

İNFORMASIYA TƏHLÜKƏSİZLİYİ – MİLLİ TƏHLÜKƏSİZLİYİN TƏRKİB HISSƏSİ KİMİ

Bəhram Zahidov,
Azərbaycan Respublikası Veteranlar
Təşkilatının hüquq və kadrlar şöbəsinin
müdiri, h.e.d., professor;
Üzeyir Həsənzadə,
hüquqşünas.
e-mail: bahram-zahidov@rambler.ru

Hər şeydən əvvəl, müasir dünyanın son dərəcə aktual və vacib olan problemlərindən birinə – informasiya təhlükəsizliyinin etibarlı müdafiəsi problemlərinə həsr olunmuş elmi konfransın təşkilatçılarna dərin minnətdarlığımı bildirirəm.

Müasir tədqiqatlar və normativ-hüquqi

aktlar bu günkü müzakirə mövzusunun açarı hesab edilən “informasiya” məfhumunun – şəxslər, əşyalar, faktlar, hadisələr, proseslər, bir sözlə hər şey haqqında məlumatlar sistemi olduğunu təsdiq edir. Müasir informasiya cəmiyyətində isə informasiyalar – bütün ictimai-siyasi quruluşlarda, bütün ölkələrdə və bütün xalqlarda işləyə bilən universal bir valyuta, dəyərlər sistemi hesab olunur. Realıq bundan ibarətdir ki, bu gün informasiyanın səviyyəsi və imkanları, ölkələrin inkişaf səviyyəsinin və qüdrətinin əsas göstəricisi kimi xarakterizə olunur. İzahlı lüğətlərdə bir qayda olaraq “təhlükəsizlik” məfhumu “təhlükə olmayan”, “təhlükəni istisna edən vəziyyət”

Qloballaşan dünyada sürətlə artan kibercinayət-karlıqla mübarizə sahəsində ölkəmizdə ardıcıl və sistemli tədbirlər həyata keçirilməkdədir. Bu sahədə informasiya təhlükəsizliyinin etibarlı müdafiəsinin təmin edilməsi, ölkəmizin geopolitik cəhətdən mürəkkəb bir regionda yerləşməsi, təbii ehtiyatlarının və enerji resurslarının bolluğu, habelə Dağlıq Qarabağ münaqişəsinə ədalətsiz olaraq cəlb edilməsi kontekstində, faktiki surətdə müharibə vəziyyətində olması ilə əlaqədar olaraq, son dərəcə aktual mahiyyət daşıyır.

Statistik məlumatlar ölkəmizdə kibercinayətkarlığın ildən-ilə artmasını və genişlənməsini təsdiq edir. Buna görə də informasiya təhlükəsizliyinin etibarlı müdafiəsinin hüquqi əsaslarının daha da təkmilləşdirilməsinə, inzibati və cinayət hüquqi vasitələrdən istifadə etməklə onun müdafiəsinə diqqətin artırılmasına və belə kriminal əməllərlə mübarizə mexanizmlərinin təkmilləşdirilməsinə zərurət vardır. Məqalədə bu məsələnin hüquqi aspektləri təhlil edilir və informasiya təhlükəsizliyinin etibarlı şəkildə müdafiə olunmasını təmin edən normaların və vasitələrin təkmilləşdirilməsinə dair fikir və mülahizələr irəli sürülür.

Açar sözlər: kibercinayətkarlıq, geopolitika, informasiya təhlükəsizliyi, cinayət hüququ, inzibati hüquq, mübarizə mexanizmləri, təkmilləşdirmə, cinayət hüquq normaları, cəza siyasəti.

kimi səciyyələndirilir. Milli təhlükəsizlik – milli mənafeyin təşkilatlanmış formada müdafiəsi hesab edilir. H.Kisincer milli təhlükəsizliyi millətin həyat tələbatının ödənilməsi hesab edirdisə, Z.Bejinski bunu



ölkənin hərbi qüdrətinin iqtisadi, sosial, siyasi, mənəvi inkişafının təmin olunması vəsitəsi kimi qiymətləndirirdi. Bunlar dünyanı idarə edən “Roma klubu”nun, “Tavistok insan münasibətləri institutu”nun, “Stenford təhqiqatlar institutu”nun, “Sosial münasibətlər institutu”nun, “Üçyüzlər komitəsi”nin başlıca simalarından hesab edilirlər.

