კავკასიის უნივერსიტეტი
კავკასიის ტექნოლოგიების სკოლა

სილაბუსი

სასწავლო კურსის დასახელება	კომპიუტერული უსაფრთხოება							
სასწავლო კურსის კოდი	C	T	C	2	2	4	4	
სასწავლო კურსის ანოტაცია	კომპიუტერული/კიბერ უსაფრთხოების ძირითადი პრინციპები, მათი მიმოხილვა და კონფიგურაცია – კურსი მოიცავს კომპიუტერულ უსაფრთხოებას, სხვადასხვა ოპერაციული სისტემის გამოყენებით და განსხვავებული მიმართულებებით (ოპერაციული სისტემის, ქსელის და მომხმარებლის კუთხიდან). განხილულია კიბერ შეტევების, ინციდენტების და მუქარების ტიპები, მათი იდენტიფიცირება და შესაბამისი ტექნიკური საშუალებებით კომპიუტერული უსაფრთხოების უზრუნველყოფა.							
სასწავლო კურსის სტატუსი	☒ სავალდებულო ☐ არჩევითი							
ECTS	5 ECTS კრედიტი							
სკოლა, საფეხური, ჯგუფი, ვისაც ეკითხება სასწავლო კურსი	სკოლა	ტექნოლოგიების სკოლა						
	სწავლის საფეხური	☒ ბაკალავრიატი, ☐ მაგისტრატურა ☐ დოქტორანტურა						
	სწავლების სემესტრი	III						
ლექტორი:	გიორგი გიორგანაშვილი							
სამუშაო ადგილი	კავკასიის უნივერსიტეტი - ტექნოლოგიების სკოლა							
აკადემიური ხარისხი								
აკად. თანამდებობა	მოწვეული ლექტორი							
სამსახურის ტელეფონი								
მობილური ტელეფონი	577 479944							
ელ–ფოსტა	ggiorganashvili@cu.edu.ge							
კონსულტაციის დრო								
სასწავლო კურსის შესწავლის წინაპირობები	კომპიუტერული მოწყობილობების და ფართოდ გავრცელებული პროგრამული უზრუნველყოფის სხვადასხვა პაკეტებთან მუშაობის გამოცდილება (მომხმარებლის დონეზე), ასევე, ოპერაციული სისტემების და კომპიუტერული ქსელების ძირითადი პრინციპების ცოდნა.							
სასწავლო კურსის ფორმატი								
ლექცია/პრაქტიკუმი	22 საათი	11 კვირა, კვირაში 2 ან 3 საკონტაქტო საათი						
სემინარი	4 საათი	4 კვირა, კვირაში 1 საკონტაქტო საათი						
გამოცდა	4 საათი	შუალედური 2 და დასკვნითი გამოცდა 2 საათი						
დამოუკიდებელი მუშაობა	95 საათი	დამოუკიდებელი მუშაობის საათები, მათ შორის შუალედური და საბოლოო შეფასებისათვის, აგრეთვე საშინაო დავალების მომზადებისთვის განკუთვნილი დრო						
სასწავლო კურსის მიზანი	კურსის მიზანია სტუდენტებს შეასწავლოს კომპიუტერული უსაფრთხოების საფუძვლები და ძირითადი პრინციპები.							
სწავლის შედეგი	**ცოდნა და გაცნობიერება** • კომპიუტერული უსაფრთხოების აუცილებლობის ცოდნა; • სხვადასხვა დაცვის მექანიზმების ტექნიკური განხორციელების უნარი სისტემაში; • ფაილების დაცვის განხორციელების და სხვადასხვა ტიპის წვდომის კონტროლის საშუალებების ცოდნა; • ინტერნეტში უსაფრთხო ინფორმაციის მიღება/გაცვლა/დამუშავების განხორციელების საშუალებების ცოდნა; • უსაფრთხოების სხვადასხვა მოდელების ცოდნა; • სისტემაში აუთენტიფიკაციის და ავტორიზაციის მექანიზმების მართვის ცოდნა;							

