AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

Azərbaycan Respublikasının
Elm və Təhsil Nazirliyinin
_____ nömrəli _____2025-ci il
tarixli əmri ilə təsdiq edilmişdir.

MAGİSTRATURA SƏVİYYƏSİNİN İXTİSAS ÜZRƏ

T Ə H S İ L P R O Q R A M I

İxtisasın şifri və adı: **7006017 - İnformasiya təhlükəsizliyi**

BAKI – 2025

1. Ümumi müddəalar

1.1. Magistratura səviyyəsinin **7006017 – İnformasiya təhlükəsizliyi** ixtisası üzrə təhsil proqramı (bundan sonra – təhsil proqramı) "Təhsil haqqında" Azərbaycan Respublikasının Qanununa, Azərbaycan Respublikasının Nazirlər Kabinetinin müvafiq qərarlarına, eləcə də "Ali təhsilin magistratura səviyyəsi üzrə ixtisasların Təsnifatı"na, qabaqcıl beynəlxalq təcrübə və əmək bazarının tələblərinə uyğun olaraq hazırlanmışdır.

1.2. Təhsil proqramının məqsədləri aşağıdakılardır:
- ixtisas üzrə məzunun səriştələrini, ixtisasın çərçivəsini, fənlər üzrə tədris və təlim metodlarını, qiymətləndirmə üsullarını, təlim nəticələrini, kadr hazırlığı aparmaq üçün infrastruktur və kadr potensialına olan tələbləri, təhsilalanın təcrübə keçmə, işə düzəlmə və təhsilini davam etdirmə imkanlarını müəyyənləşdirmək;
- təhsilalanları və işəgötürənləri məzunların əldə etdiyi bilik, bacarıq və təlim nəticələri ilə tanış etmək;
- təhsil proqramı üzrə kadr hazırlığının bu proqrama uyğunluğunun qiymətləndirilməsi zamanı prosesə cəlb olunan tərəfdaşları məlumatlandırmaq.

1.3. Təhsil proqramı, tabeliyindən, mülkiyyət növündən və təşkilati-hüquqi formasından asılı olmayaraq, Azərbaycan Respublikasında fəaliyyət göstərən və həmin ixtisas üzrə magistr hazırlığını həyata keçirən bütün ali təhsil müəssisələri üçün məcburidir.

1.4. Təhsilalanın 5 (beş) günlük iş rejimində həftəlik auditoriya və auditoriyadankənar ümumi yükünün həcmi 45 akademik saatdır (xüsusi təyinatlı ali təhsil müəssisələri istisna olmaqla). Bu zaman auditoriya saatlarının həcmi 12-16 akademik saat təşkil edir. Peşəkar məqsədlər üçün dərindən öyrənilən ixtisaslaşmalar üzrə həftəlik dərs yükünün həcmi dəyişdirilə bilər.

1.5. Ali təhsil müəssisəsi tərəfindən ixtisasın həmin müəssisədə kadr hazırlığı aparılan hər bir ixtisaslaşması üzrə ayrıca təhsil proqramı hazırlanmalıdır. Hər bir ixtisaslaşma üzrə təhsil proqramı müvafiq ixtisasın təhsil proqramındakı bölmələrlə yanaşı, həmin ixtisaslaşma üzrə tədris və təlim metodları, təlim nəticələrinin qiymətləndirilməsi üsulları, təcrübələrin təşkili və qiymətləndirilməsi və s. bölmələri də əks etdirməlidir.

2. Məzunun səriştələri

2.1. Təhsil proqramının sonunda məzun aşağıdakı ***ümumi səriştələrə*** yiyələnməlidir:
- peşəkar fəaliyyəti çərçivəsində gözlənilməz və mürəkkəb məsələləri müstəqil şəkildə həll edə bilmək;
- müvafiq fəaliyyət və metodları təklif etmək, planlaşdırmaq, onların cari və perspektiv nəticələrini təhlil etmək;
- fəaliyyət və ya təhsil sahəsi ilə bağlı problemlərin səbəblərini araşdırmaq, konkret vaxt çərçivəsində və məhdud informasiya şəraitində onları həll edə bilmək;
- fəaliyyət və ya təhsil sahəsi ilə bağlı problemlərin həlli zamanı müvafiq texnologiya və metodları seçmək və onlardan istifadə edə bilmək, həmçinin gözlənilən nəticələri müəyyənləşdirmək, dəyərləndirmək və qiymətləndirmək;
- fəaliyyət və ya təhsil sahəsi ilə bağlı problemlərin həlli zamanı öz fəaliyyətini tənqidi şəkildə dəyərləndirmək;
- fəaliyyət və ya təhsil sahəsi ilə bağlı problemləri Azərbaycan dilində və bir xarici dildə şifahi və yazılı olaraq təqdim etmək, əsaslandırmaq, həmçinin mütəxəssis və qeyri-mütəxəssislərlə birgə müvafiq müzakirələrdə iştirak etmək;
- müxtəlif üsullarla öz bilik və səriştələrini başqalarına ötürə bilmək;

- istənilən şəraitdə etik davranış qaydalarına uyğun şəkildə fəaliyyət göstərmək, şəxsi davranışlarının etik aspekt və imkanlarını, məhdudiyyətlərini və sosial rolunu anlamaq;
- davamlı öyrənmə və peşəkar inkişafla bağlı özünün və digərlərinin ehtiyaclarını qiymətləndirə bilmək, həmçinin müstəqil öyrənmə üçün zəruri olan səmərəli metodlardan istifadə edə bilmək;
- zəruri metod və alətlərdən, süni intellekt və maşın öyrənməsi üsullarından istifadə etməklə yeni təhlükəsizlik modellərinin və qorunma vasitələrinin işlənməsi istiqamətində elmi tədqiqatlar aparmaq, elmi məqalə, texniki hesabat və təqdimatlar hazırlamaq və alınmış nəticələri tətbiq etmək.

2.2. İxtisaslaşmalar üzrə məzun aşağıdakı **peşə səriştələrinə** yiyələnməlidir:

İnformasiya mühafizəsi və təhlükəsizliyi ixtisaslaşması üzrə:
- informasiya sistemlərinin və kompüter şəbəkələrinin təhlükəsizliyinin təmin olunması üçün ən son texnologiya və metodologiyalardan istifadə etmək;
- şəbəkə təhlükəsizliyi və təhlükəsizlik divarları (firewall), müdaxilənin aşkarlanması (ID), müdaxilənin qarşısının alınması (IP) sistemləri ilə işləmək;
- autentifikasiya, identifikasiya, gizliliyinin, bütövlüyünün və əlçatanlığının (CIA modeli) təmin olunması üsullarını tətbiq etmək;
- kriptoqrafik qoruma üsulları, şifrələmə alqoritmləri, elektron imza, açarların idarə edilməsi sistemlərini (PKI) reallaşdırmaq və tətbiq etmək;
- informasiya təhlükəsizliyinin təşkilati və texniki aspektlərini başa düşmək, informasiya təhlükəsizliyi risklərini qiymətləndirmək və idarə etmək;
- informasiya təhlükəsizliyi siyasətinin hazırlamaq və tətbiq etmək;
- süni intellekt və maşın öyrənməsi texnologiyalarını informasiya təhlükəsizliyinin təmin olunmasında tətbiq etmək;
- bulud xidmətləri ilə bağlı təhlükəsizlik tədbirlərini yerinə yetirmək.

Kibertəhlükəsizlik ixtisaslaşması üzrə:
- kriptoqrafiya, autentifikasiya, identifikasiya, məlumatların gizliliyi, bütövlüyü və əlçatanlığı (CIA modeli) ilə bağlı zəruri bililklərə malik olmaq, kriptoqrafik qoruma üsullarını, şifrələmə alqoritmlərini, elektron imza, açarların idarə edilməsi sistemlərini (PKI), SSL/TLS protokollarını reallaşdırmaq və tətbiq edə bilmək;
- kibertəhlükəsizlik strategiyasını hazırlamaq, təşkilatın təhlükəsizlik siyasətlərini formalaşdırmaq və tətbiq etmək;
- kibertəhlükəsizlik risklərini təhlil etmək, qiymətləndirmək, uyğun müdafiə tədbirlərinin planlaşdırılması, idarə edilməsi strategiyalarını hazırlamaq və icra etmək;
- zəif yerlərin aşkarlanması skanerlərini, penetrasiya testlərini və etik hakerliyi həyata keçirmək;
- kiberinsidentlərin aşkarlanması, təhlili və cavablandırılması, loq analizləri, forensik analiz və sübutların toplanması, qorunması, hüquqi prosedurlarla, SIEM (Splunk, Qradar və s.) sistemləri ilə işləmək;
- zərərli proqram təminatlarını (malware, phishing, DoS/DDoS, ransomware və s.) analiz etmək və qarşısını almaq;
- firewall, IDS/IPS, VPN, şəbəkə monitorinqi kimi texnologiyaları konfiqurasiya və idarə etmək;
- kibertəhlükəsizlik sahəsində yaranan problemlərin həllində süni intellekt və maşın öyrənməsi texnologiyalarını tətbiq etmək;
- ISO/IEC 27001, COBIT, NIST SP 800 seriyasından olan standartları öz fəaliyyətində rəhbər tutmaq, tətbiq etmək və onların tələblərinə riayət etmək.

