Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№1(11)/2025, səh. 66-77
HƏRBİ XÜSUSİ ELMLƏR ***MILITARY SPECIAL SCIENCES***

UOT 342 DOI: 10.30546/mk.2024.4.0116

KRİTİK İNFORMASİYA İNFRASTRUKTURLARINA QANUNSUZ MÜDAXİLƏLƏRİN NÖVLƏRİ

Rəşad Məhərrəmov
Milli Müdafiə Universiteti,
Bakı Dövlət Universiteti
maharrramov13@gmail.com

Xülasə. Kompüter və internetin hələ yeni inkişaf etməyə başladığı və qlobal cəmiyyətin bütün təbəqələrinin ona çıxışının olmadığı dövrlərdə informasiya sistemlərinə qanunsuz müdaxilələr "ağ yaxalıqlıların cinayətləri" kimi adlandırılırdı. Lakin informasiya sistemlərinin inkişafı, internetin geniş yayılması və bütün dünyada qlobal miqyasda virtual mühitdə sərhədlərin aradan qalxması ilə insanların çıxış imkanları artdıqca belə pozuntuların cəmiyyətin hər təbəqəsindən olan insanlar tərəfindən törədilməsi müşahidə olunmağa başlandı. Hətta şəxslərin informasiya sistemlərinə qarşı hücumları planlı, mürəkkəb və bir neçə nəfərin, bəzən hətta fərqli ölkələrdə olan şəxslərin şəbəkələr vasitəsilə birləşərək iştirakı ilə törədilməsi halları müşahidə olunur. Bu halda, ilk növbədə cinayətkarların tutulması və sübutların əldə edilməsi üçün ölkələrin birgə hərəkət etməsi və əməkdaşlıq etməsi zərurəti meydana çıxmışdır ki, bu da bir sıra beynəlxalq tənzimləmələrin aparılmasını şərtləndirmişdir.

Məqalədə kritik informasiya infrastrukturlarına yönəlmiş qanunsuz müdaxilələrin hüquqi aspektləri təhlil olunmuş, milli və beynəlxalq hüquqi çərçivələr nəzərdən keçirilmiş, həmçinin Azərbaycan Respublikasında bu sahədə mövcud olan normativ-hüquqi baza və onun praktiki tətbiqi araşdırılmışdır. Bundan başqa, daxili və xarici təhdidlərin qarşısının alınması üçün qarşıya çıxan problemlər və onların mümkün həll yolları təhlil olunmuşdur.

Açar sözlər: kritik informasiya infrastrukturu, kompüter sistemi, informasiya sistemi, verilən, informasiya hüquq pozuntusu, kibertəhdid, kiberhücum, kiberinsident, kibercinayət

Giriş

İnformasiya texnologiyalarının sürətlə inkişaf etdiyi müasir dövrdə dövlətlərin dayanıqlığı və təhlükəsizliyi üçün kritik informasiya infrastrukturlarının qorunması mühüm əhəmiyyət kəsb edir. Ölkənin siyasi və müdafiə təhlükəsizliyinin, milli və hərbi-siyasi maraqların qorunması kontekstində daxili və xarici mənbələrdən qaynaqlanan qanunsuz müdaxilələr, kibertəhlükələr və hibrid hücumlar bu sahənin effektiv hüquqi tənzimlənməsini zəruri edir.

İnformasiya sistemlərinə müdaxilələr törədilmə formalarına görə bəzi hallarda cinayətkarla əməl arasında məsafə fərqi olduğu kimi, cinayət təşkil edən əməllərlə əməllərin nəticələrinin baş verdiyi yerlər də fərqli ola bilər. Məsələn, cinayətkar informasiya sisteminə daxil olaraq sistemdəki məlumatları əldə edərək əməlini Azərbaycan sərhədləri daxilində həyata keçirsə də, informasiya sisteminin IP ünvanı Çikaqo mərkəzli ola biləcəyi kimi, qanunsuz yolla əldə etdiyi məlumatlarla Rusiya sərhədləri daxilində başqa bir informasiya sisteminə də qanunsuz yollarla daxil olaraq digər informasiya sisteminə qarşı da qanunsuz olaraq daxilolma cinayətini törədə bilər. Burada dəlillərin toplanması, qoruyucu tədbirlərin görülməsi və məhkəmə prosesinin hansı ölkənin qanunvericiliyinə əsasən aparılacağı kimi bir çox məsələlər qarşımıza çıxır ki, bütün bunlar tədqiqat mövzusunun aktuallığını şərtləndirir.

Məqalənin ümumi metodoloji əsasını nəzəri-tarixi təhlil, müqayisəli təhlil, statistik məlumatların təhlili təşkil edir. Tədqiqat zamanı həm Azərbaycan, həm də xarici tədqiqatçıların elmi əsərləri, eləcə də beynəlxalq hüquq normaları təhlil olunmuşdur.

Məqalənin hazırlanmasında əsas məqsəd kritik informasiya infrastrukturlarının qorunması və hüquqi tənzimləmələrin təkmilləşdirilməsi istiqamətində praktik təkliflər verməklə, bu sahədə milli təhlükəsizliyin daha etibarlı şəkildə təmin olunmasına töhfə verməkdir.

Məqalədə əvvəlcə tədqiqat mövzusu üzrə əsas anlayışlara nəzər yetirilmiş, sonra kritik informasiya infrastrukturlarına dair milli hüquqi yanaşma təhlil edilmiş, daha sonra kritik informasiya infrastrukturlarına qanunsuz müdaxilələrin təsnifatı aparılaraq, səmərəli təcrübi və hüquqi tövsiyələr işlənib hazırlanmışdır.

Kompüter sistemi və kompüter məlumatlarının mühafizəsi informasiya təhlükəsizliyinin əsas elementi kimi

İnformasiya sistemləri və informasiya sistemlərinin kommunikasiyasında zəruri olan internet gündən-günə həyatımızda daha çox yer tutur. Səhiyyə, iqtisadiyyat, müdafiə, təhsil və digər bir çox sahələrdə informasiya və internetin günbəgün daha da fəal şəkildə istifadə edildiyinin şahidi oluruq. İnformasiya sistemlərinin həyatın hər sahəsinə daxil olması ilə vaxt və işçi qüvvəsinə qənaət edilmişdir. Lakin informasiya sektorunun bu qədər inkişaf etməsinin ardınca informasiya sistemlərinin və sistem istifadəçilərinin təhlükəsizlik sferasında boşluqlar da meydana çıxır. Bəşər tarixinin hər mərhələsində olduğu kimi, kompüter və internet şəbəkələrinin geniş yayılması ilə keçmişdə və indiki dövrdə informasiya hüququnun həm texniki, həm də nəzəri cəhətdən təhlil edilərək araşdırılması və daim yenilənməsi zəruridir.

Kompüter sistemi və kompüter məlumatlarının mühafizəsini informasiya təhlükəsizliyinin obyekti qismində şərh etməzdən əvvəl, əsas anlayışlara hüquqi münasibət bildirmək lazımdır.

Kompüter anlayışı. Kompüterə müxtəlif dillərdə fərqli adlar verilsə də, 1974-cü ildə keçirilən beynəlxalq ISO (International Standard Organization) Konfransından sonra kalkulyator və ya məlumat emal maşını kimi terminlərin yerinə "kompüter" termininin kompüterin vahid adı kimi istifadə edilməsi tövsiyə olunmuşdur [1, s.9]. Buradan da aydın olur ki, kompüterin quruluşu istifadə olunan texnologiyadan tamamilə asılı deyildir [1, s.28].

