ინფორმატიკისა და ინჟინერიის სკოლა
კიბერ და ინფორმაციული უსაფრთხოება
სამაგისტრო პროგრამა

კ უ რ ი კ უ ლ უ მ ი
საგანმანათლებლო პროგრამის სახელწოდება
კიბერ და ინფორმაციული უსაფრთხოება / Cyber and Information Security
უმაღლესი აკადემიური განათლების საფეხური
მაგისტრატურა
მისანიჭებელი კვალიფიკაცია
კიბერუსაფრთხოების მაგისტრი /Master of Cybersecurity
პროგრამის ხელმძღვანელი
პროგრამის ხელმძღვანელები - ანასტასია ბაჯიაშვილი, აკაკი შეყელაძე დაწვრილებითი ინფორმაცია პროგრამის ხელმძღვანელების კვალიფიკაციისა და სამეცნიერო-პედაგოგიურ მოღვაწეობის შესახებ, მოცემულია თანდართულ ფაილებში.
პროგრამის მოცულობა
სამაგისტრო პროგრამა აგებულია ECTS სისტემის საფუძველზე. კვალიფიკაციის მისაღებად, სამაგისტრო საგანმანათლებლო პროგრამის ფარგლებში მაგისტრანტმა უნდა დააგროვოს - 120 კრედიტი, რომელიც შეადგენს პროგრამაში შემავალი ძირითადი სწავლის სფეროს შესაბამისი შინაარსის სავალდებულო და არჩევითი სასწავლო კომპონენტებისა და თავისუფალი კომპონენტების კრედიტების ჯამს. სასწავლო კომპონენტები წარმოდგენილია 120 კრედიტის მოცულობით, მათ შორის: – ძირითადი სწავლის სფეროს სავალდებულო კომპონენტები - 75 კრედიტი; – ძირითადი სწავლის სფეროს არჩევითი კომპონენტები - 25 კრედიტი; – კვლევითი კომპონენტი - 20 კრედიტი. წლის განმავლობაში სტუდენტი აგროვებს 60 კრედიტს, ე. ი სემესტრში 30 კრედიტს, თუმცა სტუდენტის ინდივიდუალური დატვირთვიდან გამომდინარე წელიწადში კრედიტების რაოდენობა შეიძლება იყოს 60 კრედიტზე ნაკლები ან მეტი, მაგრამ არაუმეტეს 75 კრედიტისა. პროგრამა ითვალისწინებს 10 თავისუფალ კრედიტს, რომლის დაგროვებაც არჩევითი კურსებისთვის განკუთვნილი კრედიტების ფარგლებში, სტუდენტს შეუძლია როგორც წინამდებარე პროგრამის ფარგლებში, ისე ინფორმატიკისა და ინჟინერიის სკოლაში ან ქართულ-ამერიკულ უნივერსიტეტში არსებული სხვა იმავე საფეხურის აკადემიური საგანმანათლებლო პროგრამიდან; საქართველოს სხვა უმაღლეს საგანმანათლებლო დაწესებულებაში არსებული აკრედიტებული იმავე საფეხურის აკადემიური საგანმანათლებლო პროგრამიდან; უცხოეთის უმაღლეს სასწავლებელში არსებული იმავე საფეხურის აკადემიური

საგანმანათლებლო პროგრამიდან, თუ ეს კრედიტები აღიარებული იქნება საქართველოს კანონმდებლობის შესაბამისად.

სწავლების ენა

ინგლისური

პროგრამის მიზანი

სამაგისტრო პროგრამის მიზანია:

მოამზადოს თანამედროვე მოთხოვნების შესაბამისი, მაღალი პასუხისმგებლობის მქონე სპეციალისტი, რომელიც:

1. აღწერს ICTs-ში კიბერუსაფრთხოების მიმართულებით ძირითად კონცეფციებს, თეორიებს, მეთოდებს, ასევე ამ სფეროში გამოყენებულ ინსტრუმენტებს, ტექნოლოგიურ გადაწყვეტილებებსა და საერთაშორისო პრაქტიკებს;
2. ინფორმაციის ანალიზის, სინთეზისა და შეფასების საფუძველზე შეძლებს ICTs-ში კიბერუსაფრთხოების მიმართულებით საქმიანობის პრაქტიკულად წარმართვას, მათ შორის, ინფორმაციული უსაფრთხოების მდგრადობის შენარჩუნებას, კიბერ-რისკების იდენტიფიცირებას, რესურსების ეფექტურ დაგეგმვასა და მართვას მულდტისიტსიპლინურ კონტექსტში;
3. დამოუკიდებლად შეძლებს ICTs-ში კიბერუსაფრთხოების მიმართულებით სამეცნიერო-კვლევითი საქმიანობის განხორციელებას დარგის შესაბამისი კვლევის მეთოდების გამოყენებით, არგუმენტირებულად და აკადემიური კეთილსინდისიერებისა და ეთიკური ნორმების დაცვით იმსჯელებს საზოგადოების წინაშე; შეაფასებს საკუთარი და გუნდის პროფესიული განვითარების საჭიროებებს და წვლილს შეიტანს დარგის განვითარებაში;
4. ICTs-ში კიბერუსაფრთხოების მიმართულებით პრობლემების გადაჭრისას, იღებს დამოუკიდებელ გადაწყვეტილებებს ინფორმაციის კონფიდენციალობის, მთლიანობისა და ხელმისაწვდომობის პრინციპების გათვალისწინებით;

პროგრამაზე დაშვების წინა პირობა

სამაგისტრო პროგრამა განკუთვნილია იმ პირთათვის, რომლებსაც უკვე მიღებული აქვთ უმაღლესი განათლება შესაბამის დარგში ინფორმაციისა და კომუნიკაციის ტექნოლოგიების (ICTs) მიმართულებით და სურთ გაიღრმავონ ცოდნა კიბერ და ინფორმაციული უსაფრთხოების მიმართულებით.

შესაბამისად, სამაგისტრო პროგრამაზე ჩარიცხვის აუცილებელ წინაპირობას წარმოადგენს :

- ბაკალავრის ან მასთან გათანაბრებული აკადემიური ხარისხი;
- საერთო სამაგისტრო გამოცდების წარმატებით ჩაბარება;
- შიდა საუნივერსიტეტო პროცედურის გავლა, რომელიც შედგება შემდეგი ეტაპებისაგან:
    - **I.** დოკუმენტაციის ანალიზი - ამ ეტაპზე ხდება უნივერსიტეტის მიერ შემუშავებული საერთო სააპლიკაციო ფორმის შევსება, რომელიც მოიცავს აპლიკანტის პროფესიული ბიოგრაფიის შეფასებას;
    - **II.** გამოცდის ჩაბარება ინგლისურ ენაში (B2 დონე) - გამოცდიდან განთავისუფლდებიან ის აპლიკანტები, რომლებიც წარმოადგენენ შესაბამისი კვალიფიკაციის დამადასტურებელ სერთიფიკატს (TOEFEL, IELTS) ან ბაკალავრის ან შემდგომი საფეხურის საგანმანათლებლო პროგრამა დასრულებული აქვთ ინგლისურ ენაზე;
    - **III.** გასაუბრება/გამოცდა სპეციალობაში* - რომლის მიზანია შეფასდეს აპლიკანტის ცოდნა ინფორმაციული ტექნოლოგიების სფეროში.

უცხო ქვეყნის მოქალაქეები პროგრამაზე მიიღებიან საერთო სამაგისტრო გამოცდების გარეშე, კანონმდებლობით დადგენილი წესით.

***** საგამოცდო საკითხები სპეციალობაში წინასწარ განთავსდება უნივერსიტეტის ვებ-გვერდზე.

დასაქმების სფერო

მაგისტრს შეუძლია წარმატებით დასაქმდეს ყველა იმ ადგილობრივ ან საერთაშორისო ორგანიზაციაში, რომელთა საქმიანობა მოიცავს კიბერ და ინფორმაციული უსაფრთხოების უზრუნველყოფასა და მართვას

კიბერუსაფრთხოების მაგისტრი შეიძლება დასაქმდეს შემდეგ პოზიციებზე:

- კიბერუსაფრთხოების ანალიტიკოსი
- ინფორმაციული უსაფრთხოების მენეჯერი
- ქსელური უსაფრთხოების ინჟინერი
- მონაცემთა დაცვის ოფიცერი (DPO)
- უსაფრთხოების აუდიტორი
- ეთიკური ჰაკერი
- უსაფრთხოების კონსულტანტი
- უსაფრთხოების პროგრამული უზრუნველყოფის არქიტექტორი
- და სხვა.

