Co-funded by the European Union

D3.1 MOKYMŲ MODULIAI AUKŠTŲJŲ MOKYKLŲ STUDENTAMS

CYBER AGENT 09.2025

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

Finansuojama Europos Sąjungos lėšomis. Tačiau išreiškiamas požiūris ar nuomonė yra tik autoriaus (-ių) ir nebūtinai atspindi Europos Sąjungos ar Europos švietimo ir kultūros vykdomosios įstaigos (EACEA) požiūrį ar nuomonę. Nei Europos Sąjunga, nei EACEA negali būti laikoma už juos atsakinga..

3 darbo paketas: CyberAgent mokymo(si) išteklių kūrimas

Rezultatas 3.1: Mokymo moduliai aukštojo mokslo įstaigų studentams

3 darbo paketo lyderis – TIMTAL. D3.1 lyderis – VU.

„MVĮ kibernetinio saugumo pokyčių agentai“ projektas remiamas pagal Erasmus+ programą.
“**Erreur ! Utilisez l'onglet Accueil pour appliquer Title au texte que vous souhaitez faire apparaître ici.**”

TURINYS

ĮVADAS

Remiantis D2.2 ataskaitą, MVĮ patiria didelį kvalifikuotų kibernetinio saugumo specialistų trūkumą, o šių organizacijų darbuotojai dažnai neturi sisteminių žinių, reikalingų tinkamai reaguoti į vis sudėtingesnes kibernetines atakas. Dėl to ypač kyla iššūkių, kaip aukštajame moksle parengti specialistus, gebančius pritaikyti savo žinias MVĮ aplinkoje – tiek techninėje, tiek valdymo srityje. Atsižvelgiant į tai, D2.3 dokumente buvo sukurtas mokymosi kelias, išskaidyta į skirtingas temines sritis, orientuotas į praktinių įgūdžių ugdymą ir grįsta kompetencijomis.

Šiame dokumente pateikiamas vienas pagrindinių projekto rezultatų – mokymo moduliai, skirti aukštųjų mokyklų (HEI) studentams (D3.1). Šios veiklos tikslas sukurti aukštojo mokslo institucijoms (HEI) skirtas mokymo programas, apimančias pagrindines kibernetinio saugumo žinių, gebėjimų ir kompetencijų sritis, aktualias mažosioms ir vidutinėms įmonėms (MVĮ).

Šie moduliai yra nuoseklaus darbo rezultatas, paremtas išsamia poreikių analize (D2.2) , kurios metu buvo apklausti MVĮ, profesinio mokymo (VET) ir aukštojo mokslo institucijų atstovai, bei sudarytos rekomendacijos mokymų kibernetinio saugumo programoms (D2.3).

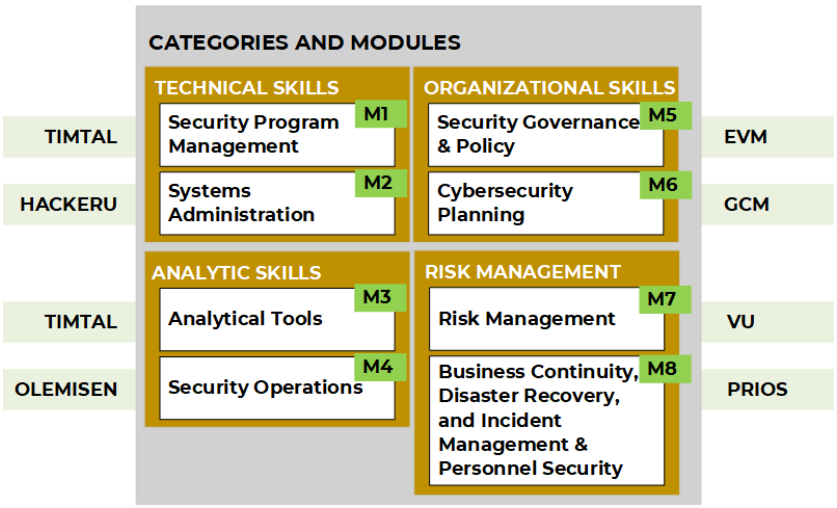
Mokymo programa, atitinkanti Europos kvalifikacijų sąrangos (EQF) 5–6 lygmenis, yra skirta aukštųjų mokyklų studentams ir pažengusiems MVĮ darbuotojams . Ją sudaro aštuoni pagrindiniai ir vienas įkvepiantis modulis, apimantys keturias esmines kompetencijų sritis :

1. **Techniniai įgūdžiai** (Saugumo programų valdymas, Sistemų administravimas).
2. **Analitiniai įgūdžiai** (Analitiniai įrankiai, Saugumo operacijos).
3. **Organizaciniai įgūdžiai** (Saugumo valdymas ir politika, Kibernetinio saugumo planavimas).
4. **Rizikų valdymas** (Rizikos valdymas ir švelninimas, Veiklos tęstinumas, atkūrimas po nelaimių ir incidentų valdymas bei personalo saugumas).

Kiekvienas modulis apima 3 ECTS kreditus (atitinkamai 75 valandų studento darbo krūvį), yra suderintas su Europos aukštojo mokslo erdvės principais bei atitinka D2.3 nurodytas metodines rekomendacijas: įtraukiami aktyvūs mokymo metodai (pvz., atvejų analizė, projektinis mokymasis) bei savarankiškas mokymasis, aiškiai išskiriant mokymosi rezultatus žinių, gebėjimų ir kompetencijų lygmenimis.

Kiekvienas modulis, kurio apimtis yra 3 ECTS kreditai, buvo sukurtas skirtingų konsorciumo partnerių, pasitelkiant jų sritį ir darbo patirtį.

Sukurti moduliai apima šias pagrindines sritis, identifikuotas kaip kritiškai svarbias D2.2 ataskaitoje:



1. M1: SAUGUMO PROGRAMOS VALDYMAS

Modulio pavadinimas	Modulio kodas
SAUGUMO PROGRAMOS VALDYMAS	

Lektorius (-iai)	Institucija ar katedra, kurioje dėstomas modulis

Pateikimo būdas	Kalba
Kontaktiniu būdu, nuotoliniu būdu, mišriuoju būdu	*Anglų, suomių, turkų, norvegų, lietuvių, rumunų, prancūzų, lenkų, ispanų*

Reikalavimai
Nėra

Suteiktų ECTS kreditų skaičius	Studento darbo krūvis	Kontaktinės darbo valandos	Individualios darbo valandos
3	75 val	50 val	25 valandos

Modulio tikslas ir rezultatai		
Baigę šį kursą, studentai įgis įgūdžių, reikalingų veiksmingai valdyti saugumo programas, reaguojant į kibernetinio saugumo grėsmes. Jie išmoks kurti gynybos strategijas nuo dabartinių grėsmių, tokių kaip phishing, ransomware ir DDoS atakos, projektų ir išteklių valdymo sistemose. Be to, studentai išmoks taikyti saugumo rodiklius ir kokybės užtikrinimo metodus, įgydami gebėjimą optimizuoti saugumo programas, efektyviai valdyti išteklius ir stiprinti organizacijos saugumą, naudodami tinkamas priemones prieš besikeičiančias grėsmes. Šis kursas taip pat padės ugdyti jų kompetenciją grėsmių vertinimo, ataskaitų teikimo ir komunikacijos srityse, leidžiant jiems efektyviai įgyvendinti kibernetinio saugumo strategijas savo organizacijose.		
Modulio mokymosi rezultatai	**Mokymo ir mokymosi metodai**	**Vertinimo metodai**
Žinios. Studentai įgyja praktinių žinių apie naujausias kibernetinio saugumo grėsmes, įskaitant phishingą, išpirkos reikalaujančius virusus ir DDoS atakas, bei apie tai, kaip jas valdyti veiksmingai valdant projektus ir išteklius bei įgyvendinant kokybės užtikrinimo ir kontrolės priemones.	Dėstytojas pasirenka mokymo ir mokymosi metodus iš D2.3 ataskaitos 1.3 dalies [Mokymo metodai, pvz., teorinės paskaitos, kviestiniai lektoriai, viktorinos, žaidimai, praktinės užduotys/laboratoriniai darbai, tarpusavio mokymas ir mokymasis, savarankiškas mokymasis ir kt.].	Savitikros testai Žinių vertinimo testas

Įgūdžiai. Studentai įgis įgūdžių naudoti įrankius ir programinę įrangą, skirtą apsaugai nuo besikeičiančių kibernetinių grėsmių, ir taikyti patikimas saugumo praktikas projektų ir išteklių valdyme, siekdami pagerinti bendrus saugumo rodiklius ir kokybės kontrolę savo organizacijose.	Dėstytojas pasirenka mokymo ir mokymosi metodus iš D2.3 ataskaitos 1.3 dalies [Mokymo metodai, pvz., praktinės užduotys/laboratoriniai darbai, praktinės veiklos, imituojamos aplinkos, viktorinos, žaidimai, atvejų analizės ir kt.	Praktiniai vertinimai
Kompetencijos. Studentai gebės įvertinti ir sumažinti potencialias saugumo grėsmes, veiksmingai komunikuoti kibernetinio saugumo klausimus ir tiksliai pranešti apie grėsmes ir pažeidimus per atitinkamus kanalus savo organizacijoje.	Dėstytojas pasirenka mokymo ir mokymosi metodus iš D2.3 ataskaitos 1.3 dalies [Mokymo metodai, pvz., simuliuojamos aplinkos, „vėliavų gaudymo“ varžybos, 5E, CBL, CL, POGIL, PBL ir kt.].	Simuliacijos Konkursai

Modulio turinys: temų suskirstymas	**Kontaktinės darbo valandos**					**Individualios darbo valandos ir užduotys**	
	Paskaitos (HEI)	Konsultacijos	Praktika (HEI)	Testai	**Visi kontaktiniai darbai**	**Individualus darbas**	**Užduotys**
Projektų valdymas • Projekto planavimas • Projekto tikslų nustatymas • Projekto apimties ir reikalavimų apibrėžimas • Projekto tvarkaraščio parengimas • Projekto valdymo priemonės • Dabartinės kibernetinio saugumo grėsmės (DDoS, išpirkos reikalaujanti programinė įranga, kenkėjiška programinė įranga, sukčiavimas elektroniniu paštu, „zero-day“ atakos, IoT atakos ir kt.) • Grėsmių modeliavimas ir pažeidžiamumo analizė • Reagavimo į ekstremalias situacijas ir incidentus planai • Kibernetinio saugumo grėsmių ir incidentų pranešimai	8	0,5	3	0,5	**12**	**6**	• Parengti kibernetinio saugumo sąmoningumo projektą MVĮ darbuotojams. • Nustatykite aiškius kibernetinio saugumo sąmoningumo projekto tikslus, kad MVĮ darbuotojai geriau suprastų galimas saugumo grėsmes. • Apibrėžkite MVĮ darbuotojams skirto kibernetinio saugumo sąmoningumo projekto apimtį ir reikalavimus, įskaitant mokymų temas ir reikalingus išteklius.

							• Parengti MVĮ darbuotojams skirtos kibernetinio saugumo sąmoningumo didinimo projekto įgyvendinimo grafiką. • Naudokite projektų valdymo įrankius, kad stebėtumėte MVĮ darbuotojams skirto kibernetinio saugumo sąmoningumo projekto pažangą ir išteklių naudojimą. • Išnagrinėkite dabartines kibernetinio saugumo grėsmes ir surinkite išvadas į ataskaitą. • Sukurti supaprastintą grėsmių modelį, kuris padėtų MVĮ darbuotojams nustatyti galimas saugumo spragas savo kasdienėje veikloje. • Raskite ir peržiūrėkite avarinių situacijų ir incidentų reagavimo planų pavyzdžius. • Kokie veiksmai turėtų būti apsvarstyti rengiant ataskaitą apie kibernetinio saugumo grėsmes ir incidentus? Atlikite tyrimą ir apibendrinkite.
Išteklių valdymas • Žmogiškųjų išteklių (projektų komandų) valdymas • Informuotumas apie saugumą ir komandos mokymas • Techninės ir programinės įrangos inventoriaus valdymas • Saugumo priemonės ir programinė įranga • Efektyvus technologinių išteklių naudojimas • Biudžetas ir išteklių paskirstymas	8	0,5	3	0,5	**12**	**6**	• Parengti išteklių valdymo strategiją, kad būtų užtikrinamas veiksmingas išteklių naudojimas fiktyvioje MVĮ. • Sukurti pavyzdinį temų planą kibernetinio saugumo sąmoningumo mokymams. • Parengti fiktyvios MVĮ techninės ir programinės įrangos inventorių.