Azərbaycan Respublikasının “Milli təhlükəsizlik haqqında” Qanununun 1-ci maddəsində milli təhlükəsizlik – dövlətin müstəqilliyinin, suverenliyinin, ərazi bütövlüyünün, konstitusiya quruluşunun, xalqın və ölkənin milli maraqlarının, insanın, cəmiyyətin və dövlətin hüquq və mənafelərinin daxili və xarici təhdidlərdən qorunmasının təmin olunması vəziyyəti kimi müəyyən edilmişdir. Həmin Qanunun 7.9 maddəsi informasiya sahəsində əsas təhdidlərin istiqamətlərini göstərmiş, 20-ci maddəsi informasiya sahəsində milli təhlükəsizliyi təmin edən tədbirlər sistemini, “Kəşfiyyat və əks-kəşfiyyat haqqında” 3 avqust 2004-cü il tarixli Qanunun 17-ci maddəsi – informasiya təminatının başlıca meyarlarını müəyyən etmişdir. Bütün bunlar onu göstərir ki, milli təhlükəsizlik, qlobal institut kimi öz tərkibində bir çox sahə elementlərini ehtiva etsə də, onun başlıca institutlarından biri də geniş mənada informasiya təhlükəsizliyi hesab olunur. Çünki təhlükəsizliyi təmin edən bütün sahələrdə – informasiyanı toplamaq, təhlil etmək, tədqiq etmək, mühafizə etmək kimi fəaliyyət elementləri geniş şəkəkdə istifadə edilir. Başqa sözlə, informasiya təhlükəsizliyini təmin etmədən, ölkənin milli təhlükəsizliyini təmin edilməsi mümkünsüzdür. Buna görə də informasiya təhlükəsizliyinin faktiki olaraq təmin edilməsi bu gün müasir millətlərin və dövlətlərin talehyüklü

problemlərindən birinə çevrilmişdir. Bu sahədə ABŞ, Rusiya, Almaniya, Böyük Britaniya, Yaponiya, Çin, Cənubi Koreya və digər inkişaf etmiş ölkələr öndə olsalar da, lakin qlobal problem kimi məsələnin aktuallığı, ilk dəfə olaraq ABŞ-da dərinlən təhlil edilmiş və bu sahəyə böyük diqqət yetirilmişdir. Bu da ABŞ-ın hərbi, iqtisadi, texnoloji, elm sahəsində super dövlət, dünyanın güc mərkəzinə çevrilmək arzusundan qaynaqlanmışdır. II Dünya Müharibəsi dünyanın “kommunizm kabusundan qurtarmaq” arzusunu reallaşıdırma bilmədiyi halda, ABŞ-ın rəhbərləri hələ, 1945-ci ildə məşhur “Dalles planı” adlanan yeni ideyanı dövriyyəyə buraxdılar. Məxfi səciyyə daşıyan bu müdhış plan – “insan şüurunun və təkəkkürünün dəyişdirilməsinin mümkünlüyü” hipotezasına əsaslanırdı. Başqa sözlə, bu təlim “insan obrazının dəyişdirilməsi” (“changing images of man”) proqramı adlanırdı. Dövlət, Amerika elmi qarşısında, insan şüuruna və təkəkkürə idarə olunan xaos təlqin etməklə, insan üçün ən ülvi dəyərlərin və ideyaların onun beynindən çıxarılması yolu ilə, konkret Mərkəzdən asılı vəziyyətə salmaq, nəticədə bu Mərkəzin sifarişi əsasında, hər hansı bir şəxsin müəyyən bir məqsədə və təyinatə yönəldilməsi ideyasının, kənardan onun şüuruna yeridilməsi və ya təlqin edilməsi sahəsində mükəmməl texnologiyaları hazırlamaq kimi məsul bir vəzifə qoymuşdu. Təsədüfi deyil ki, müəyyən bir müddət keçdikdən sonra Pentaqon rəhbərləri qarşıya qoyulan bu vəzifənin uğurla başa çatdırılmasını obrazlı şəkildə ifadə edərək göstərirdilər ki, biz, inkişafın elə bir səviyyəsinə nail olmuşuq ki, daha heç kim əsgər olmayacaq, biz hamımız döyüşün birgə iştirakçılarına çevriləcəyik. Tapşırıq belədir: Daha canlı qüvvələri – əsgərləri yox, ümu-



miyyətlə, əhalinin dünyagörüşünü və baxışlarını dağıtmaq, sosiumu birdəfəlik məhv etmək vəzifələrini həll etməliyik. Hazırda dünyada baş verən qlobal proseslər – terrorçuluq, narkobiznes, insan alveri, silah alveri, millətlər, dinlər, nəsillər, cinslər arasındakı münafişələrin və müharibələrin sürətlə genişlənməsi, transmilli mütəşəkkil cinayətlərin, zorakılığın və qəddarlığın, qeyri-insani və qeyri-əxlaqi hərəkətlərin artması və genişlənməsi, İŞİD, Taliban, Ukrayna hadisələri və s. bütün bunlar, ABŞ və digər super dövlətlərin “Dalles planı”nın artıq həyata keçirilməsi, idarə olunan kaosun dövrüyyəyə buraxılması təəssüratını yaradır. “Yeni dünya nizamı”nın yaradılması, “Mason lojası”nın, Avropanın “Qara aristokratiyası”nın, “Roma klubu”nun, “Vahid dünya hökuməti”nin diktəsi altında – “texnotronika” (Z.Bejinski) vasitəsilə hər bir insanın şüuru və təfəkkürü üzərində biokimyəvi və psixi vasitələrlə sosial və siyasi nəzarətin tam həyata keçirilməsini təmin etməlidir. Bu işə əvvəlcədən düşünülmüş və hazırlanmış xüsusi vasitələrlə – şəbəkə səciyyəsi daşıyan çoxsaylı üsul və vasitələrlə, mübahisəsiz qaydada həyata keçirilə bilərdi. Beynəlxalq və regional təşkilatlar, NATO, “Mossad”, İnterpol, Mərkəzi Kəşfiyyat İdarəsi, “Harvard Psixoloji Klinika”, “Elmi siyasətin tədqiqi institutu”, “Sistemlərin inkişaf korporasiyası” və onlarla digər qurumlar bu işə səfərbər edilmişlər. Sistemli şəkildə həyata keçirilən bu siyasət, eyni zamanda bəşəriyyət əleyhinə müxtəlif səciyyə daşıyan kriminal əməllərlə – narkobizneslə, pornoqrafiya ilə, silah alveri ilə, informasiya məlumatlarının və texnoloji sirlərin oğurlanması ilə, çirkli pulların yuyulması ilə, münafişələrin qızıqdırılması ilə, müharibələrin, terrorçuluğun, dövlət çevrilişlərinin,

