AZƏRBAYCAN RESPUBLİKASI

Əlyazması hüququnda

İNFORMASİYA TƏHLÜKƏSİZLİYİNİN BEYNƏLXALQ VƏ DÖVLƏTDAXİLİ HÜQUQİ MÜDAFİƏ MEXANİZMLƏRİ

İxtisas: 5614.01 – "İnzibati hüquq; maliyyə hüququ; informasiya hüququ"
Elm sahəsi: Hüquq

İddiaçı: **Aytəkin Nazim qızı İbrahimova**

Elmlər doktoru elmi dərəcəsi
almaq üçün təqdim edilmiş dissertasiyanın

A V T O R E F E R A T I

Bakı – 2024

Dissertasiya Bakı Dövlət Universitetinin Hüquq fakültəsinin İnsan hüquqları və informasiya hüququ UNESCO kafedrasında yerinə yetirilmişdir.

Elmi məsləhətçilər: hüquq elmləri doktoru, professor
Əmir İbrahim oğlu Əliyev
hüquq elmləri doktoru, professor
Oleq Volodimiroviç Zayçuk

Rəsmi opponentlər: hüquq elmləri doktoru, professor
Anatolii Trofimoviç Komziuk
hüquq elmləri doktoru, dosent
Yuriy Pavloviç Burilo
hüquq elmləri doktoru, professor
Petro Vasiloviç Dixtievskiy
hüquq elmləri doktoru, professor
Xristofor Petroviç Yarmaki

Azərbaycan Respublikası Prezidenti yanında Ali Attestasiya Komissiyasının 27 oktyabr 2023-cü il tarixli 3-50/3-1-1-235/2023 saylı əmri əsasında Bakı Dövlət Universiteti nəzdində fəaliyyət göstərən BED 2.44 Birdəfəlik Dissertasiya Şurası

Dissertasiya şurasının sədri: hüquq elmləri doktoru, dosent
Turqay İmamqulu oğlu Hüseynov

Dissertasiya şurasının elmi katibi: hüquq üzrə fəlsəfə doktoru, dosent
Əlizadə Qurbanəli oğlu Məmmədov

Elmi seminarın sədri: hüquq elmləri doktoru, dosent
Ramil Mahir oğlu Aslanov

BAKI DÖVLƏT UNİVERSİTETİ
ELMİ KATİB
İmzanı təsdiq edirəm
"26" 01 2024

DİSSERTASİYANIN ÜMUMİ SƏCİYYƏSİ

Mövzunun aktuallığı və işlənmə dərəcəsi. İnformasiya anlayışı olduqca genişdir, fərqli mənalarda işlədilir və fəaliyyət dairələri də müxtəlifdir. Bundan başqa, informasiya anlayışının istifadə olunmadığı fəaliyyət sahəsi də demək olar ki yoxdur. Bu isə problemə hərtərəfli və müxtəlif elm sahələrinin sıx qarşılıqlı əlaqəsində baxılmasını zəruri edir. Belə istiqamətlərdən biri də informasiya, o cümlədən informasiya ilə bağlı müxtəlif sahələrin, o cümlədən informasiya təhlükəsizliyi ilə əlaqədar məsələlərin hüquqi tənzimlənməsidir.

İnformasiya, o cümlədən informasiya təhlükəsizliyindən danışarkən, təhlükəsizlik anlayışına xüsusi diqqət yetirilməlidir. "Təhlükəsizlik" termini təhlükənin obyektindən asılı olaraq "milli təhlükəsizlik", "beynəlxalq təhlükəsizlik", "insan təhlükəsizliyi", "qlobal təhlükəsizlik" və s. kimi kateqoriyalarla təzahür etməkdədir[1]. Ümumiyyətlə, "təhlükəsizlik" anlayışı həm də xüsusi termin hesab edilir. Ümumqəbul edilmiş mənada təhlükəsizlik bütün hallarda müvafiq sferalarda müdafiə mexanizmlərinin formalaşmasını tələb edir. Belə ki, müdafiə sistemləri olmadan təhlükəsizliyi təmin etmək mümkün deyildir. İnformasiya təhlükəsizliyi dedikdə isə, bütövlükdə cəmiyyətin maraqlarını nəzərə alaraq informasiya mühitinin qorunması, bu mühitə qarşı təhlükələrin müəyyən edilməsi və müvafiq surətdə onların qarşısının alınması vəziyyəti anlaşılmalıdır. Hüquq ədəbiyyatında qeyd edilir ki, informasiya təhlükəsizliyi günü-gündən daha çox əhəmiyyət qazanan və bütün dünyada müxtəlif kateqoriya subyektlər üçün əsas müzakirə mövzularından olan olduqca aktual məsələdir[2]. İnformasiya təhlükəziliyinin hüquqi tənzimlənməsinin aktuallığını əsaslandıran daha bir tədqiqatda qeyd olunur ki, elektron kommunikasiya vasitələrinin inkişafı və geniş istifadəsi, habelə, internetdən demək olar ki bütün sahələrdə istifadə

---

[1] Əliyev Ə.İ. İnsan hüquqları. Dərslik. Bakı, 2019, s.180

[2] Soomro, T. R. Information security management: A case study of an information security culture./ Soomro, T. R., Shah, M. H., & Ahmed, J- Information Management & Computer Security 24(1),2016, s.86-102

olunması və istifadənin geniş yayılması informasiya təhlükəsizliyi tədbirlərinə hərzamankından daha çox ehtiyac olduğunu göstərməklə, istər dövlət, istər özəl, istərsə də fiziki şəxslərin fəaliyyətində informasiyanın mühafizəsinin təmin edilməsini, habelə informasiyanın qanunsuz olaraq ələ keçirilməsindən, fırıldaqçılıq və dələduzluq məqsədləri üçün istifadə edilməsindən, digər təhlükəsizlik pozuntularından qorunmasını təmin etmək günün ən aktual müzakirə mövzularından biridir[3]. Mövcud yanaşmalarından birinə görə isə, informasiya təhlükəsizliyi texnologiyanın sürətli inkişafı və kiberhücumların getdikcə təkmilləşməsi səbəbindən diqqət və yeniləmə tələb edən, o cümlədən daim inkişaf edən sahə kimi nəzərdən keçirilir[4], digərində isə ona rəqəmsal cəmiyyət üçün əsas çağırış kimi yanaşılır[5]. Qeyd olunanlar isə informasiya təhülkəsizliyi və onun hüquqi tənzimlənməsinin aktuallığını bir daha təsdiq edir.

İnformasiya cəmiyyətində dövlət təhlükəsizliyinin əsas göstəricisi onun informasiya təhlükəsizliyindən asılıdır. İnformasiya təhlükəsizliyi digər dövlət təhlükəsizliyinə nisbətən daim artan istiqamətdə inkişaf edir və üstünlük təşkil edən təhlükəsizlik obyektinə çevrilir. Onu da qeyd etmək olar ki, dövlətlərdə informasiya təhlükəsizliyinin formalaşması nəinki cəmiyyətin informasiya ehtiyaclarının təmin olunması üçün mühüm vasitə oldu, eyni zamanda daha təhlükəsiz təmin olunmaqla həyata keçirilməsinə də şərait yaratdı.

Əvvəllər informasiya təhlükəsizliyi fərdi şəkildə ya insanların özləri tərəfindən, ya da dövlət tərəfindən kağız daşıyıcılarda mühafizə edilirdisə, indi isə dövlət və cəmiyyət birlikdə bu problemlərin öhdəsindən gəlməyə çalışır, xüsusilə də elektron daşıyıcada dövr edən məlumatların müdafiəsi təşkil edilir. Bu zaman

[3] Mishra, D., Mishra.S.K. Information security management in organizations: A review of literature./ Journal of Global Information Management 24(4), 2016, s. 36-37

[4] Kumar, R. Emerging trends and challenges in information security management./ Kumar, R., & Shukla, A. K. - Journal of Advances in Management Research 15(1), 2018, s.5-17

[5] Siau, K. Research on information security in organizations: A review of the literature./ Siau, K., Nah, F. F., & Tian, Y. - Information & Management 53(6), 2016, s.804-819

təhlükəsizlik məsələsini həll etməkdə istər beynəlxalq-hüquqi çərçivədə, istərsə də milli-hüquqi çərçivədə dövlətlər öz üzərlərinə müvafiq vəzifələr götürür. Müasir dövlətlərin hər birinin miili qanunvericlik aktlarında informasiya təhlükəsizliyi öz əksini tapmışdır. İnformasiya təhlükəsizliyinin konstutision səviyyədə əks olunmasının ən birinci səbəbi isə dövlətlərin buna verdiyi əhəmiyyətlə əlaqədardır.

Azərbaycan Respublikası (AR) müstəqillik əldə etdikdən sonra bütün sahələrdə olduğu kimi, informasiya sahəsində də bir çox köklü islahatlar həyata keçirməyə başladı: informasiya təhlükəsizliyi dövlətimizin fəaliyyətinin əsasını təşkil etdi və bu sahədə qanunvericilik təkmilləşdirildi. 2009-cu il tarixdə AR Konstitusiyasının 32-ci maddəsinə edilmiş əlavə və dəyişikliklər isə bir daha onu sübut etdi ki, dövlətin əsasını təşkil edən əsas amillərdən biri də məhz informasiya təhlükəsizliyinin təmin edilməsidir. Təbii ki, informasiya təhlükəsizliyinin bütün aspektlərini konstitusiyada tapmaq mümkün deyildir, bunlar milli qanunvericlik səviyyəsində daha da inkişaf etdirilmişdir. Lakin ayrı-ayrı normativ hüquqi aktlar ilə tənzimlənən informasiya təhlükəsizliyi bütövlükdə konstitusion prinsiplərə əsaslanmalıdır.

Yuxarıda qeyd edilənlər dissertasiya işinin aktuallığını bir daha təsdiq edir. Bundan başqa, kifayət qədər beynəlxalq müqavilələrin iştirakçısı olan AR tərəfindən bu istiqamətdə bir sıra dövlətdaxili normativ-hüquqi aktlar qəbul edilmişdir. Məsələn, "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında", "Fərdi məlumatlar haqqında" və s. qanunlar qəbul edilərək, nəzərdən keçirilən və yeni yaranan informasiya mühiti, o cümlədən informasiya təhlükəsizliyi məsələləri də ətraflı tənzim edilmişdir. Bununla yanaşı, dünya praktikası göstərir ki, informasiya təhlükəsizliyi üçün hərtərəfli bir hüquq sisteminin formalaşdırılması prosesini başa çatmış hesab etmək olmaz, belə ki, burada beynəlxalq və mili hüquq normalarının uzlaşdırılması prosesi hələ kifayət qədər əhatəli bir mürəkkəb mərhələnin tərkib hissəsidir.

Hazırda AR-də informasiya cəmiyyətinin formalaşması prosesində insan hüquq və azadlıqlarını təmin etmək də dövlətin əsas vəzifələrindəndir. AR Konstitusiyasının 12-ci maddəsinin tələbləri

bu cəhətdən xüsusi qeyd edilməlidir. Əgər həmin maddənin 1-ci hissəsi bütövlükdə insan hüquq və azadlıqlarının təmin edilməsini dövlətin ali məqsədi kimi xarakterizə edirsə, 2-ci hissə isə bu sahədə beynəlxalq müqavilələrin xüsusi rolunu qeyd edir. Qeyd edilənlər isə AR Konstitusiyasının 71, 148-2 və 151-ci maddələri ilə bir daha möhkəmlənmiş və daha da inkişaf etdirilmişdir.

Bugünədək informasiya təhlükəsizliyinin beynəlxalq-hüquqi tənzimlənməsinin ayrı-ayrı aspektləri üzrə tədqiqatlar aparılsa da, bu məsələ ayrıca tədqiqat mövzusu kimi işlənilməmişdir. Müdafiəyə təqdim edilən dissertasiya informasiya təhlükəsizliyinin beynəlxalq və dövlətdaxili hüquqi müdafiə mexanizmləri aspektlərini tədqiq edən ilk elmi əsərdir. Ona qədər isə bu məsələyə müxtəlif aspektlərdən yanaşılmış və informasiya təhlükəsizliyi daha çox informasiya hüququ çərçivəsində tədqiq edilmişdir. Bu tədqiqatda isə problemə tamamilə başqa bir istiqamətdən, müasir yeni tendensiyalar və beynəlxalq hüquq da daxil olmaqla məhz insan hüquqları və beynəlxalq təhlükəsizlik kontekstindən yanaşılmışdır. Bu baxımdan hazırkı tədqiqat işi informasiya təhlükəsizliyinin ümumi və xüsusi inkişaf tendensiyalarının öyrənilməsinə həsr olunmuş ilk tədqiqat işidir. Tədqiqat işi çərçivəsində ilk dəfə olaraq, informasiya təhlükəsizliyi ilə əlaqəli ictimai münasibətlərin hüquqi tənzimlənməsində mövcud tendensiyalar müəyyən edən beynəlxalq hüquq normaları və müxtəlif dövlətlərin, o cümlədən AR-in mili qanunvericilik təcrübəsi müqayisəli təhlil edilmiş; AR-də informasiya təhlükəsizliyinin təmini institutunun və baza elementlərinin formalaşması üçün ilkin istiqamətlər müəyyənləşdirilmiş; informasiya təhlükəsizliyinin məqsədi və əsas xüsusiyyətlərinin nəzəri və praktiki hüquqi məzmunları aydınlaşdırılmış; doktrinal səviyyədə informasiya təhlükəsizliyi ilə əlaqədar bütün məsələlər geniş nəzərdən keçirilmiş; bu sahədə bir sıra mühüm boşluqlar və kolliziyalar aşkar edilmiş; həmin sfera üzrə bir sıra təkmilləşdirici təkliflər və tövsiyələr işlənib hazırlanmışdır.

Dissertasiyada mövzu ilə bağlı tədqiqatlar aparmış yerli və xarici müəlliflərin elmi əsərlərinin təhlili aparılmışdır. Bu sırada

N.H.Kuran (Türkiye İçin E-devlet Modeli)[6], B.Yıldız (Bilgi Güvenliği ve E-Devlet Kapsamında Kamu Kurumlarında Bilgi Güvenliği Yönetimi Standartlarının Uygulanması)[7], J.E.Fountain (Building the Virtual State: Information Technology and Institutional Change),[8] R.Heeks (Implementing and Managing e-Government: An International Text)[9], T.Olufohunsi (Data Encryption)[10], S.Raghavan (Information Security and Privacy: A Practical Guide for Global Executives, Lawyers, and Technologists)[11] və b. qeyd edə bilərik.

Milli hüquq ədəbiyyatında informasiya təhlükəsizliyinin milli və beynəlxalq tənzimlənməsi tədqiqat predmeti olmamışdır. Belə ki, bu sahədə bir sıra xüsusi tədqiqatlar aparılsa da, həmin tədqiqatlarla milli qanunvericiliyin yaxın elmlər və hüquq sahələri kontekstindən izah edilməsinə çalışılmışdır. Yalnız dərslik və tədris vəsaitləri səviyyəsində - R.M.Aslanov (İnformasiya cəmiyyətində demokratiyanın inkişaf istiqamətləri: rəqəmsal demokratiya[12]; İnformasiya hüququnun əsasları və aktual problemləri[13]), Ə.İ.Əliyev, G.A.Rzayeva, A.N.İbrahimova, B.A.Məhərrəmov, Ş.S.Məmmədrzalı (İnformasiya hüququ)[14], M.N.Əlizadə, H.M.Bayramov, Ə.S.Məmmədov (İnformasiya təhlükəsizliyi)[15], R.F.Əzizov (İnternet

---

[6] Kuran N.H. Türkiye İçin E-devlet Modeli. İstanbul: İstanbul Bilgi Üniversitesi Yayınları, - 2005.

[7] Yıldız.B. Bilgi Güvenliği ve E-Devlet Kapsamında Kamu Kurumlarında Bilgi Güvenliği Yönetimi Standartlarının Uygulanması/Yüksek Lisans Tezi/- 2007

[8] Fountain, J. E. Building the Virtual State: Information Technology and Institutional Change./ Brookings Institution Press/-2001

[9] Heeks, R. Implementing and Managing e-Government: An International Text./ Sage Publications/- 2006

[10] Olufohunsi, T. Data Encryption./ University of Salford/- 2019

[11] Raghavan, S. Information Security and Privacy: A Practical Guide for Global Executives, Lawyers, and Technologists/ Cambridge University Press/- 2018

[12] Aslanov R.M. İnformasiya cəmiyyətində demokratiyanın inkişaf istiqamətləri: rəqəmsal demokratiya/ Monoqrafiya/ -Bakı, - 2022

[13] Aslanov R.M. İnformasiya hüququnun əsasları və aktual problemləri/ Dərslik/- Bakı, - 2019

[14] Əliyev Ə.İ., İnformasiya hüququ. Dərslik. / Rzayeva G.A., İbrahimova A.N., Məhərrəmov B.A., Məmmədrzalı Ş.S/. -Bakı: Nurlar nəşriyyatı,- 2019

[15] Əlizadə M.N. İnformasiya təhlükəsizliyi. Dərslik. / Bayramov H.M., Məmmədov Ə.S/. -Bakı, İqtisad Universiteti nəşriyyatı, - 2016

şəbəkəsində tənzimləmənin müqayisəli hüquqi təhlili)[16] və elmi məqalələr (G.A.Rzayeva, Z.Q.Cəbrayılova, R.M.Əliquliyev, B.S.Ağayev və b.) səviyyəsində informasiya təhlükəsizliyinin ayrı-ayrı məsələlərinə toxunulmuşdur. Azərbaycan hüquq doktrinasında informasiya hüquq münasibətlərinə aid dissertasiya səviyyəsində yalnız bir tədqiqat işi aparılmışdır. Belə ki, R.M.Aslanovun "Azərbaycan Respublikası və Rusiya Federasiyasında informasiya cəmiyyəti quruculuğunda informasiya təhlükəsizliyinin hüquqi təminatının nəzəri və konstitusiya əsasları"[17] adlı dissertasiya informasiya hüquq münasibətlərinin yalnız bir aspektinə həsr edilmişdir. Bundan başqa, Azərbaycan hüquq ədəbiyyatında son vaxtlar müdafiə edilən bir dissertasiyada isə yalnız informasiya hüquq pozuntuları və informasiya-hüquqi məsuliyyətin nəzəri və təcrübi aspektləri təhlil edilmişdir[18].

