Scientific and Practical Cyber Security Journal (SPCSJ) 7(4): 60 – 76 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

გამოწვევების დაძლევა და ეფექტური კიბერუსაფრთხოების განათლების განხორციელება საშუალო სკოლებში

ზურაბ ჯიშკარიანი
Scientific Cyber Security Association

აბსტრაქტი: დღევანდელ ციფრულ ეპოქაში კიბერუსაფრთხოება სულ უფრო მნიშვნელოვანი ხდება როგორც ადამიანებისთვის, ასევე კერძო სექტორისთვის და ზოგადად ქვეყნისთვის. კიბერ საფრთხეების ზრდასთან ერთად, როგორებიცაა ჰაკინგი, პირადი ინფორმაციის ქურდობა და მონაცემთა გაჟონვა, აუცილებელია ადამიანებმა იცოდნენ, როგორ დაიცვან საკუთარი თავი და ინფორმაცია ონლაინში. თუმცა, კიბერუსაფრთხოების განათლება ჯერ კიდევ არ არის ფართოდ ინტეგრირებული საშუალო სკოლების სასწავლო გეგმასთან, რის გამოც მოსწავლეები დაუცველნი არიან კიბერ საფრთხეების წინაშე. ეს კვლევითი ნაშრომი მიზნად ისახავს საშუალო სკოლებში კიბერუსაფრთხოების განათლების ამჟამინდელი მდგომარეობის შესწავლასა და ახალგაზრდა სტუდენტებისთვის კიბერუსაფრთხოების სწავლების საუკეთესო პრაქტიკისა და სტრატეგიების იდენტიფიცირებას. ნაშრომი ასევე შეისწავლის საშუალო სკოლებში კიბერუსაფრთხოების განათლების დანერგვის ბარიერებსა და გამოწვევებს და ამ კონტექსტში კიბერუსაფრთხოების განათლების გაუმჯობესების რეკომენდაციებს.

საკვანძო სიტყვები: კიბერუსაფრთხოების განათლება, საშუალო სკოლა, საშუალო სკოლის სასწავლო გეგმა, საგანმანათლებლო მოდელები, ბარიერები და გამოწვევები

ABSTRACT: In the contemporary era characterized by pervasive digitization, the significance of cybersecurity has escalated markedly for individuals, the private sector, and the broader national landscape. Given the proliferation of cyber threats, encompassing hacking, identity theft, and data breaches, it is imperative that individuals possess the requisite knowledge to safeguard themselves and their online information. Nevertheless, the incorporation of cybersecurity education within the secondary school curriculum remains notably limited, rendering students susceptible to cyber threats. This research paper endeavors to scrutinize the existing landscape of cybersecurity education within secondary schools, aiming to identify optimal practices and strategies for imparting cybersecurity knowledge to young students. Additionally, the paper investigates the impediments and challenges associated with integrating cybersecurity education into secondary schools, proposing recommendations to enhance the effectiveness of cybersecurity education within this educational context.

KEYWORDS*:* Cybersecurity Education, Secondary School, Secondary School Curriculum, Educational Models, Obstacles and Difficulties

1. შესავალი

კიბერუსაფრთხოების განათლების მზარდი მნიშვნელობის მიუხედავად, საშუალო სკოლებში მისი ეფექტური დანერგვა მნიშვნელოვან გამოწვევად რჩება. ამ პრობლემას რამდენიმე ფაქტორი უწყობს ხელს, მათ შორის შეზღუდული რესურსები, მასწავლებელთა მომზადების ნაკლებობა და ასაკისთვის შესაბამისი და საინტერესო მასალების დეფიციტი. პირველ რიგში, ბევრ სკოლას აქვს შეზღუდული რესურსი კიბერუსაფრთხოების განათლების დაფინანსებისთვის. მათ შეიძლება არ ჰქონდეთ დაფინანსება საჭირო

აღჭურვილობის შესაძენად ან კვალიფიცირებული პერსონალის დაქირავებლად. გარდა ამისა, ზოგიერთი სკოლისთვის შეიძლება პრიორიტეტული იყოს სხვა საგნები, როგორებიცაა:მათემატიკა, მეცნიერება და უცხო ენების შესწავლა, ვიდრე კიბერუსაფრთხოების განათლება. მეორეც, მასწავლებელთა უმრავლესობას შეიძლება არ ჰქონდეს გავლილი საკმარისი ტრენინგი კიბერუსაფრთხოების ეფექტურად სწავლებისთვის.შესაბამისად არ ჰქონდეთ საგნის სწავლებისთვის საჭირო ცოდნა ან უნარები, რამაც შეიძლება გამოიწვიოს კიბერუსაფრთხოების სწავლებისადმი ნდობის ნაკლებობა. უფრო მეტიც, კიბერუსაფრთხოების განათლება მუდმივად განვითარებადი სფეროა და შეიძლება რთული იყოს უახლესი ტენდენციებისა და ტექნოლოგიების შენარჩუნება. მესამე, საშუალო სკოლებში კიბერუსაფრთხოების სწავლებისთვის ასაკის შესაბამისი და საინტერესო მასალების დეფიციტია. ბევრი არსებული მასალა ძალიან რთულია საშუალო სკოლის მოსწავლეებისთვის, რაც ართულებს მათ ეფექტურად ჩართვას. გარდა ამისა, მასალები შეიძლება არ იყოს შემუშავებული ინტერაქტიულ და ექსპერიმენტულ სწავლებაზე ფოკუსირებით, რაც აუცილებელია მცირეწლოვანი მოსწავლეებისთვის.

Introduction

The effective implementation of cybersecurity education in secondary schools poses a substantial challenge despite its increasing significance. Numerous factors contribute to this challenge, encompassing limited resources, inadequate teacher training, and a dearth of age-appropriate and engaging instructional materials.

Primarily, the constraint of limited resources within schools impedes the integration of comprehensive cybersecurity education. Insufficient funding may hinder the acquisition of requisite equipment and the recruitment of qualified staff dedicated to cybersecurity education. Furthermore, competing priorities, such as emphasis on subjects like mathematics, science, and foreign languages, may divert attention and resources away from cybersecurity education initiatives.

Secondarily, a significant proportion of educators may lack the requisite training for effectively teaching cybersecurity. The deficiency in training may result in a deficiency of knowledge and skills necessary to impart the subject matter, leading to a lack of confidence among educators. Additionally, the dynamic nature of cybersecurity, characterized by continual evolution and technological advancements, compounds the challenge of educators staying abreast of the latest trends and technologies.

Tertiary to these challenges is the insufficiency of age-appropriate and engaging instructional materials tailored for teaching cybersecurity in secondary schools. Existing materials often prove overly complex for elementary school students, impeding effective engagement. Furthermore, these materials may lack a focus on interactive and experiential learning methods, which are pivotal for the engagement and understanding of young learners.

2. კვლევის მიზანი

ეს კვლევა არ არის იმის შესახებ, თუ როგორ ისწავლება კიბერუსაფრთხოება საშუალო სკოლებში. ამ კვლევის მიზანია საშუალო სკოლის მოსწავლეებში კიბერუსაფრთხოების სწავლასთან დაკავშირებით არსებული მდგომარეობისა და გამოწვევების იდენტიფიცირება. კერძოდ, ეს კვლევა მიზნად ისახავს:

- გამოვიკვლიოთ კიბერუსაფრთხოების განათლების ამჟამინდელი მდგომარეობა საშუალო სკოლებში.
- შევისწავლოთ კიბერუსაფრთხოების განათლების თეორიები და მოდელები.
- საშუალო სკოლის მოსწავლეებისთვის კიბერუსაფრთხოების სწავლების საუკეთესო პრაქტიკისა და სტრატეგიების იდენტიფიცირება.

- გამოვიკვლიოთ ბარიერები და გამოწვევები საშუალო სკოლებში კიბერუსაფრთხოების განათლების განხორციელებისას.

ამ კვლევის შედეგები სასარგებლო იქნება პედაგოგებისთვის, სასწავლო გეგმის შემქმნელებისთვის და სხვა დაინტერესებული მხარეებისთვის, რომლებიც დაინტერესებულნი არიან საშუალო სკოლებში კიბერუსაფრთხოების განათლების გაუმჯობესებით. მიმდინარე გამოწვევებისა და საუკეთესო პრაქტიკის იდენტიფიცირებით, ამ კვლევას შეუძლია საშუალო სკოლის მოსწავლეებისთვის ეფექტური კიბერუსაფრთხოების საგანმანათლებლო პროგრამების შემუშავება.

