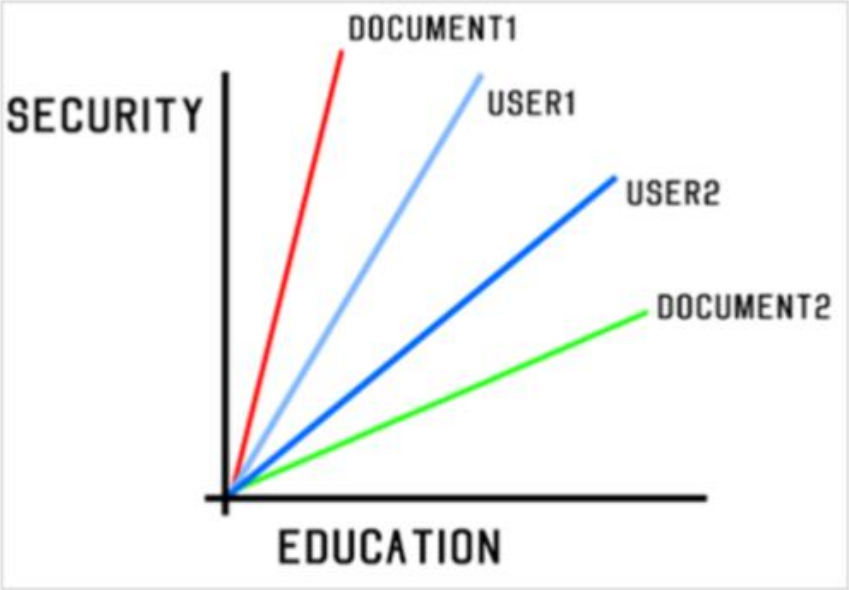
შეწონილი TF-ის მნიშვნელობები უფრო ახლოსაა ერთმანეთთან, ვიდრე ორიგინალი ტერმინის სიხშირის მნიშვნელობები. აქ ჩვენ შეგვიძლია დავინახოთ ორიგინალი ტერმინების სიხშირეების ტრანსფორმაცია:

ტერმინის სიხშირე	შეწონილი ტერმინის სიხშირე
0	0
10	2
1000	4

***ცხრილი 2**. TF და WTF მნიშვნელობების შედარება*

ვექტორული სივრცის მოდელის პრინციპი

მას შემდეგ, რაც გამოითვლება TF და IDF, უნდა განისაზღვროს, რომელი ობიექტები უფრო ახლოს არის ერთმანეთთან. ეს კეთდება ვექტორული სივრცის მოდელის საშუალებით (vector space model). VSM-ის დახმარებით შეგვიძლია გამოვთვალოთ სიახლოვე, რომელიც ვექტორებს შორის კუთხეს ეყრდნობა. VSM-ში თითოეული ობიექტი ინახება, როგორც ვექტორი n-განზომილებიან სივრცეში. ვექტორებს შორის სივრცის გამოთვლა საჭიროა ამ ვექტორებს შორის მსგავსების დასადგენად.



ნახ. 8. *ვექტორის სივრცის მოდელი*

იმის დასადგენად და გამოსათვლელად, იყენებს თუ არა სისტემას მომხმარებელი, ვექტორების ნორმალიზაციის შემდეგ გამოვთვალეთ კუთხის კოსინუსი მომხმარებლისა და დოკუმენტების ვექტორებს შორის ($User_i$). სიგრძე უდრის ერთს, ეს იმას ნიშნავს, რომ კოსინუსის გაანგარიშება ამ ვექტორების ჯამია (cos (document1, document2)) [14-16].

3.4 ფილტრაციის პრინციპების გამოყენება კიბერუსაფრთხოებაში

შინაარსზე დაფუძნებული რეკომენდაციების სისტემის მოდელი შეგვიძლია გამოვიყენოთ უსაფრთხოების მექანიზმებში. ჩვენ მიერ შემუშავებული ვებსისტემა იყენებს ჩაშენებულ ფილტრაციის მექანიზმს მომხმარებლის მიერ შეტანილი მონაცემების სიხშირის გამოსათვლელად. მას აგრეთვე შეუძლია გამოაქვეყნოს მომხმარებლისთვის შესაბამისი რეკომენდაციები.

სისტემა ორიენტირებულია მომხმარებლის მიერ შეტანილი მონაცემების ანალიზზე. მომხმარებლის მიერ შეტანილი მონაცემების საშუალებით სისტემა აწარმოებს გამოთვლებს TF-IDF ფორმულის მიხედვით, რათა აღმოაჩინოს მსგავსება სხვა მომხმარებლების მიერ ადრე შეტანილ მონაცემებთან.

იმ შემთხვევაში, თუ მომხმარებელს აქვს Intel-ის მიერ წარმოებული პროცესორი და ქსელური ბარათი TP-Link, სისტემას შეუძლია მონახოს მსგავსებები შინაარსის მიხედვით და მომხმარებელს მიაწოდოს რეკომენდაციები კონკრეტული სცენარის საფუძველზე.

შეტანილი მონაცემი	**Intel**	**CPU**	**TP Link**
ინფორმაციული ბლოკი 1	4	5	3
ინფორმაციული ბლოკი 2	5	2	1
ინფორმაციული ბლოკი 3	2	3	0
ინფორმაციული ბლოკი 4	0	1	1
ინფორმაციული ბლოკი 5	1	2	2

დოკუმენტის სიხშირე	550	1000	400

***ცხრილი 3**. ტერმინების სიხშირე*

Intel-ის შეწონილი ტერმინის სიხშირე ინფორმაციულ ბლოკში 1 გამოითვლება შემდეგნაირად:

$$1 + log_{10}4 = 1.602$$

***ნახ. 9**. შეწონილი ტერმინის სიხშირე ინფორმაციულ ბლოკში*

ანალოგიურად ტერმინის სიხშირე გამოითვლება საინფორმაციო ბლოკების სხვა ატრიბუტებისთვისაც. ეს მნიშვნელობები ქმნის ატრიბუტის ვექტორს თითოეული ინფორმაციის ბლოკისთვის.

შეტანილი მონაცემი	**Intel**	**CPU**	**TP Link**
ინფორმაციული ბლოკი 1	1.602	1.698	1.477
ინფორმაციული ბლოკი 2	1.698	1.301	1
ინფორმაციული ბლოკი 3	1.301	1.477	0
ინფორმაციული ბლოკი 4	0	1	1
ინფორმაციული ბლოკი 5	1	1.301	1.301

***ცხრილი 4**. შედეგი შეტანილი მონაცემების მიხედვით*

მას შემდეგ, რაც სისტემა მიიღებს ტერმინულ სიხშირეს, ინვერსიული დოკუმენტის სიხშირე შეიძლება გამოითვალოს დოკუმენტის სიხშირის ლოგარითმული ინვერსიის გამოყენებით ინფორმაციის მთელი სპექტრის მიხედვით. ამიტომ, თუ მონაცემთა ბაზაში შეგვიძლია ვიპოვოთ 22 000 დოკუმენტის ინფორმაცია, ხოლო 550 ბლოკში გამოჩნდეს ტერმინი „Intel“, მისი IDF გამოითვლება შემდეგნაირად:

$$log_{10}(22000 / 550) = 1.602$$

***ნახ. 10**. IDF-ის გამოთვლა*

ანალოგიურად, IDF გამოითვლება ზემოთ აღწერილი მომხმარებლის მიერ შეტანილი თითოეული ტერმინისთვის.

IDF	1.602	1.342	1.740

***ნახ. 11**. IDF მომხმარებლის მიერ შეტანილი მონაცემების მიხედვით*

მაგალითად, პირველი საინფორმაციო ბლოკისთვის სიგრძის ვექტორი (LV) უნდა გამოითვალოს შემდეგნაირად:

$$LV_1 = \sqrt{(1.602^2 + 1.698^2 + 1.477^2)} = 2{,}760$$

***ნახ. 12**. სიგრძის ვექტორი პირველი საინფორმაციო ბლოკისთვის*

ამიტომ ნორმალიზებული ვექტორის მისაღებად, თითოეული ტერმინის ვექტორი უნდა გაიყოს დოკუმენტის ვექტორის სიგრძეზე. ტერმინ "Intel"-ის ნორმალიზებული ვექტორი არის პირველ ინფორმაციულ ბლოკში.

$$1.602 / 2.760 = 1.021$$

***ნახ. 13**. ტერმინი პირველი საინფორმაციო ბლოკისთვის*

მონაცემების ნორმალიზებული ვექტორების მიღების შემდეგ, სისტემას შეუძლია დაადგინოს მსგავსი ინფორმაცია საინფორმაციო ბლოკებს შორის. ამისთვის საჭიროა მონაცემთა კოსინუსური მნიშვნელობების გაანგარიშება.

მნიშვნელობები ორი საინფორმაციო ბლოკისთვის:

ინფორმაციული ბლოკი 1	1.602	1.698	1.477
ინფორმაციული ბლოკი 2	1.698	1.301	1
ინფორმაციული ბლოკი 3	1.301	1.477	0

***ცხრილი 5**. საინფორმაციო ბლოკების მნიშვნელობები*

როგორც ვხედავთ, ინფორმაციული ბლოკების 1 და 3 მონაცემები უფრო მსგავსია, ვიდრე 2 და 3 საინფორმაციო ბლოკების მონაცემები. მიღებული მონაცემების საშუალებით სისტემას შეუძლია შემოგვთავაზოს შესაბამისი რეკომენდაციები სისტემის უსაფრთხოების გასაუმჯობესებლად, სპეციალური პროგრამული უზრუნველყოფის ინსტალაციის ან არსებული არხების და კომპონენტების განახლების ჩათვლით.

ხაზგასმით უნდა აღინიშნოს, რომ შინაარსზე დაფუძნებული სარეკომენდაციო სისტემებს აქვთ გარკვეული შეზღუდვები. ამიტომ სამომავლოდ ვაპირებთ, გავაანალიზოთ მანქანური სწავლების სხვადასხვა მიდგომები და გავაკეთოთ რომანის ჰიბრიდული მიდგომა არსებული მეთოდების გამოყენებით. ეს მიდგომა გახდის სხვადასხვა სისტემას ბევრად უფრო მოსახერხებელსა და ზუსტს. ამის შემდეგ ვიმუშავებთ ჩვენ მიერ მიღებული ახალი მიდგომის ეფექტურობის გაუმჯობესებაზე [17-19].

თავი 4. კვლევისის ფარგლებში მიღებული შედეგები

4.1 შემუშავებული სისტემა

სადოქტორო ნაშრომზე მუშაობისას განვიხილეთ და შევისწავლეთ არსებული უსაფრთხოების სისტემები, გავაანალიზეთ მათი სუსტი მხარეები გამოყენებადობის მხრივ. გავაანალიზეთ, აგრეთვე, არსებული უსაფრთხოების სისტემების ნაკლოვანებების გამოსწორების შეთავაზებული გზები, რის შემდეგაც მოხდა გამოყენებადობის მოდელებით გაუმჯობესებული სისტემის პროგრამული რეალიზაცია. ამ სამუშაოების ჩატარების შემდეგ მივიღეთ შედეგები გამოყენებადობის გაუმჯობესებისთვის და შევიმუშავეთ რამდენიმე იდეა იმის შესახებ, თუ როგორ უნდა განხორციელდეს პროგრამული ალგორითმი და მისი ვიზუალური მხარე.

ნაშრომზე მუშაობისას შევისწავლეთ უცხოური ლიტერატურა, გავითვალისწინეთ მათში მოცემული საკვანძო პრინციპები, რომლებიც აღწერილი და დადგენილი იყო კიბერუსაფრთხოების ცნობილი ექსპერტების მიერ. მიღებული იდეები და კონცეფციები განვიხილეთ თემატურ ჯგუფებსა და ფორუმებში როგორც ინტერნეტის, აგრეთვე პირადი შეხვედრების დროს. მიღებული პასუხების/რჩევების საფუძველზე გავაუმჯობესეთ პროტოტიპები და მცირე კორექტივები შევიტანეთ საერთო დიზაინში. მუშაობის პროცესში შეგვხვდა რამდენიმე რთულად ამოსახსნელი ამოცანა, რომლის გადაჭრაშიც დიდი დახმარება გაგვიწია ჩვენმა პროექტის ხელმძღვანელმა.

