Kərimov Ş.M.♦

UOT: 343

Azərbaycan Respublikasında kibercinayətkarlıq fəaliyyəti və onun səciyyəvi xüsusiyyətləri

Xülasə: Məqalə son illər respublikamızda sürətlə çoxalan kibercinayətkarlığa həsr olunub.

Məqalədə xüsusilə qeyd edilir ki, hal-hazırda kibercinayətlər respublikamızda ən geniş yayılan cinayət növlərindən biridir. Müasir dövrdə rəqəmsal texnologiyanın inkişafı sayəsində süni intellekt insan davranışını və ya düşüncəsini təqlid edən və xüsusi problemləri həll etmək üçün öyrədilə bilən və maşın ilə nümayiş etdirilən intellektdir.

Məqalədə həmçinin kibercinayətlərin latentliyi, sübutların çox tez məhv edilməsi, buna görə də bu cinayətlərin istintaqının çətin olması göstərilir.

Məqalədə həm də qeyd edilir ki, rəqəmsal və şəbəkə texnologiyaları sayəsində kibercinayətlər əsasən, dələduzluq, aldatma, zorakılıq və hədə-qorxu vasitəsilə törədilir.

Açar sözlər: kibercinayətkarlıq; internet şəbəkəsi; xakerlər; süni intellekt; rəqəmsal texnologiya; kiberhücum; kompüter cinayəti; kompüter məlumatları; dələduzluq; latentlik; virus proqramları.

Müasir dövr rəqəmsal texnologiyanın inkişafı dövrüdür. Süni intellekt keçən əsrin 60-cı illərindən meydana gəlməyə başlamışdır. İnsan təfəkkürü süni intellekt elminin tədqiqat predmeti hesab olunur. İnsan zəkasının modelini yaradıb onu kompüter vasitəsilə həyata keçirmək süni intellektin əsas məqsədidir.

Prof. İ. İsmayılov göstərir ki, süni intellekt informatikanın istiqamətlərindən biridir. Onun məqsədi proqramçı olmayan istifadəçiyə ənənəvi olaraq intellektual hesab edilən təbii dilin məhdud altçoxluğunda maşınla ünsiyyət quran öz vəzifələrini təyin etməyə və həll etməyə imkan verən aparat və proqram vasitələrinin işlənib hazırlanmasıdır.

Süni intellekt insan davranışını və ya düşüncəsini təqlid edən və xüsusi problemləri həll etmək üçün öyrədilə bilən maşınla nümayiş etdirilən intellektdir. Süni intellekt maşın və dərin öyrənmə üsullarının birləşməsidir. Böyük miqdarda məlumatlardan istifadə edərək öyrədilmiş süni intellekt modellərinin növləri ağıllı qərarlar qəbul etməyə qadirdirlər [8, s. 18].

Hal-hazırda Azərbaycan Respublikasında ən geniş yayılan cinayət növlərindən biri də kibercinayətlərdir. Keçmiş Cinayət Məcəlləsində kiber cinayətlər nəzərdə tutulmurdu. 1999-cu ilin Cinayət Məcəlləsinin XXX fəsli "Kompüter informasiyası sahəsində cinayətlər" adlanırdı [1. s, 243].

Məcəllə qəbul olunanda XXX fəsildə cəmi 3 maddə, 271-273-cü maddələr mövcud idi. 23 noyabr 2001-ci ildə Avropa Şurası "Kibercinayətlər haqqında" Konvensiya qəbul etmişdir. AR-nın Milli Məclisi "Kibercinayətkarlıq haqqında" Konvensiyanı 30 sentyabr 2009-cu ildə ratifikasiya etmişdir. AR-nın 29 iyun 2012-ci il tarixli Qanunu ilə XXX fəslin adı dəyişdirilərək

♦ **Kərimov Şöhlət Müzəffər oğlu** - Milli Aviasiya Akademiyasının "Hüquq" kafedrasının dosenti, h.f.d. (Azərbaycan). E-mail: ruslan.mirzeliyev@rambler.ru

"Kibercinayətlər" adlandırıldı. 2017-ci ilin 31 mayında həmin fəslə iki yeni maddə- "Kibercinayətlərin törədilməsi üçün hazırlanmış vasitələrin dövriyyəsi" (M-273-1) və "Kompüter məlumatlarının saxtalaşdırılması" (M-273-2) əlavə olundu [2, s. 269-270].