	• უკაბელო ქსელის უსაფრთხოების ძირითადი პრიციპების და ტექნიკური გადაწყვეტილებების განხორციელების უნარი; **ცოდნის პრაქტიკაში გამოყენების უნარი** • სისტემის უსაფრთხოების სხვადასხვა ტექნიკური საშუალებებით უზრუნველყოფის უნარი; • ფაილების უსაფრთხოების უზრუნველყოფის უნარი; • სისტემაში ინფორმაციის დაშიფრვის საშუალებების ცოდნა; • სხვადასხვა სახის პროტოკოლების უსაფრთხო გამოყენების უნარი; • კიბერ მუქარების და შეტევების იდენტიფიცირების უნარი; • ორგანიზაციის უსაფრთხოების პოლიტიკის გათვალისწინებით, არსებული სიტუაციის ანალიზის შედეგად რისკების მოპყრობის/მართვის და უსაფრთხოების გეგმის შემუშავების უნარი; **დასკვნის გაკეთების უნარი** • სისტემასა და ქსელში მოწყვლადობების აღმოჩენის, უსაფრთხოების შეფასების, კიბერ მუქარების კლასიფიკაციისა და უსაფრთხოებისათვის საჭირო შესაბამისი ძირითადი მექანიზმებისა და საშუალებების განხორციელების უნარი.
სავალდებულო ლიტერატურა	Introduction to Cybersecurity Cybersecurity Essentials CCNA Security ლექტორის მიერ მოწოდებული მასალა, ელექტრონული რესურსები
დამხმარე ლიტერატურა და ინფორმაციის სხვა წყაროები	CEH Certified Ethical Hacker All-in-One Exam Guide ლექტორის მიერ მოწოდებული მასალა ელექტრონული რესურსები
სწავლებისა და სწავლის მეთოდები	▪ ვერბალური, ანუ ზეპირსიტყვიერი მეთოდი; ▪ წიგნზე მუშაობის მეთოდი; ▪ ტესტური მუშაობის მეთოდი; ▪ წერითი მუშაობის მეთოდი; ▪ ლაბორატორიული მეთოდი და დემონსტრირების მეთოდი;
სტუდენტის მიმართ წაყენებული მოთხოვნები	სტუდენტი ვალდებულია: ▪ შეასრულოს სასწავლო კურსით გათვალისწინებული დავალებები; ▪ დაესწროს ლექცია-სემინარებს და პრაქტიკულ მეცადინეობებს; ▪ არ შეუშალოს ხელი სასწავლო პროცესის მიმდინარეობას; ▪ გამოცდების ჩაბარების დროს იხელმძღვანელოს გამოცდების ჩატარების შესახებ უნივერსიტეტში მოქმედი რეგულაციებით; ▪ სემესტრის ბოლოს, შეაფასოს აკადემიური და ადმინისტრაციული პერსონალის მუშაობა; ▪ დაიცვას უნივერსიტეტში დადგენილი სხვა წესები.

ცოდნის შეფასების ფორმები და კრიტერიუმები

გამოკითხვის ფორმა	რაოდენობა	შეფასება	სულ ქულათა რაოდენობა
ტესტირება	4	12	48
შუალედური შეფასება	1	22	22
დასკვნითი გამოცდა	1	30	30
		სულ ჯამი:	100 ქულა

ცოდნისა და უნარ–ჩვევების შეფასების სისტემა

განვლილი პროგრამის ათვისება შეფასებული იქნება 100 ქულიანი სისტემით, რომელიც სასწავლო პროცესში ჩართული კომპონენტების/მეთოდების წილისგან შედგება.

სასწავლო კომპონენტში მაქსიმალური ანუ 100 ქულიდან შუალედური შეფასებების ჯამის ხვედრითი წილი არის 70 ქულა, ხოლო დასკვნითი გამოცდის - 30 ქულა.

შუალედური და დასკვნითი შეფასების ორივე ფორმაში დადგენილია 60%-იანი მინიმალური კომპეტენციის ზღვარი.