Kompüter və şəbəkə təhlükəsizliyi ixtisaslaşması üzrə:

- əməliyyat sistemlərinin (MS Windows, Linux) təhlükəsiz idarə olunması, endpoint təhlükəsizliyi (antivirus, EDR sistemləri), proqram təminatında zəifliklərin analizi və kod səviyyəsində qoruma (secure coding, code auditing) üsullarını reallaşdırmaq;
- kompüter sistem və şəbəkələrində məlumatların qorunması, şəbəkə təhlükəsizliyi, trafiklərin analizi və təhlükələrin qarşısının alınması texnologiyalarını (firewall, VPN, IDS/IPS) tətbiq etmək;
- sistem və şəbəkələrin zəifliklərini təhlil etmək, aşkarlamaq və bu zəifliklərə qarşı mübarizə üsul və vasitələrini tətbiq etmək;
- kompüter və şəbəkə təhlükəsizliyi protokollarını, kriptoqrafik şifrələmə üsullarını, elektron imza texnologiyasını, açarların idarə olunması sistemlərini reallaşdırmaq və tətbiq etmək;
- təhlükəsiz şəbəkə arxitekturasını layihələndirmək və qurmaq, virtual maşınlar və sandbox texnologiyaları ilə test və analiz etmək;
- firewall, router, switch və digər şəbəkə avadanlıqlarında təhlükəsizlik tədbirləri, VPN texnologiyaları və təhlükəsizlik protokolları (SSL/TLS, IPSec), IDS/IPS sistemlərinin konfiqurasiya və istismar etmək;
- kompüter sistemlərində və şəbəkələrində mümkün zərərli proqramları aşkarlamaq və qarşısını almaq.

İnformasiya sistemlərinin təhlükəsizliyi (sahələr üzrə) ixtisaslaşması üzrə:

- müxtəlif əməliyyat sistemləri (Linux, Windows, Mac OS, IOS, Android və s.), onların xarakterisitik funksiyaları , fayl sistemləri, spesifik proqramları ilə işləmək, eləcə də bu əməliyyat sistemləri mühitində informasiya sistemlərini qurmaq və istismar etmək;
- informasiya sistemlərinə qoyulan təhlükəsizlik tələblərini müəyyənləşdirmək, bu tələblər nəzərə alınmaqla informasiya sistemlərini layihələndirmək, təhlükəsiz arxitekturasını qurmaq.
- informasiya sistemlərində yaranan zəiflikləri, zərərli proqram təminatlarını (malware, phishing, DoS/DDoS, ransomware və s.) aşkarlamaq, təhlil etmək və onlara qarşı müvafiq təhlükəsizlik tədbirlərini həyata keçirmək;
- informasiya sistemlərində kriptoqrafik qoruma üsullarını reallaşdırmaq, elektron imza texnologiyasını tətbiq etmək;
- İT infrastrukturunda informasiya sistemlərinə yönəlmiş təhlükələrin mənbələrini proqnozlaşdırmaq, hücumların səbəb və təsirlərini müəyyənləşdirmək, riskləri təhlil etmək, qiymətləndirmək, uyğun müdafiə tədbirlərini planlaşdırmaq, idarə etmək, zəif yerlərin aşkarlanması skanerlərini, penetrasiya testlərini və etik hakerliyi həyata keçirmək;
- informasiya sistemləri üçün təhlükəsizlik siyasətlərini hazırlamaq, tətbiq etmək, beynəlxalq təhlükəsizlik standartlarına uyğun idarəetmə sistemlərini qurmaq;
- informasiya sistemlərinin şəbəkə təhlükəsizliyini təmin etmək və hücumlardan qormaq, şəbəkə izləmə və müdafiə alətləri ilə işləmək.

Rəqəmsal kriminalistika ixtisaslaşması üzrə:

- rəqəmsal kriminalistik üçün zəruri məlumatların qorunması üçün kriptoqrafik şifrləmə üsullarının tətbiqi, təhlükəsiz məlumat mübadiləsi üçün elektron imza, açarların idarə edilməsi sistemlərini tətbiq etmək;
- rəqəmsal kriminalistik məlumatların əldə edilməsi üçün kriptoqrafik analiz üsullarını tətbiq etmək;
- kiberhücumlar zamanı ilkin cavab tədbirlərinin həyata keçirilməsi, zərərverici proqramların (malware analysis) davranışını analiz, hücum zəncirinin (kill chain) qurulması və həyata keçirilməsini təhlil edə bilmək;

- kompüterlər, mobil cihazlar, serverlər və digər rəqəmsal daşıyıcılardan sübutların toplanması və qorunması, məlumatların bərpası, şifrələnmiş və silinmiş faylların analizi üsullarını bilmək;
- FTK, EnCase, Autopsy, Cellebrite, X-Ways Forensics kimi proqramlarla, SIEM (Splunk, Qradar və s.) sistemləri ilə işləmək, forensik analiz, loq faylların və şəbəkə trafikinin, metadata və zaman məlumatlarını analiz edə bilmək;
- sübutların zəncirinin qorunması (chain of custody), rəqəmsal sübutların məhkəmədə qəbul edilə biləcək səviyyədə sənədləşdirilməsi, əldə edilən sübutların hüquqi və etik əsaslara uyğun emal edə bilmək;
- rəqəmsal sübutların qanuni statusu, məxfi və şəxsi məlumatların qorunması qanunvericiliyini bilmək, milli və beynəlxalq hüquq normalarına uyğun təhqiqat aparmaq, cinayət və kibercinayət kontekstində sübutları istifadə edə bilmək;
- təhqiqat düşüncəsi və sübutlara əsaslanan qərar vermək, cinayət hadisələrinin rəqəmsal izlərinin bərpası və analiz edilərək məntiqi nəticələr çıxarmaq, məhkəmə ekspertizası üçün texniki hesabatlar yazmaq, etik davranış və şəxsi məlumatların qorunması prinsiplərinə riayət etmək.

Kriptovalyuta və blokçeyn texnologiyaları ixtisaslaşması üzrə:
- paylanmış reyestrlər (DLT), blok strukturları və konsensus alqoritmləri (Proof of Work, Proof of Stake, BFT və s.) haqqında biliyə malik olmaq, blokçeyn şəbəkələrinin layihələndirilməsi, növləri (public, private, consortium) və funksional modelləri ilə işləmək;
- rəqəmsal aktivlərin iqtisadiyyatı, token modelləri, DeFi (Decentralized Finance) konseptləri, kriptovalyuta birjaları və rəqəmsal pul kisələri ilə işləmək;
- Ethereum, Hyperledger, Solana, Cardano və s. platformalarda smart müqavilələri (Solidity, Rust, Vyper və s. dillərində) hazırlamaq;
- DApp-ları (decentralized applications) layihələndirmək və inkişaf etdirmək, blokçeyn üzərində avtomatlaşdırılmış hüquqi və maliyyə proseslərini formalaşdırmaq;
- smart müqavilələrdə zəifliklərin təhlili (reentrancy, integer overflow/underflow, access control və s.), blokçeyn texnologiyalarında təhlükəsizlik riskləri və hücum modelləri (51% attack, Sybil attack, DAO hack və s.) ilə işləmək.
- kriptovalyutaların və blokçeyn texnologiyalarının tənzimlənməsi üzrə beynəlxalq və yerli hüquqi normaları, AML (Anti-Money Laundering), KYC (Know Your Customer) və vergi tələblərinə uyğunluğu qiymətləndirmək və nizamlamaq;
- kriptovalyutaların və blokçeyn texnologiyalarının reallaşdırılması zamanı məlumatların məxfiliyinin qorunması üçün kriptoqrafik şifrələmə üsullarını elektron imza alqoritmlərini tətbiq etmək.

İdarəetmə sistemlərinin proqram təminatının təhlükəsizliyi ixtisaslaşması üzrə:
- idarəetmə sistemlərinin strukturu və funksionallığı (məs. SCADA, PLC, HMI, RTU), onların tətbiq sahələrinin (enerji, nəqliyyat, su təchizatı, istehsalat və s.) xüsusiyyətləri nəzərə alınmaqla müvafiq proqram təminatının təhlükəsizliyini təmin etmək;
- proqram təminatının yaradılması zamanı təhlükəsiz proqramlaşdırma prinsiplərini tətbiq etmək, proqram kodlarında zəifliklər (buffer overflow, injection, privilege escalation və s.) aşkarlamaq və aradan qaldırmaq, proqram kodlarını analizetmə vasitələri və statik/dinamik təhlil metodlarını istifadə etmək;
- SCADA və digər idarəetmə sistemlərinə qarşı tipik hücumları (Stuxnet tipli hücumlar, MITM, replay attacks və s.) aşkarlamaq və onların qarşısını almaq;
- sistemlərin qorunması üçün firewall, router, switch və digər şəbəkə avadanlıqlarında təhlükəsizlik tədbirləri, VPN texnologiyaları və təhlükəsizlik protokollarını (SSL/TLS, IPSec),

IDS/IPS sistemlərinin konfiqurasiya və istismar etmək, segmentləşdirmə və autentifikasiya texnologiyaları ilə işləmək;
- idarəetmə sistemlərinin proqram təminatlarının zərərli proqramlardan qorumaq;
- idarəetmə sistemlərinin təhlükəsizlik auditi, risklərin identifikasiyası, təhlili və idarə strategiyalarını hazırlamaq, failsafe və failover mexanizmlərini qiymətləndirə bilmək;
- sənaye təhlükəsizliyi üzrə beynəlxalq standartları (IEC 62443, NIST SP 800-82, ISO/IEC 27001) tətbiq etmək, uyğunluq tələblərinə cavab verən təhlükəsizlik strategiyalarını formalaşdırmaq.

