İNFORMASİYA TƏHLÜKƏSİZLİYİNİN TƏMİN OLUNMASI: İNFORMASİYANIN MÜHAFİZƏSİ VƏ İNFORMASİYA MƏSULİYYƏTİ

Aytəkin İbrahimova*

Xülasə

Hüquqi məsuliyyət institutu əksər hüquq sahələrində mühüm mexanizmlərdən biri kimi tədqiq olunur. Məhz hüquqi məsuliyyət ictimai münasibətlərin tənzimlənməsində əsas rol oynayır. Əgər müxtəlif sahələri tənzimləyən qanunvericilik aktlarına nəzər salsaq müəyyən edə bilərik ki, həmin normativ mənbələrdə onun pozulmasının hüquqi məsuliyyətə səbəb olacağı müəyyən olunmuşdur. Bu hüququnun ümumi prinsipi olan ədalətliliyin təmin edilməsi ilə yanaşı cəmiyyətdəki fərdlər üzərində preventiv təsiri ilə də seçilir. Müəyyən olunmuş hüquqi məsuliyyət şəxsi belə qeyri-qanuni hərəkətlər etməkdən çəkindirir.

Məlumdur ki, informasiya təhlükəsizliyi daha geniş kateqoriya hesab edilməklə bir çox müxtəlif subkateqoriyaları özündə birləşdirir. İnformasiya təhlükəsizliyinin təhlili nəticəsində aydın olur ki, informasiyanın mühafizəsi sadəcə informasiya təhlükəsizliyinin təmin edilmə vasitələrindən biridir. İnformasiya təhülkəsizliyi informasiya mühafizəsinə münasibətdə daha geniş anlayış olub özündə sonuncunu da ehtiva edir. İnformasiya təhlükəsizliyinin vacib elementlərinin mühafizəsinin təmin edilməsinin informasiyanın mühafizəsi ilə olan sıx bağlılığı informasiyanın mühafizəsini müasir dövrdə bütün subyektlər üçün əsas prioritet məsələyə çevirir. İnformasiya təhlükəsizliyi yalnız qurğuların mühafizəsi ilə bağlı olmadığı informasiya texnologiyalarının inkişafından sonra öz təsdiqini tapan fakt kimi qiymətləndirilir. Hazırda üzərində əməliyyat aparılan informasiyanın mühafizəsinin təmin edilməməsi bir çox problemlərin yaranmasına səbəb olur.

Açar sözlər: *informasiya təhlükəsizliyi, informasiya hüquq pozuntusu, hüquqi məsuliyyət, məsuliyyətin növləri, informasiyanın mühafizəsi.*

Ədəbiyyatda rast gəlinən fikirlərdən biri isə hüquqi məsuliyyətin yalnız şəxsin hüquqazidd hərəkətlərinin həyata keçirilməsinin nəticəsində meydana gəlməsi ilə deyil, həmçinin başqalarının hüquqlarının məhdudlaşdırılması ehtimalının nəzərə alınmadan edilən hərəkət və ya hərəkətsizliyə görə meydana gəlməsi istiqamətində olmasıdır. [9, s.252] Hüquqi məsuliyyət özündə nəyi ehtiva etməsi araşdırılmalı əhəmiyyətli məsələlərdəndir. Əvvəla çox əhəmiyyətli məsələlərdən biri hüquqi məsuliyyət təhlükəsizliyin təmin edilməsi mexanizmi olub olmaması tədqiq edilməlidir. Hüquqi məsuliyyət qanuna və ya hüquqazidd əməl və ya fəaliyyətin (hərəkət və ya hərəkətsizlik) cəzalandırılması məqsədi güdən, qanunvericiliklə müəyyən olunan və qanunvericiliklə müəyyən edilmiş qaydada tətbiq edilən tədbirlərdir. Hüquqi məsuliyyət öz xarakterincə bir çox hüququnun ümumi prinsiplərinin yerinə yetirilməsində vacib rol oynayır. Həmçinin o, öz preventiv xüsusiyyətlərinə görə də cəmiyyətin təhlükəsizliyə aid məsələlərinə təsir edə bilir. Təhlükəsizliyə qarşı yönələn fəaliyyətlərə bir xəbərdarlıq rolu oynayır.

İnformasiya hüquq münasibətlərini tənzimləyən bir çox qanunvericilik aktlarında həmin aktların pozulmasına görə məsuliyyət müəyyən edilməsinə dair

* hüquq üzrə fəlsəfə doktoru, Bakı Dövlət Universitetinin Konstitusiya hüququ kafedrasının dosenti

norma vardır. Əvvəllərdə də qeyd etdiyimiz kimi informasiya təhlükəsizliyinin təmin edilməsinin əsas şərtlərindən biri müvafiq fəaliyyəti tənzimləyən normativ bazanın yaradılmasıdır. Normativ bazanın yaradılmasında qanunvericilik orqanının fəaliyyətindən əlavə informasiya təhlükəsizliyinə məsul olan, habelə informasiyanın ona məxsus sistemdə və ya ehtiyyatda istifadə edildiyi hüquqi təşkilati formasından asılı olmayaraq qurumların da rolu böyükdür. Bu qurumlar da öz növbəsində təşkilatdaxili normativ sənədlər qəbul etməklə informasiya təhlükəsizliyinin təmin edilməsinə istiqamətlənən fəaliyyət göstərməlidirlər. Belə normativ sənədlərə istifadəçi təlimatı, təhlükəsizlik siyasəti və s.-ni misal göstərmək olar. Həmçinin həmin qurumun və ya təşkilatın müvafiq daxili sənədlərində pozuntu hallarına səbəb ola biləcək şəxslərin qanunvericiliyin tələblərinə zidd olmayan şəkildə məsuliyyətə cəlb edilməsini müəyyən edən norma da mövcud ola bilər. Qeyd edilən növ məsuliyyət növündən geniş danışılacaqdır. Daha aydın olması üçün bir misal kimi şəxsin əmək haqqından tutulmalar, vəzifəsinin aşağı salınması və s. göstərilə bilər.

Hüquqi məsuliyyətin yaranmasının əsas şərti hüquq pozuntusu hesab edilən pozuntunun törədilməsidir. Məhz bu hal mövcud olduqdan sonra hüquqi məsuliyyətin yaranması və şəxslərin cəlb edilməsindən danışmaq olar. Hüquqi məsuliyyət xaraktercə də məcburidir. Belə ki hüquqi məsuliyyətin tətbiqi müxtəlif aktlarla təmin edilir.

Hüquqi məsuliyyətə dair aşağıdakı prinsipləri müəyyən etmək mümkündür.