Daha sonra, informasiya hüquq münasibətlərinin tənzimlənməsinin ayrı-ayrı aspektləri dərslik, dərs vəsaiti və elmi məqalələr səviyyəsində xarici müəlliflər: İ.L.Baçilo, V.A.Kopılov, V.N.Lopatin, V.A.Pojilıx, M.M.Rassolov, A.A.Fatyanov, M.A.Fedotov, A.Pazyuk, M.Sokolova, V.D.Elkin, V.M.Baranova, M.Başlıkova, E.Brodskiy, M.Y.Yemelyannikova, K.A.Zanina, N.G.Belqorodtseva, İ.A.Velder, A.V.Dvoretskiy, A.V.Kuçerenko, N.İ.Petrıkin, O.B.Prosvetova, Y.S.Telina, A.S.Fedosin, R.Uolters, S.D.Uorren, L.D.Brendays, M.Lend, A.F.Uestin, D.A.Solove, J.Uitman, D.M.Visente, L.Feyiler, E.Brauer, M.Zalnirut, P.Fişer, C.Kuner, C.Hoffman, A.C.Evans, M.Ouen, S.Qutvirt, F.Biqnami, M.Medina, M.Bakhoum, D.Kamarinou, J.Drexl, J.Dumas, J.Hölzel, B.Valtisson, J.F.Albrext, J.Stoddart, A.L.Gardner, P.Van den Bulk,

[16] Əzizov R.F. "İnternet" şəbəkəsində tənzimləmənin müqayisəli hüquqi təhlili./ - Bakı: Elm. - 2017

[17] Aslanov R.M. Azərbaycan Respublikası və Rusiya Federasiyasında informasiya cəmiyyəti quruculuğunda informasiya təhlükəsizliyinin hüquqi təminatının nəzəri və konstitusiya əsasları:/ Hüquq üzrə elmlər doktoru elmi dərəcəsi almaq üçün dissertasiya işi/-Bakı, - 2016

[18] Əlizadə H.O. İnformasiya hüquq pozuntuları və informasiya-hüquqi məsuliyyət: nəzəri və təcrübi aspektlər. Hüquq üzrə fəlsəfə doktoru elmi dərəcəsi almaq üçün təqdim edilmiş dissertasiyanın avtoreferatı. Bakı, - 2023.

E.A.Salami, F.Boexm, D.Grey, N.Terri, M.J.Blanke, L.Sotto, S.Hodjes, M.U.Brennan, C.L.Reyers və b. tərəfindən tədqiq edilmişdir. Dissertasiyada qeyd olunan tədqiqatlardan elmi-nəzəri baza olaraq geniş istifadə edilmişdir.

Tədqiqatın obyektini və predmeti. Tədqiqatın obyektini dövlətin informasiya təhlükəsizliyi və onun kompleks tədqiqi təşkil edir. Tədqiqatın predmeti dövlətin informasiya təhlükəsizliyi, informasiya təhlükəsizliyinin hüquqi əsasları, informasiya hüquqlarının müəyyən edilməsi və təminatları ilə bağlı məsələlər və bu məsələlərin tədqiq olunmasında istifadə olunan beynəlxalq sənədlər, qanuvericilik aktları, qəbul edilən dövlət proqramları və məhkəmə təcrübələri təşkil edir.

Tədqiqatın məqsəd və vəzifələri. Tədqiqatın məqsədini dövlətin informasiya təhlükəsizliyinin kompleks təhlilini aparmaq, informasiya təhlükəsizliyinin beynəlxalq və dövlətdaxili hüquqi müdafiə mexanizmlərini təhlil etmək, informasiya təhlükəsizliyinin özünəməxsus cəhətlərini və mahiyyətini araşdırmaq, AR timsalında dövlətin bütövlükdə informasiya təhlükəsizliyinin təhlilini aparmaq və dövlətin təhlükəsizliyinin təmin edilməsi içərisində informasiya təhlükəsizliyinin yeri və əhəmiyyətini tam şəkildə əsaslandırmaqdan ibarətdir.

Qeyd edilən məqsədə nail olmaq üçün tədqiqatda aşağıdakı ***vəzifələr*** müəyyən edilmişdir:

- İnformasiya təhlükəsizliyinin mahiyyətini, əsas xüsusiyyətlərini və tərkib elementlərini təhlil etmək, onun beynəlxalq və milli təhlükəsizlik sistemində yerini müəyyənləşdirmək;
- İnformasiya təhlükəsizliyinin əsas istiqamət və aspektlərini, o cümlədən informasiya təhlükəsizliyinin standartlarını nəzərdən keçirmək;
- Dövlətin informasiya təhlükəsizliyi siyasətinin əsas hədəflərini nəzərdən keçirmək, AR-in təhlükəsizliyi sistemində informasiya təhlükəsizliyinin yerini müəyyən etmək;
- İnformasiya təhlükəsizliyinin informasiya sahəsində hüquqların təmin olunmasında əhəmiyyətini müəyyən etmək;
- Elektron dövlətin informasiya hüquqlarının təminat sistemi kimi əsas xüsusiyyətlərini nəzərdən keçirmək;

- AR-də elektron dövlət üçün normativ-hüquqi bazanın yaradılması xüsusiyyətlərini araşdırmaq;

- İnsan hüquqları konteksində informasiya hüquqlarını dövlətin əsas prioriteti kimi nəzərdən keçirmək;

- Fərdi və biometrik məlumatların informasiya təhlükəsizliyinin təmin olunmasında rolunu təhlil etmək;

- Sosial şəbəkələr və informasiya təhlükəsizliyi məsələlərini geniş təhlil etmək;

- İnformasiya təhlükəsizliyi və hüquqi məsuliyyət məsələlərini qarşılıqlı nəzərdən keçirmək;

- İnformasiya təhlükəsizliyi mədəniyyətinin informasiya təhlükəsizliyinin təmin olunmasında rolunu araşdırmaq;

- İnformasiya təhlükəsizliyinin beynəlxalq və dövlətdaxili hüquqi müdafiə mexanizmlərinin qarşılıqlı əlaqəsini vahid vəhdətdə müəyyənləşdirmək və hər birinin ayrılıqda inkişaf tendensiyalarını müəyyən etmək;

- İnformasiya təhlükəsizliyinin təmin olunması üzrə AR-in beynəlxalq öhdəliklərini müəyyən etmək, bu sahədə beynəlxalq və milli mexanizmləri müəyyənləşdirmək;

- İnformasiya təhlükəsizliyi sahəsində AR-in öhdəliklərinin tam yerinə yetirilməsi sahəsində ortaya çıxan çətinliklərin aradan qaldırılması üzrə mühüm təkliflər vermək;

- İnformasiya sahəsində beynəlxalq hüquq normalarının AR-in milli qanunvericiliyinə implementasiyası məsələlərini təhlil etmək;

- Beynəlxalq universal və regional təşkilatlarda informasiya təhlükəsizliyi sahəsində əməkdaşlıq, gələcəkdə bu əməkdaşlığın daha da gücləndirilməsi istiqamətində qarşıya qoyulan vəzifələri müəyyən etmək;

- İnkişaf etmiş dövlətlərin informasiya təhlükəsizliyi sahəsində təcrübəsini nəzərə alaraq AR-də informasiya təhlükəsizliyinin təmini üzrə milli qanunvericiliyin məcəllələşdirilməsini həyata keçirmək üzrə təkliflərlə çıxış etmək.

Tədqiqat metodları. Dissertasiyanın yazılması prosesində həm ümumelmi (formal məntiqi, sistemli-struktur təhlil, tarixi yanaşma, elmi və praktik materialların ümumiləşdirilməsi), həm də xüsusi elmi metodlardan (müqayisəli hüquqşünaslıq, məntiqilik, statistik təhlil,

monitorinq və s.) istifadə edilmişdir. Belə ki, informasiya təhlükəsizliyini özündə ehtiva edən bır sıra dövlətlərin qanunvericiliyinin müqayisəli təhlili aparılmış, inkişaf etmiş dövlətlərin qanunvericiliyində əks olunan nümunəvi normaların milli qanunvericiliyə və praktikaya tətbiqi ilə bağlı təkliflər irəli sürülmüşdür. Bundan başqa müxtəlif dövrlərdə ayrı-ayrı dövlətlərin hüquqşünaslarının dövlətin informasiya təhlükəsizliyi ilə bağlı fikirləri və gəldikləri nəticələr ətraflı araşdırılmış, müxtəlif məhkəmə işləri tədqiq olunmuş, məhkəmələrin təcrübi materiallarının ümumiləşdirilməsində isə sosial və məhkəmə statistik tədqiqat üsullarından da istifadə edilmişdir.

Müdafiəyə çıxarılan əsas müddəalar. Tədqiqatın elmi yeniliyini özündə ifadə edən aşağıdakı yeni **elmi müddəalar** müdafiəyə təqdim olunur:

1. İnformasiya təhlükəsizliyi ilə əlaqədar məsələlərin təhlili zamanı onun beynəlxalq və milli təhlükəsizlik sistemində qarşılıqlı əlaqədə əsas xüsusiyyətləri nəzərdən keçirilməli, nəhayət informasiya təhlükəsizliyinin beynəlxalq və dövlətdaxili normativ-hüquqi sistem üçün mühüm əhəmiyyəti əsaslandırılmalıdır. Bu zaman, informasiya təhlükəsizliyinin təmin edilməsində informasiya anlayışının əsas elementləri, o cümlədən informasiya təhlükəsizliyinin mühüm aspektləri və təhlükəsizliyə təsir edən mühüm faktorlar, məsələn gizlilik, tamlıq, əl çatanlıq, hesabatlılıq və s. qarşılıqlı əlaqədə qeyd edilməli, daha sonra gələcəkdə ortaya çıxacaq digər faktorların da rolu əsaslandırılmalıdır.

2. İnformasiya təhlükəsizliyinin aşkar edilməsi və qarşısının alınmasında mühüm faktorlardan biri də hüquq yaradıcılığı və hüquq normalarının səmərəli tətbiqidir. Beynəlxalq hüquq yaradıcılığı üçün isə inkişaf etmiş dövlətlər praktikasının əsas götürülməsi mühüm istiqamət olmalıdır. Bundan başqa, hüquqi məsuliyyət informasiya təhlükəsizliyinin təmin olmasında preventiv tədbir kimi, o cümlədən informasiyanın mühafizəsinin informasiya təhükəsizliyinin təmin olunması vasitəsi kimi əsas xüsusiyyətləri qeyd edilməli və bir sıra elmi-nəzəri-praktiki tövsiyələr bununla əsaslandırılmalıdır.

3. İnformasiya təhlükəsizliyi mədəniyyətinin informasiya təhlükəsizliyinin təmin olunmasında rolu tam şəkildə

əsaslandırılmaqla bir sıra vacib istiqamətlər də müəyyən edilməlidir. Belə bir fikir əsaslı olaraq qeyd edilməlidir ki, informasiya təhlükəsizliyinin yalnız dövlətdaxili və beynəlxalq hüquqi müdafiə mexanizmlərinin vahid əlaqəli sistemində mühüm müsbət nəticələr əldə edilməsi mümkündür.

4. İnformasiya təhlükəsizliyinin beynəlxalq hüquqi müdafiə mexanizmləri beynəlxalq normativ-hüquqi əsaslar və beynəlxalq təşkilati mexanizmlər nöqteyi-nəzərindən və informasiya münasibətlərinin beynəlxalq-hüquqi tənzimlənməsi sistemi kimi nəzərdən keçirilməlidir. Bundan başqa, informasiya təhlükəsizliyinin təmin olunmasında dövlətlərin əməkdaşlığı konsepsiyası əsaslandırılmaqla qeyd edilməlidir ki, bu sahədə dövlətlərin əməkdaşlığı nəinki onların hüququ, eyni zamanda vəzifəsidir. İnformasiya təhlükəsizliyi insan hüquqları ilə birbaşa bağlıdır, beləliklə də insan hüquqları amilini və onun dövlətlərin və beynəlxalq cəmiyyətin əsas məqsədlərindən biri olduğunu nəzərə alaraq informasiya təhlükəsizliyinə qlobal problem kimi yanaşılmalı və bu istiqamətdə ciddi beynəlxalq tədbirlər həyata keçirilməlidir.

5. İnformasiya təhlükəsizliyi ona iki istiqamətdən yanaşılmanı zəruri edir: beynəlxalq təhlükəsizliyin tərkib hissəsi olaraq və beynəlxalq hüquqla tənzim edilməli olan beynəlxalq informasiya təhlükəsizliyi; milli təhlükəsizliyin tərkib hissəsi olaraq və beynəlxalq hüququn primatlığı qəbul edilməklə milli hüquqla tənzim edilməli olan milli informasiya təhlükəsizliyi.

6. İnformasiya hüquq münasibətlərinin müasir dövrdə sürətli inkişafı informasiya cəmiyyətində təhlükəsizliyin təmin edilməsi məsələsinin əsas elmi müzakirələrin mərkəzində yer almasına səbəb olmuşdur. Bununla bərabər, informasiya texnologiyalarının sürətli inkişafı yeni təhlükələrin meydana gəlməsi üçün də əsas olur. Buna görə də, davamlı olaraq informasiya texnologiyalarının inkişaf tendensiyasının dövlət tərəfindən izlənilməsi təmin edilməlidir. O cümlədən müvafiq sahədə elmi tədqiqatların, risklərin müəyyən edilməsi istiqamətində təhlil və araşdırmaların aparılmasında təşviqedici tədbirlər görülməli, müasir dövrün tələblərinə uyğun gələn nəzəriyyələrin hazırlanmasına dəstək göstərilməlidir.

7. İnformasiya texnologiyalarının bütün sferalarda geniş tətbiqi və rəqəmsal sistemlərdən geniş istifadə edilməsi beynəlxalq təhlükəsizliyə yeni yanaşma göstərilməsini zəruri edir. Çünki artıq müxtəlif səviyyəli terror aktları rəqəmsal mühitdə və ya informasiya texnologiya vasitələrindən istifadə edilməsi ilə törədilir. Bu isə beynəlxalq və milli səviyyədə təhlükəsizliyin təmin edilməsi prosesində informasiya təhlükəsizliyinin hüquqi mexanizmlərinin formalaşdırılması və müəyyən edilməsini gündəmə gətirir. Hazırda isə terrorizm cinayətinin dairəsinə aid edilən əməlləri müəyyən edən beynəlxalq və milli qanunvericilikdə kiberterror aktları ilə bağlı tənzimlənmə aparılmalıdır. Bu sahədə beynəlxalq-hüquqi tənzimetmənin əsasını təşkil edən beynəlxalq müqavilələrdə müvafiq dəyişikliklər aparılmalı, informasiya cəmiyyətində törədilən terror xarakterli ictimai təhlükəli əməllərin dairəsi və törədilməsinə görə məsuliyyət müəyyən edilməlidir.

8. İnformasiya təhlükəsizliyinə dair hüquq münasibətlərində iştirakçıların hüquq və vəzifələrinin müəyyən edilməsi və iştirakçıların öz öhdəliklərini lazımi qaydada icra etməsi informasiya təhlükəsizliyinin əsasını təşkil edir. Bu istiqamətdə beynəlxalq səviyyədə aktlarda və milli qanunvericilikdə informasiya hüquq münasibətlərində informasiya təhlükəsizliyinin təmin edilməsi ilə bağlı məsələlərdə subyektlərin dairəsi, həmin subyektlərin hüquq və vəzifələri müəyyən edilməlidir. Əsasən də, subyektlərin öhdəliklərinin dairəsinin dəqiq müəyyən edilməsi informasiya təhlükəsizliyi risklərinin minimuma endirilməsi üçün məqsədəmüvafiq hesab edilməlidir.

9. İnformasiya təhlükəsizliyinin təmin edilməsinin yalnız informasiya ehtiyatları və ya sistemlərinin təhlükəsizliyinə məsul subyektlərin fəaliyyəti (fəaliyyətsizliyi) ilə əlaqədar olmadığı hamıya bəlli olan haldır. Belə ki, informasiya ehtiyatı və ya sisteminin istifadəçisinin ani səhlənkarlığı və ehtiyatsızlığı həmin istifadəçiyə münasibətdə informasiyanın mühafizəsinin təmin edilməsini mümkünsüz edir. Belə olan halda ictimai savadlılığın artırılması istiqamətində tədbirlər görülməlidir. Belə tədbirlərin görülməsinin isə dövlətin əsas vəzifələrindən biri kimi müəyyən edilməsi məqsədəuyğun olardı. Odur ki, informasiya təhlükəsizliyi barədə

maarifləndirmə və savadlılığın artırılması istiqamətində müvafiq ardıcıl tədbirlər görülməli, maarifləndirici, habelə informasiya təhlükəsizliyi tədbirlərinin gücləndirilməsi barədə təşviqedici materiallar hazırlanmalı, həmin materialların əlçatanlılığı təmin edilməlidir. Bu istiqamətdə maarifləndirmə və savadlılığın artırılması tədbirlərinin müxtəlif təhsil səviyyələrində proqramlara daxil edilməsi də zəruri tədbirlərdən biri kimi qəbul edilməlidir.

