1. ÜMUMİ QAYDALAR

1.1. Proqram haqqında ümumi məlumat

3339.01 “İnformasiyanın mühafizə üsulları və sistemləri, informasiya təhlükəsizliyi” ixtisası üzrə fəlsəfə doktoru proqramı üzrə doktoranturaya qəbul imtahanının proqramı bakalavriat və magistratura səviyyəsində “Kompüter mühəndisliyi”, “Kompüter elmləri”, “İnformasiya texnologiyaları və sistemləri mühəndisliyi” ixtisasları üzrə keçirilən “İnformasiya təhlükəsizliyinin əsasları”, “Şəbəkə təhlükəsizliyi”, “Etik hakinq metodları”, “Kriptologiya”, “İnformasiya təhlükəsizliyinin idarə edilməsi sistemləri”, “Bulud texnologiyalarının təhlükəsizliyi”, “Veb təhlükəsizlik”, “Simsiz və mobil şəbəkələrin təhlükəsizliyi”, “Verilənlər bazalarının təhlükəsizliyi” fənlərinin proqramları əsasında tərtib edilmişdir.

Proqram Azərbaycan Respublikası Nazirlər Kabinetinin "Ali təhsilin doktorantura səviyyəsi uzrə ixtisasların Təsnifatı" haqqında 15 mart 2012-ci il tarixli, 65 nömrəli qərarı əsasında təsdiq edilmiş 3339.01-“ İnformasiyanın mühafizə üsulları və sistemləri, informasiya təhlükəsizliyi (texnika sahəsi)” ixtisasının pasportuna uyğun tərtib edilmişdir.

1.2. Fəlsəfə doktoru proqramı üzrə qəbul imtahanının keçirilməsinin məqsədi

3339.01 – “İnformasiyanın mühafizə üsulları və sistemləri, informasiya təhlükəsizliyi” ixtisasından fəlsəfə doktoru proqramı üzrə qəbul imtahanı həmin ixtisas üzrə doktoranturaya qəbul olmaq istəyən iddiaçının müxtəlif tətbiq sahələrində informasiya təhlükəsizliyinin təmin edilməsi üçün həyata keçirilən tədbirlər kompleksinin bütün spektrində istifadə edilən müxtəlif təbiətli yanaşmalar, metodlar və texnologiyalar ilə əlaqədar olan bilik səviyyəsini qiymətləndirmək məqsədi ilə aparılır.

1.3. İmtahan verənin bilik səviyyəsinə qoyulan tələblər

İmtahan verən 3399.01 – “İnformasiyanın mühafizə üsulları və sistemləri, informasiya təhlükəsizliyi” ixtisasının pasportuna uyğun olaraq aşağıdakı sahələrdə elmi-tədqiqatlar aparmaq üçün lazımi biliklərə malik olmalıdır:

- İnformasiya təhlükəsizliyi təhdidlərinin proqnozlaşdırılması və onlara qarşı qabaqlayıcı tədbirlərin planlaşdırılması, informasiya təhlükəsizliyi səviyyəsinin qiymətləndirilməsi məsələləri;

- Yeni nəsil informasiya texnologiyalarında informasiya təhlükəsizliyinin təmin edilməsi texnologiyalarının yaradılması və elmi əsaslandırılması;
- Zərərli proqram təminatının analizi və aşkarlanması metodları;
- Bulud texnologiyalarının təhlükəsizliyi problemləri;
- Rəqəmsal kriminalstika problemləri;
- Tətbiqi kriptoqrafiya və kriptanaliz metodlarının işlənməsi;
- Elektron identifikasiya sistemlərinin işlənməsi və praktiki tətbiqi məsələləri.

2. PROQRAMIN MƏZMUNU

2.1. Giriş. İnformasiya təhlükəsizliyinin təşkilati və hüquqi əsasları [1, 2, 4, 5]

İnformasiya təhlükəsizliyi anlayışı. İnformasiya təhlükəsizliyinin üç aspekti. İnformasiya təhlükəsizliyi təhdidi anlayışı. Təhdidlərin əsas xarakteristikaları. Təhdidlərinin təsnifatı. Konfidensial informasiya və onun növləri. Dövlət sirri. Xidməti sirr və kommersiya sirri.

İnformasiya təhlükəsizliyinin təşkilati təminatı. İnformasiya təhlükəsizliyi siyasəti. İnformasiya təhlükəsizliyi siyasətinin əsas növləri. İnformasiya təhlükəsizliyinin təmin edilməsi sahəsində qanunvericilik. Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində qanunvericilik tədbirləri.

