1.1. Transmilli cinayət kimi kibercinayətlərin anlayışı: fərqli tendensiyalar və konseptual baxışlar

Müasir dövrdə informasiya cəmiyyətinin inkişafı, qloballaşmanın daha geniş məkanlara, o cümlədən informasiya mühitinə sirayət etməsi bu sahədə transmilli cinayətlərə və dünya ölkələrinin milli hüququnda yeni cinayətlər kateqoriyasının formalaşmasına, bu cinayətlərlə mübarizəyə və cəza sisteminə öz əhəmiyyətli təsirini göstərmişdir. Beynəlxalq sistemdə İKT-nin inkişafı ilə əlaqədar fəaliyyətlər və səmərəli idarəetmə bu sistemin hüquqi cəhətdən nizamlanmasını zəruri etmişdir. Bu mənada beynəlxalq birliyi qlobal informasiya mühitinin hüquqi tənzimləməsi, xüsusilə bu məkanın cinayətkar qəsdlərdən mühafizəsi olmadan təsəvvür etmək mümkün deyil və bu, sosial tənzimetmənin mühüm vasitəsi kimi çıxış edərək, orada fəaliyyət göstərən subyektlərin qanuni maraqlarının reallaşdırılmasını təmin etməklə ictimai münasibətlərin nizamlanmasına xidmət edir. Kompüter sistemləri, şəbəkə və proqramlarının, İKT, habelə internetin fəaliyyəti ilə əlaqədar meydana çıxan ictimai münasibətlərin effektli şəkildə tənzimlənməsi üçün bu cür mexanizmlərin seçilməsi və tətbiqi olduqca mühüm əhəmiyyət kəsb edir. Virtual məkanın inkişafı, kompüterlər şəbəkəsinin geniş istifadəsi detallı hüquqi reqlamentasiya tələb edir. Hüquqi tənzimləmənin zəifliyi nəticəsində bu gün kompüter cinayətləri cinayətkar qəsdlərin ən təhlükəli növünə çevrilmişdir.[1]

Hazırda beynəlxalq praktikada kompüter sistemlərinin və şəbəkələrinin, o cümlədən internetin tənzimlənməsi sahəsində tətbiq edilən hüquqi mexanizmlər bunlardır: qanunvericilik normaları, sosial normalar, özünütənzimləmə, məhkəmə təcrübəsi, beynəlxalq hüquq.

Bu mexanizmlər isə hazırda internet hüquqlarının və insan haqlarının inkişafı ilə əlaqədar olaraq biri-biri ilə daha da sıx bağlı fəaliyyət göstərir. Burada ilk növbədə ümum məcburi hüquq normalarına cəmiyyət daxili zərurət və ya ehtiyac yaranır. Elmi-texniki tərəqqi bəzi hallarda neqativ ictimai təzahürlərlə, xüsusilə bir sıra cinayətlərlə müşayiət olunur. Daha sonra, buna adekvat olaraq dövlətlərin hüquq normaları yaratma fəaliyyətləri inkişaf edir. Hazırda qlobal şəbəkədə və informasiya kommunikasiyalarının inkişafı ilə əlaqədar mövcud olan texnoloji fəaliyyətin prioritet sahələrində əsas insan hüquq və azadlıqlarının, söz və ifadə azadlığının, şəxsi həyatın, şəbəkə istifadəçiləri haqqında məlumatların, habelə onların əqli mülkiyyət hüquqlarının qorunması, xüsusilə müasir informasiya cəmiyyəti üçün daha aktual olan problem – kibercinayətkarlıqla mübarizə məsələləri ön planda çıxış edir.

Ona görə də kibercinayətlərin anlayışı və əsas xüsusiyyətlərinə nəzəri və normativ yanaşma bu günkü dönəm üçün olduqca vacibdir.

Bu problemlə bağlı çoxsaylı elmi əsərlər yazılmış və kibercinayətlərin anlayışının ilə bağlı cəhdlər edilərək, nəzəri cəhətdən araşdırılmış, xarici ölkələrin milli hüquq normalarının qarşılıqlı təhlili əsasında məsələyə akademik münasibət sərgilənmişdir.[2]

Müasir beynəlxalq hüquqda kiberməkan quru, su və hava məkanları kimi bütün dövlətlərin hüquqi cəhətdən tənzimlənməsi və əməkdaşlıq etməsi zəruri olan sahələrdən biridir. Bu mənada onlar arasında bağlanan kibermüqavilələr də öz növbəsində beynəlxalq hüquqi cəhətdən xüsusi əhəmiyyətə malikdir. Eyni zamanda, həmin müqavilələrdə kibercinayətlərin anlayışı və təsnifatı, kibercinayətlərə görə beynəlxalq hüquqi məsuliyyət məsələlərinin də öz əksini tapması zəruridir. Bu məkanın sabitliyi, təhlükəsizliyi universal və regional təşkilatlar tərəfindən müqavilə əsasında tənzimlənməlidir. Həmçinin, bu məkanda baş verən cinayətlər üzrə hüquqi mühakimə dövlətdaxili və beynəlxalq məhkəmələrin qarşılıqlı əlaqəsi və əməkdaşlığı ilə daha çox səmərəli nəticələr verə bilər.

İnternet istifadəçilərinin hüquqazidd davranışları bəzən cinayət tərkibi yaradan əməllərin törədilməsinə səbəb olur. Buna görə də, müasir beynəlxalq hüquqda mövcud sosial-iqtisadi inkişaf, elmi-texniki tərəqqi və İKT üzrə yeniliklərdən asılı olaraq beynəlxalq xarakterli cinayətlərin də diapazonu dəyişir və genişlənir. Bu mənada hazırda veb-məkan üçün aktual olan cinayət tərkiblərindən biri kibercinayətkarlıqdır (kompüter cinayətkarlığı). Bu əməllər müasir dövrdə rəqəmsal texnologiyaların, kompüter və internet şəbəkələrinin, bankomatların, ödəniş kartlarının, ödəmə terminallarının və s. cinayətkar məqsədlərlə istifadəsi ilə əlaqədar cinayət xarakteri kəsb etmişdir. İctimai qayda əleyhinə yönələn bu cinayətlər həm milli, həm də beynəlxalq hüquqi tənzimetmənin predmetini təşkil edir. Müasir beynəlxalq hüquqda isə bu məsələlər internet hüququ və beynəlxalq cinayət hüququ kontekstində nəzərdən keçirilir.

Əlbəttə, müasir qloballaşma prosesləri müəyyən mənada cinayətkarlığın, o cümlədən, kibercinayətlərin inkişafına da rəvac vermişdir. "Kurs uqolovnoqo prava" kitabının müəllifləri hesab edirlər ki, XX əsrdə beynəlxalq cinayət hüququ cinayətkarlığın qloballaşması prosesinə adekvat surətdə inkişaf etmişdir. Digər cinayətlərlə yanaşı onlar kompüter cinayətlərini də ən təhlükəli cinayətlər kateqoriyasına aid etməklə, bu əməlləri yalnız milli cinayətlər saymayıb, onların beynəlxalq cinayətlərə çevrildiyini əsaslandırırlar.[3]

İctimai həyatın müasir qlobal inkişaf şəraiti informasiya texnologiyaları, telekommunikasiyalar, yaxud bütövlükdə kiberməkan olmadan təsəvvür edilə bilməz. Dr. Tatyana Tropina hesab edir ki, müasir dövrdə İKT o qədər surətlə inkişaf edir ki, bəzən qanunvericilik və hüquq-mühafizə orqanları bu inkişafa adekvat reaksiya

---

[1] Бикбаева Э. А. Компьютерные преступления в Уголовном Кодексе РФ. "Современные проблемы юридической науки". Часть II. Материалы VII Международной научно-практической конференции молодых исследователей. Челябинск, Издателство "Цицеро" 2011.с. 129. 233 с.

[2] Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity Press. International Telecommunication Union, 2011. Understanding Cybercrime: A Guide for Developing Countries; Explanatory Report to the Council of Europe Cybercrime Convention, ETS No. 185; Pocar, F., 2004. New challenges forinternational rules against cyber-crime. European Journal on Criminal Policy and Research, 10(1):27-37; Wall, D.S., 2007. Наумов В.Б., Право и Интернет: Очерки теории и практики, М.: Книжный дом "Университет", 2002; Номоконов В.А., Тропина Т.Л. Киберпреступность: прогнозы и проблемы борьбы. Библиотека криминалиста. № 5(10) 2013; Hasan Sınar, İnternet ve Ceza Hukuku, İstanbul, 2001; Savin A. EU internet law. Elgar European law. 2013;

[3] Курс уголовного права. В 5 томах. Том 5. Особенная часть. М., 2002. С. 346.

vermək imkanından uzaq olurlar.[4] Bu xüsusilə özünü kiberməkanın tənzimlənməsində daha bariz şəkildə göstərir.

Yeni yaranan qlobal sistemlər, informasiya texnologiyaları, bütövlükdə hüquq sistemləri, xüsusilə əsas insan hüquq və azadlıqlarına hörmət prinsipi əsasında insan və vətəndaş hüquqlarına münasibətdə zəruri qanunvericilik və təşkilati mexanizmlərin yaradılması üzrə mühüm addımların atılmasını tələb edir. Bu mənada hüquq elmləri doktoru, professor Əmir Əliyev haqlı olaraq qeyd edir ki, dünya proseslərinin qloballaşması insan hüquqlarına yeni yanaşmalar müəyyən edir, lakin onların ümumi başlanğıc prinsiplərini dəyişdirmir. Bununla yanaşı insan hüquq və azadlıqlarına yeni situasiyalarla əlaqədar bir sıra düzəlişlərin edilməsi də qaçılmazdır.[5]

Qeyd etmək lazımdır ki, informasiya kommunikasiya texnologiyaları proseslərinin dünya hüquq sisteminə təsiri bir sıra çətinliklərlə xarakterizə olunmuşdur. Bu səbəbdən də professor R.Əliquliyev qeyd edir ki, ölkənin real təhlükəsizliyinin qorunması üçün müxtəlif texnologiyalar, sərhədlər var. Amma virtual mühit artıq müəyyən məkanla bağlı deyil. Burada dünyanın istənilən ölkəsi bizim qonşumuzdur və ya əksidir. Belə bir şəraitdə virtual məkanın təhlükəsizliyinin təmin olunması çox çətindir". R.Əliquliyevin sözlərinə görə, digər bir məsələ 40-50 ildə formalaşan virtual məkanın özünün beynəlxalq hüquq sisteminin olmamasıdır: "Bu sistem yoxdur ki, qadağalar ortaya çıxsın, bu əməli törədənlər cinayət məsuliyyətinə cəlb olunsun. Bu gün dünyanı narahat edən əsas sual odur ki, hansı daha ağıllı texnikadan istifadə etməklə informasiya təhlükəsizliyinə qarşı mübarizə aparmaq olar?[6] Lakin professorun bu fikirləri ilə müəyyən mənada razılaşmaq olmaz. Çünki, bu gün artıq müasir dünyada kiberməkanın təhlükəsizliyinə təminat verən həm beynəlxalq hüquqi sistem, həm də milli normativ hüquqi sistemlər formalaşmış və bu proses davam etməkdədir.

Müasir dünyamızın sakinləri ictimai münasibətlərin, demək olar ki, bütün sahələrində istifadə edilən informasiya texnologiyalarından bu və ya digər dərəcədə asılıdır. İnkişaf etmiş dövlətlər informasiya texnologiyalarından fəal istifadə etməklə məlumat mübadiləsini sürətləndirir və insan resurslarına qənaət edirlər. Fəal məlumat mübadiləsi prosesləri cəmiyyətin şəffaflığına təsir göstərir, dövlət idarəçiliyini daha səmərəli edir, vətəndaş cəmiyyətinin formalaşmasına xidmət edir. İctimai həyatda "elektron demokratiya", "elektron dövlət" adlandırılan müasir idarəetmə formaları meydana gəlir. Bu proses qarşısıalınmazdır və o, dövlət hakimiyyətinə bu prosesi necə idarə etmək, ədalətin, insan hüquqlarının və sosial bərabərliyin təmin olunması, dövlət hakimiyyətinə inam və digər demokratik dəyərləri qorumaqla elektron aləmi necə tarazlaşdırmaq kimi konkret sxemlər təqdim edir. Alimlərin fikrincə, yaxın zamanlarda orta şəxsi kompüterlər insan beyninin imkanlarını ötüb keçəcək, 2029-cu ildə elektron intellekt insanın əqli qabiliyyətindən 1000 dəfə artıq olacaq. Əlli milyonluq auditoriyanı əhatə etmək üçün radioya 38, televiziyaya isə 13 il lazım olmuşdur. 1993-cü ildə qlobal şəbəkədə yalnız 50 səhifə olduğu halda, bu gün onların sayı milyardlarladır. Ötən il dünyada internet istifadəçilərinin sayı 3,8 milyardı keçib. Bu da dünya əhalisinin yarıdan çoxunu təşkil edir. İnternet istifadəçilərinin 53%-i Asiya-Sakit Okean, 15%-I Avropa, 13%-i Afrika və Orta Şərq, 10%-i Latın Amerika, 9%-i Şimali Amerika, 21%-i Cin, 12%-I Hindistan və ABŞ-ın payına düşüb. İnternetdən istifadə edən dünya əhalisinin göstəricisi 2009-cu ildə 24 faiz idisə, keçən il bu rəqəm 51 faizədək artıb.[7] Bu isə İKT-nin dinamik inkişafını və ictimai münasibətlərə, o cümlədən milli və beynəlxalq hüquqa da təsirini şərtləndirir.

Bütün cəmiyyətlərdə cinayətlər həmin cəmiyyətin inkişaf tendensiyasına uyğun paylanır. Ona görə də prof. Y.S.Romaşev qeyd edir ki, XX əsrin 80-90-cı illərinə qədər kompüter texnologiyasının istifadəsi ilə bağlı cinayətlərin payı çox da böyük olmamışdır. Lakin zəhmətsiz qazanc məqsədilə və əyləncə naminə kompüter şəbəkələrindən qanunsuz istifadə, uşaq pornoqrafiyasının yayılması, kompüter və informasiya sistemlərinin dağıdılması təhlükəsi, habelə kompüter şəbəkəsindən dələduzluq məqsədilə istifadə olunması kompüter cinayətlərinin adi formalarından hesab olunur.[8]

Bir sıra əlamətlərinə görə kibercinayətlərin beynəlxalq və milli hüquq prizmadan aşağıdakı növləri fərqləndirilir: kompüter məlumatlarının və sisteminin konfidensiallığı, bütövlüyü və əlverişliliyi əleyhinə cinayətlər, kompüterlə əlaqəli cinayətlər, məzmununu kompüter informasiyası təşkil edən hüquq pozuntuları, uşaq pornoqrafiyası ilə əlaqəli materiallarla bağlı hüquqazidd əməllər, müəlliflik və əlaqəli hüquqların pozulması ilə bağlı cinayətlər.

Bu məsələdə dünya hüquq ədəbiyyatında müxtəlif yanaşmalar ortaya qoyulur və fərqli terminlər təklif olunur. Türkiyəli professorlar Z.Afşar və G.Ongörən kompüterlər və şəbəkələr vasitəsilə törədilən cinayətləri Türk Cəza Qanununa istinad edərək iki qrupa ayırırlar: informasiya və kompüterlə əlaqədar cinayətlər (bilişim ve ya bilgisayarla ilgili suçlar) və İnternet vasitəsilə törədilən cinayətlər ("İnternet yoluyla işlenen suçlar).[9]

Qeyd etmək lazımdır ki, kibercinayətlərin anlayışı məsələsində beynəlxalq təşkilatların, o cümlədən Birləşmiş Millətlər Təşkilatının xüsusi yanaşması da elmi araşdırma baxımından əhəmiyyətli hesab olunur. Bu məsələyə BMT səviyyəsində münasibət bildirilməsi ona görə zəruridir ki, kibercinayətlər müasir dövrdə yalnız bir dövləti və onun milli sərhədlərini əhatə etməyərək, eləcə də bütövlükdə dünya birliyinin narahatlıq mövzusuna çevrilmişdir. BMT tərəfindən kibercinayətlərin standart tərifi Cinayətlərin qarşısının alınması və cinayətkarlıqla mübarizə üzrə BMT-nin X Konqresində müəyyən olunmuşdur. Həmin Konqresin bir seminarı kompüter

[4] Tropina, T., Self- and Co-regulation in Fighting Cybercrime and Safeguarding Cybersecurity. In: Jahnke at al. (eds.), "Current Issues in ITU Security", Duncker & Humblot, Berlin, 2012. c. 155

[5] Əliyev. Ə. Müasir beynəlxalq hüquqda insan hüquqları, əhali və miqrasiya problemləri. Dərslik, Bakı- 2007. Səh 14. 488 s.

[6] Huseynzadə F. Kibercinayətkarlıqla bağlı ayrıca qanunun qəbul olunmasına ehtiyac görülür. Paritet, 2012. - 20-21 noyabr, № 123.-C.10. 4.

[7] Dünyada internet istifadəcilərinin sayı 3,8 milyardı kecib. https://report.az/i-kt/dünyada-internet-istifadecilerinin-sayi-3-8-milyardi-kecib/

[8] Ромашев Ю.С. Международное правоохранительное право. М.2010. с.253

[9] Bilişim Hukuku. Prof. Dr. B. Zakir Avşar, Prof. Dr. Gursel Ongören. İstanbul, 2010. s.180

şəbəkələrinə dair cinayət problemlərinə həsr olunmuş, kibercinayətlərin iki əsas növü fərqləndirilərək, onun anlayışı aşağıdakı kimi müəyyən edilmişdir:

1. Dar mənada kibercinayətlər (kompüter cinayətləri). Bu o deməkdir ki, elektron əməliyyatlar vasitəsilə yönəldilən hər hansı qeyri-qanuni hərəkət və hərəkətsizliyin məqsədi kompüter sistemlərinin təhlükəsizliyinə və onlarda olan məlumat (verilənlər) bazasına xələl gətirməkdir.

2. Geniş mənada kibercinayətlər (kompüter ilə əlaqədar cinayətlər). Bu isə o deməkdir ki, hər hansı qeyri-qanuni hərəkət və hərəkətsizlik kompüter sistemləri və ya şəbəkələri, o cümlədən belə cinayətlər informasiyaların kompüter sistemləri və ya şəbəkələrindən qanunsuz olaraq əldə edilməsi, təklif olunması və yayılması vasitəsilə və ya onlarla əlaqəli şəkildə törədilir.

Lakin bir məsələni xüsusi vurğulamaq lazımdır ki, "kompüter cinayəti" anlayışının beynəlxalq hüquq müstəvisində ilk dəfə istifadəsi İnterpola məxsusdur.[10] Belə ki, İnterpolun 11-13 dekabr 1979-cu ildə keçirilmiş Üçüncü Beynəlxalq Dələduzluq üzrə Simpoziumunda "kompüter dələduzluğu" haqqında prezentasiya təqdim olunmuş və vurğulanmışdır ki, müxtəlif ölkələr arasında telefonlar, peyklər və s. vasitəsilə davamlı şəkildə artan kommunikasiyalar səbəbindən kompüter cinayətlərinin təbiəti artıq beynəlxalq xarakter kəsb edir. Beləliklə də, beynəlxalq hüquq tarixində ilk dəfə kompüter cinayətləri lokal səviyyəli kriminal aktlar çərçivəsindən çıxmaqla, İnterpol tərəfindən transmilli mahiyyətli əməllər olaraq hələ XX əsrin ikinci yarısından başlayaraq tanınmış və faktiki surətdə dövlətlərin milli cinayət qanunvericiliyi üçün tövsiyə olunan "kompüter cinayətləri" terminindən istifadə olunmağa başlanmışdır.

Qeyd etmək lazımdır ki, kibercinayətlər hələ bir çox dövlətlərin daxili qanunvericiliyinə tam implementasiya olunmadığı üçün bu əməllərin cinayət xarakteri kəsb etmələrinə münasibətdə ayrı-ayrı dövlətlərdə fərqliliklərin olması labüddür.

Xarici ölkələrin qanunvericiliyinin ümumiləşdirilmiş təhlili göstərir ki, dünyanın heç bir dövlətinin milli normaları "kibercinayət" anlayışının dəqiq tərifini verə bilməmiş, onun növləri ilə bağlı yekdil rəyə nail olmamışdır. Lakin, bir sıra ölkələrin qanunvericilərinin araşdırılması zamanı bu cinayətə münasibətdə müxtəlif terminlərin – kompüter cinayətləri[11], kibercinayətlər[12], elektron kommunikasiyalar[13], informasiya texnologiyaları[14], yüksək texnologiya cinayətləri (high-tech crimes)[15] – mövcudluğu diqqəti cəlb etmişdir.

Bu terminlər arasındakı oxşarlıqlar və fərqlər də mübahisə predmetidir. Rusiyalı hüquqşünas alimlər Nomokonov V.A və Tropina T.L. özlərinin birgə məqaləsində qeyd edirlər ki, "kibercinayətkarlıq" termini adətən "kompüter cinayətkarlığı" termini ilə birgə istifadə olunur, lakin bu anlayışlar heç də sinonim deyildir. Onların fikrincə, həqiqətən də bu terminlər biri-birinə çox yaxın olsalar da, bütün hallarda həmçinin fərqlənirlər. Belə ki, "kibercinayətkarlıq" termini "kompüter cinayətkarlığı" terminindən daha geniş anlayış olub, informasiya məkanında törədilən cinayət olaraq bu hadisənin mahiyyətini daha dəqiq əks etdirir.[16] Qeyd olunan fikirlərlə razılaşaraq, "kibercinayətkarlıq" və "kompüter cinayətkarlığı" terminlərinin hüquqi məna etibarilə biri-birindən fərqləndiyini əsas gətirir və məhz bu kontekstdə "kibercinayətlər"in anlayışının müəyyən olunması istiqamətində səylərin davam etdirilməsini məqsədəuyğun hesab edirik.

Şəbəkə və kompüter cinayətləri terminə münasibətdə prof. Marko Gerke qeyd edir ki, kibercinayət termini bir sıra cinayətləri, o cümlədən ənənəvi kompüter cinayətlərini, eləcə də şəbəkə cinayətlərini ifadə etmək üçün istifadə olunan anlayışdır. "Bu cinayətlər bir sıra xüsusiyyətlərə görə fərqlənir. Belə ki, problemlə bağlı müxtəlif beynəlxalq hüquqi yanaşmalarda kibercinayət məfhumuna daxil olan bütün hərəkət və hərəkətsizliklər üçün vahid bir kriteriya olmadığından, buraya yalnız kompüter aparatlarından istifadə edilməklə törədilən cinayətlər aid edilir".[17] Göründüyü kimi, isveçrəli alimin bu fikirləri kibercinayətlərin anlayışının müəyyən edilməsi üçün bir növ acar rolunu oynaya bilər. Çünki, bu cinayətlə əlaqədar vahid kriteriya kimi, "kompüter aparat və qurğularından istifadə" və "şəbəkədən istifadə" elementlərinin olması kifayət edir ki, müfəssəl bir anlayış ortaya qoyula bilsin.

Missisipi Universitetinin Hüquq Məktəbinin alimləri kibercinayət anlayışı ilə bağlı konsensusun olmadığını qeyd edərək vurğulayırlar ki, istənilən cinayət kimi, "kibercinayət" haqqında da demək olar ki, burada kompüter və ya başqa rəqəmsal qurğular aparıcı rol oynadığından, kompüter cinayətlərinin istənilən qanunla müəyyən edilmiş tərifinin verilməsindən asılı olmayaraq ona rəqəmsal əlamət daxil edilir.[18] Bu fikirlərdən belə nəticə hasil olur ki, əslində kibercinayət termini daha çox özündə rəqəmsallıq əlamətini ehtiva etməlidir.

Kibercinayətləri nadir cinayətlər kateqoriyasına aid edən İspaniyanın Kataloniya Universitetinin professoru J.R.Aqustina isə bu termini həddindən artıq ümumi hesab edir. Hüquqşünas alimin fikrincə, bu cinayətlərə internetdən istifadə etməklə törədilən dələduzluq, insanların narahat edilməsi və ya onlara qarşı xuliqanlıq, qanunsuz pornoqrafiyanın yüklənilməsi, musiqilərin oğurlanması, milli təhlükəsizliyin pozulması kimi əməllər

---

[10] Third Interpol Symposium on International Fraud, Paris 11-13 December 1979. Computer Fraud & Security, ISSN 1361-3723 February 2012. p. 11. 20 pp

[11] Bax, Malaysia, Computer Crimes Act 1997; Sri Lanka, Computer Crime Act 2007; Sudan, Computer Crimes Act 2007.

[12] Azərbaycan Respublikasının Cinayət Məcəlləsində dəyişikliklər edilməsi haqqında Azərbaycan Respublikasinin Qanunu, Bakı şəhəri, 29 iyun 2012-ci il № 408-IVQD.

[13] Albania, Electronic Communications in the Republic of Albania, Law no. 9918 2008; France, Code des postes etdes communications electroniques (version consolidee) 2012; Tonga, Communications Act 2000.

14 India, The Information Technology Act 2000; Saudi Arabia, IT Criminal Act 2007; Bolivarian Republic of Venezuela, Ley Especial contra los Delitos Informaticos 2001; Vietnam, Law on Information Technology 2007.

15 Serbia, Law on Organization and Competence of Government Authorities for Combating High-Tech Crime 2010.

16 Номоконов В.А., Тропина Т.Л. Киберпреступность: прогнозы и проблемы борьбы. Библиотека криминалиста. №5(10) 2013. С. 148 -160.

[17] Understanding cybercrime: phenomena, challenges and legal response. Prepared by Prof. Dr. Marco Gercke. Geneva, 2012, p.11, 356

[18] Cybercrime strategies - Coe - Council of Europe, https://rm.coe.int/16802fa3e1

aiddir.[19] Kibercinayətlərlə bağlı qeyd olunan bu mülahizə birincisi, onun genişləndirilmiş tərifinin ortaya qoyulması istiqamətində mühüm addım hesab olunmalıdır. Digər tərəfdən isə, bu tərifdən aydın olur ki, kompüter proqramları və qlobal şəbəkəyə aid olan bütün hüquqazidd hərəkətlər kibercinayət əməli kimi qəbul edilməlidir.

"İnternet hüququ və etikası" kitabında kibercinayətlərə aşağıdakı anlayış verilmişdir: "Kibercinayətlər dedikdə, internet şəbəkəsindən qanunsuz istifadə nəticəsində kompüter və informasiya sistemlərinın dağıdılması və virtual məkanda qəsdən törədilən digər cəzalandırılmalı, hüquqazidd ictimai təhlükəli əməllər başa düşülür".[20] Bu tərifdən göründüyü kimi, "kibercinayət" anlayışı təkcə bir kompüterdə və ya lokal informasiya məkanında törədilən qanunsuz əməl olmayıb, eyni zamanda, bu fəzada bütün texnoloji vasitələr arasında əlaqələndirici rolunda çıxış edən internet vasitəsilə törədilən çoxsaylı hüquqazidd əməlləri də əhatə edir.

Təcrübi baxımdan qeyd etmək zəruridir ki, kompüterlərə qanunsuz müdaxilə və informasiya sistemlərinə hücumlar müasir beynəlxalq hüquqla və milli qanunvericiliklə kriminallaşdırılan əməl hesab olunur. Lakin, terminologiyaya münasibətdə xarici ölkələrin qanunvericiliklərindən görmək mümkündür ki, onlarda bu sahəyə aid qanunun ya adı "Kibercinayətlər haqqında Qanun" (Cybercrime Act), ya da Cinayət Məcəlləsinin müvafiq bölməsinin və ya fəslinin adı "Kibercinayətlər" adlandırılır. Amma qeyd olunmalıdır ki, əksər Avropa ölkələrinin qanunvericiliklərində kibercinayətlər ayrıca fəsil və ya bölmə şəkilində müvafiq qanunda təsbit olunmuşdur. Məsələn, kibercinayətlərlə bağlı bu yanaşma Bolqarıstan Cinayət Məcəlləsinin 9-cu bölməsində öz əksini tapmaqla, bu ölkənin milli cinayət qanunvericiliyi xüsusi olaraq qanunun müvafiq bölməsini kibercinayətlər adlandırır və bu sahəyə aid normaları həmin bölmədə unifikasiya etmişdir.[21] Qeyd olunan mövqe dünyanın əksər ölkələrinin qanunvericiliklərinə xasdır.

Əlbəttə, bu praktika daha təkmil və səmərəli olduğu üçün Azərbaycan qanunvericiliyi də bu təcrübəyə istinad etmişdir. Belə ki, ölkə Prezidenti cənab İlham Əliyevin 27 dekabr 2011-ci il tarixli Sərəncamı ilə təsdiq olunmuş Azərbaycan Respublikasında insan hüquq və azadlıqlarının müdafiəsinin səmərəliliyini artırmaq sahəsində Milli Fəaliyyət Proqramının 1.2.4-cu maddəsinə görə informasiya texnologiyalarından istifadə etməklə insan hüquqlarının pozulmasına qarşı mübarizənin səmərəliliyinin artırılması məqsədilə Azərbaycan Respublikası Cinayət Məcəlləsinin "Kompüter informasiyası əleyhinə olan cinayətlər" fəslinin yenidən işlənməsi və onun "Kibercinayətkarlıq haqqında" 2001-ci il 23 noyabr tarixli Konvensiyanın tələblərinə uyğunlaşdırılması barədə təkliflərin hazırlanması tapşırığı qoyulmuşdur. Bu məsələ 2012-ci il ərzində özünün normativ əsasda həllini tapmış, Cinayət Məcəlləsinin 30-cu fəsli beynəlxalq hüquqdan implementasiya edilməklə, o cümlədən "Kibercinayətkarlıq haqqında" Konvensiyanın tələblərinə uyğun olaraq, eyni adlı termindən istifadə olunmaqla "Kibercinayətlər" adlandırılmışdır.

Kibercinayətlər haqqında qanunlarla bağlı xüsusi bir yanaşma isə bu sahəyə aid normaların "kibercinayətlərin qarşısının alınması haqqında qanunlarda" öz əksini tapmasıdır. Məsələn, bu istiqamətdə ən yaxşı təcrübə kimi Filippinin 2012-ci il tarixli "Kibercinayətlərin qarşısının alınması haqqında Qanunu"nu misal göstərə bilərik. Bu qanunda da kibercinayət anlayışından daha çox, onun profilaktikası və qarşısının alınması ilə bağlı müddəalar üstünlük təşkil edir.[22] Təqdirəlayiq haldır ki, Filippin qanununda "kibercinayət" və "kiber" terminlərinin hüquqi mənası izah edilmişdir. Belə ki, həmin qanunun 3-cü maddəsinin (i) bəndi "kiber" ifadəsinə kompüter və ya kompüter şəbəkələrində, elektron mediada, habelə onlayn kommunikasiya vasitələrində törədilən hərəkətləri aid edir. Qanunun 4-cü maddəsində isə "kibercinayət əməlləri"nə (cybercrime offenses) aşağıdakı cinayətlər aid edilir: kompüter məlumatları və sistemlərinin konfidensiallığı, bütövlüyü və əlyetərliliyi əleyhinə olan əməllər – bütövlükdə kompüter sistemlərinə və ya onun bir hissəsinin qanunsuz əldə keçirilməsi, informasiyaya qanunsuz çatım, məlumata və sistemə qanunsuz müdaxilə və s.; kompüterlə əlaqəli cinayətlər – kompüter saxtakarlığı, kompüter dələduzluğu, identifikasiya oğurluğu; kontentlə əlaqədar cinayətlər – kiberseks, uşaq pornoqrafiyası, sosial şəbəkədə böhtan və s. Göründüyü kimi, kibercinayətlərin dairəsi qanunda kifayət qədər geniş göstərilmiş və onun müfəssəl təsnifatı ortaya qoyulmuşdur. Bu mənada həmin qanunda nəzərdə tutulmuş bəzi müddəaların digər dövlətlərin, o cümlədən ölkəmizin milli qanunvericiliyinə implementasiyası məqbul sayıla bilər.

Qeyd olunan məsələ ilə bağlı digər bir yanaşma isə ondan ibarətdir ki, əksər ölkələr kiberməkanda hüquqi tənzimləmənin həyata keçirilməsi üçün daha çox "Kibercinayətlər haqqında" xüsusi qanunların qəbuluna üstünlük vermişlər. Bunlara misal olaraq, Seneqalın 2008-ci il və Kambocanın 2012-ci il tarixli Kibercinayətlər haqqında qanunlarını göstərmək olar.[23] Təqdirəlayiq haldır ki, "kibercinayətlər"lə mübarizə məsələsinə münasibətdə müasir milli hüquq sistemləri ilə beynəlxalq hüquq birgə çıxış edirlər və bu kontekstdə biri-birindən o qədər də fərqli mahiyyət kəsb etməyən mövqelər üzərində dayanırlar. Bu sistemlər arasında kibercinayətlərlə bağlı ilkin ümumi yanaşma sadəcə ondan ibarətdir ki, bu sahədə mövcud olan əməllərin məhz hüquq müstəvisinə aid olmasını, kiberməkanda baş verən hadisələri və hüquqazidd davranışları əhəmiyyətli zərərdən asılı olaraq kriminallaşdırmağı prioritet hesab edirlər.

Lakin kibercinayətlərin anlayışı məsələsində ortaq fikir mövcud deyildir. Kibercinayətlərin anlayışının müəyyən olunması ilə əlaqədar eyni yanaşmanı həm beynəlxalq, həm də regional təşkilatların rəsmi mövqeyi və qəbul etdikləri sənədlər də ortaya qoymaqdadır. Həm Avropa Şurası çərçivəsində qəbul olunmuş 2001-ci il

---

[19] Agustina J. R. Book Review of Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891, July – December 2012, Vol 6 (2): p. 1044–1048

[20] Məcidli S.T. "İnternet hüququ və etikası". Dərs vəsaiti. Bakı: "Elm və təhsil" nəşriyyatı, 2013. s 114.

[21] Bulgaria, Chapter 9, Criminal Code SG No.92/2002

[22] Philippines, Cybercrime Prevention Act 2012. Act No. 10175. Ofiicial Qazzete. http://www.gov.ph/2012/09/12/republic-act-no-10175

[23] Bax: Senegal, Law No. 2008-11 on Cybercrime 2008; Cambodia, Draft Cybercrime Law 2012.

Kibercinayətkarlıq haqqında Budapeşt Konvensiyası, həm Ərəb Dövlətləri Liqası tərəfindən qəbul olunmuş (İnformasiya texnologiyaları cinayətləri ilə mübarizə haqqında 2010-cu il tarixli Ərəb Konvensiyası) Konvensiya, həm Afrika Birliyi Konvensiyasının layihəsi (Afrikada kibertəhlükəsizlik fəaliyyətinin hüquqi çərçivəsinin yaradılması haqqında 2012-ci il tarixli Konvensiya layihəsi) bu məsələdə konkret anlayışın verilməsindən yan keçmişlər. Kibercinayətkarlıq haqqında 23 noyabr 2001-ci il Budapeşt Konvensiyasının "Terminlərdən istifadə" adlı birinci fəsli və "Anlayışlar" adlanan 1-ci maddəsində "Kibercinayətkalıq" termininin hüquqi məna yükü açıqlanmır. Orada sadəcə olaraq Konvensiyanın məqsədlərinə nail olmaq üçün bəzi texniki terminlərə – "kompüter sistemi", "kompüter verilənləri", "xidmət provayderi" və s. kimi anlayışlara aydınlıq gətirilmişdir.

Terminologiya məsələsinin izahı doktrinal mövqelərə və ekspert rəylərinə əsaslanır. BMT ekspertlərinin tövsiyələrinə əsasən "kibercinayətkarlıq" termini kompüter sistemlərinin və şəbəkələrinin köməyi ilə, yaxud kompüter sistemlərinə və şəbəkələrinə qarşı həyata keçirilən istənilən cinayət əməlini əhatə edir. Başqa sözlə desək, virtual mühitdə həyata keçirilən cinayət növünü "kibercinayət" adlandırmaq olar.[24]

Qeyd etmək lazımdır ki, "kibercinayətlərin" anlayışı məsələsində MDB dövlətlərinin bu sahəyə aid Müqaviləsində (Kompüter informasiyası sferasında cinayətlərlə mübarizədə MDB iştirakçı-dövlətlərin əməkdaşlığı haqqında Müqavilə) bir qədər irəliləyiş hiss olunmuşdur. Həmin müqavilə "kibercinayət" anlayışını məqsədini kompüter informasiyası təşkil edən kriminal akt kimi "kompüter informasiyasına aid cinayət" hesab edir.

Müasir beynəlxalq hüquqda, xüsusilə yeni yaranan beynəlxalq təşkilatlar çərçivəsində də kibercinayətkarlıqla mübarizə, o cümlədən bu cinayətin anlayışı problemi xüsusi həssaslıqla yanaşılan məsələlərdən biridir. Belə qurumlardan biri də Şanxay Əməkdaşlıq Təşkilatıdır. Kibercinayətlərə münasibətdə bu qurum daha fərqli termindən – "informasiya cinayəti" terminindən istifadə etmişdir. Bu beynəlxalq təşkilat çərçivəsində bağlanmış Müqavilə kibercinayətlərin anlayışını "qanunsuz məqsədlərlə informasiya resurslarının və (və ya) informasiya sferasında onlara təsir etmək üçün istifadəsi" ilə əlaqədar olan əməlləri "informasiya cinayətləri" kimi müəyyən edir.[25]

Qeyd olunmalıdır ki, Şanxay Əməkdaşlıq Təşkilatının istifadə etdiyi "informasiya cinayəti" termini kiberməkanda baş verən proseslərin yalnız informativ cəhətlərini əhatə etməklə, onun texniki tərəflərini, məsələn, elektron köşklərdən, bankomatlardan və digər texniki qurğulardan və ya heç bir şəbəkəyə qoşulmayan aparatlardan istifadə ilə bağlı prosesləri əks etdirmir. Bu mənada "informasiya cinayəti" termini "kibercinayət" terminindən daha dar anlamda dərk olunacaqdır.

Hüquqi baxımından daha dəqiq mənada başa düşülməsi üçün burada əlbəttə, "kiber" anlayışına da diqqətin ayrılması zəruridir. Oksford izahlı lüğətində "kiber" ("cyber") əlavəsi mürəkkəb sözün tərkib hissəsi kimi müəyyən olunur. Onun mənası "informasiya texnologiyalarına, internet şəbəkəsinə və virtual reallığa aid olan" deməkdir.[26] Bu mənada yuxarıda qeyd etdiyimiz fikir – yəni "kibercinayət" termininin həm "kompüter cinayəti", həm də "informasiya cinayəti" terminindən hüquqi, eyni zamanda leksik məna baxımından geniş olması bir daha öz təsdiqini tapır.

Əslində kibercinayətkarlıq elmi kateqoriya kimi təhlil olunarkən, bir sıra digər elmlərin, məsələn informatika, fizika və s. elmlərdə istifadə olunan terminlərə də aydınlıq gətirilməsi zərurəti ortaya çıxır. Belə ki, faktiki olaraq bu cinayət əməlləri "kiberməkan" adlanan ərazidə törədilir. Ona görə də burada kiberməkan anlayışının elmi izahına ehtiyac hiss olunur. Beynəlxalq Elektroəlaqələr İttifaqı (2009) Kibecinayətkarlıq haqqında model qanunda kiberməkanı "kompüterlər, kompüter sistemləri, şəbəkəsi, onların proqramları, kompüter məlumatları, kontent məlumatları, verilənlərin hərəkəti və istifadəçilər şəklində yaradılan və (və ya) formalaşdırılan, fiziki və fiziki olmayan məkan" kimi müəyyən etmişdir.[27]

Göründüyü kimi, müasir dövrdə beynəlxalq hüquqda kibercinayətkalıqla bağlı rəsmi normativ tərifin müəyyən olunması problem olaraq qaldığı kimi, eyni zamanda beynəlxalq əsasda kiberməkanın da rəsmi anlayışının müəyyən olunmasında problemlər qalmaqdadır.

Bütün bunları nəzərə alaraq biz yuxarıda qeyd olunan tərifləri Kembric lüğətində verilən tərifl müqayisəsindən kibercinayət anlayışına bir daha aydınlıq gətirmiş olarıq. Belə ki, həmin lüğətdə kibercinayətə aşağıdakı kimi anlayış verilmişdir: "Kibercinayət" – həm kompüterlərin istifadəsi, həm də informasiya texnologiyalarının və qlobal şəbəkələrin istifadəsi ilə bağlı olan cinayətdir. Bu anlayışların yekun təhlilindən isə belə bir nəticəyə gəlmək mümkündür ki, əslində "kompüter cinayəti" termini əsas etibarilə konkret hər hansı kompüterə qarşı və ya həmin kompüterdə mövcud olan məlumat bazasına yönəlmiş cinayəti özündə ehtiva edir.

Bu səbəbdən də BMT-nin kibercinayətlər üzrə mütəxəssisləri Kibercinayətkarlıq haqqında Konvensiyanı şərh edərkən haqlı olaraq qeyd edirlər ki, "kibercinayət" termini ən yaxşı halda kompüter və informasiyalarla əlaqədar hərəkət və ya davranışların məcmusu hesab olunur.[28]

Kibercinayətlər unikal təbiəti ilə diqqət çəkir. Bəzi mütəxəssislər hesab edirlər ki, bütün kompüter cinayətləri bir sıra fərqli xüsusiyyətlərə malikdirlər. Birincisi, müəyyən olunmuş faktlar üzrə sübutların toplanmasında həddindən artıq qapalılıq və mürəkkəblik mövcuddur. Burda sübutların mürəkkəbliyi məhkəmədə oxşar işlərə baxılması zamanı ortaya çıxır. İkincisi, hətta az təsadüf edilən cinayətlər belə həddindən artıq

[24] "İnternetlə bağlı qanunvericilik fəaliyyəti tədricən fəallaşır", Paritet qəzeti.-2010.-3-5 aprel.-N.31.-S.9.
[25] Shanghai Cooperation Organization Agreement, Annex 1. http://www.loc.gov/
[26] Explanatory - Oxford Dictionaries, www.oxforddictionaries.com/definition/english/explanatory
[27] Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts. Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean. Geneva, 2012, p.17. – 60.
[28] Comprehensive Study on Cybercrime. United Nations. New York, 2013. P.12. -286.

yüksək maddi ziyanın vurulması ilə xarakterizə olunur. Üçüncüsü, bu cinayətlər yüksək ixtisaslaşmış sistem proqramçıları, telekommunikasiya sahəsinin mütəxəssisləri tərəfindən törədilir.[29]

Hüquq elmləri doktoru, professor T.L.Tropina kibercinayətlərin anlayışını verərkən qeyd edir ki, kibercinayətlər bütün cinayət növlərini əhatə etməklə informasiya-kommunikasiya sferasında törədilir və burada cinayətin qəsd obyektini (məqsədini) informasiya, informasiya resursları, informasiya texnikası təşkil edir. Beləliklə də, müəllif belə nəticəyə gəlir ki, kibercinayətkalığa kiberməkanda kompüter sistemləri və ya kompüter şəbəkələri vasitəsilə, həmçinin kompüter sistemləri və şəbəkələri çərçivəsində kiberməkana digər çıxış vasitələrinin köməyi ilə və kompüter sistemləri, kompüter şəbəkələri və kompüter məlumatları əleyhinə törədilən cinayətlərin məcmusu kimi anlayış verilə bilər.[30]

Eyni zamanda nəzərə almaq lazımdır ki, bəşəriyyət istənilən texnologiyanı yaratdıqda onu fayda vermək üçün yaradır, amma ondan bir sıra hallarda qeyri-qanuni, cinayət məqsədləri üçün də istifadə edilir. Bu mənada R.Əliquliyev qeyd edir ki, İKT sahəsində, o cümlədən internet mühitində həyata keçirilən hüquq pozuntuları ümumi şəkildə "kibercinayətkarlıq" termini ilə ifadə olunur. Onun fikrincə, "cinayətkarlıq" termini kifayət qədər aydın şəkildə müəyyən edilsə də, "kiber" anlayışı ilə bağlı müxtəlif yanaşmalar mövcuddur. Bu mənada kibercinayətlərə münasibətdə müasir beynəlxalq hüquqda "real" və "virtual" hüquq nəzəriyyələri formalaşmaqdadır. Onlar arasında bu sahədə əsas fərqlər də özünü göstərir. "Real" hüquq tərəfdarları qeyd edirlər ki, kibercinayətkarlıq – gerçək dünyada da məlumdur, sadəcə kompüterin köməyi ilə həyata keçirilir. Cinayətkarlıq olduğu kimi qalır, yalnız vasitələr dəyişir. "Kiber" hüquq tərəfdarları isə hesab edirlər ki, kibercinayətkarlığın unikal elementləri ona xüsusi yanaşma tələb edir, o cümlədən qanunların tətbiqi və cinayətkarlığın profilaktikasında bunu nəzərə almaq lazımdır.[31]

Beynəlxalq hüquqda bu cinayətlə mübarizə bir qədər fərqli anlamda çıxış edəcək. Müasir dövrdə kibercinayətlərlə bağlı ümum məcburi konvension tərifin qəbul edilməməsi onunla mübarizə məsələlərinə özünün mənfi təsirini göstərir.

Kibercinayətlər üzrə hindistanlı mütəxəssis Talvant Sinq qeyd edir ki, bu gün kibercinayətlərlə səmərəli mübarizədə iki çox mühüm oyunçu – hüquq mühafizə orqanları və kompüter peşəkarları arasında müəyyən dərəcədə antipatiya və ya ən azı inamsızlıq vardır. Ona görə də, əgər biz kibercinayətlər probleminə nəzarət etmək və interneti onun istifadəçiləri üçün təhlükəsiz "məkana" çevirmək istəyiriksə, bunların hər ikisi arasında yaxın əməkdaşlıq həlledicidir.[32]

Ümumiyyətlə, müasir kiber hüquq nəzəriyyələri təsdiq edir ki, qeyd olunan cinayətlərlə mübarizədə müxtəlif kateqoriya fərd və təşkilatların nümayəndələri aktiv şəkildə prosesə müdaxilə etməli və mütləq şəkildə bu sferada qarşılıqlı fəaliyyət göstərməlidir. Burada həm kommersiya qurumları, həm də hüquq tətbiq fəaliyyəti ilə məşğul olan şəxslər fəal olmalıdırlar. Çünki, kiber hüquq termini özü internet və elektron kommersiya ilə əlaqədar qanunların yaranmasını təsvir etmək üçün istifadə olunan termindir.[33]

Qeyd edək ki, kibercinayətlər özlərinin zərərli təsirini əsasən insan hüquqları və iqtisadi hüquqlar istiqamətində daha çox büruzə verməkdədir. Hazırda beynəlxalq elektron ticarət və maliyyə dövriyyəsinin kəskin artımı bu faktı vurğulamağa tam əsas yaradır. Belə ki, ABŞ iqtisadiyyatı kibercinayətlər üzündən hər il 100 milyard dollar itirir. Amerika Strateji və Beynəlxalq Araşdırmalar Mərkəzinin və elektron şəbəkələrin müdafiəsi məsələləri ilə məşğul olan "McAfee" şirkətinin birgə təhlilinin nəticələrinə görə kibercinayətlərin, o cümlədən sənaye sirlərinin oğurlanmasının iqtisadiyyata mənfi təsirinin nəticələrdən biri də işsizlikdir. Aparılmış hesablamalara görə, ABŞ bu səbəbdən hər il 508 min iş yeri itirir. Kibercinayətkarların əməlləri üzündən bütövlükdə dünya iqtisadiyyatı hər il 500 milyard dollara qədər itirir.[34]

Beləliklə, kibercinayətlərin anlayışı və əsas xüsusiyyətlərinin nəzəri araşdırılması, habelə milli və beynəlxalq hüquq normalarının qarşılıqlı təhlili nəticəsində aşağıdakı təklif və müddəaların irəli sürülməsini mümkün hesab edirik: Müasir transmilli hüquqi konsepsiyalara əsasən kompüterlərdə, kompüter şəbəkələrində və ya kiberməkanda baş verən hüquqazidd hərəkət və hərəkətsizlikləri ifadə etmək üçün müxtəlif terminlərin – "kompüter cinayətləri", "kibercinayətlər", "informasiya cinayətləri", "yüksək texnologiya cinayətləri", "kompüter informasiyasına aid cinayət" – istifadə edilməsinə baxmayaraq, "kibercinayətlər" məfhumuna üstünlük verilməsi məqsədəuyğun sayılmışdır. Doktrinal mövqelərdə kibercinayətin anlayışının konvension əsaslı imperativ beynəlxalq hüquq normalarında müəyyən edilməsinin zəruriliyi əsaslandırılaraq, ona aşağıdakı anlayışın verilməsi təklif edilir: Kibercinayətlər kompüterlərdən, kompüter proqramlarından, kompüter şəbəkələrindən, o cümlədən internet və sosial şəbəkələrdən, informasiya resurslarından və informasiya daşıyıcılarının digər qurğularından qanunsuz istifadə nəticəsində kompüter və informasiya sistemlərinın dağıdılması ilə nəticələnən və əhəmiyyətli zərərlə xarakterizə olunan, virtual məkanda qəsdən törədilən, cəzalandırılmalı, hüquqazidd ictimai təhlükəli hərəkət və hərəkətsizlik kimi başa düşülür.

Əlbəttə, bu terminə münasibətdə müxtəlif yanaşmalar mövcuddur. Yekun olaraq, biz "kibercinayət" terminina aşağıdakı tərifin verilməsini məqsədəuyğun hesab edirik: **Kibercinayət kompüter sistemlərinə və ya digər informasiya texnologiyaları şəbəkələrinə, cəmiyyətin informasiya təhlükəsizliyinə və kibermaraqlarına əhəmiyyətli ziyanın vurulması ilə xarakterizə edilən hərəkət və hərəkətsizlikdən ibarət transmilli cinayət əməlidir.** Bu anlayış özündə bir neçə elementi ehtiva edir. Birincisi, "kompüter sistemi"

---

[29] Тимошкина Ю.М. Компьютерные преступления. Москва 2010. S. 5. http://workcal.ru

[30] Тропина Т.Л. Киберпреступность. Владивосток, 2009. С.34. с.156.

[31] "İnternetlə bağlı qanunvericilik fəaliyyəti tədricən fəallaşır", Paritet qəzeti.-2010.-3-5 aprel.-N.31.-S.9.

[32] Cyber law & information technology. By Talwant Singh Addl. Distt. & Sessions Judge, Delhi. http: //delhicourts.nic.in/CYBER%20LAW.pdf

[33] Cyberlaw. Hot Topics: legal issues in plain language, Sydney, N.S.W.: Legal Information Access Centre, 2009 p.1

[34] Kibercinayətlər dünya iqtisadiyyatına hər il 500 milyard dollar ziyan vurur. Palitra qəzeti. 24.07.2013. s. 5.

termini müasir beynəlxalq hüquqda daha dar anlayış təəssüratı yaratdığı üçün biz "digər informasiya texnologiyaları şəbəkələri" ifadəsini də tərifə daxil etmişik ki, bu da özündə digər informasiya daşıyıcılarını – mobil telefonları, android və yüksək texnoloji qurğuları, habelə bankomat və elektron ödəmə sistemlərini də əhatə edir. İkincisi, kibercinayətlərlə mübarizədə mühüm elementlərdən biri cəmiyyətin informasiya təhlükəsizliyi əleyhinə yönələn təhdidlərin qarşısının alınmasıdır ki, bu da tərifdə xüsusi olaraq öz ifadəsini tapmışdır. Nəhayət, üçüncüsü, tərifdə nəzərdə tutulan cəmiyyətin kibermaraqlarına əhəmiyyətli ziyanın vurulması ilə bağlı nüans da, qeyd olunan əməlin kriminallaşmasına özünün mühüm təsiri ilə xarakterizə olunur.

1.2. Kibercinayətlərin təsnifatı: yeni cinayət modelləri

Kibercinayətlərin təsnifatı məsələsi də müasir beynəlxalq hüquqda və xarici ölkələrin milli qanunvericiliklərində geniş müzakirə olunan problemlərdəndir.

Ümumilikdə bu qeyri-qanuni əməlləri aşağıdakı kimi qruplaşdırmaq olar:

1) Kompüterə qanunsuz daxil olma;
2) Kompüter məlumatına və ya proqramlarına ziyan vurma;
3) Kompüter sabotajı;
4) Kommunikasiyaların qanunsuz olaraq dayandırılması və ya kəsilməsi;
5) Kompüter casusluğu.

Əlbəttə, bu qeyd olunan məsələlər kibercinayətlərin anlayışı, növləri və cinayət tərkibi ilə bağlı təfsilatı əks etdirə bilməz. Birincisi, bu cinayətlərin xarakteri elədir ki, bunlar daim inkişafdadır və texnoloji innovasiyalara həmişə uyğun gəlməlidir. İkincisi isə bunun üçün kibercinayətlərin universal əsasda müvafiq ayrıca tərifinin müəyyən edilməsi daha məqsədəuyğun olardı.

Kibercinayətlər beynəlxalq cinayətlərin surətlə inkişaf edən sahəsidir. Əksər cinayətkarlar heç bir fiziki və ya virtual sərhədlər tanımadan cinayətkar fəaliyyətlərinin müxtəlif diapazonunu genişləndirmək üçün surət, rahatlıq və internetin anonimliyini axtarırlar.

İnterpolun mövqeyinə əsasən, kontent təsnifatı həyata keçirilərək, bu cinayətlər üç geniş sahəyə bölünür:

- Kompüter aparat vasitələrinə və proqram təminatına qarşı hücumlar;
- Maliyyə cinayətləri, onlayn dələduzluq, onlayn maliyyə xidmətlərinə nüfuzetmə;
- Xüsusilə gənclərin alçaldıcı hərəkətləri və ya "seksplotasiya" formalarından sui-istifadə etməsi.[35]

Kibercinayətlərin müxtəlif qəsd obyektlərinə, predmetlərinə və törədilmə xüsusiyyətlərinə münasibətdə müxtəlif növləri fərqləndirilir. Qeyd olunmalıdır ki, əslində kibercinayətlərlə bağlı yetkin elmi anlayışın verilməsi üçün onun növləri məsələsinə diqqətin ayrılması və bu əməllərin tərkib elementlərinin qruplaşdırılması mühüm təcrübi və elmi əhəmiyyətə malikdir. Müxtəlif ədəbiyyatlarda, beynəlxalq və milli hüquqi normalarda bununla bağlı fərqli bölgülərin aparılmasını nəzərə alaraq, onların bəzilərini araşdırmağa cəhd edəcəyik.

Xüsusi vurğulanmalıdır ki, beynəlxalq təcrübi və elmi hüquqi əhəmiyyəti və Avrasiya regionunda hüquqi qüvvəsinə görə kibercinayətlərin Kibercinayətkarlıq haqqında 2001-ci il Budapeşt Konvensiyasına müvafiq olaraq aparılan bölgüsü daha mükəmməl və məqsədəmüvafiqdir. Həmçinin, bu Konvensiya əsasında aparılan təsnifat əksər beynəlxalq hüquq mütəxəssisləri və alimləri tərəfindən təqdir olunmaqla, müasir beynəlxalq hüquqda və hətta bu sənədi ratifikasiya etməyən xarici ölkələrin milli hüquq sistemlərində də etalon kimi qəbul edilməkdədir. Kibercinayətkarlıq haqqında Konvensiyaya (və ona Əlavə Protokola) görə kibercinayətləri *beş əsas qrupa* bölmək olar:

1) Kompüter məlumatları və sisteminin konfidensiallığı, bütövlüyü və onlara çatımlılıq, o cümlədən qeyri-qanuni çıxış, qeyri-qanuni ələ keçirmə, verilənlərə müdaxilə, sistemə müdaxilə və s. əleyhinə olan kibercinayətlər;

2) Kompüterdən istifadə ilə əlaqədar, yəni kompüterin cinayəti törətmə vasitəsi kimi, xüsusilə informasiya ilə manipulyasiya vasitəsi kimi törədilən kibercinayətlər. Bu qrupa əsasən kompüter dələduzluğu və kompüter saxtakarlığı aiddir.

3) Kontentlə, yəni kompüter şəbəkəsində yerləşdirilmiş verilənlərin məzmunu ilə əlaqədar kibercinayətlər.

Qeyd etmək lazımdır ki, bu qrup cinayətlər ictimai təhlükəlilik dərəcəsinə görə və praktiki nöqteyi-nəzərindən daha ciddi xarakteri ilə diqqəti cəlb edir. Belə ki, bütün dövlətlər tərəfindən xüsusi önəm verilən uşaq pornoqrafiyası və ümumilikdə internetdə yayılan porno-materiallar ilə bağlı cinayətlər bu qrupa aid edilə bilər. Ümumiyyətlə vurğulanmalıdır ki, hazırda kompüter şəbəkələrində, İnternetdə, Facebook, Twitter, İnstagram və digər sosial şəbəkələrdə kontent məsələsində ciddi problemlər yaşanmaqdadır. Bu mənada kontent cinayətlərinin elmi baxımdan daha dəqiq və müasir beynəlxalq hüquqa uyğun şəkildə balanslaşdırılmış qaydada araşdırılması zəruridir. Çünki, bu zaman kibercinayətlərlə mübarizə məsələsində insan hüquqları amili, o cümlədən şəxsi həyata, ifadə azadlığına müdaxilə problemləri xüsusilə aktual olacaqdır.

4) Şəbəkədə müəllif hüquqlarının və əlaqəli hüquqların pozulması ilə bağlı cinayətlər. Yəni, "intellekt oğurluğu cinayətləri" son dövrlərdə aktualdır. Çünki, hazırda müasir beynəlxalq hüquqda, eyni zamanda milli qanunvericilik sistemlərində xüsusilə internetdə plagiatlıq, köçürmələr, CD, DVD və s. musiqi, habelə digər fayl və məlumatların qanunsuz olaraq yüklənməsi ilə müəllif və əlaqəli hüquqların kobud və kütləvi şəkildə pozulması faktları müşahidə edilməkdədir. Bu səbəbdən də, dövlətlər qeyd olunan istiqamətdə səylərini birləşdirməklə kibercinayətkarlığın bu növü ilə mübarizənin yeni formalarını düşünməyə başlamışlar.

[35] Cybercrime, http://www.interpol.int

5) Bu qrupa aid kibercinayətlərə kompüter şəbəkələri vasitəsilə yayılan və törədilən irqçilik və ksenofobiya aktlarını aid etmək olar. Bunlar eyni zamanda yeni nəsil cinayətlər də adlandırılır. Qeyd olunmalıdır ki, bu növ cinayətlər Kibercinayətkalıq haqqında Avropa Konvensiyasına Əlavə Protokolda da öz əksini tapmışdır.

Yuxarıda qeyd olunan təsnifatdan bir daha aydın olur ki, müasir dövrdə kibercinayətlərin diapazonu doğurdan da özünün geniş əhatəliliyi ilə diqqəti cəlb edir və bu hüquqazidd əməllərlə mübarizə aparılması əslində bütün digər cinayətlərin də qarşısının alınması və profilaktikasına özünün müsbət təsirini göstərə bilər. Çünki, biz bu cinayətləri qəsd obyektlərinə görə qruplaşdırsaq görərik ki, çoxsaylı əməllərin törədilməsi məhz kompüter şəbəkələri və digər İKT vasitələri ilə həyata keçirilir.

Qeyd olunmalıdır ki, kibercinayətlərin təsnifatı məsələsi hələ də formalaşmaqda olan elmi prosesdir. Kibercinayətlərin təkamülü ilə bağlı "Cybercriminal Activity" ("Kiberkriminal fəaliyyət") adlı məqalədə xarici ölkə tədqiqatçıları bu cinayətin texniki və kontent əlamətləri baxımından müxtəlif növlərini – kompüter servisinin dağıdılması, informasiya oğurluğu, uşaq pornoqrafiyası, reputasiyaya zərər vurulması, spamlar, informasiya saxtakarlığı cinayətlərini fərqləndirirlər.[36]

Kibercinayətlər sahəsində tanınmış ekspertlər S.Holberq və A.Hubbard yazır ki, kompüter cinayətləri özündə bütün cinayət növlərini ehtiva edə bilər ki, buraya da kompüter texnologiyalarının istifadəsi, təfərrüatları və informasiya ilə əlaqədar məsələlər aid edilməlidir. Bir sözlə müəlliflər kibercinayət kateqoriyasına kompüter sistemləri və şəbəkələri, o cümlədən internet infrastrukturu əleyhinə yönələn hücumları, bundan əlavə, internet saxtakarlığı və dələduzluğunu da aid edirlər.[37]

R.Əliquliyev isə kibercinayətləri iki qrupa bölür: yalnız kiberməkana xas olan cinayətlər və kompüter və internet vasitəsilə həyata keçirilən ənənəvi cinayətlər. Yalnız kiberməkana xas olan cinayət əməllərinə İnternet casusluğu, kiberdələduzluq, kompüter informasiyasına qanunsuz daxilolma, xüsusi təyinatlı radioelektron sistemlərinin qanunsuz dövriyyəsi, internetdə maliyyə fırıldaqçılığı və s. daxildir. İnternet vasitəsilə həyata keçirilən ənənəvi cinayətlərə isə həyat və sağlamlıq, şərəf və ləyaqətin alçaldılması, iqtisadi sahələr, ictimai təhlükəsizlik, mülkiyyət əleyhinə olan cinayətlər aiddir. Bura eyni zamanda pornoqrafiyanın yayılması, narkobiznes, konstitusiya quruluşu və dövlət əleyhinə olan cinayətlər də daxildir.[38]

Qeyd olunan bölgünün müasir beynəlxalq hüquq nöqteyi-nəzərindən faydasını inkar etmədən, xüsusi vurğulamaq lazımdır ki, beynəlxalq xarakterli cinayətlər kateqoriyasına aid olmaqla, kibercinayətlər əslində daha çox qəsd obyektləri baxımından təsnifləşdirilməlidir.

Bu səbəbdən də qəsd obyektinə görə kiberməkanda törədilən cinayətlərin fikrimizcə aşağıdakı şəkildə qruplaşdırılması daha məqsədəuyğun olardı: insanın əsas hüquq və azadlıqları əleyhinə olan kibercinayətlər – şəxsi həyat hüququna, söz və ifadə azadlığına olan kiber müdaxilələr, kiber piratlıq və s.; iqtisadi kompüter cinayətləri – kompüter dələduzluğu, bank hesablarına və post-terminallara kiber müdaxilə və s.; ictimai və dövlət maraqları əleyhinə yönələn kibercinayətlər – dövlət orqanlarının və ictimai qurumların veb saytlarının haker hücumlarına məruz qalması, qanunsuz informasiya hücumları və s.; kompüter məlumatlarının və şəbəkələrinin təhlükəsizliyi əleyhinə olan kibercinayətlər – bu sıraya istənilən fərdi və şəbəkəyə qoşulan və qoşulmayan hər hansı kompüterdə, texniki informasiya daşıyıcısında olan məlumatların məxfiliyinin pozulması, onlara müdaxilə, kompüterlərə çatım imkanlarının məhdudlaşdırılması və s. aid edilə bilər.

Kibercinayətlərin bu cür qruplaşdırılması özünün praktiki əhəmiyyəti ilə də seçilir. Çünki burada qeyd olunan hər bir kibercinayət növü üzrə hazırda beynəlxalq hüquqda bir sıra qurumlar çərçivəsində konkret cinayət işləri həyata keçirilərək, onlarla səmərəli mübarizə aparılır. Qeyd etmək lazımdır ki, son dövrlərdə kibercinayətlərin ayrı-ayrı növləri ilə mübarizədə Avropa İttifaqının da xüsusi rolu vardır. Belə ki, bu qurumun daxilində dünyada ilk dəfə olaraq 2013-cü ildə kibercinayətlər üzrə ixtisaslaşmış ayrıca orqan – Avropa Kibercinayət Mərkəzi (EC3) yaradılmış və birillik fəaliyyəti dövründə kibercinayətlərin müxtəlif növləri üzrə təhqiqat və operativ əməliyyatlar baxımından üzv dövlətlərə yardımlar üzrə səmərəli fəaliyyət göstərmişdir.[39] Evropol-un nəzdində formalaşdırılan EC3-un fəaliyyətinin təhlilindən biz kibercinayətlərin daha yeni təsnifatının şahidi oluruq. Belə ki, bu qurumda aşağıdakı kibercinayət növləri üzrə əməkdaşlıq həyata keçirilir: *yüksək-texno cinayətlər (high-tech crimes)* – kiber hücumlar, zərərli proqram təminatları (malware); *uşaqların onlayn cinsi istismarı* (online child sexual exploitation); *onlayn ödəniş dələduzluğu* (payment fraud).

Göründüyü kimi, kibercinayət termini o qədər geniş anlayışdır ki, onun cinayət tərkibi ilə bağlı müddəalarının müasir informasiya texnologiyalarının inkişafına müvafiq olaraq və sürətli texnoloji tərəqqi nəzərə alınmaqla genişlənməsi ehtimalı böyükdür. Onların bəziləri elmi dairələrdə mübahisəli məsələ kimi hələ də acıq qalmaqdadır.

Ümumiyyətlə, Kibercinayətkarlıq haqqında Konvensiyaya (və ona Əlavə Protokola) görə kibercinayətlərin beş əsas qrupa bölgüsü müasir beynəlxalq hüquq normaları baxımından və xarici ölkələrin milli hüquq sistemlərinə nəzərən optimal və təcrübi əhəmiyyətli təsnifat kimi qəbul edilir. Törədilən hər hansı istənilən dağıdıcı cinayətkar fəaliyyət məhz kompüter sistemlərinin və şəbəkələrinin, habelə onlarda mövcud olan informasiyaların məhv edilməsinə yönəlmişdirsə, həmin əməl kibercinayətlər kateqoriyasına aid edilir. Kompüter sistemləri və ya şəbəkəsindən, o cümlədən internetdən vasitə kimi istifadə olunaraq, mütəşəkkil cinayətkar qruplar və ayrıca şəxslər konkret cinayət məqsədlərini reallaşdırmağa cəhdlər etmişlərsə, bu zaman qeyd olunan vasitələr həmin cinayət əməllərinin törədilməsi üçün yalnız köməkçi alət qismində çıxış edəcəkdir. Burada ayrıca növ kimi təsnifləşdiriləcək hansısa kibercinayətdən yox, konkret tərkibi olan müstəqil cinayət

[36] Cybercriminal Activity. www.sysnet.ucsd.edu/~cfleizac/WhiteTeam-CyberCrime.pdf
[37] Harmonizing national legal approaches on cybercrime. Judge Stein Schjolberg & Amanda M. Hubbard, Geneva, 2005, p. 4. pp.24
[38] "İnternetlə bağlı qanunvericilik fəaliyyəti tədricən fəallaşır", Paritet qəzeti.-2010.-3-5 aprel.-N.31.-S.9.
[39] European Cybercrime Centre – one year on, http://europa.eu/rapid/press-release_IP-14-129_en.htm

əməlindən danışmaq mümkündür. Məsələn, "kiberterrorizm" anlayışı bu kateqoriyaya aid edilə bilər. Bununla əlaqədar növbəti paraqrafda ətraflı danışılacaqdır.

1.3. Kiberterrorizm və kibercinayətlər: müqayisəli təhlil

Müasir beynəlxalq hüquqda terrorçuluq ayrıca cinayət tərkibi kimi xüsusi statusa malikdir. Belə olan təqdirdə kiberməkandan terrorist məqsədləri ilə istifadə olunması, şəbəkə istifadəçilərinin də həm obyekti, həm də subyekti olduğu bu cinayət əməlinin terrorçuluq, yoxsa kibercinayətlərin xüsusi növü olması məsələsi bir qədər problemlərə yol acmış olacaqdır. Əlbəttə, bu kimi mübahisəli elementlərin aradan qaldırılması üçün bu sahədə unifikasiya olunmuş beynəlxalq cinayət hüquqi konsepsiyanın ortaya qoyulması və bu cinayət əmələri ilə mübarizədə yeni tendensiyaların ortaya qoyulması zəruridir. Ancaq bu məsələdə də Aİ digər beynəlxalq strukturlardan daha fəal və operativ şəkildə çıxış etmişdir. Bu qurum tərəfindən internet şəbəkəsinin terrorist təşkilatları tərəfindən istifadəsi ilə mübarizə aparmaq məqsədi ilə Clean IT layihəsi işlənib hazırlanmışdır.[40] Qeyd etmək lazımdır ki, bu cinayətlərlə mübarizədə xüsusi proqram və layihələrin hazırlanması üzrə "Evropol"un xidmətləri danılmazdır. Həmin layihənin məqsədlərindən də göründüyü kimi, internet üzərindən həyata keçirilən qeyri-qanuni fəaliyyətlərə aid olan ictimai və özəl dialoq təşəbbüsləri xüsusi olaraq terrorçu fəaliyyətlərin fokuslanmasına gətirib çıxarır. Bu mənada onlayn terrorizmlə mübarizənin bilavasitə kibercinayətkalıqla mübarizə ilə qarşılıqlı əlaqə və asılılıqda nəzərdən keçirilməsi fikrimizcə, faydalı olardı. Lakin, bu iki ayrı-ayrı cinayətlər öz tərkibləri etibarilə fərqləndiyindən, internet şəbəkəsi yalnız terror cinayətinin həyata keçirilməsinin vasitəsi olaraq qalacaqdır. Çünki, bu zaman terror cinayətinin törədilməsində əsas məqsəd kompüter sistemləri və ya məlumatları deyil, terror cinayətinin qəsd obyekti olan ictimai təhlükəsizlik olacaqdır. Burada dövlətlərin səyi ondan ibarət olacaqdır ki, terrorçuluq cinayətinin qarşısının alınmasında yalnız məhdudlaşdırıcı İT vasitələrinin köməyindən istifadə etməklə, onlayn terrorizmin fəsadları minimuma endirilsin.

Bu məsələdə daha müfəssəl yanaşmanın ortaya qoyulması üçün "kiberterrorizm" termininin yaranma tarixinə də diqqətin ayrılması zəruridir.

XX əsrin 80-ci illərinin sonlarında Amerika Təhlükəsizlik və Kəşfiyyat İnstitutunun böyük elmi işçisi Berri Kollin virtual fəzada terrorçuluq fəaliyyətini ifadə etmək üçün ilk dəfə "kibernetik terrorçuluq" terminindən istifadə etmişdir. Qeyd olunmalıdır ki, o zaman bu termin praktiki əhəmiyyət kəsb etmirdi və yalnız gələcək üçün proqnoz verməkdən ötrü istifadə olunurdu. Berri Kollinin özü isə kiberterrorçuluqdan yalnız XXI əsrin ilk onilliyində danışmağın real olduğunu qeyd etmişdir. Lakin real vəziyyətlə əlaqədar olaraq, FTB-in xüsusi agenti Mark Pollit 1996-cı ildə kiberterrorçuluq termininin tərifini təklif etmişdir.[41] Həmin tərifə görə, kiberterrorizm informasiya, kompüter sistemləri, kompüter proqramları əleyhinə yönələn, milli qruplara və mülki hədəflərə qarşı zorakılıqla nəticələnən siyasi motivli qəsdən törədilən hücumdur.[42]

Kiberməkanda terrorizm həm kibercinayət, həm də terrorizmin əlamətlərini özündə ehtiva edir. Kiberməkanda terrorist hücumları kibercinayətin kateqoriyası və informasiya texnologiyalarından kriminal sui-istifadə kimi çıxış edir.[43]

Qeyd olunduğu kimi, kiberterrorçuluq və informasiya təhlükəsizliyi müasir dövrün real vəziyyətinə əsaslanaraq, hüquq və informatika mütəxəssislərinin məşğul olduğu ciddi bir problemə çevrilmişdir. Kiberterrorçuluqla bağlı hərəkət və hərəkətsizlik artıq real olaraq baş verməkdədir. Bu, həm digər cinayətlərin, xüsusilə terrorun və təcavüzün törədilməsi üçün hərəkətverici vasitə olaraq, həm də müstəqil cinayət tərkibi olaraq artıq dunya birliyi tərəfindən cəzalandırılmalı olan əməllər kateqoriyasına aid edilmişdir. Bununla yanaşı, bu günkü Azərbaycan reallığında kibermuharibənin, kibertəcavüzün və digər beynəlxalq cinayətlərin qurbanı kimi artıq bu əməllərə görə cinayət hüquqi yurisdiksiyanın həyata keçirilməsi labüd və zəruridir. Səmərəli cinayət hüquqi yurisdiksiyanın tətbiqi üçün isə kiberməkanda baş verən hərəkət və hərəkətsizlikləri özündə ehtiva edən hüquqi terminlərin istər nəzəri, istərsə də normativ hüquqi müəyyənliyə malik olması danılmazdır.

Beləliklə, kiberterroçuluğa belə bir anlayış verilə bilər: ***Kiberterrorçuluq dedikdə*, kompüterdə** emal olunan informasiyaya, kompüter sisteminə və şəbəkəsinə düşünülmüş, siyasi motivlərə əsaslanmış hücum başa düşülür. Əgər belə hərəkətlər ictimai təhlükəsizliyin pozulması, əhalinin qorxudulması, hərbi konfliktlərin, təxribatlarının törədilməsi məqsədilə həyata keçirilmiş olarsa, onda bu hücum insanların həyatı və sağlamlığı və ya digər ağır fəsadların baş verməsi üçün daha böyük təhlükə yaradır.

Kiberterrorizm siyasi, dini və ideoloji motivlər əsasında dağıdıcı, təxribatçı və qorxu aşılayan nəticələrə səbəb olan, terroristlər tərəfindən informasiya infrastrukturuna edilən hücumlar kimi müəyyən edilir.[44]

Kiberterrorçuluq cinayətkar niyyətlərin əldə olunması məqsədilə əhalinin, hakimiyyət orqanlarının məhz kibervasitələrlə qorxudulması kimi qəbul edilir. Bu, müəyyən siyasi və ya digər məqsədlərin əldə olunması, şəxslərin, təşkilatların və ya hakimiyyət strukturlarının müəyyən hərəkətlərə məcbur edilməsi, kiberterrorçunun şəxsiyyətinə və terrorçu təşkilata diqqətin yönəldilməsi məqsədilə əhalinin təhlükəyə məruz qoyulması, daimi qorxu vəziyyətində saxlanması şəklində özünü göstərə bilər.

Transmilli mütəşəkkil cinayətkar qrupların müasir İKT-dən geniş miqyasda istifadə etməsi labüd faktdır. Beynəlxalq terrorçu təşkilatlar elmi-texniki nailiyyətlərdən yararlanmağa, kompüter, rabitə, İKT və s. sahələrdə mütəxəssisləri öz sıralarına cəlb etməyə çalışırlar. Bu terrorçu təşkilatlar tərəfindən daim yeni üzvlərin rekrut

---

[40] Clean IT Project , https://www.edri.org/files/cleanIT_sept2012.pdf

[41] İnformasiya təhlükəsizliyi problemi və onu xarakterizə edən əsas amillər, http://referat.ilkaddimlar.com/ref_info_5783

[42] Mark M. Pollitt. "A Cyberterrorism Fact or Fancy?", Proceedings of the 20th National Information Systems Security Conference, 1997, pp. 285-289

[43] ARF Chairman's Statements and Reports, https://www.aseanregionalforum.asean.org/

[44] International Handbook on Critical Information Infrastructure Protection (CIIP) 2006 Vol. II, page 14.

edilməsi, törədilmiş terror aktlarına bəraət qazandırılması, potensial terrorçulara təlimlərin keçirilməsi, üzvlər arasında müntəzəm əlaqələrin saxlanılması və s. məqsədlərlə internet şəbəkəsindən fəal istifadə edilir.

Bəzi ədəbiyyatlarda belə kateqoriya əməllər kibercinayətkarlığın bir növü kimi elektron vandalizm də adlandırılır. Orada bu cinayət növü çox ciddi problem kimi səciyyələndirilərək, qeyd olunur ki, bu gün iqtisadiyyat, idarəetmə, hətta dünyanın əksər ölkələrinin ayrı-ayrı vətəndaşları kompüter şəbəkə və sistemlərinin normal fəaliyyətindən asılıdır. Bu tipli cinayətlərin motivi ya öz iradəsini reallaşdırmaq, ya qisas və ya intiqam almaq istəyi, ya da rəqiblə hesablaşmaq istəyi ola bilər. Belə olan təqdirdə kompüter sistemləri zədələnir və onların işinə olan müdaxilələr daha ciddi və bəzən də daha faciəvi nəticələrə səbəb ola bilər.[45] Məsələn 1992-ci ildə kompüter sisteminə edilən müdaxilənin nəticəsi idi ki, Litvada İqnalinsk atom elektrostansiyasında böyük bir nüvə partlayışlarına səbəb ola biləcək hadisələrin yaşanma ehtimalı yaranmışdı. Göründüyü kimi, kompüterlərə edilən hətta təsadüfi müdaxilələr belə ağır fəsadları ilə xarakterizə olunan digər beynəlxalq cinayətlərin törədilməsinin əsas səbəbi kimi çıxış edə bilər. Bu səbəbdən də qeyd olunan cinayət növlərini kompüter cinayətləri ilə əlaqəli cinayətlər kimi adlandırmaq fikrimizcə daha məqbul olardı. Lakin əsas məqsədini və hədəfini məhz kompüter sistemləri və ya kompüter şəbəkələri təşkil edən cinayətləri isə birbaşa kibercinayətlər kateqoriyasına aid etmək olar. Məsələn, 1999-cu ildə Belqradın bombalanması zamanı NATO-nun kompüter sistemlərinin hədəflənməsi və onların işinin iflic edilməsi ilə bağlı həyata keçirilmiş cəhdlər kibercinayət kimi tövsif oluna bilər. Bu mənada kibercinayətlərdə əsas kriminal məqsədin məhz İKT-yə qarşı yönəldilməsi faktoru onun növlərə bölgüsündə əsas təsnifat meyarı kimi götürülməsi qəbul edilməlidir.

Buradan belə nəticəyə gəlmək mümkündür ki, əgər törədilən vandalizm və hər hansı istənilən dağıdıcı cinayətkar fəaliyyət məhz kompüter sistemlərinin və şəbəkələrinin, habelə onlarda mövcud olan informasiyaların məhv edilməsinə yönəlmişdirsə, həmin əməlin törədilmə miqyasından və zahiri əlamətlərindən asılı olmayaraq, onları kibercinayətlər kateqoriyasına aid etmək olar. Digər tərəfdən, əgər kompüter sistemləri və ya şəbəkəsindən, o cümlədən internetdən vasitə kimi istifadə olunaraq, mütəşəkkil cinayətkar qruplar və ayrıca şəxslər konkret cinayət məqsədlərini reallaşdırmağa cəhdlər etmişlərsə, bu zaman qeyd olunan vasitələr həmin cinayət əməllərinin törədilməsi üçün yalnız köməkçi alət qismində çıxış edəcəkdir. Burada ayrıca növ kimi təsnifləşdiriləcək hansısa kibercinayətdən yox, konkret tərkibi olan müstəqil cinayət əməlindən gedəcəkdir.

Beləliklə, "kibercinayət" və "kiberterrorizm" anlayışları fərqləndirilməklə hər biri müstəqil cinayət tərkibi olaraq təsnif edilir və kompüterlər, kompüter şəbəkələri, internet, sosial şəbəkələr yalnız "kiberterrorizm"in törədilməsində yardımçı vasitələr kimi qəbul edilir.

II FƏSİL
BEYNƏLXALQ HÜQUQDA KİBERCİNAYƏTKARLIQLA MÜBARİZƏNİN İSTİQAMƏT VƏ FORMALARI

2.1. Universal və regional müstəvidə kibercinayətlərlə mübarizənin xüsusiyyətləri

Müasir dövrdə kibercinayətkarlıqla mübarizə sahəsində dövlətlərarası münasibətlərin istər universal, istərsə də regional tənzimlənməsi məsələsi özünəməxsus xüsusiyyətləri ilə diqqəti cəlb edir. Birincisi, bu sahədə həm beynəlxalq, həm də ölkədaxili maddi hüquq normalarının və bununla əlaqədar prosessual normaların yaradılması yeni və inkişafda olan prosesdir. İkincisi, kibercinayətkarlıq sahəsində ictimai münasibətlərin tənzimlənməsinə və beynəlxalq hüquq normalarının harmonizasiyasına təsir göstərmək iqtidarında olan beynəlxalq əməkdaşlıq formaları özünün ilkin təzahür dövrünü yaşayır. Yəni, bu sahədə beynəlxalq konfranslar, forumlar, elmi-nəzəri və praktiki əməkdaşlıq, habelə kibertəhlükəsizliyin tənzimlənməsinin müxtəlif aspektlərinə dair (hüquqi, təşkilati, texniki və s.) əlaqələr nəticə etibarilə bu sahədə normativ bazanın da formalaşmasında əvəzsiz rol oynayır. Üçüncüsü, bu sahədə daha çox regional əməkdaşlığın aktivliyi və dünyanın müxtəlif regionlarında formalaşmaqda olan ölkələrarası razılaşma nümunələri (məsələn, Avropa Şurası çərçivəsində qəbul olunmuş Kibercinayətkarlıq haqqında 23 noyabr 2001-ci il Budapeşt Konvensiyası, Afrika qitəsində Afrikada kibertəhlükəsizlik fəaliyyətinin hüquqi çərçivəsinin yaradılması haqqında 2012-ci il tarixli Konvensiya layihəsi, Ərəb Şərqində Ərəb Dövlətləri Liqası tərəfindən qəbul olunmuş İnformasiya texnologiyaları cinayətləri ilə mübarizə haqqında 2010-cu il tarixli Ərəb Konvensiyası, MDB məkanında 2001-ci il tarixli Kompüter informasiyası sferasında cinayətlərlə mübarizədə MDB iştirakçı-dövlətlərin əməkdaşlığı haqqında Müqavilə, habelə bu qurum çərçivəsində 17 fevral 1996-cı il tarixdə qəbul edilmiş Model Cinayət Məcəlləsi və s.) daha çox hüquqi müstəvidə müşahidə olunur.

Beynəlxalq hüquq elmində kibercinayətlərə qarşı mübarizə üzrə əməkdaşlığın universal, regional və ikitərəfli aspektləri fərqləndirilir. Digər beynəlxalq xarakterli cinayətlərdən fərqli olaraq, kibercinayətkarlığın özünəməxsus cəhəti ondan ibarətdir ki, bu cinayətlə mübarizə üzrə ayrıca dövlətin hakimiyyət orqanlarının gücü və hüquq-mühafizə orqanlarının təkbaşına fəaliyyəti kifayət etmir. Bu səbəbdən də beynəlxalq birlik bu cinayətlə

[45] Тимошкина Ю.М. Компьютерные преступления. Москва 2010. S. 11.

mübarizədə daha effektiv nəticələrə nail olmaq üçün yalnız beynəlxalq əməkdaşlığa üstünlük verilməsini məqbul sayır.

Kibercinayətlərlə bağlı dövlətlərin əməkdaşlığı müqavilə-hüquqi (konvension) və institusional (beynəlxalq təşkilatlar daxilində) mexanizmlərə əsaslanır. Ona görə də, biz kibercinayətkarlıqla mübarizə üzrə çoxtərəfli və ikitərəfli, universal, regional və lokal beynəlxalq müqavilələrin xüsusiyyətlərini, müddəalarını və özünəməxsus cəhətlərini analiz edəcəyik. Eyni zamanda, yüksək texnologiyalar sahəsində hüquqazidd əməllərlə mübarizə üzrə fəaliyyət göstərən digər əməkdaşlıq formalarına, o cümlədən beynəlxalq forumlar, konfranslar, məhkəmə təsisatları və başqalarına da diqqət yetirəcəyik.

İnformasiya texnologiyaları sahəsində törədilən cinayətlər adətən beynəlxalq xarakter daşıyır, Çünki burada cinayətkarlar bir dövlətin ərazisində fəaliyyət göstərsə də, lakin onun qurbanları digər dövlətdə yerləşir. Ona görə də, bu cinayətlərlə mübarizə aparmaq üçün beynəlxalq əməkdaşlıq xüsusi məna kəsb edir.[46]

Əlbəttə, bu gün qlobal anlamda kibertəhlükəsizliyin təmin olunması istiqamətində xüsusi səylər göstərilir, bu sahədə kiberməkan istifadəçilərinin davranışlarına nəzarəti həyata keçirən universal və regional normativ hüquqi sistem formalaşmaqla, artıq bu normalar ölkədaxili hüquq sistemlərinə implementasiya olunmağa başlamışdır.

İKT mahiyyət etibarilə bu gün ictimai həyatın bütün sahələrinə, o cümlədən siyasi, iqtisadi, müdafiə, ekoloji, sosial və digər sahələrə, habelə hər bir dövlətin milli təhlükəsizlik sisteminə bilavasitə təsir edən mühüm faktorlardan hesab olunur.

Bu səbəbdən də, dövlətlər universal və regional əsasda internetin hüquqi tənzimlənməsi, kompüter informasiyası və digər istənilən kiberməkanın təhlükəsizliyinə xələl gətirə bilən hərəkət və hərəkətsizliklərin – cinayətlərin qarşısının alınması, aşkarlanması, açılması, təhqiqatı və istintaqı istiqamətində əməkdaşlığı prioritet hesab edirlər.

Yuxarıda qeyd etdiyimiz kimi, kiberməkanda təhlükəsizliyin təmin olunması və cinayətlərin qarşısının alınması üçün bu gün daha çox regional əməkdaşlığa üstünlük verilir, daha doğrusu kibercinayətlərin qarşısının alınması və təhqiqatı üzrə müqavilə mexanizmləri ən çox Avropa regionunda inkişaf edərək genişlənməyə və bundan sonra universal mahiyyət kəsb etməyə meylli olmuşdur.

Rusiyalı hüquq elmləri namizədi K.V.Prokofyev qeyd edir ki, internet şəbəkəsinin yaradılma və fəaliyyətinin müsbət nəticələri ilə yanaşı, onun istifadəsi ilə əlaqədar dünya ictimaiyyəti üçün çoxlu sayda təhlükələr də mövcuddur. Bunlara xüsusilə, bütövlükdə informasiya təhlükəsizliyinin təmin olunması, kibercinayətkarlıq və İnternet şəbəkəsində şəxsi məlumatların mühafizəsi problemləri aiddir. Onun fikrincə, məhz sadalanan bu problemlər bəşəriyyətin müasir kompleks qlobal problemlərinə aid olmaqla, nüfuzlu beynəlxalq təşkilatların (BMT, "Böyük Səkkizlik", Avropa Şurası və s.) müzakirə predmetini təşkil edir.[47] Qlobal informasiya infrastrukturunun sürətli inkişafı insanlar arası ünsiyyətin transmilli xarakter alması, yeni təhdidlərin meydana gəlməsinə səbəb olur və bu da öz növbəsində bu təhlükələrə qarşı dövlətlərin səylərinin birləşdirilməsilə nəticələnir, ikitərəfli və çoxtərəfli müqavilələr vasitəsilə müvafiq tədbirlərin görülməsini zəruri edir.

Göründüyü kimi, internetin dünya birliyi üçün yaratdığı faydalarla yanaşı, eyni zamanda şəbəkə və kompüter informasiyası üzrə hüquqazidd hərəkətlər – kibercinayətlərin qarşısının alınması və cəzalandırılması da eyni zamanda qloballaşma dövrünün tələbi kimi çıxış edir. Məhz bu səbəbdən də, dövlətlər qeyd olunan problemlərin həlli məqsədilə universal və regional səviyyələrdə beynəlxalq əməkdaşlığı labüd və zəruri hesab etmişlər.

2.1.1. BMT sistemində kibercinayətlərlə mübarizə

Kibercinayətlərlə beynəlxalq mübarizənin səmərəli və mühüm elementləri BMT sistemində həyata keçirilir. Bu araşdırmasın sistemli analizi baxımından ilk növbədə bu cinayətlə mübarizənin daha geniş spektrdə effektivliyinə nail olunması üçün universal beynəlxalq qurum olan BMT çərçivəsində qəbul edilən sənədlər çərçivəsində bu sahəyə dair təsbit olunmuş müqavilə müddəalarına diqqət yetirmək zəruri hesab olunur.

BMT, xüsusilə onun əsas orqanları olan Baş Assambleya, İqtisadi və Sosial Şura tərəfindən kibercinayətkarlıqla mübarizə sahəsində hələ 21-ci əsrin lap əvvəllərindən başlayaraq bir sıra qətnamələr qəbul etmişdir. Belə ki, 2001-ci ildə Baş Assambleya tərəfindən kibercinayətlərə dair "İnformasiya texnologiyalarından cinayətkar sui-istifadə ilə mübarizə" adlı qətnamə (A/RES/55/63) qəbul edilmişdir. Bu qətnamədə qeyd olunur ki, dövlətlər informasiya texnologiyalarından sui-istifadə edən hər kəsə qarşı mübarizədə, onların təhlükəsizliyinin təmin olunmasında öz daxili səlahiyyətləri çərçivəsində aktiv rol oynayacaqlar. Bundan başqa, orada vurğulanır ki, bu sahəyə aid olan transmilli problemlər bütün razılığa gələn dövlətlər tərəfindən koordinasiya olunmuş şəkildə tədqiq olunmalıdır.[48] Dövlətlər bu sahədə cinayətkar sui-istifadələrin qarşısının alınması və onunla mübarizənin daha səmərəli aparılması üçün istifadəçilərin qanunsuz fəaliyyətləri barədə bir-birini xəbərdar etməlidirlər. Qətnamədə həmçinin, bu cinayətlə mübarizənin aparılması zamanı fərdə məxsus olan digər hüquq və azadlıqlara hörmətlə yanaşılması məsələsi də xüsusi vurğulanır və önə çəkilir. Qeyd olunmalıdır ki, kibercinayətlərə münasibətdə həlli tələb olunan bu məsələlərə toxunarkən, eyni zamanda, hakimiyyət səlahiyyətlərinə malik olan qurumların bu cinayətlə mübarizə üzrə fəaliyyətini həyata keçirən zaman fərdi

---

[46] Борьба с киберпреступностью – проблема всего информационного сообщества. http://www.rusnauka.com/6_PNI_2013/Pravo/5_129511.doc.htm

[47] Прокофьев, Константин Викторович, "Международно правовыепроблемы обеспечения международной информационной безопасности всети Интернет", Автореферат, Москва, 2009, с. 6.

[48] Legal and political measures to address cybercrime, UFRGSMUN | UFRGS Model United Nations ISSN: 2318-3195 | v.2, 2014| p. 445-477

azadlıqların və şəxsi həyat hüququnun nəzərə alınması universal mahiyyət kəsb edən bu qətnamənin ən üstün cəhətlərindən biri olaraq vurğulanmalıdır.

İnnovativ xarakteri ilə diqqəti cəlb edən, internet və sosial şəbəkələrin inkişafına adekvat olaraq daim genişlənməkdə olan kibercinayətlərlə mübarizədə xüsusilə universal beynəlxalq əməkdaşlığın zəruriliyi bir çox beynəlxalq qurumların nümayəndələri və müasir dünya alimləri tərəfindən də qeyd olunmuşdur.

BMT-nin Narkotiklər və cinayətlərlə mübarizə İdarəsi 2013-cü ildə özünün verdiyi bəyanatda vurğulayır ki, 2011-ci ildə təqribən 2,3 milyard adamın (dünyanın ümumi əhalisinin üçdə biri civarında) internetə çatım imkanı olmuşdur. 2017-ci ildə isə mobil və elektron istifadəçilərinin sayı bütövlükdə dünya əhalisinin 70 faizini təşkil edib. 2020-ci ilə qədər isə internetin mövcud imkanlarından istifadə üzrə planetin hər 6 nəfərindən biri şəbəkə istifadəçisi olmaya bilər. Sabahın hiperəlaqələrə malik dünyasında isə "kompüter cinayətlərini" təsəvvür etmək belə çətin olacaq və çox ehtimal ki, İnternet Protokolla (İP) əlaqəli və elektron elementlə bağlı olmayan hər hansı bir cinayət əməli olayacandır.[49]

Bu fikirlərdən də göründüyü kimi, əslində kibercinayətlərlə bağlı beynəlxalq əməkdaşlıq daha çox bəşəriyyətin indiki və gələcək təhlükələrdən qorunması və təhlükəsizliyi baxımından vacibdir.

Isveçrəli alim Dr. Miriam Dunn Kavelti qeyd edir ki, şəbəkə informasiya mühiti və ya kiberfəza ona görə hərtərəfli təhlükəli hesab olunur ki, bu məkanın əsası qoyularkən qeyd edilən xüsusiyyət onda mövcud olmuşdur. Texnoloji innovasiyalarla əlaqədar informasiya xidmətlərinin dinamik qloballaşması bu sahədə əlaqələrin genişləndirilməsinə və mürəkkəb problemlərin kompleks həllərinin artırılmasın gətirib çıxardı. Daha çox mürəkkəblik İT sistemləri ilə əlaqədar özünü göstərdi və onların idarə olunması, habelə təhlükəsizliyinə nəzarət daha da çətinləşdi.[50]

Müasir kibercinayət hüququnun və bütövlükdə internet hüququnun da əsas vəzifəsi məhz İT sistemləri ilə bağlı yayılmaqda olan cinayətlərin qarşısının alınması və onunla bağlı profilaktik tədbirlərin görülməsidir. Bunun üçün müasir beynəlxalq hüquqda ən optimal yol əməkdaşlığın universal və regional müqavilə bazasının formalaşdırılmasıdır.

Qeyd olunduğu kimi, son dövrlərin İKT-nin sürətli inkişafı beynəlxalq hüquqi əlaqələrin müxtəlif sahələrində, o cümlədən kibercinayətlər üzrə beynəlxalq əməkdaşlığı zərurətə çevirmişdir. Çünki, bu cinayət nəticəsində bütövlükdə bəşəriyyətə, İnternet istifadəçilərinə maddi və mənəvi zərərin vurulması ilə müşayiət olunan çoxlu sayda faktlar və hadisələr baş verir. Məsələn, statistik rəqəmlərə fikir versək, bu cinayətlə mübarizənin beynəlxalq hüquqi normativliyinin hansı zərurətdən yarandığını daha dəqiqliyi ilə müəyyən etmək mümkündür. Bir çox hesabatlardan da göründüyü kimi, qlobal olaraq şəbəkəyə edilən müdaxilələr nəticəsində dəyən zərərin miqdarı il ərzində 15 milyard dollardan çox qiymətləndirilir.[51]

Yuxarıda qeyd olunan problemləri nəzərə alaraq, kompüter cinayətkarlığı ilə mübarizə sahəsində dövlətlər öz səylərini birləşdirməyə və bu məsələlərlə bağlı hüquqi müstəvidə BMT, Avropa Şurası, Avropa İttifaqı, ATƏT, MDB və beynəlxalq qurumlar çərçivəsində addımlar atmağa başladılar.[52] Kibercinayətlərin belə hüquqi çərçivəyə salınması əslində müasir beynəlxalq hüququn tələbi kimi çıxış etmişdir.

Avstriyalı mütəxəssis Martin Stoun hesab edir ki, kiberməkanda cinayətlərin artması ilk növbədə yeni formalaşmaqda olan iqtisadi və sosial institutlara əsaslı zərbə vurur. Kibercinayətlər çox surətlə törədilən və mühakimə icraatının həyata keçirilməsi çətin olan cinayətdir. Şəbəkəyə zorla daxil olmalar və informasiya şəbəkələrinin "sındırılması" tamamilə anonim şəraitdə və bir necə saniyə ərzində baş verir. Buna görə də onlar cinayət hüquq mühakiməsindən yayına bilir və beləliklə də kompüter infrastrukturunda pozuntular törədərək, müntəzəm şəkildə milli qanunlar çərçivəsindən kənarda qalmağa müvəffəq olurlar.[53]

Tomsk Dövlət Universitetinin mütəxəssisi V.Povışev özünün ekspert məruzəsində qeyd edir ki, son illər dünya ictimaiyyəti BMT-nin timsalında informasiya texnologiyaları sahəsində cinayətkarlığın səviyyəsinin artması barədə narahatlığını ifadə etməyə başlamışdır ki, bu da qeyd olunan problemin dövlətdaxili müstəvidən beynəlxalq səviyyəyə keçməsinə dəlalət edir.[54]

Qeyd etmək lazımdır ki, bu problemin unikallığı ondadır ki, sözügedən cinayətlərlə mübarizə nə təkcə BMT-nin həll edə biləcəyi məsələ deyil, nə də konkret dövlətin müstəqil məşğul olmaq imkanı olan problem sayıla bilməz. Burada dəqiq müəyyən olunmuş beynəlxalq hüquqi mexanizmlərin olması mühüm şərt hesab olunur və bütün bunlar yalnız sıx çoxtərəfli beynəlxalq hüquqi əməkdaşlıq kontekstində rellaşdırıla bilər.

Kibercinayət hüququnun universal harmonizasiyası sahəsində son dövrlər müvafiq cəhdlər edilmiş, müqavilə mexanizmlərinin təkmilləşdirilməsi və prosessual tədbirlərin həyata keçirilməsi istiqamətində müəyyən addımlar atılmışdır. Bu gün artıq elmi dairələrdə və beynəlxalq hüquqi praktikada kibercinayətlərlə transmilli mübarizə aparmaq üçün universal tətbiq gücünə malik olan razılaşdırılmış beynəlxalq konvensiyanın qəbul edilməsinin zəruriliyi ilə bağlı fikirlər səsləndirilir. Aİ və ABŞ AŞ konvensiyasını dəstəkləyərək, bir çox dövlətlərin onu imzalamasını və ratifikasiya etməsini təşviq etmişlər. Lakin bir məsələni xüsusi qeyd etmək lazımdır ki, ABŞ və Avropa tərəfindən edilən bütün cəhdlərə baxmayaraq, bu konvensiya digər regionlarda o qədər də geniş yayılmamış, Avropa regionundan kənar ölkələrə geniş miqyasda nüfuz etməmişdir. Yeni qlobal kibercinayət

---

[49] World Drug Report 2013,United Nations Office on Drugs and Crime.New York, 2013, www.unodc.org

[50] Dunn Cavelty, Myriam. The Militarisation of Cyber Security as a Source of Global Tension February 1, 2012. Strategic Trends Analysis, Zurich, Mockli, Daniel,Wenger, Andreas, eds., Center for Security Studies, 2012. P 106SSRN: http://ssrn.com/abstract=2007043 (accessed July 28, 2014).

[51] Steve Gold, Security Breaches Cost $15 Bil. Yearly, NEWSBsrEs, atwww.newsbytes.com/news/00/158197.html

[52] Məcidli S. T. İnternet hüququ və etikası. Dərs vəsaiti. Bakı: "Elm və təhsil" nəşriyyatı, 2013. S.115, 224 səh.

[53] Martin Stone, Cybercrime Growing Harder to Prosecute - Report, NEWSBYTES, www.infowar.com/law/00/law_012400aj.shtml

[54] Владислав Повышев, Борьба с киберпреступностью и кибертерроризмом, Томский государственный университет, http://tmun.utmn.ru/wp-content/uploads/SPChKiber.pdf

müqaviləsinin qəbul edilməsi 12-ci BMT Cinayətlərin xəbər verilməsi və cinayət ədliyyəsi Konqresində (2010-cu il Salvador, Braziliya) müzakirə olunmuş və Norveçdən olan hakim Stein Şolberq və Lozanna Universitetinin professoru Solang Gernauti-Helie tərəfindən müqavilə layihəsi təqdim olunmuşdur. AŞ konvensiyası ilə müqayisədə bu konvensiya layihəsində prosedur məsələlər öz əksini tapmaqla, məzmun baxımından isə kiberməkanda intellektual mülkiyyət cinayətləri, kiberhücumlar, kiberterrorizm, informasiya infrastrukrununa qarşı cinayətlər təklif edilmişdir.[55]

Bundan əlavə Norveçli hakim Stein Şolberq 2-4 dekabr 2011-cil tarixdə İtaliyada keçirilmiş kibercinayətlərlə bağlı beynəlxalq konfransda etdiyi təqdimatda yuxarıda qeyd olunan konvensiya layihəsindəki kibercinayətlərlə mübarizədə müvafiq təsisatların yaradılması və digər prosessual mahiyyət kəsb edən fikirlərini daha da inkişaf etdirərək, Kiberməkan üzrə Beynəlxalq Cinayət Tribunalının təsis olunması (International Criminal Tribunal for Cyberspace (ICTC)) təklifini irəli sürmüşdür. Onun fikrincə, Kiberməkan üzrə Beynəlxalq Cinayət Tribunalı BMT Nizamnaməsinin VII fəslinə müvafiq olaraq, Təhlükəsizlik Şurasının qətnaməsi əsasında BMT Məhkəməsi kimi yaradılmalıdır. Məhkəmənin səlahiyyətləri ağır kibercinayətlərin və qlobal narahatlığa səbəb olan kiberhücumların mühakimə olunması və qəti qərarın çıxarılmasını özündə ehtiva edərək, aşağıdakı məsələlər üzrə yurisdiksiyaya malik olmalıdır:

1) Kibercinayətlər haqqında qlobal müqavilə və ya müqavilə şəbəkələri pozuntuları,

2) Kritik əhəmiyyətli informasiya infrastrukturları əleyhinə kütləvi və koordinasiya olunmuş qlobal kiberhücumlar.

Tribunal milli məhkəmələrə münasibətdə müvafiq yurisdiksiyaya malik olmalı, lakin milli məhkəmələr üzərində üstünlük hüququna iddia edə bilər və istənilən mərhələdə istintaqın aparılmasını, habelə mühakimə prosesini nəzarətə götürə bilər.[56]

Göründüyü kimi, müasir beynəlxalq hüquqda kibercinayətlərlə mübarizə üzrə əməkdaşlığın yeni və unikal forması kimi, bu sahədə müvafiq ixtisaslaşmış məhkəmə qurumunun və ya ad hoc tribunalların yaradılması məsələsi daha da aktualdır. Bu isə öz növbəsində bəşəriyyətin təxirəsalınmaz sosial tələbatından irəli gələrək, insan hüquqları kontekstində demokratik cəmiyyətin zəruri elementi kimi özünü büruzə verir.

Son illər insan hüquq və azadlıqlarının genişlənməsi və daha səmərəli şəkildə müdafiəsi imkanlarının artması eyni zamanda, azad informasiya mübadiləsinin və internetə sərbəst çatım imkanlarının da genişlənməsinə əlverişli şərait yaratmışdır.

Xüsusilə vurğulamaq lazımdır ki, bu gün Azərbaycanda daha təkmil və azad bir kiberməkan formalaşmış, insanların şəbəkəyə çıxışı və bu müstəvidə elektron xidmətlərdən faydalanma əmsalı yüksələn xətlə inkişaf etməkdədir. Bu sahədə ölkəmiz yeni beynəlxalq əməkdaşlıq formalarından bəhrələnməklə, nəticə etibarilə kiberməkan istifadəçilərinin hüquq və azadlıqlarının, eyni zamanda kibertəhlükəsizliklərinin təminatına mühüm töhfələr verir. Bununla əlaqədar ölkə Prezidenti cənab İlham Əliyev öz çıxışlarında dəfələrlə bəyan edib. Prezident Strasburqda Avropa Şurası Parlament Assambleyasının (AŞPA) sessiyasındakı nitqində vurğulayır. "Bizdə azad internet vardır. Azərbaycanda internet istifadəçilərinin sayı 70 faizdən artıqdır. Hazırda hökumətimiz böyük sərmayələri tələb edən layihəni həyata keçirməkdədir: geniş zolaqlı internet hər bir şəhər və kənd üçün təmin edilməlidir. Digər sözlə, azad internetin mövcudluğu, senzuranın olmaması şəraitində biz mətbuat azadlığını məhdudlaşdıra bilmərik. Əksinə, biz mətbuat azadlığının tərəfdarıyıq, Çünki media azadlığı demokratiya deməkdir. O, hökumətə çatışmazlıqlara diqqət yönəltməyə yardım edir. O, hökumət ilə cəmiyyət arasında zəruri əlaqələrin qurulmasına zəmin yaradır."[57] Göründüyü kimi, kiberməkandan azad istifadə və kibertəhlükəsizliyin təminatı, azad internet məkanı kimi qlobal əhəmiyyətli məsələlərə dövlət başçısı səviyyəsində xüsusi diqqət ayrılır.

Qloballaşma proseslərinin vüsət aldığı müasir dövrümüz milli təhlükəsizlik sahəsində adekvat ixtisaslı tədbirlərin həyata keçirilməsini zəruri edir. O vurğulayır ki, geostrateji mövqeyi baxımından beynəlxalq maraqların kəsişdiyi bir məkan olan Azərbaycanın son illərdə dinamik inkişafının, tranzit əhəmiyyətinin artmasının, beynəlxalq neft-qaz kəmərlərinin işə düşməsi, dünya nizamının dəyişkənliyi, mürəkkəbliyi və ziddiyyətli olması, terrorçuluğun, informasiya müharibəsinin, kibercinayətkarlığın genişlənməsi təhlükəsizlik məsələlərini daha qabarıq formada üzə çıxarır və mübarizənin yeni formada, müasir tələblərə uyğun aparılmasını vacib edir. Müəyyən qüvvələrin internet resurslarından istifadə olunmaqla əməliyyat şəraitinə təsir göstərmə imkanları, kibercinayətkarlıq, informasiya təhlükəsizliyi bu günün reallıqlarıdır.

Yeni iqtisadi amillər, qlobal transmilli münasibətlər sistemi yeni cinayətlərin – kibercinayətlərin qarşısının alınması üzrə beynəlxalq əməkdaşlığın da yeni meyllərini şərtləndirir. İnternetin sürətli inkişafı mahiyyət etibarilə yeni hüquq pozuntularına, o cümlədən kibercinayət əməllərinin dairəsinin çoxalmasına da imkan yaratmışdır. Bunu son illər həm şəbəkə istifadəçilərinin artan sayına, həm də kibercinayətlərin statistikasına nəzərən qətiyyətlə söyləmək mümkündür. Artıq bu gün XX əsrin ortalarına və ya sonlarına nisbətdə XXI əsrin ikinci onilliyində "kibercinayət" anlayışı BMT başqa olmaqla və bu qurumun təşəbbüsü altında müxtəlif dövlətlərin milli cinayət qanunvericiliklərində yeni kriminal tərkib kimi təsbit olunmuşdur.

Bu səbəbdən də qeyd olunan cinayətlərin xüsusilə universal əsasda daha effektiv şəkildə və daha geniş dairədə mübarizə imkanları BMT çərçivəsində, eyni zamanda İnterpol vasitəsilə reallaşdırılması daha mühüm nəticələri ilə səciyyələnə bilər. Lakin burada bir xüsusi məqamı da nəzərdən qaçırmaq olmaz ki, kiberməkandakı

---

[55] Handbook of Asian Criminology. New York 2013. C. 60.- 85

[56] Potential new global legal mechanisms on combating cybercrime and global cyberattacks. A presentation at the United Nations - ISPAC International Conference on Cybercrime: Global Phenomenon and its Challenges. Courmayeur, Italy. December 2-4, 2011. By Judge Stein Schjolberg. Norway. www.cybercrimelaw.net

[57] İlham Əliyev Avropa Şurası Parlament Assambleyasının sessiyasında çıxış etmişdir, 24 iyun 2014, http://www.president.az/articles/12149

hər hansı cinayətin qarşısını alarkən insanların şəbəkəyə çatma hüququ kimi mühüm azadlıqlarına xələl gəlməsin. Bunun üçün bəşəriyyətin yeni proqressiv inkişafının mühüm stimulu kimi internetin müsbət və mənfi tərəfləri arasında balansın gözlənilməsi vacib hesab olunduğundan, burada da əsas missiya BMT-nin müvafiq qurumlarının üzərinə düşür ki, onlar ümumi standartlar müəyyən etməklə innovativ, universal və ümum məcburi əhəmiyyətə malik qaydalar müəyyən etsin.

Kibercinayətlərlə mübarizənin universal və regional əməkdaşlıq üçün əsaslı bir problem olduğunu qeyd edən hüquqşünas alim O.S.Alaverdov hesab edir ki, internet-cinayətkarlığı (hüquqşünas alim "internet cinayətkarlığı" terminə üstünlük verib) yalnız bir dövlətin özünün hakimiyyət mexanizmlərindən istifadə edərək, müstəqil həll etmək iqtidarında olmadığı məsələdir. Ona görə də transmilli təhlükə olan internet cinayətkarlığının qarşısının alınması yalnız dünya ictimaiyyətinin daimi aşkar əməkdaşlığı ilə mümkün ola bilər.[58] Göründüyü kimi, əksər doktrinal hüquqi mövqelər məhz kibercinayətlərlə mübarizənin yalnız transmilli amilini önə çəkməklə, onu konkret bir dövlətin həll etmək iqtidarında olmadığı milli məsələ kimi qəbul etmir. Buradan da belə nəticə hasil olur ki, əslində kiberməkan seqmentlərinə görə ayrı-ayrı dövlətlərin istifadəsində olsa da, burada baş verən hüquqazidd davranışlar bütün dünya birliyinə təhlükə hesab olunduğu üçün, bu cinayətlər və onlarla mübarizənin xüsusiyyətləri transmilli mahiyyət kəsb edir.

Kibercinayətkarlıqla mübarizə sahəsində münasibətlərin tənzimlənməsində universal və regional beynəlxalq müqavilələrin rolundan danışarkən çoxtərəfli qarşılıqlı yardım üzrə əməkdaşlığı xüsusilə vurğulamaq lazımdır. Bununla əlaqədar BMT Baş katibinin məruzəsində də mütəşəkkil cinayətkarlıq sahəsində birgə fəaliyyətin zəruriliyi qeyd olunub. Orada bildirilir: "Bütün beynəlxalq təşkilatlar cinayətlərin ibtidai istintaqı zamanı, qarşılıqlı yardımların göstərilməsi zamanı koordinasiya olunmuş dövlətlərarası birgə fəaliyyətin zəruriliyini qeyd edirlər."[59] Belə əməkdaşlığın nəticəsidir ki, bu gün BMT, İqtisadi Əməkdaşlıq və İnkişaf Təşkilatı, İnterpol, Böyük Səkkizlik (G8), Avropa Şurasının səyləri ilə artıq kibercinayətlər üzrə beynəlxalq qanunvericilik formalaşdırılmışdır.

Yuxarıda qeyd etdyimiz kimi, kiber məkanda daha yetkin və effektiv tənzimlənmə məqsədilə bütün beynəlxalq birlik üçün ümum məcburi qaydaların və hamı üçün ümumi xarakter daşıyan prinsiplərin işlənib hazırlanaraq formalaşdırılması, habelə bu istiqamətdə konseptual beynəlxalq hüquqi yanaşmanın ortaya qoyulması lazımdır. Fikrimizcə, burada vahid yanaşmanın ortaya qoyulması üçün aşağıdakı iki mühüm məsələyə diqqətin ayrılması zəruridir.

1) Kiberməkanda baş verən konkret cinayət tərkiblərinin ümumiləşdirilmiş siyahısının müəyyən edilməsi və beynəlxalq hüquqi unifikasiyası;

2) Bu cinayət tərkiblərinin hər birinin dövlətlərin milli cinayət qanunvericiliklərinə inkorporasiyası və ya transformasiyası.

Çünki, yalnız yuxarıda qeyd olunan faktorlar nəzərə alınmaqla, kibercinayətlərə qarşı mübarizənin qlobal miqyaslı müsbət nəticələrindən danışmaq mümkün ola bilər.

Eyni zamanda burada bir məqamı da nəzərdən qaçırmaq olmaz ki, kibercinayətlər üzrə həm universal, həm də regional müqavilələr xüsusilə kibercinayət tərkiblərinə münasibətdə ortaq mövqedən çıxış etməli və cinayət tərkiblərinin dəqiq müəyyən olunması üzrə vahid kontentə malik olmalıdır. Lakin bu cinayətlərə qarşı mübarizənin forma və vasitələrinə, eyni zamanda mübarizə mexanizmlərinə və proseduralarına münasibətdə fərqliliklərin olması mümkün ola bilər.

Kibercinayətkarlıqla mübarizə sahəsində münasibətlərin tənzimlənməsində universal və regional beynəlxalq müqavilələrin rolu ilə bağlı çox mühüm elmi əhəmiyyəti olan vasitələrdən biri də bu sahədə təşkil olunan beynəlxalq konfranslar, seminar, konqres, simpozium və forumlardır. Bunlar, əlbəttə, əməkdaşlığın ilkin cizgilərinin qurulması üçün olduqca önəmlidir.

Yeni dönəmdə kibercinayətkarlıqla mübarizə sahəsində beynəlxalq hüquqi əməkdaşlıq məsələlərini nəzərdən keçirən zaman bu sahədə 1995-ci ilin aprelində keçirilmiş Kompüter cinayətkarlığı üzrə İnterpolun I Beynəlxalq konfransı xüsusi qeyd olunmalıdır. 49 ölkənin hüquq-mühafizə, xüsusi xidmət orqanlarının nümayəndələrinin, iri bankların əməkdaşlarının və ekspertlərin iştirakı ilə keçirilmiş həmin konfrans kompüter cinayətləri üzrə beynəlxalq hüquqi müqavilə bazasının formalaşması istiqamətində ilkin əməkdaşlıq forması hesab edilir.

Kibercinayətkarlıqla mübarizə sahəsində münasibətlərin tənzimlənməsi üzrə universal beynəlxalq müqavilələrin formalaşmasında müstəsna əhəmiyyəti olan tədbirlərdən biri də BMT çərçivəsində keçirilmiş cinayətlərin xəbər verilməsi və hüquq pozuntusu törədən şəxslərlə davranış üzrə 2000-ci il tarixli X Konqresdə isə xüsusi olaraq dünyada kibercinayətlərin artım səviyyəsi qeyd olunmuş, yüksək texnologiyalar sahəsində cinayət növlərinin genişlənməsi və bu tipli əməllərin yeni təzahür formalarının meydana gəldiyi vurğulanmışdır.

Bu konfransların kibercinayətlərin qarşısının alınması və bu sahədə yeni tendensiyaların formalaşmasında xüsusi əhəmiyyəti nəzərə alınaraq, nəinki universal, eyni zamanda, regional və milli səviyyələrdə norma və prinsiplərin, qərar və qətnamələrin, habelə qanunvericilik sisteminin yaranmasına təsiri danılmazdır.

Bundan əlavə, Kibercinayətlərlə mübarizə üzrə əməkdaşlığa dair yeni tendensiyalar BMT-nin İqtisadi və Sosial Şurasının 26 fevral 2014-cü il tarixli yuxarıda qeyd etdiyimiz Cinayətlərin xəbər verilməsi və cinayət mühakiməsi üzrə Komissiyası tərəfindən keçirilmiş 23-cü sessiya çərçivəsində xüsusi qərar qəbul edilmişdir.

---

[58] Алавердов О.С. Международное сотрудничество в области борьбы с интернет-преступностью, Общество и право, 2010. http://www.juristlib.ru/book_9544.html

[59] Доклад Генерального Секретаря ООН "Воздействие организованной преступной деятельности на общество в целом" // Материалы Комиссии ООН по предупреждению преступности и уголовному правосудию. Вена, L7CN 15/1993/3.

Həmin sənədin E bölməsinin (Cinayətkarlığın yeni və yaranmaqda olan növləri ilə mübarizədə beynəlxalq əməkdaşlıq) 57-ci bəndində qeyd olunur: "Kibercinayətlər şübhəsiz ki, qlobal əks-tədbirlərin görülməsini tələb edən birinci cinayət növləri deyildir. Qeyd olunmalıdır ki, müasir kibercinayətlər, habelə elektron daşıyıcılarla əlaqədar cinayətlər beynəlxalq əməkdaşlıq sahəsində unikal çağırışlar səsləndirir. Elektron daşıyıcıların qısamüddətli xarakterini nəzərə alaraq, kibercinayətlərlə mübarizə işində beynəlxalq əməkdaşlıq öz növbəsində dərhal reaksiya verilməsini və xüsusi araşdırma tədbirlərinin görülməsi barədə sorğu göndərmək xüsusiyyətini tələb edir. Baxmayaraq ki, hüquq-mühafizə orqanları arasında əməkdaşlığın bir sıra qeyri-rəsmi metodları, o cümlədən "24/7" şəbəkəsi mövcuddur, ölkədən elektron sübutların alınması üçün əhəmiyyətli dərəcədə əvvəlki ənənəvi məhkəmə kanalları vasitəsindən, xüsusilə qarşılıqlı yardım haqqında ikitərəfli sənədlərdən istifadə olunur."[60] BMT-nin Cinayətlərin xəbər verilməsi və cinayət mühakiməsi üzrə Komissiyasının qeyd olunan sənədinin 58-ci bəndi isə qarşılıqlı hüquqi yardımın bəzi prosedur məsələlərinə aydınlıq gətirmişdir. Orada bildirilir ki, kibercinayətlərin araşdırılmasına dair qarşılıqlı hüquqi yardım haqqında belə sorğuya cavabın alınması müddəti adətən 150 gün təşkil edir. Komissiyanın hazırladığı sənədin 59-cu bəndi isə elektron informasiyalardan istifadə ilə əlaqədar şəxsi məlumatların əldə edilməsi üzrə hüquq pozuntusu törədən şəxslər barədə tədbirlərin görülməsi ilə bağlı beynəlxalq əməkdaşlıq məsələlərinə həsr edilmişdir.

Kibercinayətlərin beynəlxalq cinayət hüquq sistemində pozitivləşməsi, onların təsnifatı, profilaktikası və məsuliyyət problemlərinin həlli istiqamətində BMT-nin ayrı-ayrı orqan və komissiyalarının da əvəzsiz rolu vardır. Məsələn, Cinayətlərin xəbər verilməsi və cinayət hüquqi mühakimə üzrə BMT Komissiyası 2001-ci ildə hazırladığı məruzəsində kibercinayətkarlıqla mübarizə sahəsində daha mühüm və irəliyə doğru bir addım ataraq, kibercinayətlərin təsnifatını verməyə müvəffəq oldu. Bunun isə öz növbəsində kibercinayətkarlıqla mübarizə sahəsində ilk regional beynəlxalq müqavilə olan Budapeşt Konvensiyasının müddəalarının formalaşdırılmasına bilavasitə təsiri olmuşdur.

Beləliklə, BMT çərçivəsində cinayətkarlıqla mübarizə üzrə universal müqavilənin qəbul edilməsində problemlərin mövcudluğuna baxmayaraq, bu qurumun missiyası çərçivəsində aparılan müzakirələr kontekstində qətiyyətlə söyləmək mümkündür ki, məhz bu təşkilatın həyata keçirdiyi fəaliyyətin nəticəsində regional müqavilələrin rüşeymi formalaşmış və müasir səviyyəyə çatmışdır.

2.1.2. Budapeşt Konvensiyası kontekstində Avropa Şurasında kibercinayətlərlə mübarizə

Regional müstəvidə kibercinayətlərlə mübarizə üzrə mühüm qurumlardan biri Avropa Şurası (AŞ) hesab edilir. Qeyd olunmalıdır ki, BMT-nin İqtisadi və Sosial Şurası, Cinayətlərin xəbər verilməsi və cinayət hüquqi mühakimə üzrə BMT Komissiyasının spesifik səyləri nəticəsində regional, xüsusilə AŞ çərçivəsində qəbul olunmuş Budapeşt Konvensiyası beynəlxalq hüquqi dövriyyəyə çıxmışdır.

Ona görə də biz kibercinayətkalıqla mübarizə sahəsində əməkdaşlığın hüquqi özülünü təşkil edən regional müqavilələrdən ilkin olaraq Budapeşt Konvensiyası üzərində təhlillərimizi davam etdirməyi məqbul hesab edirik.

Qeyd edək ki, Kibercinayətkarlıq haqqında 2001-ci il Budapeşt Konvensiyasının informasiya texnologiyaları sferasında hüquqazidd hərəkət və hərəkətsizliklərin beynəlxalq hüquqi kriminallaşdırılması və onunla mübarizənin aparılması istiqamətində beynəlxalq əməkdaşlıq üzrə rolu bir necə mühüm üstünlükləri ilə xarakterizə edilə bilər:

- Bu müqavilə yuxarıda qeyd etdiyimiz kimi beynəlxalq cinayət hüququnda yüksək texnologiyalar və informasiya təhlükəsizliyinin təmin olunması üzrə ilkin rəsmi çoxtərəfli sənəd hesab olunur;
- Bu konvensiya kibercinayətlərin forma və növlərə bölgüsünü rəsmi olaraq özündə təsbit etmiş beynəlxalq hüquqi akt hesab edilir;
- Qeyd olunan sənəddə İKT sahəsində hüquqazidd əməllər ilk dəfə olaraq dövlətlər tərəfindən cəzalandırılmalı olan hərəkət və hərəkətsizliklər kimi xarakterizə olunmuşdur;
- Bu konvensiya kibercinayətlərin önlənməsi və onunla mübarizə üzrə müxtəlif dövlətlərin hüquq-mühafizə orqanlarının səylərinin birləşdirilməsi zərurətini beynəlxalq müqavilə qaydasında rəsmiləşdirən sənəd hesab edilir;
- İnformasiya texnologiyaları üzrə hüquqazidd əməllərə qarşı mübarizədə dövlətlərin fəaliyyətlərinin koordinasiya və milli qanunvericiliklərini unifikasiya edən rəsmi aktdır;
- Bu sənədin daha bir özəlliyi də ondan ibarətdir ki, hüquqi cəhətdən AŞ çərçivəsində bağlanan müqavilə olmasına baxmayaraq, 39 üzv dövləti özündə birləşdirən bu konvensiya coğrafi əhatə dairəsinə görə universal xarakterli hesab oluna bilər. Bu tezisi onunla əsaslandırmaq mümkündür ki, qeyd olunan sənədi 35 Avropa dövlətindən başqa, planetin digər dövlətləri Avstraliya, Dominikan Respublikası, Yaponiya və ABŞ da ratifikasiya etmişdir.

Lakin, müasir dövrdə 2001-ci il Budapeşt Konvensiyasının yuxarıda qeyd olunan tezislərə müxalif olan fikirlərlə də rastlaşmaq mümkündür. Belə ki, 2014-cü ilin 26 avqust tarixində Prokurorların Baykal Beynəlxalq Konfransında Rusiya Federasiyası Baş Prokurorunun müavini A.Q.Zvyaqinçeva qeyd etmişdir ki, telekommunikasiyaların müasir vasitələrinin inkişafı ilə əlaqədar olaraq, kibercinayətlərin istintaqı üzrə beynəlxalq hüquqi yardımların göstərilməsi məsələlərinin xüsusi tənzimlənməsinə zərurət yaranmışdır. Baş

[60] Организация Объединенных Наций E/CN.15/2014/12, Экономический и Социальный Совет, Distr.: General 26 February 2014, V.14-01305 (R) 240314 250314, Комиссия по предупреждению преступности и уголовному правосудию, Двадцать третья сессия, Вена, 12-16 мая 2014 года.

Prokurorun müavini daha sonra bildirir ki, dünya ictimaiyyəti informasiya texnologiyaları sahəsində BMT çərçivəsində cinayətkarlıqla mübarizə haqqında müqavilə bağlamadan keçinə bilməz. "Təəssüf ki, Avropa Şurasının eqidası altında 2001-ci ildə bağlanmış kibercinayətkarlıq əleyhinə konvensiya özünün bir sıra çatışmazlıqları ilə, xüsusilə cinayət işləri üzrə əməkdaşlıq sahəsində dünya miqyaslı müqavilə roluna iddialı ola bilməz."[61]

Göründüyü kimi, beynəlxalq hüquqda kibercinayətlər sahəsində mövcud olan beynəlxalq sazişlər əsasən regional tənzimləmə funksiyalarına malik olduğu üçün, əksər ekspert və elm xadimləri kiberfəzada transmilli münasibətlərin qlobal tənzimlənməsi üçün mövcud mexanizmləri qənaətbəxş hesab etmirlər. Bunun üçün regional müqavilələrin universal müqavilə ilə əvəzlənməsi və kibercinayətlərin qarşısının alınması, xəbər verilməsi, cəzalandırılması üzrə cinayət işlərinə yardım məsələsində dövlətlərin qarşılıqlı əlaqələrini tənzimləyən universal müqavilənin hazırlanması və qəbul edilməsi zəruridir. Belə bir təsirli müqavilə mexanizmi yalnız BMT çərçivəsində işlək xarakterli ola bilər. Digər tərəfdən fikrimizcə, bu gün kibertəhlükəsizlik dünyada ümumi təhlükəsizlik sisteminin ayrılmaz tərkib hissəsini təşkil etməklə, bəşəriyyətin həyatında qlobal tənzimlənmə tələb edən xüsusi sahələrdən biridir.

Lakin müasir beynəlxalq hüququn inkişaf tendensiyalarını, eyni zamanda Avropa regionunda milli dövlətlərin qanunvericiliklərinə təsir imkanlarına malik olan daha işlək və nüfuzlu təsisatların formalaşmasını nəzərə alsaq, kibercinayətkarlıqla mübarizədə bu regionda formalaşan müqavilə hüquq bazasına xüsusi diqqətin ayrılmasını zəruri hesab edirik.

Qeyd olunmalıdır ki, Budapeşt Konvensiyasının daha bir xüsusi əhəmiyyətli cəhətlərindən biri də odur ki, bu sənəd Avropa və digər regional qurumların informasiya texnologiyaları sferasında gələcək fəaliyyətləri üçün bir növ stimul verici akt hesab olunur.

2.1.3. Avropa İttifaqında kibertəhlükəsizlik məsələləri

Kibertəhlükəsizliyin təmin olunması üzrə aktiv fəaliyyət göstərən və Budapeşt Konvensiyasını təşviq edən qurumlardan biri və demək olar ki, birincisi Avropa İttifaqıdır. Belə ki, Avropa Komissiyasının kibercinayətlər üzrə kommunikasiyalarından və bu qurumun qəbul etdiyi digər əlaqədar siyasi sənədlərin siyahısından da yuxarıda qeyd edilən fikrin doğruluğunu təsdiq etmək mümkündür.

Qeyd olunan məsələnin vacib əhəmiyyətini vurğulayan Rusiyalı hüquqşünas N.O.Moroz hesab edir ki, bununla əlaqədar olaraq Avropa İttifaqı və Avropa Şurası çərçivəsində kibercinayətkarlıqla mübarizənin normativ-hüquqi əsaslarının öyrənilməsi zəruridir.[62]

Bu sırada Avropa Parlamenti, Şurası, Avropa İqtisadi və Sosial Şurası və Regionlar Komitəsinin birgə "Avropa İttifaqı Kibertəhlükəsizlik Strategiyası: acıq və təhlükəsiz kiberfəza" Kommunikasiyaları (7 fevral 2013-cü il), Onlayn Uşaq Seksual Cinayətləri əleyhinə Qlobal Alyans haqqında Şuranın Xülasəsi (Lüksemburq, iyun 2012-ci il) və s. sənədləri göstərmək olar.

Avropa İttifaqı kiberfəzada münasibətlərin tənzimlənməsini məzmun baxımından koordinasiya etməyə cəhdlər göstərmiş, bu istiqamətdə tövsiyə və direktivlər vermişdir. Nəzərə alsaq ki, Avropa İttifaqının qərar və direktivləri üzv dövlətlərin hökumətləri və vətəndaşları üçün məcburi hüquqi qüvvəyə malikdir, o zaman qeyd olunmalıdır ki, Aİ çərçivəsində qəbul edilən bütün qərarlar digər regional qurumların qəbul etdikləri sənədlərdən özünün məcburilik əlamətinə görə xüsusi proseduralara malik olacaq.

Ümumiyyətlə Avropa regionunda kibercinayətlərlə əlaqəli, o cümlədən internetdə uşaq pornoqrafiyasına qarşı mübarizə, məlumatların, informasiya resurslarının mühafizə edilməsi, informasiya hücumlarından müdafiə məsələləri xüsusi qanunvericilik qaydasında qorunur. Məsələn, bu sənədlərin sırasında Avropa İttifaqı Şurasının qəbul etdiyi 19 may 2011-ci il tarixli Tənqidi İnformasiya İnfrastrukturunun Mühafizəsi "Nailiyyətlər və Növbəti Addımlar: qlobal kibertəhlükəsizliyə doğru" sənədini, 2009-cu il tarixli Avropanın genişmiqyaslı kiberhücumlardan və təhlükələrdən Mühafizəsi haqqında sənədi, Aİ Şurasının İnformasiya sistemlərinə qarşı hücumlar haqqında 2005-ci il tarixli Çərçivə Qərarını, 2004-cü il tarixli Uşaqların seksual istismarı və uşaq pornoqrafiyasına qarşı mübarizə haqqında 2004-cü il tarixli Çərçivə Qərarını misal göstərmək olar. Bundan başqa, son illər İnformasiya hücumları haqqında 12 avqust 2013-cü il tarixli və İttifaq üzərindən yüksək səviyyəli ümumi şəbəkələrin və informasiya təhlükəsizliyinin təmin olunması tədbirlərinə dair 07.02.2013-cü il tarixli Aİ direktivləri də regional hüquqi tənzimlənmənin həyata keçirilməsində müstəsna əhəmiyyətə malik olmaqla, Aİ üzv dövlətlərində məcburi hüquqi qüvvəyə malikdir.

Eyni zamanda, Aİ çərçivəsində qəbul edilmiş müqavilələrdə də kibercinayətkarlıqla mübarizə və təhlükəsizlik məsələlərinə xüsusi yer ayrılmış və kibercinayətlər sferası Aİ-nin müqavilələrində və orqanlarının fəaliyyətində özünəməxsus şəkildə öz əksini tapmışdır. 2009-cu il tarixli Lissabon müqaviləsinin "Azadlıq, təhlükəsizlik və ədalət" adlı V bölməsi kibertəhlükəsizlik məsələlərinin Aİ-nin gündəliyinə daxil etməklə, qərara alınmışdır ki, Aİ azadlıq, təhlükəsizlik və ədalət məkanına çevrilsin.[63]

Göründüyü kimi, ümumi təhlükəsizlik məsələlərini də əhatə etməklə kibertəhlükəsizlik və kibercinayətlərin qarşısının alınması Aİ-də prioritet təşkil etməklə bu quruma daxil olan dövlətlər üçün eyni zamanda müqavilə bazasının da möhkəmlənməsinə öz töhfəsini vermişdir. Həmin müqavilələr isə Aİ dövlətlərində birbaşa hüquqi

---

[61] Основные тезисы выступления заместителя Генерального прокурора Российской Федерации А.Г.Звягинцева на Байкальской международной конференции прокуроров (26.08.2014) http://www.genproc.gov.ru/pda/news/news-290542/

[62] Мороз Наталия Олеговна. Международно-правовое сотрудничество в борьбе с преступностьюв сфере высоких технологий. Автореферат диссертации на соискание ученой степени кандидата юридических наук. Минск, 2014. С. 13, 23 с.

[63] Consolidation version of the Treaty on the Functioning of the European Union, Title V – Area of Freedom, Security and Justice (Official Journal C 115/47 of 09.05.2008)

qüvvəyə malik olduğundan, xüsusi qeyd olunmalıdır ki, Aİ məcburi müqavilə mexanizmlərini reallaşdırmaqla kibercinayətlərlə mübarizədə nəinki Avropada, bütövlükdə qlobal anlamda xüsusi çəkiyə malikdir.

Mühüm məsələlərdən biri də kibercinayətkarlıq sahəsində Avropa İttifaqı qurumlarının İnterpol və bu kimi digər cinayət hüquq təşkilatları ilə beynəlxalq əməkdaşlığın və əlaqələrin inkişafı məsələsidir. Bu sahədə mühüm prosessual sənədlərdən biri 25 iyun 2001-ci il tarixdə Avropa İttifaqı Şurasının qəbul etdiyi "Kibercinayətkarlıqla mübarizə üzrə 24 saatlıq növbətçi xidmətinin təsis olunması üzrə əməkdaşlıq sisteminin yaradılması haqqında" Tövsiyə hesab olunur. Həmin sənəddə İnterpol və Avropa İttifaqı tərəfindən kibercinayətkarlıqla mübarizə üzrə tətbiq olunan standartların kollizion məsələlərinə aydınlıq gətirilmiş, əməkdaşlığın qarşılıqlı prinsipləri müəyyən olunmuşdur.[64]

Bütün bunlar onu göstərir ki, kibercinayətlər Avropa regionu üçün xüsusi təhlükəli ağır cinayət əməli hesab olunduğu üçün bu məsələdə beynəlxalq əməkdaşlığa da xüsusi önəm verilir və bu istiqamətdə qərarlar, direktivlər və tövsiyələr qəbul edilir.

Bundan əlavə, yüksək texnologiyalar sahəsində cinayətkarlıqla mübarizə üzrə beynəlxalq hüquqi əməkdaşlığı təhlil edərkən, belə bir nəticə çıxarmaq olar ki, müvafiq müqavilə hüquq normaları cinayətkarlığın qarşısının alınması məsələləri üzrə konvensiyalarda, həmçinin kibercinayətkarlıqla mübarizə üzrə xüsusi müqavilələrdə öz əksini tapmışdır. Bundan başqa, xüsusi qrup beynəlxalq müqavilələr vardır ki, İKT kontekstində insan hüquqlarını özündə ehtiva edir və onların həyata keçirilməsinə təminat verir.[65] Belə müqavilələrə misal olaraq, 28 yanvar 1981-ci il tarixli Şəxsi xarakter daşıyan məlumatların avtomatik işlənməsinə münasibətdə fiziki şəxslərin müdafiəsi üzrə Avropa Şurası Konvensiyasını və Avropa İttifaqının 7 dekabr 2000-ci il tarixli Əsas Hüquqlar Xartiyasını[66] göstərmək olar.

2001-ci ilin yanvarında Avropa Komissiyası "İnformasiya infrastrukturunun müasirləşdirilməsi və kibercinayətlərlə mübarizə yolu ilə təhlükəsiz informasiya cəmiyyətinin yaradılması haqqında" Kommünike qəbul etdi. Bu sənəd yüksək texnologiyalar sahəsində cinayətkarlığa qarşı Avropa regional siyasətinin əsaslarını möhkəmlədirdi. Lakin, bu Kommünike tövsiyə xarakteri daşımaqla, üzv dövlətlər üçün kibercinayətkarlığa qarşı mübarizənin həyata keçirilməsi üzrə ümum məcburi qaydaları özündə əks etdirmir.

Aİ daxilində kibercinayətlər üzrə müqavilə mexanizmləri bu sahədə həmçinin bir sıra növbəti strategiya və fəaliyyət planlarının qəbul edilməsinə, habelə institusional strukturların formalaşmasına səbəb oldu. 26 aprel 2010-cu il tarixdə Aİ-nin Nazirlər Şurasının 3010-cu (Lüksemburq) toplanışında Kibercinayətlərlə mübarizə üzrə birgə strategiyanın implementasiyasına dair Fəaliyyət Planı, 4 iyun 2012-ci ildə Avropa Kibercinayətlər Mərkəzinin təsis olunması haqqında Aİ Şurasının qərar layihəsi qəbul olunmuşdur.

XX əsrin sonlarında Avropa İttifaqı çərçivəsində kompüter texnikasının, kommunikasiyaların və proqram təminatlarının sürətli inkişafı şəraitində bütövlükdə informasiya cəmiyyəti konsepsiyası işlənib hazırlanmışdır.[67]

Yuxarıda analiz olunan müqavilə və sənədlərdən göründüyü kimi kibercinayətkarlıqla mübarizə sahəsində münasibətlərin tənzimlənməsində universal və regional beynəlxalq müqavilələr qarşılıqlı təsiri ilə xarakterizə olunur. Burada əsas tendensiya bundan ibarətdir ki, kibercinayətlər üzrə müqavilələr üzrə fəaliyyət regional müstəvidən universal əsaslara doğru dəyişməkdədir.

2.1.4. MDB və Şərq ölkələrində kibercinayətlərlə mübarizənin hüquqi elementləri

Bu gün artıq əksəriyyət dünya ölkələrinin milli qanunvericilikləri müvafiq beynəlxalq və regional qurumların sənədlərinə adaptasiya olunmağa başlamışdır. Diqqət yetirdikdə görmək mümkündür ki, artıq nəinki Avropa regionu qurumlarının, eyni zamanda digər regionlarda da kibercinayətlərə qarşı qlobal mübarizə alətləri inkişaf etməklə, yeni müqavilə mexanizmlərinin əsasları işlənib hazırlanaraq qəbul edilir.

Ümumiyyətlə, bir məsələni xüsusi qeyd etmək lazımdır ki, Avropa regionu üzrə kibercinayətkarlıq sahəsində müqavilələrin analizi göstərir ki, Avropa qurumları bu sahədə nəinki mövcud təcrübələri beynəlxalq hüquqi qaydada ümumiləşdirərək pozitivləşdirmiş, eyni zamanda, əməkdaşlığın özünəməxsus modelinin formalaşması istiqamətində mühüm addımlar atmış, onun müsbət və mənfi tərəflərini elmi-praktiki nöqteyi-nəzərdən təhlil etmişdir. Nəticədə, beynəlxalq əməkdaşlığın bu modelləri, habelə qəbul edilmiş müqavilələr və digər sənədlər dünyanın başqa regionlarında kibercinayətkarlıq sahəsində müvafiq müqavilə bazasının formalaşmasına özünün müsbət təsirini göstərmişdir.

Belə ki, 2012-ci ildə Afrika İttifaqı tərəfindən kibertəhlükəsizlik məsələlərinin inkişafı üzrə mühüm addım atılaraq, Afrikada Kibertəhlükəsizlik fəaliyyəti üzrə Hüquqi Çərçivənin müəyyən olunması haqqında Konvensiya layihəsi qəbul edilmişdir. Bundan öncə isə bu regionda Qərbi Afrika ölkələrinin İqtisadi Birliyi (ECOWAS) tərəfindən 2009-cu ildə ECOWAS çərçivəsində Kibercinayətlərlə mübarizə haqqında Direktiv layihəsi, 2011-ci ildə Şərqi və Cənubi Afrika üçün Ümumi Bazar (COMESA) təşkilatı çərçivəsində Kibertəhlükəzsilik haqqında Model Bill layihəsi qəbul edilmişdi. Beləliklə, Afrika regionu ölkələrində biz son dövrlər kibercinayətlər və regionun kibertəhlükəsizliyi məsələlərinin tənzimlənməsində təşəbbüslərin ortada olduğunun şahidi ola bilərik.

---

[64] Council Recommendation of the 25th June 2001 on contact points maintaining a 24-hour service // for combating high-tech crime // OJ C 187 of 3.07.2001 // http://europa.eu/scadplus/leg/en/lvb/l23193.htm. – Date of access: 27.10.2007.

[65] Договорно-правовая деятельность в борьбе с преступностью в сфере высоких технологий. http://bibliofond.ru/view.aspx?id=556835

[66] Международное право и борьба с преступностью: сб-к документов / Составители: А.В. Змеевский, Ю.М. Колосов, Н.В. Прокофьев. - М.: Международные отношения, 2004. - 720 с., Convention for the protection of individuals with regard to automatic processing of personal data of 28.1.1981, Charter of Fundamental Rights of the European Union // Official Journal C 364, 18/12/2000 P. 0001 - 0022

[67] Мороз Наталия Олеговна, Международно-правовое сотрудничество в борьбе с киберпреступностью в рамках Европейского Союза и Совета Европы. http://www.pac.by/dfiles/001353_411080_moroz2.pdf

Regional əhəmiyyətinə görə Ərəb Dövlətləri Liqası tərəfindən qəbul olunmuş müqavilə xarakterli sənədlər də özünəməxsus cəhətləri ilə fərqlənir. 2010-cu il tarixli İnformasiya texnologiyaları cinayətləri ilə mübarizə haqqında Ərəb Konvensiyasında yeni terminologiya irəli sürülməklə, region ölkələrində bu cinayətlərlə mübarizənin hüquqi çərçivəsi müəyyən edilmiş, bu sahədə hüquqi yardımın elementləri öz əksini tapmışdır.

Kibercinayətlərə qarşı mübarizə üzrə regional müqavilələrin əhəmiyyətli hissəsi MDB məkanının payına düşür. İnformasiya kommunikasiya sferasında törədilən cinayətlər bu gün bütün bəşəriyyət həyatına sirayət etmiş, müasir dünyanın siyasi, iqtisadi, müdafiə, ekoloji, sosial və digər sahələrində olduğu kimi, MDB dövlətlərinin də təhlükəsizliyinə təsirsiz ötüşmür. Ona görə də, bu qurum çərçivəsində kompüter informasiyası sahəsində cinayətlərin xəbər verilməsi, aşkarlanması, açılması, təhqiqatının təmin olunması məqsədilə MDB dövlətləri arasında əməkdaşlıq effektiv həyata keçirilir.[68]

Bu qurum daxilində 2001-ci ildə Kompüter informasiyası ilə əlaqədar cinayətlərə qarşı mübarizə üzrə Əməkdaşlıq haqqında Müqavilə, habelə 2002-ci il tarixli Kompüter və kompüterlə əlaqədar cinayətlər haqında Bill və Elektron Məlumatlar haqqında Model Qanunu qeyd olunan sahədə əməkdaşlığın inkişafında əvəzsiz rola malikdir.

Beləliklə, kibercinayətkarlıqla mübarizə sahəsində istər universal, istərsə də regional əməkdaşlığın müasir formaları daim regional istiqamətdən universal istiqamətə doğru inkişaf edərək təkmilləşir. Nəticədə, beynəlxalq əməkdaşlığın bu modelləri, habelə qəbul edilmiş müqavilələr və digər sənədlər dünyanın başqa regionlarında kibercinayətkarlıq sahəsində müvafiq müqavilə bazasının formalaşmasına özünün müsbət təsirini göstərir.

2.2. İkitərəfli müqavilələrdə kibercinayətlərlə mübarizə məsələləri

Müasir beynəlxalq hüquqda kibercinayətlərin qarşısının alınması, istintaqı, hüquqi yardım, habelə informasiya mübadiləsi baxımından ikitərəfli müqavilələr olduqca mühüm əhəmiyyət kəsb edən beynəlxalq əməkdaşlıq formasıdır. Əslində ikitərəfli əməkdaşlıq dövlətlər arasında hüquqi proseduraların daha da konkretləşməsinə xidmət edir, eyni zamanda kibercinayətlərə qarşı mübarizə üzrə qüvvədə olan beynəlxalq və regional konvensiyaların səmərəli icra və ya tətbiq olunmasına yardımçı funksiya daşıyır. Əgər kibertəhlükəsizlik və kibercinayətlər sahəsində beynəlxalq konvensiyalar bu cinayətə dair ümumi məsələləri (universal anlayışların verilməsi, ümumi prosedur məsələlərini, mühakimə icraatının ümumi prinsiplərini və s.) tənzim edirsə, ikitərəfli müqavilələr isə kibercinayətlərlə mübarizənin konkret elementlərini (qarşılıqlı hüquqi yardım, texniki yardım, qarşılıqlı informasiya mübadiləsi, kibercinayət törətməkdə şübhəli şəxslərin ekstradisiyası, kibercinayətkarların verilməsi və s.) məsələlər üzrə xüsusi rol oynayır.

Kibercinayətlərə qarşı əməkdaşlıq üzrə konkret ikitərəfli müqavilələr müasir beynəlxalq hüquqda çox az saydadır. Bunun iki mühüm səbəbi var: birincisi, bu cinayət əmələri beynəlxalq əməkdaşlıq müstəvisində innovativ xarakter daşıyır və bununla əlaqədar ikitərəfli müqavilə münasibətləri yeni yaranmaqda olan davamlı proses kimi səciyyələnir. İkincisi, bu sahədə mövcud ikitərəfli münasibətlər yalnız ümumi hüquqi yardım və iki dövlət arasında bağlanan əməkdaşlıq memorandumlarının tərkib hissəsi olaraq formalaşmaqdadır. Ona görə də, bu istiqamətdə ikitərəfli müqavilə bazası günümüzün reallıqları baxımından daha çox dəyişən texnoloji yeniliklərə münasibətdə günbəgün təzələnir.

Məzmununu kibercinayətlər üzrə əməkdaşlıq və qarşılıqlı münasibətlər təşkil edən ikitərəfli müqavilələri şərti olaraq aşağıdakı qruplara ayırmaq olar:

Cinayət işləri üzrə hüquqi yardım haqqında ikitərəfli müqavilələr. Bu müqavilələrin ayrıca müddəaları kibercinayətlərə dair qarşılıqlı yardıma, o cümlədən texniki yardım və digər qarışlıqlı anlaşma, kömək və s. hərəkətlər tələb edən məsələləri əhatə edir. Misal olaraq, Azərbaycan Respublikası ilə Hindistan Respublikası arasında cinayət işləri üzrə qarşılıqlı hüquqi yardım haqqında Nyu Dehli şəhərində 04 aprel 2013-cü il tarixdə imzalanmış Müqaviləni, Azərbaycan Respublikası və Birləşmiş Ərəb Əmirlikləri arasında cinayət işləri üzrə qarşılıqlı hüquqi yardım haqqında Əbu-Dabi şəhərində 20 noyabr 2006-cı il tarixində imzalanmış Müqaviləni göstərmək olar.

Ekstradisiya, təslimetmə və məhkumların verilməsi ilə bağlı ikitərəfli müqavilələr. Bu müqavilələrdə isə daha çox iki ölkənin cinayət axtarış, istintaq və cinayət mühakimə orqanları, habelə hökmün icrasını həyata keçirən orqanlar arasında kibercinayət törətməkdə şübhəli olan şəxslərin ekstradisiyası və bu cinayətlərə görə məhkum olunmuş şəxslərin verilməsi üzrə mövcud olan əlaqələr öz əksini tapır. Buna misal olaraq, Azərbaycan Respublikası və Birləşmiş Ərəb Əmirlikləri arasında ekstradisiya haqqında Abu-Dabi şəhərində imzalanmış 20 noyabr 2006-cı il tarixli Müqaviləni, Azərbaycan Respublikası və Cin Xalq Respublikası arasında Təslimetmə haqqında Pekin şəhərində 17 mart 2005-ci ildə imzalanmış Müqaviləni, Azərbaycan Respublikası və Litva Respublikası arasında azadlıqdan məhkum olunmuş şəxslərin cəzanın qalan hissəsinin çəkilməsi üçün verilməsi haqqında Vilnüs şəhərində imzalanmış 23 oktyabr 2001-ci il tarixli Müqaviləni[69] göstərmək olar.

İki dövlət arasında dostluq və əməkdaşlıq haqqında memorandumlar. Bu xüsusdan olan sənədlərdə də iki dövlət arasında münasibətlərin daha yüksək səviyyədə inkişafına nail olmaq üçün kibercinayətlər üzrə öz qanunvericilikləri nöqteyi-nəzərindən çıxış edərək, bu sahədə geniş informasiya mübadiləsi, hər iki tərəfin qeyd olunan sahədə elmi-praktiki əməkdaşlığı məsələlərini özündə ehtiva edir. Məsələn, Azərbaycan Respublikası Ədliyyə Nazirliyi və Slovakiya Respublikası Ədliyyə Nazirliyi arasında 12 may 2009-cu il tarixdə imzalanmış Əməkdaşlıq haqqında Memorandumun 1-ci maddəsində qeyd olunur: "Tərəflər aşağıdakı sahələr üzrə əməkdaşlığı, məlumat və təcrübə mübadiləsini dəstəkləyəcəklər:

---

[68] Борьба с киберпреступлениями. http://www.cis.minsk.by/page.php?id=6636

[69] Bax: Azərbaycan Respublikasının hüquqi yardım sahəsində ikitərəfli beynəlxalq müqavilələrinin toplusu. Bakı-2014. S. -294.

a) daxili qanunvericilik və hüquqi xarakterli məlumatlar;
b) məhkəmə sisteminin idarəetməsi;
c) elektron ədliyyə və s.

”Eyni zamanda, həmin sənədin 2-ci maddəsində yuxarıda göstərilən sahələr üzrə əməkdaşlığın həyata keçirilməsi məqsədilə Tərəflərin normativ aktlar, hüquqi sənəd və rəylərlə bağlı mübadilə aparacağı, birgə seminar və məsləhətləşmələr təşkil edəcəkləri ilə bağlı müddəalar vardır.[70] Göründüyü kimi, son dövrlər elektron ədliyyə, o cümlədən kibercinayətlər üzrə əməkdaşlıq məsələləri ölkəmizin bağladığı müqavilələrin predmetini təşkil edir.

Məzmununu ayrıca kibercinayətlər üzrə əməkdaşlıq məsələləri təşkil edən xüsusi müqavilələr. Ölkəmizlə bağlanmış müqavilə və sazişlərin əksəriyyətinin analizindən görünür ki, elektron ədliyyə, o cümlədən kibercinayətlər üzrə əməkdaşlıq məsələləri bu müqavilələrdə çox az sayda təsadüf edir. Eyni zamanda Azərbaycanın müqavilə praktikasında xüsusi olaraq kibercinayətlərlə mübarizəyə həsr olunmuş ayrıca ikitərəfli sazişə rast gəlinmir.

Ümumiyyətlə, ikitərəfli müqavilələr özündə bir sıra geniş məsələləri tənzim etdiyindən, onların növündən asılı olaraq, həmin müqavilələrdə baxılan məsələlərin müəyyən konkretləşmə səviyyəsinə nail olunur. Eyni zamanda istənilən belə ikitərəfli müqavilənin məzmununa informasiya-kommunikasiya cinayətlərinə, kompüter sahəsində hüquqazidd əməllərə qarşı mübarizənin və əməkdaşlığın elementlərini daxil etmək və ya ayrıca xüsusi müqavilə bağlamaq mümkündür. Bu mənada hüquqşünas alim V.P.Talimoncik qeyd edir ki, məsələn, əgər informasiya sahəsində əməkdaşlıq haqqında müqavilələr kifayət qədər ümumi xarakter daşıyırsa və müqavilənin reallaşma mexanizmi göstərilmədən dövlətin əsas öhdəliklərindən çıxış edirsə, o zaman bu sahəyə aid ayrıca müqavilələrdə konkret qaydalar, müqavilənin həyata keçirilməsi mexanizmləri və onun müddəalarına riayət edilməsinə nəzarət üzrə müddəalar müəyyən edilə bilər.[71]

Bütövlükdə qeyd olunmalıdır ki, son illər bağlanmış ikitərəfli müqavilələrdə informasiya texnologiyalarından istifadə və bununla bağlı hər hansı hüquqazidd kiber hərəkət və hərəkətsizliklə müşayiət edilə biləcək əməllərin baş verməsi riski gözlənilən olduğu üçün belə müddəaların həmin sənəddə əks olunması məqsədəmüvafiq hesab edilir.

Ümumiyyətlə, son dövrlər ölkəmizin iqtisadi inkişaf səviyyəsinin regionda və bütün dünyada artım tendensiyasını, habelə iqtisadi yeniliklərə İKT sahəsində innovativ xarakterli müasir texnologiyaların sürətli tətbiqini nəzərə alsaq, Azərbaycan Respublikasının digər dövlətlərlə bağladığı iqtisadi əməkdaşlıq haqqında müqavilələrin məzmununda da informasiya sistemlərinin mühafizəsi, kompüter və informasiya cinayətləri riskini nəzərdə tutan müddəalara rast gəlmək mümkündür. Məsələn, Azərbaycan Respublikası və Rusiya Federasiyası arasında 2002-2010-cu illəri əhatə etmiş uzunmüddətli iqtisadi əməkdaşlıq haqqında Müqavilədə istehlak mallarının və xidmətlərin bazar vəziyyətini əks etdirən, habelə ikitərəfli ticarət əlaqələri, gömrük statistikası sahəsində İKT ilə bağlı qarşılıqlı fəaliyyətin genişləndirilməsi və metodologiyası üzrə razılaşdırılmış tədbirlər, birgə informasiya sistemlərinin yaradılması, mühafizəsi və fəaliyyəti üzrə əməkdaşlığa xüsusi diqqət yetirilmişdir.

Göründüyü kimi, bu müqavilədə əsas istiqamətlərdən biri olaraq elektron ticarət, elektron gömrük münasibətləri, İKT və informasiyalaşdırma, habelə informasiya sistemlərinin yaradılması və mühafizəsi məsələlərinə xüsusi əhəmiyyət verilmişdir. Çünki bu gün iqtisadi inkişafla informasiya təhlükəsizliyi xüsusi bir harmoniya təşkil edir. Bu mənada Lozanna Universitetinin professoru Solang Gernauti-Helie haqlı olaraq qeyd edir ki, informasiya təhlükəsizliyi regionların iqtisadi inkişafı üçün aparıcı qüvvə təşkil edir və bu inkişaf İKT infrastrukturu ilə eyni zamanda həyata keçirilməlidir. İnformasiya texnologiyası xidmətlərinin inkişafından irəli gələn faydalar İKT infrastrukturunun, lazımi təhlükəsizlik tədbirlərinin, hüquqi və tənzimləyici çərçivələri müşayiət edən inkişafdan asılıdır.[72] Ona görə də, iqtisadi əməkdaşlıq haqında müqavilələrdə də kibertəhlükəsizlik və İKT sahəsində hüquqazidd əməllərin qarşısının alınması üzrə tədbirlərin yer alması müasir dövrün tələbi kimi çıxış edir.

Yüksək texnologiyalar sahəsində cinayətkarlıqla mübarizədə ikitərəfli əməkdaşlıq əsasən ümumi xarakterli cinayətkarlıqla mübarizə üzrə hökumətlər arası müqavilələr vasitəsilə realizə olunur.

Xüsusi vurğulamaq lazımdır ki, müasir beynəlxalq hüquq mütəxəssisləri kibercinayətlərlə mübarizə sahəsində əməkdaşlığın ikitərəfli müqavilə aspektlərinə yanaşmada birmənalı mövqedən çıxış etmirlər. Bütövlükdə bu sahəyə dair çoxtərəfli müqavilələrə üstünlük verildiyindən ikitərəfli müqavilələr kifayət qədər effektiv təqdim olunmur. Beynəlxalq cinayət hüququ üzrə rusiyalı alim N.İ.Kostenko belə müqavilələrin üstün və çatışmayan cəhətlərinə aydınlıq gətirərək hesab edir ki, ikitərəfli müqavilələrin üstünlüyü ondan ibarətdir ki, onların iştirakçı dövlətlərin müəyyən tələblərinə uyğunlaşdırmaq, konkret olaraq iki dövlətin xüsusi maraqlarına asan adaptasiya etmək mümkündür. Belə müqavilələrin çatışmayan cəhətlərinə isə, o danışıqlar prosesinin özünü, razılaşdırılma və vahid mövqeyin itirilməsi ilə əlaqədar qaçılmaz vəziyyətlərin olması ilə bağlı oxşar müqavilələrin sayının artmasını aid edir. Bu mənada N.İ.Kostenko haqlı olaraq amerikalı hüquqşünas alim Bassiunidən iqtibas gətirərək, qeyd edir ki, əgər hər bir üzv dövlət digər üzv dövlətlə ikitərəfli müqavilə bağlayarsa, o zaman bu dövlətlər arasında nəticə etibarilə 20 mindən çox müqavilə bağlanmış olacaq. Təkcə

---

[70] Azərbaycan Respublikası Ədliyyə Nazirliyi və Slovakiya Respublikası Ədliyyə Nazirliyi arasında əməkdaşlıq haqqında Memorandum, http://justice.gov.az/view_agr.php?id=23

[71] Талимончик, В. П. Роль двусторонних договоров, заключенных Российской Федерацией, в международном информационном обмене //Правоведение. -2006. - № 5. - С. 105 – 120

[72] Stein Schjolberg and Solange Ghernaouti-Helie.A Global Protocol on Cybersecurity and Cybercrime.Oslo-Cybercrimedata 2009. p.6. - 83.

ABŞ digər dövlətlərlə 110-dan müqavilə bağlamalı olacaq.[73] Elə bu səbəbdən də, beynəlxalq hüquqda ikitərəfli müqavilələrin say çoxluğu müasir qanunvericililklərin inteqrasiyası baxımından əlverişli vəziyyət hesab olunmur.

Bu xüsusilə Azərbaycanda da milli qanunvericilik sisteminin formalaşmasında mühüm əhəmiyyət kəsb edir. Ölkəmizdə informasiya cəmiyyətinin qurulmasına və ümumilikdə dövlətimizin inkişafına xidmət edən "Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafı üzrə 2005-2008-ci illər üçün Dövlət Proqramı" ("Elektron Azərbaycan"), "Elektron imza və elektron sənəd haqqında", "Elektron ticarət haqqında", "Telekommunikasiya haqqında" qanunlar qəbul edilmişdir və bu istiqamətlərdə bir sıra layihələr həyata keçirilir. Bu qəbildən olan qanunların mövcudluğu ölkədə İKT-nin inkişafında böyük əhəmiyyət kəsb edir. Bununla yanaşı, İKT-nin müfəssəl elmi-hüquqi tədqiqatlar tələb etdiyini qeyd edən hüquq elmləri namizədi R.Əzizov hesab edir ki, hüquqi tənzimləmə sadəcə ayrı-ayrı qanunların qəbul edilməsini deyil, elə bir sistemli kompleks qanunvericiliyin mövcudluğunu tələb edir ki, bu zamanda, məsələn, iqtisadi hüquq münasibətlərini tənzimləyən normalar hüquqların qorunmasına və kibercinayətkarlığın qarşısının alınmasına yönəlmiş preventiv normalar ilə ziddiyyət təşkil etməməlidir. "Bu sahənin inkişafı üçün ilk növbədə informasiya-kommunikasiya hüququnun (e-law) formalaşması lazımdır. Bu sahədə ölkəmizdə hüquqi ekspertlərin azlığı özünü göstərir, elmi seminarlar isə demək olar ki, çox az keçirilir".[74]

Bundan başqa beynəlxalq əməkdaşlıq forması kimi ölkəmizin imzaladığı ümumi xarakterli cinayətkarlıqla mübarizə üzrə son hökumətlər arası ikitərəfli müqavilələrə aşağıdakıları misal göstərə bilərik: 12 may 2009-cu il tarixdə imzalanmış Azərbaycan Respublikası Ədliyyə Nazirliyi və Slovakiya Respublikası Ədliyyə Nazirliyi arasında əməkdaşlıq haqqında Memorandum, 13 avqust 2007-ci il tarixli Azərbaycan Respublikası Ədliyyə Nazirliyi və Tacikistan Respublikası Ədliyyə Nazirliyi arasında əməkdaşlıq haqqında Anlaşma Memorandum, 15 may 2007-ci il tarixli Azərbaycan Respublikası Ədliyyə Nazirliyi və Bolqarıstan Respublikasının Ədliyyə Nazirliyi arasında əməkdaşlıq haqqında Saziş, 7 may 2007-ci il tarixli Azərbaycan Respublikası Ədliyyə Nazirliyi və Misir Ərəb Respublikasının Ədliyyə Nazirliyi arasında əməkdaşlıq haqqında Saziş və s. Qeyd olunmalıdır ki, son dövrlər bağlanmış bu ikitərəfli müqavilələrdə hüquqi əməkdaşlığın, o cümlədən kibercinayətkarlıqla bağlı ikitərəfli münasibətlərin baza prinsipləri müəyyən olunmuşdur.

Eyni zamanda, kibercinayətkarlıqla bağlı ölkəmizdə ən çox istifadə olunan əməkdaşlıq formalarına hüquqi informasiya mübadiləsi sahəsində bağlanan müqavilələrdə rast gəlmək mümkündür. Hüquqi informasiya mübadiləsi haqqında ölkəmizdə qüvvədə olan sazişlər isə aşağıdakılardır: 22 mart 2000-ci il tarixli Azərbaycan Respublikası hökuməti ilə Gürcüstan hökuməti arasında hüquqi informasiya mübadiləsi haqqında Saziş, 10 iyun 1997-ci il tarixli Azərbaycan Respublikası hökuməti ilə Qazaxıstan Respublikası hökuməti arasında hüquqi informasiya mübadiləsi haqqında Saziş, 22 iyun 1994-cü il tarixli Azərbaycan Respublikası Hökuməti ilə Rusiya Federasiyası Hökuməti arasında hüquqi informasiya mübadiləsi haqqında Saziş və s.

Yuxarıda sadaladığımız müqavilələrin kontent analizi göstərir ki, bu müqavilələrdə əsasən yeni, müasir çağırışlara istinad olunaraq, yeni əməkdaşlıq modellərinə, o cümlədən İKT sahəsində innovasiyalara daha çox önəm verilir. Məsələn, Azərbaycan Respublikası Ədliyyə Nazirliyi və Tacikistan Respublikası Ədliyyə Nazirliyi arasında əməkdaşlıq haqqında13 avqust 2007-ci il tarixli Sazişdə hüquqi informasiya sistemlərinin inkişafı və Tərəflərin fəaliyyəti barədə informasiya mübadiləsinin aparılması barədə ümumi müddəanı daxil etməklə (Maddə 2) iki ölkə arasında kibertəhlükəsizlik məsələləri ilə bağlı fəaliyyət də daxil olmaqla hüquq-mühafizə orqanlarının bu istiqamətdə qarşılıqlı əməkdaşlığı təşviq olunur.[75]

Eyni zamanda Azərbaycan Respublikasının Dövlət Təhlükəsizlik Xidmətinin səlahiyyətinə aid olduğunu nəzərə alaraq bu sahədə qurum tərəfindən də məqsədyönlü işlər görülür və beynəlxalq əməkdaşlığın inkişafı baxımından irəliyə doru addımlar atılır. Mütəşəkkil transmilli cinayətkarlıq bütün dünya ölkələri, o cümlədən əlverişli geostrateji mövqeyə malik, dinamik inkişaf edən Azərbaycan üçün narahatlıq doğurur. Bu məqsədlə Dövlət Təhlükəsizlik Xidməti tərəfindən narkotik vasitələrin qaçaqmalçılığı, qeyri-leqal miqrasiya, insan ticarəti, "çirkli pulların yuyulması", kibercinayətlər və mütəşəkkil cinayətkarlıqla bağlı digər sahələrdə mübarizə ardıcıl davam etdirilir.

Müqayisə üçün kibercinayətkarlıqla bağlı digər ölkələrin ikitərəfli müqavilə hüquqi praktikasına diqqət yetirilməsi də faydalı olardı. Xarici ölkələrin müqavilə təcrübəsində də əsasən hökumətlər arası ümumi xarakterli müqavilələrə üstünlük verilir.

Rusiyanın kibercinayətlərə qarşı mübarizə üzrə ikitərəfli müqavilə praktikasına nəzər yetirən hüquq elmləri doktoru R.Z.Abdraşitova qeyd edir ki, bu müqavilələr cinayət işləri üzrə çoxtərəfli qarşılıqlı hüquqi yardımın alınması və göstərilməsinə tam mənada imkan vermir. Birincisi, onların əksər hissəsi hüquqi yardımın əhatə dairəsinin genişlənmə perspektivini təmin etmir. Bundan başqa, ikitərəfli müqavilələr üçün cinayət prosesi çərçivəsində, o cümlədən kompüter cinayətlərinin araşdırılması zamanı qarşılıqlı fəaliyyət haqqında, habelə, prosessual hərəkətlərin yerinə yetirilməsi zamanı video əlaqə vasitələrinin istifadəsi üzrə beynəlxalq əməkdaşlığın yeni istiqamətləri haqqında normanın onlarda olmaması xarakterikdir.[76]

Qeyd edək ki, kibercinayətkarlıqla mübarizə sahəsində ikitərəfli əməkdaşlıq formalarının inkişafında ayrı-ayrı dövlətlərin də xüsusi rolu vardır. Kibercinayətkarlıq sahəsində beynəlxalq əməkdaşlığın möhkəmləndirilməsi

---

73 Костенко, Н.И. Правовые механизмы международного сотрудничества в правоохранительной сфере / Н.И. Костенко // Право и политика. - 2005. - № 8. //КонсультантПлюс: Версия Проф. Технология 3000 / ООО "ЮрСпектр". - М., 2009.

74 Əzizov R. Azərbaycanda elektron dövlətin perspektivləri. Azərbaycan qəzeti.-2009.-7 fevral.-S.9. 124

75 Azərbaycan Respublikası Ədliyyə Nazirliyi və Tacikistan Respublikası Ədliyyə Nazirliyi arasında əməkdaşlıq haqqında Saziş, http://justice.gov.az/view_agr.php?id=22

76 Абдрашитова, Р.З. Международное сотрудничество в сфере уголовного судопроизводства: проблемы становления и дальнейшего развития / Р.З.Абдрашитова // Право и политика. - 2005. - № 3. // КонсультантПлюс: Версия Проф. Технология 3000 / ООО "ЮрСпектр". - М., 2009.

üzrə Rusiya Federasiyası əsas təşəbbüskar region dövləti kimi çıxış edir. Məhz bu dövlətin nümayəndələri kibercinayətkarlıq üzrə milli dövlətlərin səylərinin konsolidasiyasını zəruri sayaraq, dövlətlərarası əməkdaşlıq modellərinə, o cümlədən beynəlxalq müqavilələrə üstünlük verilməsini vacib hesab edirlər. Kibercinayətkarlıq və kiberterrorizmlə mübarizə üzrə Beynəlxalq praktiki konfransda Rusiya Dövlət Dumasının Təhlükəsizlik məsələləri Komitəsinin sədri V.A.Vasilieva öz məruzəsində qeyd edir ki, kiberməkana münasibətdə ərazi yurisdiksiyası haqqında ənənəvi təsəvvürlər, inzibati sərhədlər ümumilikdə öz mahiyyətini itirir, milli qanunvericiliyin rolu aşağı düşür, dövlətlərarası (beynəlxalq) tənzimləmə alətləri birinci plana keçir.[77]

Son vaxtlar kibercinayətkarlıq sahəsində beynəlxalq konfranslar və beynəlxalq forumlar daha mühüm alət qismində çıxış etməkdədir. Belə ki, RF İctimai Palatasının patronajlığı ilə Rusiya təhlükəsiz internet mərkəzi və İnternet texnologiyaları üzrə regional ictimai mərkəzin təşkilatçılığı ilə 2012-ci ildə Beynəlxalq təhlükəsiz internet günü ilə bağlı ənənəvi Forumun 5-ci sessiyası keçirilmiş, forumun işində kibertəhlükəsizlik məsələlərini diqqət mərkəzində saxlayan müxtəlif dövlətlərin internet industriyasının, ictimai və qeyri-kommersiya qurumlarının aparıcı şəxsləri aktiv iştirak etmişlər.[78] Göründüyü kimi, ayrı-ayrı dövlətlərin təşəbbüsü ilə keçirilən beynəlxalq forumlar, konfranslar beynəlxalq əməkdaşlıq forması kimi mühüm rola malik olmaqla, sonrakı inkişafa – ikitərəfli, regional və universal xarakterli əməkdaşlıq formalarına xüsusi stimul verir.

Beləliklə yekun olaraq kibercinayətkarlıqla mübarizə sahəsində beynəlxalq əməkdaşlığın əsas istiqamət və formalarının analizi üzrə aşağıdakı nəticələri mümkün hesab edirik.

- İnternetin dünya birliyi üçün yaratdığı faydalarla yanaşı, eyni zamanda şəbəkə və kompüter informasiyası üzrə hüquqazidd hərəkətlər – kibercinayətlərin qarşısının alınması və cəzalandırılması üzrə universal, regional və ikitərəfli səviyyələrdə beynəlxalq əməkdaşlıq qloballaşma dövrünün tələbi kimi çıxış edir;
- Bu beynəlxalq əməkdaşlığın hüquqi fəlsəfi ondan ibarətdir ki, qeyd olunan məsələ daha çox bəşəriyyətin indiki və gələcək təhlükələrdən qorunması və təhlükəsizliyi baxımından vacibdir;
- Aparılan təhlillər göstərir ki, kiberməkanda təhlükəsizliyin təmin olunması və cinayətlərin qarşısının alınması üçün bu gün daha çox regional əməkdaşlığa üstünlük verilir, bu istiqamət üzrə müqavilə mexanizmləri ən çox Avropa regionunda inkişaf edərək genişlənməyə və bundan sonra universal mahiyyət kəsb edir;
- Müasir beynəlxalq hüquqda kibercinayətlərlə mübarizə üzrə əməkdaşlığın yeni və unikal forması kimi, bu sahədə müvafiq ixtisaslaşmış məhkəmə qurumunun və ya ad hoc tribunalların yaradılması məsələsi daha da aktualdır.
- Qloballaşma dövrünün tələblərinə adekvat olaraq, Azərbaycanda azad internetin inkişafı və iqtisadiyyatın yüksək inkişaf dinamikası kibercinayətlərlə bağlı mübarizəyə də rəvac vermiş, Ölkə Prezidentinin, Dövlət Təhlükəsizlik Xidmətinin, Ədliyyə Nazirliyinin təşəbbüsü ilə bu sahədə yeni müqavilələrə və digər əməkdaşlıq formalarına üstünlük verilməklə ikitərəfli və çoxtərəfli əməkdaşlıq münasibətləri inkişaf etdirilir.
- Yeni iqtisadi amillər, qlobal transmilli münasibətlər sistemi yeni cinayətlərin – kibercinayətlərin qarşısının alınması üzrə beynəlxalq əməkdaşlığın da yeni meyllərini şərtləndirir, kiber məkanda daha yetkin və effektiv tənzimlənmə məqsədilə bütün beynəlxalq birlik üçün ümum məcburi qaydaların və hamı üçün ümumi xarakter daşıyan prinsiplərin işlənib hazırlanaraq formalaşdırılması, habelə bu istiqamətdə konseptual beynəlxalq hüquqi yanaşmanın ortaya qoyulması lazımdır.
- Kibercinayətlərlə daha mükəmməl şəkildə beynəlxalq mübarizə aparılması məqsədilə "vahid yanaşma"nın ortaya qoyulması zəruridir ki, bunun da iki əsas şərti var: kiberməkanda baş verən konkret cinayət tərkiblərinin ümumiləşdirilmiş siyahısının müəyyən edilməsi və beynəlxalq hüquqi unifikasiyası; bu cinayət tərkiblərinin hər birinin dövlətlərin milli cinayət qanunvericiliklərinə inkorporasiyası və ya transformasiyası.
- BMT çərçivəsində cinayətkarlıqla mübarizə üzrə universal müqavilənin qəbul edilməsində problemlərin mövcudluğuna baxmayaraq, bu qurumun missiyası çərçivəsində aparılan müzakirələr kontekstində qətiyyətlə söyləmək mümkündür ki, məhz bu təşkilatın həyata keçirdiyi fəaliyyətin nəticəsində regional müqavilələrin rüşeymi formalaşmış və müasir səviyyəyə çatmışdır. BMT-nin İqtisadi və Sosial Şurası, eyni zamanda, Cinayətlərin xəbər verilməsi və cinayət hüquqi mühakimə üzrə BMT Komissiyasının spesifik səyləri nəticəsində regional, xüsusilə AŞ çərçivəsində qəbul olunmuş Budapeşt Konvensiyası beynəlxalq hüquqi dövriyyəyə çıxmışdır.
- Ölkəmizlə bağlanmış müqavilə və sazişlərin əksəriyyətinin analizindən görünür ki, elektron ədliyyə, o cümlədən kibercinayətlər üzrə əməkdaşlıq məsələləri bu müqavilələrdə çox az sayda təsadüf edir. Ona görə də tövsiyə olunur ki, Azərbaycanın müqavilə praktikasında xüsusi olaraq kibercinayətlərlə mübarizəyə həsr olunmuş ayrıca ikitərəfli sazişlərə üstünlük verilməsi ölkəmizin bu sahədə beynəlxalq əməkdaşlığına mühüm töhfə ola bilər.
- Yüksək texnologiyalar sahəsində cinayətkarlıqla mübarizədə ikitərəfli əməkdaşlıq əsasən ümumi xarakterli cinayətkarlıqla mübarizə üzrə hökumətlər arası müqavilələr vasitəsilə realizə olunur.
- Kibercinayətkarlıqla mübarizə üzrə ikitərəfli müqavilələr özündə bir sıra geniş məsələləri tənzim etdiyindən, həmin müqavilələrin məzmununa informasiya-kommunikasiya cinayətlərinə, kompüter sahəsində hüquqazidd əməllərə qarşı mübarizənin və əməkdaşlığın elementlərini daxil etmək və ya ayrıca xüsusi müqavilə bağlamaq mümkündür ki, bu da nəticədə konkretləşməyə səbəb ola bilər. Son illər bağlanmış

[77] Васильев В.А. Проблемы развития законодательства в сфере борьбы с киберпреступностью // Материалы Международной практической конференции по борьбе с киберпреступностью и кибертерроризмом. Москва,19 - 20 апреля, 2006 г.

[78] Повышев Владислав. Борьба с киберпреступностью и кибертерроризмом. Томский государственный университет.http://tmun.utmn.ru/wp-content/uploads/SPChKiber.pdf

ikitərəfli müqavilələrdə informasiya texnologiyalarından istifadə və bununla bağlı hər hansı hüquqazidd kiber hərəkət və hərəkətsizliklə müşayiət oluna biləcək əməllərin baş verməsi riski gözlənilən olduğu üçün belə müddəaların həmin sənəddə əks olunması məqsədəmüvafiq hesab olunur.

- Kibercinayətlərə qarşı mübarizə üzrə ikitərəfli müqavilə praktikasının təhlili sübut edir ki, bu müqavilələr cinayət işləri üzrə çoxtərəfli qarşılıqlı hüquqi yardımın alınması və göstərilməsinə iki səbəbdən: müqavilənin hüquqi yardımın əhatə dairəsinin genişlənmə perspektivini təmin etməməsindın və kompüter cinayətlərinin araşdırılması zamanı beynəlxalq əməkdaşlığın yeni istiqamətləri haqqında normanın onlarda olmaması səbəbindən tam mənada imkan vermir.

III FƏSİL
AZƏRBAYCAN RESPUBLİKASININ MİLLİ QANUNVERİCİLİYİNDƏ KİBERCİNYƏTLƏR VƏ BEYNƏLXALQ HÜQUQ

3.1. Kibercinayətkarlıqla mübarizə üzrə beynəlxalq hüquq normalarının Azərbaycan Respublikasının milli qanunvericiliyinə implementasiya məsələləri

3.2. Azərbaycan Respublikasının Cinayət Məcəlləsində kibercinayətlərin anlayışı və tərkibi

3.3. Azərbaycan Respublikasında kibercinayətkarlıqla mübarizənin təşkilati-hüquqi əsasları

3.4. Azərbaycan milli qanunvericiliyində kibercinayətlərə görə məsuliyyət məsələləri

3.1. Kibercinayətkarlıqla mübarizə üzrə beynəlxalq hüquq normalarının Azərbaycan Respublikasının milli qanunvericiliyinə implementasiya məsələləri

Artıq qloballaşma və informasiya dövrünün tələblərinə müvafiq olaraq milli qanunvericilik sistemləri də əhəmiyyətli dərəcədə modern dəyişikliklərə məruz qalmaqdadır. Bu gün dünyanın əksər ölkələri surətlə inkişaf edən müasir İKT sistemlərinə nüfuz etdikcə milli qanunvericiliklərdə də müasir beynəlxalq hüquq norma və prinsiplərinin tələblərinə uyğun rasional dəyişiklik və inkişaf müşahidə olunur. Kibercinayətkarlıqla bağlı beynəlxalq hüquq normalarının, xüsusilə Kibercinayətkarlıq haqqında Budapeşt Konvensiyasının ölkədaxili implementasiyası beynəlxalq hüquqda təsbit olunan ümumi qaydalara müvafiq olaraq həyata keçiriləcəkdir. Lakin burada da kibercinayətkalıqla bağlı hüquq normaları, habelə milli qanunvericinin maraqları ilə əlaqədar bəzi spesifik məqamların nəzərə alınması zəruridir.

Amsterdam Virje Universitetinin professoru Henrik Kaspersen Kibercinayətkarlıq haqqında Konvensiyanın implementasiya üsullarına toxunaraq onun aşağıdakı yollarla reallaşdırılmasını qeyd edir: "Əgər Konvensiyanın mətni və mənası ilə ziddiyyət təşkil etmirsə, tərəflər razılaşdırılmış öhdəçilikləri hüdudlarını aşa bilərlər; tərəflər tətbiq etmə üçün xüsusi deklarasiyaları və xüsusi rezervasiyaları seçə bilər; qanunun mətnində digər seçimlər də təklif edilə bilər və ya konvensiyanın primatının qəbul edilməsi" yolunu seçə bilərlər. Bundan əlavə, müəllif Konvensiyanın implementasiyası ilə əlaqədar digər bir bölgünün aparılmasını məqbul saymışdır. O, maddi və prosessual hüquq normalarının implementasiyasını fərqləndirərək, maddi implementasiyanın kateqoriyalarına virtual təhqir və böhtan, kompüter ilə əlaqədar, kontentlə və intellektual mülkiyyətlə bağlı hüquqazidd əməlləri, prosessual implementasiyaya isə qanunvericiliyin hamonizasiyası və eyniləşdirilməsini aid edir.[79] Beynəlxalq hüquq ədəbiyyatlarında qeyd olunduğu kimi, daxili qanunverici beynəlxalq müqavilə öhdəliklərinin icrası naminə daxili hüquq sistemi üçün daha səmərəli və sosial əhəmiyyətli hüquqi göstərişin qəbulundan ötrü *özünəməxsus manevr etmək sərbəstliyindən* istifadə edə bilər.[80]

Bu gün Azərbaycan Respublikasında da kibercinayətkarlığa qarşı mübarizə üzrə beynəlxalq hüquq normalarının dövlətdaxili implementasiyası qanunvericilik qaydasında və bütövlükdə hüquq sistemi üzrə həyata keçirilir, eyni zamanda, qeyd olunan sahədə təşkilati-hüquqi tədbirlər görülür. Ölkəmizdə hüquq normalarının harmonizasiyası prosesi həm maddi hüquq sahələrinə, eyni zamanda prosessual qanunvericiliyə aiddir.

Kibercinayətkarlığın qarşısının alınması, bu sahədə profilaktik, habelə digər təşkilatı-hüquqi mexanizmlərin müəyyən olunması istiqamətində ölkəmizdə kompleks işlər görülərək, bu cinayətlə mübarizə tədbirlərini əhatə edən normativ-hüquqi aktlar, Dövlət Proqramları, xüsusi layihələr qəbul edilməklə və icra olunmaqla digər sahəvi qanunvericilik normalarının inkişafına dövlətimiz tərəfindən əlavə dəstək verilir, müvafiq qurumlar tərəfindən maarifləndirici fəaliyyət həyata keçirilir.

Müasir dövrdə kompüter sistemləri, bütün dünyanı vahid informasiya məkanında birləşdirən internet şəbəkəsi, virtual kitabxanalar, elektron jurnallar və bu qəbildən olan digər vasitələr Azərbaycanda cəmiyyət həyatının ayrılmaz hissəsinə çevrilib. Lakin bu informasiya axınından və sosial şəbəkələrdən heç də hamı mütərəqqi məqsədlər üçün faydalanmır, bundan bəzən cinayətkar mənafe naminə istifadə olunur, ictimai qaydalara zərər vurulur və cəmiyyətin sosial-mənəvi əsasları zərbə altında qalır. Bəzən hətta ölkəmizin milli təhlükəsizliyi, dövlətimizin ərazi bütövlüyü cinayətkar təhdid altında qalır. Bu mənada R.K.Məmmədov haqlı olaraq vurğulayır ki, dünyada cinayətkarlığın vəziyyətinin təhlili sübut edir ki, o görünməmiş səviyyəyə çatmış və dövlətlərin təhlükəsizliyi üçün real hədəyə çevrilmişdir.[81]

Buna görə də dövlət tərəfindən kibercinayətkarlıqla mübarizə məsələlərinin respublikamızın ayrı-ayrı sahəvi qanunvericiliyinə daxil edilməsi zərurəti yaranmışdır. Daha doğrusu, bu gün kibercinayətlər bütövlükdə qlobal dünya üçün real təhlükə olduğundan və Azərbaycan Respublikası da dünya birliyinin müstəqil və ayrılmaz tərkib hissəsi olaraq bu məkana sıx inteqrasiya etdiyi üçün mili hüququn bütün sahələri üzrə beynəlxalq hüquq normalarının implementasiyası dövlətimizin prioritet vəzifələrindən birini təşkil edir.

---

[79] Implementation of the Cybercrime Convention 2001. Prof. Henrik Kaspersen, Tbilisi, 29 September 2009. http://www.coe.int

[80] Huseynöv L.H. Beynəlxalq hüquq. Dərslik. Bakı, 2012, s.61; Məmmədov R.K. Beynəlxalq cinayət hüququ və Azərbaycan Respublikasının cinayət qanunvericiliyi. Monoqrafiya. Bakı, 2012, s. 52

[81] Məmmədov R.K. Beynəlxalq cinayət hüququ və Azərbaycan Respublikasının cinayət qanunvericiliyi, Bakı-2012, s.11

Qeyd olunmalıdır ki, ölkəmiz digər sahələrdə olduğu kimi, cinayətkarlıqla mübarizə, o cümlədən kibercinayətkarlığa qarşı mübarizə sahəsində də siyasi iradə nümayiş etdirir. Son dövrlərin İKT-nin sürətli inkişafı beynəlxalq hüquqi əlaqələrin müxtəlif sahələrində, o cümlədən kibercinayətlər üzrə beynəlxalq əməkdaşlığı, bu sahədə normativ hüquqi mübadiləni zərurətə çevirmişdir. Ona görə də ölkəmiz də daxil olmaqla yuxarıda qeyd olunan problemləri nəzərə alaraq, kompüter cinayətkarlığı ilə mübarizə sahəsində dövlətlər öz səylərini birləşdirməyə və bu məsələlərlə bağlı hüquqi müstəvidə BMT, Avropa Şurası, Avropa İttifaqı, ATƏT, MDB və digər beynəlxalq qurumlar çərçivəsində addımlar atmağa başlamışdır. Bu həm qarşılıqlı hüquqi yardım, həm də universal və regional təhlükəsizliyin qorunması və təhdidlərin qarşısının alınması sahələrinə aid edilə bilər.

Bu sahədə maddi və prosessual normaları unifikasiya edən və kibermünasibətləri tənzimləyən ən mühüm sənədlər Avropa Şurası çərçivəsində qəbul edilmişdir. Artıq qeyd etdiyimiz kimi, qurumun 23 noyabr 2001-ci il tarixli Kibercinayətkarlıq haqqında Konvensiyası kiberməkanda baş verən cinayətlər və onlarla mübarizə məsələlərinə həsr olunmuşdur. Bu Konvensiyada beynəlxalq təcrübədə analoqu olmayan bir sıra cinayətlər – kompüter məlumatlarının və sisteminin konfidensiallığı, bütövlüyü və əlverişliliyi əleyhinə cinayətlər, kompüterlə əlaqəli cinayətlər, habelə, məzmununu kompüter informasiyası təşkil edən hüquq pozuntuları, uşaq pornoqrafiyası ilə əlaqəli materiallarla bağlı hüquqazidd əməllər, müəlliflik və əlaqəli hüquqların pozulması ilə bağlı cinayətlər təsbit olmuşdur.

Bundan başqa, Konvensiya kibercinayətkarlıqla mübarizədə əməkdaşlığın prinsiplərini də müəyyən edir. Bunlara aiddir: bir-biri ilə geniş əməkdaşlıq prinsipi, ekstradisiya prinsipi, qarşılıqlı yardımın ümumi prinsipləri, müvafiq beynəlxalq sazişlərin istisna etdiyi hallarda yardım haqqında sorğuların yönləndirilməsi və yerinə yetirilməsi prinsipi, konfidensiallıq və məhdud istifadə prinsipi, müvəqqəti tədbirlərin görülməsi üzrə yardım prinsipi, istintaq xidmətlərinin fəaliyyətlərinə yardım prinsipi.

Kibercinayətkarlıq üzrə prinsiplərin həyata keçirilməsi fikrimizcə müasir dövr üçün daha aktual hüquqi problem olaraq araşdırılmalı və riayət olunmalıdır. Çünki, özünün transmilli mahiyyətinə və nəticələrinin ağırlığına görə bu kateqoriyaya daxil olan əməllərin təhlükəsizliyi heç də digər beynəlxalq və beynəlxalq xarakterli cinayətlərdən geri qalmır. Bu mənada amerikalı hüquqşünas alim M. Keyserin "kibercinayətlər ciddi transmilli komponentə malikdir"[82] fikrinə tamamilə şərik çıxaraq, bu əməlin törədilməsi ilə serverlər vasitəsilə ötürülən məlumatların, virusların və digər zərərli proqramların bir deyil, çoxsaylı dövlətlərin milli maraqları və mənafelərinə toxunmasını qeyd edə bilərik. Ona görə də bu sahədə universal və regional əməkdaşlıq, cinayətlə mübarizənin reallaşdırılma mexanizmlərinin müəyyən olunması mühümdür.

MDB çərçivəsində bu cinayətlə mübarizə məsələləri 2001-ci il tarixli Kompüter informasiyası sferasında cinayətlərlə mübarizədə MDB iştirakçı dövlətlərin əməkdaşlığı haqqında Müqavilə ilə tənzimlənir. Bu sənədə əsasən kompüter informasiyası sahəsində cinayətlərin xəbər verilməsi, qarşısının alınması, istintaqı və s. istiqamətlərdə birgə tədbirlərin həyata keçirilməsi nəzərdə tutulur. Bunda başqa, MDB çərçivəsində 17 fevral 1996-cı il tarixdə qəbul edilən Model Cinayət Məcəlləsində (XII fəsil – "İnformasiya təhlükəsizliyi əleyhinə cinayətlər") kompüter informasiyasına qanunsuz daxil olma, kompüter sabotajı, kompüter informasiyasının modifikasiyası, kompüter informasiyasının qanunsuz ələ keçirilməsi[83] və s. üzv dövlətlərin milli qanunlarına implementasiya məsələlərinə toxunulur. Qeyd olunmalıdır ki, mütəxəssislər MDB ölkələrində mövcud olan kibercinayətkarlıqla mübarizə üzrə təcrübəni əlverişli hesab edirlər.[84]

Əl-Fərabi adına Qazaxıstan Milli Universitetinin professoru Cansaraeva R. E. bir sıra post-sovet məkanı ölkələrinin və MDB dövlətlərinin cinayət qanunvericiliyinin müqayisəli təhlilini apararkən belə nəticəyə gəlir ki, kibercinayətkarlıqla mübarizə üzrə beynəlxalq strategiyasının işlənib hazırlanması və informasiya texnologiyaları, habelə informasiya təhlükəsizliyi sahəsində münasibətlərin cinayət hüquqi tənzimlənməsi üzrə milli qanunvericiliklərin unifikasiyası zəruridir.[85]

Digər dövlətlər kimi, Azərbaycan da kibercinayətkarlıqla bağlı həm universal, həm də regional əməkdaşlıq çərçivəsində beynəlxalq hüquqi normaların milli qanunvericiliyə implementasiyasiyası ilə bağlı zəruri tədbirlər görür.

Kibercinayətkarlıqla mübarizə sahəsində beynəlxalq hüquq normalarının ölkəmizin sahəvi qanunvericiliyinə implementasiyası məsələsi ilk növbədə dövlət başçısının diqqətində olan məsələlərdən birdir. Ölkəmizdə kibertəhlükəsizliyin təmin olunması sahəsində mühüm addımlar atılmış və bu siyasət hazırda ölkə Prezidenti cənab İlham Əliyev tərəfindən uğurla davam etdirilməkdədir. Kibercinayətkalıqla mübarizə üzrə beynəlxalq hüquq normalarının ölkəmizin sahəvi qanunvericiliyinə implementasiyası sahəsində ilk qanunvericilik tədbiri kimi ölkəmizin Kibercinayətkarlıq haqqında Budapeşt Konvensiyasına qoşulmasını qeyd edə bilərik. Bu kibercinayətkarlıqla mübarizə üzrə region dövlətləri içində Azərbaycanın bu sahəyə nə dərəcədə önəm verməsini və bu cinayətə qarşı barışmaz mövqedə dayanması faktını təsdiq edən amildir.

3.2. Azərbaycan Respublikasının Cinayət Məcəlləsində kibercinayətlərin anlayışı və tərkibi

[82] Keyser M. The Council of Europe Convention on Cybercrime. Florida State University Journal of Transnational Law & Policy. Volume 12 Spring 2003 Number 2. P. 289. 343 pp

[83] Модельный уголовный кодекс для государств – участников Содружества Независимых Государств // Межпарламентская Ассамблея государств - участников Содружества независимых государств [Электронный ресурс]. 2004. Режим доступа: http://www.iacis.ru.

[84] Абламейко М. С., Абламейко С. В., Анализ уголовного законодательства стран Таможенного Союза в сфере информационной безопасности. http://elib.bsu.by

[85] Джансараева Р.Е. Борьба с киберпреступлениями: сравнительный анализ законодательства стран СНГ // Криминологический журнал Байкальского государственного университета экономики и права. Иркутск №3(21) Июнь-июль 2012 год.- С.95.

Ölkəmizdə kibertəhlükəsizliyin təmin olunması və kibercinayətkalıqla mübarizə ilə bağlı yuxarıda qeyd etdiyimiz kimi, çoxsaylı normativ-hüquqi aktlar qəbul olunmuşdur ki, onların da əsas məqsədini bu sahəyə aid olan beynəlxalq hüquqi norma və prinsiplərin effektiv dövlətdaxili tətbiqinə nail olunması təşkil edir. Bunların qəbulu nəticəsində isə əksər milli hüquq normalarında, o cümlədən Azərbaycan Respublikasının Cinayət Məcəlləsində müvafiq dəyişikliklər həyata keçirilmişdir.

Beynəlxalq hüquqşünas alim Rahim Məmmədov belə dəyişikliklərin edilməsinin iki üsulunu – resepsiya və transformasiyanı daha məqbul sayır. Müəllif qeyd edir ki, Azərbaycan Respublikasının qüvvədə olan cinayət qanunvericiliyi yalnız Cinayət Məcəlləsindən ibarət olduğundan cinayət hüquqi əhəmiyyətə malik beynəlxalq aktın qüvvəyə minməsi zamanı Məcəllədə dəyişiklik edilməsi əvvəllər nəzərdən keçirilən üsulların ikisi ilə həyata keçirilə bilər: resepsiya, yəni beynəlxalq hüquq aktın müddəalarının Cinayət Məcəlləsinə birbaşa daxil edilməsi; transformasiya, yəni beynəlxalq hüquq aktının qaydalarına uyğun olaraq, Cinayət Məcəlləsinin müddəalarının dəyişdirilməsi.[86]

Qeyd olunmalıdır ki, kibercinayətkarlıqla bağlı beynəlxalq hüquq normalarının Azərbaycan cinayət qanunvericiliyinə implementasiyası zamanı transformasiya təcrübəsinə istinad edilmişdir. Belə ki, ölkə Prezidenti cənab İlham Əliyevin 27 dekabr 2011-ci il tarixli Sərəncamı ilə təsdiq olunmuş Azərbaycan Respublikasında insan hüquq və azadlıqlarının müdafiəsinin səmərəliliyini artırmaq sahəsində Milli Fəaliyyət Proqramının 1.2.4-cu maddəsinə görə informasiya texnologiyalarından istifadə etməklə insan hüquqlarının pozulmasına qarşı mübarizənin səmərəliliyinin artırılması məqsədilə Azərbaycan Respublikası Cinayət Məcəlləsinin "Kompüter informasiyası əleyhinə olan cinayətlər" fəslinin yenidən işlənməsi və onun "Kibercinayətkarlıq haqqında" 2001-ci il 23 noyabr tarixli Konvensiyanın tələblərinə uyğunlaşdırılması barədə təkliflərin hazırlanması tapşırığı qoyulmuşdur.[87] 2012-ci ildə özünün normativ əsasda həllini tapmış, Azərbaycan Respublikasının Cinayət Məcəlləsində dəyişikliklər edilməsi haqqında Azərbaycan Respublikasının Qanunu əsasında[88] Cinayət Məcəlləsinin 30-cu fəsli beynəlxalq hüquqdan transformasiya olunmaqla, o cümlədən "Kibercinayətkarlıq haqqında" Konvensiyanın tələblərinə uyğun olaraq, həmin fəslin "Kompüter informasiyası sahəsində cinayətlər" adı dəyişdirilərək, "Kibercinayətlər" termini ilə əvəzlənmişdir. Eyni zamanda, həmin qanuna görə, qeyd olunan fəslin müvafiq maddələri də Konvensiyasının tələblərinə uyğun olaraq dəyişdirilmişdir. Qanuna əsasən kompüter sisteminə qanunsuz daxil olma, məlumatları qanunsuz ələ keçirmə, həmin məlumatları saxtalaşdırmaya, kibercinayətlərin törədilməsi üçün hazırlanmış vasitələrin dövriyyəsi, kompüter məlumatlarının saxtalaşdırılmasına görə cəzalar sərtləşdirilmişdir.

Qeyd olunan fəsil üzrə ədəbiyyatlarda şərh olunan məsələlərə diqqət yetirilməsi maraqlı olardı. Prof. F. Səməndərovun redaktəsi ilə nəşr olunan "Azərbaycan Respublikası Cinayət Məcəlləsinin Komentariyası"nda[89] qeyd olunur ki, Azərbaycan Respublikasının cinayət qanunvericiliyində "kompüter informasiyası sahəsində cinayətlər" fəsli ilk dəfə olaraq nəzərdə tutulmuş, sonradan 29 iyun 2012-ci il tarixli qanunla bu fəslin maddələri yeni redaksiyada verilmişdir. CM-in XXX fəslinin normaları "Kibercinayətkarlıq haqqında" Avropa Şurasının 23 noyabr 2001-ci il tarixli Konvensiyasına uyğun olaraq (Azərbaycan Respublikası bu Konvensiyaya 30 sentyabr 2009-cu il tarixli, 874-IIIQ nömrəli Qanunla qoşulmuşdur) Azərbaycan Respublikasının üzərinə götürdüyü öhdəliklərin icrasından irəli gələrək cinayət qanununa daxil edilmişdir. Cinayətin ictimai təhlükəliliyi onda ifadə olunur ki, onların törədilməsi nəticəsində kompüter şəbəkələrinin, elektron məlumatların cinayətlərin törədilməsi üçün istifadə edilməsi və bu növ cinayətlərin baş verməsinə dair sübutların bu şəbəkələrdə saxlanılması və ya şəbəkələr vasitəsilə ötürülməsi təhlükəsi yaranır, kompüter sistem və şəbəkələrinin, o cümlədən kompüter verilənlərinin məxfiliyi, bütövlüyü və yararlılığına qarşı yönəlmiş əməllər baş verir, həmçinin bu sistem, şəbəkə və verilənlərdən qeyri-qanuni istifadə mümkün olur, hər kəsin fikir və mülahizələrinin maneəsiz ifadə etmək hüququna qəsd olunur.

Cinayət əməlinin obyekti kompüter sisteminin, kompüter məlumatlarının mühafizəsi sahəsində yaranan ictimai münasibətlərdir. Bu cinayətin predmeti kompüter məlumatlarıdır. Cinayətin obyektiv cəhəti kompüter sisteminə və ya onun hər hansı bir hissəsinə daxil olmaq hüququ olmadan həmin sistemə və ya saxlanılan kompüter məlumatlarını ələ keçirmək və ya başqa şəxsi niyyətlə daxil olmada ifadə olunur.

"Kibercinayətkarlıq haqqında" konvensiyaya görə kompüter məlumatları dedikdə kompüter sistemində işlənməsi, emal edilməsi üçün yararlı olan istənilən informasiya (faktlar, məlumatlar, proqramlar və anlayışlar) başa duşulur.

Kompüter informasiyasının predmeti informasiya ehtiyatlarıdır. Informasiya ehtiyatları dedikdə informasiya sistemlərində (kitabxanalarda, arxivlərdə, fondlarda məlumat banklarında və s.) sənədlər və sənəd massivləri, habelə ayrıca mövcud olan sənədlər və onların massivləri başa duşulur ("İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Qanunun 2-ci maddəsi).

Kompüter informasiyasının xüsusiyyəti onun nisbətən asan göndərilməsinin, yenidən yaradılmasının, artırılmasının mümkünlüyündə ifadə olunur.

Kompüter dedikdə simvollu (işarəli) və obrazlı informasiya üzərində informasiya aparmağa imkan verən aparat-texniki vasitələrin və proqlamlaşdırma vasitələrinin məcmusu başa duşulur.

CM-in 271-ci maddəsinin qeydinin 1-ci, "Kibercinayətkarlıq haqqında" Konvensiyanın 1-ci maddəsinin "a" bəndinə görə kompüter sistemi dedikdə müvafiq proqramlara uyğun olaraq verilənlərin avtomatik işlənməsini

---

[86] Məmmədov R.K. Beynəlxalq cinayət hüququ və Azərbaycan Respublikasının cinayət qanunvericiliyi, Bakı-2012, s.85

[87] Azərbaycan Respublikasında insan hüquq və azadlıqlarının müdafiəsinin səmərəliliyini artırmaq sahəsində Milli Fəaliyyət Proqramı, http://www.azertag.com

[88] Azərbaycan Respublikasının Cinayət Məcəlləsində dəyişikliklər edilməsi haqqında Azərbaycan Respublikasının Qanunu, 29 iyun 2012-ci il, № 408-IVQD.

[89] "Azərbaycan Respublikası Cinayət Məcəlləsinin Komentariyası". Bakı, 2018. 800 s.

həyata keçirən hər hansı qurğu və ya bir-birinə qoşulmuş və ya əlaqələndirilmiş qurğular qrupu başa duşulur. Kompüter sistemi verilənlərin işlənməsi üçün nəzərdə tutulan aparat vasitələrinin və proqram təminatının toplusudur.

Proqramları. Daxili və xarici qurğuları ilə birlikdə fərdi kompüter bir-birinə qoşulmuş bir neçə kompüterdən ibarət lokal şəbəkəyə və internetə qoşula bilər. Kompüter sisteminin bir hissəsi dedikdə şəbəkədə olmayan kompüterin yaddaş qurğusu, şəbəkədə olan kompüterlərdən hər hansı biri, onun kompakt disklərin yazılması üçün nəzərdə tutulan qurğusu və s. başa duşulur.

Kompüter şəbəkəsi dedikdə öz aralarında rabitə kanalı ilə birləşdirilmiş və bu rabitənin həyata keçirmə yə imkan verən iki və daha çox kompüterin məcmusu başa duşulur.

CM-in 271-ci maddəsinin tərkibinin olması üçün kompüter informasiyası işlənmə, emal edilmə üçün yararlı olmalıdır. Informasiyanın yararlı olması ondan istifadəsinin mümkünlüyü dərəcəsindən asılıdır. Kompüter sistemində olan informasiyanın bütövlükdə yararlı olması tələb olunmur: kifayətdir ki, ələ keçirilən informasiya onu ələ keçirən şəxsə lazım olan səviyyədə yararlı olsun. Məsələn, belə informasiyadan istifadə etməklə informasiya sahibinə zərər vurula bilsin, ictimai təhlükəsizliyə və ictimai qaydaya təhlükə yaransın.

İnsanın şəxsi həyatı, kommersiya və məlumat sirri də qanunun mühafizəsi altındadır. "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Qanunun 6-cı maddəsinə görə fiziki və hüquqi şəxslər onların vəsaitləri hesabına yaradılmış, qanuni yolla əldə edilmiş, yaxud bağışlama, vərəsəlik qaydasında toplanmış informasiya ehtiyatlarının, informasiya sistemlərinin, texnologiyalarının və onların təminat vasitələrinin mülkiyyətçisidir. Bunlara mülki qanunvericiliyin qüvvəsi şamil olunur.

Qeyd etmək lazımdır ki, son dəyişikliklərə əsasən kibercinayətlərə görə cəzaların sərtləşdirilməsi beynəlxalq təcrübəyə və Konvensiyanın müddəaları ilə ziddiyyət təşkil etmir. Eyni zamanda, bu addım ölkə ictimaiyyəti tərəfindən də təqdirəlayiq hesab olunur və bu dəyişiklik tam əsaslı hesab edilir: Çünki bütün hüquqazidd əməllərin nəticəsi olaraq, kibercinayətkarlar tərəfindən bank hesabları açıb külli miqdarda pullar götürülür, həmçinin insanların şəxsi həyatına müdaxilə olunur, habelə dövlət orqanlarının məlumat bazaları sıradan çıxarılır. Bu isə böyük bir fəlakətə də gətirib çıxara bilər.[90] Qeyd olunanların zəruriliyini nəzərə alaraq bir daha əminliklə vurğulamaq olar ki, milli qanunvericilikdə kibercinayətlərlə bağlı cəzaların sərtləşdirilməsi ictimai tələbatdan irəli gəlir və tam qanuni məqsədlər daşıyır.

Hazırda ölkəmizdə İKT sahəsində sürətli inkişafı, bu sferada texnoloji infrastrukturun daim yenilənməsini, informasiya sahəsində törədilən hüquqazidd əməllərin diapazonunun genişlənməsini və kibercinayətkarlıqla bağlı mübarizə üzrə dövlətimzin sərt və davamlı mövqeyini nəzərə alaraq qeyd etmək lazımdır ki, gələcəkdə "Kibercinayətkarlıq haqqında" ayrıca qanunun qəbul edilməsi daha məqsədəuyğun olardı.

Eyni zamanda bu gün Azərbaycan Respublikasında kibertəhlükəsiziliyin təmin olunması istiqamətində qanunvericiliyin təkmilləşdirilməsi ilə yanaşı, təşkilati mexanizmlərin inkişafı istiqamətində dövlətimiz tərəfindən informasiya təklüləsizliyi baxımından müxtəlif təbirlər həyata keçirilir.

Kibercinayətkarlıqla mübarizə üzrə səlahiyyətli qurum qismində Dövlət Təhlükəsizlik Xidməti müəyyən olunduğu üçün bu orqan tərəfindən konkret işlər görülməkdədir. Kibercinayətkarliğın, xüsusilə də kiberterrorçuluğun getdikcə daha ciddi xarakter alması bu təhlükələrin qabaqlanması istiqamətində Dövlət Təhlükəsizlik Xidmətinin fəaliyyətinin təkmilləşdirilməsi zərurətini artırmışdır. Bu sahədə qanunsuz əməllərə qarşı mübarizə müvafiq texniki avadanlıqların mövcudluğunu, habelə yüksək texnologiyalara dair xüsusi bilik və bacarıqlara yiyələnməyi tələb edir. Son illər ərzində məhz göstərilən sahələrə diqqət artırılmış, eləcə də ölkəmizin kibertəhdidlərə qarşı mübarizə imkanlarının təkmilləşdirilməsi istiqamətində adekvat tədbirlər görülmüşdür. Statistikaya görə, 2007-ci ildən bankomatladan istifadə, qanunsuz olaraq dövlət təşkilatlarının məlumat (kompüter) bazasına daxil olma, rabitə və informasiya texnologiyaları sahəsində baş vermiş digər qanunsuz əməllər üzrə cinayət məsuliyyətinə cəlb edilmə faktları baş vermişdir.

Qeyd olunmalıdır ki, kibercinayətlərin istintaqının aparılması, bu istiqamətdə baş verəcək təhdidlərin önlənməsi ilə bağlı Dövlət Təhlükəsizlik Xidməti tərəfindən müvafiq tədbirlər görülür, cinayət işləri qaldırılır, bu neqativ təzahürlərə qarşı səmərəli mübarizə aparılır.

Həmçinin, vurğulamaq lazımdır ki, "Kibercinayətkarlıq haqqında" Konvensiyanın 35-ci maddəsinin 1-ci bəndinə əsasən kompüter sistemləri və kompüter verilənləri ilə əlaqədar cinayətlərin istintaqı və ya digər icraatın aparılması məqsədilə və ya cinayətlərə dair sübutların elektron formada toplanması üçün təxirəsalınmaz yardımın göstərilməsini təmin etmək məqsədilə 24/7 şəbəkəsinin – sutkada iyirmi dörd saat, həftədə yeddi gün ərzində fəaliyyət göstərən müvafiq əlaqə mərkəzinin yaradılması müəyyən edilmişdir. Azərbaycan Respublikası Konvensiyanın həmin bəndi üzrə xüsusi Bəyanat verərək, Konvensiyanın 35-ci maddəsinin 1-ci bəndinə müvafiq olaraq, bu cür əlaqələndirici qurum qismində Dövlət Təhlükəsizlik Xidmətini təyin etmişdir.

Kibertəhlükəsizliyin təmin olunması sahəsində digər mühüm qurum Azərbaycan Respublikasının Xüsusi Dövlət Mühafizə Xidmətinin Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Agentliyidir. Agentlik ölkə Prezidentinin 2012-ci il 26 sentyabr tarixli 708 nömrəli Fərmanına əsasən yaradılmışdır. Digər əhəmiyyətli funksiyaları ilə yanaşı, Agentlik xüsusi təyinatlı informasiya-telekommunikasiya sistemlərini və şəbəkələrini, idarələr arası elektron sənəd dövriyyəsini, dövlət orqanlarının internet şəbəkəsi ilə əlaqəsini, onların internet informasiya resurslarının məlumat və resurs mərkəzində yerləşdirilməsinin təşkilini, istismarını, təhlükəsizliyini və inkişafını təmin edən, dövlət orqanlarının informasiya sistemlərinin təhlükəsizlik parametrləri üzrə monitorinqini həyata keçirən, dövlət mühafizəsi obyektlərinin və mühafizə olunan obyektlərin təhlükəsizliyini təmin etmək məqsədi ilə xüsusi texniki tədbirləri hazırlayıb həyata keçirən qurumdur. Bu orqan həmçinin,

[90] Kibercinayətkarlıqla bağlı ayrıca qanunun qəbul olunmasına ehtiyac görülür http://www.paritet.az/layihe/5863.html

informasiya təhlükəsizliyi sahəsində dövlət siyasətinin hazırlanmasında və həyata keçirilməsində iştirak edir, kriptoloji fəaliyyətin təkmilləşdirilməsinin, elmi-texniki innovasiyaların tətbiqinin təmin edilməsini, həmçinin Azərbaycan Respublikasının Təhsil Nazirliyi və digər qurumlarla birgə informasiyanın kriptoqrafik və texniki mühafizəsi, xüsusi telekommunikasiya sistemləri və şəbəkələri ixtisasları üzrə dövlət orqanları üçün mütəxəssislərin hazırlanmasının təşkil edilməsini həyata keçirir.[91]

Digər tərəfdən, kibertəhlükəsizliyin təmin olunması üzrə təşkilati tədbirlərin görülməsi sahəsində xüsusilə Rabitə və Yüksək Texnologiyalar Nazirliyinin uğurlu fəaliyyətini də vurğulamamaq olmaz. Elə bu qurumun fəaliyyətinin nəticədir ki, Azərbaycan BMT-nin "Elektron hökumət"in inkişaf səviyyəsinə görə yeni "United Nations E-Government Survey 2014: EGovernment for the Future We Want" reytinqi üzrə 28 pillə irəliləmişdir.[92]

"E-hökumət" layihəsi "Elektron Azərbaycan" proqramı çərçivəsində "Azərbaycan Respublikasının inkişafı naminə informasiya-kommunikasiya texnologiyaları üzrə Milli Strategiyaya (2003-2012-ci illər)" əsasən işlənib hazırlanmış və "Elektron Azərbaycan" Dövlət Proqramı çərçivəsində həyata keçirilir. Layihə İKT-nin geniş tətbiqi ilə dövlət orqanlarının fəaliyyətinin səmərəliliyinin və operativliyinin yüksəldilməsini, əhali, biznes qurumları, həmçinin öz aralarında əlaqələrin asanlaşdırılması və sərbəstləşdirilməsinə yönəldilmiş fəaliyyəti nəzərdə tutur, vətəndaş-məmur münasibətlərinin yeni müstəvidə qurulmasına, şəffaflığın təmin olunmasına və informasiya tələbatının dolğun ödənilməsinə şərait yaradır.[93] Bütün bunlar isə əlbəttə kiberməkanda yeni yanaşmaları, xüsusilə bu sahədə neqativ təzahürlərlə mübarizə aparacaq yeni strukturların yaradılmasını da özündə ehtiva edir.

Çünki, qlobal informasiya cəmiyyətinə keçid şəraitində dövlətlər, cəmiyyətlər, biznes strukturları, fərdlər kiberfəzada informasiyanın və onun mənbəyinin həqiqiliyi, elektron xidmətlərdən təhlükəsiz istifadə, fərdi məlumatların qorunması, tamlığı və konfidensiallığı sahəsində kritik problemlərlə qarşılaşırlar. Yeni kibertəhlükələrin müntəzəm olaraq meydana çıxdığı, təkmilləşdirildiyi mühitdə ölkələrin bu qlobal təhlükələrə qarşı çevik və operativ kibertəhlükəsizlik strategiyalarına malik olması mühüm əhəmiyyət daşıyır. Hazırda dövlət orqanlarına və özəl şirkətlərə qarşı kiberhücum və kibercasusluq halları surətlə artmaqdadır. Qarşılıqlı əlaqəli və asılı informasiya infrastrukturuna yönlük planlaşdırılmış, yerinə yetirilmiş və məqsədinə nail olmuş kiberhücumlar ağır nəticələrə gətirib çıxara bilər. Kibertəhlükəsizliyin təmin olunması – cəmiyyətin sabitliyinin və normal fəaliyyətinin müvəffəqiyyətə nail olmanın əsas şərtlərindən biri olaraq Elektron Təhlükəsizlik Mərkəzi yaradılmışdır. Bu qurum kibertəhlükəsizlik sahəsində informasiya infrastrukturu subyektlərinin fəaliyyətinin koordinasiyasını, mövcud və yarana biləcək elektron təhlükələr barədə ölkə səviyyəsində məlumatlandırmanı, əhalinin, özəl və digər qurumların kibertəhlükəsizlik sahəsində maarifləndirilməsini və onlara metodiki kömək göstərilməsini təmin edən əlaqələndirici qurum olan dövlət orqanıdır.[94] Mərkəz informasiya sistemlərinin və şəbəkələrinin, kompüter avadanlıqlarının və onların proqram təminatının, lokal və korporativ informasiya sistemlərinin və ehtiyatlarının təhlükəsizliyinə qarşı yönəldilmiş kiberhücumlar, qanunsuz müdaxilələr, ziyanverici proqramlar (elektron təhlükələr) barədə istifadəçilərdən, proqram təminatı və texniki avadanlıqların istehsalçılarından, xarici ölkələrdəki analoji strukturlardan və digər mənbələrdən daxil olan məlumatları toplayır və təhlil edir, habelə bu sahədə maarifləndirmə, elektron təhlükələrin qarşısının alınması və digər sahələr üzrə tədbirlər həyata keçirir.

Müasir mərhələdə Azərbaycanın davamlı və dayanıqlı inkişafı siyasətinin prioritet istiqamətlərindən elan olunan İKT (İKT) sosial-iqtisadi sistemin bütün sahələrinə və insanların gündəlik fəaliyyətinə surətlə nüfuz edərək, ictimai-iqtisadi münasibətlərin ayrılmaz tərkib hissəsinə çevrilmişdir. Son illərdə ölkədə informasiya cəmiyyətinin bərqərar olması və bunun tərkib hissəsi kimi İKT-nin geniş tətbiq edilməsi istiqamətində sistemli fəaliyyət aparılır. Bu baxımdan, "Azərbaycan Respublikasının inkişafı naminə informasiya və kommunikasiya texnologiyaları üzrə Milli Strategiya (2003-2012-ci illər)", Azərbaycan Respublikası Prezidentinin 2010-cu il 11 avqust tarixli, 1056 nömrəli Sərəncamı ilə təsdiq edilmiş Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafı üzrə 2010-2012-ci illər üçün Dövlət Proqramı (Elektron Azərbaycan) və həyata keçirilən genişmiqyaslı işlər qeyd edilə bilər. Hal-hazırda respublikada İKT sektorunun inkişaf tempi bu sahədə ümumdünya göstəricilərini təxminən üç dəfə qabaqlayır. Dünya İqtisadi Forumu tərəfindən 2008-2009-cu illər üçün hazırlanmış "İnformasiya texnologiyalarının qlobal inkişafı haqqında hesabat"da Azərbaycan 134 ölkə sırasında 60-cı yeri tutmaqla, bir çox nüfuzlu ölkələri qabaqlamışdır və MDB-nin iştirakçısı olan dövlətlər arasında lider olmuşdur.[95]

Bu gün artıq ölkəmizdə "Azərbaycan 2020: gələcəyə baxış" İnkişaf Konsepsiyası"na əsasən İKT sahəsi üzrə vəzifələr müəyyənləşdirilmiş, "Azərbaycan Respublikasında 2013-cü ilin "İnformasiya-kommunikasiya texnologiyaları ili" elan edilməsi ilə bağlı Tədbirlər Planı"nın təsdiq olunmuş və icra edilmiş, habelə "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya"[96] təsdiq edilmişdir. Yuxarıda qeyd etdiyimiz bütün sənədləri üzrə əlaqələndirici qurum qismində məhz Azərbaycan Respublikasının Rabitə və Yüksək Texnologiyalar Nazirliyi müəyyən olunmuşdur. Bu sənədlərdə irəli sürülən

---

[91] Xüsusi Rabitə və İnformasiya Təhlukəsizliyi Dövlət Agentliyi, http://www.dmx.gov.az/page/6.html

[92] Elektron Hökümət bulleteni. N 19, iyul 2014, səh.4. 16 s.

[93] Elektron hökumət, http://www.mincom.gov.az/layiheler/elektron-hokumet

[94] Elektron Təhlukəsizlik Mərkəzi, http://www.cert.az/

[95] Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafı üzrə 2010-2012-ci illər üçün Dövlət Proqramı (Elektron Azərbaycan). Azərbaycan Respublikası Prezidentinin 2010-cu il 11 avqust tarixli, 1056 nomrəli Sərəncamı ilə təsdiq edilmişdir. "Azərbaycan" qəzeti , 12 avqust 2010-cu il, № 174. S. 5

[96] "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya" İlham Əliyev Azərbaycan Respublikasının Prezidenti Bakı şəhəri, 2 aprel 2014-cü il.

ideyalar və həyata keçirilən tədbirlər informasiya cəmiyyətinin inkişafına yönəlmiş addımlardandır və respublikamızda kibertəhlükəsizliyin təmin olunması əhalinin bu istiqamətdə daha müasir və modern texnologiyalardan istifadə mədəniyyətinin yüksəldiləsi ilə bağlı müasir beynəlxalq birliyin qəbul etdiyi normaların ölkəmizdə səmərəli tətbiqinə hesablanmışdır.

Kibercinayətkarlığa qarşı mübarizə üzrə beynəlxalq hüquq normalarının ölkədaxili səmərəli tətbiqi üçün fikrimizcə, bu sahədə müvafiq qurumlar, o cümlədən ictimai birliklər tərəfindən maariflədirmə işlərinin aparılması vacibdir. Eyni zamanda, təlim və tədris materiallarının tərcümə edilərək əhali arasında yayımı, habelə radio, televiziya, İnternet resuarlarından istifadə olunmaqla bu sahədə biliklərin yayılması, normativ hüquqi bazanın KİV-də geniş dərc edilməsi bu istiqamətdə əsas məqsədin əldə olunmasına yardımçı ola bilər.

Kiberməkandan istifadə, habelə burada informasiya resurslarının mühafizəsi və kibercinayətkarlıqla mübarizə məsələsi digər xarici ölkələrdə olduğu kimi, Azərbaycan Respublikasında da milli təhlükəsizliyin başlıca elementlərindən hesab olunur. Bu sahədə beynəlxalq hüquq normalarının Azərbaycan Respublikasının sahəvi qanunvericiliyinə implementasiyası özünün real təcəssümünü milli təhlükəsizlik sahəsində qanunvericilikdə də tapmışdır. Belə ki, 2004-cü il tarixli "Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının Qanununun 7.9-cu maddəsində qeyd olunur ki, ölkəmizdə informasiya sahəsində əsas təhdidlər aşağıdakılardır: informasiya texnologiyaları sahəsində geriləmə və dünya informasiya məkanına daxil olmağa maneələrin mövcudluğu; informasiya azadlığı əleyhinə yönəlmiş qəsdlər; dövlət sirlərinin aşkarlanmasına yönəlmiş qəsdlər; digər ölkələr tərəfindən informasiya təcavüzü, beynəlxalq aləmdə Azərbaycan həqiqətlərinin təhrif edilməsi; informasiya sisteminə və ehtiyatlarına qarşı qəsdlər.[97]

Göründüyü kimi, qanunda müasir beynəlxalq hüquq normalarının tələblərindən irəli gələn aktual məsələlərə – istər insan hüquqlarının təmin olunması, o cümlədən informasiya azadlığının müdafiəsi, istərsə də, beynəlxalq təhlükəsizlik problemlərinə, məsələn informasiya təcavüzünə səbəb ola biləcək nüanslar öz təsbitini tapmışdır. Bundan əlavə, bilavasitə kompüter cinayətləri ilə bağlı məsələ də Qanunda öz əksini tapmışdır. Qanunun 20.2-ci maddəsində qeyd olunur ki, Azərbaycan Respublikasının informasiya sahəsində milli təhlükəsizliyinin təmin olunması üçün görülən əsas tədbirlər aşağıdakılardır:

1) Azərbaycan Respublikasında informasiyanın, həmçinin dövlət informasiya ehtiyatlarının müdafiəsi sahəsində milli sistemin yaradılması və mohkəmləndirilməsi;

2) Dövlət orqanları və vəzifəli şəxslər tərəfindən qərarların qəbul edilməsinin informasiya təminatının həyata keçirilməsi məqsədilə obyektiv və qabaqlayıcı məlumatların toplanılması;

3) İnformasiya infrastrukturunun inkişaf etdirilməsi;

4) Dövlət sirlərinin qorunmasının hüquqi mexanizmlərinin təkmilləşdirilməsi;

5) Kibercinayətlərə qarşı mübarizə;

6) İnformasiya təhlükəsizliyinin və azadlığının təmin olunması.

Göründüyü kimi, beynəlxalq hüquq normalarında ifadə olunan informasiya təminatı, infrastrukturun inkişafı, informasiya təhlükəsizliyi və informasiya azadlığının tənzimi məsələləri Qanunda təsbit edilmiş, eyni zamanda, bizim tədqiqatımız baxımından mühüm əhəmiyyətli dəyişiklik edilmişdir. Qeyd edək ki, Qanunun əvvəlki redaksiyasında "kompüter informasiyası sahəsində cinayət" anlayışından istifadə olunmuşdu. Qeyd olunan həmin ifadə müasir dövr üçün uğurlu sayılmadığından, təqdirəlayiq haldır ki, 21 dekabr 2012-ci il tarixli 522-IVQD nömrəli Azərbaycan Respublikasının Qanunu ilə 20.2.5-ci maddəsində "kompüter informasiyası sahəsində cinayətkarlığa" sözləri "kibercinayətlərə" sözü ilə əvəz edilmişdir.[98]

Beləliklə, aparılan araşdırmaların yekunu olaraq aşağıdakı təklif və tövsiyələri məqbul hesab edirik:

1) Azərbaycan Respublikasının Cinayət Məcəlləsinin 30-cu fəslinin "Kompüter informasiyası sahəsində cinayətlər" adının dəyişdirilərək, "Kibercinayətlər" termini ilə əvəzlənməsi müasir beynəlxalq hüquq, o cümlədən "Kibercinayətkarlıq haqqında" Konvensiyanın tələbləri baxımından təqdir olunur və bu terminin ölkəmizin digər sahəvi qanunvericiliyinə implementasiyası məqbul sayılır;

2) Ölkəmizin "Kibercinayətkarlıq haqqında" Konvensiyanı ratifikasiya etməsi milli hüquqi implementasiya baxımından çox mühüm irəliləyiş hesab olunur, sənədə edilən bəyanat və qeyd-şərtlər isə müvafiq olaraq kibercinayətkarlıq üzrə ekstradisiya, qarşılıqlı yardım, səmərəliliyin təmin edilməsi, cinayətlərin istintaqı və ya digər icraatın aparılması məqsədilə və ya cinayətlərə dair sübutların elektron formada toplanması üçün təxirəsalınmaz yardımın göstərilməsi, Konvensiyanın müddəalarının Azərbaycan Respublikasının Ermənistan Respublikası tərəfindən işğal olunmuş ərazilərində həyata keçirilməsi və s. məsələlərini tənzimləyərək, Konvensiyanın ölkəmizdə implementasiya şərtlərini və imkanlarını diktə edir.

3) Kibercinayətkarlıqla bağlı texnoloji inkişafı nəzərə alaraq, gələcəkdə "Kibercinayətkarlıq haqqında" ayrıca qanunun qəbul edilməsi daha məqsədəuyğun olardı.

4) Azərbaycan Respublikasında kibertəhlükəsiziliyin təmin olunması istiqamətində təşkilati mexanizmlərin inkişafı istiqamətində dövlətimiz tərəfindən müxtəlif təbirlər həyata keçirilir. Kibercinayətkarlıqla mübarizə üzrə səlahiyyətli qurum qismində Dövlət Təhlükəsizlik Xidmətinin, informasiya təhlükəsizliyinin təmin olunması üzrə isə Rabitə və Yüksək Texnologiyalar Nazirliyinin uğurlu fəaliyyətini vurğulamaq zəruridir.

5) Azərbaycan hüquq sistemi kibertəhlükəsizliyin pozulması, o cümlədən informasiya məkanında baş verən hüquqazidd davranışlarla bağlı məsələləri, eyni zamanda, inzibati qanunvericilik çərçivəsində də həllinə üstünlük verilməli, əhəmiyyətli zərərin vurulma dərəcəsinə müvafiq olaraq, milli inzibati hüquq normalarında bu kimi müddəaların təsbit olunması təqdirəlayiq hesab edilməlidir.

---

[97] "Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının Qanunu, http://www.mns.gov.az

[98] "Azərbaycan" qəzeti, 1 fevral 2013-cü il, № 23, s. 4.

6) Kibercinayətkarlığa qarşı mübarizə üzrə beynəlxalq hüquq normalarının ölkədaxili səmərəli tətbiqi üçün müvafiq qurumlar tərəfindən maariflədirmə işlərinin aparılması, təlim və tədris materiallarının tərcümə edilərək əhali arasında yayımı, normativ hüquqi bazanın KİV-də geniş dərc edilməsi bu istiqamətdə əsas məqsədin əldə olunmasının yardımçı vasitəsi kimi çıxış edir.

3.3. Azərbaycan Respublikasında kibercinayətkarlıqla mübarizənin təşkilati-hüquqi əsasları

Kibercinayətkarlıqla mübarizə, o cümlədən informasiya təhlükəsizliyi məsələsi bir çox dövlət orqanlarının birgə əlaqəli işini tələb edir. Bu sahədə fəaliyyətin həyata keçirilməsinin müxtəlif aspektləri ölkəmizdə Rabitə və Yüksək Texnologiyalar Nazirliyi, Dövlət Təhlükəsizlik Xidməti və Ədliyyə Nazirliyinə şamil edilmişdir.

Qeyd olunmalıdır ki, Rabitə və İnformasiya Texnologiyaları Nazirliyi 2005-ci ildə Azərbaycan Respublikasının "Kibercinayətkarlıq haqqında" 23 noyabr 2001-ci il tarixli Budapeşt şəhərində imzalanmış Konvensiyaya qoşulmasının təşəbbüskarı kimi çıxış etmiş, Prezident İlham Əliyevin Sərəncamı ilə ölkəmiz 2008-ci ildə bu konvensiyaya qoşulması haqqında Avropa Şurasında, Strasburqda sənəd imzalamışdır. Sözügedən Konvensiya 2009-cu il sentyabrın 30-da Azərbaycan Respublikasının Milli Məclisi tərəfindən müvafiq bəyanatlar və qeyd-şərtlərlə təsdiq olunmuşdur.[99] 2010-cu il iyulun 1-də nəzərdə tutulan müvafiq prosedurlar həyata keçirildikdən sonra ölkəmiz adı çəkilən Konvensiyaya qoşulmuşdur. Bu, kibertəhlükəsizliyin təmin olunması və onun ayrılmaz hissəsi olan kibercinayətkarlığa qarşı mübarizə sahəsində istifadə olunan beynəlxalq mexanizmlərdən biridir.[100]

Xüsusi vurğulamaq lazımdır ki, yuxarıda da qeyd olunduğu kimi, Azərbaycan Respublikası "Kibercinayətkarlıq haqqında" Konvensiyanı 5 bəyanat və 4 qeyd-şərtlə ratifikasiya etmişdir. Bunlar həmin Konvensiyanın ölkəmizdə implementasiya şərtlərini və imkanlarını diktə etməklə, müvafiq olaraq kibercinayətkarlıq üzrə ekstradisiya, qarşılıqlı yardım, səmərəliliyin təmin edilməsi, cinayətlərin istintaqı və ya digər icraatın aparılması məqsədilə və ya cinayətlərə dair subutların elektron formada toplanması üçün təxirəsalınmaz yardımın göstərilməsi, Konvensiyanın müddəalarının Azərbaycan Respublikasının Ermənistan Respublikası tərəfindən işğal olunmuş ərazilərində həyata keçirilməsi və s. məsələlərə aiddir.

Kibercinayətkalıqla mübarizənin həyata keçirilməsi və bu sahəyə aid beynəlxalq hüquq normalarının implementasiyası ilə bağlı praktiki əhəmiyyət kəsb edən problemlərdən biri ekstradisiyadır. Bununla əlaqədar olaraq, ölkəmiz Konvensiyaya qoşularkən Bəyanat verərək bildirmişdir ki, "Azərbaycan Respublikası, Konvensiyanın 24-cü maddəsinin 7-ci bəndinin "a" yarımbəndinə uyğun olaraq, ekstradisiya müqaviləsi olmadığı hallarda ekstradisiya və müvəqqəti həbsə dair sorğuları qəbul edən səlahiyyətli orqan qismində Ədliyyə Nazirliyini təyin edir". Ümumiyyətlə qeyd etmək lazımdır ki, cinayətlərə münasibətdə ekstradisiya üzrə sorğuları qəbul etmək və vermək səlahiyyətinə malik qurumların dairəsi Azərbaycanda bir qədər mürəkkəb xarakter daşıyır və elmi dairələrdə mübahisəli sayılır.

Hüquq elmləri doktoru N.A.Səfərov qeyd edir ki, ümumilikdə, hüquqi praktikada ekstradisiya haqqında sorğuların baxılmasının bir necə variantı mövcuddur: birincisi, icra hakimiyyəti orqanları tərəfindən; ikincisi, məhkəmə və icra orqanı; üçüncüsü, yalnız məhkəmə tərəfindən.[101] Ölkəmizdə mövcud olan praktikaya uyğun olaraq, bu ekstradisiya ilə bağlı sorğu məsələsi ilə iki orqan – Ədliyyə Nazirliyi və Azərbaycan Respublikasının Baş Prokurorluğu məşğul olur. Respublikamızda kibercinayətkalıq sahəsində sorğu məsələlərinin həllinin Ədliyyə Nazirliyinə həvalə olunmasının əsas səbəbi isə ondan ibarətdir ki, bir qayda olaraq, Avropa konvesiyaları, ikitərəfli müqavilələr və milli qanun çərçivəsində sorğu məsələsinə məhz Ədliyyə Nazirliyi baxır. Mövcud praktikaya uyğun olaraq, MDB konvensiyaları çərçivəsində isə bu məsələ Baş Prokurorluğun səlahiyyətinə aid edilir.

Lakin, müasir dünya praktikasını nəzərə alaraq, hüquq elmləri üzrə fəlsəfə doktoru A.Əbilov sorğuların baxılmasında vahid yanaşmanın tətbiqini, habelə belə sorğuların baxılmasına dair bir orqana səlahiyyətin verilməsini təklif edir. Eyni zamanda, müəllif ekstradisiya haqqında yekun qərarların yalnız məhkəmələr tərəfindən çıxarılmasını məqsədəuyğun hesab edir (bu zaman ağır cinayətlər üzrə bütün məhkəmələr tərəfindən yurisdiksiyasından asılı olaraq bu sorğulara baxmaq səlahiyyətinin verilməsi).[102] Müəllifin bu fikrinə şərik çıxaraq qeyd etmək lazımdır ki, əslində bu məsələdə vahid yanaşmanın olması və nəzərə alaraq ki, məhkəmələr müxtəlif cinayətlər üzrə professional qərarların qəbul edilməsində daha təcrübəli olduqları üçün məhz kibercinayətlərlə bağlı sorğu məsələsinin də məhkəmələrin səlahiyyətinə aid edilməsi müasir beynəlxalq hüquq nöqteyi-nəzərindən daha məqbul hesab oluna bilər.

Kibercinayətlərlə bağlı ölkəmiz tərəfindən verilən növbəti bəyanat qarşılıqlı yardım üzrə sorğularla bağlıdır. Bu məsələdə isə səlahiyyətli orqan Dövlət Təhlükəsizlik Xidməti müəyyən edilmişdir. Sənəddə qeyd olunur ki, "Azərbaycan Respublikası, Konvensiyanın 27-ci maddəsinin 2-ci bəndinin "c" yarımbəndinə müvafiq olaraq, qarşılıqlı yardım üçün sorğu göndərmək, sorğuları icra etmək və onların icra edilməsi üçün məsul olan səlahiyyətli orqan qismində Dövlət Təhlükəsizlik Xidmətini təyin edir". Göründüyü kimi, bu məsələ də sorğu ilə bağlı olsa da qanunda buna səlahiyyətli qurum daha fərqli mərkəzi icra hakimiyyəti orqanı müəyyən edilmişdir. Görünür burada əsas səbəb ondan ibarətdir ki, kibercinayətlər daha çox ölkəmizin milli təhlükəsizliyi ilə bağlı mənafelərini xələl gətirdiyi üçün, bu sahə ilə məhz qurumun məşğul olması məqbul sayılmışdır.

---

[99] "Kibercinayətkarlıq haqqında" konvensiyanın təsdiq edilməsi barədə Azərbaycan Respublikasının Qanunu, http://www.eqanun.az

[100] Kibercinayətkarlıqla bağlı ayrıca qanunun qəbul olunmasına ehtiyac görülür. http://www.paritet.az/layihe/5863.html

[101] Сафаров Н., Комментарий к закону Азербайджанской Республики "О выдаче (экстрадиции) лиц, совершивших преступления", Баку, Изд. Юридическая литература, 2001, стр. 145

[102] Əbilov A. F. İnsan hüquqları üzrə beynəlxalq normaların ekstradisiya haqqında Azərbaycan qanunvericiliyinə implementasiyası məsələləri. Hüquq üzrə fəlsəfə doktoru alimlik dərəcəsi almaq üçün təqdim olunmuş dissertasiyanın Avtoreferatı. Bakı -2014, s.22. 26 səh.

“Kibercinayətkarlıq haqqında” Konvensiya üzrə verilən digər Bəyanatda Konvensiyanın 27-ci maddəsinin 9-cu bəndinin “e” yarımbəndinə uyğun olaraq Azərbaycan Respublikası baş katibi məlumatlandırır ki, səmərəliliyin təmin edilməsi məqsədilə bu bənd əsasında edilmiş sorğular onun mərkəzi hakimiyyət orqanına göndərilməlidir. Qeyd etmək lazımdır ki, Konvensiyanın 27-ci maddəsi əslində kibercinayətkalıqla bağlı ipmlementasiya məsələlərinin müxtəlif nüanslarını tənzimləyir. (Maddə 27 – Tətbiq edilən beynəlxalq müqavilələr mövcud olmadıqda qarşılıqlı yardım haqqında sorğuların göndərilməsi proseduraları).[103] 27-ci maddənin 9-cu bəndinin “e” yarımbəndinə qeyd olunur ki, hər bir Tərəf hazırkı Konvensiyanı imzalayarkən və ya ratifikasiya fərmanını yaxud qəbul etmə, bəyənilmə və ya qoşulma haqqında öz sənədini saxlanılması üçün təhvil verərkən səmərəliliyin təmin edilməsi məqsədilə hazırkı bəndin müddəalarına uyğun olaraq göndərilən sorğuların onun mərkəzi orqanlarına ünvanlanmalı olduqları barədə Avropa Şurasının Baş katibini məlumatlandıra bilər. Xüsusi vurğulamaq lazımdır 9-cu bəndə müvafiq olaraq, kibercinayətlərlə bağlı qarşılıqlı yardım haqqında sorğular və ya bu sorğularla bağlı məlumatlar həm sorğu edən Tərəfin cinayət prosesini həyata keçirən orqanları tərəfindən birbaşa sorğu edilən Tərəfin müvafiq orqanlarına göndərilə bilər, həm də sorğu və ya məlumat Beynəlxalq Cinayət Polisi Təşkilatı (İnterpol) vasitəsilə göndərilə bilər. Göründüyü kimi, kibercinayətkarlıqla bağlı Konvensiyada nəzərdə tutulan prosedurlar müvafiq qaydada ölkəmizin milli hüquq sisteminə transformasiya olunmaqla, onun müddəalarının səmərəli şəkildə həyata keçirilməsi üçün əlverişli şərait yaradır.

Konvensiyanın ölkədaxili implementasiyası ilə bağlı mühüm və maraqlı məsələlərdən biri də kibercinayətlərlə bağlı istintaqın və digər icraatların aparılması ilə əlaqədardır. Bu, öz həllini Konvensiyanın 35-ci maddəsinin 1-ci bəndi üzrə ölkəmizin verdiyi Bəyanatda tapmışdır. Orada qeyd olunur ki, Azərbaycan Respublikası, Konvensiyanın 35-ci maddəsinin 1-ci bəndinə müvafiq olaraq, kompüter sistemləri və kompüter verilənləri ilə əlaqədar cinayətlərin istintaqı və ya digər icraatın aparılması məqsədilə və ya cinayətlərə dair subutların elektron formada toplanması üçün təxirəsalınmaz yardımın göstərilməsini təmin etmək məqsədilə sutkada iyirmi dörd saat, həftədə yeddi gün (7/24) ərzində fəaliyyət göstərən əlaqələndirici qurum qismində Dövlət Təhlükəsizlik Xidmətini təyin edir.

Azərbaycan Respublikasının “Kibercinayətkarlıq haqqında” Konvensiyanın 38-ci maddəsi üzrə Bəyanatı isə Ermənistanın Azərbaycana hərbi təcavüzü ilə bağlıdır. Orada ölkəmiz Konvensiyanın 38-ci maddəsinə uyğun olaraq, Konvensiyanın müddəalarının Azərbaycan Respublikasının Ermənistan Respublikası tərəfindən işğal olunmuş ərazilərində həyata keçirilməsinə həmin ərazilər işğaldan azad edilməyənədək zəmanət verə bilməyəcəyini bəyan edir. Bu müddəanı da kibercinayətkarlıqla mübarizə üzrə səmərəli implementasiyasının əsas şərtlərindən biri saymaq olar. Çünki, hal-hazırda Ermənistan tərəfindən təcavüzə məruz qalan Dağlıq Qarabağ və ətraf rayonlarda dövlətimizin hüquqi yurisdiksiyasının həyata keçirilməsi qeyri-mümkündür.

Konvensiyanın “Ərazi üzrə tətbiq” adlı 38-ci maddəsinə görə hər bir dövlət imzalama zamanı və ya ratifikasiya fərmanını, qəbuletmə, təsdiqetmə yaxud qoşulma haqqında sənədini saxlanması üçün təqdim edərkən hazırkı Konvensiyanın tətbiq ediləcəyi ərazini və ya əraziləri göstərə bilər. Təqdirəlayiq haldır ki, Konvensiyada gələcəkdə qeyd olunan konflikt öz həllini tapacağı təqdirdə, yəni Azərbaycan öz ərazilərində qanuni yurisdiksiyasını bərpa etdikdən sonrakı dövr üçün də bu məsələ ilə bağlı konkret implementasiya proseduru nəzərdə tutulmuşdur. 38-ci maddənin 3-cü bəndində qeyd olunur ki, “həmin maddənin iki bəndinə uyğun olaraq təqdim edilmiş hər hansı bir bəyanat onda göstərilən hər hansı bir əraziyə münasibətdə Baş katibin adına bildiriş təqdim etməklə geri götürülə bilər. Geri götürülmə Baş katib bu cür bildirişi aldığı tarixdən üç ay sonra gələn ayın birinci günü qüvvəyə minir”.

Maraqlı beynəlxalq hüquqi məsələlərdən biri də kiberməkanda baş verən hərəkət və hərəkətsizliklərin cinayət, inzibati və mülki, habelə digər hüquq pozuntusu sayılması problemi ilə bağlıdır. Bu məsələdən də Konvensiya yan keçməmişdi. Ona görə də ölkəmiz kibercinayətkalıqla bağlı normaların implementasiya mexanizmlərini müəyyən edərkən bu elementi nəzərdən qaçırmamış, bununla bağlı Konvensiyanın 6-cı maddəsinin 1-ci bəndinin “b” yarımbəndi üzrə xüsusi qeyd-şərt etmişdir. Həmin qeyd-şərtə əsasən, Azərbaycan Respublikası bəyan edir ki, “əməllər az əhəmiyyətli olduğuna görə ictimai təhlükəli hesab edilmədikdə, cinayət deyil, tənbeh edilə bilən hüquq pozuntuları kimi qiymətləndirilir. Cəza təhdidi altında qadağan olunmuş ictimai təhlükəli əməlin (hərəkət və ya hərəkətsizliyin) təqsirli olaraq törədilməsi əhəmiyyətli zərərə səbəb olursa, cinayət sayılır”.

Göründüyü kimi, əməlin az əhəmiyyətli zərərə malik olub olmaması onun cinayət və ya digər tənbeh tədbirləri nəzərdə tutulan hüquq pozuntuları sayılması üçün əsas hesab olunmuşdur. Bu məsələyə Azərbaycan qanunvericiliyində daha dəqiq və aydın anlayışlar müəyyən edilmişdir. Belə ki, Azərbaycan Respublikasının Cinayət Məcəlləsində 30-cu fəslin (Kibercinayətlər) məqsədləri baxımından “əhəmiyyətli zərər” terminə aydınlıq gətirilmişdir. Orada qeyd olunur ki, “bu fəslin maddələrində “əhəmiyyətli zərər” dedikdə, ictimai təhlükəli əməl nəticəsində min manatdan artıq olan məbləğdə ziyan vurulması və ya dövlətin, cəmiyyətin və ya ayrı-ayrı şəxslərin qanunla qorunan maraqlarına digər mühüm zərərin vurulması başa duşulur”. Buradan belə nəticəyə gəlmək mümkündür ki, kiberməkanda törədilən əməllərin cinayət hüquqi və ya inzibati xəta etibarilə tövsifinin aparılması zamanı bu müddəada nəzərdə tutulan göstərişin hüquq tətbiq edən orqan tərəfindən əsas götürülməsi zəruridir.

Elə bu səbəbdən də, ölkəmiz haqlı olaraq, Konvensiyanın 6-cı maddəsinin 3-cü bəndi üzrə qeyd sərt etmişdir. Orada vurğulanır ki, Azərbaycan Respublikası, Konvensiyanın 6-cı maddəsinin 3-cü bəndinə dair

[103] Convention on Cybercrime, Budapest, 23.XI.2001. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Konvensiyanın 6-cı maddəsinin 1-ci bəndində göstərilən əməlləri, az əhəmiyyətli olduğuna görə ictimai təhlükəli cinayət hesab edilmədikdə, cinayət tərkibli hüquq pozuntuları kimi yox, cəzalandırıla bilən hüquq pozuntuları kimi qiymətləndirir, cinayət məsuliyyətinin yalnız göstərilən əməllər əhəmiyyətli zərərlə nəticələndiyi halda yarandığı barədə qeyd-şərt edir.

Bundan başqa, Azərbaycan hüquq sistemi kibertəhlükəsizliyin pozulması, o cümlədən informasiya məkanında baş verən hüquqazidd davranışlarla bağlı məsələləri eyni zamanda, inzibati qanunvericilik çərçivəsində də həllinə üstünlük vermişdir.

Baxmayaraq ki, bu sahədə beynəlxalq hüququ normalarının ölkədaxili implementasiya prosesləri zəif gedir, lakin hər bir halda milli inzibati hüquq normalarında bu kimi müddəaların təsbit olunması təqdirəlayiq hesab edilməlidir.

Bununla əlaqədar qeyd olunmalıdır ki, İKT-lərin inkişafı qanunvericiliyin bütün sahələrinin təkmilləşdirilməsini şərtləndirir, milli və beynəlxalq normalarda yeni hüquq pozuntusu tərkiblərinin təsbit olunmasını ehtiva edir. Ona görə də, elektron informasiyaların yayılması ilə əlaqədar inzibati xətalar digər hüquq pozuntularından, xüsusilə yaranan məsuliyyət baxımından cinayətlərdən tamamilə fərqlənir. Bu fərq başlıca olaraq ondan ibarətdir ki, cinayət inzibati xətaya nisbətən daha böyük ictimai təhlükəyə malikdir. Şəxsin inzibati məsuliyyətə cəlb edilməsi zərurəti ondan yaranır ki, həmin hüququ pozan şəxs tərəfindən törədilmiş əməl dövlətə və cəmiyyətə ziyan vurmaqla, müəyyən ictimai münasibətlərə qəsd etmiş olur.[104]

Əhəmiyyətli ziyan məsələsinə xüsusi həssaslıq göstərildiyi və bu məsələdə cinayət hüquqi və inzibati hüquqi implementasiyanın sərhədlərinin dəqiq müəyyən edilməsi üçün ölkəmiz "Kibercinayətkarlıq haqqında" Konvensiyanın 4-cü maddəsində nəzərdə tutulan hüquqazidd əməlin (verilənlərə müdaxilə) tovsifi ilə bağlı da xüsusi qeyd-şərt etmişdir. Həmin sənəddə bildirilir ki, Azərbaycan Respublikası, Konvensiyanın 42-ci maddəsinə və 4-cü maddəsinin 2-ci bəndinə uyğun olaraq, cinayət məsuliyyətinin yalnız Konvensiyanın 4-cü maddəsində göstərilən əməllər əhəmiyyətli zərərlə nəticələndiyi halda yarandığı barədə qeyd-şərt edir. Konvensiyanın 4-cü maddəsində isə qeyd olunur ki, "Hər bir Tərəf daxili qanunvericiliyində kompüter verilənlərinin belə hüquq olmadan qəsdən zədələnməsi, silinməsi, korlanması, dəyişdirilməsi və ya təcrid edilməsi əməllərinin cinayət kimi tövsif olunması üçün zəruri olan qanunvericilik və digər tədbirləri görür". Həmin maddənin 2-ci bəndi isə nəzərdə tutur ki, hər bir Tərəf 1-ci bənddə qeyd olunmuş əməlləri yalnız əhəmiyyətli zərər vurduqda cinayət əməli kimi tövsif etmək hüququnu özündə saxlayır.

Kibercinayətkalqla bağlı prosessual implementasiya mexanizmləri müəyyən edən sonuncu qeyd-şərt "Kibercinayətkarlıq haqqında" Konvensiyanın 42-ci maddəsi və 29-cu maddəsinin 4-cü bəndi ilə bağlıdır. Orada vurğulanır ki, Azərbaycan Respublikası, Konvensiyanın 42-ci maddəsinə və 29-cu maddəsinin 4-cü bəndinə uyğun olaraq, verilənlərin mühafizəsinin təminatına dair sorğunun əsaslandığı cinayət aşkar edildiyi vaxt, həmin cinayət Azərbaycan Respublikası qanunvericiliyinə görə cinayət hesab edilmədiyi halda, verilənlərin mühafizəsinin təminatı ilə bağlı sorğunun icrasından imtina etmək hüququna malikdir.

Beləliklə, yuxarıda şərh olunan Konvensiyaya edilən qeyd-şərtlər və ölkəmiz tərəfindən verilən bəyanatlardan görünür ki, istər maddi hüquqi implementasiya, istərsə də, prosessual hüquqi implementasiyanı nəzərdə tutan müddəalar kibercinayətkalıqla bağlı normaların ölkəmizdə daha səmərəli həyata keçirilməsinin ən önəmli şərtlərindən birini təşkil etməklə, ümumilikdə milli qanunvericilik sistemimizin təkmilləşdirilməsinə və inkişafına xidmət edir.

3.4. Azərbaycan milli qanunvericiliyində kibercinayətlərə görə məsuliyyət məsələləri

Azərbaycan Respublikasının qanunvericiliyində kibercinyətkarlıqla mübarizə və bu hüquqazidd əməllərə görə məsuliyyət məsələlərinə diqqət yetirilir, milli qanunlara beynəlxalq konvensiyaların tələblərindən irəli gələn əlavə və dəyişikliklər edilir. Bununla əlaqədar 30 sentyabr 2009-cu il tarixli "Kibercinayətkarlıq haqqında" Konvensiyanın təsdiq edilməsi barədə Azərbaycan Respublikasının Qanunu[105] qəbul edilmiş, müvafiq bəyanatlar və qeyd sərtlərlə bu sənəd təsdiq olunmuşdur.

Eyni zamanda, kompüter informasiyası sahəsində cinayətlər Cinayət Məcəlləsində ayrıca fəsildə (otuzuncu fəsil) qruplaşdırılmaqla, 29 iyun 2012-ci ildə qəbul edilmiş Azərbaycan Respublikasının Cinayət Məcəlləsində dəyişikliklər edilməsi haqqında Qanunla[106] Məcəllənin həmin fəsli daha da təkmilləşdirilmiş, "Kibercinayətlər" adlandırılmış, buraya kibercinayətkarlıqla mübarizəni şərtləndirən yeni müddəalar əlavə olunmuşdur.

Qeyd edək ki, Məcəllənin müvafiq fəslinin "Kibercinayətlər" adlandırılması müasir beynəlxalq hüquq normaları ilə tam uyğunluq təşkil edir və yeni müddəalar ölkəmiz tərəfindən ratifikasiya edilmiş AŞ-nın 23 noyabr 2001-ci il tarixli Kibercinayətkarlıq haqqında Konvensiyasından implementasiya olunmuşdur.

Məcəllənin 271-ci maddəsinə görə, kompüter sisteminə və ya onun hər hansı bir hissəsinə daxil olmaq hüququ olmadan həmin sistemə və ya onun hər hansı bir hissəsinə mühafizə tədbirlərini pozmaqla, yaxud burada saxlanılan kompüter məlumatlarını ələ keçirmək və ya başqa şəxsi niyyətlə qəsdən daxil olma cinayət sayılır və cəzalandırılır.

272-ci maddədə kompüter məlumatlarını qanunsuz ələ keçirmə cinayət hesab edilir: Kompüter sisteminə, kompüter sistemindən və ya bu sistem daxilində ötürülən ümumi istifadə üçün nəzərdə tutulmayan kompüter məlumatlarının, o cümlədən bu cür kompüter məlumatlarının daşıyıcısı olan kompüter sistemlərinin

---

[104] Məcidli S.T. "İnternet hüququ və etikası". Dərs vəsaiti. Bakı: "Elm və təhsil" nəşriyyatı, 2013. S.121.

[105] "Kibercinayətkarlıq haqqında" Konvensiyanın təsdiq edilməsi barədə Azərbaycan Respublikasının Qanunu, № 874-IIIQ, http://www.meclis.gov.az

[106] Azərbaycan Respublikasının Cinayət Məcəlləsində dəyişikliklər edilməsi haqqında Azərbaycan Respublikasının Qanunu, 29 iyun 2012-ci il, № 408-IVQD.

elektromaqnit şüalanmasının, buna hüququ olmayan şəxs tərəfindən texniki vasitələrdən istifadə etməklə qəsdən ələ keçirilməsi iki ilədək müddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə min manatdan iki min manatadək miqdarda cərimə və ya iki ilədək müddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

Qanuna əsasən qeyd olunan cinayətlər üzrə, habelə kibercinayətlərin törədilməsi üçün hazırlanmış vasitələrin dövriyyəsi (273-1-ci maddə), kompüter məlumatlarının saxtalaşdırılması (273-2-ci maddə) cinayətləri ilə bağlı yeni yanaşmalar ortaya qoyulmuş, cəzalar sərtləşdirilmişdir.

Bundan əlavə, qanunla Məcəlləyə yeni – 171-1-ci maddə əlavə olunmuşdur. "Uşaq pornoqrafiyasının dövriyyəsi" adlandırılan bu müddəada "uşaq pornoqrafiyası" anlayışına aydınlıq gətirilir. "Uşaq pornoqrafiyası" dedikdə, yetkinlik yaşına çatmayan şəxsin və ya yetkinlik yaşına çatmayan təsəvvürünü yaradan şəxsin aşkar seksual xarakterli hərəkətlərdə real və ya simulyasiya edilmiş iştirakını əks etdirən, yaxud seksual məqsədlərlə yetkinlik yaşına çatmayanların cinsi orqanlarını əks etdirən istənilən əşyalar və ya materiallar, o cümlədən aşkar seksual hərəkətlərdə iştirak edən yetkinlik yaşına çatmayan şəxsi əks etdirən realistik təsvirlər başa duşulur.

Cinayət Məcəlləsinin 171-1.1-ci maddəsinə görə uşaq pornoqrafiyasını yayma, reklam etmə, satma, başqasına vermə, göndərmə, təklif etmə, əldə edilməsinə şərait yaratma, yaxud yaymaq və ya reklam etmək məqsədilə hazırlama, əldə etmə və ya saxlama səkkiz min manatdan on min manatadək miqdarda cərimə və ya beş ilədək müddətə azadlıqdan məhrum etmə ilə cəzalandırılır. Ağırlaşdırıcı hallarda isə bu əmələ görə azadlıqdan məhrum etmə cəzası maksimum 8 il müəyyən olunmuşdur.

Göründüyü kimi, informasiya əsrinin tələbləri baxımından qanunvericiliyə edilmiş bu dəyişikliklər mütərəqqi xarakter daşımaqla, ictimai qaydanın qorunmasına, İnternet cinayətkarlığının azaldılmasına, dövlətin, cəmiyyətin və ya ayrı-ayrı şəxslərin qanunla qorunan maraqlarına zərər vurulmasının qarşısının alınmasına xidmət edir.

Beləliklə, internetdə kibercinayəkarlıq ən geniş yayılmış beynəlxalq xarakterli qeyri-hüquqi əməllərdən hesab edildiyindən, bu cinayətlərin xarakteri və diapazonu sosial-iqtisadi inkişafdan və İKT üzrə yeniliklərdən asılı olaraq dəyişir və genişlənir. Eyni zamanda, bu cinayətlərlə mübarizə müasir beynəlxalq hüquqda daha aktual əhəmiyyət kəsb edir. Müasir dövrdə "elektron hökumət", "elektron imza", "elektron ticarət" strategiyalarının inkişafını nəzərə alaraq, telekommunikasiyaların, rəqəmsal texnologiyaların, kompüter və internet şəbəkələrinin, bankomatların, ödəniş kartlarının və s. cinayətkar məqsədlərlə istifadəsinin mümkünlüyü baxımından bu cinayətlər həm milli hüquqi, həm də beynəlxalq hüquqi tənzimetmənin predmetini təşkil edir.

İKT-lərin inkişafı qanunvericiliyin bütün sahələrinin təkmilləşdirilməsini şərtləndirir, milli və beynəlxalq normalarda yeni hüquq pozuntusu tərkiblərinin təsbit olunmasını ehtiva edir. Ona görə də, elektron informasiyaların yayılması ilə əlaqədar inzibati xətalar digər hüquq pozuntularından, xüsusilə yaranan məsuliyyət baxımından cinayətlərdən tamamilə fərqlənir. Bu fərq başlıca olaraq ondan ibarətdir ki, cinayət inzibati xətaya nisbətən daha böyük ictimai təhlükəyə malikdir.

Şəxsin inzibati məsuliyyətə cəlb edilməsi zərurəti ondan yaranır ki, həmin hüququ pozan şəxs tərəfindən törədilmiş əməl dövlətə və cəmiyyətə ziyan vurmaqla, müəyyən ictimai münasibətlərə qəsd etmiş olur.

İnzibati hüquqpozmaların qarşısının alınmasına və onlarla mübarizəyə dair münasibətləri nizamlayan sistemləşdirilmiş qanunvericilik aktı Azərbaycan Respublikasının İnzibatı Xətalar Məcəlləsidir. Həmin Qanunun 16-cı fəsli İnformasiyadan istifadə edilməsi, onun yayılması və mühafizəsi qaydaları əleyhinə olan inzibati xətalara həsr edilmişdir.

Qanuna əsasən bilavasitə informasiya ehtiyatlarından düzgün istifadə edilməsi ilə bağlı fiziki və hüquqi şəxslər, habelə vəzifəli şəxslər üçün konkret məsuliyyətin hüdudları müəyyən olunaraq, müvafiq cərimə cəzası müəyyən edilmişdir. Bu kateqoriya inzibati hüquq pozuntularına aiddir: informasiya ehtiyatlarından istifadə qaydalarının pozulması (maddə 181), ətraf mühitə dair informasiyanın verilməsinin qanuna zidd məhdudlaşdırılması (maddə 181-1), məxfiləşdirilmiş məlumatların məxfiliyinin açılması haqqında sorğuya mahiyyəti üzrə baxmaqdan boyun qaçırılması (maddə 181-2), informasiya əldə etmək haqqında qanunvericiliyin pozulması (maddə 181-3) Fərdi məlumatlar haqqında qanunvericiliyin pozulması gizli qaydada informasiya alınması üçün nəzərdə tutulmuş texniki vasitələri satış məqsədi olmadan qanunsuz əldə etmə (maddə 181-4).[107]

Digər tərəfdən, informasiyanın mühafizəsi qaydalarının pozulması və informasiya sistemlərinin sertifikatlaşdırılmaması da qanuna görə inzibati məsuliyyətə səbəb olur.

Bundan əlavə, Məcəllənin 183-1-ci maddəsi sertifikatlaşdırılmamış elektron imza və elektron sənəd dövriyyəsi vasitələrindən istifadə edilməsinə görə fiziki şəxslər üçün iyirmi manatdan iyirmi beş manatadək miqdarda, vəzifəli şəxslərə əlli beş manatdan yetmiş manatadək miqdarda, hüquqi şəxslərə isə iki yüz manatdan iki yüz əlli manatadək miqdarda cərimə nəzərdə tutur. Eyni zamanda, elektron sənədlərin saxlanmasında, ötürülməsində, qəbulunda vasitəçinin informasiya sistemindən etibarlı istifadəni təmin edən texnika və texnologiyalara, bilikli, təcrübəli və səriştəli işçi heyətə, xidmət göstərilmiş elektron sənədlərin vaxtını və mənbəyini teyin etməyə imkan verən şəraitə, həmin elektron sənədlərin vaxtı və mənbəyi haqqında informasiyanın saxlanması üçün etibarlı sistemə malik olmamasına görə də, inzibati məsuliyyət müəyyən edilərək inzibati tənbeh tədbirləri nəzərdə tutulmuşdur.

Göründüyü kimi, şəbəkə istifadəçilərinə inzibati məsuliyyətin subyektləri kimi Azərbaycan Respublikasının İnzibatı Xətalar Məcəlləsi ilə nəinki, informasiya ehtiyatlarından düzgün istifadə olunmaması ilə bağlı, eyni zamanda qanunvericiliyə edilmiş son dəyişikliklərə əsasən elektron imza və elektron sənədlərdən qaydalara

[107] Azərbaycan Respublikasının İnzibatı Xətalar Məcəlləsi, http://eqanun.gov.az

uyğun istifadə edilməməsinə görə də inzibati tənbeh tədbirləri tətbiq olunacaq. Bu həm fiziki və hüquqi şəxslərə, həm də vəzifəli şəxslərə aiddir.

NƏTİCƏ

Bu kitabda kibercinayətlərin anlayışı və əsas xüsusiyyətlərinin nəzəri araşdırılması, habelə milli və beynəlxalq hüquq normalarının qarşılıqlı təhlili nəticəsində yekun olaraq aşağıdakı təklif və müddəaların irəli sürülməsini mümkün hesab edirik:

1) Müasir transmilli hüquqi konsepsiyalara əsasən kompüterlərdə, kompüter şəbəkələrində və ya kiberməkanda baş verən hüquqazidd hərəkət və hərəkətsizlikləri ifadə etmək üçün müxtəlif terminlərin – "kompüter cinayətləri", "kibercinayətlər", "informasiya cinayətləri", "yüksək texnologiya cinayətləri", "kompüter informasiyasına aid cinayət" – istifadə edilməsinə baxmayaraq, "kibercinayətlər" məfhumuna üstünlük verilməsi məqsədəuyğun sayılmışdır.

2) Kibercinayətin anlayışının konvension əsaslı imperativ beynəlxalq hüquq normalarında müəyyən edilməsinin zəruriliyi əsaslandırılaraq, ona aşağıdakı anlayışın verilməsi təklif edilir: "Kibercinayətlər dedikdə kompüterlərdən, kompüter proqramlarından, kompüter şəbəkələrindən, o cümlədən İnternet və sosial şəbəkələrdən, informasiya resurslarından və informasiya daşıyıcılarının digər qurğularından qanunsuz istifadə nəticəsində kompüter və informasiya sistemlərinin dağıdılması ilə nəticələnən və əhəmiyyətli zərərlə xarakterizə olunan, virtual məkanda qəsdən törədilən, cəzalandırılmalı, hüquqazidd ictimai təhlükəli hərəkət və hərəkətsizlik başa düşülür".

3) Kibercinayətkarlıq haqqında Konvensiyaya (və ona Əlavə Protokola) görə kibercinayətlərin beş əsas qrupa bölgüsü müasir beynəlxalq hüquq normaları baxımından və xarici ölkələrin milli hüquq sistemlərinə nəzərən optimal və təcrübi əhəmiyyətli təsnifat kimi qəbul edilir.

4) Kibercinayətlərə münasibətdə müasir beynəlxalq hüquqda "real" və "kiber" hüquq nəzəriyyələri arasında əsas fərqlərə diqqət yetirilir. "Real" hüquq tərəfdarları qeyd edirlər ki, kibercinayətkarlıq – gerçək dünyada da məlumdur, sadəcə kompüterin köməyi ilə həyata keçirilir. Cinayətkarlıq olduğu kimi qalır, yalnız vasitələr dəyişir.

"Kiber" hüquq tərəfdarları isə hesab edirlər ki, kibercinayətkarlığın unikal elementləri ona xüsusi yanaşma tələb edir, o cümlədən qanunların tətbiqi və cinayətkarlığın profilaktikasında bu nəzərə alınmalıdır.

5) "Kibercinayət" və "kiberterrorizm" anlayışları fərqləndirilməklə hər biri müstəqil cinayət tərkibi olaraq təsnif edilir və kompüterlər, kompüter şəbəkələri, İnternet, sosial şəbəkələr yalnız "kiberterrorizm"in törədilməsində yardımçı vasitələr kimi qəbul edilir.

6) Törədilən hər hansı istənilən dağıdıcı cinayətkar fəaliyyət məhz kompüter sistemlərinin və şəbəkələrinin, habelə onlarda mövcud olan informasiyaların məhv edilməsinə yönəlmişdirsə, həmin əməlin törədilmə miqyasından və zahiri əlamətlərindən asılı olmayaraq, onlar kibercinayətlər kateqoriyasına aid edilir.

7) Kompüter sistemləri və ya şəbəkəsindən, o cümlədən İnternetdən vasitə kimi istifadə olunaraq, mütəşəkkil cinayətkar qruplar və ayrıca şəxslər konkret cinayət məqsədlərini reallaşdırmağa cəhdlər etmişlərsə, bu zaman qeyd olunan vasitələr həmin cinayət əməllərinin törədilməsi üçün yalnız köməkçi alət qismində çıxış edəcəkdir. Burada ayrıca növ kimi təsnifləşdiriləcək hansısa kibercinayətdən yox, konkret tərkibi olan müstəqil cinayət əməlindən danışmaq mümkündür.

ƏLAVƏLƏR

Azərbaycan Respublikasının Cinayət Məcəlləsindən çıxarış

Otuzuncu fəsil[672]

KİBERCİNAYƏTLƏR

Maddə 271. Kompüter sisteminə qanunsuz daxil olma

271.1. Kompüter sisteminə və ya onun hər hansı bir hissəsinə daxil olmaq hüququ olmadan həmin sistemə və ya onun hər hansı bir hissəsinə mühafizə tədbirlərini pozmaqla, yaxud burada saxlanılan kompüter məlumatlarını ələ keçirmək və ya başqa şəxsi niyyətlə qəsdən daxil olma - iki ilədək muddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə *iki min manatdan dord min* manatadək miqdarda cərimə və ya iki ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

[673]

271.2. Eyni əməllər:

271.2.1. təkrar törədildikdə;

271.2.2. qabaqcadan əlbir olan bir qrup şəxs, mutəşəkkil dəstə və ya cinayətkar birlik (təşkilat) tərəfindən törədildikdə;

271.2.3. vəzifəli şəxs tərəfindən öz qulluq mövqeyindən istifadə etməklə törədildikdə – üç ilədək muddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə *dord min manatdan altı min* manatadək miqdarda cərimə və ya iki ildən dord ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır.[674]

271.3. Bu Məcəllənin 271.1 və ya 271.2-ci maddələrində nəzərdə tutulmuş əməllər ictimai əhəmiyyətli infrastruktur obyektinin kompüter sisteminə və ya onun hər hansı bir hissəsinə münasibətdə törədildikdə – üç ilədək muddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə dord ildən altı ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

Qeyd:

1. Bu Məcəllənin 271-273-2-ci maddələrində “kompüter sistemi” dedikdə, müvafiq proqramlara uyğun olaraq verilənlərin avtomatlaşdırılmış işlənməsini həyata keçirən hər hansı qurğu və ya birbirinə qoşulmuş və ya əlaqələndirilmiş qurğular qrupu başa duşulur.

2. Bu Məcəllənin 271-273-2-ci maddələrində “kompüter məlumatları” dedikdə, kompüter sistemində işlənməsi, emal edilməsi üçün yararlı olan istənilən informasiya (faktlar, məlumatlar, proqramlar və anlayışlar) başa duşulur.

3. Bu Məcəllənin 271-273-cu maddələrində “ictimai əhəmiyyətli infrastruktur obyekti” dedikdə, dövlət və cəmiyyət üçün mühüm əhəmiyyət kəsb edən xidmətlər göstərən dövlət idarə, muəssisə, təşkilatları, qeyri-hökumət təşkilatları (ictimai birliklər və fondlar), kredit təşkilatları, sığorta şirkətləri, *qiymətli kağızlar bazarında lisenziyalaşdırılan şəxslər,* investisiya fondları *və bu fondların idarəciləri* başa duşulur.[675]

M a d d ə 272. Kompüter məlumatlarını qanunsuz ələ keçirmə

272.1. Kompüter sisteminə, kompüter sistemindən və ya bu sistem daxilində oturulən ümumi istifadə üçün nəzərdə tutulmayan kompüter məlumatlarının, o cümlədən bu cür kompüter məlumatlarının daşıyıcısı olan kompüter sistemlərinin elektromaqnit şualanmasının, buna hüququ olmayan şəxs tərəfindən texniki vasitələrdən istifadə etməklə qəsdən ələ keçirilməsi – iki ilədək muddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə *iki min manatdan dord min* manatadək miqdarda cərimə və ya iki ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır. [676]

272.2. Eyni əməllər:

272.2.1. təkrar törədildikdə;

272.2.2. qabaqcadan əlbir olan bir qrup şəxs, mutəşəkkil dəstə və ya cinayətkar birlik (təşkilat) tərəfindən törədildikdə;

272.2.3. vəzifəli şəxs tərəfindən öz qulluq mövqeyindən istifadə etməklə törədildikdə – üç ilədək muddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə *dord min manatdan altı min* manatadək miqdarda cərimə və ya iki ildən dord ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır.[677]

272.3. Bu Məcəllənin 272.1 və ya 272.2-ci maddələrində nəzərdə tutulmuş əməllər ictimai əhəmiyyətli infrastruktur obyektinin kompüter sisteminə və ya onun hər hansı bir hissəsinə münasibətdə törədildikdə – üç ilədək muddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə dord ildən altı ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

M a d d ə 273. Kompüter sisteminə və ya kompüter məlumatlarına qanunsuz mudaxilə

273.1. Kompüter məlumatlarının qəsdən zədələnməsi, silinməsi, korlanması, dəyişdirilməsi və ya bloklanması buna hüququ olmayan şəxs tərəfindən törədilməklə əhəmiyyətli zərər vurulmasına səbəb olduqda – üç ilədək muddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə *iki min manatdan dord min* manatadək miqdarda cərimə və ya iki ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

273.2. Kompüter məlumatlarının daxil edilməsi, oturulməsi, zədələnməsi, silinməsi, korlanması, dəyişdirilməsi və ya bloklanması yolu ilə kompüter sisteminin işləməsinə buna hüququ olmayan şəxs tərəfindən qəsdən ciddi maneə törədilməsi – üç ilədək muddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə *iki min manatdan dord min* manatadək miqdarda cərimə və ya iki ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır. [678]

273.3. Bu Məcəllənin 273.1 və ya 273.2-ci maddələrində nəzərdə tutulmuş əməllər:

273.3.1. təkrar törədildikdə;

273.3.2. qabaqcadan əlbir olan bir qrup şəxs, mutəşəkkil dəstə və ya cinayətkar birlik (təşkilat) tərəfindən törədildikdə;

273.3.3. vəzifəli şəxs tərəfindən öz qulluq mövqeyindən istifadə etməklə törədildikdə – üç ilədək muddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə *dord min manatdan altı min* manatadək miqdarda cərimə və ya iki ildən dord ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır.[679]

273.4. Bu Məcəllənin 273.1-273.3-cu maddələrində nəzərdə tutulmuş əməllər ictimai əhəmiyyətli infrastruktur obyektlərinin kompüter sisteminə və ya onun hər hansı bir hissəsinə münasibətdə törədildikdə – üç ilədək muddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə dord ildən altı ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

Qeyd:

1. Bu fəslin maddələrində “əhəmiyyətli zərər” dedikdə, ictimai təhlükəli əməl nəticəsində min manatdan artıq olan məbləğdə ziyan vurulması və ya dövlətin, cəmiyyətin və ya ayrı-ayrı şəxslərin qanunla qorunan maraqlarına digər mühüm zərərin vurulması başa duşulur.

2. Bu Məcəllənin 273.2-ci maddəsində “kompüter sisteminin işləməsinə ciddi maneə törədilməsi” kompüter sisteminin normal fəaliyyətinin elə bir pozulmasıdır ki, kompüter sisteminin sahibinin və ya istifadəcisinin bu sistemdən istifadə etmək və ya digər kompüter sistemləri ilə məlumatları mübadilə etmək imkanını mühüm dərəcədə məhdudlaşdırsın.

M a d d ə 273-1. Kibercinayətlərin törədilməsi üçün hazırlanmış vasitələrin dövriyyəsi

273-1.1. Hazırlanmasının və ya uyğunlaşdırılmasının əsas məqsədi bu Məcəllənin 271-273-cü maddələrində nəzərdə tutulmuş cinayətlərin törədilməsi olan qurğuların və ya kompüter proqramlarının istehsalı, həmin cinayətlərin törədilməsi məqsədi ilə idxalı, istifadə üçün əldə olunması, saxlanılması, satışı, yayılması və ya əldə edilməsinə digər formalarda şərait yaradılması, əhəmiyyətli zərər

vurduqda – iki ilədək muddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə *üç min manatdan beş min* manatadək miqdarda cərimə və ya iki ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

273-1.2. Kompüter parollarının, giriş kodlarının və ya kompüter sisteminə, yaxud onun hər hansı bir hissəsinə hüququ olmadan daxil olmağa imkan verən digər analoji məlumatların bu Məcəllənin 271—273-cü maddələrində nəzərdə tutulmuş cinayətlərin törədilməsi məqsədilə istehsalı, saxlanılması və ya istifadə üçün əldə olunması, əhəmiyyətli zərər vurduqda – iki ilədək muddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə *üç min manatdan beş min* manatadək miqdarda cərimə və ya iki ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

273-1.3. Kompüter parollarının, giriş kodlarının və ya kompüter sisteminə, yaxud onun hər hansı bir hissəsinə hüququ olmadan daxil olmağa imkan verən digər analoji məlumatların bu Məcəllənin 271—273-cü maddələrində nəzərdə tutulmuş cinayətlərin törədilməsi məqsədi ilə satışı, yayılması və ya onların əldə edilməsinə digər formalarda şərait yaradılması – iki ilədək muddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə *üç min manatdan beş min* manatadək miqdarda cərimə və ya iki ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır.[680]

273-1.4. Bu Məcəllənin 273-1.1-273-1.3-cü maddələrində nəzərdə tutulmuş əməllər:

273-1.4.1. təkrar törədildikdə;

273-1.4.2. qabaqcadan əlbir olan bir qrup şəxs, mutəşəkkil dəstə və ya cinayətkar birlik (təşkilat) tərəfindən törədildikdə;

273-1.4.3. vəzifəli şəxs tərəfindən öz qulluq mövqeyindən istifadə etməklə törədildikdə – üç ilədək muddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə *beş min manatdan səkkiz min* manatadək miqdarda cərimə və ya iki ildən dord ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır.[681]

M a d d ə 273-2. Kompüter məlumatlarının saxtalaşdırılması

Saxtalaşdırılmış kompüter məlumatlarını autentik (həqiqi) kompüter məlumatları kimi qələmə vermək və ya istifadə etmək məqsədilə kompüter məlumatlarını müvafiq hüquq olmadan qəsdən daxil etmə, dəyişdirmə, silmə və ya bloklama, bu əməllər ilkin kompüter məlumatlarının autentikliyinin (həqiqiliyinin) pozulmasına səbəb olduqda – üç ilədək muddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə *iki min manatdan dord min* manatadək miqdarda cərimə və ya iki ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır.[682]

[672] 29 iyun 2012-ci il tarixli 408-IVQD nomrəli Azərbaycan Respublikasının Qanunu (“Respublika” qəzeti, 17 iyul 2012-ci il, № 156, “Azərbaycan” qəzeti 18 iyul 2012-ci il, № 157, Azərbaycan Respublikasının Qanunvericilik Toplusu, 2012-ci il,

№ 07, maddə 669) ilə Məcəllənin otuzuncu fəsli yeni redaksiyada verilmişdir.

Əvvəlki redaksiyada deyilirdi:

30-cu fəsil

KOMPÜTER INFORMASIYASI SAHƏSINDƏ CINAYƏTLƏR

M a d d ə 2 7 1. Kompüter informasiyasına qanunsuz olaraq daxil olma

271.1. Qanunla qorunan kompüter informasiyasına, yəni maşın daşıyıcılarında, elektron-hesablayıcı maşınlarda (EHM), elektron-hesablayıcı maşınlar sistemində və ya onların şəbəkələrində olan infomasiyalara qanunsuz olaraq daxil olma, bu hərəkətlər informasiyanın məhv edilməsi, təcrid olunması, modifikasiya olunması, onun surətinin çıxarılması, yaxud EHM-in işinin, sisteminin və ya onların şəbəkəsinin fəaliyyətinin pozulmasına səbəb olduqda — beş yüz manatdan min manatadək miqdarda cərimə və ya bir ilədək muddətə islah işləri və ya bir ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır.[672]

271.2. Eyni əməllər:

271.2.1. qabaqcadan əlbir olan bir qrup şəxs tərəfindən törədildikdə;

271.2.2. vəzifəli şəxs tərəfindən öz qulluq mövqeyindən istifadə etməklə yaxud elektronhesablayıcı maşınlara, elektron-hesablayıcı maşınlar sisteminə və ya onların şəbəkələrinə daxil olmaq hüququ olan şəxs tərəfindən törədildikdə;

271.2.3. kulli miqdarda ziyan vurmaqla törədildikdə— min manatdan iki min manatadək miqdarda cərimə və ya iki ilədək muddətə islah işləri və ya üç ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır.[672]

M a d d ə 2 7 2 . Elektron-hesablayıcı maşınlar üçün ziyan verici proqramlar yaratma, onlardan istifadə etmə və ya onları yayma

272.1. İnformasiyanın icazəsiz məhvinə, təcrid olunmasına, modifikasiya edilməsinə və ya surətinin çıxarılmasına, EHM, EHM sisteminin və ya onların şəbəkələrinin işinin pozulmasına səbəb ola biləcəyini bilə-bilə EHM proqramlarını yaratma və ya mövcud proqramlara dəyişikliklər etmə, habelə belə proqramlardan və ya belə proqramlarla yuklənmiş maşın daşıyıcılarından istifadə etmə və ya onları yayma— beş yüz manatdan min manatadək miqdarda cərimə edilməklə iki ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır.[672]

272.2. Eyni əməllər ehtiyatsızlıqdan ağır nəticələrə səbəb olduqda— iki ildən beş ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

M a d d ə 273 . Elektron hesablayıcı maşınların (EHM), EHM sisteminin və ya onların şəbəkələrinin istismarı qaydalarını pozma

273.1. EHM-lə, EHM sistemi ilə və ya onların şəbəkələri ilə işləməyə icazəsi olan şəxs tərəfindən EHM-in, EHM sisteminin və ya onların şəbəkələrinin istismarı qaydalarının pozulması nəticəsində EHM-dəki qanunla

qorunan məlumatların məhvi, təcrid olunması və ya modifikasiya edilməsi əhəmiyyətli zərər vurulmasına səbəb olduqda – üç ilədək muddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum etmə və ya yüz altmış saatdan iki yüz saatadək ictimai işlər və ya bir ilədək muddətə islah işləri və ya iki ilədək muddətə azadlığın məhdudlaşdırılması ilə cəzalandırılır.[672]

273.2. Eyni əməllər ehtiyatsızlıqdan ağır nəticələrə səbəb olduqda – iki ilədək muddətə islah işləri və ya üç ilədək muddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

[673] 31 may 2017-ci il tarixl i 707-VQD nomrəli Azərbaycan Respublikasının Qanunu (“Azərbaycan” qəzeti, 19 iyul 2017-ci il, № 153, Azərbaycan Respublikasının Qanunvericilik Toplusu, 2017-ci il, № 7, maddə 1268) ilə 271.1-ci maddənin sanksiyasında “min manatdan iki min” sözləri “iki min manatdan dörd min” sözləri ilə əvəz edilmişdir.

[674] 31 may 2017-ci il tarixl i 707-VQD nomrəli Azərbaycan Respublikasının

Qanunu (“Azərbaycan” qəzeti, 19 iyul 2017-ci il, № 153, Azərbaycan Respublikasının Qanunvericilik Toplusu, 2017-ci il, № 7, maddə 1268) ilə 271.2-ci maddənin sanksiyasında “iki min manatdan üç min” sözləri “dörd min manatdan altı min” sözləri ilə əvəz edilmişdir.

[675] 7 aprel 2017-ci il tarixl i 563-VQD nomrəli Azərbaycan Respublikasının

Qanunu (“Azərbaycan” qəzeti, 19 may 2017-ci il, №106, Azərbaycan Respublikasının Qanunvericilik Toplusu, 2017-ci il, № 5, maddə 694) ilə 271-ci maddəsinin “Qeyd” hissəsinin 3-cü bəndinə “fondları” sözündən sonra “və bu fondların idarəciləri” sözləri əlavə edilmişdir.

7 aprel 2017-ci il tarixl i 575-VQD nomrəli Azərbaycan Respublikasının Qanunu (“Azərbaycan” qəzeti, 23 may 2017-ci il, № 109, Azərbaycan Respublikasının Qanunvericilik Toplusu, 2017-ci il, № 5, maddə 702) ilə 271-ci maddəsinin “Qeyd” hissəsinin 3-cü bəndinə “sığorta şirkətləri,” sözlərindən sonra “qiymətli kağızlar bazarında lisenziyalaşdırılan şəxslər,” sözləri əlavə edilmişdir.

[676] 31 may 2017-ci il tarixl i 707-VQD nomrəli Azərbaycan Respublikasının

Qanunu (“Azərbaycan” qəzeti, 19 iyul 2017-ci il, № 153, Azərbaycan Respublikasının Qanunvericilik Toplusu, 2017-ci il, № 7, maddə 1268) ilə 272.1-ci maddənin sanksiyasında “min manatdan iki min” sözləri “iki min manatdan dörd min” sözləri ilə əvəz edilmişdir.

[677] 31 may 2017-ci il tarixl i 707-VQD nomrəli Azərbaycan Respublikasının Qanunu (“Azərbaycan” qəzeti, 19 iyul 2017-ci il, № 153, Azərbaycan Respublikasının Qanunvericilik Toplusu, 2017-ci il, № 7, maddə 1268) ilə 272.2-ci maddənin sanksiyasında “iki min manatdan üç min” sözləri “dörd min manatdan altı min” sözləri ilə əvəz edilmişdir.

[678] 31 may 2017-ci il tarixl i 707-VQD nomrəli Azərbaycan Respublikasının

Qanunu (“Azərbaycan” qəzeti, 19 iyul 2017-ci il, № 153, Azərbaycan Respublikasının Qanunvericilik Toplusu, 2017-ci il, № 7, maddə 1268) ilə 273.1-ci və 273.2-ci maddələrin sanksiyasında “min manatdan iki min” sözləri “iki min manatdan dörd min” sözləri ilə əvəz edilmişdir.

[679] 31 may 2017-ci il tarixl i 707-VQD nomrəli Azərbaycan Respublikasının

Qanunu (“Azərbaycan” qəzeti, 19 iyul 2017-ci il, № 153, Azərbaycan Respublikasının Qanunvericilik Toplusu, 2017-ci il, № 7, maddə 1268) ilə 273.3-cü maddənin sanksiyasında “min manatdan iki min” sözləri “dörd min manatdan altı min” sözləri ilə əvəz edilmişdir.

[680] 31 may 2017-ci il tarixl i 707-VQD nomrəli Azərbaycan Respublikasının

Qanunu (“Azərbaycan” qəzeti, 19 iyul 2017-ci il, № 153, Azərbaycan Respublikasının Qanunvericilik Toplusu, 2017-ci il, № 7, maddə 1268) ilə 273-1.1-ci, 273-1.2-ci və 273-1.3-cü maddələrin sanksiyasında “iki min manatdan üç min” sözləri “üç min manatdan beş min” sözləri ilə əvəz edilmişdir.

[681] 31 may 2017-ci il tarixl i 707-VQD nomrəli Azərbaycan Respublikasının

Qanunu (“Azərbaycan” qəzeti, 19 iyul 2017-ci il, № 153, Azərbaycan Respublikasının Qanunvericilik Toplusu, 2017-ci il, № 7, maddə 1268) ilə 273-1.4-cü maddənin sanksiyasında “üç min manatdan dörd min” sözləri “beş min manatdan səkkiz min” sözləri ilə əvəz edilmişdir.

[682] 31 may 2017-ci il tarixl i 707-VQD nomrəli Azərbaycan Respublikasının

Qanunu (“Azərbaycan” qəzeti, 19 iyul 2017-ci il, № 153, Azərbaycan Respublikasının Qanunvericilik Toplusu, 2017-ci il, № 7, maddə 1268) ilə 273-2-ci maddənin sanksiyasında “min manatdan üç min” sözləri “iki min manatdan dörd min” sözləri ilə əvəz edilmişdir.

İstifadə olunmuş ədəbiyyat siyahısı:

1. İlham Əliyev Avropa Şurası Parlament Assambleyasının sessiyasında çıxış etmişdir, 24 iyun 2014, http://www.president.az

2. Azərbaycan Respublikası Prezidentinin İşlər İdarəsinin Prezident Kitabxanası, Muraciətlər, Bəyanatlar, Tədbirlər. http://www.preslib.az/

3. Azərbaycan Respublikası Ədliyyə Nazirliyi və Tacikistan Respublikası Ədliyyə Nazirliyi arasında əməkdaşlıq haqqında Saziş, http://justice.gov.az

4. Əzizov R. Azərbaycanda elektron dövlətin perspektivləri. Azərbaycan qəzeti. 2009.7 fevral.-S.9.

5. Məcidli S. T. İnternet hüququ və etikası. Dərs vəsaiti. Bakı: “Elm və təhsil” nəşriyyatı, 2013. S.115, 224 səh.

6. Алавердов О.С. Международное сотрудничество в области борьбы с интернет-преступностью, Общество и право, 2010. http://www.juristlib.ru

7. Борьба с киберпреступностью – проблема всего информационного сообщества. http://www.rusnauka.com

8. Васильев В.А. Проблемы развития законодательства в сфере борьбы с киберпреступностью // Материалы Международной практической конференции по борьбе с киберпреступностью и кибертерроризмом 19 – 20 апреля 2006 г., Москва. с.57.

9. Доклад Генерального Секретаря ООН "Воздействие организованной преступной деятельности на общество в целом" // Материалы Комиссии ООН по предупреждению преступности и уголовному правосудию. Вена, L7CN 15/1993/3.

10. Договорно-правовая деятельность в борьбе с преступностью в сфере высоких технологий. http://bibliofond.ru

11. Костенко, Н.И. Правовые механизмы международного сотрудничества в правоохранительной сфере. Право и политика. 2005. № 8. // КонсультантПлюс: Версия Проф. Технология 3000 / ООО “ЮрСпектр”. М., 2009

12. Международное право и борьба с преступностью: сб-к документов / Составители: А.В. Змеевский, Ю.М. Колосов, Н.В. Прокофьев. М.: Международные отношения, 2004. 720 с.

13. Иногамова-Хегай Л.В. Международное уголовное право. СПб.: Издательство “Юрцентр Пресс”, 2003. 495 с.

14. Кибальник А.Г. Современное международное уголовное право: понятие, задачии принципы. СПб: Юрцентр Пресс. 2003. 252 с.

15. Комметарий к Уголовному Кодексу Российской Федерации. М., Издателская группа ИНФРА М-НОРМА, 1996. 814. с.

16. Костенко Н. И. Международное уголовное право: современное теоретическое проблемы. М.: “Юрлитинформ”, 2004. 448 с.

17. Костенко Н. И. Международная уголовная юстиция. Проблемы развития. М.: РосКонсульт, 2002. 448 с.

18. Крылов Н.Е. Уголовное право современных зарубежных стран (Англии, США, Франции, Германии). Учебное пособие. М.; Зерцало, 1997. 192 с.

19. Курс международного права в семи томах. Т.3: Основные институты международного права, Отв. ред. Н.А. Ушаков. М.: “Наука”, 1990. 326 с.

20. Курс международного права. В семи томах. Т. 6. М., 1992, 287 с.

21. Лукашук И.И. Международное право. Общая часть: Учебник. М.: Изд-во “БЕК”, 2000. 432 с.

22. Лукашук И.И. Международное право. Особенная часть: Учебник. М.: Изд-во “БЕК”, 2000. 456 с.

23. Лукашук И.И. Международное право. Особенная часть. М. Издотелство БЕК, 1998. 374 с.

24. Лукашук И.И., Наумов А.В. Международное уголовное право. М.: СПАРК. 1999. 287 с.

25. Малиновский А.А. Сравнительное правоведение в сфере уголовного права. М.: Международ. отношения. 2002. 374 с. 305

26. Международное право. Учебник. Ответственный редактор К.А.Бекяшев. М.“Проспект”, 2007. 784 с.

27. Международное право. Учебник. Под редакцией А.А.Ковалева, С.В.Черниченко. Издательство. Омега-Л. М. 2006. 832 с.

28. Международное право. Учебник. Ответственный редактор Ю.М.Колосов, Э.С.Кривчикова. М., Международные отношения, 2005. 720 с.

29. Международное право. М., Международные отношения, 1998. 457с.

30. Международное право. Учебник для вузов. Ответственный редактор д.ю.н. проф. О.И.Тиунов. 4-ое изд., перераб. и доп. М.: Норма, 2006. 720 с.

31. Международное публичное право. Сборник документов.М.1996.т.2.349 с.

32. Международное уголовное право. Под общей редакцией академика В.Н.Кудрявцева. Москва “Наука” 1999. 264 с.

33. Международные акты о правах человека. Сборник документов. Сост. д.ю.н., проф. В.Е.Карташкин. д.ю.н., проф. Е.А.Лукашева, 2-ое изд.. доп. М.; Издательства НОРМА, 2002, 944с.

34. Мюллерсон Р.А. Права человека: идеи, нормы, реальность. М., 1991. 476 с.

35. Уголовное право. Особенная часть. Ответственный редактор Козаченко И.Я. М. 2001. 937 с.

36. Черниченко С.В. Теория международного права. Т. 2: Старые и новые теоретические проблемы. М.: Изд-во “НИМП”, 1999. 645 с.

37. Мороз Наталия Олеговна. Международно-правовое сотрудничество в борьбе с преступностью в сфере высоких технологий. Автореферат диссертации на соискание ученой степени кандидата юридических наук. Минск, 2014. 23 с.

38. Мороз Наталия Олеговна, Международно-правовое сотрудничество в борьбе с киберпреступностью в рамках Европейского Союза и Совета Европы. http://www.pac.by

39. Повышев Владислав. Борьба с киберпреступностью и кибертерроризмом. Томский государственный университет. http://tmun.utmn.ru

40. Прокофьев Константин Викторович "Международно правовыепроблемы обеспечения международной информационной безопасности всети Интернет", Автореферат, Москва, 2009, с. 6.

41. Основные тезисы выступления заместителя Генерального прокурора Российской Федерации А.Г. Звягинцева на Байкальской международной конференции прокуроров (26.08.2014) http://www.genproc.gov.ru

42. Талимончик, В. П. Роль двусторонних договоров, заключенных Российской Федерацией, в международном информационном обмене //Правоведение. 2006. № 5. С. 105-120

43. Akehurst's Modern Introduction to International Law, By Malanczuk P. Routlege. 1997. p. 548

44. Antonio Cassese, International Criminal Law. Oxford University Press. 2003. p.543

45. Bassiouni M. Cherif, Introduction to International Criminal Law. Ardsley, N.Y.: Transnational Publishers, 2003. p. 822

46. Bassiouni M. Cherif. The Statute of the International Criminal Court and Related Instruments: Legislative History, 1994-2000. Ardsley, NY: Transnational Publishers, forthcoming 2001. Approx. 1400-1500p. 2v.

47. Bassiouni M. Cherif, "The Time Has Come for an International Criminal Court", 1 Indiana International and Comparative Law Review 1-43 (1991). P 56.

48. Evans M. International Law. Oxford: Oxford University Press. 2003. pp 343.

49. Hays Batler A. The Doctrine of Universal Jurisdiction: A Review of the Literature, Criminal Law Forum. 2000. Vol. 11. N3. 354 p.

50. International Crimes, Peace, and Human Rights: The Role of the International Criminal Court. Dinah Shelton ed., Ardsley, NY: Transnational Publishers, 2000. 370 p.

51. Kelsen H. Prinsiples of international law. N.J., 1952, 374 p.

52. Kittichaisaree Kriangsak, International criminal law, Oxford 2001, pp.657.

53. Lyal S.Sunga, "The Crimes within the Jurisdiction of the International Criminal Court. European Journal of Crime, Criminal Law, and Criminal Justice. Part II, Articles 5-10. v.6, no.4, 1998. pages 61-83.

54. Nina H.B. Jorgensen. The responsiblity of states of international crimes. Oxford University Press. 2000. p.376

55. Salmon J.J.A., Droit des gens, Tome III, Bruxelles, 1986-1987, 437 p.

56. Shaw M.N. International law. New York, Cambridge University Press, 4th edition, 1997, 452 p.

57. Supranational Criminal Law: A System Sui Generis Roelof Haveman, Olga Kavran, Julian Nicholls. Anwerp-Oxford-New York. Intersentia, 2003. 370 p.

58. The Rome Statute of the International Criminal Court: A Commentary. Antonio Cassese, Paola Gaeta, & John R.W.D. Jones general eds., Albin Eser, Giorgio Gaja, Philip Kirsch, Alain Pellet, & Bert Swart board of advisors, Oxford University Press, 2002. 324p.

59. William A. Schabas. An Introduction to the International Criminal Court. Cambridge: Cambridge University Press. 2001. p. 406.

60. A Strong European Neighbourhood Policy, http://www.ec.europa.eu

61. Crimes within the Court's Jurisdiction http://www.un.org

62. Dunn Cavelty, Myriam. The Militarisation of Cyber Security as a Source of Global Tension February 1, 2012. Strategic Trends Analysis, Zurich, Mockli, Daniel,Wenger, Andreas, eds., Center for Security Studies, 2012. P 106SSRN: http://ssrn.com

63. Charter of Fundamental Rights of the European Union // Official Journal C 364, 18/12/2000 P. 0001 – 0022

64. Council Recommendation of the 25th June 2001 on contact points maintaining a 24-hour service // for combating high-tech crime // OJ C 187 of 3.07.2001 // http://europa.eu/scadplus/leg/en/lvb/l23193.htm.

65. Handbook of Asian Criminology. New York 2013. C. 60-85

66. Legal and political measures to address cybercrime, UFRGSMUN | UFRGS Model United Nations ISSN: 2318-3195 | v.2, 2014| p. 445-477

67. Martin Stone, Cybercrime Growing Harder to Prosecute -Report, NEWSBYTES, www.infowar.com

68. Potential new global legal mechanisms on combating cybercrime and global cyberattacks. A presentation at the United Nations – ISPAC International Conference on Cybercrime: Global Phenomenon and its Challenges. Courmayeur, Italy. December 2-4, 2011. By Judge Stein Schjolberg. Norway. www.cybercrimelaw.net

69. Stein Schjolberg and Solange Ghernaouti-Helie.A Global Protocol on Cybersecurity and Cybercrime.Oslo-Cybercrimedata 2009. p.6-83.

70. Steve Gold, Security Breaches Cost $15 Bil. Yearly, NEWSBsrEs, atwww.newsbytes.com

71. World Drug Report 2013,United Nations Office on Drugs and Crime.New York, 2013, www.unodc.org__