

İnformasiya təhlükəsizliyi kontekstində insan hüquqlarının müdafiəsi mexanizmlərinin təkmilləşdirilməsi

Həbib Hüseynov

AMEA Fəlsəfə və Hüquq İnstitutu
habib.huseynov@gmail.com

Xülasə— Məqalədə informasiya cəmiyyətində iqtisadiyyatın, elmin, təhsilin, siyasi və ictimai fəaliyyətin digər sahələrinin inkişafında informasiyanın, onun operativliyinin, dəqiqliyinin və etibarlılığının müstəsna əhəmiyyəti olduğu vurğulanır. Qeyd edilir ki, inkişaf prosesində informasiya tükənməyən, köhnəlməyən, əksinə, getdikcə daha da artan və keyfiyyətcə yaxşılaşan maddi sərvət kimi özünü göstərir. Məhz bu xüsusiyyətlərinə görə müasir dünyada informasiya yüksək dəyərə malik olan maddi və intellektual sərvət kimi qiymətləndirilir. Hazırda o, mahiyyət etibarilə insan hüquqlarının müdafiəsində mühüm və müasir vasitələrdən birinə çevrilmişdir. İnformasiyanın mübadiləsi rəqabətə deyil, əməkdaşlığa yol açdığı üçün inkişaf prosesində onun rolu getdikcə artır və mühüm əhəmiyyət kəsb edir.

Açar sözlər— informasiya; insan hüquqları; milli təhlükəsizlik; kibercinayətkarlıq; kiberterrorçuluq

Qloballaşma prosesinin sürətlə getdiyi bir zamanda cəmiyyət həyatında informasiyanın yeri və rolu günbəgün artmaqdadır. Cəmiyyətin inkişafının müasir mərhələsində informasiya resurslarının artması və genişlənməsi yalnız insan hüquqlarının etibarlı müdafiəsi ilə qarşılıqlı nisbətdə faydalı ola bilər. Ölkəmizdə hüquqi dövlətin qurulması hər kəsin şəxsi və ailə həyatına qanunsuz müdaxiləni qanunlar səviyyəsində qadağan etməklə şərtləndirmişdir. Çünki, insan hüquqlarının qorunması və ümumiyyətlə insanın cəmiyyətdə aparıcı mahiyyət daşıması, onun rolunun və dəyərinin son dərəcə yüksəlməsi məhz informasiya cəmiyyətinin və hüquqi dövlət quruculuğunun zəruri şərti kimi aktuallaşmışdır. Təsadüfi deyil ki, ölkəmizin «Milli Təhlükəsizlik Konsepsiyasının [1, s. 30-32, 43-44] 4.3.11-ci maddəsi informasiya təhlükəsizliyi siyasətinin aktuallığını şərtləndirirsə, həmin konsepsiyanın 4.3.1-ci maddəsi Azərbaycan Respublikasında insan hüquqlarının və azadlıqlarının qorunmasını və vətəndaş cəmiyyətinin inkişaf etdirilməsinin alternativsiz yolu kimi dəyərləndirmişdir.

Müasir cəmiyyətdə informasiya tükənməyən, köhnəlməyən, əksinə, getdikcə daha da artan və keyfiyyətcə yaxşılaşan maddi sərvət kimi özünü göstərir. Bu xüsusiyyətlərinə görə dünyada informasiya yüksək dəyərə malik olan maddi və intellektual sərvət kimi qiymətləndirilir. Eyni zamanda o, hazırda mahiyyət etibarilə insan hüquqlarının müdafiəsində mühüm və müasir vasitələrdən birinə çevrilmişdir. İnformasiyanın mübadiləsi rəqabətə deyil, əməkdaşlığa yol açdığı üçün inkişaf prosesində onun rolu getdikcə mühüm əhəmiyyət kəsb etməkdədir.

İnternetdən, həmçinin elektron daşıyıcılardan istifadənin genişləndiyi indiki dövrdə kibertəhlükəsizlik məsələlərinin və korrupsiya ilə mübarizənin aktuallığı daha da genişlənməmişdir. “Elektron hökumət”, “Elektron ədliyyə” və sair bu kimi

təsisatlar demokratik cəmiyyətdə insan hüquqlarının və azadlıqlarının və insana xidmətin müasir şərtinə çevrilmişdir.