Dünya miqyasında kibercinayətlərə hələ ki, vahid anlayış verilməyib. Hüquq ədəbiyyatında əsasən, informasiya və telekominikasiya texnologiyalarından istifadə etməklə törədilən təqsirli, ictimaitəhlükəli, cinayət məsuliyyəti nəzərdə tutan əməllər kibercinayət hesab edilir.

S.T.Məcidli kibercinayətləri başqa növ cinayətlərdən fərqləndirərkən qeyd edir ki, informasiya texnologiyalarından istifadə edərək həyata keçirilən, informasiya sisteminin güvənliyini, sistemə bağlı olan informasiya ehtiyatlarını və eyni zamanda bu texnologiyalardan istifadə edən istifadəçiləri hədəfə alan cinayətlər kibercinayətlər hesab olunur. Kibercinayətlər dedikdə, internet şəbəkəsindən qanunsuz istifadə nəticəsində kompüter və informasiya sistemlərinin dağıdılması və virtual məkanda qəsdən törədilən digər cəzalandırılmalı, hüquqa-zidd, ictimai-təhlükəli əməllər başa düşülür [12, s. 29].

Kibercinayətlər ilk dəfə "Kompüter cinayətləri" termini kimi 1979-cu ildə keçirilmiş Beynəlxalq Dələduzluq simpoziumunda istifadə edilmişdir.

Qeyd etmək lazımdır ki, rəqəmsal və şəbəkə texnologiyaları sayəsində ən çox yayılmış aldatma, dələduzluq, hədə-qorxu və zorakılıq kimi əməllər kibercinayətlərə aid edilir.

İşin məqsədi gündən-günə respublikamızda artan kiber hücumlardan əhalini qorumaq üçün ayıq-sayıq olmağa çağırmaqdır.Eyni zamanda kibercinayətlərin vaxtında araşdırılması və açılması üçün əhaliyə nəzəri və təcrübi bacarıqları aşılamaqdır.

Kibercinayətkarlığa qarşı mübarizədə texniki vasitələrdən geniş və düzgün istifadə edilməsi hüquqpozmaların qarşısının alınması, eləcə də qarşıya qoyulan məsələlərin müvəffəqiyyətlə həll olunmasında mühüm əhəmiyyət kəsb edir.

Kibercinayətlərlə mübarizə ən aktual bir mövzuya çevrilmişdir. "Xəzər" TV-nin 23 may 2024-cü ildə "Xəbərlər" proqramında verdiyi məlumata görə bir gündə respublikamızda banklara 22 kiberhücum olub və ümumilikdə 35500 manat dələduzluq yolu ilə bank kartlarına müdaxilə etməklə pul çıxarılıb [6].

Elm və rəqəmsal texnologiyanın yüksək inkişafı sayəsində internet cinayətkarlara dünyanın istənilən yerində olan qurbanlarına çıxış imkanı verir. Onlar internetdən aşkar edilmədən məlumat mübadiləsi, oğurlanmış məlumatların, malların və xidmətlərin ticarəti, qeyri-qanuni yolla əldə edilmiş pulların yuyulması, kibercinayətkarlıq üçün istifadə olunan üsul və vasitələrin mübadiləsi üçün istifadə edirlər. Bu növ cinayətkarlar təkbaşına və ya müxtəlif mütəşəkkil cinayətkar qrupların tərkibində fəaliyyət göstərirlər [5, s. 118].

Kibercinayətkarlıqla mübarizədə əksər postsovet ölkələri kiber savadlılığın artırılması üçün geniş tədbirlər görürlər. Məsələn, 27.05.2024-cü ildə Moskvada II Beynəlxalq Kibertəhlükəsizliyi festivalı keçirilib. Bu festivalda 50-yə yaxın komanda və kibertəhlükəsizlik üzrə ən yaxşı mütəxəssislər dəvət edilib. Azərbaycan Respublikası da bu festivala dəvət olunmuşdur.