- Qanunçuluq prinsipi: Hüququn və qanunun aliliyinin təmin olunduğu bütün dövlətlərdə bu prinsipin tətbiqi zəruridir. Belə ki, informasiya təhlükəsizliyinə qarşı yönələn hər bir fəaliyyətə dair nəzərdə tutulan hüquqi məsuliyyət qanuna və hüququn ümumi prinsiplərinə zidd olmamalıdır. İnfromasiya hüquq münasibətlərinin iştirakçıları, hüquqi məsuliyyətə cəlb edən qurum və təşkilatlar qanunvericiliyin, hüququn ümumi prinsiplərinə ciddi əməl etməlidir. Ölkəmizdə bu prinsipin tətbiqi ilə bağlı onu qeyd etmək olar ki, informasiya hüquq münasibətlərinin iştirakçıları və ya informasiya təhülkəsizliyinə məsul olan şəxslər hüquqi məsuliyyətə cəlb edilərkən AR Konstitusiyasının, informasiya hüquq münasibətlərini tənzimləyən AR qanunlarının, habelə AR-in tərəfdar çıxdığı beynəlxalq müqavilələrin müddəalarına ciddi əməl edilməlidir. AR qanunvericiliyinin müddəaları nəzərə alınmadan, hüquqi qüvvəsinə görə daha üstün aktların normalarına uyğun olmayan, hüquqi məsuliyyət müəyyən edən normativ sənədlərin və belə məsuliyyətə cəlb edən qəbul olunmuş qərarların hüquqi qüvvəsi olmamalıdır. Belə olduqda münasibətləri düzgün və dəqiq tənzimləmək, informasiya hüquq münasibəti iştirakçıları arasında hüquqa və qanuna inam yaratmaq, həmçinin informasiya təhlükəsizliyini təmin etmək olar. Bu prinsiplərə əsasən hüquqi məsuliyyətin müəyyən edilməsi və pozuntuya yol vermiş şəxslərin hüquqi məsuliyyətə cəlb edilməsi informasiya təhlükəsizliyinin təmin edilməsi və hüquqi məsuliyyətin bu sahədə olan preventiv funksiyasını daha yaxşı şəkildə həyata keçirilməsi ilə nəticələnəcəkdir.

- Bərabərlik prinsipi: Bu prinsip özünü informasiya hüquq münasibəti iştirakçılarının qanun və məhkəmə qarşısında bərabərliyini göstərir. Prinsip kimi müxtəlif qanunvericilik aktlarında və hüquq sahələrində müəyyən olunmuş bu prinsipin informasiya hüquq münasibətlərində olan hüquq pozuntularına dair hüquqi məsuliyyətin müəyyən edilməsi prosesində və məsuliyyətə cəlb edilməsi fəaliyyətində olduqca vacib rolu ilə seçilir. Qeyd olunan prinsipin konstitusion əsası AR Konstitusiyasının 25-ci maddəsində təsbit olunmuşdur. Belə ki, AR Konstitusiyasının 25-ci maddəsinin 1-ci, 3-5-ci hissələrinə əsasən hamının bərabərliyi prinsipinin əsas müddəaları təsbit olunmuşdur. [1] Belə ki, qeyd edilir ki, dövlət, irqindən, etnik mənsubiyyətindən, dinindən, dilindən, cinsindən, mənşəyindən, əmlak vəziyyətindən, qulluq mövqeyindən, əqidəsindən, siyasi partiyalara, həmkarlar ittifaqlarına və digər ictimai birliklərə mənsubiyyətindən asılı olmayaraq, hər kəsin hüquq və azadlıqlarının bərabərliyinə təminat verir. İnsan və vətəndaş hüquqlarını və azadlıqlarını irqi, etnik, dini, dil, cinsi, mənşəyi, əqidə, siyasi və sosial mənsubiyyətə görə məhdudlaşdırmaq qadağandır. Heç kəsə bu maddənin III hissəsində göstərilən əsaslara görə zərər vurula bilməz, güzəştlər və ya imtiyazlar verilə bilməz, yaxud güzəştlərin və ya imtiyazların verilməsindən imtina oluna bilməz. Göründüyü kimi məhz qeyd olunan fundamental hüquqlardan biri kimi qəbul edilmiş bərabərlik hüququnun təmin edilməsi məqsədi ilə informasiya təhlükəsizliyi sahəsində bərabərlik prinsipinin tətbiq edilməsi əhəmiyyətlidir. Bu özünü hüquqi məsuliyyətə cəlb etmə və ya bu sahədə digər fəaliyyətlərin göstərilməsi zamanı hər kəsin hüquq bərabərliyina istinad edilməsinə, məsuliyyətə cəlb etmək və ya hüquqi məsuliyyəti müəyyən etmək səlahiyyəti olan orqanların informasiya hüquq münasibətləri iştirakçısı olan şəxslərə isə hər hansı bir mülahizələrə görə üstünlük verilməməsində ehtiva edir. Təhlillərdə qeyd olunur ki, informasiya texnologiyalarının sürətli inkişaf etdiyi bir dövrdə bərabərlik prinispi öz təzahürünü informasiyaya və internətə bərabər çıxış imkanlarının yaradılmasında, habelə məlumatların mühafizəsində bütün fərdlərə eyni şərtlər və tələblərin tətbiqində tapır. Bu isə demokratik dəyərlərin və yeni nəsil insan hüquqlarının müdafiəsində mərkəzi rol oynayır. [11, s.87]

- Ədalətlilik prinsipi: Qeyd olunduğu kimi hüquqi məsuliyyət yol verilmiş hüquq pozuntusu nəticəsində dəymiş zərərin əvəzinin ödənilməsi və ya ona görə cəza müəyyən edilməsini özündə ehtiva edir. Hüquqi məsuliyyət yaradan hərəkətə yol vermiş şəxs barəsində qərar qəbul edərkən bir çox hallar nəzərə alınmalıdır. Əvvəla təyin edilən hüquqi məsuliyyət tədbiri baş tutan hüquq pozutusuna müvafiq olmalıdır. Yəni nə onun nəticələrinə və ictimai təhlükəliliyinə nisbətdə az, nə də ona nisbət çox məsuliyyət tədbirlərinin görülməsi ədalətlilik prinsipinin pozulması ilə nəticələnəckdir. Əvvəla ədalətlilik prinsipinin təmin edilməsi sosial baxımından ictimai münasibətlərdə olduqca əhəmiyyətlidir. Bununla insanların ictimai ədalətə inamı yaranır və pozuntulara görə məsuliyyətə cəlb etmə preventiv xarakterini göstərə bilir.