Cəmiyyət inkişaf etdikcə insanlar informasiyadan daha artıq dərəcədə asılı vəziyyətə düşürlər. İnformasiya təhlükəsizliyinin təmin olunmaması isə cəmiyyət, dövlət və insanlar üçün böyük fəsadlar törədə bilər. İnformasiya təhlükəsizliyinin meydana çıxmasının əsas səbəblərindən biri kimi isə beynəlxalq səviyyədə internetin fəaliyyətini tənzimləyən mexanizmlərin yetərinə olmaması ilə də əlaqədardır. Hər bir ölkədə informasiya təhlükəsizliyinin prioritetləri dövlətin, cəmiyyətin və vətəndaşların maraqlarının balanslı nisbəti əsasında müəyyənləşir. Ölkədəki siyasi, hərbi, fəvqəladə və s. vəziyyətlərdən asılı olaraq bu nisbət dəyişə bilər. Cəmiyyətin təhlükəsizliyinin əsas komponentlərindən biri kimi informasiya təhlükəsizliyinin və insan hüquqlarının qorunması vəzifələrinin həyata keçirilməsi informasiyanın konfidensiallığı, tamlığı və əlverişliliyi ilə sıx bağlıdır [2, s.3].

İnformasiyanın cəmiyyətdə rolunu bilmək üçün ona iki aspektdən yanaşmaq lazımdır:

- 1) Mənfi-neqativ informasiyanın yayılmasının qarşısının alınması.
- 2) İnformasiyanın özünün qorunması.

Qlobal informasiya cəmiyyətində informasiya iqtisadiyyatın, elmin, təhsilin, siyasi və ictimai fəaliyyətin digər sahələrinin inkişafında informasiyanın, onun operativliyinin, dəqiqliyinin və etibarlılığının müstəsna əhəmiyyəti vardır. İnformasiya cəmiyyətində çox mürəkkəb formada qarşılıqlı münasibətdə olan korporativ və açıq informasiya fəzaları formalaşdırılır.

Məlumdur ki, informasiya cəmiyyətinin formalaşması mərhələləri beş səviyyədən ibarətdir: kommunikasiyalaşma, kompyuterləşmə, şəbəkələşmə, informasiyalaşma və virtuallaşma. Cəmiyyətin informasiya təhlükəsizliyinə olan tələblər və hədəflər məhz bu mərhələlərin nəzərə alınmasını şərtləndirir [3].

Müxtəlif səviyyələrdə təhlükələrin olmasına baxmayaraq, istənilən halda, təhlükələrin mənbəyi insandır və ya onun fəaliyyətidir. Hər bir insanın daxili dünyası, yaşadığı mühit onun psixoloji durumundan asılı olaraq cəmiyyət qarşısında məsuliyyətini itirməsi başqalarının hüquqlarının pozulması ilə nəticələnə bilər. Statistik hesabatlarla görə, sistemin öz istifadəçilərinin hərəkətləri nəticəsində vurulan ziyanın həcmi artıq virusların vurduğu ziyanı üstələyir. Təhlükəsizlik sahəsində bir çox problemlər istifadəçilərin, sistem administratorlarının və digər mütəxəssislərin informasiya təhlükəsizliyi sahəsində biliklərinin lazımı səviyyədə olmaması ilə bağlı ola bilər. Təbii ki, insan amilinə bağlı olan bu problemlərin aradan qaldırılması

informasiya təhlükəsizliyi mədəniyyətinin formalaşmasını zəruri edir.

Cəmiyyət inkişaf etdikcə, ona paralel olaraq cinayətkarlıq üsulları da genişlənir və təkmilləşir. Bu isə ölkə qanunvericiliyində mütəmadi yeniləşmələri şərtləndirir. Elə virtual sistemdə artan kiber cinayətlər də bu yeniləşmələri zəruri edən amillər sırasında yer alır. Bu gün informasiya, kommunikasiya sistemlərindən və müasir elmi-texniki vasitələrdən istifadə etməklə ən müxtəlif cinayətləri – terrorizmi, narkobiznesi, insan alveri, adam oğurluğu, müxtəlif tamah və zorakı cinayətləri törətmək mümkündür. Təsadüfi deyil ki, son illər bu təhlükəli təzahürlər bəşəriyyəti ciddi surətdə narahat etməkdədir. BMT-nin və digər beynəlxalq və regional qurumların kibercinayətkarlıqla mübarizəni gücləndirmək haqqında tövsiyələri məhz bu çağırışlarla bağlıdır.