Purpose of the Research

This investigation does not center on the pedagogical approaches employed in teaching cybersecurity within secondary schools. Rather, the primary objective of this study is to discern the prevailing circumstances and confrontations associated with the acquisition of cybersecurity knowledge among secondary school students. Specifically, the study aims to:
• Scrutinize the present state of cyber security education within secondary school settings.
• Investigate theoretical frameworks and models pertinent to cyber security education.
• Ascertain optimal practices and methodologies for imparting cybersecurity knowledge to secondary school students.
• Investigate impediments and challenges encountered in the implementation of cybersecurity education within secondary schools.
The outcomes of this research will prove beneficial to educators, curriculum developers, and other stakeholders invested in advancing cybersecurity education in secondary schools. Through the identification of extant challenges and effective practices, this study has the potential to guide the formulation of impactful cybersecurity education programs tailored for secondary school students.

3. კიბერუსაფრთხოების განათლების ამჟამინდელი მდგომარეობა საშუალო სკოლებში

ბოლო კვლევებმა აჩვენა, რომ კიბერუსაფრთხოების განათლებას არ ექცევა საკმარისი ყურადღება საშუალო სკოლებში, მიუხედავად კიბერუსაფრთხოების მზარდი მნიშვნელობისა. Cyber.org-ის 2020 წლის ანგარიშის მიხედვით,K-12 პედაგოგებს შორის ჩატარებულმა გლობალურმა გამოკითხვამ აჩვენა მასწავლებლების მხოლოდ 20% გრძნობს თავს თავდაჯერებულად კიბერუსაფრთხოების თემების სწავლებაში (Cyber.org, "The State of Cybersecurity Education in K- 12 სკოლა“).
შეერთებულ შტატებში, განათლების სტატისტიკის ეროვნული ცენტრის 2022 წლის გამოკითხვამ დაადგინა, რომ საშუალო სკოლების 10%-ზე ნაკლები სთავაზობს კიბერუსაფრთხოების სპეციალურ კურსებს (წყარო: NCES, "საშუალო სკოლის კურსების ხელმისაწვდომობა და შეთავაზებები").
მკვეთრად საპირისპირო ხდება ესტონეთში,სადაც,სავალდებულოა კიბერუსაფრთხოების სასწავლო პროგრამა ყველა მოსწავლისთვის საბავშვო ბაღიდან საშუალო სკოლამდე (OECD, "Estonia: Country Review of Education Policy"). სინგაპური იღებს ეტაპობრივ მიდგომას, აერთიანებს კიბერჰიგიენის ძირითად კონცეფციებს არსებულ საგნებში, როგორიცაა IT და სოციალური კვლევები, ხოლო ასევე გთავაზობთ კიბერუსაფრთხოების მოწინავე კურსებს ზედა საშუალო საფეხურზე (სინგაპურის განათლების სამინისტრო, "კიბერუსაფრთხოების განათლების ჩარჩო").

მთლიანობაში, ეს კვლევები მიუთითებს იმაზე, რომ საჭიროა მეტი ყურადღება მიექცეს საშუალო სკოლებში კიბერუსაფრთხოების განათლებას და მოხდეს უფრო თანმიმდევრული და ყოვლისმომცველი სტანდარტების შემუშავება და დანერგვა.

The Contemporary Landscape of Cybersecurity Education in Secondary Schools

Recent research has highlighted the inadequate emphasis placed on cybersecurity education within secondary school curricula, despite the increasing significance of cybersecurity. A global survey conducted among K-12 educators revealed that, according to a 2020 report by Cyber.org, only 20% of educators worldwide feel confident in teaching cybersecurity topics (Cyber.org, "The State of Cybersecurity Education in K-12 Schools").
In the United States, a 2022 survey by the National Center for Education Statistics found that fewer than 10% of high schools offer dedicated cybersecurity courses (NCES, "High School Course Availability and Offerings").
In stark contrast, Estonia, a global leader in cybersecurity education, mandates a cybersecurity curriculum for all students from kindergarten through high school (OECD, "Estonia: Country Review of Education Policy").
Singapore adopts a tiered approach, integrating basic cyber hygiene concepts into existing subjects such as IT and social studies, while also offering advanced cybersecurity courses at the upper secondary level (Singapore Ministry of Education, "Cybersecurity Education Framework").
Overall, these data indicate that more attention should be paid to secondary education in circulation and the development and implementation of comprehensive standards.

4. თეორიები და საუკეთესო პრაქტიკები საშუალო სკოლის მოსწავლეებისთვის კიბერუსაფრთხოების სწავლებისთვის

კიბერუსაფრთხოების ეფექტური განათლება საშუალო სკოლებში უნდა იყოს დაფუძნებული თეორიებსა და მოდელებზე, რომლებიც ასახავენ პროგრამის შემუშავებასა და განხორციელებას. არსებობს რამდენიმე თეორია და მოდელი, რომლებიც დაკავშირებულია კიბერუსაფრთხოების განათლებასთან, მათ შორის:
კონსტრუქტივისტული სწავლის თეორია: ეს თეორია ხაზს უსვამს ექსპერიმენტული და ინტერაქტიული სწავლის მნიშვნელობას, ხელი შეუწყოს მოსწავლეთა ჩართულობასა და გაგებას. კიბერუსაფრთხოების განათლების კონტექსტში, კონსტრუქტივისტული სწავლება შეიძლება მოიცავდეს ისეთ აქტივობებს, როგორებიცაა:სიმულაციები, თამაშები და პრაქტიკული აქტივობები, რომლებიც საშუალებას აძლევს მოსწავლეებს ისწავლონ პრაქტიკით.
სოციალური სწავლის თეორია: კიბერუსაფრთხოების განათლების კონტექსტში, სოციალური სწავლება შეიძლება მოიცავდეს თანატოლებზე დაფუძნებულ სასწავლო აქტივობებს, როგორებიცაა ჯგუფური დისკუსიები ან ერთობლივი პროექტები.
კოგნიტური დატვირთვის თეორია: ეს თეორია ფოკუსირებულია გონებრივი ძალისხმევის რაოდენობაზე, რაც საჭიროა ახალი ინფორმაციის დასამუშავებლად. კიბერუსაფრთხოების განათლების კონტექსტში, შემეცნებითი დატვირთვის მართვა შესაძლებელია ინფორმაციის მართვად ნაწილებში წარდგენით, სწავლის მხარდასაჭერად მულტიმედიური რესურსების გამოყენებით და მოსწავლეებისთვის მიწოდებული რთული ცნებების გასაგებად.
ადამიანზე ორიენტირებული დიზაინი: ეს მოდელი ხაზს უსვამს ინტუიციური და მარტივად გამოსაყენებელი პროდუქტებისა და სერვისების დიზაინის მნიშვნელობას. კიბერუსაფრთხოების განათლების კონტექსტში, ადამიანზე ორიენტირებული დიზაინი შეიძლება მოიცავდეს ასაკის შესაბამის და საინტერესო მასალებს, რომლებიც შექმნილია ახალგაზრდა მოსწავლეების საჭიროებებისა და ინტერესების გათვალისწინებით.

კიბერუსაფრთხოების ჩარჩოები: ეს არის კიბერუსაფრთხოების რისკების იდენტიფიცირების, შეფასებისა და მართვის სისტემატური მიდგომები. კიბერუსაფრთხოების განათლების კონტექსტში, კიბერუსაფრთხოების ჩარჩოებს შეუძლიათ უზრუნველყონ სასარგებლო სტრუქტურა კიბერუსაფრთხოების ძირითადი კონცეფციებისა და უნარების ორგანიზებისა და სწავლებისთვის.
ამ თეორიებისა და მოდელების ჩართვით, კიბერუსაფრთხოების საგანმანათლებლო პროგრამების შემუშავებასა და განხორციელებაში, პედაგოგებს შეუძლიათ შექმნან უფრო ეფექტური და მიმზიდველი სასწავლო გეგმა საშუალო სკოლის მოსწავლეებისთვის.