10. İnformasiya cəmiyyətinə xas olan xüsusiyyətərdən biri ondan ibarətdir ki, burada sərhədlər mövcud deyildir. Belə ki, qeyd etmək olar ki, kiberməkan sərhədsizdir və burada konkret dövlətin yurisdiksiyasını müəyyən etmək çətin məsələlərdən biridir. İnformasiya təhlükəsizliyinin əhəmiyyətini və beynəlxalq təhlükəsizlikdəki rolunu nəzərə alaraq qeyd edilməlidir ki, bu sahədə beynəlxalq əməkdaşlıq səmərəli qurulmalı və daha yeni formatda, habelə operativ birgə fəaliyyətin həyata keçirilməsi təmin edilməlidir. İnformasiya riskləri çox ani bir anda böyük zərər vurmaq potensialına malik olduğundan, dövlətlərin əməkdaşlığını və birgə maraqlar uğrunda fəaliyyətlərin qurulmasını təmin edən yeni formatda beynəlxalq əməkdaşlıq platforması qurulmasını məqsədəuyğun hesab etmək olar. Belə ki, dövlətlərin informasiya təhlükəsizliyinin təmin edilməsində məsul olan təşkilatların (qurumların) vahid rəqəmsal platforma üzərindən koordinasiyalı, informasiya təhlükəsizliyinin təmin edilməsinə, habelə informasiya təhlükəsizliyinə dair risk və ya təhdidlərə qarşı yönələn fəaliyyətləri təmin edilməlidir.

11. İnformasiya təhlükəsizliyi cəmiyyətin müxtəlif sferalarında tətbiq olunan sistem və ehtiyatlarla sıx bağlıdır. Tədqiqatlar göstərir ki, informasiya təhlükəsizliyinin təmin edilməsi üçün nə qədər standartlar və ya normalar müəyyən edilsə də, informasiya ehtiyatları və ya sistemləri həmin normalara uyğun olaraq hazırlanmış olmur və ya tətbiq prosesində bunlara əməl edilmir. İnformasiya təhlükəsizliyi aspektindən müvafiq ekspertiza fəaliyyətinin həyata keçirilməsi milli normativ hüquqi aktlarda müəyyən edilməlidir. O cümlədən, informasiya ehtiyatı və ya sisteminin istifadəyə buraxılması həmin ekspertiza nəticələrinə müvafiq olaraq müəyyən edilməlidir. Bu istiqamətdə informasiya

təhlükəsizliyinə dair informasiya ehtiyatı və ya sistemlərinin ekspertizasının aparılması ilə məşğul olan müvafiq qurum yaradılmalı, həmin ehtiyat və sistemlərə dair tələb və ya standartlar barədə normativ sənədlər qəbul edilməlidir.

12. İnformasiya təhlükəsizliyinə təhdidlər bir çox hallarda kommersiya maraqları ilə bağlı olur. Belə ki, informasiya ehtiyatlarına qeyri-qanuni müdaxilə vasitəsi ilə əldə olunmuş informasiyadan sui istifadə edilir və bununla da müəyyən subyektlər dairəsinə maddi, bəzi hallarda isə mənəvi zərərin vurulması ilə nəticələnir. Odur ki, korporativ fəaliyyət göstərən və belə ehtiyatlara sahib olan kommersiya qurumları tərəfindən informasiya təhlükəsizliyi risklərinin idarə olunması, sistemlərin istifadə edilməsi zəruridir. Belə olan halda beynəlxalq standartlara cavab verən informasiya təhlükəsizliyinin idarəetmə sistemlərindən istifadə edilməlidir.

13. İnformasiya texnologiyalarının inkişafı və innovasiyaların tətbiqi müxtəlif ölkələrdə müxtəlif səviyyələrdə özünü biruzə verir. İnformasiya texnologiyalarının sürətli inkişaf yolu keçdiyi ölkələrdə informasiya təhlükəsizliyi ilə bağlı məsələlərin tənzimlənməsi prosesi də eyni inkişaf yolunu keçmişdir. Odur ki, bu sahədə inkişaf etməkdə olan dövlətlər müsbət dünya təcrübəsini öyrənməkdə maraqlı olmalıdırlar. Belə təcrübə mübadiləsinin aparılması və öyrənilməsi informasiya təhlükəsizliyinin təmin edilməsi, təhdid və risklərin qabaqcadan öyrənilməsi, onlara qarşı tədbirlərin görülməsi baxımından öz müsbət töhvəsini verəcəkdir. Beləliklə, inkişaf etməkdə olan dövlətlər tərəfindən inkişaf etmiş dövlətlərin təcrübələrinin öyrənilməsinə, habelə inkişaf etmiş dövlətlərin isə öz aralarında məlumat mübadiləsinin həyata keçirilməsinə imkan verən ciddi beynəlxalq əməkdaşlıq platforması qurulmalıdır.

14. İnformasiya təhlükəsizliyinin təmin edilməsində əsas rol sahiblərindən biri də bu sahə üzrə peşəkar fəaliyyətlə məşğul olan kadrlardır. Müvafiq sahədə peşəkar və dərin biliyə malik insan resurslarının mövcudluğu informasiya təhlükəsizliyi tədbirlərinin görülməsində səhvlərin minimuma endirilməsinə səbəb ola bilər. Qeyd olunan sahədə inkişaf çox sürətlə getdiyindən həmin sahədə peşəkar şəxslərin biliklərinin və təcrübələrinin dərinləşdirilməsinə

ətraflı dəstək göstərilməlidir. Bunun üçün müxtəlif ali təhsil səviyyələri üzrə ixtisaslaşma proqramları və kurslarının yaradılması, peşəkar fəaliyyətlə məşğul olan şəxslərə informasiya təhlükəsizliyi sahəsində müsbət göstəriciləri ilə fərqlənən qurumlarda təcrübə keçmə imkanının verilməsi və s. barədə səmərəli tədbirlər görülməlidir.

15. Açıqlanması məhdudlaşdırılan və ya həssas informasiya kateqoriyasına aid edilən informasiyanın istifadəsinin hüquqi rejiminin müəyyən edilməsində yol verilən boşluqlar informasiya təhlükəsizliyinə böyük təhdidlər yaradılması ilə nəticələnə bilər. Həmin kateqoriya informasiyanın hüquqi və mühafizə rejiminin dəqiq tənzimlənməsi həyata keçirilməlidir. Bundan əlavə olaraq, belə informasiyadan istifadə edən müvafiq subyektlər bu fəaliyyətlərini müəyyən tələblərə uyğun qurmalıdırlar. Belə tələblərin dairəsi isə normativ sənədlərlə dəqiq müəyyən olunmalıdır.

16. İnformasiya təhlükəsizliyi ilə bişbaşa və ya dolayısı yolla əlaqədar olan bir çox tələblər beynəlxalq səviyyədə hüquqi tənzimlənmiş və beynəlxalq standartlar halına salınmışdır. İnformasiya təhlükəsizliyi sahəsində olan bu beynəlxalq standartların tətbiqi bir çox informasiya təhlükəsizliyi riskləri və təhdidlərinin qarşısının qətiyyətlə və asan yolla alınmasına səbəb olur. Həmin beynəlxalq standartlara uyğun olan milli standartların qəbul edilməsi isə müasir dövrümüzün reallığına çevrilmişdir və bununla da bir çox problemlərin həllinə nail olmaq mümkün olacaqdır.

17. Informasiya texnologiyaları vasitələri artıq gündəlik həyatın ayrılmaz hissəsinə çevrilmişdir. Qeyd edə bilərik ki, müxtəlif yaş kateqoriyalarından olan şəxslərin informasiya təhlükəsizliyi məsələlərinə də spesifik yanaşma göstərilməlidir. Burada mövcud əsas məsələlərdən biri kibermühitdə uşaq hüquqlarının müdafiəsinin təmin edilməsidir. Bu informasiya təhlükəsizliyi tədbirlərinin görülməsinin əhəmiyyətini müvafiq sistem və ya ehtiyata uşaqların əlçatanlığının təmin edildiyi hallarda daha da artırır. Həm insan hüquqları nöqteyi nəzərdən, həm də cəmiyyətin gələcək perspektivləri baxımından uşaqların əlçatımlılığının təmin edildiyi kiber mühitdə təhlükəsizlik tədbirləri artırılmalı, onların inkişafına təhdid yaradan mühitlərə girişlər məhdudlaşdırılmalıdır.

18. Uşaqlara dair informasiyanın yayılması informasiya təhlükəsizliyi hallarının yaranmasına səbəb olmaqla böyük zərərin vurulması ilə yanaşı, uşaqların şəxsi inkişafına və psixoloji vəziyyətinə də mənfi təsir edir. Odur ki, uşaqlara dair informasiyanın hüquqi rejiminin müəyyən edilməsində bu hallar nəzərə alınmalıdır. Hazırda milli qanunverciliyimizdə qeyd olunan istiqamətdə müvafiq dəyişikliklərin aparılmasına da zərurəti vardır. Qanunvericilikdə belə boşluqların olması informasiya təhlükəsizliyi risklərinin artması, habelə insan hüquqlarının pozulması ilə nəticələnə bilər. Bundan başqa, həssas kateqoriyaya daxil edə biləcəyimiz bu informasiyanın mühafizəsinin qarşılıqlı və bir-birini tamamlayan beynəlxalq və milli hüquqi mexanizmləri yaradılmalıdır.

19. Açıqlanması məhdudlaşdırılan və öz xüsusi əhəmiyyəti ilə seçilən informasiyanın mühafizəsinə dair tədbirlərin həyata keçirilməsinin təmin edilməsi qanunvericiliyimizin əsas tələblərindəndir. Açıqlanmasına icazə verilməyən informasiyanın əldə etmək hüququ olmayan subyektlərə verilməsi, yayılması və ya onlardan qanunsuz istifadə edilməsi qanunvericiliklə müəyyən edilmiş məsuliyyət yaradır. Bu öz növbəsində həmin növ informasiyalara münasibətdə xüsusi yanaşma göstərilməli olduğunun bir əyani təzahürüdür. Odur ki, həmin kateqoriya informasiyanın mövcud olduğu ehtiyat və ya sistemlərə girişin təmin edilməsində müasir doğrulama və ya autentifikasiya metodlarından istifadə edilməlidir. Bununla daha təhlükəsiz istifadə təmin edilə bilər.

20. Müasir dövrdə tətbiq edilən yeniliklərdən biri də şəxsiyyəti və ya hüquqları təsdiq edən bəzi sənədlərdə biometrik məlumatlardan istifadə edilməsidir. Ölkəmizdə də bu geniş vüsət almış bir haldır. Belə ki, həm ümumvətəndaş pasportlarında, həm də şəxsiyyət vəsiqələrində biometrik məlumatlardan istifadə edilir. Təhlükəsizliyin təmin edilməsi və cinayətkarlıqla mübarizə sahəsində bu öz müsbət töhvəsini versə də, informasiya təhlükəsiziyi risklərinin də artmasına səbəb olur. Belə ki, həmin biometrik məlumatların saxlandığı və yoxlanıldığı sistemlərin xüsusi təhlükəsizlik tələblərinə cavab verməsi təmin edilməlidir. Belə sistemlərdə hər hansı boşluğa yol verilə bilməz. Bu növ informasiyanın mühafizəsinin təmin edilməsi məqsədi ilə biometrik

informasiyanın saxlanılması, emalı və istifadəsi üçün informasiya ehtiyatları və sistemlərinə konkret tələblər normativ aktlarla müəyyən edilməli, habelə bu sistemlərin istifadəsinə ciddi dövlət nəzarəti həyata keçirilməlidir.

21. Müxtəlif sferalarda rəqəmsallaşmanın tətbiq edilməsi hökumət xidmətləri, habelə qurumlararası sənədləşmə prosesindən də yan keçməmişdir. Elektron hökumət xidmətlərinin və elektron sənəd dövriyyəsi sistemlərindən istifadənin hüquqi tənzimlənməsi müasir hüquq tendensiyalarından birini təşkil edir. Bu istiqamətdə AR qanunvericiliyində də müəyyən dəyişikliklərin aparılması zəruridir. Bundan başqa, elektron sənəd, elektron hökumət və elektron sənəd dövriyyəsi sistemləri ilə bağlı beynəlxalq və milli səviyyədə müvafiq hüquqi mexanizmlər formalaşdırılmalıdır. Belə ki, bu müasir dövrün əsas tələbi kimi özünü biruzə verir.

22. Sosial şəbəkələrdən geniş istifadə müasir dövrün əsas xüsusiyyətlərindən biri kimi nəzərə çarpır. Ölkəmizdə də sosial şəbəkə istifadəçilərinin sayı sürətlə artmışdır. Sosial şəbəkə fikir azadlığının təmin edilməsi istiqamətində müsbət platforma mühiti kimi xarakterizə olunsa da, şərəf və ləyaqətin, habelə bu kimi digər insan hüquqlarının pozulmasının da geniş vüsət aldığı bir mühit kimi qiymətləndirilə bilər. Belə ki, informasiya təhlükəsizliyi və ya şəxsi həyatın toxunulmazlığı istiqamətində bir çox təhdidlər məhz sosial şəbəkələrdən istifadə ilə meydana gəlir. Burada şəxsin kimliyini gizlədə bilməsi, bir anda istifadəçinin sosial şəbəkədə olan profilini silə bilmə imkanı və s. hallar informasiyanın mühafizəsi istiqamətində təhlükələrin yaranmasına səbəb olur. Hazırda qanunvericiliyimizdə bu istiqamətdə müəyyən dəyişikliklər edilsə də, informasiya təhlükəsizliyi nöqteyi nəzərindən tənzimləmə tam qənaətbəxş deyildir. Hesab edirik ki, sosial şəbəkə istifadəçilərinin informasiya təhlükəsizliyi riski və ya ona təhdid edən fəaliyyətlərinə görə hüquqi məsuliyyət müəyyən edən konkret normalar da qəbul edilməlidir. Bu öz preventiv xüsusiyyətinə görə də informasiya təhlükəsizliyinin təmin edilməsinə öz töhvəsini verəcəkdir.

23. İnternet informasiya ehtiyatı, sistemi və platformalarına çıxış imkanı verən əsas vasitələrdən biri kimi qəbul edilməlidir. Hətta qeyd edə bilərik ki, internet olmadan bir çox rəqəmsal

platformalara giriş əldə etmək mümkün deyildir. Odur ki, “internet”, “informasiya”, “informasiyanın mühafizəsi” və “informasiya təhlükəsizliyi”nə ən dəqiq anlayışlar verilməli, onların qarşılıqlı əlaqəsi və bir-birinə təsiri araşdırılmalıdır. Əldə olunmuş nəticələrə müvafiq olaraq, informasiya təhlükəsizliyinin təmin edilməsində yarana biləcək bütün mənfi təsirlər aradan qaldırılmalı və təhdidlərə qarşı birgə mühafizə mexanizmləri yaradılmalıdır.

24. İnternet şəbəkəsindən istifadə etməklə birbaşa və ya dolayısı yolla informasiya təhlükəsizliyi riski olan fəaliyyətlərin dairəsi müəyyənləşdirilməlidir. Bununla səmərəli tənzimetmənin həyata keçirilməsi və informasiya təhlükəsizliyinin təmin edilməsi mümkündür. Digər tərəfdən, internetdən istifadə ilə informasiya təhlükəsizliyi riski yaradan, insidentlərin yaranmasına səbəb olan ictimai təhlükəli əməllərə görə onların təhlükəlilik dərəcəsinə uyğun hüquqi məsuliyyət də dəqiqliklə müəyyən edilməlidir.

25. İnformasiya hüquq münasibətlərində də törədilən və ictimai təhlükəli hesab olunan əməllərə (hərəkət və ya hərəkətsizlik) görə hüquqi məsuliyyət əhəmiyyətli bir məsələdir. Belə əməllərin dairəsinin dəqiq müəyyənləşdirilməli olması qanunvericilikdə informasiya texnologiyalarının inkişafına uyğun şəkildə dəyişiklik və ya əlavələrin edilməsini zəruri edir. Mövcud AR qanunvericiliyində də müasir dövrün inkişaf tələblərinə uyğun müvafiq dəyişikliklərin aparılması məqsədəmüvafiq olardı.

26. İnsan hüquq və azadlıqlarının təmin edilməsi bütün dövlətlərin qarşısında duran əsas vəzifələrdən biridir. İnsan hüquqlarının yeni nəslini təşkil edən informasiya hüquqlarının təmin edilməsinə dair də yeni yanaşmalar mövcuddur. İnsan hüquqları kontekstində informasiya təhlükəsizliyi məsələlərinin araşdırılması mövcud hüquq münasibətlərinin tənzimlənməsi, habelə insan hüquqlarının təmini və müdafiəsi istiqamətində yararlı olardı. Belə ki, informasiya təhlükəsizliyinin və ya informasiya mühafizəsinin təmin edilməməsi nəticəsində baş verən insidentlərin bəziləri əsas, fundamental insan hüquq və azadlıqlarının məhdudlaşdırılması ilə nəticələnir. Odur ki, “insan hüquqları” və “informasiya təhlükəsizliyi”nin bir-biri ilə qarşılıqlı əlaqəsi və təsiri ətraflı araşdırılmalı, insan hüquqlarının təmin edilməsində informasiya

təhlükəsizliyinin roluna hərtərəfli aydınlıq gətirilməlidir. Bu aspektdə insan hüquqlarının müdafiəsi istiqamətində informasiya təhlükəsizliyinin təmin edilməsinin hüquqi mexanizmləri də dəqiq müəyyən edilməlidir.

