AZƏRBAYCAN RESPUBLIKASI TƏHSIL NAZIRLIYI
BAKI DÖVLƏT UNIVERSITETI

Tətbiqi riyaziyyat və kibernetika fakültəsi
İnformasiya texnologiyaları və proqramlaşdırma kafedrası

060509- Kompüter elmləri ixtisasının
Kompüter elmləri və texnologiyaları ixtisaslaşması üzrə
Kibertəhlükəsizliyə giriş fənninin

P R O Q R A M I

Bakı Dövlət Universitetinin
Tətbiqi riyaziyyat və kibernetika fakültəsinin
Elmi Şurasının 07.02.2022-ci il tarixli (protokol №3) iclasının
qərarı ilə təsdiq edilmişdir

Tərtib edənlər:

Azərbaycan Texniki Universitetinin İnformasiya və telekommunikasiya texnologiyaları fakültəsinin "Mühəndis riyaziyyatı və süni intellekt" kafedrasının dosenti, t.e.n. **Y.N.İmamverdiyev**

Elmi redaktor:

Bakı Dövlət Universitetinun Tətbiqi riyaziyyat və kibernetika fakültəsinin "İnformasiya texnologiyaları və proqramlaşdırma" kafedrasının müdiri, t.e.d., prof. **Ə.Ə.Əliyev**

Rəyçilər:

Azərbaycan Memarlıq və İnşaat Universitetinin "İnformasiya texnologiyaları və sistemləri" kafedrasının professoru, t.e.d. **N.F.Musayeva**

Bakı Dövlət Universitetinun Tətbiqi riyaziyyat və kibernetika fakültəsinin "İnformasiya texnologiyaları və proqramlaşdırma" kafedrasının dosenti, f.r.e.n. **R.Ə.Mahmudzadə**

Giriş

Kibertəhlükəsizliyin təmin edilməsi müasir şəbəkələşmiş qlobal informasiya cəmiyyətində əsas həyati məsələlərdən biridir. Bu İnternet üzərindən həyata keçirilən elektron xidmətlərin hər bir istifadəçisindən həm şəxsi, həm də təşkilati kibertəhlükəsizliyin təmin edilməsi üçün adekvat bilik, bacarıq və vərdişlər tələb edir. Kibertəhlükəsizlik üzrə ixtisaslaşan mütəxəssislərə bütün dünyada böyük ethiyac vardır və belə mütəxəssislərin hazırlanması sahəsində universitetlərin üzərinə mühüm vəzifələr düşür. Eyni zamanda, ixtisasından asılı olmadan bütün tələbələrə kibertəhlükəsizliyin təmin edilməsinin aktuallığı aşılanmalı və onlara bu istiqamətdə zəruri biliklər verilməli, bacarıq və vərdişlər formalaşdırılmalıdır. Kibertəhlükəsizliyin təmin edilməsi hazırda kompleks məsələlərin həll edilməsini tələb edir. Kibertəhlükəsizlik mühiti olduqca sürətlə inkişaf edir, daha təkmil kiberhücum strategiyaları və alətləri meydana çıxır. Təəssüf ki, informasiya texnologiyaları yaradılarkən kibertəhlükəsizlik tələbləri prioritet olmur və istifadəçilərə çoxsaylı boşluqları olan vasitələr təqdim olunur. Mürəkkəb proqram vasitələrində bu boşluqların aşkarlanması və aradan qaldırılması daha da çətinləşir. Təcrübə göstərir ki, kibertəhlükəsizliyin müəyyən qənaətbəxş səviyyədə təmin edilməsinə çox vaxt elementar təhlükəsizlik tədbirlərinin həyata keçirilməsi vasitəsilə nail olmaq mümkündür. İstifadəçilər ya bu tədbirlər barədə məlumatlı olmurlar, yaxud bu tədbirləri həyata keçirmək üçün əlavə vaxt və səy göstərmirlər. Eləcə də, sistemlərin layihələndirilməsi, yaradılması, inteqrasiyası və istismarı zamanı müəyyən səbəblərdən çoxsaylı boşluqlar buraxılır və bu boşluqların artıq çoxdan təşkilatlanmış haker icmaları və kiberqoşunlar tərəfindən aşkarlanması və istismar edilməsi çətin deyil.

