BAKI UNİVERSİTETİNİN
XƏBƏRLƏRİ

ВЕСТНИК
БАКИНСКОГО УНИВЕРСИТЕТА

NEWS
OF BAKU UNIVERSITY

HUMANİTAR
elmləri seriyası

серия
ФИЗИКО-МАТЕМАТИЧЕСКИХ НАУК

series of
PHYSICO-MATHEMATICAL SCIENCES

№ 1, 2020

Bakı – 2020

HÜQUQ

ORCHID ID: https://orcid.org/0000-0002-3134-8486

KİBERTƏHLÜKƏLƏR VƏ ONLARIN TƏSNİFATI

A.N.İBRAHİMOVA
Bakı Dövlət Universiteti
aytakin_ibrahimli@mail.ru

Müasir cəmiyyətdə internet insanın gündəlik həyatının ayrılmaz hissəsinə çevrilmişdir. Lakin heç də bütün internet istifadəçiləri qanuna riayət edən insanlar deyil. İKT-dən müxtəlif qeyri-qanuni məqsədlər üçün istifadə və onun yaratdığı fəsadlar dövrümüzün aktual problemlərindən biridir ki, bu da kibercinayətlərlə bağlı məsələləri gündəmə gətirir. Məqalədə kibercinayətlərin məzmunu açılır, onların leqal və qeyri-leqal təsnifatı müqayisəli təhlil edilir, kibercinayətlərin profilaktikasına dair təklif və tövsiyələr irəli sürülür.

Açar sözlər: informasiya təhlükəsizliyi, kibertəhlükə, kiber cinayətlər, kiber cinayətlərin təsnifatı, kiber müharibə, məlumat, əlyetərlik, tamlıq, konfidensiallıq.

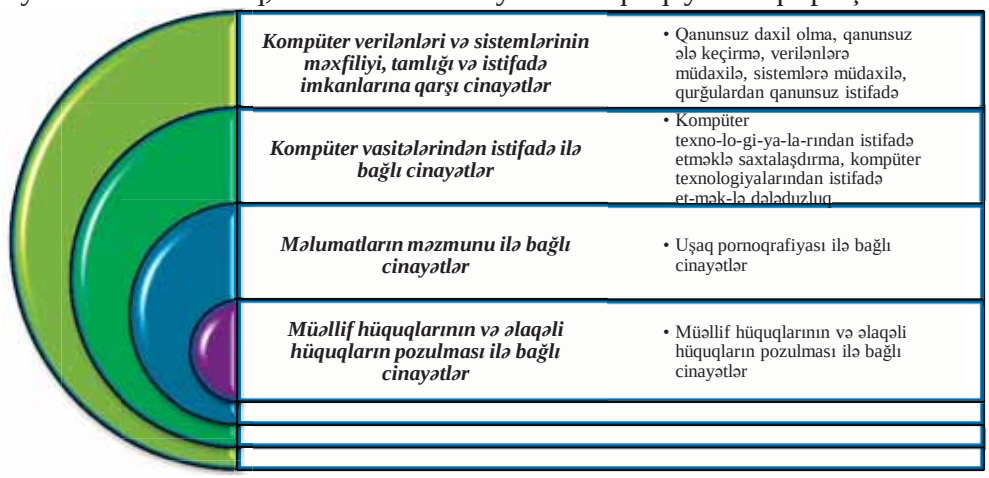
1.1. Giriş

Rəqəmsal cəmiyyətdə ənənəvi münasibətlərdə baş verən dəyişikliklər hüquq pozuntularına da təsir göstərmişdir. Dövrün aktual probleminə çevrilmiş kibertəhlükələr geniş məzmuna malikdir və onları konkret sahəvi qanunvericilik aktı ilə tənzimləmək mümkün deyil. Belə ki, ictimai təhlükəli olan kiber pozuntular cinayət qanunvericiliyində, inzibati xətanın əlamətləri ilə səciyyələnən pozuntular inzibati qanunvericilikdə, müxtəlif deliktlər mülki qanunvericilikdə nəzərdə tutulmuşdur və s. Digər bir problem ondan ibarətdir ki, kibertəhlükələrin obyekt və subyekt tərkibi çox müərəkkəbdir. Onlar nəinki konkret vətəndaşa qarşı yönəlir, hətta böyük bir xalqın mənəviyyatına mənfi təsir göstərir (məsələn, informasiya müharibələri). Bütün bu qeyd olunanlar kibertəhlükələrin qarşısının alınması üzrə təklif və tövsiyələrin işlənməsini zəruri edir.

