REPUBLIKA E SHQIPËRISË
MINISTRIA E EKONOMISË, KULTURËS DHE INOVACIONIT
Agjencia Kombëtare e Arsimit, Formimit Profesional dhe Kualifikimeve

SKELETKURRIKULI

Për Profilin Mësimor

SIGURIA KIBERNETIKE

Niveli V i KSHK
(2 vjeçar)

Kodi: T1-V-24

Miratoi

MINISTRI

Tiranë, 2024

Përmbajtja:

1. Qëllimet e arsimit profesional pas të mesmes në profilin "Siguria kibernetike", niveli V i KSHK.

Qëllimi kryesor i arsimimit profesional në profilin "Siguria kibernetike", niveli V i KSHK, është "përgatitja e nxënësve me kompetencat profesionale të nevojshme për t'u punësuar në veprimtaritë profesionale që lidhen drejtpërdrejt me profesionin e specialistit të sigurisë kibernetike në funksion të identifikimit, testimit, monitorimit, vlerësimit dhe optimizimit të parametrave të sigurisë, si dhe të reagimit ndaj sulmeve kibernetike". Për të realizuar këtë, shkolla profesionale, në nivelin pas të mesëm, u krijon nxënësve:

- mundësi të përshtatshme për të nxënë, pavarësisht nga gjinia, raca, besimi dhe aftësitë;
- mundësi për të gjithë, për të zhvilluar kompetencat profesionale, të bazuara në njohuritë, shprehitë, qëndrimet dhe vlerat, të mjaftueshme për të lehtësuar punësimin dhe përparimin drejt arsimit e formimit profesional të mëtejshëm;
- mbështetje për t'u njohur me teknologjitë e proceset teknologjike bashkëkohore e të perspektivës, që lidhen me kualifikimin profesional përkatës;
- mbështetje për të zhvilluar ndjenjën e disiplinës, kuriozitetin intelektual dhe profesional, aftësitë sipërmarrëse, si dhe vlerat morale;
- mbështetje për t'u zhvilluar psikologjikisht, për të përballuar vështirësitë që do të ndeshin gjatë veprimtarive të ardhshme profesionale;
- mbështetje për të zhvilluar frymën e tolerancës dhe të mirëbesimit nëpërmjet përvojës së punës.

II. Profili profesional i nxënësve në përfundim të arsimit profesional në profilin "Siguria kibernetike", niveli V i KSHK.

1. Kërkesat e pranimit të nxënësve në arsimin profesional, në profilin "Siguria kibernetike", niveli V i KSHK.

Në shkollat që ofrojnë arsimin profesional në profilin mësimor "Siguria kibernetike", niveli V i KSHK, kanë të drejtë të regjistrohen të gjithë individët që:

- kanë përfunduar një kualifikim profesional të nivelit IV të KSHK të drejtimit Teknologji Informacioni dhe Komunikimi;
- kanë përfunduar të paktën një kualifikim të nivelit IV në KSHK dhe kanë eksperiencë pune, të vërtetuar, të paktën një vit në fushën e Teknologjisë së Informacionit dhe Komunikimit;
- janë në kushte shëndetësore që e lejojnë kryerjen e detyrës për përballimin e kërkesave të këtij niveli të arsimit profesional
- <u>nëse kanë aftësi të kufizuara</u>, institucioni arsimor u krijon kushte dhe e përshtat programin në përputhje me paaftësitë që shfaqin.

Nëse kërkesat për të ndjekur këtë kualifikim profesional janë më të larta se kapacitetet reale të shkollave, atëherë, institucioni përgjegjës përgatit udhëzime të veçanta me kritere të posaçme pranimi.

2. Kompetencat profesionale të nxënësit në përfundim të arsimimit në profilin "Siguria kibernetike", niveli V i KSHK.

Në përfundim të arsimit profesional në profilin profesional "Siguria kibernetike", niveli V i KSHK, nxënësi do të jetë i aftë të ushtrojë kompetencat profesionale si më poshtë:

- Të zbatojë manualet e pajisjeve të sigurisë;

- Të zbatojë manualet e software-ve të sigurisë;
- Të instalojë dhe konfigurojë pajisjet fizike të sigurisë;
- Të instalojë dhe konfigurojë software-t e sigurisë;
- Të testojë funksionimin e pajisjeve dhe software-ve të sigurisë;
- Të zbatojë metodat për rritjen e sigurisë në sistemet operative të paisjeve fundore;
- Të realizojë automatizimin e sigurisë së informacionit me programe në gjuhën *Python;*
- Të zbatojë funksionin e komponentëve kryesorë për identifikinim dhe mbrojtjen e të dhënave në sigurinë kibernetike;
- Të zbatojë metodat për rritjen e sigurisë në paisjet e lëvizshme *(mobile*);
- Të zbatojë metoda për rritjen e sigurisë në rrjetat pa tel *(Wireless)*;
- Të interpretojë dobësitë dhe problematikat e komponentëve fizik të rrjetit të komunikimit;
- Të konfigurojë një makinë virtuale për përvojën e të mësuarit të testimit të depërtimit;
- Të identifikojë dobësitë dhe problematikat e sistemeve operative dhe software-ve;
- Të kryejë testimeve të sigurisë kibernetike;
- Të përdorë protokollet e autentifikimit WPA, WPA2, WPA3, LDAP, AAA etj.;
- Të zbatojë kundërmasat ndaj sulmeve gjatë fazave të procesit të hakerimit etik;
- Të përdorë sistemet e monitorimit dhe analizimit të Log-ve si Sguil, Kibana, Wireshark, Zeek etj.;
- Të instalojë dhe konfigurojë software të parandalimit te humbjes së të dhënave;
- Të kontrollojë Log-et dhe transaksionet në rrjet;
- Të monitorojë llojet e ndërhyrjeve në rrjet;
- Të monitorojë zbatimin e rregullores dhe politikave të sigurisë për rrjetin e komunikimit;
- Të zbatojë teknologjitë dhe mjetet mbrojtëse nga sulmet kibernetike;
- Të interpretojë rëndësinë e përdorimit të playbook;
- Të vlerësojë mënyrat e shkrimit të raporteve për gjetjet e situatave kritike në sisteme;
- Të kontrollojë funksionalitetin e infrastrukturës IT;
- Të vlerësojë parametrat mbi sigurinë kibernetike;
- Të kontrollojë zbatimin e protokolleve të autentifikimit WPA, WPA2, WPA3, LDAP, AAA etj.;
- Të verifikojë anomalitë e shfaqura në sisteme në kohën e duhur;
- Të zbatojë rregullat e sigurimit teknik dhe të ruajtjes së mjedisit;
- Të komunikojë me etikë profesionale

3. Mundësitë e punësimit dhe të arsimimit të mëtejshëm në përfundim të arsimimit nëprofilin mësimor “Siguria kibernetike”, niveli V i KSHK.

Përfundimi me sukses i kualifikimit profesional “Siguria kibernetike”, niveli V i KSHK, i jep individit mundësi t'i drejtohet tregut të punës si specialist i sigurisë kibernetike për infrastrukturën e Teknologjisë së Informacionit dhe Komunikimit (TIK) dhe Teknologjisë Operacionale (TO) në fushën financiare, shëndetësore, industrinë energjetike, industrinë e rëndë, telekomunikacion, prodhim etj., si dhe të krijojë një biznes, si person fizik ose juridik, i cili ofron shërbime konsulence dhe zbatimi të projekteve të sigurisë kibernetike.

III. Plani mësimor për arsimin profesional në profilin "Siguria kibernetike", niveli V i KSHK (2 vjeçar).

Plani mësimor për profilin mësimor "Siguria kibernetike", Niv. V i KSHK (2 vjeçar)				
Nr	**Kodi**	**Modulet mësimore**	**Orët mësimore**	
			Viti I	**Viti II**
1	M-26-2057-24	Hyrje në sigurinë kibernetike	54	-
2	M-26-2058-24	Sistemet e teknologjisë së informacionit.	135	-
3	M-26-2059-24	Legjislacioni, etika dhe standardet në sigurinë kibernetike	162	-
4	M-26-2060-24	Zbatimi i *Python* në sigurinë kibernetike	81	-
5	M-26-2061-24	Instalimi dhe konfigurimi i sistemeve të sigurisë kibernetike	135	-
6	M-26-2062-24	Siguria e pajisjeve fundore	108	-
7	M-26-2063-24	Gjurmimi dhe identifikimi i faktorëve të dëmshëm.	135	-
8	M-26-2064-24	Testimi i sigurisë kibernetike	-	162
9	M-26-2065-24	Kriptimi dhe parandalimi i humbjes së të dhënave.	-	162
10	M-26-2066-24	Monitorimi dhe vlerësimi i sistemeve të sigurisë kibernetike	-	162
11	M-26-2067-24	Garantimi i sigurisë së rrjetit të komunikimit	-	162
12	M-26-2068-24	Parandalimi i anomalive dhe reagimi ndaj tyre	-	162
13	P-26-006-24	Praktikë profesionale e grupuar, në biznes	150	150
Gjithsej			**960 orë**	**960 orë**

IV. Udhëzime për planin mësimor

Kohëzgjatja e kualifikimit në profilin mësimor për "Siguria kibernetike", niveli V i KSHK (pas të mesmes), zgjat 2 vite mësimore.
Viti i I-rë mësimor ka 30 javë (27 javë mësim teorik/praktik + 3 javë praktikë profesionale e grupuar, në biznes).
Viti i II-të mësimor ka 32 javë (27 javë mësim teorik/praktik + 3 javë praktikë profesionale e grupuar, në biznes + 2 javë provime).
Një javë mësimore në shkollë ka 5 ditë x 6 orë në ditë = 30 orë mësimore.
Një orë mësimore teorike ose praktike zgjat 45 - 50 minuta.
Një ditë praktikë profesionale në biznes është 8 orë 60 minutëshe = 10 orë mësimore
Praktika profesionale në biznes në klasën I dhe II është 3 javë x 5 ditë/javë x 10 orë mësimore = 150 orë mësimore
Kurrikuli i arsimit profesional në profilin "Siguria kibernetike", niveli V i KSHK, përbëhet nga modulet profesionale teorike, teoriko-praktike dhe praktike (përshkruesit e tyre janë pjesë e këtij skeletkurrikuli), si dhe nga programi i praktikës profesionale të grupuar, në biznes (tregohet në faqen e fundit të këtij dokumenti).
Rekomandohet që modulet profesionale praktike të realizohen në ndarje ditore 3 ose 6 orëshe.

Përgjithësisht, renditja e realizimit të moduleve bëhet nga vetë shkolla, duke konsideruar parimet didaktike bazë (nga më e thjeshta te më e ndërlikuara, nga niveli i ulët te më i larti, nga teoria te praktika etj.), si dhe kushtet konkrete të shkollës. Për të rritur efiçiencën e procesit mësimor, mund të realizohen paralelisht dy ose më shumë module, si dhe mund të zbatohet ndarja në grupe e nxënësve.

V. Udhëzime për procesin mësimor.

Mësuesit e moduleve profesionale duhet të përzgjedhin dhe përdorin forma dhe metoda mësimdhënieje të tilla që të nxisin maksimalisht të nxënit aktiv të nxënësve dhe të çojnë në krijimin tek ta, të kompetencave të punës, të plota dhe të qëndrueshme. E rëndësishme është që ***planifikimi i mësimdhënies*** të bazohet në një proces analize fillestare, i cili të marrë parasysh faktorë të tillë të rëndësishëm si, niveli i hyrjes së nxënësve, përmbajtja e hollësishme e moduleve profesionale të parashikuara dhe shkalla e integrimit të teorisë me praktikën në to, objektivat konkretë që do të arrihen, mundësitë reale që ka shkolla për realizimin e veprimtarive mësimore etj. Për këtë planifikim duhet një bashkëpunim i ngushtë i të gjithë personelit mësimdhënës dhe drejtues të shkollës. Elementi kyç për arritjen e suksesit në një proces të nxëni, është motivimi i nxënësve. Njohja e vazhdueshme e nxënësve me shkallën e përmbushjes së objektivave nga ana e tyre përbën një mekanizëm të fuqishëm motivimi, i cili duhet të shihet me përparësi nga mësuesit.
Një element tjetër që ndihmon suksesin është integrimi i teorisë me praktikën e profesionit. Parimi i "të nxënit duke bërë" duhet të gjejë vendin e duhur në procesin e të mësuarit në shkollat profesionale që ofrojnë profilin mësimor "Siguria kibernetike", niveli V i KSHK.
Mësuesit duhet të përdorin metoda të tilla të të mësuarit që zhvillojnë jo vetëm njohuritë teorike, shkathtësitë dhe shprehitë praktike të nxënësve, por edhe qëndrimet e tyre ndaj jetës dhe punës. Puna në grup dhe puna me projekte janë dy nga format bazë të organizimit të mësimit (teorik dhe praktik) për të zhvilluar kompetencat kyçe, të nevojshme për zgjidhjen e problemeve që kanë të bëjnë me veprimtarinë profesionale në veçanti dhe jetën e profesionistit të ardhshëm, në përgjithësi. Një parim tjetër që duhet respektuar nga mësuesit është fakti që të nxënit nuk ndodh vetëm në mjediset e shkollës, por edhe jashtë tyre. Dhënia e detyrave dhe puna kërkimore e pavarur e nxënësve ka një ndikim të dukshëm në formimin e tyre si profesionistë të ardhshëm të profilin profesional "Siguria kibernetike", niveli V i KSHK.

Udhëzime për praktikën profesionale të grupuar, në biznes:

Praktika profesionale e grupuar zhvillohet në mjediset e punës së bizneseve që kanë si veprimtari sigurinë kibernetike. Kjo praktikë profesionale ka për qëllim integrimin në mjediset reale të punës, të njohurive, shprehive dhe qëndrimeve, në lidhje me sigurinë e komunikimit dhe të dhënave, diagnostikimin e sistemeve dhe identifikimin e rreziqeve, zbatimin e njohurive të cilat i kanë fituar gjatë procesit mësimor teorik dhe praktik të zhvilluar më parë në mjediset mësimore teorike dhe praktike të shkollës.
Kjo praktikë realizohet çdo vit, gjatë një periudhe mësimore trijavore (150 orë mësimore), zakonisht në përfundim të procesit mësimor teorik dhe praktik, përpara provimeve përfundimtare.
Institucionet/bizneset ku do të kryhet praktika profesionale e grupuar, periudha e realizimit dhe programi i përgjithshëm i kësaj praktike (shih formatin në faqen e fundit të këtij dokumenti), përcaktohen nga vetë shkolla profesionale në bashkëpunim me bizneset përkatëse.
Planifikimi, organizimi dhe administrimi i praktikës profesionale të grupuar, në biznes, bëhen në bashkëpunim të ngushtë me bizneset përkatëse, në përputhje me kuadrin ligjor të posaçëm

të shkollave profesionale, për praktikat profesionale në biznese.

VI. Udhëzime për vlerësimin, provimet dhe certifikatën.

Vlerësimi vjetor i nxënësve për modulet profesionale bëhet nga vetë mësuesit përkatës, me metoda dhe instrumente vlerësimi të përgatitura ose përzgjedhura nga vetë ata. Vlerësimi i nxënësve bëhet me nota (4÷10) për modulet teoriko-praktike, si gjatë vitit, ashtu edhe në provimet përfundimtare.
Në përfundim të arsimimit për "Siguria kibernetike", niveli V i KSHK, pas të mesëm, nxënësit i nënshtrohen provimeve të mëposhtme:

a) Provimi i teorisë profesionale të integruar (test me shkrim)
b) Provimi praktik profesional (realizimi i një detyre/projekti praktik)

Në këto provime ata vlerësohen për shkallën e përvetësimit të kompetencave profesionale (njohurive, shprehive, vlerave dhe qëndrimeve), të nevojshme për të punuar në veprimtari të ndryshme profesionale të profilit "Siguria kibernetike", niveli V i KSHK.
Me përfundimin e suksesshëm të arsimit profesional në profilin mësimor "Siguria kibernetike", niveli V i KSHK, shkolla profesionale e pajis nxënësin me Certifikatën profesionale të nivelit dhe Suplementin përkatës për këtë profil profesional, të cilat njihen në territorin e Republikës së Shqipërisë. Sipas modelit të miratuar nga Ministria përgjegjëse e AFP-së, këto dëshmi përmbajnë:

a) Të dhënat për nxënësin, shkollën, vitin e përfundimit, kualifikimin e fituar etj.

b) Të dhëna për rezultatet (notat) e arrritura nga nxënësi:

- rezultatet në modulet profesionale;
- rezultatin e praktikës profesionale të grupuar, në biznes;
- rezultatet e dy provimeve përfundimtare.