İndiki şəraitdə keyfiyyətli informasiyaları seçmək və yalan informasiyaların yayılmasının qarşısının alınması mühüm bir problemə çevrilmişdir. Buna görə də şəxsiyyətin, dövlətin və cəmiyyətin təhlükəsizliyini qorumaq üçün daha mükəmməl qanunlar sisteminin işlənilib hazırlanması və həyata keçirilməsi son dərəcə aktuallaşmışdır.

İnformasiya təhlükəsizliyi – informasiya mühitində neqativ informasiyalardan qorunmaqla inkişafın təmin olunmasıdır. İnformasiya təhlükəsizliyi dövlətin müdafiə, ekoloji, iqtisadi təhlükəsizlik kimi formaları ilə yanaşı durur. Ona görə də, informasiya həm hüquqi həm texniki baxımdan müdafiə olunmalıdır [4, s.25-45].

İnformasiya təhlükəsizliyi – həmçinin televiziya, radio, çap, şəbəkə vasitəsi ilə cəmiyyət həyatında dövr edən neqativ informasiyalardan qorunmaqla da təmin olunmalıdır. Buna görə də son illər informasiya təhlükəsizliyini təmin etmək və kibercinayətkarlıqla mübarizəni gücləndirmək üçün beynəlxalq, regional və milli səviyyələrdə bir çox normativ-hüquqi aktlar hazırlanmışdır. Bu qanunlarda informasiyaların oğurlanmasının, itirilməsinin, dəyişdirilməsinin, qeyri-qanuni məhv edilməsinin, sürətinin götürülməsinin qarşısının alınmasının təmin edilməsi müddəaları xüsusi olaraq nəzərdə tutulmuşdur.

Təhlükələri müxtəlif meyarlara görə təsnifatını aparmaq və onları müxtəlif siniflərə ayırmaq olar. Meydana çıxma səbəblərinə görə təhlükələr təbii və süni xarakterli təhlükələrə ayrılır. Süni xarakterli təhlükələr də öz növbəsində bilməyə-rəkdən və qəsdən törədilən təhlükələrə bölünür. Təsir məqsədlərinə görə təhlükələrin üç əsas növü qruplaşdırılır:

- 1) İnformasiyanın konfidensiallığının pozulmasına yönələn təhlükələr;
- 2) İnformasiyanın bütövlüyünün pozulmasına yönələn təhlükələr;
- 3) Əlyətənliyin pozulmasına yönələn təhlükələr.

Konfidensiallıq informasiyanın subyektiv müəyyən olunan xassəsidir. Verilən informasiyaya müraciət icazəsi olan subyektlərin siyahısına məhdudiyət qoyulması zəruri məsələdir. Konfidensiallığın pozulmasına yönələn təhlükələr məxfi və ya gizli informasiyanın üstünün açılmasına yönəlib. Belə təhlükələrin reallaşması halında informasiya ona müraciət icazəsi olmayan şəxslərə məlum olur.

İnformasiyanın bütövlüyünün pozulmasına yönələn təhlükələr onun dəyişdirilməsinə və ya təhrifinə yönəlib ki, bunlar da onun keyfiyyətinin pozulmasına və tam məhvinə səbəb ola bilər. İnformasiyanın bütövlüyü bədniiyyətli tərəfindən qəsdən və ya sistemi əhatə edən mühit tərəfindən obyektiv təsirlər nəticəsində pozula bilər.

Əlyətənlik – yolverilən vaxt ərzində tələb olunan informasiya xidmətini almaq imkanındır. Həmçinin əlyətənlik – daxil olan sorğulara xidmət üçün onlara müraciət zəruri olduqda uyğun xidmətlərin həmişə hazır olmasıdır. Əlyətənliyin pozulmasına yönələn təhlükələr elə şəraitin yaradılmasına yönəlib ki, bu zaman müəyyən qəsdli hərəkətlər ya sistemin iş qabiliyyətini aşağı salır, ya da sistemin müəyyən resurslarına girişi bağlayır [5].

