**TARİX VƏ SİYASİ ELMLƏR**

**UOT 327**

# BEYNƏLXALQ HÜQUQİ AKTLARIN POZULMASI: KİBER CİNAYƏTLƏR NÜMUNƏSİNDƏ

**Elmin HƏSƏNOV***

Məqalə redaksiyaya daxil olmuşdur: 29 yanvar 2024; çapa qəbul edilmişdir: 21 fevral 2024; online-da çap edilmişdir: 21 mart 2024.
Received: 29th of January, 2024; accepted: 21th of February, 2024; published online: 21th of March, 2024.

**Açar sözlər:** *hüquq pozuntusu, kiber cinayətlər, hüquqi aktlar, beynəlxalq hüquq*

## Giriş

Kiberməkan internet, telekommunikasiya, kompüter sistemləri, mobil texnologiyalar, kabel və peyk rabitəsi xidmətləri kimi texniki komponentlərdən ibarət sərhədsiz qlobal platformadır. Kiberməkan öz komponentləri baxımından bütün bəşəriyyətin ortaq yaddaşı kimi təsvir edilir və kiber fəaliyyətlərin fəaliyyət göstərməsini təmin edən loqistik elementlər də ümumi əmtəə hesab edilir. Bu xüsusiyyət kiberməkanda dövlət suverenliyinin və ya mülkiyyət hüququnun yaradılmasını qeyri-mümkün edir.

Dövlətlərin öz ölkələrində kiber infrastruktura və kiber fəaliyyətlərə nəzarət etməsi, kibertəhlükəsizliklə bağlı lazımi hüquqi tənzimləmələr yaratması, sanksiya mexanizmləri yaratması da onların kiberməkanda bir növ suverenlik nümayiş etdirdiyini göstərir. Bununla belə, illər keçdikcə bu, bəşəriyyətə mənfi təsir göstərən fəaliyyətlərin həyata keçirildiyi bir sahəyə çevrilir. Kibercinayətlər bunun bir hissəsi olsa da, əslində bəşəriyyətə qarşı daha böyük təhlükə olacağı gözlənilir. Çünki klassik münaqişə məkanları ilə yanaşı, hazırda kiberməkanın yeni münaqişə meydanına çevrilmişdir [4].

## 1. Beynəlxalq səviyyədə kibercinayətlər

Dövlətlər fəaliyyətlərini həyata keçirən sistemlərini rəqəmsal dünyaya inteqrasiya etdikcə, onlar kiberhücumlara qarşı daha həssas olurlar. Kiberhücum nəticəsində dövlətlər daxilində yaradılmış bəzi infrastrukturların məxfiliyi və birliyi pozula, məlumatlara, resurslara və hər hansı əməliyyata çıxış təsir altına düşə, ictimai xidmətlərin funksiyası fəaliyyətini dayandıra bilər. Kiber dünyada baş verən nizamsızlıq, beynəlxalq sülh və təhlükəsizlik hazırda terrorizm, transmilli mütəşəkkil cinayətlər tərəfindən təhdid edilir [9].

Kompüter sistemlərinə və məlumatlarına hücum edən, bu sistemlərdə qalan, məlumatları oğurlayan, məlumatları saxlayan və bu fəaliyyətlər vasitəsilə saxtakarlıq edən şəxslər və qruplar bu hücumlar vasitəsilə kibercinayətlər törədirlər. Dünyanı geniş şəkildə əhatə edən bu cinayət növü sadəcə qısa bir dövr ərzində 378 milyondan çox insan bu fəaliyyətdən zərər çəkmiş və zərərçəkənlərə 113 milyard dollar maddi ziyan vurulmuşdur. 966,324 min kompüter insanların bank hesablarına sızmaq üçün hazırlanmış zərərli proqramdan təsirlənib. 2016-cı ildə təkcə kiberhücumlar vasitəsilə Banqladeş Mərkəzi

* *Milli Müdafiə Universitetnin adyunktu*
e-mail: elminnk@mail.ru

Bankından 101 milyon dollar oğurlanıb. Estoniya 2007-ci ildə bu hücumlardan təsirləndi və bu hücum hətta insan həyatını təhlükə altına salacaq səviyyəyə çatdı. Həmçinin, 2008-ci ilin avqustunda Rusiya ilə Gürcüstan arasında hərbi gərginlik zamanı, Rusiyanın Cənubi Osetiyanı işğalı zamanı Gürcüstanın internetinin kəsilməsi dünya ilə əlaqəsinin kəsməsi əsas məqsəd olsa da, səhiyyə daxil dövlətin təməl infrastruktur xidmətlərinin çökməsinə səbəb oldu. Bu isə beynəlxalq hüquq normativlərinin pozulması və insan hüquqlarının nəzərə alınmaması faktıdır [16]. Digər bir nümunə, 2007-ci ildə İsrail Suriyadakı obyektlərini bombalayanda Suriyanın hava radar sisteminə kiberhücum nəticəsində radar sistemi İsrail döyüş təyyarələrini aşkar edə bilməmişdir [7].

Kiberhücum kompüterlərə, oxşar şəbəkələrə və ya sistemlərə qarşı təcavüzkar fəaliyyətlər və kritik kiber sistemləri, aktivləri və funksiyaları pozan və ya tamamilə məhv edən fəaliyyətləri əhatə edir. Kiberhücumun vurduğu zərər üç səviyyədədir. Hər şeydən əvvəl, kiberhücum kompüter sistemləri və ya şəbəkələri, proqram təminatı və ya sistemləri hədəf alır. Buna görə də, kiberhücum bilavasitə kiber dünyaya zərər verir. Lakin kiber mühitdə həyata keçirilən hücum birbaşa kompüter sistemlərinə təsir etsə də, sistemə dəyən zərər kompüter sistemlərinin istifadə olunduğu xidmətlərə və bu xidmətdən faydalanan şəxslərə təsir edir. Nəticədə, kiberhücum domino effekti yaradır və təkcə kompüter sistemlərinə deyil, həm də kompüter sistemindən asılı olaraq təqdim edilən xidmətlərə və əlaqədar xidmətlərdən faydalanan şəxslərə zərər verir [11].

Kiberhücumlar, hədəf aldıqları qruplardan və istifadə etdikləri üsullardan asılı olaraq, maddi hücumlarla yanaşı, terror fəaliyyətlərinin də mövzusu ola bilər. Əslində, bəzi terror təşkilatlarının və ya mütəşəkkil cinayətkar təşkilatların dövlətin müəyyən strukturlarına kiberhücumlar həyata keçirməsi, kiberhücumların getdikcə daha çox klassik terror fəaliyyətini əvəzləməsi hadisələri baş verir. Klassik terror fəaliyyətlərindən fərqli olaraq, kiberhücumlar törədən şəxslərin və qrupların şəxsiyyətləri kiberməkanda gizlədilir və aşkarlanması çətindir. Kiberhücumlar kiberhücumun başladığı və təsir etdiyi yerə, hücumu həyata keçirən və hücumdan təsirlənən insanlara görə beynəlxalq ictimaiyyətin böyük marağına səbəb olur. Bu səbəbdən qlobal miqyasda kibertəhlükəsizliyin yaradılması üçün lazımi tədbirlər beynəlxalq hüququn əhatə dairəsindədir (2). Xüsusilə, Avstraliya, Çin, Kuba, Macarıstan, İran, İtaliya, Mali, Hollandiya, Qətər, Rusiya Federasiyası, Böyük Britaniya, ABŞ və Avropa Birliyi kimi beynəlxalq təşkilatlar və dövlətlər kiber fəaliyyətin verdiyi ziyanı doğru anlayaraq, beynəlxalq hüquq normalarının inkişafına dəstək verirlər.

Bundan əlavə, Birləşmiş Millətlər Təşkilatı (BMT), Şimali Atlantika Müqaviləsi Təşkilatı (NATO), Afrika İttifaqı, Cənub-Şərqi Asiya Millətləri Təşkilatı, Avropa Şurası, Qərbi Afrika Dövlətlərinin İqtisadi Birliyi, Avropada Təhlükəsizlik və Əməkdaşlıq, Şanxay Əməkdaşlıq Təşkilatı da beynəlxalq ictimaiyyətin üzləşdiyi kibercinayət problemləri həll edilməsi üçün müəyyən addımlar atırlar [6]. İnformasiya texnologiyaları ilə bağlı qəbul etdiyi qərarlarda məsələnin bütün beynəlxalq ictimaiyyəti əhatə etdiyi və beynəlxalq hüququn, xüsusilə də BMT Nizamnaməsinin kiber fəaliyyətlərə də şamil edildiyi bildirilir. Eyni şəkildə, BMT-də yaradılmış Ekspertlər Şurasının 2013 və 2015-ci illərdə yazdığı hesabatlarda beynəlxalq hüququn, xüsusilə də BMT Nizamnaməsinin kiberməkana tətbiq oluna biləcəyi vurğulanıb.

Kibertəhlükəsizliklə məşğul olan digər beynəlxalq təşkilat NATO-dur. Xüsusilə, Estoniyanın məruz qaldığı kiberhücumdan sonra 2010-cu ilin noyabrında NATO çərçivəsində Yeni Strategiya Konsepsiyası qəbul edildi [10].

Kibercinayətlərin kiberhücum səviyyəsinə çatdığı hallarda, kibertəhlükəsizliyi təmin etmək məqsədilə kiberhücumların qarşısının alınması və kiberterrorizmlə mübarizə məqsədilə beynəlxalq sülh və təhlükəsizliyin təmin edilməsi üçün beynəlxalq hüququn tətbiq etdiyi qayda və mexanizmlərin tətbiqi mümkündür [8, s. 5]. Buna görə də, Birləşmiş

Millətlər Təşkilatının (BMT) 2/IV Nizamnaməsində tənzimlənən güc tətbiqinə qadağa; BMT Nizamnaməsinin 51-ci maddəsində tənzimlənən özünümüdafiə hüququ və hücuma / silahlı hücuma qarşı görülə biləcək digər tədbirlər kiberməkana da aid edildi [3].

BMT Nizamnaməsinin 2/IV maddəsində tənzimlənən güc tətbiqinin qadağan edilməsi ilə; Dövlətlərin beynəlxalq münasibətlərində hər hansı bir dövlətin ərazi bütövlüyünə və ya siyasi müstəqilliyinə qarşı BMT-nin məqsədləri ilə bir araya sığmayan şəkildə təhdid və ya güc tətbiqi qadağandır. Dövlətlərin fəaliyyətinin güc tətbiqi qadağasını pozduğunu müəyyən etmək üçün iki fərqli yanaşmadan bəhs edilir. Bunlardan biri vasitəyə əsaslanan yanaşma, digəri isə təsir yanaşmasıdır. Vasitələrə əsaslanan yanaşma iddia edir ki, güc tətbiq etmək və güc tətbiq etməklə hədələmək qadağanı pozmaq üçün müəyyən alətlərdən, xüsusən də silahlardan istifadə edilməlidir. Digər yanaşmada isə istifadə edilən nəqliyyat vasitəsinin dağıdıcı və zədələyici təsirini nəzərə almaqla qadağanın pozulduğunu müəyyən etmək olar. Bununla belə, kiberhücumların həyata keçirilməsi ilə aydın olur ki, vasitəyə əsaslanan yanaşma güc tətbiq etmə qadağasının pozulmasını müəyyən etmək üçün meyar kimi istifadə edilə bilməz, çünki vasitə silah deyildir. Bu halda kiberməkanda istifadə oluna bilən vasitələrlə güc tətbiqi ilə bağlı qadağanın pozulması hesab edilə bilər.

Həmçinin iddia edilir ki, kiberhücumun güc tətbiqi ilə bağlı qadağanın pozulmasını təşkil etməsi üçün kiberhücuma səbəb olan fəaliyyətin dövlət mənşəli olması ilə yanaşı, hücumun yaratdığı təsir də olmalıdır. Buna görə də, xüsusi şəxslər və qeyri-hökumət qrupları tərəfindən həyata keçirilən kiber hücumlar, hücumun vurduğu zərər nə qədər böyük olsa da, BMT-nin 2/IV güc tətbiqi qadağası çərçivəsində sayıla bilməzdir. Əks fikir kimi, BMT Nizamnaməsinə qeyri-dövlət subyektlərinin daxil edilməsini hədəflədiyi bildirilir.

Kiberhücumlarla bağlı digər hüquqi sənəd NATO çərçivəsində hazırlanmış Tallinn Handbook-dur. NATO tərəfindən yaradılmış Birgə Kiber Müdafiə Mükəmməllik Mərkəzi kibertəhlükəsizliyin hüquqi ölçülərini müzakirə etmək üçün işə başlamış və 2009-cu ildə beynəlxalq ekspert qrupu yaradılmışdır. Mütəxəssislər qrupunun əməyinin məhsulu olan Təlimatın birinci və ikinci versiyalarında kiber fəaliyyətlərə tətbiq edilən hüquqi qaydalar ətraflı araşdırılmışdır. Mövcud beynəlxalq qaydaların işığında kiber fəaliyyətlərə tətbiq olunan prinsipləri yazmışdır. Əslində, təlimatın beynəlxalq sülh və təhlükəsizlik və kiber fəaliyyətlərin müzakirə edildiyi bölməsində gücdən istifadənin qadağan edilməsi hüququ və müdafiə hüququ ilə bağlı qaydaların rəhbər tutulduğu prinsiplər hazırlanmışdır [12].

Kiberhücum və güc tətbiqinin qadağan edilməsi arasındakı əlaqəyə gəlincə, gücdən istifadənin qadağan edilməsi və güc tətbiqi hədəsi Tallin Kitabçasının ikinci variantının 68-ci qaydasında nəzərdə tutulur və bununla paralel yanaşma BMT Nizamnaməsi müvafiq mətndə qəbul edilmişdir. Müvafiq olaraq, BMT-nin məqsədləri ilə bir araya sığmayan bir dövlətin suverenliyinə və ya müstəqilliyinə qarşı güc tətbiqi hədəsini ehtiva edən kiberhücumlar qanunsuz hesab edilir. Maddənin əsaslandırılmasında silahlı qüvvələr tərəfindən güc tətbiqinin məcburi olmadığı, fəaliyyətin dövlət qurumları, dövlət vəzifəli şəxsləri və dövlət adından çıxış edən xüsusi hüquq şəxsləri tərəfindən həyata keçirildiyi bildirilir. Bu səbəbdən güc tətbiq etmə qadağasının əhatə dairəsinə daxil olan fəaliyyətin dövlətlə əlaqələndirilməli olduğu, qeyri-dövlət subyektlərinin fəaliyyətinin şiddətindən asılı olmayaraq, qanun çərçivəsində ola bilməyəcəyi bildirilib. Davam edən 69-cu qaydada, kiberhücumun ölçüsü və təsirini nəzərə alaraq, onun güc tətbiqi qadağasına zidd ola biləcəyi tənzimlənir. Nəticə etibarilə, kiberhücum klassik mənada hücum sayıla bilər və güc tətbiqi ilə bağlı qadağanın pozulmasını təşkil edə bilər.

Eyni zamanda, kiberhücumun silahlı hücum sayılmaq üçün sırf fiziki ziyana səbəb olub-olmaması müzakirə mövzusuna çevrilib. Bir fikrə görə, kiberhücum nəticəsində xidmətin tələb olunan şəkildə yerinə yetirilməməsi nəticəsində ciddi fiziki zərər baş verərsə, güc tətbiqi qadağasının pozulmasından danışmaq olardı. Kiberhücum maliyyə bazarlarının

uzun müddət çökməsinə və dövlət iqtisadiyyatına ziyan verilərsə və milli valyutanın həddindən artıq dəyərdən düşməsi və bu təsirlər kifayət qədər ciddi həddə çatmışsa, bu kiber hücumun silahlı hücum kimi qələmə verilməsi mümkündür.

## 2. Kibercinayətlərin qarşısının alınmasında hüquq normativləri

Azərbaycan Respublikasında da Kibercinayətkarlıq haqqında Konvensiyanın Təsdiq edilməsi qanunlarında öz əksini tapmışdır. Aşağıda diqqət yetirək:

Avropa Şurasının üzv dövlətləri və bu Konvensiyanı imzalayan digər dövlətlər;

Avropa Şurasının məqsədinin onun üzvləri arasında birliyə nail olmaqdan ibarət olduğunu nəzərə alaraq;

bu Konvensiyanı imzalayan digər dövlətlərlə əməkdaşlığı möhkəmləndirməyin əhəmiyyətini etiraf edərək:

digər tədbirlərlə yanaşı, müvafiq qanunvericilik aktlarının qəbul edilməsi və beynəlxalq əməkdaşlığın möhkəmləndirilməsi vasitəsilə cəmiyyəti kibercinayətkarlıqdan qorumağa yönəlmiş cinayət hüququ sahəsində ümumi siyasətin prioritet qaydada aparılması zərurətindən əminliyi qeyd edərək;

rəqəmsal texnologiyaların həyatımıza daxil olması, kompüter şəbəkələrinin birləşməsini və qloballaşmasının səbəb olduğu əhəmiyyətli dəyişiklikləri dərk edərək;

kompüter şəbəkələrinin, elektron məlumatların cinayətlərin törədilməsi üçün istifadə edilməsi və bu növ cinayətlərin baş verməsinə dair sübutların bu şəbəkələrdə saxlanılması və ya şəbəkələr vasitəsilə ötürülməsi təhlükəsindən narahat olaraq;

kibercinayətkarlığa qarşı mübarizədə dövlətlərlə özəl sektor arasında əməkdaşlığın zəruriliyini və informasiya texnologiyalarından istifadə və onların inkişaf etdirilməsi sahəsində qanuni mənafelərin müdafiə edilməsi zərurətini anlayaraq;

kibercinayətkarlığa qarşı səmərəli mübarizə aparmaq üçün cinayət hüququ sahəsində geniş, operativ və normal beynəlxalq əməkdaşlığın tələb olunduğunu nəzərə alaraq;

Hazırkı Konvensiyanın müvafiq əməlləri cinayət kimi qeyd etmək, bu cür cinayət əməllərinə qarşı mübarizə aparmaq üçün zəruri səlahiyyətlər vermək, onların həm ölkədaxili, həm də beynəlxalq səviyyədə tədqiqatı, istintaqı və təqib olunmasına şərait yaratmaq, sürətli və etibarlı beynəlxalq əməkdaşlığı təmin etmək yolu ilə kompüter sistem və şəbəkələrinin, o cümlədən kompüter verilənlərin məxfiliyi, bütövlüyü və yararlılığına qarşı yönəlmiş əməllərin, həmçinin bu sistem, şəbəkə və verilənlərdən qeyri-qanuni istifadənin qarşısını almaq zəruriliyindən əmin olaraq;

Hüquqi qayda-qanunun saxlanması maraqları ilə 1950-ci il tarixli "İnsan hüquq və əsas azadlıqların müdafiəsi haqqında" Avropa Şurasının Konvensiyasında, Birləşmiş Millətlər Təşkilatının 1966-cı il tarixli "Mülki və Siyasi Hüquqlar haqqında" Beynəlxalq Paktında, o cümlədən hər kəsin fikir və mülahizələrinin maneəsiz ifadə etmək hüququnu və, dövlət sərhədlərindən və şəxsi həyata müdaxilə ilə bağlı hüquqdan asılı olmayaraq, hər növ məlumat və ideya axtarmaq, əldə etmək və yaymaq azadlığını təsdiq edən insan hüquqları haqqında beynəlxalq müqavilələrdə nəzərdə tutulmuş əsas insan hüquqlarına hörmət edilməsi arasında lazımi balansın təmin edilməsi zərurətini xatırlayaraq tədbirlər planını nəzərə alınmışdır [14].

İnternet və fiziki məkan arasında həm kəmiyyət, həm də keyfiyyət baxımından fərqlər bu fərqli domenlər daxilində həyata keçirilən cinayət fəaliyyətlərində də aydın görünür. Kibercinayətkarlıqla mübarizənin effektivliyi və səmərəliliyi bu fərqlərdən irəli gələn problemlərin hərtərəfli təhlilinə, həll yolları tapılarkən nəzərə alınmasına, kibercinayətkarlıqla mübarizədə informasiya-kommunikasiya texnologiyalarından (İKT) yaranan imkanların müəyyən edilməsinə və istifadəsinə əsaslanır. Beləliklə, kiberməkan

təkcə cinayət əməllərinin baş verməsini asanlaşdırmır, həm də onların aşkarlanması və ya qarşısının alınması üçün yeni perspektivlər və çətinliklər təqdim edir [1].

Kompüter cinayətlərinin obyektiv tərəfi həm aktiv, həm də passiv davranışla fərqlənir. Hərəkət kompüter məlumatlarından istifadə ilə bağlı hüquq və mənafelərin pozulması ilə əlaqədardır. Daha əvvəl qeyd edildiyi kimi, kompüter cinayətləri maddi aktivləri əhatə edir. Buna görə də, bu hərəkətsizlik fərdin, cəmiyyətin və ya dövlətin hüquq və mənafelərinə ciddi ziyan vurmalıdır. Buna baxmayaraq, AR CM-nin 272-ci maddəsində göstərilən hüquqpozmalar, elektron cihazlar üçün zərərli proqram təminatının yaradılması, istifadəsi və ya yayılması istisna olmaqla, daha çox formal cinayətlərdir. Cinayət Məcəlləsində kompüter cinayətlərinin müxtəlif kateqoriyalarına uyğun olaraq müəyyən edilmişdir. Buna görə də, qanunsuz hərəkətlər və onların nəticələri arasında səbəb-nəticə əlaqəsinin qurulması vacibdir. Kompüter cinayətlərinin subyektiv elementi qəsdin nümayişi ilə təqsirkarlığın təzahürünə aiddir. AR CM-nin 24-cü maddəsinin 2-ci hissəsinə əsasən, ehtiyatsızlıqdan törədilmiş hərəkət (hərəkət və ya hərəkətsizlik) yalnız bu Məcəllənin Xüsusi hissəsinin müvafiq maddəsində göstərilən konkret hallara aid olduqda cinayət sayılır. Cinayət Məcəlləsinin xüsusi bölməsinin 272.2 və 273.2-ci maddələrində ehtiyatsızlıq da daxil olmaqla, kompüterlə bağlı bəzi hüquqpozmalar nəzərdə tutulur.

CM-nin 271.2.2 və 273.1-ci bəndlərində xüsusi subyekt, yəni elektron hesablama maşınlarından, elektron hesablama maşın sistemindən və ya onların şəbəkələrindən istifadə etmək üçün hüququ olan fiziki şəxs üçün də meyarlar nəzərdə tutulur. Kompüter məlumatlarının icazəsiz əldə edilməsi (Cinayət Məcəlləsinin 271-ci maddəsində göstərildiyi kimi): Cinayətin birbaşa hədəfi sahibinin kompüter sistemində olan məlumatların toxunulmazlığı hüququdur. Bu cinayətinin obyektiv hissəsi qanunla qorunan kompüter məlumatlarına icazəsiz daxil olmaqdır. Buraya müxtəlif elektron cihazlarda və onların şəbəkələrində saxlanılan məlumatlar daxildir. Bu hərəkətin nəticəsi əldə edilmiş məlumatın qəsdən məhv edilməsidir. Bu kontekstdə məlumat informasiya sistemlərində saxlanılan şəxslərə, obyektlərə, faktlara, hadisələrə və əməliyyatlara aid olan məlumatlara aiddir [17].

Qanunla müəyyən edildiyi kimi, kompüter məlumatlarına "giriş" dedikdə, fiziki şəxs tərəfindən informasiyanın daxil edilməsi və ya məlumatın emalı prosesinə təsir göstərilməsi yolu ilə əldə edilməsi və ya istifadə edilməsi aktı başa düşülür. Əgər fiziki şəxs kompüter sistemi və ya şəbəkə sahibinin razılığı və ya müvafiq qanuni icazəsi olmadan bu hərəkəti həyata keçirirsə, bu, "qanunsuz" giriş hesab olunur. Bu cinayət əməlinin obyektiv hissəsinin əsas göstəricisi sahibkara və ya məlumatın saxlanmasına dəymiş ziyandır, məlumatın məhv edilməsi, təcrid edilməsi, dəyişdirilməsi, təkrarlanması və ya pozulması, habelə EHM-nin işinə müdaxilə ilə təzahür edir. Məlumatın məhv edilməsi məlumatın sadəcə silinməsi deyil, bərpasını qeyri-mümkün edəcək şəkildə qəsdən aradan qaldırılmasına aiddir [15].

**Nəticə**

Beynəlxalq hüquq baxımından ciddi nəticələrə səbəb olan kiberhücum zamanı tətbiq olunacaq hüquqi rejim beynəlxalq sülh və təhlükəsizliyin bərqərar olması üçün tətbiq edilən hüquqi rejimlə eynidir. Çünki bu xarakterli hücumlar təkcə zərər çəkmiş dövlətə deyil, həm də beynəlxalq ictimaiyyətə qarşı edilən ədalətsiz hərəkətlərdir. Bu səbəbdən kiberhücumları gücdən istifadənin qadağan edilməsi və özünümüdafiə hüququ çərçivəsində qiymətləndirmək mümkündür. Bu məsələlər kibercinayətlərin araşdırılması üçün yeni üsulların və vasitələrin, onların icrası üçün yeni yolların və imkanların yaranması ilə nəticələndi və bu, potensial kibercinayətkarlıq hədəflərinin kəmiyyət və miqyasında əhəmiyyətli artıma səbəb oldu. Kibercinayətkarlıqla mübarizə üçün əsas tələblərə kibermənin fərqli xüsusiyyətləri, infrastruktur üzərində özəl sektorun və vətəndaş nəzarətinin

üstünlüyü, effektiv institusional strukturların yaradılması, elmi-texniki nailiyyətlər və hüquqi baza daxildir. Bundan əlavə, hökumət, özəl sektor, vətəndaşlar və beynəlxalq qurumlar arasında əməkdaşlığın və tərəfdaşlığın təşviqi çox vacibdir.

## ƏDƏBİYYAT

1. Balacanov, E. Kibercinayətlərlə mübarizə: çətinliklər və imkanlar. Bakı: 2015, s. 56-58
2. Brown, G. International Law Applies to Cyber Warfare! Now What? Southwestern Law Review. 2017, 375 pp.
3. DeWeese, G. S. Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenge of Imminence. Ankara University Faculty of Law Journal// 2019, 68(1), 127-212.
4. Gervais, M. Cyber Attacks and the Laws of War. Berkeley Journal of International Law. 2012, 526 pp.
5. Gill, T. D., & Ducheine, P. A. L. Anticipatory Self Defense in the Cyber Context. International Law Studies. 2013, 439 pp.
6. Group of Governmental Experts on Developments in Information and Telecommunications in the Context of International Security. Report A/68/98// 2013, p.14
7. Hathaway, O., et al. The Law of Cyber-Attack. California Law Review// 2012, pp. 837-839
8. Jensen, E. T. The Future of the Law of Armed Conflict: Ostriches, Butterflies, and Nanobots// Michigan Journal of International Law. 2014, pp. 263-264
9. Lynn III, W. B. Department of Defense Speech. 2011 (http://archive.defense. gov/speeches/ speech.aspx?speechid=1593)
10. North Atlantic Treaty Organization. Defense and Security Strategic Concept. 2010, Clause 12, 40 pp.
11. Roscini, M. Cyber Operations and the Use of Force in International Law. Press: Oxford University. 2014, 307 pp.
12. Schmitt, M. Computer Network Attacks and the Use of Force in International Law: Reflections on a Normative Framework// Columbia Journal of Transnational Law. 1999, pp. 914-915
13. Schmitt, M., & Vihul, L. (Eds.). Tallinn Manual 2.0 On the International Law Applicable to Cyber Access. Cambridge University Press. 2017, 30 pp.
14. https://e-qanun.az/framework/18619
15. https://www.pa.edu.az/library/5/36/584_monoqrafiya_kiber_cin_2020.pdf
16. https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-human-rights-and-cybercrime-law.html
17. https://e-qanun.az/framework/46947

***Резюме***

***Эльмин Гасанов***

***Нарушения международного права: пример киберпреступлений***

Наряду с развитием технологий правительственные учреждения, а также частные учреждения и организации, работающие в критически важных инфраструктурных секторах, таких как энергетика, связь, водные ресурсы, сельское хозяйство, здравоохранение, транспорт, образование и финансовые услуги, начали использовать информационные и коммуникационные технологии. Однако использование киберпространства в важных государственных услугах и услугах, предоставляемых отдельными лицами, несет с собой новые проблемы безопасности; Аналогичным образом, использование компьютеров во многих видах деятельности отдельных лиц привело к появлению нового типа преступлений.

Киберпреступность – это незаконная деятельность, которая конкретно направлена на использование компьютера, компьютерной сети или сетевого устройства или предполагает его использование. Большая часть киберпреступлений совершается киберпреступниками или хакерами с целью

получения финансовой выгоды. Тем не менее, киберпреступность иногда нацелена на системы или сети с целью причинения вреда, а не только ради финансовой выгоды.

Киберпреступлениями могут заниматься как люди, так и организации. Некоторые киберпреступники демонстрируют высокий уровень организации, используют сложные методы и обладают исключительными техническими знаниями.

Распространение киберпреступности представляет собой серьезную проблему для международного сообщества, угрожая фундаментальным правам и безопасности как отдельных лиц, так и стран. В нем рассматриваются нарушения международного права в контексте киберпреступности, которая охватывает широкий спектр незаконной деятельности, осуществляемой через цифровые платформы и сети. Киберпреступность охватывает различные правонарушения, включая мошенничество, кибершпионаж и распространение вредоносного ПО. Эта деятельность часто пересекает национальные границы, используя взаимосвязанную природу Интернета для неизбирательной атаки на отдельных лиц, организации и правительства. Совершение киберпреступлений нарушает многочисленные международные законы и принципы, включая право на иммунитет, свободу выражения мнения и защиту персональных данных. В эпоху цифровых технологий люди более уязвимы для слежки, утечки данных и онлайн-преследований, что подрывает их способность осуществлять свои права в цифровом мире.

**Ключевые слова:** *Правонарушение, киберпреступления, правовые акты, международное право*

***Summary***

***Elmin Hasanov***

***Violations of International Law: the Example of Cyber Crimes***

Along with the development of technology, government agencies and private institutions and organizations operating in critical infrastructure sectors such as energy, communication, water resources, agriculture, health, transportation, education and financial services have started using information and communication technologies. However, the use of cyberspace in important government services and services provided by individuals brings with it new security challenges; Similarly, the use of computers in many activities of individuals has given rise to a new type of crime.

Cybercrime refers to illegal activities that specifically aim at or involve the use of a computer, computer network, or networked device. The majority of cybercrime is perpetrated by cybercriminals or hackers with the intention of financial gain. Nevertheless, cybercrime sometimes targets systems or networks with the intention of causing harm, not just for financial gain.

Both people and organizations may engage in cybercrime. Certain cybercriminals exhibit a high level of organization, use sophisticated methods, and possess exceptional technical expertise.

The spread of cybercrime is a significant challenge for the international community, threatening the fundamental rights and security of both individuals and nations. It examines violations of international law in the context of cybercrime, which covers a wide range of illegal activities carried out through digital platforms and networks. Cybercrime covers a variety of offenses including fraud, cyberespionage and the distribution of malware. These activities often cross national borders, using the interconnected nature of the Internet to target individuals, organizations, and governments indiscriminately. The commission of cybercrimes violates numerous international laws and principles, including the right to immunity, freedom of expression and protection of personal data. In the digital age, individuals are more vulnerable to surveillance, data breaches and online harassment, undermining their ability to exercise their rights in the digital world.

**Key words:** *Legal infringement, cyber crimes, legal acts, international law*

Redaksiya heyətinin üzvü s.e.d., prof. Nəsirli Elman Xudam oğlunun (şöbə redaktoru) rəyi əsasında çapa məsləhət görülmüşdür.