

AZƏRBAYCAN RESPUBLİKASI

Əlyazması hüququnda

İNFORMASIYA HÜQUQ POZUNTULARI VƏ İNFORMASIYA-HÜQUQİ MƏSULİYYƏT: NƏZƏRİ VƏ TƏCRÜBİ ASPEKTLƏR

İxtisas: 5614.01 – “İnzibati hüquq; maliyyə hüququ;
informasiya hüququ”

Elm sahəsi: Hüquq

İddiaçı: **Hüseyn Oktay oğlu Əlizadə**

Fəlsəfə doktoru elmi dərəcəsi
almaq üçün təqdim edilmiş dissertasiyanın

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

Bakı – 2023

Dissertasiya Bakı Dövlət Universiteti Hüquq fakültəsinin “İnsan hüquqları və informasiya hüququ” UNESCO kafedrasında yerinə yetirilmişdir.

Elmi rəhbərlər:

hüquq elmləri doktoru, professor
Ramil Mahir oğlu Aslanov

hüquq üzrə fəlsəfə doktoru
Gülnaz Aydın qızı Rzayeva

Rəsmi opponentlər:

hüquq elmləri doktoru, professor
Salmanova Olena Yuriyevna

hüquq üzrə fəlsəfə doktoru, dosent
Nazənin Şahin qızı Hüseynova

hüquq üzrə fəlsəfə doktoru, dosent
Əsmər Əlimusa qızı Əliyeva



Bakı Dövlət Universiteti nəzdində fəaliyyət göstərən FD 2.44
Dissertasiya şurası

Dissertasiya şurasının sədri:

hüquq elmləri doktoru, dosent

Turqay İmamqulu oğlu Hüseynov

Dissertasiya şurasının
elmi katibi:

hüquq üzrə fəlsəfə doktoru, dosent

Elmi seminarın sədri:

Əlizadə Qurbanlı oğlu Məmmədov
hüquq elmləri doktoru, professor

Əmir İbrahim oğlu Əliyev



DİSSERTASIYANIN ÜMUMİ SƏCİYYƏSİ

Mövzunun aktuallığı və işlənmə dərəcəsi. İnformasiya-hüquq pozuntularının aktual problem olaraq tədqiqatı informasiya cəmiyyətinin formalaşmasından sonra başlandı. Yarandığı ilkin dövrlərdə uğurlu nəticələr əldə olunacağı gözlənilən bu cəmiyyətdə müxtəlif neqativ halların mövcud olması da qaçılmaz idi. Hələ XX əsrin 50-ci illərində informasiyanı bizim və hisslərimizin ətraf mühitə qarşı uyğunlaşması prosesində əldə olunan məlumatlar kimi müəyyənləşdirən¹ informasiya nəzəriyyəsinin banisi Norbert Viner avtomatlaşdırma və İKT-nin tətbiqi üzrə təhlükələrin mövcudluğu ilə bağlı problemlər ortaya qoydu. N.Vinerin söylədiyi həmin təhlükələr zaman keçdikcə informasiya hüquq pozuntuları olaraq geniş yayılmağa başladı.

Qeyd edilən tədqiqat informasiya təhlükəsizliyi və insan hüquqlarının təminatı ilə sıx şəkildə əlaqədardır. Belə ki, hüquq ədəbiyyatında qeyd edilir ki, müasir qloballaşma və informasiya texnologiyalarının inkişafı şəraitində informasiya təhlükəsizliyinə qarşı təhdidlər dövlətlərin milli təhlükəsizliyinə, cəmiyyətin ümumi maraqlarına, o cümlədən insan hüquq və azadlıqlarına qarşı yönəlmişdir². Təhdidlər qlobal və transmilli xarakterdə müxtəlif istiqamət və formalarda meydana gəlir³.

İnternet bu gün gündəlik həyatın ehtiyaclarına uyğun olaraq bütün sahələrə nüfuz etmiş və dünyanın hər yerindən insanları

¹ Винер Н. Кибернетика и общество. Москва: Изд-во иностранной литературы, 1958, с.31.

² Akrivopoulou C.M., Garipidis N. Human Rights and Risks in the Digital Era: Globalization and the Effects of Information Technologies. Hershey: IGI Global, 2012, p.19.

³ Aslanov R.M. Azərbaycan Respublikası və Rusiya Federasiyasında informasiya cəmiyyəti quruculuğunda informasiya təhlükəsizliyinin hüquqi təminatının nəzəri və konstitusiyaya əsasları. H.e.d. elmi dərəcəsi almaq üçün tədqim edilmiş dissertasiyanın avtoreferatı. Bakı, 2015, s.10; Əliyev Ə.İ. İnsan hüquqları. Bakı: Nurlar, 2019, s.128-129; Aslanov R.M. The right to information in the legislation of the Azerbaijan Republic // Computer Law & Security Review, 2016, Volume 32, Issue 6, December, p. 889-891.

əlaqələndirmişdir. Bu istiqamətdə də hüquq ədəbiyyatlarında təhlillərin geniş şəkildə tarixi, nəzəri və müqayisəli şəkildə aparılması⁴ əhəmiyyətli hesab edilməlidir və bunlar tədqiqatda irəli sürdüyümüz məsələlərin təsir dairəsinin geniş olduğunu bir daha müəyyən edir. İnternetin köməkliyi ilə qurulan əlaqə insanların alışı-verişi edərək ünsiyyət qurmalarına, müxtəlif məlumatları ötürməsinə və hətta sərbəst bir mühitdə qloballaşmasına imkan verir. Bu gün hətta dövlətlər öz fəaliyyətinin icrası üçün informasiya texnologiyalarından istifadə etmək məcburiyyətindədirlər. İnternet bağlantısı ilə dövlətin qanunverici, icra və ya məhkəmə orqanlarının fəaliyyəti elə qurulmuşdur ki, klassik idarəetmə sistemindən fərqli olaraq, verilən təlimatlar dövlət orqanları arasında elektron formada ötürülməklə daha tez yerinə yetirilir. Enerji, rabitə, kənd təsərrüfatı, səhiyyə, nəqliyyat, təhsil və maliyyə kimi mühüm infrastruktur sektorlarında informasiya sistemlərinin istifadəsi milli təhlükəsizliyə bərabər olduğu düşünülmən kibertəhlükəsizlik anlayışının əhəmiyyətini meydana gətirmişdir. Bir-birinə vahid qlobal şəbəkə ilə bağlı olan müasir dünyada kiberməkənin mövcudluğu dövlətlərin hökmranlığını itirmək riski ilə yanaşı, konkret sərhədlərin də olması artıq mübahisəli bir fakta çevrilmişdir. Çünki mərkəzi idarəetmənin olmadığı bu sahədə sui-istifadə hallarının qarşısını almaq və ya onlarla mübarizə aparmaq çox çətindir və bir dövlətin tənzipləməsi kifayət etmir.

Amnesty International-ın hesabatına görə, Google və Facebook şirkətləri əşyaların interneti texnologiyası və ağıllı şəhər dizaynı infrastrukturunu olan ağıllı məişət texnikası vasitəsilə evlərimizdə vaxt keçirdiyimiz məkanları şəxsi bir məkana çevirirlər və bu yolla insanların fərdi məlumatları toplanır⁵. Ona görə də informasiya hüququ pozuntularının qarşısının alınması yalnız bir istiqamətdən vacib deyildir, həmçinin digər insan hüquqlarının təminatı üçün

⁴ Əzizov R.F. “İnternet” şəbəkəsində tənzipləmənin müqayisəli hüquqi təhlili. Bakı: Elm, 2017, 216 s; Əzizov R.F. İnternet-məkanda hüquqi tənzipləmə: tarix, nəzəriyyə, komparativizm. Bakı: Qanun, 2021, 352 s.

⁵ Surveillance giants: How the business model of google and facebook threatens human rights. <https://www.amnesty.org/en/documents/pol30/1404/2019/en/>

mühüm əhəmiyyət kəsb edir. Bununla bağlı, bir çox ədəbiyyatlarda şərhlər verilmişdir⁶.

İKT-nin inkişafı nəticəsində meydana gələn kibernetik pozuntuların səbəb olduğu və ya ola biləcəyi ziyanın aşkar edə bilməməsi, keyfiyyət və kəmiyyət baxımından hesablanmayan məlumatların miqdarı kimi səbəblər informasiya hüquq pozuntularının artmasına səbəb olur. Lakin bunu statistik rəqəmlərdə görmək də çox çətindir. Çünki bir çox pozuntular hələ də kriminallaşdırılmadığı və yaxud aşkar edilməməsi səbəbindən latent qalır və rəsmi statistikada öz əksini tapmır. Bu səbəblərdən, informasiya hüquq pozuntuları kontekstində hüquqi tənzimləmələrin effektivliyi baxımından bir çox problemlər mövcuddur. Məsələn burasındadır ki, kibernetikada törədilən əməllərin insan ölümü ilə nəticələnən hər hansı bir istintaq materialı və ya məhkəmə təcrübəsi ilə bağlı statistik məlumatlara rast gəlinmir. Heç bir dövlət informasiya müharibəsinə hüquqi anlayış verməmiş, rəsmi olaraq informasiya müharibəsi elan etməmiş və ya belə müharibəni dəstəklədiyini açıqlamamışdır. Lakin buna baxmayaraq, kibernetikada günbəgün artan informasiya hüquq pozuntularının vurduğu ziyanın hesablanması hədsiz çətinliklər yaradır. Çünki bu cür pozuntular, xüsusilə də kibernetikayətlər əksər hallarda bir şəxsə deyil, minlərlə, milyonlarla insana qarşı yönəlmiş olur. Burada ilk növbədə, müxtəlif kompüter və şəbəkələrin sıradan çıxmasına, məhvinə gətirib çıxaran əməllərin vurduğu iqtisadi ziyan qeyd olunmalıdır ki, bu ziyan hər il artan dinamika ilə dəyişir. Cybersecurity Ventures-in məlumatına görə, qlobal kibernetikayətlər üzrə xərclərin 2015-ci ildə mövcud olmuş 3 trilyon ABŞ dollarından 2025-ci ilə qədər illik 10,5 trilyon ABŞ dollarına çatacağı, önümüzdəki beş il ərzində ildə 15 % artacağı gözlənilir⁷. Bu rəqəmlər vurulan və vurulacaq iqtisadi zərərin hansı səviyyədə böyük olacağını təsdiq edir. Həmçinin dövlət sirrini təşkil edən informasiya sistemlərinə qanunsuz daxil

⁶ Susi M. Human Rights, Digital Society and the Law: A Research Companion. New York: Routledge, 2020, 3412 p.