VII. Përshkruesit e moduleve profesionale

1. Moduli "Hyrje në sigurinë kibernetike"

Profili: Siguria kibernetike
Niveli: V i KSHK

PËRSHKRUESI I MODULIT		
Titulli dhe kodi	**HYRJE NË SIGURINË KIBERNETIKE**	**M-26-2057-24**
Qëllimi i modulit	Një modul teoriko-praktik që aftëson nxënësit për të identifikuar nevojat për sigurinë kibernetike dhe mbrojtjen e të dhënave e privatësisë	
Kohëzgjatja e modulit	54 orë mësimore	
Niveli i parapëlqyer për pranim	- Të kenë përfunduar një kualifikim të nivelit IV në KSHK të fushës së TIK; - Të kenë përfunduar të paktën një kualifikim të nivelit IV në KSHK dhe kanë eksperiencë pune, të vërtetuar, të paktën një vit në fushën TIK;	
Rezultatet e të nxënit (RN) dhe procedurat e vlerësimit	**RN 1**	**Nxënësi përshkruan domosdoshmërinë e sigurisë kibernetike** ***Kriteret e vlerësimit:*** – Të interpretojë rolin e sigurisë kibernetike në jetën dhe punën e përditshme; – Të përshkruaj rëndësinë e ofrimit të sigurisë kibernetike; – Të listojë llojet e të dhënave që janë objekt i sulmeve të sigurisë kibernetike; – Të përshkruaj rolin e një punonjësi të sigurisë kibernetike; – Të shpjegojë identitenin *online* dhe *offline*; – Të identifikojë se cila nga të dhënat e individëve apo kompanive është më e cënueshme; – Të përcaktojë mënyrat dhe vendet e ruajtjes së të dhënave sipas ligjit përkatës; – Të shpjegojë sigurimin e pajisjeve të përdorimit të përditshëm për aksesimin dhe ruajtjen e materialeve personale; – Të përshkruaj përdorimin e IOT dhe databazave në sigurinë kibernetike; – Të shpjegojë treshen e kritereve të sigurise CIA; – Të gjenerojë *hash* për një dosje dhe të përdorin këtë vlerë për krahasimin e integritetit të dosjes; ***Instrumentet e vlerësimit:*** – Pyetje-përgjigje me gojë. – Vëzhgim me listë kontrolli.

RN 2 **Nxënësi dokumenton sulmet, konceptet dhe teknikat.**

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

- Të analizojë monitorimin e kryer pas një sulmi;
- Të shpjegojë sigurimin e pajisjeve fizike dhe programeve kompjuterike sipas vulnerabiliteteve të sistemeve përkatëse;
- Të zbërtheje mënyrën e cënimit të sigurisë gjatë një sulmi të përzier (*blendid attack*);
- Të kategorizojë vulnerabilitetet e sitemeve kompjuterike;
- Të konfigurojë frazëkalime dhe fjalëkalime në llogari Të ndryshme;
- Të enkriptojë të dhënat e përdoruesit;
- Të ndërtojë grafikun periodik të ruajtjes së të dhënave *back-up*;
- Të identifikojë llojet e marrëveshjeve ligjore të përshtatshme për institucionin/biznesin për shërbimet online;
- Të aktivizojë identifikimin me dy faktorë;
- Të identifikojë standardet dhe protokollet që lejojnë kredencialet e përdoruesit të aksesojnë aplikacione të palëve të treta pa ekspozuar fjalëkalimin;
- Të përcaktojë llojin dhe sasinë e informacionit që mund të përdoret pa rrezikshmëri në rrjetet sociale;
- Të konfigurojë privatësinë e *email*-eve dhe *web browser*;

Instrumentet e vlerësimit:

- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 3 **Nxënësi organizon mbrojtjen e të dhënave personale, të institucionit, të biznesit.**

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

- Të konfigurojë *firewall*-in e sistemit të shfrytëzimit
- Të përshkruajn llojet e ndryshme të *firewll*-eve që përdoren për sigurimin e komunikimit në institucione;
- Të instalojë *antivirus* dhe *antispyware*;
- Të përzgjedhë enkriptimin e duhur për internetin me *wi-fi*;
- Të përzgjedhë fjalëkalime unike për llogari të ndryshme në kompjuter dhe ato *online*;
- Të identifikojë pajisjet dhe aplikacionet e sigurisë për rrjetet e kompanive dhe organizatave;
- Të shpjegojë përdorimin e NetFlow për monitorimin e rrjetit;
- Të skanojë portat në server dhe portat e hosteve;
- Të përshkruajn procesin e zbulimit të sulmeve në kohë reale;
- Të argumentojnë praktikat më të mira të njohura pë sigurinë;

	– Të skanojë dhe analizojë sistemin konpjuterik; – Të shpjegojnë kuptimin e botnet dhe mënyrën e mbrojtjes; – Të zbatojë rregullat e sigurimit bazuar në sjelljen (*behaviour-based*); ***Instrumentet e vlerësimit:*** – Pyetje-përgjigje me gojë. – Vëzhgim me listë kontrolli.
Udhëzime për zbatimin e modulit dhe vlerësimt të nxënësve	Ky modul duhet të zhvillohet në laboratorin e TIK-ut. - Mësuesi/instruktori duhet të demonstrojë hap pas hapi mbrojtjen e të dhënave personale dhe të organizatës në sigurinë kibernetike. - Nxënësit dokumenton sulmet konceptet dhe teknikat. - Nxënësit duhet të nxiten që të diskutojnë lidhur me gjithçka paraqitet. - Gjatë vlerësimit të nxënësve duhet të zbatohet sa më shumë kontrolli i demonstrimit praktik të aftësive të tyre. - Realizimi i pranueshëm i modulit do të konsiderohet plotësimi nga nxënësi i të gjitha kritereve të realizimit të çdo rezultati të të nxënit të modulit,
Kushtet e e domosdoshme për realizimin e modulit	Për realizimin si duhet të modulit, është e domosdoshme të sigurohen mjediset, pajisjet dhe materialet si më poshtë: - Laborator me kompjutera dhe me lidhje interneti. - Në kompjutera duhet të jetë instaluar *Microsoft Windows* - *Routera, switche, firewall etj.* - Aplikacione për sigurinë. - Materiale të shkruara në mbështetje të trajtimit të modulit.

2. Moduli "Sitemet e Teknologjisë së Informacionit "

Profili: Siguria kibernetike
Niveli: V i KSHK

PËRSHKRUESI I MODULIT		
Titulli dhe kodi	**SISTEMET E TEKNOLOGJISË SË INFORMACIONIT**	**M-26-2058-24**
Qëllimi i modulit	Një modul teorik-praktik që i njeh nxënësit informacione të teknologjisë së informacionit dhe koncepteve të menaxhimit për aplikimet në mjedisin e biznesit	
Kohëzgjatja e modulit	135 orë mësimore	
Niveli i parapëlqyer për pranim	– Të kenë përfunduar një kualifikim të nivelit IV në KSHK të fushës së TIK; – Të kenë përfunduar të paktën një kualifikim të nivelit IV në KSHK dhe kanë eksperiencë pune, të vërtetuar, të paktën një vit në fushën TIK;	
Rezultatet e të nxënit (RN) dhe procedurat e vlerësimit	**RN 1**	**Nxënësi interpreton komponentet dhe kategoritë e sistemeve të informacionit - *SI*** ***Kriteret e vlerësimit:*** Nxënësi duhet të jetë i aftë: – Të interpretojë konceptin e sistemeve të informacionit- SI; – Të listojë komponentët e sistemeve të informacionit- SI; – Të tregojë funksionin e komponentëve të sistemeve të informacionit - SI – Të listojë kategorite kryesore të sistemeve të informacionit- SI; – Të interpretojë Sistemet Operacionale (*Transaction Processing Systems-TPS);* – Të interpretojë Sistemet e Informacionit të Menaxhimit (Management iInformation Systems-MIS); – Të interpretojë Sistemet e Suportit të Vendimmarrjes (Decision Dupport System-*DSS*); – Të interpretojë Sistemet e Menaxhimit të Njohurive (Knowledge Management System- *KMS*); – Të përshkruajë robotikën dhe *neural networks* si pjesë e intelegjencës artificiale -*AI;* – Të interpretojë rolin e sistemit të informacionit në biznesin global; – Të përcaktojë konceptin e firma dixhitale në organizata; – Të përshkruajë epokat e globalizimit dhe sfidat globale në sistemet e informacionit; – Të interpretojë sistemet E-Business – Të interpretojë sistemet E-commerce dhe kategorizimet e tij; – Të interpretojë proceset e pagesave elektronike; – Të interpretojë metodat e sigurisë Secure Socket Layer (SSL), Digital Wallet, Secure Electronic Transaction (SET) ***Instrumentet e vlerësimit:***

- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 2 Nxënësi përzgjedh komponentet hardware dhe software të sistemeve të informacionit

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

- Të listojë komponentë kryesorë të kompjuterit;
- Të listojë operacionet e komponentëve të kompjuterit;
- Të listojë pjesët e pajisjeve kompjuterike;
- Të interpretojë funksionet e CPU (Central Processing Unit);
- Të interpretojë funksionin e motherboard;
- Të listojë tri llojet e memories;
- Të listojë llojet dhe karakteristikt e RAM (Random Access Memory) dhe ROM (Read Only Memory);
- Të përshkruajë njësitë kryesore të ruajtjes së memories (Memory unit);
- Të listojë paisjet ruajtëse (Secondary storage devices);
- Të interpretojë paisjet e hyrje/daljes;
- Të listojë tipet e monitoreve;
- Të interpretojë karakteristikat e porteve
- Të interpretojë strukturën e një sistemi kompjuterik
- Të interpretojë kuptimin dhe funksioni e software-eve;
- Të klasifikojë sipas llojit software-in;
- Të interpretojë llojet e software-in e shfrytwzimit-(OS)
- Të interpretojë software-in e aplikacioneve ;
- Të interpretojë Cloud Computing

Instrumentet e vlerësimit:

- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 3 Nxënësi kryen organizimin e të dhënat dhe aksesin në rrjet

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

- Të interpretojë komponentin e të dhenave në sistemet e informacionit;
- Të dallojë të dhënat, informacionin dhe njohuritë;
- Të interpretojë bazat e të dhënave relacionale;
- Të dizenjonjë një bazë të dhënash;
- Të normalizojë një bazë të dhënash;
- Të përcaktojë tipet e të dhënave (datatype);
- Të përdorë DBMS për të menaxhuar dhe afishur raporte duke përdorur query nga bazat e të dhënave;
- Të listojë llojet e bazave të të dhënave;
- Të përshkruajë shtresat e modelit OSI (Open Systems Interconnection Reference Model) në përshtatjen dhe ndërveprimin e elementëve të ndryshëm të një rrjeti;
- Të përshkruajë funksionin e modelit TCP/IP dhe shtresave të

saj;
- Të interpretojë llojet e topologjive;
- Të interpretoje koncepte të networking si : Paketa, Hub, Bridge, Switch, Router (DHCP dhe NAT), IP Address, Domain name, DNS, Packet-switching, Protocol, etj
- Të përshkrujaë Wireless Networking, Mobile network, Bluetooth, VoIP;
- Të përshkruajë rrjetet e Organizatave;

Instrumentet e vlerësimit:
- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 4 Nxënësi zhvillon dhe dizenjon sistemet e sinformacionit

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:
- Të listojë pjesëmarrësit dhe detyrat e tyre në zhvillimin e sistemit të informacionit;
- Të përshkruajë planifikimi i sistemeve të informacionit;
- Të përshkruajë zhvillimi i nje avantazhi konkurues
- Të përshkruajë objektivat e performancës dhe kostos;
- Të interpretojë fazat e procesit të zhvillimit të sistemeve (Systems Development Life Cycle SDLC)
- Të përcaktojë modelin paraprak -Prototyping;
- Të përdor mjete të menaxhimit të projektit;
- Të analizojë analizën e fizibilitetit;
- Të raportoj i investigimit dhe analizën e sistemeve;
- Të përshkrujaë aspektet kyce të disenjimit te sistemit;
- Të përshkruajë dizenjimi i sigurisë së sistemit dhe kontrolleve;
- Të interpretojë procesin e implementimit të sistemeve;

Instrumentet e vlerësimit:
- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 5 Nxënësi përcakton sigurinë e sistemeve të informacionit

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:
- Të interpretojë konfidencialiteti, integretiti, disponueshmëria (Confidentiality, Integrity and Availability-CIA triad)
- Të listojë mjetet për të garantuar konfidencialitetin, integritetin dhe disponueshmërinë e informacionit;
- Të interpretojë mjete autentikimi të thjeshtë dhe multi-faktorësh;
- Të interpretojë Access Control List (ACL) dhe Role-Based Access Control (RBAC);
- Të interpretojë enkriptim me celës simetrik dhe publik;
- Të interpretojë politikat e organizatës në përcaktimin e password-eve;

	– Të sigurojë informacionit nëpërmjet një plani të gjithanshëm backup-i; – Të interpretojë implementimin e firewall-eve të shumfishtë si pjesë e konfigurimit te sigurise se rrjetit; – Të interpretojë sisteminei zbulimit të ndërhyrjeve- IDS (Intrusion Detection System); – Të interpretojë masat për implementimin e sigurisë fizike; – Të interpretojë politikat e sigurisë; – Të listojë masat për sigurine personale të informacionit; ***Instrumentet e vlerësimit:*** – Pyetje-përgjigje me gojë. – Vëzhgim me listë kontrolli.
Udhëzime për zbatimin e modulit	– Ky modul duhet të zhvillohet në laboratorin e TIK të shkollës . – Instruktori duhet të zbatojë sa më shumë demonstrime praktike të metodave për rritjen e sigurisë bazuar në rrjetat pa tel, sistemet operative të paisjeve fundore. – Nxënësit duhet të angazhohen sa më shumë në diskutimet në lidhje me llojet e sulmeve dhe metodat e sigurisë të paisjeve fundore. – Gjatë vlerësimit të kursantëve duhet të synohet më tepër në verifikimin e shkallës së aftësive praktike që ata kanë fituar për të kryer veprimtaritë e metodave të sigurisë së paisjeve fundore. – Instruktori duhet të kërkojë zbatimin nga nxënësit të rregullave të sigurimit teknik në punë, si dhe të nxitë punën në grup të tyre. – Realizimi i pranueshëm i modulit do të konsiderohet plotësimi nga nxënësi i të gjitha kritereve të realizimit të çdo rezultati të të nxënit të modulit, kritereve të realizimit të çdo rezultati të të nxënit të modulit.
Kushtet e domosdoshme për realizimin e modulit.	Për realizimin si duhet të modulit është e domosdoshme të sigurohen mjediset, veglat, pajisjet, dhe materialet e mëposhtme: – Klasë për mësim teorik dhe mjedise laboratori kompjuterik. – Pajisje kancelarie. – Shembull projekti dhe standarte të sigurisë kibernetike. – Rrjeta pa tel, sisteme operative, paisje të ndryshme fundore. – Lidhje interneti për të shkarkuar software të sigurisë. – Manuale mbi instalimin dhe konfigurimin e paisjeve të sigurisë. – Materiale ilustruese dhe materiale të shkruara në mbështetje të çështjeve që trajtohen në modul (pankarta, udhëzuesa pune, rregullore etj.).