Texnoloji inkişaf, süni intellekt sistemlərindən istifadə, əşyaların interneti kimi tandemlər kibercinayətlərin təsnifatının tez-tez yenilənməsini tələb edir. Ənənəvi bölgüdə yeni subkateqoriyalar artırmaqla yeni kiber pozuntuların da kriminallaşdırılması və onlara qarşı mübarizə aparılması vacibdir.

1.2. Kibercinayətlər kibertəhlükələrin bir növü kimi

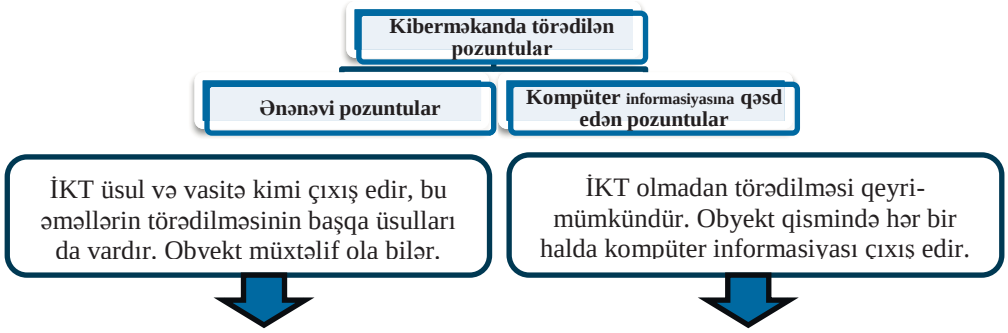
İKT-nin sürətli inkişafı nəticəsində formalaşan anlayışlardan olan ***"kibercinayətkarlıq"*** çox geniş məzmuna malikdir. Ədəbiyyatda həmçinin "kompüter cinayətkarlığı" terminindən də istifadə olunur. Fikrimizcə, ikinci anlayış texniki aspektdən yanaşmanın nəticəsidir və birinci anlayış daha geniş olduğu üçün məqbul hesab olunmalıdır. Təsadüfi deyil ki, Azərbaycan Respublikasının Cinayət Məcəlləsində əvvəllər "Kompüter informasiyası sahəsində cinayətlər" ifadəsi nəzərdə tutulmuşdusa, hal-hazırda kibercinayətlərə görə məsuliyyət 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. Bəs belə olan halda "kibercinayət" anlayışının hədləri artmırmı? Cinayət Məcəlləsində yalnız kompüter informasiyası ilə bağlı cinayətlərin kibercinayətlər qismində tanınmasında qanunvericinin mövqeyi doğrudurmu? – "Kibercinayətkarlıq haqqında" 23 noyabr 2001-ci il tarixli Budapeşt Konvensiyasına nəzər salsaq, burada kibercinayətlər fərqli qaydada qruplaşdırılır:



Göründüyü kimi, Konvensiya kibercinayətləri kompüter cinayətlərinə və kompüter vasitəsilə törədilən cinayətlərə bölür. Əslində Konvensiyanın mövqeyi ilə razılaşmaq olar. Çünki yuxarıda sadalanan cinayətlərin hamısı kibermәkanda törədilir. Təbii ki, Azərbaycan Respublikasının cinayət qanunvericiliyində həmin əməllərin hamısı sanksiyalaşdırılmışdır. Sadəcə olaraq onlar kibercinayətlər fəslində deyil, müxtəlif fəsillərdə nəzərdə tutulmuşdur. Müasir dövrdə İKT-nin bütün insan həyatını əhatə etdiyini və onlardan kriminal məqsədlər üçün istifadənin geniş vüsət aldığına əsaslansaq, informasiya texnologiyaları cinayət əməllərinin törədilməsi üçün ən asan üsul kimi qiymətləndirilməlidir. Belə olan təqdirdə kibermühitdən istifadə etməklə törədilən bütün

