**AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ**

**AZƏRBAYCAN DÖVLƏT NEFT VƏ SƏNAYE UNİVERSİTETİ**

“İnformasiya texnologiyaları və idarəetmə” fakültəsi

**050616-“İnformasiya texnologiyaları” ixtisası** üzrə

**BAKALAVR HAZIRLIĞI ÜÇÜN**

**“İnformasiya təhlükəsizliyi” fənninin**

**S İ L L A B U S U**

|  |  |
| --- | --- |
| Fənnin kodu | İPF-B15 |
| Kreditlərin sayı | 6 |
| Kurs | 3 |
| Semestr | 5 |
| Tədrisə ayrılan ümumi saatlar | 60 |
| o cümlədən: |  |
| Mühazirə | 30 |
| Məşgələ (seminar) | 30 |
| Laboratoriya | - |
| Kurs işi | - |

5-ci semestrdə imtahan nəzərdə tutulmuşdur. “İnformasiya texnologiyaları” ixtisasının tədris planına uyğun tərtib olunmuşdur.

Sillabus “Kompüter mühəndisliyi” kafedrasının iclasında (prot.№1, 09.09. 2022-ci il) müzakirə olunmuşdur.

Silabusu tərtib edən M.M. Həsənquliyeva

İTİF-in dekanı, dosent F.H. Ağayev

Kafedra müdiri, dosent N.Ə. Rəhimova

**ADNSU – 2022**

**I. Fənnin təsviri**

“İnformasiya təhlükəsizliyi” fənninin məqsədi qloballaşan müasir dünyamızda İnformasiya təhlükəsizliyinin, terminalogiyalarını, obyektləri, məqsədləri və əsas istiqamətləri haqqında müvafiq bilik və bacarığın formalaşdırılmasıdır.

**II. Fənnin hədəfi və məqsədi**

Bu fənnin əsas məqsədi - İnformasiyanın dəyərinin qorunub saxlanması üçün,

* konfidensiallığın pozulmasına yönələn təhdidlər;
* əlyetənliyin pozulmasına yönələn təhdidlər;
* tamlığın pozulmasına yönələn təhdidlərin qarşısının alınmasının ən müasir üsul və vasitələrini tələbələrə aşılamaq və müasir tələblərə cavab verməyə qadir mütəxəsisslər yetişdirməkdən ibarətdir.

**III. Fənnin qısa məzmunu**

Fənnin tədrisinə aşağıdakı mövzular daxildur:

1. İnformasiya təhlükəsizliyinin problemləri;

2. İnformasiya təhlükəsizliyi sahəsinin müasir vəziyyəti;

3. İnformasiya və informasiya sahələri;

4. İnformasiya təhlükəsizliyinin obyektləri;

5. Informasiya təhlükəsizliyinin əsaslar;

6.. Şəbəkə üzrə informasiya təhlükəsizliyi obyekti və elemenləri

7. İnformasiya təhlükəsizliyinin terminoloji əsasları;

8. İnformasiya təhlükəsizliyinin üsul və vasitələr.

9. Kompüter kriptoqrafiyası;

10.Simmetrik kriptosistemlər

11. Asimmetrik kriptosistemlər

12. Elektron imza texnologiyası

13. Steqanoqrafik mühafizə vasitələri

14. Kompüter sistemlərinin arxitekturu;

15. İnformasiya mühafizəsi

16. Zərərli proqramlar və mühafizə vasitələri;

17. İnformasiya təhlükəsizliyi konsepsiyası;

**IV. Fənnin tədrisinin növləri və müddəti**

050616 - “İnformasiya texnologiyaları” ixtisası üzrə “İnformasiya təhlükəsizliyi” fənninin tədrisində mühazirə və məşğələ dərslərinin aparılması nəzərdə tutulur.

İxtisas üzrə tədris planında nəzərdə tutulmuş dərs növləri və saatları cədvəl 1-də mövzular üzrə ayrılan saatlar cədvəl 2-də, mühazirə və məşğələ dərslərinin məzmunu isə cədvəl 3 və 4-də göstərilmişdir.