rəngli inqilabların həyata keçirilməsi və onlarla digər vasitələrlə reallaşdırılmalı idi. Bu qlobal tədbirlər sisteminin icrasında müasir informasiya texnologiyalarından, kütləvi informasiya vasitələrinin imkanlarından geniş istifadə edilir, insan psixikasına və şüuruna təsir edən, asılılıq yaradan vasitələr, təzyiqlər, meyillər şüurlu və məqsədli şəkildə geniş təbliğ olunmanı tələb edir. Super güclərin ciddi nəzarəti altında bu tədbirlər sistemi dünyada əsaslı dəyişikliklərə, dəyərlər sisteminin böhranına gətirib çıxarır. Böyük bir şəbəkə bu işə cəlb edilmişdir. Televiziyalar, qəzetlər, saytlar, digər kütləvi informasiya vasitələri müxtəlif təyinatlı qrantlar hesabına fasiləsiz olaraq “ödənişli proqramlar” və ya “layihələr” əsasında xüsusi fəallıq göstərir. Böyük və super dövlətlər yeni və kiçik dövlətləri təhdid edir, onların sərvətlərini ələ keçirir və rəngli inqilablar, demokratiya adı altında onları təhdid edirlər. İki standartlar həyat tərzinə çevrilmişdir. Beynəlxalq təşkilatlar böyük dövlətlərin diktəsi ilə işləməkdədirlər. Mənəvi-əxlaqi dəyərlərin yüksək olduğu cəmiyyətlərdən fərqli olaraq, pul, kapital böyük qələbə qazanmış və hakim mövqə əldə etmişdir. Bəşəriyyətin əşrafı olan insan ucuzlaşdırılmış, klonlaşdırılmış, ekvivalent vasitəsinə çevrilmiş, insan hüceyrələri kodlaşdırılmış, qəddarlıq, amansızlıq, əxlaqsızlıq həyat normasına çevrilməyə istiqamətləndirilmişdir. Ekstrasenslərin, psixoloqların, falçıların – insan ruhuna və psixikasına təsir edən aşkar fəallığı, kibercinayətkarlığın şəbəkə imkanlarının tətbiqi və gözlənilən daha böyük təhlükələr irəli sürdüyümüz müddəaların əsaslılığını qətiyyətlə təsdiq edir. Dünya və bəşəriyyət çox narahatdır. Yaşadığımız Yer kürəsi yeni bir müharibənin – III Dünya Müharibəsinin təhlükəsi



ilə üz-üzədir. Bütün bunlar informasiya təhlükəsizliyinin etibarlı müdafiəsinə diqqətin artırılmasını bir daha aktuallaşdırmışdır. Elə bu günkü konfrans da məhz bu narahatçılığın nəticəsi hesab oluna bilər.

ABŞ-da, yüksək inkişaf etmiş Yaponiya, Almaniya, İngiltərə, Hollandiya, Rusiya, Cənubi Koreya kimi ölkələrdə “postindustrial”, “yüksəkendustrial”, “informasiya-industrial” və “informasiya” cəmiyyətləri öz qlobal inkişafını, daha çox informasiya-kommunikasiya texnologiyalarının müasir nailiyyətləri əsasında inkişaf etdirirlər. Bu sahədə elektron hesablama maşınlarının, bioelektronik və psixokompyuter texnologiyalarının, informasiya-elektron sistemlərinin çeşidli inkişafı dünyada, ümumiyyətlə informasiya təhlükəsizliyinin daha etibarlı müdafiəsinə zərurət yaratmışdır. Cəmiyyətin, dövlətin və insanın həyatının və fəaliyyətinin elə bir sahəsi yoxdur ki, orada müasir informasiya texnologiyalardan ən müxtəlif istiqamətlərdə və formalarda geniş istifadə edilməsin. Bu proseslər kəmiyyət və keyfiyyət göstəricilərinə görə gündən-günə inkişaf edir və dərinləşir. İnsan beyninin, düşüncəsinin və qəlbinin alqoritmlərinin tədqiqi, bu sahədə bioloji və fizioloji proseslərin ultrabənövşəyi şüalara və xarici təsirlərə reaksiyasının, stressin, yorğunluğun, depressiyanın, dezinformasiyanın, psixotronic texnologiyaların, şüurun və təhtəşüurun müsbət və mənfi yönümlərinin öyrənilməsi, psixikanı dəyişmək, məhv etmək, insanı zombiləşdirmək, kənardan asılı salmaq, şəxsiyyətin deformasiyasını və kənar təsirlərə tabeçilik mexanizmlərinin tədqiqi və bütün bu proseslərin öyrənilməsi və tətbiqi sahəsində əldə edilən müasir elmi nailiyyətlər insanı heyrətə gətirir. Bu texnologiyaların əsası, yuxarıda qeyd edildiyi ki-

