

კიბერუსაფრთხოების ახალი გამოწვევები გლობალურ საინფორმაციო სივრცეში

სეზონური სკოლა

დავით აღმაშენებლის სახელობის ეროვნული
თავდაცვის აკადემია
გორი, 2019 წლის 15-19 აპრილი

ხელმძღვანელი: ტმდ, ასოცირებული პროფესორი ნანი არაბული
კოორდინატორი: ტმდ, ასოცირებული პროფესორი დავით გულუა

პრეზენტაციის შინაარსი

- თემის აქტუალობა
- ინფორმაცია სეზონური ღონისძიების შესახებ
 - ორგანიზატორები, დრო და ადგილი
 - დაგეგმილი აქტივობები
 - განმახორციელებელი პერსონალი
- მონაწილეთა შერჩევა

თემის აქტუალობა

- ინფორმაციული უსაფრთხოება გლობალურ საინფორმაციო სივრცეში დღევანდებლობის ერთერთ უმნიშვნელოვანეს საკითხს წარმოადგენს
- კრიტიკული ინფორმაციის დაკარგვა ან/და არაავტორიზებული გამოყენება შეიძლება სერიოზულ, ხოლო ხშირად კატასტროფულ პრობლემად იქცეს
- მწვავედ დგას თანამედროვე გლობალურ საინფორმაციო სივრცეში კიბერუსაფრთხოების უზრუნველყოფის პრობლემა და იგი ძალიან კრიტიკულია საქართველოშიც

კიბერუსაფრთხოების გლობალური პრობლემები

- 21-ე საუკუნე ინტერნეტის მასობრივი გავრცელების და ინფორმაციის საყოველთაო ხელმისაწვდომობის საუკუნეა, რაც ინფორმაციის დაკარგვის და მასთან არაავტო-რიზებული წვდომის რისკებს მკვეთრად ამაღლებს
- კიბერმუქარების წყაროები მრავალფეროვანია: სახელმწიფო და კერძო ჰაკერები, მავნე პროგრამები, „ინსაიდერები“
- კიბერუსაფრთხოების რისკები ეხება
 - კრიტიკული ინფორმაციულ სისტემებს და მონაცემთა ბაზებს
 - კომპიუტერულ ქსელებს
 - ინდუსტრიული სისტემებს და სხვა ინფრასტრუქტურული ობიექტებს

მაგალითი: კიბერუსაფრთხოების პრობლემები 2008 წლის რუსეთ-საქართველოს ომის დროს

- რუსული ბოტნეტები + მოხალისეები
- DDoS-შეტევები ქართული სამთავრობო და მედიარესურსების წინააღმდეგ
- ქართული ვებგვერდების უსაფრთხოების სისტემების გატეხვა და კიბერვანდალიზმის აქტები
- ქართული საბანკო სექტორის ბლოკირება და ამორთვა მსოფლიო საბანკო სერვისების ქსელიდან
- მობილური კავშირის შეფერხება

განხორციელებული ცვლილებები და მიმდინარე ამოცანები

- კიბერუსაფრთხოების უზრუნველყოფა საქართველოში სახელმწიფო პრიორიტეტებს განეკუთვნება
 - „საქართველოს ეროვნული უსაფრთხოების კონცეფციაში“ ნაციონალური ინტერესების 14-პუნქტიან სიაში ერთერთს „კიბერუსაფრთხოების უზრუნველყოფა“ წარმოადგენს
- მთავარი პრობლემა: კიბერუსაფრთხოების სპეციალისტების უკიდურესად არასაკმარისი რაოდენობა
- გამოსავალი: საკმარისი რაოდენობით კვალიფიციური კადრების მომზადება კიბერუსაფრთხოების შესაძლო რისკებთან საბრძოლველად

ღონისძიების ორგანიზაცია

- დონორი: შოთა რუსთაველის საქართველოს ეროვნული სამეცნიერო ფონდი
 - <http://rustaveli.org.ge/>
- ორგანიზატორი: საქართველოს თავდაცვის სამინისტროს დავით აღმაშენებლის სახელობის ეროვნული თავდაცვის აკადემია
 - <http://eta.edu.ge/>
- სეზონური ღონისძიების გამართვის ადგილი: ქ. გორი, ცხინვალის გზატკეცილი, მე-3 კილომეტრი