Bu gün hakerlərin sayları məhv etdiyi, qeyri-qanuni informasiya mənbələrinə daxil olmaq, viruslar yaymaq, banklardan “elektron pul” oğurlamaq, pornoqrafiya, “elektron şpionluq”, istədiyi materialı istədiyi sayta yerləşdirdiyi, hətta şəxsi, insanların özəl həyatına müdaxilə sayıla biləcək informasiyaları, foto və videoları paylaşaraq ictimailəşdirdiyi faktıdır. Statistika göstərir ki, hazırda kiber cinayətkarlıq digər analoqları ilə müqayisədə daha sürətlə artır. Bütün bunlar isə informasiya cəmiyyətində təhlükəsizliyin təmin olunmasını günün tələbinə çevirir ki, bu da ölkə qanunvericiliyi qarşısında internet istifadəçisinin fərd olaraq hüquqlarının qorunması kimi ciddi vəzifə qoyur.

Azərbaycan Respublikası Prezidentinin 2011-ci il 27 dekabr tarixli Sərəncamı ilə təsdiq edilmiş "Azərbaycan Respublikasında insan hüquq və azadlıqlarının müdafiəsinin səmərəliliyini artırmaq sahəsində Milli Fəaliyyət Proqramı" da bu zərurdən irəli gələ bilər. Lakin məsələ burasındadır ki, internetin sürətli inkişafı bu sahədə yaranan problemləri tənzimləmək üçün zəruri olan normativ-hüquqi aktların qəbulu prosesini xeyli qabaqlayır. Buna görə də sözügedən sahədə həllini gözləyən əsas problemlərdən biri də baş verən texnoloji yeniliklərə qanunvericilik sistemlərinin çevik, adekvat hüquqi mexanizmlərinin yaradılmasıdır. İnternetin tənzimlənməsi sahəsində ən mühüm məqamlardan biri dövlətin cəmiyyətin və şəxsiyyətin təhlükəsizliyi ilə insan hüquqları arasındakı tarazlığın qorunub saxlanması yönündə fəaliyyəti ilə bağlıdır. Reallıqdır ki, internetin təhlükəsizliyi və insan hüquqları arasındakı bu tarazlıq çox kövrək olub, daim bu və ya digər tərəfin xeyrinə pozulmağa meyllidir.

Transmilli mütəşəkkil cinayətkar qrupların müasir informasiya-kommunikasiya texnologiyalarından geniş miqyasda istifadə etməsi məlum faktıdır. Beynəlxalq terrorçu təşkilatlar elmi-texniki nailiyyətlərdən yararlanmağa, kompüter, rabitə, informasiya-kommunikasiya texnologiyaları və sair sahələrdə mütəxəssisləri öz sıralarına cəlb etməyə çalışırlar. Bu terrorçu təşkilatlar tərəfindən daim yeni üzvlərin rekrut edilməsi, törədilmiş terror aktlarına bəraət qazandırılması, potensial terrorçulara təlimlərin keçirilməsi, üzvlər arasında müntəzəm əlaqələrin saxlanması və sair məqsədlərlə İnternet şəbəkəsindən fəal istifadə edilir [6].

İnformasiya sistemləri üçün xarakterik olan bu xüsusiyyətləri nəzərə alaraq 2011-ci ilin sentyabr ayında "İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında" Azərbaycan Respublikasının prezidenti fərman imzaladı. Bu fərmanla ölkə-

mizdə informasiya təhlükəsizliyi ilə bağlı iki dövlət strukturunun yaradılması nəzərdə tutulur [7].