- İnformasiya hüquq münasibətləri kontekstində informasiya təhlükəsizliyinin təmin olunmasında ədalət mühakiməsinin obyektiv, qərəzsiz və ədalətli

olaraq həyata keçirilməsi: Ədalət mühakiməsinin obyektliyi, qərəzsizliyi və ədalətliliyi də əsas fundamental insan hüquqları ilə bağlı olduğundan insan hüquqlarına dair bir çox sənədlərdə öz əksini tapmışdır. Belə ki, 1950-ci il Avropa İnsan Hüquqları Konvensiyasının 6-cı maddəsi insanların ədalətli məhkəmə hüququnu hər kəsin, onun mülki hüquq və vəzifələri müəyyən edilərkən və ya ona qarşı hər hansı cinayət ittihamı irəli sürülərkən, qanun əsasında yaradılmış qərəzsiz məhkəmə vasitəsilə, ağlabatan müddətdə işinin ədalətli araşdırılması hüququna malik olması ilə müəyyən edir. [4] Bu prinsip özünü informasiya hüquq münasibətlərində informasiya təhlükəsizliyinə dair baş vermiş pozuntularında məsul olan şəxslər barəsində ədalət mühakiməsi ilə bağlı materiallara qanunvericiliyə müvafiq surətdə müəyyən edilmiş hüquqi prosedurlara uyğun faktlar əsasında, qərəzsiz və ədalətlə baxılmalı olmasını özündə ehtiva edir. Burada əsas vəzifə və öhdəlik məhkəmənin və ya ədalət məhkəməsini həyata keçirən qurumun (orqanın) üzərinə düşür. İnformasiya təhlükəsizliyi ilə əlaqədar keçirilən ədalət mühakiməsi icraatında ədalət mühakiməsini həyata keçirən orqan və ya qurumun səlahiyyətli şəxsi yalnız qanunun mənafeyini ifadə edə bilər.

Yuxarıda qeyd olunan prinsiplərin təmin edilməsi informasiya təhlükəsizliyində öz müsbət töhfəsini verə bilər. Hətta bu prinsiplərin rəhbər tutulması olduqca vacib və zəruridir. İnformasiya təhlükəsizliyini təmin etmək üçün istifadə edilə bilən müxtəlif hüquqi məsuliyyət formaları var. Hüquq ədəbiyyatında olan ortaq mövqeyə əsaslanaraq, hüquqi məsuliyyətin dörd növünü fərqləndirə bilərik. Bunlar aşağıdakılardır:

1. Mülki məsuliyyət;
2. İnzibati məsuliyyət;
3. Cinayət məsuliyyəti;
4. İntizam məsuliyyəti.

- Mülki məsuliyyət: Bu, informasiyanın elementlərinin pozulması və ya digər informasiya təhlükəsizliyi insidentləri nəticəsində fərdlərə və ya təşkilatlara dəyən hər hansı zərərin əvəzinin ödənilməsi ilə bağlı qanuni öhdəliyə aiddir. Bir çox hallarda mülki hüquqi məsuliyyətin delikt hüququndan asılı olduğu və buradan meydana gəlməsinə dair fikirlərə də rast gəlinir. [15, s.2115]

Mülki məsuliyyət adətən məhkəmə qaydasında müəyyən edilir və informasiyanın qeyri-qanuni istifadəsi, itirilməsi, məhv edilməsi, əsas elementlərinin pozulması, o cümlədən pozuntu barədə prosessual xərcləri və nüfuzun zədələnməsi ilə bağlı zərərlərin əvəzinin ödənilməsi ilə bağlı qərarın qəbul edilməsi mümkün ola bilər. Hazırda mülki məsuliyyətin müəyyən edilməsi mexanizmlərindən biri mübahisələrin məhkəmədənkənar həlli ilə bağlı yaranan institutdur. Mediasiya intitutu tərəfləri bir araya gətirə bilən və danışıqların həyata keçirilməsinə imkan verən bir müstəvidir. Mediasiya prosesi nəticəsində bir çox məsələlər məhkəmədənkənar şəkildə öz həllini tapır. Bu isə daha az prosessual xərc, daha az vaxt və daha az bürokratik məsələlərin olması ilə seçilən bir proses kimi qiymətləndirilir. Odur ki, adətən mülki dövriyyə iştirakçıları könüllü şəkildə mediasiya danışıqlarına başlanılmasını məqsədəmüvafiq və daha uyğun hesab edir-

lər. Hazırda qanunvericiliyimizdə mülki işlər üzrə mediasiya prosesi məcburi bir prosedur qayda kimi nəzərdə tutulmuşdur.

AR Mülki Məcəlləsinin 21-ci maddəsinə əsasən, zərərin əvəzinin ödənilməsini tələb etmək hüququna malik olan şəxs ona vurulmuş zərərin əvəzinin tam ödənilməsini tələb edə bilər. [2] Eyni zamanda, qanunvericiliklə zərər dedikdə, hüququ pozulmuş şəxsin pozulmuş hüququnu bərpa etmək üçün çəkdiyi və ya çəkməli olduğu xərclər, əmlakından məhrum olması və ya əmlakının zədələnməsi (real zərər), habelə hüququ pozulmasaydı, həmin şəxsin adi mülki dövriyyə şəraitində əldə edəcəyi gəlirlər (əldən çıxmış fayda) başa düşülür.

Göründüyü kimi informasiya təhlükəsizliyinə dair hüquq pozuntuları törətmiş şəxs bunun nəticəsində zərərçəkmiş şəxslərə dəymiş maddi və mənəvi zərərin əvəzinin ödəmək öhdəliyi daşıyır. Qeyd olunmalıdır ki, vurulmuş maddi zərərin həcminə həmçinin şəxsin gələcəkdə əldə edə biləcəyi lakin hüquq pozuntusunun törədilməsi səbəbindən bu imkanı itirməsi nəticəsində məhrum olduğu gəlirlər, yəni əldən çıxmış fayda da daxil edilir. O da qeyd edilməlidir ki, informasiya təhlükəsizliyinə dair hüquq pozuntusu mövcud olduğu halda hüquqları pozulmuş şəxsə maddi ziyanla bərabər mənəvi zərər də vurulur. Həmçinin mülki prosessual qanunvericiliyə əsasən informasiya təhlükəsizliyi ilə əlaqədar hüquq pozuntusu törətmiş şəxs çəkilmiş prosessual və digər xərclərin ödənilməsinə dair məsuliyyəti də mövcuddur. Yəni belə xərclər mövcud olduqda müvafiq hüquq pozuntusunu törətmiş subyektin mülki hüquqi məsuliyyəti ağırlaşır.