Theoretical Frameworks and Optimal Approaches for Imparting Cybersecurity Education to Secondary School Students

The provision of effective cybersecurity education in elementary schools necessitates a foundation built upon pertinent theories and models guiding program development and execution. Various theories and models relevant to cybersecurity education are as follows:
Constructivist Learning Theory: Emphasizing experiential and interactive learning, this theory underscores the significance of engaging students in activities such as simulations, games, and hands-on experiences within the realm of cybersecurity education, fostering learning through practical application.
Social Learning Theory: Within the context of cybersecurity education, social learning involves activities such as peer-based learning through group discussions or collaborative projects, facilitating knowledge acquisition through interpersonal interactions.
Cognitive Load Theory: Focused on managing the mental effort required for processing new information, this theory suggests strategies such as presenting information in manageable segments, utilizing multimedia resources to support learning, and simplifying complex concepts for students in the field of cybersecurity education.
Human-Centered Design: This model accentuates the creation of intuitive and user-friendly products and services. In the context of cybersecurity education, employing human-centered design involves developing age-appropriate and captivating materials aligned with the needs and interests of young learners.
Cybersecurity Frameworks: These systematic approaches are employed to identify, assess, and manage cybersecurity risks. In the realm of cybersecurity education, these frameworks serve as valuable tools for structuring and imparting essential cybersecurity concepts and skills.
By incorporating these theories and models into the planning and execution of cybersecurity education programs, educators can craft a curriculum that is not only more effective but also more engaging for middle school students.

5. კიბერუსაფრთხოების განათლების განხორციელების ბარიერები და გამოწვევები

საშუალო სკოლებში კიბერუსაფრთხოების განათლების მნიშვნელობის მიუხედავად, არსებობს რამდენიმე ბარიერი და გამოწვევა, რამაც შეიძლება გაართულოს პროგრამების ეფექტურად განხორციელება. აქ არის რამდენიმე გავრცელებული ბარიერი და გამოწვევა:
შეზღუდული რესურსები: ბევრ საშუალო სკოლას აქვს შეზღუდული რესურსები, მათ შორის დაფინანსება, პერსონალი და ტექნოლოგიური ინფრასტრუქტურა. ამან შეიძლება გაართულოს კიბერუსაფრთხოების საგანმანათლებლო პროგრამების შემუშავება და განხორციელება.
მასწავლებელთა ტრენინგების ნაკლებობა: მასწავლებლებს შეიძლება არ ჰქონდეთ გავლილი საჭირო ტრენინგი ან აკლდეთ გამოცდილება კიბერუსაფრთხოების ეფექტურად სწავლებისთვის. ამან შეიძლება გაართულოს შემუშავება საინტერესო და ეფექტური გაკვეთილების , რომელებიც აკმაყოფილებს მოსწავლეების საჭიროებებს.

ცვლილებებისადმი წინააღმდეგობა: სკოლები შეიძლება იყოს რეზისტენტული ცვლილებების მიმართ, განსაკუთრებით თუ კიბერუსაფრთხოების განათლება განიხილება, როგორც დამატებითი საგანი, ტრადიციული სასწავლო გეგმის მიღმა. ამან შეიძლება გაართულოს კიბერუსაფრთხოების საგანმანათლებლო ინიციატივების მხარდაჭერა.

სწრაფად ცვალებადი ტექნოლოგია: ტექნოლოგია მუდმივად ვითარდება და სკოლებისთვის შეიძლება რთული იყოს უახლესი მოვლენებისა და საფრთხეების ტემპის შენარჩუნება. ამან შეიძლება გაართულოს კიბერუსაფრთხოების საგანმანათლებლო პროგრამების შემუშავება და განხორციელება.

მშობლების შეზღუდული ჩართულობა: მშობლები გადამწყვეტ როლს ასრულებენ კიბერუსაფრთხოების საგანმანათლებლო სწავლებაში,მაგრამ ბევრმა მშობელმა შეიძლება არ იცოდეს ონლაინ აქტივობასთან დაკავშირებული რისკები ან შეიძლება არ ჰქონდეს საჭირო ცოდნა შვილების სწავლის მხარდასაჭერად.

სასწავლო გეგმის არ არსებობა: ამ ბარიერებისა და გამოწვევების გადაჭრა მოითხოვს მრავალმხრივ მიდგომას, რომელიც მოიცავს თანამშრომლობას პედაგოგებს, მშობლებსა და სასწავლო გეგმის შემქმნელებს შორის. ეს შეიძლება მოიცავდეს მასწავლებლებისთვის დამატებითი რესურსებისა და ტრენინგების მიწოდებას, მშობლების ჩართვას კიბერუსაფრთხოების განათლების მცდელობებში და პოლიტიკის მხარდაჭერას, რომელიც პრიორიტეტს ანიჭებს კიბერუსაფრთხოების განათლებას საშუალო სკოლებში. ამ გამოწვევების გადაჭრით ჩვენ შეგვიძლია,შევქმნათ დაცული და უსაფრთხო ონლაინ გარემო მოსწავლეებისთვის..

Obstacles and Difficulties in the Implementation of Cybersecurity Education

Despite the significance of cybersecurity education in elementary schools, various impediments and challenges hinder the effective implementation of programs. The following outlines prevalent barriers and challenges:

Limited Resources: Numerous elementary schools face constraints in terms of resources, encompassing funding, personnel, and technological infrastructure. This limitation complicates the formulation and execution of cybersecurity education programs.

Insufficient Teacher Training: Educators may lack the requisite training or experience to proficiently deliver cybersecurity education. This deficiency hampers the creation of engaging and effective lessons tailored to students' needs.

Resistance to Change: Educational institutions may exhibit resistance to change, particularly if cybersecurity education is perceived as an additional subject outside the conventional curriculum. This resistance poses challenges to endorsing initiatives related to cybersecurity education.

Rapid Technological Evolution: Technology undergoes continual advancements, rendering it challenging for schools to stay abreast of the latest developments and threats. This dynamic landscape complicates both the design and implementation of cybersecurity education programs.

Limited Parental Involvement: Parents play a pivotal role in cyber safety education. However, many may lack awareness of the risks associated with online activities or possess insufficient knowledge to support their children's learning.

Lack of Curriculum: Overcoming these barriers and challenges necessitates a comprehensive approach involving collaboration among educators, parents, and curriculum developers. Potential strategies include providing additional resources and training to teachers, engaging parents in cybersecurity education initiatives, and advocating for policies that prioritize cybersecurity education in elementary schools. By addressing these challenges, a secure online environment conducive to students' safety can be established.

6. კვლევის მეთოდოლოგია და შედეგები

გამოკითხვები: ინტერნეტზე დაფუძნებული გამოკითხვა გადანაწილდა საშუალო საფეხურის მასწავლებლებისა და სკოლის ადმინისტრაციის შემთხვევითი შერჩევით მთელი ქვეყნის მასშტაბით. კვლევაში მონაწილეობა მიიღო 269 რესპონდენტმა.
გამოკითხვა მოიცავდა კითხვებს მათ სკოლებში კიბერუსაფრთხოების განათლების ამჟამინდელი მდგომარეობის შესახებ, გამოკითხვა შემუშავდა გამოკითხვის კვლევის საუკეთესო პრაქტიკის გამოყენებით და ჩატარდა რეპუტაციის მქონე ონლაინ გამოკითხვის პლატფორმის მეშვეობით მონაცემთა უსაფრთხოებისა და კონფიდენციალურობის უზრუნველსაყოფად.

Research Methodology and Findings

Surveys: A web-based survey was disseminated to a randomly selected cohort of secondary school educators and administrators nationwide. 269 respondents took part in the research. This survey incorporated inquiries addressing the prevailing status of cybersecurity education within their respective educational institutions.
The survey instrument was meticulously crafted employing established best practices in survey research and was subsequently administered through a reputable online survey platform. This approach was undertaken to safeguard both data security and privacy throughout the data collection process.