27. İnformasiya təhlükəsizliyinin təmin edilməsi ilə bağlı yaranan mübahisələrin həlli bu münasibətlərin xaraktercə yeni və bəzi hissələrdə qeyri-müəyyən olması səbəbindən çətinliklərə səbəb olur. Bəzən informasiya təhlükəsizliyi ilə əlaqədar mübahisələr hüquqi perspektiv baxımından analiz edildikdə nəticə əldə oluna bilmir. Bu sahədə mübahisələrin alternativ həllindən istifadə də uğurlu hesab oluna bilər. Görünən isə odur ki, tərəflər bəzən mübahisələrin alternativ həlli metodalarından istifadə etmir, bundan yan qaçırlar. Bundan əlavə olaraq, bu istiqamətdə vahid məhkəmə təcrübəsinin formalaşdırılmasının da təmin edilməsi zəruri olan məsələlərdəndir. Statistikaya nəzər saldıqda, belə mübahisələrin sayı digər növ mübahisələrdən qat-qat az olsa belə, bunların həlli də olduqca zəruri məsələdir. Beləliklə, bu sahədə düzgün vahid məhkəmə təcrübəsinin formalaşdırılması təmin edilməli, habelə mübahisələrə baxan məhkəmələr bu məhkəmə təcrübəsini düzgün tətbiq etməlidirlər.

28. İnformasiya təhlükəsizliyi insidentləri və hadisələri nəticəsində müxtəlif subyektlərə müxtəlif həcmdə zərər vurulur. Bildirilməlidir ki, bu zərərin vurulmasına görə qanunvericilikdə hüquqi məsuliyyət müəyyən edilmişdir. Müəyyən edilən hüquqi məsuliyyət növlərindən biri də mülki hüquqi məsuliyyətdir. Vurulmuş zərərin əvəzinin ödənilməsi barədə mübahisələrin həllində zərərin miqdarının müəyyən edilməsində böyük çətinliklər yaranır. İnformasiyanın iqtisadi dəyərinin müəyyən edilməsi də özlüyündə çətin bir məsələyə çevrilir. Yəni informasiya təhlükəsizliyi insidenti və ya hadisəsi nəticəsində subyektin nə qədər maddi zərər çəkdiyinin müəyyən edilməsinin vahid hüquqi mexanizmi və ya qaydası müəyyənləşdirilməlidir. Bundan əlavə olaraq, informasiya təhlükəsizliyi insidentləri və hadisələri bir çox hallarda fiziki şəxslərin mənəvi zərər çəkməsinə də səbəb olur. Bu mənəvi iztirablarla şəxsə nə qədər zərər vurulması isə subyektiv və hər bir işin hallarına uyğun olaraq qiymətləndirilməli məsələ kimi nəzərdən

keçirilməlidir. Mənəvi zərərin müəyyən edilməsi ilə bağlı AR Konstitusiya Məhkəməsi və AR Ali Məhkəməsinin Plenumunun müvafiq qərarları olsa da, hələ də bu zərərin miqdarının müəyyən edilməsində müəyyən çətinliklər yaranır. Qeyd edilənləri nəzərə alaraq və beynəlxalq praktikaya uyğun olaraq bu zərərin miqdarının müəyyən edilməsində nəzərə alınmalı olan hallar, habelə bu zərərin miqdarının müəyyən edilməsinin üsulu və qaydasının dəqiq hüquqi mexanizmləri formalaşdırılmalıdır.

29. İnformasiya təhlükəsizliyi insidenti və ya hadisəsinə reaksiya təhlükəsizlik insidentlərinin aşkarlanması, təhlili və onlara cavab vermə prosesi olmaqla müasir dövrdə görülməli olan tədbirlər siyahısında öndədir. İnformasiya təhlükəsizliyi insidenti və ya hadisəsi baş verdiyi halda müvafiq məsul subyekt dərhal buna reaksiya verməli (tədbirlər görməli), lazım olduqda müvafiq icra hakimiyyəti orqanına bu barədə məlumat verməlidir. Belə hallara dair mühafizə və ya təhlükəsizlik mexanizmləri formalaşdırılmalı, insidentlərə cavab planlarının hazırlanmaları, şübhəli fəaliyyət üçün şəbəkə trafikinin monitorinqi və ekspertiza təhlillərinin aparılması təmin edilməlidir. Bundan əlavə olaraq, qeyd olunan tədbirlərin həyata keçirilməsinin dəqiq və ətraflı hüquqi tənzimlənməsi zəruridir və bu istiqamətdə də normativ sənədlər hazırlanmalı, mövcud qanunvericilikdə müvafiq dəyişikliklər aparılmalıdır.

30. İnformasiya təhlükəsizliyinin təmin edilməsində əsas mexanizmlərdən biri risklərin idarə edilməsidir. Bunu nəzərə alaraq informasiya təhlükəsizliyi üçün risklərin müəyyən edilməsi, qiymətləndirilməsi və azaldılması prosesinin təmin edilməsi zəruridir. Bu, risklərin qiymətləndirilməsini, təhlükəsizlik nəzarətinin həyata keçirilməsini və fövqəladə hallar planlarının hazırlanmasını əhatə edir. Qeyd olunan risklərin idarəedilməsinə dair ümumi tələblərin müəyyən edilməsi qeyd olunan mexanizmin səmərəliliyini artıracaqdır. Odur ki, mövcud istiqamət üzrə də normativ aktlar formalaşdırılmalı, normativ sənədlərə isə müasir dövrün tələblərinə uyğun əlavə və ya dəyişikliklər edilməlidir.

Tədqiqatın elmi yeniliyi. Bir sıra xarici müəlliflər öz tədqiqat əsərlərində informasiya təhlükəsizliyinin mühüm istiqamətlərini araşdırmış, informasiya təhlükəsizliyinin dövlətdaxili müdafiə

mexanizmlərini tədqiq etmişlər. Lakin AR-də informasiya təhlükəsizliyinin beynəlxalq və dövlətdaxili hüquqi müdafiə mexanizmləri sahəsində elmi-tədqiqatlar demək olar ki aparılmamış, bu günədək dövlətin informasiya təhlükəsizliyinin beynəlxalq və dövlətdaxili hüquqi müdafiə mexanizmləri mövzusunda kompleks tədqiqat əsəri yazılmamışdır. Bu mövzu dissertasiya səviyyəsində ilk dəfədir ki, tədqiq edilir.

Məhz dissertasiyanın elmi yeniliyi də ondadır ki, burada ilk dəfə informasiya hüquqları informasiya təhlükəsizliyinin obyekti kimi, informasiya təhlükəsizliyi sahəsində dövlət siyasəti dövlətin təhlükəsizlik sahəsində əsas funksiyasının həyata keçirilmə mexanizmi kimi, elektron dövlət informasiya hüquqlarının təminat sistemi kimi, insan hüquqları kontekstində informasiya hüququnun konstitusion hüquqi təminatları, informasiya təhlükəsizliyi ilə bağlı dövlətdaxili qanunvericilik təhlükəsizlik sisteminin mühüm hissəsi kimi nəzərdən keçirilmiş, dövlətimizin informasiya sahəsində universal və regional əməkdaşlığı tədqiq edilmiş, informasiya təhlükəsizliyi sahəsində beynəlxalq universal və regional hüquq normalarının AR qanunvericiliyinə implementasiya xüsusiyyətləri və istiqamətləri araşdırılmışdır.

Tədqiqatın nəzəri və praktiki əhəmiyyəti. Onu qeyd etmək lazımdır ki, dövlətin informasiya təhlükəsizliyinin hüquqi aspektlərinin tədqiq edilməsi nəticəsində əldə edilmiş nəticələrin və irəli sürülmüş təkliflərin həm elmi-nəzəri, həm də informasiya sahəsində qanunvericiliyin təkmilləşdirilməsi baxımından praktiki əhəmiyyəti böyükdür. Dissertasiyanın nəzəri nəticələrindən, praktik təkliflərindən hüquqyaratma fəaliyyətində, habelə ali məktəblərdə tədris prosesində, xüsusilə İnformasiya hüququ, İnsan hüquqları, Konstitusiya hüququ, İnzibati hüquq, Milli təhlükəsizlik hüququ və s. fənlər üzrə dərslik, dərs vəsaitləri, o cümlədən tədris-metodik vəsait və proqramların işlənib hazırlanmasında və informasiya təhlükəsizliyinə dair elmi tədqiqatların aparılmasında və qanunvericiliyin təkmilləşdirilməsində geniş istifadə oluna bilər.

Aprobasiyası və tətbiqi. Dissertasiyanın əsas müddəaları, nəticələr və praktik tövsiyələr AR, ABŞ, Rusiya Federasiyası, Polşa Respublikası, Qazaxıstan və Ukraynanın nüfuzlu elmi jurnallarında

və elmi məqalə toplularında açıqlanmış, müəllifin dərc edilmiş işlərində, elmi praktik konfranslarındakı məruzələrinin tezislərində və çıxışlarında öz əksini tapmışdır.

Dissertasiyanın yerinə yetirildiyi təşkilatın adı. Dissertasiya Bakı Dövlət Univeristetinin Hüquq fakültəsinin İnsan hüquqları və informasiya hüququ UNESCO kafedrasında yerinə yetirilmişdir.

Tədqiqat işinin strukturu. Dissertasiya giriş, beş fəsil, nəticə və istifadə edilmiş ədəbiyyat siyahısından ibarətdir.

DİSSERTASİYANIN ƏSAS MƏZMUNU

Dissertasiyanın giriş hissəsində mövzunun aktuallığı əsaslandırılır, tədqiqatın işlənmə dərəcəsi, obyekti və predmeti, məqsəd və vəzifələri, elmi yeniliyi, müdafiəyə təqdim edilən yeni elmi müddəaları nəzəri və praktik əhəmiyyəti izah edilir, tədqiqatın nəticələrinin aprobasiyası və tədqiqatın strukturu haqqında məlumat verilir.

Dissertasiyanın birinci fəsli "İnformasiya təhlükəsizliyi və onun milli təhlükəsizlik sistemində yeri" adlanır və iki paraqrafdan ibarətdir.

"İnformasiya təhlükəsizliyi anlayışı və təhlükəsizliyə təsir edən faktorlar" adlanan **birinci paraqraf** iki yarımparaqrafdan ibarət olmaqla informasiya təhlükəsizliyi anlayışı, onun əsas aspektləri və təhlükəsizliyə təsir edən faktorlar kimi konfidensiallıq, tamlıq, əl çatanlıq, hesabatlılıq kimi məsələlər təhlil edilir.

İnformasiya anlayışı gizlilik, tamlıq və əlçatanlıq prinsiplərinə əsaslanır. İnformasiyadan istifadə dərəcəsinə görə bu prinsiplər də öz aralarında fərqli əhəmiyyət dərəcələrinə bölünürlər. Bəzi milli araşdırmalarda öncəlik gizlilik prinsipinə verilmişdir. Media sahəsində öncəlik isə əlçatanlıqdadır. İnternet üzərindən yayın edən bir qurum üçün öncəlik informasiyanın qarşı tərəfə davamlı və ən sürətli şəkildə çatdırılmasıdır. Bəzən kiçik bir alt yazı digərlərindən fərqlənməyi bacara bilir. Verilən informasiyada gizlilik axtarılmaz, tamlıq gözlənilmədən qarşı tərəfə ötürülə bilər. Bir məhkəmə prosesində hakim üçün öncəlik tamlıq prinsipidir. Bəzən bu proses illərlə davam edir. Bəzən bəzi məsələlər ifadələr alınarkən

gizliliyini itirə bilər. Məqsəd doğru məlumatlara əsaslanaraq həyati qərarlar vermək olduqda əldə ediləcək informasiyaları daha da əhəmiyyətli hala gətirir.

Sevindirici haldır ki, AR-in qanunvericiliyində informasiya təhlükəsizliyinə anlayış verilmişdir. Belə ki, "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" AR Qanununun 2-ci maddəsinə əsasən, informasiya təhlükəsizliyi informasiyanın tamlığının (dəqiq, səlis, aktual və bütöv olması), əlçatanlığının (müraciət və əldə etmənin, nəzarətdə saxlamanın mümkün olması), konfidensiallığının (yalnız səlahiyyəti olan istifadəçilər və proseslər üçün məlum ola bilməsi) və mötəbərliliyinin (adekvat, obyektiv, faydalı olması) mühafizə edilməsidir. Göründüyü kimi, AR qanunvericiliyi ilə də informasiya təhlükəsizliyi konsepsiyası tamlıq, konfidensiallıq və əlçatanlığa əsaslanır.

Bütövlükdə isə, konfidensiallıq, tamlıq, əlçatanlıq, hesabatlılıq informasiya təhlükəsizliyinin əsas aspektləri və təhlükəsizliyə təsir edən faktorlardır.

İkinci paraqrafda – "İnformasiya təhlükəsizliyi standartları və informasiya təhlükəsizliyində risk amili"- informasiya təhlükəsizliyi standartları və informasiya təhlükəsizliyində risk amili ilə əlaqədar hüquqi problemlər tədqiq edilir və özündə üç yarımparaqrafı əhatə edir.

İnformasiya təhlükəsizliyi standartları informasiya təhlükəsizliyinin təmin edilməsi məqsədi daşıyan minumum tələblərdir. İnformasiyanın saxlandığı və üzərində əməliyyat aparıla bilən yerlərin, əsas da informasiya sistemlərinin informasiya təhlükəsizliyinin təmin edilməsi üçün sınanmış və öz təsdiqini tapan bu tələblərə cavab verməsi xüsusi ilə əhəmiyyətli məsələdir.

İnformasiya təhlükəsizliyində risk amilinin geniş izahından əvvəl ona lakonik şəkildə belə izah verilməsi mümkündür: İnformasiya təhlükəsizliyində risk informasiya sistemi və ya ehtiyatlarında mövcud olan boşluqlardan istifadə ilə orda yer alan informasiyanın qeyri-qanuni yolla ələ keçirilməsi, istifadəsi və bunun nəticəsində ziyan vurulması ilə nəticələnən hadisənin baş vermə ehtimalıdır.

Dissertasiyada informasiya təhlükəsizliynə təsir edən risklər təsnifləndirilmiş və informasiya təhlükəsizliyinə dair risklərin təsnifləşdirilməsinin əsas mahiyyəti onunla əlaqələndirilmişdir ki, mühafizə tədbirlərinin görülməsi üçün riskin haradan gələ biləcəyi və hansı üsulla təsir edə biləcəyi kimi detallar qabaqcadan məlum olsun. Belə olan halda, informasiya təhlükəsizliyinin təmin edilməsi barədə mexanizmləri daha əlverişli şəkildə müəyyən etmək və tətbiq etmək olar. İnformasiya təhlükəsizliyi həmçinin kommersiya sirləri, patentlər və müəllif hüquqları kimi əqli mülkiyyət hüququ obyektlərinin qorunmasını da əhatə edən geniş bir sahə kimi də nəzərdən keçirilir. Həm əqli mülkiyyət hüququ obyektlərinə, həm də informasiyaya tətbiq edilən hüquqi rejimlərdə olan bu fərqlər qanunvericiliyin tətbiqi məsələsini çətinləşdirir.

Ümumilikdə, informasiya təhlükəsizliyi risklərinin aşkarlanması və qarşısının alınması məlumatların qorunması və kibertəhlükəsizlik qanunlarına riayət edilməsi, məsuliyyət və hesabatlılıq, transsərhəd məlumat ötürülməsi və əqli mülkiyyətin qorunması da daxil olmaqla bir sıra hüquqi problemlər yaradır. Təşkilatlar informasiya təhlükəsizliyi strategiyalarını tərtib edərkən və həyata keçirərkən bu hüquqi məsələləri nəzərə almalıdırlar. Bu öz növbəsində onları məsuliyyətdən və yarana biləcək hüquq mübahisələrindən qoruyan haldır.

“Elektron dövlətdə informasiya təhlükəsizliyi və onun əhəmiyyəti” adlı dissertasiyanın ikinci fəsli iki paraqrafdan ibarətdir. Bu fəsildə İnformasiya təhlükəsizliyinin idarəetmə sistemində yeri, e-dövlətdə informasiya təhlükəsizliyi, e-dövlətdə informasiya təhlükəsizliyinin təmin olunması problemləri, e-imza informasiya təhlükəsizliyinin təminat vasitəsi kimi, elektron məlumat daşıyıcıları informasiya təhlükəsizliyinin obyekti kimi təhlil edilir.

“İnformasiya təhlükəsizliyinin idarəetmə sistemində yeri” adlı **birinci paraqrafda** qeyd edilmişdir ki, informasiya məkanında dövlətin, cəmiyyətin və vətəndaşların maraqlarının təmin edilməsi dövlətin əsas məqsədlərindən biridir. Hər şeydən əvvəl, insan və vətəndaş hüquq və azadlıqlarının təmin və müdafiə olunması hüquqi dövlətin əsas məqsədi olmalıdır. Odur ki, informasiya cəmiyyətində də hüquq subyektliliyi olan şəxslərin hüquqlarının və qanuni

maraqlarının təmin edilməsi dövlət qarşısında duran əsas məsələlərdən biridir. AR qanunvericiliyində bu müddəanın konstitusion əsası da mövcuddur. Belə ki, AR Konstitusiyasının 12-ci maddəsinin birinci hissəsinə əsasən, insan və vətəndaş hüquqlarının və azadlıqlarının, AR-in vətəndaşlarına layiqli həyat səviyyəsinin təmin edilməsi dövlətin ali məqsədidir.