სწავლის გაგრძელების შესაძლებლობა

ინფორმაციული ტექნოლოგიების მმართველობისა და სტრატეგიის სამაგისტრო პროგრამის კურსდამთავრებული უფლებამოსილია, სწავლა განაგრძოს საქართველოს ან სხვა ქვეყნის უმაღლეს საგანმანათლებლო დაწესებულებაში სადოქტორო პროგრამაზე, თუ ამ პროგრამაზე მიღების წინაპირობა არ არის შეზღუდული სხვა სპეციალობის მაგისტრის აკადემიური ხარისხით.

სწავლის შედეგები

პროგრამის დასრულების შემდეგ მაგისტრი:

1. სიღრმისეულად აღწერს და განმარტავს ICTs-ში კიბერუსაფრთხოების უზრუნველსაყოფად საჭირო კონცეფციებს, თეორიებს, მეთოდებს, ინსტრუმენტებს, ტექნიკებსა და საერთაშორისო პრაქტიკებს; თვალს ადევნებს დარგის განვითარების ტენდენციებს მათი პრაქტიკაში დანერგვის მიზნით;
2. შეიმუშავებს ICTs-ში კიბერუსაფრთხოების მიმართულებით სტრატეგიული და ოპერაციული მართვის დოკუმენტებს, ახდენს ინფორმაციული უსაფრთხოების მართვის სისტემის გამოწვევების იდენტიფიცირებას და მაღალი რგოლის მენეჯმენტთან კომუნიკაციას;
3. ICTs-ში კიბერუსაფრთხოების მდგრადობის უზრუნველსაყოფად, რისკ-ფაქტორების გათვალისწინებით და რესურსების (ინფორმაციული, ადამიანური, მატერიალური, ფინანსური და ა.შ) ეფექტიანი გამოყენებით, შეიმუშავებს ტექნოლოგიურ გადაწყვეტილებებს, განსაზღვრავს მათი რეალიზაციის, მონიტორინგისა და შეფასების მექანიზმებს, აყალიბებს სამუშაო გუნდს და კოორდინაციას უწევს მას;
4. აკადემიური კეთილსინდისიერების დაცვით, დამოუკიდებლად ახორციელებს კვლევას ICTs-ში კიბერუსაფრთხოების მიმართულებით, მსჯელობს და არგუმენტირებულ დასკვნებს წარუდგენს როგორც აკადემიურ, ისე პროფესიულ საზოგადოებას და შეაქვს წვლილი დარგის განვითარებაში, ითვალისწინებს რა მულტიდისციპლინურ კონტექსტს;
5. ICTs-ში კიბერუსაფრთხოების მიმართულებით პრობლემების გადაჭრისას იღებს დამოუკიდებელ გადაწყვეტილებებს, ინფორმაციის კონფიდენციალობის, მთლიანობისა და ხელმისაწვდომობის პრინციპების, ასევე, ეთიკური და პროფესიული ქცევის ნორმების გათვალისწინებით;
6. აფასებს და განსაზღვრავს საკუთარი და გუნდის წევრების პროფესიული ზრდის საჭიროებებს.

სწავლება-სწავლის მეთოდები და შესაბამისი აქტივობები

- ლექცია,
- სემინარი (ჯგუფში მუშაობა),
- პრაქტიკული მუშაობა,
- საშინაო დავალება /რეფერატი;
- ელექტრონული რესურსით სწავლება,
- სამაგისტრო ნაშრომი და სხვა.

აკადემიური და მოწვეული პერსონალი შესაძლოა იყენებდეს ზემოთ ჩამოთვლილ ერთ ან რამდენიმე მეთოდს ან ნებისმიერ სხვა მეთოდს კონკრეტული სასწავლო კურსის ამოცანიდან გამომდინარე. კონკრეტული სასწავლო კურსის სწავლება-სწავლის მეთოდები ასახულია შესაბამისი სასწავლო კურსის სილაბუსში*.

*სილაბუსებში გათვალისწინებულია საკონსულტაციო დრო, რომელიც ყოველის სემესტრის დასაწყისში ინდივიდუალურად შეთანხმდება თითოეულ პედაგოგთან პროგრამის ხელმძღვანელის მიერ და ეცნობება სტუდენტებს.

შეფასების სისტემა

სტუდენტის მიერ შესაბამის სასწავლო კომპონენტში კრედიტების მიღება/დაგროვება სწავლების პროცესში აქტიურ მონაწილეობას ითვალისწინებს და შეძენილი ცოდნის უწყვეტი შეფასების პრინციპს ეფუძნება. სწავლის შედეგების მიღწევის დონე ფასდება „უმაღლესი საგანმანათლებლო პროგრამების კრედიტებით გაანგარიშების წესის შესახებ“ საქართველოს განათლებისა და მეცნიერების მინისტრის 2007 წლის 5 იანვრის№3 ბრძანებით დამტკიცებული შეფასების სისტემის თანახმად.