							• Išnagrinėti dažniausiai naudojamas saugumo priemones ir programinę įrangą. • Sukurti hipotetinės MVĮ biudžeto ir išteklių paskirstymo plano pavyzdį.
Saugumo rodikliai • Saugumo metrikos ir matavimo metodai • Duomenų rinkimas naudojant SIEM • Saugumo metrikų analizė • Projekto stebėsena ir veiklos vertinimas • Veiksmų peržiūra ir projekto pritaikymas • Saugumo rodiklių ataskaitos	8	0,5	4	0,5	**13**	**6**	• Išnagrinėti saugumo metrikas, naudojamus MVĮ kibernetinio saugumo būklei vertinti. • Išnagrinėti šaltinius, iš kurių SIEM programinė įranga renka žurnalus. • Įdiegti ir išbandyti atvirojo kodo SIEM programinę įrangą. • Analizuoti saugumo metrikas, renkant žurnalus naudojant SIEM programinę įrangą. • Pateikti saugumo rodiklių analizės rezultatus su grafikais ir vaizdiniais elementais.
Kokybės užtikrinimas ir kokybės kontrolė • Kokybės valdymas • Kibernetinio saugumo kokybės standartai • Atitikties stebėsena ir kokybės auditas • Testavimo ir patvirtinimo metodai • Vertinimo ir tobulinimo rekomendacijos	8	0,5	4	0,5	**13**	**7**	• Planuoti kokybės užtikrinimo ir kokybės kontrolės procesus, kad būtų padidintas kibernetinio saugumo priemonių veiksmingumas MVĮ. Atlikti tyrimą ir apibendrinti. • Išnagrinėti ISO/IEC 27001:2022 standarto A priedo kontrolės elementus. • Išnagrinėti ir pateikti ataskaitą apie tai, kas yra testavimo ir patvirtinimo metodai. • Kokią naudą MVĮ teikia nuolatinis kokybės procesų peržiūrėjimas ir tobulinimas?
Iš viso	**32**	**2**	**14**	**2**	**50**	**25**	

Vertinimo strategija	Lyginamasis svorio procentas	Vertinimo kriterijai
Savitikros testas I	10	10 balų – 95–100 % teisingų atsakymų. 9 balai – 85–94 % teisingų atsakymų. 8 balai – 75–84 % teisingų atsakymų. 7 balai – 65–74 % teisingų atsakymų. 6 balai – 55–64 % teisingų atsakymų. 5 balai – 45–54 % teisingų atsakymų. 4 balai – 35–44 % teisingų atsakymų. 3 balai – 25–34 % teisingų atsakymų. 2 balai – 15–24 % teisingų atsakymų. 1 balas – 0–14 % teisingų atsakymų.
Savitikros testas II	10	
Savitikros testas III	10	
Savitikros testas IV	10	
Žinių vertinimo testas	60	

Studijų medžiaga *(Pavardė, vardo inicialas. (Metai, mėnuo, diena). Straipsnio pavadinimas. Žurnalo/laikraščio pavadinimas, tomo numeris, viso straipsnio puslapių numeriai, leidėjas, URL nuoroda)*
Privaloma literatūra
Rekomenduojama literatūra
https://sansorg.egnyte.com/dl/RFrVIbX2oc **https://edwps.com/wp-content/uploads/2018/04/Cyber-PMO-U.S.-Cyber-Magazine.pdf** **https://healthybyte.net/cybersecurity/what-is-a-security-program-management**

2. M2: SISTEMŲ ADMINISTRAVIMAS

Modulio pavadinimas	Modulio kodas
SISTEMŲ ADMINISTRAVIMAS	

Lektorius (-iai)	Institucija ar katedra, kurioje dėstomas modulis

Pateikimo būdas	Kalba
Kontaktiniu būdu, nuotoliniu būdu, mišriuoju būdu	*Anglų, suomių, turkų, norvegų, lietuvių, rumunų, prancūzų, lenkų, ispanų*

Reikalavimai
Nėra

Suteiktų ECTS kreditų skaičius	Studento darbo krūvis	Kontaktinės darbo valandos	Individualios darbo valandos
3	75	50	25

Modulio tikslas ir rezultatai
Baigę šį kursą, studentai gebės valdyti (identifikuoti, analizuoti, vertinti, įvertinti, mažinti) su kibernetiniu saugumu susijusius IKT infrastruktūrų, sistemų ir paslaugų rizikos veiksnius, planuojant, taikant, pranešant ir komunikuojant apie rizikos analizę, vertinimą ir tvarkymą. Studentai išmoks tinklų pagrindų, kad galėtų tinkamai valdyti tinklo įrenginius, dirbti su Linux ir Windows serveriais, juos valdyti ir apsaugoti. Taip pat žinios apie debesų kompiuteriją ir dirbtinį intelektą kibernetinio saugumo kontekste. Studentai taip pat išmoks, kaip sustiprinti sistemas, ieškoti grėsmių ir užtikrinti serverių prieinamumą.

Modulio mokymosi rezultatai	Mokymo ir mokymosi metodai	Vertinimo metodai

Žinios. Studentai įgyja žinių apie tinklo administravimą, operacines sistemas, tinklo pagrindus, tinklo administravimo įrankius, tinklo įrenginių saugumą, Linux sistemos administravimą, Windows sistemos administravimą, virtualizaciją, debesų kompiuteriją naudojant AI tinklų ir kibernetinio saugumo procedūroms, kibernetinio saugumo procedūras, grėsmių aptikimą, grėsmių analizę, reagavimą į grėsmes, grėsmių šalinimą, kibernetinio saugumo pagrindus, organizacijos apsaugą nuo atakų, infrastruktūros ir tinklo saugumą, tinklo stebėjimą ir analizę, incidentų tvarkymą. Jie sugebės nustatyti ir apibūdinti veiksmingas sistemos administravimo procedūras, veiklos rutinas, pritaikytas prie konkrečių MVĮ darbo vietų poreikių, laikantis atitikties standartų.	Dėstytojas pasirenka: tiesioginės paskaitos, vaizdo įrašai, pristatymai, virtualios priemonės (jei taikoma), literatūros analizė, kviestiniai lektoriai, tarpusavio mokymas ir mokymasis, mentorystė.	Savitikros testai ir žinių vertinimo testai
Įgūdžiai. Studentai įgis įgūdžių naudoti metodikas ir įrankius saugių sistemų architektūrų, įskaitant operacines sistemas, duomenų bazes, tinklus ir debesų infrastruktūras, projektavimui ir įgyvendinimui MVĮ darbo vietose.	Dėstytojas pasirenka: tiesioginės paskaitos, vaizdo įrašai, pristatymai, virtualios priemonės (jei taikoma), literatūros analizė, kviestiniai lektoriai, tarpusavio mokymas ir mokymasis, mentorystė.	Savitikros testai ir žinių vertinimo testai
Kompetencijos. Studentai įgis kompetencijų kurti ir įgyvendinti kibernetinio saugumo sistemas, skirtas sistemų administravimui, vadovauti projektams ir komandoms, siekiant sustiprinti sistemų saugumą ir prieinamumą, priimti etiškus sprendimus, siekiant išlaikyti tvirtas kibernetinio saugumo praktikas įvairiose MVĮ darbo vietų administravimo srityse.	Dėstytojas pasirenka: tiesioginės paskaitos, vaizdo įrašai, pristatymai, virtualios priemonės (jei taikoma), literatūros analizė, kviestiniai lektoriai, tarpusavio mokymas ir mokymasis, mentorystė.	Savitikros testai ir žinių vertinimo testai

Modulio turinys: temų suskirstymas	Kontaktinės darbo valandos					Individualios darbo valandos ir užduotys	
	Paskaitos (HEI)	Konsultacijos	Praktika (HEI)	Testai	**Visi kontaktiniai darbai**	**Individualus darbas**	**Užduotys**
Operacinės sistemos administravimas • Operacinės sistemos • Techninė ir programinė įranga • Dvejetainė ir šešioliktainė skaičiavimo sistema • Bitai ir baitai • Komandų eilutė operacinėje sistemoje • „Windows“ ir „Linux“ komandos • „Windows“ klientas ir serveris • Programos, procesai ir paslaugos sistemoje „Windows“ • Failų plėtiniai ir tipai • Registro raktai ir tipai • Valdymo skydelio nustatymai • Naudotojai ir grupės • Domeno struktūra ir serverio tvarkyklė • AD ir GPO • Linux sąsajos ir branduolys • Procesai Linux sistemoje • Failų ir katalogų pavadinimų suteikimo tvarka • Linux Shells ir komandų sintaksė • Failų ir aplankų tvarkymas • Darbas su Pipe & System stebėjimo komandomis • Procesų valdymas ir užduočių kontrolė • Paslaugų valdymas	4	0,5	2	0,5	**7**	**3,5**	Šešioliktainis skaičiavimas Windows komandų praktika Linux komandų praktika Užduočių tvarkyklės praktika Failų kūrimas ir tvarkymas Registro raktų ir verčių keitimas ir peržiūra Valdymo skydo nustatymų keitimas Vartotojų ir grupių valdymas Domeno struktūros valdymas Active Directory objektų kūrimas ir naikinimas Procesų tvarkymas Linux Failų ir aplankų tvarkymas Darbas su Pipe & System sistemos stebėjimo komandos Linux paslaugų valdymas
Duomenų bazių sistemos administravimas • Saugyklos ir šaltinių sąrašai • Web serverio valdymas • Sistemos žurnalai ir žurnalų stebėjimas • Užduočių planavimas Linux sistemoje • Serverių ir tinklo gedimų šalinimas • Atsarginės kopijos ir atkūrimas • GRUB apsauga • Ugniasienės	4	0,5	2	0,5	**7**	**3,5**	Saugyklų ir šaltinių sąrašų tvarkymas Tinklo serverio valdymas Sistemos žurnalų tikrinimas ir valdymas bei žurnalų stebėjimas Užduočių planavimas Linux Serverio gedimų šalinimas Atsarginių kopijų atkūrimas GRUB apsauga

• Active Directory objektų ir GPO valdymas • DNS ir DHCP • PowerShell pagrindai • Microsoft BitLocker, AppLocker ir ugniasienė • LDAP ir Kerberos • NTLM • Slaptažodžių ir blokavimo politikos • Autentiškumo patvirtinimas ir prieigos kontrolė • Interneto kontrolės pranešimų protokolas (ICMP) • TCP ir UDP • NetBIOS ir SMB • SSL ir TLS • Sertifikatai • Telnet ir Secure Shell (SSH) protokolai • HTTP ir HTTPS • Pašto sistemų protokolai • Domenų vardų sistemos protokolas (DNS) • FTP ir RDP • Inkapsuliacija ir dekapseliacija • Tinklo snifferiai ir Wireshark • TCP/UDP • DHCP, DNS							DB paslaugų valdymas Slaptažodžių politikos nustatymas Paskyrų blokavimo politikos nustatymas Autentiškumo patvirtinimo ir prieigos kontrolės nustatymas
Tinklo administravimas • Tinklų tipai ir belaidžiai tinklai • Tinklai ir topologijos • Įrenginio tapatybė ir prieigos įrenginiai • Infrastruktūra ir saugumo įrenginiai • Specializuoti įrenginiai ir tinklo architektūra • Virtualūs tinklai • Fiziniai ir loginiai adresai • OSI ir tinklo modeliai • Duomenų įkapsulavimas ir dekapsulavimas • Tinklo protokolai ir prievadų numeriai • Tinklo laikmenos ir kabeliai • Belaidės technologijos • Tinklo administravimo įrankiai • Cisco Packet Tracer • Tinklo klasės ir potinkliai • Adresų nustatymo protokolas (ARP)	4	0,5	2	0,5	**7**	**3,5**	Tinklo topologijų kūrimas Tinklo įrenginių valdymas Tinklo kūrimas Tinklo įrenginių apsauga Virtualių tinklų kūrimas Tinklo protokolų ir prievadų numerių nustatymas Darbas su „Cisco Packet Tracer“ Darbas su adresų nustatymo protokolu (ARP) Tinklo planavimas Statinio ir dinaminio IP adresavimo nustatymas DHCP ir NAT konfigūravimas Darbas su „Cisco IOS“ VLAN konfigūravimas Tinklo gedimų šalinimas