Tətbiqi kriptoqrafiya ixtisaslaşması üzrə:
- klassik və müasir simmetrik və asimmetrik şifrələmə alqoritmlərini (AES, RSA, ECC, ElGamal, ChaCha20 və s.), açarların idarə edilməsi sistemlərini (PKI), açıq və gizli açarlı sistemlərin təhlükəsizliyi və istifadə sahələrini bilmək,kriptoqrafik alqoritmləri proqramlaşdırmaq, kriptoqrafik sistemləri qurmaq və tətbiq edə bilmək;
- kriptovalyuta və elektron imza texnologiyalarını, elektron imzaların və sertifikat sistemlərinin kriptoqrafik bazaları istifadə edə bilmək;
- internetin təhlükəsiz protokollarını (SSL/TLS, IPsec, SSH və s.), açar mübadiləsi protokollarını (Diffie-Hellman, ECDH), autentifikasiya mexanizmlərini reallaşdırmaq və tətbiq edə bilmək;
- kriptoqrafik protokolların zəifliklərinin təhlil etmək və formal sübutlarla təhlükəsizlik qiymətləndirməsi aparmaq;
- PKI (Public Key Infrastructure), elektron sertifikatlar və elektron imza sistemləri ilə işləmək, açarların idarə olunması, saxlanması və rotasiya siyasətlərini hazırlamaq;
- simvol analizi və statistik kriptoanaliz, yan kanal, vaxt analizi, seçilmiş ilkin mətnin və şifrmətnin analizi üsullarını, hücum modellərini, kriptoqrafik sistemlərə real hücum ssenarilərini qurmaq, reallaşdırmaq və tətbiq edə bilmək;
- kriptoqrafiyanın istifadəsi ilə bağlı hüquqi və etik çərçivələrə riayət etmək, dövlət və korporativ təhlükəsizlik tələblərinə uyğun kriptoqrafik tətbiqlər hazırlamaq.

Telekommunikasiya sistemlərinin informasiya təhlükəsizliyi ixtisaslaşması üzrə:
- telekommunikasiya sistemlərinin (mobil şəbəkələr, IP şəbəkələr, VoIP, 5G, optik şəbəkələr və s.) arxitekturalarını reallaşdırmaq və prinsiplərini tətbiq etmək;
- şəbəkə infrastrukturunu təhlükəsizlik baxımından təhlil etmək və layihələndirmək, əsas şəbəkə protokollarını (TCP/IP, SIP, RTP, MPLS, BGP və s.) praktiki reallaşdırmaq və tətbiq etmək;
- telekommmunikasiya şəbəkələrində kriptoqrafik şifrləmə üsullarını tətbiq etmək, səs, data və siqnalları şifrələmək, genişzolaqlı şəbəkələrdə və radio kanallarda məlumatların təhlükəsiz ötürülməsi, firewall, IDS/IPS, VPN və anti-Dos/DDoS texnologiyalarından istifadə etmək;
- telekommuinkasiya infrastrukturlarına qarşı mümkün hücumları (IMSI catching, man-in-the-middle, jamming, SS7 exploit və s.) bilmək, onların aşkarlanması və qarşısının alınması üçün texnoloji və proqram təminatlarını tətbiq edə bilmək;
- telekommuinkasiya sistemlərində mümkün zəifliklərı və sızmaları aşkarlamaq, təhlil etmək, qarşısını almaq, penetrasiya testlərini həyata keçirmək;
- telekommunikasiya şəbəkələrində informasiya təhlükəsizliyi sahəsində yerli və beynəlxalq standartları (ISO/IEC 27011, ETSI, ITU-T, NIST və s.) fəaliyyətində rəhbər tutmaq;
- telekommunikasiya sistemlərində abunəçi məlumatlarının qorunması, fərdi məlumatların mühafizəsi və məxfiliyin təmin olunması tələblərini təmin etmək;
- telekommunikasiya sistemlərində təhlükəsizlik risklərini təhlil etmək, risklərin idarə olunması strategiyalarını hazırlamaq və həyata keçirmək;

- telekommunikasiya infrastrukturları üçün informasiya təhlükəsizliyi siyasətlərini və prosedurlarını layihələndirmək və yerinə yetirmək.

Sənaye idarəetmə sistemlərinin təhlükəsizliyi ixtisaslaşması üzrə:

- SCADA, DCS, PLC, RTU kimi sənaye idarəetmə sistemlərini istifadə və istismar etmək, sənaye proseslərinin avtomatlaşdırılması və real vaxt rejimində idarə edilməsi prinsiplərini tətbiq etmək;
- ICS/SCADA sistemləri üçün təhlükəsiz şəbəkə arxitekturasını qurmaq, dərin müdafiə (defense-in-depth) yanaşmasını, Firewall, IDS/IPS, ağ siyahı (whitelisting), VPN və zonalaşdırma prinsiplərini tətbiq edə bilmək;
- sənaye idarəetmə sistemlərinin kibertəhlükəsizliyi tələblərini, sənaye idarəetmə sistemləri protokollarının (Modbus, DNP3, OPC-UA, IEC 60870-5-104 və s.) təhlükəsizlik prinsiplərini təmin etmək ;
- hücum modelləri və təhlükələr (stuxnet, ransomware hücumları, insider threats, MITM və s.) barədə məlumatlarr toplusuna malik olmaq, insidentlərin aşkarlanması və qarşısının alınması üçün müdafiə tədbirlərini tətbiq etmək, bərpa planlarını hazırlamaq və yerinə yetirmək;
- sənaye müəssisələrində informasiya təhlükəsizliyi risklərini qiymətləndirmək, təhlükəsizlik boşluqlarını aşkarlamaq və müvafiq tədbirləri planlaşdırmaq;
- sənaye idarəetmə sistemləri üzrə auditləri təşkil etmək və beynəlxalq standartlara uyğunluğu qiymətləndirmək;
- əsas sənaye təhlükəsizliyi standartlarını (IEC 62443, NIST SP 800-82, ISO/IEC 27019, ANSI/ISA 99), sənaye müəssisələrində tətbiq edilən təhlükəsizlik siyasətlərini rəhbər tutmaq və onların tələblərinə riayət etmək.

Bulud hesablamalarının təhlükəsizliyi ixtisaslaşması üzrə:

- bulud xidmət modellərini (IaaS , PaaS , SaaS), paylanmış sistemləri və virtuallaşdırma texnologiyalarını reallaşdırmaq və tətbiq etmək;
- bulud xidmətlərinin qurulması üçün hibrid, ictimai (public), özəl (private) və çoxbuludlu (multi-cloud) arxitekturaları reallaşdırmaq;
- bulud xidmətlərində təhlükəsizlik tələbləri ilə bağlı autentifikasiya, identifikasiya, məlumatların gizliliyi, bütövlüyü, əlçatanlığı (CIA modeli) və mövcudluğunun təmin edilməsi üsullarını, məlumatların şifrələnməsi, yüngün şifrələmə alqoritmləri, elektron imza, açarların idarə edilməsi sistemlərini (PKI) reallaşdırmaq və tətbiq etmək;
- bulud mühitlərində spesifik hücumları (VM escape, side-channel attacks, hypervisor attacks, data leakage və s.) və təhlükəsizlik boşluqları üzrə risk analizi və onların qarşısının alınması strategiyalarını, insidentlərin aşkarlanması, onlara cavab verilməsi və insident sonrası bərpa (Disaster Recovery & Business Continuity) tədbirlərini reallaşdırmaq və tətbiq etmək;
- IAM (Identity and Access Management), MFA (Multi-Factor Authentication), SSO (Single Sign-On) texnologiyalarını tətbiq etmək;
- SIEM, CASB, DLP, WAF, SASE və digər təhlükəsizlik həlləri ilə işləmək;
- mövcud bulud platformalarında (AWS, Azure, Google Cloud və s.) təhlükəsizlik siyasətlərini idarə edə bilmək.

Elektron ticarət sistemlərinin təhlükəsizliyi ixtisaslaşması üzrə:

- E-ticarət platformalarının quruluşunu və işləmə mexanizmlərini, ödəniş sistemlərini (PayPal, Stripe, 3D Secure, PSD2 və s.), rəqəmsal pul kisələri və onlayn bankçılıq texnologiyalarını reallaşdırmaq və istifadə etmək;
- E-ticarət infrastrukturunda istifadə olunan proqram və texnologiyalarını (CMS, ERP, CRM və s.) tətbiq etmək;

- E-ticarət sistemlərində konfidensiallıq, bütövlük, əlçatanlıq (CIA modeli), identifikasiya, autentifikasiya və icazə (OAuth2, OpenID, MFA) prosedurlarını tətbiq etmək;
- kriptoqrafik şifrləmə üsul və alqoritmlərini, SSL/TLS və digər təhlükəsizlik protokollarını, elektron imza, tokenləşdirmə texnologiyalarını tətbiq etmək;
- elektron ödənişlərin təhlükəsizliyi və PCI DSS (Payment Card Industry Data Security Standard) standartlarının tələblətini təmin etmək;
- veb əsaslı hücumların aşkarlanması və qarşısının alınması (XSS, SQL injection, CSRF, session hijacking və s.), Web Application Firewall (WAF) və digər qoruma texnologiyalarını tətbiq etmək;
- GDPR, KVKK və digər məlumat mühafizəsi qanunvericilik sənədlərinin tələblərinə uyğun siyasətləri hazırlamaq, fərdi və ödəniş məlumatlarının şifrələnməsi və anonimləşdirilməsi üsullarını reallaşdırmaq və tətbiq etmək;
- E-ticarət layihələrində risklərin təhlili və minimuma endirilməsi, təhlükəsizlik auditi, zərərli fəaliyyətlərin monitorinqi və insidentlərin idarə olunması, penetrasiya testlərini və zəifliklərin aşkarlanması prosedurlarını həyata keçirmək.

