# "İnformasiya təhlükəsizliyi və kibertəhlükəsizliyin hüquqi aspektləri" Mühazirələr toplusu

**Book** · September 2024

CITATIONS
0

READS
262

**2 authors**, including:

Tabriz Jafarov

**8** PUBLICATIONS **1** CITATION

SEE PROFILE

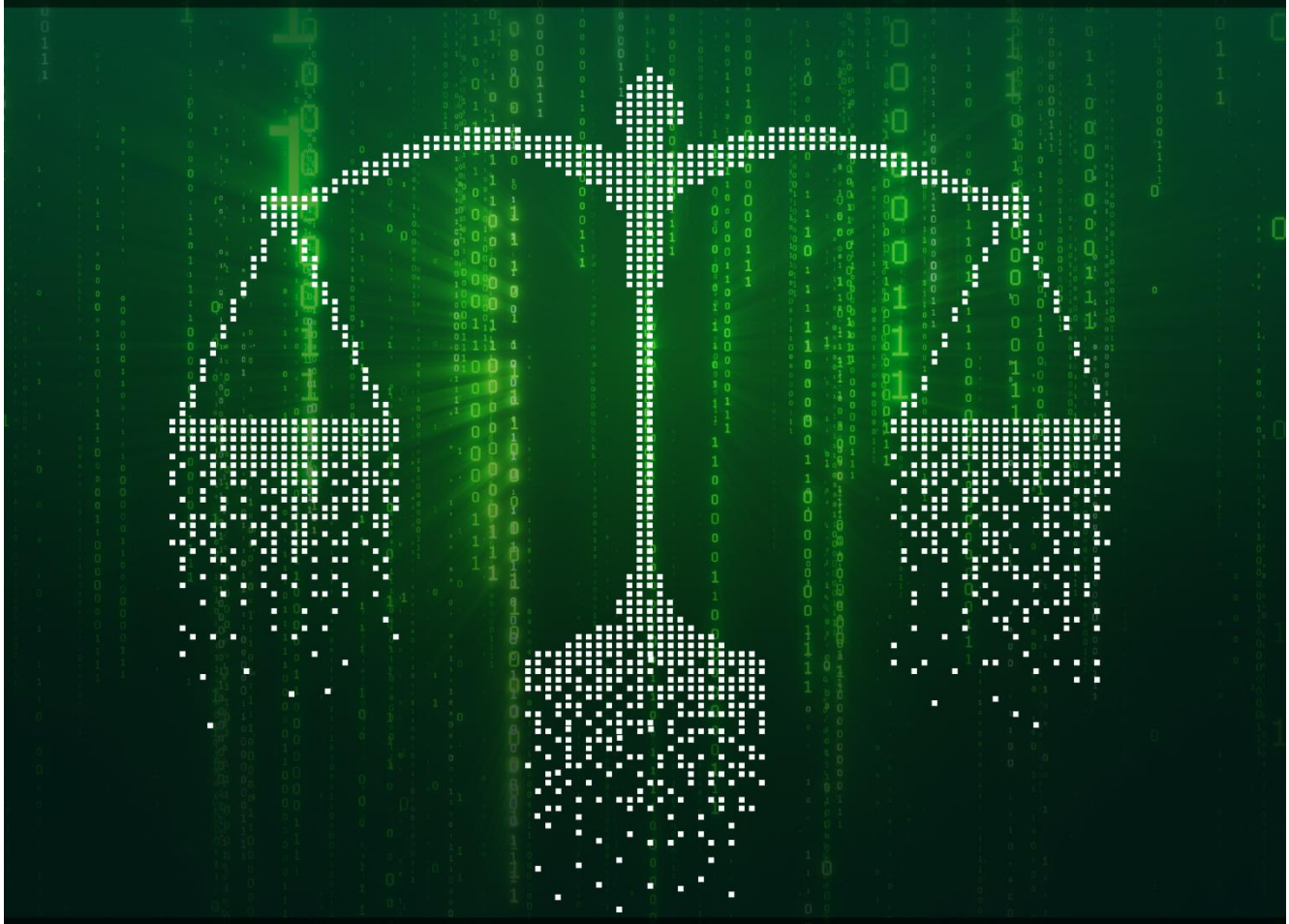
AZƏRBAYCAN RESPUBLİKASI
ELM VƏ TƏHSİL NAZİRLİYİ

Azərbaycan Kibertəhlükəsizlik
Təşkilatları Assosiasiyası

# İnformasiya təhlükəsizliyi və kibertəhlükəsizliyin hüquqi aspektləri

## fənni üzrə mühazirələr toplusu

Dr.Elvin Balacanov, Dr. Təbriz Raufoğlu, Vüqar Qədimov, Humay Hüseynova



Bu vəsait Azərbaycan Respublikasının Elm və Təhsil Nazirliyinin maliyyə dəstəyi ilə həyata keçirilən "İnformasiya təhlükəsizliyi ixtisası üzrə elmi-metodiki tədris (çap və onlayn) vəsaitlərinin hazırlanması" layihəsi çərçivəsində hazırlanmışdır.

“İnformasiya təhlükəsizliyi və kibertəhlükəsizliyin hüquqi aspektləri” fənni üzrə mühazirələr toplusu Azərbaycan Respublikasının Elm və Təhsil Nazirliyinin “Təhsildə könüllü fəaliyyətin təşkili” qrant müsabiqəsi çərçivəsində qalib elan olunmuş “İnformasiya təhlükəsizliyi ixtisası üzrə elmi-metodiki tədris (çap və onlayn) vəsaitlərinin hazırlanması” layihəsi çərçivəsində Azərbaycan Kibertəhlükəsizlik Təşkilatları Assosiasiyasının dəstəyi ilə hazırlanmışdır.

Mühazirələr toplusunun hazırlanmasının əsas məqsədini informasiya təhlükəsizliyinin və kibertəhlükəsizliyin elmi-metodoloji, nəzəri və hüquqi əsaslarının ali təhsilin bakalavriat səviyyəsində tədrisinə, habelə mövcud elmi-metodiki boşluqların aradan qaldırılmasına və azərbaycandilli elmi ədəbiyyatın formalaşmasına dəstəyin göstərilməsi təşkil edir.

Mühazirələr toplusu informasiya təhlükəsizliyi, o cümlədən kritik informasiya infrastrukturunun təhlükəsizliyi, kibercinayətkarlığa qarşı mübarizə və digər aidiyyəti sahələrdə tətbiq olunan hüquqi tənzimləmə mexanizmlərinə dair təhsilalanların biliklərinin artırılmasına dəstək verəcəkdir.



**“İnformasiya təhlükəsizliyi və kibertəhlükəsizliyin hüquqi aspektləri”**

**Mühazirələr toplusu**

**Azərbaycan Kibertəhlükəsizlik Təşkilatları Assosiasiyası, Bakı, 2024.**

# MÜNDƏRİCAT

# Mövzu 1.

## İnformasiya hüququnun əsasları, mənbələri, hüquq münasibətlərinin elementləri, hüquq normalarının subyektləri

"İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanununa əsasən, "informasiya" dedikdə, yaranma tarixindən, təqdimat formasından və təsnifatından asılı olmayaraq istənilən fəaliyyət nəticəsində yaradılan, yaxud əldə olunan faktlar, rəylər, bilgilər, xəbərlər və ya digər xarakterli məlumatlar başa düşülür.[1] Müasir elmi-hüquqi ədəbiyyatda isə "informasiya" termini müxtəlif istiqamətlər üzrə təhlil edilir. Buraya ilkin olaraq "verilənlər" anlayışı ilə "informasiya" anlayışının qarşılıqlı əlaqəsi və fərqi daxildir. Belə ki, "verilənlər" anlayışı "informasiya" anlayışı ilə sıx bağlıdır. Verilənlər, informasiya almaq üçün "xammaldır". Eyni bir verilən müxtəlif insanlara fərqli informasiyalar verə bilər. Bu, hər bir halda nisbi olaraq qiymətləndirilir. Məsələn, fizikaya aid kitabdan daha çox faydalı informasiyanı fizik ala bilər, başqa sahənin adamı (ədəbiyyatçı, tarixçi və s.) üçün isə həmin kitab heç bir informasiya daşımayan verilənlər yığınından ibarətdir.[2]

Elmi-texnoloji nailiyyət və biliklərə əsaslanan cəmiyyətlərdə "informasiya" ayrı-ayrı fərdlər, təşkilatlar və suveren dövlətlər üçün ən qiymətli sərvətlərdən biri halına gəlmişdir. Əlçatan və dəqiq informasiya əldə etmək zərurəti dövlət üçün əhəmiyyəli olan əsaslandırılmış qərarların qəbul edilməsindən tutmuş biznes məqsədlərinə nail olmağa qədər vacib məsələlərdə mühüm rol oynayır. İnformasiyanın hansı aspektdən qiymətləndirilməsindən asılı olmayaraq, onun əsas funksiyasını qeyri-müəyyənliyi müəyyənliyə çevirmək təşkil edir.

---

[1] Maddə 2, "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanunu (3 aprel 1998-ci il, № 460-IQ) (460-IQ - İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında (e-qanun.az)

[2] Calallı (Sadıqov) İ., "İnformatika terminlərinin izahlı lüğəti", 2017, "Bakı" nəşriyyatı, 996 s.

Digər tərəfdən, “Verilən-İnformasiya-Bilik” üçlüyü burada əsas əhəmiyyət kəsb edir. Yalnız mənalı və əhəmiyyət kəsb edən verilənlər birləşdiyi zaman informasiyaya çevrilir. Bu informasiya lazımi metod və üsullarla sübut edildikdən sonra “bilik” formasını alır.[3] Ənənəvi olaraq yaddaş “qurğuları” kimi kitablar çıxış etsə də, hazırda daha çox elektron kitabxana və media biliyin saxlanılmasında daha çox əhəmiyyət kəsb etməkdədir.

İnformasiya ətraf mühitdə “məlumat ötürmək” funksiyasını da daşıyır. İnformasiya bir sıra fakt və hadisələrə əsaslanan verilənlərdən əldə edilə bilər. Bunların hamısı məlumat “ötürmək” üçün nəzərdə tutulmasa da, müvafiq şəkildə şərh edildikdə informativ xarakter alır.

İnformasiya ünsiyyət prosesinin bir hissəsi kimi də çıxış edir. Biliklər informasiya vasitəsilə nəsildən nəsilə ötürülür. Bir çox informasiya sahəsi üzrə ixtisaslaşmış alimlər tərəfindən məcazi anlamda informasiyanın bütün canlı orqanizmlərin mülkiyyəti olduğu qəbul edilir. Lakin bu fikir informasiyanın yalnız bioloji səviyyədə öyrənilməli olduğu anlamına gəlmir. Bu əsasda “informasiya” həm də varlığın sosial kateqoriyası kimi insanlar arasındakı münasibətlərin inikası olaraq qiymətləndirilə bilər[4].

İnformasiya yaranma tarixindən, təqdimat formasından və təsnifatından asılı olmayaraq, istənilən fəaliyyət nəticəsində yaradılan, yaxud əldə olunan faktlar, rəylər, bilgilər, xəbərlər və ya digər xarakterli məlumatlardır[5]. İnformasiya özlüyündə açıq və konfidensial olaraq iki yerə təsnif edilir. Qanunla müəyyən edilmiş qaydada hər bir şəxs informasiya məhsullarından istifadə edib informasiyanın istifadəçisi ola bilər. Belə ki, “İnformasiya, informasiyalaşdırma və

[3] Cəfərov T. “Uluslararası hukuki yönleri ile siber alanda yetki sorunu”, Adalet yayın evi, Ankara, 2022.
[4] Hacıyev Z.C. Fəlsəfə. “Turan evi” nəşriyyatı, Bakı 2012, 488 səh.
[5] “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikasının Qanunu (3 aprel 1998-ci il, № 460-IQ) (460-IQ - İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında (e-qanun.az)

informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanununun 2-ci maddəsinə əsasən, "informasiyanın istifadəçisi" dedikdə, özü üçün zəruri informasiyanın alınması məqsədilə bilavasitə informasiya sisteminə və ya vasitəçiyə müraciət edən və ondan ancaq istifadə hüququna malik subyekt başa düşülür. Həmin Qanuna əsasən, informasiya məhsulları isə istifadəçilərin tələblərinə əsasən yaradılmış və onların tələbatlarının ödənilməsi üçün təyin olunmuş və ya tətbiq edilən sənədləşdirilmiş informasiya, informasiya sistemləri, texnologiyaları və onların təminat vasitələridir.

Yuxarıda sadalananlar informasiyalaşdırma prosesinin tərkib hissəsini təşkil edir. Hüquqi anlayışa uyğun olaraq, informasiyalaşdırma dedikdə, informasiya ehtiyatlarının formalaşdırılması, təqdim edilməsi, istifadə olunması əsasında dövlət hakimiyyəti və yerli özünüidarə orqanlarının, təşkilati-hüquqi və mülkiyyət formasından asılı olmayaraq bütün müəssisə, idarə və təşkilatların, vətəndaşların informasiya tələbatlarının və bu sahədəki hüquqlarının təmin edilməsinin optimal şəraitinin yaradılması üçün təşkilati, sosial-iqtisadi və elmi-texniki proses başa düşülür.[6]

Ümumi hüquq nəzəriyyəsində maddi və formal hüquq mənbələri fərqləndirilir. Buna uyğun olaraq, maddi mənada informasiya hüququnun mənbəyini tənzim olunan informasiya hüquq münasibətlərinin özü, yəni mövcud maddi həyat şəraiti təşkil edirsə, formal mənada informasiya hüququnun mənbələri dedikdə, informasiya hüquq normalarının xarici ifadə formaları başa düşülür. Bu o deməkdir ki, hüquq subyektlərinin davranış qaydasının hüquq norması olması üçün onun müəyyən hüquqi formaya salınması zəruridir. Belə hüquqi forma dövlətin hüquqyaratma fəaliyyəti nəticəsində baş verir və bir sıra hüquqi aktlarda öz əksini

[6] Maddə 2, "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanunu (3 aprel 1998-ci il, № 460-IQ) (460-IQ - İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında (e-qanun.az) .

tapır. Həmin hüquqi aktlar dövlətin qanunvericilik fəaliyyətinin təzahür forması kimi hüquq mənbələrini təşkil edir. Bununla yanaşı, hüquq mənbələrinin təsnifatı yalnız qanunvericilik aktları ilə məhdudlaşmayıb, müxtəlif hüquqi adətləri, presedentləri və s. mənbələri də əhatə edir. Lakin Azərbaycan Respublikası Roman-German hüquq sisteminə daxil olan dövlətlərdən olduğu üçün milli hüquq sistemində hüququn mənbələri dedikdə, konstitusion əsaslara söykənən yazılı qanunvericilik aktları nəzərdə tutulur.[7] Belə ki, Azərbaycan Respublikası Konstitusiyasının 148-ci maddəsinə müvafiq olaraq, qanunvericilik sistemi aşağıdakı normativ hüquqi aktlardan ibarətdir:

1) Konstitusiya;

2) Referendumla qəbul edilmiş aktlar;

3) Qanunlar;

4) Fərmanlar;

5) Azərbaycan Respublikası Nazirlər Kabinetinin qərarları;

6) Mərkəzi icra hakimiyyəti orqanlarının normativ aktları.

Qeyd edilənlərə əsaslanaraq deyə bilərik ki, Azərbaycan Respublikasının informasiya məkanının müasir təhdidlərdən qorunması milli təhlükəsizliyin əsas istiqamətlərindəndir. Qloballaşan dünyada informasiya təhlükəsizliyinin və kibertəhlükəsizliyin təmin olunması istər milli, istərsə də beynəlxalq səviyyədə əsas məsələyə çevrilmişdir. Bu fəaliyyətdə insan, cəmiyyət və dövlət maraqlarının qorunması başlıca məqsəddir. Son zamanlar Azərbaycanın informasiya məkanına, o cümlədən onun tərkib hissələrinə (dövlət, özəl və qeyri-hökumət qurumlarının, fiziki şəxslərin sahib olduğu informasiya ehtiyatlarına və infrastrukturlarına, bu

[7] Əliyev Ə., Rzayeva G., İbrahimova A., Məhərrəmov B., Məmmədrzalı Ş. İnformasiya hüququ. Dərslik. Bakı: "Nurlar" nəşriyyatı, 2019, 141.

ehtiyatlarda olan məlumatların həyat boyu proseslərinə, həmin proseslər üçün istifadə olunan maddi və qeyri-maddi obyektlərə və onlar arasında əlaqələrə) qarşı texnoloji cəhətdən çoxşaxəli hücumlar genişlənməkdədir[8].

İnformasiya hüquq münasibətlərinin subyektləri qismində fiziki və hüquqi şəxslər çıxış edir. Lakin daxil olduğu informasiya hüquq münasibətinin növündən və məzmunundan asılı olaraq subyekt müxtəlif cür adlandırıla bilər. Məsələn, informasiya sorğusu verən və informasiya sahibi, müraciət edən və müraciətə baxan subyekt və s.[9]

"İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında informasiya" Azərbaycan Respublikasının Qanununa əsasən, "İnformasiya təhlükəsizliyi" dedikdə, informasiya təhlükəsizliyi informasiyanın tamlığının (dəqiq, səlis, aktual və bütöv olması), əlçatanlığının (müraciət və əldə etmənin, nəzarətdə saxlamanın mümkün olması), konfidensiallığının (yalnız səlahiyyəti olan istifadəçilər və proseslər üçün məlum ola bilməsi) və mötəbərliliyinin (adekvat, obyektiv, faydalı olması) mühafizə edilməsi başa düşülür.

İnformasiya təhlükəsizliyinin əsas məqsədi informasiyanın məxfilik, bütövlük və əlçatanlıq prinsiplərinə uyğun olaraq mühafizəsinin təmin edilməsidir. İnformasiya təhlükəsizliyi həm fərdi istifadəçilər, həm də qurumlar üçün vacib nüansdır, çünki təhlükəsizlik pozuntusu ciddi nəticələrə və böyük ziyana səbəb ola bilər.

İnformasiya təhlükəsizliyi özündə bir sıra əsas elementləri ehtiva edir. Bu elementlər ayrı-ayrı prinsiplərlə məlumat təhlükəsizliyinin təmin edilməsi üçün

[8] 4060 - "Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023 – 2027-ci illər üçün Strategiyası"nın təsdiq edilməsi haqqında (e-qanun.az)
[9] Əliyev Ə., Rzayeva G., İbrahimova A., Məhərrəmov B., Məmmədrzalı Ş. İnformasiya hüququ. Dərslik. Bakı: "Nurlar" nəşriyyatı, 2019, 19.

əməl edilməli olan qaydaları ehtiva edir[10]. İnformasiya təhlükəsizliyinin əsas prinsiplərinə aşağıdakılar daxildir:

- **Məxfilik**: İnformasiyanın icazəsiz şəxslərdən gizli saxlanılması prinsipidir. Məxfilik şəxsi və həssas məlumatların yalnız səlahiyyətli şəxslər üçün əlçatan olmasını təmin edir. Güclü parollar, məlumatların şifrələnməsi və avtorizasiya mexanizmləri kimi üsullar məxfiliyi təmin etməyə kömək edir.
- **Tamlıq**: İnformasiyanın dəqiq, tam və etibarlı olması prinsipidir. İnformasiyanın tamlığı prinsipi informasiyanın icazəsiz şəxslər tərəfindən dəyişdirilməsindən və ya korlanmasından qorunmasını təmin edir. Məlumatların tamlığını təmin etmək üçün verilənlərin ehtiyat nüsxəsinin yaradılmas, məlumatların davamlı olaraq yoxlanılması və antivirus proqramlarından istifadə edilə bilər.
- **Əlçatanlıq**: Bu, lazım gəldikdə məlumatın səlahiyyətli şəxslər tərəfindən əlçatan olması prinsipidir. İnformasiyaya çıxış doğru zamanda və lazımi insanlara təmin edilməlidir. Bu prinsipi təmin etmək üçün təhlükəsiz şəbəkə konfiqurasiyaları, artıq sistemlər və etibarlı məlumat saxlama üsullarından istifadə edilə bilər.

İnformasiya təhlükəsizliyini təmin etmək üçün yerinə yetirilə biləcək bəzi vacib addımlar bunlardır:

- **Risk Qiymətləndirilməsi**: İnformasiya təhlükəsizliyi risklərini müəyyən etmək üçün təşkilatların mütəmadi olaraq risk qiymətləndirmələri aparması vacibdir. Bu qiymətləndirmə prosesi potensial təhlükələri, zəiflikləri və risk səviyyələrini müəyyən etmək məqsədi daşıyır. Risklərin qiymətləndirilməsi nəticəsində əldə

[10] İmamverdiyev Y., "Kibertəhlükəsizliyə giriş-I Mühazirə", BDU, 2022, 8.

edilən məlumatlar müvafiq təhlükəsizlik tədbirlərinin müəyyən edilməsinə kömək edir[11].

- **Təhlükəsizlik Siyasətləri və Prosedurları**: Təşkilatların təhlükəsizlik siyasətlərini və prosedurlarını müəyyən etməsi və onları işçilərə effektiv şəkildə çatdırması vacibdir. Bu siyasətlərə informasiya təhlükəsizliyi məqsədləri, məsuliyyətlər, istifadəçi davranışı və məqbul istifadə siyasətləri daxil edilməlidir. Bundan əlavə, təhlükəsizlik prosedurları təhlükəsizlik siyasətlərinin həyata keçirilməsini təmin edən addımları və təlimatları müəyyən edir.
- **Fiziki Təhlükəsizlik**: İnformasiya təhlükəsizliyini təmin etmək üçün fiziki təhlükəsizlik tədbirlərinin görülməsi vacibdir. Bunlar icazəsiz girişin qarşısını almaq və oğurluqdan, zədələnmədən və ya təbii fəlakətlərdən qorunmaq üçün görülən tədbirlərdir. Məsələn, server otaqlarının, təhlükəsizlik kameralarının, giriş kartları və ya biometrik təhlükəsizlik sistemlərinin kilidlənməsi kimi ehtiyat tədbirləri görülə bilər.
- **Məlumatların Şifrələnməsi**: Həssas məlumatların şifrələnməsi məlumatların icazəsiz şəxslərin əlinə keçməsinin qarşısını alır. Şifrələmə üsullarından istifadə etməklə məlumatlar qorunur və rabitə təhlükəsiz olur. Bu, portativ cihazlarda və ya internet üzərindən məlumat ötürülməsi zamanı xüsusilə vacibdir.
- **Təlim və Maarifləndirmə**: İşçilərin informasiya təhlükəsizliyi mövzusunda maarifləndirilməsi və məlumatlılığının artırılması vacibdir. İnformasiya təhlükəsizliyi siyasətləri və prosedurları üzrə müntəzəm təlimlərin keçirilməsi işçilərin düzgün təhlükəsizlik təcrübələrini öyrənmələrini təmin edir. Bundan əlavə, sosial mühəndislik hücumları kimi təhlükəsizlik risklərinə qarşı diqqətli olmaq üçün məlumatlılıq artırılmalıdır.

[11] Nieles M., Dempsey K., Pillitteri V.Y., "An Introduction to Information Security", USA, 2017, 101 p.

Bundan başqa, informasiya təhlükəsizliyi, insan hüquq və azadlıqlarının müdafiəsi baxımından həm internet provayderlərinin, həm də istifadəçilərin məsuliyyəti məsələsi də internet hüququnun tənzimetmə premetidir. Bunlara aiddir: internetə çıxış, internetin məzmun tənzimlənməsi, bloklama, məzmunun silinməsi və süzgəcdən keçirmə (filtrasiya), lisenziya və məsuliyyət[12].

Müasir dövrdə internetin günü-gündən sürətlə inkişafı insanların real dünyada olduğu kimi virtual aləmdə də təhlükəsizliklərinə diqqət etməli olduqlarının vacibliyini göstərir. İnsanların virtual mühitdə zərərverici şəxslər tərəfindən yaradılan təhdidlərdən və hücumlardan qorunmağa çalışması nəticəsində kiber təhlükəsizlik sferasının formalaşdırılması əsas şərtə çevrilmişdir. "Kibertəhlükəsizlik" sözü yunanca yönləndirmək mənasını verən "kubernan" sözünün 1948-ci ildə ingilis dilinə "cybernetics" olaraq daxil edilməsi sonra isə 1958-ci ildə Lois Couffignal tərəfindən canlılar və robotlar arasında əlaqəni izah etmək üçün "cyber" olaraq istifadə edilməsi nəticəsində yaranmışdır[13].

"Cyber" sözü Azərbaycan dilinə "kiber" olaraq tərcümə edildiyi üçün bu termin Azərbaycan dilində "Kibertəhlükəsizlik" olaraq adlandırılmışdır. Kibertəhlükəsizlik dedikdə, kompüterlərin, şəbəkələrin, serverlərin, elektron cihazların, elektron sistemlərin, proqram təminatlarının və məlumatların mümkün virtual təhdidlərdən və hücumlardan qorunmasının üsul və vasitələrinin məcmusu başa düşülür. Beynəlxalq yanaşmaya əsasən, kibertəhlükəsizlik informasiya təhlükəsizliyinin tərkib elementi kimi yox, kiberfəzanın təhlükəsizliyini özündə ehtiva edən müstəqil bir sahə olaraq müəyyən edilmişdir. Eyni zamanda, kibertəhlükəsizliyin informasiya təhlükəsizliyi ilə bir sıra ortaq cəhətləri də mövcuddur.

[12] Qaliboğlu E., "İnformasiya azadlığı, internet hüququ və etik problemlər", X-C, 2021.
[13] Couffignal L., "La Cyberne'tique", Paris, 1968, p.130

Kibertəhlükəsizliyin illər keçdikcə önəminin artmasına səbəb kibertəhdidlərin artım dinamikası və onun qlobal problemə çevrilməsidir. “Kibertəhdid” dedikdə, informasiya sistemlərinə və ya ehtiyatlarına qanunsuz daxilolma, müdaxilə, habelə digər formalarda informasiya təhlükəsizliyinin pozulmasına səbəb ola bilən amil və ya vəziyyət başa düşülür.

Kibertəhdidlər ayrı-ayrı fərdlər, təşkilatlar və müxtəlif mənbələrdən qaynaqlana bilər. Kibertəhdidləri ümumi olaraq iki kateqoriyaya ayırmaq mümkündür. Bunlar “kompüter mühitində yaranan kibertəhdidlər” və “kiberfəzadakı strateji təhdidlər”dir.. Dövlət təhlükəsizliyinə qarşı olan kibertəhdidlər isə “daxili kibertəhdidlər” və “xarici kibertəhdidlər” olaraq iki qrupa ayrılır.

Eyni zamanda, proseslərin məhdud hüdudları olan bir məkanı əhatə etməməsi, yəni sadəcə şəbəkə mütəxəssisləri və kompüter mühəndislərinin həll edə biləcəyi texniki problemlər olmaması həm həll yolları baxımından, həm də veriləcək reaksiyalar baxımından fərqliliklər yarada bilməkdə, yəni proseslər zaman və məkana uyğun olaraq dəyişə bilməkdədir.