სტუდენტმა შუალედურ შეფასებებში ჯამურად უნდა დააგროვოს 70 ქულის 60%, რომ მოიპოვოს დასკვნით გამოცდაზე გასვლის უფლება.

სტუდენტს დასკვნითი გამოცდა ეთვლება ჩაბარებულად, თუ მან მიიღო 30 ქულის 60% ან მეტი. დასკვნით შეფასებაში 60%-ზე ნაკლები ქულის მიღების შემთხვევაში დასკვნითი გამოცდა ჩაბარებულად არ ითვლება.

სწავლის თითოეულ ეტაპზე, სტუდენტს დასკვნით გამოცდაზე ხელახლა გასვლის უფლება ეძლევა მხოლოდ იმ შემთხვევაში, თუ მის მიერ, დასკვნით გამოცდამდე დაგროვილი შუალედური შეფასებების ჯამური ქულა მინიმუმ 41-ის ტოლია.

სტუდენტს დასკვნით გამოცდაზე ხელახლა გასვლის უფლება აქვს ადმინისტრაციის მიერ დადგენილ ვადაში, რომელიც ინიშნება დასკვნითი გამოცდის შედეგების გამოცხადებიდან არანაკლებ 5 დღის ვადაში.

სტუდენტს კრედიტი ენიჭება საბოლოო შეფასების საფუძველზე, რომელიც შედგება შუალედურ და დასკვნით შეფასებებში მიღებული ქულათა ჯამისაგან.

ქვიზი - ტარდება ტესტური სახით და მოიცავს წინა გამოკითხვამდე განვლილ მასალას. ტესტი შეიცავს თეორიულ და პრაქტიკულ საკითხებს და თითოეული ფასდება სირთულის მიხედვით.
შუალედური და დასკვნითი გამოცდა – ტარდება ასევე ტესტური სახით. ტესტი შეიცავს თეორიულ და პრაქტიკულ საკითხებს და თითოეული ფასდება სირთულის მიხედვით.

დახურული ტიპის (მრავლობითი არჩევანით) საკითხი ფასდება:
მაქსიმალურის ქულა - პასუხი სწორია
0 ქულა- პასუხი არასწორია

ღია ტიპის საკითხი ფასდება:
მაქსიმალური ქულა - პასუხი სრულყოფილია.
ნახევარი ქულა - პასუხი არასრულია, ნაკლოვანია.
0 ქულა - პასუხი შესაბამისი არ არის ან საერთოდ არაა მოცემული.

პრაქტიკული საკითხი ფასდება:
მაქსიმალური ქულა - დავალება სრულყოფილად არის შესრულებული.
ნახევარი ქულა - პასუხი არასრულია, ნაკლოვანია, ამოხსნის გზა მცდარია ან შესრულებულია ნაწილობრივ.
0 ქულა - პასუხი დავალების შესაბამისი არ არის ან საერთოდ არაა მოცემული.

შეფასების ინდექსირებული სისტემა და მაჩვენებლები		
შეფასება	**შეფასების შკალა**	**ქულა**
ფრიადი	**A (91% და მეტი)**	**91-100**
ძალიან კარგი	**B (81%-90%)**	**81-90**
კარგი	**C (71%-80%)**	**71-80**
დამაკმაყოფილებელი	**D (61%-70%)**	**61-70**
საკმარისი	**E (51%-60%)**	**51-60**
ვერ ჩააბარა	**FX (41%-50%)**	**41-50**
ჩაიჭრა	**F (40% და ნაკლები)**	**0-40**

აკადემიური კალენდარი			
I	**II**	**III**	**IV**
ლექცია **2 საათი**	ლექცია / პრაქტიკული **2 საათი**	ლექცია / პრაქტიკული ქვიზი **3 საათი**	ლექცია / პრაქტიკული **2 საათი**
V	**VI**	**VII - IX**	**X**
ლექცია / პრაქტიკული ქვიზი **3 საათი**	ლექცია / პრაქტიკული **2 საათი**	**შულედური გამოცდა** **2 საათი.**	ლექცია / პრაქტიკული **2 საათი**
XI	**XII**	**XIII**	**XIV**
ლექცია / პრაქტიკული ქვიზი **3 საათი**	ლექცია / პრაქტიკული **2 საათი**	ლექცია / პრაქტიკული ქვიზი **3 საათი**	ლექცია / პრაქტიკული **2 საათი**
XV-XVII		**XVIII - XIX**	
დასკვნითი გამოცდა **2 საათი.**		დამატებითი გამოცდა	