• Statinis ir dinaminis IP adresavimas • Tinklo adresų vertimas (NAT) • Komutatoriai ir Cisco IOS • Komutatorių prievadų saugumas ir maršrutizatorių sąsajos • VLAN ir DTP konfigūravimas • Maršrutizavimas tarp VLAN • Įvadas į ACL • Tinklo gedimų šalinimas							
Debesų administravimas • Hipervizoriai ir virtualios mašinos • Konteineriai • Virtualių aplinkų saugumo užtikrinimas • Atsarginės kopijos ir atkūrimas • Debesų kompiuterija ir CSP • Kas yra debesų paslaugų modeliai • Debesų diegimo tipai • Virtualūs tinklai • AWS skaičiavimo paslaugos • „Amazon Elastic Compute Cloud“ (EC2) • Debesų stebėjimo įrankiai • Automatizavimo ir koordinavimo įrankiai • Debesų saugumo grėsmės ir pažeidžiamumai • Tapatybės ir prieigos valdymas (IAM) • Prieigos kontrolė pagal vaidmenis (RBAC) • Daugialypė autentifikacija (MFA) • Debesų duomenų šifravimas • Virtualus privatusis debesų kompiuteris (VPC) • Docker ir Kubernetes	4	0,5	2	0,5	**7**	**3,5**	Virtualiųjų mašinų kūrimas Konteinerių nustatymas Virtualių aplinkų apsauga Darbas su atsarginėmis kopijomis Debesų tinklo valdymas Virtualių tinklų konfigūravimas Darbas su debesų stebėjimo įrankiais Automatizavimo ir koordinavimo įgyvendinimas Debesų saugumo grėsmių ir pažeidžiamumų aptikimas Tapatybės ir prieigos valdymo (IAM) nustatymas Debesų duomenų šifravimo diegimas Darbas su „Docker“ ir „Kubernetes“
Kiberfizinės sistemos administravimas • Saugumo ir prieigos kontrolė • Autentiškumo patvirtinimo tipai • TACACS+ ir RADIUS • AAA konfigūracija • Rizikos valdymo tikslai • Šifravimas ir dešifravimas • Hash ir Rainbow lentelės • MAC „Spoofing“ & ARP „Poisoning“ • VLAN „Hopping“ & „Rogue“ DHCP • ICMP „Flood” • TCP ir UDP „Flood” • Sesijos perėmimas • DNS suklastojimas	4	0,5	2	0,5	**7**	**3,5**	Infrastruktūros pagrindinių komponentų nustatymas Saugumo kontrolės priemonių įgyvendinimas Darbas su TACACS+ ir RADIUS AAA konfigūracija Šifravimo ir dešifravimo bandymai Dažniausių atakų ir gynybos metodų analizė Demilitarizuotų zonų (DMZ) nustatymas

• „Defense in Depth (DID) & Zero Trust“ • Demilitarizuotos zonos (DMZ) • Honeypots ir tinklo stiprinimas • Geriausia praktika saugiam tinklui • VPN • SSH ir VNC • „Stateful“ ir „Stateless“ ugniasienės • „Host-Based“ vs. „Network-Based“ • Aparatinės ir programinės ugniasienės • Tinklo programų ugniasienės (WAF) • AI ugniasienėse • IDS ir IPS • NIDS ir HIDS • Snort • tcpdump							Honeypot analizė Saugumo stiprinimas taikant geriausią saugaus tinklo praktiką VPN diegimas Darbas su Secure Shell (SSH) Darbas su virtualaus tinklo kompiuterija (VNC) Ugniasienės darbo technikos AI diegimas ugniasienėse Snort ir tcpdump naudojimas apsaugai ir aptikimui
Sistemos stiprinimas • GenAI technikos • Kodo generavimas • Vartotojų paskyrų valdymas ir prieigos kontrolė • Anomalijų aptikimas ir trikčių šalinimas • Apache2 paslaugos klaidų sprendimas • Pataisų valdymas ir atnaujinimai • Automatinis atsarginių kopijų kūrimas ir atkūrimas • IT turto valdymas ir inventorizacija • Ištrintų failų atkūrimas naudojant GenAI • Kibernetinio saugumo procedūros • Grėsmių aptikimas ir analizė • Reagavimas į grėsmes ir jų šalinimas • AI panaudojimas realaus laiko grėsmių aptikimui • GenAI modelių patvirtinimas ir testavimas • Valdymo ir reguliavimo sistemos • DNS konfigūracija ir saugumas • DHCP konfigūracija ir saugumas • PowerShell pagrindai • Komutatoriaus prievado saugumas • Tinklo pagrindinė įvesties/išvesties sistema (NetBIOS) • Serverio pranešimų blokavimo protokolas (SMB)	4	0,5	2	0,5	**7**	**3,5**	Darbas su GenAI technikomis Vartotojų paskyrų valdymas ir prieigos kontrolė Anomalijų aptikimas ir trikčių šalinimas Apache2 paslaugos klaidų sprendimas naudojant GenAI Pataisų valdymo ir atnaujinimų konfigūravimas Automatinio atsarginių kopijų kūrimo ir atkūrimo nustatymas IT turto valdymas Ištrintų failų atkūrimas naudojant GenAI DNS ir DHCP saugumo įgyvendinimas Darbas su „Microsoft BitLocker“ ir „Microsoft AppLocker“ „Microsoft“ užkardos nustatymas Switch Port Security nustatymas FTP (File Transfer Protocol) saugumo užtikrinimas Nuotolinio darbalaukio protokolo (RDP) saugumo užtikrinimas

• Saugių lizdų sluoksnis (SSL) ir transporto sluoksnio saugumas (TLS) • Saugumo sertifikatai • Pašto sistemų protokolai • Domenų vardų sistemos protokolas (DNS) • Failų perdavimo protokolas (FTP) • Nuotolinio darbalaukio protokolas (RDP) • Užduočių planavimas Linux • Serverio gedimų šalinimas • Tinklo gedimų šalinimas • Atsarginės kopijos ir atkūrimas • GRUB apsauga • Ugniasienių nustatymas ir apsauga							Saugumo užduočių planavimas Linux GRUB apsauga Ugniasienių (iptables) nustatymas ir saugumo užtikrinimas
Prieinamumas • IR ir SOC • Įvykiai ir incidentai • Įspėjimų aptikimas ir įspėjimų rūšiavimas • Dokumentacija ir ataskaitos • Kas yra internetinės atakos? • DoS ir DDoS • SQL įterpimas ir XSS • „Command Injection & Local File Inclusion“ (LFI) • „Cross-Site Request Forgery“ (CSRF) • „Brute-Force“ ir „Credential Stuffing“ • „Pass the Hash & Pass the Ticket“ • LDAP žvalgyba • Sugadinta prieigos kontrolė • Išpirkos reikalaujantis virusas • Kompiuteriniai virusai ir kirminai • Trojos arklys ir reklamos programinė įranga • Keylogger ir kriptovaliutų kasyba • „Fileless Malware“ • Kenkėjiškų programų plitimo supratimas • Statinė ir dinaminė kenkėjiškų programų analizė • Saugi kenkėjiškų programų analizė • Hibridinė analizė, kenkėjiškų programų tyrimas • Statinės ir dinaminės kenkėjiškų programų analizės atlikimas	4	0,5	3	0,5	**8**	4	Įvykių ir incidentų aptikimas Įspėjimų rūšiavimas Dokumentacijos rengimas ir tinkamas ataskaitų teikimas Įvykio pasekmių likvidavimo veiksmų įgyvendinimas Atliekant ir apsaugant nuo DoS ir DDoS Interneto atakų ir kenkėjiškų programų plitimo aptikimas Saugios statinės ir dinaminės kenkėjiškų programų analizės atlikimas IOC valdymas Slaptažodžių politikos nustatymas „Bring Your Own Device“ (BYOD) politikos nustatymas Nuotolinio prieigos politikos nustatymas

• IOC ir slaptažodžių politikos valdymas • „Acceptable Use Policies“ (AUP) • „Bring Your Own Device“ (BYOD) politika • Nuotolinės prieigos politika							
Iš viso	**28**	**3,5**	**15**	**3,5**	**50**	**25**	

Vertinimo strategija	**Lyginamasis svorio procentas**	**Vertinimo kriterijai**
Savitikros testas (1)	5 %	10 balų – 95–100 % teisingų atsakymų. 9 balai – 85–94 % teisingų atsakymų. 8 balai – 75–84 % teisingų atsakymų. 7 balai – 65–74 % teisingų atsakymų. 6 balai – 55–64 % teisingų atsakymų. 5 balai – 45–54 % teisingų atsakymų. 4 balai – 35–44 % teisingų atsakymų. 3 balai – 25–34 % teisingų atsakymų. 2 balai – 15–24 % teisingų atsakymų. 1 balas – 0–14 % teisingų atsakymų.
Savitikros testas (2)	5 %	
Savitikros testas (3)	5 %	
Savitikros testas (4)	5	
Savitikros testas (5)	5	
Savitikros testas (6)	5	
Savitikros testas (7)	5	
Žinių vertinimo testas	65 %	

3. M3: ANALITINĖS PRIEMONĖS

Modulio pavadinimas	Modulio kodas
ANALITINĖS PRIEMONĖS	

Lektorius (-iai)	Institucija ar katedra, kurioje dėstomas modulis

Pateikimo būdas	Kalba
Kontaktiniu būdu, nuotoliniu būdu, mišriuoju būdu	*Anglų, suomių, turkų, norvegų, lietuvių, rumunų, prancūzų, lenkų, ispanų*

Reikalavimai
Nėra

Suteiktų ECTS kreditų skaičius	Studento darbo krūvis	Kontaktinės darbo valandos	Individualios darbo valandos
3	75	50	25

Modulio tikslas ir rezultatai		
Baigę šį kursą, studentai įgis įgūdžių, kaip apsaugoti organizacijos turtą naudojant veiklos rodiklius, duomenų analizę ir saugumo informaciją. Jie išmoks veiksmingai taikyti analitines priemones, kad nustatytų galimas kibernetinio saugumo rizikas ir pažeidžiamumą, panaudotų duomenimis pagrįstą informaciją saugumo priemonėms stiprinti ir naudotų veiklos rodiklius, susijusius su slaptažodžiais, naršyklės naudojimu, elektroniniu paštu ir duomenų apdorojimo programomis. Baigę modulį, dalyviai sugebės įvertinti ir sumažinti potencialias saugumo grėsmes naudodami tinkamas priemones ir pranešti apie bet kokias grėsmes ar sutrikimus atitinkamoms reguliavimo institucijoms.		
Modulio mokymosi rezultatai	**Mokymo ir mokymosi metodai**	**Vertinimo metodai**
Žinios. Studentai įgyja praktinių žinių apie tai, kaip taikyti veiklos rodiklius, duomenų analizę ir saugumo informaciją organizacijos turtui apsaugoti.	Dėstytojas pasirenka mokymo ir mokymosi metodus iš D2.3 ataskaitos 1.3 dalies [Mokymo metodai, pvz., teorinės paskaitos, kviestiniai lektoriai, viktorinos, žaidimai, praktinės užduotys/laboratoriniai darbai, tarpusavio mokymas ir mokymasis, savarankiškas mokymasis ir kt.].	Savitikros testai Žinių vertinimo testas
Įgūdžiai. Studentai įgis įgūdžių naudoti analitines priemones potencialiems kibernetinio saugumo rizikos veiksniams ir pažeidžiamumams nustatyti, taikyti duomenimis pagrįstą informaciją kibernetinio saugumo praktikoms stiprinti ir	Dėstytojas pasirenka mokymo ir mokymosi metodus iš D2.3 ataskaitos 1.3 dalies [Mokymo metodai, pvz., praktinės užduotys/laboratoriniai darbai, praktinės veiklos, imituojamos aplinkos, viktorinos, žaidimai, atvejų analizės ir kt.].	Praktiniai vertinimai

naudoti veiklos rodiklius slaptažodžių, naršymo, elektroninio pašto ir duomenų tvarkymo saugumui vertinti ir stiprinti.		
Kompetencijos. Studentai gebės vertinti ir mažinti potencialias saugumo grėsmes naudodami analitinius įrankius, tiksliai pranešdami apie grėsmes ir pažeidimus atitinkamiems kanalams savo organizacijoje.	Dėstytojas pasirenka mokymo ir mokymosi metodus iš D2.3 ataskaitos 1.3 dalies [Mokymo metodai, pvz., simuliuojamos aplinkos, „vėliavos gaudymo“ varžybos, 5E, CBL, CL, POGIL, PBL ir kt.].	Simuliacijos Konkursai

Modulio turinys: temų suskirstymas	**Kontaktinės darbo valandos**					**Individualios darbo valandos ir užduotys**	
	Paskaitos (HEI)	Konsultacijos	Praktika (HEI)	Testai	**Visi kontaktiniai darbai**	**Individualus darbas**	**Užduotys**
Veiklos vertinimas (metrika) • Veiklos rodikliai • Sistemos ir tinklo stebėjimas • Veiklos rodiklių stebėjimas • Tinklo žemėlapiai • Pažeidžiamumo skenavimas • Tinklo srauto analizė	10	0,5	5	0,5	**16**	**8,5**	• Atlikti tyrimą apie našumo rodiklius ir priemones. Palyginti našumo stebėjimo įrankius ir nustatyti jų skirtumus. • Užbaigti „Zabbix“ diegimą ir atlikti pagrindinį konfigūravimą. • Sukurti programą, skirtą našumo rodikliams stebėti naudojant Zabbix. • Nustatyti tikslinės sistemos pažeidžiamumą naudojant tinklo žemėlapių kūrimo programinę įrangą (pvz., nmap, rustscan ir kt.). • Atlikti pažeidžiamumo skenavimą tikslinėje sistemoje naudojant Nessus programinę įrangą. Paruošti pažeidžiamumo testavimo ataskaitą.

