**Məlikzadə T. A.,**
**Kərimov Ş.M.♦**

**DOI: 10.25108/2304-1730-1749.iolr.2025.79.76-84**
**UOT: 34:343.1**

## Kibercinayətin anlayışı və ümumi xarakteristikası

**Xülasə:** Məqalə kibercinayətkarlığın anlayışı və kibercinayətlərin ümumi xarakteristikasına həsr olunub, Məqalədə qeyd olunur ki, müasir dövrdə rəqəmsal texnologiyalarının inkişafı və elektron məlumatların geniş yayılması nəticəsində kibercinayətlər sürətlə artmaqda davam edir.

Məqalədə qeyd olunur ki, süni intellekt nəticəsində rəqəmsal texnologiya inkişaf etdikcə onun müsbət nəticələri ilə yanaşı mənfi tərəfləri də özünü göstərir.

Həmçinin məqalədə respublikamızda və bir sıra xarici ölkələrin milli qanunvericiliyində “kompüter cinayəti” və “kibercinayət” anlayışları araşdırılaraq təhlil edilib.

**Açar sözlər:** süni intellekt, rəqəmsal texnologiya, kibercinayətkarlıq, kompüter cinayəti, informasiya cinayəti, internet şəbəkəsi, informasiya texnologiyaları, hakerlər, kiberməkan.

**Malikzada T.A.,**
**Karimov Sh.M.♦**

**DOI: 10.25108/2304-1730-1749.iolr.2025.79.76-84**
**UDC: 34:343.1**

## Definition and general characteristics of cybercrime

**Abstract:** The article is devoted to the concept of cybercrime and the general characteristics of cybercrimes. The article notes that in modern times, as a result of the development of digital technologies and the widespread distribution of electronic information, cybercrimes continue to increase rapidly.

The article mentions that as a result of artificial intelligence, as digital technology develops, its positive results and negative sides also appear.

The article also examines and analyzes the concepts of “computer crime” and “cybercrime” in the national legislation of our republic and a number of foreign countries.

**Keywords:** artificial intelligence, digital technology, cybercrime, computer crime, information crime, internet network, information technology, hackers, cyberspace.

---

♦ **Məlikzadə Toğrul Azər oğlu -** Azərbaycan Respublikası Ədliyyə Nazirliyi Məhkəmə Ekspertizası Mərkəzinin doktorantı (Azərbaycan). E-mail: togrul1996@gmail.com
**Kərimov Şöhlət Müzəffər oğlu -** MAA-nın “Hüquq” kafedrasının dosenti, hüquq üzrə fəlsəfə doktoru (Azərbaycan). E-mail: sohlet.kerimov@mail.ru

♦ **Malikzada Toghrul Azer oglu -** Doctoral student of the Forensic Expertise Center of the Ministry of Justice of the Republic of Azerbaijan (Azerbaijan). E-mail: togrul1996@gmail.com
**Karimov Shohlat Muzaffar oglu –** PhD in Law, Associate Professor of the “Law” Department of the NAA (Azerbaijan). E-mail: sohlet.kerimov@mail.ru

Respublikamızda bu gün kibercinayətlər hüquqi tənzimləmənin yetərincə lazımi səviyyədə olmaması nəticəsində cinayətkar qəsdlərin ən təhlükəli bir növü hesab edilir. Rəqəmsal texnologiyaların yüksək inkişafı nəticəsində yaşadığımız XXI əsr qlobal informasiya əsrinə çevrilib.

Azərbaycan Respublikası müstəqilliyini bərpa etdikdən sonra ən prioritet məsələlərdən biri də hüquq islahatlarının həyata keçirilməsi oldu.

Belə ki, insanlar məhkəmələrə müraciət edərək vaxt itkisi ilə, artıq maddi xərclərlə, kargüzarlığın düzgün aparılmaması və s. bu kimi digər problemlərlə qarşılaşırlar. Həmin problemlərin həll olunması üçün elektron məhkəmələrin istifadə olunması zəruri oldugundan Azərbaycan Respublikasının Prezidenti cənab İlham Əliyev 13 fevral 2014-cü il tarixində "Elektron məhkəmə informasiya sisteminin yaradılması haqqında" sərəncam imzaladı [1, s.5].