სასწავლო კურსის შინაარსი

მეცადინეობების კალენდარული გეგმა

მეცადინეობის დრო და ადგილი	დღე:	დაწყება:	დამთავრება:	აუდიტორია:

N	თარიღი	მეცადინეობის თემა, საშინაო დავალება, ლიტერატურა
I		🕮**თემა 1.** **განსახილველი საკითხები:** **კიბერუსაფრთხოების საჭიროება** – პირადი მონაცემები, ორგანიზაციის მონაცემები, დამნაშავეები და კიბერუსაფრთხოების პროფესიონალები, კიბერომი. **კიბერუსაფრთხოება – ექსპერტებისა და დამნაშავეების სამყარო** – კიბერ სამყარო, კიბერ დამნაშავეები კიბერ სპეციალისტების წინააღმდეგ, გავრცელებული საფრთხეები, კიბერ საფრთხეების გავრცელება, მეტი ექსპერტების აღზრდა; **კიბერუსაფრთხოების კუბი** - კიბერუსაფრთხოების კუბის სამი განზომილება, CIA ტრიადა, მონაცემთა მდგომარეობა, კიბერუსაფრთხოების კონტროლისძიებები, IT უსაფრთხოების მართვის სტრუქტურა; **სავალდებულო ლიტერატურა** Introduction to Cybersecurity – Chapter №1 Cybersecurity Essentials - Chapter №1, 2 **დამატებითი ლიტერატურა და სხვა სასწავლო მასალა** CEH Certified Ethical Hacker All-in-One Exam Guide (1-27)
II		🕮**თემა 2.** **განსახილველი საკითხები:** იდენტიფიკაცია, იდენტიფიკაციის კონტროლი: რა ვიცით, რა გვაქვს, ვინ ვართ, აუთენტიკაცია, მრავალფაქტორული აუთენტიკაცია; ავტორიზაცია, ავტორიზაციის გამოყენება; ანგარიშები, ანგარიშვალდებულების განხორციელება; უფლებათა დონეების განსაზღვრა, როლები; პრივილეგირებული სააღრიცხვო ჩანაწერები, მომხმარებლები და ჯგუფები, ჯგუფური პოლიტიკები, უსაფრთხოების ლოკალური პოლიტიკა **სავალდებულო ლიტერატურა** Introduction to Cybersecurity – Chapter №3 Cybersecurity Essentials - Chapter №4.2 CCNA Security – Chapter №2 **დამატებითი ლიტერატურა და სხვა სასწავლო მასალა** CEH Certified Ethical Hacker All-in-One Exam Guide (155-193)
III		🕮**თემა 3.** **განსახილველი საკითხები:** ინფორმაციულ რესურსებზე წვდომების განსაზღვრა და კონტროლი, ფიზიკური წვდომის კონტროლი, ლოგიკური წვდომის კონტროლი, ადმინისტრაციული წვდომის კონტროლი, სავალდებულო (Mandatory) წვდომის კონტროლი, წესებზე დაფუძნებული წვდომის კონტროლი, შემაკავებელი კონტროლი, სამძებრო კონტროლი, მაკორექტირებელი კონტროლი, დისკრეციული წვდომის კონტროლი, პრევენციული კონტროლი, როლებზე დაფუძნებული წვდომის კონტროლი, ფაილზე წვდომის კონტროლი; ინფორმაციულ რესურსებზე უფლებების განსაზღვრა **სავალდებულო ლიტერატურა** Cybersecurity Essentials - Chapter №4.2 CCNA Security – Chapter №3 **დამატებითი ლიტერატურა და სხვა სასწავლო მასალა** CEH Certified Ethical Hacker All-in-One Exam Guide (155-193) **გამოკითხვის ფორმა:** ქვიზი #1 (12 ქულა)
IV		🕮**თემა 4.** **განსახილველი საკითხები:** კრიპტოგრაფიული სისტემები – კრიპტოგრაფიული სერვისები, ბაზისური მთლიანობა და ნამდვილობა, კონფიდენციალობა, კრიპტოგრაფია ღია გასაღებით; კრიპტოგრაფია, მონაცემთა დაფარვა