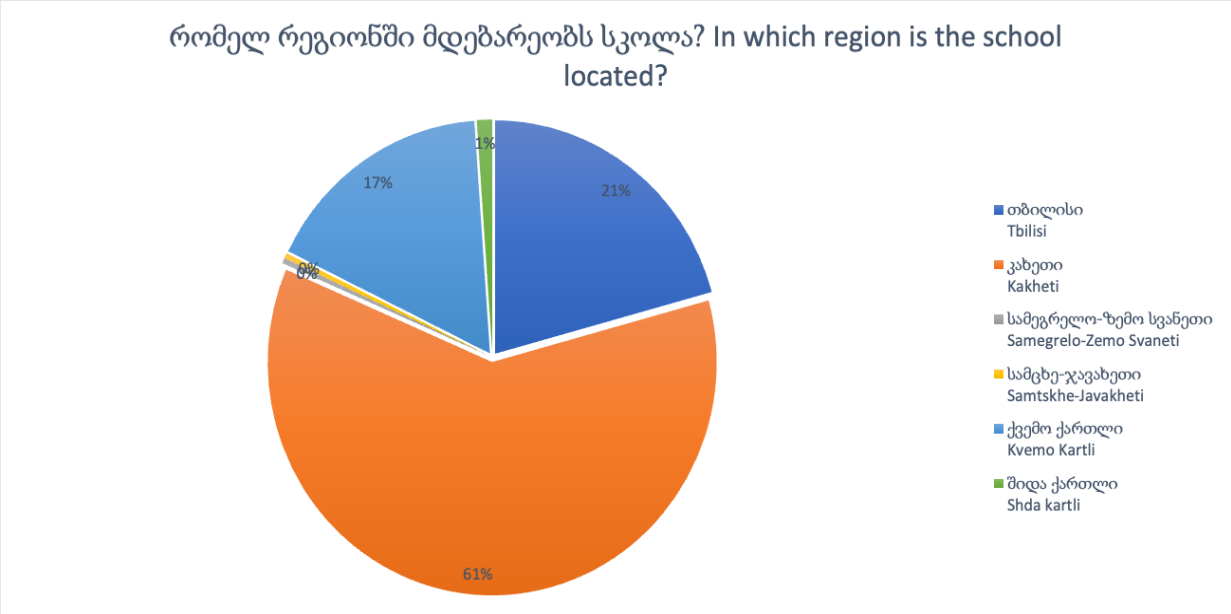

Fig.1. Question#1

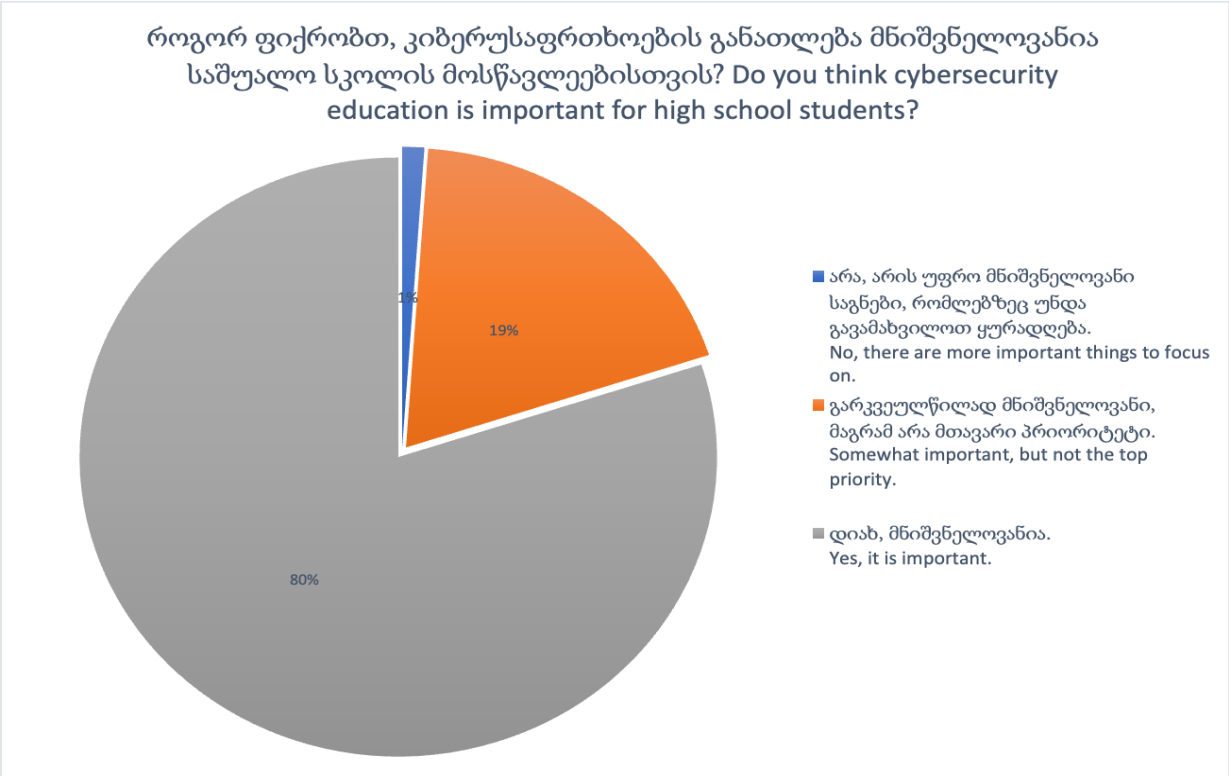

Fig.2. Question#2

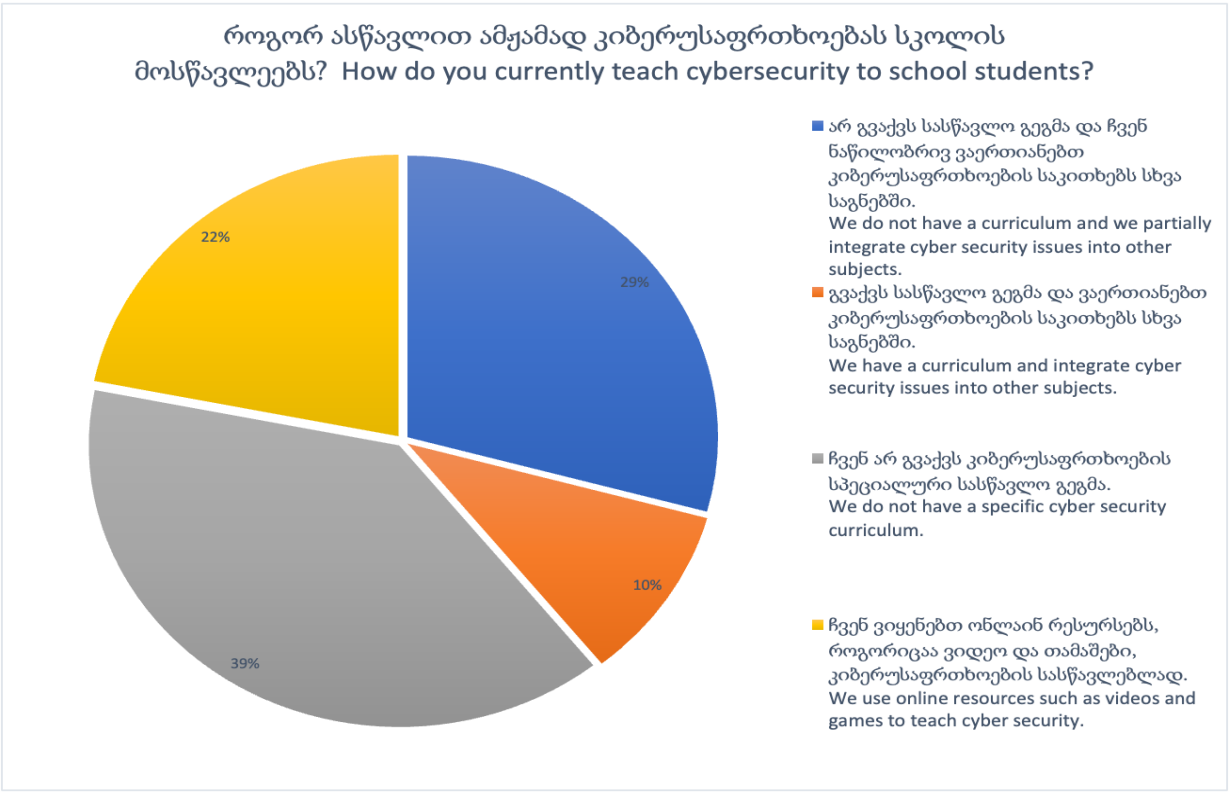

Fig.3. Question#3

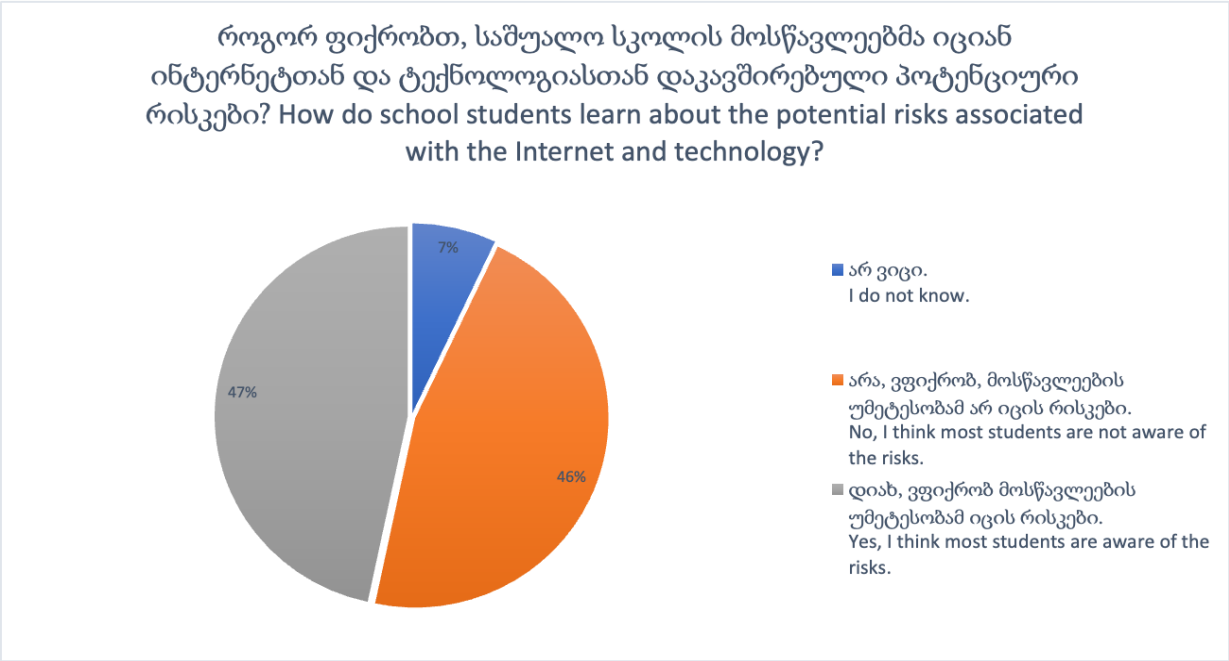

Fig.4. Question#4

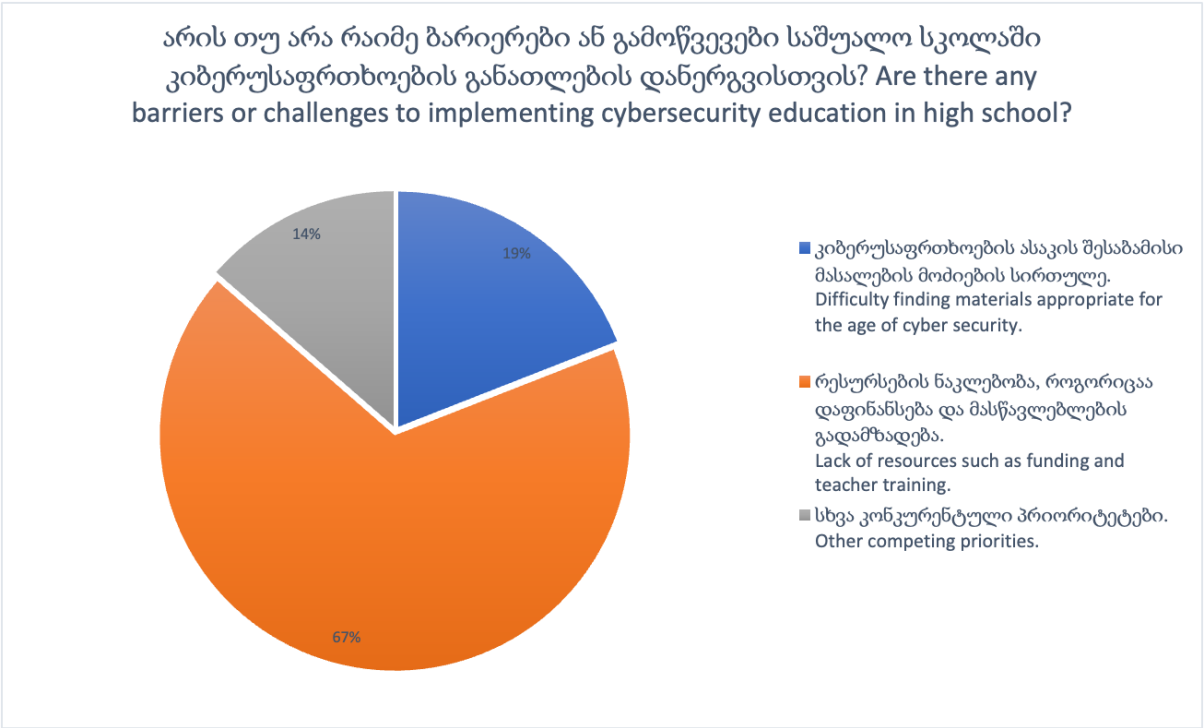

Fig.5. Question#5

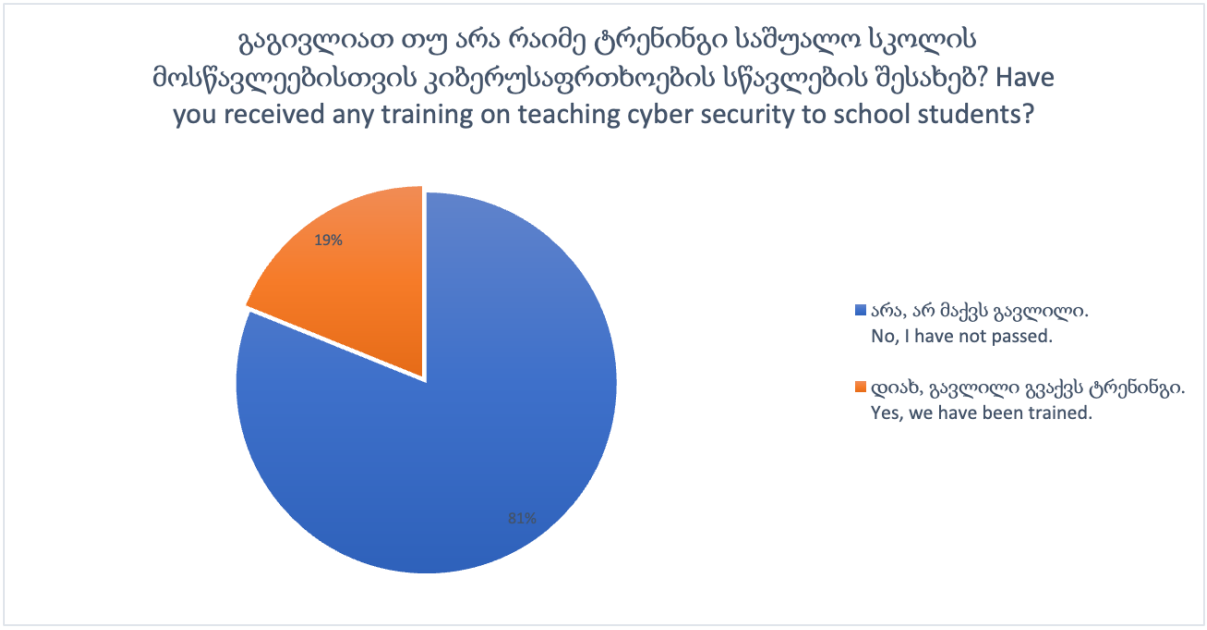

Fig.6. Question#6

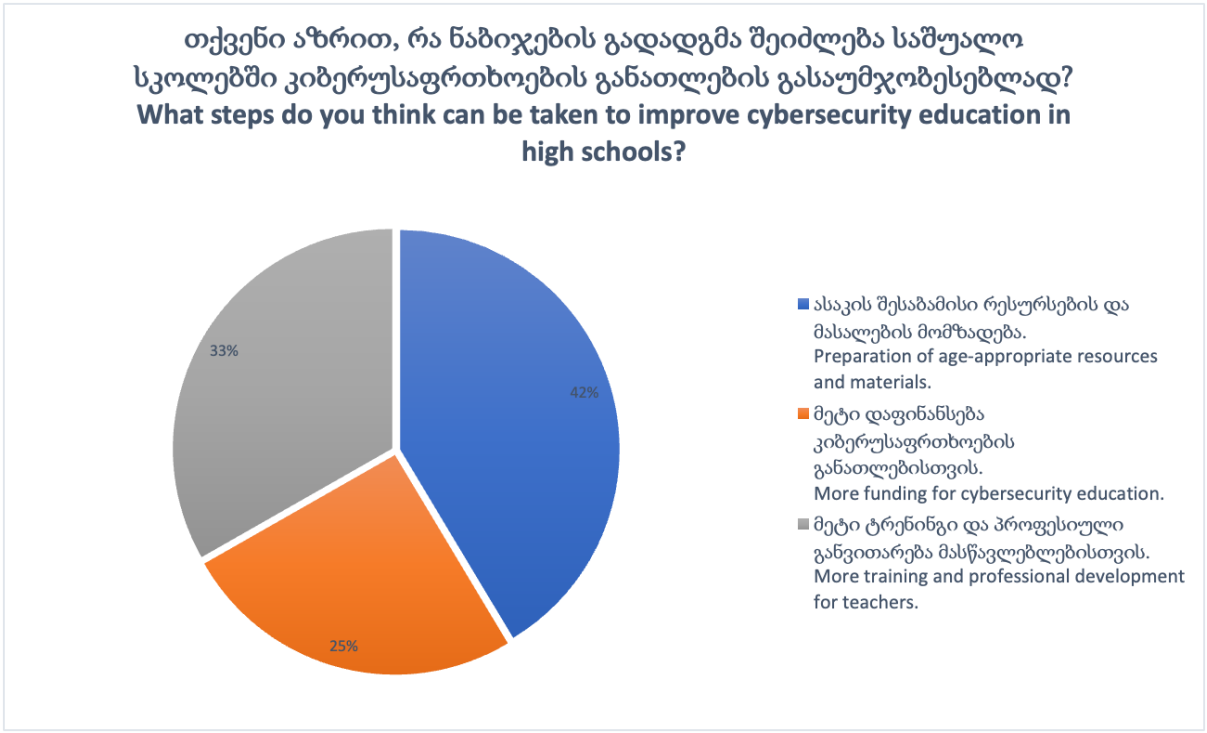

Fig.7. Question#7

7. შედეგების შეჯამება

გამოკითხვისა და ინტერვიუების შედეგად შეგროვებულმა მონაცემებმა გამოავლინა რამდენიმე ძირითადი სიახლე საშუალო სკოლებში კიბერუსაფრთხოების განათლების ამჟამინდელ მდგომარეობასთან დაკავშირებით. უპირველეს ყოვლისა, აღმოჩნდა, რომ

მიუხედავად იმისა, რომ ზოგიერთი სკოლა შეიცავს კიბერუსაფრთხოების განათლების გარკვეულ ფორმას თავის სასწავლო გეგმაში, არ არის თანმიმდევრულობა მიდგომებსა და გაშუქებულ თემებში.
მეორეც, დადგინდა, რომ მასწავლებლები ხშირად თავს მოუმზადებლად გრძნობდნენ კიბერუსაფრთხოების თემების სწავლებისთვის და არ ჰქონდათ საჭირო ტრენინგი და რესურსები ამის ეფექტურად გასაკეთებლად. ამან შეიძლება გამოიწვიოს მოსწავლეების ნდობისა და ჩართულობის ნაკლებობა.
მესამე, აღმოჩნდა, რომ არსებობს მნიშვნელოვანი ბარიერები სკოლებში ეფექტური კიბერუსაფრთხოების განათლების განსახორციელებლად, მათ შორის, დაფინანსებისა და მხარდაჭერის ნაკლებობა სკოლის რაიონებისა და ადმინისტრატორების მხრიდან და მშობლებსა და სხვა დაინტერესებულ მხარეებს შორის კიბერუსაფრთხოების განათლების მნიშვნელობის შესახებ ინფორმირებულობის ნაკლებობა.

Summary of Findings

The analysis of data derived from both survey responses and interviews has yielded noteworthy insights into the prevailing state of cybersecurity education within elementary schools. Firstly, the findings indicate that although many schools integrate some form of cybersecurity education into their curricula, there exists a notable lack of uniformity in the approaches employed and the