Müasir dövrdə rəqəmsal texnologiyalarının inkişafı və elektron məlumatların geniş yayılması nəticəsində kibercinayətlər sürətlə artmaqda davam edir. Son vaxtlar respublikamızda banklara müdaxilələr artmaqdadır. Demək olar ki, hər gün banklardan kiberdələduzluq yolu ilə hakerlər tərəfindən maddi vəsaitlər oğurlanır. Bu cinayətlər saniyələr içərisində baş verir və dərhal sübutlar silinir. Kiber müdaxilələrdə məkan anlayışı yoxdur. Bütün bunlar sübütların toplanmasını çətinləşdirir.

**İşin məqsədi** kibercinayətin vahid anlayışının olmaması məsələsinə aydınlıq gətirmək, "kompüter cinayəti" və "kibercinayət" terminlərinin oxşar və fərqli cəhətlərini izah etməkdir.

Kibercinayətlər unikal təbiəti ilə diqqəti cəlb edir. Bəzi mütəxəssislər hesab edirlər ki, bütün kompüter cinayətləri bir sıra fərqli xüsusiyyətlərə malikdirlər. Birincisi, müəyyən olunmuş faktlar üzrə sübutların toplanmasında həddindən artıq qapalılıq və mürəkkəblilik mövcuddur. Burda sübutların mürəkkəbliyi məhkəmədə oxşar işlərə baxılması zamanı ortaya çıxır. İkincisi, hətta az təsadüf edilən cinayətlər belə həddindən artıq yüksək maddi ziyanın vurulması ilə xarakterizə olunur. Üçüncüsü, bu cinayətlər yüksək ixtisaslaşmış sistem proqramistləri, telekommunikasiya sahəsinin mütəxəssisləri tərəfindən törədilir [2, s.5].

DİN-nin rəsmi məlumatına görə hər gün orta hesabla respublikada 20 min manat pul oğurlanır. Belə ki, AzTV-nin 29 aprel 2025-ci il tarixli məlumatına görə təkcə bir gündə vətəndaşların bank kartlarından kiberdələduzluqla 36 min manatdan çox pul çıxarılıb və bu proses hər gün davam edir [3]. Rəsmi məlumata görə kibercinayətlər hər il dünya iqtisadiyyatına 500 milyard dollar zərər vurur.

İnformasiya texnologiyaları sürətlə inkişaf edir. Demək olar ki, bütün sahələrdə rəqəmsallaşma prosesi başlamış və davam edir. Bu proses, öz növbəsində neqativ təzahürlərdən də yan keçməmişdir. Ən mühüm neqativ təzahürlərdən biri hesab edilən cinayətkarlığın yeni rəqəmsal növü olan kibercinayətkarlıq meydana qəlmiş və sürətlə inkişaf etmişdir. Kibercinayətkarlıq kifayət qədər mürəkkəb və xüsusi bilik tələb edən sahə olduğundan, həm onu törədən şəxslər, həm də bu cinayətlərlə mübarizə aparan orqanlar üçün müəyyən bacarıqlar tələb olunur [4, s.146].

Son vaxtlar respublikamızda rəqəmsal texnologiyaların sürətlə inkişafı və elektron məlumatların geniş yayılması nəticəsində kiberməkanla bağlı cinayətlərin sayı əhəmiyyətli dərəcədə artmışdır. Rəqəmsal sənədlərin saxtalaşdırılması süni intellektin vacib tətbiq istiqamətlərindən biri sayılır. Rəqəmsal texnologiya inkişaf etdikcə onun müsbət nəticələri ilə yanaşı mənfi tərəfləri də özünü büruzə verir. Belə ki, rəqəmsal texnologiyaların geniş tətbiq edildiyi vaxtda informasiya texnologiyalarından istifadə zamanı həm idarə və müəssisələrin, həm də insanların kiber hücumlara məruz qalması real həqiqətdir. Kibercinayətlərdə məkan söhbəti yoxdur. Kiber hücumlar ölkə

ərazisi ilə yanaşı istənilən xarici ölkə ərazisindən də törədilə bilər. Kibercinayətkarlığa qarşı səmərəli mübarizə aparmaq üçün cinayət hüququ sahəsində geniş və operativ beynəlxalqəməkdaşlıq tələb olunur. Kibercinayətkarlıqla mübarizədə müvafiq orqanların zəruri səlahiyyətlərinin artırılması, bu əməllərin həm ölkədaxili, həm də beynəlxalqsəviyyədə tədqiqatı, istintaqı və təqib olunmasına şəraitin yaradılması, sürətli və etibarlı beynəlxalq əməkdaşlığı təmin etmək yolu ilə kompüter sistem və şəbəkələrinin, o cümlədən kompüter verilənlərinin məxfiliyi, tamlığı və istifadə imkanlarına qarşı yönəlmiş hərəkətlərin, həmçinin bu sistem, şəbəkə və verilənlərdən qeyri-qanuni istifadənin qarşısının alınması mütləqdir [5, s.6].