Kibertəhlükəsizliyin inkişafı “kibermәkan”nın virtual fenomen kimi yaranmasını şərtləndirmişdir. Oksford lüğətinə görə, kibermәkan "kompüter şəbəkələri üzərindən rabitənin aparıldığı və fiziki məkanı olmayan konseptual mühitdir" və Collins lüğətinə görə, “Virtual reallıq istifadəçisinin içindən keçə biləcəyi üç ölçülü model olaraq təmsil edilən böyük kompüter və ya şəbəkədə saxlanılan bütün məlumatlardır", Merriam-Webster lüğətinə görə "kompüter şəbəkələrinin virtual dünyası", Vikilüğətə görə isə "İnternet vasitəsilə əldə edilən məlumat dünyası" mənasını verir. Britannica-ya görə isə “Kiberfəza termini ilk dəfə Amerika-Kanada yazıçısı William Gibson tərəfindən 1982-ci ildə “Omni” jurnalında nəşr olunan hekayəsində və daha sonra isə müəllifin “Neuromancer”

adlı kitabında istifadə edilmişdir. Bu elmi fantastika romanında Gibson kiberməkanı süni intellektli varlıqlarla dolu bir dünyada kompüter şəbəkəsinin yaradılması kimi izah etmişdir. Kiberməkan və internet anlayışları əslində bir-birini tamamlamaqda və xüsusilə, internet kiberməkanın vasitələrindən biri kimi görülməkdədir. İlk öncə, kiberməkanın internetsiz də mövcud ola biləcəyi nəzərə alınaraq, internetlə kiberməkan arasında müəyyən fərqlər olduğunu iddia etmək olar. Habelə, internet dediyimiz obyekt kiberməkan anlayışı ilə demək olar ki, eyni tarixi prosesi paylaşır və mahiyyət etibarı ilə eyni universal kəşfləri ehtiva edir[14].

Son zamanlarda, informasiya və kommunikasiya texnologiyalarının inqilabi inkişafı hüququn müstəqil bir sahəsi kimi "informasiya hüququ" sahəsinin inkişafını şərtləndirmişdir. Müasir texnoloji bacarıqlar məlumatları böyük miqyasda toplamaq, istifadə etmək, təhlil etmək və yaymaq imkanı verdiyindən beynəlxalq ictimaiyyət informasiya hüququ çərçivəsində lazımi qanunvericilik bazası ilə cari sahənin tənzimlənməli olduğunu qəbul edir. İnformasiya hüququ, inzibati hüquq, cinayət hüququ, əmək hüququ, kommersiya hüququ kimi hüququn digər sahələri ilə də qarşılıqlı əlaqədədir.

İnformasiya sahəsinin genişliyi və təhdidlərə açıq olması bu sahədə dövlət tənzimlənməsinin həyata keçirilməsini labüd edir. Buna görə də cari sahənin hüquqi tənzimlənməsi həm fərdlərin maraqları, həm də dövlət təhlükəsizliyi aspektindən əhəmiyyətlidir.

İnformasiya hüququ dedikdə, informasiyanın dövriyyəsi, informasiya ehtiyatlarının formalaşdırılması və istifadəsi, vətəndaşların, təşkilatların, dövlətin və cəmiyyətin informasiya ehtiyaclarının təhlükəsiz şəkildə ödənilməsə yönəlmiş informasiya sistemlərinin yaradılması və fəaliyyəti ilə bağlı informasiya sahəsində

[14] Tabriz Raufoglu (JAFAROV). "Uluslararasi hukuki yönleri ile siber alanda yetki sorunu", Adalet yayın evi, Ankara, 2022, s. 5-30.

yaranan ictimai münasibətləri tənzimləyən hüquq normalarının məcmusu başa düşülür.

İnformasiya hüququnun hüquqi tənzimlənməsinin əsas predmeti qismində informasiya çıxış edir. Bu predmetə informasiya proseslərini daxil edə bilərik. İnformasiya proseslərinə informasiyanın yığılması, işlənməsi, saxlanması, axtarışı, yayılması əsasında informasiya ehtiyatlarının formalaşdırılması, informasiya sistemləri, texnologiyaları, onların təminat vasitələrinin yaradılmasını aid edə bilərik[15]. İnformasiya hüququ inzibati hüququn alt sahəsi kimi qiymətləndirildikdə, informasiya-hüquqi münasibətlərə tənzimləyici təsir metodlarının bütün kompleksindən, yəni həm dispozitiv tənzimləmədən (seçim azadlığı, tərəflərin bərabərliyi, mərkəzsizləşdirmə, koordinasiya), həm də imperativ tənzimləmədən (hakimiyyətin mərkəzləşdirilmiş şəkildə həyata keçirilməsi, ciddi tabeçilik) ibarətdir. İnformasiya hüququ sisteminə müxtəlif üsulların daxil edilməsi onların özbaşına toqquşması və ya rəqabəti demək deyil. İnformasiya hüququ üçün müəyyən metodların əhəmiyyəti ilə bağlı müzakirələr yalnız informasiya ilə bağlı münasibətlərdə yaranan problemləri həll etmək üçün müstəqil hüquq sistemini inkişaf etdirməklə uzlaşdırıla bilər[16].

İnformasiya hüquq münasibətlərinin subyektləri qismində fiziki və hüquqi şəxslər çıxış edir. Lakin daxil olduğu informasiya hüquq münasibətinin növündən və məzmunundan asılı olaraq subyekt müxtəlif cür adlandırıla bilər. Məsələn, informasiya sorğusu verən və informasiya sahibi, müraciət edən və müraciətə baxan subyekt və s. Bundan başqa, informasiya sahəsinin modelinə əsasən, informasiya hüquq münasibətlərinin subyektlərini aşağıdakı qruplara bölmək olar:

[15] "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanunu (3 aprel 1998-ci il, № 460-IQ) (460-IQ - İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında (e-qanun.az)

[16] Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право./Под ред. академика РАН Б. Н. Топорнина. СПб.: Издательство Р. Асланова «Юридический центр Пресс», 2005.

informasiyanın istehsalçıları və ya yaradıcıları; informasiyanın istehlakçıları. Lakin belə bölgünü aparmaq bir qədər şərti xarakter daşıyır. Çünki müasir informasiya cəmiyyətində informasiya istehlakçısı informasiyanı yenidən emal edərək, istehsalçıya çevrilə bilir. Bu baxımdan, subyektlərin bölgüsü və xarakterik xüsusiyyətlərinin ayrı-ayrı informasiya hüquq münasibətləri üzrə aparılması daha düzgün hesab edilir[17]. Subyektlər arasında əlaqənin quruluşuna görə mütləq və nisbi informasiya hüquq münasibətləri fərqləndirilir. Birinci qrup münasibətlərdə bir tərəf səlahiyyətli subyekt qismində çıxış edir, digər tərəfə isə passiv öhdəlik daşıyan qeyri-müəyyən şəxslər dairəsi aiddir. Bu o deməkdir ki, mütləq informasiya hüquq münasibətlərində bir tərəfin səlahiyyətləri dəqiq müəyyən olunur, digər iştirakçılar isə hamısı həmin subyekt qarşısında vəzifələr daşıyırlar. Məsələn, dövlət sirrinin hüquqi rejimi ilə bağlı yaranan münasibətlərdə dövlət sirri məlum olan subyekt və bu məlumatları əldə etməsi qadağan olunan üçüncü şəxslər münasibətin iştirakçıları kimi tanınır. Nisbi informasiya hüquq münasibətlərində isə ikinci subyektlərin dairəsi konkret müəyyən olunur, yəni münasibətin bütün iştirakçılarının hüquq və vəzifələri dəqiq məlumdur. Məsələn, fərdi məlumatlarla bağlı işçi və işəgötürən arasında yaranan münasibətlər.

[17] Əliyev Ə., Rzayeva G., İbrahimova A., Məhərrəmov B., Məmmədrzalı Ş. İnformasiya hüququ. Dərslik. Bakı: "Nurlar" nəşriyyatı, 2019, 448 s.

# Mövzu 2.

## Azərbaycan Respublikasında informasiyalaşdırma sahəsində dövlət siyasətinin əsas istiqamətləri, müvafiq strategiya, dövlət proqramları, ölkənin informasiya sahəsində milli təhlükəsizlik maraqları və informasiya təhlükəsizliyi siyasəti.

İnformasiya təhlükəsizliyi dedikdə "İnformasiyanın tamlığının (dəqiq, səlis, aktual və bütöv olması), əlçatanlığının (müraciət və əldə etmənin, nəzarətdə saxlamanın mümkün olması), konfidensiallığının (yalnız səlahiyyəti olan istifadəçilər və proseslər üçün məlum ola bilməsi) və mötəbərliliyinin (adekvat, obyektiv, faydalı olması) mühafizə edilməsi" başa düşülür.[18]

İnformasiya təhlükəsizliyi hüquqi aspektdən informasiyanın əlyetərliyinin, tamlığının və konfidensiallığının pozulmasına yönəlmiş təhlükələrin qarşısının alınması məqsədini daşıyır. Bəs qeyd edilən həmin təhlükələr nədən ibarətdir? İnformasiya təhlükəsizlyinin təminatı, dedikdə nə başa düşülür və onun məzmununa hansı tədbirlər daxildir? Bu kimi sualların cavablandırılması üçün ilk növbədə, qanunvericilik normalarına nəzər yetirmək lazımdır. "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikası Qanununun 17-19-cu maddələrində informasiyanın mühafizəsindən bəhs olunur. 17-ci maddənin şərhinə əsasən, belə bir nəticəyə gəlmək olar ki, informasiyanın mühafizəsi informasiya təhlükəsizliyinin təminatına yönəlmiş tədbirlər kompleksini ehtiva edir. Burada sadalanan aşağıdakı məqsədlər mahiyyət etibarilə informasiya sahəsində olan təhdid və təhlükələrin qarşısının alınmasına xidmət edir:

[18] Maddə 2, "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanunu (3 aprel 1998-ci il, № 460-IQ) (460-IQ - İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında (e-qanun.az)

- informasiyanın məhvinin, itməsinin, saxtalaşdırılmasının qarşısının alınması;
- dövlətin, ictimaiyyətin, vətəndaşların təhlükəsizliyinin təmin edilməsi;
- informasiyanın məhvi, modifikasiyası, surətinin çıxarılması, təcrid edilməsi ilə bağlı sanksiyalaşdırılmamış hərəkətlərin qarşısının alınması;
- dövlət sirri təşkil edən və konfidensial informasiyanın qorunması;
- informasiya proseslərində habelə informasiya sistemlərinin, texnologiyalarının və onların təminat vasitələrinin işlənməsi, istehsalı, tətbiqi zamanı fiziki və hüquqi şəxslərin hüquqlarının təmin olunması.

Bu əsasda "informasiya təhlükəsizliyi" və "informasiyanın mühafizəsi" anlayışlarının qarşılıqlı əlaqəsini tamın hissəyə və ya ümuminin xüsusiyə nisbəti kimi qiymətləndirmək olar. Birinci anlayış geniş səciyyə daşıyaraq vahid tam halında ikinci termini də özündə ehtiva edir. Ona görə də informasiya təhlükəsizliyi yalnız informasiyanın mühafizə edilməsi kimi qiymətləndirilməməlidir. Bu anlayış eyni zamanda, təhlükəsiz informasiya mübadiləsini də əhatə edir. Çünki, subyektlər arasında informasiya mübadiləsinin normal olmadığı bir şəraitdə informasiya cəmiyyətinin məqsəd və vəzifələrinə nail olmaq mümkün deyil. Məhz bu baxımdan, həm milli strategiyalarda, həm də dövlət proqramlarında təhlükəsiz informasiya mübadiləsinin təmin olunması əsas vəzifələrdən biri kimi nəzərdə tutulmuşdur. Bu məqsədlə dövlət orqanlarının vahid konfidensial multiservis rabitə şəbəkəsi inkişaf etdirilmişdir.[19] Lakin bu şəbəkə dövlət orqanları arasında təhlükəsiz və operativ informasiya mübadiləsinin təmin olunması məqsədini daşıyır. Adi vətəndaşlar arasında təhlükəsiz informasiya mübadiləsi necə təmin olunmalıdır? Hesab edirik ki, bütövlükdə informasiyanın konfidensiallığının, tamlığının və əlyetərliyinin qorunmasına yönəlmiş tədbirlər

[19] "Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafı üzrə 2010 - 2012-ci illər üçün Dövlət Proqramı"nın (Elektron Azərbaycan)" təsdiq edilməsi haqqında Azərbaycan Respublikası Prezidentinin Sərəncamı

nəticə etibarilə, bütün istiqamətlərdə təhlükəsiz informasiya mübadiləsinə təminat verir. Bundan irəli gələrək, həm 2003- 2012, həm də 2014-2020-ci illər üçün Milli Strategiyalarda, eyni zamanda "Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023 – 2027-ci illər üçün Strategiyası"nda da informasiya təhlükəsizliyinin təmin olunması əsas vəzifələr və fəaliyyət istiqamətləri sırasında göstərilmişdir.

Onu da xüsusilə qeyd etmək lazımdır ki, zaman keçdikcə "informasiya təhlükəsizliyi" anlayışına yanaşma da dəyişir. Əgər internetin yarandığı ilkin dövrlərdə bu anlayış bilavasitə texniki aspektləri – informasiya infrastrukturunun sıradan çıxarılmasının qarşısının alınması ilə bağlı məsələləri əhatə edirdisə, hal-hazırda informasiya hücumlarının məqsədi dəyişdiyi (müxtəlif konfidensial məlumatların əldə olunması) üçün artıq "informasiya təhlükəsizliyi"nə dair fərqli yanaşma formalaşmışdır. Ona görə cari dövrdə kompüter şəbəkə və sistemlərinin təhlükəsizliyi ilə yanaşı, ötürülən informasiyanın mühafizəsi də mütləq şəkildə təmin olunmalıdır. Bütün bunlar yeni təhlükəsizlik trendlərinin meydana gəlməsinə səbəb olur. Qeyd etməliyik ki, hər bir inkişaf trendi öz daxilində digər inkişaf trendini formalaşdırır və bu da nəticə etibarilə uyğun təhlükəsizlik trendinin yaradılmasını şərtləndirir. Məsələn, portativ və fərdi mobil qurğuların yaradılması infrastruktur inkişaf trendi olaraq, tətbiq və istifadə trendlərini artırmışdır. Hər bir mobil qurğu da kiberhücumlar üçün yeni imkan yaradır. Ona görə bunun qarşısının alınması üçün mobil qurğularda kiberhücumların qarşısını ala biləcək yeni proqram və digər təhlükəsizlik tədbirləri planlaşdırılır və həyata keçirilir.

Son dövrlərdə elektron dövlət quruculuğu ilə əlaqədar yaranan digər bir anlayış isə "elektron təhlükəsizlik"dir. "İnformasiya təhlükəsizliyi" və "elektron təhlükəsizlik" eyni anlayışlardırmı? Elektron təhlükəsizlik – kompüterlər, şəbəkələr, proqramlar və verilənlərə gözlənilməyən və icazəsiz giriş, onların

dəyişdirilməsi və dağıdılmasından mühafizəni nəzərdə tutur.[20]Elektron təhlükəsizlik anlayışı, həmçinin informasiya texnologiyalarının təhlükəsizliyi kimi də ifadə oluna bilər. Göründüyü kimi, elektron təhlükəsizlik əsas etibarilə texniki aspektləri əhatə edir. İnformasiya təhlükəsizliyi isə daha geniş səciyyə daşıyır. Doğrudur, informasiya təhlükəsizliyinin təminatına yönəlmiş tədbirlərin böyük bir hissəsini texniki-təşkilati tədbirlər təşkil edir. Lakin informasiya təhlükəsizliyi yalnız bu növ tədbirlərin icrası ilə deyil, başqa fəaliyyət istiqamətlərinin də həyata keçirilməsi ilə təmin olunur.

Qeyd olunanları ümumiləşdirərək, "informasiya təhlükəsizliyi"nin təminatı anlayışının məzmununa aşağıdakı istiqamətləri daxil etmək olar:

- **Hüquqi istiqamət**. Müvafiq qanunvericilik bazası formalaşdırmadan informasiya təhlükəsizliyinin təminatına yönəlmiş tədbirlərin icrası qeyri-mümkündür. Bu sahədə hüquqi bazanın təkmilləşdirilməsi – informasiya təhlükəsizliyi sahəsində vahid dövlət siyasətinin formalaşdırılmasına, informasiya sahəsində milli təhlükəsizliyin təmin olunmasına, kibercinayətkarlığa qarşı mübarizə aparılmasına, milli maraqları nəzərə almaqla vətəndaşların və bütün təşkilatların təhlükəsiz olaraq informasiya əldə etmək və ondan istifadə etmək hüquqlarının təmin olunması üçün şəraitin yaradılmasına, habelə vətəndaşların informasiya təhlükəsizliyini təmin edən mühitin yaradılmasına xidmət edir.
- **Nəzəri-konseptual istiqamət**. Cəmiyyətdə baş verən bütün hadisə və proseslərin şərhini nəzəri və empirik biliklərin qarşılıqlı təhlili əsasında vermək olar. Ona görə də "informasiya təhlükəsizliyi" və onunla bağlı yaranan yeni terminlərin elmi izahı, eləcə də mövcud problemlər istiqamətində tədqiqatlar

[20] Əliyev Ə., Rzayeva G., İbrahimova A., Məhərrəmov B., Məmmədrzalı Ş. İnformasiya hüququ. Dərslik. Bakı: "Nurlar" nəşriyyatı, 2019, 399 s.

genişləndirilməli və bu tədqiqatların nəticələri hüquqi bazaya aprobasiya olunmalıdır. Belə olan halda informasiya təhlükəsizliyi ilə bağlı hüquqi yanaşma da formalaşmış olacaqdır.

- **Texniki-təşkilati istiqamət**. Əvvəlki fəsillərdə qeyd olunduğu kimi, informasiya cəmiyyətinin vacib elementlərindən biri yüksək səviyyəli informasiya infrastrukturunun mövcudluğudur. Təbii ki, normal texniki təminat olmadan təhlükəsiz informasiya mübadiləsini həyata keçirmək mümkün deyil. Şəbəkədə, informasiya sistemlərində yaranan boşluqlar nəticə etibarilə informasiyanın tamlığının pozulmasına, konfidensiallığının qorunmamasına, eləcə də əldə edilmə ilə bağlı ləngimə və maneələrin artmasına səbəb olur. Ona görə də Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023 – 2027-ci illər üçün Strategiyasında nəzərdə tutulan aşağıdakı texniki-təşkilati xarakterli tədbirlər bilavasitə informasiya təhlükəsizliyinin təminatına yönəlmişdir: ölkənin milli informasiya məkanının və kritik infrastrukturunun, o cümlədən informasiya infrastrukturunun informasiya təhlükəsizliyini təmin edən sistemin inkişaf etdirilməsi; "e-hökumət" infrastrukturunun informasiya təhlükəsizliyinin təmin edilməsi; dövlət və qeyri-dövlət informasiya infrastrukturu subyektlərinin kibertəhlükəsizlik üzrə fəaliyyətlərinin əlaqələndirilməsi; ölkənin informasiya əlaqələrində xarici ölkələrdən texniki və texnoloji asılılığın azaldılması üzrə tədbirlərin həyata keçirilməsi və s. Texniki baxımdan, informasiya təhlükəsizliyinin təminatında kriptoqrafiyanın böyük rolu vardır. Hazırda kriptoqrafiya konfidensiallığın təmin edilməsi, tamlığa nəzarət, autentifikasiya və rəqəmsal imza kimi informasiya təhlükəsizliyi funksiyalarının təmin edilməsi üçün ən səmərəli vasitədir.

- **Beynəlxalq-hüquqi istiqamət**. Qlobal informasiya məkanının, internetin bütün dünyanı əhatə etməsindən irəli gələrək, "informasiya təhlükəsizliyi" problemi artıq yalnız milli çərçivədə deyil, həm də beynəlxalq istiqamətdə həll olunmanı tələb edir. Təsadüfi deyil ki, dünya rabitə və informasiya sisteminə daxil olma Azərbaycan Respublikasının informasiya sahəsində milli maraqlarından biridir ("Milli təhlükəsizlik haqqında" Azərbaycan Respublikası Qanununun 6.6-cı maddəsi). Bu baxımdan, informasiya təhlükəsizliyi sahəsində beynəlxalq əməkdaşlığın təmin olunması mühüm əhəmiyyət kəsb edir. Həmçinin bir çox kibercinayətlər milli sərhədlərdən kənara çıxır ki, belə əməllərlə mübarizənin gücləndirilməsi milli normaların beynəlxalq normalara uzlaşdırılması və beynəlxalq qurumlarla qarşılıqlı fəaliyyət nəticəsində reallaşdırılır. Başqa bir məsələ digər ölkələr tərəfindən informasiya təcavüzü, beynəlxalq aləmdə Azərbaycan həqiqətlərinin təhrif edilməsi təhdidi ilə bağlıdır. Bu cür təhdidlərin qarşısının alınmasında da beynəlxalq əməkdaşlıq xüsusi əhəmiyyətə malikdir.
- **Sosial istiqamət**. İnformasiya təhlükəsizliyinin təmin olunmasında insan faktorunun təsiri heç də az deyil. Onu da nəzərə almaq lazımdır ki, bu sahədə olan təhdidlərin əksəriyyəti insan hüquq və azadlıqlarına qəsd edir. Məhz bu baxımdan, cəmiyyətdə maarifləndirmə işinin gücləndirilməsi informasiya təhlükələrinin də sayının azalmasına gətirib çıxara bilər. Kibermühitdə öz hüquq və azadlıqlarını, müdafiə üsullarını bilən hər bir kəs informasiya təhlükələrindən qorunma imkanına malik olur. Milli strategiyalarda qarşıya məqsəd kimi qoyulan elektron təhlükələr barədə ölkə səviyyəsində məlumatlandırmanın həyata keçirilməsi, kibertəhlükəsizliyin gücləndirilməsi istiqamətində müvafiq texniki və metodiki vasitələrin yaradılması, tövsiyələrin hazırlanması və metodiki dəstəyin göstərilməsi, əhalinin, özəl və digər qurumların kibertəhlükəsizlik sahəsində maarifləndirilməsi və informasiya

təhlükəsizliyi mədəniyyətinin formalaşdırılması, bu sahədə ixtisaslı kadrların hazırlanması kimi tədbirlər cəmiyyət üzvlərinin informasiya təhlükəsizliyi ilə bağlı savadlılıq səviyyəsinin qaldırılmasına xidmət edir.

XX-ci əsrin sonları və XXI-ci əsrin əvvəllərində ölkəmizdə və bütün dünyada baş verən müharibələr və münaqişələr nəticəsində geosiyasiyasi vəziyyətin dəyişməsi, beynəlxalq münasibətlərin tənzimlənməsi, dövlətlərin milli təhlükəsizliyinin təmin edilməsi və bu kimi məsələlər informasiya sahəsində dövlət siyasətinin formalaşdırılmasını və tənzimlənməsini zərurət halına çevirmişdir.

YUNESKO-nun "İnformasiya Hamı Üçün (İnformation for All) Proqramı" Milli İnformasiya Cəmiyyəti Siyasətində (MİCS)-də yazılanlara da əsaslanaraq informasiya siyasətinin həyata keçirilməsi prosesini informasiya strategiyası və informasiya taktikası olaraq iki hissəyə ayırmaq mümkündür. İnformasiya strategiyası müəyyən bir dövrdə qüvvədə olması təyin edilməklə ölkə üzrə qəbul edilən informasiya təhlükəsizliyinin təmin edilməsi prosesində mövcud vəziyyəti, problemləri, aktual məsələləri və atılacaq addımları özündə ehtiva edən hüquqi aktdır. İnformasiya taktikası dedikdə isə informasiya strategiyasında əksini tapmış məsələlərin təmini üçün atılacaq olan konkret tədbirlərdir. Yəni, informasiya strategiyası ortaya qoyulmuş problemlər və görüləcək işləri, informasiya strategiyası isə sözügedən məsələlərlə bağlı atılacaq addımları özündə ehtiva edir.

Dövlətin informasiya siyasəti hazırlanarkən qanunvericilik aktları rəhbər götürülməlidir və dövlət siyasətinin bütün aspektləri nəzərə alınmalıdır. Yəni, informasiya siyasəti dövlətin iqtisadi, sosial, hüquqi, xarici və təhlükəsizlik maraqlarına və siyasətlərinə, həmçinin beynəlxalq hüquq normalarından irəli gələn prinsiplərə və qanunvericilik aktlarına uyğun formada hazırlanılmalıdır.

"İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikası Qanununda milli informasiya siyasətinə anlayış

verilməsə də, “informasiyalaşdırma” termini nəzərdə tutulmuşdur (maddə 2). Bu termin hər kəsin informasiya hüquqlarının təminatına yönəlmiş təşkilati, sosial-iqtisadi və elmi-texniki prosesi əhatə etdiyi üçün müəyyən mənada dövlətin informasiya siyasəti ilə eyni məna kəsb edir. Eyni zamanda, Qanunun 3-cü maddəsində göstərilən informasiyalaşdırma sahəsində dövlət siyasətinin əsas istiqamətləri də bilavasitə milli informasiya siyasətinin əsas istiqamətlərini müəyyən edir ki, bu istiqamətlər aşağıdakılardan ibarətdir:

- milli informasiya fəzasının formalaşdırılması;
- informasiyalaşdırma üzrə fəaliyyətin başlıca istiqamətlərinin təyini və meydana çıxan münasibətlərin tənzimlənməsi;
- informasiya ehtiyatları, sistemləri, texnologiyaları və onların təminat vasitələri üzərində mülkiyyətin bütün formalarının inkişafına, informasiya məhsulları və xidmətləri bazarının formalaşmasına yardım edilməsi;
- dövlət informasiya ehtiyatlarının formalaşdırılması və mühafizəsi üçün zəruri olan şəraitin yaradılması;
- ərazi informasiya şəbəkələrinin yaradılması, onların beynəlxalq informasiya şəbəkələri ilə uzlaşması, qarşılıqlı əlaqəsinin təmin edilməsi üçün lazımi təşkilati, hüquqi, texniki siyasətin təyin edilməsi;
- dövlət informasiya ehtiyatları əsasında dövlət hakimiyyəti və yerli özünüidarə orqanları, təşkilati-hüquqi və mülkiyyət formasından asılı olmayaraq bütün müəssisə, idarə və təşkilatların, vətəndaşların müvafiq informasiya ilə təmin olunması üçün şərait yaradılması;
- informasiya fəzasında milli təhlükəsizliyin təmin edilməsi;
- informasiya məhsulları və xidmətləri bazarında informasiya münasibətlərinin subyektləri, o cümlədən xarici subyektlər tərəfindən inhisar fəaliyyəti və haqsız rəqabətin qarşısının alınması və yol verilməməsi;

- informasiyalaşdırma mühitində dövlət hakimiyyəti və yerli özünüidarə orqanlarının, təşkilati-hüquqi və mülkiyyət formasından asılı olmayaraq bütün müəssisə, idarə və təşkilatların, vətəndaşların hüquqlarının təmin olunması;
- informasiyalaşdırma mühitində elmi-texniki və istehsal siyasətinin formalaşdırılması və həyata keçirilməsi;
- informasiyalaşdırma layihələri və proqramlarının dəstəklənməsi, onların işlənməsi və həyata keçirilməsi üçün investisiyaların cəlb olunması sisteminin və stimullaşdırma mexanizminin yaradılması;
- informasiya prosesləri, informasiyalaşdırma və informasiyanın mühafizəsi sahəsində hüquqi bazanın inkişaf etdirilməsi.