specific topics addressed. Secondly, it has been observed that educators frequently express a sense of inadequacy in preparing for and delivering cybersecurity content, citing insufficient training and resources as contributing factors. This deficiency in preparedness has the potential to undermine the confidence and active participation of students.
Thirdly, substantial impediments to the successful implementation of cybersecurity education initiatives in schools have been identified. These obstacles encompass a dearth of financial backing and support from school districts and administrators, as well as a lack of awareness among parents and other stakeholders regarding the pivotal role of cybersecurity education.

8. კვლევის შედეგები საშუალო სკოლებში კიბერუსაფრთხოების განათლების შესახებ

ამ კვლევის შედეგებს მნიშვნელოვანი გავლენა აქვს საშუალო სკოლებში კიბერუსაფრთხოების განათლებაზე. შედეგები ვარაუდობს, რომ საგანი უნდა იყოს სუფრო ფორმალიზებული და ყოვლისმომცველი , რათა მოამზადოს ახალგაზრდა მოსწავლეები ციფრული ეპოქისთვის. ქვემოთ მოცემულია ამ კვლევის რამდენიმე ძირითადი შედეგი საშუალო სკოლებში კიბერუსაფრთხოების განათლებისთვის:
კიბერუსაფრთხოების ფორმალიზებული სასწავლო გეგმის საჭიროება: ამ კვლევის შედეგები ვარაუდობს, რომ საშუალოი სკოლების მხოლოდ მცირე პროცენტს აქვს კიბერუსაფრთხოების ფორმალური სასწავლო გეგმა ან პროგრამა. ეს ხაზს უსვამს მნიშვნელოვან ხარვეზს საშუალო სკოლებში კიბერუსაფრთხოების განათლებაში. აქედან გამომდინარე, საჭიროა შეიქმნას კიბერუსაფრთხოების ფორმალიზებული სასწავლო პროგრამა, რომელიც შეიძლება განხორციელდეს საშუალო სკოლებში, რათა უზრუნველყოფილი იყოს ახალგაზრდა მოსწავლეების ადეკვატურად მომზადება ციფრული ეპოქისთვის.
ტრენინგისა და პროფესიული განვითარების მნიშვნელობა: კვლევამ გამოავლინა მასწავლებლების პროფესიული განვითარებისა და კიბერუსაფრთხოების ტრენინგების საჭიროება. ეს მიუთითებს იმაზე, რომ მასწავლებლების ტრენინგსა და პროფესიულ განვითარებაში ინვესტირებას შეუძლია გააუმჯობესოს კიბერუსაფრთხოების განათლების ხარისხი საშუალო სკოლებში.