Kibercinayətkarlıqla mübarizə sahəsində Azərbaycan Respublikasında daKibertəhlükəsizlik Mərkəzi yaradılıb. Rəsmi statistikaya görə 2023-cü ildə 7 mindən çox şəxs respublikamızda xakerlərin qurbanı olub. Elə ona görə də respublikamızda kibertəhlükəsizlik kursları fəaliyyət göstərir. 60-dan çox mütəxəssisə sertifikat verilib və onların çoxu banklarda işləyir.

Ümid edirik ki, respublikamızda bizi təhlükəsiz rəqəmsal gələcək gözləyir.

Kibercinayətkarlıq başqalarından onunla fərqlənir ki, bu cinayətləri törədənlər heç də savadsız, avara deyillər, onların çoxu yüksək intellektə malik olan, savadlı, "ağköynəkli", "boynu

qalstuklu" şəxslərdir. Kibercinayətləri törədən şəxslərin internet şəbəkəsi ilə işləmələri və kompüter bacarıqları mükəmməl olur. Həm də kibercinayətkarlığın latentliyi daha çox olur.

Statistikaya nəzər salsaq görərik ki, Azərbaycan Respublikasında kibercinayətkarlığın səviyyəsi gündən-günə artır. DİN-nin mətbuat xidmətinin verdiyi məlumata görə iki gün ərzində- 6-7 iyul 2024-cü il tarixində 51 vətəndaşa qarşı kiber üsulla banklardan 90000 manat pul çıxardılıb. Bu da respublikamızda kiber hücumların artım sürətinin gündən-günə çoxaldığını göstərir. Bunun qarşısının alınmasının əsas üsulu şəxsi məlumatların, bank hesablarının qorunub saxlanmasıdır. Kiber hücumların qarşısını almaq üçün radio, televizor və KİV-də gündəlik maarifləndirmə işi aparılmalıdır. Belə maarifləndirmə işlərinə mütləq mütəxəssislər dəvət edilməlidir. Bəs nə etməli? Bunun qarşısını almaq, kökünü kəsmək mümkündürmü? Respublikamızda kibercinayətkarlığın gələcəyi necə olacaq? Bu problemi necə həll etmək olar?

Ümumiyyətlə, "cinayətlərin kökünü kəsmək" sovet ideologiyasına məxsusdur. Cinayətkalıqla mübarizə insan imkanları daxilindədir. Ancaq bu məsələdə onun tam kökünün kəsilməsi haqqında absurd məsələlər qoyulmamalıdır [14, s. 7]. Cinayət bütün zamanlarda mövcud olmuş və olacaqdır. E. Pozdnyakov qeyd edir ki, cinayətkarlıq insan təbiətinin, yəni bütün insanlığın gözəl və hərtərəfli elementlərindən biridir [15, s. 502]. Beləliklə, həqiqət ondan ibarətdir ki, cinayətkarlıq problemini heç bir sosial-siyasi sistem həll edə bilməmişdir. Kibercinayətkarlığın gələcəyi haqqında problem maraq kəsb edir. Burada söhbət yalnız bu hadisənin əbədi və ya müvəqqəti olmasında deyil, həm də onun yaxın gələcəyindən bəhs edir. Bu maraq təbii olaraq onun qarşısının alınmasına hazır olmaq zərurətindən doğur [13, s. 131, 133].

Kibercinayətkarlığın səciyyəvi xüsusiyyətlərindən biri də ondan ibarətdir ki, başqa cinayətlərdən fərqi olaraq bu cinayətlərin üstü çox gec açılır. Çünki, kibercinayətlərdə onu törədənlərin şəxsiyyətini və yerini müəyyən etmək çox çətindir. Çünki bu cinayətlər həm latentliyi, həm də bir çox hallarda transmilli olması ilə fərqlənir.

Kibertexnologiyalardan asılı olmaqla, kibertexnologiyalardan istifadə etməklə kibercinayətkarlıq iki hissəyə ayrılır.

