AZƏRBAYCAN RESPUBLİKASININ PREZİDENTİ YANINDA
ELMİN İNKİŞAFI FONDU

Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişafı Fondunun və Azərbaycan Respublikasının Rabitə və İnformasiya Texnologiyaları Nazirliyinin İKT-nin inkişafına yönəlmiş əhəmiyyətli layihələrin dəstəklənməsi məqsədi ilə qrantların verilməsi üzrə 2013-cü il üçün 2-ci məqsədli birgə İKT müsabiqəsinin (EİF-RİTN-MQM-2/İKT-2-2013-7(13)) qalibi olmuş və yerinə yetirilmiş layihə üzrə

YEKUN ELMİ-TEXNİKİ HESABAT

Layihənin adı: **İnternet mühitində Azərbaycan Respublikasına qarşı reallaşdırılan informasiya müharibəsi texnologiyalarının analizi və problemin həlli üçün təkliflərin işlənilməsi**
Layihə rəhbərinin soyadı, adı və atasının adı: **Ələkbərova İradə Yavər qızı**
Qrantın məbləği: **12 000 manat**
Layihənin nömrəsi: **EİF-RİTN-MQM-2/İKT-2-2013-7(13)-29/22/1-M-13**
Müqavilənin imzalanma tarixi: **21 aprel 2014-cü il**
Qrant layihəsinin yerinə yetirilmə müddəti: **12 ay**
Layihənin icra müddəti (başlama və bitmə tarixi): **01 may 2014-cü il – 01 may 2015-ci il**

Diqqət! Bütün məlumatlar 12 ölçülü Arial şrifti ilə, 1 intervalla doldurulmalıdır
Diqqət! Uyğun məlumat olmadığı təqdirdə müvafiq bölmə boş buraxılır

Hesabatda aşağıdakı məsələlər işıqlandırılmalıdır:

1	Layihənin həyata keçirilməsi üzrə yerinə yetirilmiş işlər, istifadə olunmuş üsul və yanaşmalar
	İnternet mühitində Azərbaycan Respublikasına qarşı reallaşdırılan informasiya müharibəsi texnologiyalarının analizində beynəlxalq təcrübə öyrənilmişdir. Kiberməkan anlayışına müxtəlif ölkələrin rəsmi dairələrində müxtəlif isahlar 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 malikdirlər. Digər tərəfdən kiberməkan domen zonalara, 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. Kiberməkan kiberəməliyyatların reallaşdırıldığı məkandır. Kiberməkanda informasiya əməliyyatları hücum, müdafiə və kəşfiyyat xarakterli olurlar.

Müasir informasiya müharibəsi texnologiyalarının yaranması, inkişafı və geniş tətbiqinin müxtəlif izahları var:

Hesablama texnikası və kommunikasiya vasitələrinin sürətli inkişafı, şəbəkə texnologiyasının təkmilləşdirilməsi cəmiyyətdə əsas resurs kimi informasiyanın rolunun artmasına səbəb olur.

Effektivliyinə görə informasiya maddi resurslardan daha yuxarıda dayanır. Elmi-texniki nailiyyətlər hərbi sahədə istifadə edilən ənənəvi silahlarla yanaşı bir sıra İKT vasitələrinin kütləvi istehsalına və informasiya təhlükəsizliyinin təmini üçün geniş istifadəsinə şərait yaranır.

İnsanların beynlərinin və davranışlarının öyrənilməsində əldə edilən nailiyyətlər insanlara müxtəlif istiqamətlərdə psixo-fizioloji təsirlərin yollarını və vasitələrini daha yaxşı başa düşməyə imkan verir.

"İnformasiya müharibəsi" terminini ilk dəfə, 1976-cı ildə amerikalı mütəxəssis Tomas Rona "Boeing" şirkəti üçün hazırladığı "Silah sistemləri və informasiya müharibəsi" (Weapon Systems and Information War) adlı hesabatında istifadə etmişdir. Rona hesabatında sübut etmişdir ki, IKT-nin inkişafı informasiya infrastrukturunun dövlətlin iqtisadiyyatının əsas komponentinə çevrilməsinə səbəb olmuşdur.

İnformasiya müharibəsinin ilk tədqiqatçılarından biri, ABŞ-ın Milli Müdafiə Universitetinin əməkdaşı Martin Libiki 1995-ci ildə yazdığı "İnformasiya müharibəsi nədir?" (What Is Information Warfare?) məqaləsində informasiya müharibəsi texnologiyalarının təsnifatını vermiş və göstərmişdir ki, son dövrlərdə İKT-nin inkişafı nəticəsində artıq informasiya müharibəsində yalnız psixoloji deyil, həm də iqtisadi və hərbi aspektlərə üstünlük verilir. İnformasiya müharibəsinin mərhələləri aşağıdakılardır:

Məqsədin müəyyən edilməsi. İnformasiya müharibəsi nə üçün lazımdır və nəticədə nə əldə ediləcəyi gözlənilir.