Milli informasiya siyasətinin qeyd olunan bu istiqamətləri müxtəlif mərhələlərlə həyata keçirilmiş və keçirilməkdə davam edir. İnformasiya cəmiyyətinin qurulması zamanı milli səviyyədə aşağıdakı prinsiplərə əməl olunmalıdır: liderlik – dövlət idarəetmə və yerli özünüidarəetmə orqanlarının, təşkilat və müəssisələrinin rəhbərləri İKT-nin inkişafını və geniş tətbiqini öz fəaliyyətləri ilə bilavasitə təmin etməlidirlər;

- bərabərlik – cəmiyyətdəki mövqeyindən və mülkiyyət formasından asılı olmayaraq, prosesin bütün iştirakçılarının maraqları eyni dərəcədə nəzərə alınmalı, sosial ədalət prinsipi gözlənilməlidir;

- şəffaflıq və cəlbolunma – həyata keçirilən fəaliyyət barədə ictimaiyyət geniş məlumatlandırılmalı, açıq ictimai müzakirələr təşkil edilməli və qərarların qəbulunda vətəndaşların, ictimai təşkilatların təklifləri nəzərə alınmalıdır;

- əməkdaşlıq – həyata keçirilən fəaliyyətdə dövlət, biznes və vətəndaş cəmiyyəti tərəfdaşlığına xüsusi fikir verilməlidir;

- maarifləndirmə – informasiya cəmiyyəti quruculuğuna geniş kütlələrin cəlb olunması, cəmiyyətin hər bir üzvünün bu prosesdə fəal iştirakının təmin edilməsi üçün bu texnologiyalara dair bilik və məlumatlar əhatəli şəkildə əhaliyə çatdırılmalıdır;

- sosialyönlülük – vətəndaşların sosial maraqlarının qorunması, hüquqlarının təmin olunmasına hərtərəfli şərait yaradılması əsas götürülməlidir;

- millilik – ölkədə yaşayan bütün xalqların mənafeyi nəzərə alınmaqla, milli informasiya resurslarının inkişafına, elmi və mədəni irsin müasir texnologiyalar vasitəsilə qorunmasına, yerli İKT sənayesinin inkişafına, yerli istehsalçıların maraqlarına üstünlük verilməlidir;

- mərhələlilik – İKT-nin sürətli inkişafını nəzərə alaraq və mövcud imkanlardan səmərəli istifadəni təmin etmək məqsədi ilə fəaliyyət ardıcıl və mərhələlərlə həyata keçirilməli, proqram və layihələr hazırlanarkən prioritetlər, maliyyə və nəticələrin qısa müddətdə əldə edilməsi əsas götürülməlidir;

- innovativlik – elmi-texniki tərəqqinin yenilikləri nəzərə alınmalı, müasir elmi tədqiqatların aparılmasına diqqət artırılmalıdır;

- beynəlxalq əməkdaşlıq – qlobal informasiya cəmiyyəti quruculuğunda, İKT sahəsi ilə bağlı beynəlxalq layihələrin həyata keçirilməsində ölkəmiz fəal iştirak etməli, ikitərəfli və çoxtərəfli əməkdaşlıq genişləndirilməli, həyata keçirilən fəaliyyətin ümumdünya informasiya cəmiyyətinin inkişafı ilə sıx əlaqəsi təmin olunmalıdır.[21]

[21] Əliyev Ə., Rzayeva G., İbrahimova A., Məhərrəmov B., Məmmədrzalı Ş. İnformasiya hüququ. Dərslik. Bakı: "Nurlar" nəşriyyatı, 2019, 254 s.

İnformasiya siyasəti dövlət siyasətinin bir qolu olmaqla cari sahə üzrə dövlət fəaliyyətini, strateji məqsəd və proqramları ehtiva edir[22]. Demokratik və hüquqi cəmiyyətin qorunub saxlanılması, cəmiyyətin və vətəndaşların normal həyat şəraitinin təmin edilməsi, habelə informasiya təhlükəsizliyi sahəsində ümumi maarifləndirmə tədbirləri informasiya sahəsində dövlət siyasətinin əsas istiqamətlərindəndir. Belə ki, hələ ibtidai təhsildən başlayaraq, vətəndaşların savadlılıq və məlumatlılıq səviyyəsinin artırılması zəruridir və dövlətin milli strategiyalarının əsas istiqamətlərində bunu nəzərə alması vacibdir.

Təsadüfi deyildir ki, Azərbaycan Respublikası Prezidentinin 6 dekabr 2016-cı il tarixli Fərmanı ilə təsdiq edilmiş "Azərbaycan Respublikasında telekommunikasiya və informasiya texnologiyalarının inkişafına dair Strateji Yol Xəritəsi"nin Strateji Məqsədlər adlı 6-cı bəndində milli mədəni irsin qorunması, təhsil, səhiyyə, mədəniyyət sahələri üzrə geniş istifadə üçün təyin edilmiş elektron resursların inkişaf etdirilməsi və informasiya təhlükəsizliyi üzrə ümummilli hazırlıq və maarifləndirmə səviyyəsinin artırılması məqsədlər siyahısında yer alır. Mədəni dəyərlərin bəşəriyyət üçün son dərəcə vacib olduğunu nəzərə alaraq, informasiya sahəsində milli informasiya siyasətinin ayrıca bir istiqaməti kimi milli kontentin inkişaf etdirilməsinə xüsusi önəm verilməlidir. 2014-2020-ci illər üçün Milli Strategiyada nəzərdə tutulan bəzi tədbirlər – Azərbaycan tarixi, vətənpərvərlik mövzuları, ədəbi və mədəni irs üzrə internet resurslarının (rəqəmli arxivlərin) yaradılması və inkişaf etdirilməsi, milli-mədəni nailiyyətlərə, yerli xalqların və milli azlıqların adət-ənənələrinə həsr olunmuş elektron resursların formalaşdırılması və s. milli-mədəni irsin qorunub saxlanmasında əvəzsiz rola malikdir[23].

[22] Furnell S., "Information security policy compliance model in organisations". Reserach, 2016, p.11
[23] Əliyev Ə., Rzayeva G., İbrahimova A., Məhərrəmov B., Məmmədrzalı Ş. İnformasiya hüququ. Dərslik. Bakı: "Nurlar" nəşriyyatı, 2019, 448 s.

Beynəlxalq müstəvidə dövlətlərin informasiya sahəsində siyasətinin formalaşdırılması ikitərəfli və çoxtərəfli əməkdaşlıqlarda daim prioritet mövqedə olmuşdur. Belə ki, "İnformasiya cəmiyyətinə doğru: prinsiplər, strategiyalar, prioritetlər" adlı 7-9 noyabr 2002-ci il tarixində keçirilmiş 7 noyabr 2002-ci il - 9 noyabr 2002-ci il Buxarestdə (Rumıniya) İnformasiya Cəmiyyəti üzrə keçirilmiş Pan-Avropa Regional Konfransının nəticələrinə əsasən ilkin müddəalar qəbul edilmişdir[24]. Bu bəyannamədə başlıca olaraq, informasiya cəmiyyətinin aşağıdakı prinsipləri öz əksini tapmışdır:

- informasiya və biliklərin əlyetərliyi;
- münasib qiymətlərlə universal əlyetərliyin təşviqi;
- linqvistik müxtəliflik və mədəni irsin təşviqi;
- təhsil və peşəkar hazırlıq yolu ilə insan potensialının inkişafı;
- stimullaşdırıcı mühitin yaradılması;
- İKT-dən istifadə üzrə təhlükəsizliyin və etimadın möhkəmləndirilməsi; qlobal məsələlərin həlli.

Qeyd edilənlərlə yanaşı, Buxarest Bəyannaməsində elektron strategiyalarla bağlı ümumi müddəalar da öz əksini tapmışdır. Göstərilir ki, bu strategiyaların səmərəliliyi üçün onlar zaman hədlərinə malik olmalı, planlaşdırılan proqramların icrasına nəzarət mexanizmləri işlənib hazırlanmalı, bu strategiyalar həm kəmiyyət, həm də keyfiyyət meyarları ilə xarakterizə olunmalıdır.

Müasir dövrün obyektiv gerçəkliyinin ümumi dövlət siyasətinə uyğunlaşdırılması məqsədilə "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair Milli Strategiyanın həyata keçirilməsi üzrə 2016-

[24] https://digital.gov.ru/ru/events/841/

2020-ci illər üçün Dövlət Proqramı" qəbul edilmişdir. Həmin dövlət proqramında "Azərbaycan həqiqətlərinin virtual məkanda təbliği və yayılmasının genişləndirilməsi üzrə tədbirlər görülməsi" milli kontentin inkişaf etdirilməsi üzrə tədbirlər sırasında qeyd olunmuşdur.

Azərbaycan Respublikasında informasiya sahəsində dövlət siyasətinin ümumi təzahürlərinə aşağıdakılar aid edilə bilər:

- "Azərbaycan Respublikasının inkişafı naminə informasiya və kommunikasiya texnologiyaları üzrə Milli Strategiya (2003 – 2012-ci illər)";
- "Açıq Hökumətin təşviqinə dair 2012 – 2015-ci illər üçün Milli Fəaliyyət Planı";
- "Elektron Azərbaycan Dövlət Proqramı" və onun icrası;
- AR-da "İnformasiyakommunikasiya texnologiyaları ili"nin elan edilməsi;
- AR Prezidenti yanında Vətəndaşlara Xidmət və Sosial İnnovasiyalar üzrə Dövlət Agentliyi və onun tabeliyində "ASAN xidmət" mərkəzlərinin yaradılması;
- "Elektron hökumət" portalının yaradılması;
- Trans Avrasiya Super İnformasiya Magistralı - TASİM layihəsi;
- İnformasiya Texnologiyalarının İnkişafı Dövlət Fondu və "Yüksək Texnologiyalar Parkı";
- "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014 – 2020-ci illər üçün Milli Strategiya" və onun əsas istiqamətlərinin həyata keçirilməsi;
- "Elektron Hökumət 2016" hesabatında Azərbaycanın yüksələn xətt üzrə inkişafı;
- "Açıq hökumətin təşviqinə dair 2016 – 2018-ci illər üçün Milli Fəaliyyət Planı" və onun icrası;

- “Elektron Hökumət 2018” (“E-Government Survey 2018”) hesabatında Azərbaycanın inkişafına müsbət yanaşma.

“Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023 – 2027-ci illər üçün Strategiyasında qeyd edildiyi kimi, qloballaşan dünyada informasiya təhlükəsizliyinin və kibertəhlükəsizliyin təmin olunması istər milli, istərsə də beynəlxalq səviyyədə əsas məsələyə çevrilmişdir. Bu fəaliyyətdə insan, cəmiyyət və dövlət maraqlarının qorunması başlıca məqsəddir. Son zamanlar Azərbaycanın informasiya məkanına, o cümlədən onun tərkib hissələrinə (dövlət, özəl və qeyri-hökumət qurumlarının, fiziki şəxslərin sahib olduğu informasiya ehtiyatlarına və infrastrukturlarına, bu ehtiyatlarda olan məlumatların həyat boyu proseslərinə, həmin proseslər üçün istifadə olunan maddi və qeyri-maddi obyektlərə və onlar arasında əlaqələrə) qarşı texnoloji cəhətdən çoxşaxəli hücumlar genişlənməkdədir.

Azərbaycan Respublikasında informasiya təhlükəsizliyi informasiya sahəsində milli təhlükəsizliyə təhdidləri müəyyən etmək, bu təhdidlərin istifadə edə biləcəyi zəifliklərin, boşluqların və təhdid nəticəsində yarana bilən fəsadların aradan qaldırılması və ya əvvəldən təyin edilmiş hədlərə qədər azaldılması üçün hüquqi, təşkilati, əməliyyat-axtarış, kəşfiyyat və əks-kəşfiyyat, elmi-texniki və təhsil, informasiya-təhlil, kommunikasiya, kadr təminatı, iqtisadi və digər sahələr üzrə tədbirləri əlaqələndirilmiş qaydada təşkil, icra, nəzarət və davamlı təkmilləşdirmək üçün qanunvericiliklə müəyyən edilən mühafizə üsulları və vasitələri ilə təmin edilir. Strategiya informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində Azərbaycan Respublikasında ilk strategiya olmaqla, ölkədə informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə dövlət siyasətinin tərkib hissəsidir və bu sahədə fəaliyyətin əsas məqsədlərini, prinsiplərini, istiqamətlərini və prioritet vəzifələrini müəyyən edir. Strategiyada qeyd olunan

məsələlər həm milli, həm də ümumbəşəri xarakter daşıyır, insanların, cəmiyyətin və dövlətin maraqlarını nəzərə alaraq, dövlət, özəl və qeyri-hökumət təşkilatlarına, fiziki şəxslərə şamil edilir. İnsanların, cəmiyyətin və dövlətin həyati əhəmiyyətli bütün maraqlarının daha yüksək və təkmil səviyyədə qorunması hazırda həm də ölkənin informasiya təhlükəsizliyi və kibertəhlükəsizlik siyasətinin əsas məqsədi kimi müəyyənləşdirilir və onun dinamik inkişaf tələblərinə cavab verməsi nəzərdə tutulur. Strategiyada informasiya, informasiyalaşdırma və informasiyanın mühafizəsi sahəsində münasibətləri tənzimləyən Azərbaycan Respublikasının qanunlarında, digər müvafiq normativ hüquqi aktlarda, həmçinin texniki normativ hüquqi aktlarda müəyyən olunmuş anlayışlardan istifadə edilir.

"Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023-2027-ci illər üçün Strategiyası"nda aşağıdakı prioritetlər müəyyənləşdirilmişdir:

- Prioritet 1.Təhdidlərin müəyyənləşdirilməsi və risklərin idarə edilməsi
- Prioritet 2. İnformasiya təhlükəsizliyi hadisələrinin aşkarlanması tədbirlərinin və mühafizə texnologiyalarının gücləndirilməsi
- Prioritet 3. İnformasiya məkanının informasiya təhlükəsizliyinin təmin olunması səviyyəsinin yüksəldilməs
- Prioritet 4. Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi
- Prioritet 5. Kibercinayətkarlığa qarşı mübarizə, o cümlədən kiberkriminalistika sahəsində fəaliyyətin gücləndirilməsi
- Prioritet 6. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində potensialın gücləndirilməsi, institusional bazanın inkişaf etdirilməsi

- Prioritet 7. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində normativ bazanın təkmilləşdirilməsi
- Prioritet 8. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik mədəniyyətinin yüksəldilməsi
- Prioritet 9. İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə ölkədaxili və beynəlxalq əməkdaşlığın inkişaf etdirilməsi.

Ölkənin informasiya sahəsində milli təhlükəsizlik maraqlarından bəhs edərkən qeyd etmək lazımdır ki, Azərbaycan Respublikasının müstəqilliyini, ərazi bütövlüyünü, konstitusiya quruluşunu, xalqın və ölkənin milli maraqlarının daxili və xarici təhdidlərdən qorumağa yönəlmiş siyasətin məqsəd, prinsip və yanaşmalarının müəyyən edilməsi məqsədilə Azərbaycan Respublikası Prezidentinin 23 may 2007-ci il tarixli 2198 nömrəli Sərəncamı ilə "Azərbaycan Respublikasının milli təhlükəsizlik konsepsiyası"nın ilə təsdiq edilmişdir. Konsepsiyada qeyd olunur ki, Azərbaycan Respublikasının milli təhlükəsizliyinin təmin edilməsində əsas vəzifələrdən biri onun milli təhlükəsizliyinə təhdidlərin aradan qaldırılması və ya nəzarətdə saxlanılması təşkil edir. Həmin konsepsiyanın 4.3.11-ci yarımbəndində "İnformasiya təhlükəsizliyi" siyasətinə yer verilmişdir. Burada deyilir ki, Azərbaycan Respublikasının informasiya təhlükəsizliyi siyasəti dövlət, ictimai və fərdi informasiya ehtiyatlarının qorunmasına, habelə informasiya sahəsində milli maraqların müdafiəsinə yönəlmiş tədbirlər kompleksinin həyata keçirilməsindən ibarətdir. Habelə, qeyd olunur ki, Azərbaycan Respublikasının informasiya sahəsində milli təhlükəsizliyinin təmin olunması üçün ölkədə informasiyanın, həmçinin dövlət informasiya ehtiyatlarının müdafiəsi sahəsində milli sistem və informasiya infrastrukturu inkişaf etdirilir və möhkəmləndirilir. Dövlət orqanları və vəzifəli şəxslər tərəfindən qərarların qəbul edilməsinin

informasiya təminatının həyata keçirilməsi məqsədilə obyektiv və mühüm məlumatlar toplanılır.

Konsepsiyada o da vurğulanmışdır ki, kəşfiyyat və əks-kəşfiyyat qabiliyyətinin uzlaşdırılması və səmərəliliyinin artırılması, habelə məxfi informasiyanın mühafizə olunmasının koordinasiyası milli təhlükəsizlik sektorunun bu sahəsində əsas məsələlərdəndir. Azərbaycan Respublikası öz milli kəşfiyyat və əks-kəşfiyyat qabiliyyətini artıracaq və dövlət sirrinə aid edilmiş məlumatların mühafizəsi ilə bağlı fəaliyyətin təkmilləşdirilməsini davam etdirəcəkdir.

Konsepsiyada qeyd olunur ki, informasiya təhlükəsizliyini tənzimləmək məqsədilə dövlət sirri təşkil edən məlumatların mühafizəsinin hüquqi mexanizmləri təkmilləşdirilir və informasiya azadlığı təmin olunur. Bununla yanaşı, hüquqi və inzibati mexanizmlərin vətəndaşların hüquqlarını və dövlət strukturlarının fəaliyyəti üzərində demokratik nəzarəti təmin edəcəyi vurğulanır.[25]

Əlavə olaraq, qeyd etmək lazımdır ki, "Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının Qanununun 20-ci maddəsi Azərbaycan Respublikasının informasiya sahəsində milli təhlükəsizliyinin təmin olunmasına həsr olunmuşdur. Burada qeyd edilir ki, Azərbaycan Respublikasının informasiya sahəsində milli təhlükəsizliyinin təmin olunması dövlət, ictimai və fərdi informasiya ehtiyatlarının qorunmasına, habelə informasiya sahəsində milli maraqların müdafiəsinə yönəlmiş tədbirlər kompleksinin həyata keçirilməsidir.

Azərbaycan Respublikasının informasiya sahəsində milli təhlükəsizliyinin təmin olunması üçün görülən əsas tədbirlər qismində aşağıdakılar sadalanır: Azərbaycan Respublikasında informasiyanın, həmçinin dövlət informasiya

[25] 2198 - Azərbaycan Respublikasının milli təhlükəsizlik konsepsiyasının təsdiq edilməsi haqqında (e-qanun.az)

ehtiyatlarının müdafiəsi sahəsində milli sistemin yaradılması və möhkəmləndirilməsi; dövlət orqanları və vəzifəli şəxslər tərəfindən qərarların qəbul edilməsinin informasiya təminatının həyata keçirilməsi məqsədilə obyektiv və qabaqlayıcı məlumatların toplanılması; informasiya infrastrukturunun inkişaf etdirilməsi; dövlət sirlərinin qorunmasının hüquqi mexanizmlərinin təkmilləşdirilməsi; kibercinayətlərə qarşı mübarizə; informasiya təhlükəsizliyinin və azadlığının təmin olunması. [26]

[26] 712-IIQ - Milli təhlükəsizlik haqqında (e-qanun.az)

# Mövzu 3.

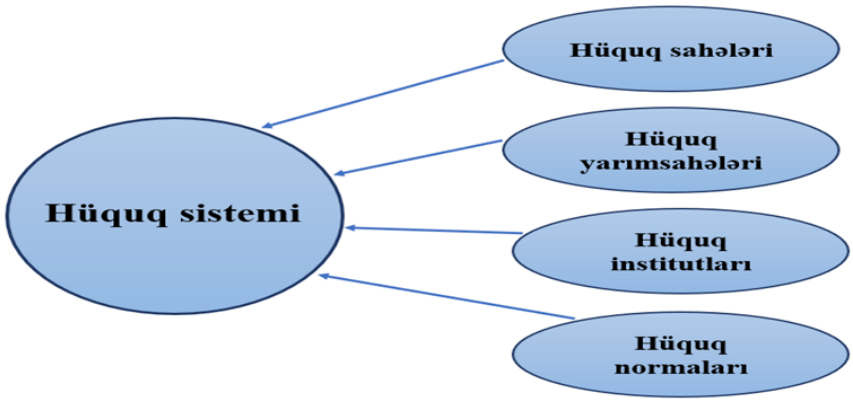
## İnformasiya təhlükəsizliyi və kibertəhlükəsizliklə bağlı rəhbər normativ hüquqi aktlar

Azərbaycan Respublikasında informasiya təhlükəsizliyi və kibertəhlükəsizliklə bağlı qüvvədə olan normativ hüquqi aktlar barədə ətraflı məlumat verilməsindən öncə ölkəmizdə mövcud hüquq sistemi və hüquqi aktlarla bağlı bir sıra terminlərə qısa izah verilməsi labüddür.

"Hüquq sistemi" dedikdə, hüququn tərkib elementi olan qanunvericilik aktlarının, normalarının və hüququn bütün elementlərinin vahid sistemdə birləşməsi və uzlaşması nəzərdə tutulur. Hüquq sistemi hüquq normalarının nizamsız toplusu deyil, yəni hər bir sahə ilə bağlı qəbul edilən qanunlar, digər hüquqi aktlar bir-biri ilə ziddiyyət təşkil etməməli, əksinə vahid sistemin ayrılmaz elementinə çevrilməli və qarşılıqlı formada mövcud hüquqi vəziyyətin inkişafını təmin etməlidir. Dünyada bir sıra fərqli hüquq sistemləri mövcuddur ki, onlardan da ən geniş yayılmış hüquq sistemlərinə Roman-German (Kontinental), Anqlo-Sakson (İngilis sakson) və dini (müsəlman) hüquq sistemlərini aid etmək olar [27]. Azərbaycan Respublikası Roman-German hüquq sisteminə daxil olan dövlətlərdəndir və bu səbəbdən milli hüquq sistemində hüququn mənbələri dedikdə, konstitusion əsaslara söykənən qanunvericilik aktları nəzərdə tutulur.

Bütün ölkələrdə olduğu kimi, Azərbaycan Respublikasında da qanunvericilik sisteminin formalaşdırılması, insanların hüquq və azadlıqlarının müdafiəsi və əhali arasında hüquqi mədəniyyət səviyyəsinin artırılması həmin ölkədəki hüquq sistemindən birbaşa asılıdır. Azərbaycan Respublikasında hüquq sisteminin klassifikasiyası aşağıdakı şəkildə göstərilmişdir:

[27] Presser S., "Anglo-saxon law", Research, 2014, 18 p.




**Hüquq sahəsi** - cəmiyyət həyatının konkret bir sahəsində mövcud olan ictimai münasibətləri nizamlayan və bir-biri ilə qarşılıqlı əlaqədə olan hüquq normalarının məcmusudur. Hüquq sahələrinə konstitusiya hüququ, inzibati hüquq, maliyyə hüququ, aqrar hüququ, mülki hüquq, ailə hüququ, əmək hüququ, cinayət hüququ, mülki-prosessual hüquq, cinayət-prosessual hüquq, informasiya hüququ və digər hüquq sahələri aiddir.

**Hüquq yarımsahəsi –** hüquq sahəsi daxilində konkret bir mövzuya qaydalar toplusuna və ya hüquqi prinsiplərə diqqət yetirən ixtisaslaşdırılmış sahədir. Yəni, hüquq sahəsi daha geniş anlayışdır və tərkibində fərqli hüquq münasibətlərilə bağlı bir sıra hüquq yarımsahələri mövcuddur. Məsələn, informasiya hüququnun yarımsahəsinə fərdi məlumatların mühafizəsi ilə bağlı qanunvericilik aktlarını nümunə göstərmək olar.

**Hüquq institutu** – eynicinsli ictimai münasibətlər qrupunu nizama salan hüquq normalarının məcmusudur. Hüquq normaları təkbaşına deyil, hüquq institutları vasitəsilə hüquq sahələrini yaradırlar. Yəni, normaların birləşməsindən hüquq institutları və hüquq institutlarının əsasında isə hüquq sahələri yaranır.

**Hüquq norması** – cəmiyyət daxilində davranış qaydalarını tənzimləmək, mübahisələri həll etmək və nizam-intizamı qorumaq, bir sözlə hüquq

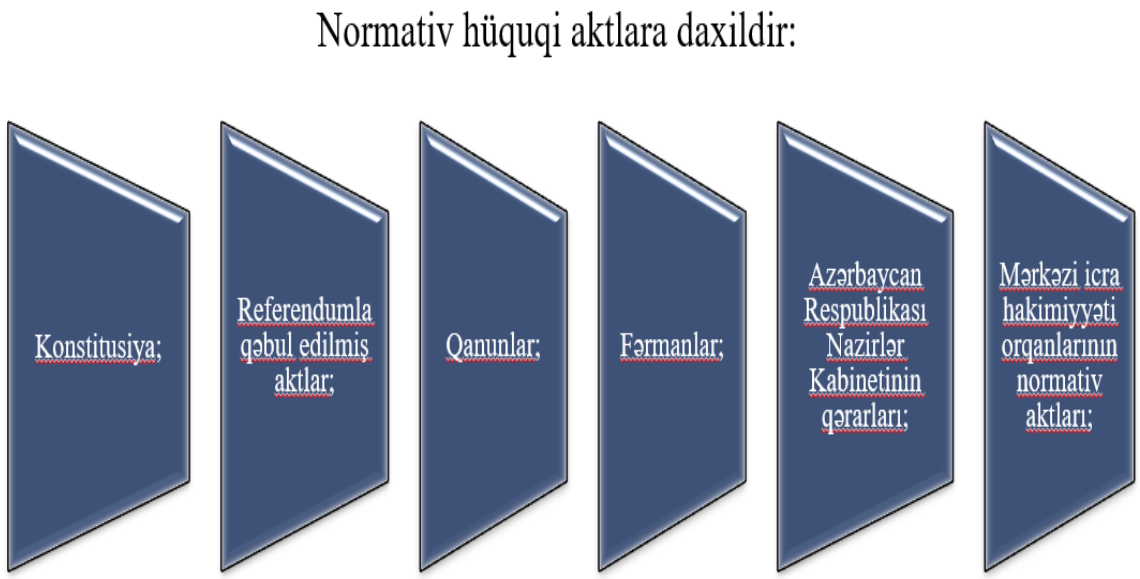
mədəniyyətini formalaşdırmaq üçün hüquq sistemi tərəfindən müəyyən edilən və tətbiq edilən qayda, prinsip və ya standartlardır. Bütün hüquq münasibətlərinin bazisini hüquq normaları təşkil edir. Hüquq normasının əlamətlərinə aiddir:

- Dövlət tərəfindən yaradılır və sanksiyalaşdırılır;
- İnsanlara hüquq və azadlıqlarını müdafiə etmə ixtiyarı verdiyi kimi eyni zamanda, insanları müəyyən davranış və əməllərdən çəkindirmə üçün yaradılıb tətbiq edildiyi üçün səlahiyyətverici və ya məcburedici xarakter daşıyır;
- Realizəsi insanlar tərəfindən şüurlu qaydada mümkün olmadıqda dövlət tərəfindən görülən tədbirlər nəticəsində həyata keçirilir;
- İctimai münasibətləri istiqamətləndirir və tənzimləyir.