Hüquq ədəbiyyatında kibercinayətlərin törədilmə səbəbləri barədə müxtəlif fikirlər mövcuddur. Kibercinayətkarları həm cinayət törətməyə sövq edən, həm də onları motivasiya edən amilləri üç yerə ayırırlar:

1. Xakerlər və həvəsli gənclər internetlə və kompüterlə əyləncəli bir oyun aparatı kimi məşğul olurlar. Onların məqsədi başqalarına ziyan vurmaq deyil, sadəcə olaraq öz bacarıqlarını nümayiş etdirməkdir. Bununla da onlar başqalarının şəbəkələrinə qanunsuz daxil olur, onların veb səhifələrini "dağıdır": Belə halda niyyətləri olmasa da digərlərinə zərər vururlar.

2. Şan-şöhrət hissinin üstün gəlməsi: burada söhbət populyar olmaqdan, özünü "gözə soxmaqdan", özünün bacarıq və qabiliyyətini başqalarına göstərməkdən ibarətdir.

3. Səbəblərdən biri də tamahdır. Burada tək gənclər deyil, kişilər, qadınlar, qocalar və peşəkarların məqsədi qanunsuz pullar əldə etməkdir. Xakerlər və ya bank işçisi tərəfindən başqa şəxsin bank hesabının ələ keçirilməsi və kredit kartının oğurlanmasını göstərə bilərik. Məsələn, Bakıda sosial evlərin onlayn bölüşdürülməsi zamanı xakerlər kibercinayətkarlıq törədərək pul müqabilində yüksək tezliklə mənzillərin əksər satışını ələ keçirmişlər. Dövlət tərəfindən xakerlər tərəfindən bu müəyyənləşdirilən nəticələr ləğv edildi və 7 nəfər cinayət məsuliyyətinə cəlb edildi.

"Kibercinayətkarlıq haqqında " 23 noyabr 2001-ci il tarixli Budapeşt Konvensiyasında kibercinayətlərin dörd kateqoriyası göstərilir:

- Kompüter verilənləri və sistemlərinin məxfiliyi, tamlığı və istifadə imkanlarına qarşı cinayətlər;
- Məlumatların məzmunu ilə bağlı cinayətlər;
- Kompüter vasitələrindən istifadə ilə bağlı cinayətlər;
- Müəllif hüquqlarının və əlaqəli hüquqların pozulması ilə bağlı cinayətlər [9].

Kibercinayətkarlıqda bəzən hüquq ədəbiyyatlarında kiber hücumlara "xaker" hücumları da deyilir. Ümumiyyətlə, kompüter sisteminə, şəbəkələrə və məlumatlara icazəsiz olaraq kənardan qanunsuz müdaxilə etmə xaker hücumu hesab edilir. Sistemə giriş icazəsinin müddəti başa çatdıqdan sonra da qanunsuz daxil olma xaker hücumu sayılır. ABŞ-da 1960-cı illərdən Massaçusets Texnologiya İnstitutunda informasiya texnologiyalarının yüksək inkişafı ilə əlaqədar olaraq "kiber hücumu" "xaker hücumu" ilə əvəz olunmağa başlanıldı. Xaker sözü "sındırmaq", "dağıtmaq", "müdaxilə etmək" kimi mənalarda da başa düşülür.

Kiberhücumların əksəriyyəti sakitcə, qurbanların xəbəri olmadan səssiz həyata keçirilir. Qurbanların bu zaman cinayətkarın şəbəkəyə daxil olmasından və məlumatları oğurlamasından xəbəri olmur.

Respublikamız iqtisadi cəhətdən inkişaf etdikcə kibercinayətkarlıq da sürətlə inkişaf edir. Elə bir gün olmur ki, KİV respublikamızda törədilən kibercinayətkarlıq barədə məlumat verməsin. Kibercinayətkarlar tez-tez kompüter sistemlərinə qanunsuz müdaxilə edirlər. Xakerlər bu zaman məlumatları, sistemləri, xidmətləri dəyişə bilirlər, əlavələr edirlər, başqa yerlərə ötürürlər, silirlər, ya da ki, bloklayırlar. "Kibercinayətkarlıq haqqında " Budapeşt Konvensiyası kompüter məlumatlarının qəsdən və qeyri-qanuni zədələnməsi, dəyişdirilməsi, korlanması və ya bloklanması kimi hərəkətləri qadağan edir. Belə hərəkətlər AR CM-in 273-cü maddəsinə əsasən cinayət hesab edilir və cəzalandırılır.