"Süni intellekt" ifadəsi kompüter elmi sahəsində XX əsrin 60-cı illərində meydana gəlmişdir. İnsan təfəkkürü "süni intellekt" elminin tədqiqat predmetini təşkil edir. Belə tədqiqatların məqsədi insan zəkasının modelini yaratmaq və onu kompüterdə həyata keçirməkdir, yəni maşına düşünməyi öyrətməkdir.

Professor İ.M.İsmayılov qeyd edir ki süni intellekt (Sİ) insan davranışını və ya düşüncəsini təqlid edən və xüsusi problemləri həll etmək üçün öyrədilə bilən maşınla nümayiş etdirilən intellektdir. Sİ maşın və dərin öyrənmə üsullarının birləşməsidir. Böyük miqdarda məlumatlardan istifadə edərək öyrədilmiş süni intellekt modellərinin növləri ağıllı qərarlar qəbul etməyə qadirdirlər [6, s.18].

Hər hansı istənilən bir işi kompüter proqrama uyğun yerinə yetirir. Məlumdur ki, proqramları insanlar hazırlayır, kompüter isə icra edir. Süni intellektin tərtibatçıları maşına problemin şərtlərindən asılı olaraq bir şəxs kimi öz hərəkətlərinin proqramını müstəqil şəkildə qurmağı öyrətməyə çalışırlar, yəni məqsəd kompüteri formal icraçıdan intellektual icraçıya çevirməkdir [6, s.19].

Haqlı olaraq XXI əsri qlobal informasiya əsri adlandırırlar. Son dövrlər informasiya əhəmiyyətinin sürətli inkişafı, qloballaşmanın daha geniş məkanlara, o cümlədən informasiya mühitinə təsir etməsi transmilli cinayətlərə, ayrı-ayrı ölkələrinin milli hüququnda yeni cinayətlər kateqoriyasının yaranmasına və cəza sisteminə öz təsirini göstərmişdir.

Respublikamızda kibercinayətlər bu gün hüquqi tənzimləmənin zəifliyi nəticəsində cinayətkar qəsdlərin ən təhlükəli növlərindən birinə çevrilmişdir.

Bəzi internet istifadəçiləri yüksək intellektual bacarıq və qabiliyyətlərindən sui-istifadə edərək hüquqazidd davranışları ilə cinayət tərkibi yaradan əməllərə səbəb olur. Belə şəxslər tez-tez rəqəmsal texnologiyalardan, kompüter və internet şəbəkələrindən, bankomatlardan, ödəniş kartlarından və s. cinayətkar məqsədlərlə kiberdələduzluq yolu ilə cinayət xarakterli əməllər törədirlər.

Transmilli cinayət hesab olunan kibercinayətlərə beynəlxalq hüquqda hələ ki, vahid anlayış verilməyib. Dünya ölkələri bu sahədə konsensusa gəlməyiblər. 1979-cu ildə kompüter cinayəti termini ilk dəfə İNTERPOL tərəfindən Üçüncü Beynəlxalq Dələduzluq Simpoziumunda işlədilmişdir.

Maraqlıdır ki, nə kibercinayətkarlıq haqqında 2001-ci il Budapeşt Konvensiyasında [7], nə 2010-cu ildə qəbul olunmuş Ərəb Dövlətləri Liqası tərəfindən İnformasiya texnologiyaları cinayətləri ilə mübarizə haqqında Ərəb Konvensiyasında, nə də Afrika Birliyinin Afrikada kibertəhlükəsizlik fəaliyyəti haqqında 2012-ci il tarixli Konvensiyalarının heç birində kibercinayətkarlıq termininə anlayış verilməyib. Milli hüquq ədəbiyyatlarında kibercinayətkarlığa hər bir ölkə ayrı-ayrı anlayışlar vermişlər.

Beynəlxalq aləmdə kibercinayətlərə vahid anlayış verilmədiyinə görə bu gün dünyanın heç bir dövlətinin milli qanunvericiliyində kibercinayətin dəqiq tərifi verilməmişdir.

Oksford izahlı lüğətində “kiber” (cyber) anlayışının hərfi mənası “informasiya texnologiyalarına, internet şəbəkəsinə və virtual reallığa aid olan” kimi dilimizə tərcümə olunur.