Mobil tətbiqlərin təhlükəsizliyi ixtisaslaşması üzrə:

- mobil əməliyyat sistemlərinin (Android, iOS) arxitekturası və təhlükəsizlik modellərini, mobil tətbiqlərin yaradılması mühitlərini və proqramlaşdırma dillərini (Java/Kotlin, Swift, Dart/Flutter, React Native və s.), mobil tətbiqləri reallaşdırmaq və tətbiq etmək;
- OWASP Mobile Top 10 (insecure data storage, insecure communication, code tampering və s.) əsasında zəifliklərin müəyyən edilməsi, statik (SAST), dinamik (DAST) və davranış analizləri vasitəsilə mobil tətbiqlərdə mümkün zəifliklərı aşkarlamaq;
- tərs mühəndislik və tətbiq kodunun qorunması üsullarını (obfuscation, anti-debugging və s.) tətbiq etmək;
- mobil tətbiqlərdə konfidensial məlumatların təhlükəsiz saxlanması (Keychain, Keystore, Secure Storage və s.), TLS/SSL protokolları ilə məlumatların şifrələnməsi və etibarlı ötürülməsi üsullarını, token əsaslı autentifikasiya sistemlərini (OAuth 2.0, JWT və s.) tətbiq etmək;
- mobil tətbiqlərə yoluxan zərərli proqramların (mobile malware) aşkarlanması və qarşısının alınması üsul və vasitələrini tətbiq etmək;
- Runtime təhlükələrə qarşı müdafiə tədbirlərini, Rooted/jailbroken cihazlarda təhlükəsizlik risklərinin qiymətləndirilməsi üsullarını, təhlükəsizlik testlərini reallaşdırmaq və tətbiq etmək;
- mobil tətbiqlərin tənzimləyici normativ sənədlərin və standartların (ISO/IEC 27034, GDPR, PCI-DSS və s.), mobil tətbiq mağazalarının (App Store, Google Play) təhlükəsizlik tələblərinə uyğunluğunu qiymətləndirmək və təmin etmək.

Veb texnologiyaların təhlükəsizliyi ixtisaslaşması üzrə:

- veb proqramlaşdırma dillərində və mühitlərində (HTML, CSS, JavaScript, PHP, Python, Node.js, React, Angular, Django, Laravel və s.) proqramlaşdırmaq;
- müştəri-server əsaslı tətbiqlərin qurulması və qarşılıqlı əlaqəsinin təmin edilməsi strategiyalarını, RESTful API-lər, AJAX texnologiyalarını, mikroxidmət arxitekturasını tətbiq etmək;
- veb texnologiya mühitində məlumatların konfidensiallığı, bütövlüyü və əlçatanlığının (CIA modeli) təmin edilməsi üsullarını, identifikasiya və autentifikasiya prosedurlarını reallaşdırmaq və tətbiq etmək;
- təhlükəsiz proqramlaşdırma prinsipləri, kodda zəifliklərin, o cümlədən OWASP Top 10 zəifliklərin aşkarlanması və qarşısının alınması vasitələri (SQL Injection, Cross-Site Scripting

– XSS, Cross-Site Request Forgery – CSRF, Insecure Deserialization, Broken Authentication və s.) ilə işləmək;
- SAST, DAST, IAST kimi təhlükəsizlik testləri metodologiyalarını, əl ilə və avtomatlaşdırılmış zəiflik aşkarlama vasitələrini (Burp Suite, OWASP ZAP, Nikto, Acunetix və s.), penetrasiya testlərini və "bug bounty" metodologiyasını tətbiq etmək;
- HTTPS, TLS/SSL protokolları ilə məlumatların təhlükəsiz ötürülməsi, token əsaslı autentifikasiya (OAuth 2.0, JWT (JSON Web Token), SSO və MFA), sessiyaların idarə olunması və cookie təhlükəsizliyi texnologiyalarını reallaşdırmaq;
- Apache, Nginx, IIS və s. serverlərin təhlükəsizlik konfiqurasiyaları, CDN, WAF (Web Application Firewall), Reverse Proxy, DDoS qorunması texnologiyalarını, bulud əsaslı veb platformalarda təhlükəsizlik (AWS, Azure, Google Cloud) yanaşmalarını tətbiq etmək;
- veb sistemlərin tənzimləyici normativ sənədlərin və standartların (ISO/IEC 27001, GDPR, PCI-DSS, NIST və s.) tələblərinə uyğunluğunu qiymətləndirmək və təmin etmək.

3. Təhsil proqramının strukturu

3.1. Təhsil proqramının mənimsənilməsinin normativ müddəti və məzunlara verilən ali elmi-ixtisas dərəcəsi:

İxtisaslaşmaların adları	Verilən dərəcə	Əyani forma üzrə təhsil müddəti	Kreditlərin sayı
İnformasiya mühafizəsi və təhlükəsizliyi	Magistr ali elmi-ixtisas	2 il	120
Kibertəhlükəsizlik			
Kompüter və şəbəkə təhlükəsizliyi			
İnformasiya sistemlərinin təhlükəsizliyi (sahələr üzrə)			
Rəqəmsal kriminalistika			
Kriptovalyuta və blokçeyn texnologiyaları			
İdarəetmə sistemlərinin proqram təminatının təhlükəsizliyi			
Tətbiqi kriptoqrafiya			
Telekommunikasiya sistemlərinin informasiya təhlükəsizliyi			
Sənaye idarəetmə sistemlərinin təhlükəsizliyi			
Bulud hesablamalarının təhlükəsizliyi			
Elektron ticarət sistemlərinin təhlükəsizliyi			
Mobil tətbiqlərin təhlükəsizliyi			
Veb texnologiyaların təhlükəsizliyi			

3.2. Təhsil proqramı 120 (2 il) AKTS kreditindən ibarət olmalıdır. Hər semestrdə 5 fəndən çox olmamaq şərti ilə 30 kredit nəzərdə tutulmuşdur. Kreditlər aşağıdakı şəkildə bölüşdürülür:

Sıra sayı	Fənnin adı	AKTS krediti
1	**Tədqiqat metodları** *Bu fənn kəmiyyət və keyfiyyət tədqiqat metodlarının, ölçmə, tədqiqat dizaynı və təhlilin qarşılıqlı asılılığına diqqət yetirir. Fənn çərçivəsində tədqiqat*	

	səriştələri, kitabxana və internet resurslarından məlumat qaynağı kimi istifadə edilməsi, verilənlərin araşdırılması, təhlil edilərək təqdim edilməsi kimi keyfiyyətin aşılanmasını nəzərdə tutur.	6
2	**Akademik yazı və etika** *Bu fənnin məqsədi akademik yazı, danışıq və dürüstlüyün əsaslarını öyrətmək, magistrantların elmi məqalə, dissertasiya, esse və digər akademik sənədləri peşəkar şəkildə yazmaq, konfrans, simpozium, seminar və elmi diskussiyalarda peşəkar şəkildə danışmaq, nəşr etikası bacarıqlarını inkişaf etdirməkdir. Fənn təhsilalanlara akademik üslub, mənbələrdən düzgün istifadə, istinad qaydaları və etik normalar haqqında bilik və səriştələr verəcəkdir.*	6
3	**Tədqiqat analitikası** *Bu fənnin tədrisi məlumat təhlili prosesi, məlumat növləri, məlumatların toplanma mənbələri, məlumat təhlili üzrə strategiyanın qurulması, məlumatların təhlil üçün hazırlanması və təmizlənməsi, təhlil üçün məlumatların sistemləşdirilməsi, məlumatların vizuallaşdırılması, sahəyə uyğun olaraq təhlillərdə istifadə olunacaq proqram təminatları ilə tanışlıq ("Excel", "SPSS", "Stata", "R", "MAXQDA", "Matlab", "Python" və s. kimi), ixtisas sahəsində tədqiqatlarda istifadə olunan təhlil metodları ilə təhlillərin aparılması (statistik testlər və təhlillər, kəmiyyət və keyfiyyət təhlilləri, eksperimental təhlillər, anket və sorğu təhlilləri və s. kimi) və təhlillərin əsasında müvafiq rəylərin hazırlanmasını nəzərdə tutur.*	6
4	**Ali təhsil müəssisəsi tərəfindən müəyyən edilən məcburi fənlər**[1] *ixtisaslaşmadan asılı olaraq buraya daxil edilən fənlər hər bir ali təhsil müəssisəsi tərəfindən fərdi qaydada müəyyən edilir və həmin ixtisaslaşmanın təhsil proqramında öz əksini tapır.*	72
...	**Ali təhsil müəssisəsi tərəfindən müəyyən edilən seçmə fənlər**[2] *Müvafiq fənlər hər bir ali təhsil müəssisəsi tərəfindən fərdi qaydada ixtisaslaşmadan asılı olaraq müəyyən edilir və həmin ixtisaslaşmanın təhsil proqramında əksini tapır.*	
Təcrübə		

[1] Burada "fənlər" dedikdə fənlərlə yanaşı, layihələr (eləcə də "Capstone" layihəsi), yaradıcılıq işi, laboratoriya işləri və digər aidiyyəti tədris fəaliyyətləri (olduğu təqdirdə) başa düşülür. Bu fənlər akademik heyətin təcrübəsi, tədqiqat infrastrukturu, yerli və beynəlxalq iş imkanları nəzərə alınaraq ali təhsil müəssisəsi tərəfindən müəyyən edilir və müvafiq ixtisaslaşma üzrə qəbul olan təhsilalan üçün məcburi xarakter daşıyır. Bu bölmədə minimum 4 fənn olmalıdır.

[2] Burada "fənlər" dedikdə fənlərlə yanaşı, layihələr (eləcə də "Capstone" layihəsi), yaradıcılıq işi, laboratoriya işləri və digər aidiyyəti tədris fəaliyyətləri (olduğu təqdirdə) başa düşülür. Bu fənlər akademik heyətin təcrübəsi, tədqiqat infrastrukturu, yerli və beynəlxalq iş imkanları nəzərə alınaraq ali təhsil müəssisəsi tərəfindən təklif edilir. Sözügedən fənlər müəyyən edilən zaman əmək bazarının təklifləri də nəzərə alınır və bu məqsədlə ali təhsil müəssisələri və əmək bazarı nümayəndələrindən ibarət işçi qrupunun yaradılması tövsiyə olunur. Ali təhsil müəssisəsi tərəfindən müəyyən edilən fənlər təhsilalanlar üçün seçmə xarakter daşımalı, eləcə də təhsilalanların xarici mübadilə proqramlarında iştirakına şərait yaratmalıdır. Bu bölmədə minimum 3 fənn olmalıdır.