3. Moduli "Legjislacioni, etika dhe standardet në sigurinë kibernetike"

Profili: Siguria kibernetike
Niveli: V i KSHK

PËRSHKRUESI I MODULIT		
Titulli dhe kodi	**LEGJISLACIONI, ETIKA DHE STANDARDET NË SIGURINË KIBERNETIKE**	**M-26-2059-24**
Qëllimi i modulit	Një modul teorik-praktik që i njeh nxënësit me legjislacionin kombëtar në fuqi, standartet e sigurisë kibernetike që zbatohen në nivel ndërkombëtar dhe aplikimet e tyre në tekonologji.	
Kohëzgjatja e modulit	162 orë mësimore	
Niveli i parapëlqyer për pranim	- Të kenë përfunduar një kualifikim të nivelit IV në KSHK të fushës së TIK; - Të kenë përfunduar të paktën një kualifikim të nivelit IV në KSHK dhe kanë eksperiencë pune, të vërtetuar, të paktën një vit në fushën TIK;	
Rezultatet e të nxënit (RN) dhe procedurat e vlerësimit	**RN 1**	**Nxënësi interpreton legjislacionin në fuqi për sigurinë kibernetike.** ***Kriteret e vlerësimit:*** – Të përshkruajë legjislacionin në fuqi për sigurinë kiberenetike. – Të inerpretojë proceset dhe veprimtaritë e parashikuara në legjislacion. – Të asistojë në hartimin e rregullores së brendshme dhe politkave të sigurisë, bazuar në legjislacion. – Të përshkruajë metodat apo teknikat që nevojiten për plotësimin e objektivave të parashikuara ne legjislacion. – Të përshkruajë parimet bazë të standartit ndërkombëtar "NIST" – Të përshkruajë parimet bazë të standartit ndërkombëtar "ISO27001-2022". – Të përshkruajë parimet bazë të standartit ndërkombëtar të ruajtjes së të dhënave "GDPR". ***Instrumentet e vlerësimit:*** – Pyetje-përgjigje me gojë. – Vëzhgim me listë kontrolli.
	RN 2	**Nxënësi organizon proceset dhe veprimtaritë në funksion të zbatimit të legjislacionit dhe rregullores së brendshme.** ***Kriteret e vlerësimit:*** Nxënësi duhet të jetë i aftë: – Të vërë në dispozicion të stafit të gjithë informacionin e nevojshmëm ne lidhje me rregulloren dhe legjislacionin.

- Të organizojë proceset e punës sipas praktikave të parashikuara në standart ose legjislacionin përkatës.
- Të hartojë planin e punës me qëllim përkthimin e parimeve teorike në veprimtari praktike sipas standartit apo legjislacionit përkatës.
- Të analizojë infrastrukturën e organizatës me qëllim evidentimin e njësive që nuk janë në përputhje me standartin apo legjislacionin në fuqi.
- Të hartojë rregullore apo materiale udhëzuese sipas nevojës për sigurinë kibernetike ne organizatë.
- Të komunikojë me koleget dhe stafin juridik të organizatës me qëllim ndarjen e përgjegjësive, nxitjen e zbatimin të rregullores dhe rritjen e bashkëpunimit mes kolegeve/departamenteve.
- Të njoftoje stafin e organizatës në mënyrë dinamike të gjithë ndryshimet në rregullore apo legjislacion.

Instrumentet e vlerësimit:

- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 3 Nxënësi menaxhon zbatimin e legjislacionit dhe rregullores së brendshme në mjedisin e punës.

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

- Të tregojë cilat janë funksionet dhe detyrat kryesore të personit përgjegjës për sigurinë kibernetike.
- Të përshkruajë strukturat organizative, rolet, përshkrimet e punës dhe pergjegjësitë e të gjitha palëve në mjedisin e punës.
- Të sigurohet që të gjitha palët e përfshira në procesin e punës zbatojnë rregulloren e përcaktuar për sigurinë kibernetike.
- Të aplikoje politikat e sigurisë në sisteme konform rregullores dhe legjislacionit.
- Të kryeje kontrolle (audit) për zbatimin e rregullores dhe legjislacionit në organizatë.
- Të hartojë raporte periodike për të gjitha incidentet dhe rregulla të etikës profesionale dhe të komunikimit në autoservis
- Të ruajë historikun dhe të gjithë dokumentacionin e nevojshëm sipas standartit/legjislacionit.

Instrumentet e vlerësimit:

- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 4 **Nxënësi menaxhon të dhënat e gjeneruara nga procesi i punës me konfidencialitet dhe etikë.**

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

- Të kujdeset për ruajtjen dhe përpunimin e sigurt të të dhënave të gjeneruara nga sistemet e monitorimit dhe filtrimit.
- Të realizojë ruajtjen në mënyrë të sigurt të të gjitha të dhënave të gjeneruara nga proceset e punës si kredenciale, raporte, dokumenta personale etj.
- Të infromojë paraprakisht të gjith përdoruesit fundor për rregulloren dhe mënyrat e monitorimit që aplikohen ndaj tyre.
- Të respektojë rregulloren, standartin dhe legjislacionin në fuqi për mbrotjen e të dhënave personale dhe mënyrat e lejuara të monitorimit dhe filtrimit të të dhenave.
- Të komunikojë në mënyrë etike dhe profesionale për secilin rast kur nevojitet ndërhyrja operacionale në të dhena personale, kritike, konfidenciale apo të klasifikuara.
- Të kujdeset për ruajten e të gjitha të dhenave që ka në administrim nga humbja, aksesimi nga persona të paautorizuar, shpërndarja apo cënimi i kredibilitetit të të dhënave.

Instrumentet e vlerësimit:

- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

Udhëzime për zbatimin e modulit

- Mësuesi duhet të vërë në dispozicion të nxënësve dokumentacione të ndryshme në lidhje me legjislacionin dhe standartet ndërkombëtare. (fizike ose online)
- Ky modul duhet të zhvillohet në klasë dhe laborator TIK.
- Instruktori duhet të relizojë simulime të rasteve të ndryshme të kryerjes së verpimtarive praktike të analizimit të një organizate lidhur me legjislacionin, rregulloren e brendshme dhe standartet.
- Nxënësit duhet të angazhohen në diskutime të ndryshme në lidhje legjislacionin, standartet ndërkombëtare dhe teknologjitë e ndryshme që ndihmojnë në zbatimin e tyre.
- Instruktori duhet të nxisë diskutime në lidhje me krahasimin e standtareve të ndryshme të sigurisë kibernetike, avantazhet dhe disavantazhet e tyre, si edhe ngjashmëritë e tyre me legjislacionin kombëtar.
- Realizimi i pranueshëm i modulit do të konsiderohet plotësimi nga nxënësi i të gjitha kritereve të realizimit të çdo rezultati të të nxënit të modulit, kritereve të realizimit të çdo rezultati mësimor të modulit.
- Instruktori mund të përdorë mjete të ndryshëm online për kryerjen e analizave të standarteve (Cybersecurity Compliance Software).

Kushtet e domosdoshme për realizimin e modulit.	Per realizimin si duhet te modulit eshte e domosdoshme te sigurohen mjediset, veglat, pajisjet, dhe materialet e meposhtme: – Klase per mesim teorik dhe laborator TIK. – Dokumentacion i standarteve ndërkombëtare. – Legjislacioni ne fushën e cybersecurity.

4. Moduli "Zbatimi i *Python* në sigurinë kibernetike"
Profili: Siguria kibernitike
Niveli: V i KSHK

PËRSHKRUESI I MODULIT		
Titulli dhe kodi	**ZBATIMI I *PYTHON* NË SIGURINË KIBERNETIKE**	**M-26-2060-24**
Qëllimi i modulit	Një modul teorik-praktik që i njeh nxënësit me zbatimin e librarive në python për të rritur sigurinë kibernetike dhe automatizimin e sigurisë së informacionit.	
Kohëzgjatja e modulit	81 orë mësimore	
Niveli i parapëlqyer për pranim	– Të kenë përfunduar një kualifikim të nivelit IV në KSHK të fushës së TIK; – Të kenë përfunduar të paktën një kualifikim të nivelit IV në KSHK dhe kanë eksperiencë pune, të vërtetuar, të paktën një vit në fushën TIK;	
Rezultatet e të nxënit (RN) dhe procedurat e vlerësimit	**RN 1** **Nxënësi shkruan programe të thjeshta në gjuhën *Python*** ***Kriteret e vlerësimit:*** – Të deklarojë variablat dhe tipin e të dhënave, për secilin variabël; – Të ndërtojë intruksione duke përdorur operatorët aritmetik; – Të ndërtojë intruksione duke përdorur operatorët logjik; – Të ndërtojë intruksione duke përdorur operatorët krahasimi; – Të ndërtojë programe në *python* duke përdorur operatorët pre/post incrementimi dhe dekrementimi; – Të ndërtojë programe që kryejnë veprime mbi bazën e shprehjeve logjike *if else*; – Të ndërtojë programe duke implementuar ciklin *for*; – Të ndërtojë programe duke implementuar ciklin *while*; – Të ndërtojë programe duke implementuar komandën switch – Të shkruajë programe që kryejnë veprime me vargjet e numrave duke implementuar ciklet; – Të komunikojë me etikë dhe profesionalizëm; – Të zbatojë rregullat e sigurimit teknike dhe të sigurisë në punë; ***Instrumentet e vlerësimit:*** – Pyetje-përgjigje me gojë. – Vëzhgim me listë kontrolli. **RN 2** **Nxënësi shkruan programe duke përdorur funksionet** ***Kriteret e vlerësimit:***	

Nxënësi duhet të jetë i aftë:

- Të ndërtojë funksione në *python*;
- Të thërrasë funksione në *python*;
- Të ndërtojë funksione me dy apo më shumë argumenta në *python*;
- Të thërrasë funksione brenda funksioneve të tjera;
- Të shkruajë programe për marrjen e vlerave nga një funksion;
- Të komunikojë me etikë dhe profesionalizëm;
- Të zbatojë rregullat e sigurimit teknike dhe të sigurisë në punë;

Instrumentet e vlerësimit:

- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 3 Nxënësi ndërtonë programe që manipulojnë klasat dhe objektet

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

- Të ndërtojë një klasë në *python*;
- Të ndërtojë deklasimin e klasës me metodë;
- Të ndërtojë deklarimin e metodës me parametër;
- Të ndërtojë diagramat e klasave nga një klasë e dhënë;
- Të krijojë objekt të klasës;
- Të ndërtojë inicializimin e objekteve nëpërmjet konstruktorve;
- Të ndërtojë klasa të trashguara;
- Të implementojë mënyrën se si trashgohet një klasë;
- Të komunikojë me etikë dhe profesionalizëm;
- Të zbatojë rregullat e sigurimit teknike dhe të sigurisë në punë;

Instrumentet e vlerësimit:

- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 4 Nxënësi përshkruan funksionin e komponentëve kryesorë për identifikinim dhe mbrojtjen e të dhënave në sigurinë kibernetike;

Nxënësi duhet të jetë i aftë:

- Të përshkruajë funksionin e *identifying vulnerabilities* në sigurinë kibernetike;
- Të përshkruajë rolin e *web application security;*
- Të përshkruajë funksionin e *cryptography;*
- Të përshkruajë mënyrën e mbrojtjesë së të dhënave nëpërmjet *cryptography;*
- Të shpjegojë funksionin *e blockchain ;*
- Të shpjegojë funksionin e *automating në sigurinë*

kibernetike;

- Të përshkruajnë funskionin *e machine learning;*
- Të indentikojnë sulment nëpërmjet *machine learning;*
- Të përshkruajnë funskionin e *password cracking;*
- Të përshkruajnë funskionin *e reverse engineering;*
- Të përshkruajnë mënyrat e mbrojtjes së të dhënave nëpërmjet *network security;*
- Të përshkruajë funksionin e *IoT Security* në identifikimin dhe analiziminë e sulmeve;
- Të përshkruajë funksionin e *Penetration Testing*;

Instrumentet e vlerësimit:

- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 5 Nxënësi implementon librarit në python për të rritur sigurinë kibernetike.

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

- Të implementojë librarin *Scapy* për dekodimin e paketave të rrjetit;
- Të implementojë librarin *Requests* për testimin, analizën dhe nxjerrjen e të dhënave;
- Të implementojë *Paramiko* për auditimin dhe menaxhimin e pajisjeve të rrjetit;
- Të implementojë *PyCryptodome për encryption, decryption, digital signatures,* dhe *hashing;*
- Të implementojë *YARA* për të identifikuar dhe klasifikuar *malware;*
- Të implementojë librarin *Pycrypto;*
- Të implementojë *Security Monkey* për monitorimin dhe analizimin e sigurisë së infrastrukturës *cloud;*
- Të implementojë librarin Nmap ;

Instrumentet e vlerësimit:

- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 6 Nxënësi realizon automatizimin e sigurisë së informacionit

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

- Të aksesojë *oracle virtualbox installed*;
- Të instalojë kali linux 64-bit *virtualbox* image;
- Të shkarkojë dhe të instalojë *pycharm IDE Kali;*
- Të shkruajë, modifikojë dhe testojë një *skripti exploit* ;
- Të analizojë skedarët e paketave;
- Të përshkruajë *open- source intelligence*;
- Të analizojë një skedar *log;*
- Të realizojë shkrimin dhe zëvendësimin *netcat;*

	– Të përshkruiajë dhe interpretojë *enetration testing tool;* – Të komunikojë me etikë dhe profesionalizëm; – Të zbatojë rregullat e sigurimit teknike dhe të sigurisë në punë; ***Instrumentet e vlerësimit:*** – Pyetje-përgjigje me gojë. – Vëzhgim me listë kontrolli.
Udhëzime për zbatimin e modulit	– Ky modul duhet të zhvillohet në laboratorin e shkollës për sigurinë kibernetike. – Instruktori duhet të zbatojë sa më shumë demonstrime praktike në zbatimin e *python* në sigurinë kibernetike – Nxënësit duhet të angazhohen sa më shumë të jetë e mundur në diskutimet në lidhje me ndërtimin e programeve në *python*, implementimin e librarive etj. – Gjatë vlerësimit të nxënësve duhet të synohet më tepër në verifikimin e shkallës së aftësive praktike që ata kanë fituar për ndërtimin dhe implementimin e librarive në *python.* – Instruktori duhet të kërkojë me rreptësi zbatimin nga nxënësit të rregullave të sigurimit teknik në punë, si dhe të nxitë punën në grup të tyre. – Realizimi i pranueshëm i modulit do të konsiderohet plotësimi nga nxënësi i të gjitha kritereve të realizimit të çdo rezultati të të nxënit të modulit, kritereve të realizimit të çdo rezultati mësimor të modulit.
Kushtet e domosdoshme për realizimin e modulit.	Për realizimin si duhet të modulit është e domosdoshme të sigurohen mjediset, veglat, pajisjet, dhe materialet e mëposhtme: – Mjedisë laboratori kompjuterik. – Lidhje interneti për të shkarkuar software të sigurisë. – Materiale ilustruese dhe materiale të shkruara në mbështetje të çështjeve që trajtohen në modul (pankarta, udhëzuesa pune, rregullore etj.).

5. Moduli "Instalimi dhe konfigurimi i sistemeve të sigurisë kibernetike"

Profili: Siguria kibernetike
Niveli: V i KSHK

PËRSHKRUESI I MODULIT		
Titulli dhe kodi	**INSTALIMI DHE KONFIGURIMI I SISTEMEVE TË SIGURISË KIBERNETIKE**	**M-26-2061-24**
Qëllimi i modulit	Një modul teorik-praktik që i njeh nxënësit me teknikat e instalimit dhe konfigurimit të pajisjeve dhe software-ve të sigurisë kibernetike dhe rëndësinë e testimit të funksionimit të tyre.	
Kohëzgjatja e modulit	135 orë mësimore	
Niveli i parapëlqyer për pranim	– Të kenë përfunduar një kualifikim të nivelit IV në KSHK të fushës së TIK; – Të kenë përfunduar të paktën një kualifikim të nivelit IV në KSHK dhe kanë eksperiencë pune, të vërtetuar, të paktën një vit në fushën TIK; –	
Rezultatet e të nxënit (RN) dhe procedurat e vlerësimit	**RN 1** **Nxënësi përshkruan funksionimin e pajisjeve dhe software-ve të sigurisë kibernetike** ***Kriteret e vlerësimit:*** – Të listojë llojet e ndryshme të pajisjeve të sigurisë kibernetike; – Të përshkruajë rëndësinë e pajisjeve të sigurisë kibernetike; – Të përshkruajë tipet e ndryshme të *firewall*-ve; – Të shpjegojë komponentët e një *firewall*-i; – Të përshkruajë metodat e implementimit të *firewal*l-ve; – Të interpretojë mënyrën e funksionimit të *firewall*-ve; – Të shpjegojë ndryshimet midis software *firewall* dhe hardware *firewall*; – Të listojë llojet e ndryshme të software-ve të sigurisë kibernetike; – Të përshkruajë llojet e ndryshme të software-ve të sigurisë kibernetike; – Të përshkruajë rëndësinë e software-ve të sigurisë kibernetike; – Të përshkruajë mënyrën e funksionimit të software-ve të sigurisë kibernetike; ***Instrumentet e vlerësimit:*** – Pyetje-përgjigje me gojë. – Vëzhgim me listë kontrolli. **RN 2** **Nxënësi kryen instalimin dhe konfigurimin e pajisjeve të sigurisë kibernetike** ***Kriteret e vlerësimit:*** Nxënësi duhet të jetë i aftë: – Të përzgjedh serverat dhe pajisjet e nevojshme për mbrojtjen e rrjetit dhe të dhënave. (*firewall*, sistemе detektimi dhe	

parandalimi të intruzionit (*IDPS*), servera të posaçëm për *SIEM* dhe pajisje të tjera të sigurisë.);
- Të përzgjedh pajisjen *firewall* që i përshtatet nevojave të projektit dhe infrastrukturës së rrjetit;
- Të interpretojë manualet e pajisjes firewall të përzgjedhur;
- Të vendos fizikisht *firewall*-in në vendin e përshtatshëm në rrjet, duke u siguruar që të ketë qasje të mirë dhe fuqi të mjaftueshme;
- Të lidhë *firewall*-in me rrjetin duke përdorur lidhjet e duhura fizike;
- Të konfigurojë portat e *firewall*-it sipas projektit përkatës të sigurës kibernetike;
- Të aktivizojë *firewall*-in duke e ndezuar atë;
- Të përfundojë procesin e aktivizimit duke kryer disa konfigurime bazike;
- Të konfigurojë ndërfaqen e menaxhimit të *firewall*-it për konfigurimin e detajuar sipas projektit përkatës të sigurisë kibernetike;
- Të vendosë politikat e sigurisë, rregullat e filtrimit të trafikut dhe parametrat e tjera të nevojshme për sigurinë e rrjetit;
- Të dokumentojë instalimin dhe detajet e konfigurimeve të *hardware*-it përfshirë rregullat e sigurisë dhe procedurat e implementuara.