							• Atlikti tinklo srauto analizę naudodami Wireshark.
Duomenų analizė • Duomenų rinkimas • Duomenų valymas ir pirminis apdorojimas • Duomenų analizė • Duomenų vizualizavimas • Analitinės priemonės • Duomenų analizės taikymas kibernetiniame saugume	10	0,5	5	0,5	**16**	**8,5**	• Atlikti duomenų valymo ir išankstinio apdorojimo veiksmus su hipotetinei MVĮ parengtu duomenų rinkiniu, susijusiu su kibernetinio saugumo klausimais. • Analizuoti išvalytą ir apdorotą hipotetinės MVĮ duomenų rinkinį ir vizualizuoti rezultatus. • Kokie yra duomenų analizės taikymo kibernetiniame saugume pavyzdžiai? Atlikti tyrimą.
Saugumo žvalgyba • Saugumo žvalgybos supratimas • Saugumo žvalgybos šaltiniai • Grėsmių žvalgybos rinkimo metodai • Grėsmių žvalgybos sistemos • AI pagrįstos saugumo žvalgybos platformos • Saugumo žvalgybos taikymo atvejų analizė	10	0,5	7	0,5	**18**	**8**	• Išnagrinėti, kaip saugumo žvalgyba prisideda prie aktyvių MVĮ saugumo strategijų. • Kokie yra dažniausi saugumo žvalgybos informacijos šaltiniai? Kaip vertinti šių šaltinių patikimumą? • Apibūdinti kiekvieno grėsmių žvalgybos informacijos rinkimo metodo privalumus ir trūkumus. • Paaiškinti pagrindines grėsmių žvalgybos sistemų, pvz., MITRE ATT&CK ir Cyber Kill Chain, savybes. • Išnagrinėti realų atvejį, kai buvo panaudota saugumo informacija. Apibūdinti toje atvejo analizėje naudotus informacijos rinkimo metodus.
Iš viso	**30**	**1,5**	**17**	**1,5**	**50**	**25**	

Vertinimo strategija	Lyginamasis svorio procentas	Vertinimo kriterijai
Savitikros testas I	15	10 balų – 95–100 % teisingų atsakymų. 9 balai – 85–94 % teisingų atsakymų. 8 balai – 75–84 % teisingų atsakymų. 7 balai – 65–74 % teisingų atsakymų. 6 balai – 55–64 % teisingų atsakymų. 5 balai – 45–54 % teisingų atsakymų. 4 balai – 35–44 % teisingų atsakymų. 3 balai – 25–34 % teisingų atsakymų. 2 balai – 15–24 % teisingų atsakymų. 1 balas – 0–14 % teisingų atsakymų.
Savitikros testas II	15	
Savitikros testas III	15	
Žinių vertinimo testas	55	

Studijų medžiaga *(Pavardė, vardo inicialas. (Metai, mėnuo, diena). Straipsnio pavadinimas. Žurnalo/laikraščio pavadinimas, tomo numeris, viso straipsnio puslapių numeriai, leidėjas, URL nuoroda)*
Privaloma literatūra
...
Rekomenduojama literatūra
https://brainstation.io/career-guides/what-tools-do-cybersecurity-analysts-use **https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it** **https://medium.com/@jcm3/wireshark-traffic-analysis-part-1-tryhackme-walkthrough-a9bec11d94d9** **https://www.kali.org/tools/nmap/** **https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/** **https://www.varonis.com/blog/cyber-kill-chain** **https://www.youtube.com/watch?v=kVnvIBNiC58**

4. M4: SAUGUMO OPERACIJOS

Modulio pavadinimas	Modulio kodas
SAUGUMO OPERACIJOS	

Lektorius (-iai)	Institucija ar katedra, kurioje dėstomas modulis

Pateikimo būdas	Kalba
Kontaktiniu būdu, nuotoliniu būdu, mišriuoju būdu, konsultacijos	*Anglų, suomių, turkų, norvegų, lietuvių, rumunų, prancūzų, lenkų, ispanų*

Reikalavimai
Nėra

Paskirti ECTS kreditai	Studentų darbo krūvis	Kontaktinės darbo valandos	Individualios darbo valandos
3	75	5	25

Modulio tikslas ir rezultatai		
Baigę šį kursą, studentai gebės veiksmingai valdyti saugumo operacijas informacinių ir ryšių technologijų infrastruktūrose, sistemose ir paslaugose. Jie įgis įgūdžių stebėti, aptikti, reaguoti į kibernetinio saugumo incidentus ir atsigauti po jų, taikydami geriausią praktiką, įrankius ir sistemas, susijusias su saugumo operacijomis.		
Modulio mokymosi rezultatai	**Mokymo ir mokymosi metodai**	**Vertinimo metodai**
Žinios. Studentai įgis žinių apie saugumo operacijas, įskaitant stebėjimą, aptikimą, reagavimą į incidentus ir atkūrimą. Jie sugebės nustatyti ir apibūdinti veiksmingas kibernetinio saugumo operacijų procedūras, pritaikytas prie konkrečių MVĮ darbo vietų poreikių, laikantis kibernetinio saugumo standartų.	Dėstytojas pasirenka mokymo ir mokymosi metodus iš D2.3 ataskaitos 1.3 dalies [Mokymo metodai, pvz., teorinės paskaitos, literatūros analizė, kviestiniai lektoriai, tarpusavio mokymas ir mokymasis, mentorystė ir kt.].	Savitikros testai Žinių vertinimo testas

Įgūdžiai. Studentai įgis įgūdžių taikyti pažangias metodikas ir priemones saugumo operacijų užduotims atlikti, kurti ir įgyvendinti veiksmingas stebėjimo strategijas, reaguoti į incidentus ir kurti patikimas veiklos procedūras, pritaikytas konkrečiai MVĮ darbo vietoms.	Dėstytojas pasirenka mokymo ir mokymosi metodus iš D2.3 ataskaitos 1.3 dalies [*Mokymo metodai, pvz., teorinės paskaitos, literatūros analizė, kviestiniai lektoriai, tarpusavio mokymas ir mokymasis, mentorystė ir kt.*].	Savitikros testai Žinių vertinimo testas
Kompetencijos. Studentai įgis kompetencijų kurti ir įgyvendinti strategines saugumo operacijų politikas ir procedūras MVĮ darbo vietose.	Dėstytojas pasirenka mokymo ir mokymosi metodus iš D2.3 ataskaitos 1.3 dalies [*Mokymo metodai, pvz., teorinės paskaitos, literatūros analizė, kviestiniai lektoriai, tarpusavio mokymas ir mokymasis, mentorystė ir kt.*].	Savitikros testai Žinių vertinimo testas

Modulio turinys: temų suskirstymas	**Kontaktinės darbo valandos**					**Individualios darbo valandos ir užduotys**	
	Paskaitos (HEI)	Konsultacijos (MVĮ)	Praktika (HEI)	Testai	Visi kontaktiniai darbai	Individualus darbas	Užduotys
Saugumo operacijų pagrindai - Saugumo operacijų ir SOC (saugumo operacijų centro) supratimas - Saugumo operacijų vaidmenys ir atsakomybė - Saugumo operacijų įrankių ir technologijų apžvalga	6	0,5	2	0,5	**9**	6	Atpažinti ir suprasti SOC struktūrą ir funkcijas, analizuoti įvairius vaidmenis saugumo operacijose, tirti saugumo operacijose naudojamas priemones ir analizuoti atvejo studiją.

Saugumo konvergencija - Saugumo konvergencijos supratimas - Fizinio saugumo pagrindai (fizinio saugumo principai, fizinio turto apsauga, politika) - Atvejo analizė, pabrėžianti saugumo konvergencijos principus	8	0,5	4	0,5	**13**	6	Peržiūrėti saugumo konvergencijos apibrėžimą ir principus, susipažinti su fizinio ir skaitmeninio saugumo operacijų integravimo svarba, nustatyti ir įvertinti riziką kibernetinėje ir fizinėje srityse.
Saugumo informacijos ir įvykių valdymas - Saugumo stebėjimo principų peržiūra - SIEM sprendimų įgyvendinimas	8	0,5	4	0,5	**13**	6	Įvadas į saugumo stebėjimą ir SIEM diegimą. Pagrindiniai principai, tokie kaip žurnalo tipai, aptikimo metodai ir stebėjimo ciklas. Praktiniai SIEM diegimo aspektai, įskaitant architektūrą, duomenų rinkimą, taisyklių kūrimą ir įspėjimų valdymą.
Saugumo operacijų praktika - Duomenų šaltinių identifikavimas ir žurnalų rinkimo optimizavimas - Įspėjimų centralizavimas naudojant SIEM - SIEM testavimas	4	0,5	10	0,5	**15**	7	Išsami ir praktinė mokymo programa, suteikianti būtinas žinias ir praktinius įgūdžius žurnalų tvarkymo, SIEM konfigūravimo ir grėsmių aptikimo įvairiose IT aplinkose srityse.
Iš viso	**26**	**2**	**20**	**2**	**50**	**25**	

Vertinimo strategija	**Lyginamasis svorio procentas**	**Vertinimo kriterijai**
Savitikros testas (1)	10	10 balų – 95–100 % teisingų atsakymų. 9 balai – 85–94 % teisingų atsakymų.
Savitikros testas (2)	10 %	

Savitikros testas (3)	10 %	8 balai – 75–84 % teisingų atsakymų. 7 balai – 65–74 % teisingų atsakymų. 6 balai – 55–64 % teisingų atsakymų. 5 balai – 45–54 % teisingų atsakymų. 4 balai – 35–44 % teisingų atsakymų. 3 balai – 25–34 % teisingų atsakymų. 2 balai – 15–24 % teisingų atsakymų. 1 balas – 0–14 % teisingų atsakymų.
Savitikros testas (4)	10	
Žinių vertinimo testas	60 %	

Studijų medžiaga *(Pavardė, vardo inicialas. (Metai, mėnuo, diena). Straipsnio pavadinimas. Žurnalo/laikraščio pavadinimas, tomo numeris, viso straipsnio puslapių numeriai, leidėjas, URL nuoroda)*
Privaloma literatūra
Cybellium (2024). *Saugumo operacijų centrų (SOC) studijų vadovas: išsamus vadovas saugumo operacijų centrų (SOC) mokymuisi* Muniz, J. (2021). *Šiuolaikinis saugumo operacijų centras*. Pearson Education. ENISA (2017). *Incidentų reagavimo ir bendradarbiavimo kibernetinių krizių atveju strategijos*. **Incidentų reagavimo ir bendradarbiavimo kibernetinių krizių atveju strategijos — ENISA (europa.eu)**
Rekomenduojama literatūra
Basta, A., Basta, N., Anwar, W., Essar, M. I. (2024). Atvirojo kodo saugumo operacijų centras (SOC): išsamus vadovas, kaip įsteigti, valdyti ir prižiūrėti šiuolaikinį SOC. Cybellium (2023). Saugumo operacijų centro (SOC) valdymas.

5. M5: SAUGUMO VALDYMAS IR POLITIKA

Modulio pavadinimas	Modulio kodas
SAUGUMO VALDYMAS IR POLITIKA	

Lektorius (-iai)	Institucija ar katedra, kurioje dėstomas modulis

Pateikimo būdas	Kalba
Kontaktiniu būdu, nuotoliniu būdu, mišriuoju būdu	*Anglų, suomių, turkų, norvegų, lietuvių, rumunų, prancūzų, lenkų, ispanų*

Reikalavimai
Nėra

Suteiktų ECTS kreditų skaičius	Studento darbo krūvis	Kontaktinės darbo valandos	Individualios darbo valandos
3	75	50	25

Modulio tikslas ir rezultatai
Dalykas „Saugumo valdymas ir politika“ skirtas parengti studentus spręsti MVĮ kibernetinio saugumo uždavinius, integruojant saugumo valdymą į verslo strategiją ir užtikrinant atitiktį teisiniams reikalavimams, pvz., BDAR. Modulis apima tokius aspektus kaip grėsmių ir pažeidžiamumų nustatymas, patikimų ir prisitaikančių saugumo politikos priemonių kūrimas ir veiksmingas incidentų valdymas. Be to, jis skirtas valdymo struktūrų, kuriose organizacijoje būtų aiškiai paskirstyti vaidmenys, kūrimui, suderinant kibernetinį saugumą su strateginiais tikslais. Studentai įgis techninių kompetencijų kibernetinių rizikų vertinimo ir mažinimo srityje bei ugdys analizės įgūdžius, kad galėtų siūlyti saugumo brandos tobulinimo būdus. Jie taip pat įgis įgūdžių veiksmingai komunikuoti kibernetinio saugumo poreikius vadovams, remti pagrįstą sprendimų priėmimą ir užtikrinti reguliavimo reikalavimų laikymąsi bei etiką. Modulis „Saugumo valdymas ir politika“ taip pat apima išsamų *phishing* prevencijos, AI valdomų kibernetinių atakų ir išpirkos reikalaujančių virusų valdymo tyrimą, analizuojant, kaip šios konkrečios grėsmės reikalauja integruoto požiūrio į valdymą ir atitiktį. Saugumo politikos veiksmingumas bus vertinamas ne tik pagal jos gebėjimą užkirsti kelią incidentams, bet ir pagal jos prisitaikymą prie naujų grėsmių ir atitiktį galiojantiems teisės aktams.