ჩვენი კვლევის პირველ ეტაპზე ნათლად გამოჩნდა არსებული პრობლემა. ამ პრობლემას არსებული თანამედროვე უსაფრთხოების მექანიზმების გამოყენებადობის დაბალი დონე წარმოადგენს, რაც იმას ნიშნავს, რომ რიგითი მომხმარებელი ყოველდღიურ ცხოვრებაში ამ უსაფრთხოების მექანიზმების უმრავლესობას ვერ გამოიყენებს. ეს ფაქტი საგრძნობლად ამცირებს უსაფრთხოების დონეს როგორც მრავალმომხმარებლიან საიტებზე, ასევე სხვა სამუშაო სისტემებში. პროექტის ერთ-ერთ მიმართულებას წარმოადგენს უსაფრთხოებასა და გამოყენებადობას შორის ბალანსის დამყარება და მომხმარებლისთვის უფრო მარტივი სამუშაო გარემოს შექმნა.

ამავე ეტაპზე, პარალელურად, ხდებოდა უცხოური სამეცნიერო ნაშრომების შესწავლა, შერჩეულ იქნა მომხმარებლისთვის საუკეთესო ბალანსი უსაფრთხოებასა და გამოყენებადობას შორის. აღნიშნული ლიტერატურის გაანალიზების და დასკვნების გამოტანის შემდეგ შევიმუშავეთ პრობლემის მოგვარების ერთ-ერთი ასპექტის პროტოტიპი. მასში გათვალისწინებული იყო არსებული პრაქტიკული პრობლემები.

მომხმარებელს ჰქონდა შესაძლებლობა, თავად გაევლო უსაფრთხოების სისტემის პროცესები უფრო გასაგებ და გამარტივებულ გარემოში. ამასთან ერთად, სატესტო პროტოტიპი იყო გაზიარებული კიბერუსაფრთხოების დარგის ექსპერტებთან, რაც ძალიან მნიშვნელოვანია, რადგან სპეციალისტების მიერ გაკეთებული კომენტარები სისტემის პროტოტიპის გაუმჯობესების თაობაზე პროექტის წარმატების მნიშვნელოვანი პირობაა.

კიბერუსაფრთხოების დარგის სპეციალისტებისგან მიღებული გამოხმაურების საფუძველზე არსებულ პროტოტიპში შევიტანეთ შესაბამისი ცვლილებები როგორც სტრუქტურული, ასევე დიზაინერული კუთხით. ასევე გათვალისწინებული იყო სატესტო პროტოტიპის გაგზავნაში მონაწილე მომხმარებლის მოსაზრება განახლებული სისტემის კომფორტულობის შესახებ. ყველა არსებული და გაანალიზებული ცვლილება შევიდა ძალაში, მოხდა მათი ინტეგრაცია არსებულ პრაქტიკულ პროტოტიპში.

გაუმჯობესებული პროტოტიპი შემოწმდა, დადგინდა მისი დადებითი და უარყოფითი მხარეები. მნიშვნელოვანია, რომ პროტოტიპში მომხმარებლისთვის მარტივი ელემენტების დამატებასთან ერთად არ მოიკლოს უსაფრთხოების დონემ, წინააღმდეგ შემთხვევაში პროტოტიპს დაეკარგება აზრი. მომხმარებლისთვის გათვლილი სისტემა აუცილებლად უსაფრთხო უნდა იყოს.

მას შემდეგ, რაც სისტემა გავაუმჯობესეთ, ის ხელახლა გაიგზავნა შესამოწმებლად ექსპერტებთან და მომხმარებელთან. ახალი გამოხმაურებები კიდევ უფრო სასარგებლო აღმოჩნდა, გამომდინარე იქიდან, რომ პროტოტიპი იყო ბეტა ტესტირების დონეზე და შესაძლებელი გახდა მისი მიღება და გამოყენება ღია წყაროებიდან. შესაბამისად, ნებისმიერ მსურველს შეეძლება სისტემის ბეტა ვერსიის დანერგვა უკვე არსებულ

პროექტებში, კვლევებსა ან სხვა ნაშრომებში. პროტოტიპი გარკვეული დროის მანძილზე აუცილებლად იყო ბეტა ტესტირების ეტაპზე, რათა მომხმარებელმა მიიღოს მაქსიმალურად მორგებული და ხარისხიანი პროდუქტი.

ბეტა ტესტირების მთელი პერიოდის მანძილზე იმუშავა ჩვენ მიერ შექმნილმა მხარდაჭერის და აზრების გაზიარების პლატფორმამ. ამ პლატფორმაზე ნებისმიერ მომხმარებელს შეეძლება საკუთარი აზრის დაფიქსირება და სასურველ კითხვაზე ადეკვატური და სწრაფი პასუხის მიღება. მხარდაჭერის პლატფორმა იმუშავებს Online რეჟიმში, შესაბამისად იგი იქნება ხელმისაწვდომი როგორც კომპიუტერის დახმარებით, ასევე მობილური მოწყობილობებიდან. პლატფორმა თავადაც ითამაშებს დიდ როლს საბოლოო პროდუქტის გაუმჯობესებასა და უფრო დახვეწილი და მომხმარებელზე მორგებული პროდუქტის რეალიზაციაში.

შესაბამისი გამოხმაურების მიღების შემდეგ, ეტაპობრივად მოხდა გამოყენებადი სისტემის გაუმჯობესება. გათვალისწინებული იქნა როგორც თანამედროვე მომხმარებლისთვის მისაღები დიზაინის ტენდენციები, ასევე სტრუქტურული უსაფრთხოების მექანიზმები და სტანდარტები. სისტემა შემოწმებული იყო არსებულ სტანდარტებზე, რადგან მხოლოდ სტანდარტად ქცეული სისტემების გამოყენება არის რეკომენდირებული. მით უმეტეს, როდესაც საქმე გვაქვს ისეთ საკითხთან, როგორიც არის მომხმარებლის და მისი მონაცემების უსაფრთხოება.

სადოქტორო ნაშრომზე მუშაობისას განვიხილეთ ისეთი დარგის ასპექტები, რომლებიც უფრო მეტ ყურადღებას და დაკვირვებას მოითხოვს, შევაფასეთ უსაფრთხოების მეთოდები შემდეგი კრიტერიუმების გათვალისწინებით:

1. **დაცვის დონე** – ყოველთვის ძნელია იმის გარკვევა, თუ რა დონის დაცვაა საჭირო კონკრეტულ სისტემაში. ძირითადად ეს განიხილება, როგორც აუცილებელი მეთოდებისა და ოპერაციების ერთობლიობა, რომ სისტემამ იმოქმედოს უპრობლემოდ, ასევე ხელი შეუშალოს მასზე უნებართვო წვდომას.

2. **ფუნქციონალურობა** – იმისათვის, რომ სისტემამ იმუშაოს, აუცილებელია დალაგებული კომბინაცია. თუ რომელია ყველაზე ეფექტური, დამოკიდებულია მათ თვისებებზე.

3. **მუშაობის მეთოდები –** როდესაც უსაფრთხოების მეთოდები გამოიყენება სხვადასხვა გზით და განსხვავებული შეტანით, ისინი სხვა თვისებებს იძენენ. ამრიგად, ერთ მექანიზმს შეიძლება ჰქონდეს განსხვავებული ფუნქციები. ეს ყველაფერი დამოკიდებულია იმაზე, თუ როგორ გარემოში გამოიყენება მექანიზმი.

4. **შესრულება** – ეს კრიტერიუმი მოიცავს მექანიზმების ეფექტურობას კონკრეტული დავალების შესრულების დროს. მაგალითად, დაშიფვრის ალგორითმი ფასდება წამში დაშიფრული ბიტების რაოდენობით.

5. **განხორციელების სიმარტივე** – ეს კრიტერიუმი მოიცავს კონკრეტული ამოცანისთვის მექანიზმის განხორციელების სირთულეს. მექანიზმების რეალიზაცია შესაძლებელია როგორც პროგრამულად, ისე აპარატურის დახმარებით. სხვადასხვა კრიტერიუმის მნიშვნელობა დამოკიდებულია დავალებასა და არსებულ რესურსებზე. მაგალითად, იმ გარემოში, სადაც კომპიუტერის რესურსები შეზღუდულია, დაცვა არ შეიძლება ძალიან მაღალ დონეზე აიყვანოს, რადგან სისტემას უპრობლემოდ მუშაობა გაუჭირდება.

სადოქტორო კვლევის ამ ეტაპზე მივიღეთ შედეგები უსაფრთხოების არსებული სისტემების მომხმარებელთა ეფექტურობის გაზრდის მიზნით. კერძოდ, შეიქმნა სხვადასხვა სისტემის მქონე ვებსისტემის რამდენიმე პროტოტიპი, რომლებიც კვლევის ფარგლებში წარუდგინეს სისტემის მომხმარებელს და უსაფრთხოების მოდულის რამდენიმე ვიზუალური ელემენტის გამოყენება სთხოვეს. მოდულების უსაფრთხოების დონე იგივე იყო, მაგრამ გარე ფუნქციონირება – განსხვავებული. შეიქმნა აგრეთვე რამდენიმე მოქმედი პროტოტიპი, რომელთა პრინციპები ემყარება მომხმარებლის როგორც ტექნიკურ, ასევე ვიზუალურ მოთხოვნებს.

ვიზუალური პროტოტიპების შემუშავებიათვის გამოვიყენეთ თანამედროვე ქსელი და უსაფრთხოების ტექნოლოგიები, როგორებიცაა: HTML, CSS, JavaScript. როგორც წინა,

ასევე სერვერული პროგრამირებისთვის გამოყენებულ იქნა php და MySQL ტექნოლოგიები. შედეგად, ჩვენ გვაქვს სისტემის პროტოტიპი, რომელიც ნათლად აჩვენებს მომხმარებელთა სისტემასთან ურთიერთქმედებას და საშუალებას გვაძლევს შევისწავლოთ ამ უკანასკნელის ძირითადი მოთხოვნები და სისტემის მუშაობის პრინციპები. უსაფრთხო და მოსახერხებელი სისტემის შექმნისას მნიშვნელოვანია გავითვალისწინოთ როგორც სისტემის მოთხოვნები, ასევე მომხმარებლის გამოცდილება. მრავალი მომხმარებლისთვის უსაფრთხოების მექანიზმები უბრალოდ გაუგებარია მათი სირთულის გამო.

პროტოტიპებში გამოყენებული უსაფრთხოების მექანიზმები, გაუმარტივებს მომხმარებელს მუშაობას. ის საშუალებას გვაძლევს, განსაზღვროთ მომხმარებლისთვის კომფორტის ზონა და, რაც მთავარია, მისთვის გასაგები უსაფრთხოების მექანიზმები.

ჩვენი კვლევისას შევიმუშავეთ სპეციალიზებული პლატფორმა, რომელზეც განთავსებულია მომხმარებლისთვის განკუთვნილი ინტერაქტიული ფორმა. ამ ფორმის შევსების შედეგად მომხმარებელი იღებს შესაბამის რეკომენდაციებს კონკრეტულ თემაზე.

სისტემაში გათვალისწინებულია მანქანური სწავლების ალგორითმები, რომლებიც წარმოადგენს ამ მიმართულებით ახალ მიდგომას. გამომდინარე იქიდან, რომ ამ პერიოდისთვის სარეკომენდაციო სისტემები, რომლებიც დაფუძნებულია მანქანურ სწავლებაზე და, კერძოდ, შინაარსის ფილტრაციის ალგორითმზე, არ იყო გამოყენებული კიბერუსაფრთხოების სარეკომენდაციო სისტემისთვის.

აგრეთვე შევიმუშავეთ ალგორითმი, რომელიც ორიენტირებულია კონკრეტულად კიბერუსაფრთხოების რეკომენდაციების გაცემაზე, ის ამუშავებს მოწოდებულ ინფორმაციას ამ დარგის მიხედვით.

ვებსისტემას საფუძვლად უდევს შინაარსზე დაფუძნებული ფილტრაციის სარეკომენდაციო ალგორითმი. სისტემის ძირითადი ნაწილი გათვლილია მონაცემთა

მოგროვება/შენახვაზე, რაც შემდგომი მუშაობისთვის და სარეკომენდაციო ფუნქციონალის გაუმჯობესებისთვის არის გამოყენებული.

შიგთავსზე დაფუძნებული სისტემის ალგორითმის მუშაობის სქემა იწყება საბაზისო კონფიგურაციით, რაც მოიაზრებს სისტემის მონაცემთა ბაზასთან დაკავშირებას. სისტემის მონაცემთა ბაზასთან დაკავშირების პროცესის შესრულების შემდეგ, აუცილებელია, არსებულ მონაცემთა ბაზაში შეიქმნას ორი ცხრილი:

მომხმარებლების ინფორმაცია – ეს ცხრილი მონაცემთა ბაზაში განკუთვნილია თითოეული მომხმარებლის მონაცემების შესანახად. როდესაც მომხმარებელი სისტემაში ახალი დარეგისტრირებულია, ცხრილის მნიშვნელობები ცარიელია და ივსება მომხმარებლის სისტემაში ქცევების მიხედვით. გამომდინარე იქიდან, რომ სისტემაში ინახება თითოეული მომხმარებლის პროფილი, ეს მონაცემები უნდა იყოს ასახული მონაცემთა ბაზაში როგორც სტატისტიკური, ასევე დინამიკური მონაცემების დასამუშავებლად. მნიშვნელობები ცხრილში ანგარიშდება უკვე ცნობილი მეთოდებით, რომლებიც აღწერილია შინაარსზე დაფუძნებული ფილტრაციის სისტემის მუშაობის პრინციპებში.