Kembric lüğətində isə “kibercinayət” - həm kompüterlərin istifadəsi ilə, həm də informasiya texnologiyalarının və qlobal şəbəkələrin istifadəsi ilə bağlı olan cinayət kimi verilir. Kembric lüğətində “cybercrime” – “kibercinayəykarlıq” kimi tərcümə olunur. Xarici müəlliflərin əksəriyyəti “cybercrime” – “kibercinayətkarlıq” termini daha uğurlu hesab edirlər. Qeyd olunur ki, kibercinayətkarlıq termini kompüter cinayətləri terminindən daha geniş mənada işlədilir.

Azərbaycanlı alim S.T.Məcidli kibercinayətlərə belə anlayış vermişdir: “kibercinayətlər dedikdə, internet şəbəkəsindən qanunsuz sui-istifadə nəticəsində kompüter və informasiya sistemlərinin dağıdılması və cəzalandırılmalı, hüquqazidd ictimai təhlükəli əməllər başa düşülür” [8, s.114]. S.T.Məcidli haqlı olaraq bu tərifdə göstərir ki, kibercinayət anlayışı təkcə bir kompüterdə və ya lokal informasiya məkanında törədilən qanunsuz əməl olmayıb, eyni zamanda, bu fəzada bütün texnoloji vasitələr arasında əlaqələndirici rolunda çıxış edən internet vasitəsilə törədilən çoxsaylı hüquqazidd əməlləri özündə birləşdirir.

DİN-nin Polis Akademiyasında buraxılan dərs vəsaitində göstərilir ki, “kibercinayət – informasiya və telekommunikasiya texnologiyalarından istifadə etməklə törədilən təqsirli, ictimai təhlükəli, cinayət məsuliyyəti nəzərdə tutulan əməldir” [9, s.19].

Başqa bir anlayışda isə qeyd edilir ki, “kibercinayət – informasiya texnologiyalarından istifadə edilərək həyata keçirilən, informasiya sisteminin güvənliyini, sistemə bağlı informasiya ehtiyatlarını və eyni zamanda bu texnologiyalardan istifadə edən istifadəçiləri hədəfə alan cinayətdir. Kibercinayət əsasən kompüter və internetlə bağlı törədilən cinayətlər hesab edilir” [5, s.12].

“Kibercinayət – həm kompüterlərin istifadəsi, həm də informasiya texnologiyalarının və qlobal şəbəkələrinin istifadəsi ilə bağlı olan cinayətdir”.

Kibercinayətlərə dair vahid beynəlxalq anlayış olmadığı üçün xarici ölkələrdə də bu sahəyə yanaşma müxtəlifdir. Məsələn, ispaniyalı professor J.R.Agustina kibercinayətləri nadir cinayətlər kateqoriyasına aid edir və göstərir ki, bu cinayətlərə internetdən istifadə etməklə törədilən dələduzluq, insanların narahat edilməsi və ya onlara qarşı xuliqanlıq, qanunsuz pornoqrafiyanın yüklənilməsi, musiqilərin oğurlanması, milli təhlükəsizliyinin pozulması kimi əməllər aiddir [10,s.1044-1048]. Bu tərifdən görünür ki, kompüter proqramları və qlobal şəbəkəyə aid olan digər hüquqazidd əməllər kibercinayət kimi qiymətləndirilir. Bəzi beynəlxalq təşkilatlar da kibercinayətlərin anlayışı ilə bağlı məsələlərə həssaslıqla yanaşırlar. Belə ki, Şanxay Əməkdaşlıq Təşkilatına üzv olan dövlətlər kibercinayətkarlıqla mübarizə aparmaq üçün bağladıqları müqavilədə “qanunsuz məqsədlərlə informasiya resurslarının və (və ya) informasiya sferasında onlara təsir etmək üçün istifadəsi” ilə əlaqədar olan əməlləri “informasiya cinayətləri” kimi müəyyən edir [11]. Bu tərifdən belə görünür ki, Şanxay Əməkdaşlıq Təşkilatı “kibercinayətləri” “informasiya cinayətləri” hesab edirlər.

Ukrayna cinayət məcəlləsinin XVI bölməsində kibercinayətlərlə bağlı üç maddə nəzərdə tutulub. 361-ci maddə elektron-hesablama maşınlarının (kompüterlərin), kompüter sistemlərinin və şəbəkələrinin işinə qanunsuz müdaxilə, 362-ci maddə kompüter informasiyanın oğurlanması, mənimsənilməsi, zorla əldə edilməsi və ya dələduzluq yolu ilə ona malik olma, 363-cü maddəsi isə avtomatlaşdırılmış elektron-hesablama sistemlərinin istismar qaydaların pozmağa həsr olunub.