mi, super dövlətlərin güclənməsinə, onların hərbi qüdrətinin artırılmasına xidmət edir. Zaman keçdikcə, onların bir hissəsi mülki həyatda istifadə edilməyə istiqamətləndirilir. Bu gün mobil telefon rabitəsi, televiziya-ötürücü vasitələrin çeşidli imkanları, nüvə və atom fizikası, günəş enerjisi, internet və digər texniki vasitələrin səviyyəsi və geniş miqyasda tətbiqi həyatımızın ayrılmaz hissəsinə çevrilmişdir. Buna görə də bu gün dünya dövlətlərinin inkişaf səviyyəsi orada elm və texnikanın inkişaf səviyyəsi ilə sıx bağlıdır. Alimlər cəmiyyətdə, təbiətdə, dövlətdə və insan həyatında baş verən bütün prosesləri dünyada gedən qloballaşma kontekstində izah etməyə çalışırlar. Reallıq isə bundan ibarətdir ki, əslində dünyanın maddi sərhədləri dəyişməzdir. Bununla yanaşı bu gün dünya məhz elmin inkişafı nəticəsində maddi aləmlə yanaşı, paralel olaraq həm də virtual dünyanın, ruhi, mənəvi, ideal və xəyali aləmin – saysız-hesabsız mərhələləri özündə birləşdirən internet məkanının mövcudluğu haqqında dərin elmi tədqiqatlar aparılmasına zərurət yaratmışdır. Dünyanın elmi mənzərəsini, böyük kəşfləri, elmi uğurları, informasiya sirlərini özündə qoruyub saxlayan resursların ələ keçirilməsi uğrunda mübarizə genişlənmişdir. Başqa planetlərdən gələnlərin axtarılıb tapılması, onlarla ünsiyyətin yaradılması, texnoloji uğurlarının öyrənilməsi, yerdən kənardan mövcud olan həyatın dərinə tədqiq edilməsi kimi tələbatlar təbii sərvətlər uğrunda üstünlüyü əldə etməyə hesablanmışdır. Təbiətə çətinliklərdən həmişə qaçan, asan və rahat həyata meylli olan müasir insan texniki vasitələrin köməyi ilə bu gün böyük və geniş imkanlar qazanmışdır. Mürəkkəb sistemlərin, əks əlaqələrin üzvi surətdə vəhdətinə əsaslanan dövlət idarəçiliyinin hə-



yata keçirilməsində, riyaziyyat, texnika və neyrofiziologiyanın birgə səyi ilə yaradılmış kibernetik idarəçilik metodlarının həyata keçirilməsi, elektron hesablama maşınlarının, müxtəlif təyinatlı kompyuterlərdən istifadə, elektron hökumətin yaradılması insanın bir çox problemlərinin həllini asanlaşdırmaqla yanaşı, həm də ona yeni-yeni problemlər və təhlükələr yaratmaqdadır. Dövlət idarəçiliyinin həyata keçirilməsində, insanın arzu və tələblərinin reallaşmasında, elektron hökumətin, elektron məhkəmənin, elektron ədliyyənin, elektron təbabətin müasir vəziyyəti və s. bu kimi yeni institutların imkanları genişlənməkdə və inkişaf etməkdədir. Az qala insan təfəkkürü ilə rəqabətə girə bilən internet və kompyuter texnologiyalarının imkanları tarixən çox çətin, mürəkkəb və əziyyətli prosedurlardan kəskin surətdə fərqlənən yeni, müasir və asan üsulların tətbiqi, informasiya daşıyıcılarından daha çevik və geniş mənada istifadə etmək imkanları güclənməkdədir. Bu gün elə bir fəaliyyət sahəsi yoxdur ki, orada informasiya texnologiyalarının imkanlarından istifadə edilməsin. Reallıq bundan ibarətdir ki, texniki-kommunikasiyalardan istifadə etmək nə qədər rahatlıq və komfort yaradırsa, mütənasib qaydada cəmiyyət, dövlət və insan üçün də yeni-yeni təhlükələr yaratmaqdadır. Bu mənada kompyuter cinayətkarlığı belə geniş yayılmış təzahürlərdən birinə çevrilmişdir. Bu sahədə müxtəlif təyinatlı informasiyaların – siyasi, iqtisadi, elmi, texniki, hərbi və s. məlumatların mühafizəsinin təmin olunması həyatı tələbata çevrilmişdir.