cinayətlərin kibercinayət kimi qəbul olunması bir qədər məntiqi sayılmır. Çünki cinayət əməllərinin obyekti və motivi (məqsədi) fərqli olur. Digər tərəfdən isə kiberməkanda törədilən bir çox əməllərin ənənəvi üsullarla da törədilməsi mümkündür. Məsələn, Azərbaycan Respublikası Cinayət Məcəlləsinin 171-1-ci maddəsində nəzərdə tutulan uşaq pornoqrafiyasının dövriyyəsi – uşaq pornoqrafiyasını yayma, reklam etmə, satma, başqasına vermə, göndərmə, təklif etmə, əldə edilməsinə şərait yaratma, yaxud yaymaq və ya reklam etmək məqsədilə hazırlama, əldə etmə və ya saxlama ilə müşayiət olunur. Belə pornoqrafik məhsullar isə yalnız kiberməkanda deyil, müxtəlif nəşrlər, əşya və materiallar formasında da yayıla bilər. Bütün bunlara istinad edərək, Azərbaycan Respublikasının qanunvericiliyinin yanaşmasını məqbul saymaq olar. Sadəcə olaraq İKT-nin inkişaf etdiyi mühitin xüsusiyyətlərini nəzərə alıb, bir çox ənənəvi cinayətlərin törədilməsi üsulları ilə bağlı dəyişikliklərin edilməsi məqsədəmüvafiqdir. Digər bir məsələ isə ondan ibarətdir ki, terrorizm və s. bu kimi təhlükəli cinayətlər Konvensiyanın normalarından kənarda qalmışdır. Tvitter, Youtube və digər şəbəkələrdə müxtəlif terrorçuluğa açıq çağırışların (məsələn, İŞİD) yayılması kompüter vasitəsilə törədilən cinayətlərin siyahısının artırılmasını tələb edir.

Qeyd olunanlar əsasında belə bir nəticəyə gəlmək olar:



Adı çəkilən Konvensiya ilə yanaşı, başqa rəsmi təsnifatlar da vardır. Belə təsnifatlardan biri 1991-ci ildə İnterpolun işçi qrupu tərəfindən hazırlanmışdır. Bu təsnifatda bütün kodlar "Q" hərfi ilə başlayan eyniləşdiriciyə (identifikatora) malikdir. Onlar özləri də qəsdin növündən asılı olaraq 6 qrupa bölünür ki, burada da "A", "F", "D", "R", "S", "Z" hərflərindən istifadə olunur. Məsələn, "QA" hərf birləşməsindən ibarət kod – İcazəsiz (sanksiyalaşdırılmamış) giriş və ələ keçirməni, "QF" birləşməsindən ibarət kod – kompüter dələduzluğunu, "QR" kodu – qanunsuz surətçıxarmanı (piratçılığı) əks etdirir və s. Bu kodların hər birinin cinayətin törədilmə üsulundan asılı olaraq öz təsnifatı aparılır. Hər bir təsnifatda ardıcıllıq cinayətin ictimai təhlükəsinin azalması istiqamətində gedir.

Avtomatlaşdırılmış axtarış-informasiya sisteminə daxil edilmiş İnterpol kodlaşdırması bir çox kibercinayətlərin aşkar edilməsində geniş imkanlara malikdir.

Qeyri-rəsmi təsnifatlardan isə Debra Littlejon Şinderin verdiyi təsnifatı daha geniş şərh kimi qiymətləndirmək olar. Belə ki, D.L.Şinder kibercinayətlərin iki kateqoriyasını [2, p. 19-33] fərqləndirir: zorakılıqla törədilən və zorakılıqla müşayiət olunmayan (qeyri-zorakı) cinayətlər. Müəllif zorakılıqla törədilən cinayətlərə kiberterrorçuluğu, hədə-qorxu ilə (təhdidlə) hücumu,[1] kibertəcavüzü,[2] uşaq pornoqrafiyasını daxil edir. Zorakılıqla müşayiət olunmayan kibercinayətləri isə D.L.Şinder müxtəlif subkateqoriyalara ayırır: qanunsuz daxil olma,[3] kiberoğurluq, kiberdələduzluq, dağıdıcı kibercinayətlər[4] və digər kibercinayətlər.