Digər tərəfdən, AR Mülki Məcəlləsinin 23-cü maddəsinə əsasən, fiziki şəxs onun şərəfini, ləyaqətini və ya işgüzar nüfuzunu ləkələyən, şəxsi və ailə həyatının sirrini və ya şəxsi və ailə toxunulmazlığını pozan məlumatların məhkəmə qaydasında təkzib olunmasını tələb edə bilər, bu şərtlə ki, həmin məlumatları yaymış şəxs onların həqiqətə uyğun olduğunu sübuta yetirməsin. [2] Əgər fiziki şəxsin şərəfini, ləyaqətini, işgüzar nüfuzunu ləkələyən və ya şəxsi və ailə həyatının sirrinə qəsd edən məlumatlar kütləvi informasiya vasitələrində yayılmışdırsa, həmin kütləvi informasiya vasitələrində də təkzib edilməlidir. Şərəfini, ləyaqətini və ya işgüzar nüfuzunu ləkələyən məlumatlar yayılmış fiziki şəxsin həmin məlumatların təkzibi ilə yanaşı, onların yayılması nəticəsində vurulmuş zərərin əvəzinin ödənilməsini tələb etmək hüququ vardır.

Qeyd olunan normanın da məzmunundan göründüyü kimi, mülki hüquqi məsuliyyət informasiya təhlükəsizliyi ilə əlaqədar törədilmiş hüquq pozuntusu nəticəsində subyektin şərəfin, ləyaqətin və işgüzar nüfuzun müdafiəsinin təmin edilməsini və ona dəyən zərərin əvəzinin ödənilməsini də ehtiva edir.

Həmçinin informasiya təhlükəsizliyinə dair bağlanılmış müqavilə öhdəliklərin yerinə yetirilməməsi də mülki hüquqi məsuliyyətin yaranması üçün əsasdır. Bu, xidmət səviyyəsi müqavilələri və ya məlumatların işlənməsi müqavilələri kimi informasiya təhlükəsizliyi ilə bağlı müqavilə öhdəliklərinə əməl etmək üçün hüquqi öhdəliyin təmin edilməsini özündə ehtiva edir. Bu öhdəliklərin yerinə yetirilməməsi müqavilə tələblərinin pozulması və zərərin ödənilməsi ilə nəticələnir.

- İnzibati məsuliyyət: İnformasiya təhlükəsizliyi əlaqədar törədilmiş hüquq pozuntusu ictimai təhlükəliliyinin dərəcəsinə əsasən müxtəli hüquqi məsuliyyətə səbəb olur. Belə ki, informasiya təhlükəsizliyi ilə əlaqədar bəzi hüquq pozmaları cinayət əməllərinə nisbətdə daha yüngül olduğundan belə əməllər (hərəkət və ya hərəkətsizlik) inzibati məsuliyyətin yaranması üçün əsas olur. İnzibati məsuliyyətə cəlb edilən şəxs müxtəlif sanksiyalara məruz qala bilər. Belə sanksiyalara inzibati xətanın törədilməsində istifadə edilmiş alət və ya vasitələrin müsadirə edilməsi və ya məhv edilməsi, cərimə, inzibati həbs, müəyyən növ fəaliyyətlə məşğul olmamaq və s. ola bilər.

AR İnzibati Xətalar Məcəlləsində informasiya hüquq münasibətləri ilə əlaqədar, xüsusən də informasiya təhlükəsizliyi əleyhinə inzibati xətalar həmin Məcəllənin "İnformasiyadan istifadə edilməsi, onun yayılması və mühafizəsi qaydaları əleyhinə olan inzibati xətalar" adlı fəslində müəyyən edilmişdir. Belə ki, AR İnzibati Xətalar Məcəlləsində özündə bununla əlaqədar mühüm normaları birləşdirən inzibati xətalar əks olunmuşdur (məsələn, informasiya ehtiyatlarından istifadə qaydalarının pozulması, kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydasının pozulması, fərdi məlumatlar haqqında qanunvericiliyin pozulması, internet informasiya ehtiyatında və ya informasiya-telekommunikasiya şəbəkəsində yayılması qadağan edilən informasiyanın yerləşdirilməsi, habelə belə informasiyanın yerləşdirilməsinin qarşısının alınmaması və s.) [3].

- Cinayət məsuliyyəti: Bəzi əməllər isə daha çox ictimai təhlükəli olduğundan qanunvericiliklə cinayət kimi müəyyən edilmişdir. Cinayət hüquqi məsuliyyətini mövcud ən ağır hüquqi məsuliyyət kimi qiymətləndirilməsinə dair ədəbiyyatda ortaq fikirlər mövcuddur. Qeyd edilməlidir ki, hüquqi məsuliyyət olmaqla ağırlığı ilə seçilən cinayət məsuliyyəti tətbiq olunduğu hallarda da əməllər öz ictimai təhlükəliliyinə görə daha ağır olur. Bu, kibertəhlükəsizlik riayət edilməməsi və hakerlik, oğurluq və fırıldaqçılıq kimi ictimai təhlükəli cinayət fəaliyyətlərindən qaçmaq üçün hüquqi məsuliyyəti özündə ehtiva edir. Məsələn, AR-in də tərəfdar çıxdığı "Kibercinayətkarlıq haqqında" Konvensiya kompüter məlumatları və sistemlərinin məxfiliyi, tamlığı və istifadə imkanlarına qarşı, kompüter vasitələrindən istifadə ilə bağlı, məlumatların məzmunu ilə bağlı, əqli mülkiyyət hüquqlarının pozulması ilə bağlı cinayətləri müəyyən etmişdir. [8] Həmçinin konvensiya məsuliyyətin əlavə növləri və sanksiyaların da müəyyən edilməsi istiqamətində xüsusi əhəmiyyəti ilə seçilir.

Qeyd edilməlidir ki, yuxarıda göstərilən prinsiplərin tətbiq edilməsi və törədilmiş cinayətlərə görə müvafiq cəza tədbirlərinin tətbiq edilməsi ilə informasiya təhlükəsizliyini də təmin etməyə müsbət təsir göstərmək olar.