Son illər mütəşəkkil cinayətkarlığın bütün təhlükəli, ağır və geniş yayılmış növlərinin həyata keçirilməsində informasiya mənbələrindən və internet imkanlarından geniş is-

tifadə edilməkdədir. SSRİ miqyasında ilk kompyuter cinayətkarlığı 1979-cu ildə, 78584 rubl məbləğində vəsaitin ələ keçirilməsi məqsədilə Vilnus şəhərində törədilmişdir. Sonralar analogi cinayət Qorki (Nijniy Novqorod), Moskva, Sankt-Peterburq, Nyu-York, Təl-Əviv, Rotterdam, Lyuksemburq və digər ölkələrdə də sürətlə artmışdır. Bu qəbildən olan cinayətlər hazırda MDB ölkələrində, Qərb ölkələrində o dərəcədə artmışdır ki, statistiklər hər 12 saniyədən bir dünyada kibercinayətkarlığın baş verməsi nəticəsinə gəlmişlər. Çirkli pulların yuyulması, bank resurslarının ələ keçirilməsi, saxtalaşdırılması, mənimsənilməsi, plagiat, layihələrin və texnologiyaların, iqtisadi, hərbi sirlərin oğurlanması və milyard ABŞ dolları məbləğində mənimsəmə faktları günümüzün reallığına çevrilmişdir. Bundan daha təhlükəli kompyuter texnologiyalarından istifadə etməklə hərbi sirlərin ələ keçirilməsi, təyyarələrin, atom elektrik stansiyalarının, metroların, nəqliyyat-kommunikasiya sistemlərinin terrorçular tərəfindən öz maraqları xatirinə istifadə edə bilmək imkanları bu gün böyük təhlükələrdən xəbər verir .

Keçən əsrin sonlarından başlayaraq, kompyuter cinayətkarlığı transmilli mütəşəkkil cinayətkarlığın törədilmə vasitələrindən birinə çevrilmişdir. Rusiya Federasiyasında bu qəbildən olan cinayətlər 1997-ci ildə 33, 2000-ci ildə 800, 2005-ci ildə 10214, 2014-cü ildə isə 20000-dən çox fakt qeydə alınmışdırsa, analogi vəziyyət MDB-nin başqa ölkələrində də, o cümlədən Azərbaycanda da müşahidə edilir. Belə ki, Milli Təhlükəsizlik Nazirliyinin məlumatlarından görünür ki, 2007-ci ildə 8 nəfər, 2008-ci ildə 4 nəfər, 2009-cu ildə 32 nəfər, 2011-ci ildə 3 nəfər, 2012-ci ildə 13 nəfər şəxs kibercinayətkarlığa görə cinayət



məsuliyyətinə cəlb edilib, məhkəmə hökmü ilə cəzalandırılmışlar. Buna görə də müstəqillik illərində Azərbaycan Respublikasında kibercinayətkarlıqla mübarizə və informasiya təhlükəsizliyinin təmin edilməsi sahəsində ardıcıl və sistemli tədbirlər kompleksı həyata keçirilmişdir. 1996-cı ildə Milli Məclis “İnformasiya, informasiyalaşdırma və informasiya təhlükəsizliyi haqqında”, 3 aprel 1998-ci ildə “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında”, 9 sentyabr 1998-ci ildə “Məlumat azadlığı haqqında”, 7 dekabr 1999-cu ildə “Kütləvi informasiya vasitələri haqqında”, 30 sentyabr 2005-ci il tarixdə “İnformasiya əldə etmək” haqqında Qanunlar qəbul etmiş, cinayət və inzibati qanunvericilikdə müəyyən normalar nəzərdə tutulmuşdur. Bu sahədə 7 sentyabr 2004-cü il tarixdə “Dövlət sirri haqqında” Azərbaycan Respublikası Qanununun qəbul edilməsi və sonralar onun daha da təkmilləşdirilməsi istiqamətində həyata keçirilən tədbirlər mühüm əhəmiyyət kəsb etmişdir.

Azərbaycan Respublikasında, Avropa Şurasının 23 noyabr 2001-ci il tarixli “Kibercinayətkarlıq haqqında” Konvensiyasını 30 sentyabr 2009-cu ildə ratifikasiya edilmiş və qanunvericiliyin uyğunlaşdırılması istiqamətində müəyyən işlər görülmüşdür. İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında Azərbaycan Respublikası Prezidentinin 26 sentyabr 2012-ci il tarixli Fərmanı bu sahədə kompleks tədbirlər müəyyənləşdirmiş, konkret subyektlərin dairəsini, onların hüquq və vəzifələrini və öhdəliklərini müəyyən etmişdir. 23 may 2007-ci ildə Azərbaycan Respublikasının Milli Təhlükəsizlik Konsepsiyası təsdiq olunmuşdur. Azərbaycan Respublikasının “Milli təhlükəsizlik haqqında” və “Kəşfiyyat və

əks-kəşfiyyat fəaliyyəti haqqında” 29 iyun 2004-cü il tarixdə Qanunlar qəbul edilmişdir. Eləcə də “Terrorizmin maliyyələşdirilməsi haqqında” BMT-nin 9 dekabr 1999-cu il tarixli Konvensiyası, BMT-nin və Avropa Şurasının cinayətkarlığın mütəşəkkil formaları ilə mübarizəni təmin edən bütün Konvensiyaları ölkəmizdə ratifikasiya etmiş və öz üzərinə müvafiq öhdəliklər götürmüşdür.