		სავალდებულო ლიტერატურა
		Cybersecurity Essentials - Chapter №4.1 Cybersecurity Essentials - Chapter №4.3 CCNA Security - Chapter №7
		დამატებითი ლიტერატურა და სხვა სასწავლო მასალა
		CEH Certified Ethical Hacker All-in-One Exam Guide (27-53)
V		🕮**თემა 5.** **განსახილველი საკითხები:** მონაცემთა მთლიანობის კონტროლის ტიპები; მონაცემთა ბაზის მთლიანობის უზრუნველყოფა; ციფრული ხელმოწერები; სერტიფიკატები
		სავალდებულო ლიტერატურა
		Cybersecurity Essentials - Chapter №5
		დამატებითი ლიტერატურა და სხვა სასწავლო მასალა
		CEH Certified Ethical Hacker All-in-One Exam Guide (27-53)
		გამოკითხვის ფორმა: ქვიზი #2 (12 ქულა)
VI		🕮**თემა 6.** **განსახილველი საკითხები:** მავნე პროგრამები და კოდები; გავრცელებული საზიანო პროგრამები (მავნე პროგრამები – ტროიანი, ქსელური ჭია, ვირუსი; სარეკლამო პროგრამა (Adware), ლოგიკური ბომბები, გამომძალველი პროგრამა (Ransomware), „შავი შესასვლელი“ (Backdoor), რუტკიტი, სპამი, შესაშინებელი პროგრამა (Scareware), ჯაშუშური პროგრამები (Spyware, Keylogger); ანტივირუსი: ანტივირუსული პროგრამების ინსტალაცია/კონფიგურაცია; პროგრამული უზრუნველყოფების განახლება, პატჩების მართვა, ანტიჯაშუშური პროგრამული უზრუნველყოფა. სხვა დამაზიანებელ პროგრამებთან საბრძოლველად სხვადასხვა უტილიტების გამოყენება; უსაფრთხოების შესამოწმებელი უტილიტები
		სავალდებულო ლიტერატურა
		Cybersecurity Essentials - Chapter №3.1 Cybersecurity Essentials - Chapter №3.2 ინსტრუქტორის მიერ მოწოდებული პრეზენტაცია, სასწავლო მასალა
		დამატებითი ლიტერატურა და სხვა სასწავლო მასალა
		CEH Certified Ethical Hacker All-in-One Exam Guide (53-85) CEH Certified Ethical Hacker All-in-One Exam Guide (283 - 311)
VII - IX		**შუალედური გამოცდა –** (მაქს. შეფასება 22 ქულა) მთელი განვლილი მასალა
X		🕮**თემა 7.** **განსახილველი საკითხები;** შეტევები, კონცეფციები და ტექნიკები – კიბერთავდასხმების ანალიზი, კიბერუსაფრთხოების ლანდშაფტი გავრცელებული ქსელური საფრთხეები; შეტევები: ფიშინგი, უხეში ძალით შეტევა (Brute Force), კლავიატურის ლოგირება, კოდის დაშორებული შესრულება, ინექცია, სოციალური ინჟინერია; მომსახურებაზე უარის თქმა (DoS), განაწილებული შეტევა მომსახურების დაბლოკვის მიზნით (DDoS), კაცი შუაში (Man-in-the-middle), სნიფინგი, სპუფინგი, SynFlood, ბუფერის გადავსება, ნულოვანი დღის შეტევები).
		სავალდებულო ლიტერატურა
		Introduction to Cybersecurity – Chapter №2 Cybersecurity Essentials - Chapter №3.3 CCNA Security - Chapter №1.2, Chapter №6
		დამატებითი ლიტერატურა და სხვა სასწავლო მასალა
		CEH Certified Ethical Hacker All-in-One Exam Guide (85-121) CEH Certified Ethical Hacker All-in-One Exam Guide (193-219)
XI		🕮**თემა 8.** **განსახილველი საკითხები;** საფრთხეების შესუსტება; ფაიერვოლური ტექნოლოგიების დანერგვა: წვდომის კონტროლის სიები (ACL), ფაიერვოლური ტექნოლოგიები, ზონაზე დაფუძნებული ფაიერვოლის პოლიტიკა. შემოჭრის აღკვეთის განხორციელება: IPS ტექნოლოგიები, IPS