რეკომენდაციების ცხრილი – ეს ცხრილი განკუთვნილია მონაცემთა ბაზაში სხვადასხვა კატეგორიების მიხედვით რეკომენდაციების შენახვა/დამუშავებისთვის. ამ პროცესის დახმარებით ინახება რელევანტური კომბინაციები, მომხმარებლის მიერ შეტანილი და მიღებული მონაცემების მიხედვით. აღსანიშნავია, რომ რეკომენდაციების ცხრილში მონაცემები მუდმივად იცვლება და ახლდება იმის მიხედვით, თუ როგორი არჩევანი აქვს გაკეთებული მომხმარებელს.

მონაცემთა ბაზაში არსებული ცხრილების დამუშავების შემდეგ სისტემა ადგენს, რომელი რეკომენდაცია იქნება უფრო რელევანტური მომხმარებლის კონკრეტული არჩევანის მიხედვით. ამის შემდეგ მონაცემები ჩაიწერება ე. წ. დროებით ცხრილში, სადაც ხდება დაკავშირება სხვადასხვა გარე რესურსებთან თანამედროვე კიბერუსაფრთხოების შემთხვევების და პრობლემების ასახვისთვის.

```php
public $max_view_history = 30; // დღეებში
public $max_post_age = 1000;
public $max_results = 3;
private $taxonomy_selection = array();
private $category_selection = array();
private $user_selection = array();
private $viewed_post_IDs = array();
private $use_cache = false;
private $max_cache_time = 1;
private $recommendation_box_title_default = 'Recommended for you';
private $included_post_types = 'post';
private $show_on_page_types = array('post');
private $browser_locate;
private $plugin_options_name = 'plugin_sosere';
private $array_sosere_options;
private $prefetch_request = false;
private $show_thumbs_title = false;
private $title_leng = 50;
private $show_thumbs = false;
private $sosere_custom_thumbnail_size = '150x150';
private $default_thumbnail_img_url = null;
private $use_custom_css = false;
private $hide_output = false;
private $dnt = null;
private $data_sources = array('tag'=>'tag', 'category'=>'category', 'session'=>'session');
```

ნახ. 14. *სარეკომენდაციო სქემის კოდი*

სარეკომენდაციო სქემის კოდში აღწერილია მომხმარებლის მიერ შეტანილი პარამეტრების შენახვის და შემდგომი შედარება/დამუშავების მექანიზმი. მონაცემთა ბაზაში შენახვამდე, მომხმარებლის მიერ შეტანილი ინფორმაცია მუშავდება სისტემის მიერ. გათვალისწინებულია ისეთი პარამეტრები, როგორებიცაა მომხმარებლის მიერ შერჩეული კატეგორია და შესაძლო პასუხების სიზუსტე. ამასთან ერთად, ხდება უკვე არსებული, სხვა მომხმარებლის მიერ შეტანილი ინფორმაციის დამუშავება, რის საფუძველზეც უფრო რელევანტური ხდება სარეკომენდაციო ბლოკების შექმნა. მონაცემების წყაროდ ასევე გამოყენებულია ე. წ. ტეგები, რომლებიც ლოგიკურად ებმევა მომხმარებლის მიერ შერჩეულ კატეგორიას და მომხმარებლის სამუშაო სესიას, პლატფორმაზე გატარებულ დროსა და სხვა აქტივობებს.

მსოფლიო ქსელში ინფორმაციის გადატვირთვა იწვევს სარეკომენდაციო სისტემების განვითარებას ეფექტური გადაწყვეტილებებით. სანდოობის შესაფასებლად სწორი რეკომენდატორის პოვნა სარეკომენდაციო სისტემების არსებითი მახასიათებელია. ინფორმაციის მოძიება მონაცემთა უზარმაზარ მასაში მოსაწყენი პროცესია. ამრიგად, ხდება სარეკომენდაციო სისტემების გაფილტვრა, რადგან რეკომენდაციის პროცესი ტრივიალურია.

ერთიანი ფუნქცია, რომელიც გამოიყენება გამოსათვლელად და რეკომენდაციის ხარისხი დამოკიდებულია რეიტინგის განაწილებასა და აგრეგიტის ანალიზის ტიპზე. უფრო მეტიც, კიდევ ერთი დემოგრაფიული ნაკრების ატრიბუტების გამოყენება შესაძლებელია კლასტერების მოსაძებნად, შესაბამისად, რეკომენდაციების სიზუსტე შეიძლება გაუმჯობესდეს მომავალში. ამ დემოგრაფიული ატრიბუტების შეგროვება მომხმარებლის პროფილში შეიძლება გაიზარდოს უკეთესი რეკომენდაციების მისაღებად.

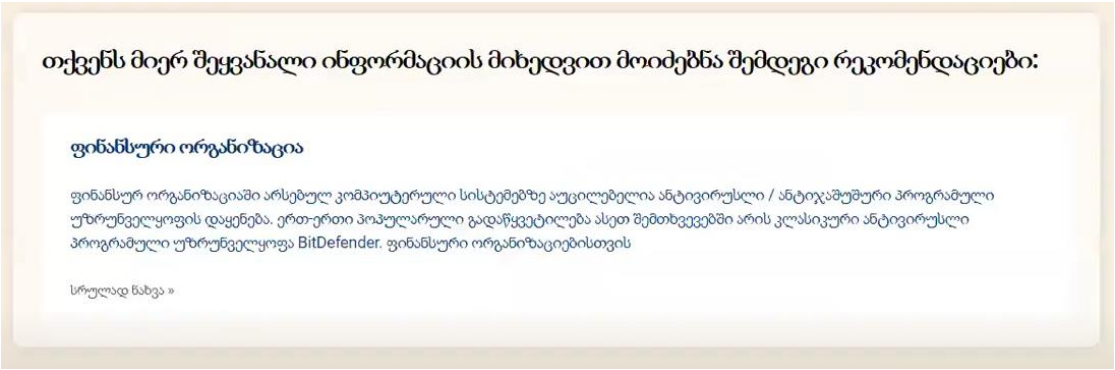
პლატფორმას, რომელიც ჩვენი კვლევის პერიოდში შევიმუშავეთ, აქვს გამართული და მომხმარებელზე მორგებული გრაფიკული ინტერფეისი, რომელიც წარმოდგენილია ვებაპლიკაციის სახით და ხელმისაწვდომია სისტემაში რეგისტრირებული მომხმარებლისთვის. ფორმის ველები, საჭიროებისამებრ, შეიძლება შეიცვალოს. ასევე ფორმაში არის გათვალისწინებული ველების დინამიკური ცვლილება მოთხოვნადი კატეგორიების და შეტანილი მონაცემების საფუძველზე. ამ ეტაპისთვის პლატფორმას გააჩნია სამართავი პანელი, რომლის მეშვეობითაც ხდება კომპონენტების მართვა/მოდიფიცირება.

ნახ. 15. *პლატფორმის ფორმის ინტერფეისი*

აღსანიშნავია, რომ ინტერაქტიული ფორმა ხელმისაწვდომია მხოლოდ სისტემაში რეგისტრირებული მომხმარებლისთვის. პორტალზე შესვლისას ის აუცილებლად მოგვთხოვს ავტორიზაციის გავლას, წინააღმდეგ შემთხვევაში პორტალით ვერ ვისარგებლებთ.

ნახ. 16. *ავტორიზაციის მოთხოვნის ფორმა*

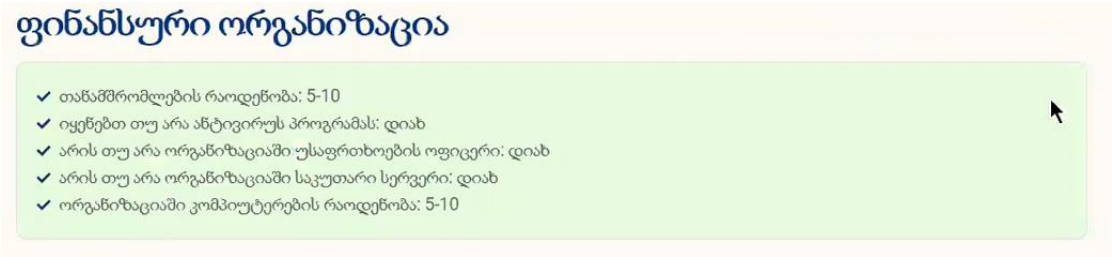
ასეთი მიდგომა პლატფორმის სტრუქტურისადმი განპირობებულია მანქანური სწავლების ელემენტების დანერგვით, რათა უკეთ იყოს შესწავლილი კონკრეტული ავტორიზებული მომხმარებლის ქცევა და მის მიერ შეტანილი მონაცემები. ამასთან ერთად, ასეთი მეთოდის გამოყენებით შესაძლებელია დადგინდეს კონკრეტული მომხმარებლისთვის სარეიტინგო განაკვეთი, რომელიც გააუმჯობესებს მომხმარებლისთვის მიწოდებული რეკომენდაციების რელევანტურობას და სასარგებლო იქნება სამომავლო რეკომენდაციების ბაზისთვის.



ნახ. 17. *მომხმარებლის შედეგების გამოტანა*

სურათზე 22 წარმოდგენილია მომხმარებლის ფორმის შევსების შემდეგ მიღებული შედეგი. ამ შემთხვევაში სისტემაში მოიძებნა კონკრეტული რელევანტური რეკომენდაცია მომხმარებლის მიერ შეტანილი მონაცემების საფუძველზე. არსებულ რეკომენდაციაში მომხმარებელს შეუძლია, წაიკითხოს სრული აღწერა და ამასთან ერთად იხილოს, თუ რა პარამეტრებს აკმაყოფილებს კონკრეტული რეკომენდაცია (სურ. 22).

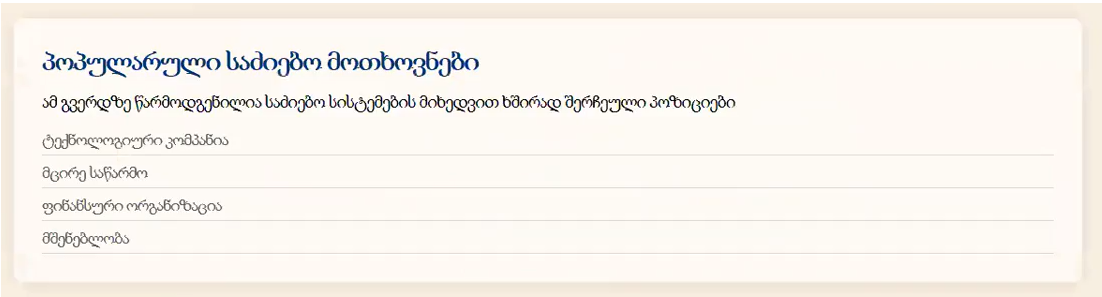
ამასთან ერთად, სარეკომენდაციო გვერდზე წარმოდგენილია ე. წ. რეფერენსები, თემატური საინფორმაციო წყაროები, რომელთა დახმარებით მომხმარებელი მიიღებს უფრო მეტ ცოდნას კონკრეტული საკითხის შესახებ. აღსანიშნავია, რომ წყაროების მითითება და განახლება ხდება რეგულარულად, რათა მომხმარებელმა მიიღოს მისთვის საჭირო ინფორმაცია.



ნახ. 18. *რეკომენდაცია პარამეტრების მიხედვით*

აღსანიშნავია, რომ თითოეულ რეკომენდაციას პლატფორმაზე მოეძებნება სტატისტიკური მონაცემები, ისეთები, როგორებიცაა: თითოეული რეკომენდაციის ნახვების სიხშირე, რაც საგრძნობლად ზრდის მომხმარებლისთვის შეთავაზებული ინფორმაციის რელევანტურობას. მონაცემების მიხედვით შესაძლებელია გავაუმჯობესოთ პლატფორმა მომხმარებლებისთვის უფრო საინტერესო თემებით და შევადგინოთ ყველაზე პოპულარული მოთხოვნების რეიტინგი.