2.2. Kiberhücumların təşkili texnologiyaları [1, 4, 10, 11, 12]

Ziyanverici proqramlar. Kompüter virusları və şəbəkə soxulcanlarının müxtəlif sinifləri. Troyanlar və onların təsnifatı. Ziyanverici proqramların statik və dinamik analizi. Antivirus proqramlarının iş prinsipləri.

Kiberhücumların təsnifatı. Hədəfyönlü hücumlar. “Cyber kill chain” modeli. Botnetlər və onların arxitekturası. DoS hücumların növləri. TCP SYN flooding hücumu. DDoS hücum üçün üçsəviyyəli arxitektura. DDoS-hücumlardan müdafiə mexanizmləri.

2.3. İnformasiya təhlükəsizliyinin idarə edilməsi sistemləri [1, 2, 4, 10, 11]

İnformasiya təhlükəsizliyi üzrə standartlar. ISO/IEC 27001 standartı. PDCA dövrü.

İnformasiya təhlükəsizliyi risklərinin idarə edilməsi. Risklərin kəmiyyət və keyfiyyət qiymətləndirilməsi. Risklərin emalına yanaşmalar.

İnformasiya təhlükəsizliyi insidentlərinin idarə edilməsi. İnsidentlərin emalı prosesinin mərhələləri. CERT-komandaları və onların funksiyaları.

İnformasiya təhlükəsizliyinin auditi və onun mərhələləri. Standarta uyğunluğun auditi. Nüfuzetmə testlərinin ümumi metodologiyası.

2.4. Proqram təminatının təhlükəsizliyi [1, 2, 4, 5, 10, 11, 12]

Əməliyyat sistemlərinin (ƏS-nin) ümumi xarakteristikaları. ƏS-nin nüvəsinin funksiyaları. ƏS-nin təsnifatı. Şəbəkə əməliyyat sistemləri. Əməliyyat sistemlərində informasiya təhlükəsizliyinin əsas mexanizmləri.

Müasir proqramlaşdırma texnologiyaları. Obyektyönlü proqramlaşdırmanın əsas konsepsiyaları. Proqram təminatının təhlükəsizliyi. Boşluqların idarə edilməsinin həyat dövrü. Boşluqların qiymətləndirilməsinə yanaşamlar (CVSS metodikası).

Veb təhlükəsizlik təhdidləri (OWASP 2021 üzrə). SQL inyeksiyanın növləri. SQL inyeksiya alətləri və əks-tədbirlər.

Paylanmış sistemlərdə informasiya təhlükəsizliyi funksiyaları. İdentifikasiya və autentifikasiya. Girişə nəzarət. Girişə nəzarət siyahıları. Rollar əsasında girişə nəzarət.

2.5. Kompüter şəbəkələrinin təhlükəsizliyi [1, 2, 5, 9, 12, 13]

Kompüter şəbəkələri. Şəbəkə topologiyaları. Şəbəkələrin növləri. Lokal və qlobal şəbəkələr, onların proqram təminatı. Ethernet texnologiyası.

OSI modeli. OSI modelinin səviyyələri. TCP/IP protokollar steki. TCP və UDP protokolları. IP-protokolu. IP-protokolunun ünvan sxemi. DNS xidməti.

Şəbəkələrarası ekranların funksiyaları və iş prinsipləri. Şəbəkələrarası ekranların təsnifatı. Şəbəkə təhlükəsizliyinin kriptoqrafik protokolları. IPSec protokolu. SSL protokolu. Virtual xüsusi şəbəkələr.

Müdaxilələrin aşkarlanmasına yanaşmalar. Müdaxilələrin aşkarlanması sisteminin komponentləri. Müdaxilələrin aşkarlanmasının host və şəbəkə sistemləri. Honeypot sistemləri.

2.6. Kriptoqrafiya metodları [3, 13]

Kriptoqrafiyanın əsas anlayışları. Klassik şifrlər: sadə əvəzetmə və yerdəyişmə şifrləri. Vijener şifri. Vernam şifri. Simmetrik blok şifrləri. Şifrlərin qurulması üçün Şennon prinsipləri. Feystel şəbəkəsi.

DES (Data Encryption Standard) standartı. AES (Advanced Encryption Standard) şifrləmə standartı: AES-in riyazi əsasları və Qalua meydanları. AES alqoritminin strukturu. Blok şifrlərin iş rejimləri: ECB, CBC, CFB, OFB və CTR.

Açıq açarlı kriptoqrafiyanın əsas anlayışları. RSA kriptosistemi: açarların generasiyası, şifrləmə və deşifrləmə alqoritmləri. Diskret loqarifm məsələsi və ona əsaslanan kriptosistemlər. Diffi-Hellman açar mübadiləsi sxemi.