"Normativ hüquqi aktlar haqqında" 21 dekabr 2010-cu il Azərbaycan Respublikası Konstitusiya Qanununun 1-ci maddəsinə əsasən qanunvericilik aktları dedikdə Azərbaycan Respublikasının qanunvericilik sistemini təşkil edən normativ hüquqi aktlar nəzərdə tutulur. Eyni zamanda, sözügedən qanunda hüquqi aktların normativ hüquqi akt, normativ xarakterli akt və ya qeyri-normativ hüquqi akt olaraq üç yerə ayrılması da qeyd edilmişdir.

Ümumilikdə, hüququn geniş və mürəkkəb mənzərəsinə nəzər saldıqda normativ hüquqi aktların cəmiyyətin hüquqi çərçivəsinin strukturunu, istiqamətini və icrasını təmin edən dayaq rolunu oynadığı qənaətinə gəlmək mümkündür. Bu zaman sual yaranır ki, normativ hüquqi akt dedikdə nə nəzərdə tutulur və normativ hüquqi aktlara nələr daxildir? "Normativ hüquqi aktlar haqqında" 21 dekabr 2010-cu il Azərbaycan Respublikası Konstitusiya Qanununun 1-ci maddəsi normativ hüquqi aktlara aşağıdakı kimi anlayış verir:

**Normativ hüquqi akt** – tənzimlənməsi Azərbaycan Respublikasının Konstitusiyası ilə, qanunla və ya fərmanla dövlət orqanının səlahiyyətlərinə aid edilən məsələlər üzrə həmin dövlət orqanı tərəfindən və ya referendum yolu ilə qəbul edilmiş, hamı üçün məcburi davranış qaydalarını əks etdirən, qeyri-müəyyən subyektlər dairəsi üçün və dəfələrlə tətbiq olunmaq üçün nəzərdə tutulmuş müəyyən formalı rəsmi sənəddir. Belə ki, Azərbaycan Respublikası Konstitusiyasının 148-ci maddəsinə müvafiq olaraq, qanunvericilik sistemi aşağıdakı şəkildə qeyd edilmiş normativ hüquqi aktlardan ibarətdir:




◊ Qanun – hüquq normalarının sistemli toplusu olub ictimai münasibətləri tənzimləməyə və hüquq mədəniyyətini formalaşdırmağa və təkmilləşdirməyə xidmət edir.

◊ Fərman – bütün əhali və ya əhalinin böyük bir hissəsi üçün, yəni ümumi məsələlərlə bağlı yalnız ölkə başçısı tərəfindən verilən qanunvericilik aktıdır. Fərmanlar yazılı formada olur, dərc edildiyi, yayıldığı gündən qüvvəyə minir.

◊ Sərəncam – konkret məsələlərlə üçün bir və ya bir neçə şəxslə bağlı həm ölkə başçısı həm də, digər səlahiyyətli şəxslər tərəfindən verilən qanunvericilik aktıdır.

Azərbaycan Respublikasının qanunvericiliyi kibermühitdə törədilən hüquq pozuntularına milli təhlükəsizlik konteksindən yanaşmışdır. Belə ki, "Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının qanununun 20-ci maddəsində informasiya sahəsində milli təhlükəsizliyin təmin edilməsinin anlayışı verilmişdir. Burada dövlət, cəmiyyət və fərdi informasiya resurslarının mühafizəsinə, həmçinin informasiya sahəsində milli maraqların qorunmasına yönəlmiş tədbirlər kompleksinin həyata keçirilməsi milli təhlükəsizliyin təmin edilməsi kimi qəbul edilmişdir.

İnformasiya təhlükəsizliyi və kiber mühitdə dövlət tənzimetməsi ilə bağlı digər vacib məsələ isə xüsusi təyinatli telekommunikasiya şəbəkələrinin təhlükəsizliyinin təmin edilməsidir. Azərbaycan Respublikasının "Dövlət hakimiyyəti orqanlarının xüsusi təyinatlı telekommunikasiya şəbəkələrinin qurulması, istismarı, təhlükəsizliyinin təmin edilməsi, onlara sərəncam verilməsi Qaydası"nın təsdiq edilməsi haqqında Nazirlər Kabinetinin Qərarının 4-cü bəndinə əsasən dövlət orqanları xüsusi təyinatlı telekommunikasiya şəbəkələrinin təhlükəsizliyini təmin etmək məqsədilə öz səlahiyyətləri çərçivəsində dövlət hakimiyyəti orqanlarının binalarında və mülkiyyət formasından asılı olmayaraq digər təşkilatlarda xüsusi təyinatlı telekommunikasiya şəbəkələrinə aid olan vasitə və qurğularda informasiya təhlükəsizliyinin təminatı üzrə işləri təşkil edir və yerinə

yetirirlər, habelə dövlət informasiya ehtiyatlarının mühafizəsi sahəsində milli sistemin yaradılmasını və möhkəmləndirilməsini həyata keçirirlər.

Kritik informasiya infranstrukturunun ölkə üçün əhəmiyyətini nəzərə alaraq onun kibermühafizəsi naminə hüquqi və texniki tədbirlərin təkmilləşdirilməsi məqsədilə 17 aprel 2021-ci il tarixində Azərbaycan Respublikasının Prezidenti tərəfindən Fərman imzalanmışdır. Həmin Fərmanda vurğulanır ki, dövlət əhəmiyyətli məsələlərin həlli üçün müvafiq informasiya infrastrukturlarının yaradılmasıyla həmin infrastrukturların qlobal informasiya şəbəkələrinə, o cümlədən internet şəbəkəsinə daxil edilməsi infrastruktur obyektlərinin kiberhücumların hədəfinə çevrilməsinə səbəb olur. Bütün bunlar dövlətin, cəmiyyətin və fərdlərin maraqları baxımından vacib hesab edilən məsələlərin həlli məqsədilə yaradılan kritik informasiya infrastrukturuna daxil olan sistem və şəbəkələrin sıradan çıxarılması və ya funksionallığının pozulması, eyni zamanda ciddi ziyan vurulması ilə nəticələnir ki, bu, kritik informasiya infrastrukturunun kibertəhlükəsizliyinə prioritet məsələ kimi baxılmasını zəruri edir. Fərmana əsasən müəyyən edilir ki, kritik informasiya infrastrukturunun (mühafizə olunan şəxslərin və qorunan obyektlərin informasiya infrastrukturu istisna olmaqla) təhlükəsizliyinin təmin edilməsi, həmçinin gələcəkdəki qanun layihələri Nazirlər Kabineti tərəfindən kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsinin hüquqi tənzimlənməsi məqsədilə müvafiq normativ hüquqi aktların layihələrini səlahiyyətli orqanların təklifləri əsasında işlənib hazırlanıb Azərbaycan Respublikasının Prezidentinə təqdim edilməlidir.

Azərbaycan Respublikasında kibercinayətkarlıqla mübarizə məqsədilə cinayət-hüquqi sferada həyata keçirilən tədbirlərlə bağlı qeyd olunmalıdır ki, 29 iyun 2012-ci il tarixli 408-IVQD nömrəli “Azərbaycan Respublikasının Cinayət Məcəlləsində dəyişikliklər edilməsi haqqında” Azərbaycan Respublikasının

Qanunu ilə Cinayət Məcəlləsinin otuzuncu fəsli Konvensiyaya uyğunlaşdırılaraq yeni redaksiyada verilmiş, habelə Məcəlləyə uşaq pronoqrafiyasının dövriyyəsi ilə bağlı cinayət məsuliyyətinin əsaslarını müəyyən edən yeni bir maddə (Maddə 171-1) əlavə olunmuşdur. Eyni zamanda, bir sıra əməllərə görə cinayət məsuliyyəti müəyyən edən maddələrdə cinayətin obyektiv cəhətində kiber elementlərin ehtiva olunmasının da ayrılıqda nəzərdə alınması üçün müvafiq dəyişikliklər həyata keçirilmiş və əlavələr olunmuşdur. Məsələn, oğurluq əməlinin "elektron məlumat daşıyıcılarından, yaxud informasiya texnologiyalarından" istifadə edilməklə törədilməsinin ağırlaşdırıcı tərkib əlaməti kimi nəzərdə tutulması ilə bağlı 30 aprel 2013-cü il tarixli 633-IVQD nömrəli "AzərbaycanRespublikasının Cinayət Məcəlləsində dəyişiklik edilməsi haqqında"Azərbaycan Respublikasının Qanunu ilə Cinayət Məcəlləsinə 177.2.3-1-ci maddə əlavə edilmişdir.

3 avqust 2004-cü il tarixli "**Milli təhlükəsizlik haqqında**" Azərbaycan Respublikasının Qanununa əsasən, Azərbaycan Respublikasının informasiya sahəsində əsas milli maraqları aşağıdakılardır: məlumatların qanuni yolla əldə edilməsi, ötürülməsi, hazırlanması və yayılması kimi vətəndaşların konstitusiya hüquqlarının təmin edilməsi; informasiya ehtiyatlarının qorunması və inkişaf etdirilməsi; informasiya məkanının formalaşdırılması və onun qorunmasının təmin edilməsi; dünya rabitə və informasiya sisteminə daxil olma.

5 iyun 1996-cı il tarixli **"Müəlliflik hüququ və əlaqəli hüquqlar haqqında"** Azərbaycan Respublikasının Qanuna əsasən, Azərbaycan Respublikası ərazisində elm, ədəbiyyat və incəsənət əsərlərinin (müəlliflik hüququ), habelə ifaların, fonoqramların, efir və ya kabel yayımı təşkilatlarının verilişlərinin (əlaqəli hüquqlar) yaradılması və istifadəsi ilə əlaqədar yaranan münasibətləri tənzimləyir. Müəllif hüquqlarının pozulması müəllif hüququ təsdiqlənmiş hər hansı bir mülkiyyətdən hüquq sahibinin icazəsi olmadan müəllif hüququ təsdiqlənmiş

mülkiyyətin və ya işin təkrar istehsal, dəyişiklik edilmə kimi xüsusi haqlarını pozmaqla istifadəsini nəzərdə tutur. Bir çox hallarda müəllif hüququ pozuntusu oğurluqla eyniləşdirilir lakin müəyyən mənada onlar fərqlidir. İstər oğurluq istərsə də müəllif hüququ pozuntusu müəyyən maddi ziyana səbəb olsa da burada əsas fərq 2-ci halda əsl sahibin istifadə hüququnu itirməməsi və hələ də obyektdən istifadə edə bilməsidir.

3 aprel 1998-ci il tarixli "**İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında**" Azərbaycan Respublikasının Qanununa əsasən, bu Qanun informasiyanın yığılması, işlənməsi, saxlanması, axtarışı, yayılması əsasında informasiya ehtiyatlarının formalaşdırılması, informasiya sistemləri, texnologiyaları, onların təminat vasitələrinin yaradılması və onlardan istifadə olunması, informasiyanın mühafizəsi ilə əlaqədar olaraq yaranan münasibətləri tənzimləyir və informasiya proseslərində iştirak edən subyektlərin hüquqlarını müəyyən edir. “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Qanununun “Əsas anlayışlar” adlı 2-ci maddəsinin müvafiq bəndlərində “informasiya təhlükəsizliyi” “kibertəhdid”, “kiberhücum”, “kiberinsident”, “kritik informasiya infrasturkturu” və s. terminlərə əhatəli anlayış verilmişdir. Müvafiq bəndlərə əsasən, “informasiya təhlükəsizliyi” dedikdə, informasiyanın tamlığının (dəqiq, səlis, aktual və bütöv olması), əlçatanlığının (müraciət və əldə etmənin, nəzarətdə saxlamanın mümkün olması), konfidensiallığının (yalnız səlahiyyəti olan istifadəçilər və proseslər üçün məlum ola bilməsi) və mötəbərliliyinin (adekvat, obyektiv, faydalı olması) mühafizə edilməsi başa düşülür. Qanunverici “kibertəhdid” terminində informasiya sistemlərinə və ya ehtiyatlarına qanunsuz daxil olma, müdaxilə, habelə digər formalarda informasiya təhlükəsizliyinin pozulmasına səbəb ola bilən amil və ya vəziyyət, “kiberhücum” terminində informasiya sistemlərinin və ya ehtiyatlarının

informasiya təhlükəsizliyinə təhdid yaradan, yaxud onların fəaliyyətinin pozulmasına və ya dayanmasına səbəb olan kibermәkan vasitəsilə qəsdən törədilən əməl və nəhayət, “kiberinsident” terminina, informasiya sistemlərinin, avtomatlaşdırılmış idarəetmə sistemlərinin və informasiya-kommunikasiya şəbəkələrinin fəaliyyətinin dayanması və ya pozulması, yaxud həmin obyektlərdə informasiya təhlükəsizliyinin pozulmasına səbəb olan hadisə kimi anlayış vermişdir.

4 dekabr 2001-ci il tarixli “**Kommersiya sirri haqqında**” Azərbaycan Respublikasının Qanuna əsasən, bu Qanun Azərbaycan Respublikasında kommersiya sirri ilə əlaqədar yaranan münasibətləri tənzimləyir. Azərbaycan Respublikasında bütün hüquqi və fiziki şəxslərin kommersiya sirrini təşkil edən məlumatlarının, onların ifadə edilməsi üsulundan və daşıyıcısından asılı olmayaraq qorunma hüququ vardır. Kommersiya sirrindən dövlətin, hüquqi və fiziki şəxslərin qanuni mənafelərinin ziddinə istifadə edilə bilməz.

9 mart 2004-cü il tarixli "**Elektron imza və elektron sənəd haqqında**" Azərbaycan Respublikasının Qanununa əsasən, bu Qanun elektron imzanın və elektron sənədin istifadəsinin, onların elektron sənəd dövriyyəsində tətbiqinin təşkilati, hüquqi əsaslarını və əlaqədar subyektlərin hüquqlarım müəyyən edir, aralarında yaranan münasibətləri tənzimləyir. Elektron imza və elektron sənədin hüquqi qüvvəsi ilə bağlı deyə bilərik ki, Elektron formada və ya sertifikatsız olduğuna, sertifikatlaşdırılmamış imza vasitələri ilə yaradıldığına görə elektron imza etibarsız sayıla bilməz. Azərbaycan Respublikasının qanunvericiliyində nəzərdə tutulmuş hallar istisna olmaqla, sertifikatlaşdırılmış imza vasitələri ilə yaradılmış və qüvvədə olan təkmil sertifikatlı gücləndirilmiş imza əl imzası ilə bərabər hüquqi qüvvəyə malikdir. Təkmil sertifikatda imza sahibinin səlahiyyətlərinə dair məlumatlar göstərildikdə bu Qanunun 3.2-ci maddəsinə

müvafiq olan gücləndirilmiş imza şəxsin kağız daşıyıcısı üzərindəki və möhürlə təsdiq edilmiş əl imzasına bərabər tutulur. Azərbaycan Respublikasının qanunvericiliyi ilə sənədin yazılı şəkildə təqdim olunması tələb olunduqda bu Qanunun 3.2-ci, 3.3-cü maddələrinə müvafiq qaydada imzalanmış elektron sənəd bu şərtlərə cavab verən hesab edilir. Azərbaycan Respublikasının qanunvericiliyi ilə sənədin notariat qaydasında təsdiqi və (və ya) dövlət qeydiyyatı tələb olunduğu hallar istisna olmaqla, elektron sənəd kağız daşıyıcıda olan sənədə bərabər tutulur və onunla eyni hüquqi qüvvəyə malikdir. Azərbaycan Respublikasının qanunvericiliyi ilə sənədin notariat qaydasında təsdiqi və ya dövlət qeydiyyatı tələb olunduqda elektron sənəd və ya onun bu Qanunun 25.1-ci maddəsinin tələblərinə cavab verən surəti Azərbaycan Respublikasının qanunvericiliyinə müvafiq olaraq qeydiyyata alınır və ya təsdiq edilir.

7 sentyabr 2004-cü il tarixli "**Dövlət sirri haqqında**" Azərbaycan Respublikasının Qanununa əsasən, bu Qanun Azərbaycan Respublikasının təhlükəsizliyini təmin etmək məqsədilə məlumatların dövlət sirrinə aid edilməsi, mühafizəsi və istifadə edilməsi, onların məxfiləşdirilməsi və ya məxfiliyinin açılması ilə əlaqədar yaranan münasibətləri tənzimləyir. Dövlət sirri dedikdə, dövlət orqanının məxfiliyinin , bütövlüyünün və ya mövcudluğunun qorunmasını tələb edən həssas məlumatdır. Bu cür məlumatlara giriş qanun və ya qaydalarla məhdudlaşdırılır və yalnız icazəsi və səlahiyyəti olan şəxslər tərəfindən əldə edilə bilər. Dövlətin hərbi, xarici-siyasi, iqtisadi, kəşfiyyat, əks-kəşfiyyat və əməliyyat-axtarış fəaliyyəti ilə bağlı olub, dövlət tərəfindən mühafizə edilən və yayılması Azərbaycan Respublikasının təhlükəsizliyinə ziyan vura bilən məlumatlardır; Dövlət sirri təşkil edən məlumatların daşıyıcıları − dövlət sirri təşkil edən məlumatların rəmzlər, obrazlar, siqnallar, texniki qərarlar və proseslər şəklində əks olunduğu maddi obyektlər, o cümlədən fiziki sahələrdir; Dövlət sirrinin mühafizəsi

sistemi − dövlət sirrini mühafizə orqanlarının, dövlət sirri təşkil edən məlumatların və həmin məlumatların daşıyıcılarının mühafizəsi üçün bu orqanların istifadə etdikləri vasitə və metodların, habelə bu məqsədlə həyata keçirilən tədbirlərin məcmusudur.

14 sentyabr 2004-cü il tarixli "**Məlumat toplularının hüquqi qorunması haqqında**" Azərbaycan Respublikasının Qanununa əsasən, bu Qanun formasından asılı olmayaraq məlumat toplularının yaradılması və istifadəsi ilə bağlı yaranan hüquqi münasibətləri tənzimləyir.

14 iyun 2005-ci il tarixli "**Telekommunikasiya haqqında**" Azərbaycan Respublikasının Qanunu.na əsasən, bu Qanun Azərbaycan Respublikasında telekommunikasiya sahəsində fəaliyyətin hüquqi, iqtisadi, təşkilati əsaslarını müəyyənləşdirir və telekommunikasiya resurslarının məqsədyönlü planlaşdırılmasını və ədalətli istifadə olunmasını tənzimləyir.

Azərbaycan Respublikasında elektron ticarətin təşkili və həyata keçirilməsinin hüquqi əsaslarını, onun iştirakçılarının hüquq və vəzifələrini, habelə elektron ticarət haqqında qanunvericiliyin pozulmasına görə məsuliyyəti isə "**Elektron ticarət haqqında"** 10 may 2005-ci il 908 nömrəli Azərbaycan Respublikasının Qanunu müəyyən edir. Maliyyə bazarı, o cümlədən sığorta və qiymətli kağızlar bazarı istisna olmaqla, bu Qanun Azərbaycan Respublikasında bütün digər sahələrdə həyata keçirilən elektron ticarətə şamil olunur.

30 sentyabr 2005-ci il tarixli "**İnformasiya əldə etmək haqqında**" Azərbaycan Respublikasının Qanununa əsasən, bu Qanunun məqsədi Azərbaycan Respublikası Konstitusiyasının 50-ci maddəsi ilə təsbit olunmuş məlumat əldə etmək hüququnun sərbəst, maneəsiz və hamı üçün bərabər şərtlərlə, açıq cəmiyyətin və demokratik hüquqi dövlətin prinsipləri əsasında təmin edilməsinin

hüquqi əsaslarını müəyyənləşdirməkdən, həmçinin, ictimai vəzifələrin yerinə yetirilməsinə vətəndaşlar tərəfindən nəzarət olunmasına şərait yaratmaqdan ibarətdir.

13 iyun 2008-ci il tarixli "**Biometrik informasiya haqqında**" Azərbaycan Respublikasının Qanununa əsasən, bu Qanun biometrik informasiya ehtiyatlarının formalaşdırılmasını və onlara dair tələbləri, biometrik identifikasiya sisteminin fəaliyyətinin təşkili və təyinatını, biometrik texnologiyaların tətbiqi sahələrini müəyyən edir və bu sahədə yaranan münasibətləri tənzimləyir.

30 sentyabr 2009-cu il tarixli "**Kibercinayətkarlıq haqqında" Konvensiyanın təsdiq edilməsi barədə"** Azərbaycan Respublikasının Qanunu. Bu barədə geniş məlumat digər mövzularda verilmişdir.

04 iyun 2010-cu il tarixli "**Fərdi məlumatlar haqqında**" Azərbaycan Respublikasının Qanununa əsasən, bu Qanun fərdi məlumatların toplanılması, işlənilməsi və mühafizəsi ilə bağlı münasibətləri, milli informasiya məkanının fərdi məlumatlar bölümünün formalaşdırılması, habelə fərdi məlumatların transsərhəd ötürülməsi ilə əlaqədar məsələləri tənzimləyir, bu sahədə fəaliyyət göstərən dövlət və yerli özünüidarə orqanlarının, hüquqi və fiziki şəxslərin hüquq və vəzifələrini müəyyən edir. Azərbaycanın "Fərdi məlumatlar haqqında" Qanunu fərdi məlumatları şəxsin şəxsiyyətini birbaşa və ya dolayı yolla müəyyənləşdirməyə imkan verən hər hansı bir məlumat kimi müəyyənləşdirir. Qeyd etmək lazımdır ki, Qanunda göstərilən fərdi məlumatların toplanması və işlənməsi şərtləri insan orqanizminin bioloji xüsusiyyətlərini səciyyələndirən və onun kimliyini birmənalı olaraq müəyyənləşdirməyə imkan verən məlumatların — əl-barmaq və ovuc izləri, üz təsviri, gözün qüzehli və tor qişası, səs fraqmenti və onun akustik parametrləri, DNT analizinin nəticələri, bədən ölçüləri, bədənin xüsusi əlamətlərinin və qüsurlarının təsviri, yazı xətti və imzası, habelə digər biometrik məlumatların

toplanılmasına və işlənilməsinə tam həcmdə şamil edilir. Qeyd olunan qanuna əsasən fərdi məlumatlar toplandığı andan mühafizə olunur və bu məqsədlə daxilolma (əldə olunma) növünə görə konfidensial və açıq kateqoriyalara bölünür. Azərbaycanda fərdi məlumatların subyekti ona məxsus olan məlumatların məxfilik statusunu dəyişdirmək və məlumatları açıq elan etmək hüququna malikdir. Fərdi məlumatların mülkiyyətçisi və operatorlarının vəzifəsi, əldə etdikləri fərdi məlumatların qorunmasını təmin etməkdir. Bu səbəbdən hüquqi şəxslər, hansı hallarda bu məlumatların mülkiyyətçisi və ya operatoru olduqlarını müəyyənləşdirməli və məlumatların mühafizəsi qaydalarına tabe olmalıdırlar.

Yuxarıda qeyd olunanlarla yanaşı, sahə üzrə digər normativ hüquqi aktlar qismində aşağıdakılar nəzərə alına bilər:

- ◊ 29 dekabr 2004-cü il tarixli "Azərbaycan Respublikasının dövlət orqanlarında informasiya təhlükəsizliyinin təmin edilməsi üzrə tədbirlər haqqında" Azərbaycan Respublikası Prezidentinin Fərmanı;
- ◊ 23 may 2007-ci il tarixli "Azərbaycan Respublikasının milli təhlükəsizlik konsepsiyası";
- ◊ 27 avqust 2007-ci il tarixli "Tərkibində dövlət sirri təşkil edən məlumatlar olan elektron sənədlərin tərtibi, emalı və mübadiləsi üçün istifadə olunan informasiya sistemlərinin ekspertizasının keçirilməsi Qaydası"nın təsdiq edilməsi haqqında Azərbaycan Respublikasının Nazirlər Kabinetinin Qərarı;
- ◊ 28 yanvar 2006-cı il tarixli “Azərbaycan Respublikasında elektron imza və elektron sənədlə bağlı bəzi normativ hüquqi aktların təsdiq edilməsi haqqında” Azərbaycan Respublikasının Nazirlər Kabinetinin Qərarı;
- ◊ 17 may 2010-cu il tarixli “Dövlət informasiya ehtiyatlarının reyestrinin aparılması qaydaları haqqında Əsasnamə”nin təsdiq edilməsi barədə Azərbaycan Respublikasının Nazirlər Kabinetinin Qərarı;

- ◊ 26 sentyabr 2012-ci il tarixli “İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında” Azərbaycan Respublikası Prezidentinin Fərmanı
- ◊ 29 mart 2018-ci il tarixli “İnformasiya Təhlükəsizliyi üzrə Koordinasiya Komissiyasının yaradılması haqqında” Azərbaycan Respublikası Prezidentinin Sərəncamı;
- ◊ 30 oktyabr 2018-ci il tarixli “Uşaqların zərərli informasiyadan qorunması haqqında” Azərbaycan Respublikasının Qanunu;
- ◊ 17 iyul 2023-cü il tarixli “Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydaları”nın təsdiq edilməsi haqqında Azərbaycan Respublikasının Nazirlər Kabinetinin Qərarı.
- ◊ 17 iyul 2023-cü il tarixli “Kritik informasiya infrastrukturu obyektlərinin reyestrinin strukturu, yaradılması və aparılması qaydası”nın təsdiq edilməsi haqqında Azərbaycan Respublikası Nazirlər Kabinetinin Qərarı.

# Mövzu 4.

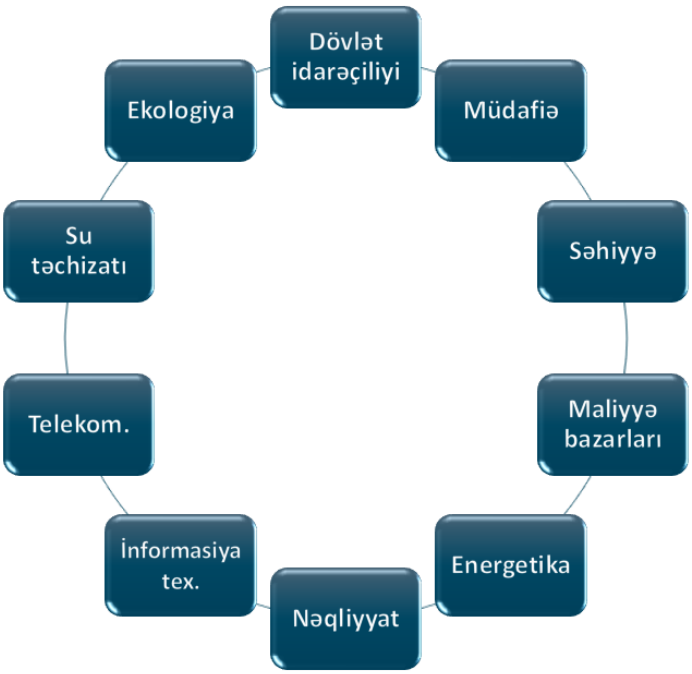
## Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin olunması sahəsində hüquqi və təşkilati məsələlər, infrastruktur obyektlərinin təsnifatlaşdırılması, minimal təhlükəsizlik tələbləri, nəzarət mexanizmləri

"Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində bəzi tədbirlər haqqında" Azərbaycan Respublikası Prezidentinin 17 aprel 2021-ci il tarixli Fərmanında qeyd edildiyi kimi, informasiya texnologiyalarının davamlı təkamülü, informasiyanın və informasiya sistemlərinin qloballaşması dövlətin və cəmiyyətin tərəqqisinə xidmət edən mühüm vasitəyə çevrilmişdir. Azərbaycan Respublikasında da informasiya texnologiyaları əsasında dövlət əhəmiyyətli məsələlərin həlli üçün müvafiq informasiya infrastrukturu yaradılmaqdadır. Həmin infrastrukturun qlobal informasiya şəbəkələrinə, o cümlədən internet şəbəkəsinə daxil edilməsi infrastruktur obyektlərinin kiberhücumların hədəfinə çevrilməsinə səbəb olur.