Azərbaycan Respublikasının Cinayət qanunvericiliyində kibercinayətlərin beş növü sadalanır:
- Kompüter sisteminə qanunsuz daxil olma (271-ci maddə)
- Kompüter məlumatlarını qanunsuz ələ keçirmə (272-ci maddə)
- Kompüter sisteminə və ya kompüter məlumatlarına qanunsuz müdaxilə (273-cü maddə)
- Kibercinayətlərin törədilməsi üçün hazırlanmış vasitələrin dövriyyəsi (273-1-ci maddə)
- Kompüter məlumatlarının saxtalaşdırılması (273-2-ci maddə)

M.N.İmanlı yazır ki, kompüter məlumatlarının saxtalaşdırılması dedikdə, həqiqi kompüter məlumatlarının məzmununu dəyişdirmə, məlumatların sırasına yeni elementlərin əlavə edilməsi, yaxud silinməsi və s. hərəkətlər başa düşülür [7, s. 384].

Kompüter sisteminin bir hissəsi dedikdə, şəbəkədə olmayan kompüterin yaddaş qurğusu, şəbəkədə olan kompüterlərdən hər hansı biri, onun kompakt-disklərin yazılması üçün nəzərdə tutulan qurğusu və s. başa düşülür.

Kompüter şəbəkəsi dedikdə, öz aralarında rabitə kanalı ilə birləşdirilmiş və bu rabitəni həyata keçirməyə imkan verən iki və ya daha çox kompüterin məcmusu başa düşülür [3, s. 571].

Son illər dünya üzrə kiberhücumların SSL oğurlanması, DNS spoofing, IP spoofing, Spear-phishinge, ARP Cache zəhərlənməsi, ransomware, troyanatı, bruteforce, XSS, SQL inyeksiyası və b. hücum növləri artmağa başlamışdır.

AR CM-ə əlavə edilən 177.2.3-1-ci maddədə oğurluğun elektron məlumat daşıyıcılarından, yaxud informasiya texnologiyalarından istifadə etməklə törədilməsi göstərilir.

AR Konstitusiya Məhkəməsi Plenumunun "Azərbaycan Respublikası Cinayət Məcəlləsinin 177.2.3-1-ci maddəsinin şərh edilməsinə dair" 22 iyun 2015-ci il tarixli Qərarına əsasən ödəniş

kartında şəxs və onun bank hesabında olan pul vəsaiti barədə məlumat əks olunduğundan, bu kart elektron məlumat daşıyıcısı hesab edilməli və ondan istifadə edilməklə törədilən oğurluq cinayəti CM-nin 177.2.3-1-ci maddəsi ilə tövsif olunmalıdır.

Elektron məlumat daşıyıcılarından və informasiya texnologiyalarından istifadə etməklə oğurluq CM-nin otuzuncu fəslində nəzərdə tutulan cinayətlərin (kibercinayətlər) törədilməsi ilə müşayiət olunduqda, şəxsin əməli CM-in 177.2.3-1 və 30-cu fəslin müvafiq maddəsi (maddələri) ilə cinayətlərin məcmusu qaydasında tövsif edilməlidir [4].

AR Konstitusiya Məhkəməsinin bu Qərarı RF-nın CM-nin 158 "q" bəndinin 3-cü hissəsi ilə eyniyyət təşkil edir. Orada qeyd olunur ki, bank hesabından, habelə elektron pul vəsaitlərinə qarşı törədilmiş oğurluq (bu Məcəllənin 159.3-cü maddəsində nəzərdə tutulan cinayət əlamətəri olmadıqda). RF-nın 159.3-cü maddəsində elektron ödəniş vasitələrindən istifadə etməklə dələ-duzluq nəzərdə tutulub.