- İntizam məsuliyyəti: Bu informasiya təhlükəsizliyinin təmin edilməsi vəzifə funksiyalarına aid edilən şəxslərin yol verdikləri səhv ucbatından hüquq pozuntusu baş verildiyi hallarda xüsusi subyektlər dairəsinə tətbiq edilən hüquqi məsuliyyət növüdür. Bu, peşəkar fəaliyyətlə məşğul olan şəxslərin sənaye standartlarına və informasiya təhlükəsizliyi üçün ən yaxşı təcrübələrə uyğun xidmət göstərmək üçün qanuni öhdəliyinin təmin edilməsi məqsədini güdür. Bu stan-

dartlara əməl edilməməsi intizam məsuliyyətinə cəlb edilmə və hüquq sahiblərinə ziyan vurulması ilə nəticələnə bilər. İntizam məsuliyyətinə misal kimi dövlət qulluqçuların öz qulluq funksiyalarını tam yerinə yetirmədiyi hallarda tətbiq olunan intizam məsuliyyəti tədbirlərini göstərə bilərik. Belə ki, "Dövlət qulluğu haqqında" AR Qanununun müddəalarına əsasən dövlət qulluqçusuna həvalə olunmuş vəzifələrin yerinə yetirilməməsi və ya lazımi şəkildə yerinə yetirilməməsi, habelə bu Qanunla müəyyən edilmiş məhdudiyyətlərə əməl olunmaması, qanunda başqa qayda nəzərdə tutulmayıbsa, intizam məsuliyyətinə səbəb olur. [5] İntizam məsuliyyətinə cəlb etmə halları mövcud olduqda dövlət qulluqçusu barəsində bir sıra intizam tənbeh tədbirləri tətbiq edilə bilər (məsələn, töhmət verilməsi, həmin təsnifatda olmaqla vəzifə maaşı aşağı olan vəzifəyə keçirilməsi, və s.).

Hüquqi məsuliyyətin bu müxtəlif formalarından informasiya təhlükəsizliyinin təmin edilməsi üçün hərtərəfli hüquqi baza yaratmaq üçün birgə istifadə oluna bilər. Hüquqi məsuliyyət informasiya təhlükəsizliyinin təmin edilməsində təsirli mexanizm kimi qiymətləndirilməlidir. Bu, fərdlərin və təşkilatların informasiya təhlükəsizliyini təmin etmək, məlumatı qorumaq və məxfi məlumatların icazəsiz və qeyri qanuni istifadəsinin və ya açıqlanmasının qarşısını almaq üçün qanuni öhdəlikləri özündə ehtiva edir. Hüquqi məsuliyyət informasiyanın qorunması, kibertəhlükəsizlik, informasiyanın məxfiliyi, ictimai təhlükəlilik dərəcələrinə görə inzibati hüquq münasibətləri və cinayət ilə əlaqədar müxtəlif normativ hüquqi aktlarla müəyyən edilə bilər.

Hüquqi məsuliyyət fərdləri və təşkilatları informasiya təhlükəsizliyini təmin etmək üçün fəal addımlar atmağa həvəsləndirmək üçün istifadə edilə bilər, çünki bunun edilməməsi cərimələr, məhkəmə iddiaları və ya cinayət ittihamları kimi hüquqi nəticələrlə nəticələnə bilər. Bu, fərdlərin və təşkilatların informasiya təhlükəsizliyinə ciddi yanaşmağa və öz fəaliyyətlərində onu prioritetləşdirməyə, hesabatlılıq və məsuliyyət mədəniyyətinin yaradılmasına köməklik edə bilər.

Qanunlar və qaydalar hüquqi məsuliyyət müəyyən etməklə yanaşı, məlumatların qorunması, şifrələmə və insidentlərə reaksiya standartları kimi informasiya təhlükəsizliyi üçün ən yaxşı təcrübələrə dair təlimatlar da təmin edə bilər. Bu, fərdlərin və təşkilatların öz öhdəliklərini aydın dərk etmələrini və məlumatı qorumaq üçün fəal addımlar ata bilmələrini təmin etməyə kömək edə bilər.

Bununla belə, yalnız hüquqi məsuliyyət informasiya təhlükəsizliyini təmin etmək üçün kifayət olmaya bilər, çünki o, effektiv icra və uyğunluq mexanizmlərinə əsaslanır. İnformasiya təhlükəsizliyinə hüquqi məsuliyyət, texniki tədbirlər, təşkilati siyasət və prosedurlar, işçilərin təlimi və maarifləndirilməsinin məcmusunu əhatə edən kompleks yanaşmanın olması vacibdir.

Məlumdur ki, informasiyanın mühafizə edilməsi informasiya təhlükəsizliyində öz xüsusi rolu ilə seçilir. İnformasiyanın həm pozitiv, həm də neqativ məqsədlər üçün istifadə edilə bilməsinə baxmayaraq, informasiya təhlükəsizliyi-

nin məhz həmin neqativ məqsədlərin qarşısının alınması, pozitiv məqsədlər üçün isə istifadə olunan informasiyanın mühafizəsi funksiyası bu zaman xüsusilə mühüm əhəmiyyət kəsb edir. Nəticə etibarı ilə bütövün hissəyə, yaxud ümuminin xüsusiyə nisbəti "informasiya təhlükəsizliyi" və "informasiyanın mühafizəsi" anlayışlarının bir-biri ilə qarşılıqlı əlaqəsini qiymətləndirmək üçün istifadə edilə bilər. [6, s.170]

İnformasiyanın mühafizəsinə qeyri müəyyən filosofik anlayış kimi baxılmamalıdır. Real təcrübədə informasiyanın mühafizəsi informasiya təhlükəsizliyinin təmin edilməsi prosesinin ən əsas mərhələlərindən biri kimi çıxış edir. Çünki təhlillərdən birinə əsasən qeyd edilə bilər ki, iqtisadi dəyərə malik olan informasiyanın əsas elementlərini (məxfiliyini, bütövlüyünü və əlçatanlığını) təmin etmək və qorumaq informasiyanın mühafizəsi ilə mümkündür. [10, s.412]

Qısacası belə qeyd etmək olar ki, informasiyanın mühafiəzsinin təmin edilmədiyi halda informasiya təhlükəsizliyi də pozulacaqdır. Bu münasibəti nəzərə alaraq onu da qeyd etmək zəruridir ki, informasiyanın mühafizəsinin təmin edilməməsi informasiya təhlükəsizliyinə təhdid risq təşkil etsə də, informasiya təhlükəsizliyinin təmin edilməməsinə səbəb olan halların heç də hamısı informasiyanın mühafizəsi ilə bağlı deyildir.