სწავლის შედეგების მიღწევის დონის შეფასება მოიცავს შეფასების ფორმებს - შუალედურ და დასკვნით შეფასებას, რომელთა ჯამი წარმოადგენს საბოლოო შეფასებას - 100 ქულას.

შეფასების ფორმები მოიცავს შეფასების კომპონენტს/კომპონენტებს, რომელიც განსაზღვრავს სტუდენტის ცოდნა/გაცნობიერების ან/და უნარის ან/და ავტონომიურობა/პასუხისმგებლობის შეფასების ხერხს (ზეპირი/წერითი გამოცდა, ზეპირი/წერითი გამოკითხვა, პრაქტიკული/თეორიული სამუშაო, საშინაო დავალება და სხვა.). შეფასების კომპონენტები აერთიანებს შეფასების მეთოდებს (ტესტი, პრეზენტაცია და სხვა). შეფასების მეთოდი იზომება შეფასების კრიტერიუმებით.

შეფასების თითოეულ ფორმას და კომპონენტს შეფასების საერთო ქულიდან (100) განსაზღვრული აქვს ხვედრითი წილი, რაც აისახება კონკრეტულ სილაბუსში.

შეფასების თითოეულ ფორმას აქვს მინიმალური კომპეტენციის ზღვარი - შუალედური შეფასებისთვის მინიმუმ 25 ქულა, დასკვნითი შეფასებისთვის მინიმუმ 16 ქულა.

მინიმალური კომპეტენციის ზღვარი შეიძლება დადგინდეს შეფასების კომპონენტის/კომპონენტებისთვისაც, რაც დაწვრილებით გაიწერება სასწავლო კურსის სილაბუსით.

დაუშვებელია კრედიტის მინიჭება შეფასების მხოლოდ ერთი ფორმის გამოყენებით. სტუდენტს კრედიტი ენიჭება დადებითი შეფასების მინიჭების შემთხვევაში.

პროგრამის სასწავლო კომპონენტის შეფასების სისტემა:

შეფასების სისტემა უშვებს:
ა) ხუთი სახის დადებით შეფასებას:

ა.ა) (A) ფრიადი – 91-100 ქულა;
ა.ბ) (B) ძალიან კარგი – 81-90 ქულა;
ა.გ) (C) კარგი – 71-80 ქულა;
ა.დ) (D) დამაკმაყოფილებელი – 61-70 ქულა;
ა.ე) (E) საკმარისი – 51-60 ქულა.

ბ) ორი სახის უარყოფით შეფასებას:
ბ.ა) (FX) ვერ ჩააბარა – 41-50 ქულა, რაც ნიშნავს, რომ სტუდენტს ჩასაბარებლად მეტი მუშაობა სჭირდება და ეძლევა დამოუკიდებელი მუშაობით დამატებით გამოცდაზე ერთხელ გასვლის უფლება;
ბ.ბ) (F) ჩაიჭრა – 40 ქულა და ნაკლები, რაც ნიშნავს, რომ სტუდენტის მიერ ჩატარებული სამუშაო არ არის საკმარისი და მას სასწავლო კურსი/საგანი ახლიდან აქვს შესასწავლი.

სტუდენტის საბოლოო რეიტინგის დასადგენად და მათ წასახალისებლად სასწავლო პროცესის დასრულებისას გამოითვლება კუმულატიური ქულა (GPA). კუმულატიური ქულის გამოთვლა შემდეგნაირად ხორციელდება: ყოველ სასწავლო კურსში სტუდენტის მიერ მიღებული ქულის რაოდენობრივი მაჩვენებელი მრავლდება ამ სასწავლო კურსისათვის განკუთვნილი კრედიტის რაოდენობაზე და შემდეგ ამ რიცხვების საერთო ჯამი იყოფა სტუდენტის მიერ დაგროვილი კრედიტების რაოდენობაზე.

სამაგისტრო საგანმანათლებლო პროგრამის კვლევითი კომპონენტი (სამაგისტრო ნაშრომის შესრულება და დაცვა) უნდა შეფასდეს იმავე ან მომდევნო სემესტრში, რომელშიც სტუდენტი დაასრულებს მასზე მუშაობას. კვლევითი კომპონენტი, მოიცავს კვლევით და პრაქტიკულ ასპექტებს, აღნიშნული კომპონენტი სრულდება ინფორმაციული ტექნოლოგიების დარგში და ფასდება ერთჯერადად (დასკვნითი შეფასებით).