Modulio mokymosi rezultatai	Mokymo ir mokymosi metodai	Vertinimo metodai
Žinios. Studentai įgis žinių apie tai, kaip įgyvendinti naujas kibernetinio saugumo procedūras ir darbo eigą MVĮ darbo vietose, įtraukiant dabartinius kibernetinio saugumo principus, tendencijas ir atitiktį nacionaliniams ir tarptautiniams teisės aktams, susijusiems su jų pramonės šaka. Įgis pažengusių žinių apie tai, kaip integruoti *phishing* prevenciją, valdyti AI keliamas grėsmes ir reaguoti į išpirkos reikalaujančius virusus MVĮ aplinkoje.	**Paskaitos.** Paskaitos suteiks tvirtą koncepcinį pagrindą kibernetinio saugumo, valdymo, privatumo ir atitikties srityse, skatindamos aktyvų studentų dalyvavimą. Gali būti naudojamos interaktyvios paskaitos, apimančios reguliarias klausimų ir atsakymų sesijas, apklausas ir tiesioginius problemų sprendimo pratimus. Naudojant tokias priemones kaip „Mentimeter“ ir „Poll Everywhere“, **Dalyvavimas diskusijose ir forumuose.** Dalyvavimas diskusijose ir forumuose leis studentams diskutuoti ir kritiškai analizuoti kibernetinio saugumo klausimus, ugdant jų argumentavimo įgūdžius. Tai bus taikoma klausimams, susijusiems su etika, politika ir sprendimų priėmimu kibernetinio saugumo srityje. **Atvejų analizė** leis studentams analizuoti kibernetinio saugumo situacijas MVĮ, taikant teorines žinias realių problemų sprendimui. Bus sutelkiama dėmesys į tokias temas kaip duomenų pažeidimų valdymas, išpirkos reikalaujantys virusai, sukčiavimas elektroniniu paštu, dirbtinio intelekto pagrįsti išpuoliai, saugumo politikos įgyvendinimas ir valdymas.	**Savitikros testai** leidžia studentams įvertinti savo supratimą apie kiekvieną potemę, atsakant į įvairius klausimus, kad būtų galima nustatyti sritis, kurias reikia tobulinti. Jie neturi įtakos galutiniam vertinimo balui, bet yra svarbūs savarankiškam mokymuisi. **Galutinis egzaminas** yra neprivalomas ir leidžia studentams gauti baigimo pažymėjimą, įvertinant jų bendrą kurso supratimą per plėtros klausimus, atvejų analizę ir daugkartinio pasirinkimo klausimus. Norint gauti baigimo pažymėjimą, reikia išlaikyti egzaminą, o tie, kurie jo nelaiko, gaus lankymo pažymėjimą.
Įgūdžiai. Studentai įgis įgūdžių naudoti pažangias metodikas rizikos vertinimui atlikti, naujoms kibernetinio saugumo procedūroms kurti ir įgyvendinti bei reagavimo strategijoms parengti, užtikrinant veiksmingą valdymą ir atitiktį MVĮ darbo vietose. Išugdyti įgūdžius kuriant ir įgyvendinant išsamias kibernetinio saugumo	**Praktiniai seminarai** leis studentams taikyti kibernetinio saugumo koncepcijas per pratimus, pvz., politikos kūrimą ir incidentų simuliacijas, su instruktoriaus atsiliepimais realiuoju laiku. Jie skirti stiprinti praktinius įgūdžius ir parengti studentus taikyti tai, ko jie išmoko, realiose situacijose.	**Praktinės užduotys** per visą kursą leis studentams pritaikyti teorines žinias imituojamose situacijose, pvz., kibernetinio saugumo politikos kūrimas ir incidentų imitavimas, siekiant įvertinti jų gebėjimą spręsti realias problemas MVĮ kontekste.

procedūras, kurios padeda kovoti su pažangiomis grėsmėmis ir užtikrina	**Praktinis darbas ir individualūs projektai** leis studentams taikyti kibernetinio saugumo koncepcijas per užduotis, pvz., politikos formavimą ir rizikos analizę, ugdant savarankiško darbo įgūdžius ir praktiškai taikant teorines žinias. **Bendri projektai** leis studentams dirbti komandose, kuriant kibernetinio saugumo sprendimus MVĮ, įskaitant saugumo politiką ir valdymo modelius. Jie skatins komandinį darbą, projektų valdymą ir įgytų žinių praktinį pritaikymą, gaunant grįžtamąjį ryšį iš mokytojų ir bendramokslių.	**Grupiniai projektai** leis studentams parengti išsamų kibernetinio saugumo projektą, nuo rizikos identifikavimo iki valdymo modelių ir incidentų reagavimo planų pasiūlymų, vertinant tiek turinio kokybę, tiek gebėjimą bendradarbiauti. Šis projektas yra svarbus galutiniam vertinimui ir apima visą kurso medžiagą.
Kompetencijos. Studentai įgis kompetencijų kurti ir įgyvendinti strategines kibernetinio saugumo politikos priemones, vadovauti iniciatyvoms, skirtoms naujų darbo tvarkų ir darbo srautų kūrimui MVĮ darbo vietose, priimti etiškus sprendimus, atitinkančius organizacijos tikslus ir atitikties reikalavimus. Įgyti kompetencijų formuluojant ir įgyvendinant kibernetinio saugumo politiką, kuri užkirstų kelią sudėtingoms kibernetinėms grėsmėms ir užtikrintų atitiktį tarptautiniams reglamentams.	**Scenarijų imitavimas** leis studentams valdyti kibernetinio saugumo incidentus virtualioje aplinkoje, atkartojančioje realius išpuolius, priimant strateginius sprendimus esant spaudimui. Šis metodas stiprina krizės valdymo ir reagavimo į incidentus įgūdžius ir yra svarbus mokant saugumo politikos vertinimo ir sprendimų priėmimo kritinėse situacijose. Studentai turės parodyti, kaip jie taikytų valdymo politiką, kad užkirstų kelią konkretiems incidentams, pvz., *phishing* atakoms, išpirkos reikalaujančiam virusui ir dirbtinio intelekto valdomoms atakoms, arba į juos reaguotų, įvertindami savo supratimą apie atitinkamą reguliavimo sistemą.	**Simuliacijos ir incidentų valdymas:** studentai bus vertinami pagal jų gebėjimą valdyti kibernetinio saugumo incidentus simuliacijose, atkartojančiose realias krizes MVĮ. Tikslas – įvertinti jų gebėjimą dirbti spaudimo sąlygomis, priimti strateginius sprendimus ir vykdyti reagavimo planus realiuoju laiku, vertinant jų praktinį pritaikymą dinamiškose situacijose.

Modulio turinys: temų suskirstymas	Kontaktinės darbo valandos					Individualios darbo valandos ir užduotys	
	Paskaitos (HEI)	Konsultacijos (MVĮ)	Praktika (HEI)	Testai	**Visi kontaktiniai darbai**	**Individualus darbas**	**Užduotys**
Organizacinis kontekstas -Kibernetinio saugumo raida MVĮ -Dabartinės pagrindinės grėsmės ir pažeidžiamumas -Kibernetinio saugumo poveikis verslo strategijai -Konkretūs kibernetinio saugumo iššūkiai MVĮ, palyginti su didžiosiomis įmonėmis - Suprasti kibernetinio saugumo praktikos reguliavimo pasekmes ir kaip jos dera su valdymo struktūromis. - Įprasti kibernetinio saugumo iššūkiai, būdingi MVĮ, pvz., ribotas biudžetas, specializuoto saugumo personalo trūkumas ir praktiniai metodai, kaip nustatyti kibernetinio saugumo investicijų prioritetus.	5	0,5	3	0,5	**9**	**4**	Literatūros nagrinėjimas, tyrimai, atvejų analizės rengimas
Privatumas -Privatumo principai kibernetiniame saugume -Asmens duomenų apsauga ir BDAR -Privatumo poveikis MVĮ veiklai -Privatumo apsaugos priemonės ir metodai	4	0,5	3	0,5	**8**	**4**	Politikos analizė, individualus užduotis
Teisės aktai, etika ir atitiktis -Kibernetinio saugumo organizacijos politika ir standartai -Atitinkami nacionaliniai ir tarptautiniai teisės aktai -Reglamentų laikymasis MVĮ -Etika kibernetiniame saugume -Teisinės pasekmės dėl kibernetinio saugumo reikalavimų nesilaikymo - Analizė, kaip AI pagrįsti įrankiai gali būti naudojami siekiant sustiprinti kibernetinio saugumo valdymą ir užtikrinti atitiktį nuolat stebint ir automatizuotai reaguojant į grėsmes.	5	0,5	3	0,5	**9**	**5**	Atvejo tyrimas, teisės aktų analizė

Saugumo valdymas -Kibernetinio saugumo valdymo struktūra -Saugumo valdymo vaidmenys ir atsakomybė -Kibernetinio saugumo brandos modeliai -Kibernetinio saugumo integravimas į įmonių valdymą - Gebėjimų atlikti rizikos vertinimus ir formuluoti strateginius reagavimo planus imituojamomis krizinėmis sąlygomis (išpirkos reikalaujantis virusas, sukčiavimo atakos ir kt.) stiprinimas	4	0,5	3	0,5	**8**	**4**	Rizikos valdymo scenarijų analizė
Komunikacija vykdomojo ir valdybos lygiu -Kibernetinio saugumo komunikacijos strategijos -Saugumo ataskaitos aukščiausiajai vadovybei -Sprendimų priėmimas remiantis saugumo duomenimis -Krizių valdymas ir komunikacija kibernetinio saugumo srityje -Krizių valdymo ir sprendimų priėmimo įgūdžių įsisavinimas didelio streso scenarijuose, susijusiuose su AI valdomomis atakomis ir išpirkos reikalaujančiais virusais.	4	0,5	3	0,5	**8**	**4**	Pristatymo paruošimas, bendravimas su suinteresuotosio mis šalimis
Valdymo politika -Saugumo politikos kūrimas -Politikos įgyvendinimas ir stebėsena -Politikos vertinimas ir nuolatinis tobulinimas -Saugumo politikos pritaikymas prie technologinių ir reguliavimo pokyčių - Tyrimas, kaip veiksmingos mokymo ir informavimo politikos gali būti svarbi reguliavimo laikymosi ir rizikos mažinimo sudedamoji dalis.	4	0,5	3	0,5	**8**	**4**	Politikos dokumento rengimas ir peržiūra
Iš viso	**26**	**3**	**18**	**3**	**50**	**25**	

Vertinimo strategija	**Lyginamasis svorio procentas**	**Vertinimo kriterijai**
Savikontrolės testas I	10	Organizacijos konteksto pagrindinių sąvokų vertinimas.
Savikontrolės testas II	10	Pagrindinių sąvokų apie privatumą vertinimas.
Savikontrolės testas III	10	Įstatymų, etikos ir atitikties politikos vertinimas.
Savikontrolės testas IV	10	Kibernetinio saugumo politikos vertinimas.
Savikontrolės testas V	10	Vadovų lygio komunikacijos vertinimas.
Savikontrolės testas VI	10	Vadybos politikos ir politikos formavimo saugumo srityje vertinimas.
Žinių vertinimo testas	40	Baigiamasis egzaminas, apimantis integruotus klausimus apie visas kurso temas.

10 balų – 95–100 % teisingų atsakymų. 9 balai – 85–94 % teisingų atsakymų. 8 balai – 75–84 % teisingų atsakymų. 7 balai – 65–74 % teisingų atsakymų. 6 balai – 55–64 % teisingų atsakymų. 5 balai – 45–54 % teisingų atsakymų. 4 balai – 35–44 % teisingų atsakymų. 3 balai – 25–34 % teisingų atsakymų. 2 balai – 15–24 % teisingų atsakymų. 1 balas – 0–14 % teisingų atsakymų.