İnformasiyanın mühafizə edilməsi ilə bağlı olan normativ tənzimləmə və prosedur qaydalar özü özlüyündə inkişaf yolu keçmişdir. İnformasiyanın mühafizəsi ilə əlaqədar təhlillərin birində göstərilir ki, informasiyanın qanunsuz yollarla əldə olunması, açıqlanması və məhv edilməsi insanların şəxsi həyatına təsir edən bir məsələdir. Bu isə özlüyündə informasiyanın mühafizəsinin zəruriliyinin əsas göstəricilərindən biridir. [12, s.85]

İçərisində açıqlanması məhdudlaşdırılan informasiyanın da yer aldığı rəqəmsal cəmiyyətin inkişafı informasiya mühafizəsinə diqqət ayrılmasını daha da zəruri edir. [14, s.542] Təhlillərin birində haqlı olaraq gösətilir ki, effektiv informasiya mühafizəsi informasiyanın üzərində əməliyyatlar aparılarkən əsas elementlərin (gizlilik, əlçatanlıq, tamlıq) qorunması üçün nəzərdə tutulmuş texniki, inzibati və fiziki nəzarət vasitələrinin tətbiqi ilə mümkündür. [13, s.39]

Odur ki, informasiyanın mühafizəsi dedikdə, informasiyanı icazəsiz daxil olmaqdan, istifadədən, açıqlamadan, pozulmaqdan, dəyişdirilməkdən və ya məhv edilməsindən qorumaq üçün görülən tədbirlər nəzərdə tutulur. İnformasiyanı müxtəlif yollarla, o cümlədən fiziki, texniki və inzibati vasitələrlə mühafizə etmək mümkündür. İnformasiyanın qanunvericiliklə müəyyən edilmiş qaydada istifadəsinin təmin edilməsi elə informasiyanın mühafizəsinin təmin edilməsi ilə nəticələnir.

İnformasiyanın fiziki mühafizəsi kompüter sistemləri, serverlər və saxlama cihazları kimi fiziki aktivlərin təhlükəsizliyini əhatə edir. Bu, bu aktivlərə fiziki girişi məhdudlaşdırmaq üçün kilidlərdən və giriş nəzarətlərindən istifadə kimi tədbirlər vasitəsilə həyata keçirilə bilər. İnformasiyanın mühafizəsinin təmin edilməsi məqsədi ilə onun saxlandığı və ya emal olunduğu daşıyıcıların mühafizə edilməsi informasiya təhlükəsizliyinə təsir edən əsaslı faktordur. Təcrübə-

yə əsaslanaraq qeyd edilə bilər ki, bir çox infiormasiya təhlükəsizliyi risqləri məhz informasiya daşıyıcıların təhüləkizliyinin təmin edilməməsi üzündən meydana çıxır.

Texniki mühafizə informasiyaya icazəsiz daxil olmadan, istifadəsindən və ya dəyişdirilməsindən qorumaq üçün müxtəlif təhlükəsizlik texnologiyalarından istifadəni nəzərdə tutur. Texniki mühafizə tədbirlərinə misal olaraq şifrələmə, firewall, antivirus proqram təminatı, müdaxilənin aşkarlanması və qarşısının alınması sistemləri və girişə nəzarət mexanizmləri daxildir.

İnformasiyanın inzibati mühafizə üsulları məlumatın mühafizəsini təmin etmək üçün siyasətlərdən, prosedurlardan və təlimatlardən istifadəni nəzərdə tutur. İnformasiyanın inzibati mühafizə üsulları təhlükəsizlik siyasəti və prosedurlarının işlənib hazırlanması və həyata keçirilməsi, işçilər üçün təhlükəsizliklə bağlı maarifləndirmə təliminin keçirilməsi və təhlükəsizlik siyasəti və prosedurlarının həyata keçirilməsini ehtiva edir.

Bütövlükdə, informasiyanın mühafizəsi informasiya təhlükəsizliyinin təmin edilməsi üçün mühüm əhəmiyyət kəsb edir, çünki o, həssas və qiymətli məlumatların yalnız səlahiyyətli şəxslər üçün əlçatan olmasını və icazəsiz giriş və ya istifadə nəticəsində təhlükəyə məruz qalmamasını təmin etməyə kömək edir.

Belə ki, informsiyanın mühafizəsinin təmin edilməsi informasiyanın qanuni yollarla əldə edilməsi, ötürülməsi, saxlanılması və ya məhv edilməsinə zəmanət verir. Belə olan hallarda qanunla müəyyən edilməmiş hərəkətlərdən mühafizə tədbirləri planlaşdırılır və tətbiq edilir. İnformasiyanın mühafizəsi şəxsin ona dair məlumatlarının sorğulandığı subyektlər dairəsi barədə məlumat əldə etmək hüququnun təmin edilməsi ilə də sıx bağlıdır. Məhz bu yol və üsulla informasiyanın mühafizə edilməsi prosesində boşluq mövcud olması və ya pozuntu olması hallarının müəyyənləşdirilməsi mümkündür. İnformasiyanın mühafizəsi prosesində nəzarət digər əhəmiyyətli məsələdir. Əgər əvvəllər bu prosesin həyata keçirilməsi yalnız fiziki şəxsin özü tərəfindən mümkün idisə, hazırda informasiya texnologiyalarının inkişafi nəticəsində əldə olunmuş nəaliyyətlər bu prosesinin elektronlaşdırılmasına imkan vermişdir. Yəni süni intellekt vasitəsi ilə informasiya üzərində aparılan əməliyyatlara daha asan və az enerji sərfi ilə nəzarət etmək, informasiya mühafizəsinin təmin edilməsinə dəstək göstərmək mümkün olur. Lakin bunun özlüyündə mütləq süni intellektin fəaliyyəti üzərində səlahiyyətli şəxs tərəfindən nəzarət aparılmasını da zəruri edir. Belə ki, hətta bütün proses süni intellekt tərəfindən aparılsa belə, onun fəaliyyətinə cavabdeh olan səlahiyyətli şəxs müəyyən edilməli, həmin şəxs tərəfindən minimal tələblərə müvafiq olaraq vaxt aşırı süni intellektin işləkliyi və ya fəaliyyətinə nəzarət həyata keçirilməlidir.

İnformasiyanın mühafizəsində nəzərə çarpan digər əhəmiyyətli məsələlərdən biri də informasiya sahibinin razılığıdır. Hüquqi baxımdan bu razılıq təsdiqinin tapması olduqca zəruridir. Odur ki, açıqlanması məhdudlaşdırılan informasiya ilə əlaqədar informasiya mühafizəsi tədbirlərinin həyata keçirilməsi zamanı yalnız yazılı və şübhə doğurmayan razılıqların nəzərə alınması informasiyanın

mühafizəsinə öz müsbət töhvəsini verə bilər. Həmçinin belə razılığın əldə edilməsindən əvvəl razılığını ifadə edən subyektə razılığı nəticəsində baş verə biləcək və əvvəldən ehtimal olunan bütün hallar barədə xəbərdarlıq edilməsi arzu olunandır. Elektronlaşdırılmış belə sistemlərdə qeyd olunan prosesin tətbiqi daha rahat olur. O da nəzərə alınmalıdır ki, subyektin razılıq verməməsi və ya verdiyi razılığa xitam verməsi onun subyektiv hüququdur. Razılığa xitam verildiyi andan bu məlumatı qəbul edən subyekt müvafiq tədbirlərin görülməsini təmin etməlidir. Qeyd olunur ki, informasiya sahibinin razılığı məhz informasiya təhlükəsizliyinə dair münasibətlərdə meydana çıxan bir sıra məsələlərin hüquqi və etik əsasını təşkil edir. Habelə Avropa İttifaqı çərçivəsində qəbul edilmiş Ümumi Məlumatların Mühafizə edilməsi Qaydaları (GDPR) kimi bir çox qanunvericiliklər belə razılıqlara dair tələblər müəyyən edir, habelə bu razılığın verilməsi məlumatın istifadə edilməsinə icazə verilən subyektə də mühafizə tədbirlərinin görülməsi öhdəliyinin əsasını qoyur. [17, s.148]

İnformasiya texnologiyalarının və süni intellektin inkişafi informasiyanın mühafizəsi sahəsində yeni təhdidlərin və risqlərin yaranmasına, habelə hücumlarda məlum olmayan üsul və vasitələrdən istifadə edilməsinə səbəb olur. Bu isə özülüyündə informasiyanın mühafizəsini, dolayısı yolla informasiya təhlükəsizliyinin təmin edilməsində müəyyən çətinlikləri yaradır.