Strategiyanın müəyyən edilməsi. Burada İKT-nin dörd baza komponenti nəzərə alınmalıdır: informasiyanın hazırlanması, informasiyanın yönələcəyi kommunikasiya kanalının təyin edilməsi, informasiyanın təsiri altına düşəcək auditoriyanın müəyyənləşdirilməsi, informasiya müharibəsi metodunun seçilməsi.

Taktiki fəaliyyət planının hazırlanması.

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

"Kibermüharibə" termini ilk dəfə 1993-cü ildə Con Arkuilla və Devid Ronfeldt tərəfindən "Kibermüharibə gəlir!" (Cyber War Is Coming!) məqaləsində istifadə edilmişdir. 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 (enerji sistemi, nəqliyyat, dövlət idarələri) sıradan çıxarılmasına və ya vətəndaşların qorxudularaq psixoloji təsirə məruz qoymaq məqsədi daşıyır. İqtisadi və

dövlət sistemlərinin şəbəkədən asılılığı cəmiyyətdə kiberterrorizm təhlükəsinin artmasına səbəb olmuşdur.

Beləliklə, beynəlxalq təcrübə sahəsində aparılan təhlillər ona əsas verir ki, informasiya müharibəsi vətəndaşların davranışlarının idarə olunması və informasiya resurslarının sıradan çıxması və ya funksional nasazlıqların yaradılması kimi nəticələrə yönəlmişdir. Qarşı tərəfdə hissediləcək iqtisadi böhranın yaranması və əhali arasında narazılıqların artması ilə bağlı problemlərin həllində yeni yanaşma və üsullara ehtiyac vardır. Təklif olunan yanaşmada İnternet məkanında informasiya müharibəsinin məqsəd və hədəflərinin təyini ilə yanaşı, bu informasiya müharibəsində iştirak edən gizli sosial şəbəkələrin aşkarlanması məsələsini həll edir. Çünki nəzərə almaq lazımdır ki, informasiya müharibəsi xüsusi təlim görmüş mütəxəssislər tərəfindən aparılır. Yeni yanaşma dövlətin iqtisadi və elmi-texniki siyasətinin təhlükəsizliyini təmin etməklə dünya açıq şəbəkəsinə qoşulmazdan öncə milli informasiya təhlükəsizliyi məsələsini həll edə bilər.

İnternet məkanında Azərbaycanın informasiya təhlükəsizliyinin təmin olunmasında viki-cəmiyyətin rolu analiz olunmuş, onun informasiya təhlükəsizliyində rolunu artırmaq üçün şərtlər göstərilmişdir.

Tədqiqatlar göstərdi ki, viki-texnologiyaları ilə idarə olunan Vikipediya virtual ensiklopediyasının dinamikliyi, viki-səhifələrin sayının və həcminin son illər həddən artıq çoxalması, ensiklopedik məqalələrin yaradılması prosesinə milyonlarla İnternet istifadəçisinin cəlb olunması viki-mühitdə informasiya təhlükəsizliyi və viki-səhifələrin keyfiyyəti ilə bağlı bir sıra problemlərin meydana çıxmasına səbəb olmuşdur. Viki-cəmiyyətin sosial-demoqrafik portretini analiz edərkən məlum olmuşdur ki, ixtisasından, yaşıdan, sosial durumundan, yaşadığı məkandan asılı olmayaraq wiki-mühitdə hər kəs aktiv fəaliyyət göstərə bilər. Viki-cəmiyyət üzvləri fəaliyyətlərindən asılı olaraq aşağıdakı kateqoriyalara bölünürlər:

Öz biliyini könüllü olaraq dünya ictimaiyyətinə çatdırmaq istəyən mütəxəssislər və elm adamları;

Əlavə bilik əldə etmək və bu biliyin daşıyıcıları ilə bilavasitə tanış olmaq istəyənlər;

Wiki-mühitin verdiyi geniş imkanlardan faydalanaraq yeni sosial münasibətlər və wiki-layihələr yaratmaq istəyində olan insanlar;

Wiki-texnologiyadan hər hansı siyasi-ideoloji baxışın yayılmasında istifadə etməyə çalışanlar.

Təsnifatlandırma sübut etdi ki, viki-cəmiyyət tərkibi və fəaliyyət istiqamətlərinə görə müxtəlif insanlardan təşkil olunur. Bu isə cəmiyyətin aktivliyinə, hadisələrə münasibətinə və s. amillərə təsir edir. Wikipedia layihəsi cəmiyyətdə baş verən proseslərə münasibətini, siyasi baxışını dünyaya ötürmək istəyən istifadəçilərin kollektiv işlədiyi yerdir. Bu baxımdan məqalələrin mövzusu onu redaktə edən istifadəçilərin biliyini, dünya görüşünü əks etdirir. Tədqiqatlar nəticəsində məlum olmuşdur ki, viki-istifadəçilər ensiklopediyaya tələb olunan informasiyanı deyil, şəxsən onları maraqlandıran məlumatları daxil etmələri viki-səhifələrdə informasiyanın həcminə, aktuallığına, keyfiyyətinə təsir göstərir və informasiya tutumuna görə viki-səhifələr arasında kəskin fərq yaradır. Digər tərəfdən, dünyada baş verən hər hansı hadisə (beynəlxal konfliktlər, Prezident seçkiləri, qlobal siyasi proseslər, idman yarışları və s.) viki-cəmiyyətin aktivliyini kəskin artırır və wiki-səhifələrin reytinqinə təsir edir.