ასაკის შესაბამისი რესურსებისა და მასალების მნიშვნელობა: ამ კვლევამ გამოავლინა რომ სკოლებში არ არსებობს მოსწავლეებისთვის ასაკის შესაბამისი რესურსები და მასალები კიბერუსაფრთხოების შესახებ. აქედან გამომდინარე, საჭიროა შემუშავდეს ასაკის შესაბამისი რესურსები და მასალები, რომლებიც ადვილად ხელმისაწვდომი იქნება მასწავლებლებისა და მოსწავლეებისათვის.

კიბერუსაფრთხოების განათლების ინოვაციური მიდგომების მნიშვნელობა: ამ კვლევამ გამოავლინა,რომ საჭიროა კიბერუსაფრთხოების განათლებისადმი ინოვაციური მიდგომა, როგორიცაა გემიფიკაცია და პროექტზე დაფუძნებული სწავლება. ეს დასკვნები ვარაუდობს, რომ კიბერუსაფრთხოების განათლების შესახებ ინოვაციური მიდგომების ჩართვამ შეიძლება ის უფრო მიმზიდველი და ეფექტური გახადოს მოსწავლეებისთვის.

Research Findings on Cybersecurity Education in Secondary Schools

This study's outcomes bear significant implications for the realm of cybersecurity education within elementary schools. The findings underscore the necessity for a more formalized and comprehensive approach to equip young learners for the challenges of the digital age. The ensuing discussion delineates key discoveries pertinent to cybersecurity education in elementary schools:

Imperative for a Formalized Cybersecurity Curriculum:

The study indicates that merely a marginal percentage of elementary schools currently possess a formal cybersecurity curriculum or program. This observation accentuates a noteworthy void in cybersecurity education at the primary level. Consequently, there exists a compelling requirement to construct a formalized cyber safety curriculum tailored for implementation in secondary schools. This initiative aims to ensure that young students receive thorough preparation for navigating the complexities of the digital age.