Hazırki dövrün informasiya dövrü olduğunu nəzərə alaraq açıqlanması məhdudlaşdırılan dövlət sirri, hərbi sirr, fərdi məlumatlar və ya bu kimi digər informasiyanın mühafizəsinin təmin edilməməsi dövlət idarəetməsində böyük çətinliklər yarada, dövlət və ictimai maraqlara böyük ziyan vurulması ilə nəticələnə bilər. Hazırda informasiyanın yayılması ötən dövrlərə nisbətdə daha sürətli şəkildə həyata keçirilir. Bunun səbəbi hər bir şəxsin gündəlik həyatlarında informasiya texnologiya vasitələrindən geniş istifadə etməsi, belə vasitələrə və internetə əlçatanlığın rahatlaşması olmuşdur. Nəticə olaraq informasiya təhlükəsizliyi idarəetmə sisteminin keyfiyyətli idarəetmə sistemi ilə inteqrasiya edilməsi sistemin təsirlilik və keyfiyyət ilə bərabər zamandan və mənbələrdən əhəmiyyətli şəkildə qənaətlənməsi bundan başqa mövcud sistemi inkişaf etdirməyin yanında tətbiq oluna biləcək bir çox problemə də həll gətirəcəkdir.

“E-dövlətdə informasiya təhlükəsizliyi” adlı **ikinci paraqrafda** E-dövlətdə informasiya təhlükəsizliyinin təmin olunması problemləri, E-imza informasiya təhlükəsizliyinin təminat vasitəsi kimi, elektron məlumat daşıyıcıları informasiya təhlükəsizliyinin obyekti kimi məsələlər tədqiq edilir və üç yarımparaqrafdan ibarətdir.

İctimai həyatın bütün sahələrində və demək olar ki bütün dövlət orqanlarında elektron dövlətə keçidin təmin edilməsi insan hüquq və azadlıqlarının daha rahat təmin edilməsi, statistik göstəricilərin və dövlət orqanlarının fəaliyyətinin şəffaflaşması kimi müsbət nəticələr ortaya çıxarır.

Göstərilənləri nəzərə alaraq qeyd edilə bilər ki, elektron hökumətdə informasiya təhlükəsizliyinin təmin edilməsi barədə danışmazdan əvvəl ondan istifadə edən subyektlər dairəsi, həmin subyektlərin hər birinin ayrı-ayrılıqda aralarında olan münasibətlərinin xarakteri və təbiəti təhlil edilməli və nəzərə

alınmalıdır. Ümumilikdə elektron hökumətdən istifadə ilə bağlı və ya onunla əlaqəli olan hüquq münasibətlərinin iştirakçılarını 4 kateqoriyada cəmləşdirə bilərik. Bunlar hökumət (goverment-G), dövlət orqanı və ya qurumunun əməkdaşı (officials-O), biznes subyekti (business-B), vətəndaş (citizen-C) kateqoriyalarıdır.

Elektron dövlət və ya hökumət sistemlərində informasiya təhlükəsizliyinə dair bir çox problemlər məhz informasiya təhlükəsizliyinin əsas elementlərinin təmin edilməməsi ilə bağı olur. Bu yanaşma özünü praktikada da doğruldur. Elektron dövlət və ya hökumətdə informasiya təhlükəsizliyi problemləri bir çox hallarda ya istifadəçilərin səhlənkarlıqla etdikləri hərəkətdən (hərəkətsizlikdən), ya da informasiya təhlükəsizliyinə məsul olan subyektin yaratdığı sistemdə olan texniki nasazlıq və ya sistemdə olan boşluqlardan, hüquqi tənzimləmə məqsədi ilə qəbul edilmiş məxfilik siyasəti və s. kimi digər sənədlərdə yol verilmiş açıq səhvlərdən qaynaqlana bilər.

Digər tərəfdən elektron dövlətdə informasiya təhlükəsizliyinin əsas sütunlarından biri olan informasiyanın gizliliyinin təmin edilməsi və elektron dövlət informasiya kommunikasiya sistem və ya şəbəkəsinin və orada aparılan əməliyyatların gizliliyinin təmin edilməsi olduqca zəruridir. Məhz bu gizliliyin təmin edilməməsi və ya lazımi səviyyədə təmin edilə bilinməməsi gələcəkdə informasiya platformasında mövcud olan, ötürülən, emal edilən və ya saxlanılan informasiyanın üçüncü şəxslər tərəfindən qanunsuz yolla əldə olunması, nəticədə informasiya təhlükəsizliyininə böyük təhdidlərin yaranması ilə nəticələnə bilər.

Beləliklə, informasiya təhlükəsizliyi elektron dövlət sistemləri üçün vətəndaşların məlumatlarını qorumaq, hökumət sistemlərinin bütövlüyünü təmin etmək, ictimai etimadı qorumaq, qanun və normativ tələblərə riayət etmək üçün vacibdir. İnformasiya texnologiyalarının sürətli inkişafı və onun bütün sahələrdə tətbiq edilməsi elektron sənəd dövriyyəsi sistemlərinin tətbiq edilməsi, həmçinin elektron formada olan sənədlərin həqiqiliyinin, dəyişməzliyinin təmin edilməsi məqsədilə müəyyən doğrulama üsul və ya mexanizmlərinin tətbiq edilməsini zəruri edir. Elektron imzanın xüsusi əhəmiyyəti onun imza sahibini identifikləşdirmə, elektron imza vasitələri ilə imzalanmış sənədlərin həqiqiliyinin

mübahisələndirilə bilməməsi, o cümlədən elektron imza vasitələri ilə təsdiqlənmiş sənədlərin məzmunca dəyişdirilməsinin mümkün olmamasıdır.

Qeyd olunanları nəzərə alaraq sadə formada elektron imza sənədin və ya müqavilənin imzalanmasının rəqəmsal üsulu və ya forması kimi müəyyən edilməlidir. Bu, imzalayanın sənədin və ya müqavilənin məzmununu qəbul etdiyini və onun şərtləri ilə razılaşdığını göstərən qanuni olaraq tanınmış bir üsuldur. Elektron məlumat daşıyıcılarının təhlükəsizliyi mühüm əhəmiyyət kəsb edir, çünki onlar həssas və ya məxfi məlumatları ehtiva edə bilər ki, bu məlumatlar əldə olunarsa və ya ələ keçirilərsə, oğurluq, maliyyə itkisi və nüfuzun zədələnməsi kimi ciddi nəticələrə səbəb ola bilər.

Dissertasiyanın üçüncü fəsli "Mülki hüquq və azadlıqların müdafiəsində informasiya təhlükəsizliyi və onun hüquqi problemləri" adlanır və üç paraqrafdan ibarətdir.

İki yarımparaqrafdan ibarət olan **birinci paraqraf "Fərdi məlumatların informasiya təhlükəsizliyi"** adlanır və burada fərdi məlumatlar və onlardan istifadə qaydası, fərdi məlumatların informasiya təhlükəsizliyinin təmin olunması məsələləri nəzərdən keçirilir.

Burada toxunulması və aydınlaşdırılmalı olan əsas məsələ informasiyanın təbiəti və ya xarakterinə görə onun yer aldığı kateqoriyanın müəyyənləşdirilməsidir. Aparılmış elmi tədqiqat və ədəbiyyatlara nəzər salaraq və ümumiləşdirərək deyə bilərik ki, informasiya əlçatanlılıq səviyyəsinə görə açıq informasiya və əldə olunması məhdudlaşdırılan informasiya, bəzi hallarda isə həssas informasiya olaraq təsnifləşdirilə bilər. Onu da qeyd etmək mümkündür ki, əldə olunması məhdudlaşdırılan informasiya öz növbəsində qanunla və müqavilə ilə əldə olunması məhdudlaşdırılan informasiya kimi təsnifləşdirilə bilər. Əldə edilməsi qanunla məhdudlaşdırılan informasiyalar hüquqi rejiminə görə təsnifləşdirilərək məxfi və gizli (konfidensial) informasiyalar kimi müəyyən edilir. Məxfi informasiyaya əsasən dövlət sirri aid edilirsə, konfidensial informasiyalara isə bir qayda olaraq vətəndaşların, müəssisə, idarə, təşkilatların, o cümlədən digər hüquqi şəxslərin qanuni maraqlarının qorunması məqsədilə əldə edilməsinə müəyyən

məhdudiyyət qoyulan peşə, kommersiya, istintaq və məhkəmə sirləri daxil edilir. Qeyd edilənlər AR qanunvericlik praktikasında da təsdiq edilmişdir. Qanunvericiliyimizdə fərdi məlumatlara verilən anlayışı mövcud hüquq münasibətlərinin cəmiyyətimiz üçün yeni xarakter daşımasını nəzərə alaraq uğurlu hesab etmək olar. Lakin fərdi məlumatlara qanunvericiliyimizdə daha geniş və onun təbiətini tam açan anlayış verilməsi daha məqsədəmüvafiq olardı. Odur ki, bu sahədə beynəlxalq müqavilələr, o cümlədən xarici ölkələrin praktikasında müəyyən normativ hüquqi aktların nəzərdən keçirilməsi zəruridir. Həmin aktlar və ədəbiyyatda olan mövcud anlayışların müqayisəli təhlili və cəmiyyətimizin özünəməxsus xüsusiyyətləri nəzərə alınmaqla qanunvericiliyə dəyişiklik edilməsi təklifinin verilməsi daha doğru olardı.

Fərdi məlumatların təhlükəsizliyini təmin etmək üçün təşkilati hüquqi formasından asılıq olmayaraq bütün təşkilatlar bir sıra informasiya təhlükəsizliyi tədbirləri görən hərtərəfli bir fəaliyyət qurmalıdırlar. Əvvəla bu təşkilatların qanunla üzərinə qoyulan öhdəliklərindən irəli gəlir. Konfidensial fərdi məlumatların qanunauyğun istifadəsinin və mühafizəsinin təmin edilməsi konfidensial fərdi məlumatın mövcud olduğu informasiya ehtiyatının mülkiyyətçisi və ya müvafiq xidmətləri göstərən operatorun üzərinə düşür. Odur ki, informasiya təhlükəsizliyi tədbirlərinin lazımi səviyyədə və üsulda görülməməsi subyektlərin qanunla müəyyən edilmiş məsuliyyətə cəlb olunması ilə nəticələnə bilər. İnformasiya təhlükəsizliyi kontekstində fərdi məlumatların məxfiliyi vacibdir, çünki fərdi məlumatlar tez-tez öz qazancları üçün oğurlamaq və ya sui-istifadə etmək istəyən kibercinayətkarlar üçün əsas hədəfdir.

İki yaramparaqrafdan ibarət olan **ikinci paraqraf** "**Biometrik məlumatların informasiya təhlükəsizliyi"** adlanır və burada biometrik məlumatlar və onlardan istifadə qaydası, müxtəlif sahələrdə biometrik məlumatlar və onların informasiya təhlükəsizliyi məsələləri təhlil edilir.

Biometrik məlumatlar öz unikallıq xüsusiyyətinə görə tamamilə müxtəlif sahələrdə istifadə olunur. Belə ki, müxtəlif elm sahələrinin, həmçinin ictimai sferaların predmetini təşkil edən və qeyri-müəyyən qalan məsələlər məhz biometrik məlumatlardan

istifadə edilməsi ilə aydınlaşdırıla bilər. Əvvəla bəzi biometrik məlumatlar ömrü boyu dəyişilməzliyi və unikallığı ilə seçilir. Bu biometrik məlumatlar şəxslərin identifikləşdirilməsi prosesində əsrarəngiz rol oynayır. Məsələn, şəxsin əl izi, üz izi, DNK məlumatları kimi fərdi unikal məlumatlar. Bunlar cinayət prosesi, kriminalistika, əməliyyat axtarış fəaliyyəti kimi sahələrdə qarşıya qoyulmuş məsələlərin həllinin təmin edilməsində əhəmiyyətli rola malikdir. Həmçinin şəxsin genetik məlumatlarını özündə əks etdirən biometrik məlumatlar bəzi mülki mübahisələrin həllində xüsusi rol oynayır. Buna misal olaraq, atalığın mübahisələndirilməsi, atalığın müəyyən edilməsi, vərəsəlik üzrə münasibətlərə dair qaldırılan iddialar barədə mülki işlər göstərilə bilər. Qeyd olunanlar biometrik məlumatların və biometik texnologiyaların informasiya təhlükəsizliyinin təmin edilməsi üçün istifadəsinin əhəmiyyətini bir daha təsdiq edir. Məhz informasiya təhlüksizliyinin müasir rəqəmsal informasiya cəmiyyətində az riskli və daha rahat təmin edilməsinin ən əlverişli üsullarından biri biometrik texnologiya, sistem və məlumatlardan istifadəni özündə ehtiva edir.

"Fərdi və biometrik məlumatların informasiya təhlükəsizliyinin təmin olunmasının dövlətdaxili və beynəlxalq hüquqi müdafiə mexanizmləri" adlı **üçüncü paraqrafda** AR qanunvericiliyində fərdi, biometrik məlumatların istifadəsi və təhlükəsizliyin hüquqi aspektləri və fərdi, biometrik məlumatların istifadəsi və onların informasiya təhlükəsizliyinin beynəlxalq hüquqi aspektləri məsələləri təhlil edilməklə iki yarımparaqrafdan ibarətdir.

Fərdi məlumatların istifadəsi və mühafizəsinin hüquqi mexanizmlərinin müəyyən edilməsi ona görə zəruridir ki, bu birbaşa insan və vətəndaşın əsas insan hüquq və azadlıqları ilə əlaqədardır. Fərdi məlumatların istifadəsi və mühafizəsi məsələsi yalnız informasiya hüququna aid edilən bir məsələ deyildir. Yeni nəsil insan hüquqlarında olan informasiya hüquqlarının, o cümlədən şəxsin rəqəmsal cəmiyyətdə şəxsi həyatın toxunulmazlığı hüququnun təmin edilməsi dövlətin əsas məqsədlərindən birinə çevrilmişdir.

Fərdi məlumatların mühafizəsi şəxsi həyatın toxunulmazlığına təsir edən əsas vasitələrdən biridir. Qeyd olunan prizmadan yanaşdıqda görürük ki, fərdi məlumatların mühafizəsinin

və düzgün istifadəsinin təmin edilməsi məqsədi ilə dövlətlər bir çox tədbirlər görməli və bu sahədə xüsusi nəzarət aparmalıdır. Çünki, əsas insan hüquq və azadlıqlarının təmin edilməsi ilə sıx əlaqədar olan bu problem özü-özlüyündə dövlətdə bu sahəyə xüsusi diqqət göstərməsini zəruri edən faktorlardandır.

Dördüncü fəsil "Cəmiyyətin informasiya təhlükəsizliyinin əsas problemləri: hüquqi məsuliyyət və informasiyanın mühafizəsi" adlanır və iki paraqrafı özündə birləşdirir.

Birinci paraqraf "Sosial şəbəkələr və onların yaratdığı informasiya təhlükələri" adlanmaqla iki parımparaqrafdan ibarətdir və burada sosial media və onun informasiya cəmiyyətinə təsiri, daha sonra internet cəmiyyətin informasiya təhlükəsizliyinə təsir edən vasitə kimi məsələlər təhlil edilir.

Qanunvericiliyimizdə sosial mediaya anlayış verilməsə də, media ifadəsinə anlayış verilmişdir. Belə ki, media sahəsində münasibətləri tənzim edən "Media haqqında" AR Qanununun 1-ci maddəsinə əsasən media dedikdə kütləvi informasiyanın dövri və ya müntəzəm olaraq dərc olunmasını və (və ya) yayımlanmasını həyata keçirmək üçün istifadə olunan alət və vasitələr, habelə onlar vasitəsilə formalaşan informasiya mühiti başa düşülür.

Qeyd olunanlara əsasən, dissertasiyada sosial mediaya belə anlayış verilir: sosial media dedikdə, istifadəçilərə məzmun yaratmağa, özü və ya digər istifadəçi tərəfindən yaradılan məzmunu izləməyə, paylaşmağa, mübadilə etməyə, bəzi hallarda mövcud məzmun barədə şərh etməyə və fikir mübadiləsi aparmağa və ya ümumi şəkildə sosial şəbəkələrdə iştirak etməyə imkan verən veb əsaslı platformalar, tətbiqetmələr və texnologiyalar başa düşülür. Bununla belə, internet informasiya təhlükəsizliyi və məxfilik baxımından da ciddi problemlər yaradır. Bu da onun mənfi cəhəti kimi qiymətləndirilə bilər.

Onlayn şəkildə ötürülən və saxlanılan böyük miqdarda əldə olunması məhdudlaşdırılan informasiya, yəni fərdi məlumatlar, dövlət sirri, hərbi sirr, şəxsi və ailə həyatı sirri və s. kiberhücumlara və haker hücumlarına qarşı həssas ola bilirlər. İnternet müstəvisində informasiya təhlükəsizliyinə dair risklər bəzi situasiyalarda çap edilmiş daşıyıcılarda saxlanılan informasiyaya nisbətdə daha çox faiz

təşkil edir. Bu da fərdləri və təşkilatları məlumat oğurluğu, maliyyə fırıldaqlığı və digər kibercinayətkarlıq formaları riski altına qoyur. Müəyyən mənada bəzən internet üzərində aparılan əməliyyatlar məsul şəxslərdə şübhə doğura və bununla bağlı araşdırmaya başlamasına səbəb ola bilər. İnternet insanların gündəlik həyatını rahatlaşdırsa da, informasiyadan sui-istifadə edilməsi və bununla da maddi zərər vurulması hallarına görə geniş şəkildə bir çox tədqiqatçılar tərəfindən tənqid edilir.