Instrumentet e vlerësimit:
- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 3 Nxënësi kryen instalimin dhe konfigurimin e software-ve të sigurisë kibernetike

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:
- Të përzgjedh softwaret e sigurisë kibernetike që përshtaten me sistemin operativ dhe përmasat e rrjetit sipas specifikimeve të projektit;
- Të shkarkojë softwaret e sigurisë kibernetike nga burimet e besueshme;
- Të zbatojë manualet dhe udhëzimet për instalimin softwareve të sigurësë kibernetike;
- Të konfigurojë softwaret e sigurisë kibernetike duke përcaktuar parametrat e sigurisë dhe preferencat e përdoruesit sipas projektit përkatës;
- Të aktivizojë softwaret duke u siguruar që të bëhen azhornime të rregullta për të mbajtur sigurinë e sistemit të përditësuar;
- Të dokumentojë instalimin dhe detajet e konfigurimeve të *software*-it, përfshirë rregullat e sigurisë dhe procedurat e implementuara.

Instrumentet e vlerësimit:
- Pyetje-përgjigje me gojë.

– Vëzhgim me listë kontrolli.

RN 4 Nxënësi teston funksionimin e pajisjeve dhe software-ve të sigurisë kibernetike

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

– Të kontrollojë intalimet fizike për t'u siguruar që pajisja të jetë vendosur dhe lidhur sipas specifikimeve në manual;
– Të kontrollojë nëse të gjitha lidhjet dhe kabllot janë të vendosura në mënyrë të duhur;
– Të testojë konfigurimin fillestar të pajisjes për të siguruar që të gjitha parametrat dhe rregullat e konfiguruara janë në përputhje me politikat e sigurisë të kërkuara;
– Të testojë filtrimin e trafikut, funksionet e autentikimit, dhe aftësinë e pajisjes për të ndaluar ose lejuar trafikun e rrjetit;
– Të testojë performancën e pajisjes së sigurisë për qëndrueshmërinë dhe efikasitetin;
– Të testojë përshatshmërinë e pajisjes së sigurisë kibernetike me infrastrukturën ekzistuese dhe me *software*-t e tjera të përdorura në rrjet;
– Të testojë mbrojtjen nga sulmet duke simuluar skenare të sulmeve për të testuar se sa mirë pajisja e sigurisë kibernetike mund të zbulojë dhe të parandalojë sulmet e mundshme;
– Të testojë nëse *log*-ët dhe sistemet e monitorimit të pajisjes së sigurisë janë të konfiguruara dhe punojnë si duhet për të regjistruar dhe monitoruar aktivitetin e rrjetit dhe të sistemit;
– Të testojë aftësinë e *software*-ve të sigurisë kibernetike për të identifikuar dhe fshirë *malware*-t e mundshme nga sistemi;
– Të testojë funksionin e skanimit të plotë të software-ve të sigurisë kibernetike për të verifikuar aftësinë mbi identifikimin dhe fshirjen e *malware-ve* dhe programeve që cënojnë sigurinë;
– Të testojë aftësinë e *software*-ve të sigurisë kibernetike për mbrojtjen në internet duke verifikuar se cilat faqe identifikohen si të rrezikshme dhe cilat lejohen;
– Të testojë funksionin e mbrojtjes së rrjetit dhe firewall-it (*software*) duke verifikuar aftësinë e tij për të ndaluar hyrjet e padëshiruara dhe trafikun e rrezikshëm;
– Të testojë proçesin e përditësimit të *software*-ve të sigurisë kibernetike për t'u siguruar që funksionon si duhet;
– Të testojë performancën e softuerit për të vlerësuar ndikimin e tij në performancën e sistemit dhe për të siguruar që nuk ka konflikte të padëshiruara ose ngadalësime në performancë;
– Të sigurojë që *software*-ri i sigurisë funksionon në rregull me aplikacionet dhe pajisjet e tjera në infrastrukturën dhe nuk shkakton konflikte të papritura ose probleme të përshtatshmërisë;

Instrumentet e vlerësimit:

	– Pyetje-përgjigje me gojë. – Vëzhgim me listë kontrolli.
Udhëzime për zbatimin e modulit	– Ky modul duhet të zhvillohet në laboratorin e TIK – Instruktori duhet të zbatojë sa më shumë demonstrime praktike në zbatimin e *python* në sigurinë kibernetike. – Nxënësit duhet të angazhohen sa më shumë të jetë e mundur në diskutimet në lidhje me teknikat e instalimit dhe konfigurimit të pajisjeve dhe softwareve të sigurisë, interpretimin e manualeve dhe në rëndësinë e testimit të funksionimit të tyre. – Gjatë vlerësimit të kursantëve duhet të synohet më tepër në verifikimin e shkallës së aftësive praktike që ata kanë fituar për të kryer veprimtaritë e instalimit dhe konfigurimit. – Instruktori duhet të kërkojë zbatimin nga nxënësit tërregullave të sigurimit teknik në punë, si dhe të nxitë punën në grup të tyre. – Realizimi i pranueshëm i modulit do të konsiderohet plotësimi nga nxënësi i të gjitha kritereve të realizimit të çdo rezultati të të nxënit të modulit, kritereve të realizimit të çdo rezultati të të nxënit të modulit.
Kushtet e domosdoshme për realizimin e modulit.	Për realizimin si duhet të modulit është e domosdoshme të sigurohen mjediset, veglat, pajisjet, dhe materialet e mëposhtme: – Mjedise laboratori kompjuterik. – Lidhje interneti për të shkarkuar software të sigurisë. – Materiale ilustruese dhe materiale të shkruara në mbështetje të çështjeve që trajtohen në modul (pankarta, udhëzuesa pune, rregullore etj.).

6. Moduli "Siguria e pajisjeve fundore "

Profili: Siguria kibernitike
Niveli: V i KSHK

PËRSHKRUESI I MODULIT		
Titulli dhe kodi	**SIGURIA E PAJISJEVE FUNDORE**	**M-26-2062-24**
Qëllimi i modulit	Një modul teorik-praktik që i njeh nxënësit me metodat dhe teknologjitë që përdoren për të mbrojtur pajisjet fundore të rrjetit nga kërcënimet e sigurisë. Pajisjet fundore përfshijnë kompjuterët, laptopët, tabletët, telefonat inteligjentë dhe pajisjet e tjera që lidhen me rrjetin e një organizatë.	
Kohëzgjatja e modulit	108 orë mësimore	
Niveli i parapëlqyer për pranim	– Të kenë përfunduar një kualifikim të nivelit IV në KSHK të fushës së TIK; – Të kenë përfunduar të paktën një kualifikim të nivelit IV në KSHK dhe kanë eksperiencë pune, të vërtetuar, të paktën një vit në fushën TIK;	
Rezultatet e të nxënit (RN) dhe procedurat e vlerësimit	**RN 1**	**Nxënësi zbaton metodat për rritjen e sigurisë në sistemet operative të pajisjeve fundore.** ***Kriteret e vlerësimit:*** – Të interpretojë llojet e sulmeve dhe kërcënimeve të sistemit operativ të pajisjeve fundore; – Të aktivizojë dhe përditësojë *Windows Defender* për mbrojtje të vazhdueshme kundër *malware*-it dhe virusëve; – Të konfigurojë dhe aktivizojë *Firewall*-in e *Windows* për të mbrojtur pajisjet nga sulmet e rrjetit; – Të aktivizojë *BitLocker* për të kriptuar të dhënat në hardisk dhe të sigurojë mbrojtje në rast të vjedhjes; – Të përditësojë rregullisht *Windows* dhe aplikacionet e tjera për të mbajtur sistemin të mbrojtur nga dobësitë e sigurisë; – Të kontrollojë funksionimin e antivirusëve/antimalware të instaluar në pajisjen fundore; – Të konfigurojë *UAC* (Kontrolli i Llogarive të Përdoruesve) në nivelin më të lartë për të kërkuar autorizim para ndryshimeve të rëndësishme në pajisjen fundore; – Të kontrollojë qasjen dhe autentifikimin në pajisjen fundore; – Të aktivizojë dhe përdorë shfletuesin e sigurt për të parandaluar sulmet ndaj shfletuesit; – Të përdor kontrollin e aplikacioneve për të kufizuar ekzekutimin e softuerëve të paautorizuar; – Të aktivizojë back up-in periodik të të dhënave; – Të aktivizoj auditimin dhe monitorimin për të gjurmuar veprimtaritë e dyshimta në sistem;

Instrumentet e vlerësimit:

- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 2 Nxënësi zbaton metodat për rritjen e sigurisë në pajisjet *mobile*.

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

- Të interpretojë llojet e sulmeve dhe kërcënimeve të pajisjeve fundore *mobile*;
- Të aktivizojë autentikimin me fjalëkalim ose sensor biometrik (si skanimi i shenjave të gishtërinjve ose skanimi i fytyrës);
- Të aktivizojë shërbimin e gjetjes së pajisjes (si *Find My iPhone për pajisjet Apple ose Find My Device* për pajisjet *Android)* ose një funksion i ngjashëm për të gjurmuar ose bllokuar pajisjen në rast humbje ose vjedhje;
- Të aktivizojë përditësimi automatik të sistemit operativ dhe i aplikacioneve;
- Të aktivizojë bllokimin e numrit *IMEI* në rast të vjedhjes së pajisjes;
- Të aktivizojë shkarkimin e aplikacioneve vetëm nga dyqanet zyrtare (*App Store* për *iPhone dhe Google Play Store* për *Android);*
- Të aktivizojë kufizimin e qasjes së aplikacioneve në të dhënat personale dhe vendndodhjen;
- Të aktivizojë kriptimin e të dhënave të rëndësishme në pajisje;
- Të përdorë lidhje të sigurta (*VPN*) për komunikim në rrjet;
- Të aktivizojë autentifikimin me faktorë të dyfishtë për hyrje në pajisje dhe aplikacione;
- Të monitorohet lejet e aplikacioneve që kërkojnë qasje në të dhëna të ndjeshme ose funksione të pajisjes që nuk janë të nevojshme për veprimtarinë e tyre;

Instrumentet e vlerësimit:

- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 3 Nxënësi zbaton metoda për rritjen e sigurisë në rrjetat pa tel (*Wireless).*

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

- Të interpretojë llojet e sulmeve dhe kërcënimeve të pajisjeve fundore në një rrjet pa tel;
- Të konfigurojë dhe të përditësojë sistemin e enkriptimit të rrjetit *WiFi* për të siguruar qasje vetëm për pajisjet e lejuara;
- Të implementojë autentifikim të fortë për pajisjet që lidhen me rrjetin (duke përdorur protokolle të tilla si *WPA2-Enterprise ose 802.1X);*

	– Të përdorë një sistem identifikimi të pajisjeve për të zbuluar dhe autorizuar automatikisht pajisjet e reja që lidhen me rrjetin; – Të vendosë një politikë të qasjes së rrjetit, duke përcaktuar privilegjet dhe kufizimet e qasjes së pajisjeve të ndryshme; – Të implementojë një *firewall* të dedikuar për rrjetin pa tel, që mund të bllokojë trafikun e panjohur dhe të parandalojë sulmet; – Të përdorë certifikata dhe shfrytëzojë çelësat publikë/private për të siguruar komunikimin e sigurt në rrjet; – Të kufizojë qasjet dhe privilegjet e përdoruesit sipas nevojave të biznesit; – Të zbatojë dhe të monitorojë përmbajtjen e përdorimit të internetit për të parandaluar aksese të paautorizuara dhe për të mbrojtur të dhënat sensitive; – Të përdorë një platformë të menaxhimit të sigurisë së rrjetit që mund të koordinojë dhe të monitorojë politikat dhe veprimet e sigurisë në të gjitha pajisjet e fundit të rrjetit; – Të simulojë një trajnim dhe ndërgjegjësim për përdoruesit rreth praktikave të sigurisë të rrjetit dhe rreziqeve potenciale të sigurisë; – Të zbatojë përdorimin e një platforme mbi zbulimin, monitorimin dhe reagimin ndaj kërcënimeve të sigurisë në pajisjet e lidhura me rrjetin pa tel në kohë reale; ***Instrumentet e vlerësimit:*** – Pyetje-përgjigje me gojë. – Vëzhgim me listë kontrolli.
Udhëzime për zbatimin e modulit	– Ky modul duhet të zhvillohet në laboratorin e TIK të shkollës. – Instruktori duhet të zbatojë sa më shumë demonstrime praktike të metodave për rritjen e sigurisë bazuar në rrjetat pa tel, sistemet operative të pajisjeve fundore. – Nxënësit duhet të angazhohen sa më shumë të jetë e mundur në diskutimet në lidhje me llojet e sulmeve dhe metodat e sigurisë të pajisjeve fundore. – Gjatë vlerësimit të kursantëve duhet të synohet më tepër në verifikimin e shkallës së aftësive praktike që ata kanë fituar për të kryer veprimtaritë e metodave të sigurisë së pajisjeve fundore. – Instruktori duhet të kërkojë me rreptësi zbatimin nga nxënësit të rregullave të sigurimit teknik në punë, si dhe të nxitë punën në grup të tyre. – Realizimi i pranueshëm i modulit do të konsiderohet plotësimi nga nxënësi i të gjitha kritereve të realizimit të çdo rezultati të të nxënit të modulit, kritereve të realizimit të çdo rezultati të të nxënit të modulit.

Kushtet e domosdoshme për realizimin e modulit.	Për realizimin si duhet të modulit është e domosdoshme të sigurohen mjediset, veglat, pajisjet, dhe materialet e mëposhtme: – Klasë për mësim teorik dhe mjedise laboratori kompjuterik. – Pajisje kancelarie. – Shembull projekti dhe standarte të sigurisë kibernetike. – Rrjeta pa tel, sisteme operative, pajisje të ndryshme fundore. – Lidhje interneti për të shkarkuar software të sigurisë. – Manuale mbi instalimin dhe konfigurimin e pajisjeve të sigurisë. – Materiale ilustruese dhe materiale të shkruara në mbështetje të çështjeve që trajtohen në modul (pankarta, udhëzuesa pune, rregullore etj.).