...	**Elmi-pedaqoji təcrübə**	6
...	**Elmi tədqiqat təcrübəsi**	6
Dissertasiya işi		
...	**Magistrlik dissertasiyası**	18
CƏMİ		**120**

4. Proqramın və hər bir fənnin təlim nəticələri

4.1. Bu təhsil proqramı üzrə məzunlar təhsil və ya fəaliyyət sahəsi ilə bağlı əsas anlayışlar, nəzəri prinsip və tədqiqat metodları haqqında sistemli, ümumi təsəvvürə və geniş biliyə malik olmalı, konkret (ixtisaslaşmış) təhsil və ya fəaliyyət sahəsində dərin biliklərə yiyələnməlidirlər.

4.2. İxtisaslaşmanın təhsil proqramının hər bir fənn üzrə təlim nəticələrinin müəyyənləşdirilməsi və hər bir fənnin sillabusunun hazırlanması ali təhsil müəssisəsinin/akademik heyətin səlahiyyətindədir.

4.3. İxtisaslaşma üzrə proqramın təlim nəticələri Əlavə 1-də müəyyən olunur. Fənlər üzrə təlim nəticələri isə hər bir ali təhsil müəssisəsi tərəfindən müəyyənləşdirilir. Təlim nəticələri matrisində (Əlavə 2) fənlərlə təhsil proqramının təlim nəticələri arasındakı əlaqə əks olunmalıdır.

4.4. Təhsil proqramının cəmiyyətin və əmək bazarının dəyişən ehtiyaclarına cavab verən elmi və praktiki məzmunu təmin etməsi məqsədilə fənlərin sillabusları müntəzəm şəkildə yenilənməlidir.

5. İnfrastruktur və kadr potensialı

5.1. Təhsil proqramının tədris, təlim və qiymətləndirmə prosesi ali təhsil müəssisəsinin aşağıdakı infrastruktura malik olmasını zəruri edir:

- müasir informasiya texnologiyaları ilə (müasir kompüterlər, multimedia proyektoru, interaktiv lövhə, yüksək sürətli internet) təchiz olunmuş auditoriyalar və dərs otaqları;
- kibertəlükəsizlik və informasiya təhlükəsizliyinin digər aspektləri üzrə təlimlər üçün nəzərdə tutulmuş ixtisaslaşdırılmış laboratoriyalar.
- rəqəmsal tədris və idarəetmə vasitələri.

5.2. Ali təhsil müəssisələrinin tədrisə cəlb olunan akademik heyəti, bir qayda olaraq, elmi dərəcəyə malik olur. Elmi dərəcəsi olmayan, lakin müvafiq sahədə ən az 5 il iş təcrübəsi olan mütəxəssislər də tədrisə cəlb oluna bilərlər.

5.3. Magistrlik dissertasiyalarına elmi rəhbərlik, bir qayda olaraq, elmi ada və ya elmi dərəcəyə sahib olan şəxslər tərəfindən həyata keçirilir.

6. Karyera imkanları və ömürboyu təhsil

6.1. “İnformasiya təhlükəsizliyi” ixtisası üzrə magistr proqramını uğurla başa vuran məzunlar aşağıdakı sahələrdə və vəzifələrdə fəaliyyət göstərə bilərlər:

Məşğulluq sahələri:

- Milli təhlükəsizlik və kiberhücumlarla mübarizə mərkəzləri;

- Dövlət informasiya sistemləri və təhlükəsizlik xidmətləri;
- Hərbi və müdafiə qurumları (kiberhücumlara qarşı mübarizə üçün);
- Hüquq-mühafizə orqanları;
- Kriminalistik təhqiqat müəssisələri;
- Səhiyyə təşkilatları (xəstəxanalar, klinikalar, tibb mərkəzləri və s.);
- Maliyyə, bank, kredit, vergi, gömrük və digər hökumət təşkilatları;
- Sığorta şirkətləri;
- Telekommunikasiya və rabitə təşkilatları;
- İnternet provayderləri;
- Mobil operatorlar;
- Bulud xidməti təminatı şirkətləri;
- İnformasiya texnologiyaları sahəsində fəaliyyət göstərən şirkərlər;
- Təhlükəsizlik məhsulları və proqram təminatları istehsal edən şirkətlər;
- Kibertəhlükəsizlik və bulud təhlükəsizliyi üzrə məsləhət və xidmət təminatı təşkilatları;
- Penetrasiya testləri və şəbəkə təhlükəsizliyi auditləri aparan şirkətlər;
- Ticarət və kommersiya şirkətləri;
- Elektron ticarət və rəqəmsal xidmət platformaları;
- Universitetlər, elmi tədqiqat institutları;
- Kütləvi informasiya vasitələri (televiziya, radio, xəbər portalları).

Peşələr və vəzifələr:

- İnformasiya təhlükəsizliyi mütəxəssisi;
- Kibertəhlükəsizlik mütəxəssisi;
- Sistem təhlükəsizliyi inzibatçısı;
- Şəbəkə təhlükəsizliyi mütəxəssisi;
- Verilənlər bazası təhlükəsizliyi mütəxəssisi;
- Kibertəhlükəsizlik analitiki;
- Risk meneceri;
- Audit mütəxəssisi;
- Rəqəmsal kriminalistika və ekspertiza mütəxəssisi;
- Forensika analitiki;
- Penetrasiya testi üzrə mütəxəssis;
- Etik haker;
- DevSecOps mühəndisi;
- Universitetlərdə müəllim;
- Elmi-tədqiqat institutlarında elmi-tədqiqatçı.

6.2. Ali təhsil müəssisəsi təhsil proqramının məzunlarının məşğulluğuna dair müntəzəm sorğular keçirməli, eləcə də vakant iş yerlərinə dair məlumatları öz veb-səhifələrində yerləşdirm
6.3. əlidir.
6.4. Ali təhsil pilləsinin magistratura səviyyəsini bitirən (magistrlik dissertasiyasını müdafiə edən), yaxud təhsili ona bərabər tutulan şəxslər (tibbi təhsildə həkim-mütəxəssis) fəlsəfə doktoru proqramı üzrə doktoranturaya qəbul oluna bilərlər.
6.5. Təhsil müddətində əldə olunan bilik, bacarıq və yanaşmalar məzunların müstəqil şəkildə ömür boyu təhsil almaları üçün ilkin şərtlərdəndir.

Əlavə 1

Təhsil proqramı və tədris fəaliyyəti üzrə təlim nəticələri

Proqramın təlim nəticələri (PTN)
PTN 1. İnformasiya təhlükəsizliyi probleminin mahiyyətini, konsepsiyasını, əsas prinsiplərini, CIA modelini (konfidensiallıq, bütövlük, mövcudluq), rəqəmsal sistemlər, şəbəkələr, əməliyyat sistemləri və proqram təminatının təhlükəsizlik aspektləri, kompüter və telekommunikasiya şəbəkələrinin qorunması üsul və vasitələrini bilir.
PTN 2. Klassik və müasir kriptoqrafik üsulları (simmetrik/asimmetrik şifrələmə, rəqəmsal imza, açar mübadiləsi), kriptoqrafiyanın real sistemlərdə tətbiqi protokollarını (VPN, SSL/TLS, PKI və s.), elektron sertifikatları, rəqəmsal identifikasiya və autentifikasiya texnologiyaları (biometrik sistemlər, çoxmərhələli autentifikasiya (MFA), SSO və s.) ilə işləyir, Firewall, IDS/IPS, WAF, NAT, DMZ, VLAN və digər qoruma texnologiyalarını bilir və tətbiq edir, infrastruktur və bulud sistemlərinin təhlükəsiz arxitekturasını layihələndirməyi bacarır.
PTN 3. Təhlükəsizlik risklərinin identifikasiyası, qiymətləndirilməsi və qarşısının alınması üsulları bilir və tətbiq edir, müəssisələrdə təhlükəsizlik strategiyasını, təhlükəsizlik siyasətlərini və prosedurlarını hazırlayır və həyata keçirir, informasiya təhlükəsizliyi idarəetmə sistemlərini (ISMS) qurur.
PTN 4. Penetrasiya testləri keçirir, etik hacking texnikalarını tətbiq edir, təhlükəsizlik insidentlərinin aşkarlanması, cavablandırılması və təhlili, rəqəmsal forensika və sübutların toplanması üsul və vasitələri ilə işləyir.
PTN 5. İnformasiya təhlükəsizliyi üzrə yerli və beynəlxalq normativ hüquqi sənədləri, standart və protokollarl (ISO/IEC 27001, NIST, COBIT, GDPR və s.) bilir və fəaliyyətində rəhbər tutur, uyğunluq (compliance) və audit proseslərinin təşkil edir.
PTN 6. İnformasiya təhlükəsizliyi sahəsində, informasiya təhlükəsizliyi üsul və vasitələrinin, yeni texnologiyaların (süni intellekt, blokçeyn, post-kvant kriptoqrafiya və s.) işlənməsi, təhlükəsizlik aspektlərinin qiymətləndirilməsi istiqamətlərində elmi-tədqiqat işləri aparır, tədris və metodoloji fəaliyyət üçün elmi əsaslar hazırlayır.