D.L.Şinder hər subkateqoriyanın tərkibində müxtəlif cinayətləri qruplaşdırır. Məsələn, kiberoğurluğun plagiat, qanunsuz mənimsəmə, piratçılıq, fərdi məlumatların ələ keçirilməsi və s. növlərini fərqləndirir [2, p. 24]. Digər kibercinayətlərə isə internet-qumarxanaların təşkili, internet qaçaqmalçılığı, internet vasitəsilə narkotik vasitələrin dövriyyəsi və s. əməllər daxil edilir. Müəllif tərəfindən digər kibercinayətlərin ayrıca bir subkateqoriya kimi göstərilməsi cəmiyyət inkişaf etdikcə kiberməkanda meydana çıxan yeni cinayət əməllərinin də təsnifata daxil edilməsinə imkan verir (Qeyd etmək lazımdır ki, kibercinayətlər haqqında cinayət hüquq elmində ətraflı məlumat verildiyi üçün bu məsələyə cinayətlərin adını qeyd etməklə toxunmağa üstünlük veririk).

Kibercinayətlərin törədilməsinin müxtəlif üsulları vardır. 2016-cı ilin məlumatına görə, informasiya təhlükəsizliyinin ən zəif nöqtəsi insan faktorudur və ona qarşı yönəlmiş hücumların geniş yayılan 4 növünə Azərbaycanda çox təsadüf edilir [4]:

1. Sosial mühəndislik (Social engineering, Human hacking). Sosial mühəndislik – insanlarla qarşılıqlı əlaqədə olaraq onlardan məlumat toplamaqdır. Bu növün əsas amillərindən biri saxta profillərdən (başqa adla və ya hər hansı bir saxta şirkət, kampaniya və s.), virtual dostluq və tanışlıqdan

---

[1] D.L.Şinderin verdiyi anlayışa görə, **hədə-qorxu ilə (təhdidlə) hücum (assault by threat)** – e-mail vasitəsilə həyata keçirilə bilər. Bu kibercinayət insanların özü və onların yaxınlarının həyatı ilə bağlı hədələməklə törədilir və həmçinin müəssisələrə və ya dövlət qurumlarına e-poçtla göndərilən bomba təhdidlərini də əhatə edə bilər.

[2] D.L.Şinderin verdiyi anlayışa görə, **kibertəcavüz (cyberstalking)** – cinayətin qurbanında mütəmadi şəkildə qorxu yaradan və real həyatda mövcud olan fiziki təcavüz və digər şiddətli davranışa səbəb ola biləcək ifadə və təhdidləri əks etdirən elektron təcavüz formasıdır.

[3] D.L.Şinderin verdiyi anlayışa görə, **özbaşına (qanunsuz) müdaxilə (cyber trespass)** – zamanı cinayətkar kompüter və şəbəkə resurslarını qanunsuz əldə edir, lakin burada informasiyanın zədələnməsi və korlanması məqsədi olmur. Məsələn, yetkinlik yaşına çatmayan hakerlərin "özünü yaşıdlarına sübut etmək" və ya müxtəlif "fərdi çağırışlar" məqsədilə törətdiyi əməllər.

[4] D.L.Şinderin verdiyi anlayışa görə, **dağıdıcı kibercinayətlər (destructive cybercrimes)** – şəbəkənin dağıdılması və məlumatların zədələnməsi və ya məhv edilməsi ilə müşayiət olunur. Bu növ əməllərə şəbəkəyə müdaxilə və məlumatların və proqramların silinməsi, veb-server və veb-səhifələrə müdaxilə, şəbəkə və kompüterlərə viruslar və digər ziyanverici proqramlarla ziyan vurulması, Dos hücumlar daxildir.

istifadə edib istifadəçini aldatmaqdan ibarətdir. Əsas məqsədi tanışlıq, virtual dostluq və ya hər hansı digər etibar qazanmış mənbədən sui-istifadə etməklə məlumatın toplanmasıdır. Ona görə də istifadəçilərin onlara gələn məktubların ünvanına xüsusi diqqət yetirməsi vacibdir. Hətta bir hərf dəyişməklə belə saxta sayt yaradıla bilər. (məsələn, www.facebook.com saytı əvəzinə www.facabook.com və s.)

2. "Brute-forcing". "Brute-force" – istifadəçinin hər hansı e-mail hesabına və ya digər hesabındakı şifrələr toplusuna edilən hücumdur. Bu zaman istifadəçiyə aid olan məlumatlardan (məsələn, ad, soyad, valideyn və ya övladın adı və doğum tarixləri, maşın nömrəsi, telefon nömrəsi və s.) istifadə edərək manual (əl ilə bir-bir) və ya avtomatik şəkildə müxtəlif vasitələrlə hesabdakı şifrlər yoxlanılır və şifrə (parol) tapılır. Bəs brute-force hücumunun məqsədi nədir? – Social engineering kimi bu hücumlar da istifadəçi haqqında məlumatların toplanması və sonradan həmin məlumatların qeyri-qanuni məqsədlərlə istifadəsi məqsədini daşıyır.