İnformasiya təhlükəsizliyinin təmin olunmasında informasiyanın mühafizəsi əsas təşkil edir. Qanunvericiliklə informasiyanın mühafizəsinin təmin edilməsinin hüquqi rejimi və şərtləri müəyyən olunmuşdur. "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" AR Qanununun 18-ci maddəsi informasiyanın mühafizəsinin təşkilinin normativ məzmununu müəyyən edir. [7] Belə ki, həmin maddənin normativ məzmununa görə barəsində qanunsuz əməliyyatlar və davranış nəticəsində mülkiyyətçiyə, sahibə, istifadəçiyə və ya başqa şəxslərə ziyan vurula bilən hər hansı sənədləşdirilmiş informasiya mühafizə olunmalıdır.

İnformasiyanın mühafizəsinin təşkilində informasiya sahibi olan subyektlərin də hüquqlarının müdafiəsi zəruridir. Odur ki, həmçinin qanunvericiliklə həmin subyektlərin hüquq və vəzifələri dəqiq müəyyən edilmişdir. Bundan başqa, istifadəçilərin informasiyadan istifadə etmə qaydaları normativ sənədlərlə müəyyən olunmuşdur ki, bu qaydalara uyğun şəkildə informasiyanın istifadə edilməsi məhz informasiyanın mühafiəzisinin və ümumilikdə informasiya təhlükəsizliyinin əsasını təşkil edir. Daha sonra, informasiyanın mühafizəsi ilə bağlı məsuliyyətin qanunvericiliklə dəqiq müəyyən edilməsi informasiya təhülkəsizliyinin təmin edilməsində xüsusi rola malikdir. Bu həm preventiv funksiya, həm də ictimai münasibətlərin tənzimlənməsində boşluqların aradan qaldırılması istiqamətində olduqca əhəmiyyətlidir.

İnformasiyanın qorunması informasiya təhlükəsizliyinin vacib komponentidir. Bu, həssas və ya məxfi məlumatları icazəsiz daxil olmaqdan, istifadədən, açıqlamadan, dəyişdirmədən və ya məhv etməkdən qorumaq üçün istifadə olunan tədbirlərə və mexanizmlərə aiddir. İnformasiyanın mühafizəsi müxtəlif

texniki, fiziki və inzibati nəzarət vasitələri ilə təmin edilir. Belə üsul və ya vasitələrə şifrələmə, girişə nəzarət, təhlükəsizlik divarları, məlumatların ehtiyat nüsxəsinin çıxarılması və bərpası və təhlükəsizliklə bağlı maarifləndirmə təlimlərinin keçirilməsi və s.-nin tətbiq edilməsi aid edilə bilər.

İnformasiyanın mühafizəsinin əhəmiyyəti istiqamətindən təhlillərindən birində mövcud olan yanaşmaya görə, informasiyanın qorunması yalnız informasiya təhlükəsizliyini təmin etməklə kifayətlənmir, bu proses həmçinin informasiya təhlükəsizliyinə məsul olan subyektin işgüzar nüfuzunu qoruyur və fəaliyyətini daha da təhlükəsiz edir. [16, s.437]

İnformasiya təhlükəsizliyində informasiyanın mühafizəsinin rolunu aşağıdakı kimi ümumiləşdirmək olar:

İnformasiyanın mühafizəsinin təşkili ilə məlumatın qorunması həssas və ya məxfi məlumatın yalnız qanunvericiliklə müəyyən edilən şəxslər kateqoriyasına aid edilən səlahiyyətli istifadəçilər üçün əlçatan olması təmin edilir və bununla da informasiya təhlükəsizliyinə qarşı yarana biləcək təhlükələr və risqlər azalır. Bu, icazəsiz girişin qarşısını alan giriş nəzarəti, şifrələmə və digər təhlükəsizlik tədbirlərindən istifadə etməklə əldə edilir. Əvəllərdə də qeyd edildiyi kimi informasiya mühafizəsinin bu üsulları informasiya təhlükəsizliyi tədbirlərinin bir hissəsini təşkil edir.

İnformasiyanın mühafizəsi məlumatın dəqiq, tam və dəyişdirilməmiş olmasını təmin edir. Bu, məlumatların yoxlanılması, səhvlərin yoxlanılması və məlumatların itirilməməsini və ya zədələnməməsini təmin edən ehtiyat və bərpa mexanizmlərindən istifadə etməklə əldə edilir. Bu da informasiya təhülkəsizliyi elementlərindən olan tamlığın təmin edilməsi üçün zəruri məsələlərdən biridir. İnformasiya təhlükəsizliyində istifadə edilən elemktron imza, təsdiqləmə kimi metodlar informasiya mühafizəsi ilə bağlıdır. Bu da informasiyanın mühafizəsinin üsul və mexanizmlərindən informasiya təhlükəsizliyində geniş istifadə olunduğunu göstərir.

İnformasiyanın mühafizəsi məlumatın səlahiyyətli istifadəçilərə lazım olduqda onların əlçatan olmasını təmin edir. Bu, texniki nasazlıqlar və ya təbii fəlakətlər səbəbindən məlumatın itirilməməsini və ya əlçatmaz olmasını təmin edən lazımsız sistemlərdən, ehtiyat nüsxələrdən və fəlakətin bərpası planlarından istifadə etməklə əldə edilir. Məlumdur ki, əlçatımlılığın təmin edilməsi informasiya təhlükəsizliyinin əsasını təşkil edir.