Ukraynada “kibercinayətlərə” əsasən kompüter cinayətləri kimi yanaşılır. Ukraynada 2003-cü ildə kibercinayətlərlə mübarizə məqsədi ilə “İctimai əxlaqın müdafiəsi haqqında” Qanun qəbul olunmuşdur. Həmin qanunda internet və digər kütləvi informasiya vasitələrində pornoqrafik məlumatların, pornoqrafik xarakter daşıyan şəkillərin, rəsmlərin, xüsusən, uşaq pornoqrafiyasının yayılmasına görə ciddi məsuliyyət nəzərdə tutulur.

Tarixi inkişaf baxımından kibercinayətlər elə ilk dəfə ABŞ-də törədilmişdir. Bu ölkədə kibercinayətlər artdıqca və transmilli əhəmiyyət kəsb etdikcə dövlət məcbur olub 1977-ci ildə “ABŞ federal kompüter sistemlərinin müdafiəsi haqqında” Qanun layihəsi hazırladı. 1984-cü ildə isə həmin Qanun layihəsi əsasında ABŞ-də “Kompüter dələduzluğu və sui-istifadəsi haqqında” kibercinayətlərə dair ilk Qanun qəbul edildi.

Bu Qanun hal-hazırda ABŞ-ın 18-ci Qanunlar külliyatına daxil edilmiş və fəaliyyət göstərir. ABŞ-də həmin külliyatın 47-ci fəslinin 1030-cu maddəsində kompüter cinayətləri yeddi əsas tərkibə - kompüterlərdən istifadə etməklə dələduzluq; kompüter casusluğu; ABŞ hökümət idarələrinin müstəsna istifadəsində olan kompüterlərə təsiretmə və ya fəaliyyətinin pozulması; kompüter texnologiyalarından istifadə etməklə törədilən hədələr, şantaj, zorakılıq və başqa hüquqazidd əməllərə və s. görə cinayət məsuliyyətinə səbəb olur.

ABŞ-ın 2013-cü il “kibertəhlükəsizlik haqqında” yeni Qanun layihəsində cəza sərtləşdirilərək 30 il müddətinə verilə bilər.

Kiberhücumlar qardaş Türkiyə Cümhuriyyətindən də yan keçməmişdir. Türkiyə Cümhuriyyətində kibercinayətlərlə mübarizənin əsası 1991-ci ildə qoyulmuşdur. Belə ki, həmin ildə kibercinayətlərlə mübarizə məqsədi ilə Türk Cəza Qanununa 525-ci maddə əlavə edildi. 2005-ci ildə Türkiyədə yeni 5237 saylı Türk Cəza Qanunu qəbul edilmişdir. Bu qanunun 10-dan çox maddəsi kibercinayətlərə həsr olunub. Məsələn, 243-cü maddə kompüter sisteminə qanunsuz olaraq girmə və sistemdə qalma adlanır. Qanunun 244-cü maddəsi sistemi ənqəlləmə, pozma, verilənlərinin yox etmə və ya dəyişdirmə, 245-ci maddə isə bank və ya kredit kartları ilə pis davranmaya həsr olunub.

2012-ci ildə Türkiyədə Milli Kibertəhlükəsizlik çalışmalarinin yürüdülməsi, yönəldilməsi və əlaqələndirilməsi haqqında Qərar qəbul edilmişdir. Həmin qərarda 2013-2014-cü illəri əhatə edən Milli kibertəhlükəsizlik strategiyasının həyata keçirilməsi Türkiyə dövlətinin prioritet vəzifəsi elan edilmişdir. Kibercinayətlərdə təqsirli şəxslərin tutulması, həbs olunması, ibtidai araşdırılması Türkiyədə polis şöbələrində, Baş istintaq idarəsində və Kibercinayətlərlə mübarizə idarəsində həyata keçirilir.

S.T.Məcidli kibercinayətə 2019-cu ildə verdiyi sonuncu anlayış daha ağlabatandır. O, yazır: “kibercinayət kompüter sistemlərinə və ya digər informasiya texnologiyaları şəbəkələrinə, cəmiyyətin informasiya təhlükəsizliyinə və kiber maraqlarına əhəmiyyətli ziyanın vurulması ilə xarakterizə edilən hərəkət və hərəkətsizlikdən ibarət transmilli cinayətdir” [12, s.45]. Bu tərifin üstün cəhəti ondan ibarətdir ki, digər anlayışlarda dar mənada işlədilən “kompüter sistemi” termini ifadəsi yerinə daha geniş “digər informasiya texnologiyaları şəbəkələri” ifadəsindən istifadə olunmuşdur ki, bu da android və ya yüksək texnoloji qurğuları, mobil telefonları, eyni zamanda bankomat və elektron ödəmə sistemlərini də özündə birləşdirir.