		ხელმოწერები; ვირტუალური დაცული ქსელების დანერგვა: ვირტუალური დაცული ქსელები, IPsec VPN კომპონენტები და ექსპლუატაცია
		სავალდებულო ლიტერატურა
		Introduction to Cybersecurity – Chapter №4 Cybersecurity Essentials - Chapter №7 CCNA Security – Chapter №1.3 CCNA Security – Chapter №1.3, 4 CCNA Security – Chapter №5 CCNA Security – Chapter №8
		დამატებითი ლიტერატურა და სხვა სასწავლო მასალა
		CEH Certified Ethical Hacker All-in-One Exam Guide (121-155)
		გამოკითხვის ფორმა: ქვიზი #3(12 ქულა)
XII		🕮**თემა 9.** **განსახილველი საკითხები;** ვებ-უსაფრთხოება - ვებ-შეტევები: ინექცია, დარღვეული აუთენტიკაცია და სესიის მართვა, საიტთაშორისი სკრიპტინგი, დაუცველი პირდაპირი ობიექტის მიმართვები, არასწორი კონფიგურაცია, მნიშვნელოვანი ინფორმაციის გასაჯაროება, წვდომის კონტროლის არარსებული ფუნქციური დონე, საიტთაშორისი მოთხოვნების გაყალბება (CSRF), ცნობილი სუსტი კომპონენტების გამოყენება, შეუმოწმებელი გადამისამართებები და გადაგზავნები; WAF - ვებ-აპლიკაციის ფაიერვოლი - ნაგულისხმევი პოლიტიკები; ახალი პოლიტიკების შექმნა; ხელწერები (Signatures); მონიტორინგი; ანგარიშის მომზადება (Report); შექმნილი ჩანაწერების (log) ანალიზი და რეაგირება. უსაფრთხოება ბრაუზერებში: დაცული ნავიგაცია, ActiveX ფილტრაცია, SmartScreen ფილტრი, ამოტივტივებადი ფანჯრების დაბლოკვა; ბრაუზერის ინექცია; ActiveX კონტროლები და ჯავა, შემცველობის სკრინინგი & ბლოკირება, აპლიკაციების შეტევებისგან დაცვა, უსაფრთხო ნავიგაცია. უსაფრთხოება ონლაინ გადახდის სისტემებში, უსაფრთხო გადარიცხვები: SSL შიფრაცია, HTTPs-ის განხილვა; ელექტრონული ფოსტების უსაფრთხოება (Gmail, Hotmail);
		სავალდებულო ლიტერატურა
		OWASP – 2017; WEB Application Firewall Manual ინსტრუქტორის მიერ მოწოდებული პრეზენტაცია, სასწავლო მასალა
		დამატებითი ლიტერატურა და სხვა სასწავლო მასალა
		CEH Certified Ethical Hacker All-in-One Exam Guide (219 – 251) CEH Certified Ethical Hacker All-in-One Exam Guide (251 – 283)
XIII		🕮**თემა 10.** **განსახილველი საკითხები;** უსაფრთხოება სოციალურ ქსელებში: ორმაგი ავტორიზაცია, ავტორიზაციის შეტყობინებები, ავტორიზაციის დადასტურება, აპლიკაციების პაროლები, საჯარო გასაღები, სანდო კონტაქტები, დადასტურებული მოწყობილობები, მასალების ნახვის პარამეტრები, არასასურველი კონტაქტების, შეტყობინებების, აპლიკაციების და ღონისძიებების დაბლოკვა; მობილური ტექნოლოგიების უსაფრთხოება, მობილური მოწყობილობების დაცვის მეთოდები: Passcode Locks, სისტემაში შესვლის წარუმატებელი მცდელობების აკრძალვა, დაშორებული სარეზერვო ასლის შექმნა, ლოკაციის აპლიკაციები, დაშორებული ბლოკირება და მონაცემების დაშორებული გაწმენდა, ანტივირუსები, ოპერაციული სისტემების (Android, iOS) პატჩირება და განახლება, შეტევები: არასასურველი პროგრამა (Grayware), SMiShing, GPS თვალთვალი, Inventory & RFID Tags. უსაფრთხოება უკაბელო ქსელებში: ყალბი წვდომის წერტილები, რადიოსიხშირის ჩახშობა, Bluejacking, Bluesnarfing, WEP და WPA/WPA2 შეტევები, ორმხრივი აუთენტიკაცია, RFID და უკაბელო ქსელის თვალთვალი; უსაფრთხოება კაბელურ და უკაბელო მარშრუტიზატორებში (TP-Link, MikroTik – Wireless უსაფრთხოების რეჟიმები (WEP, WPA2), ფაიერვოლი, MAC ფილტრაცია, DMZ, UPnP, პორტის გადამისამართება, Port Triggering, სარეზერვო ასლის შექმნა და აღდგენა, მიკროპროგრამის განახლება)
		სავალდებულო ლიტერატურა