Kompüteri digər elektron hesablama və proqramlaşdırıla bilən sistemlərdən fərqləndirən cəhət onun hesablama xüsusiyyətinə malik olması, yəni ümumi məqsədli istifadə oluna bilməsidir. Bu səbəbdən, kompüter yetərincə yaxşı təyin olunmuş və tərtib edilmiş hər cür problem üzərində işləyə bilən məlumat emal maşındır [2, s.26]. Beləliklə, gündəlik həyatda istifadə etdiyimiz soyuducu, qabyuyan maşın və ya soba kimi müəyyən məqsədlər üçün əmrləri yerinə yetirən elektron cihazlardan fərqli olaraq, kompüter özünə daxil edilən məlumatlar/kodlar vasitəsilə çoxsaylı problemləri həll etmək üçün proqramlaşdırılmışdır. Nəticə etibarilə, kompüter rəqəmsal kodlarla ifadə olunan məlumatlarla ümumi proqramlaşdırma apara bilən cihazdır.

"İnformasiya" termini fransız dilində olan "informatique" sözünün Azərbaycan dilinə tərcümə olunması ilə yaranmışdır. İnformasiya anlayışı Avropa İqtisadi Birliyi Ekspertlər Komissiyasının may 1983-cü il tarixli Paris Görüşündə "məlumatları avtomatik emala tabe tutan və ya məlumatların ötürülməsinə xidmət edən bir sistemdə qanunsuz, qeyri-etik və ya səlahiyyətsiz həyata keçirilən hər cür davranış" kimi müəyyən olunmuşdur [3, s.21].

İnformasiya anlayışı elektron şəkildə məlumat axınını təmin edən cihazlarla nizamlı şəkildə işlənməsi işlənmiş məlumatlar nəticəsində yaranan informasiya prosesinin ötürülməsi və bu şəkildə məlumat axını trafikini ifadə edən bir anlayışdır [4, s.546]. Beləliklə, informasiya anlayışı daha geniş şəkildə insanların texniki, sosial, iqtisadi, hüquqi, mədəni və digər müxtəlif məlumatların elektron mühitdə müxtəlif əməliyyat vasitələri ilə işləndikdən sonra yüksək sürətli məlumat, səs və görüntü daşıyan rabitə vasitələri ilə ötürülməsinin aparıldığı elektron mühit kimi müəyyən oluna bilər [5, s.870; 2, s.131]

"İnformasiya" və "kompüter" terminlərini anlayış baxımından təhlil etdikdə, onların bir-birindən fərqli olması aşkar görünür. Buna görə də qanunvericilikdə bu iki anlayışın bir-birinin yerinə istifadəsinin doğru olmadığı qəbul edilir [5, s.858]. Müəlliflərə görə, informasiya kompüterə nisbətən daha böyük bir anlayışı ifadə edən üst termindir. Kompüter məlumatların saxlanılması, işlənməsi və yenidən qiymətləndirilməsi fəaliyyətlərini, yəni məlumatların emalı proseslərini təkbaşına yerinə yetirə bilir. İnformasiya isə kompüterdən fərqli olaraq, həm məlumatların işlənməsini, həm də məlumatların ötürülməsini, yəni əlaqəsini ifadə edir [6, s.30-31].

İnformasiya cinayətləri ümumilikdə kompüter sistemi üzərindən törədilə bildiyinə görə "kompüter cinayətləri" kimi (anlayış baxımından informasiya cinayətləri yerinə) adlandırılsa da, kompüter, informasiya sistemində "kompüter" terminə verdiyimiz tərifə əsasən informasiyanın alt anlayışıdır. Bu anlayış qarışıqlığının səbəbi informasiya cinayətlərinin Amerikada ortaya çıxması nəticəsində Amerika Qanunvericiliyində "computer crimes" ifadəsinin digər ölkələrdəki hüquqşünaslar tərəfindən də informasiya cinayətlərində qəbul edilməsidir [5, s.858].

Amerika qanunvericiliyində geniş şəkildə istifadə olunan "kompüter cinayətləri" ifadəsi ilə yanaşı, "kompüterlə bağlı cinayət" (computer-related crime), "kompüter vasitəsilə törədilən cinayət" (computer-assisted crime), "kompüterə qarşı cinayətlər" (crimes against computer), "kibercinayətlər" (cybercrimes), "yüksək texnologiyalı cinayətlər" (high-tech crimes) və "texnoloji cinayətlər" (techno-crimes) kimi ifadələr də bu cür cinayətləri ifadə etmək üçün istifadə olunur [7, s.104]. Lakin cinayəti adlandırarkən yalnız cinayətin törədilməsində istifadə edilən vasitə olan "kompüter" terminini istifadə etməyimiz əhatə dairəsi baxımından qeyri-kafi (səhv) olar. İnternetin geniş yayılması və baş verən böyük inkişaflar nəticəsində cinayətləri ifadə etmək üçün "internet cinayəti" və ya "kiber cinayət" anlayışlarının istifadə edildiyi müşahidə olunur. Ünverin fikrinə görə, İnternet/kompüter cinayətkarlığı sahəsindəki qurumlar, subyektlər və əməl xüsusiyyətləri baxımından termin və anlayış birliyinə nail olunmalıdır. Bəzi müəlliflərin seçdiyi "internet cinayəti" termini yanlışdır. Burada internet, intranet və ya ekstraneti də əhatə edən "kiber məkan" və ya "informasiya sistemi" anlayışları cinayətin törədildiyi məkanı, cinayətin işlənməsində vasitəni və ya bəzən maddi obyekti ifadə edir, deyərək, "internet cinayəti" ifadəsinin yalnız internet mühitində və internet vasitəsilə törədilən cinayətlər üçün istifadə edilə biləcəyini bildirmişlər [8, s.78-79].

Qeyd edilməli olan digər bir məsələ isə Avropa Şurasının Budapeşt Konvensiyasında yer alan "kibercinayət" anlayışıdır. Kibercinayət informasiya sisteminin təhlükəsizliyini və/və ya ona bağlı olan məlumatları və/və ya istifadəçini hədəf alan və informasiya sistemindən istifadə edilməklə törədilə bilən cinayətdir. Respublikamızın tərəfdaş olduğu Avropa Şurasının Kiber Cinayət Konvensiyasına əsasən, kompüter məlumatları və sistemlərinin məxfiliyinə, bütövlüyünə və əlçatanlığına qarşı cinayətlər kateqoriyasında qanunsuz giriş, müdaxilə, məlumatlara müdaxilə, sistemə müdaxilə, cihazların sui-istifadəsi; kompüterlə bağlı cinayətlər kateqoriyasında isə kompüterlə bağlı saxtakarlıq, kompüterlə bağlı dələduzluq, uşaq pornoqrafiyası ilə bağlı cinayətlər, müəllif hüququ və ona bağlı hüquqların pozulması ilə əlaqədar cinayətlər sadalanmışdır. Bizim fikrimizcə, yuxarıda da qeyd etdiyimiz kimi, dar mənada özünə hesab kodları ilə verilən konkret məlumatları işləyən və bu əmrlərə uyğun olaraq proqramlaşdırma apara bilən kompüterin yerinə, "kompüter" anlayışını da özündə ehtiva edən daha geniş və üst anlayış olan "informasiya" ifadəsinin bütün cinayət növlərini ifadə etmək üçün istifadə olunması daha uyğundur.

Hərf, rəqəm, qrafik və ya təsbit edilməsi mümkün olan digər işarələrdən ibarət məlumatlar kompüterin özünə görə işlədiyi məlumatlardır. "Sistem daxilindəki bütün elementlər məlumat xarakteri daşıyır" şəklində informasiya sisteminin tərifi verilərək kompüterin informasiya fəaliyyətində əməliyyatın həyata keçirildiyi vasitə olduğu qeyd olunmuşdur. Bu ifadədən də aydın olduğu kimi, "informasiya" anlayışı "kompüter" anlayışına görə daha geniş, əhatəli və texnoloji inkişaflarla birlikdə dəyişən cinayət potensialını qarşılamağa xidmət edən ifadə olduğuna görə bu sahədəki bütün cinayət növlərini əhatə edən bir məfhum kimi istifadə olunur.