Dövlət orqanlarının informasiya ehtiyatlarının qorunması, bu sahədə təhdidlərin qarşısının alınması, dövlət informasiya infrastrukturunu subyektlərinin, onların istifadəçilərinin fəaliyyətinin əlaqələndirilməsi məqsədilə Azərbaycan Respublikası Xüsusi Dövlət Mühafizə Xidmətinin Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Agentliyi yaradıldı. Dövlət Agentliyi dövlət orqanları üçün xüsusi dövlət rabitəsinin, xüsusi təyinatlı informasiya-telekommunikasiya sistemlərinin və şəbəkələrinin, idarələrarası elektron sənəd dövriyyəsinin, dövlət orqanlarının internet şəbəkəsi ilə əlaqəsinin, onların internet informasiya resurslarının məlumat və resurs mərkəzində yerləşdirilməsinin təşkilini, istismarını, təhlükəsizliyini və inkişafını təmin edən, dövlət mühafizəsi obyektlərinin və mühafizə olunan obyektlərin təhlükəsizliyini təmin etmək məqsədi ilə xüsusi texniki tədbirləri həyata keçirir.

Agentlik dövlət orqanlarında kibertəhlükəsizlik sahəsində hazırlığın artırılması, bu sahədə qabaqlayıcı tədbirlərin həyata keçirilməsi məqsədi ilə məlumat və resurs mərkəzinin təhlükəsizliyinin təmini istiqamətində müvafiq tədbirlər görür. Həmçinin dövlət orqanlarının internet informasiya resurslarının və informasiya sistemlərinin təhlükəsizlik parametrləri üzrə monitorinqini həyata keçirir və bu sistemlərin kibertəhlükəsizliyinin artırılması istiqamətində dövlət orqanlarına müvafiq texniki və metodiki kömək göstərir.

Bu fərmanla yaradılan ikinci təşkilat Rabitə və İnformasiya Texnologiyaları Nazirliyinin tabeliyində olan Elektron Təhlükəsizlik Mərkəzidir. Mərkəzin əsas işi ölkədə ümumi kibertəhlükəsizlik vəziyyətini təhlil etmək, əhalinin, özəl və digər qurumların elektron vasitələrdən istifadə zamanı mövcud və yarana biləcək elektron təhlükələr barədə məlumatlandırılmasını həyata keçirmək, onlara texniki və metodiki kömək göstərmək, ölkəyə daxil olan ümumi internet trafikində global kiberrücumların qarşısını almaq məqsədi ilə milli internet operatoru ilə birlikdə qabaqlayıcı tədbirlər görməkdir.

Kibercinayətkarlığın, xüsusilə də kiberterrorçuluğun getdikcə daha ciddi xarakter alması bu təhlükələrin qabaqlanması istiqamətində Milli Təhlükəsizlik Nazirliyinin fəaliyyətinin təkmilləşdirilməsi zərurətini artırmışdır. Bu sahədə qanunsuz əməllərə qarşı mübarizə müvafiq texniki avadanlıqların mövcudluğunu, habelə yüksək texnolojiyalara dair xüsusi bilik və bacarıqlara yiyələnməyi tələb edir. Son illər ərzində məhz göstərilən sahələrə diqqət artırılmış, eləcə də ölkəmizin kibertəhdidlərə qarşı mübarizə imkanlarının təkmilləşdirilməsi istiqamətində adekvat tədbirlər görülmüşdür. Ötən dövrlərdə bankomatlardan istifadə edən şəxslərə məxsus hesablardan pulların oğurlanması ilə məşğul olan transmilli mütəşəkkil dəstə zərərsizləşdirilmiş, 8 nəfər, o cümlədən 2 xarici vətəndaş cinayət məsuliyyətinə cəlb edilmişdir. Rabitə və informasiya texnologiyaları sahəsində cinayətkarlıqla mübarizə tədbirləri çərçivəsində xarici vətəndaşlar tərəfindən Azərbaycan Respublikası ərazisində qeyri-qanuni beynəlxalq rabitə kanalının təşkili barədə toplanmış materiallar hüquqi qiymətin verilməsi üçün müvafiq dövlət orqanına göndərilmişdir. Qanunsuz olaraq dövlət təşkilatının məlumat (kompüter) bazasına daxil olma faktı ilə bağlı Azərbaycan

Respublikası Cinayət Məcəlləsinin 271.1 və 271.2 maddələri ilə cinayət işi açılmışdır. Kibercinayətkarlığa qarşı mübarizə istiqaməti üzrə həyata keçirilmiş tədbirlər nəticəsində bir çox cinayət işi açılmış və müəyyən qədər şəxslər cinayət məsuliyyətinə cəlb edilmişdir [6].