		ინსტრუქტორის მიერ მოწოდებული პრეზენტაცია, სასწავლო მასალა
		დამატებითი ლიტერატურა და სხვა სასწავლო მასალა
		CEH Certified Ethical Hacker All-in-One Exam Guide (251-283)
		გამოკითხვის ფორმა: ქვიზი #4(12 ქულა)
XIV		🕮**თემა 11.** **განსახილველი საკითხები;** რისკების ანალიზი, ბიზნეს უწყვეტობა, აქტივების იდენტიფიკაცია, აქტივების კლასიფიკაცია, აქტივების სტანდარტიზაცია, ბიზნეს უწყვეტობის საუკეთესო გადაწყვეტები; ხელმისაწვდომობა: ხუთი ცხრიანი - 99.999%, ხელმისაწვდომობის საფრთხეები, მაღალი ხელმისაწვდომობის სისტემის შექმნა. სარეზერვო ასლების შექმნა/აღდგენა, Fault Tolerance Drive Systems, სერვერების კლასტერიზაცია, მონაცემთა ბაზების „ჩრდილოვანი“ ასლის შექმნა, RAID მასივები, Redundancy, Spanning Tree, დისკის კლონირება, Deep Freeze; მონაცემთა გაწმენდა/განადგურება. მონაცემთა და ოპერაციული სისტემის სარეზერვო ასლის შექმნა/აღდგენა Acronis პროგრამის საშუალებით; მყარი დისკის კლონირება. Cloud Backup Tools; მონაცემთა გაწმენდა/განადგურება ინფორმაციული უსაფრთხოების სტანდარტები, რეკომენდაციები, პროცედურები და კანონმდებლობის საკითხები; ინფორმაციული უსაფრთხოების პოლიტიკები: უსაფრთხოების პოლიტიკის სტრუქტურა, ტექნიკური პოლიტიკები, როლები და პასუხისმგებლობები, აუდიტი.
		სავალდებულო ლიტერატურა
		Cybersecurity Essentials - Chapter №6 CCNA Security – Chapter №11
		დამატებითი ლიტერატურა და სხვა სასწავლო მასალა
		ინსტრუქტორის მიერ მოწოდებული პრეზენტაცია, სასწავლო მასალა
XV-XVII		**დასკვნითი გამოცდა -** (მაქს. შეფასება 30 ქულა) მთელი სემესტრის განმავლობაში განვლილი მასალა