⁷ Cybercrime To Cost The World \$10.5 Trillion Annually By 2025. <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>

olmalar və s. bu kimi əməllər nəticə etibarilə müxtəlif dövlətlərə siyasi ziyan da vurmuş olur. Fərdi məlumatların oğurlanması ilə qeyri-qanuni yolla gəlir əldə olunmasına yönəlmiş müxtəlif informasiya hüquq pozuntuları bilavasitə insan hüquq və azadlıqlarına qəsd etdiyi üçün bu cür pozuntularla bağlı insan amili də ön plana çəkilməlidir. Qeyd olunan səbəblərdən, onların qarşısının alınması, məsuliyyət məsələsinin həlli aktual problem hesab olunur.

Hətta son dövəmdə Rəqəmsal İpək Yolunun çəkilişinə başlanılması özü də respublikamızda kiberməkanın hüquqi tənzimlənməsini, xüsusilə də informasiya hüquq pozuntularına görə məsuliyyət məsələlərinin hüquqi həllini zəruri edir. Region üzrə dövlətlərin internet bağlantısı tələbatının bu üsulla Azərbaycan Respublikası (AR) vasitəsilə ödənilməsinə nəzərdə tutan layihə respublikamızın kiberməkanda tranzit ölkəyə çevrilməsinə şərait yaradacaqdır.

Kibercinayətkarlıqla mübarizə hər zaman İKT şəbəkəsi istifadəçilərinin sayı, İnternetin transsərhəd xüsusiyyətləri və mərkəzləşdirilməmiş arxitekturası sayəsində kompleks bir məsələ olmuşdur. Həm ənənəvi, həm də yalnız onlayn fəaliyyət göstərən kiberməkanda mütəşəkkil cinayətkar qruplar qanunvericilərdən və hüquq-mühafizə orqanlarından bir neçə addım qabaqda qalırlar və ehtimal ki, qalmağa davam edəcəklər. Çünki kiberməkanda olan texnoloji yeniliklər heç də həmişə qanuni məqsədlər üçün istifadə olunmur. Hətta, 2019-cu ildə aparılmış hesablamalara görə, sorğuda iştirak edən mütəxəssislərin 69%-i internetdəki sui-istifadə hallarının, daha dəqiq desək informasiya hüquq pozuntularının artdığını qəti şəkildə təsdiq etmişdir⁸.

Kibercinayətkarların cinayət törədərkən texnologiyanın ən son yeniliklərindən istifadə etməsi cinayətlərlə mübarizə aparən hüquq-mühafizə orqanlarının işini daha da çətinləşdirir. Bu baxımdan, bu cinayətlərlə mübarizə aparən bölmələrin cinayətkarların istifadə

⁸ Dan Jerker B. Svantesson. Internet & Jurisdiction Global Status Report 2019. <https://digital-strategy.ec.europa.eu/en/library/internet-and-jurisdiction-global-status-report-2019>

etdikləri texnologiyanı və cinayətkarların xüsusiyyətlərini bilmələri və buna uyğun olaraq strategiyalar hazırlamaları vacibdir.

Mövcud qanunvericilikdə informasiya texnologiyaları sahəsindəki pozuntuların qiymətləndirilməsinə vahid yanaşmanın olmaması, istifadə olunan konseptual aparatda birlik və nəticədə gözlənilən nəticəni verməyən uyğunsuz və sistemsiz dəyişikliklərin tətbiqi ilə xarakterizə olunur. Bundan əlavə, elmi və texnoloji tərəqqinin nailiyyətlərinin tətbiqi və istifadəsini tənzimləyən qanunvericiliyin mükəmməl olmaması, texnoloji tərəqqinin müxtəlif aspektlərinin hüquqi tənzimlənməsinə yanaşmalarda tənzimləyici bazanın bölünməsi ümumi hüquqi problem olaraq qalmaqda davam edir.

Xarici mənbələrdə türk müəllifləri daha çox kibercinayətlərlə bağlı istiqamətləri araşdırmışlar və bu sahədə kifayət qədər tədqiqatlar vardır. Məsələn, Murat Volkan Dülger (“Bilişim suçları” kitabı), İsmail Ergün (“Siber Suçların Cezalandırılması və Türkiyə'de Durum” kitabı), Dr. Muammer Ketizmen (“Türk Ceza Hukukunda Bilişim Suçları” kitabı), Ali Karagülmez (“Bilişim Suçları və Soruşturma - Kovuşturma Evreleri” kitabı), Levent Kurt (“Bilişim suçları” kitabı) və başqaları İKT vasitəsilə törədilən cinayətlərlə bağlı müxtəlif yanaşmalar təqdim etmişlər.

İnformasiya hüququnu yeni yaranmış sahə kimi tədqiq edən İ.L.Baçılo, P.U.Kuznetsov, V.A.Kopilev, O.A.Qorodov, M.M.Rassolov kimi alimlər informasiya hüquq pozuntuları və informasiya hüquqi məsuliyyətlə bağlı məsələlərə ümumi şəkildə şərh vermişlər. Xarici müəlliflərdən N.Winner, M.Castells, M.McLuhan, E.Tofler və başqalarının elmi yanaşmalarına nəzər yetirilmişdir.

Respublikamızda yalnız Ə.İ.Əliyev və G.A.Rzayevanın elmi redaktorluğu ilə dərc etdirilmiş “İnformasiya hüququ” dərsliyində bu sahədə bəzi ümumi məqamlara aydınlıq gətirilmişdir. Bundan başqa, R.M.Aslanovun və R.F.Əzizovun əsərlərində də informasiya hüquq pozuntuları və informasiya-hüquqi məsuliyyətlə əlaqədar bəzi yaxın hüquqi məsələlərin təhlili aparılmışdır. Daha sonra, informasiya mühiti, təhlükəsizliyi və s. sahədə müxtəlif aspektlərdə və elmi istiqamətlərdə geniş təhlillərin (R.M.Əliquliyev, R.Ş.Mahmudov və b.) aparılmasına baxmayaraq, bunlar demək olar ki, hüquqi sahələri əhatə etmir.

Tədqiqatın obyektini və predmeti. Tədqiqatın obyektini informasiya hüquq pozuntuları və informasiya-hüquqi məsuliyyətlə bağlı beynəlxalq və milli-hüquqi tənzimləmənin əsas problemləri, eləcə də texniki və təşkilati aspektlərin hüquqi həlli sahəsində mövcud ziddiyyətlər təşkil edir. Tədqiqatın predmetini informasiya hüquq pozuntuları və informasiya-hüquqi məsuliyyətlə bağlı beynəlxalq və milli-hüquqi aspektdən hüquqi normalar və təcrübə boşluqları təşkil edir.

Tədqiqatın məqsəd və vəzifələri. Tədqiqatın məqsədini informasiya hüquq pozuntularının əsas fərqləndirici xüsusiyyətlərini müəyyənləşdirməklə onların təsnifatını aparmaq, bu təsnifat əsasında informasiya-hüquqi məsuliyyət formalarını təhlil etmək, qeyd olunan məsələlərlə bağlı beynəlxalq-hüquqi tənzimləmədəki kolliziyaları aşkara çıxarmaq, o cümlədən milli-hüquq normalarındakı qeyri-müəyyənlikləri təhlil etməklə, hüquqi tənzimləmənin təkmilləşdirilməsi üzrə təklif və tövsiyələr irəli sürülmək təşkil edir.

Tədqiqat işində aşağıdakı vəzifələr müəyyən edilmişdir:

- informasiya hüquq pozuntusunun anlayışının və xarakterik xüsusiyyətlərinin müəyyən olunması, onun məzmununda əhəmiyyətli və qeyri-əhəmiyyətli elementlərin fərqləndirilməsi;

- informasiya hüquq pozuntularının qeyri-əhəmiyyətli elementləri ilə bağlı hüquqi tənzimləmədəki problemlərin təhlili və optimal təkliflərin təqdim olunması;

- informasiya hüquq pozuntularının hüquqi təsnifatının aparılması və təcrübə əhəmiyyətinin müəyyən olunması;

- informasiya hüquq pozuntularına dair beynəlxalq-hüquqi tənzimləmənin təhlili, bu sahədə “köhnəlmiş” və ziddiyyətli normaların müəyyən edilməsi, yeni redaktələrin təqdim olunması;

- informasiya hüquq pozuntuları və informasiya-hüquqi məsuliyyət sahəsində xarici dövlətlərin qanunvericilik təcrübəsinin təhlili;

- informasiya hüquq pozuntuları və informasiya-hüquqi məsuliyyət üzrə AR qanunvericiliyinin ətraflı nəzərdən keçirilməsi;

- informasiya hüquq pozuntularının oxşar və əlaqəli pozuntulardan fərqləndirilməsi, o cümlədən problemin insan hüquqları kontekstindən təhlili;

- informasiya hüquqi məsuliyyətin formalarının hüquqi tənzimlənməsində beynəlxalq və milli-hüquqi problemlərin təhlili;
- informasiya təhlükəsizliyinin informasiya-hüquqi məsuliyyət aspektindən təhlili;
- hüquqi şəxslərin informasiya-hüquqi məsuliyyətinin səciyyəvi tərəflərinin şərhı;
- fiziki şəxslərin informasiya-hüquqi məsuliyyətinin spesifik xüsusiyyətlərinin təhlili, insanabənzər robotların məsuliyyət problemlərinin araşdırılması;
- kibercinayətlərin məzmununun açılması və onlarla mübarizəyə dair təkliflərin təqdim olunması;
- informasiya hüquq pozuntuları, informasiya-hüquqi məsuliyyət və digər yaxın sahələrdə kifayət qədər sxem və cədvəllər hazırlamaqla bu sahədə əyani müqayisəli araşdırmanın qurulması;
- informasiya hüquq pozuntuları, informasiya-hüquqi məsuliyyət və digər yaxın sahələrdə AR qanunvericiliyinin təkmilləşdirilməsi istiqamətində bəzi təkliflərin verilməsi.

Tədqiqat metodları. Tədqiqat zamanı ümumelmi və xüsusi metodlardan kompleks şəkildə istifadə olunmuşdur. Xarici dövlətlərin təcrübəsinin, beynəlxalq normalarla dövlətdaxili normaların uyğunluğunun müəyyən olunmasında müqayisəli-hüquqi təhlilə daha geniş yer verilmişdir. Aparılmış təhlilin nəticələri üzrə sintezdən istifadə edərək ümumiləşdirmələr aparılmış, müəyyən təklif və tövsiyələr irəli sürülmüşdür.

İnformasiya hüquq pozuntularının elementləri analiz əsasında ayrı-ayrılıqda tədqiq olunmuşdur. Bu zaman həmçinin vahid modelin təklifi müxtəlif xəyali (qeyri-maddi) modellərin qurulması ilə mümkün olmuşdur. Müxtəlif hüquq normalarının şərhı və ziddiyyətlərin aşkar edilməsi formal məntiq metodlarının əsasında həyata keçirilmişdir.

Tədqiqatın elmi yeniliyi. Milli hüquq elmində bu günədək informasiya hüquq pozuntuları və informasiya-hüquqi məsuliyyət problemi barəsində hələ də kompleks tədqiqat aparılmamışdır. Bu da nəticə etibarilə informasiya hüquq pozuntularının sərhədlərinin hədsiz dərəcədə genişləndirilməsinə gətirib çıxarmışdır. Dissertasiyada

informasiya hüquq pozuntularının məzmununda elementlər ilk dəfə olaraq iki qrupda təsnifləşdirilmiş və bu təsnifat meyarı əsasında informasiya hüquq pozuntularının dairəsi müəyyənləşdirilmişdir.

Dissertasiyada hüquq ədəbiyyatında ilk dəfə olaraq informasiya hüquq pozuntusunun texniki yanaşmasından fərqli yanaşma təqdim olunmuşdur. Digər elmi yenilik İKT-nin təsirindən irəli gələrək, beynəlxalq-hüquqi tənzimləmələrin özündə mövcud boşluqların üzə çıxarılmasından ibarətdir.

Müdafiyyə çıxarılan əsas yeni elmi müddəalar aşağıdakılardır:

1. İnformasiya-hüquq pozuntuları ilə bağlı ziddiyyət bu pozuntuların ənənəvi şərh ilə müasir izahı arasında mövcuddur. Ənənəvi olaraq, informasiya əsas etibarilə KİV və xəbərlərlə əlaqələndirildiyi üçün informasiya hüquq pozuntuları da bu kontekstdən şərh olunurdu. Müasir cəmiyyətdə kiberməkanın formalaşması informasiya hüquq pozuntularının yalnız bu məkanda törədildiyi və İKT ilə əlaqədar olduğu mövqeyini formalaşdırmışdır. Aparılan təhlillərlə belə dar yanaşma qəbul edilməyərək informasiya məkanının daha geniş anlayış olduğu vurğulanır və qeyd olunan pozuntuların məhz informasiya məkanında törədilməsi qəbul edilir. Çünki informasiya cəmiyyətində informasiya həyatımızın ayrılmaz hissəsinə çevrilmişdir. Belə olduğu halda, kibercinayətlərin özünün də dar mənada şərh hüquqi baxımdan düzgün sayılmır. Kiberməkanda və İKT ilə əlaqəli pozuntuların fərqləndirilməsi bilavasitə obyektə asılı olaraq müəyyən olunmalıdır ki, bu obyekt müxtəlif sistemlərdə qeydə alınmış informasiya, yəni verilənlər təşkil edir. Ona görə də respublikamızın cinayət qanunvericiliyində kibercinayətlərə aid sanksiyaların nəzərdə tutulduğu fəslin adını bir qədər uğursuz saymaq olar. Bu, Budapeşt Konvensiyası müstəvisində də qarışıqlıq yaradır. Konvensiya kibercinayətləri qüsurlu olsa da, geniş mənada qəbul edərək, kiberməkanda törədilən əməllər kimi qiymətləndirir. Konvensiyanın belə mövqeyi kiberməkanda törədilən əməllərin transsərhəd xarakter daşması və ümumilikdə onların yurisdiksiya məsələlərinin tənzimlənməsi üçün vahid beynəlxalq-hüquqi çərçivəyə ehtiyacın olmasından irəli gəlir. Lakin qeyd etdiyimiz fəsil

bilavasitə verilənlərə qəsd edən əməlləri nəzərdə tutur. Ona görə də fəslin adının “Verilənlər (və yaxud da Kompüter verilənləri) əleyhinə cinayətlər” kimi adlandırmaq daha məqsəduyğundur. Bir-birindən çox fərqli statusu olan cinayətlərin eyni sanksiya ilə cəzalandırılmasını tələb edəcəyi üçün bütün İKT-dən istifadə edilməklə törədilən bütün cinayətləri kibercinayət daxilində birləşdirmək düzgün olmazdı. Bundan əlavə, bu fərq qoyulmadıqda, kibercinayətlərin əhatə dairəsi o dərəcədə genişlənəcəkdir ki, gələcəkdə təcrübə üçün çox böyük problemlər yaranacaqdır.

2. Əksər hallarda beynəlxalq normalar “etalon” kimi qəbul edilir və milli hüquqda implementasiya edilir. Lakin müasir dövrün zərurəti artıq bir çox beynəlxalq normaların da köhnəlməsini və dəyişiklik edilməsini təsdiq edir. Tədqiqatda informasiya hüquq pozuntuları ilə bağlı belə beynəlxalq sənədlər üzrə müxtəlif redaktələrin aparılması təklif olunmuşdur. Hesab etmək olar ki, milli hüquq əksər hallarda beynəlxalq hüquqa əsaslandığı üçün belə redaktə və dəyişikliklər dövlətdaxili hüquqa da öz töhfəsini verə bilər. Bundan əlavə, hüquqi tərcümədə olan problemlər bütün dünya üzrə qəbul edilmiş bir çox terminlərin milli qanunvericilikdə yanlış tərcüməsinə səbəb olmuşdur. Məsələn, informasiya təhlükəsizliyinin “üçlüyü” adlanan tamlıq, əlyətərlik və konfidensiallıq elementləri ümumi qəbul olunmuşdur. Lakin Budapeşt Konvensiyasının tərcüməsi üzrə əlyətərlik “istifadə imkanları”, “konfidensiallıq” isə “məxfilik” kimi qeyd olunmuşdur. Konfidensiallığın məxfiliyə bərabər tutulması, eləcə də əlyətərliyin nəzərdə tutulmaması kibercinayətlərin ümumi məzmununun müəyyən olunmasında çaşqınlıq yarada bilər. Bu da vahid terminologiyadan istifadə olunma zərurətini bir daha təsdiq edir.

3. Informasiya hüquq pozuntularının qarşısının alınması üzrə xüsusi əhəmiyyət kəsb edən informasiya təhlükəsizliyi yalnız dövlətlərin informasiya siyasətinin əsas istiqamətlərindən biri olmamalıdır. Həmçinin ayrı-ayrı təşkilatlar çərçivəsində də informasiya təhlükəsizliyi təmin olunmalı və bununla bağlı təşkilatdaxili siyasət planı işlənib hazırlanmalıdır. Belə ki, bədniyyətlilər əksər hallarda kiberpозuntuların törədilməsi üçün müxtəlif təşkilatların informasiya

sistemlərindən istifadə edirlər. Ona görə də informasiya təhlükəsizliyi yalnız informasiyanın mühafizəsi kimi qiymətləndirilməməlidir. Respublikamızda 27 may 2022-ci il tarixli dəyişikliklərlə qanunvericilikdə informasiya təhlükəsizliyinə hüquqi anlayışın verilməsini təqdirəlayiq hal saymaq olar. Lakin leqal anlayışda olan bəzi çatışmazlıqların aradan qaldırılması məqsədmüvafiqdir. Belə ki, mötəbərlik elementinin də informasiyanın tamlığı, əlyetərliyi və konfidensiallığı ilə birlikdə anlayışa daxil edilməsi məqbul deyildir. Çünki sadaladığımız üç elementin təminatı hər bir halda informasiyanın mötəbər olmasına yönəlmişdir.

4. Son dövrdə milli qanunvericiliyə edilən dəyişikliklərlə kritik informasiya infrastrukturuna hüquqi yanaşmanın təqdim olunması və “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Qanuna “Kritik informasiya infrastrukturunun təhlükəsizliyi” adlı fəslin əlavə olunması bu sahədə törədilən pozuntularla bağlı tənziqləmələrə yenidən baxılmanı şərtləndirmişdir. Belə ki, müvafiq dəyişikliyə əsasən, kritik informasiya infrastrukturunun təhlükəsizliyi üzrə tələblərin pozulması inzibati-hüquqi məsuliyyətə səbəb olur (Qanunun 20-4.6-cı maddəsi və İXM-in 371-1-ci maddəsi). Lakin bununla cinayət qanunvericiliyində heç bir dəyişiklik edilməmişdir. Kritik informasiya təhlükəsizliyinin əhatə etdiyi obyektlərin dövlət və ictimai əhəmiyyətini nəzərə alsaq, cinayət-hüquqi müstəvidə də tənziqləmənin nəzərdə tutulmasını məqsədmüvafiq sayırıq.

5. İnformasiya texnologiyaları sürətlə dəyişir və eyni zamanda informasiya sahəsində pozuntuların törədilmə üsulları, ümumilikdə təbiəti də dəyişir. Lakin qanunvericilik bu dəyişikliklərlə tam uyğunlaşa bilmir. Ona görə də informasiya sahəsində normalarda konkretliyə yol verilməməlidir ki, gələcək dəyişikliklərə cavab verə bilsin. “Kiberhücüm”, “kibermüharibə”, “kibercasusluq”, “kibercinayət” kimi anlayışların beynəlxalq səviyyədə qəbul edilmiş vahid tərifləri yoxdur. Eyni zamanda, dövlətlərin qəbul etdiyi jus cogens qaydaları kiberhüquq sahəsində yaradılmamışdır. Əslində, inkişaf etmiş ölkələrin internetdən asılılığının artması nəticəsində internetdəki çatışmazlıqlar düşmənlərin

dövlətlərin hücumları üçün uyğun bir mühit yaratmışdır. Belə ki, internetin yaratdığı təhlükəsizlik boşluqları səbəbindən inkişaf etmiş dövlətlər daha az inkişaf etmiş dövlətlərə qarşı müxtəlif kibernetik pozuntular icra edir. Beynəlxalq hüquq sahəsində tərifi olmayanların nəticələrindən biri də budur. Dövlətlərarası münaqişələrə səbəb ola biləcək kibernetik hücumların beynəlxalq hüquqda heç bir ekvivalentinin olmaması əhəmiyyətli bir çatışmazlıqdır. Milli qanunvericilikdə son dövrdə edilən dəyişikliklərlə kibernetik hücum, kibernetik insident, kibernetik təhdid kimi anlayışlar daxil edilsə də, bu, kibernetik məkanda törədilən pozuntularla bağlı hüquqi tənziyyət üçün yetərli deyildir.

6. Digər bir vacib problem kibernetik məkanda törədilən pozuntuların internetin transsərhəd təbiətindən irəli gələrək, yurisdiksiya məsələlərini aşması ilə bağlıdır. Ona görə də belə pozuntuların qarşısının alınması üçün mövcud qanunvericilik bazasının möhkəmləndirilməsi, köhnə beynəlxalq və milli normaların yenilənməsi və uyğunlaşdırılması ilə yanaşı, həm də milli səviyyədə sektorlararası əməkdaşlıq, həm də elektron mühitdə törədilən cinayətlərin aşkarlanması, istintaqı və qarşısının alınması sahəsində beynəlxalq əməkdaşlığın inkişafı tələb olunur. Burada kibernetik mühitdə törədilən əməllərin mütəşəkkilliyi də nəzərə alınmalıdır. Bir çox dövlətlərdə mütəşəkkil kibernetik cinayətkarların fəaliyyətlərinə cavab vermək üçün lazımi tənziyyət mövcud deyildir. Ona görə də problemin həlli qlobal səviyyədə mümkün ola bilər. Çünki İnternet şəbəkəsi qlobal bir şəbəkədir. Qlobal strategiyanın olmaması ilə yaxın gələcəkdə problemin daha da dərinləşməsi ehtimalı çox yüksəkdir. Bu baxımdan, problemi həll etməyin yolu həm milli, həm də beynəlxalq səviyyədə səylərin koordinasiyası və uyğunlaşdırılmasını ehtiva edən uzunmüddətli tədbirlər planının hazırlanması ola bilər.

7. Milli qanunvericiliyimizdə olan əsas problemlərdən biri bir çox terminlərdə təkrarçılığa yol verilməsidir. Belə ki, informasiya hüquq pozuntularının başlıca obyekt olan informasiyanın hüquqi rejimi və növləri ilə bağlı bir çox normalar müxtəlif qanunvericilik aktlarında təkrarlanır. Məsələn:

- Sənədləşdirilmiş informasiyanın anlayışı həm “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında”

Qanunda (maddə 1), həm də “İnformasiya əldə etmək haqqında” Qanunda (maddə 7) nəzərdə tutulmuşdur. Məzmun etibarilə qeyd olunan hər iki maddə üst-üstə düşür;

- İnformasiyanın əldə olunması ilə bağlı prinsiplərin əksəriyyəti həm “İnformasiya əldə etmək haqqında” Qanunda, həm də “Məlumat azadlığı haqqında” Qanunda təkrarlanır;

- İnformasiya sistemləri, xidmətləri ilə bağlı anlayış normaları qeyd olunan qanunvericilik aktlarının hər birində nəzərdə tutulmuşdur və s.

Qeyd olunan təkrarçılıqların qarşısının alınması iki yolla mümkündür: birincisi, müəlliflərin “İnformasiya Məcəlləsi”nin qəbulu ilə bağlı mövqeyinin dəstəklənməsi və belə Məcəllənin qəbul olunması; ikinci isə mövcud qanunvericilik aktlarında müvafiq redaktələrin edilməsi və təkrar normaların çıxarılması.

8. Ümumi olaraq, kibercinayətlərin anlayışı nə beynəlxalq, nə milli tənzimləmədə verilmədiyi səbəbi ilə hüquq ədəbiyyatında müxtəlif şərhlərin verilməsinə gətirib çıxarmışdır. Əksər tədqiqatçılar kibercinayətlər dedikdə, İKT-yə qəsd edən və İKT vasitəsilə törədilən əməlləri başa düşürlər. Lakin İKT vasitəsilə törədilən əməllərin də kibercinayət sayılması hüquq elminin ənənəvi baxışları üçün ciddi problemlərə gətirib çıxara bilər. İnformasiya sistemindən verilənlərin qanunsuz ələ keçirilməsi ilə kiberməkanda hər hansı bir şəxsin təhqir olunmasının eyni ad – kibercinayət altında birləşdirilməsi məntiqi və praktiki baxımdan düzgün deyildir. Bu halı bir çox cinayətlərə tətbiq etmək olar. Ona görə də kibercinayət üçün ən vacib element qəsd obyektini götürülməlidir. Məsələn, bank məlumatlarını qanunsuz ələ keçirməklə talamanı kibercinayət kimi deyil, oğurluq kimi qiymətləndirmək lazımdır. Lakin əgər müvafiq əməli nəzərdə tutan dispozişiyada İKT-dən istifadə tərkib elementi kimi təsbit olunmamışdırsa, o zaman əmələ cinayətlərin məcmusu kimi tövsiyə etmək lazım olacaqdır. Çünki İKT-dən istifadə etməklə məlumatların qanunsuz ələ keçirilməsi özü də ayrıca bir cinayət əməli kimi (Cinayət Məcəlləsinin 272-ci maddəsi) kriminallaşdırılmışdır.

Hesab edirik ki, bu məsələ ilə bağlı BMT-nin Cinayətkarlığın qarşısının alınması və Cinayət Ədliyyəsi üzrə XIII Konqresində maraqlı və tutarlı əsaslandırma edilmişdir. Yeni cinayət formalarının müəyyənləşdirilməsi üzrə problemlərin, xüsusilə də terminologiya probleminin mövcudluğu qeyd olunur və “yeni yaranan cinayət formaları” ifadəsinə müraciət edilir. Kibercinayətlər də bu yeni cinayət formalarına daxil edilir. Qeyd etməliyik ki, belə yeni cinayət formaları yalnız yeni səbəb və törədilmə üsullarını əhatə etmir, eyni zamanda aşkarlanması daha çətin ola biləcək yeni qurban növlərinə də yönəldilə bilər. Həmçinin bu növ əməllərdə qurban sayının çoxluğu da müşahidə edilir. Belə ki, bir zərərli proqramın paylanması eyni vaxtda çoxsaylı istifadəçilərə ziyan vura bilər.

9. “İnformasiya, informasiyanın mühafizəsi və informasiyalaşdırma haqqında” Qanunda əks olunan internet və host provayderlərin hüquqi anlayışı provayderlərin məsuliyyətini nəzərdə tutan “Telekommunikasiya haqqında” Qanunda nəzərdə tutulsa, daha düzgün olardı. Bundan əlavə, qanunvericinin tranzit provayderinə də öz münasibətini bildirməsi lazımdır. Çünki praktikada bu xidmətdən istifadə olunur.

10. Bir çox hallarda informasiya sahəsində pozuntular nə xəta, nə cinayət tərkibi yaratmayıb, sadəcə müvəqqəti “istifadəçi narahatlıqları”ndan ibarət olur. Lakin təqdim etdiyimiz təcrübi misallar da bir daha təsdiq edir ki, sadə çatlaşma nəticədə insan itkisinə gətirib çıxara bilər. Ona görə də hüquq-mühafizə orqanları bu tip kompüter və internet istifadəsindən yaranan şikayətlərə biganə qalmamalı, onların qarşısının alınması üzrə profilaktik tədbirlər görməlidirlər.

Tədqiqatın nəzəri və praktiki əhəmiyyəti. Tədqiqatın nəzəri əhəmiyyəti ondan ibarətdir ki, burada informasiya hüquq pozuntularının təsnifatı aparılmış və onların digər hüquq pozuntularından fərqli cəhətləri müəyyən olunmuşdur. Qarşıya qoyulan problemlərə kompleks yanaşılması, mövcud sahəvi qanunvericilik aktlarında olan çatışmazlıqların aradan qaldırılması üzrə irəli sürülən yeni terminoloji izahlar nəzəri cəhətdən mühüm əhəmiyyət kəsb edə bilər.

Tədqiqatın praktiki əhəmiyyəti informasiya hüquq pozuntularına qarşı mübarizə üzrə təklif olunan əməkdaşlıq formaları, informasiya-hüquqi məsuliyyətin növləri və formaları ilə bağlı qeyd olunmalıdır.

Eyni zamanda, tədqiqatdan İnformasiya hüququ, İnformasiya təhlükəsizliyinin hüquqi əsasları, İnformasiya sahəsində hüquqi məsuliyyət, Elektron dövlət, Kibertəhlükəsizlik hüququ və s. fənlərin tədrisində də geniş istifadə edilə bilər.

Tədqiqatın nəticələrinin aprobasiyası və tətbiqi. Tədqiqat işində əldə olunmuş nəticələr və yeniliklər müəllifin dissertasiya mövzusu üzrə respublikamızın və xarici dövlətlərin nüfuzlu elmi jurnallarında müxtəlif dillərdə dərc etdirdiyi elmi əsərlərdə, o cümlədən beynəlxalq elmi konfransların materiallarında öz əksini tapmışdır.

Tədqiqat işinin strukturu. Tədqiqat işi struktur baxımından giriş, üç fəsil, nəticə və istifadə edilmiş ədəbiyyat siyahısından ibarətdir.

DİSSERTASIYANIN ƏSAS MƏZMUNU

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

Birinci fəsil “İnformasiya-hüquq pozuntularının mahiyyəti və hüquqi təsbiti” adlanır və üç paragrafdan ibarətdir.

Birinci paragrafda informasiya hüquq pozuntusunun məzmununda ənənəvi və qeyri-ənənəvi elementlər təhlil olunur.

İnformasiya-hüquq pozuntularının bir çox spesifik xüsusiyyətləri vardır ki, bu onları ənənəvi pozuntulardan fərqləndirir: İKT-nin dinamik və sürətli inkişafını nəzərə alaraq, bu pozuntuların aşkara çıxarılması və onlarla mübarizə çox çətindir; bu cür pozuntuların hədəfi bəzən bir şəxs, bəzən də bir təşkilat və ya minlərlə insan ola bilər; kiberməkanın qlobal xarakterindən asılı olaraq, informasiya hüquq pozuntuları ilə mübarizə beynəlxalq səviyyədə aparılmazsa, uğurlu nəticələr əldə etmək mümkün olmaz.

İnformasiya cəmiyyətinin formalaşdığı və rəqəmsallaşma proseslərinin sürətlə inkişaf etdiyi bir dövrdə demək olar ki, əksər hüquq pozuntularının törədilməsində İKT başlıca amil və ya üsul kimi istifadə olunur. Lakin bu həmin pozuntuların hamısının informasiya hüquq pozuntularına aid edilməməsi anlamına gəlməməlidir. Hüquq ədəbiyyatında belə genişləndirici yanaşmaya üstünlük verən mövqelərlə razılaşmaq düzgün deyildir. Hər hansı bir pozuntunun informasiya hüquq pozuntusu kimi qiymətləndirilməsi üçün təbii ki, İKT-dən istifadə etməklə törədilmə əsas şərtidir. Lakin burada digər elementlərə də diqqət yetirilməlidir. Əsas etibarilə, pozuntunun qəsd etdiyi ictimai münasibətlər dairəsi vacib məqamlardan biridir. Məsələn, sosial şəbəkədə şəxsin təhqir olunması və ya onun şəxsi həyatına dair məlumatların açıqlanması İKT vasitəsilə törədilməsinə baxmayaraq, təbii ki, şəxsi toxunulmazlıq hüququnu pozmuş bir əməldir. Ona görə də informasiya hüquq pozuntusunun məzmununun əsas elementi olan informasiya bu pozuntular üzrə qeydə alınmış, daha dəqiq desək müxtəlif şəbəkələrdə yerləşdirilmiş məlumatlardan ibarət olur. Belə məlumatlar isə verilənləri təşkil edir. Ona görə də daha yaxşı olar ki, informasiya hüquq pozuntuları ilə bağlı (istər inzibati, istər mülki, istərsə də cinayət) kompüter informasiyası deyil, verilən anlayışından istifadə olunsun.

İkinci paraqrafda informasiya hüquq pozuntularının təsnifatına dair nəzəri və hüquqi yanaşmalar tədqiq edilir.

İnformasiya-hüquq pozuntuları ilə bağlı yalnız cinayət-hüquqi aspekti qəbul etmək onların mahiyyətinin açılmasında yetərli deyildir. Ona görə də inzibati xəta, mülki delikt və cinayət kimi bu pozuntuların nəzərdən keçirilməsi daha düzgündür. Rəqəmsal cəmiyyətdə mülki hüquq münasibətlərinə qəsd edən çoxsaylı informasiya pozuntularına rast gəlinir. Belə ki, milyardlarla istifadəçi bazası olan sosial mediada bu cür pozuntuların törədilməsi çox geniş vüsət almışdır. Hətta kiberməkanda neqativ aspektdən yayılan informasiyaya qarşı yaradılmış təşkilatlar fəaliyyət göstərir və dövlətlərin fəaliyyətini pozitiv istiqamətdən təbliğ edir. Məsələn, WikiLeaks şəbəkəsi korporativ və hökumət korrupsiyası ilə bağlı çoxsaylı yüksək səviyyəli hadisələri açıqlayır, “Troll fabrikləri”

saxta sosial media profilləri, troll əməliyyatlarını dəstəkləmək üçün veb saytlar yaradır. Troll fabrikinin işçiləri nəinki mesaj yazırlar, həm də şərhlərə cavab verir və onlayn müzakirələrdə iştirak edirlər. Yaratdıqları məzmunu yaydıqları saxta profillərin həqiqət təəssüratını artırmaq üçün mübahisələri simulyasiya edə bilirlər.

İnformasiya-hüquq pozuntuları qəti şəkildə kibercinayətlərlə məhdudlaşdırılmamalıdır. Təbii ki, kibercinayətlər informasiyanın tamlığı, konfidensiallığı və əlyetərliyinə qəsd edən başlıca əməllərdir. Lakin informasiya münasibətləri daha geniş səciyyə daşdığı üçün informasiya hüquq pozuntuları da geniş məzmunu malik olmalıdır.

Üçüncü paraqrafda kibercinayətlərin rəsmi və qeyri-rəsmi təsnifatına dair problemlər təhlil olunur.

Praktiki səviyyədə konkret tərifin olmaması ənənəvi cinayətlərdən fərqli olaraq transsərhəd və transyurisdiksiyalı xarakter daşıyan kibercinayətlərlə bağlı xüsusi narahatlıq doğurur. Uzun müddət konkret leqal yanaşmanın olmaması internetlə əlaqəli cinayətlərin iki qrupa ayrılması ilə nəticələnmişdir: dar mənada kibercinayətlər – kompüterlərə və proqram təminatına qəsd edən əməlləri əhatə edir; geniş mənada kibercinayətlər – İKT ilə əlaqəli və ya onun vasitəsilə törədilən bütün əməlləri ehtiva edir.

Rəsmi təsnifatlardan başlıcası 1991-ci ildə INTERPOL işçi qrupu tərəfindən hazırlanmışdır. Bu təsnifatda bütün kodlar “Q” hərfi ilə başlayan eyniləşdiriciyə (identifikatora) malikdir. Onlar özləri də qəsdin növündən asılı olaraq 6 qrupa bölünür ki, burada da “A”, “F”, “D”, “R”, “S”, “Z” hərflərindən istifadə olunur. Məsələn, “QA” hərf birləşməsindən ibarət kod – İcazəsiz (sanksiyalaşdırılmamış) daxil olma və ələ keçirməni, “QF” birləşməsindən ibarət kod – kompüter dələduzluğunu, “QR” kodu – qanunsuz surətçıxarmanı (piratçılığı) əks etdirir və s. Bu kodların hər birinin cinayətin törədilmə üsulundan asılı olaraq öz təsnifatı aparılır.

İkinci fəsil - “İnformasiya hüquq pozuntularının qarşısının alınması və informasiya təhlükəsizliyi”- üç paraqraftan ibarətdir.

Birinci paraqrafda informasiya hüquq pozuntularının qarşısının alınmasına dair beynəlxalq əməkdaşlıq tədqiq olunur, universal və regional normaların təhlili aparılır.

Kiberməkanda törədilən bir pozuntunun araşdırılması əksər hallarda bir çox fərqli dövlətin hüquq sistemini əhatə edir və cinayətkarların ədalət mühakiməsinə çıxarılması üçün sıx beynəlxalq əməkdaşlıq tələb olunur. AR bu əməkdaşlığı nümayiş etdirən bir sıra rəsmi və qeyri-rəsmi mexanizmlərin üzvüdür. Bura müxtəlif Konvensiyaların, xüsusilə Budapeşt Konvensiyasının ratifikasiyası, o cümlədən əsas şəbəkələrin və çöxtərəfli forumların üzvü olmaq daxildir.

Ümumiyyətlə, beynəlxalq əməkdaşlıq formal və qeyri-formal ola bilər. Formal əməkdaşlığa universal və regional səviyyədə qəbul edilmiş konvensiyalar və sazişlər daxildir. İnternet üzərindən törədilən cinayətlər tez-tez bir dövlətin yurisdiksiyasını aşır ki, bu, bütün beynəlxalq birlik üçün təhlükədir. Bu qlobal problem regional və ya məhdud münasibətləri tənzimləyən normalarla həll edilə bilmədiyi üçün, hazırda yalnız Budapeşt Konvensiyasının təmin etdiyi beynəlxalq həll və çöxtərəfli yanaşma tələb olunur. Bir yurisdiksiyada cinayət sayılan İnternetdəki davranışların digər yurisdiksiyalarda da eyni şəkildə cinayətkar sayılması vacibdir. Lakin bir məqamı da qeyd etməliyik ki, Budapeşt Konvensiyasının özü hələ də bir çox dövlətlər tərəfindən ratifikasiya edilməmişdir. Bu da Konvensiyanın effektivliyini azaldır, çünki Konvensiyanı ratifikasiya edən 66 dövlət dünyanın internet istifadəçilərinin yarısından azını təşkil edir.

İkinci paraqrafda informasiya hüquq pozuntularının hüquqi təsbiti və onlarla mübarizə üzrə xarici dövlətlərin təcrübəsinin səciyyəvi xüsusiyyətləri tədqiq olunur.

Informasiya hüquq pozuntuları ilə bağlı xarici dövlətlərdə daha çox cinayət əməllərinə diqqət yetirilir. Mülki deliktlər və inzibati xətlər diqqətdən bir qədər kənar qalır. Bunun başlıca səbəbi kiberməkanda insan hüquqlarına edilən çoxsaylı qəsdlərdir. Xarici dövlətlərin hamısında qanunsuz daxil olma kriminallaşdırılmışdır. Lakin artıq kompüter verilənlərinin gəlir əldə etmək məqsədilə istifadəsi üzrə tənzimləmədə fərqlər vardır. Bəzi dövlətlərdə bu da informasiya

cinayətləri sırasına daxil edilirsə, digər dövlətlərdə müstəqil tərkib kimi (məsələn, kompüter dələduzluğu) müəyyənləşdirilir.

Müqayisəli təhlillərin aparılması məqsədilə dissertasiyada bir neçə dövlətin qanunvericilik mənbələrinə istinad olunmuş və belə qənaətə gəlinmişdir ki, Almaniya qanunvericiliyi informasiya hüquq pozuntularını daha səliqə və konkret formada müəyyənləşdirmişdir. Maraqlı xüsusiyyət onunla bağlıdır ki, Almaniya kibercinayətlər ayrıca bir fəsilə nəzərdə tutulmamışdır. Müxtəlif cinayət obyektlərindən asılı olaraq konkret maddələrdə İKT ilə bağlı əməllərə görə cəza müəyyən olunmuşdur. Belə ki, Almaniya Cinayət Məcəlləsində “Şəxsi və özəl sahənin konfidensiallığının pozulması” üzrə İKT ilə bağlı aşağıdakı cinayətlər nəzərdə tutulmuşdur: informasiya casusluğu; fişinq; məlumat casusluğu və fişinqə hazırlıq; oğurlanmış verilənlərin emalı (işlənməsi). “Dələduzluq və mənimsəmə”nin ayrıca bir növü kimi “Kompüter dələduzluğu” (maddə 263a) tərkibi nəzərdə tutulmuşdur. Bundan əlavə, “Verilənlərin manipulyasiyası” (maddə 303a) və “Kompüter sabotajı” (maddə 303b) ayrıca cinayətlər kimi müəyyən olunmuşdur.

Üçüncü paragrafda informasiya hüquq pozuntularının qarşısının alınması və informasiya təhlükəsizliyinin təminatı üzrə texniki, təşkilati və hüquqi problemlər tədqiq olunur.

Informasiya təhlükəsizliyi informasiyanın tamlığı, əlyətərliyi və konfidensiallığının təminatına yönəlmiş tədbirlər məcmusundan ibarətdir. Bir çox hallarda bu termini “kibertəhlükəsizlik”lə eyniləşdirirlər. Lakin onlar fərqli təhlükəsizlik növlərinə aiddir. Sadəcə dildə desək, kibertəhlükəsizlik təşkilat daxilindən və ya xaricindən edilən hücumlarla əlaqədardır. Əsasən kompüterlərdən, cihazlardan, şəbəkələrdən, serverlərdən və proqramlardan ibarət olan hücumlara və ya icazəsiz girişlərə həssas olan bütün aspektləri mühafizə etmək çərçivəsidir. Kibertəhlükəsizlik yalnız rəqəmsal formada olan məlumatların qorunması ilə əlaqədardır. Bunun əksinə olaraq, informasiya təhlükəsizliyi analog və ya rəqəmsal olmasından asılı olmayaraq məlumatları hər cür təhdiddən qorumaq məqsədi daşıyır.

Deməli, informasiya təhlükəsizliyi daha geniş məzmununa malik olub, özündə kibertəhlükəsizliyi də ehtiva edir.

Kibertəhlükəsizlik sənayeni və müxtəlif sahələri əhatə edən geniş tətbiq sahəsinə malik olduğundan, hər bir ölkənin inkişaf və ya məşğulluq səviyyəsi beş meyar üzrə qiymətləndirilir: hüquqi tədbirlər, texniki tədbirlər, təşkilati tədbirlər, kadr potensialının inkişafı və əməkdaşlıq.

Üçüncü fəsil “İnformasiya-hüquqi məsuliyyət institutu: beynəlxalq və milli-hüquqi tənzimləmə” adlanır və iki paragrafı özündə birləşdirir.

Birinci paragrafda hüquqi şəxslərin informasiya-hüquqi məsuliyyəti, AR-də elektron idarəetmənin formalaşdırılması və informasiya-hüquqi məsuliyyət institutuna yeni yanaşma ilə bağlı məsələlər araşdırılır.

İnformasiya hüquqi məsuliyyətin fiziki və hüquqi şəxslər üzrə bölünməsi xüsusi praktiki əhəmiyyətə malikdir. Bu, tətbiq olunacaq müvafiq inzibati və ya cinayət sanksiyasının müəyyən olunmasında, eləcə də mülki mübahisənin həllində mühüm rol oynayır. İnformasiya cəmiyyətinin ilkin dövrlərində daha çox fiziki şəxslər informasiya hüquq pozuntularına meyilli idilərsə, tədricən kriminal təşkilatlar İKT-nin təqdim etdiyi “rahat və münasib” imkanlardan istifadə etməyə başladılar. Nəticə etibarilə mütəşəkkil cinayətkarlığın bir növü olaraq kibercinayətkarlıq inkişafa başladı ki, bu da məsuliyyətin müəyyən olunmasına öz təsirini göstərir.

Budapeşt Konvensiyası da bununla bağlı özünəməxsus tənzimləmə nəzərdə tutur. Birincisi, Konvensiya hər hansı hüquqi şəxsin adından qərarlar vermək, nəzarət funksiyalarını həyata keçirmək, hüquqi şəxsin təmsil etmək kimi səlahiyyətlərə malik olan şəxsin hüquqi şəxsin xeyrinə törətdiyi pozuntulara görə həm fiziki şəxsin özünün, həm də müvafiq hüquqi şəxsin məsuliyyətinin müəyyən olunmasını dövlətlərdən tələb edir. İkincisi, burada yalnız cinayət-hüquqi deyil, digər məsuliyyət növlərindən də söhbət gedir. Üçüncüsü, hüquqi şəxslərin məsuliyyətinin müəyyən olunmasını Konvensiya

yüngülləşdirici vəziyyət kimi qiymətləndirməyərək, bunun şəxsin fiziki şəxs kimi məsuliyyətini istisna etmədiyini xüsusi vurğulayır.

Ümumilikdə, informasiya hüquq pozuntuları üzrə hüquqi şəxslərin məsuliyyəti aşağıdakı istiqamətlərdə təhlil olunmalıdır: mütəşəkkil cinayətkarlıqla məşğul olan hüquqi şəxslərin informasiya-hüquqi məsuliyyəti; internet provayderlərin informasiya-hüquqi məsuliyyəti; informasiya sahiblərinin informasiya-hüquqi məsuliyyəti.

İkinci paraqrafta fiziki şəxslərin informasiya-hüquqi məsuliyyətinin formaları tədqiq edilir.

İnformasiya hüquq pozuntularına dair fiziki şəxslərin məsuliyyətinin müəyyən olunması üzrə əsas problem onların sürətlə yeni növlərinin meydana gəlməsidir. Hətta bir çox hallarda mövcud pozuntunun hansı növə aid ediləcəyi problem yaradır. Bununla bağlı, eyniyyətin oğurlanması xüsusi qeyd olunmalıdır. Bir şəxsin qeydə alınmış rəqəmsal şəxsiyyətindən başqa bir şəxs tərəfindən vicdansız şəkildə sui-istifadə etmək ədəbiyyatda “eyniyyətin (şəxsiyyətin) oğurlanması” (theft of identity) kimi adlandırılır. Ümumi dələduzluq cinayətlərindən fərqli olaraq, oğurluq həmin şəxsi cinayətin qurbanı olaraq təyin edir.

Fiziki şəxslərin informasiya-hüquqi məsuliyyəti də hüquqi şəxslər kimi sahəvi normalarla tənzimlənir. Hüquqi şəxslərdən fərqli olaraq, fiziki şəxslər istifadəçi qismində məsuliyyət daşıyırlar. Problem ondadır ki, informasiya ehtiyatlarından istifadə qaydalarını pozma xətasının (İnzibati Xətalər Məcəlləsinin 371-ci maddəsi) cinayət ekvivalenti nəzərdə tutulmamışdır. İnformasiyanı əldə edən şəxsin həmin informasiyadan istifadə qaydalarını pozma verilənlər əleyhinə cinayətlərin heç birinə aid edilə bilməz. Deməli, qanunverici əldə olunmuş informasiyanın məzmunundan asılı olaraq, ictimai təhlükəliliyi müəyyən etmiş və müxtəlif sirlərin yayılmasına görə cinayət məsuliyyəti nəzərdə tutmuşdur. Məsələn, vəkillik fəaliyyəti ilə məşğul olan şəxs öz müştərisinin boşanma işi üzrə qarşı tərəfin əmlakı barədə müvafiq orqana sorğu ilə müraciət etmişdir. Mülkiyyətə dair məlumatlar fərdi məlumat sayıldığı üçün vəkil bu məlumatların özbaşına yayılmasına, açıqlanmasına yol verməməlidir. Bundan əlavə, hüquqi qaydada da müəyyən olunmuşdur ki, vəkil öz

peşə fəaliyyəti zamanı məlum olan məlumatların konfidensiallığını qorunmalıdır və bu məlumatlar vəkil sirtini təşkil edir. Deməli, bu vəziyyətdə vəkilin fərdi məlumatları açıqlaması vəkil sirtinin yayılmasına görə məsuliyyət yaradır. Buna uyğun kirminallaşdırılmış əməl olmadığı üçün fərdi məlumatlara dair dispozişiyaya (156-cı maddənin 2.1-ci bəndi) istinad etmək lazımdır. Hüquqi ziddiyyətlər də elə buradan irəli gəlir. Müxtəlif konfidensial məlumatları təsnifləşdirən qanunverici həmin məlumatların yayılmasına görə məsul olan şəxslər üçün məsuliyyət differensiasiyasını etmir.

Dissertasiyanın nəticə hissəsində əldə edilmiş mühüm təklif və nəticələr ümumi şəkildə belə ifadə edilə bilər:

1. İnformasiya-hüquq pozuntularının mahiyyətini açmaq üçün bu pozuntuların məzmununa daxil olan elementlər tərəfimizdən ənənəvi və qeyri-ənənəvi olmaqla şərh olunmuşdur. İnformasiya-hüquq pozuntularının məzmununda əsas ənənəvi üç element qeyd olunmuşdur. Çünki məhz bu elementlərin xarakterik xüsusiyyətləri həmin pozuntuları digər hüquq pozuntularından fərqləndirir: pozuntunun törədilməsi üçün şərait; pozuntunun obyekt; pozuntunun subyekt və onun məqsədi.

2. Çox təəssüf ki, AR-in informasiya qanunvericiliyinin ümumi anlayışları nəzərdə tutan maddələrində informasiya sistemlərinə çox qarışıq və qeyri-müəyyən anlayış verilmişdir. Fikrimizcə, aşağıdakı redaktənin edilməsi daha məqsədəuyğundur: “İnformasiya sistemi – verilənlərin avtomatik və müvafiq proqramlar əsasında işlənməsini həyata keçirən və qarşılıqlı əlaqəli fəaliyyət göstərən qurğu və ya qurğular qrupudur”.

3. Milli qanunvericilikdə “informasiya” və “verilən” terminlərinin leqal şərhə üzrə qeyri-müəyyənliklər mövcuddur. Həm nəzəri, həm də hüquqi aspektləri ümumiləşdirsək, qanunverici qəti şəkildə müəyyən etmir ki, məlumat qeydə alındıqdan sonra informasiya formasında təzahür edir. Lakin bir çox normaların (məsələn, qeydə alınmış məlumatı əldə etmək üçün şəxs informasiya sorğusunu təqdim etməlidir, məlumat sorğusunu deyil) şərhindən açıq-aydın görünür ki, hüquqi tənzimləmədə istər elektron, istərsə də kağız daşıyıcılarda qeydə

alınmış məlumatlar informasiya kimi qəbul olunur. Lakin bu özü də ziddiyyətlidir. Çünki adı çəkilən qanunlarda “şəxsi və ailə həyatına dair məlumat” (fərdi məlumat) ifadəsindən istifadə olunur. Belə olduğu halda terminoloji aparatda çəşnınlıq yaranmış olur. Ona görə də hesab edirik ki, “İnformasiya əldə etmək haqqında” və “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” AR Qanunlarında informasiya sistemindən hər hansı bir informasiyanın çıxarılması ilə bağılı normalarda “verilənlər” terminindən istifadə olunsa, daha düzgün olar. Bundan başqa, verilənlərin anlayışının aşağıdakı kimi redaktəsini təklif edirik: “Verilənlər – faktların, məlumatların və ya anlayışların hər hansı funksiyanın həyata keçirilməsini təmin edən informasiya kommunikasiya texnologiyaları vasitəsilə emal üçün yararlı olan istənilən təqdim formasıdır”.

4. Qlobal şəbəkənin bütün dövlətləri əhatə etməsi səbəbindən informasiya hüquq pozuntuları ilə mübarizə aparən dövlətlər səmərəli əməkdaşlığı həyata keçirmək üçün öz aralarında ortağ bir hüquqi dil inkişaf etdirməlidirlər. Həmin hüquqi dil əsasında beynəlxalq normaların standart hala gətirilməsi vacib şərtədir ki, dünya dövlətləri öz hüquqi tənzimləmələrini həmin beynəlxalq qaydalara uyğun həyata keçirməlidirlər. Maraqlı məqam ondadır ki, artıq bir çox beynəlxalq normaların özündə də köhnəlmə müşahidə olunur və İKT-nin inkişafını nəzərə alaraq, terminoloji aparatda dəyişikliklərin edilməsi daha yaxşı olar.

5. Bütün dünyada informasiya təhlükəsizliyinin “üçlüyü” kimi tanınan tamlıq, əlyetərlik və konfidensiallıq ifadələrinin yalnız biri – “tamlıq” düzgün tərcümə olunmuşdur. “Konfidensiallıq” “məxfilik” sözü ilə ifadə olunur ki, bu, informasiya qanunvericiliyinə tamamilə ziddir. “Əlyetərlik” isə “istifadə imkanları” ekvivalenti ilə tərcümə olunmuşdur. Bundan əlavə, Konvensiyada istinad edilən “təcrid olunma” ifadəsi “bloklanma”nı bildirir. Milli cinayət qanunvericiliyində də ikinci anlayışdan istifadə olunur. Bu kimi problemlərin aradan qaldırılması üçün beynəlxalq-hüquqi sənədlərin hüquqi tərcüməsinə yenidən baxılmalıdır.

6. Milli informasiya qanunvericiliyinə edilən 27 may 2022-ci il tarixli dəyişikliklərlə informasiya təhlükəsizliyinə anlayış verilmişdir. Burada nəzərdə tutulan mötəbərlik elementi əslində ilk üç elementin (tamlıq, əlyetərlik və konfidensiallıq) təmin olunduğu təqdirdə mövcud olacaqdır. Ona görə də hüquqi anlayışda yalnız üç elementin nəzərdə tutulmasını məqbul sayırıq.

7. İnformasiya hüquq pozuntuları informasiya sahəsində törədilən və informasiya hüquq münasibətlərinə qəsd edən hüquqazidd, qəsdən törədilmiş əməllərdir. Burada əsas etibarilə İKT-dən istifadə olunur. Lakin İKT-dən istifadə edilməklə törədilən hər bir əməl informasiya hüquq pozuntusu kimi qiymətləndirilə bilməz. Qeyd olunduğu kimi, rəqəmsallaşma kiberməkandan müxtəlif hüquqpozumaların icrası üçün istifadəyə gətirib çıxarmışdır. Bu məkanda yalnız informasiya sahəsində olan informasiya hüquq münasibətlərinə qarşı həyata keçirilən əməllər informasiya hüquq pozuntusu hesab olunacaqdır. Deməli, İKT-dən istifadə etmədən törədilən informasiya hüquq pozuntuları da ola bilər. Qeyd etməliyik ki, bu günə qədər aparılan tədqiqatlarda belə bir yanaşma təqdim olunmamışdır. Bütün şərhlərdə informasiya hüquq pozuntuları İKT ilə əlaqələndirilərək, yalnız texniki aspektdən təhlil olunur. Lakin qeyd etdiyimiz kimi, informasiya hüquq pozuntusu üçün əsas şərt informasiya hüquq münasibətlərinə qəsd etməsidir. Belə olduğu təqdirdə, informasiya hüquqlarının məhdudlaşdırılması və pozulması ilə bağlı pozuntuları informasiya hüquq pozuntuları kontekstində şərh etmək qeyri-mümkündür.

8. İnformasiya hüquq pozuntuları yalnız kibercinayətlərlə məhdudlaşdırılmamalıdır. Belə ki, əksər ədəbiyyatlarda “informasiya hüquq pozuntusu” dedikdə, yalnız kibercinayətlər nəzərdə tutulur. Problem ondadır ki, informasiya sahəsində pozuntular törədildiyi halda, əksər halda cinayət qanunvericiliyinin tətbiq olunması zərurəti vardır. Çünki Cinayət Məcəlləsində kriminallaşdırılmış kibercinayətlərin daha yüngül forması İnzibati Xətalər Məcəlləsində nəzərdə tutulmamışdır. Belə ki, adi oğurluğun belə qəsd predmetinin dəyərindən asılı olaraq, cinayət və xəta kimi tövsif edildiyi vəziyyətlər olduğu halda, kiberməkanda törədilən və informasiya sistemlərinə və

verilənlərinə qarşı yönəlmiş əməllərin yüngül nəticələrə səbəb olduğu şərait üçün qanunverici heç bir alternativ nəzərdə tutmamışdır. “İnformasiya ehtiyatlarının istifadə qaydalarının pozulması” kimi ümumi bir xətanı (AR İnzibati Xətalər Məcəlləsinin 371-ci maddəsi) təsbit edən İnzibati Xətalər Məcəlləsinin tətbiqində çətinliklərin olacağı göz önündədir. Eyni zamanda, digər problem demək olar ki, əksər kibercinayətlər üçün xüsusi subyektin tərkib elementi kimi qəbul edilməsi ilə bağlıdır. Rəqəmsal dünyamızda sırasıyla şəxslər tərəfindən İKT-dən istifadə etməklə məlumatların ələ keçirilməsi hallarına az rast gəlinmir. Hesab edirik ki, Cinayət Məcəlləsində nəzərdə tutulmuş formal tərkiblərin inzibati xəta kimi də İnzibati Xətalər Məcəlləsinə daxil edilməsinə ehtiyac vardır. Həmçinin xüsusi subyekt deyil, bütün şəxslər tərəfindən həmin əməllərin icrası məsuliyyətə səbəb olmalıdır.

9. İKT-dən istifadə etməklə verilənlərlə bağlı edilən qeyri-qanuni hərəkətlər bir çox hallarda ağır nəticələrə səbəb olmasa da, müxtəlif insanlar üçün müəyyən narahatlıqlar yaradır. Məsələn, virus məzmunlu maillərin e-poçta gəlməsini qeyd edə bilərik. İstifadəçi həmin maili açmasa, heç bir mənfi nəticə olmur. Amma bununla belə narahatlıqlar yaranır. Məsələn, bir şəxsin administratorlar tərəfindən tez-tez istifadə etdiyi bir veb saytın (çat, müzakirə forumu və s.) müvəqqəti olaraq bloklanması. Qanuni olaraq heç bir cinayətdən söhbət getməsə də, problemin həllini inzibati xəta kimi məsuliyyət tətbiq etməklə həll etmək mümkündür. Hətta, virtual məkanda vurulan zərərlə bağlı şikayətlər üzrə xarici dövlətlərin təcrübəsi də vardır. Qeyd olunan ağır nəticələrə səbəb olmayan narahatlıqlar inzibati məsuliyyət yarada bilər.

10. Beynəlxalq normaların özündə “kibercinayət” termininə aydınlıq gətirilmir. Bundan irəli gələrək, müxtəlif dövlətlərin milli qanunlarında bu cür əməllər müxtəlif cür (elektron cinayətlər, kompüter cinayətləri, kompüter informasiyası sahəsindəki cinayətlər, yüksək texnologiyalarla bağlı cinayətlər və s.) adlandırılır. Həmçinin kibercinayətlər əksər mənbələrdə geniş mənada şərh olunur, yəni kiberməkanda törədilən bütün pozuntular kibercinayət kimi qiymətləndirilir. Budapeşt Konvensiyasının da yanaşması belədir. Lakin fikrimizcə, bu cür yanaşma zaman keçdikcə bütün kriminal

əməllərin kibercinayət hesab olunması ilə nəticələnə bilər. Çünki rəqəmsallaşma kriminal aləm üçün də geniş imkanlar yaradır. Məsələn, artıq ənənəvi formada təhqir və ya böhtana demək olar ki, rast gəlinmir. Bu əməllərin kibercinayət kimi qəbul edilməsi heç də doğru olmaz. Çünki qəsdin obyektindən asılı olaraq cinayətlərin təsnifatı aparılmalıdır. Ona görə də kibercinayətlərin geniş mənada şərhini məqbul sayıla bilməz. Bu baxımdan, Budapeşt Konvensiyasının özündə də dəyişiklik edilməsi daha məqsədəuyğundur. Çünki Konvensiya geniş mənada təhlil yanaşmasını əsas götürsə də, İKT-dən istifadə etməklə törədilən bir çox əməllər (məsələn, terrorçuluğa açıq çağırış etmə) tənzimləmədən kənar qalmışdır. Öz mövqeyimizi kibercinayətlərin dar mənada şərhinə əsaslanmaqla ifadə etmək istədik: “Kibercinayətlər kiberməkanda İKT və kompüter informasiyasının istifadəsi ilə törədilən cinayətlərdir”.

11. AR-in cinayət və inzibati xətlər qanunvericiliyində informasiya hüquq pozuntularının hüquqi təsnifatı o qədər də uğurlu aparılmamışdır. Birincisi, Cinayət Məcəlləsinin “Kibercinayətlər” adlı fəslində nəzərdə tutulan əməllər qeydə alınmış informasiyaya, daha dəqiq desək verilənlərə qəsd edən əməllərdir. Konvensiyanın özündə Cinayət Məcəlləsinin “kibercinayətlər” adlandırdığı əməllər “kompüter verilənləri və sistemlərinin konfidensiallığı, tamlığı və əlyetərliyinə qarşı cinayətlər” adlandırılmışdır və bu, daha düzgündür.

12. Hüquqi tədbirlər kibercinayətkarlığın qarşısının alınmasında və onunla mübarizədə əsas rol oynayır ki, bura kiberepozuntuların kriminallaşdırılması və inzibati məsuliyyətin, eləcə də internet provayderlərin məsuliyyətinin müəyyən olunması, prosessual səlahiyyətlər və yurisdiksiyanın tənzimlənməsi, beynəlxalq əməkdaşlıq daxildir. İlkin dövrlərdə milli səviyyədə həm mövcud, həm də yeni (və ya planlaşdırılan) qanunvericilik aktları yalnız kriminallaşdırma ilə əlaqədar idisə, hal-hazırda dünya ictimaiyyəti xüsusi səhəvi normaların yenidən redaktəsinə üstünlük verir. İnformasiya hüquq pozuntuları təcrid olunmuş bir məsələ deyildir, yalnız qlobal kibertəhlükəsizlik şüuruna və qlobal potensialın

artırılmasına ehtiyac duyan hərtərəfli, əməkdaşlıq edən, qlobal bir yanaşma ilə mübarizə edilə bilər.

13. İnformasiya-hüquq pozuntularının qarşısının alınması üçün həm təşkilati, həm də maddi əsaslarla universal və regional əməkdaşlıq tələb olunur. Dövlətlərarası əməkdaşlığın əhəmiyyəti mərkəzləşmə və müstəqilliyin saxlanması ilə bağlıdır. Maddi əsaslara gəldikdə isə, kiberməkanda törədilən pozuntuların yalnız bir dövlətin məsələsi olmadığı artıq qeyd olunmuşdur. Bu baxımdan, əməkdaşlığın təşkili mükəmməl səviyyədə olmalıdır.

14. Cəmiyyət həyatının “kiberməkana transferi” hüquqi qeyri-müəyyənliyin artmasına gətirib çıxarmışdır. Həm fiziki, həm də hüquqi şəxslərin (şirkətlər və digər təşkilatlar) fəaliyyəti müvafiq qanunlarla tənzimlənir. Oflayn mühitdə tətbiq olunan qanunu müəyyən etmək çox asandır. Lakin onlayn mühitdə bu iş olduqca çətin və mürəkkəbdir. Hal-hazırda internet və ya kiberməkanda yurisdiksiya məsələlərini tənzimləyən vahid normativ mənbənin olmaması informasiya hüquq pozuntuları üzrə icraat zamanı çox böyük çətinliklər yaradır. Doğrudur, Budapeşt Konvensiyasında yurisdiksiya ilə bağlı məsələlər tənzimlənir. Lakin tədqiqat zamanı qeyd etdiyimiz kimi, Konvensiyayı ratifikasiya edən 66 dövlət heç də bütün dünya dövlətlərini əhatə etmir. Ona görə də unifikasiya olunmuş beynəlxalq-hüquqi sənədin qəbul edilməsinə zərurət vardır.

15. İnformasiya-hüquqi məsuliyyətlə bağlı ən problemlı məqam qanunvericiliyin əksər normalarında İKT-dən istifadənin ağırlaşdırıcı hal hesab edilməsidir. Rəqəmsallaşmanın dinamikasını nəzərə alaraq, İKT-nin tətbiqini ağırlaşdırıcı hal kimi qəbul etmək məntiqə uyğun sayıla bilməz. Belə tətbiq də digər üsullardan biri kimi qəbul edilməlidir.

16. İnformasiya-hüquq pozuntuları ilə mübarizə, həmçinin onların artma səbəblərinin də minimuma endirilməsi təqdirdə uğurla nəticələne bilər. Bu səbəblər, bir tərəfdən kiberməkanın hüquqi və texniki tənzimlənməsində problemlərlə əlaqədardırsa, digər tərəfdən ayrı-ayrı şəxslərin məlumatlılıq səviyyəsinin aşağı olmasından asılıdır.

Dissertasiyanın əsas müddəaları iddiaçının aşağıdakı elmi əsərlərində öz əksini tapmışdır:

1. Information offense or cybercrime: an international and national-international approach // - Bakı: International law and integration problems, - 2020. № 1(59), - p. 52-56.

2. İnformasiya hüquq pozuntuları və kibertəhlükəsizlik: beynəlxalq-hüquqi tənzimetmədə problemlər // “Müasir dövrdə hüquq sahələrinin qarşılıqlı əlaqəsi və tətbiqi: nəzəriyyə və təcrübə” mövzusunda beynəlxalq elmi-praktiki konfransın materialları, 2020, Bakı: - s. 366-370.

3. Theoretical and legal approaches to the classification of information-legal violations // - Київ: Право України, - 2021. № 9, p. 144–154.

4. İnformasiya hüquq pozuntularının qarşısının alınmasına dair universal və regional normaların təhlili // - Bakı: Azərbaycan Hüquq Jurnalı, - 2021. № 1, - s. 98-108.

5. Hüquqi şəxslərin informasiya-hüquqi məsuliyyəti: Azərbaycan Respublikasında elektron idarəetmənin formalaşdırılması və informasiya-hüquqi məsuliyyət institutuna yeni yanaşma təhlili // - Bakı: Polis Akademiyasının Elmi Xəbərləri, - 2021. № 4 (32), - s. 103-112.

6. Fiziki şəxslərin informasiya-hüquqi məsuliyyəti // - Bakı: Nəqliyyat hüququ, - 2021. № 1, s. 207–216.

7. Traditional and non-traditional elements in the content of information offenses: act as a major factor changing the nature of information offenses // - International Halich Congress On Multidisciplinary Scientific Research, 2021, İstanbul: - p. 271-275.

8. Kibercinayətlər: rəsmi və qeyri-rəsmi təsnifat // “XXI əsr, yeni çağırışlar və hüququn müasir inkişaf tendensiyaları” mövzusunda beynəlxalq elmi-praktiki konfransın materialları, - 21–22 dekabr, 2021, Bakı: - s. 217-218.

9. İnformasiya hüquq pozuntularının qarşısının alınması və informasiya təhlükəsizliyinin təminatı: texniki, təşkilati və hüquqi problemlərin həlli yolları // Doktorantların və gənc tədqiqatçıların XXIV Respublika elmi konfransın materialları, 2021, Bakı: - s. 150-153.

10. İnformasiya hüquq pozuntuları və informasiya-hüquqi məsuliyyət: nəzəri və təcrübi aspektlər// - Bakı: Azərbaycan Hüquq Jurnalı, - 2022. № 3, - s. 62-67.

Dissertasiyanın müdafiəsi “29” “sentyabr”
“2023” il tarixində saat “10:00” Bakı Dövlət
Universiteti nəzdində fəaliyyət göstərən FD 2.44 Dissertasiya
şurasının iclasında keçiriləcək.

Ünvan: AZ 1148, Bakı şəhəri, Zahid Xəlilov-33, I korpus, auditoriya
002.

Dissertasiya ilə Bakı Dövlət Universitetinin kitabxanasında tanış
olmaq mümkündür.

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

Avtoreferat “18” “iyul” “2023”
il tarixində zəruri ünvanlara göndərilmişdir.

Çapa imzalanmışdır: 13.07.2023.
Formatı: 60x84 1/16.
Həcmi: 2 ç.v.
Sayı:100

“Adiloğlu” MMC-də çap edilmişdir.

Ünvan: Bakı şəh., Tbilisi pr.,3007-ci məhəllə, 44 C
Tel.: (050) 593 27 77, (055) 339 75 77
E-mail: adiloglu2000@gmail.com