"Kibertəhlükəsizliyə giriş" fənninin əsas məqsəd tələbələri "kibertəhlükəsizliyin baza anlayışları, geniş yayılmış kibertəhdidlər və onlardan müdafiə texnologiyaları ilə tanış etmək, kibertəhlükəsizliyin təmin edilməsinin təşkili və əsas məsələlərin həlli üzrə praktiki vərdişlər verməkdir.

"Kibertəhlükəsizliyə giriş" fənni "Kompüter şəbəkələri", "İnformatika" , "Diskret riyaziyyat" fənləri ilə əlaqəyə malikdir.

Fənnin mənimsənilməsi nəticəsində magistrantlar **bilməlidir:**

- müasit kibermühitdə geniş yayılmış risklərin, kibertəhdidlərin, boşluqların və kiberhücumların təsnifatını;
- etik hakinq üçün istifadə edilən açıq kodlu proqram alətlərini;
- kiberhücumların proses modelini və əsas mərhələlərin həyata keçirilməsi mexanizmlərini;
- tipik kiberhücumlardan müdafiə tədbirlərini və vasitələrini;
- sızma testlərinin aparılması metodikasının ümumi sxemini;
- veb sistemlərə kiberhücumların əsas siniflərini;
- kibertəhlükəsizliyin təmin edilməsi sisteminin funksiyalarını;
- açıq açarlı kriptoqrafiya alqoritmlərini;
- açıq açarlar infrastrukturunun iş prinsiplərini;
- kibertəhlükəsizliyi təmin etmək üçün şəbəkə davranışının əsas qaydalarını.

Bacarmalıdırlar:

- kibertəhdidləri identifikasiya etməyi;
- zərərli proqram təminatının və hücumların müxtəlif tiplərini təsvir etməyi;
- kibertəhlükəsizlik vasitələrini sadə şəkildə kökləməyi;
- kiberhücumlarla mübarizə üçün müdafiə strategiyasını formalaşdırmağı;
- açıq kodlu proqram vasitələrindən istifadə etməklə obyekt və sistemlərin kibertəhlükəsizliyinin analizini aparmağı.

Yiyələnməlidir:

- kibertəhlükəsizlik üzrə elmi-texniki materialları seçmək, öyrənmək və ümumiləşdirmək qabiliyyətinə;
- kibertəhlükəsizliyin təmin edilməsi üzrə baza tədbirlər kompleksini formalaşdırmaq bacarığına;
- kibertəhlükəsizlik sisteminin qiymətləndirilməsini aparmaq və təkmilləşdirilməsi üzrə təklifləri işləmək bacarığına.

Mövzuların saatlar üzrə paylanması

№	Mövzular	Auditoriya saatlarının miqdarı	
		Müh. 30 saat	**Məş. 30 saat**
1	Kibertəhlükəsizliyin əsas anlayışları	2	2
2	Kiberhücumların proses modeli. Etik hakinqə giriş	2	2
3	İnformasiyanın toplanması və inventarlaşdırma	2	2
4	Boşluqların analizi. Sistemin hakinqi	2	2
5	Zərərli proqram təminatı təhdidləri	2	2
6	DDoS-hücumları və müdafiə üsulları	2	2
7	Veb tətbiqlərin təhlükəsizliyi. SQL inyeksiyası hücumu	2	2
8	Kibertəhlükəsizliyin auditi. Sızma testləri		
9	Müdaxilələrin aşkarlanması sistemləri	2	2
10	Kibertəhlükəsizlik insidentlərinin idarə edilməsi	2	2
11	İnformasiya təhlükəsizliyi standartları	2	2
12	Açıq açarlı kriptoqrafiya. RSA alqoritmi	2	2
13	Kriptoqrafik heş funksiyalar	2	2
14	Rəqəmsal imza sxemləri	2	2
15	Elektron imza. Açıq açarlar infrastrukturu	2	2