Proqramın təlim nəticələri (PTN) – ixtisaslaşmalar üzrə
İnformasiya mühafizəsi və təhlükəsizliyi ixtisaslaşması üzrə:
PTN1. İnformasiya sistemlərinin və kompüter şəbəkələrinin təhlükəsizliyinin təmin olunması üçün ən son texnologiya və metodologiyalardan istifadə edir.
PTN2. Şəbəkə təhlükəsizliyi, kompüter sistem və şəbəkələrində məlumatların qorunması, təhlükəli trafiklərin analizi və qarşısının alınması texnologiyaları (firewall, VPN, IDS/IPS) ilə işləyir, Firewall, IDS/IPS, VPN, şəbəkə monitorinqi kimi texnologiyaları konfiqurasiya və idarə edir.
PTN3. Autentifikasiya, identifikasiya, gizliliyinin, bütövlüyünün və əlçatanlığının (CIA modeli) təmin olunması üsullarını, kriptoqrafik qoruma üsulları, şifrələmə alqoritmləri, elektron imza, açarların idarə edilməsi sistemlərini (PKI) reallaşdıra və tətbiq edə bilir.
PTN4. İnformasiya təhlükəsizliyinin təşkilati və texniki aspektlərini başa düşmək, informasiya təhlükəsizliyi risklərini qiymətləndirməyi və idarə etməyi bacarır.
PTN5. Müəssisə üçün təhlükəsizlik strategiyası, təhlükəsizlik siyasətini hazırlayır və tətbiq edir.
PTN6. Süni intellekt və maşın öyrənməsi texnologiyalarını informasiya təhlükəsizliyinin təmin olunmasında tətbiq etməyi, bulud xidmətləri ilə bağlı təhlükəsizlik tədbirlərini yerinə yetirməyi bilir.
Kibertəhlükəsizlik ixtisaslaşması üzrə:
PTN1. Kriptoqrafiya, autentifikasiya, identifikasiya, məlumatların gizliliyi, bütövlüyü və əlçatanlığı (CIA modeli) ilə bağlı zəruri bililklərə malik olur, kriptoqrafik qoruma üsullarını, şifrələmə

alqoritmlərini, elektron imza, açarların idarə edilməsi sistemlərini (PKI), SSL/TLS protokollarını reallaşdırır və tətbiq edir.
PTN2. Kibertəhlükəsizlik strategiyasını hazırlayır, təşkilatın təhlükəsizlik siyasətlərini formalaşdırırı və tətbiq edir.
PTN3. Risklərin təhlili, qiymətləndirilməsi, uyğun müdafiə tədbirlərinin planlaşdırılması, idarə edilməsi strategiyalarını bilir və tətbiq edir, zəif yerlərin aşkarlanması skanerləri, penetrasiya testləri və etik hakerliyi həyata keçirir, zərərli proqram təminatlarının (malware, phishing, DoS/DDoS, ransomware və s.) analizini edir və qarşısını alır.
PTN4. Kiberinsidentlərin aşkarlanması, təhlili və cavablandırılması, loq analizləri, forensik analiz və sübutların toplanması, qorunması, hüquqi prosedurlarla, SIEM (Splunk, Qradar və s.) sistemləri ilə işləyir, firewall, IDS/IPS, VPN, şəbəkə monitorinqi kimi texnologiyaları konfiqurasiya və idarə edir.
PTN5. Kiberbertəhlükəsizlik sahəsində yaranan problemlərin həllində süni intellekt və maşın öyrənməsi texnologiyalarını tətbiq edə bilir.
PTN6. ISO/IEC 27001, COBIT, NIST SP 800 seriyasından olan standartları bilir, öz fəaliyyətində rəhbər tuturvə onların tələblərinə riayət edir.
Kompüter və şəbəkə təhlükəsizliyi ixtisaslaşması üzrə:
PTN1. Əməliyyat sistemlərinin (MS Windows, Linux) təhlükəsiz idarə olunması, endpoint təhlükəsizliyi (antivirus, EDR sistemləri), proqram təminatında zəifliklərin analizi və kod səviyyəsində qorumanı (secure coding, code auditing) həyata keçirir**.**
PTN2. Kompüter sistem və şəbəkələrində məlumatların qorunması, şəbəkə təhlükəsizliyi, trafiklərin analizi və təhlükələrin qarşısının alınması texnologiyalarını (firewall, VPN, IDS/IPS) tətbiq edir.
PTN3. Sistem və şəbəkələrin zəifliklərini təhlil etmək, aşkarlamaq və bu zəifliklərə qarşı mübarizə üsul və vasitələrini tətbiq edir
PTN4. Kompüter və şəbəkə təhlükəsizliyi protokollarını, kriptoqrafik şifrələmə üsullarını, elektron imza texnologiyasını, açarların idarə olunması sistemlərini reallaşdırır və tətbiq edir.
PTN5. Təhlükəsiz şəbəkə arxitekturasını layihələndirir və qurur, virtual maşınlar və sandbox texnologiyaları ilə test aparır və analiz edir, firewall, router, switch və digər şəbəkə avadanlıqlarında təhlükəsizlik tədbirlərini, VPN texnologiyaları və təhlükəsizlik protokolları (SSL/TLS, IPSec), IDS/IPS sistemlərinin konfiqurasiya və istismar edir.
PTN6. Kompüter sistemlərində və şəbəkələrində mümkün zərərli proqramları aşkarlayır və qarşısını alır.
İnformasiya sistemlərinin təhlükəsizliyi (sahələr üzrə) ixtisaslaşması üzrə:
PTN1. Müxtəlif əməliyyat sistemlərinin (Linux, Windows, Mac OS, IOS, Android və s.) xarakterisitik funksiyalarını və iş prinsiplərini, fayl sistemlərini, xüsusi xidmət proqramlarını bilir və tətbiq edir.
PTN2. İnformasiya sistemlərinə qoyulan təhlükəsizlik tələblərini müəyyənləşdirmək, bu tələblər nəzərə alınmaqla informasiya sistemlərini layihələndirir və təhlükəsiz arxitekturasını qura bilir.
PTN3. İnformasiya sistemlərində yaranan zəifliklərı, zərərli proqram təminatlarını (malware, phishing, DoS/DDoS, ransomware və s.) aşkarlamağı, təhlil etməyi və onlara qarşı müvafiq təhlükəsizlik tədbirlərini həyata keçirməyi bacarır, kriptoqrafik qoruma üsullarını reallaşdırır, elektron imza texnologiyasını tətbiq edir.
PTN4. İT infrastrukturunda informasiya sistemlərinə yönəlmiş təhlükələrin mənbələrini proqnozlaşdırır, hücumların səbəb və təsirlərini müəyyənləşdirir, riskləri təhlil edir, qiymətləndirir, uyğun müdafiə tədbirlərini planlaşdırır, idarə edir, zəif yerlərin aşkarlanması skanerlərini, penetrasiya testlərini və etik hakerliyi həyata keçirir.
PTN5. İnformasiya sistemləri üçün təhlükəsizlik siyasətlərini hazırlayır, tətbiq edir, beynəlxalq təhlükəsizlik standartlarına uyğun idarəetmə sistemlərini qurur. .
PTN6. İnformasiya sistemlərinin şəbəkə təhlükəsizliyini təmin etməyi və hücumlardan qormağı bacarır, şəbəkə izləmə və müdafiə alətləri ilə işləyir.

Rəqəmsal kriminalistika ixtisaslaşması üzrə:
PTN1. Rəqəmsal kriminalistik üçün zəruri məlumatların qorunması üçün kriptoqrafik şifrləmə üsullarının tətbiqi, təhlükəsiz məlumat mübadiləsi üçün elektron imza, açarların idarə edilməsi sistemlərinitətbiq edir.
PTN2. Rəqəmsal kriminalistik məlumatların əldə edilməsi üçün kriptoqrafik analiz üsullarını tətbiq edir.
PTN3. Kiberhücumlar zamanı ilkin cavab tədbirlərinin həyata keçirir, zərərverici proqramların (malware analysis) davranışını analiz edir, hücum zəncirinin (kill chain) qurulması və həyata keçirilməsini təhlil edir.
PTN4. FTK, EnCase, Autopsy, Cellebrite, X-Ways Forensics kimi proqramlarla, SIEM (Splunk, Qradar və s.) sistemləri ilə işləyir, forensik analiz, loq faylların və şəbəkə trafikinin, metadata və zaman məlumatlarını analiz edir.
PTN5. Kompüterlər, mobil cihazlar, serverlər və digər rəqəmsal daşıyıcılardan sübutları toplayır və qoruyur, itmiş məlumatları, şifrələnmiş və silinmiş faylları analiz və bərpa edir, sübutlar zəncirinin qoruyur, rəqəmsal sübutları məhkəmədə qəbul edilə biləcək səviyyədə sənədləşdirir, əldə edilən sübutları hüquqi və etik əsaslara uyğun emal edir.
PTN6. Təhqiqat düşüncəsi və sübutlara əsaslanan qərar verir, cinayət hadisələrinin rəqəmsal izlərini bərpa edir və analiz edilərək məntiqi nəticələr çıxarır, məhkəmə ekspertizası üçün texniki hesabatlar yazır, etik davranış və şəxsi məlumatların qorunması prinsiplərinə riayət edir, rəqəmsal sübutların qanuni statusu, məxfi və şəxsi məlumatların qorunması qanunvericiliyini bilir, milli və beynəlxalq hüquq normalarına uyğun təhqiqat aparır, cinayət və kibercinayət kontekstində sübutları istifadə edir.
Kriptovalyuta və blokçeyn texnologiyaları ixtisaslaşması üzrə:
PTN1. Paylanmış reyestrlər (DLT), blok strukturları və konsensus alqoritmləri (Proof of Work, Proof of Stake, BFT və s.) haqqında biliyə malik olur, blokçeyn şəbəkələrinin layihələndirilməsi, növləri (public, private, consortium) və funksional modelləri ilə işləyir.
PTN2. Rəqəmsal aktivlərin iqtisadiyyatı, token modelləri, DeFi (Decentralized Finance) konseptləri, kriptovalyuta birjaları və rəqəmsal pul kisələri ilə işləyir.
PTN3. Ethereum, Hyperledger, Solana, Cardano və s. platformalarda smart müqavilələri (Solidity, Rust, Vyper dillərində) yaza bilir.
PTN4. DApp-ları (decentralized applications) layihələndirir və inkişaf etdirir, blokçeyn üzərində avtomatlaşdırılmış hüquqi və maliyyə proseslərini formalaşdırır.
PTN5. Smart müqavilələrdə zəiflikləri (reentrancy, integer overflow/underflow, access control və s.) təhlil edir, blokçeyn texnologiyalarında təhlükəsizlik risklərini təhlil edir və hücum modelləri (51% attack, Sybil attack, DAO hack və s.) ilə işləyir.
PTN6. Kriptovalyutaların və blokçeyn texnologiyalarının tənzimlənməsi üzrə beynəlxalq və lokal hüquqi normalarını bilir, AML (Anti-Money Laundering), KYC (Know Your Customer) və vergi tələblərinə uyğunluğunu nizamlayır, kriptovalyutaların və blokçeyn texnologiyalarının reallaşdırılması zamanı məlumatların məxfiliyinin qorunması üçün kriptoqrafik şifrələmə üsullarını elektron imza alqoritmlərini tətbiq edir.
İdarəetmə sistemlərinin proqram təminatının təhlükəsizliyi ixtisaslaşması üzrə:
PTN1. Sənaye və təşkilati idarəetmə sistemlərinin strukturu və funksionallığını (SCADA, PLC, HMI, RTU), onların tətbiq sahələrinin (enerji, nəqliyyat, su təchizatı, istehsalat və s.) xüsusiyyətlərini nəzərə alınmaqla müvafiq proqram təminatının təhlükəsizliyini təmin edir.
PTN2. SCADA və digər idarəetmə sistemlərinə qarşı tipik hücumları (Stuxnet tipli hücumlar, MITM, replay attacks və s.) bilir və onların qarşısını almaq üçün tədbirlər görür.
PTN3. Proqram təminatının yaradılması zamanı təhlükəsiz proqramlaşdırma prinsiplərini tətbiq edir, proqram kodlarında zəiflikləri (buffer overflow, injection, privilege escalation və s.) aşkarlayır və