სტატისტიკური მონაცემების საშუალებით შესაძლებელია შეიქმნას სრული სურათი იმისა, თუ რა უფრო მოსწონს მომხმარებელს, რა თემები და რეკომენდაციები აინტერესებს მას და ამ მიმართულებით გავაკეთოთ მთავარი აქცენტი. ნებისმიერი სისტემის შემუშავების დროს ერთ-ერთი მნიშვნელოვანი ფაქტორია მომხმარებლის გამოხმაურება. ამგვარად, ჩვენი სისტემის სტატისტიკური მონაცემების მიხედვით, ბევრად უფრო ნათელი ხდება ის ასპექტები, რომლებიც დროის კონკრეტულ მონაკვეთში უფრო მოთხოვნადია მომხმარებლისთვის.



ნახ. 19. *პოპულარული საძიებო მოთხოვნები*

პოპულარული საძიებო მოთხოვნები დგინდება მომხმარებლის მიერ შეტანილი მონაცემების მიხედვით, რაც საშუალებას იძლევა დადგინდეს რეალურად მოთხოვნადი თემატიკების რეიტინგი. ეს კიდევ უფრო აუმჯობესებს მომხმარებლისთვის სისტემის გამოყენებადობის დონეს და გავლენას ახდენს მის მუშაობის პრინციპებზე.

ნახ. 20. *რეკომენდაციის ნახვები და ბმულები*

4.2 მომხმარებელი და სისტემა

მომხმარებელზე ორიენტირებული სისტემის ერთ-ერთი ყველაზე მნიშვნელოვანი ფაქტორია მომხმარებლის და სისტემის ურთიერთქმედება. შეუძლებელია გამოყენებადი სისტემის შექმნა ამ კონცეფციის გათვალისწინების გარეშე. HCI (Human Computer Interaction) შეისწავლის, თუ როგორ ურთიერთქმედებს მომხმარებელი ტექნოლოგიასთან: ეს შეიძლება იყოს სტაციონალურ კომპიუტერთან, ლეპტოპთან მომუშავე ადამიანი ან მობილური ტელეფონის და პლანშეტური კომპიუტერის მომხმარებელი. უფრო მეტიც, შესაძლოა, მომხმარებელმა გამოიყენოს სხვადასხვა სახის პორტატული მოწყობილობა, როგორიც არის ჭკვიანი საათი, სამაჯურები და სხვ. სისტემაში გათვალისწინებულია მომხმარებლის გონებრივი შესაძლებლობები და მისი ფსიქოლოგიური მდგომარეობა, რათა სისტემასთან მუშაობისას არ ვაიძულოთ იგი, შედეგის მისაღწევად განახორციელოს რთული ქმედებები.

HCI-ის დახმარებით საჭიროა შევისწავლოთ მომხმარებელი და ტექნოლოგიები და გავიგოთ, თუ როგორ ერგებიან ისინი ერთმანეთს. მომხმარებლის პერსპექტივის

მიხედვით უნდა დადგინდეს მისი ცოდნა და ფსიქოლოგიური მახასიათებლები, რაც იძლევა შესაძლებლობას, მივიღოთ ისეთი ტექნოლოგია, რომელიც მომხმარებლისთვის იქნება მარტივად ასათვისებელი და მაქსიმალურად კომფორტული.

HCI-ს საფუძველზე დამუშავდება ტექნოლოგია და შემდეგ შეფასდება. მისი პროექტირების დროს გათვალისწინებული იქნება მომხმარებლის შესაძლებლობები, მათი ამოცანები და სისტემასთან ურთიერთქმედების უნარები. ჩვენი მიზანია, მივიღოთ სისტემა, რომელთანაც მუშაობისას, შედეგის მისაღებად, მომხმარებელს არ დასჭირდება ზედმეტი ქმედებების შესრულება.

ტექნოლოგიის მორგებული უნდა იყოს ნებიესმიერი ასაკის ადამიანზე/ადამიანთა ჯგუფზე. თითოეულ მათგანს გააჩნია გარკვეული მიზნები და ამოცანები, რომელთა განხორციელებაშიც უნდა დაეხმაროს ტექნოლოგია.

მომხმარებლის მიზნები ტექნოლოგიასთან მუშაობისას განსხვავებულია ერთმანეთისგან: დაწყებული პირად გვერდზე შესვლით, დამთავრებული დიდი მოცულობის მონაცემების ანალიზით. მომხმარებელი და ამოცანები შეიძლება იყოს მსგავსი, მაგრამ ამოცანის განხორციელების პირობებზე ხშირად არის დამოკიდებული ტექნოლოგიის მუშაობა.

მომხმარებელი და უსაფრთხოება

დღეისთვის კიბერუსაფრთხოების ექსპერტებში მეტად პოპულარულია HCI მიმართულება. პრაქტიკაში გამოიყენება HCI-ის მოდელები და მეთოდები, რომლებმაც გახადა ის თანამედროვე კიბერუსაფრთხოებაში მეტად საინტერესო და აქტუალური.

ბოლო პერიოდის მანძილზე ხშირად გვხვდება კიბერუსაფრთხოების ხელსაწყოები, რომლებიც მომხმარებლისთვის უფრო გასაგებია, ამიტომ მათ მარტივად იყენებს. ამ იდეის მთავარი არსი იმაში მდგომარეობს, რომ თუკი უსაფრთხოების მექანიზმი მომხმარებლისთვის გასაგები იქნება, იგი მას მომავალშიც გამოიყენებს.

Facebook-ის მიერ ჩატარებული კვლევის საფუძველზე აღმოჩნდა, რომ მომხმარებელმა შედარებით ნაკლები იცოდა Facebook-ის დაცვითი პოლიტიკის შესახებ, მაგრამ გაცილებით ინფორმირებული იყო თამაშების (FarmVille და Candy Crush) ამ საკითხზე. ჩვენი კვლევიდან გამომდინარე ნათელი გახდა, რომ იმისთვის, რომ დაინერგოს ეფექტური უსაფრთხოების/დაცვის კონტროლი, უნდა დადგინდეს, თუ როგორ ურთიერთქმედებს მომხმარებელი ამ სისტემასთან.

HCISec-ს შესწავლის მთავარი მიზანია, გაუმჯობესდეს და გაცილებით კომფორტული გახდეს მომხმარებლისთვის უსაფრთხოების ფუნქციები. HCI-გან განსხვავებით, რომლის შესწავლა დაიწყო 1970-იან წლებში, HCISec ყალიბდება მექანიზმების და ურთიერთქმედების შედარების საფუძველზე. უსაფრთხოების პრობლემებთან ერთად ინტერესი ამ თემის მიმართ იზრდება, რაც ნათლად ჩანს ინტერნეტ სივრცეში არსებულ გამოხმაურებებზე დაყრდნობით.

იმის დასადგენად, თუ როგორ ხდება მომხმარებლის და სისტემის ურთიერთქმედება, აუცილებელია შეფასდეს ტექნოლოგია. ამ შემთხვევაში ხდება არა სისტემის უსაფრთხოების დადგენა, არამედ იმის შეფასება, თუ რამდენად მარტივად მუშაობს მომხმარებელი ამ სისტემასთან.

თუკი სისტემის გამოყენება ძალიან რთულია, მომხმარებელი ქმედებისთვის მოძებნის საფრთხის შემცველ გზას, ან მიიღებს მისთვის ამგვარ გადაწყვეტილებას. ამგვარად, HCI მუშაობს გამოყენებითი უსაფრთხოების პრაქტიკის მიხედვით.

უსაფრთხოება – გამოყენებადობის ბალანსი.

გამოყენებადობა – დადგენა იმისა, თუ რამდენად გასაგები და კომფორტულია მომხმარებლისთვის სისტემასთან მუშაობა. ის შეიძლება პირობითად დავყოთ რამდენიმე ნაწილად:

სისწრაფე – დრო, რომელიც საჭიროა მომხმარებლისთვის კონკრეტული ამოცანის განხორციელებისთვის. ანაბეჭდის გამოყენებით ბლოკის მოხსნა ხდება დაახლოებით 1 წამში, ხოლო პაროლის შეყვანისას დაგვჭირდება 3 წამი.

პროდუქტიულობა – შეცდომები, რომლებიც დაშვებულია შედეგის მიღწევამდე. სმარტფონის ეკრანის ბლოკის მოხსნისას, შესაძლოა დაშვებული იქნეს ისეთი შეცდომები, როგორებიცაა: ანაბეჭდის ამოცნობის შეცდომა, ან არასწორი პაროლის შეყვანა. სისტემის პროდუქტიულობა გამოითვლება შედეგის მიღწევამდე დაშვებული შეცდომების რაოდენობით. პაროლი შეიძლება შეიცვალოს, თითის ანაბეჭდი – არა.

ათვისება – რამდენად სწრაფად სწავლობს მომხმარებელი სისტემასთან მუშაობას.

პროცესის გამარტივებისთვის გამოიყენება ისეთი მეთოდი, როგორიც არის მითითებები მუშაობის გასაგრძელებლად. ათვისების პარამეტრის გამოთვლა შეგვიძლია მომხმარებლის მიერ სისტემაში კონკრეტული შედეგის მისაღწევად დახარჯული დროის მიხედვით პირველ ჯერზე და შემდგომში, მეორე, მესამე და მეოთხე ჯერზე. შედეგის მისაღწევად საჭირო დრო ყოველ შემდგომ ცდაზე უნდა მცირდებოდეს.

გამოხმაურება – გამოსვლისთანავე სისტემა აუცილებლად უნდა იყოს შემოწმებული მომხმარებლის მიერ. მათი მოწონების ან/და შენიშვნების საფუძველზე ხდება პროდუქტის გაუმჯობესება/გადაკეთება. ეს პარამეტრი შეიძლება გამოვიყვანოთ ჯგუფური დისკუსიების ან თემების საფუძველზე. მომხმარებლის გამოკითხვები ასევე ასრულებენ მნიშვნელოვან როლს სისტემის გაუმჯობესების პროცესში.

ყველა ზემოაღნიშნული პარამეტრი დაკარგავს აქტუალობას, თუკი სისტემაში არ იქნება გათვალისწინებული დაცვითი მექანიზმები. გამოყენებითი უსაფრთხოების ერთ-ერთი მთავარი მიზანია, მომხმარებლის კომფორტულ მუშაობასთან ერთად მივაღწიოთ მაქსიმალურ უსაფრთხოებას.

უსაფრთხოება არ არის ის, რაც უნდა მომხმარებელს. მას სჭირდება შედეგის მიღება. ხშირ შემთხვევაში მომხმარებელმა არ იცის, რა არის უსაფრთხოება.

უსაფრთხოება მოითხოვს მომხმარებლისგან რთულ გადაწყვეტილებას, მაგრამ მომხმარებელს ამისთვის არ გააჩნია საკმარისი დრო ან/და ცოდნა.

გაძლიერებული უსაფრთხოება მოითხოვს მეტ რესურსს: მაღალი ფასი, პროცესის შენელება, უფრო რთულად გასაგები მომხმარებლისთვის, რაც საფრთხის შემცველია.

დიდი სისტემები იყენებენ მრავალ კომპონენტს და მომხმარებლის სხვადასხვა ჯგუფებს. მრავალი კომპონენტის გამოყენებამ და მომხმარებელმა შეიძლება კონფლიქტი გამოიწვიოს.

უსაფრთხოების სხვადასხვა ასპექტმა ასევე შეიძლება გამოიწვიოს კონფლიქტი ერთმანეთში, რაც კიდევ უფრო ართულებს პრობლემას.

უსაფრთხოება არის პროცესი და არა პროდუქტი. თუ პროდუქტი დაცულია, შესაბამისად, პროცესიც დაცულია. ჰაკერის მიზანია, დაანგრიოს პროცესში სუსტი რგოლი – ადამიანი!

ხშირ შემთხვევაში მომხმარებელი არ აქცევს ყურადღებას უსაფრთხოებას დროის ან ინფორმაციის არქონის გამო. სისტემაში მომხმარებელს აქვს კონკრეტული ამოცანები, რომელთა გადასაწყვეტადაც იგი იყენებს ამა თუ იმ სისტემას. მომხმარებლის ქმედება პირდაპირპროპორციულია მის ამოცანებთან. რიგით მომხმარებელს არ აინტერესებს ვებსაიტის კიბერუსაფრთხოების ჯგუფის წევრების ვინაობა, სისტემის რთულად ან ზედმეტად დეტალური აღწერა (Facebook-ის კვლევა უსაფრთხოების პოლიტიკასთან დაკავშირებით).

მენტალური მოდელები საკმაოდ მნიშვნელოვანია. ეს მოდელები გვეხმარება იმის გაგებაში, თუ როგორ აღიქვამს მომხმარებელი სისტემას. ისინი გამოიყენება სისტემის დიზაინის შექმნის დროს. ამ მიდგომამ შეიძლება გააძლიეროს გამოყენებადობა თითოეულ კომპონენტში.