060509-**Kompüter elmləri ixtisası üzrə Kibertəhlükəsizliyə giriş** adlı proqram tətbiqi riyaziyyat və kibernetika fakültəsinin "kompüter elmləri və texnologiyaları" ixtisaslaşması üçün nəzərdə tutulmuşdur (30 saat mühazirə, 30 saat məşğələ).

Mövzu 1. Kibertəhlükəsizliyin əsas anlayışları

Kibertəhlükəsizlik, təhdid və hücum anlayışlarına tərif verilir. Konfidensial informasiyanın təsnifatına baxılır. Kiber-təhlükəsizliyinin təmin edilməsi üçün əsas kibertəhlükəsizlik funksiyaları və onların iş prinsipləri izah olunur. [4], [5], [10].

Mövzu 2. Kiberhücumların proses modeli. Etik hakinqə giriş.

Kiberhücumların "Cyber kill chain" proses modeli və onun əsas komponentləri izah edilir. Şəbəkə kəşfiyyatı, kibersilahın hədəf sistemə çatdırılması, quraşdırılması və istismarı mərhələləri təhlil olunur. Etik hakinq anlayışı və Kali Linux barədə məlumat verilir. [4], [5], [6].

Mövzu 3. İnformasiyanın toplanması və inventarlaşdırma.

Kiberhücumun hədəfi olacaq kompüter şəbəkəsi barədə müxtəlif mənbələrdən informasiyanın toplanması metodları və alətləri diqqətə çatdırılır. Şəbəkə obyektlərinin inventarlaşdırılması konsepsiyası və üsulları barədə məlumat verilir. [6],[7],[8].

Mövzu 4. Boşluqların analizi. Sistemin hakinqi.

Boşluqların idarə edilməsinin həyat dövrü, boşluqların qiymətləndirilməsinə və skorinqinə yanaşamlar analiz edilir. Sistemin hakinq edilməsi metodologiyası, keyloqqerlər, casus proqram təminatı, izlərin gizlədilməsi alətləri izah edilir. [6],[7],[8].

Mövzu 5. Zərərli proqram təminatı təhdidləri.

Kompüter virusları və şəbəkə soxulcanlarının müxtəlif siniflərinə baxılır. İnformasiya sistemində icazəsiz hərəkətlərin həyata keçirilməsində əsas vasitə olan troyanlar analiz olunur. Zərərli proqramların digər növləri haqqında da məlumat verilir. [3], [4] ,[5], [10].

Mövzu 6. DDoS-hücumları və müdafiə üsulları.

Botnetlər və onların arxitekturası, DDoS-hücumların sinifləri, DDoS-hücum alətləri, DDoS-hücumlardan müdafiə mexanizmləri öyrənilir. [4], [5] ,[10].

Mövzu 7. Veb tətbiqlərin təhlükəsizliyi. SQL inyeksiyası hücumu

OWASP (Open Web Application Security Project) yanaşmasına əsasən veb sistemlərə hücumların əsas sinifləri izah edilir. SQL inyeksiyanın növləri, SQL inyeksiyanın metodologiyası, SQL inyeksiya alətləri və əks-tədbirlər müzakirə olunur. [8], [9]

Mövzu 8. Kibertəhlükəsizliyin auditi. Sızma testləri.

Kibertəhlükəsizlik auditinin növləri və mərhələləri, auditora qoyulan tələblər, ISO/IEC 27001:2013 standartına uyğunluğun auditi və sızma testlərinin metodikası müzakirə edilir. [3], [6], [7], [8].

Mövzu 9. Müdaxilələrin aşkarlanması sistemləri.