Hüquq ədəbiyyatında kibercinayətkarları müxtəlif tiplərə ayırırlar:

- Dələduzlar- əsasən internet vasitəsilə şübhəli linklər göndərərək insanların şəxsi məlumatlarını və bank kartı məlumatlarını ələ keçirənlərdir,
- Təbliğatçılar- internet şəbəkəsi vasitəsilə siyasi və dini təbliğatı yayanlardır.
- Hədə-qorxu ilə tələb edənlər- insanların etibarını qazanaraq onlardan şantaj etməyə imkan verən məlumatı əldə edən və daha sonra onları şantaj edərək pul və ya müəyyən hərəkətlərin edilməsini tələb edən şəxslərdir.
- Şərəf və ləyaqətin alçaldılması ilə məşğul olanlar- bunlar əsasən sosial şəbəkələrdə təhqiramiz sözlərlə insanların şəxsiyyətini alçaldanlardır,
- Uşaq pornoqrafiyasını yayanlar- əsasən "darkweb" şəbəkəsi vasitəsilə şəxsiyyətini gizlədərək uşaq pornoqrafiyası materiallarını yayanlar və satanlardır,
- Xakerlər- şəbəkə soxulcanı və viruslarını yayan və insanların kompüterlərini və şəbəkələrini ələ keçirən şəxslərdir.

Kibercinayətkarlıq bütün dünya ölkələri kimi Azərbaycan dövləti üçün də çox təhlükəli bir hal olduğu üçün dövlətimiz "Kibercinayətkarlıq haqqında" Konvensiyanın təsdiq edilməsi barədə 30 sentyabr 2009-cu il tarixli Qanunla Avropa Şurasının "Kibercinayətkarlıq haqqında" Konvensiyasına qoşulmuşdur.

Kibercinayətlər üçün yüksək latentlik xarakterikdir, çünki onların törədilməsini təsdiq edən sübutları bir neçə saniyə müddətində məhv etmək olur ki, bu da kompüter məlumatlarını qanunsuz daxil olma yerinin müəyyən edilməsi və konkret kompüterin müəyyən edilməsi və konkret kompüterin eyniləşdirilməsi üçün çox böyük çətinliklər törədir.

Artıq məlumat təhlükəsizliyi kompüterlərdə, onların sistemlərində və şəbəkələrində saxlanılan, emal və istifadə edilən məlumatların mühafizəsi problemi müasir dünyanın millətlərarası münaqişələr, ekoloji böhran, mütəşəkkil cinayətkarlıq, narkomaniya və s. kimi qlobal problemləri ilə bir sırada durur. Plastik ödəmə kartları ilə dələ-duzluq, bank hesablarından pul vəsaitlərinin oğurlanması, kompüter casusluğu, kiberterrorizm və s. kimi kompüter cinayətləri yüksək ictimai təhlükəliliyi ilə xarakterizə olunur. Bu da kibercinayətlərin getdikcə transmilli və mütəşəkkil xarakter aldığını göstərir [11, s. 905, 906].

Kibercinayətlərin istintaqının çətinliyi ondan ibarətdir. ki, onlar latent olmaqla bərabər, həm də sübutlar əldə etmək çətindir.

Kibercinayətlərin ibtidai istintaqı zamanı ehtimal olunan əsas sübutlar cinayətin törədilmə üsuluna uyğun olaraq əsasən elektron formada olur. Elektron sübutlar elektron qurğulardan (printer,

skaner və s.) kompüter şəbəkələrindən, planşetlərdən, mobil telefonlardan, rəqəmsal kameralardan və digər portativ avadanlıqlardan, habelə internetdən əldə edilir. Bu növ sübutların əldə edilməsi zamanı müstəntiq ənənəvi kriminalistik dəlillərin oynadığı mühüm rolu heç vaxt yaddan çıxarmamalıdır [10, s. 46].

Beləliklə, işin məqsədi kibercinayətkarlığın qarşısının alınması üzrə ümumi sosial tədbirlərin görülməsi, respublikada informasiya təhlükəsizliyinin təmin edilməsi və kiberhücumlardan qorunmaq üçün tədbirlərin görülməsi və kibercinayətlərin qarşısının alınmasının əsas istiqamətlərini müəyyən etməkdir.