aradan qaldırır, proqram kodlarını analizetmə vasitələri ilə işləyir və statik/dinamik təhlil metodlarını istifadə edir.
PTN4. İdarəetmə sistemlərinin təhlükəsizlik auditi, risklərin identifikasiyası, təhlili və idarə strategiyalarını hazırlayır, failsafe və failover mexanizmlərini qiymətləndirə bilir.
PTN5. Sistemlərin qorunması üçün firewall, router, switch və digər şəbəkə avadanlıqlarında təhlükəsizlik tədbirlərini bilir və həyata keçirir, VPN texnologiyaları və təhlükəsizlik protokollarını (SSL/TLS, IPSec), IDS/IPS sistemlərini konfiqurasiya və istismar edir, segmentləşdirmə və autentifikasiya texnologiyaları ilə işləyir.
PTN6. Sənaye təhlükəsizliyi üzrə beynəlxalq standartları (IEC 62443, NIST SP 800-82, ISO/IEC 27001) tətbiq edir, uyğunluq tələblərinə cavab verən təhlükəsizlik strategiyalarını formalaşdırır.
Tətbiqi kriptoqrafiya ixtisaslaşması üzrə:
PTN1. Klassik və müasir simmetrik və asimmetrik şifrələmə alqoritmlərini (AES, RSA, ECC, ElGamal, ChaCha20 və s.), açarların idarə edilməsi sistemlərini (PKI), açıq və gizli açarlı sistemlərin təhlükəsizliyi və istifadə sahələrini bilir, kriptoqrafik alqoritmləri proqramlaşdırır, kriptoqrafik sistemləri qurur və tətbiq edir.
PTN2. Kriptovalyuta və elektron imza texnologiyalarını, elektron imzaların və sertifikat sistemlərinin kriptoqrafik bazalarını istifadə edir.
PTN3. İnternetin təhlükəsiz protokollarını (SSL/TLS, IPsec, SSH və s.), açar mübadiləsi protokollarını (Diffie-Hellman, ECDH), autentifikasiya mexanizmlərini bilir və tətbiq edir, kriptoqrafik protokolların zəifliklərinin təhlil edir və formal sübutlarla təhlükəsizlik qiymətləndirməsi aparır.
PTN4. PKI (Public Key Infrastructure), elektron sertifikatlar və elektron imza sistemləri ilə işləyir, açarların idarə olunması, saxlanması və rotasiya siyasətlərini hazırlayır.
PTN5. Simvol analizi və statistik kriptoanaliz, yan kanal, vaxt analizi, seçilmiş ilkin mətnin və şifrmətnin analizi üsullarını, hücum modellərini, kriptoqrafik sistemlərə real hücum ssenarilərini qurur, reallaşdırır və tətbiq edir.
PTN6. Kriptoqrafiyanın istifadəsi ilə bağlı hüquqi və etik çərçivələrə riayət edir, dövlət və korporativ təhlükəsizlik tələblərinə uyğun kriptoqrafik tətbiqlər hazırlayır, yerli və beynəlxalq normativ hüquqi sənədləri və standartları bilir və fəaliyyətində rəhbər tutur.
Telekommunikasiya sistemlərinin informasiya təhlükəsizliyi ixtisaslaşması üzrə:
PTN1. Telekommunikasiya sistemlərinin (mobil şəbəkələr, IP şəbəkələr, VoIP, 5G, optik şəbəkələr və s.) arxitekturalarını və prinsiplərini bilir və tətbiq edir, şəbəkə protokollarını (TCP/IP, SIP, RTP, MPLS, BGP və s.) nəzəri və praktiki aspektlərdən bilir, şəbəkə infrastrukturunu təhlükəsizlik baxımından təhlil edir və layihələndirir.
PTN2. Telekommmunikasiya şəbəkələrində kriptoqrafik şifrləmə üsullarını tətbiq edir, səs, data və siqnalları şifrələyir, genişzolaqlı şəbəkələrdə və radio kanallarda məlumatların təhlükəsiz ötürülməsi, firewall, IDS/IPS, VPN və anti-DDoS texnologiyalarından istifadə edir.
PTN3. Telekommuinkasiya infrastrukturlarına qarşı mümkün hücumları (IMSI catching, man-in-the-middle, jamming, SS7 exploit və s.) bilir, onların aşkarlanması və qarşısının alınması üçün texnoloji və proqram təminatlarını tətbiq etdir, telekommuinkasiya sistemlərində mümkün zəiflikləri və sızmaları təhlil edir, penetrasiya testlərini həyata keçirir.
PTN4. Telekommmunikasiya sistemlərində təhlükəsizlik risklərini təhlil edir, idarəetmə strategiyalarını hazırlayır, telekommunikasiya operatorları üçün təhlükəsizlik siyasətlərini və prosedurlarını layihələndirir
PTN5. Telekommunikasiya sektorunda informasiya təhlükəsizliyi ilə bağlı yerli və beynəlxalq standartları (ISO/IEC 27011, ETSI, ITU-T, NIST və s.), abunəçi məlumatlarının qorunması, fərdi məlumatların mühafizəsi və məxfiliyin təmin olunması tələblərini bilir və fəaliyyətində rəhbər tutur.