მომხმარებელმა არ იცის, როგორ მუშაობს სისტემა, რომელსაც ის იყენებს. იგი უბრალოდ იწყებს სისტემის გამოყენებას, ხოლო გამოყენების წესი და მიდგომები ჩნდება ცხოვრების გამოცდილების საფუძველზე. ამას ემატება სხვა სისტემების გამოყენების გამოცდილებაც (თუკი მომხმარებელს ჰქონია როდესმე მათთან შეხება).

მენტალური მოდელები შეგვიძლია დავყოთ რამდენიმე ტიპად:

მითითება – მითითების ნათელ მაგალითს წარმოადგენს ყველასთვის ცნობილი გაზქურა. გაზქურას აქვს ოთხი გამაცხელებელი ნაწილი, თითოეულს გააჩნია თავისი ჩამრთველი. განლაგების მიხედვით ძალიან რთულია თქმა, თუ რომელი ჩამრთველი

რომელ ნაწილს მართავს. მარეგულირებლების განლაგების შეცვლასთან ერთად, ხდება ბევრად უფრო გასაგები, როგორ უნდა მოხდეს თითოეული ელემენტის მართვა.

შეიძლება შემუშავდეს კიდევ ერთი, გასაგები ვარიანტი, რომელშიც იქნება გათვალისწინებული ორივე პარამეტრი, კომპაქტურობა და მარტივი ადვილი ინტერფეისი. მითითება ხდება უფრო გასაგები ელემენტების განლაგების მიხედვით. ამ შემთხვევაში აშკარაა, რომელი მარეგულირებელი რომელ ელემენტს მართავს. კარგი მაგალითია ასევე ავტომობილის საჭე. ლოგიკურია, რომ როდესაც იგი ტრიალებს მარცხნიდან მარჯვნივ (საათის ისრის საწინააღმდეგოდ), მანქანა მოუხვევს მარჯვნივ და პირიქით. ამავე მაგალითზე მუშაობს მოხვევის მანიშნებელი შუქიც. მარჯვენა შუქის ჩასართავად იგი უნდა გადავრთოთ ზემოთ, ხოლო მარცხენა შუქის ჩასართავად – ქვემოთ.

ხილვადობა – თვალსაჩინო მაგალითს წარმოადგენს GOOGLE-ის საიტი. როდესაც ადამიანი მას იყენებს ინფორმაციის მოძიებისთვის, მას მაშინათვე ხვდება საძიებო ველი. თუკი ადამიანს სჭირდება დამატებითი სერვისები, ისეთები, როგორებიც არის სარეკლამო ინფორმაცია, Drive, GOOGLE Map ან სხვა, მომხმარებელს ამ შემთხვევაშიც აქვს შესაძლებლობა, მარტივად მიაგნოს მისთვის სასურველ ელემენტს.

სისტემის გამოხმაურება – Feedback-ის ან სისტემის გამოხმაურების კარგი მაგალითია ინტერნეტ მაღაზია. მაგალითად, ინტერნეტ მაღაზიაში არ არის დარჩენილი XS ზომა საქონელი, მაგრამ თუ ჩვენ დავაჭერთ აღნიშნულ ზომას, აქტიურდება იმავე მოდელის XS ზომის სხვა ფერები.

კარგად აგებული და გამართული თანამედროვე უსაფრთხოების სისტემა, რომელიც მორგებულია მომხმარებელზე, მის არა მხოლოდ დაცულ, არამედ კომფორტულ მუშაობაზე, უნდა მოიცავდეს სამ ძირითად კომპონენტს:

უსაფრთხო ავტორიზაცია – არსებული უსაფრთხოების სისტემის მომხმარებლის მიერ შეტანილი მონაცემები უნდა იყოს დაცული და მესამე პირს არ უნდა ჰქონდეს წვდომა ამ მონაცემებზე. წინააღმდეგ შემთხვევაში უსაფრთხოების სისტემაში შესაძლოა შეიქმნას გარკვეული პრობლემები. ნათელ მაგალითს წარმოადგენს მომხმარებლის

სისტემაში ავტორიზაცია, როდესაც სისტემის მომხმარებელი სპეციალურ ფორმაში ავსებს პირად მონაცემებს, ისეთებს, როგორებიც არის: მომხმარებლის სახელი/ელ-ფოსტა და პაროლი. ეს პირველი ეტაპი არის გასავლელი მომხმარებლის სისტემაში იდენტიფიკაციისთვის.

უსაფრთხო იდენტიფიკაცია – მომხმარებლის სისტემასთან მუშაობის მეორე საფეხურია. სისტემაში წარმატებით შესვლის შემდეგ მომხმარებელს ეძლევა უფლება, გამოიყენოს სისტემის მიერ მისთვის მინიჭებული პრივილეგიები. განსხვავებულია მომხმარებლის როლები სისტემაში. მომხმარებელმა უნდა მიიღოს მხოლოდ ის პრივილეგიები, რომლებიც მისთვის არის განკუთვნილი. ზოგ მომხმარებელს შეუძლია სისტემაში მართოს მხოლოდ ერთი კონკრეტული განყოფილება, ამავდროულად, ზოგ მომხმარებელს, რომელიც იმყოფება სხვა მომხმარებელთა ჯგუფში (მაგალითად, ადმინისტრატორი), უფლება აქვს მართოს როგორც უფრო დაბალი რანგის მქონე მომხმარებელი, ასევე მისი ცალკეული თუ საერთო განყოფილებები ამა თუ იმ სისტემაში.

უსაფრთხო მიმდინარეობის დრო – სისტემაში მუშაობის პროცესში არ უნდა იყოს შესაძლებელი მომხმარებლის კაბინეტთან ურთიერთქმედება. პრაქტიკაში ხშირად გამოიყენება პროფილიდან ავტომატური გამოსვლის მექანიზმები. ამის ნათელ მაგალითს წარმოადგენს საოფისე სისტემა. როგორც კი მომხმარებელი დაამთავრებს/შეწყვეტს მასთან მუშაობას, იგი გარკვეული დროის უმოქმედობის შემდეგ (მაგ., 5-10 წუთის შემდეგ) ავტომატურად ითიშება.

ინტერაქტიული, მომხმარებელზე მორგებული უსაფრთხოების სისტემის შექმნაზე მუშაობისას აუცილებლად გასათვალისწინებელია ისეთი მნიშვნელოვანი ასპექტი, რასაც მომხმარებლის მახასიათებლები წარმოადგენს. ყურადღება უნდა გამახვილდეს მომხმარებლის მეხსიერებაზე, რადგან ადამიანის მეხსიერებას აქვს გარკვეული შესაძლებლობები და შეზღუდვები. ამის გათვალისწინებით, უნდა შევქმნათ ისეთი დიზაინი, რომელიც მომხმარებელს დაეხმარება და არ დაღლის მას.

მეხსიერების ტიპი, რომელიც დიზაინის შექმნისას დიდ ინტერესს წარმოადგენს, მომუშავე მეხსიერებაა (Working memory), ე. წ. მოკლევადიანი მეხსიერება, სადაც ინახება ინფორმაცია, რომელიც მარტივად და სწრაფად იქნება ხელმისაწვდომი.

1956 წელს ჯორჯ მილერმა წარმოადგინა თეორია, რომლის მიხედვით მომუშავე მეხსიერება იტევს 7 + ან - 2 ინფორმაციის ნაწილს. დროის შემდეგ ეს ციფრი მოდიფიცირდა: იხ.: Broadbent (1975): 4-6 LeCompte (1999): 3. გავრცელებულმა პრაქტიკამ გვიჩვენა, რომ სისტემაში საჭიროა: 4 +/- 1.

თუ რა არის მომუშავე მეხსიერება, ამას განვიხილავთ ინფორმაციის დაყოფის მაგალითით. ჩვენ წარმოვადგენთ სიმბოლოების გარკვეულ სტრიქონს და თქვენ უნდა დაიმახსოვროთ ის მომუშავე მეხსიერებაში. რამდენიმე წამის მანძილზე უნდა დააკვირდეთ ამ სიმბოლოებს. როცა სტრიქონი გაქრება, უნდა აღადგინოთ არსებული სიმბოლოები მეხსიერების დახმარებით.

ეს სტრიქონი შედგება 10 სიმბოლოსგან, რაც აღემატება კლასიკურ 7 + / - 2 რაოდენობას. მსგავსი სიმბოლოების მიმდევრობა იქნება საკმაოდ რთულად დასამახსოვრებელი.

ინფორმაციის დამუშავება

ჩვენ განვიხილეთ სამეცნიერო პუბლიკაციები კრიპტოგრაფიის, პრაქტიკული კიბერუსაფრთხოების და უსაფრთხო დიზაინის დარგში და გავაანალიზეთ მიღებული შედეგები. პრაქტიკული ნაშრომების განხილვისთანავე, გამოიკვეთა უსაფრთხოების კრიპტოგრაფიული სისტემების გამოყენებადობის ძირითადი პრობლემები და თვალსაჩინო გახდა მათი გადაჭრის გზები.

მომხმარებელზე მორგებული სისტემის შესაფასებლად საჭიროა მასზე დეტალურად დაკვირვება. არსებობს სისტემაზე დაკვირვების რამდენიმე მეთოდი: ჩუმი დაკვირვება – არ ვერევით მომხმარებლის მუშაობის პროცესში, არ ვუსვამთ მას კითხვებს და არ ვაძლევთ მითითებებს; ხმამაღლა ფიქრი – მომხმარებელი მოქმედებს და ამასთან ერთად ყველა აზრს ხმამაღლა გამოთქვამს: „ამ საიტზე შევედი ვიდეო გაკვეთილის

სანახავად“; კონსტრუქციული ურთიერთქმედება – მომხმარებელს ვუსვამთ კითხვებს და ვაძლევთ მითითებებს, მაგრამ არ ვაძლევთ რჩევას, თუ როგორ უნდა შეასრულოს ამოცანა. დაკვირვების შემდეგ, როდესაც მომხმარებელი შეასრულებს ყველა ამოცანას, ვიღებთ მისგან ინტერვიუს: მომხმარებლის გამოხმაურება დაკვირვების დროს გაკეთებული ჩანაწერების გამოყენება ინტერვიუს პერიოდში, პასუხების დაფიქსირება შემდგომი ანალიზისთვის.

ინფორმაციის და შედეგების მიღების შემდეგ ვადგენთ ანგარიშს:

მომხმარებლის გამოცდილების შეჯამება და დამუშავება; ბევრ მომხმარებელზე დაკვირვება იძლევა უფრო ზუსტ მონაცემებს გამოყენებადობის და უსაფრთხოების თვალსაზრისით; იმის ანალიზი, როცა რამდენიმე ადამიანი უშვებს ერთსა და იმავე შეცდომას; პრობლემების გამოსწორების გზების მითითება.

მაგალითად, თუ საბანკო პროფილში შესვლა რთული იყო, ეს პროცესი მომხმარებლისთვის ისე უნდა გამარტივდეს, რომ მუშა უსაფრთხოების მექანიზმი სამუშაო ვარიანტი არ გახდეს შესაცვლელი.

გავრცელებულია მეთოდი მომხმარებლის სისტემაში უფრო კომფორტული მუშაობის შესწავლისთვის. ამისთვის ხშირად გამოიყენება ე. წ. გაყოფილი ტესტირება, ან A/B ტესტირება. ამ ტესტირების დროს მოწმდება, თუ რომელი სტრუქტურა იქნება მომხმარებლისთვის უფრო კომფორტული და გამოსადეგი. მზადდება გვერდების ორი ვერსია: პირველ ვერსიას უჩვენებენ მომხმარებლების ერთ ნაწილს, ხოლო მეორეს – მეორე ნაწილს.

სადოქტორო ნაშრომზე მუშაობისას განვიხილეთ და შევისწავლეთ არსებული უსაფრთხოების და დაშიფრვის სისტემები, აგრეთვე გავაანალიზეთ მათი გამოყენებადობის პრობლემები. გაანალიზებული იყო აგრეთვე არსებული კრიპტოსისტემების ნაკლოვანებების გამოსწორების შეთავაზებული გზები, რის შემდეგაც მიმდინარეობს აქტიური მუშაობა გაუმჯობესებული სისტემის პროგრამული რეალიზაციისთვის. ამ ეტაპისთვის უკვე მიღებულია გარკვეული შედეგები, შემუშავდა

რამდენიმე იდეა, თუ როგორ უნდა განხორციელდეს პროგრამული ალგორითმი და მისი ვიზუალური მხარე.