Significance of Training and Professional Development:

A discernible need for professional development and cybersecurity training for teachers was identified through this study. This underscores the proposition that investing in teacher training and professional development endeavors can enhance the quality of cybersecurity education within secondary schools.

Relevance of Age-Appropriate Resources and Materials:

The research identifies a deficiency in age-appropriate resources and materials dedicated to educating students on cyber safety within school environments. Hence, it is imperative to conceive and develop resources and materials tailored to the specific age group, ensuring accessibility for both educators and students.

Importance of Innovative Approaches to Cybersecurity Education:

Findings from this study emphasize the necessity for innovative pedagogical approaches in cybersecurity education, such as gamification and project-based learning. The implication is that the incorporation of innovative methodologies can render cybersecurity education more engaging and efficacious for students.

9. რეკომენდაციები კიბერუსაფრთხოების განათლების გასაუმჯობესებლად

ამ კვლევის დასკვნებსა და შედეგებზე დაყრდნობით,შემოთავაზებული შემდეგი რეკომენდაციები საშუალ სკოლებში კიბერუსაფრთხოების განათლების გასაუმჯობესებლად:

კიბერუსაფრთხოების ფორმალიზებული სასწავლო გეგმის შემუშავება და განხორციელება: საშუალო სკოლებში კიბერუსაფრთხოების განათლების მნიშვნელოვანი ხარვეზის გათვალისწინებით, რეკომენდებულია კიბერუსაფრთხოების ფორმალიზებული სასწავლო გეგმის შემუშავება და დანერგვა ყველა საშუალო კლასში. სასწავლო პროგრამა უნდა იყოს ასაკის შესაბამისი, ყოვლისმომცველი და მოიცავდეს კიბერუსაფრთხოების

თემებს, მათ შორის ონლაინ უსაფრთხოებას, პაროლის უსაფრთხოებას და კიბერბულინგის.

უზრუნველყოს მასწავლებლების პროფესიული განვითარება და ტრენინგი: მასწავლებლები უნდა იყვნენ აღჭურვილი ცოდნითა და უნარებით, რათა ეფექტურად ასწავლონ კიბერუსაფრთხოება მოსწავლეებს. ამიტომ, რეკომენდებულია პროფესიული განვითარებისა და სატრენინგო პროგრამების შემუშავება და მიწოდება მასწავლებლებსთვის, რათა გააუმჯობესონ კიბერუსაფრთხოების კონცეფციების გაგება და შეისწავლონ როგორ ასწავლონ ისინი მოსწავლეებს.

ასაკის შესაბამისი რესურსების და მასალების შემუშავება: საშუალო სკოლებში კიბერუსაფრთხოების სწავლების მხარდასაჭერად, რეკომენდებულია ასაკის შესაბამისი რესურსების და მასალების შემუშავება. ეს რესურსები და მასალები უნდა იყოს ადვილად ხელმისაწვდომი, მიმზიდველი და სპეციალურად შექმნილი მოსწავლეებისთვის.

კიბერუსაფრთხოების განათლების ინოვაციური მიდგომების ჩართვა: კიბერუსაფრთხოების განათლების ინოვაციური მიდგომები, როგორიცაა გემიფიკაცია და პროექტზე დაფუძნებული სწავლება, ნაჩვენებია, რომ ეფექტურია მოსწავლეების ჩართვაში. ამიტომ, რეკომენდირებულია, რომ ეს მიდგომები ჩაერთოს საშუალო სკოლებში კიბერუსაფრთხოების განათლებაში, რათა ის უფრო მიმზიდველი და ეფექტური გახდეს.

პარტნიორობა მშობლებთან და მეურვეებთან: კიბერუსაფრთხოების განათლება არ უნდა შემოიფარგლოს საკლასო ოთახით. მშობლებსა და მეურვეებს , გადამწყვეტი როლი აქვთ სახლში კიბერუსაფრთხოების კონცეფციების განმტკიცებაში. ამიტომ, რეკომენდებულია სკოლების თანამშრომლობა მშობლებთან და მეურვეებთან, რათა მათ მიაწოდონ ცოდნა და რესურსები მშობლებს სახლში კიბერუსაფრთხოების განათლების მხარდასაჭერად.

Recommendations for Enhancing Cybersecurity Education

In light of the findings and outcomes derived from the present study, the following recommendations are posited to augment cybersecurity education within secondary school settings:

Development and Implementation of a Formalized Cybersecurity Curriculum:

In response to the discernible deficiency in cybersecurity education at the elementary level, it is advisable to devise and institute a structured cybersecurity curriculum encompassing all grades. This curriculum should be tailored to the age group, thorough in its coverage, and address pertinent cybersecurity subjects such as online safety, password security, and cyberbullying.

Provision of Professional Development and Training for Educators:

Recognizing the pivotal role of educators in imparting cybersecurity knowledge to students, it is imperative to offer professional development and training initiatives. These programs should be designed to enhance educators' proficiency in cybersecurity concepts, enabling them to effectively convey this knowledge to their students.

Development of Age-Appropriate Resources and Materials:

To facilitate the effective delivery of cybersecurity education in secondary schools, the creation of age-appropriate educational resources and materials is recommended. These resources should be readily accessible, engaging, and specifically tailored to the cognitive level of the learners.

Incorporation of Innovative Approaches to Cybersecurity Education:

Acknowledging the efficacy of innovative pedagogical strategies, such as gamification and project-based learning, it is advisable to integrate these approaches into secondary school cybersecurity education. Doing so is anticipated to enhance both the attractiveness and effectiveness of the educational process.

Collaboration with Parents and Guardians:

Recognizing the multifaceted nature of cybersecurity education, collaboration with parents and guardians is encouraged. Schools should actively engage with parents and guardians, providing them with knowledge and resources to reinforce cybersecurity concepts within the home environment. This

collaborative effort ensures a comprehensive approach to cybersecurity education that extends beyond the confines of the classroom.

10. კვლევის შეზღუდვები და მომავალი კვლევის მიმართულებები

ეს კვლევა იძლევა მნიშვნელოვან ინფორმაციას საშუალო სკოლებში კიბერუსაფრთხოების განათლების ამჟამინდელი მდგომარეობის შესახებ და გთავაზობთ რეკომენდაციებს მოსწავლეებისთვის კიბერუსაფრთხოების განათლების გასაუმჯობესებლად. თუმცა, ამ კვლევას აქვს რამდენიმე შეზღუდვა, რომელებიც გასათვალისწინებელია შედეგების ინტერპრეტაციისას. ეს შეზღუდვები მოიცავს:

ნიმუშის მცირე ზომა: ამ კვლევის შერჩევის ზომა შედარებით მცირე იყო, რამაც შესაძლოა შეზღუდოს დასკვნების განზოგადება. სამომავლო კვლევა მიზნად ისახავს სკოლების უფრო დიდი და მრავალფეროვანი ნიმუშის შეტანას, რათა დავინახოთ კიბერუსაფრთხოების განათლების მდგომარეობის უფრო სრულყოფილი სურათი.

თვითშედგენილი მონაცემები: ამ კვლევის მონაცემები შეგროვდა თვითშედგენილი გამოკითხვების მეშვეობით, რომლებიც შეიძლება ექვემდებარებოდეს მიკერძოებას ან სოციალურ სასურველ ეფექტს. სამომავლო კვლევამ უნდა განიხილოს მონაცემთა შეგროვების ალტერნატიული მეთოდების გამოყენება, როგორიცაა საკლასო ოთახში დაკვირვება ან ინტერვიუ მასწავლებლებთან და მოსწავლეებთან, რათა უზრუნველყოს საშუალო სკოლებში კიბერუსაფრთხოების განათლების უფრო ზუსტი და სიღრმისეული შესწავლა.

შეზღუდული სფერო: ეს კვლევა ფოკუსირებული იყო მხოლოდ საშუალო სკოლებში კიბერუსაფრთხოების განათლების მდგომარეობაზე და არ მოიცავდა კიბერუსაფრთხოების განათლების გავლენას მოსწავლეთა შედეგებზე. მომავალი კვლევა მიზნად ისახავს შეისწავლოს კიბერუსაფრთხოების განათლების სხვადასხვა მიდგომების ეფექტურობა მოსწავლეთა შედეგებზე, როგორებიცაა მათი ცოდნა, დამოკიდებულებები და კიბერუსაფრთხოებასთან დაკავშირებული ქცევები.

