Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№2(10)/2024, səh. 22-33
HƏRBİ NƏZƏRİ ELMLƏR ***MILITARY THEORETICAL SCIENCES***

UOT 351/354 DOI: 10.30546/9878.2024.2.10.0014.

KİBERCİNAYƏTLƏRİN MİLLİ VƏ BEYNƏLXALQ HÜQUQİ-QANUNVERİCİ ASPEKTLƏRİ

Zahid Oruc
Milli Müdafiə Universitetinin Hərbi Elmi Tədqiqat İnstitutu
zahidoruc@gmail.com

Xülasə. Məqalədə milli və beynəlxalq qanunvericilik təcrübəsinə əsaslanaraq kibercinayətkarlıq və kibertəhlükəsizlik məsələlərinin hüquqi aspektləri, mümkün təhlükələr və bu təhlükələrin mənbələrinin aradan qaldırılması ilə bağlı yanaşmalar təhlil edilir. Həmçinin vurğulanır ki, kibertəhlükəsizlik sahəsində mövcud qanunların və mütərəqqi təcrübələrin qarşılıqlı öyrənilməsi və tətbiqi kibertəhlükəsizliyin təmin olunmasına xidmət edir. Kibercinayətlər "internet cinayətindən" daha geniş anlayışdır, çünki istənilən informasiya və ya telekommunikasiya şəbəkələrindən istifadə etməklə cinayət törətmək imkanlarını özündə ehtiva edir. Kibercinayətkarlıq kompüter sistemləri və ya kompüter şəbəkələrinə, habelə kiberməkana daxil olmaq üçün digər vasitələrdən istifadə etməklə və ya onlar vasitəsilə, kompüter şəbəkələri daxilində saxlanan, emal edilən, yaxud ötürülən məlumatlara qarşı kiberməkanda törədilən cinayətləri əks etdirir. Bununla belə, kibercinayətkarlığın dəqiq və tam başa düşülməsi, habelə onun dünyada qanunvericilik baxımından modifikasiyası, ümumən qəbul edilmiş yanaşma, vahid bitkin təriflər məsələsi hələ də araşdırılmayıb. Tədqiqat nəticəsində məlum olur ki, yalnız qanunvericilik sahəsində deyil, kibercinayətin tərifi ilə bağlı nəzəri, doktrinal yanaşmalarda da alimlər arasında ümumi konsensus hələ də formalaşmayıb. Bu isə kiberməkanda cinayətlərin həm sürətli artımı, həm də cinayət törədilərkən kompüter sistemlərindən istifadənin forma və üsulları ilə bağlıdır.

Açar sözlər: kibercinayət, hüquqi aspektlər, kibertəhlükəsizlik, milli qanunvericilik, beynəlxalq qanunvericilik, hüquqi mübarizə, Azərbaycan

Giriş

İnformasiya texnologiyalarının sürətli inkişafı ilə paralel olaraq, kiberməkanda törədilən cinayətlərin sayı internet və kompüter şəbəkələrindən istifadə edənlərin sayına mütənasib olaraq artır. Hazırkı dövrdə kibercinayətkarlığın çox ciddi qlobal təhdidlərdən olması, onun çoxsaylı formalarının əhatəli təsnifatı, habelə qanunvericilikdə adekvat təsbit edilməsi məsələsini aktuallaşdırır. Yeni cinayətkarlıq fenomeninin qanunverici əsaslarının hazırlanması üçün milli və beynəlxalq səviyyədə səylərin davam etdirilməsinə baxmayaraq, hər ay, yaxud hər il yeni kibercinayət növləri meydana çıxır. Hüquq mühafizə orqanlarının belə cinayətlərin qarşısının alınması üzrə işinin səmərəliliyi isə kibercinayətkarlığın düzgün elmi-hüquqi definisiyası, qanunvericilikdə operativ təsbit və tətbiq edilməsi, cəmiyyətdə hüquqi maarifləndirmənin aparılması ilə bilavasitə bağlıdır.

İnternet istifadəçilərinin sayı artdıqca, bu haldan sui-istifadə edərək, müxtəlif qanun pozuntularına yol verən fırıldaqçıların da sayı çoxalır. Kibercinayətlərin, internet fırıldaqçılığının maraqlı xüsusiyyəti ondan ibarətdir ki, bir çox üsullar açıq şəkildə qanuna zidd olmur və bu, fırıldaqçıların qanun çərçivəsində təqib edilməsini çətinləşdirir. Kiberfırıldaqçılar eyni sxem üzrə fəaliyyət göstərirlər: birincisi, onlar e-poçt və ya sosial şəbəkələr vasitəsilə qurbanla əlaqə qurur, həmçinin e-poçt, telefon, faks və ya hər hansı digər yolla cavab almağa çalışırlar. Cavab alan fırıldaqçılar qurbanın etimadını qazandıqdan sonra müxtəlif bəhanələrlə müxtəlif məbləğdə pul istəyirlər. Belə fırıldaqçıların qurbanı olmamaq üçün onların üsullarını yaxşı bilmək, internetdə hansı fırıldaqçılıq üsullarının mövcud olması ilə bağlı məlumatlı olmaq lazımdır.

Pandemiya dövründə məsafədən və hibrid iş rejimlərinin, biznes platformalarının (ZOOM, Microsoft Teams, Skype və s.) texnoloji-informasiya müstəvisindən genişlənərək, sosial məkan müstəvisinə çevirilməsi və qlobal miqyas alması kibertəhlükəsizliyi, həm də ictimai-sosial təhlükəsizliyin ayrılmaz tərkib hissəsi etmişdir.

Dünyanın əksər ölkələrindəki normativ qaydalar kibercinayətləri cinayət kimi qeydə alır, cərimədən tutmuş ölüm cəzasına qədər cəza növlərini nəzərdə tutur.

Kibercinayətkarlığın hüquqi aspektlərini müəyyən etmək və bu anlayışı sistemləşdirmək üçün hüquqi ədəbiyyatda mövcud olan tərifl ərin təhlili vacibdir. Ümumi olaraq, kibercinayətkarlıq informasiya-kommunikasiya texnologiyalarının istifadəsi ilə informasiya məkanında məsafədən törədilmiş cinayətlər sistemi olan, tarixən dəyişkən, gizli sosial və cinayət hüququnun neqativ hadisəsi kimi başadüşülməlidir. Bütövlükdə, elmi-nəzəri və doktrinal yanaşmaların təhlili, kibercinayətin tərifində alimlər arasında konsensusun mövcud olmadığını göstərir. Eyni vəziyyət, həm də kiberməkanda müxtəlif şərhləri və qanunsuz hərəkətləri törədərkən kompüter sistemlərindən istifadənin forma və üsulları ilə də bağlıdır. Fərqlərə baxmayaraq, araşdırmaçılar kiberməkanda törədilən cinayətlər kimi təsnif edilən qeyri-qanuni hərəkətlərin siyahısı ilə bağlı beynəlxalq və milli qanunvericiliklər arasında əlaqə məsələsinin vacibliyini vurğulayırlar. Hesab edilir ki, "kibercinayət" anlayışı istənilən informasiya-kommunikasiya texnologiyalarından istifadə etməklə törədilən cinayətlərə şamil oluna bilər.

XXI əsrdə texnoloji inkişaf və informasiya inqilabının nailiyyəti nəticəsində formalaşan, ənənəvi olaraq, "real məkan" kimi başa düşülən məkana alternativ olan, sərhədlərinin, demək olar ki, tamamilə aradan qaldırıldığı yeni "virtual məkan" qismində – kiberməkanın mövcudluğu ümumən qəbul edilmişdir. Mobil telefonlar, kompüter və planşetlər və sair hər bir fərdin kiberməkanda təmsilçiliyini təmin edir. İnternet və kompüter vasitəsilə ünsiyyət bütün dünyada insanların məlumat mübadiləsi üsullarını kəskin şəkildə dəyişdirmişdir. İnformasiya texnologiyalarının insanlara verdiyi rahatlıq artdıqca, elektron daşıyıcılardan istifadə də geniş vüsət almış, zaman və məkandan asılı olmayaraq, istənilən məlumatın işləndiyi, saxlandığı, daşındığı və ötürüldüyü mühitlərə əlçatanlıq daha da asanlaşmışdır.