İnformasiya təhlükəsizliyinin təmin olunması və kibercinayətkarlıqla mübarizənin gücləndirilməsi sahəsində görülmüş cinayət hüquqi tədbirlər diqqəti daha çox cəlb edir. Bu gün 30 dekabr 1999-cu il tarixdə təsdiq edilmiş və 1 sentyabr 2000-ci il tarixdən qüvvəyə minən Azərbaycan Respublikası Cinayət Məcəlləsində “Kibercinayətlər” müstəqil fəsilə, “İctimai təhlükəsizlik və ictimai qayda əleyhinə olan” X bölmənin 30-cu fəslində müstəqil bir sahə kimi ilk dəfə olaraq Məcəlləyə daxil edilmişdir. Bu fəsilə kompyuter texnologiyaları sahəsində ictimai münasibətlərə, dəyərlərə və sərvətlərə qəsd edən əməllər cəza təhdidi ilə mühafizə edilir. Belə ki, kompyuter sistemə qanunsuz daxil olmağa görə CM-nin 271-ci maddəsində, kompyuter məlumatlarını qanunsuz ələ keçirməyə görə 272-ci maddə və kompyuter sistemə və ya kompyuter məlumatlarına qanunsuz müdaxiləyə görə 273-cü maddə, beləliklə cəmi 3 tərkib Cinayət Məcəlləsində nəzərdə tutulurdu. Lakin sonradan yaranmış zərurətlə əlaqədar olaraq 29 iyun 2012-ci il tarixli qanunlarla həmin fəsilə 2 yeni tərkib də əlavə edilmişdir. Belə ki, kibercinayətlərin törədilməsi üçün hazırlanmış vasitələrin dövriyyəsinə görə CM-nin 273-1 və kompyuter məlumatlarının saxtalaşdırılmasına görə məsuliyyət müəyyən edən 273-2 maddəsi CM-nə əlavə edilməklə bu fəsilə daha da təkmil-



ləşdirilmişdir. Lakin konkret olaraq CM-nin qeyd edilən fəslində 5 tərkibdə belə əməllərlə cinayət-hüquqi mübarizənin təmin olunması xüsusi olaraq qeyd edilməlidir.

Ölkədə və dünyada aparılan təhlillər göstərir ki, bu gün bir çox ölkələrdə, o cümlədən Azərbaycanda törədilən cinayətlərin əksəriyyətində informasiya texnologiyalarından bu və ya digər dərəcədə istifadə edilir. Apardığımız təhlillər göstərir ki, Azərbaycan Respublikası Cinayət Məcəlləsində 20-yə qədər maddə bilavasitə, 25 maddə isə bilavasitə kompyuter texnologiyalarından istifadə edilməklə törədilə bilər. Həmin cinayətlər cəza təhdidi ilə qorunan ayrı-ayrı ictimai münasibətlərə, dəyərlərə və sərvətlərə qəsd etdiyinə görə, CM-nin ayrı-ayrı bölmələrində, fəsilələrində yerləşdirilmişdir. Yazışma, telefon danışıqları, poçt, teleqraf və digər məlumatların sirrini pozmağa görə məsuliyyət müəyyən edən 125-ci maddə, inteqral, sxem tiptologiyasından istifadəyə müstəsna hüququ pozmağa görə məsuliyyət müəyyən edən 165-1 maddə, məlumat topluların qeyri-qanunu istifadəyə görə 163-3 maddə, poronqrafik materialları və ya əşyaları qanunsuz yaymağa görə məsuliyyət müəyyən edən 242-ci maddə, kommersiya və ya bank sirri olan məlumatları qanunsuz yolla əldə etməyə və ya yaymağa görə məsuliyyət müəyyən edən 202-ci maddə, insayder tərəfindən xidməti məlumatlardan qanunsuz istifadə etməyə görə məsuliyyət müəyyən edən 202-2 maddə, telefon xətlərinə qanunsuz daxil olmaqla danışıqlar aparmağa görə məsuliyyət müəyyən edən 189-cu maddə, sertifikatlaşdırılmamış rabitə vasitələrinin satışını təşkil etməyə görə məsuliyyət müəyyən edən 233-2-ci maddə, məzmununda dövlət sirri olan sənədləri itirməyə görə məsuliyyət müəyyən edən 285-

ci maddə, dövlət sirrini yaymağa görə məsuliyyət müəyyən edən 284-cü maddə buna misal ola bilər.

Apardığımız təhlillər göstərir ki, Cinayət Məcəlləsinin bir sıra, məsələn, 165, 163, 166, 193-1, 197, 198, 204, 313 və digər bu kimi maddələrində nəzərdə tutulmuş əməllərin törədilməsi zamanı da kompyuter texnologiyalarından bir qayda olaraq geniş istifadə edilir. İnzibati Xətalər Məcəlləsində nisbətən az ictimai təhlükə təşkil edən əməllərə görə məsuliyyət nəzərdə tutulmuşdur. Bu qəbildən olan cinayət və inzibati səciiyə daşıyan əməllərə görə vurulmuş zərərlərin ödənilməsi imkanları da əmək və mülki qanunvericilik ilə müəyyən edilmişdir.