უცხოური ლიტერატურის გაცნობისა და შესწავლის შემდეგ, ჩვენს ნაშრომში ვითვალისწინებთ იმ საკვანძო პრინციპებს, რომლებიც იყო მათში აღწერილი და დადგენილი კიბერუსაფრთხოების და, კონკრეტულად, უსაფრთხო დიზაინის ექსპერტების მიერ. მიღებული იდეები და კონცეფციები განხილული იყო თემატურ ჯგუფებსა და ფორუმებში როგორც ინტერნეტის მეშვეობით, აგრეთვე პირადი შეხვედრების დროს. პასუხების/რჩევების მიღების საფუძველზე გავაუმჯობესეთ პროტოტიპები და კორექტირება შევიტანეთ საერთო დიზაინში. სადოქტორო ნაშრომზე მუშაობის პროცესში საჭირო გახდა რამდენიმე რთულად ამოსახსნელი ამოცანის გადაჭრა, რაშიც ჩვენი პროექტის ხელმძღვანელი დაგვეხმარა. ამ ეტაპის შემდეგ კიდევ ერთხელ ვგეგმავთ მიღებული შედეგების გაზიარებას, რის შემდეგაც, მიღებული რჩევების და შენიშვნების საფუძველზე, საბოლოო სახით ჩამოყალიბდება შემუშავებული პროდუქტის სტრუქტურა და დიზაინი. იგეგმება, აგრეთვე, ახალი კვლევის და დაკვირვების მეთოდების გამოყენება.

4.3 სისტემის განვითარება

ჩვენი კვლევისას მივიღეთ თანამედროვე და, რაც მთავარია, მომხმარებლის და დღევანდელი ბაზრის მოთხოვნებზე მორგებული სისტემა. როგორც აღინიშნა, შემუშავებული სისტემის ერთ-ერთი მთავარი მიზანია კიბერუსაფრთხოების 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, შინაარსზე დაფუძნებულ ფილტრაციის კონცეფციაზე, რაც საფუძვლად უდევს თანამედროვე სარეკომენდაციო სისტემებს.

ეს ხერხი ძალიან კარგად ასახავს თანამედროვე სისტემების მომხმარებლის უსაფრთხოების მექანიზმების უკეთესი გამოყენების მეთოდებს. შინაარსზე დაფუძნებული ფილტრაციის მექანიზმებს გააჩნია განვითარების პერსპექტივა, რადგან მანქანური სწავლების მეთოდები ეფუძნება სისტემასთან მუშაობისას მიღებული შედეგების დამუშავებას და ამ არსებულ გამოცდილებაზე უსაფრთხოების რეკომენდაციების ჩამოყალიბებას. რეკომენდაციების სიზუსტე და რელევანტურობა განპირობებულია მომხდარი და შეტანილი ინფორმაციის მიხედვით. რაც უფრო მეტია კიბერუსაფრთხოების სხვადასხვა დარგის შემთხვევა, რომელიც ასახულია სისტემაში, მით უფრო დიდია სისტემის მიერ გაცემული რეკომენდაციის სისუსტე, გამომდინარე იქიდან, რომ შინაარსზე დაფუძნებული ფილტრაცია სარეკომენდაციო სისტემის საფუძველია და უნდა იქნეს გათვალისწინებული მისი სპეციფიკა და მუშაობის პრინციპები.

ამგვარად, უკეთესი და უფრო წერტილოვანი რეკომენდაციების გასაცემად, სისტემაში უნდა იყოს შეტანილი რაც შეიძლება მეტი მონაცემი მომხმარებლის მიერ, ის ქმნის ერთგვარ პროფილს კონკრეტული შემთხვევისთვის. ამ პროფილის მიხედვით ხდება კონკრეტული რეკომენდაციის შექმნა. პროფილი შეიძლება შეიქმნას რამდენიმე მიმართულებით:

- მომხმარებლის მიერ შევსებული ინფორმაციის საფუძველზე, რაც იმას ნიშნავს, რომ პლატფორმაზე ივსება სპეციალური ფორის ზოგადი ველები, რათა სისტემაში მომხმარებლისთვის შეიქმნას შესაბამისი ჩანაწერი;
- უკვე არსებული ვარიანტების შერჩევა და საკუთარი დეტალების დამატება. ამ შემთხვევაში მომხმარებელი თავისი შეტანილი ტექსტის გარდა, ასევე ახდენს უკვე არსებული მიმართულების არჩევას;
- კითხვარის შევსება, სადაც ხდება მომხმარებლის სცენარის მიხედვით შესაბამის კითხვებზე პასუხის გაცემა. ამ შემთხვევაში, როგორც პირველში, მონაცემების შეყვანა ხდება უშუალოდ მომხმარებლის მიერ, მაგრამ ამ დროს ხდება კონკრეტულ კითხვებთან მუშაობა, რაც მომხმარებელს და ასევე სისტემას აძლევს უფრო სწორ, ვიწრო მიმართულებას.

თუ ვისაუბრებთ იმის შესახებ, რომ მოტანილი მაგალითებიდან რომელი მეთოდი იქნება უფრო გამოსადეგი, მივხვდებით, რომ უსაფრთხოება, გამომდინარე იქიდან, რომ ცოცხალი პროცესია, ხშირად თავად გვკარნახობს, რა სამოქმედო მოდელს უნდა მიმართოს მომხმარებელმა. კვლევის ფარგლებში შემუშავებულ სისტემაში გამოყენებულია ერთგვარი მიქსი (ნარევი) რამდენიმე მეთოდისა. ამგვარად, მომხმარებელს შეუძლია მონაცემების პირდაპირ შეყვანა. ასევე არსებობს რამდენიმე ველი, სადაც, უკვე არსებული ვარიანტებიდან, მომხმარებელი ირჩევს მონაცემებს, რომელიც ეყრდნობა წინა, უკვე შეტანილ გამოცდილებას. ამ კუთხით, წინა გამოცდილებაზე დაყრნობით, რეკომენდაციების გაცემა ხდება უფრო გააზრებულად და მონაცემები ამ შემთხვევაში მუშავდება მაქსიმალურად დეტალურად.

ნაშრომს გააჩნია პრაქტიკული მნიშვნელობა კიბერუსაფრთხოების და გამოყენებადობის გაუმჯობესების კუთხით. კვლევისას შემუშავდა სპეციალიზებული პლატფორმა, რომელზეც მომხმარებელს შეუძლია მოხმარების და მუშაობის სცენარის მიხედვით კონკრეტული მონაცემების შეტანა. ამისთვის პლატფორმას გააჩნია სპეციალიზებული ინტერაქტიული ფორმა. ამგვარად მომხმარებელი ახდენს მონაცემების შეტანას, რის შემდეგაც სისტემა აყალიბებს შესაბამისი რეკომენდაციების ვარიანტს და მომხმარებელს შეუძლია საჭირო ინფორმაციის მიღება მარტივი და გასაგები ფორმით. უსაფრთხოების მექანიზმების უმრავლესობას გააჩნია გამოყენებადობის პრობლემები, შესაბამისად, მომხმარებლისთვის საკმაოდ რთულია მათი პრაქტიკაში გამოყენება. ეს იმით არის განპირობებული, რომ ყველა მომხმარებელი თანაბრად არ ფლობს თანამედროვე საინფორმაციო ტექნოლოგიებს და არ არის გათვითცნობიერებული კიბერუსაფრთხოების საკითხებში.

ჩვენ მიერ შექმნილი პლატფორმის მეშვეობით საგრძნობლად იზრდება უსაფრთხოების მექანიზმების გამოყენებადობის დონე, რადგან მიღებული მონაცემების საფუძველზე სისტემა ახდენს შესაბამისი რეკომენდაციების წარდგენას მომხმარებლისთვის მაქსიმალურად მარტივი ფორმით. აღნიშნული პლატფორმისა და

ინტერაქტიული ფორმის გამოყენება პრაქტიკაში ბევრი დარგისთვის მისაღები იქნება, მიუხედავად მომხმარებლის სამუშაო მიმართულების ან გამოცდილებისა.

4.4 სარეკომენდაციო მიდგომები

ჩვენი კვლევის თეორიული და მეთოდოლოგიური საფუძვლები წარმოდგენილია როგორც თეორიული მიდგომების და მეთოდების სიღრმისეული განხილვით, ასევე პრაქტიკული შედეგების გაანალიზებით. სადოქტორო ნაშრომზე მუშაობისას გავეცანით ქართულ და უცხოურ სამეცნიერო ლიტერატურას, სტატიებს, წიგნებსა და სხვადასხვა თემატურ კონფერენციებზე წარმოდგენილი პრაქტიკული შედეგების ნიმუშებს. მოხმობილი წყაროები კვლევის თეორიული და მეთოდოლოგიური საფუძვლებია. ამასთან, კვლევის მეთოდოლოგიურ საფუძვლებზე გავლენა მოახდინა გლობალურ ქსელში სპეციალიზებულ ინტერნეტ რესურსებზე არსებულმა პრაქტიკამ. მათში განხილულია სხვადასხვა უსაფრთხოების სისტემების გამოყენებადობის მაგალითები და არსებული პრობლემები. ასევე შევისწავლეთ და განვიხილეთ კიბერუსაფრთხოებაში არსებული გამოყენებადობის პრობლემები. კერძოდ, თანამედროვე უსაფრთხოების სისტემების მორგება მომხმარებელზე, რამაც გამოიწვია მომხმარებლის მიერ ამ აუცილებელი უსაფრთხოების მექანიზმების პრაქტიკაში ხშირი გამოყენება.

კვლევისას შევისწავლეთ კიბერუსაფრთხოების დარგის წამყვანი პრაქტიკოსი სპეციალისტების მიერ გამოქვეყნებული სამეცნიერო ნაშრომები. მათში დასმულია პრობლემა თანამედროვე უსაფრთხოების სისტემების გამოყენების, კერძოდ კი, უსაფრთხოების სისტემების გამოყენებადობის შესახებ. თავისი სტრუქტურით დღევანდელი უსაფრთხოების მექანიზმები რთულია და მომხმარებლის უმრავლესობისთვის გაუგებარიც კი.

ჩვენი მიზანი იყო მაქსიმალურად გაგვემარტივებინა უსაფრთხოების მექანიზმების გამოყენება მომხმარებლისთვის. უსაფრთხოების მექანიზმების ხშირი გამოყენება კი გაზრდის ზოგად უსაფრთხოების დონეს. გათვალისწინებული უნდა იყოს კრიპტოგრაფიული მექანიზმების სირთულეები და გამოყენებადობის პრობლემები. ამის შემდეგ უნდა იყოს გაანალიზებული კრიპტოგრაფიული მექანიზმების მოხმარებისთვის

რთული ასპექტები. ყველაზე რთული ასპექტების გამოვლენის შემდეგ შესაძლებელი იქნება აქცენტების განაწილება და სამუშაოს მიმართულების აღება. გამოყენებადობის პრობლემების ჩამოყალიბება მოხდება შესაბამისი სამეცნიერო ლიტერატურის გაანალიზებით.

კვლევის ერთი ეტაპი დაეთმო 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 შემუშავდა შესაბამისი პროტოტიპი, რომელიც შემოწმდა როგორც რიგითი მომხმარებლის მიერ, ასევე იქნება გაგზავნილი კიბერუსაფრთხოების დარგის ექსპერტებთან ანალიზისთვის და პრაქტიკული შემოწმებისთვის. მიღებული შედეგები იქნება შესწავლილი, ხოლო კიბერუსაფრთხოების სპეციალისტების მითითებები იქნება გათვალისწინებული და დანერგილი სისტემის მექანიზმში [20,21].

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 თითოეულ მათგანს გააჩნია საკუთარი დატვირთვა. ჩვენთვის მნიშვნელოვანი იყო სწორი ალგორითმის გამოყენება და ამის შემდეგ მისი ახალი ვარიანტის შეთავაზება, რომელიც მორგებული იქნებოდა კიბერუსაფრთხოების რეალობას.

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

როგორც წესი, პრაქტიკაში დღეს სარეკომენდაციო ალგორითმები ჩაშენებულია ე. წ. სარეკომენდაციო მოდელებში, რომლებიც პასუხისმგებელია მომხმარებლისგან ინფორმაციის მიღებაზე, მის დამუშავებასა და შესაბამისი პასუხის გაცემაზე [22-24].

განვიხილოთ ოთხი ძირითადი ალგორითმი, რომლებიც გამოიყენება სარეკომენდაციო სისტემებში:

- კოლაბორატიული ფილტრაცია (Collaborative Filtering);
- შინაარსზე დაფუძნებული ფილტრაცია (Content-based Filtering);
- ჰიბრიდული მიდგომები (Hybrid Approaches);
- პოპულარულობა (Popularity);

გარდა ამ მიდგომებისა, საკმაოდ ხშირად შეიძლება შევხვდეთ სხვა არატრადიციულ მიდგომებს. პრაქტიკაში აპრობირებულია და გამოიყენება ზემოაღნიშნული მიდგომები:

1 - კოლაბორატიული ფილტრაცია

ასეთი ტიპის სარეკომენდაციო მეთოდი ეძებს დამთხვევებს მომხმარებლის ქცევაში, ამ ქცევებიდან ქმნის შესაბამის შაბლონებს და ამის შემდეგ აწვდის მომხმარებელს შესაბამის რეკომენდაციებს.