Biblioqrafiya

1. Azərbaycan Respublikasının Cinayət Məcəlləsi. – Bakı: Hüquq ədəbiyyatı nəşriyyatı, 2004. - 404 s.

2. Azərbaycan Respublikasının Cinayət Məcəlləsi. – Bakı: Hüquq ədəbiyyatı nəşriyyatı, 2023. - 908 s.

3. Azərbaycan Respublikası Cinayət Məcəlləsinin Kommentariyası, II hissə. – Bakı: Hüquq Yayın Evi, 2023. - 872 s.

4. Azərbaycan Respublikası Konstitusiya Məhkəməsi Plenumunun "AR CM-nin 177.2.3-1-ci maddəsinin şərh edilməsinə dair" 22 iyun 2015-ci il tarixli Qərarı.

5. Daxili işlər orqanlarında xüsusi texnika və kibertəhlükəsizlik fəaliyyəti. – Bakı: Bakı nəş., 2023. - 208 s.

6. "Xəzər" TV-nin 23 may 2024-cü il "Xəbərlər" proqramı.

7. İmanlı M.N. Cinayət hüququ. Xüsusi hissə. Dərslik. –Bakı: ADMİU nəş., 2019. - 768 s.

8. İsmayılov İ. Süni intellekt fənnindən praktikum, dərs vəsaiti. - Bakı, 2023. - 233 s.

9. Kibercinayətkarlıq haqqında konvensiya. Budapeşt, 23 noyabr 2001-ci il. 30 s.

10. Kibercinayətlərin istintiqanına dair. Metodik vəsait. - Bakı, 2022. - 66 s.

11. Kriminalistika. Dərslik. – Bakı: Hüquq Yayın Evi, 2021. - 996 s.

12. Məcidli S.T. Kibercinayətlər. - Bakı, 2019. - 315 s.

13. Rəhimov İ.M. Cinayət və cəzanın fəlsəfəsi. Bakı: Şərq-Qərb Nəşriyyat evi, 2014. - 320 s.

14. Антонян Ю.М. Причины преступности. – М: ИД Камерон, 2006. - 283 с.

15. Поздняков Э. Философия преступления. – М: 2001. - 576 с.

Karimov Sh.M.♦

UDC: 343

Cybercrime activity in the Republic of Azerbaijan and its characteristic features

Abstract: The article is dedicated to cybercrime, which has increased rapidly in our republic in recent years.

The article especially mentions that currently cybercrimes are one of the most widespread types of crimes in our republic. Thanks to the advancement of digital technology in modern times, artificial intelligence is an intelligence that mimics human behavior or thought and can be trained and demonstrated through high technology to solve specific problems.

The article also points out the latency of cybercrimes, the rapid destruction of evidence, and therefore the difficulty of investigating these crimes.

The article also notes that cybercrimes are mainly committed through fraud, deception, violence and intimidation thanks to digital and network technologies.

Keywords: cybercrime; internet network; hackers; artificial intelligence; digital technology; cyberattack; computer crime; computer data; fraud; latency; virus programs.

References

1. Criminal Code of the Republic of Azerbaijan. Baku, Huquq Edebiyyati Publ., 2004, 404 p. (in Azerbaijani).

2. Criminal Code of the Republic of Azerbaijan. Baku: Huquq Edebiyyati Publ., 2023, 908 p. (in Azerbaijani).

3. Commentary to the Criminal Code of the Republic of Azerbaijan. Part II. Baku, Huquq Yayin Evi Publ., 2023, 872 p. (in Azerbaijani).

4. Decision of the Plenum of the Constitutional Court of the Republic of Azerbaijan "On the interpretation of Article 177.2.3-1 of the Criminal Code of the Republic of Azerbaijan" dated June 22, 2015 (in Azerbaijani).

5. Special techniques and cyber security activities in internal affairs bodies. Baku, Baku Publ., 2023, 208 p. (in Azerbaijani).

6. "Khazar" TV "News" program dated May 23, 2024 (in Azerbaijani).