Mövzumuzla bağlı digər termin isə kompüter tərəfindən üzərində əməliyyat aparıla bilən hər cür dəyər kimi təyin olunan "kompüter məlumatı"dır. "Məlumat" ingilis dilindəki "data" sözünün qarşılığı olaraq dilimizdə yer almışdır. Məlumat hər cür informasiyanın kompüterlərin işləyə biləcəyi, işlədiyi informasiya ilə əməliyyat apara biləcəyi, lazım gəldikdə saxlaya biləcəyi və saxladığı informasiyanı zərurət olduqda yenidən işləməyə başlaya biləcəyi informasiyaların mücərrəd rəqəmsal formatda çevrilmiş halıdır [9, s.23; 2, s.29]. Kompüter və ya informasiya sistemi tərəfindən saxlanıla bilən, əməliyyat aparıla bilinən hər cür səsli, vizual, rəqəmsal, loqaritmik məlumatlardır.

Avropa Şurasının Kibercinayətkarlıq haqqında Konvensiyası "kompüter məlumatı" anlayışına yer verərək, bu anlayışı kompüter sisteminin müəyyən funksiyanı yerinə yetirməsini təmin edən proqramlar

da daxil olmaqla, kompüter sistemində işlənməyə yararlı hər cür məlumat və konsept kimi müəyyən etmişdir.

Kompüter və internetin cəmiyyət tərəfindən daha asan əldə edilə bilməsi, qlobal olaraq fərdlər tərəfindən gündəlik həyatın hər sahəsində istifadə olunması və daha da əhəmiyyətlisi, "kompüter" anlayışını özündə ehtiva edən və "kompüter" anlayışını aşan xüsusiyyətdəki informasiya sektoruna daxil olan bütün proqramların geniş yayılması ilə informasiya sahəsində törədilən cinayətlərin tərifi və təsnifatı qaçılmaz olmuşdur.

İlk olaraq informasiya sahəsində törədilən cinayətlərin terminoloji baxımından adlandırılmasında fərqliliklərin olduğunu görürük. 2001-ci il tarixli Avropa Şurası Konvensiyasında "kibercinayət" ifadəsi yer aldığı üçün 2012-ci ildən etibarən ölkəmizin cinayət qanununda da bu termindən istifadə olunur.

Əslində, informasiya sahəsindəki cinayətlərin tərifində istifadə olunan anlayışlar arasındakı müxtəliflik tarixi inkişafla müasirləşən texnologiyadan irəli gələn yeni ehtiyacları və anlayış bütövlüyünü daha yaxşı qarşılamaq probleminin nəticəsidir. Baş verən texnoloji inkişaflar, hər gün internetə çıxışın genişlənməsi və qloballaşan dünyada informasiya axınının və informasiyanın gündən-günə artması informasiya cinayətlərinə tərif verilməsini çətinləşdirir və bu cinayətlərin anlayış məzmununu genişləndirir.

Hal-hazırda kompüter və internet vasitəsilə informasiya cinayətlərinin törədilməsi səbəbindən "internet cinayətləri" [10, s.447] kimi adlandırma aparılsa da, belə bir terminin istifadəsi informasiya cinayətlərini izah etmək üçün doğru deyil. Daha əvvəl də izah etdiyimiz kimi, "informasiya" anlayışı üst anlayış olub, informasiya sahəsindəki bütün anlayışları özündə ehtiva edir. Bu səbəbdən, informasiya cinayətləri geniş şəkildə internet mühitində həyata keçirilsə də, internet cinayətləri terminini istifadə etmək informasiya cinayətlərinin bütün növlərini əhatə etmək üçün yetərli deyil.

Hazırda informasiya sistemi vasitəsilə törədilmə halı ilə, xüsusilə internet mühitində tez-tez rast gəlinən saxtakarlıq, narkotik və ya psixotrop maddə istehsalı və ticarəti, xüsusi işarə və geyimlərdən qanunsuz istifadə, qanunsuz qumar və mərc oyunları, qumar oynanması üçün yer və imkan təmin edilməsi, hədə-qorxu, şantaj, xalqı nifrət və düşmənçiliyə təhrik etmə və ya alçaltma, məlumatları qanunsuz olaraq vermə və ya əldə etmə cinayəti kimi bir çox cinayət informasiya sistemləri vasitəsilə daha asan törədilə bilsə də, qanun müddəalarında bu cinayətlərin informasiya sistemləri ilə törədilməsi halında xüsusi tənzimləmə və ya ağırlaşdırıcı səbəb qanun maddələrində açıq şəkildə tənzimlənmiş formada yoxdur. Qeyd etdiyimiz bu cinayətlərin informasiya sistemləri vasitəsilə törədilməsi həm cinayətkarların bu cinayətlərə çıxışını asanlaşdırır, həm də cinayətlərə hazırlıq hərəkətləri ilə cinayətin tamamlanmasını asanlaşdırır. Bundan əlavə, informasiya sistemləri vasitəsilə baş verən texnoloji inkişaflar nəticəsində informasiya sistemlərində törədilən cinayətlərə dair dəlil əldə etmə və cinayətkarların müəyyən edilməsinin gündən-günə çətinləşməsi qarşısında bu cinayətlərə qarşı ədalətsizlik məzmunu artır. Saxtakarlıq, narkotik və ya psixotrop maddə istehsalı və ticarəti, xüsusi işarə və geyimlərdən qanunsuz istifadə, qanunsuz qumar və mərc oyunları, qumar oynanması üçün yer və imkan təmin edilməsi, hədə-qorxu, şantaj, xalqı nifrət və düşmənçiliyə təhrik etmə və ya alçaltma kimi cinayətlərin informasiya sistemləri vasitəsilə törədilməsinin Qanunda açıq şəkildə ağırlaşdırıcı hal kimi tənzimlənməsi cinayətkarların daha ağır cəzalarla qarşılaşması vəziyyətini yaradacağından, cinayətlərin qarşısının alınmasına yönəlik töhfəsi nəzərə alındıqda belə bir tənzimləmənin zəruriliyi ortaya çıxır.

Kritik informasiya infrastrukturlarına müdaxilələr milli təhlükəsizliyə təhdidlərdən biri kimi

Əvvəlcə, "kritik infrastruktur" və "kritik informasiya infrastrukturu" terminlərinə aydınlıq gətirək. Kritik infrastrukturlar zədələndiyi və ya məhv edildiyi təqdirdə tədarük zənciri, sağlamlıq, təhlükəsizlik və iqtisadi və ya iqtisadi sistemlər də daxil olmaqla cəmiyyətin mühüm funksiyalarına ciddi təsir göstərəcək maddi resurslar, xidmətlər, informasiya texnologiyaları sistemləri, şəbəkələr və infrastruktur aktivləri zərər görmüş olar. Kritik infrastruktur termini 2001-ci il ABŞ Patriot Aktının 1016(e) Bölməsində millət üçün müəyyən həyati əhəmiyyət kəsb edən həm fiziki, həm də virtual sistemlər və mallar kimi müəyyən edilmişdir ki, onların nasazlığı və ya məhv edilməsi ölkənin təhlükəsizliyinə,

millətin iqtisadi təhlükəsizliyinə, milli ictimai sağlamlıq və yuxarıda göstərilənlərin hər hansı bir kombinasiyasına zəiflədici təsir göstərəcək. 2004-cü ilin iyununda Avropa Şurası İttifaq ərazisində kritik infrastrukturların mümkün terror hücumlarından qorunması strategiyasının hazırlanmasına çağırış təşəbbüsü ilə çıxış etdi və bu, Komissiyanın 2004-cü il tarixli 702 saylı Kommunikasiyasını dərc etməsinə səbəb oldu. 2008-ci ildə Komissiya 2008/114/EC Direktivinin təsdiq edilməsinə rəhbərlik etmişdir ki, bu Direktiv hazırda kritik infrastrukturlara dair Aİ qanunvericiliyinin əsasını təşkil edir. Direktivdə kritik infrastrukturlar üzv dövlətlərdə yerləşən və cəmiyyətin həyati funksiyalarının, vətəndaşların sağlamlığının, təhlükəsizliyinin və iqtisadi və sosial rifahının təmin edilməsi üçün vacib və zəruri olan element, sistem və ya onun bir hissəsi kimi müəyyən edilmişdir.

"İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanununun 2-ci maddəsinə əsasən, kritik infrastruktur – dövlətin, cəmiyyətin və vətəndaşların normal fəaliyyətini təmin edən və fəaliyyətində fasilə yaranması milli təhlükəsizlik, ictimai sabitlik və rifaha ciddi təsir göstərə biləcək aşağıdakı sahələri əhatə edir:

- dövlət idarəçiliyi;
- müdafiə və təhlükəsizlik;
- səhiyyə sistemi;
- maliyyə bazarları;
- energetika sektoru;
- nəqliyyat infrastrukturu;
- informasiya texnologiyaları və telekommunikasiya;
- su təchizatı və ətraf mühitin qorunması.

Kritik informasiya infrastrukturu isə bu sahələrin fasiləsiz və təhlükəsiz fəaliyyətini təmin edən texnoloji vasitələrin məcmusudur. Bu vasitələrə aşağıdakılar daxildir:

- avtomatlaşdırılmış idarəetmə sistemləri;
- informasiya-kommunikasiya şəbəkələri;
- informasiya sistemləri.

Bu infrastrukturun funksional pozuntuları milli təhlükəsizliyə, ictimai maraqlara və vətəndaş hüquqlarına əhəmiyyətli dərəcədə zərər vura bilər.

Kritik infrastrukturlar həm informasiya texnologiyaları, həm də əməliyyat texnologiyaları şəbəkələrini ehtiva edir. Əməliyyat texnologiyalarının təhlükəsizliyinin təmin edilməsi ilk növbədə informasiya texnologiyalarından keçir. Çünki təcavüzkarlar əməliyyat texnologiyalarına çatmaq üçün informasiya texnologiyalarından sıçrayış nöqtəsi kimi istifadə edirlər. Bu vəziyyətin nümunəsi 2015-ci ildə Ukraynada 225.000 istifadəçinin elektrik enerjisinin kəsilməsinə səbəb olan kiberhücumda özünü göstərmişdir. Təcavüzkarlar əvvəlcə hədəfli fişinq hücumu ilə informasiya texnologiyalarına, sonra BlackEnergy 3 zərərli proqram təminatından istifadə edərək istifadəçi hesabı məlumatlarını əldə etmiş və əməliyyat texnologiyaları şəbəkəsinə sızmışlar [11, s.5-6].

Kritik informasiya infrastrukturlarına müdaxilələrin milli hüquqda təsnifləndirilməsi

Kritik informasiya infrastrukturlarına müdaxilələr daxili və xarici təhdid formasında ola bilər. Məhz bu baxımdan müdaxilənin hüquqi qiymətləndirilməsi beynəlxalq və milli-hüquqi aspektdən aparılır. Belə ki, kiberməkanın sərhədlərinin genişliyi səbəbindən ilə bir çox hallarda xarici təhdidlər bir neçə dövlətin ərazisini əhatə etmiş olur. Bu zaman müdaxiləyə hüquqi yanaşma fərqli xüsusiyyətlərə malik olur.

Qeyd olunanları nəzərə alaraq, informasiya sistemlərinə müdaxilələr çərçivəsində kiberhücumları və informasiya hüquq pozuntularını (həm cinayətlər, həm də inzibati pozuntular) nəzərdən keçirməyi məqsədəuyğun sayırıq.

Kritik informasiya infrastrukturlarına qarşı təhdidlərin ortaya çıxmasında üç səbəb var. Bunlar internet mühiti və informasiya bazasındakı boşluqlar (internet ünvanlaşdırma sahəsi, adı, sistemi, internetə çıxışı təmin edən sistemlərin əksəriyyətinin ümumi çıxışa açıq və şifrsiz olması, zərərli və

təhlükəli proqramları yaymaq qabiliyyəti və internetin mərkəzləşdirilməmiş geniş şəbəkə olması), informasiya avadanlığı ilə proqramlar arasındakı xətalar və boşluqlar, kritik sistemlərə onlayn çıxışın asan olmasıdır [12, s.25].

İnformasiya sahəsinə qarşı ən çox həyata keçirilən hücum növləri bunlardır:

1. **Gizli dinləmə (Sniffing).** İnformasiya axınının olduğu virtual yolu kəsmək kimi təyin olunur. İngilis dilindəki qarşılığı "iyləmək" olan "sniffing" informasiya sistemləri arasındakı informasiya mübadiləsinin dinlənilməsi deməkdir. Sniffingin məqsədi şifrləri (*e-poçt, veb, ftp, telnet, SQL*) və ötürülən fayllardakı məlumatları ələ keçirməkdir [13, s.3].

2. **Xidmətdən kənarlaşdırma (Denial of Service).** Təqdim olunan xidməti yavaşlatmaq və ya tamamilə dayandırmaqdır. Xidmətdən kənarlaşdırma hücumlarının məqsədi sistemi həddindən artıq yükləyərək, onun normal işləməsinin qarşısını almaqdır [13, s.4].

3. **IP saxtakarlığı (IP Spoofing).** Yuxarıda da qeyd etdiyimiz kimi, internetdə informasiya mübadiləsi müxtəlif protokollar vasitəsilə təmin olunur. IP saxtakarlığı da bu protokollar vasitəsilə qoşulan kompüterdə həqiqi IP ünvanının gizlədilərək qoşulan sistemə IP-nin göstərilməməsidir [13, s.4-5]. Saxta IP göndərilən kompüter göndərilən IP-nin həqiqi olub-olmadığını bilməyəcək. Bu hücum ümumilikdə başqasının IP ünvanından e-poçt göndərilməsi və ya müxtəlif informasiya bazalarına (saytlara, forumlara və s.) məzmun yazılması şəklində qarşımıza çıxır. Nəzəri cəhətdən bu hücum həyata keçirilə bilsə də, praktikada IP göndərilən sistem ələ keçirilmədən başqasının kompüterinə fərqli IP-dən qoşulmaq mümkün olmayacaq.

4. **Sosial mühəndislik hücumları.** Bu hücumlar insanların düşüncə, şəxsi ünsiyyət sahələrindən istifadə etməklə müxtəlif aldatma üsullarından istifadə edərək hədəf sistem haqqında məlumat əldə etmək, sistemi ələ keçirmək və ya sistemə daxil olaraq məlumat sızdırmaq şəklində həyata keçirilir. Sosial mühəndislik hücumları vacib məlumatlara və informasiya sistemlərinə qanuni istifadəçilər vasitəsilə çatmaq məqsədilə hücum edənlər tərəfindən texnoloji vasitələrdən istifadə etməkdənsə, insanları aldadaraq istifadəçilərin zəif cəhətlərindən istifadə etməklə həyata keçirilən üsullardır [14, s.9]. Fişinq və istənməyən e-poçt göndərmək sosial mühəndislik hücumlarına nümunədir. Bundan əlavə, sosial mühəndislik hücumunu həyata keçirən şəxsin hücumu hədəflədiyi şirkətə zəng edərək özünü informasiya texnologiyaları mütəxəssisi kimi təqdim etməsi və ya müxtəlif bəhanələrlə sistemə daxil olmaq üçün lazım olan istifadəçi adı və şifri öyrənməsi də sosial mühəndislik hücumudur [15, s.144].

Sosial mühəndislik hücumları ilə əlaqəli digər hücum növü şəxsiyyət oğurluğudur. Şəxsiyyət oğurluğu bir şəxsə məxsus şəxsi məlumatların oğurlandıqdan sonra ümumilikdə şəxsin etibarını qazanmaqla şəxsi inandırdıqdan sonra onun digər şəxsi məlumatlarını əldə edərək qanunsuz əməliyyatlar həyata keçirmək şəklində edilir. Bu hücum texnikası ilə şəxslərin qanuni hesablarından və ya onlayn hesablarından əməliyyat aparmaqla yanaşı, məlumatları ələ keçirilən şəxslər adına icazəsiz pulçıxarma əməliyyatları kimi böyük maddi zərərlərə də səbəb olur [16].

5. **SQL enjeksiyası texnikası.** SQL (Structured Query Language) məlumat bazalarından məlumat seçmək, silmək və yeniləmək kimi əməliyyatları apara bilmək üçün istifadə olunan əməliyyat informasiya bazası dilidir [17, s.62]. SQL enjeksiyası informasiya bazasında olan tətbiqlərə qarşı SQL sorğu dili quruluşu istifadə edilərək sorğu əməliyyatına qarşı edilən hücum növüdür. SQL enjeksiyası veb tətbiqlərdən əldə olunan istifadəçi girişləri ilə yaradılan SQL sorğularının yönləndirilməsi kimi də təyin oluna bilər [13, s.5-6].

6. **Arxa qapılar (Backdoors).** İnformasiya sistemində adi yoxlama zamanı aşkarlanmayacaq, normal identifikasiya proseslərini keçməyə və ya yaradılan bu sistemdən məlumatı olan şəxsə həmin informasiya sisteminə uzaqdan çıxışa imkan verən üsullar "arxa qapı" kimi təyin olunur [17, s.62; 18, s.34]. İnformasiya sisteminə daxil olmaq üçün səy göstərən kibercinayətkarlar sonrakı mərhələlərdə bu sistem boşluqlarını saxlamaq istəyirlər, bu səbəbdən də tez-tez rast gəlinən hal olan arxa qapı üsulu dinləmə agenti yerləşdirilmiş "açıq qapı" buraxmaqdır. Arxa qapı boşluqları bəzi hallarda sistem qurucusu tərəfindən səhvən və ya qəsdən buraxıla bilər.

7. **Fişinq (Phishing).** Ümumilikdə bank məlumatları, hesab məlumatları, kredit kartları və maliyyə məlumatlarının ələ keçirilməsi üçün bu qurumlardan göndərilmiş təəssüratı yaradaraq saxta e-

poçt göndərilməklə məlumatların əldə edilməsi şəklində edilən hücum növüdür. Bu saxta e-poçtun mövzusu ümumilikdə şəxsi şifrlərin dəyişdirilməsi, məlumatların yenilənməsi və ya müvafiq şirkətin veb saytına saxta keçid imitasiyası şəklində göstərilərək dələduzluq fəaliyyəti həyata keçirilir [19, s.57-58]. Bu hücum növü yalnız bank əməliyyatlarına giriş imkanını təmin edən sayt və ya tətbiqlərdə deyil, həmçinin tanışlıq saytlarında, söhbət saytlarında, onlayn alış-veriş saytlarında, aviaşirkətlərin saytlarında və digər bir çox veb saytlarda da qarşımıza çıxır [13, s.7]. Bu hücum növü hal-hazırda tez-tez maliyyə və bank şirkətlərinin korporativ mobil tətbiqlərinin saxta variantının hazırlanması və ya bankomatlara yerləşdirilən kartoxuyucu və saxta klaviatura kimi qurğularla həyata keçirilir. Yenə də sosial media üzərindən kampaniya bildirişi şəklində, e-poçt və ya SMS göndərilməsi yolu ilə məlumatların yenilənməsi kimi aldadıcı ifadələrə yer verərək şəxsləri saxta internet saytlarına yönləndirə və daha sonra şəxslərin bu saxta saytların informasiya sisteminə daxil etdikləri məlumatları oğurlaya bilərlər.

8. **Casus Proqram (Spyware).** Əksər hallarda istifadəçinin razılığı və məlumatı olmadan informasiya sistemindən məlumat toplayaraq bu məlumatları üçüncü şəxslərə çatdırmaq üçün yaradılmış proqram kimi təyin olunur [20]. Ümumilikdə şifrlər, PIN kodları, hesab məlumatları, istifadəçi adları və kredit kartı nömrələri kimi məxfi və şəxsi təhlükəsizliyi maraqlandıran məlumatların toplanması, klaviatura düymələrinə basılmasının izlənməsi, internet tarixçəsinin izlənməsi, sessiya və hesabaçma məlumatları və e-poçt ünvanlarının əldə edilməsi şəklində həyata keçirilir. Casus proqramlar kompüter və ya internet parametrlərinizi öz əmrləri çərçivəsində dəyişdirə, informasiya sistemini istədikləri sistemə və ya informasiya bazasına yönləndirə və bəzən kompüterdə istifadəçinin məlumatı və əməliyyatı olmadan ümumilikdə reklam məzmunlu yeni pəncərələr açа bilər [13, s.7].

9. **Troyanlar (Trojan).** Troyan adlandırılan bu zərərli proqramlar özlərini faydalı proqram kimi göstərərək qarşı tərəfdən yüklənmələrini təmin etməklə informasiya sisteminə daxil olur. Əsasən iki fərqli fayldan ibarətdir. Bu fayllardan birincisi sistem istifadəçisinə göndərilir və istifadəçi zərərli proqramı işə saldıqda informasiya sisteminin bir informasiya kanalını özü üçün açaraq proqramçıya istifadəçinin informasiya sisteminə çıxış imkanı verir. İnformasiya sisteminə Troyan yerləşdirən proqramçı isə ikinci faylı işə salaraq informasiya sistemi sahibinin sisteminə çata bilir [21]. Bu zərərli proqramlar daxil olduqları informasiya sistemindəki istifadəçilərin şəxsi məlumatlarını (şifr, kredit kartı məlumatları, hesab nömrələri, xüsusi və vacib sənədlər) əldə etmək məqsədilə istifadə olunur və bu vəziyyət sistem istifadəçilərinə virus və qurdlardan daha çox ziyan vura bilər. Bundan əlavə, Troyanlar informasiya sistemində bilinməyən açıq qapı buraxa bilər və bununla da digər casus və zərərli proqramların müvafiq informasiya sisteminə çıxışını asanlaşdırmış olar.

Troyanlar yalnız sistemə daxil olmaq və açıq qapı buraxmaqla kifayətlənmir, məlumatları silmək, qarşısını almaq, dəyişdirmək, kopyalamaq və kompüterlərin və ya kompüter şəbəkələrinin işini pozmaq kimi zərərlərə də səbəb olur [22].

10. **Viruslar.** Virus sistemdəki digər məlumatlara və fayllara yoluxaraq yayılan, xüsusi olaraq yaradılmış zərərli proqram növü kimi təyin olunur [13, s.7]. Virus informasiya sisteminə daxil ola bilən, işləyən proqramlara özünü əlavə edə bilən, daxil olduğu proqram və məlumatların strukturunu dəyişdirə və ya poza bilən və özünü çoxalda bilən zərərli proqramlardır. Texniki cəhətdən bu cür zərərli proqramların virus kimi təyin olunması üçün özünün oxşarını yaradıb bunu digər fayl və məlumatlara yerləşdirə bilməsi tələb olunur [19, s.53].

Tarixi baxımdan virus adlandıra biləcəyimiz ilk zərərli proqram 1970-ci illərin əvvəllərində The Rabbit (dovşan) adlandırılan proqramlarla ortaya çıxdı. Milli Standartlar və Texnologiya İnstitutunun (NIST) qeydlərinə görə isə, virus 1986-cı ildə IBM-PC əsaslı "Brain" adlı bir yükləmə sektoru virusudur. Viruslar hal-hazırda zərərli proqramlar arasında ən çox istifadə olunanıdır. Ümumilikdə viruslar informasiya sisteminə daxil olur, istifadəçi fərqinə varmadan özünü sistemdə çoxaldır, informasiya sisteminin əksər hallarda işləməsi üçün zəruri və vacib olan fayl və məlumatlarına yerləşir, yerləşdiyi proqramı qismən və ya tamamilə işləməz hala gətirərək sistemə ziyan vurur. Viruslar ümumilikdə informasiya sisteminə daxil olaraq xüsusi və həssas məlumatları əldə etmək, əldə olunan məlumatlar

müqabilində pul tələb etmək, şəxsi şifrləri əldə etmək və şantaj cinayətini törətmək kimi bir çox səbəblə istehsal olunur və informasiya sisteminə hücum edilir.

11. **Qurdlar (Worms), Bot və Spam.** Özünü informasiya sistemindəki məlumatlara yerləşdirmək əvəzinə, informasiya sisteminə daxil olmaq üçün şəbəkə bağlantıları üzərindən sistem boşluqlarından istifadə edərək sürətlə yayılan zərərli proqramlardır [23, s.56]. Qurdlar özünü bir sistemdən digər sistemə kopyalamaq üçün yaradılmışdır. Lakin viruslardan fərqli olaraq qurdların informasiya sisteminə yoluxması və sistemdə və ya digər informasiya sistemlərinə yayılması üçün heç bir insan hərəkəti tələb olunmur. Əvvəlcə informasiya sistemində fayl və ya məlumat ötürülməsini həyata keçirən proqramların nəzarətinə və işinə təsir edərək ora yerləşir və bir dəfə sistemə yoluxduqdan sonra özü-özünə çoxalaraq digər informasiya sistemlərinə daxil ola bilir [13, s.8]. Bir dəfə informasiya sisteminə yoluxduqdan sonra digər informasiya sistemlərinə çata bilmək üçün şəxsin köməyi olmadan informasiya şəbəkələrindən istifadə edərək digər sistemlərə yayılır [24, s.216].

Botlar müəyyən əmrləri avtomatik olaraq yerinə yetirmək üçün yaradılmış proqramlardır. Botlar informasiya sisteminə daxil olduqdan sonra sistem sahibinin razılığı və ya məlumatı olmadan müəyyən hərəkət və əməliyyatları həyata keçirə bilər [24, s.216]. Hal-hazırda kommersiya məlumatlarının toplanması, e-poçt, oyun, ictimai xəbər qrupu, söhbət, alış-veriş, səhm, proqram təminatı və s. kimi məqsədlərinə görə adlandırılan bir çox bot növlü zərərli proqram mövcuddur.

Spam nformasiya sistemində eyni məzmuna malik birdən çox nüsxəsi olan mesajın belə bir mesajı almaq istəməyən istifadəçilərə istəmədikləri halda göndərilməsidir [25]. Mesaj yağışı kimi də adlandırılan bu cür reklam, məhsul təqdimatı, kampaniya [18, s.46] və ya promosyon qazanma kimi məzmunlarla informasiya sisteminə daxil olmaq istəyən şəxslərin informasiya sistemi istifadəçisinin e-poçt ünvanlarına istənməyən e-poçt göndərməsi şəklində həyata keçirilir. Spam e-poçtlarla birlikdə ötürülən zərərli proqramların informasiya sistemi tərəfindən aşkarlanması çətin ola bilər. Daha çox özlərini faydalı proqram və ya vacib məlumat kimi göstərərək informasiya sistemi istifadəçisinin razılığını alaraq sistemə yerləşir, bu səbəbdən də bir çox təhlükəsizlik tədbirini aşa bilir.

Azərbaycan Respublikasının Cinayət Məcəlləsində əvvəllər "Kompüter informasiyası sahəsində cinayətlər" ifadəsi nəzərdə tutulmuşdusa, hal-hazırda kibercinayətlərə görə məsuliyyəti müəyyənləşdirən fəsil "Kibercinayətlər" adlanır. Maraqlı məqam ondan ibarətdir ki, kibermәkan çox geniş əhatə dairəsinə malikdir və burada yalnız kompüter informasiyası ilə bağlı cinayətlər törədilmir, eyni zamanda kibermühitdən istifadə edərək, digər qeyri-qanuni əməllər (dələduzluq, müəlliflik hüquqlarını pozma, təhqir, böhtan və s.) icra olunur, yəni kibermәkanda mövcud əlaqələr və texniki vasitələr ənənəvi cinayətlərin törədilməsinin yeni üsulları qismində çıxış edə bilir [26, s.414].

İnformasiya hüquq pozuntularının törədilmə üsullarına geniş şərh verən G.A.Rzayeva yazır ki, İKT inkişaf etdikcə kibercinayətlərin törədilmə üsulları da artır və buna adekvat olaraq onlarla mübarizə tədbirləri də gücləndirilməlidir. Çünki bu növ cinayətlər yüksək latentlik səviyyəsi ilə xarakterizə olunur və bu latentlik onların törədilmə üsullarının xüsusiyyətlərindən irəli gəlir. Demək olar ki, əksər tədqiqatçılar latentlik dərəcəsindən asılı olaraq kibercinayətlərin 4 növünü fərqləndirir:

Birinci qrupa baş vermə faktı haqqında nə hüquq mühafizə orqanlarının, nə də zərər çəkmiş şəxslərin heç bir məlumatının olmadığı cinayətlər daxildir. Buna "təbii latentlik" deyilir. Bu növ cinayətlərdə "aşkara çıxarma problemi" hökm sürür.

İkinci qrupa kibercinayətin baş verməməsi barədə məlumat vermək vəzifəsi daşıyan şəxslərin hüquq-mühafizə orqanlarını məlumatlandırmaması ilə bağlı cinayətlər daxildir. Bu isə "süni latentlik" kimi qiymətləndirilir və "məlumat verilməməsi problemi" mövcud olur.

Üçüncü qrupa törədilmiş kibercinayət barəsində hüquq-mühafizə orqanlarına məlumat verilsə də, istintaqı aparan şəxslərin peşəkarlıq səviyyəsinin aşağı olmasından irəli gələrək, əmələ düzgün qiymət verilməməsi və əməldə cinayət tərkibi əlamətlərinin aşkar edilməməsi nəticəsində latent qalan cinayətlər daxildir. Bu isə ədəbiyyatda "sərhəd və ya hissəvi latentlik" adlandırılır.

Dördüncü qrup kibercinayətlər baş vermə halı barəsində hüquq mühafizə orqanlarının məlumatının olduğu, lakin müxtəlif səbəblərdən qeydiyyatı aparılmayan cinayətlər (gizlədilən və ya ört-basdır edilən cinayətlər) hesab olunur [26, s.419].

Tədqiqat mövzumuz kompüter sistemlərinə müdaxilələrlə bağlı olduğu üçün cinayət qanunvericiliyində belə müdaxilələrlə əlaqədar dispozisiyaları da nəzərdən keçirməyi uyğun sayırıq. Bunun üçün 3 maddə üzrə – 271-273-cü maddələr üzrə şərh vermək daha düzgündür. İnformasiya sisteminə qanunsuz daxil olma cinayəti CM-nin 271-ci maddəsində tənzimlənmişdir. Maddənin mətninə 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 olmaya görə məsuliyyət nəzərdə tutulmuşdur. Lakin müdaxilə yalnız qanunsuz daxil olma ilə kifayətlənmir. Ona görə də növbəti dispozisiyanı – 273-cü maddəni də şərhimizə əlavə etməliyik: "Kompüter sisteminə və ya kompüter məlumatlarına qanunsuz müdaxilə, yəni kompüter məlumatlarının qəsdən zədələnməsi, silinməsi, korlanması, dəyişdirilməsi və ya bloklanması buna hüququ olmayan şəxs tərəfindən törədilməklə əhəmiyyətli zərər vurulmasına səbəb olduqda cinayət məsuliyyəti yaranır".

İnformasiya sisteminə qanunsuz daxil olma cinayəti ilə bir növ cinayətin törədilməsinin qarşısını almaq məqsəd güdülür. Çünki informasiya cinayətlərinin ilk mərhələsi əksər hallarda sistemə icazəsiz girişlə başladığından, bu əməl digər cinayətlərin də ilk mərhələsini təşkil edir.

İnformasiya sisteminə qanunsuz daxil olma cinayətindəki "daxil olma" termini ilə informasiya sistemində olan məlumatların bir hissəsinə və ya hamısına fiziki və ya məsafədən başqa sistemlər, proqramlar və yaxud cihazlar vasitəsilə daxil olma halı nəzərdə tutulur. "İcazəsiz giriş" Avropa Komissiyası tərəfindən də "kompüter sistemlərinin bir hissəsinə və ya bütününə edilən icazəsiz girişləri" təsvir etmək üçün istifadə olunur [27, s.117].

Hesab edirik ki, qanunsuz daxil olma əməlini əksər hallarda müdaxilə baş verdikdən sonra aşkar etmək olur. Ona görə də müdaxilə zamanı qanunsuz giriş məqsədi və niyyəti müəyyənləşdirilir.

Nəticə

Kritik informasiya infrastrukturlarına müdaxilələr və ya kibertəhdidlər həm ölkəmizdə, həm də dünyada informasiya sektorunun və informasiya sistemlərinin inkişafına paralel olaraq sürətli inkişaf etmişdir. Lakin hər keçən gün dünya miqyasında yeni bir informasiya cinayəti, yeni bir hücum törədilir və ona görə də dövlətlər informasiya pozuntularına dair tənzimləmələri yeniləməkdə daha operativ olmalıdırlar.

İnformasiya sistemlərinə yönəlmiş və ya informasiya sistemləri vasitəsilə törədilən cinayətlər kiber cinayət, internet cinayətləri, kompüter cinayətləri, virtual cinayətlər kimi adlarla tanınsa da, informasiya sistemlərinə yönəlmiş və ya informasiya sistemləri vasitəsilə törədilən cinayətlərin kibercinayət kimi adlandırılması hüquqi tənzimləmələr baxımından ən uyğun olandır. Tədqiqat mövzumuz çərçivəsində isə daha çox informasiya qanunvericiliyində öz əksini tapmış kiberhücum və kibertəhdid terminlərinə müraciət etmişik. Çünki sistemə müdaxilə və qanunsuz daxil olma yalnız cinayət xarakteri daşımayıb, bir çox hallarda inzibati xəta kimi də törədilə bilir.

Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi Qaydaları kompüter sistemlərinə müdaxilələrlə bağlı bir çox təznimləmələri nəzərdə tutur. Lakin nəzərə almalıyıq ki, nə Qaydalar, nə də informasiya qanunvericiliyi daxili və xarici təhdidləri təsnifləndirmir. Yalnız kiberhücum, kibertəhdid və kiberinsident terminlərinə müraciət edən qanunverici onlara öz hüquqi yanaşmasını təqdim edir. Yaxşı olardı ki, "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Qanunun anlayışlar maddəsində bu məsələ də öz əksini tapmış olardı. Çünki təhdidin daxili və xarici xarakteri onun aşkarlanmasına, subyektlər dairəsinin müəyyən olunmasına, sübutların toplanmasına bilavasitə təsir göstərir.

Azərbaycan Respublikasının cinayət qanunvericiliyində kompüter sistemlərinə müdaxilələr bir neçə tərkib formasında nəzərdə tutulmuşdur. Fikrimizcə, bunlardan qanunsuz daxil olma ilə bağlı 271-ci maddənin mətnində "şəxsi niyyət" ifadəsinin əvəzinə, "bəd niyyət" ifadəsi əlavə olunsa, daha yaxşı olar. Çünki şəxsi xarakteri olmayan, lakin sistemin pozulmasına, məhvinə hədəflənən bir çox niyyətlər ola bilər. Budapeşt Konvensiyasında da belə tənzimləmə nəzərdə tutulmuşdur. Digər bir yanlış tənzimləmə 271-273-cü maddələrə dair qeyddə "ictimai əhəmiyyətli infrastruktur" terminə müraciət

olunmasıdır. Qanunvericiliyin kritik informasiya infrastrukturuna verdiyi hüquqi anlayışı ("İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Qanunun 2-ci maddəsi) qənaətbəxş saydığımız üçün digər sahəvi qanunlarda da bu termindən istifadə olunmasını daha düzgün sayırıq.

Sistemi bloklama, pozma, məlumatları silmə və ya dəyişdirmə başlığı altında törədilən əməl bir informasiya sisteminin işləməsini bloklayan və ya pozan şəxsə qarşı cinayət sanksiyası nəzərdə tutulur. Kiberhücumların dövlət qurumlarına qarşı törədilməsi halında bütün cəmiyyətin zərərçəkən vəziyyətində olacağı və dövlət qurumunun zərərinin bütün cəmiyyəti maraqlandıracağı şübhəsiz bir həqiqətdir. Həm dövlət təşkilatlarının informasiya sistemləri olsun, həm də bank və ya kredit təşkilatının informasiya sisteminə yönəlmiş olsun, törədilən informasiya cinayətinin xüsusi şəxsə yönəlmiş şəkildə həyata keçirilən cinayət əməllərindən daha çox zərər vurması mümkündür. Bu səbəbdən, dövlət qurumlarındakı sistemin təhlükəsizliyinin və məlumatların məxfiliyinin əhəmiyyəti nəzərə alınarsa, bu qurum və təşkilatlarda tətbiq edilən informasiya sistemini istifadə etmək, ona daxil olmaq, sistemdəki məlumatlara giriş səlahiyyəti olan şəxslərin ehtiyatsızlıq əməllərinə görə də məsuliyyət daşıması lazımdır. Ona görə də AR CM-in 273-cü maddəsində 1-ci bənddə təqsirin formasının nəzərdə tutulmamasını təqdirəlayiq hal saymaq olar. Çünki qurum və təşkilatlarda çalışan şəxslərin vəzifələrini yerinə yetirərkən tam diqqət və ehtiyatlılıqla davranması lazımdır.

İnformasiya sistemləri bağlı elementlərin istifadəsinin hər keçən gün həm vaxta, həm də rəqəmsal mühitdə kağız, element və yerə qənaət etməyə imkan yaratması səbəbindən cəmiyyətlərin böyük əksəriyyətində və təşkilatların çoxunda geniş şəkildə istifadəsinə rast gəlirik. Bu da bizim daim informasiya pozuntularının törədilməsində yeni üsullarla qarşılaşmağımıza səbəb olur. Bu məsələni də qeyd etmək istərdik ki, kibertəhdidlərin qarşısının alınması üçün istifadəçilərdən informasiya sistemlərini virus proqramı və ya şifrlə kodlaşdırmaqla qorumasına dair bir məcburiyyət qoyulması gözlənilə bilməz. Burada maarifləndirmə işinin aparılması da zəruri xarakter daşıyır. Sistemə daxil olan hər kəs oradakı verilənlərin qorunmasına dair vəzifə daşıdığını dərk etməlidir.

İstifadə edilmiş ədəbiyyat siyahısı

1. Ifrah. Bilgisayar Ne Sayar: Rakamların Evrensel Tarihi IX. – İstanbul: Kalkedon Yayınları, – 2011. – 134 s.
2. Yazıcıoğlu. Bilgisayar Suçları Kriminolojik, Sosyolojik ve Hukuksal Boyutları ile. – İstanbul: Seçkin Yayıncılık, – 1997. – 185 s.
3. İsmail Tulum. Bilişim Suçları ile Mücadele. – İstanbul: Seçkin Yayıncılık, – 2016. – 195 s.
4. Berrin Akbulut. Bilişim Suçları // Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 2000. 8/1-2, – s. 624
5. Artuk, Ahmet Gökcen ve A. Caner. Yenidünya, Ceza Hukuku Özel Hükümler. – Ankara: Adalet Yayınevi, – 2015. – 903 s.
6. Yenidünya ve Değirmenci, Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları. – İstanbul: Yetkin Yayınları, – 2012. – 220 s.
7. Ö.Umut Eker. Türk Ceza Hukuku"nda bilişim Suçları Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 sayılı Yeni Türk Ceza Kanunu"nun İlgili Hükümlerinin Yorumu // Ankara, Türkiye Barolar Birliği Dergisi, 2006. Sayı 62, – 129 s.
8. Yener Ünver. Türk Ceza Kanunu"nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi. – İstanbul, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 59/1-2, – 2001. – 148 s.
9. Dülger, M. Volkan. Türk Ceza Hukukunda bilişim Suçları. – İstanbul: On İki Levha Yayıncılık, – 2014. – 176 s.
10. Feridun Yenisey. İnternet suçlarının yeni işleniş biçimleri // Uluslararası İnternet Hukuku Sempozyumu, – Dokuz Eylül Üniversitesi Yayını, İzmir, 2002. – 491 s.
11. Lee, R.M., Assante, M.J., Conway, T. Analysis of the cyber attack on the Ukrainian power grid, Electricity Information and Analysis Center, Washington: SANS Institute, – 2016. – 44 p.

12. Fulya Aslay. Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi // International Journal of Multidisciplinary Studies and Innovative Technologies. – İstanbul, – 2017. 1/1, – s.34
13. Arslan. Siber Güvenlik ve Siber Saldırı Türleri: [Elektron resurs] – URL: http://www.academia.edu/31827545
14. M.Zekeriya Gündüz, ve Resul DAİ. Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri: [Elektron resurs] – URL:www.bingol.edu.tr/documents/Sosyal%20M%C3%bchendislikyayg%C4%b1n%20Ataklar%20ve%20G%C3%bcvenlik%20%C3%96nlemleri
15. Hakan Hekim, ve Oğuzhan Başıbüyük. Siber Suçlar ve Türkiye‟nin Siber Güvenlik Politikaları. – Ankara, Uluslararası Güvenlik ve Terörizm Dergisi , – 2013. – 216 s.
16. Kimlik Hırsızlığı Nedir? : [Elektron resurs] – URL: https://www.eset.com/tr/identity-theft
17. Demirol, Daş ve Baykara, SQL Enjeksiyon Saldırı Uygulaması ve Güvenlik Önerileri. Ankara: Çıra Yayıncılık, – 2016. – 142 s.
18. Canbek ve Sağıroğlu. Kötücül ve Casus Yazılımlar: Kapsamlı Bir araştırma // Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, – 2007. 22/1 2007, – s. 64
19. Turhan. Bilgisayar Ağları ile İlgili Suçlar (Siber Suçlar). – İstanbul: İstanbul Hukuk Yayınları, – 2013. – 188 s.
20. Casus Yazılım Nedir? – Tanım: [Elektron resurs] – URL: https://www.kaspersky.com.tr-/resource-center/threats/spyware
21. Virüs, Solucan ve Truva Atı: [Elektron resurs] – URL: http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/vir%C3%bcs-solucan-ve-truva-at
22. Truva Atı Virüsü Nedir?: [Elektron resurs] – URL: https://www.kaspersky.com.tr/resourcecenter/threats/trojans
23. Əmir Əliyev, Qulu Novruzov, Gülnaz Rzayeva, Azər Səfərov, Şahin Məmmədrzalı. İnsan hüquqları, əqli mülkiyyət və informasiya: qarşılıqlı hüquqi əlaqələr. Dərs vəsaiti. Bakı: “Nurlar” nəşriyyatı, – 2021. – 250 s.
24. Əzizov, R.F. “İnternet” şəbəkəsində tənzimləmənin müqayisəli hüquqi təhlili. – Bakı: Elm, – 2017. – 352 s.
25. Spam Nedir? Ne Değildir?: [Elektron resurs] – URL: https://www.chip.com.tr/blog/corpixx-/spam-nedir-ne-degildir
26. İnformasiya hüququ: dərslik / Ə.İ.Əliyev, G.A.Rzayeva, A.N.İbrahimova, B.A.Məhərrəmov, Ş.S.Məmmədrzalı – Bakı: Nurlar nəşriyyatı, – 2019. – 519 s.
27. Erdoğan. Türk Ceza Kanununda Bilişim Suçları. – İstanbul: Seçkin Yayıncılık, – 2015. – 237 s.

Аннотация
Виды незаконного вмешательства в критическую информационную инфраструктуру
Рашад Магеррамов

В те времена, когда компьютеры и интернет только начинали развиваться и различные слои глобального общества не имели к ним доступа, незаконные вмешательства в информационные системы назывались «преступлениями белых воротничков». Однако с развитием информационных систем, широким распространением интернета и устранением границ в виртуальной среде на глобальном уровне доступ к этим технологиям стал более доступным для всех слоёв общества. В результате было замечено, что подобные правонарушения совершаются представителями различных социальных групп. Более того, фиксируются случаи, когда атаки на информационные системы планируются заранее, имеют сложный характер и совершаются группами лиц, иногда находящихся в разных странах и действующих через сетевые объединения. В таких условиях возникает необходимость совместных действий и

сотрудничества между государствами для задержания преступников и сбора доказательств, что обусловило проведение ряда международных правовых регулирований.

В статье сначала рассматриваются основные понятия, относящиеся к исследуемой теме, затем анализируется национальный правовой подход к критической информационной инфраструктуре. Далее проводится классификация незаконных вмешательств в критическую информационную инфраструктуру и разрабатываются эффективные практические и правовые рекомендации.

Ключевые слова: критическая информационная инфраструктура, компьютерная система, информационная система, данные, информационное правонарушение, киберугроза, кибератака, киберинцидент, киберпреступление

Abstract

Types of Unlawful Interference with Critical Information Infrastructures

Rashad Mahharamov

During the early stages of computer and internet development, when access to these technologies was not available to all layers of the global society, unauthorized intrusions into information systems were classified as "white-collar crimes". However, with the advancement of information systems, the widespread availability of the internet, and the removal of borders in the virtual environment on a global scale, access became more accessible to a broader spectrum of people. Consequently, such violations began to be committed by individuals from various social backgrounds. Moreover, instances have been observed where attacks on information systems are planned, complex, and carried out by multiple individuals, sometimes operating from different countries through coordinated networks. In such cases, it has become imperative for countries to act jointly and cooperate to apprehend perpetrators and obtain evidence, which has necessitated the development of various international legal regulations.

The article initially reviews key concepts related to the research topic and then analyzes the national legal approach to critical information infrastructures. Subsequently, a classification of unlawful intrusions into critical information infrastructures is conducted, and effective practical and legal recommendations are developed.

Keywords: critical information infrastructure, computer system, information system, data, information infringement, cyber threat, cyberattack, cyber incident, cybercrime

Məqalə redaksiyaya daxil olmuşdur: 20.04.2025
Təkrar işlənməyə göndərilmişdir: 22.04.2025
Çapa qəbul edilmişdir: 23.04.2025