**V. Tələbənin təqdimatı yerinə yetirilmə müddəti, məsləhət saatları**

Fənnin tələbələr tərəfindən semestr ərzində ardıcıl mənimsənilməsi üçün 1 təqdimatın yerinə yetirilməsi nəzərdə tutulur. Təqdimatın mövzusu passiv sillabus əsasında müəllim tərəfindən verilir. Tələbələr təqdimatı sərbəst yerinə yetirirlər.

Yerinə yetirilmiş təqdimat 0 - 10 balla qiymətləndirilir.

**VI. Müəllim haqqında məlumat**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Müəllimin  s.a.a. | Elmi adı, dərəcəsi | Müharizə otağı | Tələbələrə audi- toriyadan kənar məsləhət vaxtları | Məsləhət üçün otaq |
| Həsənquliyeva Mətanət Məhəmməd qızı | Texnika üzrə fəlsəfə doktoru |  | 1200-1600 | 1430 |

**VII. Müəllimin tələbləri**

Müəllimin tələblərinə aşağıdakı meyarlar daxildir:

1) tələbələrin dərslərdə müntəzəm iştirak etmələri;

2) mühazirə və laboratoriya dərslərində keçilmiş materialları müntəzəm öyrənmələri;

3) təklif olunan ədəbiyyatlarla sərbəst işləmələri;

4) dərslərdə aktiv iştirak etmələri, aydın olmayan məsələlərlə bağlı müəllimə suallar vermələri;

5) fənnin tədrisinə ayrılmış ümumi saatın 50%-ni auditoriyadan kənar sərbəst, 50% -ni isə müəllimlə birgə işləmələri;

# 6) semestr ərzində hər dərsdə cari biliyin yoxlanılmasının aparılması və nəticəsinin qrup jurnalında qeyd olunması;

# 7) sərbəst tapşırıqları vaxtında tələb olunan səviyyədə hazırlamaları;

# 8) fənnin dərindən mənimsənilməsi ilə bağlı müəllimə qarşı tələbkarlıq göstərmələri;

# 9) semestr ərzində fənnin mənimsənilməsi ilə bağlı nəzərdə tutulmuş maksimum 50 balın qazanılması üçün ciddi cəhd göstərmələri.

**VIII. Cari biliyin qiymətləndirmə meyarları, aralıq qiymətləndirmə cədvəli**

Tələbələr tərəfindən fənnin mənimsənilməsi səviyyəsini müəyyən etmək məqsədilə mühazirə və laboratoriya dərslərində cari biliyin qiymətləndirilməsi aparılır. Bunlardan əlavə semestr ərzində 1 dəfə 6 həftəlik material əsasında 7-ci və ya 8-ci həftədə aralıq imtahan keçirilir. Aparılan aralıq imtahanın nəticəsi qrup jurnalında 0 – 20 balla qeyd olunur.

Biliyin qiymətləndirilməsi çoxballı sistem əsasında aparılır. Fənn üzrə tələbələrin topladığı maksimum balın həddi 100-dür. Bunun 50 balı imtahanda, 50 balı isə semestr müddətində qazanılır.

Semestr ərzində toplanılacaq maksimum 50 balın tədris göstəriciləri üzrə paylanması “ADNSU Elmi Şurasının 22 sentyabr 2021-ci il tarixli iclasında qəbul olunmuş “Fənn üzrə imtahanqabağı balların komponentlərinə görə yeni qiymətləndirmə meyarları”na əsasən aparılır. Başqa sözlə imtahanqabağı bal aşağıdakı kimi formalaşır:

- Təqdimata görə - 20 bal;

- Aralıq imtahana görə - 20 bal;

- Semestr ərzində tələbənin aktivliyinə görə - 10 bal (semestrin sonuncu həftəsində müəllim tərəfindən yazılır).