Bu problemləri həll etmək və internetin kommunikasiya, innovasiya və inkişaf üçün təhlükəsiz və açıq platforma olaraq qalmasını təmin etmək üçün hökumətlər, vətəndaş cəmiyyəti təşkilatları və özəl sektor yeni siyasətlər, texnologiyalar və təcrübələr hazırlamaq üçün birlikdə işləyirlər. Buraya rəqəmsal savadlılığın təşviqi, kibertəhlükəsizliyin təkmilləşdirilməsi, fərdlərin və təşkilatların məxfiliyinin qorunması səyləri daxildir.

"Hüquqi məsuliyyət və informasiyanın mühafizəsi" adlanan **ikinci paraqraf** üç yarımparaqrafdan ibarət olmaqla hüquqi məsuliyyət informasiya təhlükəsizliyinin təmin olumasında preventiv tədbir kimi, informasiyanın mühafizəsi informasiya təhükəsizliyinin təmin olunması vasitəsi kimi, informasiya təhlükəsizliyi mədəniyyəti və onun informasiya təhlükəsizliyinin təmin olunmasında rolu kimi aktual məsələlər təhlil edilir.

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. 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 informasiya təhlükəsizliyini təmin etmək

üçün kifayət olmaya bilər, çünki o, effektiv icra və uyğunluq mexanizmlərinə əsaslanır. Məlumdur ki, informasiyanın mühafizə edilməsi informasiya təhlükəsizliyində öz xüsusi rolu ilə seçilir. Real təcrübədə informasiyanın mühafizəsi informasiya təhlükəsizliyinin təmin edilməsi prosesinin ən əsas mərhələlərindən biri kimi çıxış edir. İnformasiya təhlükəsizliyi mədəniyyəti informasiyanın mühafizəsi sahəsində mövcud olan təhlükə və risklərin azaldılmasına istiqamət verən əsas faktorlardan biri kimi çıxış edir. İnformasiya təhlükəsizliyi mədəniyyətinin formalaşdırılmasında ilkin və ən əsas məqam maarifləndirmə işinin təşkilidir. İnformasiya hüquq münasibətlərinin iştirakçıları informasiya təhlükəsizliyi ilə əlaqədar bilik və davranış qaydaları barədə məlumatlar əldə etdikdə öz fəaliyyətlərinə daha yaxşı nəzarət həyata keçirə bilir, informasiya üzərində əməliyyatların daha təhlükəsiz aparılmasına nail ola bilirlər.

Dissertasiyanın beşinci fəsli "İnformasiya təhlükəsizliyinin dövlətdaxili və beynəlxalq hüquqi təminat mexanizmlərinin qarşılıqlı fəaliyyəti və inkişafı" adlanır və üç paraqrafdan ibarətdir.

Birinci paraqraf "İnformasiya təhlükəsizliyinin dövlətdaxili müdafiə mexanizmləri" adlanır və özündə iki yarımparaqrafı əhatə edir. Bu paraqrafda informasiya təhlükəsizliyini təmin edən normativ hüquqi bazanın vəziyyəti, qloballaşan dünyada informasiya təhlükəsizliyinin təmin olunmasında milli qanunvericiliyin tətbiqi problemləri təhlil edilir.

AR-də informasiya təhlükəsizliyinin təmin edilməsi ilə birbaşa və ya dolayı bağlı olan normalar müxtəlif iyerarxik səviyyədə dayanan normativ hüquqi aktlarla müəyyən edilmişdir.

İnformasiya təhlükəsizliyinin təmin edilməsi barədə vahid kodifikasiya edilmiş normativ hüquqi akt olmasa da, bir çox qanunvericilik aktları birbaşa və ya dolayı yolla informasiya təhlükəsizliyinin təmin edilməsinə yönələn normaları özündə əks etdirir.

Qloballaşma prosesi, bu proses çərçivəsində həyata keçirilən fəaliyyət, qloballaşma elementləri informasiya təhlükəsizliyinə göstərdiyi əhəmiyyətli təsiri ilə seçilir. İnformasiya təhlükəsizliyi sahəsində qloballaşma vahid kiberməkanda informasiya təhlükəsizliyi tədbirlərinin görülməsi və qlobal müdafiə

mexanizmlərinin formalaşdırılmasını özündə əks etdirir. Qloballaşma nəticəsində vahid kiberməkan insan hüquqlarına yeni yanaşmalar müəyyən etməklə bərabər, həm də qeyd edilməlidir ki, burada insan hüquqlarına aid olan ümumi başlanğıc prinsiplərə toxunula bilməz.

Qloballaşma mövcud hüquq münasibətlərinin mürəkkəbləşməsi halı ilə nəticələnsə də, hətta müəyyən mənfi təsirləri olsa da, bir çox müsbət təsirləri ilə də fərqlənir. Belə ki, qloballaşma insanların həyat səviyyyəsinin yüksəlməsi, mövcud tətbiq edilən standartların inkişaf etdirilməsi və yüksəldilməsi və xalqın rifahının artırılması istiqamətində işlərin daha sıx görülməsinin zəruriliyində öz müsbət təsirini göstərir.

"İnformasiya təhlükəsizliyinin beynəlxalq hüquqi müdafiə mexanizmləri" adlanan **ikinci paraqraf** özündə iki yarımparaqrafı əhatə edir. Bu paraqrafda informasiya təhlükəsizliyi nöqteyi-nəzərindən informasiya münasibətlərinin beynəlxalq-hüquqi tənzimlənməsi, dövlətin informasiya təhlükəsizliyinin təmin olunmasının beynəlxalq-hüquqi problemləri təhlil edilir.

İnformasiya təhlükəsizliyi baxımından informasiya münasibətlərinin beynəlxalq hüquqi tənzimlənməsi qloballaşan dünyada məlumatın məxfiliyini, bütövlüyünü və əlçatanlığını qorumaq üçün nəzərdə tutulmuş və bu sahədə olan münasibətləri tənzimləyən beynəlxalq hüququn mənbələrini, beynəlxalq qaydalar və standartları əhatə edir. İnformasiya təhlükəsizliyi baxımından informasiya münasibətlərinin beynəlxalq hüquqi tənzimlənməsi çoxşaxəli hüquqi, texniki və siyasi mülahizələrə toxunan mürəkkəb məsələdir. İnformasiya hüquq münasibətləri kontekstində informasiya təhlükəsizliyi sahəsində tənzimedici beynəlxalq normaların qəbul edilməsi qlobal məkanda informasiya təhlükəsizliyinin təmin edilməsi sahəsində əməkdaşlıq, habelə minimum standartların müəyyən edilməsi baxımından zəruridir. İnformasya üçün qəbul edilmiş əsas beynəlxalq hüquqi çərçivə normalarının tətbiqi informasiya təhülkəsizliyi sahəsində riskləri minimuma endirməyə istiqamətlənmişdir. İnformasiya təhlükəsizliyi baxımından informasiya münasibətlərinin beynəlxalq-hüquqi tənzimlənməsi mürəkkəb və sürətlə inkişaf edən bir sahədir və gələcək illərdə də texnoloji, siyasi və sosial inkişaflarla

formalaşmağa davam edəcəkdir. İnformasiya təhlükəsizliyinin təmin edilməsində bəzi beynəlxalq aktların birbaşa, bəzilərinin isə dolayı təsiri mövcuddur. Əvvəla onu qeyd etmək lazımdır ki, informasiya təhükəsizliyi əsas insan hüquq və azadlıqları ilə sıx bağlıdır. Odur ki, həmçinin insan hüquq və azadlıqlarını müəyyən edən beynəlxalq aktlar da informasiya təhlükəsizliyinin tənzimlənməsində rol oynayır.

"İnformasiya təhlükəsizliyinin təmin olunmasında ayrı-ayrı dövlətlərin təcrübələri" adlı **üçüncü paraqraf** da özündə iki yarımparaqrafı əhatə edir. Bu paraqrafda informasiya təhlükəsizliyinin normativ-hüquqi təminatında xarici dövlətlərin təcrübələri və beynəlxalq informasiya təhlükəsizliyi sferasında dövlətlərin əməkdaşlığının əhəmiyyəti təhlil edilir.

İnformasiya təhlükəsizliyi sferasında digər dövlətlərin qanunvericiliyinin təhlil edilməsi normativ bazanın inkişaf etdirilməsi istiqamətində olduqca səmərəlidir. Demək olar ki, böyük bir qisim dövlətlər informasiya təhlükəsizliyinə dair qanunvericilik bazasının formalaşdırılmasına başlamışdır. İnformasiya hüquq münasibətlərinin inkişaf səviyyəsi çox yüksək olan dövlətlər isə demək olar ki, informasiya təhlükəsizliyinin təmin edilməsinə yönələn qanunvericlik fəaliyyətini yüksək səviyyədə həyata keçirmiş, hazırda da buna davam edirlər. Bu paraqrafda ABŞ, Sinqapur, Cənubi Kareya, Çin, Yaponiya, Polşa, Ukrayna, Türkiyə və s. kimi dövlətlərin təcrübələri təhlil edilmişdir.

Beynəlxalq təhlükəsizliyin təmin edilməsi və bu sahədə əməkdaşlığın həyata keçirilməsi, habelə bu istiqamətdə hər bir dövlətin öz öhdəsinə düşən vəzifələri həyata keçirməsi müasir dövrün əsas məsələlərindən biri kimi çıxış edir. Əvvəla bunun səbəbi dövlətlərin ortaq maraqlarına uyğun gəlməsidir. Belə ki, beynəlxalq səviyyədə təhlükə yaradan subyektlərin ictimai təhlükəli olmaqla birdən çox ölkənin sosial, iqtisadi və ya siyasi və s. sferada olan gündəlik fəaliyyətə ziyan vurulması ilə nəticələnir. Bu da müxtəlif sferalarda törədilə biləcək hadisələrin qarşısının alınması məqsədi ilə birgə əməkdaşlığı zəruri edir. Bu həmçinin özünü regional və ya universal əməkdaşlıq səviyyəsində daha da geniş formada göstərə bilir. Beynəlxalq təhlükəsizlik sistematik və struktural xarakteri nəzərə alındıqda müasir dövrdə tam hərtəfərəfli bir neçə alternativi özündə

ehtiva edən təhlükəsizlik sisteminin hazırlanması məsələsini gündəmə gətirir.

Dissertasiyanın nəticə hissəsində tədqiqatın yekunu olaraq əldə edilmiş nəticələr 15 bənddə müəyyən edilmişdir:

1. 27 may 2022-ci ildə "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" 3 aprel 1998-ci il tarixli AR Qanununa edilən dəyişikliyə əsasən, informasiya təhlükəsizliyinə anlayış verilmişdir. Lakin qeyd edilən anlayış tamlıq, konfidensiallıq və əlçatanlıqla yanaşı mötəbərlik əlamətini də özündə ehtiva edir. Nəzərə alsaq ki, dünya praktikasında yalnız 3 element (CIA) əsas götürülmüşdür və tamlıq eyni zamanda mötəbərliyi də əhatə edir (tam - dəqiq, aktual, bütöv, səlis informasiya hər bir halda mötəbər olur). Bu baxımdan hesab etmək olar ki, mötəbərlik elementi əsaslı fərq olmadan təkrarlıq yaradır.

2. İnformasiya təhlükəsizliyinin təminatı qlobal informasiya cəmiyyətinin qurulduğu müasir dövrdə daha çox aktuallaşmışdır. Ona görə də bu sahədə bir çox beynəlxalq-hüquqi mənbələr qəbul edilmişdir. Dövlətdaxili hüquqda informasiya təhlükəsizliyinin hüquqi problemlərinin həlli zamanı həmin beynəlxalq-hüquqi mənbələrin nəzərə alınması və rəhbər tutulması vacibdir. Eyni zamanda, informasiya təhlükəsizliyinin təminatı üzrə inkişaf etmiş xarici dövlətlərin təcrübəsinin öyrənilməsi və respublikamızda tətbiqi də əlverişli hesab olunur. Həmçinin, onu da qeyd etməliyik ki, informasiya təhlükəsizliyi dinamik inkişaf edən istiqamət olduğu üçün İKT-nin sürətlə inkişafı ilə əlaqədar olaraq, hər gün müxtəlif termin və anlayışlar meydana gəlir. Məhz belə anlayışlara beynəlxalq səviyyədə hüquqi izahın verilməsi çox vacibdir. Çünki bütün dünya dövlətləri öz milli qanunvericiliyinin formalaşdırılması zamanı beynəlxalq normalara istinad edirlər. Hesab etsək ki, son dövrlər artıq bütün dünya süni intellekt, robotlar, elektron şəxsiyyət, ağıllı əşyalar, sürücüsüz avtomobil anlayışından istifadə edir. Bu anlayışların qanunvericilikdə təsbiti və onlardan istifadə mexanizmlərinin tənzimlənməsinə artıq ehtiyac yaranır.

3. İnformasiya təhlükəsizliyinin obyektlərini dövlətin, cəmiyyətin və şəxsiyyətin informasiya təhlükəsizliyinin təminatı ilə bağlı problemlər təşkil edir. Dövlətin informasiya təhlükəsizliyi –

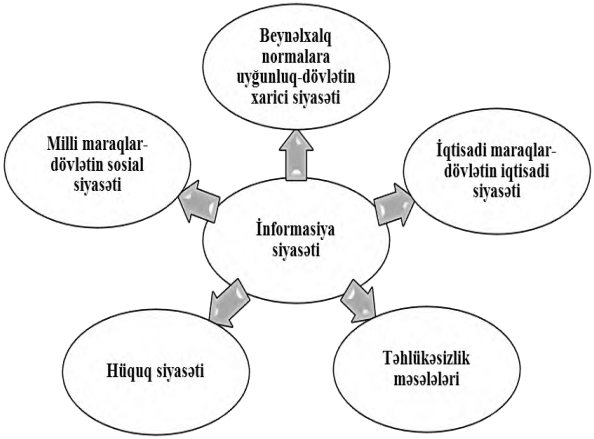
onun milli təhlükəsizliyinin, konstitusion quruluşunun, ərazi bütövlüyünün və suverenliyinin qorunmasına, cəmiyyətin informasiya təhlükəsizliyi – onun maddi və mənəvi rifahının qorunmasına, şəxsiyyətin informasiya təhlükəsizliyi isə – insan hüquq və azadlıqlarının qorunmasına xidmət edir. Hər bir obyektin informasiya təhlükəsizliyinin təminatı üzrə hüquqi problemlərin həlli özünəməxsus istiqamətdə aparılır. Belə ki, dövlətin informasiya təhlükəsizliyi üzrə qarşıya çıxan problemlərdən biri elektron məlumatların saxlanması üçün istifadə olunan mikrosxemlərin və digər daşıyıcıların yerli istehsalının olmamasında özünü biruzə verir. Bu isə xarici dövlətlərdən idxal olunan həmin daşıyıcılara istehsalçı və ya başqa dövlətlər tərəfindən nəzarət olunmasını istisna etmir. Qeyd olunan problem AR-də dövlət sirrini təşkil edən məlumatların başqa dövlətlərə ötürülməsinə, müxtəlif informasiya hücumlarına, nəticə etibarilə dövlət təhlükəsizliyinə zərər vurulmasına gətirib çıxara bilər. 27 may 2022-ci ildə "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" 3 aprel 1998-ci il tarixli AR Qanununa edilən dəyişikliyə əsasən kritik informasiya strukturuna, onun obyektinə, subyektinə və bu informasiya strukturunun təhlükəsizliyini təmin edən səlahiyyətli orqana anlayış verilmişdir. Eyni zamanda 27 may 2022-ci ildə İnzibati Xətalar Məcəlləsinə bu qaydaların pozulması halları ilə bağlı inzibatı xəta və inzibati məsuliyyət növü nəzərdə tutulmuşdur. Məsələnin dövlətin təhlükəsizliyi baxımından aktuallığını nəzərə alaraq hesab etmək olar ki, kritik informasiya strukturuna məxsus olan obyektərdən informasiya məlumatlarının götürülməsi əməlin ictimai təhlükəliliyi baxımından eyni zamanda cinayət hesab edilməli və Cinayət Məcəlləsinin dövlətin konstitusiya quruluşunun əsasları və təhlükəsizliyi əleyhinə olan cinayətlər fəslində nəzərdə tutulmalıdır.

4. Dövlətin milli informasiya siyasətinin istiqamətləri sırasında informasiya təhlükəsizliyinin təminatı qeyd olunmalıdır. UNESCO-nun İnformasiya hamı üçün (İnformation for All) Proqramı Milli İnformasiya Cəmiyyəti Siyasətində (MİCS) beş prioritet istiqaməti müəyyənləşdirir: İnformasiya inkişaf üçün; İnformasiya mədəniyyəti; İnformasiyanın saxlanması; İnformasiya etikası; İnformasiya əlyetərliyi.

Milli informasiya siyasəti bütövlükdə cəmiyyət üçün informasiyanın əlyetərliyinin təminatına yönəlmiş tədbirlər və qaydalar sistemini özündə birləşdirir və 2 yerə bölünür: informasiya strategiyası və informasiya taktikası.