7. Moduli "Gjurmimi dhe identifikimi i faktorëve të dëmshëm."

Profili: Siguria kibernetike
Niveli: V i KSHK

PËRSHKRUESI I MODULIT		
Titulli dhe kodi	**GJURMIMI DHE IDENTIFIKIMI I FAKTORËVE TË DËMSHËM**	**M-26-2063-24**
Qëllimi i modulit	Një modul teorik-praktik që i njeh nxënësit me legjislacionin kombëtar në fuqi, standartet e sigurisë kibernetike që zbatohen në nivel ndërkombëtar dhe aplikimet e tyre në tekonologji.	
Kohëzgjatja e modulit	135 orë mësimore	
Niveli i parapëlqyer për pranim	– Të kenë përfunduar një kualifikim të nivelit IV në KSHK të fushës së TIK; – Të kenë përfunduar të paktën një kualifikim të nivelit IV në KSHK dhe kanë eksperiencë pune, të vërtetuar, të paktën një vit në fushën TIK;	

Rezultatet e të nxënit (RN) dhe procedurat e vlerësimit	**RN 1**	**Nxënësi kryen analizë të detajuar të sjelljes së përdoruesve bazuar në historikun e ngjarjeve të raportuara dhe raportet e gjeneruara nga sistemet.** ***Kriteret e vlerësimit:*** – Të përshkruajë burimet e të dhënave që nevojiten për të kryer analizën e sigurisë kibernetike. – Të përshkruajë teknikat e përftimit të të dhënave të vlefshme nga sistemet hardëare dhe softëare të sigurisë kibernetike. – Të përshkruajë metodat e analizës së historikut të raportimeve dhe monitorimit të përdoruesve. – Të dallojë sjelljet e rrezikshme aksidendale apo të qëllimshme. – Të raportojë menjëherë sipas hierarkisë në raste urgjente. – Të komunikojë në mënyrë profesionale me përdoruesit në rast të nevojës për thellim të analizës. – Të hartojë një raport të përbledhur të gjetjeve të analizuara të përdoruesve dhe sistemeve. ***Instrumentet e vlerësimit:*** – Pyetje-përgjigje me gojë. – Vëzhgim me listë kontrolli. – Projekt.
	RN 2	**Nxënësi kryen testime të vazhdueshme të vurnerabilitetit të infrastrukturës IT.** ***Kriteret e vlerësimit:*** Nxënësi duhet të jetë i aftë: – Të kryejë kontrolle të vazhdueshme të proceseve të punës që cënojnë direkt apo indirekt infrastrukturën IT.

- Të kryejë rregullisht kontrolle të komunikimit hyrje-dalje të sistemeve që lidhen me të dhëna kritike.
- Të verifikojë të drejtat e aksesit në sisteme sipas rregullores.
- Të kryeje kontrolle të vazhdueshme me apo pa lajmërim të sistemeve dhe përdoruesve sipas rregullores.
- Të kryeje testime të procesve të punës që lidhen me akesin në të dhëna sensitive.
- Të kryeje testime të vazhdueshme të akesit në ambjente të kufizuara.
- Të kryejë kontrolle të vazhdueshme për përdoresit që konsiderohen "me rrezikshmëri të lartë" për shkak të pozicionit kritik.
- Të kryejë kontrolle të vazhdueshme për përdoresit që konsiderohen "me rrezikshmëri të lartë" për shkak të historikut të keq.

Instrumentet e vlerësimit:

- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 3 Nxënësi i komunikon të gjithë përdoruesve strategjitë dhe praktikat me të fundit për shmangjen e rrezikut dhe faktorët e dëmshëm.

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

- Të njoftojë sipas rregullores të gjithë përdoruesit për përgjegjësitë personale në ruajtjen e të dhënave.
- Të informojë në mënyrë të qartë përdoruesit për rreziqet e mundshme që vijnë nga faqet ËEB.
- Të informojë në mënyrë të qartë përdoruesit për rreziqet e mundshme që vijnë nga Email.
- Të informojë në mënyrë të qartë përdoruesit për rreziqet e mundshme që vijnë nga pajisjet periferike HDD, USB, Smartphone etj.
- Të informojë në mënyrë të qartë përdoruesit për rreziqet e mundshme që vijnë nga materiale PDF apo file të panjohur të ekzekutueshëm.
- Të informojë në mënyrë të qartë përdoruesit për rreziqet e mundshme që vijnë nga rreziku i instalimit të programeve të palicencuara, me "crack" apo nga prodhues jo legjitim.
- Të shpjegojë teknikat e raportimit të ngjarjeve të dyshimta dhe rëndësine e raportimit në kohë të tyre.
- Të informojë dhe trajnojë përdoruestit për metodat e reagimit dhe eskalimit të situatave.
- Të informojë përdoruesit për sjelljet dhe mënyrat e identifikimit të faktorëve të dyshimtë.
- Të nxit ndërgjegjësimin e përdoruesve duke dërguar njoftime dhe materiale informuese në mënryrë periodike.

Instrumentet e vlerësimit:

- Pyetje-përgjigje me gojë.

– Vëzhgim me listë kontrolli.

RN 4 Nxënësi rifreskon rregullat dhe aksesin në sisteme sipas politikave, udhëzimeve dhe azhornimeve më të fundit të sigurisë.

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

– Të kryejë kontrolle të vazhdueshme të historikut të aksesit në sistemet kritike.
– Të verifikojë rrugët e komunikimit dhe transferimit të të dhënave kritike.
– Të njoftojë në mënyrë të shpejtë dhe efikasë të gjithë përdoruesit fundor që lidhen me ngjarje që cënojnë sigurinë.
– Të infromojë përdoruesit për ndryshime apo nevojë për ndërhyrje në sisteme.
– Të infromojë përdoruesit për rreziqe dhe metoda sulmi të reja që mund ti kanosen organizatës.
– Të informojë përdoruesit për cështje të përmirësimit dhe rifreskimit të sistemeve të sigurisë.

Instrumentet e vlerësimit:

– Pyetje-përgjigje me gojë.
– Vëzhgim me listë kontrolli.

Udhëzime për zbatimin e modulit	– Mësuesi duhet të vërë në dispozicion të nxënësve dokumentacione të ndryshme në lidhje me legjislacionin dhe standartet ndërkombëtare. (fizike ose online) – Ky modul duhet të zhvillohet në klasë dhe laborator TIK. – Instruktori duhet të kryejë seancat praktike, ku të relizohen simulime të ndryshme të analizimit të legjislacionit, rregullores së brendshme dhe standartet e një organizate. – Nxënësit duhet të angazhohen në diskutime të ndryshme në lidhje legjislacionin, standartet ndërkombëtare dhe teknologjitë e ndryshme që ndihmojnë në zbatimin e tyre. – Instruktori nxit diskutime për krahasimin e standtareve të ndryshme të sigurisë kibernetike, avantazhet dhe disavantazhet e tyre, si edhe ngjashmëritë e tyre me legjislacionin kombëtar. – Realizimi i pranueshëm i modulit do të konsiderohet plotësimi nga nxënësi i të gjitha kritereve të realizimit të çdo rezultati të të nxënit të modulit, kritereve të realizimit të çdo rezultati të të nxënit. –
Kushtet e domosdoshme për realizimin e modulit.	Per realizimin si duhet te modulit eshte e domosdoshme te sigurohen mjediset, veglat, pajisjet, dhe materialet e meposhtme: – Klase per mesim teorik dhe praktik. – Dokumentacion i standarteve ndërkombëtare. – Legjislacioni ne fushën e cybersecurity.

8-Moduli "Testimi i sigurisë kibernetike"

Profili: Siguria kibernetike
Niveli: V i KSHK

PËRSHKRUESI I MODULIT		
Titulli dhe kodi	**TESTIMI I SIGURISË KIBERNETIKE**	**M-26-2064-24**
Qëllimi i modulit	Një modul teorik-praktik që i njeh nxënësit me mentalitetin e aktorëve të kërcënimit, i aftëson të të zbatojnë në mënyrë më efektive kontrollet e sigurisë dhe të monitorimit, analizimit dhe të përgjigjen ndaj kërcënimeve aktuale të sigurisë	
Kohëzgjatja e modulit	162 orë mësimore	
Niveli i parapëlqyer për pranim	– Të kenë përfunduar një kualifikim të nivelit IV në KSHK të fushës së TIK; – Të kenë përfunduar të paktën një kualifikim të nivelit IV në KSHK dhe kanë eksperiencë pune, të vërtetuar, të paktën një vit në fushën TIK;	
Rezultatet e të nxënit (RN) dhe procedurat e vlerësimit	**RN 1**	**Nxënësi shpjegoni rëndësinë e hakimit metodologjik etik dhe testimit të depërtimit.** ***Kriteret e vlerësimit:*** – Të interpretojë konceptin e Ethical hacking; – Të interpretojë llojet e hakimit (hacking); – Të përshkruajë aktivitetin e identifikimit të dobësive në një sistem kompjuterik – *Hacking;* – Të klasifikojë sipas kategorive llojet e ndryshme të hakerave në sigurinë kibernetike; – të interpretojë lloje të ndryshme metodologjish të ndjekur nga Hakerët; – Të interpretojë funksionin e *Ethical Hacking*; – Të zbatojë aftësitë dhe rregullat e Hakerit etikë; ***Instrumentet e vlerësimit:*** – Pyetje-përgjigje me gojë. Vëzhgim me listë kontrolli.
	RN2	**Nxënësi konfiguron një makinë virtuale për përvojën e të mësuarit të testimit të depërtimit** ***Kriteret e vlerësimit*** – Të përdorë gjuhë programimi për hakimin etik; – Të përdor terminologjinë në Ethical Hacking; – të përzgjedhë *hardware-in* e nevojshëm për të konfiguruar laboratorin e hakimit etik; – Të përzgjedhë software-in e nevojshëm për konfigurimin e laboratorit të hakerimit etik; – Të instalojë softuer *Virtual Machine (VM)* për konfigurimin

e laboratorit të hakerimit etik;
- Të instalojë sistemin operativ për testimin e dobësive;
- Të instalojë mjete dhe programet për të parandaluar hakerimin dhe marrjen e aksesit të paautorizuar në një kompjuter ose sistem rrjeti
- Të identifikojë mjetet më të mira për VAPT (Vulnerability Assessment and Penetration Testing)
- Të instalojë e përdor Kali Linux duke përdorur Virtual Box

Instrumentet e vlerësimit:
- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 3 Nxënësi interpreton dhe zbaton kundërmasat ndaj sulmeve gjatë fazave të procesit të hakerimit etik

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:
- Të zbatojë fazat e procesit të hakerimit etik;
- Të interpretojë llojet e sulmeve kibernetike në një system;
- Të identifikojë kërcënimet e sigurisë kompjuterike;
- Të interpretojë rrezikun e *Security Threat*;
- Të klasifikojë kërcënimet fizike në tre (3) kategori kryesore
- Të mbrojë sistemet kompjuterike nga kërcënimet fizike nëpërmjet masa të kontrollit;
- Të interpretojë llojet e kërcënimeve jo-fizike;
- Të përshkruajë procesin e zhvillimit të zbulimit *(Reconnaissance)*
- Të interpretojë lloje të ndryshme të *footprintin*
- Të mbledhë llojet e informacionit nëpërmjet procesit të *footprinting;*
- Të përdor teknikat e *footprinting* në hakimin etik;
- Të përdor metodën OS fingerprinting për të përcaktuar se cili sistem operativ po funksionon në një kompjuter të largët;
- Të përshkruajë llojet e procesit të *Enumeration*;
- Të përdorë metodat e teknikat e *Enumeration* në hakimin etik;
- Të përshkruajë metodologjitë e skanimit të rrjeteve në sigurinë kibernetike;
- Të përshkruajë llojet e ndryshme të sulmeve të mashtrimit- *Spoofing Attacks;*
- Të zbatojë masat e parandalimit të kërcënimeve jo-fizike përmes programeve antivirus, metodave të autentifikimit, DoS etj
- Të listojë llojet dhe teknikat e sulmeve inxhinierike sociale në sigurinë kibernetike;
- Të parandalojnë sulmet e inxhinierisë sociale
- të interpretojë kriptografinë, kriptologjinë (*Cryptology*) dhe aplikimet e saj;
- Të listojë lloje të ndryshme të kriptografisë në sigurinë kibernetike;

- Të përdorë algorimet e enkriptimit;
- Të identifikojë teknikat për të thyer fjalëkalimet – *Password*
- Të përdor programe softuerike që përdoren për të thyer fjalëkalimet e përdoruesve;
- Të aplikojë masa mbrojtëse nga sulmet e thyerjes së fjalëkalimit;
- Të intërpretojë mënyrat se si hakerat mund të përdorin *trojans,viruse* dhe *worms* për të kompromet uar një sistem kompjuterik;
- Të aplikojë kundërmasat që mund të përdoren për t'u mbrojtur *trojans,viruse* dhe worms;
- Të interpretojë *ARP Poisoning* dhe llojet e saj;
- Të parandalojë sulmet *ARP Poisoning*;
- Të interpretojë teknikat dhe mjetet e zakonshme network sniffing;
- Të interpretojë *Passive* dhe *Active Sniffing*;
- Të interpretojnë *Wi-Fi Authentication* dhe tri llojet e protokollet e enkriptimit *Wi-Fi*;
- Të listojë llojet e ndryshme të sulmeve Wi-Fi (*Wi-Fi attacks):*
- Të thyejnë fjalëkalimin WiFi (*Wireless*); duke përdorur mjetet e Hackerit;
- Të vendosin sigurinë nëpërmjet politikave të Wi-Fi;
- Të interpretojë sulmin *Denial of Service Attack* (DoS) dhe llojet e tij;
- Të ilustrojnë teknikat dhe mjetet se si kryhen sulmet *DoS* dhe teknikat e përdorura;
- Të përcaktojë politkat për të parandaluar sulmet *DoS* ndaj organizatave;
- Të përdor mjete ose programe të automatizuara për të skanuar në mënyrë aktive rrjetin, aplikacionin ose sistemet dhe për të identifikuar dobësitë ku dhe kur vijnë;
- Të përdor teknika si: *email spamming, social engineering, trojans, worms, phishing, port vulnerabilities,* etj për të nisur sulmet e hakerimit të sistemit;
- Të interpretojë teknikat e hakimit të aplikacioneve në web dhe kundërmasat që mund të vendosni për t'u mbrojtur nga sulme të tilla;
- Të interpretojë llojet dhe metodologjitë e sulmeve të serverit në web;
- Të interpretojë llojet e sulmit me injeksion *SQL* në aplikacion Web;
- Të përdorë mjetet e automatizimit për injektimin *SQL*;
- Të aplikojë politikat për parandalimin e sulmeve të injektimit SQL në një organizatë;
- Të ekzekutojë komadat për të identifikuar sistemin operativ që shërben një faqe interneti dhe të gjitha portat e hapura të lidhura me emrin e domenit, d.m.th., adresën IP;
- Të listojë mjetet e hakerimit të *Linux*;

	– Të aplikojë politikat për të parandaluar hakimet e *Linux* në një organizatë; – Të listojë lloje të ndryshme të sulmeve Bluetooth *(Bluetooth Attacks);* – Të interpretojë teknika të përdorura nga hakerat për të sulmuar pajisjen mobile; ***Instrumentet e vlerësimit:*** – Pyetje-përgjigje me gojë. – Vëzhgim me listë kontrolli.
Udhëzime për zbatimin e modulit	– Ky modul duhet të zhvillohet në laboratorin e TIK. – Instruktori duhet të shpjegojë dhe demonstrojë rëndësinë dhe teknikat e hakimit metodologjik etik dhe testimit të depërtimit. – Nxënësit duhet të angazhohen sa më shumë të jetë e mundur në diskutimet në lidhje me konfigurimin një makinë virtuale për përvojën e të mësuarit të testimit të depërtimit – Gjatë vlerësimit të kursantëve duhet të synohet më tepër në verifikimin e shkallës së aftësive praktike që ata kanë fituar për të kryer zbatimin e kundërmasave ndaj sulmeve gjatë fazave të procesit të hakerimit etik. – Instruktori duhet të kërkojë me rreptësi zbatimin nga nxënësit të rregullave të sigurimit teknik në punë, si dhe të nxitë punën në grup të tyre. – Realizimi i pranueshëm i modulit do të konsiderohet plotësimi nga nxënësi i të gjitha kritereve të realizimit të çdo rezultati të të nxënit të modulit, kritereve të realizimit të çdo rezultati mësimor të modulit.
Kushtet e domosdoshme për realizimin e modulit.	Për realizimin si duhet të modulit është e domosdoshme të sigurohen mjediset, veglat, pajisjet, dhe materialet e mëposhtme: – Klasë për mësim teorik dhe mjedise laboratori kompjuterik. – Pajisje kancelarie. – Shembull projekti dhe standarte të sigurisë kibernetike. – Paisje firewall të sigurisë kibernetike. – Lidhje interneti. – Materiale ilustruese dhe materiale të shkruara në mbështetje të çështjeve që trajtohen në modul (pankarta, udhëzuesa pune, rregullore etj.).