პროგრამის განსახორციელებლად მისაღწევი რესურსები

მატერიალური რესურსი:

- კანონმდებლობით გათვალისწინებული ფართი (სასწავლო და დამხმარე);
- სათანადო ინვენტარით აღჭურვილი აუდიტორიები, საკონფერენციო დარბაზები, აკადემიური პერსონალის სამუშაო ოთახები, ადმინისტრაციის მუშაობისათვის განკუთვნილი ფართი;
- ელექტროენერგიის მიწოდების უწყვეტი სისტემა;
- სველი წერტილები;
- ბუნებრივი განათება;
- გათბობის საშუალებები;
- ხანძარსაწინააღმდეგო უსაფრთხოების უზრუნველყოფის მექანიზმები და ხანძარსაწინააღმდეგო ინვენტარი;
- ევაკუაციის გეგმა;
- სამედიცინო დახმარების მექანიზმები (სამედიცინო კაბინეტი);
- წესრიგის დაცვის უზრუნველყოფის მექანიზმები (უნივერსიტეტის დაცვა);
- კომპიუტერთა სათანადო რაოდენობა და ინტერნეტით სარგებლობის შესაძლებლობა;
- საგანმანათლებლო პროგრამის შესაბამისი სახელმძღვანელოებითა და თანამედროვე საინფორმაციო–საკომუნიკაციო ტექნოლოგიებით აღჭურვილი ბიბლიოთეკა;

ადამიანური რესურსი:

- აკადემიური პერსონალი შერჩეული საქართველოს კანონმდებლობის შესაბამისად და მათი კვალიფიკაციის გათვალისწინებით.
- მკვლევარებად და მასწავლებლებად უნივერსიტეტში მოწვეულნი არიან შესაბამისი კვალიფიკაციის მქონე პრაქტიკოსი მუშაკები და სამეცნიერო ხარისხის მქონე პირები.

სამაგისტრო პროგრამის მიზნებისა და შედეგების რუქა
Master's Program Goals and Outcomes Map

მიზნები/შედეგები Goals/Outcomes	შედეგი Outcome 1	შედეგი Outcome 2	შედეგი Outcome 3	შედეგი Outcome 4	შედეგი Outcome 5	შედეგი Outcome 6
1. მოამზადოს თანამედროვე მოთხოვნების შესაბამისი, მაღალი პასუხისმგებლობის მქონე სპეციალისტი, რომელიც აღწერს ICTs-ში კიბერუსაფრთხოების მიმართულებით ძირითად კონცეფციებს, თეორიებს, მეთოდებს, ასევე ამ სფეროში გამოყენებულ ინსტრუმენტებს, ტექნოლოგიურ გადაწყვეტილებებსა და საერთაშორისო პრაქტიკებს; 1. To prepare a highly responsible specialist aligned with modern requirements, who describes the fundamental concepts, theories, methods, and tools in cybersecurity within ICTs, as well as technological solutions and international practices used in the field;	x					x
2. მოამზადოს თანამედროვე მოთხოვნების შესაბამისი, მაღალი პასუხისმგებლობის მქონე სპეციალისტი, რომელიც ინფორმაციის ანალიზის, სინთეზისა და შეფასების საფუძველზე შეძლებს ICTs-ში კიბერუსაფრთხოების მიმართულებით საქმიანობის პრაქტიკულად წარმართვას, მათ შორის, ინფორმაციული უსაფრთხოების მდგრადობის შენარჩუნებას, კიბერ-რისკების იდენტიფიცირებას, რესურსების ეფექტურ დაგეგმვასა და მართვას მულდტისიტსიპლინურ კონტექსტში; 2. To prepare a highly responsible specialist aligned with modern requirements, who based on the analysis, synthesis, and evaluation of information, is capable of practically conducting activities in the field of cybersecurity within ICTs — including maintaining the resilience of information security, identifying cyber risks, and effectively planning and managing resources in a multidisciplinary context;	x	x	x			
3. მოამზადოს თანამედროვე მოთხოვნების შესაბამისი, მაღალი პასუხისმგებლობის მქონე სპეციალისტი, რომელიც დამოუკიდებლად შეძლებს ICTs-ში კიბერუსაფრთხოების მიმართულებით სამეცნიერო-კვლევითი საქმიანობის განხორციელებას დარგის შესაბამისი კვლევის მეთოდების გამოყენებით, არგუმენტირებულად და აკადემიური კეთილსინდისიერებისა და ეთიკური ნორმების დაცვით იმსჯელებს საზოგადოების წინაშე; შეაფასებს საკუთარი და გუნდის პროფესიული განვითარების საჭიროებებს და წვლილს შეიტანს დარგის განვითარებაში; 3. To prepare a highly responsible specialist aligned with modern requirements, who independently conducts scientific-research activities in the field of cybersecurity within ICTs using relevant research methods, and engages in public discourse with reasoned arguments while upholding academic integrity and ethical norms; evaluates the professional development needs of themselves and their teams and contributes to the development of the field;	x			x	x	x
4. მოამზადოს თანამედროვე მოთხოვნების შესაბამისი, მაღალი პასუხისმგებლობის მქონე სპეციალისტი, რომელიც ICTs-ში კიბერუსაფრთხოების მიმართულებით პრობლემების გადაჭრისას, იღებს დამოუკიდებელ გადაწყვეტილებებს ინფორმაციის კონფიდენციალობის, მთლიანობისა და ხელმისაწვდომობის პრინციპების გათვალისწინებით; 4. To prepare a highly responsible specialist aligned with modern requirements, who makes independent decisions in addressing problems in cybersecurity within ICTs, based on the principles of confidentiality, integrity, and availability.			x		x	