Müdaxilələrin aşkarlanması sistemlərinin ümumi modeli, təsnifatı, anomaliyaların aşkarlanması üsulları öyrədilir, müxtəlif sistemlər haqqında qısa məlumat verilir. [4], [9] ,[10]

Mövzu 10. Kibertəhlükəsizlik insidentlərinin idarə edilməsi.

İnsident anlayışına baxılır, CERT-komandaları və onların əsas xidmətləri haqqında məlumat verilir. İnsidentlərin emalı prosesinin mərhələləri analiz edilir. [3], [4], [5]

Mövzu 11. İnformasiya təhlükəsizliyi standartları.

İnformasiya təhlükəsizliyi sahəsində standartların tarixi, ISO/IEC 15408, ISO/IEC 27001:2013 və ISO/IEC 27005:2018 standartları haqqında məlumat verilir. [3], [4], [5], [10].

Mövzu 12. Açıq açarlı kriptoqrafiya. RSA alqoritmi.

Açıq açarlı kriptoqrafiyanın əsas prinsipləri izah olunur, RSA kriptosisteminin izahı üçün zəruri riyazi faktlar diqqətə çatdırılır və

RSA kriptosisteminin şifrləmə və deşifrləmə alqoritmləri verilir. [1], [2], [3], [4].

Mövzu 13. Kriptoqrafik heş funksiyalar.

Tamlığa nəzarət mexanizmi kimi heş funksiyaların tərifi, xassələri və qurulmasının əsas prinsipləri verilir. SHA-1 alqoritmi izah edilir, SHA-2 və SHA-3 alqoritmləri qısa izah edilir. [1], [2], [3], [4].

Mövzu 14. Rəqəmsal imza sxemləri.

Rəqəmsal imzanın ümumi sxemi izah edilir, ElGamal və Şnorr rəqəmsal imza sxemləri öyrədilir. [1], [2], [3], [4].

Mövzu 15. Elektron imza. Açıq açarlar infrastrukturu.

Elektron imzanın tərifi verilir və imzanın funksiyaları təhlil olunur. Elektron imzanın praktikada tətbiqi üçün qurulan açıq açarlar infrastrukturunun komponentləri təhlil olunur. [1], [2], [3], [4].

Əsas ədəbiyyat

1. R.M. Əliquliyev, Y.N. İmamverdiyev. Rəqəm imzası texnologiyası. Bakı, Elm, 2003, 132 s.
2. R.M. Əliquliyev, Y.N. İmamverdiyev. Kriptoqrafiyanın əsasları. Bakı, İnformasiya texnologiyaları, 2006, 700 s.
3. R.M. Əliquliyev, Y.N. İmamverdiyev. İnformasiya təhlükəsizliyi insidentləri. Bakı, İnformasiya texnologiyaları, 2012, 212 s.
4. V.Ə. Qasımov. İnformasiya təhlükəsizliyinin əsasları. Dərslik. Bakı, 2009, - 340 s.
5. C.J. Brooks, C. Grow, P.A. Craig Jr., D. Short. Cybersecurity Essentials. Wiley, 2018, 784 p.
6. R. Baloch. Ethical Hacking and Penetration Testing Guide. Auerbach Publications, 2014, 531 p.
7. G. Khawaja. Kali Linux Penetration Testing Bible. Wiley, 2021, 512 p.

8. G. Weidman. Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press, 2014, 528 p.
9. A. Hoffman. Web Application Security: Exploitation and Countermeasures for Modern Web Applications. O'Reilly Media, 2020, 330 p.
10. Y. Diogenes, E. Ozkaya. Cybersecurity – Attack and Defense Strategies. Packt Publishing, 2019, 634 p.

Əlavə ədəbiyyat

1. E. Ozkaya. Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity. Packt Publishing, 2019, 356 p.
2. W. Stallings. Cryptography and Network Security: Principles and Practice (6th Edition). Wiley, 2013, 752 p.