შეტანილი მონაცემები: აქტივობიდან გამომდინარე მიღებული მონაცემები, ისეთები, როგორებიცაა: გადმოწერები, შეფასება, მომხმარებლის მიერ შერჩეული პრიორიტეტები.

ფილტრაციის ტიპები:

- ახლომდებარე ინფორმაციაზე დაფუძნებული (მომხმარებელზე დაფუძნებული ან ერთეულზე დაფუძნებული);
- მოდელზე დაფუძნებული (მატრიცის ფაქტორიზაცია, შეზღუდული ბოტზმანის მანქანები და ა. შ.).

დადებითი მხარეები:

- საჭიროა დომენის მინიმალური ცოდნა;

- მომხმარებლის და ობიექტების პარამეტრები არ არის აუცილებელი;
- იძლევა კარგ შედეგს უმეტეს შემთხვევებში.

უარყოფითი მხარეები:

- სჭირდება გახურება (დაწყება არის შედარებით ხანგრძლივი);
- სჭირდება სტანდარტიზაციის პროდუქტები;
- სჭირდება მაღალი მომხმარებლის/ერთეულის პროპორცია (1:10);
- რთულია ასახსნელად.

2 - შინაარსზე დაფუძნებული ფილტრაცია

ამ ტიპის სარეკომენდაციო სისტემა ახდენს მსგავსი ტიპის კონტენტის წარდგენას უკვე არსებული გამოცდილების საფუძველზე. ეს შეიძლება იყოს მოწონებული ობიექტები, შეფასებული გარემო ან სხვა მომხმარებლის მხრიდან განსაზღვრული პრეფერენცია.

შეტანილი მონაცემები:

დამოკიდებულია მხოლოდ შინაარსის/აღწერის სიზუსტეზე, რაც საფუძველს აძლევს, გაიცეს შესაბამისი რეკომენდაცია.

ტიპები:

- ინფორმაციის დაბრუნება (TF-IDF, OKAPI BM25);
- კლასიკური მანქანური სწავლება.

დადებითი მხარეები:

- არ გააჩნია ცივი სტარტის პრობლემა;
- არ არის საჭირო გამოყენებული მონაცემები;
- შეუძლია რეკომენდაციის შექმნა იშვიათი თვისებებისგანაც;
- შეუძლია შეტანილი მონაცემების გამოყენება რეკომენდაციისთვის.

უარყოფითი მხარეები:

- ერთეული უნდა იყოს წარმოდგენილი მანქანისთვის საჭირო ფორმატით;

- რთულია რამდენიმე თვისების კომბინირება ერთში.

3 - ჰიბრიდული მიდგომა

ახდენს შინაარსის ფილტრაციის და კოლაბორატიული ფილტრაციის შერევას და ქმნის ორივე მეთოდის შერეულ ვარიანტს, რაც საშუალებას იძლევა ორივე მეთოდის დადებითი მხარეები და თვისებები დაინერგოს ერთი მექანიზმის ფარგლებში.

შეყვანა:

გამოიყენება მომხმარებლის მიერ შეტანილი მონაცემები. ამასთან ერთად იყენებს ორივე მეთოდის უპირატესობას უკეთესი ანალიზისთვის.

ტიპები:

- წონის გამოყენებით;
- ჩანაცვლება;
- შერევა;
- თვისებების კომბინაცია;
- კასკადური;
- თვისებების არგუმენტირება;
- მეტა დონეზე მუშაობა.

დადებითი მხარეები:

- არ აქვს ცივი სტარტის პრობლემა;
- შესაძლებელია დაინერგოს დამოუკიდებლად.

უარყოფითი მხარეები:

- ზოგ შემთხვევაში შეიძლება დასჭირდეს ბევრი დრო პროგრამული რეალიზაციისთვის.

4 - პოპულარულობა

ამ მიდგომაში გამოიყენება ყველაზე პოპულარული ერთეულების მეთოდი (მაგ., ყველაზე ხშირად გადმოწერილი პროდუქტი, ხშირად ნანახი გვერდები და ა. შ.).

შეყვანა:

იყენებს გამოყენებულ მონაცემებს და ერთეულების შიგთავსს. მაგალითად, კონკრეტულ კატეგორიებს ან მიმართულებას.

დადებითი მხარეები:

- შედარებით მარტივია რეალიზაციისთვის;
- მყარი ალგორითმია;
- ეხმარება მომხმარებელს ცივი სტარტის დროს;

უარყოფითი მხარეები:

- სჭირდება სტანდარტული პროდუქტები;
- სჭირდება გარკვეული ტიპის კატეგორიზაცია;
- არ შეუძლია ახლის შეთავაზება;
- სარეკომენდაციო სიო არ უნდა შეიცვალოს;

4.5 განვითარების პერსპექტივები

სადოქტორო ნაშრომზე მუშაობისას გამოიკვეთა დღეისთვის არსებული მანქანური სწავლების რამდენიმე მიდგომა და ალგორითმი. აღსანიშნავია, რომ თითოეული ალგორითმი წარმოადგენს კონკრეტულ მიმართულებას და გააჩნია საკუთარი სამუშაო დარგი. ჩვენს შემთხვევაში შერჩეული იყო შინაარსზე დაფუძნებული მიდგომა, რადგან კვლევისას გამოიკვეთა რამდენიმე პრინციპი, რაც აუცილებლად უნდა შედიოდეს კიბერუსაფრთხოების 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 შეტანილ მონაცემს, რითიც სამომავლოდ არის განპირობებული რეკომენდაციის სიზუსტე და რელევანტურობა.

გამომდინარე იქიდან, რომ კიბერუსაფრთხოების ბაზრის მოთხოვნები მუდმივად იცვლება და სისტემები ვითარდება, სარეკომენდაციო სისტემა უნდა იყოს მაქსიმალურად მოქნილი და მზად ნებისმიერი ცვლილებისთვის, იქნება ეს სტრუქტურული თუ ლოგიკური.

ამიტომაც სამომავლოდ ვაპირებთ, რომ კვლევა ამ მიმართულებით გავაგრძელოთ და შინაარსზე დაფუძნებულ მექანიზმებს არსებულ სისტემაში დავუმატოთ კიდევ კოლაბორატიული მიდგომაც. შექმნილი მიქსი უფრო კარგად იქნება მორგებული მომხმარებლის მოთხოვნებზე და შეძლებს მონაცემების უფრო დეტალურად დამუშავებას.

კოლაბორაციული ფილტრაციის (CF) ალგორითმები ეძებენ მომხმარებლის აქტივობის ნიმუშებს მომხმარებლისთვის სპეციფიკური რეკომენდაციების შესაქმნელად. ეს დამოკიდებულია სისტემაში მომხმარებლის გამოყენების მონაცემების არსებობაზე. მაგალითად, მომხმარებლის მიერ წაკითხულ წიგნებზე მომხმარებლის შეფასებები მიუთითებს, თუ რამდენად მოსწონთ ისინი. მთავარი იდეა ის არის, რომ მომხმარებლის რეიტინგი ახალი ნივთისთვის, სავარაუდოდ, მსგავსი იქნება სხვა მომხმარებლის შეფასებისა, თუ სხვა ელემენტები ორივე მომხმარებელმა ანალოგიურად შეაფასა.

აღსანიშნავია, რომ ეს არ არის დამოკიდებული რაიმე დამატებითი ინფორმაციის მიღებაზე ნივთების შესახებ (მაგ., აღწერა, მეტამონაცემები და ა. შ.), ან მომხმარებლის შესახებ (მაგ., ინტერესები, დემოგრაფიული მონაცემები და ა. შ.), რეკომენდაციების შემუშავების მიზნით. თანამშრომლობის ფილტრაციის მიდგომები შეიძლება დაიყოს ორ კატეგორიად: სამეზობლო და მოდელებზე დაფუძნებული მეთოდები.

სამეზობლო მეთოდებში (მეხსიერებაზე დაფუძნებული CF), მომხმარებლის ნივთების რეიტინგი გამოიყენება ახალი ნივთების შეფასების პროგნოზირებისთვის. ამის საპირისპიროდ, მოდელზე დაფუძნებული მიდგომები იყენებს რეიტინგებს, რათა შეისწავლონ ისეთი მოდელი, რომლის საფუძველზეც ხდება ახალი საგნების პროგნოზირება. ზოგადი იდეა მიუთითებს მომხმარებლის ნივთების ურთიერთქმედების

მოდელირებაზე მანქანური სწავლების ალგორითმების გამოყენებით, რომლებიც მონაცემთა ნიმუშებს პოულობენ.

მომხმარებელზე დაფუძნებული ერთობლივი ფილტრაციისას, პირველი, რისი გაკეთებაც გვინდა, არის წიგნებისადმი მათი უპირატესობის გამოანგარიშება, თუ რამდენად ჰგვანან მომხმარებლები ერთმანეთს. ბუნებრივია, რომ თითოეული მომხმარებელი წარმოადგენს ვექტორს (ან მასივს), რომელიც შეიცავს მომხმარებლის პარამეტრების ნივთებს. საკმაოდ მარტივია მომხმარებლის შედარება ერთმანეთთან სხვადასხვა მსგავსების საზომების გამოყენებით.

ამ მაგალითში ჩვენ გამოვიყენებთ კოსინუსის მსგავსებას. თუ პირველ მომხმარებელს შევადარებთ ხუთ სხვა მომხმარებელს, დავინახავთ, რამდენად ჰგავს ის დანარჩენებს, ისევე, როგორც უმეტესობა მსგავსების მეტრებისა: რაც უფრო მაღალია მსგავსება ვექტორებს შორის, მით უფრო ჰგვანან ისინი ერთმანეთს. ამ შემთხვევაში, პირველი მომხმარებელი საკმაოდ ჰგავს ორ მომხმარებელს, რადგან მათ აქვთ ორი საერთო წიგნი, ნაკლებად ჰგავს ორ სხვა მომხმარებელს, რომლებიც აზიარებენ მხოლოდ ერთ წიგნს და საერთოდ არ ჰგავს ბოლო მომხმარებელს, რომელსაც არ აქვს მათთან გაზიარებული საერთო წიგნები.

ჰიბრიდული მიდგომები აერთიანებს მომხმარებლისა და ნივთის შინაარსის მახასიათებლებს და გამოყენების მონაცემებს, რათა ისარგებლოს ორივე ტიპის მონაცემებით. ჰიბრიდული რეკომენდატორი, რომელიც აერთიანებს A და B ალგორითმებს, ცდილობს გამოიყენოს A-ს უპირატესობები B-ს უარყოფითი მხარეების გამოსასწორებლად.

მაგალითად, CF ალგორითმს აქვს ახალი ელემენტის პრობლემები, ანუ მათ არ შეუძლიათ რეკომენდაცია გაუწიონ იმ ნივთებს, რომლებსაც არ აქვთ შეფასებები/გამოყენება. ეს არ ზღუდავს შინაარსზე დაფუძნებულ ალგორითმებს, ვინაიდან ახალი საგნების პროგნოზი ემყარება მათ შინაარსს (მახასიათებლებს), რომლებიც, როგორც წესი, ხელმისაწვდომია, როდესაც ახალი ელემენტი შედის სისტემაში.

ჰიბრიდული რეკომენდატორის შექმნით, რომელიც აერთიანებს კოლაბორაციულ ფილტრაციასა და შინაარსზე დაფუძნებულ ფილტრაციას, ჩვენ შეგვიძლია გადავლახოთ ინდივიდუალური ალგორითმების ზოგიერთი შეზღუდვა, როგორიცაა ცივი დაწყება და პოპულარობა.

აღსანიშნავია ისიც, რომ პოპულარობაზე დაფუძნებული მიდგომები კარგი გამოსავალია ახალი მომხმარებლის „ცივი დაწყებისთვის“. ეს მიდგომები აფასებს ერთეულებს პოპულარობის გარკვეული ფორმის გამოყენებით, როგორებიცაა ყველაზე ხშირად ჩამოტვირთული ან შეძენილი პოპულარული ნივთები და ურჩევს მათ ახალ მომხმარებლებს. ეს არის ძირითადი, მაგრამ მყარი მიდგომა, როდესაც პოპულარობის კარგი საზომი გაქვთ და ხშირად გთავაზობთ კარგ საფუძველს, რომლითაც შეგიძლიათ შეადაროთ სხვა რეკომენდატორის ალგორითმები.