3. Ziyanverici proqramlar (malware) vasitəsilə yoluxdurma. Zərərverici yoluxdurma texnikası istifadəçiyə video, şəkil, musiqi, kino, hər hansı fayl, link göndərməklə kompüterə ziyanverici proqram (troyanlar, casus proqramları, soxulcanlar, viruslar və botnetlər) yüklənməsinə nail olmaqdır. Bu proqramların əsas məqsədi hədəfdən informasiyanın oğurlanmasıdır.

4. Fişinq (Phishing). Fişinq – ingilis dilindən tərcümədə "balıq ovu" deməkdir və qlobal şəbəkədə balıq ovunu xatırladan fırıldaqçılığın bir növüdür. Belə ki, fırıldaqçı (fişer) internetdə "tələ" quraraq, bu tələyə düşən internet istifadəçilərini aldatmaqla məşğul olur. Fişer müxtəlif üsullarla internet istifadəçilərindən bank hesablarını, kredit kartlarını və internetə çıxış üçün lazım olan informasiyaları öyrənir. Fişinq kiberdələduzluğun xüsusi növüdür, istifadəçiləri aldatma yolu ilə adətən maliyyə xarakterli fərdi məlumatların təqdim olunmasına məcbur etməyə yönəlir. Dələduz bank saytı kimi görünən (və ya maliyyə əməliyyatları aparılan istənilən digər sayt kimi, məsələn, eBay) saxta veb-sayt yaradır. Sonra cinayətkarlar istifadəçiləri bu sayta aldadıb aparmağa cəhd edirlər ki, bu saytda onlar login, parol və ya PIN-kod kimi konfidensial məlumatları daxil etsinlər.

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 [11, c. 171-176]:

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" adlandırılı

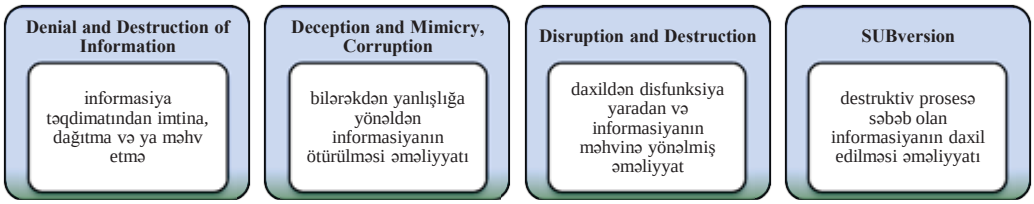
Dördüncü qrup kibercinayətlər baş vermə halı barəsində hüquq mühafizə orqanlarının məlumatının olduğu, lakin müxtəlif təsəvvürlərdən irəli gələrək qeydiyyatı aparılmayan cinayətlər (gizlədilən və ya ört-basdır edilən cinayətlər) hesab olunur.

1.3. İnformasiya müharibələri kibertəhlükələrin növü kimi

İnformasiya qarşıdurması – tərəflərin xüsusi metodlardan, informasiya ehtiyatlarına təsir üsulları və vasitələrindən istifadə etməklə qarşı tərəfin informasiya ehtiyatlarının məhvinə və ya nəzarətdə saxlanmasına yönəlmiş informasiya əməliyyatlarıdır. ***İnformasiya hücumu*** – icazə olmadan istənilən formada informasiyanın köçürülməsi, dəyişdirilməsi və məhvinə, həmçinin proqram təminatlarına, məxfi informasiyanın saxlandığı texniki qurğulara və insan psixologiyasına yönəlmiş əməliyyatlardır. ***İnformasiya müharibəsi*** isə özündə informasiya hücumu və informasiya qarşıdurması kimi əməliyyatları birləşdirən daha təhlükəli informasiya təsiri forması olub, qarşı tərəfin informasiyasına, informasiya proseslərinə və sistemlərinə zərər vurmaqla informasiya üstünlüyü əldə etmək, qarşı tərəfin iqtisadi, hərbi potensialını ələ keçirmək, ictimai şüura informasiya təsiri göstərməklə insanların davranışlarını dəyişmək uğrunda həyata keçirilən məqsədyönlü fəaliyyətdir. İnformasiya müharibəsində informasiya həm silah, həm də məqsəd, həm də müdafiə obyekti kimi çıxış edir. Mənbələrdə informasiya müharibəsi kombinə edilmiş kibercinayətlərə aid olunur [9, c. 57].

Ədəbiyyatda "şəbəkə müharibəsi" və "kibermüharibə" terminlərini irəli sürən mövqelər də vardır ki, bu qrup müəlliflər şəbəkə müharibəsini daha çox ictimai səviyyəli konseptual münaqişə kimi qiymətləndirərək, onun iqtisadi, siyasi və sosial sferaları əhatə etdiyini, kibermüharibənin isə əksinə hərbi məqsəd daşıdığını iddia edirlər [5, p. 27-30].

İnformasiya müharibəsinin fundamental paradiqmasının aşağıdakı informasiya əməliyyatlarından ibarət olması qeyd edilir:



İnformasiya müharibəsini daha çox texniki istiqamətdə izah edən yuxarıdakı bölgü informasiya-hüquqi aspektdən qarşıya çıxan sualları cavablandırmaq üçün yetərli deyil. Fikrimizcə, bu məsələ ilə bağlı ABŞ tədqiqatçısı Martin Libikinin təsnifatı daha dolğun səciyyə daşıyır. Belə ki, o, informasiya müharibəsinin 7 formasını fərqləndirir [6, p. 7-8]:

1. Komanda-nəzarət müharibəsi (Command and Control Warfare) – komandanlıq və icraçılar arasındakı əlaqə kanallarına istiqamətlənmiş informasiya müharibəsidir. Bu növ müharibədə əvvəlki dövrlərdə geniş yayılmış anti-rəhbər (anti-head) və müasir dövrdə inkişaf etmiş, İKT-dən istifadə etməklə icra olunan antineek əməliyyatlardan istifadə olunur.

2. Kəşfiyyat müharibəsi (Information Based Warfare) – mühüm informasiyanın toplanması və bu zaman hücum edən tərəfin öz informasiya resurslarını mühafizə etməsi prosesidir.

3.Elektron müharibə (Electronic Warfare) – elektron kommunikasiya vasitələrinə qarşı yönəlmiş müharibədir. Elektron kommunikasiya vasitələri dedikdə, radio əlaqə, radarlar, kompüter şəbəkəsi nəzərdə tutulur. Elektron dövlətin formalaşdırılmasından sonra geniş vüsət alan bu növ müharibələrin əsas obyektini kriptoqrafik istiqamətlər təşkil edir. Məhz belə növ müharibələrin artmasının nəticəsidir ki, respublikamızda da dövlət əhəmiyyətli informasiya resurslarının mühafizəsi üçün xüsusi qaydalar müəyyənləşdirilmişdir.

4. Psixoloji müharibə (Psychological Warfare) – insanların psixologiyasına təsir edən müharibə növüdür. M.Libiki psixoloji müharibənin 4 kateqoriyasını fərqləndirir: milli iradəyə qarşı yönəlmiş əməliyyatlar, rəhbərliyə (komandanlığa) qarşı yönəlmiş əməliyyatlar, hərbi qüvvələrdə əsgərlərə qarşı yönəlmiş və buna oxşar digər əməliyyatlar, mədəniyyətlərin müharibəsi [6, p. 35].

5. Haker müharibəsi (Hacker Warfare) – qarşı tərəfin mülki obyektlərinə yönəlmiş diversiya əməliyyatlarıdır. Hakerlərin silahı viruslardır.

6. İqtisadi informasiya müharibəsi (Economic Info-Warfare) – M.Libiki bu müharibəni iki formada təsvir edir: informasiya blokadası və informasiya imperializmi. Tədqiqatçı informasiya blokadasını iqtisadi blokadanın bir versiyası kimi qiymətləndirərək, informasiyanın kəsilməsini iqtisadi sahənin – ticarət əlaqələrinin də kəsilməsi ilə nəticələnəcəyini əsaslandırır. İnformasiya imperializmini isə müəllif ümumi iqtisadi imperializm siyasətinin bir hissəsi kimi şərh edir və ticarətin özünü də bir müharibə kimi qiymətləndirir. O iddia edir ki, ticarət sahəsində üstünlüyün əldə olunması nəticə etibarilə həmin dövlətlərdə bilik üstünlüyünə gətirib çıxarır və belə hakim mövqeni əldən vermə-

mək üçün bu dövlətlər daima "zəif" dövlətlərə "təzyiq göstərməyə" cəhd edirlər [6, p. 67-74].

7. Kibermüharibə (Cyberwar). Sonuncu təsnifat olan kibermüharibə müasir dövrümüzün ən aktual probleminə çevrilmişdir. Xüsusilə, informasiya terrorizmi təhlükəli xarakteri ilə fərqlənir. Məlum olduğu kimi, bütün dövlətlər elektron dövlət quruculuğuna keçdiyi üçün bütün informasiyalar informasiya sistemlərində yerləşdirilir. Artıq hər hansı bir dövlətin informasiya sahəsinə "hücum" etməklə, həmin dövləti yalnız siyasi, hərbi deyil, həmçinin iqtisadi, sosial və digər istiqamətlərdə də "iflic" etmək olar. Qeyd etmək lazımdır ki, tədricən dünya üzrə virtuallaşmanın sürətlənməsi insanları bir çox real varlıqlardan uzaqlaşdırır və bu da simulyasiya müharibələrinin formalaşmasını şərtləndirmişdir. Belə müharibələrdə real döyüş meydanındakı hərbi əməliyyatlar kompüter modeli ilə əvəz olunur. Hadisələrin gedişatına əsasən israrla deyə bilərik ki, yaxın gələcəkdə simulyasiya müharibəsi real müharibə ilə eyni məna kəsb edəcəkdir. Bütün bunlar həqiqətən də real müharibədən qat-qat təhlükəlidir. Hesab edirik ki, 2003-cü ildə yaradılan və virtual aləm kimi bir milyondan çox aktiv istifadəçisi olan "Second life" mövqeyimizi əsaslandırmaq üçün bariz nümunə kimi götürülə bilər. İnsanları tədricən real aləmdən uzaqlaşdıran bu şəbəkə "güclü" dövlətlər üçün "zəif" dövlətlərə asan və operativ psixoloji təsir vasitəsi rolunu oynaya bilər. Eyni zamanda, bu məsələ ilə bağlı müxtəlif virtual oyunların təsiri də az deyil. Məsələn, son dövrlərdə geniş yayılmış "Mavi balina" oyununun nə qədər intihar faktlarına səbəb olması göz qabağındadır. Bütün bunlar bir daha göstərir ki, "informasiya müharibəsi" nəzəri anlayış olmaqdan daha çox, təcrübi istiqamətdə təhlil olunmalı, onunla mübarizə tədbirləri yalnız beynəlxalq deyil, milli səviyyədə də aparılmalıdır. Hal-hazırda dövlətlər öz informasiya sistemlərinin məxfiliyini elektron vasitələrlə yetərincə qorumağa nail olurlar və bu da siyasi, hərbi və iqtisadi sahədə törədilən kiberhücumların sayını azaltmışdır. Lakin psixoloji hücumların necə təhlükəli olması və daha ağır nəticələrə gətirib çıxarması Dünya ictimaiyyətinin diqqətindən bir qədər kənarda qalmışdır. Hesab edirik ki, belə psixoloji hücumlar xalqların mənəviyyatının pozulması nəticəsində sonda bütün sahələrə (hərbi, siyasi, iqtisadi) öz mənfi təsirini göstərə bilər. Bu istiqamətdə respublikamızda aparılan işləri təqdirəlayiq hal kimi qiymətləndirmək lazımdır. Elektron Təhlükəsizlik Mərkəzinin gördüyü işlər vətəndaşlarda psixoloji təsir vasitələrindən qorunmaq üçün "immunitet" formalaşdırmış olur.

1.4. Nəticə

İKT-nin sürətlə inkişaf etdiyi bir dövrdə ənənəvi cinayətlərin də İKT-dən isitfadə edilməklə törədilməsinə daha çox üstünlük verilir. Bu günkü dövrdə şəxsin üzərinə silah çəkməklə pulunu almağa gərək yoxdur, texnologiyanın köməyilə daha asan yollarla (bank dələduzluğu və s.) varlanmaq olur. Hətta, məsafədən virtual aləmdə insanı öünü öldürməyə məcbur etmək belə mümkündür. Ona görə də kibertəhükələrlə bağlı hüquqi mənbələrdə "kibercinayət" anlayışına yenidən baxılmasını məqsədəmüvafiq hesab edirik. Bu zaman nəzəri ədəbiyyatda kibercinayətlərin müxtəlif təsnifatlarından istifadə etmək olar.

Beləliklə, kiberməkanda insan hüquqlarının təminatı və müdafiəsi üçün informasiya ekologiyasının aradan qaldırılması, informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması və inkişaf etdirilməsi, fərdi məlumatların mühafizəsi üzrə tədbirlərin gücləndirilməsi, kibermühitin insan psixologiyasına mənfi təsir üsullarının aradan qaldırılması və s. bu kimi tədbirlər planlaşdırılmalı və icra olunmalıdır.

ƏDƏBİYYAT

1. Əliyev Ə.İ., Rzayeva G.A., İbrahimova A.N., Məhərrəmov B.A., Məmmədrzalı Ş.S. İnformasiya hüququ. Dərslik. Bakı: Nurlar, 2019, 448 s.
2. Debra Littlejohn Shinder. Scene of the Cybercrime: Computer Forensics Handbook. Canada: Syngress Publishing, Inc., 2002, 749 p.
3. Fiordalisi E. The Tangled Web: Cross-Border Conflicts of Copyright Law in the Age of Internet Sharing. // Loyola University Chicago International Law Review, 2015, Vol. 12, İssue 2, pp. 197-213.
4. Elektron Təhlükəsizlik Mərkəzinin rəsmi saytı. https://cert.az/
5. John Arquilla and David Ronfeldt. Cyberwar is coming! // National Security Research Division. https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf
6. Martin C. Libicki. What Is Information Warfare? Washington, 1995, 104 p.
7. Official site of CERT Azerbaijan. https://www.cert.az/news/2016/informasiya-tehlukesizliyi-ve-ona-qarsi-yonelmis-hucumlar
8. Recommendations of the Electronic Security Center for the prevention and elimination of the consequences of information security incidents. // Electronic Security Center, 2014. https://www.cert.az/s/u/document/tovsiye.pdf,
9. Understanding Cybercrime: A Guide For Developing Countries. ICT Applications and Cybersecurity Division Policies and Strategies Department, ITU Telecommunication Development Sector Draft April 2009, 225 p.
10. К вопросу о латентности киберпреступлений. https://infourok.ru/statya-k-voprosu-latentnosti-kiberprestupleniy-1460496.html
11. Платошин Ю.А.Сущность латентной преступности. // Право и образование, 2011, №5, с. 171-176.
12. Рассолов И.М. Право и Интернет: Теоретические проблемы. М.: Норма, 2009, 383 с.

КИБЕРУГРОЗЫ И ИХ КЛАССИФИКАЦИЯ

А.Н.ИБРАГИМОВА

РЕЗЮМЕ

В современном обществе Интернет стал неотъемлемой частью человеческой жизни. Однако не все пользователи интернета являются законопослушными людьми. Использование ИКТ в различных незаконных целях и его результаты - одна из самых актуальных проблем нашего времени, которая поднимает проблему «киберпреступности». В статье даны пояснения терминов «киберпреступность», «кибервойна» и «киберпреступления», сравнительно проанализированы их легальная и нелегальная классификация, а также выдвинуты предложения и рекомендации по предупреждению киберпреступности.

Ключевые слова: информационная безопасность, киберпреступления, киберпреступность, классификация киберпреступлений, кибервойна, данные, доступность, конфиденциальность, полнота.

CYBER THREATS AND THEIR CLASSIFICATION

A.N.IBRAHIMOVA

SUMMARY

In modern society, the Internet has become an integral part of human life. However, not all internet users are law-abiding people. The use of ICTs for various unlawful purposes and its results is one of the most pressing problems of our time, which raises the issue of "cybercrime". In the article were given an explanation of the terms "cybercrime", "cyber war" and "cyber offences", were comparatively analyzed their legal and illegal classification, and were put forward suggestions and recommendations for the prevention of cybercrime.

Keywords: information security, cyber offences, cybercrime, classification of cyber-crimes, cyber war, data, accessibility, confidentiality, completeness.