9. Moduli "Kriptimi dhe parandalimi i humbjes së të dhënave."

Profili: Siguria kibernetike
Niveli: V i KSHK

PËRSHKRUESI I MODULIT		
Titulli dhe kodi	**KRIPTIMI DHE PARANDALIMI I HUMBJES SË TË DHËNAVE**	**M-26-2065-24**
Qëllimi i modulit	Një modul teorik-praktik që i njeh nxënësit me teknikat dhe metodat e enkriptimit te informacionit, sistemet e parandalimit te humbjes se informacionit dhe konfigurimit te software-ve për këtë qëllim, dhe rëndësinë e testimit të funksionimit të tyre.	
Kohëzgjatja e modulit	162 orë mësimore	
Niveli i parapëlqyer për pranim	– Të kenë përfunduar një kualifikim të nivelit IV në KSHK të fushës së TIK; – Të kenë përfunduar të paktën një kualifikim të nivelit IV në KSHK dhe kanë eksperiencë pune, të vërtetuar, të paktën një vit në fushën TIK;	
Rezultatet e të nxënit (RN) dhe procedurat e vlerësimit	**RN 1** **Nxënësi përshkruan llojet e ndryshme të enkriptimit të informacionit.** ***Kriteret e vlerësimit:*** – Të përshkruajë koncepti en trekëndëshit CIA; – Të listojë tipet dhe metodat e ndryshme të enkriptimit të informacionit; – Të përshkruajë rëndësinë e enkriptimit të informacionit; – Të përshkruajë procesin e hashimit; – Të shpjegojë ndryshimin midis enkriptimit dhe hashimit; – Të përshkruajë llojet e çelësave të enkriptimit; – Të interpretojë mënyrën enkriptimit dhe dekriptimit të informacionit; ***Instrumentet e vlerësimit:*** – Pyetje-përgjigje me gojë. – Vëzhgim me listë kontrolli. **RN 2** **Nxënësi kryen përshkrimin e sistemeve të parandalimit të humbjes së të dhënave.** ***Kriteret e vlerësimit:*** Nxënësi duhet të jetë i aftë: – Të përshkruajë rëndësinë e klasifikimit të informacionit; – Të përshkruajë rëndësinë e përdorimit të softwareve për parandalimin e humbjes së të dhënave; – Të përshkruajë procesin dhe hapat e punës së *software*-ve për parandalimin e humbjes së të dhënave; – Të përshkruajë politikat dhe filtrat e vendosur në një sistem	

DLP;
- Të shpjegojë rëndësinë e integrimit të këtij sistemi me sistemet e tjera të sigurisë kibernetike, si *firewall*, SIEM, Antivirus… etj.

Instrumentet e vlerësimit:
- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 3 Nxënësi kryen instalimin dhe konfigurimin e software-ve të parandalimit te humbjes se te dhenave.

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:
- Të përzgjedh *software*-et e parandalimit të humbjes së të dhënave që përshtaten me sistemin operativ dhe përmasat e rrjetit sipas specifikimeve të projektit;
- Të shkarkojë *softwaret* e parandalimit të humbjes së të dhënave nga burimet e besueshme;
- Të zbatojë manualet dhe udhëzimet për instalimin softwareve të parandalimit të humbjes së të dhënave;
- Të konfigurojë softwaret e parandalimit te humbjes se te dhenave duke përcaktuar parametrat e sigurisë dhe preferencat e përdoruesit sipas projektit përkatës;
- Të aktivizojë softwaret duke u siguruar që të bëhen azhornime të rregullta për të mbajtur sigurinë e sistemit të përditësuar;
- Të dokumentojë instalimin dhe detajet e konfigurimeve të software-it, përfshirë rregullat e sigurisë dhe procedurat e implementuara.

Instrumentet e vlerësimit:
- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 4 Nxënësi teston funksionimin e software-ve të parandalimit te humbjes se te dhenave

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:
- Të testojë konfigurimin e sistemit te parandalimit te humbjes se te dhenave për të siguruar që të gjitha parametrat dhe rregullat e konfiguruara janë në përputhje me politikat e sigurisë të kërkuara;
- Të testojë filtrimin e informacionit dhe aftësinë e software për të ndaluar ose lejuar transferimin e informacionit;
- Të testojë nëse log-ët per software perkates jane te konfiguruara ne rregull dhe shruhen ne sistemet e monitorimit dhe ruajtes se log-eve;
- Të testojë proçesin e përditësimit të software-ve të parandalimit te humbjes se te dhenave për t'u siguruar që funksionon si duhet;
- Të testojë performancën e softwerit për të vlerësuar ndikimin

	e tij në performancën e sistemit dhe për të siguruar që nuk ka konflikte të padëshiruara ose ngadalësime në performancë; – Të sigurojë që software-ri funksionon në rregull me aplikacionet dhe pajisjet e tjera në infrastrukturën dhe nuk shkakton konflikte të papritura ose probleme të përshtatshmërisë; ***Instrumentet e vlerësimit:*** – Pyetje-përgjigje me gojë. – Vëzhgim me listë kontrolli.
Udhëzime për zbatimin e modulit	– Ky modul duhet të zhvillohet në laboratorin e shkollës për sigurinë kibernetike. – Instruktori duhet të zbatojë sa më shumë demonstrime enkriptimi të informacionit – Nxënësit duhet të angazhohen sa më shumë të jetë e mundur në diskutimet në lidhje me sistemet për parandalimin e humbjes së të dhënave – Gjatë vlerësimit të nxënësve duhet të synohet më tepër në verifikimin e shkallës së aftësive praktike që ata kanë fituar për të kryer veprimtaritë praktike. – Realizimi i pranueshëm i modulit do të konsiderohet plotësimi nga nxënësi i të gjitha kritereve të realizimit të çdo rezultati të të nxënit të modulit, kritereve të realizimit të çdo rezultati mësimor të modulit.
Kushtet e domosdoshme për realizimin e modulit.	Për realizimin si duhet të modulit është e domosdoshme të sigurohen mjediset, veglat, pajisjet, dhe materialet e mëposhtme: – Klasë për mësim teorik dhe mjedise laboratori kompjuterik. – Shembull projekti dhe standarte të sigurisë kibernetike. – Software te ndryshem te parandalimit te humbjes se te dhenave. – Lidhje interneti për të shkarkuar software të parandalimit te humbjes se te dhenave. – Manuale mbi instalimin dhe konfigurimin e software-ve te parandalimit te humbjes se te dhenave. – Materiale ilustruese dhe materiale të shkruara në mbështetje të çështjeve që trajtohen në modul (pankarta, udhëzuesa pune, rregullore etj.).

10. Moduli "Monitorimi dhe vlerësimi i sistemeve të sigurisë kibernetike"

Profili: Siguria kibernetike
Niveli: V i KSHK

PËRSHKRUESI I MODULIT		
Titulli dhe kodi	**MONITORIMI DHE VLERËSIMI I SISTEMEVE TË SIGURISË KIBERNETIKE**	**M-26-2066-24**
Qëllimi i modulit	Një modul teorik-praktik që i njeh nxënësit me rëndësinë e vlerësimit të parametrave mbi sigurinë kibernetike dhe monitorimin e tyre. Ky modul përshkruan dobësitë e problematikat e komponentëve fizik të rrjetit, llojet e testimeve, protokollet e autentifikimit, sistemet e monitorimit dhe analizimit të *Log-ve*.	
Kohëzgjatja e modulit	162 orë mësimore	
Niveli i parapëlqyer për pranim	– Të kenë përfunduar një kualifikim të nivelit IV në KSHK të fushës së TIK; – Të kenë përfunduar të paktën një kualifikim të nivelit IV në KSHK dhe kanë eksperiencë pune, të vërtetuar, të paktën një vit në fushën TIK;	
Rezultatet e të nxënit (RN) dhe procedurat e vlerësimit	**RN 1**	**Nxënësi përshkruan rëndësinë e vlerësimit të parametrave dhe problematikat e komponentve fizik të sistemeve operative dhe software-ve kibernetike** ***Kriteret e vlerësimit:*** – Të shpjegojë identifikimi e dobësive në infrastrukturë dhe proceset që mund të shfrytëzohen sulmet kibernetike ; – Të përshkruajë prioritetin e investimeve në sigurinë kibernetike; – Të shpjegojë kërkesat e pajtueshmërisë; – Të përshkruajë mekanizmat e duhura për zbulimin dhe reagimin ndaj sulmeve; – Të shpjegojë mbrojtjen e të dhënav sensitive; – Të përshkruajë parandalimin e defekteve në komponentët *hardware* ; – Të interpretojë risqet e sigurisë ndaj aksesit të paautorizuar ose ndërhyrjeve; – Të përshkruajë masat e marra për dëmtimet fizike ndaj fatkeqësive natyrore; – Të përshkruajë kufizimet e kapacitetit në performancën e rrjetit dhe përmirësimin e hardware sipas kërkesave të rritjes së trafikut; – Të përshkruajnë versionet e *update* ; – Të përshkruajë dobësitë e sigurisë në sistemet operative dhe *software*; – Të përshkruajë menaxhimin e *patcheve*;

- Të përshkruajë përputhshmërin dhe sigurinë e sistemeve ;
- Të përshkruajë mirëmbëjtjen, monitorimin e performancës dhe optimizimin e sistemeve;
- Të përshkruajë minimizimin e instalimeve të panevojshme të *software* dhe kryerjen e auditimeve të rregullta për uljen e kompleksitetit;
- Të përshkruajnë versionet e *update* për sistemet operative dhe *software*;
- Të përshkruajë konfigurimet e gabuara nga përdoruesi mbi sistemet operative dhe *software*;

Instrumentet e vlerësimit:

- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 2 Nxënësi përshruan llojet e testimeve të sigurisë dhe protokollet e autetifikimit (*WPA, WPA2, WPA3, LDAP, AAA* etj)

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

- Të përshkruajë testimin *Penetration* (*Pen Testing*);
- Të përshkruajë testimin *vulnerability (Vuln Testing);*
- Të përshkruajë testimin e sigurisë së aplikacioneve (*Application Security Testing);*
- Të përshkruajë testimin e sigurisë së rrjetit (*Network Security Testing);*
- Të përshkruajë testimin e sigurisë së shërbimeve *web (Web Services Security Testing);*
- Të përshkruajë protokollin *WPA2(Wi-Fi Protected Access 2);*
- Të përshkruajë protokollin *WPA3(Wi-Fi Protected Access 3);*
- Të përshkruajë *protokollin LDAP (Lightweight Directory Access Protocol);*
- Të përshkruajë protokollin *AAA (Authentication, Authorization, and Accounting*);

Instrumentet e vlerësimit:

- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 3 Nxënësi përshkruan sistemet e monitorimit, analizimin e *Log-eve* dhe transaksionet në rrjet

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

- Të përshkruajë sistemin e monitorimit dhe analizimit të sigurisë së rrjetit *Sguil*;
- Të përshkruajë platformën e vizualizimit të të dhënave *Kibana;*
- Të përshkruajë sistemin e monitorimit *Wireshark*;

- Të përshkruajë platformën për monitorim dhe analizimin e trafikut të rrjetit *Zeek;*
- Të analizojë të dhënat për të identifikuar sjellje të dyshimta, shkelje të sigurisë, dhe rreziqe të tjera potenciale;
- Të identifikojë llojet e *log-eve* ose transaksioneve;
- Të përshkruajë informacionet kryesore të *log-ut* ose transaksioneve;
- Të përshkruajë kontekstin e veprimit të *log-eve*;
- Të përshkruajë politikatë dhe protokollet e sigurisë;
- Të përshkruajë anomalit në *log* ;
- Të përshkruajë llojet e sulmeve të brendshme dhe të jashtme;
- Të ndërtojë raporte dhe të specifikojë rekomandime për veprime të mëtejshme;

Instrumentet e vlerësimit:

- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 4 Nxënësi përshkruan llojet e ndërhyrjeve, teknologjitë dhe mjetet mbrojtëse nga sulmet kibernetike

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

- Të përshkruajë sulmet fizike (*Physical Attacks);*
- Të përshkruajë sulmet logjike (*Logical Attacks);*
- Të përshkruajë *unauthorized network access*;
- Të përshkruajë *information disclosure;*
- Të përshkruajë *service interruption;*
- Të përshkruajë *traffic hijacking;*
- Të përshkruajë *identity spoofing;*
- Të përshkruajë funksionin e *hacking*;
- Të përshkruajë *firewall;*
- Të përshkruajë *antivirus dhe antimalware*;
- Të përshkruajë *intrusion detection systems (IDS) dhe intrusion prevention systems (IPS);*
- Të përshkruajë *encryption;*
- Të përshkruajë *multi-factor authentication (MFA);*
- Të përshkruajë *security information dhe event management (SIEM);*

Instrumentet e vlerësimit:

- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 5 Nxënësi shpjegon rëndësinë e përdorimit të *playbook* dhe mënyrat e shkrimit të raporteve mbi gjetjet

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

- Të përshkruajë standartizimin e veprimeve të *playbook*;
- Të përshkruajë rëndësinë e implementimit të *playbook* në

zgjidhjen e problemeve;
- Të përshkruajë rëduktimin e risqeve nga implementimi i *playbook*;
- Të përshkruajë përditësimet e *playbook* për të përfshirë praktika më të mira për menaxhimin e incidenteve;
- Të interpretojë ndërgjegjsimin e ekipit për sigurinë dhe mbrojtjen e kompanisë;
- Të shpjegojë strukturën e raportit mbi gjetjet;
- Të shpjegojë përshkrimin e situatës;
- Të analizojë faktorët që kanë ndikuar në situata;
- Të shpjegojë pasojat e mundshme të sitatës për sistemin apo kompaninë;
- Të listojë rekomandimet për zgjidhjen e situatës dhe uljen e rrezikut në të ardhmen;
- Të pasqyrojë dokumentimet e gjetjeve dhe rekomandimet;
- Të shkruajë raportin e gjetjeve me terma të qarta;
- Të përcaktohen në raport prioritetet për situatat kritike;

Instrumentet e vlerësimit:
- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 6 Nxënësi kontrollon funksionalitetin e infrastrukturës së *IT*-së.

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:
- Të monitorojë performancën e komponentëve hardwarë;
- Të realizojë testimet regressive në strukturën e *IT*-së;
- Të realizojë testimin e skripteve automatike;
- Të realizojë *backup dhe disaster recovery (DR);*
- Të monitorojë dhe menaxhojë infrastrukturën e *IT*-së *(Infrastructure Automation Monitoring Systems);*
- Të implementojë një strategji të sofistikuar mbi sigurinë;

Instrumentet e vlerësimit:
- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 7 Nxënësi vlerësonë parametrat mbi sigurinë kibernetike.

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:
- Të identifikojë dhe vlerësojë risqet mbi sigurinë kibernetike;
- Të vlerësojë integritetin e të dhënave;
- Të vlerësojë konfidencialitetin e të dhënave;
- Të përshkruajë aftësitë e kompanisë për të identifikuar,zbuluar dhe reaguar ndaj sulmeve për mbrojtjen e të dhënave;
- Të përshkruajë mbrojtjen dhe instalimin e mjeteve të sigurisë ndaj sulmeve të ndryshme;
- Të monitorojë dhe analizojë aktivitetin e rrjetit dhe sistemit për të indetifikuar sulmet;

– Të minimizojë kohën e ndërprerjes dhe pasojat negative në sistem ndaj sulmeve ;

Instrumentet e vlerësimit:

– Pyetje-përgjigje me gojë.
– Vëzhgim me listë kontrolli.

RN 8 Nxënësi analizonë *log-et* dhe transaksionet në rrjet.

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

– Të analizojë përzgjedhjen e burimeve të *log-eve;*
– Të analizojë platforma të specializuara për menaxhimin e *log-eve;*
– Të analizojë teknikat e *log-et* për të identifikuar sulmet dhe përpjekjet e ndërprerjes së shërbimeve;
– Të analizojë identifikimin e anomalive;
– Të analizojë monitorimin e sesioneve në rrjet;
– Të analizojë reagimin ndaj incidenteve;
– Të përcaktojë dhe implementojë masat të sigurisë shtesë për të përballuar rreziqet potenciale;

Instrumentet e vlerësimit:

– Pyetje-përgjigje me gojë.
– Vëzhgim me listë kontrolli.