Kibercinayətlərin leqal aspektləri

Virtual məkanda qlobal kibercinayətkarlığın getdikcə yüksələn yeni dalğası, müvafiq olaraq, fərqli reallıqları aşkara çıxarmışdır. Müasir dövrdə heç bir, hətta ən güclü dövlət belə, "Ümumdünya Hörümçək Toru"nda – internetdə cinayətkarlıqla təkbaşına mübarizə aparmaq gücündə deyil. Potensial kibercinayətkarlığın subyekt və obyektlərinin say və miqyasının sürətlə artması, ona qarşı mübarizədə yeni üsul və vasitələrin daha da təkmilləşdirilməsi birgə – hüquqi, texnoloji, siyasi, iqtisadi, elmi, mədəni əməkdaşlıq çərçivəsində – tənzimləmə mexanizmlərinin hazırlanmasını şərtləndirir. Hər bir dövlətin informasiya infrastrukturu qlobal internet şəbəkəsi ilə sıx bağlı olduğundan, yeni cinayətkarlıq növü dövlətin milli təhlükəsizliyinə ciddi təhdidlər yaradır.

Kibercinayətlərlə beynəlxalq mübarizənin səmərəli və mühüm elementləri Birləşmiş Millətlər Təşkilatı (BMT) sistemində həyata keçirilir. Bu cinayətlə mübarizənin daha geniş spektrdə effektivliyinə nail olmaq üçün universal beynəlxalq qurum olan BMT çərçivəsində qəbul edilən sənədlər əsasında bu sahəyə dair təsbit olunmuş müqavilə müddəalarına üzv ölkələrin diqqət yetirməsi zəruri hesab olunur.

Kibercinayətkarlıqla bağlı beynəlxalq hüquq normalarının, xüsusilə "Kibercinayətkarlıq haqqında Budapeşt Konvensiyasının" ölkədaxili implementasiyası beynəlxalq hüquqda təsbit olunan ümumi qaydalara uyğun şəkildə həyata keçirilir. Lakin burada kibercinayətkarlıqla bağlı hüquqi normalar, habelə milli qanunvericiliyin maraqları ilə əlaqədar bəzi spesifik məqamlar nəzərə alınmalıdır.

Budapeşt Konvensiyası kibercinayətkarlıqla mübarizənin aşağıdakı prinsiplərini müəyyən etmişdir:

– geniş əməkdaşlıq prinsipləri;
– köçürmə prinsipi;
– qarşılıqlı yardımın ümumi prinsipi;
– təcili yardım tələblərinin rəhbər tutulması və həyata keçirilməsi prinsipi;
– məxfilik və məhdud istifadə prinsipi;
– müvəqqəti yardım prinsipi;
– yardımın göstərilməsi prinsipi və s. [1, s.14].

Kibercinayətkarlıq transmilli komponentə malikdir və transmilli xarakterinə, nəticələrinin ciddiliyinə görə digər beynəlxalq cinayətlərdən, heç də geri qalmır. Kibercanilər serverdə quraşdırılmış məlumatların, virusların və digər zərərli proqramların təminatçılarıdır. Bu baxımdan kibercinayətkarlığa qarşı hərtərəfli regional əməkdaşlığın qurulması və cinayətlə mübarizə mexanizmlərinin müəyyənləşdirilməsi vacibdir.

Bir çox amillər, kiberməkanın səciyyəvi xüsusiyyətləri, habelə informasiya infrastrukturunun dövlətlə yanaşı, özəl sektor və vətəndaşların əlində cəmlənməsi kibercinayətkarlıqla mübarizədə adekvat institutsional qurumların, elmi-texniki və normativ-hüquqi bazanın formalaşdırılması və təkmilləşdirilməsi ilə yanaşı, dövlət, özəl sektor və vətəndaşlar arasında, həmçinin beynəlxalq səviyyədə tərəfdaşlıq və əməkdaşlığın genişləndirilməsini tələb edir. Qeyd edilənlərin həyata keçirilməməsi (çoxtərəfli və beynəlxalq tərəfdaşlıq və əməkdaşlığın qurulmaması, adekvat mexanizmlərin, zəruri institutların yaradılmaması və s.) kibercinayətkarlıqla mübarizəni daha da çətinləşdirir.

Kiberməkanda insan amili və gündəlik sosial həyat özünün bütün komponentləri ilə təmsil olunur ki, bu da öz növbəsində cinayət fenomeninin tamamilə yeni təzahürlərinə gətirib çıxarır. Texnoloji tərəqqinin nəticəsi olaraq, müsbət sosial təzahürlərlə yanaşı, mənfi təzahürlər, o cümlədən cinayətkarlığın yeni üsul və formaları kiberməkanda yayılaraq qloballaşır. İnternetin yaratdığı imkanların genişləndirdiyi bu yeni cinayətlər kibercinayətlər kimi müəyyən edilir.

Bəzi dövlətlər kibertəhlükəsizliyə mülki və ya iqtisadi məsələ kimi yanaşsalar da, bir çoxları kibertəhlükəsizlik siyasətinin yaradılması və ya həyata keçirilməsinə kəşfiyyat agentliklərini cəlb edirlər. Kibertəhdidlər insanların təhlükəsizlik və milli təhlükəsizlik qaydaları və təcrübələri haqqında fikirlərinə inqilabi dəyişiklikləri şərtləndirir. Kibertəhlükənin bütün ölkələr tərəfindən qəbul edilən vahid və hərtərəfli tərifi mövcud olmasa da, demək olar ki, bütün dövlətlər kiberməkanda təhlükə və risklərin öz milli təhlükəsizlik siyasətinə daxil edilməsi fikrində yekdildirlər. Bu məsələnin tədqiqatçılar tərəfindən öyrənilməsi davam etdirilsə də, onun aktuallığı səngimir. Belə ki, texnologiyaların sürətli inkişafının səbəb olduğu mühitdə siyasətçilər və hüquqşünaslar yaranmış yeni tənzimlənmə problemlərinə çevik cavab vermək üçün çox vaxt dəyişən reallıqla ayaqlaşa bilmirlər [2; 3; 10].

Ayrı-ayrı fərdlər kiberməkanda virtual kimliklərini (virtual identiklik), real dünyadakı kimlikləri ilə eyniləşdirirlər. Bu inteqrasiya ictimai şüurda və psixi strukturlaşmada "dissosiasiya" adlanan prosesləri şərtləndirir. Toplumda insanların şüurunda yaranan yayınmalar, amneziya, diqqətsizlik və affektiv hərəkətliliklə səciyyələnən "dissosiativ təcrübələr" getdikcə kiberməkanda fərdlərin "kiberqurbana" (cyber victims) çevrilməsinə səbəb ola, onları cinayətin şahidi və ya cinayətkar edə bilər. Optimal məsafənin, real və virtual məkanlar arasında sərhədlərin qeyri-müəyyənliyi, kiberməkandakı dissosiativ psixoloji potensial və zəminlər fərdlərin cinayətə üz tutmasını asanlaşdırır. Kibercinayətin hüquqi aspektləri fərdin kiberməkanda olduğu dissosiativ və mobil (dinamik, səyyar) affektiv zəminlərdə qiymətləndirilməlidir. Bütün bu məsələlər, dəyişən sosial-mədəni dinamika qeyd olunan cinayətlərin inkişafı üçün zəmin rolu oynayır. Bu cinayətlərin psixoloji dinamikası cinayətkarın və qurbanın tipologiyasının müəyyən edilməsində, beləliklə də profilaktik tədbirlər planının işlənib hazırlanmasında və davam etdirilməsində mühüm əhəmiyyət kəsb edir.

Digər tərəfdən hüquqi-qanuni çərçivədə "məlumat sisteminə daxil olmaq", "sistemi bloklamaq, məlumatları məhv etmək və ya dəyişdirmək", "bank və ya kredit kartlarından sui-istifadə" və s. kimi əməllər də kibercinayətkarlıqdır. Bütün bunlar "informatika sahəsində cinayətlər" başlığı altında tənzimlənir [4].

Məlumdur ki, cinayətkar və deviant qruplar artıq bir-birindən çox uzaq məsafələrdə belə informasiya mübadiləsi aparmaq üçün forumlar və xəbər qrupları kimi kompüter vasitəsilə işləyən kommunikasiya texnologiyalarından istifadə edə bilirlər.

Əlavə olaraq, hakerlər təhlükəsizlik resurslarına çıxış əldə etmək və məlumatları oğurlamaq üçün demək olar ki, istənilən növ kompüter proqramı və avadanlıqlarından istifadə imkanına malikdirlər [5, s.87].

Kibercinayətlərə qarşı hüquqi mübarizə: bəzi beynəlxalq və milli təcrübələr

Milli, regional və beynəlxalq qanunlar real həyatda olduğu kimi, kiberməkanda da davranışları və kibercinayətlərlə bağlı cinayət mühakiməsi məsələlərini tənzimləyə bilər. Bu qanunlar yalnız baş vermiş hallarla bağlı qayda və gözləntiləri deyil, həm də bu qayda və gözləntilərin pozulması halında əməl edilməli olan prosedurları müəyyən edir. Bununla belə, kibercinayətin əsas növləri ilə bağlı müxtəlif ölkələrin milli qanunvericiliyində təsbit edilən müddəalardakı fərqlər cinayət mühakiməsi və ona qarşı mübarizə sahəsində beynəlxalq əməkdaşlığı mürəkkəbləşdirir. Kibercinayətkarlığa qarşı beynəlxalq əməkdaşlıq, müvafiq olaraq, transmilli mütəşəkkil cinayətkarlıqla mübarizədə beynəlxalq əməkdaşlıq sferasının daha da genişlənməsini tələb edir.

Kibercinayətkarlıqla milli qanunvericiliklərdən bəhs edərkən qeyd olunmalıdır ki, bu hallar mövcud qanunlara kibercinayətkarlıqla bağlı müddəaları əlavə etmək yaxud, dəyişiklik etməklə təmin edilə bilər. Digər tərəfdən, mövcud qanunların bütün hallarda kibercinayətlərə tətbiqi mümkün olmaya bilər. Belə ki, onlar internet və rəqəmsal texnologiyaların yaranmasından əvvəl qəbul edilmiş, yaxud internet və rəqəmsal texnologiyalar nəzərə alınmadan hazırlanmış ola bilər. Buna görə də real həyatdakı cinayətlərlə əlaqədar nəzərdə tutulmuş qanunlar, virtual məkandakı kibercinayətkarlara və informasiya-kommunikasiya texnologiyalarından (İKT) cinayətin törədilməsinin subyekti və ya vasitəsi kimi istifadə edən digər cinayətkarların əməllərinə tətbiq edilməyə, yaxud onlara sadəcə məhdud çərçivədə təsir göstərə bilər. Nəticədə kibercinayətlərlə bağlı xüsusi qanunlara ehtiyac duyulur. Kibercinayətkarlıqla bağlı qanunların qəbul edilib-edilməməsi, milli qanunvericiliyin əhatə dairəsindən, normativ aktların xarakteri və şərhindən asılıdır.

Kibertəhlükə və kiberhücumların getdikcə daha çox yayıldığı bir şəraitdə, nəinki dövlət və qurumlar səviyyəsində, hətta ayrı-ayrı müəssisələr və təşkilatlar səviyyəsində də biznes və informasiya təhlükəsizliyi siyasəti, eləcə də texnoloji siyasətin prioritet hesab edilməsi kibercinayətlərdən qorunmağa ciddi töhfə verə bilər. Təşkilatlardan keçən məlumatlar hüquqi baxımdan fərqli ola bilər. Məsələn, hər hansı bir müəssisə və ya şirkətin bütün işçilərinin məxfi məlumatlara bütövlükdə çıxışı varsa, o zaman "müəssisənin məlumatlarının sızmayacağına necə əmin olmaq olar?".

Kibercinayətlər haqqında qanunun yeri və roluna gəldikdə, bu qəbildən olan qanunlar informasiya və kommunikasiya texnologiyaları (İKT) istifadəçiləri üçün məqbul davranış standartlarını müəyyən edir; kibercinayətlərə görə sosial və hüquqi sanksiyalar müəyyən edir; ümumilikdə İKT istifadəçilərini qoruyur və xüsusilə insanlara, verilənlərə, sistemlərə, xidmətlərə və infrastruktura dəyən ziyanı minimuma endirir və ya qarşısını alır; insan hüquqlarını qoruyur; internetdə (virtual dünyada) törədilmiş cinayətləri araşdırmaq və mühakimə etmək imkanı verir; kibercinayətkarlıq halları üzrə ölkələr arasında əməkdaşlığı təşviq edir [6, s.57].

Kibercinayətkarlıq qanunvericiliyi internetdən, kompüterlərdən və əlaqəli rəqəmsal texnologiyalardan istifadə dövlət və özəl təşkilatların hərəkətlərində davranış qaydaları və standartlarını təmin edir; sübut qaydaları; cinayət prosesinin həyata keçirilməsi qaydaları və cinayət hüququnun kiberməkana aid digər məsələləri; kibercinayətkarlıq halında şəxslərə, təşkilatlara və infrastruktura dəyən riskin azaldılması və ya zərərin azaldılması üçün müddəalar. Beləliklə, kibercinayətkarlıq qanunvericiliyi maddi, prosessual və qabaqlayıcı hüquq normalarını ehtiva edir.

Bəzi ölkələr kibercinayətkarlıqla bağlı yeni spesifik qanunlar hazırlamaq əvəzinə, öz milli qanunlarına və ya məcəllələrinə ayrıca kibercinayətkarlıqla bağlı müddəaları daxil edərək düzəlişlər etmişlər. Digər ölkələr cinayət törətmək üçün informasiya və kommunikasiya texnologiyalarından qeyri-qanuni istifadə ilə bağlı ayrıca qanunvericilik aktlarını qəbul etməyə üstünlük verirlər. Belə ki, cinayəti törədən şəxs saxtakarlıq və ya dələduzluq etmək üçün qeyri-qanuni girişdən istifadə edibsə, belə bir əməl eyni vaxtda iki cinayət təşkil edir.

Bir sıra ölkələrdə kibercinayətkarlıqla mübarizəyə dair ayrıca qanunlar hazırlanmışdır. Məsələn, Almaniya, Yaponiya və Çin kibercinayətkarlıqla mübarizə sahəsində öz cinayət məcəllələrinin müvafiq müddəalarına düzəlişlər etmişlər. Bəzi ölkələr, həmçinin kibercinayətlərin və kibercinayətkarların müəyyən növlərini əhatə etmək üçün mövcud qanunlardan istifadə edirlər.

Hər bir dövlətin kibercinayətkarlıq sahəsində maddi cinayət hüququnun yaradılmasına təsir göstərən öz hüquq sistemi var:

1. Ümumi hüquq (Common law). Burada qanunlar qəbul edilmiş ayrıca qanunlar və presedent hüququ (yəni, məhkəmə qərarları və ya məhkəmə presedentləri əsasında formalaşan qanun) şəklində mövcuddur.

2. Mülki hüquq (Civil law). Belə hüquq sisteminə malik olan ölkələr əsas hüquqların, öhdəliklərin, və davranış gözləntilərinin sərhədlərini müəyyən edən kodifikasiya olunmuş, birləşdirilmiş və hərtərəfli normativ qaydalar və qanunlara malikdirlər. Bu sistemlər, əsasən, qanunvericiliyə və konstitusiyaya əsaslanır.

3. Adi hüquq (Customary law). Bu hüquq sistemlərinə konkret tarixi-mədəni ənənələrin daşıyıcıları tərəfindən qanun kimi qəbul edilən ümumi davranış nümunələri daxildir (opinio juris – qanuniliyə inam). Beynəlxalq hüquqda adət hüququ dövlətlər arasında münasibətləri və praktikanı tənzimləyir və bütün dövlətlər üçün məcburi hesab olunur.

4. Dini hüquq (Religious law). Dini hüquq sistemləri hüququn mənbəyi kimi dini təlimlərə və ya dini ədəbiyyata əsaslanan qaydalardan istifadə edir.

5. Hüquqi plüralizm (Legal pluralism). Bu tip hüquq sistemində yuxarıda qeyd olunan hüquq sistemlərindən iki və ya daha çoxu (məsələn, ümumi hüquq, mülki hüquq, adət hüququ və ya dini hüquq) bir yerdə mövcud ola bilər [7, s.101].

Kibercinayətkarlığın beynəlxalq səviyyəsinə gəldikdə, bu sahədə bir sıra beynəlxalq müqavilələrin bağlandığı qeyd edilə bilər. Ümumiyyətlə, mövcud çoxtərəfli və regional hüquqi sənədlər və milli qanunlar öz tematik məzmunu və kriminallaşma, istintaq tədbirləri və səlahiyyətləri, rəqəmsal sübutların toplanması və istifadəsi, tənzimləmə və risk, yurisdiksiya və beynəlxalq əməkdaşlıq kimi aspektləri əhatəetmə dərəcəsi ilə fərqlənir. Bu müqavilələr, həm də coğrafi əhatə dairəsi (yəni regional və ya çoxtərəfli olması) ilə fərqlənir. Bu cür fərqlər kibercinayətkarların effektiv müəyyən edilməsi, araşdırılması və mühakimə olunmasına, eləcə də kibercinayətkarlığın qarşısının alınmasına maneələr yaradır. İnternet məzmununu və girişi məhdudlaşdıran qanunların qanuni məqsədlər üçün tətbiqini, qanunun aliliyi və insan hüquqları standartlarına uyğunluğunu təmin etmək üçün də təminatların nəzərə alınması lazım gəlir. Bundan əlavə, kibercinayətkarlıq qanunlarının əhatə dairəsi və tətbiqi "bir ölkədə yaradılan və məqbul olan internet məzmunu üçüncü ölkədə əlçatan olduqda" belə məzmunun qeyri-qanuni hesab edildiyi məqamlarda çətinləşir [5, s.128].

Kibercinayətkarlıqla bağlı ayrı-ayrı ölkələrin hüquqi praktikalarına gəldikdə, Çin, ABŞ, Estoniya, Ukrayna, Niderland, İspaniya, Avstriya, Böyük Britaniya və digər ölkələrdə kiberterrorizmlə bağlı xüsusi qanun qəbul edilmiş, həmçinin bir sıra qanunvericiliyə əlavə və dəyişikliklər də edilmişdir.

Kibertəhlükəsizlik siyasətinin həyata keçirilməsi ilə məşğul olan ölkə kimi Estoniyanın təcrübəsi maraqlıdır. Dövlət tərəfindən bu sahədə bir sıra strateji sənədlər hazırlanmış, qəbul edilmiş, müvafiq institusional strukturlar yaradılmışdır. Strateji planlaşdırma bütün kibertəhlükəsizlik arxitekturasının vəhdətini təmin edir. 2008-ci ildə Estoniya Respublikası dünyada ilklərdən biri olaraq beynəlxalq hüquq normaları çərçivəsində yazılmış Milli Kibertəhlükəsizlik Strategiyasını [10] qəbul edib. Estoniya informasiya-kommunikasiya texnologiyalarından istifadəni və "ağıllı həllər"in işlənməsini asanlaşdıran şərait yaratmağa başlamışdır [8].

Çin bir-biri ilə bağlı olan: 2015-ci il iyulun 1-də "Dövlət təhlükəsizliyi haqqında", 2017-ci il iyunun 1-də "Kibertəhlükəsizlik haqqında", 2016-cı ildə "Terrorizmlə mübarizə haqqında" Qanun qəbul etmişdir. Böyük Britaniyanın 2000-ci il "Terrorizm Aktı"na əsasən kompüterlərə, onların sistemlərinə və ya şəbəkələrinə ciddi ziyan vurmaq, yaxud onların kütləvi zorakılıq aksiyalarını təşkil etmək üçün əldə edilmiş kompüter məlumatlarının isifadəsinə dair, Fransa Cinayət Məcəlləsinin 4211 – "İnformatika sahəsindəki hərəkətlərlə bağlı terror aktları"nda kibercinayətkarlığın terror aktlarına bərabər tutula biləcəyi müəyyənləşdirilmişdir [9, s.93].

Rusiya, Ukrayna, Gürcüstan, Qazaxıstan və Estoniyada qəbul edilmiş qanunlarda artıq informasiya texnologiyaları və kommunikasiyaların terrorizmdə rolunu aydın şəkildə müəyyən edir.

Ukraynanın 21 iyun 2018-ci il tarixli 2469-VIII nömrəli "Kibertəhlükəsizliyin təmin edilməsinin əsas prinsipləri haqqında" Qanununun 1-ci maddəsində kiberməkanda və ya ondan istifadə etməklə həyata keçirilən terror fəaliyyəti (kiberterrorizm) ilə bağlı tədbirlər nəzərdə tutulmuşdur.

Xarici ölkələrdə kibercinayətkarlıqla mübarizənin aparılması həvalə edilən sahəvi səlahiyyətli qurumların fəaliyyəti də fərqlidir. Başqa sözlə, bu səlahiyyət Avstraliyada Müdafiə Departamenti, Belçikada Təhlükəsizlik Nazirliyinin Komitəsi, Braziliyada İnformasiya Təhlükəsizliyi Komitəsi, Kanadada Kanada Kompüter Şəbəkəsinin Fövqəladə Hallara Cavab Mərkəzi, Estoniyada İqtisadiyyat, Rabitə və Nəqliyyat Nazirliyi, Finlandiyada, Baş Nazirlik strukturunda Milli Müdafiə Baş Katibliyi, Fransada Milli İnformasiya Təhlükəsizliyi Agentliyi, Almaniyada Federal İnformasiya Təhlükəsizliyi Agentliyi, Macarıstanda İnformatika və Rabitə Nazirliyi, Hindistanda Milli İnformasiya Şurası, İtaliyada Daxili İşlər Nazirliyi, Yaponiyada Nazirlər Kabineti, Koreya Respublikasındakı bütün dövlət təşkilatları və onların törəmə qurumları, Malayziyada Modernləşdirmə və Planlaşdırmanı İdarəetmə Mərkəzi, Niderlandda Daxili İşlər Nazirliyi və Kral İşləri Nazirliyi, Yeni Zelandiyada Kritik İnfrastrukturun Mühafizəsi, Norveçdə Mülki Müdafiə və Böhran Planlaması İdarəsi, Elm və Ali Təhsil Nazirliyi və Daxili İşlər Nazirliyi, Polşada sahəvi idarələr, Sinqapurda İnformasiya Şəbəkələri və Rabitə Təhlükəsizliyi Müdirliyi, İspaniyanın Dövlət İdarəçilik Nazirliyi və Daxili İşlər Nazirliyi, Böyük Britaniyada Nazirlər Kabineti yanında Kibertəhlükəsizlik İdarəsi, həmçinin bir sıra müxtəlif təşkilati bölmələrdə kiberterrorizmlə məşğul olan qurumlar mövcuddur [11, s.35-45].

Macarıstan Respublikasında "Dövlət-Özəl Tərəfdaşlıq Fondu" kibertəhlükəsizlik üçün vəsaitlərin sistemli şəkildə bölüşdürülməsini təmin edir. Həmçinin Macarıstanda kiberterrorizmlə mübarizədə "CERT– Macarıstan Təcili Müdaxilə Qüvvəsi". Hindistanda Hindistan Respublikası Milli Təhlükəsizlik Şurasının Katibliyinin 21-ci üzvü yanında kiberterrorizmlə mübarizə məqsədilə "Hindistanın Milli İnformasiya Şurası" yaradılmışdır. İtaliyada Daxili İşlər Nazirliyi və İnnovasiya və Texnologiyalar Nazirliyi kiberterrorizmlə mübarizə sahəsində dövlət siyasətinin işlənib hazırlanması və həyata keçirilməsi üzrə səlahiyyətli dövlət orqanı kimi müəyyən edilir. Həmçinin İtaliyada poçt polisi xidməti yaradılmışdır və o, milli və regional səviyyələrdə kompüter cinayətlərinə operativ reaksiya mərkəzlərinə nəzarət edir. İtaliyanın "Kritik İnfrastruktur Mütəxəssisləri Assosiasiyası" dövlət və özəl sektorların kibertəhlükəsizlik işini əlaqələndirir [12, s.35-45].

Bütövlükdə, hüquq sistemləri daxilində hüquqi tənzimləmələr kibercinayət qurbanlarının hüquqlarının qorunmasında, günahkarların lazımi sanksiyalarla üzləşməsinin təmin edilməsində və cinayətin reallaşmasının qarşısının alınmasında mühüm rol oynayır.

Artıq qloballaşma və informasiya dövrünün tələblərinə müvafiq olaraq, milli qanunvericilik sistemləri də modern dəyişikliklərə məruz qalmaqdadır.

Bu gün dünyanın əksər ölkələri sürətlə inkişaf edən müasir İKT sistemlərinə nüfuz etdikcə milli qanunvericiliklərdə də müasir beynəlxalq hüquq norma və prinsiplərin tələblərinə uyğun rasional dəyişiklik və inkişaf müşahidə olunur [13, s.98].

Azərbaycanda kibertəhlükəsizliyin təminatı. Azərbaycanda kibertəhlükəsizlik sahəsində hüquqi-tənzimləyici çərçivələr

Ölkəmizdə informasiya-kommunikasiya texnologiyalarının sürətli inkişafı beynəlxalq hüquqi münasibətlərin kibercinayətkarlıq kimi müxtəlif sahələrində beynəlxalq əməkdaşlığa və bu sahədə hüquqi mübadilələrin zəruriliyinə səbəb olmuşdur. Dövlətimiz kibercinayətlərə qarşı mübarizədə Birləşmiş Millətlər Təşkilatı, Avropa Şurası, və Avropa İttifaqı (Aİ) çərçivəsində hüquqi addımlar atmağa başlamışdır.

Digər ölkələr kimi, Azərbaycanda da kibercinayətkarlıqla mübarizədə hərtərəfli əməkdaşlıq çərçivəsində beynəlxalq hüququn milli qanunvericiliyə daxil edilməsi və tətbiqi istiqamətində zəruri tədbirlər həyata keçirilir. Azərbaycan Respublikasında kiberməkandan istifadə, o cümlədən informasiya ehtiyatlarının mühafizəsi və kibercinayətkarlığa qarşı mübarizə milli təhlükəsizlik qədər mühümdür. Bu sahədə beynəlxalq hüququn tətbiqi Azərbaycan Respublikasının milli təhlükəsizlik sahəsinə dair qanunvericiliyində öz əksini tapmışdır [14].

Ölkəmizdə kibertəhlükəsizlik sahəsində mühüm addımlar atılmışdır və Prezident İlham Əliyev bu sahədə uğurlu siyasət həyata keçirir. Budapeşt Konvensiyası kibercinayətkarlıqla bağlı qoşulduğumuz ilk qanunvericilik sənədidir.

Bütün dünyada olduğu kimi, Azərbaycanda da milli kibertəhlükəsizlik siyasətinin inkişaf etdirilməsi zəruri məsələdir. Hökumətin informasiya və kommunikasiya sistemləri, o cümlədən hərbi, texnoloji və kommersiya layihələri kiberhücumlar və kibercasusluğunun hədəfi kimi getdikcə daha həssas qrupu təşkil edir. Bu baxımdan kiberməkanın idarə edilməsinə dövlət səviyyəsində əhəmiyyət verilir.

Qeyd edilən istiqamətdə hüquqi-tənzimləyici məzmunlu (strategiya, qanunlar, doktrinalar və qanunvericiliyin təkmilləşdirilməsi) dövlətin kibertəhlükəsizliyinin, bu sahədə dövlət siyasətinin prinsip və istiqamətlərinin yaradılması üzrə hüquqi və təşkilati çərçivə formalaşdırılmışdır. Buraya, həmçinin dövlət orqanları, müəssisələr, institutlar, təşkilatlar, fərdlər və vətəndaşların sözügedən sferada səlahiyyətləri, eyni zamanda onların fəaliyyətlərinin koordinasiyası üzrə başlıca prinsipləri də daxildir. Azərbaycanın kibertəhlükəsizlik siyasəti ilə bağlı hüquqi-tənzimləyici bazanın inkişafına əsas etibarilə 1999–2000-ci illərdə başlanılıb. Kibertəhlükəsizliklə bağlı ayrıca strategiya, hələlik hazırlanmasa da, müxtəlif sahələrdə dövlət siyasətlərinin həyata keçirilməsində kibertəhlükəsizlik məsələlərinin inkişafı üçün mühüm müddəalar artıq təsbit edilib.

Bu kimi strategiyalara "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014–2020-ci illər üçün Milli Strategiya" və "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair Milli Strategiyanın həyata keçirilməsi üzrə 2016–2020-ci illər üçün Dövlət Proqramı"nı, həmçinin "Azərbaycan 2020 gələcəyə baxış" İnkişaf Konsepsiyasını və "Azərbaycan Respublikasında telekommunikasiya və informasiya texnologiyalarının inkişafına dair Strateji Yol Xəritəsi"ni aid etmək olar. Həmçinin "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya" Beynəlxalq Telekommunikasiya İttifaqı (BTİ) və Aİ tərəfindən hazırlanmış bütün təcrübə və tövsiyələri nəzərə alan sənəddir. Strategiyanın əsas məqsədi informasiya cəmiyyətinin qurulması və İKT-nin inkişafı daxil olmaqla ölkənin davamlı sosial-iqtisadi və mədəni səviyyədə yüksəlişi üçün vətəndaşlar, icmalar və dövlət tərəfindən onun imkanlarından səmərəli istifadə etməkdir. Müvafiq strategiyanın həyata keçirilməsi üçün Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi əlaqələndirici qurum təyin edilmişdir. Məqsəd, rəqəmsal məkanda təhlükəsizliyi inkişaf etdirmək, İKT-dən istifadəyə inamı artırmaq, qanunvericilik bazasını təkmilləşdirmək və məlumatlılığı yüksəltməkdir. Bu məqsədlərə çatmaq üçün vəzifələr sırasına isə informasiya təhlükəsizliyi üzrə dövlət siyasətinin hazırlanması, bu istiqamətdə xarici ölkələrdən asılılığın azaldılması, "elektron hökumət" şəbəkələrinin mühafizəsi, kibertəhlükələrin əhəmiyyətinin ölkə miqyasında elan edilməsi, kibertəhlükəsizlik sahəsində texniki peşəkarlığın inkişaf etdirilməsi, uşaqların istifadəsi üçün "təhlükəsiz internet" platformasının gücləndirilməsi, cəmiyyətdə və şirkətlər arasında məlumatlılığın artırılması, eləcə də informasiya təhlükəsizliyi mədəniyyətinin təşviqi daxildir.

Yuxarıda qeyd edilən strategiya hər biri dövlət proqramları ilə müşayiət olunan iki mərhələdə həyata keçirilir. "2016–2020-ci illər üçün Dövlət Proqramı" Milli Strategiyanın tətbiqi istiqamətində yeddi prioritet üzrə konkret addımlardan ibarətdir. İnformasiya təhlükəsizliyinə dair tədbirlər planına əsasən Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi (RİNN), Dövlət Təhlükəsizliyi Xidməti (DTX) və Müdafiə Nazirliyi (MN) kibertəhlükəsizliyə dair normativ hüquqi aktların yenilənməsinə məsul olan qurumlardır. "Telekommunikasiya və informasiya texnologiyalarının inkişafına dair Strateji Yol Xəritəsi"nə və İKT sektorunun "SWOT" təhlilinə əsasən şəbəkə və informasiya təhlükəsizliyinə qarşı artan çağırışlar əsas təhlükələr sırasındadır. Bu baxımdan, strateji məqsədlərdən biri, milli kibertəhlükəsizliyə hazırlığın və məlumatlılığın artırılmasıdır.

Qanunvericilik bazasına aid sənədlərin bəziləri kimi aşağıdakılar qeyd edilə bilər:

"Dövlət sirri haqqında" Azərbaycan Respublikasının Qanunu, 2004; Milli Təhlükəsizlik Konsepsiyası, 2007; "Kibercinayətkarlıq haqqında" Konvensiyanın təsdiq edilməsi barədə Azərbaycan Respublikasının Qanunu, 2009; Azərbaycan Respublikasının Hərbi doktrinası, 2010; "Fərdi məlumatlar haqqında" Azərbaycan Respublikasının Qanunu, 2010; "İnformasiya təhlükəsizliyi sahəsində

fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında" Azərbaycan Respublikası Prezidentinin Fərmanı, 2012; "Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının Qanununda dəyişiklik edilməsi barədə Azərbaycan Respublikasının Qanunu, 2012; "Azərbaycan Respublikasının Cinayət Məcəlləsi. Otuzuncu fəsil. Kibercinayətlər", 2012; "Azərbaycan Respublikasının Xüsusi Dövlət Mühafizə Xidmətinin Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Agentliyi haqqında Əsasnamənin və Agentliyin strukturunun təsdiq edilməsi" barədə Azərbaycan Respublikası Prezidentinin Fərmanı, 2012; "Azərbaycan Respublikasının Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi yanında Elektron Təhlükəsizlik Xidmətinin fəaliyyətinin təmin edilməsi haqqında" Azərbaycan Respublikası Prezidentinin Fərmanı, 2012; "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanununda dəyişikliklər edilməsi barədə Azərbaycan Respublikasının Qanunu, 2017; "Rəqəmsal transformasiya sahəsində idarəetmənin təkmilləşdirilməsi haqqında" Azərbaycan Respublikası Prezidentinin Fərmanı, 2021; "Banklarda informasiya təhlükəsizliyinin idarə edilməsi Qaydası", 2021; "Azərbaycan Respublikasının Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti haqqında Əsasnamənin təsdiq edilməsi" barədə Azərbaycan Respublikası Prezidentinin Fərmanı, 2021;"Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində bəzi tədbirlər haqqında" Azərbaycan Respublikası Prezidentinin Fərmanı, 2021.

Bundan əlavə, Azərbaycan Respublikası Prezidentinin 2005 və 2010-cu illərdəki sərəncamları, habelə Azərbaycan Respublikası Nazirlər Kabinetinin 14 may 2010-cu il tarixli sərəncamı ilə Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafına dair Dövlət proqramları təsdiq edilmişdir.

2011-ci ildə "Elektron hökumətin formalaşdırılması üzrə Fəaliyyət Proqramı"nda İKT-nin inkişafı ilə bağlı əməli tədbirlərin həyata keçirilməsi nəzərdə tutulmuşdur.

2014-cü ildə Azərbaycan Respublikası Prezidentinin Sərəncamı ilə kibertəhlükəsizlik strategiyası qəbul edilmişdir. Azərbaycanda informasiya cəmiyyətinin əsaslarını yaratmış İKT üzrə Milli Strategiya vətəndaşlar, cəmiyyət və özəl sektor tərəfindən İKT-dən geniş istifadəni nəzərdə tutur.

Milli Strategiyanın başlıca məqsədi və vəzifələri ölkənin informasiya məkanının təhlükəsizliyinin təmin edilməsi, İKT-dən istifadəyə inamın artırılması, bu sahəni tənzimləyən normativ hüquqi bazanın işlənib hazırlanması, informasiya və maarifləndirmə işinin həyata keçirilməsi ilə bağlıdır.

Strategiyanın məqsədlərinə nailolmanın siyasi istiqamətləri:

a) informasiya təhlükəsizliyi sahəsində vahid dövlət siyasətinin və hüquqi bazanın təkmilləşdirilməsi;

b) ölkənin milli informasiya məkanının və strateji infrastrukturunun, habelə informasiya infrastrukturunun, informasiya təhlükəsizliyini təmin edən sistemin inkişafı;

c) ölkənin informasiya əlaqələrində texniki və texnoloji asılılığın azaldılması üzrə tədbirlərin həyata keçirilməsi;

d) "elektron hökumət" infrastrukturunun informasiya təhlükəsizliyinin təmin edilməsi;

e) elektron təhlükələr haqqında məlumatın milli səviyyədə həyata keçirilməsi;

f) kibertəhlükəsizliyin gücləndirilməsi sahəsində müvafiq texniki və metodiki vasitələrin yaradılması, tövsiyələrin hazırlanması və metodiki dəstəyin göstərilməsi;

g) uşaqları qeyri-qanuni və təhlükəli məzmundan qorumaq üçün "təhlükəsiz internet" mexanizminin işlənib hazırlanması və tətbiqi;

h) dövlət və qeyri-dövlət informasiya infrastrukturu subyektlərinin kibertəhlükəsizlik üzrə fəaliyyətinin əlaqələndirilməsi;

i) əhalinin, özəl və digər qurumların kibertəhlükəsizlik sahəsində maarifləndirilməsi və informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması, bu sahədə ixtisaslı kadrların hazırlanması;

j) ölkənin informasiya təhlükəsizliyi sahəsində beynəlxalq əməkdaşlığının təmin edilməsi.

Milli Strategiyanın icrası prosesində dövlət orqanları, özəl sektor və vətəndaş cəmiyyəti institutları arasında sıx əməkdaşlıq və əlaqələndirilmiş fəaliyyət təmin edilir, informasiya cəmiyyəti ideyalarının geniş yayılması üçün fəal təbliğat aparılır.

Azərbaycanın kibersərhədlərinin mühafizəsi ilə üç əsas dövlət qurumu məşğul olur: Rabitə və İnformasiya Texnologiyaları Nazirliyi (RİTN), Dövlət Təhlükəsizlik Xidməti (DTX) və İnformasiya Texnologiyaları İnstitutu (İTİ). Azərbaycanın Dövlət Departamentləri üzrə kompüter şəbəkələrinin mühafizəsi məqsədilə Xüsusi Dövlət Mühafizə Xidmətinin nəzdində informasiya təhlükəsizliyi insidentlərinə cavab vermək üçün CERT-GOV-AZ18 kompüter fövqəladə hallar qrupu yaradılmışdır.

Dövlət Təhlükəsizlik Xidməti kibercinayətkarlıqla mübarizə üzrə səlahiyyətli orqan kimi təyin olunmuşdur və kibercinayətkarlıq hallarının araşdırılması, bu istiqamətdə yaranan təhlükələrin qarşısının alınması məqsədilə səmərəli mübarizənin aparılması üçün müvafiq addımlar atmaqdadır.

Kibercinayətkarların, xüsusən də kiberterrorizmin artması bu təhlükənin qarşısının alınması üçün Dövlət Təhlükəsizlik Xidmətinin işinin təkmilləşdirilməsi məsələsini daha da aktuallaşdırmışdır. Bu sahədə qeyri-qanuni fəaliyyətlə mübarizə aparmaq üçün müvafiq texniki təchizat, eləcə də yüksək texnologiyalar üzrə xüsusi bilik və bacarıqlar tələb olunur [1, s.204-205].

Ölkəmizdə kibertəhlükəsizliyin təmin edilməsi məqsədilə Azərbaycan Respublikası Prezidentinin 26 sentyabr 2012-ci il tarixli Fərmanının 5-ci hissəsinə uyğun olaraq, Azərbaycan Respublikasının Rabitə və İnformasiya Texnologiyaları Nazirliyinin tabeliyində Kibertəhlükəsizlik Mərkəzi (CERT.GOV.AZ) yaradılmışdır. Kibertəhlükəsizlik Mərkəzi sosial sabitlik və virtual məkanda normal fəaliyyəti təmin edir, kibertəhlükəsizlik sahəsində informasiya infrastrukturunun fəaliyyətini əlaqələndirir, mövcud və potensial elektron təhlükələr barədə aidiyyəti orqanları məlumatlandırır.

Elektron idarəetmənin bu missiyasının davamlılığına nail olmaq üçün hökumətin qarşıya qoyduğu tapşırıqlar [15]:

1. Elektron Hökumət Akademiyasının yaradılması.
2. Elektron Hökumət Araşdırma Mərkəzinin yaradılması.
3. Elektron hökumət üzrə bacarıqların artırılması və biliklərin paylaşılması.
4. Elektron hökumət infrastrukturunun inkişafı (G-Cloud adlı hökumət buludunun tətbiqi).

Prezidentin Fərmanı ilə nəqliyyat, rabitə və yüksək texnologiyalar sahəsində idarəetmənin təkmilləşdirilməsi ilə bağlı əlavə tədbirlər haqqında Azərbaycan Respublikasının 12 yanvar 2018-ci il tarixli sərəncamı ilə Elektron Təhlükəsizlik Xidməti (ETX) kimi Nəqliyyat, Rabitə və Yüksək Texnologiyalar Nazirliyinin strukturuna daxil edilmişdir. Ümumiyyətlə, ETX infrastruktur haqqında məlumat verən, ölkə səviyyəsində mövcud və potensial elektron təhlükələr barədə məlumatlılığı, əhalinin, özəl qurumların və digər təşkilatların kibertəhlükəsizlik sahəsində maarifləndirilməsini təmin edən, həmçinin metodiki köməklik göstərən əlaqələndirici dövlət orqanıdır.

Elektron Təhlükəsizlik Xidməti aşağıdakı fəaliyyətləri həyata keçirir:

a) kibertəhlükəsizlik sahəsində informasiya infrastrukturu subyektlərinin fəaliyyətini əlaqələndirmək;

b) istifadəçilərdən, proqram təminatı, aparat və texniki avadanlıq istehsalçılarından, xarici ölkələrdəki analoji strukturlardan və digər mənbələrdən kiberhücumlar, müdaxilələr, zərərli kompüter proqramları (bundan sonra elektron təhlükə və təhdidləri) haqqında məlumatları toplamaq və təhlil etmək;

c) istifadəçilərin kibertəhlükəsizlik məsələlərinə dair məlumatlılığının artırılması məqsədilə mövcud və potensial kibertəhlükələrin bildirilməsini həyata keçirmək;

d) istifadəçiləri təhdid edən proqramlar və texniki vasitələr haqqında təlimat və tövsiyələr hazırlamaq, kibertəhlükələrə qarşı mübarizəyə metodiki dəstək göstərmək;

e) qlobal internet trafikində kiberhücumların dəf edilməsi üçün milli İnternet operatoru və aidiyyətli beynəlxalq qurumlarla birgə qabaqlayıcı tədbirlər həyata keçirmək;

f) kibertəhlükəsizliyə hazırlığı təmin etmək üçün ölkədə fəaliyyət göstərən digər aidiyyəti qurumlarla əməkdaşlıq etmək [4, s.133].

2002-ci ildə yaradılan İnformasiya və Telekommunikasiya Elmi Mərkəzinin (BTRM) əsasında AMEA-da İnformasiya Texnologiyaları İnstitutu (İTİ) fəaliyyətə başlamışdır. İnstitut 2022-ci ildə Elm və Təhsil Nazirliyinə tabe edilmişdir. İnformasiya Texnologiyaları İnstitutu İKT-nin müasir problemlərinə dair innovativ elmi tədqiqatlar aparan təşkilatdır. Burada informasiya texnologiyaları və

informasiya cəmiyyətinin aktual elmi-nəzəri problemləri üzrə tədqiqatların əsası qoyulmuş, yeni elmi-tədqiqat şöbələri və mərkəzləri açılmışdır. İnstitutda mühüm layihələr həyata keçirilir, səmərəli tədqiqat nəticələrinin əldə edilməsi və təşkilatın daha yüksək innovasiya fəaliyyətinin təşkili üçün beynəlxalq standartlara cavab verən bütün imkanlar yaradılır. İnstitut elmi-texniki və innovasiya siyasətinin həyata keçirilməsi istiqamətində uğurlu işlərini davam etdirir.

İnstitutun əsas məqsədləri İKT-nin geniş imkanlarından istifadə etməklə elmi fəaliyyətin müasir tələblərə uyğun təşkili və inkişaf etdirilməsi, elmi idarəetmənin təkmilləşdirilməsi, milli elmi informasiya məkanının formalaşdırılması, beynəlxalq elmi mühitə inteqrasiya və yüksək səviyyəli kadr hazırlığıdır. İnstitutun mühüm elmi nailiyyətləri bunlardır:

a) uyğunlaşan şəbəkələr üçün dəyər və vaxt göstəriciləri üzrə paylanmış optimal autentifikasiya sistemi hazırlanmış və korporativ şəbəkələrdə müxtəlif təhlükələrə qarşı mübarizədə qərarların qəbulu üçün nəzəri oyun modeli təklif edilmişdir;

b) virtual mühitdə informasiya müharibəsinin təzahürünün aşkarlanması üçün üsul və alqoritmlər işlənib hazırlanmışdır. Respublikada elektron elmin formalaşdırılması, idarə olunması və qiymətləndirilməsi, informasiya təhlükəsizliyinin təmin edilməsi üçün model və metodlar təklif edilmişdir;

c) böyük verilənlər bazasının (Data Mining) intellektual təhlili üçün metodlar və alqoritmlər işlənib hazırlanmışdır. Mətn sənədləri dəstlərinin məzmununa görə qruplaşdırılması, onların avtomatlaşdırılmış ümumiləşdirilməsi və xülasələrin qiymətləndirilməsi (Text Mining) üçün çoxsaylı üsullar və alqoritmlər təklif edilmişdir;

d) elektron imza infrastrukturunun yaradılması üçün sonlu sahələr üzərində elliptik əyrilərə əsaslanan kriptoqrafik üsullar və alqoritmlər işlənib hazırlanmışdır.

Nəticə

Məqalədə milli və beynəlxalq qanunvericilik təcrübəsi əsasında kibercinayətkarlıq və kibertəhlükəsizliyin təmin edilməsi, mümkün təhlükələrin və onların mənbələrinin dərk edilməsi məsələlərinə müxtəlif yanaşmaların hüquqi aspektləri təhlil olunmuşdur. Nəticədə kibercinayətkarlıqla bağlı qanunlara olan tələbatın, onların rolunun müəyyən edilməsinə, müzakirə və öyrənilməsinə hələ də ehtiyac olduğu qənaətinə gəlinmişdir. Qeyd etmək lazımdır ki, maddi, prosessual və preventiv-qabaqlayıcı kibercinayətkarlıqla bağlı qanunvericiliyin müəyyənləşdirilməsi, həmçinin sözügedən istiqamətlər arasındakı fərqlərin tədqiqi zəruridir.

Milli, regional və beynəlxalq səviyyəli kibercinayətkarlıq qanunlarının müəyyənləşdirilməsi və müqayisəli dəyərləndirilməsi mübarizənin hüquqi aspektlərinin daha da təkmilləşdirilməsini şərtləndirir.

Qənaətə görə, kibertəhlükəsizliyin təminatında ən yaxşı profilaktik üsullarından biri elmi tədqiqat və hüquqi maarifləndirmə sahəsində beynəlxalq əməkdaşlığın təşkilidir. Demək olar ki, hər bir ölkədə kibercinayətkarlıqla mübarizədə beynəlxalq və milli hüquq sistemlərinin əməkdaşlığının qurulması səmərəli nəticələrin ilkin şərtidir. Təlim və maarifləndirici materialların ictimaiyyətə çatdırılması, o cümlədən bu sahəyə aid məlumatların kütləviləşməsi məqsədilə radio, televiziya və internet resurslarından istifadə, normativ-hüquqi bazaların kütləvi informasiya vasitələri tərəfindən geniş təbliği də bu şərtə daxildir.

İstifadə edilmiş ədəbiyyat siyahısı

1. Convention on Cybercrime. European Treaty Series // – Budapest, –2001 № 185. 23. (XI) – 22 p.: [Electronic resource] / URL: https://rm.coe.int/1680081561

2. Kibertəhlükəsizlik 2021: [Elektron resurs] / URL: http://aggression.az/wp-content/uploads/2019/10/kıtab-kiber-2019-son.pdf

3. Mitra, A., Schwartz, R.L. From Cyber Space to Cybernetic Space: Rethinking the Relationship between Real and Virtual Spaces // Journal of Computer-Mediated Communication's, – 2001, № 1.Vol. 7: [Electronic resource] / URL: http://jcmc.indiana.edu/vol7/issue1/mitra.html.

4. Comprehensive Study on Cybercrime: [Electronic resource] / URL:https:www.unodc.org/documents/organizedcrime/unodc_ccpcj_eg.4_2013/cybercrıme_study_210213.pdf
5. Maras, Marie-Helen. Computer Forensics: Cybercriminals Laws, and Evidence / Oxford University Press. – 2014. – 408 p.
6. Maras, Marie-Helen. Counterterrorism. Jones & Bartlett Learning / – 2012. – 148 p.
7. Основы политики безопасности Эстонской Республики: [Электронный ресурс] / URL:http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/julgeolekupoliitika_aluset_2010.pdf
8. Расулев, А. Противодействие кибертерроризму: международно-правовые и уголовно-правовые аспекты. / А. Расулев – 2018. – 253с.
9. Бенджамин, С. Демократическое управление и вызовы кибербезопасности / С.Бенджамин, Ф. Шрайер, Х. Теодор. – Женева: Женевский центр демократического контроля над вооруженными силами, – 2013. – 334с.
10. Həsənov A.H. Kiber Təhlükəsizlik // Hərbi Bilik, Bakı, 2014, № 5, s. 3-7.
11. Талимончик, В. П. Роль двусторонних договоров, заключенных Российской Федерацией, в международном информационном обмене // Правоведение – 2006. № 5. – 220 с.
12. Якимова, Е., Нарутто, С. Международное сотрудничество в борьбе с киберпреступностью. Криминологический журнал Байкальского национального университета экономики и права // –2016.№.2.Т.1.– с.10: [Электронный ресурс] / URL: https://e-qanun.az/framework/5455
13. “Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya”nın təsdiq edilməsi haqqında // [Elektron resurs] / – qanun.az. URL: https://e-qanun.az/framework/27456
14. Ali məktəblərdə kibertəhlükəsizlik üzrə mütəxəssis hazırlığı problemləri // [Elektron resurs] / URL:https://ict.az/uploads/konfrans/info_sec_2018/rs16_problems_of_educatıng_cybersecurıty_specıalısts_ınunıversıtıes.pdf
15. Məcidli, S.T. Kibercinayətlər / S.Məcidli – Bakı, – 2019. – 314 s.

Аннотация
Киберпреступления: национальные и международные правовые-законодательные аспекты
Захид Орудж

В статье анализируются правовые аспекты различных подходов к вопросам киберпреступности и обеспечения кибербезопасности и понимания возможных угроз и их источников на основе национального и международного законодательного опыта. В настоящее время в период бурного развития информационных технологий количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей. В исследовании подчеркивается, что взаимное изучение и применение существующих законов и прогрессивных практик в области кибербезопасности служат обеспечению лучшей кибербезопасности.

Киберпреступность – это более широкое понятие, чем «интернет-преступность», так как оно включает в себя возможность совершения преступлений с использованием любых информационных или телекоммуникационных сетей. Киберпреступность – это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных.

Однако вопрос о точном и полном понимании киберпреступности, а также о его законодательном закреплении до сегодняшнего дня остается открытым. Сущность данной проблемы заключается в том, что от правильного понимания киберпреступности зависит эффективность работы правоохранительных органов по предупреждению такого рода преступлений.

Исследование позволило прийти к выводу, что анализ доктринальных подходов не показывает единого мнения среди ученых в определении киберпреступности. Это обусловлено различными трактовками киберпространства и способов использования компьютерных систем при совершении противоправных действий. Несмотря на различия ученые ставят вопрос о соотношении национального и международного законодательства относительно перечня противоправных действий, совершаемым в киберсфере.

Ключевые слова: киберпреступность, правовые аспекты, кибербезопасность, национальное законодательство, международное законодательство, правовая борьба, Азербайджан

Abstract

Cyber crimes: national and international legal-legislative aspects

Zahid Oruj

The article analyzes the legal aspects of various approaches to cybercrime and cybersecurity issues and understanding of possible threats and their sources based on national and international legislative experience. Currently, during the period of rapid development of information technology, the number of crimes committed in cyberspace is growing in proportion to the number of users of computer networks. The study emphasizes that the mutual study and application of existing laws and progressive practices in the field of cybersecurity serve to ensure better cybersecurity.

As a concept, it is noted that cybercrime is a broader concept than "Internet crime", since in the first case it includes the possibility of committing a crime using any information or telecommunication networks. Cybercrime - crimes committed in cyberspace against computer systems or computer networks, as well as computer data stored, announced or transmitted in computer networks using other means of access to cyberspace or through them. However, the issue of an accurate and complete understanding of cybercrime, as well as its modification from the point of view of the legislation in the world, the generally accepted approach and uniform definitions, remains open to this day.

The extremely important significance of this problem lies in the fact that the effectiveness of the activities and mutual cooperation of law enforcement agencies in the direction of preventing such crimes directly depends on the correct understanding of cybercrime, common approaches, and the availability of similar legislation.

The study led to the conclusion that the analysis of doctrinal approaches does not show a consensus among scientists in the definition of cybercrime. This is due to different interpretations of cyberspace and ways of using computer systems when committing illegal acts. Despite the differences, scientists raise the question of the relationship between national and international legislation regarding the list of illegal actions committed in the cyber sphere.

Keywords: cybercrime, legal aspects, cyber security, national legislation, international legislation, legal struggle, Azerbaijan

Məqalə redaksiyaya daxil olmuşdur: 08.01.2024
Təkrar işlənməyə göndərilmişdir: 16.01.2024
Çapa qəbul edilmişdir: 05.02.2024