PTN6. Telekommunikasiya sistemlərində təhlükəsizlik risklərini təhlil edir, risklərin idarə olunması strategiyalarını, telekommunikasiya infrastrukturları üçün informasiya təhlükəsizliyi siyasətlərini və prosedurlarını hazırlayır və həyata keçirir.
Sənaye idarəetmə sistemlərinin təhlükəsizliyi ixtisaslaşması üzrə:
PTN1. SCADA, DCS, PLC, RTU kimi sənaye idarəetmə sistemlərinin quruluşunu və iş prinsiplərini, sənaye proseslərinin avtomatlaşdırılması və real vaxt rejimində idarə edilməsi prinsiplərini bilir və istifadə edir.
PTN2. ICS/SCADA sistemləri üçün təhlükəsiz şəbəkə arxitekturasını qurur, dərin müdafiə (defense-in-depth) yanaşmasını, Firewall, IDS/IPS, ağ siyahı (whitelisting), VPN və zonalaşdırma prinsiplərini bilir və tətbiq edir.
PTN3. Sənaye idarəetmə sistemlərinin kibertəhlükəsizliyi tələblərini, sənaye idarəetmə sistemləri protokollarının (Modbus, DNP3, OPC-UA, IEC 60870-5-104 və s.) təhlükəsizlik prinsiplərini bilir və tətbiq edir.
PTN4. Hücum modellərini və təhlükə növlərini (stuxnet, ransomware hücumları, insider threats, MITM və s.) bilir, insidentlərin aşkarlanması və qarşısının alınması üçün müdafiə tədbirlərini və bərpa planlarını hazırlayır və tətbiq edir.
PTN5. Sənaye müəssisələrində informasiya təhlükəsizliyi risklərini qiymətləndirir, təhlükəsizlik boşluqlarını aşkarlayır və tədbirləri planlaşdırır, sənaye idarəetmə sistemləri üzrə auditləri təşkil edir və beynəlxalq standartlara uyğunluğu qiymətləndirir.
PTN6. Əsas sənaye təhlükəsizliyi standartlarını (IEC 62443, NIST SP 800-82, ISO/IEC 27019, ANSI/ISA 99), sənaye müəssisələrində tətbiq edilən təhlükəsizlik siyasətlərini bilir, öz fəaliyyətində rəhbər tutur və onların tələblərinə əməl edir.
Bulud hesablamalarının təhlükəsizliyi ixtisaslaşması üzrə:
PTN1. Bulud xidmət modellərini (IaaS, PaaS, SaaS, paylanmış sistemlər və virtuallaşdırma texnologiyalarını reallaşdıra bilir və tətbiq edir.
PTN2. Bulud xidmətlərinin qurulması üçün hibrid, ictimai (public), özəl (private) və çoxbuludlu (multi-cloud) arxitekturaları reallaşdırır.
PTN3. Bulud xidmətlərində təhlükəsizlik tələbləri ilə bağlı autentifikasiya, identifikasiya, məlumatların gizliliyi, bütövlüyü, əlçatanlığı (CIA modeli) və mövcudluğunun təmin edilməsi üsullarını, məlumatların şifrələnməsi, yüngün şifrələmə alqoritmləri, elektron imza, açarların idarə edilməsi sistemlərini (PKI) reallaşdırır və tətbiq edir.
PTN4. Bulud mühitlərində spesifik hücumları (VM escape, side-channel attacks, hypervisor attacks, data leakage və s.), təhlükəsizlik boşluqları üzrə risk analizi və qarşısının alınması strategiyalarını, insidentlərin aşkarlanması, cavab verilməsi və insident sonrası bərpa (Disaster Recovery & Business Continuity) prinsiplərini bilir və tətbiq edir.
PTN5. IAM (Identity and Access Management), MFA (Multi-Factor Authentication), SSO (Single Sign-On) texnologiyalarını tətbiq edir, SIEM, CASB, DLP, WAF, SASE və digər təhlükəsizlik həlləri ilə işləyir.
PTN6. Mövcud bulud platformalarında (AWS, Azure, Google Cloud və s.) təhlükəsizlik siyasətlərini bilir və idarə edir.
Elektron ticarət sistemlərinin təhlükəsizliyi ixtisaslaşması üzrə:
PTN1. E-ticarət platformalarının quruluşunu və işləmə mexanizmlərini, ödəniş sistemlərini (PayPal, Stripe, 3D Secure, PSD2 və s.), rəqəmsal pul kisələri və onlayn bankçılıq texnologiyalarını, E-ticarət infrastrukturunda istifadə olunan proqram və texnologiyalarını (CMS, ERP, CRM və s.) bilir və istifadə edir.
PTN2. E-ticarət sistemlərində konfidensiallıq, bütövlük, əlçatanlıq (CIA modeli), identifikasiya, autentifikasiya və icazə (OAuth2, OpenID, MFA) prosedurlarını bilir və tətbiq edir, kriptoqrafik

şifrləmə üsul və alqoritmlərini, SSL/TLS və digər təhlükəsizlik protokollarını, elektron imza və tokenləşdirmə texnologiyalarını bilir və tətbiq edir.
PTN3. Elektron ödənişlərin təhlükəsizliyi və PCI DSS (Payment Card Industry Data Security Standard) standartlarını bilir və tətbiq edir.
PTN4. Veb əsaslı hücumların aşkarlanması və qarşısının alınması (XSS, SQL injection, CSRF, session hijacking və s.), Web Application Firewall (WAF) və digər qoruma texnologiyalarını bilir və tətbiq edir.
PTN5. GDPR, KVKK və digər məlumat mühafizəsi qanunvericilik sənədlərinin tələblərinə uyğun siyasətləri hazırlayır, fərdi və ödəniş məlumatlarının şifrələnməsi və anonimləşdirilməsi üsulları ilə işləyir.
PTN6. E-ticarət layihələrində risklərin təhlili və minimuma endirilməsi, təhlükəsizlik auditi, zərərli fəaliyyətlərin monitorinqi və insidentlərin idarə olunması, penetrasiya testlərini və zəifliklərin aşkarlanması prosedurlarını həyata keçirə bilir.
Mobil tətbiqlərin təhlükəsizliyi ixtisaslaşması üzrə:
PTN1. Mobil əməliyyat sistemlərinin (Android, iOS) arxitekturasını və təhlükəsizlik modellərini, mobil tətbiqlərin yaradılması mühitlərini və proqramlaşdırma dillərini (Java/Kotlin, Swift, Dart/Flutter, React Native və s.), tətbiqlərin strukturunu və iş prinsiplərini bilir və tətbiq edir.
PTN2. OWASP Mobile Top 10 (insecure data storage, insecure communication, code tampering və s.) əsasında zəifliklərin müəyyən edilməsi, statik (SAST), dinamik (DAST) və davranış analizləri vasitəsilə tətbiq zəifliklərinin aşkarlanması, tərs mühəndislik və tətbiq kodunun qorunması üsullarını (obfuscation, anti-debugging və s.) tətbiq edir.
PTN3. Mobil tətbiqlərdə konfidensial məlumatların təhlükəsiz saxlanması (Keychain, Keystore, Secure Storage və s.), TLS/SSL protokolları ilə məlumatların şifrələnməsi və etibarlı ötürülməsi üsullarını, token əsaslı autentifikasiya sistemlərini (OAuth 2.0, JWT və s.) tətbiq edir.
PTN4. Mobil tətbiqlərdə zərərli proqramların (mobile malware) növlərini bilir, onların aşkarlanması və qarşısının alınması üsullarını tətbiq edir.
PTN5. Runtime təhlükələrə qarşı müdafiə tədbirlərini, Rooted/jailbroken cihazlarda təhlükəsizlik risklərinin qiymətləndirilməsi üsullarını, təhlükəsizlik testlərini reallaşdırır və tətbiq edir.
PTN6. Tənzimləyici normativ sənədləri və standartları (ISO/IEC 27034, GDPR, PCI-DSS və s.) bilir, mobil tətbiqlərin onların tələblərinə uyğunluğunu, mobil tətbiq mağazalarının (App Store, Google Play) təhlükəsizlik tələblərinə uyğunluğunu qiymətləndirir.
Veb texnologiyaların təhlükəsizliyi ixtisaslaşması üzrə:
PTN1. Veb proqramlaşdırma dillərini və mühitlərini (HTML, CSS, JavaScript, PHP, Python, Node.js, React, Angular, Django, Laravel və s.) bilir və həmin dillərdə proqramlaşdırır.
PTN2. Müştəri-server əsaslı tətbiqlərin qurulması və qarşılıqlı əlaqəsinin təmin edilməsini bilir, RESTful API-lər, AJAX texnologiyası tətbiq edir, mikroxidmət arxitekturasını təşkil edir, HTTPS, TLS/SSL protokolları ilə məlumatların təhlükəsiz ötürülməsi, token əsaslı autentifikasiya (OAuth 2.0, JWT (JSON Web Token), SSO və MFA), sessiyaların idarə olunması və cookie təhlükəsizliyi texnologiyalarını tətbiq edir.
PTN3. Veb texnologiya mühitində məlumatların konfidensiallığı, bütövlüyü və əlçatanlığının (CIA modeli) təmin edilməsi üsullarını, identifikasiya və autentifikasiya prosedurlarını tətbiq edir. SAST, DAST, IAST kimi təhlükəsizlik testləri metodologiyalarını, əl ilə və avtomatlaşdırılmış zəiflik aşkarlama vasitələrini (Burp Suite, OWASP ZAP, Nikto, Acunetix və s.), penetrasiya testlərini və "bug bounty" metodologiyasını tətbiq edir.
PTN4. Təhlükəsiz proqramlaşdırma prinsipləri, kodda zəifliklərin aşkarlanması və qarşısının alınması, OWASP Top 10 zəifliklərin aşkarlnaması və qorunma vasitələrini (SQL Injection, Cross-Site Scripting – XSS, Cross-Site Request Forgery – CSRF, Insecure Deserialization, Broken Authentication və s.) tətbiq edir.

PTN5. Apache, Nginx, IIS və s. serverlərin təhlükəsizlik konfiqurasiyalarını, CDN, WAF (Web Application Firewall), Reverse Proxy, DDoS qorunması texnologiyalarını, bulud əsaslı veb platformalarda təhlükəsizlik (AWS, Azure, Google Cloud) yanaşmalarını bilir və tətbiq edir.
PTN6. Veb sistemləri üçün tənzimləyici normativ sənədlərin və standartların (ISO/IEC 27001, GDPR, PCI-DSS, NIST və s.) bilir, veb sistemlərin onların tələblərinə uyğunluğunu qiymətləndirir və təmin edir.

Əlavə 2

Təhsil proqramı və tədris fəaliyyətlərinin təlim nəticələrinin matrisi

Ali təhsil müəssisəsi aşağıdakı cədvəldən istifadə edərək ixtisaslaşmanın təhsil proqramının təlim nəticələrinin əldə olunmasına necə dəstək verdiyini müəyyənləşdirməlidir.

Tədris fəaliyyətinin (fənnin) adı	Proqramın təlim nəticələri					
	PTN 1	PTN 2	PTN 3	PTN 4	PTN 5	PTN 6
Tədqiqat metodları						
Akademik yazı və etika						
Tədqiqat analitikası						
Ali təhsil müəssisəsi tərəfindən müəyyən edilən məcburi fənlər						
Ali təhsil müəssisəsi tərəfindən müəyyən edilən seçmə fənlər						
Elmi-pedaqoji təcrübə						
Elmi tədqiqat təcrübəsi						
Magistrlik dissertasiyası						

Razılaşdırıldı:

Elm və təhsil nazirinin müavini

_____İdris İsayev

Texniki və texnoloji ixtisaslar qrupu üzrə İşçi qrupunun həmsədrləri

_____dosent Yaqub Piriyev

Elm, ali və peşə təhsili şöbəsinin müdiri

_____dosent Turxan Süleyman

_____Hicran Valehov