Belə nəticəyə gəlmək olar ki, kibercinayətlər beynəlxalq cinayətlərin sürətlə inkişaf edən bir sahəsidir. Kibercinayətlərə həm milli, həm də beynəlxalq ədəbiyyatlarda verilən anlayışları araşdıraraq bu nəticəyə gəlmək olar ki, kompüter şəbəkələrində və ya kibeməkanda törədilən hüquqazidd hərəkət və hərəkətsizlikləri göstərən “kompüter cinayətləri”, “informasiya cinayətləri”,

“yüksək texnologiya cinayətləri”, “kompüter informasiyasına aid cinayətlər” və “kibercinayətlər” terminlərininarasında ən çox “kibercinayətlər” ifadəsinin işlədilməsi məqsədəuyğün hesab olunur.

Beynəlxalq aləmdə baş verdiyinə, məkansız olduğuna və transmilli xarakter daşıdığına görə kibercinayətlərə aşağıdakı anlayışın verilməsi təklif olunur: “Kibercinayətlər kompüterlərdən, kompüter proqramlarından, kompüter şəbəkələrindən, o cümlədən internet və sosial şəbəkələrdən, informasiya resurslarından və informasiya daşıyıcılarının digər qurğularından qanunsuz istifadə nəticəsində kompüter və informasiya sistemlərinin dağıdılması ilə nəticələnən və əhəmiyyətli zərərlə xarakterizə olunan, virtual məkanda qəsdən törədilən, cəzalandırılmalı, hüquqazidd ictimai təhlükəli hərəkət və hərəkətsizlik kimi başa düşülür” [12, s.44].

Xüsusilə qeyd etməliyik ki, nə nəzəriyyədə, nə praktika, nə də kibercinayətkarlıq sahəsində ən vacib beynəlxalq sənəd olan 23 noyabr 2001-ci il tarixli Budapeşt Konvensiyasında kibercinayətlərə vahid anlayış verilmədiyinə görə, beynəlxalq konsensusun mövcud olmamasına görə dünyanın hər bir ölkəsi öz milli maraqlarına uyğun kibercinayətlərə anlayış vermişlər.

Bu sadəcə insanların hüquq və mənafelərinə, dünya ölkələrinin iqtisadiyyatına vurulan milyardlarla dollar həcmində maddi və mənəvi ziyanı nəzərə alaraq dünya ölkələrinin konsensusa gəlməsi və kibercinayətlərə vahid anlayışının verilməsi ən vacib və qaçılmaz məsələlərdən biridir. Bu zamananın tələbidir, çünki bütün dünya ölkələri kiberdələduzluqdan əziyyət çəkir. Rəsmi statistikaya görə müasir dövrdə tək respublikamızda deyil, dünyanın əksər ölkələrində rəqəmsal texnologiyalardan, kompüter və internet şəbəkələrindən, bankomatlardan, ödəniş kartlarından və s. cinayətkar məqsədlərlə istifadə edilməsi ilə əlaqədar törədilən cinayətlər artmaqda davam edir.

BMT, İƏT, İNTERPOL, Avropa Şurası və Avropa Birliyi kimi beynəlxalq təşkilatlar kibercinayətkarlığın təhlükəsini, transsərhəd xarakterə malik olduğundan bir tərəfli yanaşmanın məhdudluğunu, həm də bu problemin həlli üçün texniki tədbirlərlə yanaşı beynəlxalq qanunvericiliyin yaradılmasında beynəlxalq əməkdaşlığın gücləndirilməsini istəyirlər. Bu beynəlxalq təşkilatlar yüksək texnologiyalar sferasında cinayətlərlə mübarizədə beynəlxalq əməkdaşlığın qurulmasında mühüm rola malikdirlər.