Dövlətin, cəmiyyətin və vətəndaşların maraqları baxımından vacib hesab edilən məsələlərin həlli məqsədilə yaradılan kritik informasiya infrastrukturuna daxil olan sistem və şəbəkələrin sıradan çıxarılması və ya funksionallığının pozulması ciddi ziyan vurulması ilə nəticələnir ki, bu da kritik informasiya infrastrukturunun kibertəhlükəsizliyinə prioritet məsələ kimi baxılmasını zəruri edir.

Qeyd etmək lazımdır ki, 27 may 2022-ci il tarixli 539-VIQD nömrəli Azərbaycan Respublikasının Qanunu ilə "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Qanuna "Kritik informasiya infrastrukturunun təhlükəsizliyi" başlıqlı yeni fəsil və sahə üzrə bir sıra anlayışlar əlavə edilmişdir. Həmin Qanuna əsasən, ***kritik informasiya infranstrukturu*** dedikdə *dövlət idarəçiliyi, müdafiə, səhiyyə, maliyyə bazarları, energetika,*

*nəqliyyat, informasiya texnologiyaları, telekommunikasiya, su təchizatı* və ya *ekologiya* sahəsində fəaliyyəti təmin edən və funksionallığının pozulması dövlətin, cəmiyyətin və vətəndaşların maraqlarına mühüm zərər vura bilən informasiya sistemlərinin, avtomatlaşdırılmış idarəetmə sistemlərinin və informasiya-kommunikasiya şəbəkələrinin məcmusu başa düşülür. Beləliklə, Azərbaycan Respublikasında **kritik informasiya infrastrukturunun** mövcud olduğu 10 sahə təsbit olunmuşdur:




Qanuna əsasən, *kritik informasiya infrastrukturu obyekti* dedikdə kritik informasiya infrastrukturunun tərkib hissəsi olan informasiya sistemi, avtomatlaşdırılmış idarəetmə sistemi və ya informasiya-kommunikasiya şəbəkəsi, *kritik informasiya infrastrukturu subyekti* dedikdə isə kritik informasiya infrastrukturu obyektinin sahibi (istifadəçisi) olan dövlət orqanları (qurumları), o cümlədən dövlətə məxsus olan hüquqi şəxslər, dövlət adından yaradılmış publik hüquqi şəxslər, habelə digər hüquqi şəxslər və ya fərdi sahibkarlar (mikro, kiçik və orta sahibkarlıq subyektləri istisna olmaqla) başa düşülür.

Eyni zamanda, qeyd etmək lazımdır ki, Qanunda ilk dəfə kibertəhlükəsizlik xidməti provayderinə də anlayış verilmişdir. Belə ki, kibertəhlükəsizlik xidməti provayderi dedikdə kibertəhlükəsizlik xidmətlərinin göstərilməsi sahəsində fəaliyyət göstərən, provayderə, onun işçi heyətinə, texnoloji resurslarına və fəaliyyət proseslərinə dair müvafiq icra hakimiyyəti orqanının müəyyən etdiyi orqan (qurum) tərəfindən müəyyən edilən tələblərə cavab verən və kritik informasiya infrastrukturu subyekti ilə bağlanılmış müqavilə əsasında onlara kibertəhlükəsizlik xidməti göstərən hüquqi şəxslər başa düşülür.

Ümumilikdə, "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Qanunun 20-1.1-ci maddəsinə əsasən, kritik informasiya infrastrukturunun təhlükəsizliyi həmin infrastrukturun təhlükəsizliyinə dair *tələblərin müəyyən edilməsi, bu tələblərə uyğunluğunun qiymətləndirilməsi və aşkar olunan uyğunsuzluqların aradan qaldırılması, həmin tələblərə müvafiq olan informasiya təhlükəsizliyini idarəetmə sisteminin tətbiq edilməsi, habelə kritik informasiya infrastrukturunun təhlükəsizliyinin təmin olunması vəziyyətinə nəzarətin* həyata keçirilməsi yolu ilə təmin edilir.

*Qanunun* ***20-2-ci maddəsinə əsasən*** Azərbaycan Respublikasında kritik informasiya infrastrukturu obyektlərinin siyahısı bir sıra tələblər nəzərə alınmaqla təsdiq edilir. Belə ki, obyektin funksionallığının pozulmasının aşağıdakı nəticələrə səbəb ola bilməsi onun kritik informasiya infrastrukturu obyekti hesab edilməsinə əsasdır:

*1. dövlətin müstəqilliyi, suverenliyi, konstitusiya quruluşu, ərazi bütövlüyü və müdafiə qabiliyyətinin pozulmasına təhlükənin, habelə ictimai təhlükəsizliyə mühüm təhdidlərin yaranması;*

*2. dövlət orqanlarının (qurumlarının) fəaliyyətinin pozulması, həyat təminatı infrastrukturunun normal fəaliyyət göstərməsinə ciddi maneələrin yaranması, nəqliyyat və kommunikasiya əlaqələrinin kəsilməsi və ya səhiyyə xidmətlərinin göstərilməsinin əhəmiyyətli dərəcədə məhdudlaşdırılması nəticəsində əhalinin mühüm təminatlardan məhrum olması;*

*3. iqtisadi və maliyyə sabitliyinin pozulması, dövlət büdcəsinin formalaşdırılmasına əhəmiyyətli zərərin vurulması;*

*4. ekoloji tarazlığın pozulması və ekoloji vəziyyətin kəskin pisləşməsi.*

Kritik informasiya infrastrukturunun təhlükəsizliyinə dair *ümumi*, eləcə də onun təyinatı və fəaliyyət xüsusiyyətlərinə müvafiq olaraq *xüsusi* tələblər və tələblər müəyyən edilir və kritik informasiya infrastrukturu obyektlərinin reyestrində yerləşdirilməsi təmin edilir.

Qeyd olunmalıdır ki, kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydaları, o cümlədən kritik informasiya infrastrukturunun təhlükəsizliyinə dair ümumi tələblər və kibertəhlükəsizlik xidməti provayderinə, onun işçi heyətinə, texnoloji resurslarına və fəaliyyət proseslərinə dair tələbləri Azərbaycan Respublikasının Nazirlər Kabinetinin 17 iyul 2023-cü il tarixli 229 nömrəli Qərarı ilə təsdiq edilmiş *"Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydaları*" ilə müəyyən edilmişdir. Adıçəkilən qaydalara əsasən kritik informasiya infrastrukturu subyektləri tərəfindən aşağıdakı **7** istiqamət/məqsəd üzrə **29** ümumi tələbə, eləcə də xüsusi tələblərə riayət edilməlidir:


Qeyd etmək lazımdır ki, kritik informasiya infrastrukturunun təhlükəsizliyi üzrə fəaliyyətin ümumi təşkili və əlaqələndirilməsi səlahiyyətli orqan tərəfindən həyata keçirilir. Qanunvericiliyə əsasən, kritik informasiya infrastrukturunun (mühafizə olunan şəxslərin və qorunan obyektlərin informasiya infrastrukturu istisna olmaqla) təhlükəsizliyinin təmin edilməsi, o cümlədən kibertəhdidlərə qarşı mübarizə sahəsində səlahiyyətli orqanın funksiyalarını *Azərbaycan Respublikasının Dövlət Təhlükəsizliyi Xidməti*, dövlət orqanlarına, dövlət adından yaradılan publik hüquqi şəxslərə, dövlətə məxsus olan hüquqi şəxslərə münasibətdə həmin funksiyaları Azərbaycan Respublikasının Dövlət Təhlükəsizliyi Xidməti Azərbaycan Respublikasının Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti ilə birgə həyata keçirir. Öz növbəsində, kritik informasiya infrastrukturu subyekti ona məxsus olan kritik informasiya infrastrukturunun təhlükəsizliyini infrastrukturun təhlükəsizliyinə dair müəyyən edilmiş ümumi və xüsusi tələblərə uyğun olaraq təmin edir.

*“Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydaları”na əsasən, k*ritik informasiya infrastrukturunun təhlükəsizliyi üzrə ümumi və xüsusi tələblərə riayət olunmasının təmin edilməsi, o cümlədən bu sahədə kritik informasiya infrastrukturu subyektlərinə kömək göstərilməsi yolu ilə dövlətin və cəmiyyətin qanunla qorunan maraqlarının mühafizəsi məqsədilə səlahiyyətli orqan və kritik informasiya infrastrukturu subyektləri tərəfindən kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi vəziyyətinə nəzarət həyata keçirilir. Həmçinin, Qaydalara əsasən müəyyən olunmuşdur ki, kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi vəziyyətinə nəzarət ümumi və xüsusi tələblərə uyğunluğun qiymətləndirilməsi və aşkar olunan uyğunsuzluqların aradan qaldırılması, bu tələblərə riayət edilməsinin yoxlanılması, kritik informasiya infrastrukturunun təhlükəsizliyinin fasiləsiz (24/7 rejimdə) monitorinqi, müdaxilə sınaqları və kənar audit yoxlamalarının aparılması vasitəsilə həyata keçirilir.

**Kİİ təhlükəsizliyinin təmin olunması vəziyyətinə nəzarət**


Əlavə olaraq qeyd edilməlidir ki, Azərbaycan Respublikası Nazirlər Kabinetinin 17 iyul 2023-cü il tarixli qərarı ilə kritik informasiya infrastrukturu

obyektlərinin reyestrinin strukturunu, yaradılması və aparılmasının hüquqi, təşkilati və texnoloji əsaslarını müəyyən edən *"Kritik informasiya infrastrukturu obyektlərinin reyestrinin strukturu, yaradılması və aparılması qaydası"* təsdiq edilmişdir.

Adıçəkilən qaydaya əsasən reyestr kritik informasiya infrastrukturu obyektləri ilə bağlı informasiya proseslərinin (məlumatların yaradılması, toplanılması, işlənilməsi, saxlanılması, axtarışı, mühafizəsi və mübadiləsi) həyata keçirilməsi, eləcə də kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi, o cümlədən kibertəhdidlərə qarşı mübarizənin həyata keçirilməsi ilə bağlı tədbirlərin planlaşdırılması və icra olunması məqsədilə təhlillərin aparılması üçün nəzərdə tutulan informasiya sistemidir.

Reyestrin ***operatoru*** *Azərbaycan Respublikası Dövlət Təhlükəsizliyi Xidmətinin Kibertəhlükəsizlik Əməliyyatları Mərkəzidir*. Dövlət qurumlarına münasibətdə operatorun funksiyası *Azərbaycan Respublikası Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidmətinin kibermərkəzi ilə birgə* həyata keçirilir.

Reyestrin fəaliyyətinin təşkili və funskionallığının həyata keçirilməsi kritik informasiya infrastrukturu subyektləri tərəfindən Reyestrə *"Kritik informasiya infrastrukturu obyektlərinin reyestrinin strukturu, yaradılması və aparılması qaydası"* uyğun olaraq təqdim edilən məlumatlar əsasında təmin edilir. Reyestrə məlumatların təqdim edilməsi operatorun metodiki tövsiyələrinə və təqdim etdiyi nümunələrə uyğun həyata keçirilir.

Adıçəkilən qaydaya əsasən, reyestrin yaradılması və aparılması Azərbaycan Respublikası Prezidentinin 2018-ci il 12 sentyabr tarixli 263 nömrəli Fərmanı ilə təsdiq edilmiş "Dövlət informasiya ehtiyatları və sistemlərinin formalaşdırılması,

aparılması, inteqrasiyası və arxivləşdirilməsi Qaydaları"nda müəyyən edilən prinsiplər nəzərə alınmaqla aşağıdakı prinsiplər əsasında həyata keçirilir:

◊ **mütənasiblik** – Reyestrdə görülən tədbirlərin risk səviyyəsinə mütənasib olması;

◊ **operativlik** – Reyestr vasitəsilə məlumat mübadiləsinin mümkün ən qısa müddətdə həyata keçirilməsi;

◊ **funksionallıq və davamlı inkişaf** – Reyestrin inkişaf etdirilməsi imkanını təmin edən proqram-texniki komponentlərin olması, həmçinin ən son texnologiyalardan istifadə edilməklə Reyestrin daim təkmilləşdirilməsi;

◊ **əməkdaşlıq** – Reyestrin fəaliyyətinin təmin edilməsi ilə bağlı sahibin, operatorun və iştirakçıların qarşılıqlı əməkdaşlıq və təhlükəsizlik tədbirlərinin görülməsində fəal iştirak etməsi.

Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin olunması sahəsində hüquqi məsuliyyət tədbirləri qismində isə nəzərə alınmalıdır ki, *Azərbaycan Respublikasının İnzibati Xətalar Məcəlləsinin 371-1.1-ci maddəsinə* əsasən, ümumi və xüsusi tələblərin infrastrukturun sahibi, onun vəzifəli şəxsi və ya ona kibertəhlükəsizlik xidməti göstərən provayder (təchizatçı) tərəfindən pozulmasına görə vəzifəli şəxslər *500-1000 azn*, hüquqi şəxslər *3000-4000* azn məbləğdə cərimə edilir. *Məcəllənin 371-1.2 -ci maddəsinə əsasən,* informasiya təhlükəsizliyini idarəetmə sisteminin yaradılmasına və funksionallığının təmin olunmasına dair tələblərin pozulmasına görə isə vəzifəli şəxslər *1000-1500 azn*, hüquqi şəxslər isə *4000-5000* azn cərimə edilir. Habelə, kritik informasiya infrastrukturu obyektinə yönəlmiş kibertəhdidlər, kiberhücumlar, kiberinsidentlər və bu əməllərin törədilməsinə cəhdlər barədə məlumatın subyekt tərəfindən aidiyyəti dövlət orqanına təqdim edilməməsinə görə vəzifəli şəxslər *300-500 azn*,

hüquqi şəxslər isə *500-1000 azn* məbləğdə cərimə edilir. Bununla yanaşı, İnzibati Xətalar Məcəlləsinin *602-3-cü maddəsinə əsasən,* ümumi və xüsusi tələblərin pozulması hallarının aradan qaldırılmasına dair səlahiyyətli orqanın (vəzifəli şəxsin) tələbinin yerinə yetirilməməsinə, yaxud kibertəhdidlərin və kiberhücumların aşkarlanması, qarşısının alınması və təhlükəsizlik insidentlərinin araşdırılması üçün səlahiyyətli orqana (vəzifəli şəxsə) lazımi şəraitin yaradılmamasına və ya maneçilik törədilməsinə görə vəzifəli şəxslər *1000-1500 azn*, hüquqi şəxslər *4000-5000 azn* məbləğdə cərimə edilir.

Əlavə olaraq, qeyd etmək lazımdır ki, Azərbaycan Respublikasının Cinayət Məcəlləsinə (bax, maddə 271-273) əsasən kritik informasiya infrastrukturu obyektinin ("ictimai əhəmiyyətli infrastruktur obyektinin") kompüter sisteminə və ya onun hər hansı bir hissəsinə münasibətdə həyata keçirilən qanunsuz daxil olma, qanunsuz müdaxilə və məlumatların qanunsuz ələ keçirilməsi halları cinayət məsuliyyətinə səbəb olur və bu cinayətin subyektləri üç ilədək müddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə *dörd ildən altı ilədək müddətə azadlıqdan məhrum etmə* ilə cəzalandırılır.

Kritik informasiya infranstrukturlarının təhlükəsizliyinin təmin olunması sahəsində beynəlxalq təcrübə araşdırılarkən Avropa İttifaqının mövcud yanaşması diqqəti cəlb edir. Belə ki, Avropa İttifaqında kritik informasiya infrastrukturları cəmiyyətin və iqtisadiyyatın fəaliyyəti üçün əhəmiyyətinə, habelə pozulduğu təqdirdə potensial təsirinə görə təsnif edilmişdir. Bu sektorlar cəmiyyət, iqtisadiyyat və milli təhlükəsizlik üçün əhəmiyyətinə görə müəyyən edilir və onların müxtəlif təhlükələrə, o cümlədən təbii fəlakətlərə, kiberhücumlara, terrorizmə və pandemiyalara qarşı davamlılığını təmin etmək üçün səylər göstərilir. Qeyd etmək lazımdır ki, yenilənmiş "Şəbəkə və İnformasiya

Təhlükəsizliyi Direktivinə (NIS2)" əsasən, Avropa İttifaqında kritik informasiya infrastrukturunun müəyyən edildiyi sektorların sayı 15-dir:

1) **Enerji** - elektrik enerjisinin istehsalı, ötürülməsi və paylanması, həmçinin neft və qaz hasilatı, emalı, paylanması və bərpa olunan enerji mənbələri;
2) **Səhiyyə** - dövlət və özəl səhiyyə təminatçıları, tibbi avadanlıq və dərman istehsalçıları, tibbi sığorta təminatçıları və sağlamlıqla bağlı digər mühüm xidmətlər;
3) **Nəqliyyat** - hava, dəniz, dəmir yolu və avtomobil nəqliyyatı sistemləri, eləcə də limanlar, hava limanları, dəmir yolları və avtomobil yolları kimi əlaqədar infrastrukturlar;
4) **Maliyyə bazarları** - banklar, birjalar, sığorta, ödəniş sistemləri və digər maliyyə institutları;
5) **Su** - su təchizatı sistemləri, o cümlədən içməli suyun təmizlənməsi və paylanması, çirkab suların təmizlənməsi və su anbarları;
6) **Rəqəmsal infrastruktur –** Telekom, DNS, TLD, məlumat mərkəzləri, "trust" və bulud xidmətləri.
7) **Dövlət xidmətləri** - dövlətin fəaliyyəti üçün vacib olan mühüm dövlət obyektləri, informasiya sistemləri və inzibati xidmətlər;
8) **Kosmos**
9) **Rəqəmsal xidmət təminatı** - axtarış motorları, onlayn market və sosial şəbəkələr;
10) **Poçt xidmətləri** – poçt və kuryer xidmətləri;
11) **Tullantıların idarə edilməsi** - tullantıların toplanması, daşınması, təmizlənməsi və utilizasiyası;
12) **Qida** - qida tədarükü zəncirinin bütün aspektləri - əkinçilikdən tutmuş qida emalına, qablaşdırmaya, daşınmaya və pərakəndə satışa qədər.

13) **İstehsal** – xüsusilə də aşağıdakıların istehsalı daxildir: tibbi cihazlar, kompüterlər və elektronika, maşın və avadanlıqlar, mühərrikli nəqliyyat vasitələri, qoşqulu və yarımqoşqulu nəqliyyat vasitələri, digər nəqliyyat avadanlıqları;
14) **Kimya sənayesi** - kimyəvi maddələrin istehsalı, saxlanmasını və daşınması.
15) **Tədqiqat**

Mövzu üzrə aidiyyəti nəzərə alınaraq, kritik informasiya infrastrukturu obyektlərinə münasibətdə törədilmiş və qlobal səviyyədə rezonansa səbəb olmuş bir sıra edilmiş kibercinayətlərə aşağıdakıları misal göstərmək olar:

- Stuxnet (2010) – "Stuxnet" kritik infrastrukturu hədəf alan ən məşhur kiberhücumlardan biridir. O, nüvə sentrifuqası qurğularında istifadə olunan sənaye nəzarət sistemlərini (ICS-industrial control systems) hədəf alaraq İranın nüvə proqramını sabotaj etmək üçün nəzərdə tutulmuşdu. Stuxnet sentrifuqa sürətini manipulyasiya etmək üçün Windows əməliyyat sistemlərində və Siemens SCADA (Supervisory Control and Data Acquisition) proqramında olan boşluqlardan istifadə edərək avadanlıqlara fiziki ziyan vurmuşdu.
- Ukrayna Elektrik şəbəkəsinə hücum (2015 və 2016) – 2015 və 2016-cı ilin dekabr aylarında Ukraynanın elektrik şəbəkəsini hədəf alan kiberhücumlar elektrik enerjisinin geniş kəsilməsi ilə nəticələnmişdir. Hücumlar SCADA sistemlərini sıradan çıxarmaq və enerji paylayıcı avadanlıqlarını uzaqdan idarə etmək üçün zərərli proqramlardan istifadəni əhatə edirdi.
- TRITON (2017) - TRISIS kimi də tanınan TRITON zərərli proqramı Səudiyyə Ərəbistanındakı neft-kimya zavodunda təhlükəsizlik alətləri ilə təchiz edilmiş sistemləri (SIS-safety instrumented systems) hədəf almışdır.

Hücum fəlakətli istehsalat qəzalarının qarşısının alınması üçün vacib olan SIS-i manipulyasiya etmək və ya söndürmək məqsədi daşıyırdı. TRITON kritik infrastruktur sektorlarında istifadə olunan sənaye nəzarət sistemləri üçün inkişaf etmiş və çox ciddi təhlükəni təmsil edir.

- Colonial Pipeline Ransomware Attack (2021) - 2021-ci ilin may ayında ABŞ-ın şərqini yanacaqla təmin edən Colonial Pipeline ransomware hücumunun hədəfinə çevrilmişdir. DarkSide ransomware qrupu ilə əlaqəli olduğu güman edilən hücumçular kritik sistemləri şifrələyərək və fidyə tələb edərək boru kəməri əməliyyatlarını pozmuşdurlar. Hadisə yanacaq qıtlığına səbəb olmuş və kritik infrastrukturun kibertəhlükələrə qarşı həssaslığını bir daha göstərmişdir.
- Water Treatment Facility Hack (2021) - 2021-ci ilin fevralında kibercinayətkar ABŞ-ın Florida ştatının Oldsmar şəhərindəki su təmizləyici qurğuya icazəsiz giriş əldə etmiş və suda natrium hidroksid (lye) miqdarını təhlükəli səviyyəyə çatdırmaq üçün artırmağa cəhd etmişdir. Zavod operatorlarının çevik tədbirləri nəticəsində dəyə biləcək zərərin qarşısı alınmışdır. Bu hadisə su infrastrukturuna edilə biləcək potensial kiberhücumlara qarşı ciddi tədbirlərin görülməli olduğunu dünyanın diqqətinə çatdırmışdır.

# Mövzu 5.

## Fərdi məlumatların, eləcə də dövlət sirri təşkil edən və konfidensial informasiyanın, habelə peşə, kommersiya, istintaq və məhkəmə sirrinin mühafizəsi sahəsində müvafiq qanunvericilik, eləcə də mövcud qanunverciliyin tələblərinin pozulmasına görə nəzərdə tutulan məsuliyyət tədbirləri

Fərdi məlumat dedikdə şəxsin kimliyini birbaşa və ya dolayı yolla identikləşdirən bütün məlumatlar nəzərdə tutulur. Fərdi məlumatların tərifini başqa cür versək deyə bilərik ki, fərdi məlumatlar bizi biz edən, yəni yalnız bizə məxsus olan bütün məlumatlardır. Fərdi məlumatlara ən sadə nümunə kimi ad, soyad və ata adı kimi daimi açıq məlumatları nümunə göstərmək olar.

Biz həyatımızın hər anında fərdi məlumatlarımızdan istifadə edirik, hətta bəzən fərdi məlumatlarımızı tanımadığımız şəxslərlə paylaşmaq məcburiyyətində qalırıq. İstənilən halda fərdi məlumatlarımızın digər şəxslərin əlinə keçməsi halında, fərdi məlumatlarımızdan bizim icazəmiz olmadan müxtəlif əməllər üçün istifadə edilə, həm bizə, həm də digər insanlara zərər verilə bilər.

Məsələn, bank kartı məlumatlarının kənar şəxslərin əlinə keçməsi halında, bank kartı müxtəlif məqsədlər üçün istifadə oluna və kartdakı pullar oğurlana bilər. Bu kimi hallarla qarşılaşmamaq üçün isə fərdi məlumatların mühafizəsinə hər zaman diqqət edilməli, yəni hər kəslə, bizə aid olan məlumatları paylaşmaqdan çəkinməliyik.

"**Fərdi məlumatlar haqqında**" 04 iyun 2010-cu il tarixli Azərbaycan Respublikasının Qanununun 8-ci maddəsinə əsasən Azərbaycan Respublikasının qanunvericiliyi ilə müəyyən olunmuş qaydada fərdi məlumatların məcburi şəkildə

toplanılması və işlənilməsi halları istisna olmaqla, hər hansı şəxs barəsində fərdi məlumatların toplanılmasına və işlənilməsinə yalnız subyekt (yəni barəsində fərdi məlumatlar toplanılan, işlənilən və mühafizə edilən, kimliyi müəyyənləşdirilmiş və ya müəyyənləşdirilən fiziki şəxs) tərəfindən verilmiş yazılı, o cümlədən gücləndirilmiş elektron imzalı elektron sənəd formasında razılıq və ya özünün yazılı təqdim etdiyi məlumatlar əsasında yol verilir.

Fərdi məlumatların informasiya ehtiyatlarının formalaşdırılması, onların informasiya sistemlərinin yaradılması Azərbaycan Respublikasının Konstitusiyasında təsbit edilmiş əsas insan və vətəndaş hüquq və azadlıqlarına riayət edilməklə, qanunçuluq, konfidensiallıq, könüllülüyün məcburiliklə uzlaşdırılması prinsiplərinə uyğun həyata keçirilir.

Fərdi məlumatların toplanılması, işlənilməsi və mühafizəsi prosesində insanın həyat və sağlamlığı üçün təhlükə yaradılmasına, onun şərəf və ləyaqətinin alçaldılmasına yol verilmir.

Fərdi məlumatlar sahəsində qanunvericilik Azərbaycan Respublikasının Konstitusiyasından, Azərbaycan Respublikasının tərəfdar çıxdığı beynəlxalq müqavilələrdən, "Fərdi məlumatlar haqqında" Azərbaycan Respublikası Qanunu, habelə digər normativ hüquqi aktlardan ibarətdir.

Fərdi məlumatlar haqqında Qanuna əsasən, fərdi məlumatlar toplandığı andan mühafizə olunur və bu məqsədlə daxilolma (əldə olunma) növünə görə konfidensial və açıq kateqoriyalara bölünür.

Konfidensial fərdi məlumatlar qanunvericilikdə nəzərdə tutulmuş tələblərə uyğun səviyyədə mülkiyyətçi, operator və bu məlumatlara giriş hüququ olan istifadəçilər tərəfindən mühafizə olunmalıdır. Konfidensial fərdi məlumatlar

qanunla müəyyən olunmuş hallar istisna olmaqla, üçüncü şəxslərə yalnız subyektin razılığı əsasında verilə bilər.

Açıq fərdi məlumatlar kateqoriyasına müəyyən olunmuş qaydada adsızlaşdırılmış, subyekt tərəfindən açıq elan olunmuş və ya ümumi istifadə üçün yaradılmış informasiya sisteminə subyektin razılığı ilə onun barəsində daxil edilmiş məlumatlar aiddir. Şəxsin adı, soyadı və atasının adı daimi açıq fərdi məlumatdır. Açıq kateqoriyalı fərdi məlumatların konfidensiallığının təmin edilməsi tələb olunmur.

