სეზონური სკოლის აბსტრაქტი

კიბერუსაფრთხოების ახალი გამოწვევები გლობალურ საინფორმაციო სივრცეში

ინფორმაციული უსაფრთხოება გლობალურ საინფორმაციო სივრცეში დღევანდელობის ერთერთ აქტუალურ თემას წარმოადგენს. 21-ე საუკუნეში მკვეთრად განვითარდა ინფორმაციის დაგროვების საშუალებები, მატულობს დაგროვილი ინფორმაციის მოცულობა და დახვეწილია მისი ტრანსპორტირების ინფრასტრუქტურა. გლობალურ საინფორმაციო სივრცეში ხშირად კონფიდენციალური შინაარსის მონაცემები მოძრაობს, რომლის დაკარგვა და არაავტორიზებული გამოყენება შეიძლება სერიოზულ, ხოლო ხშირად კატასტროფულ პრობლემად იქცეს. მწვავედ დგას თანამედროვე გლობალურ საინფორმაციო სივრცეში **კიბერუსაფრთხოების** უზრუნველყოფის პრობლემა, რაც მოცემული პროექტის საგანს წარმოადგენს.

ინფორმაციული უსაფრთხოების პრობლემათა სიმწვავე კარგად ჩანს საქართველოს მთავარი პროკურატურის დოკუმენტში **„ინფორმაცია კიბერდანაშაულის შესახებ“**, ხოლო **„საქართველოს ეროვნული უსაფრთხოების კონცეფციაში“** კიბერუსაფრთხოებას თვალსაჩინო ადგილი უჭირავს. რიგ სახელმწიფო და კერძო დაწესებულებებში წარმატებით ინერგება და გამოიყენება კიბერთავდაცვის მრავალდონიანი სისტემები. სამეცნიერო ღონისძიების „კიბერუსაფრთხოების ახალი გამოწვევები გლობალურ საინფორმაციო სივრცეში“ მთავარ დანიშნულებას კიბერუსაფრთხოების სფეროს უახლესი გამოწვევების და მათთან გამკლავების მეთოდების და ინსტრუმენტების განხილვა წარმოადგენდა. საქართველოს უმაღლესი განათლების სფეროში კიბერუსაფრთხოების მიმართულება ჯერ კიდევ არასაკმარისადაა განვითარებული, ხოლო კიბერუსაფრთხოების, როგორც ერთიანი დისციპლინისთვის (იურიდიული, თეორიული და პრაქტიკული კომპონენტებით) საკმარისი კომპეტენციით აღჭურვილი სპეციალისტები დიდ იშვიათობას წარმოადგენს. წარდგენილი პროექტი განხორციელდა ამ მიმართულებით არსებული „თეთრი ლაქების“ შესავსებად. სამეცნიერო თუ არასამეცნიერო მიმართულებით მომუშავე ახალგაზრდებს მიეცათ შესაძლებლობა გაცნობოდნენ კიბერუსაფრთხოების მთლიან სივრცეს. კიბერუსაფრთხოების სფეროში საინფორმაციო უსაფრთხოების სფეროში მომუშავე ქართველი და უცხოელი სპეციალისტების მიერ წარმართულ ღონისძიებაზე მსმენელებს შესაძლებლობა მიეცათ შეექმნათ სრული წარმოდგენა თანამედროვე ციფრულ საინფორმაციო სივრცეში არსებულ საფრთხეებზე როგორც გლობალური, ასევე ჩვენი ქვეყნის მასშტაბით.

პროექტის ძირითადი კომპონენტია ერთკვირიანი სეზონური სკოლა, რომელიც გაიმართა 2019 წლის აპრილში, გორში, **დავით აღმაშენებლის სახელობის ეროვნული თავდაცვის აკადემიაში.** სეზონური სკოლის მუშაობაში მონაწილეობას მიიღებდა კიბერუსაფრთხოების ხუთი ქართველი და ერთი უცხოელი სპეციალისტი, რომლებიც 15 მსმენელისთვის უმნიშვნელოვანეს თემებს აშუქებდნენ:

- გლობალურ საინფორმაციო სივრცეში განთავსებული ინფორმაცია, მასთან მიმართვის უფლებები და ვალდებულებები. სამართლებრივ რეგულაციები, რომლებიც ინფორმაციასთან წვდომას და მის გამოყენებას არეგულირებენ
- კიბერუსაფრთხოების სტრუქტურა და მისი სხვადასხვა დონეების (ფიზიკური, ლოგიკური, სოციალური), აგრეთვე სფეროს საბაზისო და ახალი ტენდეციების დეტალური განხილვა
- ინფორმაციული ტექნოლოგიების და კიბერუსაფრთხოების კვლევის და ანალიზის მეთოდები
- ტერმინ „კრიტიკული ინფრასტრუქტურის“ განსაზღვრა, ინფრასტრუქტურული რისკების კლასიფიკაცია და მათი მინიმუმამდე შემცირების მეთოდები
- საქართველოს კიბერუსართხოების სისტემა - უპირატესობები და ნაკლოვანებები. ჩვენი ქვეყნის კიბერუსაფრთხოების წინაშე არსებული გამოწვევები და მათთან გამკლავების სტატეგია მოკლე- და გრძელვადიანი პერიოდებისთვის
- კიბერცნობიერების ამაღლების და კიბერჰიგიენის დაცვის მეთოდები
- ინფორმაციის დაცვის თეორიული მეთოდები და ინსტრუმენტები. კრიპტოგრაფიული ალგორითმების კლასიფიკაცია და გამოყენების სფეროები (ინფორმაციის მთლიანობის დაცვა, ციფრული ხელმოწერა);
- კიბერუსაფრთხოება ინტრანეტში. ორგანიზაციის კორპორაციულ ქსელში კიბერუსაფრთხოების მრავალდონიანი სისტემების აგების მეთოდები და ინსტრუმენტები
- კიბერუსაფრთხოება ლოკალურ ქსელებში. ქსელის პერიმეტრის და დემილიტარიზებული ზონის გამართვის და დაცვის აპარატული და პროგრამული საშუალებები (AAA, ფაიერვოლი, აუთენტიფიკაციის ერთიანი სისტემები, შემოჭრათა დეტექცია ან/და პრევენცია)
- კიბერუსაფრთხოება სერვერულ სისტემებსა და მონაცემთა საცავებში. მონაცემთა დაცვის ფიზიკური, აპარატული და პროგრამული საშუალებები. აპარატულ და პროგრამულ რესურსებთან წვდომათა ცენტრალიზებული მართვა. ბრძოლა მონაცემთა გაჟონვასა და გარე მუქარების ყველა, მათ შორის ადამიანურ და პროგრამულ რისკებთან
- კიბერუსაფრთხოება მონაცემთა ბაზებში. კრიტიკულ მონაცემთა უსაფრთხო ორგანიზაციის უზრუნველყოფა. სარგებლიანი და საიმედო მონაცემთა ბაზების ინფრასტრუქტურის შექმნა.

სეზონური სკოლის სამიზნე სამიზნე აუდიტორიას წარმოადგენდა ქვეყნის სხვადასხვა რეგიონში არსებული უმაღლესი სასწავლო დაწესებულებების მაგისტრები, დოქტორანტები, ასევე კიბერუსაფრთხოების სფეროში საკმარისი კომპტენციის მქონე ყველა დაინტერესებული პირი.

პროექტის პროგრამა მოიცავდა ლექციებს, დისკუსიებს და პრაქტიკულ მეცადინეობებს. სასწავლო მასალა - პრეზენტაციები, ინტერაქტიული სასწავლო ინსტრუმენტები, ვიდეო მასალა, სიმულატორები და ინოვაციური სწავლების სხვა დამხმარე ინსტრუმენტები.

სეზონური სკოლის დასრულებისთანავე ჩატარდა შემაჯამებელი კონფერენცია ფართო აუდიტორიის წინაშე, სადაც პროექტში მონაწილე სტუდენტებს გადაეცათ პროგრამაში მონაწილის სერტიფიკატი.

პროგრამაში ჩართული 15 ახალგაზრდისთვის სწავლა, განთავსება, კვება, კულტურული პროგრამა საგრანტო პროგრამის ფარგლებში სრულად დაფინანსდა.

ძირითადი და პლენარული მოხსენებების წასაკითხად პროექტში ჩართული ყვნენ მაღალი კვალიფიკაციის მქონე პერსონალი როგორც საზღვარგარეთიდან, ასევე საქართველოში კიბერუსაფრთხოების პრობლემებზე მომუშავე ორგანიზაციებიდან. მოხსენებათა თემატიკა სამ ძირითად ჯგუფში გადანაწილდა:

- კიბერუსაფრთხოების სტანდარტები, კონცეპტუალური და სამართლებრივი ასპექტები
- კიბერუსაფრთხოების თეორიული საფუძვლები
- კიბერუსაფრთხოების პრაქტიკული იმპლემენტაციის მეთოდები და ინსტრუმენტები

სესია 1.