7. Imanli M.N. Criminal law. Special part. Textbook. Baku, ADMIU Publ., 2019, 768 p. (in Azerbaijani).

8. Ismayilov I. Practical tutorial on artificial intelligence. - Baku, 2023. - 233 p. (in Azerbaijani).

9. Convention on cybercrime. Budapest, November 23, 2001. Baku, 2023, 30 p. (in Azerbaijani).

10. On the investigation of cybercrimes. Methodical aid. - Baku, 2022, 66 p. (in Azerbaijani).

♦ **Karimov Shohlet Muzaffar oglu** – PhD in Law, Associate Professor of the Law Department of the National Aviation Academy (Azerbaijan). E-mail: ruslan.mirzeliyev@rambler.ru

11. Criminalistics. Textbook. Baku, Law Publishing House., 2021, 996 p. (in Azerbaijani).
12. Majidli S.T. Cyber crimes. Baku, 2019, 315 p. (in Azerbaijani).
13. Rahimov I.M. Philosophy of crime and punishment. Baku, East-West Publ., 2014, 320 p. (in Azerbaijani).
14. Antonyan Yu.M. Causes of crime. Moscow, ID Kameron Publ., 2006, 283 p. (in Russian).
15. Pozdnyakov E. Philosophy of crime. Moscow, 2001, 576 p. (in Russian).

Каримов Ш.М.♦

УДК: 343

Киберпреступная деятельность в Азербайджанской Республике и ее характерные особенности

Аннотация: Статья посвящена киберпреступности, которая в последние годы стремительно растет в нашей республике.

Особо отмечается, что в настоящее время киберпреступления являются одним из самых распространенных видов преступлений в нашей республике. В настоящие время благодаря развитию цифровых технологий искусственный интеллект — это интеллект, который имитирует и регулирует человеческое поведение или мышление и одновременно может быть обучен,осознан и продемонстрирован с помощью высоких технологий для решения конкретных проблем.

Указывается на латентность киберпреступлений, быстрое уничтожение доказательств и, следовательно, на сложность расследования этих преступлений.

Также отмечается, что киберпреступления в основном совершаются посредством мошенничества, обмана, насилия и запугивания благодаря цифровым и сетевым технологиям.

Ключевые слова: киберпреступность; интернет-сеть; хакеры; искусственный интеллект; цифровые технологии; кибератака; компьютерная преступность; компьютерные данные; мошенничество; латентность; вирусные программы.

Библиография

1. Уголовный кодекс Азербайджанской Республики. – Баку: Изд-во Юридическая литература, 2004. – 404 с. (на азерб. яз.).
2. Уголовный кодекс Азербайджанской Республики. – Баку: Изд-во Юридическая литература, 2023. – 908 с. (на азерб. яз.).
3. Комментарий к Уголовному Кодексу Азербайджанской Республики. Часть II. – Баку: Изд-во Дом права, 2023. – 872 с. (на азерб. яз.).

♦ **Каримов Шохлет Музаффар оглы** – доктор философии права, доцент кафедры «Право», Национальная Академия Авиации (Азербайджан). E-mail: ruslan.mirzeliyev@rambler.ru

4. Решение Пленума Конституционного Суда Азербайджанской Республики «О толковании статьи 177.2.3-1 Гражданского Кодекса» от 22 июня 2015 года.

5. Специальная техника и мероприятия по обеспечению кибербезопасности в деятельности органов внутренних дел. – Баку: Изд-во Баку, 2023. – 208 с. (на азерб. яз.).

6. Программа «Новости» телеканала «Хазар» от 23.05.2024 г. (на азерб. яз.).

7. Иманли М.Н. Уголовное право. Особенная часть. Учебник. – Баку: Изд-во АГУКИ, 2019. – 768 с. (на азерб. яз.).

8. Исмайлов И. Практикум по искусственному интеллекту, учебное пособие. – Баку, 2023. – 233 с. (на азерб. яз.).

9. Конвенция о киберпреступности. Будапешт, 23.11.2001. 30 с. (на азерб. яз.).

10. О расследовании киберпреступлений. Метод. пособие. – Баку, 2022. – 66 с. (на азерб. яз.).

11. Криминалистика. Учебник. – Баку: Изд-во Дом права, 2021. – 996 с. (на азерб. яз.).

12. Меджидли С.Т. Киберпреступность. – Баку, 2019. – 315 с. (на азерб. яз.).

13. Рагимов И.М. Философия преступления и наказания. – Баку: Изд-во Восток-Запад, 2014. – 320 с. (на азерб. яз.).

14. Антонян Ю.М. Причины преступности. – М: ИД Камерон, 2006. - 283 с.

15. Поздняков Э. Философия преступления. – М: 2001. - 576 с.