RN 9 Nxënësi implementon teknologjitë dhe mjetet mbrojtëse nga sulmet kibernetike;

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:

– Të implementojë metodat e analizës së rrezikut për të vlerësuar ndikimin e mundshëm të sulmeve në kompani;
– Të implementojë *firewall-e* për të mbrojtur rrjetin tuaj nga sulment;
– Të implementojë enkriptimin e të dhënave;
– Të implementojë sistemet e monitorimit të sigurisë;
– Të implementojë plane për reagime ndaj sulmeve për të trajtuar dhe zvogëluar dëmet;
– Të përdorë manuale për edukimin dhe ndërgjegjësimin e personelit:
– Të testojë rregullisht sigurinë e infrastrukturës dhe përditësojë politikat dhe mjetet mbrojtëse për sigurinë e të dhënave;
– Të realizojë bashkëpunime me organizata për të ndarë informacion dhe për të përmirësuar koordinimin e reagimit ndaj rreziqeve kibernetike;

Instrumentet e vlerësimit:

– Pyetje-përgjigje me gojë.
– Vëzhgim me listë kontrolli.

Udhëzime për zbatimin e modulit	– Ky modul duhet të zhvillohet në laboratorin e shkollës për sigurinë kibernetike.

	– Instruktori duhet të zbatojë sa më shumë demonstrime praktike për llojet e testimeve, funksionalitetin e infrastrukturës së *IT*-së, vlerësime të parametrave si dhe kontrolle mbi zbatimin e protokolleve të autentifikimit . – Nxënësit duhet të angazhohen sa më shumë të jetë e mundur në diskutimet në lidhje veprimtaritë e vlerësimit dhe monitorimit të sistemeve për sigurinë kibernetike. – Gjatë vlerësimit të nxënësve duhet të synohet më tepër në verifikimin e shkallës së aftësive praktike që ata kanë fituar për të kryer veprimtaritë e vlerësimit dhe monitorimit të sistemit. – Instruktori duhet të kërkojë me rreptësi zbatimin nga nxënësit të rregullave të sigurimit teknik në punë, si dhe të nxitë punën në grup të tyre. – Realizimi i pranueshëm i modulit do të konsiderohet plotësimi nga nxënësi i të gjitha kritereve të realizimit të çdo rezultati të të nxënit të modulit, kritereve të realizimit të çdo rezultati mësimor të modulit.
Kushtet e domosdoshme për realizimin e modulit.	Për realizimin si duhet të modulit është e domosdoshme të sigurohen mjediset, veglat, pajisjet, dhe materialet e mëposhtme: – Mjedise laboratori kompjuterik. – Paisje *firewall* të sigurisë kibernetike. – Lidhje interneti për të shkarkuar *software* të sigurisë. – Manuale të përdorimit të pajisjeve . – Materiale ilustruese dhe materiale të shkruara në mbështetje të çështjeve që trajtohen në modul (pankarta, udhëzuesa pune, rregullore etj.).

11. Moduli "Garantimi i sigurisë së rrjetit të komunikimit".

Profili: Siguria kibernitike
Niveli: V i KSHK

PËRSHKRUESI I MODULIT		
Titulli dhe kodi	**GARANTIMI I SIGURISË SË RRJETIT TË KOMUNIKIMIT**	**M-26-2067-24**
Qëllimi i modulit	Një modul teorik-praktik që i njeh nxënësit me legjislacionin kombëtar në fuqi, standartet e sigurisë kibernetike që zbatohen në nivel ndërkombëtar dhe aplikimet e tyre në tekonologji.	
Kohëzgjatja e modulit	162 orë mësimore	
Niveli i parapëlqyer për pranim	– Të kenë përfunduar një kualifikim të nivelit IV në KSHK të fushës së TIK; – Të kenë përfunduar të paktën një kualifikim të nivelit IV në KSHK dhe kanë eksperiencë pune, të vërtetuar, të paktën një vit në fushën TIK;	
Rezultatet e të nxënit (RN) dhe procedurat e vlerësimit	**RN 1** **Nxënësi kryen analizë të detajuar të rrjetit.** ***Kriteret e vlerësimit:*** – Të përshkruajë burimet e të dhënave që nevojiten për të kryer analizën fiziket të komunikimit në rrjet; – Të përshkruajë burimet e të dhënave që nevojiten për të kryer analizën e konfigurimit të rrjetit; – Të përshkruajë metodat identifikimit të fijeve hyrëse dhe dalëse në *patch-panel*; – Të përshkruajë metodat e identifikimit të fijeve hyrëse dhe dalëse në *switch*; – Të përdorë pajisje për testimin e komunikimit në rrjet; – Të dallojë lloje të ndryshme të kabujve të komunikimit; – Të përdorë pajisje të markimit të portave dhe kabllove; – Të hartojë një raport për analizën e rrjetit; ***Instrumentet e vlerësimit:*** – Pyetje-përgjigje me gojë. – Vëzhgim me listë kontrolli. **RN 2** **Nxënësi monitoron zbatimit e rregullores dhe politikave të sigurisë për rrjetin e komunikimit.** ***Kriteret e vlerësimit:*** Nxënësi duhet të jetë i aftë: – Të përzgjedhë pajisjet e duhura për sigurinë e rrjetit kompjuterik; – Të kryejë rregullisht kontrolle të komunikimit hyrje-dalje të sistemeve që lidhen me të dhëna kritike; – Të verifikojë të drejtat e aksesit në sisteme sipas rregullores; – Të kryeje testime të procesve të punës që lidhen me akesin dhe	

komunikimin për të dhënat sensitive;
- Të kryejë testime të vazhdueshme të akesit të rrjetit në ambjente të kufizuara;
- Të monitorojë zbatimin e rregullores gjatë instalimit të infrastrukturës fizike të rrjetit kompjuterik;
- Të monitorojë zbatimin e politikave të sigurisë gjatë konfigurimit të rrjetit;
- Të konfigurojë *hostet*/pajisjet e rrjetit konform me rregulloren dhe udhëzimet;
- Të vlerësojë sigurinë e rrjetit kompjuterik;
- Të sigurojë adresimin e komponentëve dhe rrugëzimin e saktë të të dhënave nëpërmjet konfigurimit të *IP, Hostname, NetworkPath* etj.;

Instrumentet e vlerësimit:
- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 3 Nxënësi kryen instalime dhe konfigurime që lidhen me sigurinë e rrjetit të komunikimit.

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:
- Të përcaktojë teknologjinë e rrjetit kompjuterik;
- Të përcaktojë topologjinë e rrjetit kompjuterik;
- Të përcaktojë pajisjet dhe programet e duhura për sigurinë e rrjetit kompjuterik;
- Të konfigurojë parametrat e sigurisë në rrjete kabllore .(*Wired/LAN*), pa kabëll (*Wireless/WLAN*) dhe rrjetat virtuale (*VPN,VLAN*);
- Të konfigurojë pajisjet e rrjetit konform topologjisë së përcaktuar;
- Të aplikojë rregulla të menaxhimit në teknologjitë e ndryshme *hardware* dhe *software* sipas rregullores;
- Të hartojë strategji të menaxhimit dhe konfigurimit të parametrave të sigurisë sipas praktikave më të mira;
- Të testojë instalimet dhe konfigurimet e kryera duke ruajtur balancat ndërmjet performancës dhe sigurisë;
- Të identifikojë problemet në rrjetin kompjuterik;
- Të dokumentojë infrastrukturën e rrjetit kompjuterik;
- Të raportojë ndërhyrjet në rrjetin kompjuterik;

Instrumentet e vlerësimit:
- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

	RN 4 Nxënësi rifreskon rregullat dhe aksesin në sisteme sipas politikave, udhëzimeve dhe azhornimeve më të fundit të sigurisë. ***Kriteret e vlerësimit:*** Nxënësi duhet të jetë i aftë: – Të kryejë kontrolle të vazhdueshme të historikut të aksesit në sistemet kritike; – Të verifikojë rrugët e komunikimit dhe transferimit të të dhënave kritike; – Të njoftojë në mënyrë të shpejtë dhe efikasë të gjithë përdoruesit fundor që lidhen me ngjarje që cënojnë sigurinë; – Të infromojë përdoruesit për ndryshime apo nevojë për ndërhyrje në sisteme; – Të infromojë përdoruesit për rreziqe dhe metoda sulmi të reja që mund ti kanosen organizatës; – Të informojë përdoruesit për cështje të përmirësimit dhe rifreskimit të sistemeve të sigurisë; ***Instrumentet e vlerësimit:*** – Pyetje-përgjigje me gojë. – Vëzhgim me listë kontrolli.
Udhëzime për zbatimin e modulit	– Mësuesi duhet të vërë në dispozicion të nxënësve dokumentacione të ndryshme në lidhje me legjislacionin dhe standartet ndërkombëtare. – Ky modul duhet të zhvillohet në klasë ose laborator TIK. – Instruktori duhet të zhvillojë seanca praktike, ku të relizohen simulime të ndryshme për analizimin e legjislacionit të një organizate, rregulloren e brendshme dhe standardet. – Nxënësit duhet të angazhohen në diskutime të ndryshme në lidhje legjislacionin, standartet ndërkombëtare dhe teknologjitë e ndryshme që ndihmojnë në zbatimin e tyre. – Instruktori të nxisë diskutime në lidhje me krahasimin e standardeve të sigurisë kibernetike, avantazhet dhe disavantazhet e tyre, si edhe ngjashmëritë me legjislacionin kombëtar. – Realizimi i pranueshëm i modulit do të konsiderohet plotësimi nga nxënësi i të gjitha kritereve të realizimit të çdo rezultati të të nxënit të modulit, kritereve të realizimit të çdo rezultati mësimor të modulit.
Kushtet e domosdoshme për realizimin e modulit.	Për realizimin si duhet të modulit është e domosdoshme të sigurohen mjediset, veglat, pajisjet, dhe materialet e mëposhtme: – Klasë për mësim teorik. – Dokumentacion i standarteve ndërkombëtare. – Legjislacioni në fushën e *cybersecurity*.

12. Moduli "Parandalimi i anomalive dhe reagimi ndaj tyre"

Profili: Siguria kibernetike
Niveli: V i KSHK

PËRSHKRUESI I MODULIT		
Titulli dhe kodi	**PARANDALIMI I ANOMALIVE DHE REAGIMI NDAJ TYRE**	**M-26-2068-24**
Qëllimi i modulit	Një modul teorik-praktik që i njeh nxënësit me teknikat e parandalimit të anomalive dhe teknikave të reagimit ndaj anomalive të ndryshme të ndodhura në një infrastrukturë *IT*.	
Kohëzgjatja e modulit	162 orë mësimore	
Niveli i parapëlqyer për pranim	– Të kenë përfunduar një kualifikim të nivelit IV në KSHK të fushës së TIK; – Të kenë përfunduar të paktën një kualifikim të nivelit IV në KSHK dhe kanë eksperiencë pune, të vërtetuar, të paktën një vit në fushën TIK;	
Rezultatet e të nxënit (RN) dhe procedurat e vlerësimit	**RN 1**	**Nxënësi përshkruan menyrat dhe masat e parandalimit te anomalive kibernetike** ***Kriteret e vlerësimit:*** – Të shpjegojë rëndësinë e standardeve të sigurisë kibernetike dhe infrastrukturave *IT (ISO/IEC-27001/NIST*, etj); – të përzgjedhë standardin bazuar në kërkesat e projektit dhe politikave të institucionit/kompanisë; – të shpjegojë modelin *Zero Trust* në një infrastrukturë *IT*; – të përshkruajë metodat e autentifikimit; – të zbatojë modelin *Zero Trust* në një infrastrukturë *IT*; – Të realizojë ndërlidhjen e sistemit *Zero Trust* me të gjithë sistemet e tjera të sigurisë kibernetike; – Të testojë sistemin *Zero Trust* për të parë reagimin për performancë dhe funksionalitet; – Të jetë në gjendje të perzgjedhë metodat e autentifikimit bazuar në kërkesat e infrastrukturës dhe projektit; – të instalojë dhe konfigurojë metodat e autentifikimit duke përdorur manualet dhe praktikat më të mira; ***Instrumentet e vlerësimit:*** – Pyetje-përgjigje me gojë. – Vëzhgim me listë kontrolli.
	RN 2	**Nxënësi kryen analizimin e mangesive ne nje infrastrukture IT (*Gap Analysis*)** ***Kriteret e vlerësimit:*** Nxënësi duhet të jetë i aftë: – Të përshkruajë rëndësinë e procesit te analizimit te

mangesive (*Gap Analysis*);
- Të shpejgojë disa metoda të ndryshme të procesit të analizimit të mangesive;
- Të perzgjedhë metoden, duke marrë parasysh infrastrukturën IT, kërkesat e projektit apo rregulloren e brendëshme të institucionit/biznesit;
- Të kryejë procesin e analizimit të magesive;
- Të identifikojë rezultatet e procesit te analizimit te magësive;
- Të kategorizojë rezultatet sipas rëndësisë;
- Të raportojë tek departamentet përkatëse rezultatet së bashku me sygjerimet për përmirësimin e pikave të raportuara;
- Të dokumentojë të gjithë procesin e analizës së mangësive;
- Të ndjekë gjithë procesin e përmirësimit dhe kryer procesin vetëm për raportimet e realizuara.

Instrumentet e vlerësimit:
- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 3 Nxënësi vlerëson rreziqet për të identifikuar dhe kategorizuar anomali të mundshme

Kriteret e vlerësimit:

Nxënësi duhet të jetë i aftë:
- Të shpjegojë rëndësinë e përdorimit te sistemeve të monitorimit të *logs (SIEM);*
- Të përzgjdhë sistemin e monitorimit të *log-eve*, bazuar në insfrastrukturën IT, kërkesat dhe paramentrat e projektit;
- Të instalojë sistemin e monitorimit, menaxhimit dhe ruajtjes së *logs-eve (SIEM);*
- Të konfigurojë sistemin e monitorimit, menaxhimit dhe ruajtjes së *logs-eve (SIEM)* duke përcaktuar parametrat e sigurisë dhe preferencat e përdoruesit sipas projektit përkatës;
- Të konfigurojë pajisjet e ndryshme të cilat duhet të sjellin informacion *(log)* në *SIEM;*
- Të realizojë testim të sistemit për të parë nëse informacioni vjen nga të gjitha pajisjet e konfiguruara;
- Të analizojë të dhënat e *logs* duke kryer analizë në opsionet e sistemit ose me sisteme te jashtëme;
- Të konfigurojë *alert* të ndryshme për të realizuar kërkime dhe njoftime automatike në sistemin *SIEM;*
- Të shkruajë dhe konfigurojë *query* të ndryshme për të marrë vetëm informacionin e nevojshëm që i duhet për analizimin e informacionit;
- Të kategorizojë eventet dhe rreziqet e identifikuara;

Instrumentet e vlerësimit:
- Pyetje-përgjigje me gojë.
- Vëzhgim me listë kontrolli.

RN 4 Nxënësi reagon kunder nje anomalie ne nje infrastrukture

	IT ***Kriteret e vlerësimit:*** Nxënësi duhet të jetë i aftë: – Të kontrollojë sistemet e ndryshme për anomali; – Të izolojë pajisjet e infektuara, duke i shkëputur nga lidhja në rrjet, deri në marjen e masave dhe analizimin e situatës; – Të analizojë rrjetin/sistemin për pajisje të tjera me sjellje të dyshimta; – Të përcaktojë anomalinë dhe nivelin e rrezikut; – Të bllokojë akseset e përdoruesve në sistem apo të bllokoje *userin* nësë ka evente të dyshimta nga *useri* përkatës; – Të kryejë analizë nësë ka *usera* të tjerë me të njëjtën sjellje; – Të relizojë kopje të paprekur së makinës së prekur nga anomalia, për analiza të mëtejshme; – Të kryejë pastrimin e pajisjeve të prekura, nëse është e mundur dhe të relizojë rikthimin e tyre në rrjet në mënyrë të sigurtë; – Të raportojë tek ekipet e specializuara për anomali për të cilat kërkohet një analizë më e thelluar; ***Instrumentet e vlerësimit:*** – Pyetje-përgjigje me gojë. – Vëzhgim me listë kontrolli.
Udhëzime për zbatimin e modulit	– Ky modul duhet të zhvillohet në laboratorin TIK të shkollës . – Instruktori duhet të zbatojë sa më shumë elemente të standardeve të sigurisë kibernetike. – Instruktori duhet të zbatojë sa më shumë demonstrime praktike të teknikave të instalimit dhe konfigurimit të sistemeve te ndryshme *Zero Trust* dhe *SIEM.* – Instruktori duhet të përfshije sa më shumë nxënësit në përdorimin e metodave për abalizimin e mangësive. – Nxënësit duhet të angazhohen sa më shumë në mënyren e konfigurimit të metodave të *authentikimit*. – Nxënësit duhet të angazhohen sa më shumë të jetë e mundur në diskutimet në lidhje me përzgjdhjen e metodave të ndryshme për analizimin e mangësive. – Gjatë vlerësimit të kursantëve duhet të synohet më tepër në verifikimin e shkallës së aftësive praktike që ata kanë fituar për të kryer veprimtaritë e instalimit dhe konfigurimit të sistemeve të authentikimit, *Zero Trust, SIEM.* – Nxenesit duhet te përfshihen ne testime te ndryshme anomalish në rrjet dhe të jenë në gjendje të identifikojnë anomalinë dhe të përgjigjen kundër saj. – Instruktori duhet të kërkojë me rreptësi zbatimin nga nxënësit të rregullave të sigurimit teknik në punë, si dhe të nxitë punën në grup të tyre. – Realizimi i pranueshëm i modulit do të konsiderohet plotësimi nga nxënësi i të gjitha kritereve të realizimit të çdo rezultati të të nxënit të modulit, kritereve të realizimit të çdo rezultati mësimor të

	modulit.
Kushtet e domosdoshme për realizimin e modulit.	Për realizimin si duhet të modulit është e domosdoshme të sigurohen mjediset, veglat, pajisjet, dhe materialet e mëposhtme: – Klasë për mësim teorik dhe mjedisë laboratori kompjuterik. – Pajisje kancelarie. – Shembull projekti dhe standarte të sigurisë kibernetike. – *Software* dhe pajisje per implementimin e një modeli *Zero Trust.* – *Software* të ndryshëm për implementimin e sistemeve të authentikimit. – *Software* për monitorimit, menaxhimit dhe ruajtjes së *logs-eve (SIEM)* – Lidhje interneti për të shkarkuar *software* të sigurisë. – Manuale mbi instalimin dhe konfigurimin *softwareve*. – Materiale ilustruese dhe materiale të shkruara në mbështetje të çështjeve që trajtohen në modul (pankarta, udhëzuesa pune, rregullore etj.).