Studijų medžiaga *(Pavardė, vardo inicialas. (Metai, mėnuo, diena). Straipsnio pavadinimas. Žurnalo/laikraščio pavadinimas, tomo numeris, viso straipsnio puslapių numeriai, leidėjas, URL nuoroda)*
Privaloma literatūra
... **„ES kibernetinio saugumo teisė: atsparumo ir nuoseklumo reguliavimas skaitmeniniame amžiuje“** autorė Luisa Marin • Šioje knygoje pateikiama išsami ES kibernetinio saugumo įstatymų ir politikos analizė, kuri yra labai svarbi norint suprasti, kaip ES kontekste struktūrizuojamas ir įgyvendinamas kibernetinio saugumo valdymas. **„Kibernetinis saugumas Europos Sąjungoje: atsparumas ir prisitaikymas valdymo politikoje“** autorius George Christou • Šioje knygoje nagrinėjami kibernetinio saugumo valdymo sistemos ir politikos formavimo procesai ES, padedantys studentams suprasti dinamišką įvairių valdymo lygių sąveiką. **„Sukčiavimas elektroniniu būdu ir kovos priemonės: suprasti didėjančią elektroninės tapatybės vagystės problemą“ (Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft)**, Markus Jakobsson ir Steven Myers • Nors ši knyga nėra skirta konkrečiai ES, joje išsamiai nagrinėjamos phishingo technikos ir kovos priemonės gali būti pritaikytos ES kontekstui, sutelkiant dėmesį į BDAR atitiktį ir duomenų apsaugos principus. **„Europos kibernetinio saugumo teisė ir reguliavimas“,** redagavo Nadya Purtova ir Bert-Jaap Koops • Šiame leidinyje aptariamos Europos Sąjungos kibernetiniam saugumui būdingos teisinės ir reguliavimo priemonės, įskaitant atitikties reikalavimams iššūkius ir sistemas, pvz., NIS direktyvą ir BDAR. **„Išpirkos reikalaujanti programinė įranga: suprasti skaitmeninį šantažą ir jo keliamą grėsmę jūsų organizacijai“ (Ransomware: Understanding Digital Extortion and its Threat to Your Organization)**, autoriai Allan • Ši publikacija, papildyta ES specifinių atvejų tyrimais ir pavyzdžiais, padės studentams suprasti išpirkos reikalaujančių virusų atakų pasekmes pagal ES reglamentus.
Rekomenduojama literatūra
„ES bendrasis duomenų apsaugos reglamentas (BDAR): komentaras“, Lukas Feiler ir Nikolaus Forgó • Šiame komentare pateikiama išsami informacija apie BDAR, kuri yra būtina norint suprasti ES reguliavimo aplinką ir jos poveikį kibernetinio saugumo praktikai.

„Duomenų apsauga ir kibernetinis saugumas Europoje: teisiniai pagrindai ir praktiniai aspektai“ (Data Protection and Cybersecurity in Europe: Legal Frameworks and Practical Considerations), autorius Paul Lambert

- Šioje knygoje pateikiama praktinė informacija apie duomenų apsaugos ir kibernetinio saugumo strategijų suderinimą ES, įskaitant atitiktį reglamentams ir geriausią saugumo priemonių praktiką.

„Tinklų ir informacijos saugumas: Europos ir tarptautinės perspektyvos“, redagavo Jeanne Pia Mifsud Bonnici ir Joe Cannataci

- Šiame rinkinyje nagrinėjama tinklų ir informacijos saugumo padėtis tiek Europos, tiek tarptautiniu mastu, pateikiant platesnį ES kibernetinio saugumo pastangų kontekstą.

„Dirbtinis intelektas kibernetiniame saugume: praktika, iššūkiai ir etika“, Elena Fersman ir Martin Fredriksson

- Išsami apžvalga apie dirbtinio intelekto technologijų integravimą į kibernetinį saugumą, kurioje nagrinėjami etiniai, operaciniai ir reguliavimo iššūkiai, ypač aktualūs ES kontekste.

„Kibernetinis saugumas skaitmeniniame amžiuje: įrankiai, technikos ir taikymas“, autoriai Gregory B. White, Eric A. Fisher ir James L. Antonakos

- Nors ši knyga nėra skirta išskirtinai ES, joje taip pat aptariama daugybė šiuolaikinių kibernetinio saugumo aspektų.

Studijų medžiaga *(HackerU ir Cybint originali medžiaga)*
Privaloma literatūra
• TCP/IP tinklo administravimas: pagalba Unix sistemos administratoriams, 3-iasis leidimas, Craig Hunt (O'Reilly) • „Būtiniausi sistemos administravimo žinios: komandos ir failų formatai“ (Pocket Administrator), Eleen Frisch (O'Reilly) • Kompiuterių tinklai: pradedančiųjų vadovas kompiuterių tinklų, interneto ir OSI modelio įsisavinimui, autorius Ramon Nastase
Rekomenduojama literatūra
• CompTIA A+ sertifikatas „Viskas viename“ pradedantiesiems (kompiuteriai/technologijos), 5-asis leidimas, autoriai Glen E. Clarke, Edward Tetz, Timothy L. Warner • „Coding All-in-One For Dummies“ 1-asis leidimas, autorius Nikhil Abraham • Informacinių technologijų pagrindai, 1 tomas: Įvadas į informacines sistemas, autorius Eric Frick • IT architektūra pradedantiesiems, 1-asis leidimas, autoriai: Kalani Kirk Hausman, Susan L. Cook • Kibernetinis saugumas „For Dummies“ (kompiuteriai/technologijos) 1-asis leidimas, autorius Steinberg • Linux pradedantiesiems, 10-asis leidimas, autorius Richard Blum • „Windows 10 pradedantiesiems“, 3-iasis leidimas (kompiuteriai/technologijos), autorius Rathbone • Tinklai pradedantiesiems, 12-asis leidimas, autorius Doug Lowe

6. M6: KIBERSAUGUMO PLANAVIMAS

Modulio pavadinimas	Modulio kodas
KIBERSAUGUMO PLANAVIMAS	

Lektorius (-iai)	Institucija ar katedra, kurioje dėstomas modulis

Pateikimo būdas	Kalba
Kontaktiniu būdu, nuotoliniu būdu, mišriuoju būdu, konsultacijos	*Anglų, suomių, turkų, norvegų, lietuvių, rumunų, prancūzų, lenkų, ispanų*

Reikalavimai
-

Suteiktų ECTS kreditų skaičius	Studento darbo krūvis	Kontaktinės darbo valandos	Individualios darbo valandos
3	75	50	25

Modulio tikslas ir rezultatai		
Baigę šį kursą, studentai sugebės suprasti ir taikyti pagrindinius kibernetinio saugumo planavimo ir valdymo principus. Jie įgis gebėjimų įgyvendinti tarptautinius standartus ir sistemas, kurti ilgalaikes saugumo strategijas, valdyti operacines ir taktines kibernetinio saugumo priemones bei planuoti saugias tinklo architektūras, pvz., debesų ir „zero trust“. Be to, studentai bus pasirengę kurti veiksmingus incidentų reagavimo planus ir įgyvendinti verslo tęstinumo strategijas, užtikrinančias organizacijos atsparumą ir veiksmingas kibernetinio saugumo priemones kintančių grėsmių akivaizdoje.		
Modulio mokymosi rezultatai	**Mokymo ir mokymosi metodai**	**Vertinimo metodai**
Žinios. Studentai įgis pažengusių žinių apie tai, kaip integruoti pažangius kibernetinio saugumo principus ir dabartines tendencijas į strateginį planavimą ir operacinį valdymą.	Paskaitos, atvejų analizė, grupinės diskusijos, savarankiškas mokymasis	Savitikros testai, žinių vertinimo testai
Įgūdžiai. Studentai įgis strateginio planavimo ir operacinio valdymo įgūdžių, kurie leis jiems veiksmingai kurti ir įgyvendinti kibernetinio saugumo strategijas, skirtas naujiems rizikos veiksniams spręsti ir užtikrinti tvirtus taktinius atsakus.	Praktiniai užsiėmimai, seminarai, atvejų analizė	Projektų vertinimai, praktiniai vertinimai

Kompetencijos. Studentai įgis kompetencijų kurti ir įgyvendinti strategines kibernetinio saugumo sistemas, vadovauti kibernetinio saugumo iniciatyvoms ir jas valdyti	Seminarai, praktiniai užsiėmimai, vaidmenų žaidimai	Nuolatinis vertinimas, scenarijų pagrįsti testai

Modulio turinys: temų suskirstymas	**Kontaktinės darbo valandos**					**Individualios darbo valandos ir užduotys**	
	Paskaitos (HEI)	Konsultacijos	Praktika (HEI)	Testai	**Visi kontaktiniai darbai**	**Individualus darbas**	**Užduotys**
1. Įvadas į kibernetinio saugumo planavimą: duomenų, žmonių ir visuomenės saugumas - duomenų saugumas - informacijos saugojimo saugumas, tyrimo procesas - duomenų saugumas – slaptažodžių atakos metodai -žmogaus saugumas – sąmoningumas ir supratimas - visuomenės saugumas – kas yra kibernetiniai nusikaltimai, kibernetinė etika - visuomenės saugumas – kibernetiniai įstatymai – skaitmeniniai įrodymai, skaitmeniniai kontraktai, tarptautinės konvencijos (susitarimai)	8	0,5	6	0,5	**15**	**8**	Apibrėžti duomenų, žmonių ir visuomenės saugumo teisinius aspektus, įstatymus ir politiką, reglamentuojančią duomenis MVĮ. Klasifikuoti MVĮ aktualius kibernetinių atakų tipus. Nustatyti naudingas priemones kibernetinėms atakoms užkirsti kelią.
2. Strateginis planavimas -Kibernetinio saugumo tikslų ir uždavinių apibrėžimas -SWOT analizė (stiprybės, silpnybės, galimybės, grėsmės) -Ilgalaikių saugumo strategijų kūrimas -Pagrindinių veiklos rodiklių (KPI) nustatymas -Saugumo strategijos peržiūra ir atnaujinimas	8	2	6	2	**18**	**8**	Naudojantis SWOT analize, apibrėžti MVĮ aktualius kibernetinio saugumo tikslus, parengti ilgalaikes strategijas rizikai mažinti, atitinkamai paskirstyti išteklius ir biudžetą, nustatyti KPI, kad galima būtų įvertinti pažangą, ir reguliariai atnaujinti strategiją atsižvelgdami į naujas grėsmes.

3. Operacinis ir taktinis valdymas -Prieigos kontrolės įgyvendinimas -Pataisų valdymas ir programinės įrangos atnaujinimai -Nuolatinis sistemos stebėjimas - Darbuotojų saugumo sąmoningumo mokymas	8	1	6	2	**17**	**9**	Įgyvendinti prieigos kontrolės priemones, siekiant apriboti neteisėtą prieigą, prižiūrėti sistemas naudojant pataisų valdymą, nustatyti neįprastos veiklos stebėjimą ir teikti darbuotojams mokymus apie kibernetines grėsmes.
Iš viso	**24**	**3,5**	**18**	**4,5**	**50**	**25**	

Vertinimo strategija	**Lyginamasis svorio procentas**	**Vertinimo kriterijai**
Savitikros testas (1)	10	10 balų – 95–100 % teisingų atsakymų. 9 balai – 85–94 % teisingų atsakymų. 8 balai – 75–84 % teisingų atsakymų. 7 balai – 65–74 % teisingų atsakymų. 6 balai – 55–64 % teisingų atsakymų. 5 balai – 45–54 % teisingų atsakymų. 4 balai – 35–44 % teisingų atsakymų. 3 balai – 25–34 % teisingų atsakymų. 2 balai – 15–24 % teisingų atsakymų. 1 balas – 0–14 % teisingų atsakymų.
Savitikros testas (2)	10	
Savitikros testas (3)	10	
Žinių vertinimo testas	70	

Tyrimų medžiaga *(Pavardė, vardo inicialas. (Metai, mėnuo, diena). Straipsnio pavadinimas. Žurnalo/laikraščio pavadinimas, tomo numeris, viso straipsnio puslapių numeriai, leidėjas, URL nuoroda)*

Privaloma literatūra

1. Nair, A., & Greeshma, M. R. (2023). Informacijos saugumo atitikties valdymo įsisavinimas: išsamus vadovas apie ISO/IEC 27001:2022 atitiktį. Packt Publishing Limited.
2. Falco, G. J., & Rosenbach, E. (2021). Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity. Oxford University Press.
3. NIST kibernetinio saugumo sistema (CSF) 2.0, Nacionalinis standartų ir technologijų institutas, 2024 m. vasario 26 d.