Fərdi məlumatların mühafizəsi mülkiyyətçilər və operatorlar tərəfindən təmin olunmalıdır. Fərdi məlumatların toplanılması, işlənilməsi və mühafizəsi sahəsində fəaliyyət göstərən fiziki şəxslər fəaliyyət müddətində və işdən çıxdıqdan sonra həmin məlumatların yayılmaması barədə yazılı iltizam verməlidirlər.

Telekommunikasiya, poçt rabitəsi, ünvan və digər sahələr üzrə cəmiyyətin informasiya təminatını ödəmək məqsədi ilə ümumi istifadəli informasiya sistemlərinə subyektin yazılı razılığı əsasında onun təqdim etdiyi məlumatlar (adı, soyadı, atasının adı, doğulduğu tarix və yer, cinsi, vətəndaşlığı, telefon nömrəsi və elektron ünvanı, yaşadığı və olduğu yer, ixtisası və iş yeri, məşğul olduğu fəaliyyət növü, ailə vəziyyəti, şəkli və digər məlumatlar) daxil edilə bilər.

Qanunun 19-cu maddəsinə əsasən, Qanunun pozulmasında təqsirli olan şəxslər Azərbaycan Respublikasının qanunvericiliyi ilə nəzərdə tutulmuş qaydada məsuliyyət daşıyırlar[28].

Azərbayca Respublikasının İnzibati Xətalar Məcəlləsinin 375-ci maddəsində **fərdi məlumatlar haqqında qanunvericiliyin** pozulmasına görə məsuliyyət nəzərdə tutulmuşdur.

[28] AR-in "Fərdi məlumatlar haqqında" Qanunu. https://e-qanun.az/framework/19675

- 375.0. Fərdi məlumatlar haqqında qanunvericiliyin pozulmasına, yəni:
- 375.0.1. “Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanunu ilə dövlət qeydiyyatı tələb olunan, lakin dövlət qeydiyyatından keçməyən informasiya sistemində fərdi məlumatların toplanılmasına və ya işlənilməsinə;
- 375.0.2. fərdi məlumatların mülkiyyətçisi və ya operatoru tərəfindən fərdi məlumatların mühafizəsinin təmin olunmamasına, “Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanunu ilə tələb olunduğu hallarda və müddətlərdə fərdi məlumatların məhv edilməməsinə, yaxud fərdi məlumatların toplanılmasının, işlənilməsinin və ya verilməsinin dayandırılmamasına görə-
  - üç yüz manatdan beş yüz manatadək məbləğdə cərimə edilir.
- Habelə, 326-2.2-ci maddə üzrə taksi sifarişi operatorları tərəfindən “Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanununa uyğun olaraq, taksi sifarişi xidmətinin göstərilməsi zamanı istifadə olunan fərdi məlumatların informasiya sistemlərinin dövlət qeydiyyatından keçirilməməsinə və fərdi məlumatların mühafizəsi ilə bağlı tələblərə riayət olunmamasına görə
  - vəzifəli şəxslər beş min manat məbləğində, hüquqi şəxslər iyirmi min manat məbləğində cərimə edilir[29].

"**Dövlət sirri haqqında**" 07 sentyabr 2004-cü il tarixli Azərbaycan Respublikasının Qanunun 2-ci maddəsinə dövlətin hərbi, xarici-siyasi, iqtisadi, kəşfiyyat, əks-kəşfiyyat və əməliyyat-axtarış fəaliyyəti ilə bağlı olub, dövlət

[29] **İnzibati Xətalar Məcəlləsi**. https://e-qanun.az/framework/46960

tərəfindən mühafizə edilən və yayılması Azərbaycan Respublikasının təhlükəsizliyinə ziyan vura bilən məlumatlar dövlət sirri hesab olunur. "Dövlət sirri haqqında" Qanunun 5-ci maddəsində isə “dövlət sirri”nə verilən anlayışda adıçəkilən lar üzrə dövlət sirri təşkil edən məlumatların siyahısı təqdim edilmişdir:

**1. Hərbi sahədə** aşağıdakı məlumatlar dövlət sirrini təşkil edir:

- *Azərbaycan Respublikası Silahlı Qüvvələrinin, başqa silahlı birləşmələrinin, qanunvericiliklə nəzərdə tutulmuş digər qoşunlarının strateji, operativ və səfərbərlik üzrə yerləşdirilməsinə dair əməliyyatların hazırlanması və keçirilməsi üzrə strateji və əməliyyat planlarının, döyüşü idarəetməyə dair sənədlərinin məzmunu, onların döyüş və səfərbərlik hazırlığı, səfərbərlik ehtiyatlarının yaradılması və istifadəsi haqqında;*
- *Azərbaycan Respublikası Silahlı Qüvvələrinin və Azərbaycan Respublikasının qanunvericiliyinə uyğun olaraq yaradılmış digər silahlı birləşmələrinin quruculuq planları, silahların və hərbi texnikanın inkişafının istiqamətləri, silah və hərbi texnika nümunələrinin yaradılması və modernləşdirilməsi üzrə məqsədli proqramların, elmi tədqiqat və təcrübi-konstruktor işlərinin məzmunu və yerinə yetirilməsinin nəticələri haqqında;*
- *silah və hərbi texnika nümunələrinin taktiki-texniki xarakteristikaları və döyüşdə tətbiqi imkanları, hərbi təyinatlı yeni növ maddələrin xüsusiyyətləri, resepturaları və ya texnologiyaları haqqında;*
- *milli təhlükəsizlik və müdafiə mülahizələrinə görə xüsusi əhəmiyyət kəsb edən obyektlərin dislokasiyası, təyinatı, hazırlıq və müdafiə olunma dərəcəsi, tikintisi və istismarı, habelə bu obyektlər üçün torpaq, yer təki və akvatoriyalar ayrılması haqqında;*

- *qoşunların dislokasiyası, həqiqi adları, təşkilati strukturu, şəxsi heyətinin sayı və onların döyüş təminatı haqqında, həmçinin hərbi-siyasi və ya əməliyyat şəraiti haqqında;*
- *Azərbaycan Respublikası ərazisinin müdafiə və mühüm iqtisadi əhəmiyyətli geodeziya məntəqələrinin və coğrafi obyektlərinin koordinatları haqqında.*

2. **İqtisadi sahədə** aşağıdakı məlumatlar dövlət sirrini təşkil edir:

- *Azərbaycan Respublikasının və onun ayrı-ayrı bölgələrinin mümkün hərbi əməliyyatlara hazırlıq planlarının məzmunu, silah və hərbi texnikanın istehsalı və təmiri üzrə sənayenin səfərbərlik gücü, hərbi sahədə istifadə edilən xammal və materialların strateji növlərinin göndərilməsi həcmi, ehtiyatları, həmçinin dövlət ehtiyatlarının yerləşdirilməsi, faktik həcmi və istifadəsi haqqında;*
- *Azərbaycan Respublikasının müdafiə qabiliyyətinin və təhlükəsizliyinin təmin olunması məqsədilə onun infrastrukturundan istifadə olunması haqqında;*
- *mülki müdafiə qüvvələri və vasitələri, inzibati idarəetmə obyektlərinin dislokasiyası, təyinatı və müdafiə olunma dərəcəsi, əhalinin təhlükəsizliyinin təmin olunma dərəcəsi, dövlətin təhlükəsizliyinin təmin olunması üçün nəzərdə tutulan nəqliyyat və rabitənin fəaliyyəti haqqında;*
- *dövlət müdafiə sifarişlərinin həcmləri, planları (tapşırıqları), silah, hərbi texnika və digər hərbi məhsulların buraxılması və göndərilməsi (pul və ya natura ifadəsində), onların buraxılışı üzrə mövcud güc və bu gücün artırılması haqqında, göstərilən silah, hərbi texnika və digər hərbi məhsulların işlənib hazırlanmasını, istehsalını, ixracını, satışını, habelə onların istehsalının, ixracının, satışının təşkilini həyata keçirən*

*müəssisələr və onların maliyyə hesabatları, kooperasiya üzrə əlaqələri haqqında;*

- *dövlətin təhlükəsizliyinə təsir edən mühüm müdafiə və ya iqtisadi əhəmiyyəti olan elmi və texniki nailiyyətlər, elmi tədqiqat, təcrübi-konstruktor, layihə işləri və texnologiyaları haqqında;*
- *siyahısı qanunvericiliklə müəyyənləşdirilən strateji növlü faydalı qazıntıların ehtiyatlarının, istehsalının, idxalı və ixracının, satışının həcmi, dövlət ehtiyatlan haqqında, pul əskinaslarının, qiymətli kağızların hazırlanması, saxtalaşdırmadan qorunması, həmçinin dövlətin maliyyə fəaliyyətinin digər xüsusi tədbirləri haqqında.*

3. **Xarici siyasət** sahəsində aşağıdakı məlumatlar dövlət sirrini təşkil edir:

- *Azərbaycan Respublikasının xarici-siyasi və xarici-iqtisadi fəaliyyəti haqqında, əgər onların vaxtından əvvəl açıqlanması dövlətin təhlükəsizliyinə ziyan vura bilərsə;*
- *Azərbaycan Respublikasının digər dövlətlərlə hərbi, elmi-texniki və başqa sahələrdə əməkdaşlığı haqqında, əgər onların vaxtından əvvəl açıqlanması tərəflərdən heç olmasa biri üçün diplomatik fəaliyyətinin həyata keçirilməsində çətinlik yaranmasına səbəb ola bilərsə.*

4. **Kəşfiyyat, əks-kəşfiyyat və əməliyyat-axtarış fəaliyyəti sahəsində** məlumatlar:

- *kəşfiyyat, əks-kəşfiyyat və əməliyyat-axtarış fəaliyyətinin qüvvə və vasitələri, mənbələri, metodları, planları və nəticələri haqqında, habelə bu fəaliyyətin maliyyələşdirilməsinin göstəriciləri haqqında, əgər bu göstəricilər sadalanan məlumatları açıqlayırsa;*

- *kəşfiyyat, əks-kəşfiyyat və əməliyyat-axtarış fəaliyyətini həyata keçirən orqanlarla konfidensial əsaslarla əməkdaşlıq edən və əməkdaşlıq etmiş şəxslər haqqında;*
- *müvafiq icra hakimiyyəti orqanlarının əsasnamələrində göstərilən mühafizə olunan şəxslərin, qorunan obyektlərin və strateji obyektlərin təhlükəsizliyinin təmin olunmasının təşkili, qüvvə və vasitələri, metodları haqqında, habelə bu fəaliyyətin maliyyələşdirilməsinin göstəriciləri haqqında, əgər bu göstəricilər sadalanan məlumatlan açıqlayırsa;*
- *şifrlənmiş, o cümlədən kodlaşdırılmış və məxfiləşdirilmiş rabitə sistemləri haqqında, şifrlər, şifrlərin işlənməsi və hazırlanması, onlarla təminat, şifrləmə və xüsusi mühafizə vasitələri haqqında, xüsusi təyinatlı informasiya-analitik sistemləri haqqında;*
- *məxfi məlumatların mühafizəsi metodları və vasitələri haqqında;*
- *dövlət sirrinin mühafizəsinin təşkili və faktiki vəziyyəti haqqında;*
- *Azərbaycan Respublikasının dövlət sərhədinin mühafizəsi haqqında;*
- *Azərbaycan Respublikasında dövlətin müdafiəsinin, təhlükəsizliyinin və hüquq mühafizə fəaliyyətinin təmin olunması ilə əlaqədar dövlət büdcəsinin xərcləri haqqında;*
- *dövlətin təhlükəsizliyinin təmin olunması məqsədilə keçirilən tədbirləri açıqlayan kadr hazırlığı haqqında.*

Yuxarıda qeyd olunan/dövlət sirri təşkil edən məlumatların üç məxfilik dərəcəsi və müvafiq olaraq, bu məlumatların daşıyıcıları üçün üç məxfilik qrifi müəyyənləşdirilir: ***"xüsusi əhəmiyyətli", "tam məxfi"*** və ***"məxfi".***

"Dövlət sirri haqqında" Qanunun 21-ci maddəsinə əsasən, vəzifəli şəxslərin və vətəndaşların dövlət sirri ilə işləməyə buraxılması könüllülük qaydasında həyata

keçirilir. Dövlət sirri ilə işləməyə isə, bir qayda olaraq, Azərbaycan Respublikasının vətəndaşları buraxılırlar. Əcnəbilərin və vətəndaşlığı olmayan şəxslərin dövlət sirri ilə işləməyə buraxılması müvafiq icra hakimiyyəti orqanının müəyyənləşdirdiyi qaydada həyata keçirilir.

Eyni zamanda, qanunla təsbit olunmuşdur ki, vəzifəli şəxsin və vətəndaşın dövlət sirri ilə işləməyə buraxılması aşağıdakıları nəzərdə tutur:

*1. ona etibar ediləcək dövlət sirri təşkil edən məlumatları yaymayacağı barədə dövlət qarşısında öhdəlik götürməsini;*

*2. dövlət sirri haqqında qanunvericiliyin pozulmasına görə məsuliyyət nəzərdə tutan Azərbaycan Respublikasının qanunvericiliyi ilə tanış olmasını;*

*3. Qanunun 25-ci maddəsində nəzərdə tutulan qismən və müvəqqəti məhdudiyyətlərə rəsmi yazılı razılıq verilməsini;*

*4. onun barəsində səlahiyyətli orqanlar tərəfindən yoxlama tədbirlərinin keçirilməsinə yazılı razılıq verməsini;*

*5. dövlət hakimiyyəti orqanının, müəssisə, idarə və təşkilatın rəhbəri tərəfindən dövlət sirri ilə işləməyə buraxılma haqqında qərar qəbul edilməsini.*

Qanunun 30-cu maddəsində qeyd olunur ki, dövlət sirri haqqında Azərbaycan Respublikasının qanunvericiliyini pozan hüquqi şəxslər, vəzifəli şəxslər və vətəndaşlar qüvvədə olan qanunvericiliyə müvafiq olaraq məsuliyyət daşıyırlar. Müvafiq dövlət hakimiyyəti orqanları və onların vəzifəli şəxsləri məlumatların qeyri-qanuni yayılması üzrə qərar qəbul edərkən qeyri-qanuni yayılmış məlumatın dövlət sirri təşkil etməsi haqqında ekspert rəyinə əsaslanırlar. Ekspert rəyinin hazırlanması və təsdiqi qaydası müvafiq icra hakimiyyəti orqanı tərəfindən müəyyən edilir. Dövlət sirri təşkil edən məlumatların qeyri-qanuni yayılması

bütövlükdə Azərbaycan Respublikası və ya mərkəzi icra hakimiyyəti orqanı üzrə dövlətin təhlükəsizliyinə ziyan vurulmaqla nəticələndiyi hallarda məlumatların yayılması faktı üzrə materiallara müvafiq icra hakimiyyəti orqanı tərəfindən baxılır və rəy verilir.

Dövlət sirri haqqında Azərbaycan Respublikasının qanunvericiliyinin pozulmasına görə Azərbaycan Respublikasının İnzibati Xətalar Məcəlləsində, habelə Azərbaycan Respublikasının Cinayət Məcəlləsində hüquqi məsuliyyət müəyyən edən normalar nəzərdə tutulmuşdur.

Azərbaycan Respublikasının İnzibati Xətalar Məcəlləsinin 378-ci maddəsinə əsasən, dövlət sirri ilə işləməyə buraxılışı olmayan şəxsin dövlət sirrindən istifadə ilə bağlı vəzifəyə təyin edilməsinə görə vəzifəli şəxslər beş yüz manatdan yeddi yüz manatadək məbləğdə, hüquqi şəxslər min beş yüz manatdan iki min manatadək məbləğdə cərimə edilir.

Azərbaycan Respublikasının Cinayət Məcəlləsində isə dövlət sirri haqqında qanunvericiliyin pozulmasına görə məsuliyyət nəzərdə tutulan bir neçə maddə mövcuddur. Belə ki, CM-nin 274-cü maddəsində qeyd edilir ki, dövlətə xəyanət, yəni Azərbaycan Respublikasının suverenliyi, ərazi toxunulmazlığı, dövlət təhlükəsizliyi və ya müdafiə qabiliyyəti zərərinə olaraq ***Azərbaycan Respublikasının vətəndaşı tərəfindən*** qəsdən törədilən əməl: düşmən tərəfinə keçmə, casusluq, **dövlət sirrini xarici dövlətə vermə**, Azərbaycan Respublikasına qarşı düşmənçilik fəaliyyəti aparmaqda xarici dövlətə, təşkilata və ya onların nümayəndələrinə kömək etmə ***dövlətə xəyanət*** hesab olunur. Dövlətə xəyanət cinayətinin subyekti isə *on iki ildən iyirmi ilədək müddətə azadlıqdan məhrum etmə* və ya *ömürlük azadlıqdan məhrum* etmə ilə cəzalandırılır.

Bundan başqa, Cinayət Məcəlləsinin 276-cı maddəsinə əsasən, **dövlət sirri** olan məlumatları xarici dövlətə, xarici təşkilata və ya onların nümayəndələrinə vermə, yaxud vermək məqsədilə oğurlama, toplama və ya saxlama, habelə xarici ölkələrin xüsusi xidmət orqanlarının tapşırığı ilə Azərbaycan Respublikasının təhlükəsizliyi zərərinə olaraq istifadə etmək üçün sair məlumatları vermə, vermək məqsədilə oğurlama və ya toplama, əgər casusluq ***əcnəbi və ya vətəndaşlığı olmayan şəxs tərəfindən törədilərsə***, bu, ***casusluq*** hesab olunur. Casusluq cinayətinin subyekti isə *on ildən on beş ilədək müddətə azadlıqdan məhrum* etmə ilə cəzalandırılır.

Habelə, CM-nin 284-cü maddəsinə əsasən, şəxs tərəfindən ona etibar edilmiş və ya xidməti vəzifəsinə və yaxud işinə görə ona məlum olan dövlət sirrini təşkil edən məlumatların yayılması, dövlətə xəyanət əlamətləri olmadıqda bu, ***dövlət sirrini yayma*** hesab olunur. Qanunverici eyni əməllərin ağır nəticələrə səbəb olması halında məsuliyyəti ağırlaşdırmışdır. Belə ki, eyni əməllər ağır nəticələrə səbəb olduqda üç ilədək müddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə *dörd ildən səkkiz ilədək müddətə azadlıqdan məhrum etmə* ilə cəzalandırılır.

Cinayət Məcəlləsinin 284-1-ci maddəsinə əsasən, ***dövlət sirri təşkil edən məlumatların***, məzmununda dövlət sirri olan sənədlərin, habelə barəsindəki məlumatlar dövlət sirri olan əşyaların zor tətbiq etmək hədəsi ilə və ya zor tətbiq etməklə, hədə-qorxu və ya digər məcburetmə vasitələri ilə, talama, aldatma yolu ilə, yaxud məxfi məlumatların gizli əldə edilməsi üçün nəzərdə tutulmuş xüsusi və ya digər texniki vasitələrdən istifadə etməklə ***qanunsuz əldə edilməsi***, dövlətə xəyanət və ya casusluq əlamətləri olmadıqda, *iki ildən beş ilədək müddətə azadlıqdan məhrum etmə* ilə cəzalandırılır.

Cinayət Məcəlləsinə edilmiş yeni əlavəyə əsasən, Azərbaycan Respublikası ***Silahlı Qüvvələrinin*** *şəxsi heyətinin, hərbi silah, sursat və ya hərbi texnikasının hərəkəti, yaxud dislokasiyası* ***haqqında məlumatları yayma*** müharibə vaxtı və ya döyüş şəraitində törədildikdə və Cinayət Məcəllənin 274-cü, 276-cı və ya 284-cü maddələrində nəzərdə tutulmuş əməllərin əlamətləri olmadıqda *üç ildən altı ilədək müddətə azadlıqdan məhrum* etmə, eyni əməllər ***ağır nəticələrə səbəb olduqda*** isə *beş ildən səkkiz ilədək müddətə azadlıqdan məhrum* etmə ilə cəzalandırılır.

Cinayət Məcəlləsi üzrə daha bir maddə − 285-ci maddə məzmununda dövlət sirri olan sənədləri itirməyə görə cinayət məsuliyyətinin əsaslarını müəyyən edir. Burada deyilir ki, məzmununda ***dövlət sirri*** olan sənədlərin, habelə barəsindəki məlumatlar dövlət sirri olan əşyaların, etibar olunan şəxs tərəfindən göstərilən sənədlərlə və ya əşyalarla Azərbaycan Respublikasının qanunvericiliyi ilə müəyyən edilmiş davranış qaydalarının pozulması nəticəsində onların ***ehtiyatsızlıqdan itirilməsi*** *ağır nəticələrə səbəb olduqda* cinayət məsuliyyəti yaradır.

"**Kommersiya sirri haqqında**" 04 dekabr 2001-ci il tarixli Azərbaycan Respublikasının Qanununa əsasən, kommersiya sirri dedikdə, hüquqi və fiziki şəxslərin istehsal, texnoloji, idarəetmə, maliyyə və başqa fəaliyyəti ilə bağlı, sahibinin razılığı olmadan açıqlanması, onların qanuni maraqlarına ziyan vura bilən məlumatlar başa düşülür və Azərbaycan Respublikasında bütün hüquqi və fiziki şəxslərin kommersiya sirrini təşkil edən məlumatlarının, onların ifadə edilməsi üsulundan və daşıyıcısından asılı olmayaraq qorunma hüququ vardır. Kommersiya sirrindən dövlətin, hüquqi və fiziki şəxslərin qanuni mənafelərinin ziddinə istifadə edilə bilməz. Qanuna əsasən məlumatların kommersiya dəyərinə malik olması (başqa şəxslərə məlum olmadığına görə fəaliyyət sahəsində üstünlük qazanmaq və mənfəət əldə etmək baxımından əhəmiyyətlidir, digər

şəxslərə bütövlükdə, yaxud hissələrlə satıla, bağışlanıla, müqavilə əsasında, yaxud varislik qaydasında verilə bilər və s.), habelə məlumatın məxfiliyinin qorunması məqsədilə sahibi tərəfindən hüquqi, təşkilati, texniki və digər tədbirlərin həyata keçirilməsi, eləcə də bu məlumatların sərbəst əldə olunmasının qanuni əsaslarla məhdudlaşdırılması məlumatların kommersiya sirrinə aid edilməsinin meyarları qismində çıxış edir.

Qanunun 4-cü maddəsinə əsasən, **aşağıdakılar istisna edilməklə**, hüquqi və fiziki şəxslərin bu Qanunun tələblərinə uyğun olan məlumatları kommersiya sirri hesab edilir:

- təsis sənədlərində əksini tapan məlumatlar (kommersiya hüquqi şəxslərin təsisçiləri (iştirakçıları) və onların nizamnamə kapitalındakı payları barədə məlumatlar istisna olmaqla);
- sahibkarlıq fəaliyyətinin bəzi növləri ilə məşğul olmaq hüququ verən lisenziyalar haqqında məlumatlar;
- qanunvericilikdə nəzərdə tutulan hallarda auditor rəyi daxil olmaqla maliyyə (mühasibat) hesabatlarında olan məlumatlar;
- Azərbaycan Respublikasının vergi qanunvericiliyinə əsasən vergi ödəyicisi barədə vergi sirri hesab olunmayan məlumatlar;
- əməyin ödənilməsi formaları və məbləği barədə, əmək haqqı və sosial ödənişlər üzrə borclar, işçilərin say tərkibini, boş iş yerlərinin mövcudluğunu əks etdirən məlumatlar;
- patent və digər mühafizə sənədləri ilə qorunan əqli mülkiyyət obyektləri haqqında məlumatlar;
- qiymətli kağızlar bazarı haqqında Azərbaycan Respublikasının qanunvericiliyinə əsasən qiymətli kağızların emitenti, qiymətli kağızlar bazarında lisenziyalaşdırılan şəxslər, mərkəzi depozitar, səhmdar

investisiya fondu və investisiya fondunun idarəçisi tərəfindən açılmalı olan məlumatlar;

- qeyri-kommersiya təşkilatlarının fəaliyyəti barədə məlumatlar;
- özəlləşdirmənin dövlət proqramının həyata keçirilməsi və konkret obyektlərin özəlləşdirmə şərtləri barədə məlumatlar;
- hüquqi şəxsin ləğvi və onun kreditorları tərəfindən tələblərin irəli sürülməsi qaydası və müddəti barədə məlumatlar;
- Azərbaycan Respublikasının qanunvericiliyinə əsasən barəsində məsuliyyət növü nəzərdə tutulan əməllərə dair məlumatlar ;
- ekoloji və antiinhisar qanunvericiliyinə əməl olunması, əməyin təhlükəsizliyinin təmin edilməsi, əhalinin sağlamlığına ziyan vura bilən məhsulların satışı ilə bağlı məlumatlar;
- kommersiya sirri rejiminin qoyulması qüvvədə olan qanunvericiliklə məhdudlaşdırılan məlumatlar;

  telekommunikasiya operatoruna və telekommunikasiya provayderinə nömrə resursunun ayrılması, dəyişdirilməsi və geri alınması haqqında məlumatlar;
- qanunvericiliyə əsasən kommersiya sirri hesab edilməyən digər məlumatlar.

Kommersiya sirrinin rejimi kommersiya sirrinin sahibi, yəni kommersiya sirrinə qanuni əsaslarla malik olan hüquqi və ya fiziki şəxs tərəfindən müəyyən olunur. Məlumatın Kommersiya sirrinə aid olması **"Kommersiya sirri"** şifri ilə ifadə edilir. Qeyd olunan şifr məlumatın daşıyıcısında və (və ya) onu müşayiət edən sənədlərdə həkk olunur. Qanunvericilikdə nəzərdə tutulan hallar istisna olmaqla, kommersiya sirri rejimini müəyyən edən şəxs kommersiya sirri şifrinin qoyulmasını və götürülməsini, kommersiya sirrinin əldə edilməsi və açıqlanması

şərtlərini, kommersiya sirrini təşkil edən məlumatın qorunması üsullarını, ötürülməsi vasitələrinin seçilməsini, istifadə olunma şərt sərbəst müəyyənləşdirir.

"**Kommersiya sirri haqqında**" Qanuna əsasən, kommersiya sirri təşkil edən məlumatları ***qeyri-qanuni yolla əldə edən*** və ya ***yayan şəxslər*** Azərbaycan Respublikasının müvafiq qanunvericiliyində nəzərdə tutulmuş qaydada məsuliyyət daşıyırlar.

Onu da qeyd etmək lazımdır ki, **"Banklar haqqında"** Azərbaycan Respublikasının 16 yanvar 2004-cü il tarixli Qanununun 41-ci maddəsinə əsasən, Azərbaycan Respublikasının Mülki Məcəlləsinə müvafiq olaraq *bank hesabının, hesab üzrə əməliyyatlar və qalıqların, habelə müştəri haqqında məlumatların*, o cümlədən *müştərinin adı, ünvanı, rəhbərləri haqqında məlumatların* sirrinə bank təminat verir. *Müştərilərin bank saxlancında əmlakının mövcudluğu, bu cür əmlakın sahibləri, xarakteri və dəyəri haqqında məlumatların* sirrinə də bank təminat verir.