VIII. Programi i praktikës profesionale të grupuar, në biznes.

“Programi i Praktikës Profesionale të Grupuar, në Biznes”

Kodi P-26-006-24

Shkolla Profesionale ..... **Viti shkollor 202...-202...**

Profili mësimor “Siguria kibernetike”, Niv. V i KSHK

Klasa .....

Biznesi: .....

Mësuesi i praktikës ..... **Instruktori i biznesit .....**

Nr	Vendi i punës	Veprimtaritë praktike	Kompetencat profesionale që zhvillohen	Koha (orë)
1	Administrimi i Rrjetave	Konfigurim *Firewall.* Konfigurim sistemi *Zero Trust*. Konfigurim të protokolleve të sigurisë në *routera* dhe *switch-e.* Konfigurim të *IDS/IPS* Konfurime të sigurisë në rrjetat *WiFi*	Konfigurim dhe mirëmbajtje në siguri rrjetash	20
2	Administrimi i sistemeve	Instalim dhe konfigurim *antivirus* Instalim dhe konfigurim sistemesh authentikimi Instalim dhe konfigurim sistemesh për menaxhimin e *log* Konfigurim sigurie në *servera* Instalim dhe konfigurim të sisteme *DLP* Instalim dhe konfigurim në sistemet e mbrojtjes *email*	Mënyra e instalimit dhe konfigurimeve në sistemet e IT	30
3	*SOC* Analist (Analist Sigurie Niveli II)	Leximi dhe interpretimi i *logs* Kategorizim i gjetjeve duke bërë analizë të *logs* Ndjekje e *Playbook* në rast incidenti dhe tejkalim kur duhet më tepër *support*.	Analiza e *log* në sistemet *SIEM* Identifikimi i anomalive nëpërmjet leximit të *log-s* Ndjekja e procedurave të punës.	25
4	Analist *CSIRT* (Analist Sigurie Niveli II)	Mënyra e reagimit kundër incidenteve. Marja e masave paraprake për izolimin e një sulmi. Realizimi i kopjeve të sistemeve të infektuar.	Menxhimi dhe reagimi kundër incidenteve kibernetike.	25
5	Simulim i incidenteve kibernetike	Kryerja e *GAP Analysis* Kryerja e simulimeve të	Metodat e *GAP* Analysis Metodat e skanimit të	25

		incidenteve kibernetike	infrastrukturës IT për vulnerabilitete.	
6	*ISO / CISO*	Zbatimi i standardeve të sigurisë kibernetike *ISO/NIST* Trajnime të higjienës kibernetike Analizimi i raporteve të sigurisë kibernetike	Standardet dhe rëndësia e zbatimit të tyre. Zbatimi i politikave dhe procedurave. Rëndësia e trajnimit të stafit dhe vlerësimi i mangësive në trajnime.	25
			Totali i kohës	**150 orë**

IX. Programi orientues i provimeve përfundimtare

A) Programi orientues për Provimin e Teorisë Profesionale të integruar

Programi orientues për Provimin e teorisë profesionale të integruar, në profilin mësimor "Siguria kibernetike", Niveli V i KSHK, është hartuar duke u mbështetur në përmbajtjet teorike (njohuritë) që përmbajnë modulet mësimore në dy vitet mësimore të këtij kualifikimi. Modulet mësimore, përmbajtjet teorike dhe peshat e tyre përkatëse tregohen në tabelën e mëposhtme:

Nr	Moduli mësimor / Temat teorike	Peshat
1	**Hyrje në sigurinë kibernetike** - Domosdoshmëria e sigurisë kibernetike - Dokumentimi i sulmeve, konceptet dhe teknikat - Mbrojtja e të dhënave personale, të institucionit, të biznesit	10
2	**Sistemet e teknologjisë së informacionit** - Komponentët dhe kategoritë e sistemeve të informacionit – *SI* - Organizimi i të dhënave dhe aksesin në rrjet - Zhvillimi dhe dizenjimi i sistemeve të informacionit - Përcaktimi sigurisë e sistemeve të informacionit	10
3	**Legjislacioni, etika dhe standardet në sigurinë kibernetike** - Legjislacionin në fuqi për sigurinë kibernetike - Zbatimi i legjislacionit dhe rregullores **s**ë brendshme në mjedisin e punës	10
4	**Zbatimi i Python në sigurinë kibernetike** - Programe të thjeshta në gjuhën *Python* - Funksionet, klasat dhe objektet në gjuhën *Python* në funksion të sigurisë kibernetike - Implementimi i librarive në *python* për të rritur sigurinë kibernetike. - Automatizimi i sigurisë së informacionit	10
4	**Gjurmimi dhe identifikimi i faktorëve të dëmshëm** - Analiza e sjelljes së përdoruesve bazuar në historikun e ngjarjeve të raportuara dhe raportet e gjeneruara nga sistemet. - Komunikimi i përdoruesve strategjitë dhe praktikat me të fundit për shmangjen e rrezikut dhe faktorët e dëmshëm. - Rregullat e aksesit në sisteme sipas politikave, udhëzimeve dhe azhornimeve më të fundit të sigurisë.	20
5	**Kriptimi dhe parandalimi i humbjes se te dhenave (DLP)** - Llojet e ndryshme të enkriptimit të informacionit. - Përshkrimi i sistemeve të parandalimit të humbjes së të dhënave.	10
6	**Monitorimi dhe vlerësimi i sistemeve të sigurisë kibernetike** - Vlerësimi i parametrave dhe problematikat e komponentve fizike të sistemeve operative dhe *software-ve* - Llojet e testimeve të sigurisë dhe protokollet e autetifikimit(*WPA, WPA2, WPA3, LDAP, AAA* etj) - Sistemet e monitorimit, analizimin e *Log-eve* dhe transaksionet në rrjet - Ndërhyrjet, teknologjitë dhe mjetet mbrojtëse nga sulmet kibernetike - Rëndësia e përdorimit të *playbook* dhe mënyrat e shkrimit të raporteve mbi gjetjet - Kontrolli i funksionalitetit të infrastrukturës së IT-së. - Vlerësimi i parametrave të sigurinë kibernetike	20

7	**Siguria e rrjetit të komunikimit** -Analiza e detajuar e rrjetit - Rregulloret dhe politikat e sigurisë për rrjetin e komunikimit.	10
	TOTALI	**100%**

Provimi i teorisë profesionale të integruar do të jetë me test me shkrim, i cili zgjat 1,5 (një presje pesë orë) dhe përgatitet nga Komisioni i Provimit Përfundimtar i drejtimit të nivelit përkatës. Në hartimin e testit komisioni duhet të mbajë parasysh rregullat, parimet dhe formatet, për ndërtimin e testit.

Testi duhet të përmbajë 20 njësi testi me një total prej 40 pikë. Nga këto, 10 njësi testi (10 pikë) të jenë me zgjedhje të shumëfishtë (me 4 alternativa) dhe 10 të tjerat (30 pikë) të jenë njësi testi me përgjigje të kufizuara/të mbyllura (me PO/JO; me e Vërtetë e Gabuar; me plotësim të fjalës që mungon; etj.) Testi nuk duhet të përmbajë pyetje me përgjigje të hapura.

Njësitë e testit duhet të jenë në tri nivele vështirësie, me shpërndarje pothuaj të barabartë, si më poshtë:

Niveli I (i ulët)	Niveli II (mesatar)	Niveli III (i lartë)
Aftësia për të rikujtuar/ identifikuar dhe për të përshkruar...	Aftësia për të zbatuar/argumentuar/ shpjeguar/krahasuar dhe për të analizuar...	Aftësia për të vlerësuar dhe për të nxjerrë përfundime...

Më poshtë tregohet skema e konvertimit në nota të pikëve të fituara:

Pikët	**0 ÷ 10**	**11 ÷ 15**	**16 ÷ 20**	**21 ÷ 25**	**16 ÷ 30**	**31 ÷ 35**	**36 ÷ 40**
Notat	**4**	**5**	**6**	**7**	**8**	**9**	**10**

B) Programi orientues për Provimin e Praktikës Profesionale të integruar

Programi orientues për provimin e praktikës profesionale të integruar, në profilin mësimor "Siguria kibernetike", është hartuar duke u mbështetur në listën e kompetencave profesionale dhe në modulet mësimore, që përmban Skeletkurrikuli përkatës.
Lista e kompetencave profesionale për të cilat duhet të vlerësohen nxënësit**, detyrat e punës** dhe **pikët** për secilën kompetencë janë si më poshtë:

Nr	Kompetencat profesionale	Detyrat e punës	Pikët
1	- Ndërtimi i programit në gjuhën *Python* për manipulimin e klasave dhe objekteve në identifikimin dhe mbrojtjen e të dhënave. - Automatizimi i sistemeve të sigurisë me anë të një programi në gjuhën *Python.*	**Detyra 1:** Veprime në fushën e programimit ne *Python*	15
2	- Instalimi dhe konfigurimi i pajisjeve dhe programeve të sigurisë kibernetike - Zbatimi i metodave për rritjen e sigurisë në	**Detyra 2:** Veprime në fushën e sistemeve të sigurisë	30

	sistemet operative të pajisjeve fundore për lidhje fizike dhe *mobile.*	së informacionit	
3	- Analizimi i detajuar i sjelljes së përdoruesve bazuar në historikun e ngjarjeve dhe raporteve të sistemeve - Testimi i vulnerbiliteteve të infrastrukturës IT	**Detyra 3:** Veprime në fushën e testimit të ngjarjeve dhe raporteve të vulnerabiliteteve	15
4	- Krijimi i një makine për testimin e depërtimit - Përcaktimi i metodave të enkriptimit dhe dekriptimit - Instalimi dhe testimi i programeve që shmangin humbjet e të dhënave - Testimi i sigurisë dhe i protokolleve të autentifikimit - Analizimi i *Log*-eve dhe i transaksioneve në rrjet - Analizimi i mangësive në një infrastrukturë IT (*Gap Analysis*)	**Detyra 4:** Veprime në fushën e enkriptimit, monitorimit dhe testimit të programeve për parandalimin e humbjeve të të dhënave	40
		Shuma	**100**

Më poshtë tregohet skema e konvertimit në nota të pikëve të fituara:

Pikët	**0 ÷ 40**	**41 ÷ 50**	**51 ÷ 60**	**61 ÷ 70**	**71 ÷ 80**	**81 ÷ 90**	**91 ÷ 100**
Notat	**4**	**5**	**6**	**7**	**8**	**9**	**10**

<u>Shënime</u>:

- Provimi praktik do të realizohet me anë të metodës së vlerësimit të nxënësve në "***detyra pune***" (në tabelë tregohen katër detyrat kryesore të punës). Ai do të realizohet në laboratorët e praktikave pranë shkollave profesionale për të gjitha ato procese që garantohen plotësisht në ambientet e bazës praktike. Për proceset që nuk garantohen në laboratorin e praktikave të shkollës, ato do të kryhen në ndërmarrje apo biznese, që plotësojnë kushtet për realizimin e tyre. Në rast të kundërt, rekomandohen si zgjidhje e vetme përfundimtare programet e virtualizimit dhe simulimit.
- Koha për realizimin e të gjitha detyrave duhet të jetë jo më shumë se 3 (tre) orë, në përputhje kjo me udhëzimin për organizimin dhe zhvillimin e provimeve në AFP.
- Në vlerësimin e kompetencave profesionale, rekomandohet t'i lihet hapësirë për vlerësime edhe bashkëbisedimit profesional ndërmjet komisionit dhe nxënësit, pasi ai është element i rëndësishëm i secilës prej kompetencave të listuara.
- Është ***e domosdoshme dhe shumë e rëndësishme*** që për çdo detyrë, që në fillim të provimit të praktikës profesionale, nga mësuesit/instruktorët (organizatorët e provimit) t'i kushtohet vëmendje ***"përcaktimit dhe zbatimit të rregullave të sigurimit teknik dhe të ruajtjes së mjedisit"*** gjatë gjithë kryerjes së detyrës për çdo nxënës**.**
- Për çdo detyrë, komisioni i vlerësimit duhet të përgatisë instrumentet përkatëse të vlerësimit sipas kompetencave profesionale. Instrumenti i vlerësimit për secilën detyrë duhet të përfshijë të gjitha hapat e realizimit të saj, duke filluar nga përgatitja e vendit, mjeteve dhe pajisjeve të punës etj.

- Gjithashtu për çdo detyrë komisioni duhet të përfshijë në vlerësim një element shumë të rëndësishëm, i cili është sistemimi dhe mirëmbajtja e mjeteve dhe pajisjeve të punës, pasi nxënësi ka realizuar dhe përfunduar detyrën.
- Për realizimin e detyrës, nxënësve duhet t'u sigurohen mjete, pajisjet si dhe materialet për realizimin e këtyre detyrave.
- Nxënësit duhet t'i realizojë të gjitha detyrat.
- Instrumenti i vlerësimit duhet të përfshijë në përmbajtjen e tij edhe kritere për vlerësimin e kompetencave kyçe profesionale si vetëkontrolli, përgjegjshmëria, manifestimi i guximit, angazhimi fizikisht, mendërisht dhe emocionalisht në kryerjen e detyrave të ndryshme si dhe komunikimi, bashkëpunimi në grup, bashkëveprimi ndërmjet njëri tjetrit etj.
- Gjithashtu, komisioni duhet të hartojë dhe një listë kriteresh vlerësimi për detyrën përfundimtare, si dhe mund të hartohet një grafik për përcaktimin e kohës së realizimit të secilës detyrë.
- Komisioni i provimit për secilën detyrë parapërgatit tezat e provimit ku nxënësi në mënyrë të rastësishme zgjedh njërën prej tyre. Komisioni i provimit duhet të përgatisë paraprakisht instrumentin e vlerësimit me procedurat/hapat/etapat e kryerjes së detyrave. Komisioni nuk duhet të ndërhyjë gjatë zhvillimit të provimit.
- Të katër detyrat e përcaktuara nga komisioni, paraqiten me anë të fletëve të punës (tezave të provimit), të cilat do të përzgjidhen nga nxënësit në mënyrë të rastësishme (duhet të hartohen disa variante për secilën detyrë).
- Nxënësit do të vlerësohen me anë të "listës së kontrollit", me anë të së cilës verifikohen arritjet e tyre kundrejt "kritereve të vlerësimit".
- Fletët e punës (tezat e provimit), udhëzuesi dhe grafiku i kohës të bashkangjitura janë të detyrueshme t'i jepet çdo nxënësi. Gjithashtu një kopje bashkë me listën e vlerësimit mbahet nga komisioni. Në fund bëhet lidhja e fletës së punës së nxënësit me listën e kontrollit për arsye dokumentimi.