**IX. İstifadə olunan ədəbiyyatlar**

1. Musayev V.H, Qənbərov M.M. Qənbərova G.T. və b. «İnformasiya təhlükəsizliyi və kompüter şəbəkələri», Bakı, 2015.

2. Informasiya təhlükəsizliyi – dərslik, Bakı – 2016. Əlizadə Mətləb Nuruş oğlu, Bayramov Hafiz Məhərrəm oğlu, Məmmədov Əlövsət Suliddin oğlu

3. Васильков А.В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков.— Москва : ФОРУМ: ИНФРА-М, 2013.— 368 с

4. Куликов С. С. Модели безопасности компьютерных систем. Учебное пособие для вузов. Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2015.- 179с. 2. «Модернизация и ремонт ПК», Скотт Мюллер

5. Е.В. Вострецова. Основы информационной безопасности - Екатеринбург Издательство Уральского университета 2019

# 6. Jeremy Martin, Richard Medlin, Nitin Sharma, James Ma, Dominic Martin, Amy Martin - Threat Hunting, Hacking, and Intrusion Detection - (SCADA, Dark Web, and APTs): Cyber Secrets 1, 2020 – 137 p

Cədvəl 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| İxtisaslar üzrə nəzərdə tutulmuş saatlar | | | | | |
| **050616-“İnformasiya texnologiyaları”** | | | | | |
| Cəmi | Müh. | Məş. | Lab. | Kredit | Sem. |
| 60 | 30 | 30 | - | 6 | 5 |

Cədvəl 2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Fənn proq  ramı  möv-  zularının nömrələri | Mövzular | Fənnin tədrisinə  ayrılan saatların  sayı | | |
| cəmi | müh | məş |
| 1. | Giriş. İnformasiya təhlükəsizliyi haqqında məlumat İnformasiya və informasiya sahələri. | 4 | 2 | 2 |
| 2 | İnformasiya təhlükəsizliyinin problemi və onu xarakterizə edən amillər. | 4 | 2 | 2 |
| 3. | İnformasiya təhlükəsizliyi sahəsinin müasir vəziyyəti. | 4 | 2 | 2 |
| 4. | İnformasıya təhlükəsizliyi obyektlərı. Kompyüter sistemlərinin arxitekturu. | 4 | 2 | 2 |
| 5. | İnformasiya mühafizəsi üçün aparat – proqram metodları. İnformasiya mühafizəsi üçün proqram sistemləri. | 4 | 2 | 2 |
| 6. | Şəbəkə üzrə informasiya təhlükəsizliyi obyekti və elemenləri. Kompüter sistemlərində və şəbəkələrində informasiyanın sızması yolları. | 4 | 2 | 2 |
| 7. | İnformasiya təhlükəsizliyinin terminoloji əsasları. | 4 | 2 | 2 |
| 8. | İnformasiya təhlükəsizliyinin üsul və vasitələri. İnformasiya təhlükəsizliyinə olan təhdidlərin təsnifatı. Təhlükələr və onların pozulmasının nəticələri | 4 | 2 | 2 |
| 9. | Kompüter kriptoqrafiyası. Kriptoqrafiyanin əsas anlayışları. Simmetrik kriptosistemlər. Asimmetrik kriptosistemlər. | 4 | 2 | 2 |
| 10. | Steqanoqrafik mühafizə vasitələr. | 4 | 2 | 2 |
| 11. | Rəqəm imzası və ona qoyulan tələblər. Elektron imza texnologiyası. | 4 | 2 | 2 |
| 12. | Zərərli proqramlar və mühafizə vasitələri. Viruslarla mübarizə proqramları. | 4 | 2 | 2 |
| 13. | Kompüter cinayətlərinə qarşı mübarizə işinin təşkili. Kompüter cinayətkarlığı və kiberterrorçuluq sahəsində əsas anlayışlar. Kompüter hücumları – kiberhücumlar. | 4 | 2 | 2 |
| 14. | İnformasiya sahəsi üzrə milli maraqlar | 4 | 2 | 2 |
| 15. | İnformasiya təhlükəsizliyi siyasəti | 4 | 2 | 2 |
|  | Cəmi | 60 | 30 | 30 |