İnformasiya strategiyası böyükhəcmli informasiya problemlərinin həllinə yönəlmiş planlı fəaliyyət modelidir ki, bu model nəticə etibarilə informasiyalaşdırma proseslərinin uğurla başa çatmasına və informasiya hüquq və azadlıqlarının maneəsiz təminatına yönəlmişdir. İnformasiya taktikası isə informasiya strategiyasının əsasında formalaşır, qarşıya qoyulan məqsəd və vəzifələrə çatmaq üçün icra olunan konkret tədbirləri əhatə edir. Bu o deməkdir ki, informasiya strategiyası "nə" və "niyə" suallarını cavablandırırsa, informasiya taktikası "necə" sualına cavab verir. Strategiyadan fərqli olaraq, informasiya taktikası çevikliyi ilə xarakterizə olunur.

Milli informasiya siyasətinin həyata keçirilməsi dövlətin fəaliyyətinin digər aspektləri nəzərə alınmadan qeyri-mümkündür. Belə ki, iqtisadi baxımdan səmərəsiz bir şəraitdə informasiyalaşdırma və elektronlaşdırma proseslərindən, informasiya əlyetərliyinin təminatından danışmaq bir qədər məntiqsiz olar. Digər tərəfdən milli maraqları nəzərə almayan informasiya siyasəti uğurla icra oluna bilməz. Həmçinin beynəlxalq normalara riayət etmədən həyata keçirilən və hüquqi bazası olmayan informasiya siyasəti nəticədə maraqların toqquşmasına gətirib çıxaracaqdır. Başqa bir tərəf onda özünü büruzə verir ki, milli təhlükəsizlik qorunmadığı bir şəraitdə informasiya siyasətinin normal icrasına nail olmaq mümkünsüzdür.



Yuxarıdakı sxemi nəzərə almaqla belə qənaətə gəlmək olar ki, milli informasiya siyasəti dedikdə, dövlət orqanları tərəfindən həyata keçirilən kompleks tədbirlər sistemi başa düşülür. Milli informasiya siyasətinin yalnız dövlət hakimiyyət orqanlarında cəmləşməsi insan hüquq və azadlıqlarının məhdudlaşdırılması anlamına gələ bilməz. Əslində, hüquq və azadlıqların təminatı, hüquq pozuntularının qarşısının alınması və s. bu kimi vəzifələrin icrası üçün dövlət hər bir zaman idarəedici təsisat olaraq mövcud olmuşdur. Hüquqi dövlət ideyasının geniş vüsət aldığı bir dövrdə dövlətin rolu olmadan qarşıya qoyulan məqsədlərə nail olmaq mümkün deyildir. Təbii ki, dövlət orqanlarının özünün də fəaliyyətinə nəzarət olunması vacib faktorlardan sayılır. Məhz ona görə də hüquqi dövlətin əsas prinsiplərindən biri kimi - qarşılıqlı məsuliyyət, yəni şəxsin dövlət qarşısında və dövlətin şəxs qarşısında məsuliyyəti- hər zaman rəhbər tutulur. Bununla yanaşı, açıq hökumət, ictimai nəzarət, vətəndaş cəmiyyəti və digər ideyaların ön plana çəkilməsi dövlətin milli informasiya siyasətinin həyata keçirilməsinə mühüm təsirini göstərir. Fikrimizi ümumiləşdirərək belə qənaətə gəlmək olar ki, dövlətin milli informasiya siyəsəti təktərəfli deyil, kompleks tədbirlər çərçivəsində əlaqəli şəkildə həyata keçirilməlidir.

5. Şəxsiyyətin informasiya təhlükəsizliyinə gəldikdə isə, müasir informasiya cəmiyyətində insan faktoru ön plana çəkildiyi üçün şəxsiyyətə qarşı yönəlmiş informasiya təhdidlərinin qarşısının alınmasına da xüsusi diqqət yetirilir. Respublikamızda Xüsusi Rabitə

və İnformasiya Təhlükəsizliyi Dövlət Xidmətinin Kompüter İnsidentlərinə Qarşı Mübarizə Mərkəzi, AR Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi yanında Elektron Təhlükəsizlik Xidməti və sair qurumların fəaliyyət göstərməsinə baxmayaraq, kompüter insidentlərinin sayı günbəgün artmaqda davam edir. Hətta, artıq əksər cinayətlərin törədilməsində İKT bir alət, vasitəyə çevrildiyinə görə, bütün bunlar informasiyanın tamlığının, əlyetərliyinin və konfidensiallığının pozulmasına gətirib çıxarır. Şəbəkədən istifadə etməklə, şəxsin istənilən məlumatı əldə etməklə, onun istənilən hüquq və azadlığına qəsd etmək olur. Bütün bunlar şəxsiyyətə yönələn qəsdlərə bir daha hüquqi cəhətdən hərtərəfli yanaşılmanı, bir çox qanunvericilik aktlarında bununla bağlı dəyişiklik və düzəlişlər edilməsini tələb edir. Qeyd olunan məsələ ilə bağlı bütün həll yollarının tapılmasının yalnız qanunvericinin üzərinə qoyulması isə düzgün deyildir. Ona görə də informasiya təhlükəsizliyi sahəsində, eləcə də ümumilikdə informasiya hüququ sahəsində elmi tədqiqatların sayının artırılması, təkliflərin işlənib hazırlanması və qanunverici orqana təqdim olunması məqsədəmüvafiqdir. Bundan əlavə, virtual mühitdə baş verən hüquq pozuntularının əksər hallarda subyektini müəyyənləşdirmək olmur. Müxtəlif saxta profillərdən istifadə etməklə, şəxsiyyətə qarşı yönəlmiş bir sıra əməlləri (təhqir, böhtan və s.) icra etmək olur. Lakin məsuliyyət məsələsinə gəldikdə, provayderlərin məhdud məsuliyyətinin olması pozuntunun subyektinin müəyyən olunmasında bir sıra problemlər yaradır. Digər tərəfdən isə, şəxsiyyətə qəsd edən müxtəlif informasiya təhdidlərinin həyata keçirilmə vaxtını və ardıcıllığını təyin etmək olduqca çətindir. Bu o deməkdir ki, belə təhlükələrin latentlik səviyyəsi yüksəkdir. Sadalanan bu kimi problemlərin aradan qaldırılması üçün İnformasiya Məcəlləsinin qəbul olunması və ya bu sahədə olan qanunvericilik aktlarına yenidən baxılması daha məqsədəuyğun hesab olunur.

6. Fərdi məlumatların istifadəsi ilə bağlı münasibətlərin hüquqi tənzimlənməsi məqsədi ilə AR-də müxtəlif normativ hüquqi aktlar qəbul edilmişdir. Qeyd edilməlidir ki, “Fərdi məlumatlar haqqında” AR Qanununda verilmiş anlayışa əsasən məlumatların xarakterini müəyyən etmək mümkündür. Belə ki, AR-in qanunvericiliyinin

tələblərinə əsasən məlumatın fərdi məlumat kateqoriyasına aid edilməsi üçün aşağıda qeyd olunan əlamətlərdən birinə malik olmalıdır: şəxsin kimliyini birbaşa müəyyənləşdirməyə imkan verməlidir; şəxsin kimliyini dolayısı ilə müəyyənləşdirməyə imkan verməlidir. Qanunvericiliyimizdə fərdi məlumatlara verilən anlayışı mövcud hüquq münasibətlərinin cəmiyyətimiz üçün yeni xarakter daşımasını nəzərə alaraq uğurlu hesab etmək olar. Lakin fərdi məlumatlara qanunvericiliyimizdə daha geniş və onun təbiətini tam açan anlayış verilməsi daha məqsədəmüvafiq olardı. Odur ki, bu sahədə beynəlxalq müqavilələr, o cümlədən xarici ölkələrin praktikasında müəyyən normativ hüquqi aktlar dissertasiyada nəzərdən keçirilmişdir. Həmin aktlar və ədəbiyyatda olan mövcud anlayışların müqayisəli təhlili və cəmiyyətimizin özünəməxsus xüsusiyyətləri nəzərə alınmaqla qanunvericiliyə dəyişikliklər edilməsi məqsədəmüvafiqdir. Məsələn, AR-in də tərəfdar çıxdığı Fərdi məlumatların avtomatlaşdırılmış qaydada işlənməsi ilə əlaqədar şəxslərin qorunması haqqında 1981-ci il tarixli Avropa Konvensiyasında da fərdi məlumatlara anlayış verilmişdir.

7. Qeyd olunan konvensiyada müəyyən edilmiş yanaşma daha da ümumi olmaqla müəyyən və ya müəyyən edilə bilən fərdə aid istənilən məlumatı fərdi məlumat kateqoriyasına aid edir. Belə məlumatlara şəxsin adı, soyadı, atasının adı, doğum tarixi, şəxsiyyəti təsdiq edən sənədlərdə olan digər məlumatlar, habelə irqi, etnik mənşə, ailə həyatı, dini etiqad, əqidə, sağlamlıq və ya məhkumluq barədə məlumatlar da aid edilə bilər. Amma belə detallar "Fərdi məlumatların mühafizəsi haqqında" AR Qanununda açıqlanmır. Bu sahədə yaranan hüquq münasibətlərində qeyri-müəyyənliklərin və hüquqi mübahisələrin qarşısını almaq üçün anlayışı daha geniş şəkildə müəyyən etmək olar. Mövcud praktika təhlil edildikdə müəyyən olunur ki, anlayışın belə ümumi şəkildə verilməsi məlumatlar kateqoriyasının təfsir məsələsini gündəmə gətirəcəkdir. Bu isə peşəkarların, hüquqşünas, hakim və ya digər vəzifəli şəxslərin subyektiv yanaşmasında çətinliklər yarada, o cümlədən vətəndaşların vəziyyətinin çətinləşməsi ilə nəticələnə bilər. Bu baxımdan hesab edirik ki, şəxsin kimliyini birbaşa və dolayı yolla müəyyənləşdirməyə imkan verən məlumatlar kateqoriyası

Konvensiyada olduğu kimi sadalanmalıdır ki, bu da gələcəkdə fərdi məlumatların toxunulmazlığı ilə bağlı mübahisəli məsələnin həll edilməsində fərqli yanaşmaların qarşısını alacaqdır.

8. E-dövlətin ən çox inkişaf edən istiqaməti icraedici orqanın elektronlaşdırılmasında özünü biruzə verir. Müxtəlif saytlar vasitəsilə vətəndaşa təqdim olunan elektron xidmətlər onun hüquq və azadlıqlarını sərbəst və maneəsiz reallaşdırması üçün geniş imkanlar açır. Lakin üstün cəhətlərlə yanaşı, bu sistemdə də bəzi problemlər mövcuddur. Məsələn, Elektron Hökumət Portalından qeydiyyatdan keçmək üçün şəxsin adına mobil nömrənin olması və şəxsiyyətini eyniləşdirməyə əsas verən sənədlərin olması əsas şərtdir. Məsələ burasındadır ki, qeydiyyat üçün ən azı üç əsas sənədin mövcudluğu tələb olunur. Fikrimizcə, bu tələblərin sayının azaldılması daha məqsədəuyğundur. Çünki bir çox vətəndaşlarda xarici pasport, DSMF kartı və ya sürücülük vəsiqəsi olmur. Ona görə də sistemdə qeydiyyatdan keçmək üçün yalnız mobil nömrə və şəxsiyyət vəsiqəsinin tələb kimi qoyulması daha əlyetərli ola bilər. Bu yolla təqdim olunan elektron xidmətdən istifadə daha asan və əlyetər olacaqdır. Yeni dəyişikliklə üçlü sənədə alternativ kimi video qeydiyyat əlavə edilmişdir, lakin bu zaman da video müraciətin nəticəsi 5 iş günü ərzində yoxlanılır və təsdiq olunduqdan sonra hesab aktivləşir, bu isə artıq vaxt itkisinə səbəb olur ki, əslində elektron dövlətin təməl ideyasına ziddir. Hesab edirik ki, yalnız FİN və mobil nömrə ilə qeydiyyat yetərlidir.

9. Kibertəhlükələrin qarşısının alınması üzrə ümumi tədbirlər isə dövlət tərəfindən həyata keçirilir. Birinci növbədə, müxtəlif pozuntulara görə məsuliyyətin müəyyən olunması və sanksiyaların təyin edilməsi qeyd olunmalıdır. Ənənəvi olaraq, hüquq pozuntularının xarakterindən asılı olaraq dörd növ – cinayət, inzibati, mülki və intizam məsuliyyəti fərqləndirilir. Lakin müasir dövrdə beynəlxalq-hüquqi məsuliyyət, konstitusiya-hüquqi məsuliyyət kimi anlayışlara da rast gəlinir. İnformasiya hüquqi məsuliyyətin hansı növə aid olması və necə tənzimlənməsi bu zaman aktuallıq kəsb edir. Məsələ burasındadır ki, informasiya sahəsində münasibətlərin realizəsi zamanı törədilən hüquq pozuntularına görə sanksiyalar informasiya qanunvericilik aktlarında təsbit olunmamışdır. İctimai təhlükəli olan

informasiya-hüquq pozuntuları cinayət qanunvericiliyində, inzibati xətanın əlamətləri ilə səciyyələnən pozuntular inzibati qanunvericilikdə, müxtəlif deliktlər mülki qanunvericilikdə nəzərdə tutulmuşdur və s. Lakin informasiya sahəsinin sərhədsiz olmasını, informasiya-hüquq pozuntuları ilə bağlı problemlərin və kolliziyaların mövcudluğunu nəzərə alsaq, həmin problemlərin cinayət, mülki və inzibati hüquq sahələri üzrə şərhi mümkün deyildir. Məsələn, kibertəhlükələr, informasiya təhdidləri nəinki konkret vətəndaşa qarşı yönəlir, hətta cəmiyyətin mənəviyyatına mənfi təsir göstərir. Belə təhlükələrin qarşısının alınması üzrə təklif və tövsiyələrin işlənməsi isə yalnız informasiya hüquq elmi çərçivəsində mümkün ola bilər. Bütün bunları rəhbər tutaraq, informasiya-hüquqi məsuliyyətin müstəqil bir hüquq institutu kimi təhlilini məqsədəmüvafiq hesab etmək olar.

10. Cəmiyyətin bütün sferalarının qloballaşması, kiberməkanın formalaşması daha asan və çevik yolla informasiya hüquq pozuntusunun törədilməsinə imkan yaradır. Müasir dövrün ən aktual problemlərindən olan kibertəhlükələrlə mübarizə dünya miqyasında həyata keçirilir. Elektron informasiya sistemlərində olan hər hansı bir boşluq və ya çatışmazlıq nəticə etibarilə bütün məlumatların məhvinə gətirib çıxarır. Ona görə də həm beynəlxaq, həm də milli səviyyədə e-dövlətin informasiya təhlükəsizliyi dövlətin informasiya siyasətinin əsas istiqamətlərindən biri kimi ön plana çəkilməlidir. İnformasiya təhlükəsizliyi elektron təhlükəsizlikdən daha geniş anlayış olduğu üçün e-idarəetmədə elektron təhlükəsizliyin təminatı informasiyanın tamlığının, əlyetərliyinin və gizliliyinin təmin olunmasına xidmət edir. Ona görə də e-dövlətin yaratdığı imkanlardan istifadə edən sadə vətəndaş əmin olmalıdır ki, onun hüquq və azadlıqları qorunur və o, cinayətkar qəsdlərə məruz qalmayacaqdır. Sərhədləri bilinməyən bir məkanda cinayətkarın axtarılması son dərəcə çətin olduğu üçün həm milli səviyyədə, həm də beynəlxalq səviyyədə kibermühitdə törədilən cinayətlərə "həssaslıqla" yanaşılmanı tələb edir. Hətta, onu deyə bilərik ki, kibercinayətlər ənənəvi üsulla törədilən cinayətlə müqayisədə daha ağır nəticələrə səbəb olur. Bu baxımdan, kibertəhlükələrin qarşısının alınması üzrə əməkdaşlıq prinsipi rəhbər tutulmalıdır. Bu, iki istiqamətdə aparılsa, daha operativ nəticələr əldə etmək olar: dövlətlərin əməkdaşlığı – beynəlxalq səviyyədə və

vətəndaşla dövlət orqanlarının əməkdaşlığı – milli səviyyədə. İKT-nin sürətlə inkişaf etdiyi bir dövrdə ənənəvi cinayətlərin də İKT-dən istifadə edilməklə törədilməsinə daha çox üstünlük verilir. Bu günkü dövrdə şəxsin üzərinə silah çəkməklə pulunu almağa gərək yoxdur, texnologiyanın köməyilə daha asan yollarla (kiberdələduzluq və s.) varlanmaq olur. Hətta, məsafədən virtual aləmdə insanı özünü öldürmə həddinə çatdırmaq belə mümkündür. Ona görə də kibertəhükələrlə bağlı hüquqi mənbələrdə "kibercinayət" anlayışına yenidən baxılmasını məqsədəmüvafiq hesab edirik. Bu zaman nəzəri ədəbiyyatda kibercinayətlərin müxtəlif təsnifatlarından istifadə etmək olar. Belə ki, AR-in də qoşulduğu Kibercinayətkarlıq haqqında 2001-ci il tarixli Konvensiyada təsbit olunmuş ayrı-ayrı kateqoriyalar üzrə cinayətlərdən AR Cinayət Məcəlləsinə 2012-ci il 29 iyun tarixində 30-cu fəsil yeni redaksiyada verilərək, yalnızca kompüter sisteminə daxil olma (maddə 271), kompüter məlumatlarını qanunsuz ələ keçirmə (maddə 272), kompüter sisteminə və kompüter məlumatlarına qanunsuz müdaxilə (maddə 273), kibercinayətlərin törədilməsi üçün hazırlanmış vasitələrin dövriyyəsi (maddə 273-1), kompüter məlumatlarının saxtalaşdırılması (maddə 273-2) təsbit edilmişdir. Lakin nə kompüter texnologiyalarından istifadə etməklə dələduzluq, məlumatların məzmunu ilə bağlı cinayətlər (uşaq pornoqrafiyası ilə bağlı cinayət), müəllif hüquqlarının və əlaqəli hüquqların pozulması ilə bağlı, nə də ki, ictimai təhlükəsizlik və təcavüzlə bağlı olan cinayətlər (bu kateqoriyaya kiberterrorizm və terror məqsədləri ilə kiberməkandan istifadə olunması kimi cinayətlər daxildir) Cinayət Məcəlləsində təsbit edilməmişdir. Nəzərə almaq lazımdır ki, elektron dövlətdə mövcud cinayətlər daha çox elektron mühitdə baş verdiyindən əslində yuxarıda sadaladığımız cinayətlərin AR Cinayət Məcəlləsində eyni maddə daxilində ayrıca bənd şəklində təsbit olunması olduqca əhəmiyyət kəsb edir. O cümlədən qeyd etmək istərdik ki, son zamanlar virtual oyunlar, sosial şəbəkələr vasitəsilə fərdi məlumatların oğurlanması və onlardan şantaj üsulu kimi istifadə edilməsinin nəticəsi olaraq, özünü öldürmə həddinə çatdırma cinayətinin statistikasında artım müşahidə olunur. Qeyd olunan məsələlər AR Cinayət Məcəlləsinin 125-ci maddəsində tərkib elementi kimi, ya da yeni 125-1 maddəsinin əlavə edilməsini zərurətə çevirir.