პარტნიორი ორგანიზაციები

- NATO-ს თავდაცვის განათლების განვითარების პროგრამა;
- საქართველოს თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიურო;
- საქართველოს ტექნიკური უნივერსიტეტი, კომპიუტერული ქსელის მართვის ცენტრი;
- ინოვაციებისა და ტექნოლოგიების სააგენტო

ორგანიზაციული საკითხები

- პროექტის ფარგლებში შეირჩევა სეზონური ღონისძიების 15 მონაწილე (შერჩევის პროცედურის დეტალური აღწერა იხილეთ ქვემოთ)
- სეზონური სკოლის სამიზნე აუდიტორიას წარმოადგენს ქვეყნის სხვადასხვა რეგიონში არსებული უმაღლესი სასწავლო დაწესებულებების მაგისტრანტები და დოქტორანტები, ასევე კიბერუსაფრთხოების სფეროში საკმარისი კომპტენციის მქონე ყველა დაინტერესებული პირი
- პროექტის ფარგლებში სრულად დაფინანსდება: სწავლა, განთავსება, კულტურული პროგრამა და კვება
- სეზონური სკოლის დასრულებისთანავე მონაწილეებს გადაეცემათ პროგრამაში მონაწილის სერტიფიკატი



აკადემიის შესახებ

- 1919 – საქართველოს სამხედრო სკოლის დაარსება (საქართველოს დემოკრატიული რესპუბლიკა, 1918-1921)
 - სკოლის იუნკერთა გმირული ბრძოლა თბილისის დასაცავად საბჭოთა კავშირ - საქართველოს ომის დროს
- 1993 – საქართველოს რესპუბლიკის გაერთიანებული სამხედრო აკადემიის დაარსება
- 2003 - აკადემიას დავით აღმაშენებლის სახელი მიენიჭა
- 2009 – აკადემია თბილისიდან გორში გადავიდა
- 2010 - აკადემიამ მიიღო უმაღლესი საგანმანათლებლო დაწესებულების სტატუსი
- 2014 - აკადემიის კურსანტებს „იუნკრები“ ეწოდათ

უმაღლესი განათლება აკადემიაში

- საბაკალავრო და სამაგისტრო პროგრამები (ინფორმატიკა, მენეჯმენტი, თავდაცვა და უსაფრთხოება)
- უცხო ენების გაძლიერებული სწავლება
- ინტენსიური სასწავლო-სამეცნიერო კავშირები უცხოეთის ანალოგიური პროფილის სასწავლებლებთან
- სასწავლო პროცესში ინფორმაციული უსაფრთხოების თემატიკაზე განსაკუთრებული ყურადღების გამახვილება (ქსელების ადმინისტრირების საფუძვლები, კიბერუსაფრთხოება, საინფორმაციო ომი)
- განვითარებული სასწავლო ქსელური ინფრასტრუქტურა (Cisco-ს ლაბორატორია)

ღონისძიების პროგრამა

- პირადი თუ ორგანიზაციის ინფორმაციული ინფრასტრუქტურა როგორც „აღყაშემოტყმული ციხესიმაგრე“. პოტენციური მეტოქე - მთლიანი ინტერნეტ-სივრცე და არა მარტო...
- კიბერუსაფრთხოების უზრუნველყოფის ყველა ასპექტი - ელემენტარული კიბერჰიგიენიდან დიდი ინფორმაციული ინფრასტრუქტურის მრავალდონიან თავდაცვის სისტემამდე

ღონისძიების დეტალური პროგრამა

- გლობალურ საინფორმაციო სივრცეში განთავსებული ინფორმაცია, მასთან მიმართვის უფლებები და ვალდებულებები. სამართლებრივი 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

ღონისძიების დეტალური პროგრამა

- 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

ლონისძიების დეტალური პროგრამა

- 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

ღონისძიების გრაფიკი

- **14.04** - ღონისძიების მონაწილეთა მიღება და განთავსება სასტუმროში
- **15.04** - სეზონული სკოლის გახსნა
- **15.04– 19.04** - პლენარული სესიები
- **19.04** - შემაჯამებელი კონფერენცია და სეზონური სკოლის დახურვა

სეზონური სკოლის შემდეგ...