Azərbaycan Respublikasının Cinayət Məcəlləsinin 202-ci maddəsinə əsasən isə, **kommersiya və ya bank sirlərini** təşkil edən məlumatların toplanması həmin məlumatları yaymaq və ya onlardan qanunsuz istifadə etmək məqsədi ilə sənədləri oğurlamaqla, satın almaqla və ya hədələməklə, habelə digər qanunsuz üsulla törədildikdə min beş yüz manatdan iki min beş yüz manatadək miqdarda cərimə və ya bir ilədək müddətə islah işləri və ya iki ilədək müddətə azadlıqdan məhrum etmə ilə cəzalandırılır. Sahibkarın razılığı olmadan kommersiya və ya bank sirri olan məlumatların tamah və ya başqa şəxsi niyyətlə ***qanunsuz yolla istifadə edilməsi və ya yayılması*** *külli miqdarda ziyan vurmaqla törədildikdə* isə cinayətin subyekti cinayət nəticəsində vurulmuş ziyanın iki misli miqdarında

cərimə və ya iki ilədək müddətə islah işləri və ya altı ayadək müddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

Eyni zamanda, Cinayət Məcəlləsinin 202-ci maddəsinin qeyd hissəsində göstərilmişdir ki, kommersiya və ya bank sirri olan məlumatları "Cinayət yolu ilə əldə edilmiş əmlakın leqallaşdırılmasına və terrorçuluğun maliyyələşdirilməsinə qarşı mübarizə haqqında" Azərbaycan Respublikasının Qanunu ilə müəyyən edilmiş qaydada maliyyə monitorinqi orqanına təqdim edən şəxsə bu Məcəllənin 202.2-ci maddəsinin qüvvəsi şamil edilmir.

Milli qanunvericilikdə məhkəməyədək icraatın sirrləri də mühafizə edilir. Belə ki, Cinayət Məcəlləsinin 300-cü maddəsində təhqiqat və ya ibtidai istintaq məlumatlarını yaymaya görə cinayət məsuliyyətinin əsasları təsbit olunmuşdur. Burada deyilir ki, qanunla müəyyən edilmiş qaydada yayılmaması barədə xəbərdarlıq edilmiş şəxs tərəfindən təhqiqatçının, müstəntiqin, prokurorun və ya məhkəmə nəzarəti funksiyasını həyata keçirən hakimin icazəsi olmadan təhqiqat və ya ibtidai istintaq məlumatlarının yayılması ibtidai araşdırmanın aparılmasına mane olduqda, yaxud maraqlı şəxsə mənəvi və ya maddi ziyanın vurulmasına səbəb olduqda min manatdan iki min manatadək miqdarda cərimə və ya iki ilədək müddətə islah işləri və ya altı ayadək müddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

# Mövzu 6.

## Kibercinayətlərin anlayışı, təsnifatı, və kibercinayətkarlığa qarşı mübarizənin hüquqi əsasları

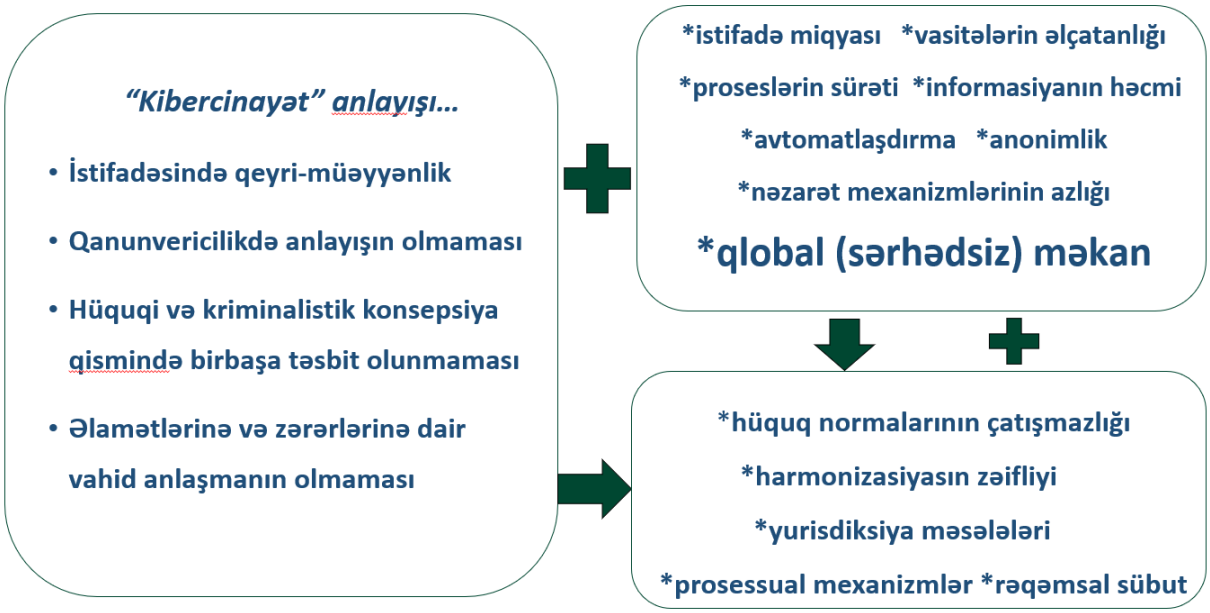
İnformasiya və kommunikasiya texnologiyalarının (İKT) gündəlik həyatda və müxtəlif səviyyələrdə idarəetmənin həyata keçirilməsində geniş və intensiv istifadəsi informasiya cəmiyyətinin sürətli inkişafını təmin etməklə yanaşı, həm də dəqiq müəyyənləşdirilməli, hərtərəfli təhlil edilməli və zərərli təsirlərinin minimuma endirilməli olduğu bir sıra yeni nəsil təhlükə və təhdidlərin yaranması ilə nəticələnmişdir. Xüsusilə də, son üç onillikdə cinayətkarlar tərəfindən cinayətlərin yeni formalarının yaradılması məqsədilə İKT-dən istifadə hallarının sayında ciddi artım müşahidə edilmişdir.[30] Bəzi proqnozlara görə isə 2024-cü ildə kibercinayətlər nəticəsində dəyəcək illik qlobal zərər **9.5 trilyon ABŞ dollarına çata bilər.**[31] Bundan başqa, kibercinayətlər və fiziki məkanda törədilən cinayətlər arasındakı "keyfiyyət fərqləri" - genişlənmiş miqyas, transmilli əhatə dairəsi və məsafədən idarəetmənin mümkünlüyü - İKT infrastrukturunun həssaslığını və cinayətkar məqsədlər üçün bu zəifliklərin istismarı imkanlarını artırır.

Kiberməkanın səciyyəvi xüsusiyətləri, habelə infrastrukturun, əsasən, özəl sektor və vətəndaşların əlində cəmlənməsi kibercinayətkarlıqla mübarizədə adekvat institutsional strukturların, elmi-texniki və normativ-hüquqi bazanın formalaşdırılması və təkmilləşdirilməsi ilə yanaşı, dövlət, özəl sektor və vətəndaşlar arasında, həmçinin beynəlxalq səviyyədə tərəfdaşlığın və əməkdaşlığın genişləndirilməsini tələb edir. Adekvat mexanizmlərin, zəruri institutların,

[30] Holt J.T., Bossler A., Seigfried-Spellar K. C., *Cybercrime and Digital Forensics*, Routledge 2017, 5.
[31] *2023 official Cybercrime report, eSentire*. Available at: https://www.esentire.com/resources/library/2023-official-cybercrime-report (Accessed: 14 April 2024).

çoxtərəfli və beynəlxalq tərəfdaşlıq və əməkdaşlığın yerində olmaması isə kibercinayətkarlıqla mübarizəni daha da müəkkəbləşdirir və çətinləşdirir.

Ümumilikdə, kibercinayətkarlığa qarşı mübarizədə qarşıya çıxan çətinlikləri aşağıdakı şəkildə ümümiləşdirmək olar:




Kibercinayətlərin anlayışı ilə əlaqədar qeyd olunmalıdır ki, milli və beynəlxalq hüquqda **"kibercinayət"in birbaşa anlayışı verilməyib**. Bu cinayətlərlə bağlı bir sıra hallarda digər yaxın anlayışlar - 'computer crime', electronic crime', 'digital crime', 'IT crime', 'Internet crime', 'virtual crime', 'high-tech crime' - istifadə edilir. Eyni zamanda, müxtəlif mənbələrdə bəzi anlayışlara rast gəlmək olur. Məsələn, ISO 27032:2012ISO/IEC 27032-2012 "İnformasiya texnologiyaları – Kibertəhlükəsizlik üzrə təlimatlar" sənədinə əsasən, **kibercinayət** dedikdə kiberməkanda xidmət və tətbiqlərdən istifadə etməklə və ya onlara qarşı törədilən və ya kiberməkanın mənbə, alət, hədəf və ya törədilmə yeri qismində çıxış etdiyi cinayət başa düşülür. Birləşmiş Krallıqda 2013-cü ildə qəbul edilmiş strategiyada ("*The Serious and Organised Crime Strategy (2013*)") "kibercinayətlər" anlayışı altında həm "*cyber-dependent (kiber-asılı)"* - yalnız

kompüterlər, kompüter şəbəkələri və ya digər İKT vasitələrindən istifadə etməklə törədilən (törədilə bilən) cinayətlər, həm də "*cyber-enabled" - h*əm onlayn həm də offlayn şəkildə törədilə bilən, lakin onlayn şəkildə (daha az resurslarla) xüsusilə geniş miqyasda və yüksək sürətlə törədilə bilən digər ənənəvi cinayətlər - əhatə olunmuşdur. Bu anlayış çox geniş olduğu üçün təcrübədə kibercinayətkarlığa qarşı mübarizəni daha da mürəkkəbləşdirmişdir.

"Kibercinayətkarlıq haqqında" 2001-ci il noyabrın 23-də Budapeşt şəhərində imzalanmış Konvensiyada da "kibercinayət"ə anlayış verilməsə də, kriminallaşdırılmalı olan bir sıra əməllər ayrıca göstərilmişdir. Həmin əməllərin aşağıdakı şəkildə təsnifatlaşdırıldığı müşahidə olunur:

- "Kompüter verilənləri və sistemlərinin konfidensiallığı, tamlığı və əlçatanlığına qarşı cinayətlər"
- "Kompüterlə bağlı/əlaqəli (computer-related) cinayətlər"
- "Məlumatların məzmunu ilə bağlı cinayətlər"
- "Müəllif hüquqlarının və əlaqəli hüquqların pozulması ilə bağlı cinayətlər".

Azərbaycan Respublikasında kibercinayətlərlə mübarizə imkanlarının genişləndirilməsi məqsədilə hüquqi sferada bir sıra mühüm tədbirlər həyata keçirilmişdir. "Kibercinayətkarlıq haqqında" 2001-ci il noyabrın 23-də Budapeşt şəhərində imzalanmış Konvensiyanın müvafiq bəyanatlar və qeyd-şərtlərlə 30 sentyabr 2009-cu il tarixdə "Kibercinayətkarlıq haqqında" Konvensiyanın təsdiq edilməsi barədə" 874-IIIQ nömrəli Azərbaycan Respublikasının Qanunu ilə təsdiq edilməsi kibercinayətkarlıqla mübarizə sahəsində atılan ən mühüm addımlardan biridir. Xüsusilə də, ölkədə kibercinayətkarlıqla mübarizə məqsədilə cinayət-hüquqi sferada həyata keçirilən tədbirlərlə bağlı qeyd olunmalıdır ki, 29 iyun 2012-ci il tarixli 408-IVQD nömrəli "Azərbaycan Respublikasının Cinayət Məcəlləsində

dəyişikliklər edilməsi haqqında" Azərbaycan Respublikasının Qanunu ilə Cinayət Məcəlləsinin otuzuncu fəsli Konvensiyaya uyğunlaşdırılaraq yeni redaksiyada verilmiş və Məcəlləyə uşaq pronoqrafiyasının dövriyyəsi ilə bağlı cinayət məsuliyyətinin əsaslarını müəyyən edən yeni bir maddə (Maddə 171-1) əlavə olunmuşdur. Qeyd etmək lazımdır ki, köhnə redaksiyada verilmiş "Kompüter informasiyası sahəsində cinayətlər" fəslindən fərqli olaraq yeni redaksiyada verilmiş "Kibercinayətlər" fəslində daha mütərəqqi və daha spesifik müddəalar təsbit olunmuşdur. Beləliklə, **"Kibercinayətlər"** adlı otuzuncu fəsildə **kompyuter sisteminə qanunsuz daxil olma (maddə 271), kompyuter məlumatlarını qanunsuz ələ keçirmə (maddə 272), kompyuter sisteminə və ya kompyuter məlumatlarına qanunsuz müdaxilə (maddə 273), kibercinayətlərin törədilməsi üçün hazırlanmış vasitələrin dövriyyəsi (maddə 273-1)** və **kompyuter məlumatlarının saxtalaşdırılması (maddə 273-2)** əməllərinin dairəsi müəyyən olunaraq bu əməllərə görə cinayət məsuliyyəti nəzərdə tutulmuşdur.

# Xüsusi normalar

## Budapeşt Konvensiyası (2001)

Maddə 2. **Qanunsuz daxil olma**

Maddə 3. **Qanunsuz ələ keçirmə**

Maddə 4. **Verilənlərə müdaxilə**

Maddə 5. **Sistemlərə müdaxilə**

Maddə 6. **Qurğulardan qanunsuz istifadə**

Maddə 7. **Kompüter texnologiyalarından istifadə etməklə saxtalaşdırma**

Maddə 8. **Kompüter texnologiyalarından istifadə etməklə dələduzluq**

Maddə 9. **Uşaq pornoqrafiyası ilə bağlı cinayətlər**

Maddə 10. **Müəllif hüquqlarının və əlaqəli hüquqların pozulması ilə bağlı cinayətlər**

## Azərbaycan Respublikası Cinayət Məcəlləsi

(29 iyun 2012-ci ildən yeni redaksiyada)

Maddə 271.**Kompyuter sisteminə qanunsuz daxil olma**

Maddə 272. **Kompyuter məlumatlarını qanunsuz ələ keçirmə**

Maddə 273. **Kompyuter sisteminə və ya kompyuter məlumatlarına qanunsuz müdaxilə**

Maddə 273-1. **Kibercinayətlərin törədilməsi üçün hazırlanmış vasitələrin dövriyyəsi**

Maddə 273-2. **Kompyuter məlumatlarının saxtalaşdırılması**

Maddə 171-1. **Uşaq pornoqrafiyasının dövriyyəsi**

Maddə 165. **Müəlliflik hüquqlarını və ya əlaqəli hüquqları pozma**

Cinayət Məcəlləsinin 271-ci maddəsi kompyuter sisteminə **qanunsuz daxil olmaya** gösə cinayət məsuliyyətinin əsaslarını müəyyən edir. Belə ki, həmin maddəyə əsasən, kompyuter sisteminə və ya onun hər hansı bir hissəsinə daxil olmaq hüququ olmadan həmin sistemə və ya onun hər hansı bir hissəsinə mühafizə tədbirlərini pozmaqla, yaxud burada saxlanılan kompyuter məlumatlarını ələ keçirmək və ya başqa şəxsi niyyətlə **qəsdən daxil olma** iki ilədək müddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə iki min manatdan dörd min manatadək miqdarda cərimə və ya iki ilədək müddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

271-ci maddənin qeyd hissəsinə əsasən, **"kompyuter sistemi"** dedikdə, müvafiq proqramlara uyğun olaraq verilənlərin avtomatlaşdırılmış işlənməsini həyata keçirən hər hansı qurğu və ya bir-birinə qoşulmuş və ya əlaqələndirilmiş qurğular qrupu başa düşülür. **"Kompyuter məlumatları"** dedikdə, kompyuter sistemində işlənməsi, emal edilməsi üçün yararlı olan istənilən informasiya (faktlar, məlumatlar, proqramlar və anlayışlar) başa düşülür.

Cinayət Məcəlləsinin 272-ci maddəsində isə **kompyuter məlumatlarını qanunsuz ələ keçirməyə** görə cinayət məsuliyyəti nəzərdə tutulur. Belə ki, həmin maddəyə əsasən, kompyuter sisteminə, kompyuter sistemindən və ya bu sistem daxilində ötürülən ümumi istifadə üçün nəzərdə tutulmayan kompyuter məlumatlarının, o cümlədən bu cür kompyuter məlumatlarının daşıyıcısı olan kompyuter sistemlərinin elektromaqnit şüalanmasının, buna hüququ olmayan şəxs tərəfindən texniki vasitələrdən istifadə etməklə **qəsdən ələ keçirilməsi** iki ilədək müddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə iki min manatdan dörd min manatadək miqdarda cərimə və ya iki ilədək müddətə azadlığın məhdudlaşdırılması və ya iki ilədək müddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

**Kompyuter sisteminə və ya kompyuter məlumatlarına qanunsuz müdaxilə** əməli isə Cinayət Məcəlləsinin 273-cü maddəsinə əsasən kriminallaşdırılmışdır. Belə ki, kompyuter məlumatlarının qəsdən zədələnməsi, silinməsi, korlanması, dəyişdirilməsi və ya bloklanması buna hüququ olmayan şəxs tərəfindən törədilməklə əhəmiyyətli zərər vurulmasına səbəb olduqda, habelə kompyuter məlumatlarının daxil edilməsi, ötürülməsi, zədələnməsi, silinməsi, korlanması, dəyişdirilməsi və ya bloklanması yolu ilə kompyuter sisteminin işləməsinə buna hüququ olmayan şəxs tərəfindən qəsdən ciddi maneə törədilməsi bu maddə ilə cinayət məsuliyyətinə səbəb olur.

Onu da qeyd etmək lazımdır ki, Cinayət Məcəlləsinin yuxarıda adıçəkilən maddələrinə əsasən, **kritik informasiya infrastrukturu** obyektinin (**"ictimai əhəmiyyətli infrastruktur obyektinin"**[32]) kompüter sisteminə və ya onun hər hansı bir hissəsinə münasibətdə həyata keçirilən qanunsuz daxil olma, qanunsuz müdaxilə və məlumatların qanunsuz ələ keçirilməsi hallarında cinayətin subyektləri üç ilədək müddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə *dörd ildən altı ilədək müddətə azadlıqdan məhrum etmə* ilə cəzalandırılır.

Müasir dövrdə geniş vüsət almış **kibercinayətlərin törədilməsi üçün hazırlanmış vasitələrin dövriyyəsi** ilə əlaqədar əməllər də Cinayət Məcəlləsinin 273-1-ci maddəsinə əsasən kriminallaşdırılmışdır. Belə ki. Hazırlanmasının və ya uyğunlaşdırılmasının əsas məqsədi Məcəllənin 271-273-cü maddələrində nəzərdə tutulmuş cinayətlərin törədilməsi olan qurğuların və ya kompyuter proqramlarının istehsalı, həmin cinayətlərin törədilməsi məqsədi ilə idxalı, istifadə üçün əldə olunması, saxlanılması, satışı, yayılması və ya əldə edilməsinə digər formalarda

[32] "İctimai əhəmiyyətli infrastruktur obyekti" dedikdə, dövlət və cəmiyyət üçün mühüm əhəmiyyət kəsb edən xidmətlər göstərən dövlət idarə, müəssisə, təşkilatları, qeyri-hökumət təşkilatları (ictimai birliklər və fondlar), kredit təşkilatları, sığorta şirkətləri, *qiymətli kağızlar bazarında lisenziyalaşdırılan şəxslər,* investisiya fondları *və bu fondların idarəçiləri* başa düşülür.

şərait yaradılması, əhəmiyyətli zərər vurduqda cinayətin subyekti iki ilədək müddətə azadlıqdan məhrum etmə ilə cəzalandırıla bilər. Hebelə, kompyuter parollarının, giriş kodlarının və ya kompyuter sisteminə, yaxud onun hər hansı bir hissəsinə hüququ olmadan daxil olmağa imkan verən digər analoji məlumatların bu Məcəllənin 271—273-cü maddələrində nəzərdə tutulmuş cinayətlərin törədilməsi məqsədilə istehsalı, saxlanılması və ya istifadə üçün əldə olunması, eləcə də həmin məqsədlərlə satışı, yayılması və ya onların əldə edilməsinə digər formalarda şərait yaradılması cinayət məsuliyyətinə səbəb olur.

Cinayət Məcəlləsində həm də **kompyuter məlumatlarının saxtalaşdırılmasına** görə cinayət məsuliyyəti nəzərdə tutulmuşdur (maddə 273-2). Belə ki, saxtalaşdırılmış kompyuter məlumatlarını autentik (həqiqi) kompyuter məlumatları kimi qələmə vermək və ya istifadə etmək məqsədilə kompyuter məlumatlarını müvafiq hüquq olmadan qəsdən daxil etmə, dəyişdirmə, silmə və ya bloklama, bu əməllər ilkin kompyuter məlumatlarının autentikliyinin (həqiqiliyinin) pozulmasına səbəb cinayət məsuliyyəti üçün əsas yaranır.

Kibercinayət əməllərinin kriminallaşdırılması ilə bağlı milli yanaşmaya nəzər salarkən ilk öncə qeyd olunmalıdır ki, Cinayət Məcəlləsinə əsasən əməlin cinayət hesab olunması üçün zəruri şərtlərdən biri də əməlin ictimai təhlükəli olmasıdır.

Cinayət Məcəlləsinin “Kibercinayətlər” (otuzuncu) fəslində qeyd olunmuş cinayətlər isə ya “böyük ictimai təhlükə törətməyən”, ya da “az ağır” cinayətlər kateqoriyasına daxil edilir ki, bu da ölkədə bu cinayətlərin ictimai təhlükəlilik dərəcəsinin nisbətən aşağı qəbul olunması qənaətinə gəlməyə əsas verir. Nəticədə, məsələn, törədilməsi üçün əsasən xüsusi hazırlıq tələb edən “ictimai əhəmiyyətli infrastruktur obyektlərinin kompyuter sisteminə və ya onun hər hansı

bir hissəsinə" qanunsuz daxil olma və ya qanunsuz müdaxilə əməlinin (Maddə 273.4) törədilməsinə yönəlmiş hazırlıq əməlləri Cinayət Məcəlləsinin tələbinə əsasən cinayət məsuliyyətinə səbəb olmur. Konvensiyada kriminallaşdırılmalı olan əməllərin siyahısı və onların kriminallaşdırılması şərtləri müəyyən edilsə də, kibercinayətlərə görə cinayət məsuliyyətinə cəlb etməyə imkan verən minimum yaş həddi, habelə kibercinayətlərə görə tətbiq olunmalı olan sanksiyalarla bağlı spesifik müddəalar təsbit edilməmişdir. Cinayət Məcəlləsinin 20.2-ci maddəsinə əsasən on dörd yaşı tamam olmuş şəxslər tərəfindən törədilməsinə görə cinayət məsuliyyətinə cəlb edildiyi cinayətlərin siyahısında "kibercinayətlərin" olmaması bu cinayətlərin subyektinin Məcəllənin 20.1-ci maddəsinə əsasən cinayət törədənədək **on altı yaşı** tamam olmuş şəxslər olması anlamına gəlir. Digər cinayətlərdən fərqli olaraq kibercinayətləri törədən şəxslərin orta yaşının daha aşağı olması, hətta 13-14 yaşlarında olan yetkinlik yaşına çatmayan şəxslər tərəfindən də bu mürəkkəb və xüsusi bacarıq tələb edən əməllərin rahatlıqla və ictimai-təhlükəliliyi dərk edilərək törədilə bilməsi nəzərə alınmalıdır. Eyni zamanda, Konvensiyaya qoşulan dövlətlərdə bu əməllərə görə cinayət məsuliyyətinə cəlb etməyə imkan verən minimum orta yaşın hətta 14 yaşdan aşağı olması, gənclərin getdikcə daha çox onlayn qanun pozuntularının və kibercinayətlərin subyektinə çevrilməsi və beynəlxalq əməkdaşlıq zamanı kriminallaşdırma sahəsində fərqli yanaşmaların yarada biləcəyi potensial problemlər diqqət mərkəzində saxlanılmalıdır.[33]

Əlavə olaraq qeyd etmək lazımdır ki, Cinayət Məcəlləsində bir sıra əməllərə görə cinayət məsuliyyəti müəyyən edən maddələrdə cinayətin obyektiv cəhətində kiber elementlərin ehtiva olunmasının da ayrılıqda nəzərdə alınması üçün müvafiq dəyişikliklər həyata keçirilmiş və əlavələr olunmuşdur. Məsələn, oğurluq əməlinin

[33] Balajanov E., 'Setting the Minimum Age of Criminal Responsibility for Cybercrime' 32 International Review of Law, Computers & Technology, (2017). Pp. 2-20

“elektron məlumat daşıyıcılarından, yaxud informasiya texnologiyalarından” istifadə edilməklə törədilməsinin ağırlaşdırıcı tərkib əlaməti kimi nəzərdə tutulması ilə bağlı 30 aprel 2013-cü il tarixli 633-IVQD nömrəli “Azərbaycan Respublikasının Cinayət Məcəlləsində dəyişiklik edilməsi haqqında” Azərbaycan Respublikasının Qanunu ilə Cinayət Məcəlləsinə 177.2.3-1- ci maddə əlavə edilmişdir. Əlavə olaraq, 29 noyabr 2016-cı il tarixli 444-VQD nömrəli “Azərbaycan Respublikasının Cinayət Məcəlləsində dəyişikliklər edilməsi haqqında” Azərbaycan Respublikasının Qanunu ilə internet informasiya ehtiyatında saxta istifadəçi adlar, profil və ya hesablardan istifadə edərək böhtan atma və ya təhqir etmə kimi əməllərə görə cinayət məsuliyyətini nəzərdə tutan yeni məzmunda 148-1-ci maddə əlavə edilmişdir.

Onu da qeyd etmək lazımdır ki, kiberməkanın imkanları “məlumatların məzmunu ilə bağlı cinayətlər”in də dairəsini xeyli genişləndirmiş, birbaşa “kibercinayət” hesab olunmasa da bir sıra digər cinayətlərin törədilməsi üçün imkanlar yaratmışdır. Cinayət Məcəlləsində təsbit olunmuş bu cinayətlərə misal olaraq aşağıdakıları göstərmək olar:

- **Maddə 155. Yazışma, telefon danışıqları, poçt, teleqraf və digər məlumatların sirrini pozma;**
- **Maddə 156.1. Şəxsi və ailə həyatının sirri olan məlumatların,** belə məlumatları əks etdirən sənədlərin, video və foto çəkilişi materiallarının, səs yazılarının yayılması, habelə satılması və ya başqasına verilməsi qanunsuz toplanılması**;**
- **Maddə 167-2.** Qanunsuz olaraq **dini təyinatlı** ədəbiyyatı, audio və video materialları, mal və məmulatları və dini məzmunlu başqa məlumat materiallarını istehsal etmə, idxal etmə, satma və ya yayma;

- **Maddə 167-3.1. Dini ekstremist** materialları, hazırlama, saxlama və ya **yayma**;
- **Maddə 182. Hədə-qorxu ilə tələb etmə,** yəni zərərçəkmiş şəxsin və ya onun yaxın qohumlarının şəxsiyyəti ... haqqında **rüsvayedici məlumatlar yayma ...** hədəsi ilə özgənin əmlakını və ya əmlaka olan hüququnu və ya əmlak xarakteri daşıyan digər hərəkətlər etməsin**i tələb etmə;**
- **Maddə 216. Terrorçuluq barədə bilə-bilə yalan məlumat vermə;**
- **Maddə 281. Dövlət əleyhinə yönələn açıq çağırışlar** - ... konstitusiya quruluşunun zorla dəyişdirilməsinə və ya ərazi bütövlüyünün parçalanmasına yönələn **açıq çağırışlar etmə,** habelə bu cür məzmunlu materialları yayma**;**
- **Maddə 281-1. Azərbaycan Respublikasının ərazi bütövlüyünün parçalanmasına yönələn atributları və ya simvolları nümayiş etdirmə, yayma, hazırlama, əldə etmə, saxlama, daşıma və ya gəzdirmə;**
- **Maddə 283. Milli, irqi, sosial və ya dini nifrət və düşmənçiliyin salınmasına...** yönələn hərəkətlər, **aşkar surətdə,** o cümlədən **mediadan istifadə olunmaqla törədildikdə;**
- **Maddə 284. Dövlət sirrini yayma** - ... dövlətə xəyanət əlamətləri olmadıqda;
- **Maddə 284-2.1. A. R. Silahlı Qüvvələrinin** şəxsi heyətinin, hərbi silah, sursat və ya hərbi texnikasının hərəkəti, yaxud dislokasiyası haqqında **məlumatları yayma**, müharibə vaxtı və ya döyüş şəraitində törədildikdə.