Xarici ölkələrin qanunvericiliyində indi də fərqli anlayışlardan – kompüter cinayətləri, yüksəktexnologiya cinayətləri, elektron kommunikasiyalar, informasiya texnologiyaları və kibercinayətlər terminlərindən istifadə olunur. Bu terminlər arasındakı oxşarlıq və fərqli cəhətlər mübahisə predmeti olaraq qalmaqda davam edir. “Kibercinayətkarlıq” termini adətən “kompüter cinayətkarlığı” termini ilə birgə istifadə olunur. Lakin bu anlayışlar heç də sinonim deyildir. Həqiqətən də bu terminlər bir-birinə çox yaxın olsalarda, bütün hallarda həmçinin fərqlənirlər. Belə ki, “kibercinayətkarlıq” termini «kompüter cinayətkarlığı» terminindən daha geniş anlayış olub, informasiya məkanında törədilən cinayət olaraq bu hadisənin mahiyyətini daha dəqiq əks etdirir [13, s.148].

Azərbaycan Respublikasında süni intellektin inkişafını sürətləndirmək, bu sahədə tədqiqatlarınaparılmasını təşviq etmək, süni intellekt üzrə informasiya texnologiyalarının və onların idarə edilməsi mexanizmlərinin təkmilləşdirilməsini, infrastrukturunun əlçatanlığını təmin etmək, habelə ixtisaslı kadr potensialını gücləndirmək məqsədilə cənab Prezident İlham Əliyev “Azərbaycan Respublikasının 2025-2028-ci illər üçün süni intellekt strateqiyası”nın təsdiq edilməsi haqqında 19 mart 2025-ci ildə 530 saylı Sərəncam imzalamışdır. Həmin Sərəncamda AR-nın Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti dövlət orqanlarında süni intellektin tətbiq edildiyi sahələrdə informasiya təhlükəsizliyi risklərinin həyata keçirilməsi, o cümlədən dövlət

orqanlarında (qurumlarında) süni intellektlə bağlı informasiya təhlükəsizliyinin təmin edilməsi üçün zəruri tədbirlərin görülməsi nəzərdə tutulur [14].

Beləliklə, **bu nəticəyə gəlmək olur ki**, transmilli cinayət olan kibercinayətlərin beynəlxalq hüquqda vahid anlayışının olmamasının səbəbi Avropa Şurasının "Kibercinayətkarlıq haqqında" Konvensiyasında "kibercinayət" anlayışının verilməməsidir. Dünya ölkələri də vahid anlayışın olmadığına görə öz ölkələrinin milli maraqlarına uyğun kibercinayətlərə müxtəlif səpgidəanlayışlar vermişlər. Kibercinayətlərə anlayış verilərkən tək hüquq elminin deyil, həm də informatika, fizika və s. elmlərdə olan terminlərindən istifadə olunmalıdır.

## Biblioqrafiya

1. Ayxan Rüstəmzadə, Könül Məmmədova. Elektron məhkəmənin ədalət mühakiməsi sistemində hüquqi əsasları. – Bakı: Elm və təhsil, 2017. - 76 s.

2. Тимошкина Ю.М.,Компьютерные преступления. – М., 2010. [Elektron resurs]. URL: http://workcal.ru

3. AzTV-nin"Xəbərlər" programı. Bakı, 29.04.2025-ci il

4. Ağayev Kənan. Yetkinlik yaşına çatmayan şəxslər barəsində törədilən kibercinayətlərin araşdırılmasının texniki-kriminalistik problemləri/Beynəlxalq elmi-praktik konfransın materialları. DİN-nin Polis Akademiyası. Bakı, 23 aprel 2025-ci il, 293 s.

5. Kibercinayətlərin istintaqına dair metodik vəsait. - Bakı, AR-nın Baş Prokurorluğu, AR-nın DTX, 2022. - 66 s.

6. İsmayılov İ.M. Süni intellekt. - Bakı, MAA, 2023. - 233 s.

7. Kibercinayətkarlıq haqqında Konvensiya. Budapeşt, 23 noyabr 2001-ci il, 114 s.

8. Məcidli S.T. İnternet hüququ və etikası. Dərs vəsaiti. - Bakı: Elm və təhsil. -114 s.

9. Məmmədov O., Rzayev E., Hüseynov N., Daxili İşlər orqanlarında xüsusi texnika və kibertəhlükəsizlik fəaliyyəti. -Bakı, 2023. - 207 s.

10. Agustina J.R., Book rewiew of cyber criminology: Exploring internet crimes and criminal behaviour// International Journal of Cyber Criminology (IJCC). İCCN: 0974-2891, July-December 2012, vol.6(2)p1044-1048.