- კიბერუსაფრთხოების თემაზე მომუშავე მეცნიერთა და სპეციალისტთა უწყვეტად გაფართოებადი თანამეგობრობის ჩამოყალიბება ინფორმაციის და ცოდნის გაცვლისთვის
- საკონტაქტო პლატფორმების (ფორუმების) შექმნა სოციალურ ქსელ ფეისბუქში და სეზონური სკოლის ვებ-გვერდზე



ღონისძიების განმახორციელებელი პერსონალი

სახელი, გვარი	ორგანიზაცია	თანამდებობა
ნანი არაბული	ეროვნული თავდაცვის აკადემია	ასოცირებული პროფესორი
დავით გულუა	ეროვნული თავდაცვის აკადემია	ასოცირებული პროფესორი
ჩეზარ ვასილესკუ	თავდაცვის რესურსების მართვის რეგიონალური დეპარტამენტი (DRESMARA), რუმინეთი	პროფესორი
ანდრია გოცირიძე	ინოვაციებისა და ტექნოლოგიების სააგენტო	ლექტორი
ვლადიმერ ადამია	საქართველოს ტექნიკური უნივერსიტეტი	ასოცირებული პროფესორი
რომეო გალდავა	ეროვნული თავდაცვის აკადემია	ასოცირებული პროფესორი
ომარ აბშილავა	სსიპ კიბერუსაფრთხოების ბიურო, თავდაცვის სამინისტრო	ლექტორი

წინასწარი მოთხოვნები სეზონური სკოლის მონაწილეებისთვის

- უმაღლესი საგანმანათლებლო დაწესებულების შტატიან ან მოწვეულ პედაგოგებს უნდა გააჩნდეთ სამეცნიერო ხარისხი (დოქტორი ან დოქტორთან გათანაბრებული)
- საქართველოს უმაღლესი საგანმანათლებლო დაწესებულებების მაგისტრანტებს და დოქტორანტებს სპეციალიზაციად არჩეული უნდა ჰქონდეთ კიბერუსაფრთხოების კვლევის და ანალიზის მეთოდები ან რომელიმე მომიჯნავე მიმართულება
- კვლევითი ან სხვა ტიპის, კერძო, არასამთავრობო თუ სამთავრობო ორგანიზაციების წარმომადგენლებს უნდა გააჩნდეთ კიბერუსაფრთხოების სფეროში საკმარისი წინასწარი კომპეტენცია და პრაქტიკული მუშაობის გამოცდილება

შესარჩევი პროცედურები

- პირველი ეტაპი - ინფორმაციის გავრცელება
 - საინფორმაციო ვიზიტები საქართველოს რეგიონებში (თელავი, გორი, ახალციხე, ბათუმი, ზუგდიდი, ქუთაისი)
 - ვებ-გვერდი პროექტის შესახებ ამომწურავი ინფორმაციით Cybergeorgia.ge
- მეორე ეტაპი (01.03 – 15.03) - მონაწილეთა რეგისტრაცია კონკურსისთვის
 - ინფორმაცია კონკურსის შესახებ დასაქმების საჯარო ვებ-გვერდებზე (jobs.ge, hr.ge, hr.ge)
 - განაცხადის გაკეთება სეზონური სკოლის ვებ-გვერდზე Cybergeorgia.ge შემდეგი ასატვირთი დოკუმენტების თანხლებით:
 - სამოტივაციო წერილი (MS WORD ან PDF-ფორმატის ფაილში)
 - ავტობიოგრაფია (CV) ქართულ ენაზე (MS WORD ან PDF-ფორმატის ფაილში)

შესარჩევი პროცედურები (გაგრძ.)

- მესამე ეტაპი (15.03 – 25.03) - ტესტირება გაფილტრული სიის („შორტ-ლისტის“) შედგენა
ტესტირება კიბეუსაფრთხოების საბაზო კომპეტენციებზე
- მეოთხე ეტაპი (25.03 – 31.03) - ზეპირი გასაუბრება კანდიდატებთან
საჭიროების შემთხვევაში კომუნიკაცია განხორციელდება მყისიერ შეტყობინებათა რომელიმე საიმედო სერვისით (სკაიპი, ვაიბერი, მესენჯერი)

გასაუბრების შედეგად შეიქმნება სეზონური სკოლის მონაწილეთა საბოლოო, 15-კაციანი სია

გმადლობთ ყურადღებისთვის!