სამაგისტრო პროგრამის შედეგების მიღწევის უზრუნველსაყოფად, წარმოადგენილია თითოეული სავალდებულო საგანის თანაკვეთა სწავლის კონკრეტულ შედეგ(ებ)თან, შესაბამისი დონის აღნიშვნით.

საგნები ჩაშლილია სამ დონედ:

ა) გაცნობაზე ორიენტირებული (I-Introduction)

ბ) გაღრმავებაზე ორიენტირებული (D -Development)

გ) განმტკიცებაზე ორიენტირებული (M - Mastering).

საგნისა და შედეგის თანაკვეთის უჯრაში მითითებულია ერთ-ერთი დონის აღმნიშვნელი ინდიკატორი - I, D ან M.

#	Core Components ძირითადი სასწავლო კომპონენტები	შედეგი Outcome 1	შედეგი Outcome 2	შედეგი Outcome 3	შედეგი Outcome 4	შედეგი Outcome 5	შედეგი Outcome 6
I სემესტრი/ Semester							
1	Network Defense/ ქსელის უსაფრთხოება	I		I			
2	Operation System Security/ ოპერაციული სისტემის უსაფრთხოება	I		I		I	
3	Digital Project Management/ ციფრული პროექტების მართვა		I	I	I		I
4	Principles of Cyber Security/ კიბერუსაფრთხოების პრინციპები	I				I	
5	Math in Cybersecurity/ მატემატიკა კიბერუსაფრთხოებაში	I			I		
II სემესტრი/ Semester							
6	Management Systems and Operational Risks/ მართვის სტანდარტები და ოპერაციული რისკები		I	I		I	
7	DevSecOps/დევსეკოპსი		I	I			D
8	Cloud and AI Security Practices/ ღრუბლოვანი და ხელოვნური ინტელექტის უსაფრთხოების პრაქტიკები	I	I		I		
9	Ethical Hacking and Penetration Testing/ ეთიკური ჰაკინგი და შეღწევადობის ტესტირება	I	I			D	
10	Algorithms and Data Structures / ალგორითმები და მონაცემთა სტრუქტურები		I	I			
III სემესტრი/ Semester							
11	Threat Hunting and Cyber Threat Intelligence/ კიბერ საფრთხეების ანალიტიკა	I	I				
12	Security Operations / უსაფრთხოების ოპერაციები	D		D	D		
13	Incident Response and Digital Forensics/ ინციდენტებზე რეაგირება და ციფრული ექსპერტიზა		D	M	M		D
14	Python in Cybersecurity/ პითონი კიბერუსაფრთხოებაში	D	D				
IV სემესტრი/ Semester							
15	Cybersecurity Law and Compliance/ კიბერ სამართალი და შესაბამისობა		M	M	M		M
16	Master Thesis / სამაგისტრო ნაშრომი	M	M	M	M	M	M

დანართი-1: პროგრამის სასწავლო გეგმა
დანართი-2: პროგრამის ხელმძღვანელების CV-ები