11. Shanghai Cooperation Organisation Agreement, Annex 1. [Elektron resurs]. URL: http//www.loc.gov/

12. Məcidli S.T., Kibercinayətlər. - Bakı, 2019. - 314 s.

13. Номоконов В.А., Тропина Т.Л., Киберпреступность: угрозы, прогнозы, проблемы борьбы. // Библиотека криминалиста. - №5(10). – 2013. - 148 с.

14. "Azərbaycan Respublikasının 2025-2028-ci illər üçün süni intellekt Strategiyası"nın təsdiq edilməsi haqqında Sərəncam №530. Bakı, 19 mart 2025-ci il.

***Məqalə daxil olmuşdur:*** *20 mart 2025-ci il*
***Çapa qəbul edilmişdir:*** *11 aprel 2025-ci il*

### References


1. Aykhan Rustamzade, Konul Mammadova. Legal foundations of electronic court in the justice system. Baku, Science and Education Publ., 2017, 76 p. (in Azerbaijani).
2. Timoshkina Y.M., Computer crimes. Moscow, 2010. Available at: https://workcal.ru (in Russian).
3. AzTV's "News" program. Baku, 04.29.2025 (in Azerbaijani).
4. Aghayev Kenan. Technical and forensic problems of investigating cybercrimes committed against minors / Materials of the International Scientific and Practical Conference. Police Academy of the Ministry of Internal Affairs. Baku, April 23, 2025, 293 p. (in Azerbaijani).
5. Methodological manual on the investigation of cybercrimes. Baku, Prosecutor General's Office of the Republic of Azerbaijan, State Security Service of the Republic of Azerbaijan, 2022, 66 p. (in Azerbaijani).
6. Ismayilov I.M. Artificial intelligence. Baku, NAA Publ., 2023, 233 p. (in Azerbaijani).
7. Convention on Cybercrime. Budapest, November 23, 2001, 114 p.
8. Majidli S.T. Internet law and ethics. Textbook. Baku, Science and Education Publ., 114 p. (in Azerbaijani).
9. Mammadov O., Rzayev E., Huseynov N., Special equipment and cybersecurity activities in internal affairs bodies. Baku, 2023, 207 p. (in Azerbaijani).
10. Agustina J.R., Book review of cyber criminology: Exploring internet crimes and criminal behavior// International Journal of Cyber Criminology (IJCC). ICCN: 0974-2891, July-December 2012, vol.6(2) p.1044-1048.
11. Shanghai Cooperation Organization Agreement, Annex 1. Available at: https://loc.gov/
12. Majidli S.T., Cybercrimes, Baku, 2019, 314 p. (in Azerbaijani).
13. Nomokonov V.A., Tropina T.L., Cybercrime: threats, prognoses, problems of struggle // Biblioteka criminalista. No. 5(10) 2013, 148 p. (in Russian).
14. Decree No. 530 on approval of the "Artificial Intelligence Strategy of the Republic of Azerbaijan for 2025–2028". Baku, March 19, 2025. (in Azerbaijani).


***The article was submitted:*** *2025 March 20*

***Accepted for publication:*** *2025 April 11*

**Маликзаде Т.А.,**
**Каримов Ш.М.**♦

**DOI: 10.25108/2304-1730-1749.iolr.2025.79.76-84**
**УДК: 34:343.1**

## Определение и общая характеристика киберпреступности

♦ **Маликзаде Тогрул Азер оглы -** докторант Центра судебно-медицинской экспертизы Министерства Юстиции Азербайджанской Республики (Азербайджан). E-mail: togrul1996@gmail.com
**Каримов Шохлет Музаффар оглы -** доктор философии права, доцент кафедры «Право» НАА (Азербайджан). E-mail: sohlet.kerimov@mail.ru

**Аннотация:** Работа посвящена понятию киберпреступности и общей характеристике киберпреступлений. Отмечается, что в настоящее время киберпреступность продолжает стремительно расти в результате развития цифровых технологий и повсеместного распространения электронной информации.

Отмечается, что по мере развития цифровых технологий в результате применения искусственного интеллекта наряду с положительными результатами становятся очевидными и его отрицательные стороны.

Рассматриваются и анализируются понятия «компьютерная преступность» и «киберпреступность» в национальном законодательстве нашей республики и ряда зарубежных стран.

**Ключевые слова:** искусственный интеллект; цифровые технологии; киберпреступность; компьютерная преступность; информационная преступность; интернет-сеть; информационные технологии; хакеры; киберпространство.

***Дата поступления:*** *20 марта 2025 г.*
***Дата принятия в печать:*** *11 апреля 2025 г.*