Rəqəmsal imza sxemi və onun növləri. ElGamal imza sxemində imzalama və imzanı yoxlama alqoritmləri.

Kriptoqrafik heş funksiyaların tərifi, xassələri və qurulmasının əsas prinsipləri. “Ad günü” hücumu. SHA-1 heş funksiyası. Məlumatı autentifikasiya kodları. Açarlı heş funksiyalar (HMAC).

Elektron imzanın tərifi və funksiyaları. Açıq açarlar infrastrukturunun komponentləri. Açıq açarlar infrastrukturunun modelləri.

2.7. İnformasiya təhlükəsizliyi metodlarında istifadə edilən riyazi aparat [3, 6, 7, 8]

İnformasiya anlayışı. İnformasiyanın miqdarı. Entropiya. Şərti entropiya. Qarşılıqlı informasiya və onun xassələri.

Qraflar nəzəriyyəsinin elementləri: qrafın tərifi, qrafların növləri. Qrafın əlaqəlilik və insidentlik matrisləri. Qraflar üzərində optimallaşdırma məsələləri. Deykstra alqoritmi.

Matrislər üzərində əməllər. Minor və cəbri tamamlayıcı anlayışı. Determinant və onun xassələri. Tərs matrisin və onun varlığı. Matrisin məxsusi ədədi və vektoru anlayışları.

Ehtimalın klassik tərifi. Ehtimal fəzası. Şərti ehtimal. Ehtimalların vurulması teoremi. Ehtimalların toplanması teoremi. Bayes düsturu.

Təsadüfi kəmiyyətlər və onların xarakteristikaları: paylanma funksiyası, momentlər. Bəzi paylanma qanunları (binomial, Puasson, üstlü, müntəzəm). Normal paylanma.

Riyazi statistikanın əsas məsələləri. Variasiya sırası və onun statistik parametrləri (ədədi orta və dispersiya). Paylanma parametrlərinin statistik qiymətləndirilməsi. Nöqtəvi qiymətləndirmə. İnam intervalının qurulması. Statistik hipotezlərin yoxlanması. Pirson kriteriyası. Korrelyasiya analzinin əsas elementləri. Reqressiya analizi. Ən kiçik kvadratlar üsulu.

Riyazi proqramlaşdırma məsələsinin komponentləriı. Riyazi proqramlaşdırma məsələlərinin təsnifatı. Xətti proqramlaşdırma (XP) məsələsinin qoyuluşu və yazılış formaları. XP məsələsinin həndəsi mənası. XP haqqında teoremlər. XP-nin düz və qoşma məsələləri.

ƏDƏBİYYAT

1. Qasımov V.Ə. İnformasiya təhlükəsizliyinin əsasları. Dərslik. Bakı. MTN-in nəşriyyat-poliqrafiya mərkəzi. 2009, 340 s.
2. Qasımov V.Ə. İnformasiyanın qorunmasının müasir texnologiyaları. Dərslik. MTN-in Heydər Əliyev adına Akademiyasının nəşriyyatı. 2011. 112 s.
3. Əliquliyev R.M., İmamverdiyev Y.N. Kriptoqrafiyanın əsasları. Bakı: İnformasiya texnologiyaları, 2006, 698 s.
4. Əliquliyev R.M., İmamverdiyev Y.N. İnformasiya təhlükəsizliyi insidentləri. Bakı, İnformasiya texnologiyaları, 2012, 212 s.
5. Məmmədov F.H., Cəfərov Z.Ə. İnformasiya mühafizəsi üsullari və vasitələri. Dərslik. Bakı: AzTU, 2010.
6. Kərimov S., Sərdarov Y. Kompyuter elminin nəzəri əsasları, Bakı, 2009, 290 s.
7. Hüseynov Ə.Ə. Diskret riyaziyyat. Dərs vəsaiti. Bakı: Çaşıoğlu, 2010. – 408 s.
8. Əliyev F.N., Mikayılov C.İ., Əliyev Y.N. Statistika. Dərslik. Bakı, 2015, 240 s.
9. Таненбаум Э.С. Компьютерные сети. 4-е изд. 2004, СПб, Издательский дом "Питер", 992 с.
10. Weidman G. Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press, 2014, 528 p.
11. Hoffman A. Web Application Security: Exploitation and Countermeasures for Modern Web Applications. O'Reilly Media, 2020, 330 p.
12. Diogenes Y., Ozkaya E. Cybersecurity – Attack and Defense Strategies. Packt Publishing, 2019, 634 p.
13. Stallings W. Cryptography and Network Security: Principles and Practice (6th Edition). Wiley, 2013, 752 p.