Tədqiqatlarımız göstərir ki, informasiya təhlükəsizliyinin təmin edilməsi üçün ölkəmizdə bir çox normativ-hüquqi aktlar yaradılmış, təşkilati-hüquqi tədbirlər və mexanizmlər bu sahəyə səfərbər edilmişlər. Buna baxmayaraq, informasiya təhlükəsizliyinin təmin edilməsi məqsədilə bir sıra təxirəsalınmaz tədbirlərin görülməsi də məqsədəmüvafiq olardı. Bunları aşağıdakı kimi qruplaşdırmaq olar:

Azərbaycan Respublikasının Konstitusiyasında vətəndaşların bir sıra hüquq və azadlıqları fundamental dəyərlər kimi nəzərdə tutulmuşdur. Buna baxmayaraq hesab edirik ki, bu gün belə hüquq və azadlıqlar sahəsində Azərbaycan Respublikası vətəndaşlarının "informasiya hüququ" da Konstitusiyada təsbit edilməlidir. Onun məzmununun aşağıdakı kimi verilməsi tövsiyyə edilir:

"Maddə 50-1. İnformasiya hüququ

I. Hər kəsin informasiya hüququ vardır.

II. Bu hüquq əsasında hər kəs, dövlət hakimiyyəti, yerli özünü idarə orqanları, təş-



kilati-hüquqi və mülkiyyət formasından asılı olmayaraq bütün müəssisə, idarə və təşkilatlardan və vətəndaşlardan qanunvericiliklə qadağan edilməyən məlumatları almaq, toplamaq, yığmaq, təhlil etmək, saxlamaq, axtarmaq, yaymaq, istifadə etmək, mühafizə etmək, satmaq, istifadəçisi olmaq hüququna malikdir

III. Dövlət informasiya hüququnun həyata keçirilməsinə təminat verir”.

Bundan başqa “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında”, “Dövlət sirri haqqında”, “Kütləvi-informasiya vasitələri haqqında”, “Milli təhlükəsizlik haqqında”, “Əməliyyat-axtarış fəaliyyəti haqqında”, “Kəşfiyyat və əks-kəşfiyyat fəaliyyəti haqqında” və bir sıra əlaqədar normativ-hüquqi aktların da ayrı-ayrı müddələrinin müasirləşdirilməsi və təkmilləşdirilməsi haqqında tədbirlər görülməlidir. Ölkəmiz “Kibercinayətkarlıq haqqında” 23 noyabr 2001-ci il tarixli beynəlxalq Konvensiyaya qoşulmasına baxmayaraq, “Kompyuter texnologiyalarından istifadə etməklə dələduzluq” əməllərinə görə müstəqil tərkib Cinayət Məcəlləsində nəzərdə tutulmamışdır. İnzibati Xətalar və Əmək Məcəlləsində də müvafiq təkmilləşdirilmələrin aparılması zəruridir. Eləcə də bu və ya digər cinayət əməllərinin informasiya texnologiyalarından istifadə edilməklə törədilməsi halları hesab edirəm ki, ağırlaşdırıcı hallar kimi ayrı-ayrı tərkiblərdə nəzərə alınmalıdır.

İnformasiya təhlükəsizliyinin elmi-nəzəri əsaslarının möhkəmləndirilməsi, təkmilləşdirilməsi və ixtisaslaşmış kadr hazırlığını təmin etmək üçün müstəqil “İnformasiya hüququ” fənninin tədrisinə zərurət yaranmışdır. Belə bir dərslinin və ya dərslərinin hazırlanması, orta və ali məktəblərdə tədrisinin

daha səmərəli üsullarının tapılması faydalı ola bilər.

İnformasiya təhlükəsizliyinin texnoloji problemləri sahəsində dünya səviyyəsində olmasa da, ölkəmizdə müəyyən işlər görülməkdədir. Bununla yanaşı, informasiya təhlükəsizliyi problemi multidisiplinar yanaşma tələb edir. Bir qlobal problem olaraq onun texniki, fiziki, kimyəvi, bioloji, psixoloji, riyazi, sosial, siyasi, hərbi və hüquq elmləri tərəfindən birgə tədqiqinə hazırda böyük zərurət yaranmışdır. Milli təhlükəsizlik və onun tərkib hissəsi olan informasiya təhlükəsizliyi, virtual dünya məkanının zaman və məkan göstəricisinin müəyyən edilməsinə, bu sahədə ictimai münasibətlərin mükəmməl hüquqi tənzimlənməsinə həyatı zərurət yaratmışdır. Reallıq bundan ibarətdir ki, bu gün müxtəlif elm sahələrini əhatə edən və elmi səyləri birləşdirən kompleks tədbirlər planının hazırlanması çox vacibdir. Bu işə informasiya təhlükəsizliyini təmin edən kompleks tədbirlər planının və mexanizmlərinin hazırlanması sahəsində vahid elmi Mərkəzin yaradılması, hüquqi tənzimlənmənin və hüquq maarifçiliyinin planlı şəkildə həyata keçirilməsi son dərəcə vacibdir. Bu işdə yalnız təchizat və təminat məsələsi deyil, habelə orta məktəblərdə informasiya təhlükəsizliyinin tədrisinə diqqət verilməsi günün reallıqlarından irəli gəlir. Xüsusilə qeyd edilməsi zəruridir ki, informasiya təhlükəsizliyinin müxtəlif elm sahələri və müxtəlif ixtisaslardan təcrübəli mütəxəssislər tərəfindən işlənilməsi olduqca vacibdir. Əminliklə demək olar ki, belə kompleks tədbirlərin hazırlanması və həyata keçirilməsi informasiya təhlükəsizliyinin təmin olunmasına dəyərli töhfələr verə bilər.



İSTİFADƏ EDİLMİŞ ƏDƏBİYYAT

1. Azərbaycan Respublikasının “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” 3 aprel 1998-ci il tarixli Qanunun 2-ci maddəsi.
2. Axundov Ağamusa. Azərbaycan dilinin izahlı lüğəti. B., 2005, s.396.
3. Вах: Основы национальной безопасности. М., 2014, с.7.
4. Вах ətraflı: Dr.John Coleman. Üçyüzlər Komitəsi (Dünya Hökumətinin sirləri). B., 2011, s.20-26.
5. Təhlükəsizlik xidməti. Normativ-hüquqi aktlar toplusu. B., 2009, s.65.
6. Yenə orada.
7. Журнал «Правопорядок». М., 2002, № 2, с.3.
8. Новая газета. 2001. 8-11 июня.
9. Вах ətraflı: Dr.John Coleman. Üçyüzlər Komitəsi (Dünya Hökumətinin sirləri). B., 2011, s.54-56.
10. Российская газета. 2007. 18 сент.

INFORMATION SECURITY - AS AN INTEGRAL PART OF NATIONAL SECURITY

Bahram Zahidov,
Doctor of Law, Professor, Head of the Law and
Personnel Department of the Veterans Organization of the Republic of Azerbaijan;
Uzeyir Hasanzadeh,
lawyer.

The consecutive and systematic measures in a sphere of fight against rapidly increasing cybercriminality in globalization world are being taken in our country. Ensuring trustworthy protection of information security in this sphere in connection with location of our country in a complex region from the geopolitical point of view, richness of natural reserves and energetic resources, as well being in fact, in war state in the context of its unjust drawing into Nagorno-Karabakh conflict, acquires even more actuality.

Statistic information testifies to that in our country cybercriminality increases and expands in organized form. Therefore in order to improve more the legal foundations of information security increasing attention to this sphere and improving the fight mechanisms in this sphere using the administrative and criminal law means, are required. In the article the legal aspects of this problem are analyzed and thoughts and views on improving activities are suggested.

Key word: cybercriminality, geopolitics, Information security, criminal law, administrative law, fight mechanisms, improvement, criminal law norms, punishment politics.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ - КАК СОСТАВНОЙ ЧАСТИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Бахрам Захидов,
заведующий юридического и кадрового отдела Организации Ветеранов Азербай-
джанской Республики, доктор юридических наук, профессор;
Узеир Гасанзаде,
юрист.

В глобализирующемся мире в борьбе со стремительно растущей киберпреступностью в нашей стране реализуются последовательные и систематические меры. В области обес-



печения надежной защиты информационной безопасности, это является более актуальным в связи с размещением нашей страны с геополитической стороны в сложном регионе, обилием природных ресурсов и энергетических ресурсов, а также в контексте привлечения к участию в несправедливом нагорно-карабахском конфликте, по сути нахождения в состоянии войны.

Статистические данные подтверждают рост и расширение в нашей стране организованной киберпреступности. Поэтому, дальнейшее совершенствование правовой базы обеспечения информационной безопасности, с привлечением административных и уголовно-правовых средств, требует большего внимания и совершенствования механизмов борьбы в этой сфере. В статье анализируются правовые аспекты этой проблемы и предлагаются взгляды и мнения для совершенствования деятельности.

Ключевые слова: киберпреступность, геополитика, информационная безопасность, уголовное право, административное право, механизмы борьбы, совершенствование, нормы уголовного права, уголовная политика.

BİLGİ GÜVENLİĞİ - ULUSAL GÜVENLİĞİN AYRILMAZ BİR PARÇASI OLARAK

Bahram Zahidov,
Azərbaycan Cumhuriyeti Gaziler Təşkilatı hüquq və
personel dairesi başkanı, h.e.d., profesör;
Üzeyir Hasanzadə,
avukat.

Hızla küreselleşen dünyada, ülkemizde hızla büyüyen siber suçlarla mücadele için tutarlı ve sistematik tedbirler alınmaktadır. Bu alanda bilgi güvenliğinin güvenilir bir şekilde korunmasının sağlanması, ülkenin jeopolitik olarak karmaşık bir bölgede yer alması, doğal kaynakların ve enerji kaynaklarının bolluğu ve Dağlık Karabağ ihtilafına haksız katılımın sağlanması gerçeği bağlamında son derece önemlidir. savaş durumunda olmasıdır.

İstatistikler, ülkemizde siber suçların büyümesini ve yayılmasını doğrulamaktadır. Bu nedenle, bilgi güvenliğinin güvenilir bir şekilde korunması için yasal çerçevenin daha da iyileştirilmesi, idari ve cezai hukuk yollarının kullanılması yoluyla korunmasına daha fazla dikkat edilmesi ve bu tür suç eylemleriyle mücadele mekanizmalarının iyileştirilmesi gerekmektedir. diriliş ihtiyacı. Makale, bu konunun yasal yönlerini analiz etmekte ve bilgi güvenliğinin güvenilir bir şekilde korunmasını sağlamak için normların ve araçların iyileştirilmesine ilişkin fikir ve değerlendirmeleri ortaya koymaktadır.

Anahtar Kelimeler: siber suç, jeopolitik, bilgi güvenliği, ceza hukuku, idare hukuku, mücadele mekanizmaları, iyileştirme, ceza hukuku, ceza politikası.