Rekomenduojama literatūra

1. Mehta, S. (2023). *ISACA sertifikuotas rizikos ir informacinių sistemų kontrolės (CRISC®) egzaminų vadovas*. Packt Publishing Limited.
2. Gregory, P. H. (2021). *CISM sertifikuoto informacijos saugumo vadybininko visapusiškas egzaminų vadovas*. McGraw-Hill.
3. ISACA. (2021). *CRISC peržiūros vadovas, 7-asis leidimas*. ISACA.
4. Europos Parlamentas ir Taryba. (2022 m. gruodžio 14 d.). *Reglamentas (ES) 2022/2554 dėl finansų sektoriaus skaitmeninio veiklos atsparumo*.
5. Bendrojo duomenų apsaugos reglamento (BDAR) vadovas, Informacijos komisaro biuras

7. M7: RIZIKOS VALDYMAS IR RIKIKOS ŠVELNINIMAS

Modulio pavadinimas	Modulio kodas
RIZIKOS VALDYMAS IR RIZIKOS ŠVELNINIMAS	

Lektorius (-iai)	Institucija ar katedra, kurioje dėstomas modulis

Pateikimo būdas	Kalba
Kontaktiniu būdu, nuotoliniu būdu, mišriuoju būdu, konsultacijos	*Anglų, suomių, turkų, norvegų, lietuvių, rumunų, prancūzų, lenkų, ispanų*

Reikalavimai			
Nėra			
Suteiktų ECTS kreditų skaičius	**Studento darbo krūvis**	**Kontaktinės darbo valandos**	**Individualios darbo valandos**
3	75	50	25

Modulio tikslas ir rezultatai		
Baigę šį kursą, studentai gebės nuolat valdyti (identifikuoti, analizuoti, vertinti, įvertinti, mažinti) su kibernetiniu saugumu susijusius IKT infrastruktūrų, sistemų ir paslaugų rizikos veiksnius, planuojant, taikant, pranešant ir komunikuojant rizikos analizę, vertinimą ir tvarkymą.		
Modulio mokymosi rezultatai	**Mokymo ir mokymosi metodai**	**Vertinimo metodai**
Žinios. Studentai įgis žinių apie rizikos valdymo procesus, įskaitant rizikos identifikavimą, vertinimą ir kontrolę, kurios leis jiems nustatyti ir apibūdinti veiksmingas kibernetinio saugumo procedūras, pritaikytas prie konkrečių MVĮ darbo vietų poreikių, laikantis nacionalinių ir tarptautinių standartų.	Dėstytojas pasirenka mokymo ir mokymosi metodus iš D2.3 ataskaitos 1.3 dalies [*Mokymo metodai, pvz., teorinės paskaitos, literatūros analizė, kviestiniai lektoriai, tarpusavio mokymas ir mokymasis, mentorystė ir kt.].*	Savitikros testai Žinių vertinimo testas

Įgūdžiai. Studentai įgis įgūdžių taikyti metodikas ir priemones, kad galėtų atlikti rizikos vertinimus, kurti ir įgyvendinti veiksmingas rizikos valdymo strategijas bei kurti patikimas kibernetinio saugumo procedūras, pritaikytas konkrečiai MVĮ darbo vietoms.	Dėstytojas pasirenka mokymo ir mokymosi metodus iš D2.3 ataskaitos 1.3 dalies [*Mokymo metodai, pvz., praktinės užduotys/laboratoriniai darbai, viktorinos, žaidimai, techninių vaizdo įrašų analizė, atvejų analizė, praktinės veiklos ir kt.*].	Savitikros testai Žinių vertinimo testas
Kompetencijos. Studentai įgis kompetencijų kurti ir įgyvendinti strategines kibernetinio saugumo politikos priemones MVĮ darbo vietose.	Dėstytojas pasirenka mokymo ir mokymosi metodus iš D2.3 ataskaitos 1.3 dalies [*Mokymo metodai, pvz., konkursai, CTF, imituojamos aplinkos, 5E, CBL, CL, PBL* ir *kt.*].	Savitikros testai Žinių vertinimo testas

Modulio turinys: temų suskirstymas	Kontaktinės darbo valandos					Individualios darbo valandos ir užduotys	
	Paskaitos (HEI)	Konsultacijos	Praktika (HEI)	Testai	Visi kontaktiniai darbai	Individualūs darbai	Užduotys
Rizikos vertinimas - Bendrasis rizikos valdymo procesas - Bendrasis rizikos valdymo modelis - Rizikos valdymo principai - Rizikos valdymo standartai - Praktiniai pavyzdžiai	2	0	2	0	**4**	5	- Trumpai apibūdinti pagrindinius rizikos valdymo proceso etapus, įskaitant rizikos identifikavimą, vertinimą ir kontrolę. - Apibrėžti vidinius ir išorinius rizikos valdymo kontekstus MVĮ. Nurodyti rizikos vertinimo apimtį ir identifikuoti pagrindinius rizikos veiksnius. - Parengti rizikos kriterijus, būdingus pasirinktam MVĮ.
Rizikos identifikavimas - Lyderystė ir įsipareigojimas rizikos valdymo srityje - Rizikos valdymo veiklos apimties apibrėžimas - Rizikos valdymo konteksto išorinis ir vidinis kontekstas - Apčiuopiami ir neapčiuopiami rizikos šaltiniai - Priežastys ir įvykiai - Grėsmės ir galimybės - Pažeidžiamumai ir gebėjimai - Išorinio ir vidinio konteksto pokyčiai - Kylančių rizikų rodikliai - Turto ir išteklių pobūdis ir vertė - Pasekmės ir jų poveikis tikslams - Žinių ribotumas ir informacijos patikimumas	4	0	4	0	**8**	5	- Nustatyti apčiuopiamus ir neapčiuopiamus rizikos šaltinius MVĮ. Klasifikuoti rizikas pagal priežastis, įvykius, grėsmes ir galimybes. - Analizuoti MVĮ vidinius pažeidžiamumus ir galimybes bei įvertinti, kaip išoriniai ir vidiniai pokyčiai gali paveikti verslą. - Nustatyti potencialias naujas rizikas MVĮ ir pasiūlyti rodiklius joms stebėti. Apsvarstyti, kaip turto ir išteklių pobūdis ir vertė daro įtaką šiai

- Dalyvių šališkumas, prielaidos ir įsitikinimai - Praktiniai pavyzdžiai ir atvejų analizė							analizei.
Vidaus grėsmės - Vidinių grėsmių apibrėžimas ir tipai - Vidinių grėsmių kuriama žala - Vidinių grėsmių mažinimo programos kūrimas - Vidinių grėsmių aptikimas ir nustatymas - Vidinių grėsmių vertinimas - Vidinių grėsmių valdymas - Praktiniai pavyzdžiai ir atvejų analizė	6	0	6	0	**12**	5	- Apibrėžti ir klasifikuoti įvairių tipų vidinius pavojus, susijusius su MVĮ. Aptarti galimas išlaidas, kurias šie pavojai gali sukelti verslui. - Parengti pagrindinę vidinių grėsmių mažinimo programą MVĮ. Išskirti pagrindinius komponentus, pvz., aptikimo, identifikavimo ir valdymo strategijas. - Pasiūlyti vidinių grėsmių vertinimo metodą ir apibūdinti veiksmus, kuriais šias grėsmes galima veiksmingai valdyti MVĮ kontekste.
Rizikos matavimo ir vertinimo modeliai bei metodikos - Kiekybiniai ir kokybiniai rizikos vertinimo modeliai ir metodikos - Įvykių tikimybė ir pasekmės - Pasekmių pobūdis ir mastas - Sudėtingumas ir sąsajumas - Su laiku susiję veiksniai ir kintamumas - Esamų valdymo priemonių veiksmingumo vertinimas - Jautrumo ir pasitikėjimo lygmenys - Praktiniai pavyzdžiai ir atvejų analizė	6	0	6	0	**12**	5	- Palyginti ir kontrastuoti vieną kiekybinį ir vieną kokybinį rizikos vertinimo modelį. - Įvertinti rizikos įvykio tikimybę ir jo pasekmių pobūdį bei mastą MVĮ. Apsvarstyti, kaip sudėtingumas, su laiku susiję veiksniai ir nepastovumas įtakoja šį vertinimą. - Įvertinti esamų kontrolės priemonių veiksmingumą nustatytų rizikų valdymo srityje. Įtraukti kontrolės

							priemonių jautrumo ir patikimumo lygių analizę.
Rizikos kontrolė - Rizikos valdymo variantų formulavimas ir pasirinkimas - Rizikos valdymo planavimas ir įgyvendinimas - Vertinimas, kaip veiksmingai rizika buvo valdyta - Sprendimas, ar likusi rizika yra priimtina - Stebėjimas ir peržiūra - Registravimas ir ataskaitų teikimas - Praktiniai pavyzdžiai ir atvejų analizė	6	0	6	0	**12**	5	- Nustatyti ir pasirinkti tinkamas rizikos valdymo galimybes MVĮ. Pateikti savo pasirinkimo motyvus, remiantis susijusių rizikų pobūdžiu. - Parengti trumpą rizikos valdymo planą, kuriame būtų apibūdinta, kaip pasirinktos rizikos valdymo priemonės bus įgyvendinamos MVĮ aplinkoje. - Pasiūlyti metodą, kaip įvertinti rizikos valdymo veiksmingumą ir nustatyti, ar likusi rizika yra priimtina.
Iš viso	**24**	**2**	**24**	**0**	**50**	**25**	

Vertinimo strategija	**Lyginamasis svorio procentas**	**Vertinimo kriterijai**
Savitikros testas (1)	5	10 balų – 95–100 % teisingų atsakymų. 9 balai – 85–94 % teisingų atsakymų. 8 balai – 75–84 % teisingų atsakymų. 7 balai – 65–74 % teisingų atsakymų. 6 balai – 55–64 % teisingų atsakymų. 5 balai – 45–54 % teisingų atsakymų. 4 balai – 35–44 % teisingų atsakymų. 3 balai – 25–34 % teisingų atsakymų. 2 balai – 15–24 % teisingų atsakymų. 1 balas – 0–14 % teisingų atsakymų.
Savitikros testas (2)	5	
Savitikros testas (3)	5	
Savitikros testas (4)	5	
Savitikros testas (5)	5	
Žinių vertinimo testas	75	

Studijų medžiaga *(Pavardė, vardo inicialas. (Metai, mėnuo, diena). Straipsnio pavadinimas. Žurnalo/laikraščio pavadinimas, tomo numeris, viso straipsnio puslapių numeriai, leidėjas, URL nuoroda)*

Privaloma literatūra

1. Adarsh Nair ir Greeshma M. R. (2023) Informacijos saugumo atitikties valdymo įsisavinimas: išsamus vadovas apie atitiktį ISO/IEC 27001:2022 standartui. Packt Publishing, Limited https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30652023&query=risk%20management

2. Gregory J. Falco, Eric Rosenbach (2021) Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity. Oxford university press, eBook
3. Kristina Narvaez, Betty Simkins, John Fraser (2014) Įmonės rizikos valdymo įgyvendinimas: atvejų analizė ir geriausia praktika. John Wiley & Sons
4. ENISA (2022) Rizikos valdymo standartai
5. 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių, skirtų užtikrinti aukštą bendrą kibernetinio saugumo lygį visoje Sąjungoje, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyvą (ES) 2018/1972 bei panaikinanti Direktyvą (ES) 2016/1148 (NIS 2 direktyva)
6. ISO 31000 Rizikos valdymas. Gairės

Rekomenduojama literatūra

1. Shobhit Mehta (2023) ISACA sertifikuotas rizikos ir informacinių sistemų kontrolės (CRISC®) egzaminų vadovas. Packt Publishing, Limited **https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30806680&query=risk%20management**
2. Peter H. Gregory (2021) CISM sertifikuoto informacijos saugumo vadybininko visapusiškas egzaminų vadovas. McGraw-Hill
3. ISACA (2021) CRISC peržiūros vadovas, 7-asis leidimas. ISACA
4. 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 dėl finansų sektoriaus skaitmeninio veiklos atsparumo ir reglamentų (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011

8. M8: VERSLO TĘSTINUMAS, VEIKLOS ATKŪRIMAS PO NELAIMIŲ, INCIDENTŲ VALDYMAS IR PERSONALO SAUGUMAS

Modulio pavadinimas	Modulio kodas
VERSLO TĘSTINUMAS, VEIKLOS ATKŪRIMAS PO NELAIMIŲ, INCIDENTŲ VALDYMAS IR PERSONALO SAUGUMAS	

Lektorius (-iai)	Institucija ar katedra, kurioje dėstomas modulis

Pateikimo būdas	Kalba
Kontaktiniu būdu, nuotoliniu būdu, mišriuoju būdu, konsultacijos	*Anglų, suomių, turkų, norvegų, lietuvių, rumunų, prancūzų, lenkų, ispanų*

Reikalavimai
Nėra

Suteiktų ECTS kreditų skaičius	Studento darbo krūvis	Kontaktinės darbo valandos	Individualios darbo valandos
3	75	50	25

Modulio tikslas ir rezultatai

Baigę šį kursą, studentai gebės formuluoti ir administruoti išsamius verslo tęstinumo ir nelaimių atkūrimo (BC/DR) planus, kurti funkcionalią incidentų valdymo programą ir nustatyti tvirtą ir veiksmingą personalo saugumo politiką. Studentai išmoks, kaip apsaugoti turtą, užtikrinti, kad būtų išvengta pernelyg didelių nuostolių, užkirsti kelią prastovoms, išvengti ar apriboti krizines situacijas ir krizės valdymo aplinką.
Baigę šį kursą, studentai sugebės parengti ir stebėti nuolatinį išsamaus kibernetinio saugumo vadovo, skirto MVĮ, įgyvendinimą, naudodami pažangius kibernetinio saugumo principus ir technologijas, integruotas pagal visus nacionalinius ir tarptautinius įstatymus. Studentai taip pat stebės, kaip šis vadovas yra įgyvendinamas.