ამავე სექციაში დავით აღმაშენებლის სახელობის ეროვნული თავდაცვის აკადემიის ასოცირებული პროფესორი **დავით გულუა** სერვერული სისტემების და კორპორაციული მონაცემთა ბაზების უსაფრთხოების დაცვის მეთოდები და ინსტრუმენტები წარმოადგინა:

- ორგანიზაციის IT-ინფრასტრუქტურის ცენტრალიზებული მართვა ერთიანი დომენური ინფრასტრუქტურის ფარგლებში (Active Directory-ტექნოლოგიის საფუძველზე)
- ჯგუფური პოლიტიკების (Group Policies) დაგეგმვა, შექმნა, განაწილება და მართვა ორგანიზაციის სტრუქტურული ერთეულებისთვის
- შიდა ქსელურ რესურსებთან წვდომის კონტროლი ფაილური და სხვა სერვისების ფარგლებში
- ინტერნეტთან წვდომის კონტროლი Proxy-სერვისის საფუძველზე
- მონაცემთა ბაზების სარეზერვო კოპირება
- წვდომათა მართვა და აუდიტი მონაცემთა ბაზებში
- მონაცემთა ბაზებთან არაავტორიზებული წვდომები და მათთან ბრძოლის მეთოდები

სესია 2

ინოვაციებისა და ტექნოლოგიების სააგენტოს თანამშრომელი, თავდაცვის სამინისტროს სსიპ კიბერუსაფრთხოების ბიუროს ყოფილი დირექტორი და გენერალური ინსპექტორი **ანდრია გოცირიძე** მსმენელებს საქართველოში არსებული კიბერსაფრთხეების ანალიზი და მათთან გამკლავების მეთოდები წარმოადგინა:

- საქართველოს კიბერსივრცეში არსებული საფრთხეები
- კიბერსივრცის გამოყენება პროპაგანდისა და საინფორმაციო-ფსიქოლოგური ზემოქმედებისათვის
- კიბერტერორიზმი
- მავნე პროგრამული უზრუნველყოფა და მისი სახეები;

- სამუშაო კომპიუტერის უსაფრთხოება;
- ელექტრონული ფოსტის უსაფრთხოება;
- ფიშინგი;
- პასვორდის უსაფრთხოება;
- უსაფრთხო ინტერნეტი მოგზაურობისას;
- უკაბელო ინტერნეტის უსაფრთხოება;
- მობილური მოწყობილობების უსაფრთხოება;
- უსაფრთხო ონლაინ - ბანკინგი და შოპინგი;
- სოციალური ქსელების უსაფრთხოება;
- ID მოპარვა და ინტერნეტ-თაღლითობა;
- ქლაუდის უსაფრთხოება;
- რჩევები მშობლებს

სესია 3

საქართველოს ტექნიკური უნივერსიტეტის ასოცირებული პროფესორი, კომპანია Cisco-ს სერტიფიცირებული ტრენერი **ვლადიმერ ადამიამ** აქცენტი კომპიუტერული ქსელების კიბერუსაფრთხოების უზრუნველყოფაზე გააკეთა და შემდეგი ძირითადი საკითხები განიხილა:

- ლოკალური ქსელის უსაფრთხოება
- აუტენტიფიკაცია, ავტორიზაცია და აღრიცხვა(AAA) და აუტენტიფიკაციის დაშორებული სისტემები (RADIUS, TACACS+)
- კიბერთავდაცვის პრევენციული სისტემის (IPS) დანერგვა
- ვირტუალური კერძო ქსელი(VPN ტექნოლოგია)
- უკაბელო ქსელების უსაფრთხოების საკითხები

სესია 4

მოხსენებათა **მეორე თემატურ სექციაში** დავით აღმაშენებლის სახელობის ეროვნული თავდაცვის აკადემიის ასოცირებული პროფესორი **რომეო გალდავა** კიბერუსაფრთხოების უზრუნველყოფის თეორიულ ასპექტებს წარმოადგენს. მისი მოხსენებები მოიცავს ინფორმაციის დაცვის კრიპტოგრაფიული ალგორითმების ზოგად მიმოხილვას და ელექტრონული საქმისწარმოების სხვადასხვა ამოცანებისთვის მათი გამოყენების მეთოდებს. რომეო გალდავას მიერ გაშუქებული საკითხების ძირითადი ჩამონათვალი შემდეგი პუნქტებისგან შედგება:

- ინფორმაციული უსაფრთხოების პრობლემები და დაცვის კრიპტოგრაფიული ტექნოლოგიები, თანამედროვე სიმეტრიული კრიპტოგრაფია. ბლოკური დაშიფვრის ალგორითმები
- კონფიდენციალობის დაცვის სტანდარტი - ალგორითმი AES RIJNDAEL. კონფიდენციალურობის დაცვის რეჟიმები
- ინფორმაციის მთლიანობის პრობლემა და მისი გადაჭრის გზები.
- ჰეშ-ფუნქციების როლი თანამედროვე კრიპტოგრაფიაში. კრიპტოგრაფიულად საიმედო ჰეშ-ფუნქციები, მათი გამოთვლის ალგორითმები
- შეტყობინების აუთენტიფიკაციის კოდების (MAC) გამოთვლის სტანდარტები CMAC, PMAC და HMAC
- ასიმეტრიული კრიპტოსისტემები.
- ავტორობის ვერუარყოფის პრობლემა და ციფრული ხელმოწერის სტანდარტი - ECDSS.

ამავე სესიის ფარგლებში სსიპ კიბერუსაფრთხოების ბიუროს თანამშრომელმა **ომარ აბშილავამ** ორგანიზაციაში კიბერცნობიერების ამაღლების ასპექტები მიმოიხილა:

- თავდაცვის სფეროს სუბიექტებში კრიტიკული ინფორმაციული სისტემების ინფორმაციული უსაფრთხოების აუდიტი
- კიბერუსაფრთხოების უზრუნველყოფის სამოქმედო გეგმები და უსაფრთხოების პოლიტიკების მართვის სახელმძღვანელოების შექმნის ასპექტები
- ტრენინგები სამინისტროს თანამშრომელთა კიბერცნობიერების ასამაღლებლად
- თანამშრომელთა სერტიფიცირება კიბერუსაფრთხოების მიმართულებით

სესია 5

უცხოელი სპეციალისტი, რუმინეთის ეროვნული თავდაცვის უნივერსიტეტ „კაროლ I“-ის პროფესორი, პოლკოვნიკი **ჩეზარ ვასილესკუ** გლობალური კიბერუსაფრთხოების თანამედროვე ტენდენციებს და რისკებს აშუქებდა:

- თანამედროვე კიბერუსაფრთხოების სპეციფიკური ასპექტები
- კიბერსივრცის დონეები - ფიზიკური, ლოგიკური და სოციალური
- კრიტიკული ინფორმაციული ინფრასტრუქტურა
- კიბერუსაფრთხოება და მომავალი კონფლიქტები - როგორ იქცევა ტექნოლოგიური უპირატესობა ნაკლოვანებად

- ეროვნული და საერთაშორისო ინსტიტუციების როლი გლობალური საინფორმაციო სივრცის კიბერუსაფრთხოების უზრუნველყოფაში
- სამოქალაქო და სამხედრო SCADA-სისტემები – მომავალი კიბერშეტევების „რჩეული“ სამიზნეები

სეზონური სკოლის დასკვნით დღეს ჩატარდა კონფერენცია, რომელზეც შეჯამდება განვლილი აქტივობების შედეგები და გამოიკვეთება ის რეკომენდაციები, რომელთა გათვალისწინებაც სკოლის მსმენელების კიბერუსაფრთხოების სფეროში თავიანთი მომავალი საქმიანობისას გამოადგებათ.

ღონისძიების მნიშვნელობა დიდია ჩვენი ქვეყნის შიგნით და მის ფარგლებს გარეთ ინსტიტუციათშორისი კავშირების გასაღრმავებლად. კიბერინციდენტების, მათთან ბრძოლის და კიბერპრობლემების აღმოფხვრის თითოეული ქეისი, გარკვეული საერთო მახასიათებლების არსებობის მიუხედავად, უნიკალურ შემთხვევას წარმოადგენს მრავალი თავისებურებით.

კიბერუსაფრთხოების სეზონური სკოლის მონაწილეებისა და ყველა დაინტერესებული პირისთვის ვებგვერდზე cybergeorgia.ge ამოქმედდა ფორუმი, სადაც შეგიძლიათ გაეცნოთ კოლეგების რჩევებს კიბერუსაფრთხოების აქტუალურ საკითხებზე, ხოლო საიტზე დარეგისტრირების შემდეგ რჩევა ჰკითხოთ მათ ან თავად დაეხმაროთ კიბერუსაფრთხოების პრობლემებთან გამკლავებაში.