Cədvəl 3

|  |  |  |
| --- | --- | --- |
| № | Mühazirə dərslərində müzakirə olunan mövzuların məzmunu | Ixtisas 050616 |
| Saatların həcmi |
| 1 | Təhlükəsizlik haqqında məlumat | 1 |
| 2 | Informasiya təhlükəsizliyi haqqında məlumat | 2 |
| 3 | Informasiya təhlükəsizliyinin pozulmasının əsas kateqoriyaları | 1 |
| 4 | Informasiya təhlükəsizliyinin siyasəti | 1 |
| 5 | Informasiya icazəli girişin təmin edilməsi | 1 |
| 6 | Informasiya təhlükəsizliyinin pozulmasına məruz qala bilən əsas komponentlər | 1 |
| 7 | Süni təhlükələr | 1 |
| 8 | Təbii təhlükələr | 1 |
| 9 | Təhlükəsizliyin pozulması təhlükəsi (təhdidlər) | 2 |
| 10 | Informasiya təhlükəsizliyi probleminin həllinə kompleks yanaşma | 1 |
| 11 | Virusların yayılması | 1 |
| 12 | Antivirus proqramları | 2 |
| 13 | Farminq, skamminq, vişinq | 2 |
| 14 | Xakerlər | 1 |
| 15 | Kriptologiya elmi haqqında məlumat | 3 |
| 16 | Şifrləmə | 1 |
| 17 | Rəqəmsal imzanın iş prinsipi | 2 |
| 18 | Elektron hökumət | 2 |
| 19 | Kibertəhlükə və kibermüdaxilə | 2 |
| 20 | Kiberhücumlar | 2 |
|  | Cəmi | 30 |

|  |  |  |
| --- | --- | --- |
|  | Tələbənin S.A.A. | Təqdimat mövzuları |
| 1 |  | Informasiya təhlükəsizliyinin müasir üsullarla qorunması |
| 2 |  | Xüsusi virtual şəbəkə (VPN) |
| 3 |  | Kriptoqrafik protokol anlayışı |
| 4 |  | Təhlükəsizliyin auditi və monitorinqi |
| 5 |  | İdentifikasiya, autentifikasiya, aftorizasiya anlayışları |
| 6 |  | Şəbəkə təhlükəsizliyinin vasitələrlə idarəetmə  arxitekturasi |
| 7 |  | Əməliyyat sisteminin təhlükəsizliyinin təmin edilməsi  problemləri |
| 8 |  | AİS-də müdafiə sisteminin qurulmasının əsas  prinsipləri |
| 9 |  | Zorla müdaxiləni aşkarlayan sistemlər (IDS) |
| 10 |  | Parola hücum üsulları. Parolun təhlükəsizliyinin  təmini |
| 11 |  | Hədələr və naqilsiz korporativ şəbəkələrin  əlaqələndirilməsi |
| 12 |  | Viruslarla mübarizə |
| 13 |  | Əlçatanlığa hədd qoyma sistemləri |
| 14 |  | Kompüter virusları |
| 15 |  | Parola hücum üsulları. Parolun təhlükəsizliyinin təmini |
| 16 |  | Adekvat təhlükəsizlik siyasəti |
| 17 |  | Təhlükəsizlik hədələrinə qarşı tədbirlər |
| 18 |  | İnformasiya təhlükəsizliyinin beynəlxalq standartı |
| 19 |  | Fişinq |
| 20 |  | İnternet şəbəkədən istifadə |
| 21 |  | Təhlükəsizlik siyasətinin əsas anlayışları |
| 22 |  | Təhlükəsizliyin qlobal və lokal siyasəti |
| 23 |  | Təhlükəsizlik hədələrinə qarşı tədbirlər |
| 24 |  | Dövlət səviyyəsində informasiya təhlükəsizliyi |
| 25 |  | Təhlükəsizliyin baza siyasəti |
| 26 |  | Şifrələmə |
| 27 |  | Dayaqlıq alqoritmi |
| 28 |  | Şəbəkənin müdafiə vasitələri |
| 29 |  | Antivirus proqramları |
| 30 |  | Müasir simmetrik şifrələmə alqoritmi |