Cəmiyyətin təhlükəsizliyinin təmin olunmasında biometrik informasiya texnologiyaları böyük imkanlara malikdir. Təcrübədən məlumdur ki, informasiya-kommunikasiya sistemlərində, xüsusən də, İnternet mühitində baş verən cinayətlərin, qeyri-etik davranışın əsas səbəblərindən biri istifadəçilərin zəruri hallarda identifikasiyası mexanizmlərinin mükəmməl olmamasıdır. 2001-ci ilin 11 sentyabrında ABŞ-da baş verən terror hadisəsindən sonra BMT-nin Təhlükəsizlik Şurası insanların onlara məxsus biometrik məlumatlara əsasən identifikasiyasının həyata keçirilməsi, yeni nəsil sənədlərin tətbiqi haqqında qətnamə qəbul etmişdir. 2007-ci ildə Azərbaycanda da "Biometrik eyniləşdirmə sisteminin yaradılması haqqında" Dövlət Proqramı qəbul olunmuşdur.[8] Bu sistemin tətbiqi ilə milli təhlükəsizlik sisteminin təkmilləşdirilməsi, o cümlədən terrorçuluğa, qanunsuz miqrasiya və insan alverinə qarşı mübarizənin gücləndirilməsi, informasiya cəmiyyətinin qurulması kimi məsələlər öz həllini tapacaqdır. Biometrik texnologiyalar əsasında biometrik pasport-viza və şəxsiyyəti təsdiq edən digər sənədlər istehsalı və tətbiqinin təşkili də qarşıda duran məsələlərdəndir.

Məhz milli biometrik eyniləşdirmə sisteminin və 9 mart 2004-cü il tarixli «Elektron sənəd və elektron imza haqqında» Azərbaycan Respublikasının Qanununa əsasən yaradılan elektron imza [9] infrastrukturunun imkanlarının səmərəli şəkildə birləşdirilməsi və istifadəsi yalnız bu sənədlərdən irəli gələn problemlərin həllində deyil, ümumiyyətlə, informasiya məkanının, o cümlədən cəmiyyətin təhlükəsizliyinin yüksək səviyyədə təmin olunması üçün geniş imkanlar yaradacaqdır.

Hazırkı dövrdə informasiya təhlükəsizliyi şəraitində insan hüquq və azadlıqlarının ehtibarlı müdafiəsi daha da aktuallaşmışdır. Bu istiqamətdə ölkəmizdə hazırlanmış həyata keçirilən Milli fəaliyyət proqramları kompleks və sistemli şəkildə həyata keçirilməkdədir.

ƏDƏBİYYAT

- [1] Azərbaycan Respublikası Milli Təhlükəsizlik Konsepsiyası. Bakı: Hüquq ədəbiyyatı. 2009.
- [2] R. M. Əliquliyev, Y. N. İmamverdiyev, F. F. Yusifov, "Cəmiyyətin informasiya təhlükəsizliyinə dair bəzi konseptual baxışlar," *İnformasiya cəmiyyəti problemləri*, №2(4), s.3-9, 2011.
- [3] R. M. Əliquliyev, C. F. Valehov, R.Ş. Mahmudov, *İnternet-jurnalistikanın formalaşmasının bəzi aspektləri*. Ekspress-informasiya. *İnformasiya cəmiyyəti seriyası*. Bakı: "İnformasiya Texnologiyaları" nəşriyyatı, 2008, 32 s.
- [4] M.S. Xəlilov *İnformatika*, Bakı: 2008. 311 s.
- [5] *İnformasiya təhlükəsizliyi*. http://az.wikipedia.org/wiki/İnformasiya_təhlükəsizliyi
- [6] Kibercinayətkarlığa qarşı mübarizə <http://www.mns.gov.az/az/pages/47-125.html>.
- [7] *İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında Azərbaycan Respublikası Prezidentinin Fərmanı*. Bakı şəhəri, 26 sentyabr 2012-ci il.
- [8] *Biometrik eyniləşdirmə sisteminin yaradılması haqqında 2007-2012-ci illər üçün Dövlət Proqramı*, 13 fevral 2007-ci il.
- [9] *Elektron sənəd və elektron imza haqqında» Azərbaycan Respublikasının Qanunu*, 9 mart 2004-cü il.