İnformasiyanın mühafizəsi məlumatın qanuni və normativ tələblərə uyğun idarə olunmasınında əsas təminatçıdır. Bu, qüvvədə olan qanun və normativ sənədlərə uyğunluğu təmin edən təhlükəsizlik siyasətləri, prosedurları və nəzarət mexanizmlərindən istifadə etməklə əldə edilir. Bunun üçün informasiyanın mühafizəsi ilə bağlı təşkilatdaxili sənədlərin hazırlanması zəruri olur. Belə addımların atılması ilə informasiya təhlükəsizliyinə yönələn bir çox hədələrin və hücumların qarşısı müvəffiqiyyətlə alınır. İnformasiyanın mühafizəsi məxfi və ya həssas məlumatların məxfiliyini, bütövlüyünü, mövcudluğunu və uyğunluğunu təmin etməyə kömək edən informasiya təhlükəsizliyinin mühüm komponen-

tidir. Effektiv informasiya təhlükəsizliyinə nail olmaq üçün müvafiq informasiyanın mühafizəsi tədbirlərinin həyata keçirilməsi vacibdir.

İstinadlar:

1. Azərbaycan Respublikasının Konstitusiyası - https://www.e-qanun.az/framework/897, 10.02.2022

2. Azərbaycan Respublikasının Mülki Məcəlləsi, https://www.e-qanun.az/framework/46944, 10.02.2022

3. Azərbaycan Respublikasının İnzibati Xətalar Məcəlləsi- https://www.e-qanun.az/framework/46960, 10.02.2022

4. Avropa İnsan hüquqları Konvensiyası, https://www.echr.coe.int/documents/convention_aze.pdf, 10.02.2022

5. "Dövlət qulluğu haqqında" Azərbaycan Respublikasının Qanunu, https://www.e-qanun.az/framework/4481, 10.02.2022

6. Əliyev Ə.İ., Rzayeva G.A., İbrahimova A.N., Məhərrəmov B.A., Məmmədrzalı Ş.S. İnformasiya hüququ. Dərslik. Bakı: "Nurlar" nəşriyyatı, 2019. 448 səh.

7. "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanunu, https://e-qanun.az/framework/3525ç 10.02.2023

8. "Kibercinayətkarlıq haqqında" Konvensiyanın Təsdiq edilməsi barədə", Azərbaycan Respublikasının Qanunu, https://e-qanun.az/framework/18619, 10.02.2022

9. Ansen, Nils. (2013). The Idea of Legal Responsibility. Oxford Journal of Legal Studies. 34. P. 221-252.

10. Bagchi S. A. Information protection in the age of cyber threats: Challenges and solutions / Bagchi S. A. & S. U. Khan. Journal of Business Research, 70, 2017, p.408-416

11. Dhamija, S., & Vaidya, J. "Protecting Privacy and Promoting Equality in the Digital Age: Challenges and Approaches." In L. Jain, M. Al-Hussein, & M. Misra (Eds.), Digital Governance: Concepts, Systems and Practical Applications, 2020, p. 83-98

12.Katrin Nyman Metcalf. Legal aspects of privacy law and data protection -The right to privacy as a human right and everyday technologies, p. 82-99 https://www.humanrightsestonia.ee/wp/wp-content/uploads/2014/12/ENG-Study-V-part-Legal-aspects-of-privacy-law-and-data-protection.pdf

13. Lin D. D. Effective information protection: A holistic approach. Journal of Information Privacy and Security, 10(3), 2014 p.31-47

14. Shieh M. T. A framework for information protection based on business goals./ M. T. Shieh, H. P. Chen, & C. W. Huang. International Journal of Information Management, 34(4), 2014, p.538-546

15. Smith L, 'Restitution: The Heart of Corrective Justice' (2000–01) 79 Texas L Rev, p.2115–2175

16. Wang K. Information protection and its impact on firm performance: A study of Taiwanese firms. /Wang K. C, Wu M. H., & Kuo T. T. Journal of Business Research, 70, 2017, p.434-441

17. Yeung K., and Bygrave L. A., Demystifying the modernized European data protectionregime: Cross-disciplinary insights from legaland regulatory governance scholarship. Regulation & Governance 16, 2022, p.137–155

ENSURING INFORMATION SECURITY: INFORMATION PROTECTION AND INFORMATION RESPONSIBILITY

Aytekin Ibrahimova*

Abstract

The institution of legal responsibility is studied as one of the important mechanisms in most legal fields. It is legal responsibility that plays a key role in the regulation of social relations. If we look at the legislative acts regulating various fields, we can determine that in those normative sources it is determined that its violation will lead to legal responsibility. In addition to ensuring justice, which is the general principle of this right, it is distinguished by its preventive effect on individuals in society. Established legal liability deters a person from committing such illegal acts.

It is known that information security is considered a broader category and includes many different subcategories. As a result of information security analysis, it becomes clear that information protection is just one of the means of ensuring information security. Information security is a broader concept in relation to information protection and includes the latter. The close connection of ensuring the protection of important elements of information security with the protection of information makes the protection of information the main priority issue for all subjects in the modern era. Information security is evaluated as a fact that was confirmed after the development of information technologies, which is not only related to the protection of devices. Failure to ensure the protection of the information currently operated on causes many problems.

Keywords: *information security, information law violation, legal responsibility, types of responsibility, information protection.*

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ЗАЩИТА ИНФОРМАЦИИ И ИНФОРМАЦИОННАЯ ОТВЕТСТВЕННОСТЬ

Айтекин Ибрагимова**

Резюме

Институт юридической ответственности исследуется как один из важных механизмов в большинстве правовых областей. Именно юридическая ответственность играет ключевую роль в регулировании общественных отношений. Если посмотреть на законодательные акты, регулирующие различные сферы, то можно определить, что в этих нормативных источниках определено, что его нарушение влечет за собой юридическую ответственность. Помимо обеспечения справедливости, что является общим принципом этого права, его отличает превентивное воздействие на индивидуумов в обществе. Установленная юридическая ответственность удерживает лицо от совершения таких противоправных действий.

Известно, что информационная безопасность считается более широкой категорией и включает множество различных подкатегорий. В результате анализа информационной безопасности становится ясно, что защита информации является лишь одним из средств обеспечения информационной безопасности. Информационная безопасность является более широким понятием по отношению к защите информации и включает

* Ph.D., Associate Professor of the Constitutional Law Department of Baku State University

** Д.ф.п.п., доцент кафедры конституционного права Бакинского государственного университета

последнюю. Тесная связь обеспечения защиты важных элементов информационной безопасности с защитой информации делает защиту информации главным приоритетным вопросом для всех субъектов в современную эпоху. Информационная безопасность оценивается как факт, подтвердившийся после развития информационных технологий, что связано не только с защитой устройств. Необеспечение защиты информации, с которой в настоящее время оперируют, вызывает множество проблем.

Ключевые слова*: информационная безопасность, нарушение информационного права, правовая ответственность, виды ответственности, защита информации.*