Modulio mokymosi rezultatai	Mokymo ir mokymosi metodai	Vertinimo metodai
Žinios. Studentai įgis pažengusių žinių apie tai, kaip sukurti ir įgyvendinti išsamų MVĮ darbo vietos kibernetinio saugumo vadovą, įtraukiant pažangius kibernetinio saugumo principus, naujausius gynybos mechanizmus ir laikantis nacionalinių bei tarptautinių teisės aktų ir standartų incidentų valdymo, verslo tęstinumo ir personalo saugumo srityse.	Dėstytojas pasirenka mokymo ir mokymosi metodus iš D2.3 ataskaitos 1.3 dalies [Mokymo metodai].	Savitikros testai, žinių vertinimo testas

Įgūdžiai. Studentai įgis įgūdžių, kaip kurti ir prižiūrėti MVĮ darbo vietos kibernetinio saugumo vadovą, naudodami pažangias metodikas rizikai vertinti, kurti veiksmingas rizikos valdymo ir incidentų reagavimo strategijas bei rengti išsamius verslo tęstinumo planus, pritaikytus jų organizacijos poreikiams.	Dėstytojas pasirenka mokymo ir mokymosi metodus iš D2.3 ataskaitos 1.3 dalies [Mokymo metodai].	Savitikros testai, žinių vertinimo testas
Kompetencijos. Studentai įgis kompetencijų kurti ir įgyvendinti kibernetinio saugumo vadovą MVĮ, veiksmingai vadovauti saugumo projektams ir komandoms, užtikrinti atitiktį organizacijos tikslams ir atitikties įsipareigojimams.	Dėstytojas pasirenka mokymo ir mokymosi metodus iš D2.3 ataskaitos 1.3 dalies [Mokymo metodai].	Savitikros testai, žinių vertinimo testas

Modulio turinys: temų suskirstymas	**Kontaktinės darbo valandos**					**Individualios darbo valandos ir užduotys**	
	Paskaitos (HEI)	Konsultacijos	Praktika (HEI)	Testai	**Visi kontaktiniai darbai**	**Individualus darbas**	**Užduotys**
Reagavimas į incidentus - Incidentų reagavimo apibrėžimas ir svarba kibernetiniame saugume - Veiksmingo reagavimo į incidentus atkūrimo pagrindiniai komponentai - Dažniausių kibernetinio saugumo grėsmių apžvalga (phishing, vidinės grėsmės) - Incidentų reagavimo plano (IRP) rengimas - Incidentų reagavimo komandos narių vaidmenys ir atsakomybė - Incidento imitavimas: imitacinio plano įgyvendinimas	5	0,5	3	0,5	**9**	**5**	Parengti išsamų incidentų reagavimo planą savo MVĮ, įskaitant vaidmenis, atsakomybę ir veiksmus, kurių reikia imtis kibernetinio saugumo incidento metu. Imituoti incidentą ir surengti pratybas, siekiant patikrinti savo plano veiksmingumą.

Atkūrimas po nelaimių - Supratimas apie atkūrimą po nelaimės - Nelaimių atkūrimo plano parengimas - Vaidmenys ir atsakomybė atkuriant veiklą po nelaimės - Atkūrimo veiksmai po nelaimės	5	0,5	3	0,5	**9**	**5**	Sukurti nelaimių atkūrimo planą, kuriame būtų apibrėžtos IT infrastruktūros ir duomenų atkūrimo procedūros po katastrofiško įvykio. Įtraukti atkūrimo grafiką ir paskirstyti atsakomybę komandos nariams už kiekvieną proceso etapą.
Verslo tęstinumas - Verslo tęstinumo supratimas - Verslo tęstinumo plano (BCP) kūrimas - Vaidmenys ir atsakomybė užtikrinant verslo tęstinumą - Verslo poveikio analizė - BCP testavimas ir tobulinimas	5	0,5	3	0,5	**9**	**5**	Parengti verslo tęstinumo planą, kuris užtikrintų, kad kritinės verslo funkcijos veiktų ir per sutrikimus, ir po jų. Nustatyti esmines paslaugas ir išteklius bei apibrėžti nepaprastųjų situacijų strategijas, kad jos būtų išlaikytos įvairiais scenarijais.
Saugumo sąmoningumas, mokymas ir švietimas - Saugumo sąmoningumo supratimas - Saugumo mokymo programos kūrimas - Darbuotojų atsakomybė kibernetinio saugumo srityje - Saugumo sąmoningumo veiksmingumo vertinimas	1	0,5	2	0,5	**4**	**1**	Parengti saugumo sąmoningumo mokymo programą savo MVĮ, sutelkiant dėmesį į pagrindines kibernetinio saugumo politikos nuostatas ir geriausią praktiką. Surengti mokymo sesiją darbuotojams ir įvertinkite jų supratimą per viktorinas ar interaktyvias veiklas.
Saugumo įdarbinimo praktika - Saugumo pareigų reikalavimų apibrėžimas - Išsamios praeities patikros - Interviu dėl saugumo komponentų - Nuolatinis vertinimas ir tobulinimas	1	0,5	2	0,5	**4**	**1**	Nustatyti saugumu grindžiamas įdarbinimo praktikas, įskaitant kandidatų praeities patikrinimus ir pokalbių klausimus, skirtus įvertinti kandidatų supratimą apie kibernetinį saugumą. Sudaryti būsimų darbuotojų būtinų saugumo kvalifikacijų ir savybių planą.

Saugumo nutraukimo praktika - Nedelsiant atšaukti prieigą - Duomenų ir įrenginių susigrąžinimas - Išėjimo iš darbo pokalbis dėl saugumo įžvalgų - Pranešimas atitinkamoms komandoms - Teisiniai ir atitikties reikalavimams aspektai	1	0,5	2	0,5	**4**	**2**	Parengti saugią atleidimo iš darbo procedūrą, apimančią prieigos atšaukimą, įmonės turto susigrąžinimą ir išėjimo iš darbo pokalbius. Įgyvendinti imituotą atleidimo iš darbo scenarijų, kad būtų galima įvertinti procedūros veiksmingumą.
Trečiųjų šalių saugumas - Trečiųjų šalių rizikos vertinimas - Tinkamas tiekėjų atrankos procesas - Kontrastų ir saugumo reikalavimų įgyvendinimas - Nuolatinis stebėjimas ir auditas - Reagavimas į incidentus ir komunikacija	2	0,5	2	0,5	**5**	**2**	Nustatyti galimas rizikas, susijusias su trečiosiomis šalimis, ir sukurti saugumo vertinimo kontrolinį sąrašą, kad būtų galima įvertinti, ar jos atitinka jūsų MVĮ kibernetinio saugumo standartus. Parengti sutarties šabloną, kuriame būtų nurodyti saugumo reikalavimai ir baudos už jų nesilaikymą.
Saugumas peržiūros procesuose - Saugumo įtraukimas į peržiūras - Reguliarių saugumo auditų atlikimas - Pažeidžiamumo vertinimas ir įsiskverbimo testavimas - Peržiūros po incidentų	1	0,5	1,5	0,5	**3, 5**	**2**	Parengti procesą, skirtą reguliariai peržiūrėti ir atnaujinti savo MVĮ kibernetinio saugumo politiką ir procedūras. Suplanuoti ir atlikti imituojamą auditą, siekiant įsitikinti , jog visos saugumo priemonės yra atnaujintos ir atitinka atitinkamus standartus.

Darbuotojų duomenų saugumas - Duomenų rinkimo apribojimai - Saugojimas ir prieigos kontrolė - Privatumo taisyklių laikymasis - Duomenų dalijimasis ir trečiosios šalys - Darbuotojų sutikimas ir teisės	2	0,5	2	0,5	**5**	**2**	Parengti privatumo politiką, skirtą darbuotojų asmeninės informacijos tvarkymui, užtikrinant atitiktį duomenų apsaugos įstatymams ir geriausiai praktikai. Atlikti rizikos vertinimą, siekiant nustatyti galimas pažeidžiamas vietas, susijusias su darbuotojų duomenų saugojimu ir tvarkymu.
Iš viso	**23**	**2**	**20,5**	**4,5**	**50**	**25**	

Vertinimo strategija	**Lyginamasis svorio procentas**	**Vertinimo kriterijai**
Savitikros testas (1)	5	10 balų – 95–100 % teisingų atsakymų. 9 balai – 85–94 % teisingų atsakymų. 8 balai – 75–84 % teisingų atsakymų. 7 balai – 65–74 % teisingų atsakymų. 6 balai – 55–64 % teisingų atsakymų. 5 balai – 45–54 % teisingų atsakymų. 4 balai – 35–44 % teisingų atsakymų. 3 balai – 25–34 % teisingų atsakymų. 2 balai – 15–24 % teisingų atsakymų. 1 balas – 0–14 % teisingų atsakymų.
Savitikros testas (2)	5	
Savitikros testas (3)	5	
Savitikros testas (4)	5	
Savitikros testas (5)	5	
Žinių vertinimo testas	75	

Studijų medžiaga *(Pavardė, vardo inicialas. (Metai, mėnuo, diena). Straipsnio pavadinimas. Žurnalo/laikraščio pavadinimas, tomo numeris, viso straipsnio puslapių numeriai, leidėjas, URL nuoroda)*

Privaloma literatūra

- Gregory J. Falco, Eric Rosenbach (2021). *Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity*. Oxford University Press, eBook.
- Michael Wallace, Lawrence Webber (2017). *Nelaimių atkūrimo vadovas: žingsnis po žingsnio planas, skirtas užtikrinti verslo tęstinumą ir apsaugoti svarbias operacijas, įrenginius ir turtą.* AMACOM.
- Nacionalinis standartų ir technologijų institutas (NIST). *Informacinių technologijų sistemų nenumatytų atvejų planavimo vadovas*. NIST SP 800-34 Rev. 1.
- Cochran, K.A. (2024). Incidentų reagavimas, verslo tęstinumas ir atkūrimas po nelaimės. Įtraukta į: „Kibernetinio saugumo pagrindai“. Apress, Berkeley, CA. **https://doi.org/10.1007/979-8-8688-0432-8_14**

Rekomenduojama literatūra

- ISACA (2023). *CISM peržiūros vadovas, 15-asis leidimas*. ISACA.

- Peter H. Gregory (2021). *CISM sertifikuoto informacijos saugumo vadybininko visapusiškas egzaminų vadovas*. McGraw-Hill.
- IT valdymas (2022). *ISO 22301:2019 – Verslo tęstinumo valdymo sistemos. Reikalavimai*.
- M. Souppaya, L. Feldman, G. Witte [2024], Kibernetinio saugumo incidentų atkūrimo vadovas, Kompiuterinio saugumo skyrius, Informacinių technologijų laboratorija, Nacionalinis standartų ir technologijų institutas, JAV prekybos departamentas
- Ihab Hanna Sawalha [2021]. Nuomonės apie verslo tęstinumą ir atkūrimą po nelaimių. Tarptautinis skubios pagalbos tarnybų žurnalas

PRIEDAI

MODULIO APRAŠYMO ŠABLONAS

MODULIO APRAŠYMAS

Modulio pavadinimas	Modulio kodas
...	

Lektorius (-iai)	Institucija ar katedra, kurioje dėstomas modulis
...	...

Pateikimo būdas	Kalba
	Anglų, ...

Reikalavimai
...

Paskirtų ECTS kreditų skaičius	Studento darbo krūvis	Kontaktinės darbo valandos	Individualios darbo valandos
3	...	...	...

Modulio tikslas ir rezultatai		
...		
Modulio mokymosi rezultatai	**Mokymo ir mokymosi metodai**	**Vertinimo metodai**

Išteklių (įrangos, programinės įrangos, technologijų) naudojimas
...

Modulio turinys: temų suskirstymas	Kontaktinės darbo valandos					Individualios darbo valandos ir užduotys	
	Paskaitos (HEI)	Konsultacijos	Praktika (HEI)	Testai	**Visi kontaktiniai darbai**	**Individualus darbas**	**Užduotys**
1							
...							
n							
Iš viso							

Vertinimo strategija	Lyginamasis svorio procentas	Vertinimo kriterijai
Savęs vertinimas I		...
...		...
Savikontrolės testas n		...
Žinių vertinimo testas		...

Tyrimų medžiaga *(Pavardė, vardo inicialas. (Metai, mėnuo, diena). Straipsnio pavadinimas. Žurnalo/laikraščio pavadinimas, tomo numeris, viso straipsnio puslapių numeriai, leidėjas, URL nuoroda)*
Privaloma literatūra
...
Rekomenduojama literatūra
...

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau