DİN-in Polis Akademiyası "DİO-da idarəetmənin təşkili" kafedrasının rəisi, polis polkovniki, f-r.e.ü.f.d., dosent, əməkdar müəllim

Səməd Hümbətov

Kibertəhlükəsizlik və Azərbaycan

Son on ildə bir çox sahələrdə olduğu kimi idarəetmədə də informasiya kommunikasiya texnologiyalarının geniş tətbiqi müasir dünyada effektiv və sürətli inkişafın optimal yolu kimi qəbul edilir. Artıq demək mümkündür ki, planetimizdə bütün qabaqcıl infrastruktur və istehsal-xidmət sahələri informasiya texnologiyaları vasitəsilə idarə olunur və bu tendensiya daha da artır. Hətta artıq müasir döyüş texnologiyalarını belə, İKT-siz təsəvvür etmək döyüşdə uduzmağa bərabər ölçülür.

Müasir dövrdə informasiya kommunikasiya texnologiyalarının inkişafı kiber-cinayətkarlığın meydana gəlməsinə və gündən günə artmasına gətirib çıxarmışdır. Birləşmiş Millətlər Təşkilatının hesabatında hər il 1.5 milyondan çox insanın internet vasitəsilə edilən cinayətlərin qurbanı olduğu və kibercinayət xarakterli fəaliyyət nəticəsində dəymiş ümumi ziyanın 1 milyard ABŞ dolları təşkil etdiyi bildirilir. Təbii ki, dünyaya tam inteqrasiya olunan dövlətimizdə aidiyyəti sahəyə diqqətin artırılması həm təqdirəlayiq, həm müasir dövrümüzün tələblərindəndir.

Bir çox ədəbiyyatlarda qeyd olunduğu kimi, kibercinayətkarların əsas hədəfi son dövrlərdə yalnız bank sektoru deyil, həm də energetika sahəsidir. Qeyd edilən təhdid obyekti bir çox mənbələrdə enerji infrastrukturu adlandırılır. Narahatlıq yaradan əsas məqam budur ki, son dövrlərdə Azərbaycan regionda adı çəkilən sahədə iri layihələr reallaşdıran ölkələrdən biridir. Davamlı və innovativ iqtisadiyyatın qurulması kursunu götürmüş Azərbaycan şübhəsiz ki, cinayətkarların hədəfinə çevriləcək. Buna görə də bütün əhəmiyyətli sahələrdə kibertəhlükəsizliyi təmin etmək reallığın tələbidir. Nəzərə almaq lazımdır ki, ölkəmizdə bu istiqamətdə az iş görülməyib. Lakin Azərbaycanın təmsil olunduğu layihələrin strateji əhəmiyyətini nəzərə alsaq, kibertəhlükəsizlik tədbirlərinin genişləndirilməsinin zəruriliyi heç kimdə şübhə yaratmayacaqdır.

Dayanıqlı və innovativ iqtisadiyyat qurmağı hədəfləyən respublikamız təbii olaraq kiberorduların hücumlarının hədəfi olacaqdır. Bu baxımdan Azərbaycanda bütün mühüm sahələrdə kibertəhlükəsizliyin təmin edilməsi, elektron kəşfiyyatın, elektron əks-kəşfiyyatın, kiberhücumların dəf edilməsi yönündə xüsusi tədbirlərin görülməsinə böyük ehtiyac yaranmaqdadır. Bu istiqamətdə bir çox addımlar atılmışdır. Bununla belə ölkənin sürətlə ən yeni layihələrə daxil olması və bu layihələrin strateji əhəmiyyət kəsb etməsi paralel olaraq kibertəhlükəsizliyin də təmin edilməsini "A" səviyyəsinə qaldırmağı qaçılmaz edəcək.

Beynəlxalq Telekommunikasiya Şurası (ITU) 2017-ci il üzrə Qlobal kibertəhlükəsizlik indeksini açıqlayıb.

İndeks ITU-nun üzvü olan ölkələrin kibertəhlükəsizliyə məruz qalma səviyyəsini özündə əks etdirir. 193 ölkəni özündə birləşdirən indeks qanunvericilik bazasını, texniki məlumatlar, təşkilati məsələlər, kooperasiya kimi məsələləri əhatə edir. Azərbaycan indeksdə 48-ci yeri (0.559 bal) tutub. Qonşularımıza gəlincə, Gürcüstan 8-ci, Rusiya 10-cu, Türkiyə 43-cü yeri tutub. Ermənistan isə siyahının 111-cisi olmaqla sonda yer alanlardandır.

İnformasiya ehtiyatlarının qorunması, kibertəhdidlərin qarşısının alınması və dəf edilməsi üzrə Rabitə və Yüksək Texnologiyalar Nazirliyi yanında Elektron Təhlükəsizlik Mərkəzinin, həmçinin Xüsusi Dövlət Mühafizə Xidmətinin Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Agentliyinin fəaliyyəti böyük əhəmiyyətə malikdir.

Ölkəmizdə getdikcə artmaqda olan internet istifadəçilərinin sayının hazırda 80 faizə çatdığı, milli internet resurslarının, Azərbaycandilli heyətin inkişaf etdirilməsi üzrə işlərin aparıldığı indiki məqamda məlumatların təhlükəsizliyinin təmin edilməsi, kənardan daxil olan kibertəhdidlərin qarşısının alınması, məlumatlar bazasının müdafiəsinin ən yüksək səviyyədə təşkili məsələləri böyük DATA mərkəzlərinə ehtiyacı ortaya çıxarır. Bu baxımdan beynəlxalq təcrübə əsasında ölkəmizdə ən müasir DATA mərkəzlərinin qurulması istiqamətində intensiv əlaqələr yaradılmışdır.

Azərbaycanda strateji əhəmiyyətli layihələrin reallaşdırılması ilə birlikdə kibertəhlükəsizlik tədbirlərini də gücləndirmək lazımdır. Bu zaman təbii olaraq informasiya-kommunikasiya texnologiyalarının tətbiqi zonalarının və şəbəkəsinin təhlükəsizliyi ön plana çıxır. Çünki bu halda rəqibin İKT sisteminə daxil olmaq artıq onun tam iflic olmasına qədər gətirib çıxara bilir: "Bu məqsədlə artıq bir çox dövlətlər digər ölkələrin gizli məlumatlarını əldə etmək üçün geniş kiberhücumlar təşkil edir və həmin ölkələrdə kiberhucumlar vasitəsilə xaosların yaranması ehtimallarını öyrənirlər. Və təbii olaraq özünümüdafiə tədbirləri də görürlər. Məsələn, artıq Çin-də 50 000 insandan ibarət kiberordu formalaşdırılıb. Rusiyada 12 000 nəfərdən ibarət xüsusi ixtisaslaşdırılmış mərkəz fəaliyyət göstərir. Avropa ölkələrində də xüsusi ordu hissələri və mərkəzlər mövcuddur. Kiber hücumlar vasitəsilə mühüm dövlət təsisatlarının (nəqliyyat, avia, pilotsuz uçan aparatlar, sərhəd-buraxılış, viza və s.) fəaliyyətini iflic etmək və ya digər istiqamətə yönəltmək, bank sistemini iflic etmək mümkündür".

Kibercinayətkarlığın artması bütün dünyada dövlət idarəçiliyi, bank, nəqliyyat, milli təhlükəsizik və digər sistemlərin təkmilləşdirilməsini, kibermüdafiə tədbirlərinin genişləndirilməsini aktual edir. 2012-ci ildə NATO-nun Çikaqoda keçirilən sammitində qəbul olunmuş yekun bəyannamədə də kiberhücumların kəmiyyət və keyfiyyətinin artması faktları bir daha qeyd olunmuş və Alyansa üzv dövlətlərinin

ayrı-ayrılıqda, həmçinin beynəlxalq təşkilatlarla (BMT, Avropa İttifaqı, Avropa Şurası və digərləri) birlikdə vahid kibermüdafiənin təşkilinin vacibliyi vurğulanmışdır. Artıq ABŞ, Rusiya, Çin, İngiltərə, Fransa, Almaniya və bir sıra başqa inkişaf etmiş dövlətlər öz xüsusi kiber qoşunlarını yaradıblar. Bu dövlətlər əsas məqsədlərinin öz şəbəkələrini müdafiə etmək olduğu bildirsələr də, burada hücum əməliyyatlarının aparılması da nəzərdə tutulur.

Ölkəmizdə informasiya kommunikasiyası texnologiyalarının (İKT) geniş tətbiqi bu sahədə davamlı kibertəhlükəsizlik tədbirlərinin həyata keçirilməsini gündəmə gətirmişdir. Xüsusən Dağlıq Qarabağ probleminin mövcudluğu bizi bu məsələ ətrafında daha ciddi tədbirlər görməyə sövq edir. İstənilən situasiyanın, xüsusilə də hərbi münaqişə vəziyyətinin qalibi statusuna yüksəlmək üçün informasiya məkanında son dərəcə tədbirli, çevik, ağıllı məsuliyyətli və peşəkar olmaq lazımdır.

Müasir dövrdə medianın ən mühüm funksiyalarından biri də milli maraqları hər şeydən üstün tutmaq, vətəndaşları, cəmiyyəti vahid məqsəd uğrunda səfərbər etməkdir. Vətənpərvərlik, milli dövlətçiliyə sədaqət, milli maraqlar uğrunda prinsipiallıq KİV-in fəaliyyətinin başlıca prinsiplərini təşkil etməlidir. KİV cəmiyyətdə, xüsusilə gənc nəsil arasında vətənə sevgi hissləri, insanlara mənəvi saflıq aşılamalı, onlarda əsl vətəndaşlıq mövqeyinin formalaşmasına dəyərli töhfəsini verməlidir. Ölkəmizin ərazi bütövlüyünün erməni qəsbkarları tərəfindən pozulması qeyd edilən yönümdə bütün sahələr üzrə təbliğatın vacibliyini şərtləndirir. Və bütün bunlar xüsusi amil kimi kibertəhlükəsizlik məsələlərinə ciddi önəm verilməsini ön sıraya çıxarır.

Bu sahədə hüquqi bazanın formalaşdırılması istiqamətində Azərbaycan beynəlxalq konvensiya və proqramlara qoşulmuş, daxili qanunvericilik bazasını daha da təkmilləşdirmişdir. Belə ki, Azərbaycan 2008-ci ildə Avropa Şurasının "Kibercinayətkarlıq haqqında" Konvensiyasını imzalamışdır (2010-cu ildə ratifikasiya etmişdir). ATƏT çərçivəsində Azərbaycan ATƏT Daimi Şurasının 1039 saylı, "İnformasiya və kommunikasiya texnologiyalarından istifadə ilə bağlı münaqişə risklərinin azaldılması sahəsində etimad quruculuğu tədbirlərinin hazırlanması" adlı qərarı əsasında təsis edilmiş işçi Qrupun işində fəal iştirak edir. İşci qrup tərəfindən hazırlanan və ATƏT-in 2013-cu il Kiyev Nazirlər Şurasında qəbul edilən 1106 sayli qərarin mətninin hazirlanmasinda Azərbaycan nümayəndə heyətinin fəal töhfəsi olmuşdur.

Avropa Şurası çərçivəsində kibercinayətkarlığa qarşı mübarizə daha çox Azərbaycanın aidiyyəti dövlət qurumlarının kibercinayətkarlığa qarşı mübarizə sahəsində imkanlarının təkmilləşdirilməsi ilə əlaqədar layihələrin həyata keçirilməsi ilə bağlı olmuşdur. Avropa İttifaqının maliyyə dəstəyi və Avropa Şurasının icraçılığı ilə hal hazırda 2 əsas layihə həyata keçirilir: "Cybercrime@EAPII" ve

"Cybercrime@EAPIII". Qeyd olunan layihələr Şərq Tərəfdaşlığı regionuna daxil olan dövlətlər üçün həyata keçirilir.

BMT çərçivəsində kibercinayətkarlığa qarşı mübarizədə Azərbaycan BMT Baş Assambleyası tərəfindən qəbul edilən bütün qətnamələrə həmmüəllif qismində qoşulmuşdur.Respublikada informasiya proseslərinin mühafizəsi, sabitliyi və fasiləsizliyi, dövlət orqanlarının informasiya ehtiyatlarının qorunması, bu sahədə təhdidlərin qarşısının alınması, təhlili və qabaqlanması üçün dövlət və qeyri-dövlət informasiya infrastrukturu subyektlərinin, onların istifadəçilərinin fəaliyyətinin əlaqələndirilməsi, kibertəhlükəsizlik sahəsində risklərin qiymətləndirilməsi və idarə olunması, ümummilli hazırlığın və maarifləndirmənin təmin edilməsi məqsədilə 26 sentyabr 2012-ci il tarixində "İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında" Azərbaycan Respublikası Prezidenti tərəfindən Fərman imzalanmışdır. Fərmana əsasən Azərbaycan Respublikası Xüsusi Dövlət Mühafizə Xidmətinin Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Agentliyi və Azərbaycan Respublikası Nəqliyyat, Rabitə və Yüksək Texnologiyalar Nazirliyi yanında əlaqələndirici qurum olan Elektron Təhlükəsizlik Mərkəzi yaradılmışdır.

Bu gün kibertəhlükəsizlik, onlayn təhlükəsizlik, şəbəkələrin etibarlılığı üçün həlledici təminat məsələləri ən mühüm prioritet istiqamətlərdən biri kimi dəyərləndirilir. Bu sahədə effektiv beynəlxalq əməkdaşlıq, çoxtərəfli dialoqun nailiyyəti, uğurlu qərarların qəbulu və bu qərarların həyata keçirilməsi məqsədilə hər il regional və qlobal səviyyədə dövlət, qeyri-dövlət və beynəlxalq qurumlar tərəfindən müxtəlif tədbirlər həyata keçirilir.

Kibertəhlükəsizlik tədbirləri sırasında İKT istifadəçilərinin maarifləndirilməsi də mühüm əhəmiyyət kəsb edir. Bu baxımdan, 30 may 2013-cü ildə "Azərbaycanda kibertəhlükəsizlik" mövzüsunda keçirilmiş dəyirmi masa, NATO Azərbaycan Beynəlxalq Məktəbinin təqdimatında "kibertəhlükəszilik: mövcüd vəziyyət və mühafizə vasitələri", "İnformasiya təhlükəsiziliyi", "Fərdi məlumatların mühafizəsi" mövzularında keçirilmiş seminarlar, 2013-cü ildə Bakıda keçirilmiş Təhlükəsizlik Şurasının "Qərarların qəbulunda və siyasətin həyata keçirilməsində gənclərin iştirakı" konfransı, hər il keçirilən və Xəzər regionunun aparıcı İKT formuna çevrilmiş "Azərbaycan Beynəlxalq Telekommunikasiya və İnformasiya texnologiyaları" (Bakutel) sərgi və konfranslarını göstərmək olar.

Yeri gəlmişkən qeyd edilməsi vacibdir ki, Azərbaycan Respublikası Nəqliyyat, Rabitə və Yüksək Texnologiyalar Nazirliyi (RYTN) yanında Elektron Təhlükəsizlik Mərkəzi kibertəhlükəsizlik sahəsində fəaliyyət göstərən "First" beynəlxalq təşkilatına tamhüquqlu üzv seçilib. Bu isə öz növbəsində ölkədə aidiyyəti sahədə dövlət tərəfindən aparılan siyasətin beynəlxalq səviyyədə davam etdirilməsidir. Zənnimizcə,

bununla da qeyd edilən sahədə təhlükələrdən müasir mühafizə yolları və əlaqəli məsələlərlə bağlı qabaqcıl təcrübə öyrənilməsi daha da əlçatan olar.

Son illərdə təkcə Azərbaycanda deyil, bütün dünyada kibercinayətkarlıqla mübarizə ən aktual məsələlərdən biridir. İldən-ilə internet istifadəçilərinin sayı artır və bununla bağlı kibertəhdidlərin də miqyası artır. Son məlumatlara görə, dünyada il ərzində 500 milyondan ox adam bu cür təhdidlərin qurbanına çevrilir. Azərbaycan bu sahədə Avropa Konvensiyasına qoşulandan sonra həm qanunvericilik, həm də aidiyyəti təcrübə beynəlxalq standartlara uyğunlaşdırılır. Eyni zamanda, “Azərbaycan 2020: gələcəyə baxış” İnkişaf Konsepsiyasında ölkəmizdə kibertəhlükəsizlik sahəsində ciddi tədbirlərin görülməsi, bu sahədə maarifləndirmə işinin aparılması qarşıda duran mühüm vəzifələr kimi müəyyən edilmişdir.

Söylənilən fikirləri tam başa düşmək üçün real həyatın bir hissəsi ilə deyil, tam olaraq müqayisəsinin aparılması məqsədəuyğundur. Başqa sözlə desək, real həyatda istənilən bir inzibati-ərazi vahidində (respublikada, şəhərdə, rayonda və s.) əhalinin sayı çoxalırsa, orada hadisələrin, o cümlədən hüquqpozmaların sayı artır. Bu halda dövlət əlavə olaraq maddi resurslar ayırır, zəruri sayılan tədbirlər hazırlanır və həyata keçirilməsinə başlanılır. Təbii ki, virtual aləmdə də bu eyni cür baş verir və bu səbəbdən də qeyd edilən sahəyə real olaraq diqqət artırılmasını və aidiyyəti hüquq-mühafizə fəaliyyətinin genişləndirilməsini (struktur vahid olaraq, maliyyə resursları, qabaqcıl təcrübənin öyrənilməsi, tətbiqi və s.) məqsədəuyğun hesab edirik.