Kibercinayətlərin ibtidai istintaqının həyata keçirilməsi üzrə səlahiyyətli dövlət orqanları ilə əlaqədar isə qeyd etmək lazımdır ki, Cinayət Məcəlləsinin 271–273-2-ci maddələrində ("Kibercinayətlər" fəslində") nəzərdə tutulmuş cinayətlərə dair işlər üzrə ibtidai istintaq - bu işi başlamış **Azərbaycan Respublikasının Dövlət Təhlükəsizliyi Xidməti** və ya **daxili işlər (polis) orqanları** tərəfindən həyata keçirilir.

# Mövzu 7.

## İnformasiya müharibəsi və kibermüharibə anlayışları və onların xüsusiyyətləri, müasir çağırışlar və hibrid müharibələrin hüquqi aspektləri

Müasir dünyada informasiya cəmiyyətinin bir çox müsbət yönləri olsa belə bir sıra mənfi cəhətləri də mövcuddur. Bu problemlərə aşağıdakıları nümunə göstərmək olar:

- İnformasiya qarşıdurması, böhranı cəmiyyətdə baş verən ziddiyyətlərin, təzadların həllində yeni forma kimi çıxış edir. Bu problemin mahiyyəti ondan ibarətdir ki, bir tərəfdən İKT-nin istehsalı və yayılması üzrə inhisarçılığın geniş vüsət alması qaçılmaz haldır, digər tərəfdən isə müasir informasiya sistemləri beynəlxalq münasibətlərdə yeni "güc tətbiqetmə" vasitələrinə çevrilmişdir. Bu faktor siyasi-iqtisadi xarakter daşıyır və onun ən bariz nümunəsi qismində informasiya müharibələri çıxış edir.
- İnformasiya təhlükəsizliyi və kibercinayətkarlıq. Yeni texnologiyaların inkişafı yeni cinayətlərin meydana çıxmasını şərtləndirmişdir ki, bunlar ənənəvi cinayətlərlə müqayisədə daha çox ziyan yetirmək xüsusiyyətinə malikdir. Məsələn, viruslar vasitəsilə eyni zamanda, milyonlarla kompüter sistemini sıradan çıxarmaq mümkün olur. Bundan başqa, müxtəlif "çirkli" məlumatların şəbəkəyə daxil edilməsi nəticə etibarilə ənənəvi dünya mədəniyyətinin əxlaqi dəyərlərini aşağı salır. Məhz belə təhlükələrin qarşısının alınması tədbirləri həm beynəlxalq, həm də dövlətdaxili səviyyədə planlaşdırılmalı və operativ şəkildə icra olunmalıdır.
- İnformasiya mühitində insanın şəxsi həyatının müdafiəsi. İKT-nin inkişafı və fərdi məlumatların şəbəkədə yerləşdirilməsi həmin məlumatların müxtəlif

vasitələrlə əldə olunması ilə nəticələnə bilər. Bu baxımdan, fərdi məlumatların qorunması ilə bağlı texniki, təşkilati, hüquqi tədbirlərin görülməsi informasiya hüququnun ən vacib problemlərindən biri olmalıdır.

- Müəlliflik hüquqlarının qorunması. İnformasiyanın hər kəs üçün açıq və əlyetər olması əksər hallarda müəlliflik hüquqlarının pozulması ilə nəticələnir. İlkin mənbəyə istinad tələbi demək olar ki, bütün dövlətlərin qanunvericilik aktlarında nəzərdə tutulsa da, plagiat hallarının sayı günbəgün artmaqdadır. Belə halların aradan qaldırılması informasiya hüququnun problemlərindən biridir və bu problem informasiya cəmiyyətinin formalaşması nəticəsində geniş vüsət almışdır.
- "Bioloji inqilab"ın baş vermə təhlükəsi. İKT-nin inkişafı nəticəsində insanın genetik məlumatlarının əldə olunması və müxtəlif eyniləşdirmə məqsədləri üçün istifadəsi təbiətdə ekoloji balansın pozulmasına gətirib çıxara bilər. Bu da hər şeydən əvvəl, insanın özü üçün təhlükəli olan "bioloji inqilab"la nəticələnəcəkdir.[34]

Dövlətlər arasında yaranan siyasi gərginliklərin ən pik həddi dövlətlər arası müharibələrin baş verməsidir. Müasir dövrdə qloballaşan dünyamızda yeni texnologiyaların inkişafı nəticəsində klassik müharibələr də öz təsirini göstərmiş və yeni müharibə termini meydana gəlmişdir. Yeni yaranmış virtual müharibələr kiber fəzada baş verdiyi üçün kiber müharibə adlandırılmışdır. Kiber fəzanın inkişafı kiber müharibələrin də inkişafına yeni hücum texnikalarının və növlərinin meydana çıxmasına şərait yaratmışdır. Hal-hazırda kiber müharibələr klassik müharibələr qədər istifadə olunan müharibə növünə çevrilmişdir.

[34] Кузнецов П.У. Основы информационного права: Учебник для бакалавров. Москва: Проспект, 2016, с. 21-25.

**İnformasiya qarşıdurması** – tərəflərin xüsusi metodlardan, informasiya ehtiyatlarına təsir üsulları və vasitələrindən istifadə etməklə qarşı tərəfin informasiya ehtiyatlarının məhvinə və ya nəzarətdə saxlanmasına yönəlmiş informasiya əməliyyatlarıdır.

**İnformasiya hücumu** – icazə olmadan istənilən formada informasiyanın köçürülməsi, dəyişdirilməsi və məhvinə, həmçinin proqram təminatlarına, məxfi informasiyanın saxlandığı texniki qurğulara və insan psixologiyasına yönəlmiş əməliyyatlardır.[35]

**İnformasiya müharibəsi** isə özündə informasiya hücumu və informasiya qarşıdurması kimi əməliyyatları birləşdirən daha təhlükəli informasiya təsiri forması olub, qarşı tərəfin informasiyasına, informasiya proseslərinə və sistemlərinə zərər vurmaqla informasiya üstünlüyü əldə etmək, qarşı tərəfin iqtisadi, hərbi potensialını ələ keçirmək, ictimai şüura informasiya təsiri göstərməklə insanların davranışlarını dəyişmək uğrunda həyata keçirilən məqsədyönlü fəaliyyətdir.[36]

İnformasiya müharibəsində informasiya həm silah, həm də məqsəd, həm də müdafiə obyekti kimi çıxış edir. Mənbələrdə informasiya müharibəsi kombinə edilmiş kibercinayətlərə aid olunur.[37] Ədəbiyyatda "şəbəkə müharibəsi" və "kibermüharibə" terminlərini irəli sürən mövqelər də vardır ki, bu qrup müəlliflər şəbəkə müharibəsini daha çox ictimai səviyyəli konseptual münaqişə kimi

[35] Tabriz Jafarov (Raufoğlu), "İç İşlerine Karışmama İlkesi Bağlamında Enformasyon Tekeli Ve Dezenformasyon: Şangay İşbirliği Örgütü Uygulamaları Açısından Bir Değerlendirme", Ankara Üniversitesi Hukuk Fak. Dergisi, 71 (4) 2022, s. 1755.

[36] Ələkbərova İ.Y. İnformasiya müharibəsinin bəzi modelləri haqqında. // İnformasiya cəmiyyəti problemləri, 2015, №1, 42.

[37] Understanding Cybercrime: A Guide For Developing Countries. ICT Applications and Cybersecurity Division Policies and Strategies Department, ITU, p 57.

qiymətləndirərək, onun iqtisadi, siyasi və sosial sferaları əhatə etdiyini, kibermüharibənin isə əksinə hərbi məqsəd daşıdığını iddia edirlər.[38]

İnformasiya müharibəsinin iki istiqamətdə aparılması ilə bağlı fikirlərə də rast gəlinir: informasiya-texniki müharibə və informasiya-psixoloji müharibə. İnformasiya-texniki müharibədə müxtəlif növ informasiya sistemlərinə (verilənlər bazası, analitik sistemlər və s.), telekommunikasiya vasitələrinə, kompüter şəbəkəsinə və s. texniki vasitələrə hücum əməliyyatları nəzərdə tutulur. Nəticədə informasiya sistemlərinin ələ keçirilərək nəzarətdə saxlanması və ya məhv edilməsi əməliyyatları reallaşdırılır. İnformasiya-psixoloji müharibədə isə hədəf ayrı-ayrı insanlar, sosial qruplar, təşkilatlar, bir və ya bir neçə dövlətin vətəndaşları, dünya ictimaiyyətidir.[39]

Əslində belə bölgünün aparılması bir qədər məntiqi ziddiyyət doğurur. Bir tərəfdən informasiya müharibəsinin məqsəd və strategiyasının (siyasi, hərbi, iqtisadi və s.) vacib məqam olmasını nəzərə alsaq, bu cür təhlükəli əməliyyatlar sisteminin yalnız texniki istiqamətdə xarakterizə olunması onun əsl mahiyyətini açmağa imkan vermir. Çünki hər bir halda həyata keçirilən fəaliyyətin məqsədi əsas faktor hesab olunur. Digər tərəfdən isə müasir dövrdə psixoloji informasiya müharibəsinin özü belə informasiya sistemlərindən istifadə etmədən mümkün deyil və burada da texniki əməliyyatlar həyata keçirilir. Ona görə də informasiya müharibəsinin məqsəd və strategiya aspektindən fərqləndirilməsi daha düzgün olar. İnformasiyanın ələ keçirilməsi, korlanması, dəyişdirilməsi, məhv edilməsi və s. bu kimi texniki əməliyyatlar isə informasiya müharibəsinin həyata keçirilməsinin

[38] Arquilla J., Ronfeldt D., Cyberwar is coming! // National Security Research Division, https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf p. 27-30.
[39] Ələkbərova İ.Y. İnformasiya müharibəsinin bəzi modelləri haqqında. // İnformasiya cəmiyyəti problemləri, 2015, №1, 44.

üsulları kimi qəbul olunmalıdır. İnformasiya müharibəsinin fundamental paradiqmasının aşağıdakı informasiya əməliyyatlarından ibarət olması qeyd edilir:

- İnformasiya təqdimatından imtina (Denial of Information), dağıtma və ya məhv etmə (Degradation or Destruction).
- Aldatma və imitasiya (Deception and Mimicry), təhrif (Corruption) – bilərəkdən yanlışlığa yönəldən informasiyanın ötürülməsi əməliyyatı nəzərdə tutulur.
- Ayırma və məhv etmə (Disruption and Destruction) – daxildən disfunksiya yaradan və informasiyanın məhvinə yönəlmiş əməliyyatdır.
- Təxribat əməliyyatları (SUBversion) – destruktiv prosesə səbəb olan informasiyanın daxil edilməsi əməliyyatıdır.[40]

İnformasiya müharibəsini daha çox texniki istiqamətdə izah edən yuxarıdakı bölgü informasiya-hüquqi aspektdən qarşıya çıxan sualları cavablandırmaq üçün yetərli deyil. Fikrimizcə, bu məsələ ilə bağlı ABŞ tədqiqatçısı Martin Libikinin təsnifatı daha dolğun səciyyə daşıyır. Belə ki, o, informasiya müharibəsinin 7 formasını fərqləndirir:[41]

◊ Komanda-nəzarət müharibəsi (Command and Control Warfare) – komandanlıq və icraçılar arasındakı əlaqə kanallarına istiqamətlənmiş informasiya müharibəsidir. Bu növ müharibədə əvvəlki dövrlərdə geniş yayılmış anti-rəhbər (anti-head) və müasir dövrdə inkişaf etmiş, İKT-dən istifadə etməklə icra olunan antineek əməliyyatlardan istifadə olunur.

[40] Ələkbərova İ.Y. İnformasiya müharibəsinin bəzi modelləri haqqında. // İnformasiya cəmiyyəti problemləri, 2015, №1, s. 43.
[41] Martin C. Libicki. What Is Information Warfare? Washington, 1995, pp. 7-8

◊ 2.Kəşfiyyat müharibəsi (Information Based Warfare) – mühüm informasiyanın toplanması və bu zaman hücum edən tərəfin öz informasiya resurslarını mühafizə etməsi prosesidir.

◊ 3.Elektron müharibə (Electronic Warfare) – elektron kommunikasiya vasitələrinə qarşı yönəlmiş müharibədir. Elektron kommunikasiya vasitələri dedikdə, radio əlaqə, radarlar, kompüter şəbəkəsi nəzərdə tutulur. Elektron dövlətin formalaşdırılmasından sonra geniş vüsət alan bu növ müharibələrin əsas obyektini kriptoqrafik istiqamətlər təşkil edir. Məhz belə növ müharibələrin artmasının nəticəsidir ki, respublikamızda da dövlət əhəmiyyətli informasiya resurslarının mühafizəsi üçün xüsusi qaydalar müəyyənləşdirilmişdir.

◊ 4.Psixoloji müharibə (Psychological Warfare) – insanların psixologiyasına təsir edən müharibə növüdür. M.Libiki psixoloji müharibənin 4 kateqoriyasını fərqləndirir: milli iradəyə qarşı yönəlmiş əməliyyatlar, rəhbərliyə (komandanlığa) qarşı yönəlmiş əməliyyatlar, hərbi qüvvələrdə əsgərlərə qarşı yönəlmiş və buna oxşar digər əməliyyatlar, mədəniyyətlərin müharibəsi.[42]

◊ 5.Haker müharibəsi (Hacker Warfare) – qarşı tərəfin mülki obyektlərinə yönəlmiş diversiya əməliyyatlarıdır. Hakerlərin silahı viruslardır.

◊ 6.İqtisadi informasiya müharibəsi (Economic Info-Warfare) – M.Libicki bu müharibəni iki formada təsvir edir: informasiya blokadası və informasiya imperializmi. Tədqiqatçı informasiya blokadasını iqtisadi blokadanın bir versiyası kimi qiymətləndirərək, informasiyanın kəsilməsini iqtisadi sahənin – ticarət əlaqələrinin də kəsilməsi ilə nəticələnəcəyini əsaslandırır. İnformasiya imperializmini isə müəllif ümumi iqtisadi imperializm siyasətinin bir hissəsi

[42] Martin C. Libicki. What Is Information Warfare? Washington, 1995, p. 35.

kimi şərh edir və ticarətin özünü də bir müharibə kimi qiymətləndirir. O iddia edir ki, ticarət sahəsində üstünlüyün əldə olunması nəticə etibarilə həmin dövlətlərdə bilik üstünlüyünə gətirib çıxarır və belə hakim mövqeni əldən verməmək üçün bu dövlətlər daima "zəif" dövlətlərə "təzyiq göstərməyə" cəhd edirlər.[43]

◊ 7. Kibermüharibə (Cyberwar). Sonuncu təsnifat olan kibermüharibə müasir dövrümüzün ən aktual probleminə çevrilmişdir. Xüsusilə, informasiya terrorizmi təhlükəli xarakteri ilə fərqlənir.

Məlum olduğu kimi, bütün dövlətlər elektron dövlət quruculuğuna keçdiyi üçün bütün informasiyalar informasiya sistemlərində yerləşdirilir. Artıq hər hansı bir dövlətin informasiya sahəsinə "hücum" etməklə, həmin dövləti yalnız siyasi, hərbi deyil, həmçinin iqtisadi, sosial və digər istiqamətlərdə də "iflic" etmək olar. Qeyd etmək lazımdır ki, tədricən dünya üzrə virtuallaşmanın sürətlənməsi insanları bir çox real varlıqlardan uzaqlaşdırır və bu da simulyasiya müharibələrinin formalaşmasını şərtləndirmişdir. Belə müharibələrdə real döyüş meydanındakı hərbi əməliyyatlar kompüter modeli ilə əvəz olunur. Hadisələrin gedişatına əsasən israrla deyə bilərik ki, yaxın gələcəkdə simulyasiya müharibəsi real müharibə ilə eyni məna kəsb edəcəkdir. Bütün bunlar həqiqətən də real müharibədən qat-qat təhlükəlidir. Hesab edirik ki, 2003-cü ildə yaradılan və virtual aləm kimi bir milyondan çox aktiv istifadəçisi olan "Second life" [44]mövqeyimizi əsaslandırmaq üçün bariz nümunə kimi götürülə bilər.

İnsanları tədricən real aləmdən uzaqlaşdıran bu şəbəkə "güclü" dövlətlər üçün "zəif" dövlətlərə asan və operativ psixoloji təsir vasitəsi rolunu oynaya bilər. Eyni zamanda, bu məsələ ilə bağlı müxtəlif virtual oyunların təsiri də az deyil. Məsələn,

[43] Martin C. Libicki. What Is Information Warfare? Washington, 1995, p. 67-74.
[44] http://secondlife.com/

son dövrlərdə geniş yayılmış “Mavi balina” oyununun nə qədər intihar faktlarına səbəb olması göz qabağındadır. Bütün bunlar bir daha göstərir ki, “informasiya müharibəsi” nəzəri anlayış olmaqdan daha çox, təcrübi istiqamətdə təhlil olunmalı, onunla mübarizə tədbirləri yalnız beynəlxalq deyil, milli səviyyədə də aparılmalıdır. Hal-hazırda dövlətlər öz informasiya sistemlərinin məxfiliyini elektron vasitələrlə yetərincə qorumağa nail olurlar və bu da siyasi, hərbi və iqtisadi sahədə törədilən kiberhücumların sayını azaltmışdır. Lakin psixoloji hücumların necə təhlükəli olması və daha ağır nəticələrə gətirib çıxarması Dünya ictimaiyyətinin diqqətindən bir qədər kənarda qalmışdır. Hesab edirik ki, belə psixoloji hücumlar xalqların mənəviyyatının pozulması nəticəsində sonda bütün sahələrə (hərbi, siyasi, iqtisadi) öz mənfi təsirini göstərə bilər. Bu istiqamətdə respublikamızda aparılan işləri təqdirəlayiq hal kimi qiymətləndirmək lazımdır. Belə ki, aidiyyəti dövlət qurumları tərəfindən görülən işlər vətəndaşlarda psixoloji təsir vasitələrindən qorunmaq üçün “immunitet” formalaşdırmış olur.[45]

[45] Əliyev Ə., Rzayeva G., İbrahimova A., Məhərrəmov B., Məmmədrzalı Ş. İnformasiya hüququ. Dərslik. Bakı: “Nurlar” nəşriyyatı, 2019, 448 s.

## ƏDƏBİYYAT SİYAHISI:


1. Azərbaycan Respublikasının Konstitusiyası (1995) (https://e-qanun.az/framework/897).
2. Council of Europe Convention on Cybercrime (2001).
3. “Normativ hüquqi aktlar haqqında” Azərbaycan Respublikasının Konstitusiya Qanunu (21 dekabr 2010-cu il).
4. Azərbaycan Respublikasının Cinayət Məcəlləsi (http://e-qanun.az/framework/46947)
5. Azərbaycan Respublikasının İnzibati Xətalar Məcəlləsi (https://e-qanun.az/framework/46960).
6. “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikasının Qanunu (3 aprel 1998-ci il).
7. "Dövlət sirri haqqında" Azərbaycan Respublikasının Qanunu (7 sentyabr 2004-cü il).
8. “Kommersiya sirri haqqında” Azərbaycan Respublikasının Qanunu (4 dekabr 2001-ci il tarixli).
9. “Milli təhlükəsizlik haqqında” Azərbaycan Respublikasının Qanunu (29 iyun 2004-cü il).
10. "Azərbaycan Respublikasının milli təhlükəsizlik konsepsiyası" (23 may 2007-ci il).
11. “Telekommunikasiya haqqında” Azərbaycan Respublikasının Qanunu (14 iyun 2005-ci il).
12. “Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanunu (04 iyun 2010-cu il).

13. “Müəlliflik hüququ və əlaqəli hüquqlar haqqında” Azərbaycan Respublikasının Qanunu (5 iyun 1996-cı il).
14. "Elektron imza və elektron sənəd haqqında" Azərbaycan Respublikasının Qanunu (9 mart 2004-cü il).
15. "Məlumat toplularının hüquqi qorunması haqqında" Azərbaycan Respublikasının Qanunu (14 sentyabr 2004-cü il).
16. “Elektron ticarət haqqında” Azərbaycan Respublikasının Qanunu (10 may 2005-ci il).
17. "İnformasiya əldə etmək haqqında" Azərbaycan Respublikasının Qanunu (30 sentyabr 2005-ci il).
18. "Biometrik informasiya haqqında" Azərbaycan Respublikasının Qanunu (13 iyun 2008-ci il).
19. “Kibercinayətkarlıq haqqında” Konvensiyanın təsdiq edilməsi barədə” Azərbaycan Respublikasının Qanunu (30 sentyabr 2009-cu il).
20. “Uşaqların zərərli informasiyadan qorunması haqqında” Azərbaycan Respublikasının Qanunu (30 oktyabr 2018-ci il).
21. "Azərbaycan Respublikasının dövlət orqanlarında informasiya təhlükəsizliyinin təmin edilməsi üzrə tədbirlər haqqında" Azərbaycan Respublikası Prezidentinin Fərmanı (29 dekabr 2004-cü il).
22. “İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında” Azərbaycan Respublikası Prezidentinin Fərmanı (26 sentyabr 2012-ci il).

23. “İnformasiya Təhlükəsizliyi üzrə Koordinasiya Komissiyasının yaradılması haqqında” Azərbaycan Respublikası Prezidentinin Sərəncamı (29 mart 2018-ci il).

24. "Tərkibində dövlət sirri təşkil edən məlumatlar olan elektron sənədlərin tərtibi, emalı və mübadiləsi üçün istifadə olunan informasiya sistemlərinin ekspertizasının keçirilməsi Qaydası"nın təsdiq edilməsi haqqında Azərbaycan Respublikasının Nazirlər Kabinetinin Qərarı (27 avqust 2007-ci il).

25. “Dövlət informasiya ehtiyatlarının reyestrinin aparılması qaydaları haqqında Əsasnamə”nin təsdiq edilməsi barədə Azərbaycan Respublikasının Nazirlər Kabinetinin Qərarı (17 may 2010-cu il).

26. “Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydaları”nın təsdiq edilməsi haqqında Azərbaycan Respublikasının Nazirlər Kabinetinin Qərarı (17 iyul 2023-cü il).

27. “Kritik informasiya infrastrukturu obyektlərinin reyestrinin strukturu, yaradılması və aparılması qaydası”nın təsdiq edilməsi haqqında Azərbaycan Respublikası Nazirlər Kabinetinin Qərarı (17 iyul 2023-cü il).

28. "Azərbaycan Respublikasının inkişafı naminə informasiya və kommunikasiya texnologiyaları üzrə Milli Strategiya (2003-2012-ci illər)" (Azərbaycan Respublikası Prezidentinin 17 fevral 2003-cü il tarixli 1146 nömrəli sərəncamı ilə təsdiq olunmuşdur.).

29. "Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafı üzrə 2010 - 2012-ci illər üçün Dövlət Proqramı"nın (Elektron Azərbaycan)" (Azərbaycan Respublikası Prezidentinin 2010-cu il 11 avqust tarixli, 1056 nömrəli Sərəncamı ilə təsdiq edilmişdir).

30. “Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair Milli Strategiyanın həyata keçirilməsi üzrə 2016-2020-ci illər üçün Dövlət Proqramı” (Azərbaycan Respublikası Prezidentinin 2016-cı il 20 sentyabr tarixli 2345 nömrəli Sərəncamı ilə təsdiq edilmişdir).
31. Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023 – 2027-ci illər üçün Strategiyası (Azərbaycan Respublikası Prezidentinin 2023-cü il 28 avqust tarixli 4060 nömrəli Sərəncamı ilə təsdiq edilmişdir).

32. (Draft) Comprehensive international convention on countering the use of information and communications technologies for criminal purposes (drafted by UN Ad Hoc Committee - 2024).
33. Balacanov E., Kibercinayətkarlıqla Mübarizədə Hüquqi Tənzimetmənin və Cinayət-hüquqi Normaların Rolu və Əhəmiyyəti, 1 Azərbaycan Hüquq Jurnalı, 26-37, 2020.
34. Balajanov E., ‘Setting the Minimum Age of Criminal Responsibility for Cybercrime’// 32 International Review of Law, Computers & Technology, 2-20, 2017.
35. Balajanov E., Criminalization of Illegal Access to a Computer System: the Standpoint of the Criminal Legislation of the Republic of Azerbaijan, “Cinayət hüququnun 97ctual problemləri” konfransı, Bakı Dövlət Universiteti, 125-130, 2022.
36. Calallı (Sadıqov) İ., “İnformatika terminlərinin izahlı lüğəti”, “Bakı” nəşriyyatı, 2017

37. Jafarov T. “Uluslararası hukuki yönleri ile siber alanda yetki sorunu”, Adalet yayın evi, Ankara, 2022.
38. Jafarov (Raufoğlu) T, “İç İşlerine Karışmama İlkesi Bağlamında Enformasyon Tekeli Ve Dezenformasyon: Şangay İşbirliği Örgütü Uygulamaları Açısından Bir Değerlendirme”, Ankara Üniversitesi Hukuk Fak. Dergisi, 71 (4) 2022, s. 1755.
39. Couffignal L., “La Cyberne’tique”, Paris, 1968.
40. Hacıyev Z.C. Fəlsəfə. “Turan evi” nəşriyyatı, Bakı, 2012.
41. İmamverdiyev Y., “Kibertəhlükəsizliyə giriş-I Mühazirə”, BDU, 2022.
42. Əliyev Ə., Rzayeva G., İbrahimova A., Məhərrəmov B., Məmmədrzalı Ş. İnformasiya hüququ. Dərslik. Bakı: “Nurlar” nəşriyyatı, 2019.
43. Ələkbərova İ.Y. İnformasiya müharibəsinin bəzi modelləri haqqında. // İnformasiya cəmiyyəti problemləri, №1, 2015.
44. Martin C. Libicki. What Is Information Warfare? Washington, 1995.
45. Nieles M., Dempsey K., Pillitteri V.Y., “An Introduction to Information Security”, USA, 2017.
46. Qaliboğlu E., “İnformasiya azadlığı, internet hüququ və etik problemlər”, X-C, 2021.
47. United Nations Office on Drugs and Crime (UNODC), Comprehensive Study on Cybercrime, 2013.

## İnternet resurslar:

48. Azərbaycan Republikasının Normativ hüquqi aktların vahid internet elektron bazası: www.e-qanun.az
49. Nazirlər Kabineti – https://nk.gov.az/