პოპულარობა შეიძლება გამოყენებულ იქნეს, როგორც ალგორითმი რეკომენდატორთა სისტემის დასაყენებლად, რომ მომხმარებელს ჰქონდეს საკმარისი აქტივობა და გამოყენება მიდგომებზე გადასვლამდე, რაც უკეთესად შეძლებს მომხმარებლის ისეთი ინტერესების მოდელირებას, როგორებიცაა კოლაბორაციული ფილტრაცია და შინაარსის ფილტრაცია. პოპულარობის მოდელები ასევე შეიძლება შევიდეს ჰიბრიდულ მიდგომებში, რაც მათ საშუალებას მისცემს გაუმკლავდნენ ახალი მომხმარებლის „ცივი დაწყების“ პრობლემას.

რეკომენდატორების სისტემების უფრო ტრადიციული მიდგომების გარდა, რაც ჩვენ აქამდე განვიხილეთ (მაგ., პოპულარობა, კოლაბორაციული ფილტრაცია, შინაარსზე დაფუძნებული ფილტრაცია, ჰიბრიდული მიდგომები), არსებობს მრავალი სხვა მეთოდიც, რომელთა გამოყენება ასევე შეიძლება სარეკომენდაციო სისტემების შესანარჩუნებლად, მათ შორის:

- ღრმა სწავლება;
- სოციალური რეკომენდაციები;
- რანგის სწავლა;
- კარგად შეიარაღებული ბოროტმოქმედები (შესწავლა/ექსპლუატირება);

- ტენზორის ფაქტორიზაციისა და ფაქტორიზაციის აპარატები (კონტექსტის გათვალისწინებული რეკომენდაციები).

ეს მოწინავე და არატრადიციული მეთოდები კარგია თქვენი რეკომენდატორების ხარისხის შემდეგ საფეხურზე გადასასვლელად, მაგრამ ნაკლებად გასაგებია და არც ისე კარგად არის მხარდაჭერილი სარეკომენდაციო ინსტრუმენტებში. პრაქტიკაში გამოყენების შემდეგ ნათლად გამოჩნდება, ღირს თუ არა მოწინავე მეთოდების დანერგვა, რომელიც უნდა იყოს გაცილებით უკეთესი ძირითად მიდგომებთან შედარებით.

განვიხილეთ რეკომენდატორთა მოდულის მრავალი ალგორითმი, მათ შორის მომხმარებელზე დაფუძნებული კოლაბორაციული ფილტრი, ნივთებზე დაფუძნებული კოლაბორაციული ფილტრაცია, შინაარსზე დაფუძნებული ფილტრაცია და ჰიბრიდული მეთოდები. ეს ეფექტი ასევე მოქმედებს დიდ, რეალურ სამყაროში მოცემულ მონაცემებზე. ამიტომ იმის გადაწყვეტა, თუ რომელი ალგორითმი გამოვიყენოთ, განხილული უნდა იქნეს მათი დადებითი და უარყოფითი მხარეები და რამდენად კარგად ასრულებენ ისინი მათი შეფასებისას [25-27].

დასკვნა

წარმოდგენილ სადოქტორო ნაშრომში განხილულია კვლევის შედეგად მიღებული ინტერაქტიული სისტემა, რომელსაც საფუძვლად დაედო მანქანური სწავლების ერთ-ერთი რელევანტური პრინციპი – შინაარსზე დაფუძნებული ფილტრაციის სარეკომენდაციო ალგორითმი (content-based filtering). ამ ალგორითმის დახმარებით ხორციელდება სარეკომენდაციო პროცედურები ისეთ დარგებში, როგორებიცაა, მაგალითად, სოციალური ქსელები, სხვადასხვა ფილმების ან ტურიზმის პლატფორმები, საგანმანათლებლო სისტემები და სხვ. ასეთი ტიპის ალგორითმი ეყრდნობა რამდენიმე ფაქტორს და საშუალებას გვაძლევს, მომხმარებელს შევთავაზოთ უკეთესი შინაარსი. გამომდინარე იქიდან, რომ კრიპტოგრაფიული უსაფრთხოების მექანიზმების უმრავლესობა მომხმარებლისთვის რთულად არის გასაგები, მათი გამოყენებადობის დონე საკმაოდ დაბალია, რაც იწვევს სხვადასხვა ვებპლატფორმებზე ამ მექანიზმების შედარებით იშვიათ სწორი კონფიგურაციით გამოყენებას.

კვლევისას შემუშავდა სარეკომენდაციო ალგორითმის ახალი მიდგომა კიბერუსაფრთხოების რეკომენდაციების მიმართულებით. აქამდე ასეთი ტიპის ალგორითმები ხშირად გამოიყენებოდა სხვა დარგებში რეკომენდაციების გასაწევად. ჩვენ შევქმენით სარეკომენდაციო სისტემის ისეთი მიმართულება, რომელიც დაგვეხმარება მომხმარებლისთვის კომფორტული და გასაგები ფორმით შესაბამისი უსაფრთხოების რეკომენდაციების გაცემაში.

ამასთან ერთად, კვლევისას გათვალისწინებული იყო და საბოლოო პროდუქტში შეტანილი უსაფრთხო დიზაინის და გამოყენებადობის ძირითადი კონცეფციები: სწავლებადობა (Learnability), რაც მომხმარებელს ეხმარება სისტემის უკეთ ათვისებაში და დამახსოვრებადობა (Memorability), რომელიც მომავალში მომხმარებელს მსგავსი ტიპის სისტემებთან მუშაობას გაუადვილებს. ამასთან ერთად, სისტემაში მომხმარებელს შეუძლია გამოხმაურების (Feedback) დატოვება, რაც დადებითად იმოქმედებს სისტემის განვითარებისთვის გამოყენებადობის კუთხით. გამოყენებადობის ეს მიდგომები დაინერგა, რათა სისტემა გამხდარიყო მომხმარებლისთვის ბევრად უფრო

მოსახერხებელი და გასაგები. აქვე აღვნიშნავთ, რომ ნაშრომზე მუშაობისას აღმოვაჩინეთ, რომ მანქანური სწავლების ალგორითმები დღეისთვის რამდენიმე მიმართულებით მომუშავე სქემებია და შესაძლებელია რამდენიმე ალგორითმის პრინციპის გაერთიანება. ესენია: ღრმა სწავლება, სოციალური რეკომენდაციები, რანგის სწავლა, კარგად შეიარაღებული ბოროტმოქმედი პირები (შესწავლა/ექსპლუატირება), ტენზორის ფაქტორიზაციისა და ფაქტორიზაციის აპარატები (კონტექსტის გათვალისწინებული რეკომენდაციები), რაც სამომავლოდ უფრო დახვეწილ და რელევანტურ შედეგს მოიტანს.

გამოყენებული ლიტერატურა:

1. Gagnidze A.G., Iavich M.P., Iashvili G.U. (2016) Post-Quantum Cryptosystems. *Modern scientific researches and innovations*, 5.
2. Iavich M.P., Isaev P.D. (2014) Problems Associated With The Creation Of The Own Cryptosystems // *Modern scientific researches and innovations*, 4.

3. J.-F. Gallais, I. Kizhvatov, and M. Tunstall, „Improved tracedriven cache-collision attacks against embedded AES implementations“, in WISA 2010.
4. B. Brumley and R. Hakala, „Cache-timing template attacks“, in *ASIACRYPT 2009, ser. LNCS, S. Halevi, Ed.,* vol. 5677. Springer, 2009.
5. O. Aciic, mez, W. Schindler, and C¸. Koc, „Cache based remotetiming attack on the AES“, in *CT-RSA 2007, ser. LNCS,M. Abe, Ed.*, vol. 4377. Springer, 2007.
6. M. Neve, J.-P. Seifert, and Z. Wang, „A refined look atBernstein's AES side-channel analysis“, in *ASIACCS 2006, F.-C. Lin*, D.-T. Lee, B.-S. Lin, S. Shieh, and S. Jajodia, Eds.ACM, 2006.
7. Y. Tsunoo, T. Saito, T. Suzaki, M. Shigeri, and H. Miyauchi, „Cryptanalysis of DES implemented on computers with cache“, in *CHES 2003, ser. LNCS, C. D.* Walter, C. Koc¸,and C. Paar, Eds., vol. 2779. Springer, 2003.
8. M. N. Wegman and J. L. Carter, New hash functions and their use in authentication and set equality*, Journal of Computer and System Sciences 22*, pp. 265-279 (1981).
9. Bernstein D.J. (2009) Introduction to post-quantum cryptography. In: *Bernstein D.J., Buchmann J., Dahmen E. (eds) Post-Quantum Cryptography*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-88702-7_1
10. Pazzani M.J., Billsus D. „Content-Based Recommendation Systems“. In: *Brusilovsky P., Kobsa A., Nejdl W. (eds) The Adaptive Web. Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg. 2007, 4321:325-341.
11. Lops, P., Jannach, D., Musto, C. et al. „Trends in content-based recommendation“. *User Model User-Adap Inter*, 2019 29:239-249.
12. P. Kumar Roy, S. Singh Chowdhary, R. Bhatia. „A Machine Learning approach for automation of Resume Recommendation system“. *Procedia Computer Science*, 2020 167:2318-2327.
13. S. K. Gorakala. Building Recommendation Engines. *Packt Publishing*. 2016.11.
14. S.M. Mohidul Islam, Rameswar Debnath, „A Comparative Evaluation of Feature Extraction and Similarity Measurement Methods for Content-based Image Retrieval“ *International*

Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.12, No.6, pp. 19-32, 2020. DOI: 10.5815/ijigsp.2020.06.03.

15. Md. Farhan Sadique, S M Rafizul Haque, „Content-Based Image Retrieval Using Color Layout Descriptor, Gray-Level Co-Occurrence Matrix and K-Nearest Neighbors“, *International Journal of Information Technology and Computer Science (IJITCS),* Vol.12, No.3, pp.1 9-25, 2020. DOI: 10.5815/ijitcs.2020.03.03.
16. Hanan A. Al-Jubouri, „Integration Colour and Texture Features for Content-based Image Retrieval“, *International Journal of Modern Education and Computer Science (IJMECS),* Vol. 12, No. 2, pp. 10-18, 2020. DOI: 10.5815/ijmecs.2020.02.02.
17. Shubham Bauskar, Vijay Badole, Prajal Jain, Meenu Chawla, „Natural Language Processing based Hybrid Model for Detecting Fake News Using Content-Based Features and Social Features“, *International Journal of Information Engineering and Electronic Business (IJIEEB),* Vol. 11, No. 4, pp. 1-10, 2019. DOI: 10.5815/ijieeb.2019.04.01.
18. Achakulvisut T, Acuna DE, Ruangrong T, Kording K. „Science Concierge: A Fast Content-Based Recommendation System for Scientific Publications“. *PLoS One.* 2016 11(7): e0158423.
19. Gnatyuk S., Barchenko N., Azarenko O., Tolbatov A., Obodiak V., Tolbatov V. „Ergonomic support for decision-making management of the chief information security officer“, *CEUR Workshop Proceedings*, Vol. 2588, pp. 459-471, 2019.
20. Smriti Ayushi, V R Badri Prasad, „Cross-Domain Recommendation Model based on Hybrid Approach“, *International Journal of Modern Education and Computer Science(IJMECS),* Vol. 10, No. 11, pp. 36-42, 2018. DOI: 10.5815/ijmecs.2018.11.05.
21. Gulara A. Mammadova, Firudin T. Aghayev, Lala A. Zeynalova, „Use of Social Networks for Personalization of Electronic Education“*, International Journal of Education and Management Engineering (IJEME),* Vol. 9, No. 2, pp. 25-33, 2019. DOI: 10.5815/ijeme.2019.02.03.

22. Frank Kane. „Building Recommender Systems with Machine Learning and AI: Help People Discover New Products and Content with Deep Learning, Neural Networks, and Mach“, 2018.
23. A. Jain , A. Fandango , et al. „TensorFlow Machine Learning Projects: Build 13 real-world projects with advanced numerical computations using the Python ecosystem“, 2018.
24. M. Gori. „Machine Learning: A Constraint-Based Approach“, 2017.
25. F. Gedikli. „Recommender Systems and the Social Web“, 2013.
26. C. Preisach, H. Burkhardt, B., Decker, R, „Data Analysis, Machine Learning and Applications“, *Proceedings of the 31st Annual Conference of the Gesellschaft für Klassifikation e.V.,* Albert-Ludwigs-Universität Freiburg, March 7-9, 2007.
27. G. Iashvili, Scientific and Practical Cyber Security Journal (SPCSJ) 5(2), ISSN 2587-4667, 2021, 1-11 pp.