11. Kibeməkanda insan hüquqlarının təminatı və müdafiəsi üçün informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması və inkişaf etdirilməsi zəruridir. İnformasiya təhlükəsizliyi mədəniyyətinin formalaşadırılması xüsusilə fərdi məlumatların mühafizəsi üzrə tədbirlərin gücləndirilməsində, kibermühitin insan psixologiyasına mənfi təsir üsullarının aradan qaldırılmasında olduqca əhəmiyyətlidir. Bu baxımdan, informasiya təhlükəsizliyinin təmin edilməsi üçün ingilis müəlliflərinin həm valideynlər, həm də uşaqlar üçün təklif etdiyi şüarlardan istifadə (məsələn, üzbəüz edə bilmədiyin hərəkəti onlayn üsulla etməyə cəhd etmə, uşaqlara internet təhlükəsizliyini erkən yaşlarından öyrətməyə çalışın və s.) və həmçinin kompüter insidentləri ilə mübarizə aparan orqanların işinin daha da gücləndirilməsi məqsədəmüvafiq hesab edilə bilər.

12. Bu gün media sahəsində sosial medianın əhəmiyyəti və rolunu nəzərə aldıqda qanunvericiliyimizdə müstəqil olaraq sosial media terminina də anlayış verilməsi daha uyğun olardı. Çünki bu gün bir çox media subyektləri, informasiya agentlikləri və media platforma sahibləri sosial media və şəbəkələrin gücündən geniş istifadə edir. Hətta bir çox media qurumlarının fəaliyyəti yalnız sosial şəbəkə platformaları üzərində qurulmuşdur. Bu istiqamətdən yanaşdıqda qeyd etmək olar ki, sosial media terminina Media haqqında Qanunda anlayış verilməsi yarana biləcək hüquq mübahisələrindəki boşluqları və anlaşılmazlıqları aradan qaldıracaqdır. O da qeyd edilməlidir ki, həmin Qanunda onlayn mediaya anlayış verilməsi təqdirəlayiq hal kimi qiymətləndirilməlidir. Qeyd olunanlara əsasən sosial mediaya belə anlayış verə bilərik: sosial media dedikdə, istifadəçilərə məzmun yaratmağa, özü və ya digər istifadəçi tərəfindən yaradılan məzmunu izləməyə, paylaşmağa, mübadilə etməyə, bəzi hallarda mövcud məzmun barədə şərh etməyə və fikir mübadiləsi aparmağa və ya ümumi şəkildə sosial şəbəkələrdə iştirak etməyə imkan verən veb əsaslı platformalar, tətbiqetmələr və texnologiyalar başa düşülür. Sosial media platformaları və ya tətbiqetmələri adətən mətn, fotoşəkillər, videolar və audio yazılar kimi məzmunun yaradılması və paylaşılmasını asanlaşdırmaq üçün internet və mobil texnologiyalardan istifadəni nəzərdə tutur.

13. İnformasiya təhlükəsizliyi sahəsində beynəlxalq əməkdaşlığın xüsusi platformasının və ya institusional təşkilati mexanizminin formalaşdırılması informasiya təhlükəsizliyinin, daha geniş spektrdə isə beynəlxalq və milli təhlükəsizliyin təmin edilməsinin əlaqələndirilməsi baxımından məqsədəmüvafiq olardı. Həmin beynəlxalq platforma və ya təşkilat çərçivəsində beynəlxalq normativ aktların qəbul edilməsi, habelə, hökumətlərarası universal icra mexanizmlərinin formalaşdırılması və s. olduqca zəruridir. Digər tərəfdən kibercinayətlərin özünəməxsusluğu, spesifikliyi onun istintaqı və ya bu əməllərə görə məsuliyyət prosesində də çətinliklərin yaranmasına səbəb olur. Bu zaman təklif edilən universal platforma və ya beynəlxalq təşkilat çərçivəsində əməkdaşlıq bu sahədə təcrübə və hüquqi yardımın göstərilməsi ilə istintaq və sübutların toplanılması prosesini də asanlaşdırar, qeyd edilən sahədə dövlətlərarası əməkdaşlığı səmərəli etməklə, nəhayət kibercinayətkarlıqla mübarizənin yüksək səviyyəsinə nail oluna bilər.

14. Qloballaşan dünyanın əsas vasitələrindən və insanların gündəlik həyatının bir parçasına çevrilən internet platformalarından istifadə etməklə informasiya təhlükəsizliyi üzrə maarifləndirici materialların yayılmasını təmin etməklə hüquqi maarifləndirmənin həyata keçirilməsi beynəlxalq səviyyədə informasiya təhlükəsizliyinin təmin edilməsinə öz müsbət töhfəsini verir. Bunun səmərəli həyata keçirilməsi üçün qlobal internet və ya sosial şəbəkə platformalarının sahibləri iş prosesinə cəlb edilə, sosial (ictimai) məsuliyyət tədbirləri qismində bu cür maarifləndirici materialların daha geniş kütləyə çatmasını təmin etmək olar. Bütün bu tədbirlərin həyata keçirilməsi isə qlobal informasiya cəmiyyəti subyektlərinin hüquq düşüncələrinin inkişafına, universal informasiya təhlükəsizliyi mədəniyyətinin formalaşması və inkişafına səbəb olar.

15. İnformasiya təhlükəsizliyi sahəsində artan kibercinayətkarlıq və ictimai təhlükəli əməllərlə mübarizə məqsədi ilə səmərəli regional hüquqi mexanizmlərin qurulması informasiya təhlükəsizliyi risklərinin azaldılmasına müsbət töhvəsini vermiş olardı. Region ölkələrinin oxşar tarixi, mədəni və hüquqi düşüncəsi belə mexanizmlərin daha faydalı olmasının göstəricisi kimi qəbul edilə bilər. Oxşar sosial, iqtisadi və hüquq sistemlərinin xüsusiyyətləri nəzərə alınmaqla qəbul edilən

regional beynəlxalq müqavilələr isə informasiya təhlükəsizliyinin daha yaxşı tənzimlənməsinə əsas olur. Habelə regional müdafiə mexanizmi kimi müxtəlif təşkilat və ya institutlar çərçivəsində əməkdaşlıqla, kibercinayətkarlıqla mübarizə, informasiya təhlükəsizliyini tənzimləyən normativ hüquqi bazanın inkişaf etdirilməsilə, öz müsbət nəticələrini praktikada təcəssüm etdirmiş təcrübə mübadiləsi, mövcud sahədə fəaliyyət göstərən kadr potensialının və insan kapitalının inkişaf etdirilməsilə, habelə akademik və sosial tədqiqat sahəsində birgə fəaliyyət nəticəsində dövlətlərin rastlaşdığı bir çox hüquqi və təcrübi problemlərin səmərəli şəkildə həllini tapmasına nail olmaq mümkündür.

Dissertasiyanın əsas müddəaları iddiaçının aşağıdakı elmi əsərlərində öz əksini tapmışdır:

1. Информационное общество и глобализация: тенденции развития информационного общества и правовые реформы в Азербайджанской Республике / Рзаева Г.А // Юридична наука і практика: пошук правової гармонії: збірник матеріалів Міжнародної юридичної науково-практичної конференції «Актуальна юриспруденція», - Киев, - 2017, - с.65-69
2. Fərdi məlumatların müdafiəsində informasiya təhlükəsizliyinin rolu // M.N.Ələsgərovun 90 illik yubileyinə həsr olunmuş "Azərbaycanda hüquq elminin müasir inkişaf istiqamətləri və tendensiyaları" mövzusunda beynəlxalq elmi-praktik konfrans, - Bakı, - 2018, - s.197-201
3. İnformasiya mədəniyyətinin informasiya təhlükəsizliyində rolu // BDU Hüquq fakültəsinin 90 illik yubileyinə həsr olunmuş "Azərbaycan Respublikasının Beynəlxalq cəmiyyətə inteqrasiyası və hüquqi dövlət quruculuğunda hüquq elminin müasir inkişaf tendensiyaları" mövzusunda beynəlxalq elmi-praktik konfrans. - Bakı, - 2018, - s. 53-56
4. Информационная безопасность: проблема неприкосновенности личностных прав / Алиев А.И., Рзаева Г.А // Міжнародний журнал право і суспільство, - Івано-Франківськ, -2018, № 7. - с. 5-24
5. Основные тенденции развития информационной сферы: отрасль публичного, или частного права? / Рзаева Г.А // Министерство образования и науки Украины Национальный авиационный університет, VIII Международной научно-

практической конференции «Современное университетское правовое образование и наука» - Киев, - 2018, - с.117-121
6. Понятие информации, ее социальная, правовая природа и специфические особенности / Алиев А.И., Рзаева Г.А // - LUBLIN: Fundacja “Ośrodek Rozwoju Kompetencji Akademickich” area nauki, kwartalne międzynarodowe czasopismo naukowe, - 2019, - с.4-16,
7. Информационное общество и тенденции его развития / Рзаева Г.А // - Волгоград: Актуальная наука: международный научный журнал., - 2019, №1 (18), - с.69-75
8. Information and media rights in the information society: social and legal analysis. / Amir Aliyev, Gulnaz Rzayeva, Nigar Alakbarova // XIV international scientific and practical conference social and economic aspects of education in modern society. - Warsaw, - 2019, - p.41-49
9. Национальный опыт обеспечения информационной безопасности / Алиев А.И // X International scientific conference «juridical science innovative development in conditions of social modernization». - 2020, p.130-133
10. Cybercrimes and struggle agains them// Науковий вісник Дніпропетровського Державного Університету Внутрішніх Справ, - 2020, №2, p.151-157
11. Digital citizen and information security// Proceedings of the 7 th international conference on control and optimization with industrial applications. Baku,-2020, p.326-329
12. Digital divide as an obstacle to the formation of information society / Amir Aliyev, Gulnaz Rzayeva // Proceedings of the 7 th international conference on control and optimization with industrial applications. - Baku, - 2020, - p.107-110
13.Kibertəhlükələr və onların təsnifatı// Bakı: Bakı Univeristetinin xəbərləri sosial-siyasi elmlər seriyası. - 2020, №1, - s.5-14
14. Milli təhlükəsizlik sistemində informasiya təhlükəsizliyinin yeri.// - Bakı: Azərbaycan hüquq jurnalı, - 2020, №1, - s.48-59
15. Peşə və kommersiya sirrinin müdafiəsində informasiya təhlükəsizliyinin rolu// Umummilli Lider Heydər Əliyevin anadan olmasının 97-ci ildönümünə həsr edilmiş “Müasir dövrdə hüquq sahələrinin qarşılıqlı əlaqəsi və tətbiqi: nəzəriyyə və təcrübə mövzusunda Beynəlxalq elmi-praktik konfrans. - Bakı,-2020,-s.93-96

16. Information security: theoretical, legal and organizational challenges/ Amir Aliyev, Gulnaz Rzayeva // Journal of Information Science, - 2020, vol.8, - p.1-14
17. Meaning and position of human dignity in the constitution - theoretical and dogmatic dimensions/ Amir Aliyev, Gulnaz Rzayeva, Shahin Mammadrzalı // Global human dignity project, - 2020, - p.1-11
18. Organization of information security in e-government as means of information rights protection / Gulnaz Rzayeva // Legal Journal "Law of Ukraine". - 2020, №4, - c.225-244
19. The defintions of information and security; history of information security development // Vilnius:The future decade of the eu law, 8th international conference of phd students and young researchers, «teise» journal of Law faculty, - 2020, №.2, - p.48-58
20. Dövlətlərin fərdi məlumatların mühafizəsində öhdəlikləri; Avropa İnsan hüquqları Konvensiyasında fərdi məlumatların mühafizəsi // International conference: XXI century, new challenges and modern development tendencies of law, Baku State University Baku, - 2021, - s. 97-105
21.E-dövlətdə informasiya təhlükəsizliyinin təşkili və informasiya hüquqlarının müdafiəsi anlayışı // - Bakı: Polis Akademiyasının elmi xəbərləri elmi hüquq jurnalı.- 2021, № 2 (30), - s.96-112
22. Fərdi məlumatlar və əlaqədar hüquqlar; fərdi məlumatların mühafizəsi // - Bakı: Bakı Univeristetinin xəbərləri sosial-siyasi elmlər seriyası. - 2021, №4, - s.64-78
23. İnformasiya təhlükəsizliyi; təhlükəsizlik və informasiya anlayışı // - Bakı: Polis Akademiyasının elmi xəbərləri elmi hüquq jurnalı.- 2021, № 4 (32), - s.85-93
24. İnformasiya təhlükəsizliyində standartlar və onların əhəmiyyəti// Ulu Öndər Heydər Əliyevin anadan olmasının 98-ci ildönümünə həsr olunmuş "Heydər Əliyev və Azərbaycanın inkişaf strategiyası" adlı respublika elmi-praktiki konfrans. - Bakı, - 2021, - s.71-74
25. Şəxsi həyat və onun informasiya təhlükəsizliyi / AR DTX Heydər Əliyev adına Akademiyasının "Azərbaycan Respublikasının suverenliyinin, müstəqilliyinin və ərazi bütövlüyünün Konstitusiya əsasları" adlı Respublika elmi-praktik Konfransı. - Bakı. -2021, - s.150-159

26. Virtual məkanda kibertəhlükələr və insan hüquqlarının müdafiəsi: beynəlxalq və milli-hüquqi tənzimetmə // Gülnaz Rzayeva // - Bakı:Azərbaycan hüquq jurnalı, - 2021, №1, - s.42-65
27. Информационная безопасность в информационном обществе// XI міжнародної науково-практичної конференції XI international scientific conference «Сучасне право в епоху соціальних змін» «modern law in the era of social transformation»- Київ, -2021, - с.96-99
28. Понятие персональных данных; информационная безопасность права на неприкосновенность частной жизни согласно анализу статьи 8 Европейской конвенции по правам человека// Северо-кавказский юридический вестник научно-практический журнал, - 2021, №4, - с.92-104
29. Information rights and information security in the context of fair trial / Amir Aliyev, Gulnaz Rzayeva // International Asian congress on contemporary, 2021, p.124-167
30. Artificial intelligence and personal data: international and national framework / Amir Aliyev, Gulnaz Rzayeva // International conference "Data-driven human rights research" University of Padova, -2021, - p.97-123
31. Information security and influencing factors // Право Украини, юридический журнал.- 2021, №4, - с.234-244
32. The factor of the risk and risk management in information security //«Вестник КазНУ. Серия юридическая», Казахский национальный университет имени аль-Фараби, - 2021, №4 (100), - с.97-106
33. The impact of new technologies on human rights in the context of the right to be forgotten and the right to privacy / Gulnaz Rzayeva // Legal Journal "Law of Ukraine". - 2021, №2, - с.125-150
34. The impact of information and communication technologies on intellectual property rights / Zaur Aliyev, Nazrin Aliyeva // Proceedings of the 8th international conference on control and optimization with industrial applications, - Baku, - 2022, Vol II, - p.84-87

Dissertasiyanın müdafiəsi "28" fevral 2024-cü il tarixində saat 11:00 Bakı Dövlət Universiteti nəzdində fəaliyyət göstərən BED 2.44 Birdəfəlik Dissertasiya Şurasının iclasında keçiriləcək.

Ünvan: AZ 1148, Bakı ş., Zahid Xəlilov-23. I korpus, auditoriya 805.

Dissertasiya ilə Bakı Dövlət Universitetinin kitabxanasında tanış olmaq mümkündür.

Dissertasiya və avtoreferatın elektron versiyaları Bakı Dövlət Universitetinin rəsmi internet saytında yerləşdirilmişdir.

Avtoreferat "26" yanvar 2024-cü il tarixində zəruri ünvanlara göndərilmişdir.

Çapa imzalanıb:
Kağızın formatı:
Həcm:
Tiraj: