UOT 004.351

Ələkbərova İ.Y.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
airada.09@gmail.com

KİBERMÜNAQİŞƏLƏRİN YARATDIĞI PROBLEMLƏR VƏ ONLARIN HƏLLİ YOLLARI

Məqalədə kiberməkanda baş verən münaqişələr və informasiya qarşıdurmaları ilə bağlı problemlər analiz edilir. Kiberhücumların məqsəd və hədəfləri göstərilir, kiberməkanda informasiya qarşıdurmasının üsul və vasitələri təsnifatlandırılır. Kibermünaqişələrdə informasiya təhlükəsizliyi vasitələrindən effektiv istifadə üçün əsas şərtlər göstərilir.

Açar sözlər: *kibermünaqişə, kiberməkan, informasiya təhlükəsizliyi, şəbəkə müharibəsi, kiberhücum, kompüter cinayətkarlığı*

Giriş

Son illər informasiya-kommunikasiya texnologiyaları (İKT) elə bir sürətlə inkişaf edir ki, onun sonrakı fəsadlarının əvvəlcədən dəqiq müəyyən edilməsi çox zaman mümkün olmur və sonradan yaranan neqativ vəziyyətin aradan qaldırılmasına yetərincə vəsait, zaman və bilik sərf etmək lazım gəlir. Əsasən də, İnternet qlobal şəbəkəsində tətbiq edilən yeni texnologiyalar, layihələr və müxtəlif proqramlar ilk baxışdan faydalı və zərərsiz görünsə də, təcrübə göstərir ki, bir çox hallarda onların yaratdığı problemlərin qarşısını tam almaq mümkün olmur. Məsələn, sosial şəbəkələr, açıq ensiklopediyalar, bloqlar və s. layihələr bu gün İnternet istifadəçilərinin əsas fəaliyyət meydanına çevrilmişlər. Lakin bu layihələrin özündə də informasiya təcavüzü, informasiya ilə manipulyasiya, dezinformasiyanın yayılması halları geniş vüsət almışdır.

İnternet genişlənir, yəni, şəbəkəyə daha çox serverlər qoşulur, informasiya çoxalır, istifadəçilərin sayı artır. Kompüter şəbəkələrinin genişlənməsi kibermünaqişələrdə şəbəkə texnologiyalarının imkanlarından daha geniş istifadə etməyə, şəbəkə istifadəçilərinin fəaliyyətlərində koordinasiyanın, əhatəliliyin və mürəkkəbliyin artmasına şərait yaradır. Bu isə kibermünaqişələrin çoxalmasına, onların daha təcrübəli və müasir İKT vasitələri ilə təmin olunmuş istifadəçilər tərəfindən aparılmasına səbəb olur [1].

Kiberməkanda fəaliyyət göstərən gizli sosial şəbəkələrin həyata keçirdikləri mütəşəkkil cinayətkarlıq dövlət və cəmiyyətə qarşı, ilk növbədə isə, ölkə iqtisadiyyatına dağıdıcı təsir gücünə malikdir. Bu gün kiberməkanda "qaranlıq veblər" (*dark webs*), "gizli iqtisadiyyat" (*underground economy*), gizli şəbəkə (*covert network*) kimi yeni problemlər yaranmışdır. Gizli şəbəkələr heç bir dövlət tərəfindən nəzarət olunmayan şəbəkələrdir və insan alveri, kibercinayətkarlığın və terrorizmin yayılmasında əsas əlaqələndirici vasitədir. Eyni zamanda, kibermünaqişələrdə bu şəbəkələrdən geniş istifadə olunmaqdadır.

Müasir İKT-nin müxtəlif sahələrə tətbiqi kiberməkanda yeni fəaliyyət növlərinin – şəbəkə müharibələrinin, kiberhücumların, kibercinayətkarlığın, kibermünaqişələrin, kiberterrorizmin və buna bənzər bir sıra xoşagəlməz hadisələrin yaranmasına və genişlənməsinə səbəb olmuşdur. Yuxarıda sadalanan informasiya əməliyyatları yüksək dərəcədə təsiretmə və çox az ehtimalla aşkar olunma qabiliyyətinə malik olduqlarından, bu gün kiberməkanda milli informasiya təhlükəsizliyinin təmini məsələsi hər bir dövlətin üzərinə düşən ən aktual problemlərdəndir. Bu gün kibermünaqişələrdə yalnız dövlət orqanları deyil, müxtəlif koalisiyalar, siyasi partiyalar və qruplar (terrorçu qruplar da daxil olmaqla), böyük şirkətlər iştirak edirlər. Tədqiqatlar göstərir ki, İnternet də daxil olmaqla, kiberməkanda informasiya hücumlarının hədəfləri dövlətin kritik infrastrukturu (enerji sistemi, nəqliyyat, dövlət idarələri, bank və maliyyə), vətəndaşlar və müxtəlif informasiya resurslarıdır [2, 3].

Kibermünaqişə ilə əlaqədar əsas anlayışlar və terminlər

"Kiber" sözü "kibernetika" sözündən yaranmışdır. "Kibernetika" termini qədim yunan dilində "kibernetes" sözündən alınmış, mənası "idarə edən" deməkdir. İnternet texnologiyalarının inkişafı ilə "kiber" əsaslı yeni sözlər yaranmağa başladı, bu sözlərdə "kiber" sözü "İnternet və virtual reallığa aid olan" mənasında işlənir [4].

"Kiberməkan" sözü ilk dəfə kanadalı yazıçı-fantast Uilliam Gibson tərəfindən 1982-ci ildə işlədilmişdir. Müəllif sonrakı əsərlərində kiberməkanı "unversal qarabasma" kimi təsvir edir [5].

Bizi əhatə edən kiber ekosistemi qlobal və dinamik olub, yüz minlərlə şəbəkəni və milyonlarla qurğuları əhatə edir. Kiberməkan anlayışına müxtəlif ölkələrin rəsmi dairələrində müxtəlif izahlar verirlər. Məsələn, ABŞ-da kibertəhlükəsizlik üzrə milli strategiya ilə bağlı sənədlərdə göstərilir ki, kiberməkan yüz minlərlə bir-biri ilə əlaqəli kompüter, server, kabel, kommutator və yönəldicilərdən ibarət olub, dövlətin kritik infrastrukturunun normal işini təmin edir. Bu isə o deməkdir ki, kiberməkan ölkədə iqtisadiyyatın inkişafında və milli təhlükəsizlikdə mühüm rol oynayır.

Sənədlərdə o da göstərilir ki, kiberməkan real coğrafiya ilə əlaqəlidir və geosiyasətin əsas elementidir. Belə ki, kommunikasiyalar, serverlər və texniki əlaqələr coğrafi lokalizasiyaya malikdir. Digər tərəfdən, kiberməkan domen zonalarına, istifadə olunan dilə və dövlət nəzarətinə görə milli identifikasiyaya malikdir. Kiberməkan fiziki coğrafiyanı xüsusi şəkildə xarakterizə edir: müxtəlif xidmətlər, naviqasiya cihazları, texniki qadjetlər və mobil cihazlar, sensorlar informasiya axınından, qurğulardan və insanlardan ibarət interaktiv xəritə yaradırlar [6].

Kiberməkan kiberəməliyyatların reallaşdırıldığı məkandır. Kiberməkanda informasiya əməliyyatları hücum, müdafiə və kəşfiyyat xarakterli olur [1, 4].

Amerikanın "*The Economist*" jurnalı kiberməkanı yer, dəniz, hava və kosmosdan sonra 5-ci müharibə məkanı elan etmişdir. Kiberməkan təbii məkanlardan onunla fərqlənir ki, bu məkan zamanla dəyişdirilən İKT vasitələri ilə yaradılmışdır. ABŞ və Avropanın bir sıra inkişaf etmiş ölkələrində kibermüharibələrdə iştirak etmək üçün xüsusi kiberəsgərlər hazırlanır [7].

"Kibermüharibə" termini ilk dəfə 1993-cü ildə Con Arkuilla və Devid Ronfeldt tərəfindən "Kibermüharibə gəlir!" (*Cyber War Is Coming!*) məqaləsində istifadə edilmişdir [8]. Məqalədə müəlliflər "kibermüharibə" və "şəbəkə müharibəsi" konsepsiyalarını irəli sürməklə müasir dövrdə şəbəkə müharibəsinin təsəvvür ediləndən daha ciddi problemlər yaratmaq imkanına malik olduğunu sübut etməyə çalışmışlar. Tədqiqatlar göstərir ki, "kiberterrorizm", "kibermünaqişə", "şəbəkə müharibəsi" və "kiberhücum" terminləri sinonim deyillər. Lakin nəzərə alsaq ki, onların hər biri İnternetlə və kompüter şəbəkəsi ilə sıx bağlıdır, demək, bu terminlər arasında ümumi cəhətlər çoxdur.

Kiberterrorizm kompüter şəbəkələrindən istifadə etməklə dövlətin kritik infrastrukturunun sıradan çıxarılmasına və ya vətəndaşlara psixoloji təsir məqsədi daşıyır. İqtisadi və dövlət sistemlərinin şəbəkədən asılılığı cəmiyyətdə kiberterrorizm təhlükəsinin artmasına səbəb olmuşdur [2, 6, 9].

Kibermünaqişənin yaranma səbəbləri və mərhələləri

Kiberməkanda baş verən münaqişələr informasiya müharibəsinin tərkib hissəsidir. Bu gün kibermünaqişə müxtəlif formalarda – sosial şəbəklərdə baş verən qarşıdurmalardan başlamış dövlətin milli dəyərlərini əks etdirən domen adların ələ keçirilməsinə, haker hücumlarına kimi bütün istiqamətlərdə həyata keçirilir. Münaqişə tərəflər arasında obyektiv və subyektiv ziddiyyətlərin təzahürüdür. Kibermünaqişə isə kiberməkanda yaranan kəskin qarşıdurmadır [9]. Kibermünaqişələr gizli, təhlükəli, passiv, məkrli ola bilərlər və enerji, maliyyə sistemlərinin dağıdılmasından başlayaraq, şəbəkə mühafizəsinin neytrallaşdırılmasına kimi bütün əməliyyatları əhatə edirlər.

Kibermünaqişələrin analizini aparmaq üçün, ilk növbədə, bu münaqişələrin yaranması və genişlənməsinin səbəbləri araşdırılmalıdır. Bu səbəblər aşağadakılardır:

1. Qlobal şəbəkədə nəzarət mexanizminin olmaması;

2. Şəbəkə istifadəçilərinin sayının durmadan artması;
3. İstifadəçilərin anonimliyi, proksi-serverdən istifadə;
4. Şəbəkədə boşluqların olması;
5. Avtomatlaşma, şəbəkədə zaman və məkandan asılılığın aradan qaldırılması;
6. Kibermühitdə hüquqi əməkdaşlıqla bağlı problemlər.

İnternet genişləndikcə kibermünaqişələr dayanıqlı templə miqyasına, mürəkkəbliyinə və s. xüsusiyyətlərə görə güclənməkdə davam edir. Kibermünaqişələr qlobal xarakter almaqla ayrı-ayrı təşkilatları, cəmiyyəti, ümumilikdə millətləri və dövlətləri əhatə edir [10].

Kibermünaqişə mürəkkəb dinamik proses olub aşağıdakı mərhələləri özündə birləşdirir:

– obyektiv vəziyyət – kibermünaqişənin yaranmasının obyektiv səbəbləri;
– münaqişə təsiri – kibermünaqişənin davam etməsi və ya genişlənməsi;
– kibermünaqişənin həlli (tam və ya qismən).

Kibermünaqişə iki istiqamətdə reallaşdırılır: kibermüdfiə və kiberhücum. Müdafiə və hücum əməliyyatlarının əsasında qərarların qəbulu sistemləri və onların təhlükəsizlik məsələləri dayanır [11].

Kibermüdafiə kiberməkanda informasiyanın aşkarlanması, analizi, dəyişdirilməsi və icazəsiz müdaxilələrin xəbərdar edilməsinə yönələn kiberəməliyyatdır. Kibermüdafiə özü də iki cür olur: passiv və aktiv kibermüdafiə. Aktiv kibermüdafiə dedikdə, şəbəkəyə edilən hücumların aktiv təyini, analizi, şəbəkə təhlükəsizliyinin pozulması nəticəsində yaranan fəsadların tez bir zamanda aradan qaldırılması və real zaman çərçivəsində əks-tədbirlərin görülməsi nəzərdə tutulur. Passiv kibermüdafiə dedikdə isə, informasiya təhlükəsizliyi məsələlərini həll etməklə, şəbəkə kəşfiyyatı vasitələrindən istifadə edərək qarşı tərəfə aid sistemdəki məxfi informasiyanın oğurlanması və nəzarətdə saxlanması nəzərdə tutulur. Cəmiyyətdə siyasi və iqtisadi gərginlik artdıqca kiberməkanda reallaşdırılan passiv kibermüdafiə bir çox hallarda aktiv kibermüdafiə ilə əvəz olunur, kibermünaqişələr çoxalır [9, 11].

Qloballaşma kibermüdafiə əməliyyatlarında bir sıra çətinliklərə səbəb olur. Bir tərəfdən, informasiya sistemləri və şəbəkələri arasındakı qarşılıqlı əlaqə informasiya təhlükəsizliyi ilə bağlı bir çox məsələlərin həllində çətinliklər yaradır, belə ki, şəbəkədə hansısa bəndin zəif olmayacağına tam əmin olmaq mümkün deyil. Digər tərəfdən, kibermünaqişədə istifadə olunan müasir texnologiyalar məsələnin həllini çətinləşdirir [10, 11]

Kiberhücumda müxtəlif İKT vasitələrindən istifadə edilir ki, nəticədə qarşıya qoyulan məqsədə çatmaq üçün şəbəkə ilə ötürülən informasiyanın məqsədyönlü olaraq dəyişdirilməsi, köçürülməsi, hüquqi istifadəçilərin müraciətlərinə məhdudiyyət qoyulması, dezinformasiyanın ötürülməsi, informasiya daşıyıcılarının funksionallığının pozulması və s. əməliyyatlar həyata keçirilir.

Kiberhücumlarda informasiya mübadiləsinə zərər yetirən, qarşı tərəfin informasiya şəbəkəsindən lazım olan informasiyanı çıxara bilən vasitələr də mövcuddur. Kiberhücum vasitələrinə, əsasən, dövlət və korporativ informasiya sistemlərinə daxil edilərək bu sistemləri uzaq məsafədən idarə edən xüsusu proqramlar daxildir. Kiberhücumlar zamanı reallaşdırılan əsas əməliyyatlar şəbəkənin struktur elementlərinin funksionallığında effektivliyin azaldılması və ya şəbəkənin bütünlükdə sıradan çıxarılmasıdır. Şəbəkənin ayrı-ayrı elementlərinin fəaliyyətinin effektivliyini aşağı salan üsullardan ən çox istifadə edilənlər şəbəkəyə robot proqramlarının müdaxiləsi, xidmətdən imtina ilə bağlı DoS hücumlar (*Denial of Service Attack*) və müxtəlif zərərli proqramların tətbiqidir. Kiberhücum əməliyyatını ilk dəfə xüsusi informasiya təminatından istifadə edən hakerlər həyata keçirmişlər [12].

Kiberhücumlar hərbi, iqtisadi, bank, sosial və digər sahələri əhatə edir və aşağıdakı məqsədləri daşıyır:

– idarə strukturlarının, nəqliyyat axınının və kommunikasiya vasitələrinin fəaliyyətinin pozulması;
– çoxhissəli texnoloji əlaqələri və qarşılıqlı hesab əməliyyatlarını pozmaqla, valyuta-

maliyyə fırıldaqları həyata keçirməklə ayrı-ayrı müəssisələrin, bankların, müxtəlif istehsal sahələrinin fəaliyyətlərinin məhdudlaşdırılması və ya tamam təcrid edilməsi;
- təhlükəli maddələr və enerjinin yüksək konsentrasiyaları ilə əlaqəli olan texnoloji proseslərin və obyektlərin düzgün idarəsinin pozulması nəticəsində qarşı tərəfin ərazisində iri texnogen qəzaların təşkili;
- insanların şüuruna müəyyən təsəvvürlərin, davranışların və əxlaqi stereotiplərin kütləvi şəkildə yönəldilməsi və yayılması;
- əhali arasında hərcmərcliyin və narazılığın, eləcə də, ayrı-ayrı sosial qruplar arasında destruktiv fəaliyyətlərin təşkil edilməsi.

Kiberhücumlar aşağıda göstərilən xüsusi strukturlar tərəfindən həyata keçirilir [11, 12]:
- dövlət təşkilatları tərəfindən idarəetmə funksiyalarını yerinə yetirən kompüter və rabitə sistemləri;
- ordunun və hərbi texnikanın idarə edilməsi məsələləri ilə, eləcə də, hərbi qüvvələrin maraqlarına uyğun olaraq informasiyanın yığılması və emalı ilə məşğul olan hərbi informasiya infrastrukturları;
- bankların, nəqliyyat və istehsal müəssisələrinin informasiya və idarəetmə strukturları.

Kiberhücumlar, aşağıda göstərildiyi kimi, daxili və xarici mənbələrdən ola bilərlər:
- Daxili mənbələr:
  - Sistemin nasazlığı nəticəsində baş verən pozuntular;
  - Müəssisənin əməkdaşı tərəfindən təsadüfi xarakterli, yəni bilməyərəkdən edilən xətalar;
  - Müəssisənin əməkdaşı tərəfindən bilərəkdən edilən müdaxilələr.
- Xarici mənbələr:
  - Hakerlər tərəfindən kiberhücumlar;
  - Virusların ötürülməsi;
  - Xüsusi hazırlanmış kriminal qruplar;
  - Müəyyən ideologiyaya malik aktivistlər;
  - Terrorçular;
  - Xarici dövlət orqanları.

Kibermünaqişədə effektivliyin əldə edilməsi şərtləri

Kibermünaqişədə effektivliyin əldə edilməsi yalnız bir sıra şərtlərin ödənməsi nəticəsində həyata keçirilə bilər. Bu şərtlərə, əsasən, şəbəkəyə icazəsiz müdaxilələrin təyini və qarşı tərəfin informasiya hücumlarının qarşısının alınması daxildir [13].

Kibermünaqişədə nəzərə alınmalı olan əsas şərtlər aşağıdakılardır:
- münaqişə predmeti;
- münaqişə tərəfləri;
- kibermünaqişənin davamlı olması üçün şərtlər;
- kibermünaqişənin miqyası: təşkilatlararası, dövlətlərarası və s.;
- tərəflərin strateji və taktiki davranışı;
- kibermünaqişənin fəsadları.

Kibermünaqişə nəticəsində baş verən neqativ hallar kimi aşağıdakıları göstərmək olar:
- informasiya axınının dəyişdirilməsi və ya qarşısının alınması yolu ilə istehsalat prosesinin iflic olunması;
- qurğuların zədələnməsi, işinin dayandırılması yolu ilə istehsalat prosesinin iflic edilməsi, insanların həyatına təhlükə yaradılması və ya ətraf mühitə neqativ təsir;
- operatorlara yalan məlumat göndərməklə onların fəaliyyətlərində səhv addımlar atmağa sövq edilməsi və bununla da, təşkilatın normal fəaliyyətinin pozulması və iqtisadi zərərin baş verməsi;
- sistemi sıradan çıxarmaq üçün proqram təminatının pozulması;

– ziyanverici proqramlar vasitəsi ilə sistemə xaricdən müdaxilə nəticəsində onun normal fəaliyyətinin pozulması və informasiyanın oğurlanması;
– təhlükəsizlik sistemlərini sıradan çıxarmaqla insanların həyatının təhlükəyə məruz qalması.

Kibermünaqişənin qarşısını almaq üçün aşağıdakı şərtlər ödənməlidir:
– münaqişənin mənbəyi təyin edilməlidir;
– münaqişədə istifadə olunan proqram və aparat təminatı (münaqişə vasitələri) analiz olunmalıdır;
– münaqişənin növü müəyyən edilməlidir;
– münaqişənin səbəbləri öyrənilməlidir;
– münaqişənin xüsusiyyətləri təyin edilməlidir.

Kibermünaqişələrdə qarşı tərəf üzərində üstünlüyün əldə olunması ilə əlaqədar məsələləri həll etmək üçün şəbəkədə münaqişələrin hər üç aspekti nəzərə alınmalıdır. Bu aspektlər aşağıdakılardır:

1. Kompüter şəbəkəsinə icazəsiz müdaxilənin vaxtında aşkar edilməsi və müvafiq tədbirlərin görülməsi;
2. Şəbəkənin yüklənməsinin qarşısının alınması.
3. Əkshücumun təşkil edilməsi: qarşı tərəfə aid olan şəbəkənin nəzarətdə saxlanması, yəni şəbəkədəki informasiya resurslarına təsir, dezinformasiyanın ötürülməsi, şəbəkənin normal fəaliyyətinin pozulması.

Kompüter şəbəkələrində baş verən münaqişələrin yuxarıda göstərilən aspektləri kibermünaqişənin əsas məqsədini təyin edir və sübut edir ki, informasiya təhlükəsizliyi üzrə ənənəvi funksiyalar şəbəkədə informasiya mühafizəsi sisteminin yaradılması üçün kifayət deyildir. Kibermünaqişələrdə, eyni zamanda, informasiya təhlükəsizliyi, icazəsiz müdaxilə və informasiya əks hücumu üzrə bütün məsələləri həll edə biləcək xüsusi sistem işlənməlidir.

Nəzərə almaq lazımdır ki, kibermünaqişələrdə kiberkinetik əməliyyatlardan geniş istifadə olunur. Kiberkinetik əməliyyatlar dedikdə, şəbəkənin kənardan və daxildən icazəsiz müdaxiləyə davamlı olmasının təmin edilməsi nəzərdə tutulur. Bu da şəbəkənin informasiya təhlükəsizliyində bir nömrəli məsələdir. Məsələnin həllində sistemin dəyişən situasiyaya adaptasiya olması, potensial kiberdüşmənin qısa zaman intervalında proqnozlaşdırılması və özünütəşkil xüsusiyyətinə malik olması müasir dövrün tələbidir.

Nəticə

Kibermünaqişə və kibercinayətkarlıqla bağlı problemlər ümumi informasiya müharibəsi problemləri ilə müqayisədə daha yenidir və İnternetin genişlənməsinə paralel olaraq son onillikləri əhatə edir. Odur ki, hazırkı vəziyyət və gələcək perspektivlərlə bağlı konkret fikir söyləmək çətindir. Lakin bir şey aydındır ki, problem zaman keçdikcə insan fəaliyyətinin yeni-yeni sahələrini əhatə edir və yüksək templə inkişaf edərək ona qarşı milli və beynəlxalq səviyyədə adekvat və müasir tədbirlərin görülməsini tələb edir. Kibermünaqişənin vətəndaşların davranışlarının idarə olunması və informasiya resurslarının sıradan çıxması və ya funksional nasazlıqların yaradılması kimi nəticələri qarşı tərəfdə hissediləcək iqtisadi böhranın yaranmasına və əhali arasında narazılıqların artmasına yönəlmişdir. Bu isə dövlətin iqtisadi və elmi-texniki siyasətinin bir istiqaməti kimi qlobal açıq şəbəkəyə qoşulmazdan öncə milli informasiya təhlükəsizliyi məsələsinin həllini tələb edir.

Dövlətin və vətəndaşların informasiya və intellektual mülkiyyəti ilə bağlı qanuni mənafelərinə istiqamətlənmiş açıq siyasət ölkə daxilində şəbəkə vasitələrinin mühafizəsi fəaliyyətini dəstəkləməli və bu şəbəkəyə informasiya silahının gizli elementlərinin daxil olmasının qarşısı bütün mümkün üsullarla alınmalıdır. Şəbəkənin informasiya təhlükəsizliyinin təmin edilməsi sistemli və kompleks yanaşma tələb edir. Bu sahədə əlaqədar qurumlar tərəfindən konseptual, təşkilati, elmi-metodoloji, qanunvericilik, maddi-texniki əsasların yaradılması üzrə işlərin aparılması müasir dövrün ən vacib tələbidir.

Ədəbiyyat

1. Алекперова И.Я. Comparative analysis of information attacks in Internet // Информационные технологии и компьютерная инженерия, №3 (19), 2010, стр. 81–87.
2. Имамвердиев Я.Н. Модель ситуационного управления информационной безопасностью электронного правительства // Информационные технологии. 2014. № 8. С. 24–33.
3. Алгулиев Р.М., Володин А.В., Устинов Г.Н. Некоторые подходы к технологии обеспечения информационной безопасности при работе в сети Интернет // Тез. докл. юбилейной научно-технической конференции профессорско-преподавательского, научно и инженерно-технического состава МТУСИ. М., 2001, с. 265–266.
4. İmamverdiyev Y.N. Yeni nəsil milli kibertəhlükəsizlik strategiyalari // İnformasiya cəmiyyəti problemləri, 2013, №2 (8), 42–51.
5. GibsonW. Neuromancer, Ace Books, 1984, 271 p.
6. Klimburg A., Mirtl Ph. Cyberspace and Governance. The Austrian Institute for International Affairs, 2012, 65 p.
7. http://www.economist.com/node/16478792
8. Arguilla J., Ronfeldt D. Cyberwar is coming! // Comparative Strategy, vol. 12, no 2, 1993, pp. 141-165.
9. Lewis J.A. Assessing the risks of cyber terrorism, cyber war and other cyber threats // Center for Strategic and International Studies, 2002, pp. 3–12.
10. Сойер П. Третья мировая может начаться в Интернете // Computerworld Россия, М., № 32, 2009, с. 29.
11. Ələkbərova İ.Y. İnformasiya müharibəsi texnologiyaları, "İnformasiya texnologiyaları" nəşriyyatı, Bakı, 2012, 108 səh.
12. Schmitt M. N. Classification of cyber conflict // Conflict and Security, 2012, vol. 17, no. 2, pp. 241–250.
13. Applegate S.D., Stavrou A. Towards a cyber conflict taxonomy / Proceedings of the 5th International Conference On Cyber Conflict, 4-7 June, 2013, Tallinn, pp. 431–448.

УДК 004.351

Алекперова Ирада Я.
Институт Информационных Технологий НАНА, г. Баку, Азербайджан
airada.09@gmail.com

Проблемы, созданные киберконфликтами, и способы их решения

В статье проанализированы проблемы, связанные с информационными противостояниями и конфликтами, происходящими в киберпространстве. Рассмотрены цели и задачи кибератак, осуществлена классификация способов и средств информационного противоборства в киберпространстве. Предложены способы для эффективного выбора средств информационной безопасности во время киберконфликтов.

Ключевые слова: *киберконфликт, киберпространство, информационная безопасность, сетевая война, кибератака.*

Irada Y. Alakbarova
ANAS Institute of Information Technology, Baku, Azerbaijan
airada.09@gmail.com

Problems created by cyberconflicts and the methods of their solution

In the article, the problems related to information confrontations and conflicts in cyber environment were analyzed. Purposes and goals of cyber-attacks were observed. Also the classification of the tools of information confrontations in cyber environment was researched. The methods of the effective choice of information security tools during cyber conflicts were proposed.

Key words: *cyber-conflict, cyber-environment, information security, net-war, cyber-attack.*