11. მომავალი კვლევის მიმართულებები მოიცავს:

გრძივი კვლევები: გრძივმა კვლევებმა შეიძლება მოგვაწოდოს კიბერუსაფრთხოების განათლების გრძელვადიანი გავლენა მოსწავლეების შედეგებზე, როგორებიცაა მათი ციფრული წიგნიერება და კიბერუსაფრთხოების ცნობიერება.

შედარებითი კვლევები: შედარებით კვლევებს შეუძლია შეადაროს საშუალო სკოლებში კიბერუსაფრთხოების განათლების სხვადასხვა მიდგომის ეფექტურობა, როგორიცაა ტრადიციული საკლასო სწავლება ინოვაციურ მიდგომებთან, გემიფიკაცია ან პროექტზე დაფუძნებული სწავლება.

კულტურათაშორისი კვლევები: კულტურათაშორისმა კვლევებმა შეიძლება შეისწავლოს კიბერუსაფრთხოების განათლების მსგავსება და განსხვავებები სხვადასხვა კულტურებსა და ქვეყნებში, რაც უზრუნველყოფს კულტურულ ფაქტორებს, რამაც შეიძლება გავლენა მოახდინოს კიბერუსაფრთხოების განათლების ეფექტურობაზე.

Research Limitations and Prospects for Future Investigation in the Field of Cybersecurity Education in Secondary Schools

This study contributes valuable insights into the current landscape of cybersecurity education within elementary schools and proposes recommendations to enhance the educational framework for students.

Nonetheless, it is imperative to acknowledge the study's inherent limitations for a nuanced interpretation of the results. These constraints encompass:

Small Sample Size:

The relatively modest sample size employed in this study poses a potential constraint on the generalizability of the findings. Subsequent research endeavors should strive to incorporate a more extensive and diverse array of schools, thus offering a more comprehensive understanding of the state of cybersecurity education.

Self-Administered Data:

Data acquisition for this study relied on self-administered surveys, introducing the possibility of bias or social desirability effects. Future investigations should contemplate alternative data collection methodologies, such as classroom observations or interviews with both teachers and students, to afford a more precise and thorough examination of cybersecurity education within secondary schools.

Limited Scope:

This study exclusively focused on assessing the state of cybersecurity education in secondary schools, omitting an exploration of the potential impact of such education on student outcomes. Future research endeavors should seek to scrutinize the efficacy of varied cybersecurity education approaches concerning student outcomes, encompassing facets such as knowledge acquisition, attitudinal shifts, and behavioral changes pertaining to cybersecurity.

Future avenues for research may include:

Longitudinal Studies:

Undertaking longitudinal studies can furnish valuable insights into the enduring impact of cybersecurity education on student outcomes, specifically gauging aspects such as digital literacy and cybersecurity awareness over an extended timeframe.

Comparative Studies:

Comparative studies have the potential to assess the effectiveness of diverse cybersecurity education approaches within secondary schools. This may involve a comparative analysis of traditional classroom teaching methodologies against innovative approaches, gamification strategies, or project-based learning.

Cross-Cultural Studies:

Cross-cultural studies provide an avenue for investigating commonalities and disparities in cybersecurity education across various cultures and countries. Such studies can yield valuable insights into cultural factors that may influence the effectiveness of cybersecurity education initiatives.

კვლევის შეჯამება და მნიშვნელობა

ამ კვლევით გამოირკვა კიბერუსაფრთხოების განათლების ამჟამინდელი მდგომარეობა საშუალო სკოლებში, გამოკვლეულ იქნა თეორიები და საუკეთესო პრაქტიკა საშუალო სკოლის მოსწავლეებისთვის კიბერუსაფრთხოების სწავლებისთვის, გამოვლინდა კიბერუსაფრთხოების სწავლების საუკეთესო პრაქტიკა და სტრატეგიები და გამოვიკვლიეთ ბარიერები და გამოწვევები სკოლებში კიბერუსაფრთხოების განათლების განხორციელებისთვის.

კვლევამ აჩვენა, მიუხედავად იმისა, რომ კიბერუსაფრთხოების განათლება იძენს აღიარებას, როგორც სწავლის მნიშვნელოვანი სფერო, მას ჯერ კიდევ არ ექცევა საკმარისი ყურადღება სკოლებში. კვლევამ გამოავლინა რამდენიმე ბარიერი და გამოწვევა სკოლებში ეფექტური კიბერუსაფრთხოების საგანმანათლებლო პროგრამების განხორციელებისთვის, როგორიცაა მოუმზადებული პერსონალისა და ადეკვატური რესურსების ნაკლებობა.

Summary and significance of the study

This research delves into the contemporary landscape of cybersecurity education within middle school settings. The investigation entails an assessment of prevailing practices, an exploration of pedagogical

theories relevant to instructing cybersecurity to middle school students, the delineation of optimal practices and instructional strategies for cybersecurity education, and an examination of impediments and challenges associated with the integration of cybersecurity education in educational institutions.
Current research indicates a growing acknowledgment of the significance of cybersecurity education, yet its incorporation into school curricula remains inadequate. Noteworthy barriers and challenges hindering the effective implementation of cybersecurity education programs in schools include insufficiently trained faculty and a dearth of essential resources.

REFERENCES:

1. Gitterman, A. (2004). Interactive andragogy: Principles, methods, and skills. Journal of Teaching in Social Work, 24(¾), 95-112. Retrieved from https://www.bu.edu/ssw/files/2010/11/Alex-Gitterman1.pdfMallon, M. N. (2013). Extending the learning process: Using the theory of connectivism to inspire student collaboration. CULS Proceedings, 3, 18-27. Retrieved from https://soar.wichita.edu/bitstream/handle/10057/5571/1833-6771-1-PB.pdf?sequence=1
2. Schell, G. P. & Janicki, T. J. (2013). Online course pedagogy and the constructivist learning model. Journal of the Southern Association for Information Systems, 1(1). Retrieved from https://dx.doi.org/10.3998/jsais.11880084.0001.104
3. Sobels, J. Szili, G., & Bass, D. (2015). Using constructivist teaching tools to stimulate active learning in first year environmental management undergraduates. Planet, 25(1), 21-26. Retrieved from https://doi.org/10.11120/plan.2012.00250021
4. Xu, W.L, Pedersen, N.L., Keller, L., Kalpouzos, G., Wang, H.X., Graff, C,. Fratiglioni, L. (2015). HHEX_23 AA Genotype Exacerbates Effect of Diabetes on Dementia and Alzheimer Disease: A Population-Based Longitudinal Study. PLOS. Retrieved from https://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1001853
5. The State of Cybersecurity Education in K-12 Schools https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf
6. CISA: Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity https://www.cisa.gov/news-events/news/cisa-releases-report-k-12-schools-help-address-evolving-cybersecurity-threats
7. EdTech Leadership Survey (2022): https://www.cosn.org/tools-and-resources/resource/edtech-leadership-survey-report-2022/
8. L. Wang, J. Yang, P. Wan Educational modules and research surveys on critical cybersecurity topics Int J Distrib Sens Netw, 16 (9) (2020), pp. 1-18 https://scholar.google.com/scholar_lookup?title=Educational%20modules%20and%20research%20surveys%20on%20critical%20cybersecurity%20topics&publication_year=2020&author=L.%20Wang&author=J.%20Yang&author=P.%20Wan
9. F. Katz Breadth vs. depth: Best practices teaching cybersecurity in a small public university The Cyber Defense Review, 3 (2) (2018), pp. 65-72 https://scholar.google.com/scholar_lookup?title=Breadth%20vs.%20depth%3A%20Best%20practices%20teaching%20cybersecurity%20in%20a%20small%20public%20university&publication_year=2018&author=F.%20Katz
10. M. Lauver Top 4 obstacles to K-12 cybersecurity https://www.securitymagazine.com/articles/97290-top-4-obstacles-to-k-12-cybersecurity
11. M. Coenraad, A. Pellicone, D. Jass Ketelhut, M. Cukier, J. Plane, D. Weintrop Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games Simulation & Gaming, 51 (5) (2020), pp. 586-611

https://scholar.google.com/scholar_lookup?title=Experiencing%20cybersecurity%20one%20game%20at%20a%20time%3A%20A%20systematic%20review%20of%20cybersecurity%20digital%20games&publication_year=2020&author=M.%20Coenraad&author=A.%20Pellicone&author=D.%20Jass%20Ketelhut&author=M.%20Cukier&author=J.%20Plane&author=D.%20Weintrop