Tədqiqatlar göstərdi ki, əsas problem viki-cəmiyyətin yaratdığı kontentin ictimai fikrə təsirində rolunun artmasıdır. Viki-cəmiyyətdə daima yenilənən kollektiv biliyin yaranma prosesini öyrənmək, wiki-istifadəçilər arasında münasibətləri və hansının daha çox nüfuza malik olmasını təyin etmək üçün müəyyən elmi yanaşmalar təklif edilir. Araşdırma zamanı məlum olmuşdur ki, bu gün bir çox şirkətlər viki-layihələrdən ənənəvi statistik İnternet saytlarını əvəz edən biliklər bazası kimi istifadə etməkdədirlər və adi veb-saytlara nisbətən viki-texnologiya əsasında idarə olunan layihələrə daha çox üstünlük verilir.

Tədqiq olunan predmet sahəsinə müxtəlif baxışların analizi göstərir ki, viki-cəmiyyətin e-dövlətdə rolu, viki-cəmiyyəti təşkil edən və ya onun aparıcı qüvvəsi olan ayrı-ayrı sosial qrupların davranışları tam öyrənilməmişdir.

Viki-mühitdə informasiya qarşıdurmalarının kəskinləşməsi və uzun müddət davam etməsi Vikipediya və onun layihələrinin (Vikilüğət, Vikisitat, Vikikitab. Vikimənbə, Vikixəbər, Vikiversitet və s.) inkişafına, ensiklopedik məqalələrin keyfiyyətinə, Vikipediya fəlsəfəsinin əsasını təşkil edən istifadəçilər arasında qarşılıqlı hörmət və tərəfsizlik prinsiplərinə ciddi zərbə vurmaqdadır. İstifadəçilər arasında konfliktlərin aradan qaldırılması, ensiklopedik məqalələrin vandalizm hallarından, əks təbliğat, dezinformasiya tipli məlumatlardan qorunması üçün viki-mühitin aktiv istifadəçiləri də cəlb olunmaqla administratorlar tərəfindən müxtəlif qaydalar işlənməkdədir

Tədqiqat zamanı viki-cəmiyyətin informasiya təhlükəsizliyində rolunu artırmaq üçün şərtlər dəqiqləşdirilmişdir və onlar aşağıdakılardır:

Problemlərin həlli ilə bağlı mütəmadi olaraq forumlar keçirilməlidir. Görülən işlərə nəzarət edilməli və problemlər tez bir zamanda öz həllini tapmalıdır.

Viki-cəmiyyətin birgə əməkdaşlığında və mütəşəkkil fəaliyyətində mühüm rol oynayan görüşlər keçirilməli, bu görüşlərə müxtəlif dövlət strukturlarından nümayəndələr dəvət etməlidir. Viki-cəmiyyətin fəaliyyəti vətəndaşların vaxtında məlumatlandırılmasına yönəldiyi üçün, o, e-dövlət prinsiplərinin cəmiyyətdə tanınmasında mühüm rol oynaya bilər.

İnternetin ən qlobal layihələrindən olan viki-layihələrin ölkədə tanınması üçün birgə tədbirlər planı işlənməlidir.

Dövlətin informasiya-şəbəkə infrastrukturunun yaradılmasında viki-cəmiyyətdən istifadə bürokratik maneələrin dəf edilməsi üçün mühüm amildir. E-dövlətin formalaşmasında viki-cəmiyyətdən istifadə edilməsi təklifi dövlət idarəçiliyi sisteminin müasirləşdirilməsi və təkmilləşdirilməsi prosesində, Azərbaycana qarşı təbliğat xarakterli kontentin İnternetdə azalmasında mühüm addım ola bilər.

İnternet məkanında Azərbaycana qarşı informasiya müharibəsi aparan gizli sosial şəbəkələrin aşkarlanması üçün model təklif edilmişdir.

Tədqiqatlar göstərir ki, İnternetdə 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.

Çox zaman mübahisə və qarşıdurma yaradan veb-saytlar İnternet istifadəçilərinin maraq obyektinə çevrilirlər. Bunları nəzərə alaraq, tədqiqat zamanı Vikipediya açıq saytı poliqon kimi istifadə olunmuş və bu saytdakı gizli sosial qrupları aşkarlamaq üçün yeni metod təklif edilmişdir.

Gizli sosial şəbəkələri aşkarlamaq üçün məsələnin mərhələlərlə həll olunması təklif olunur. Məsələnin həlli informasiya qarşıdurmasına səbəb olan veb-səhifələrin aşkarlanması, konfliktli səhifələrin məzmuna görə qruplaşdırılması, hər bir qrupdakı səhifələrin hazırlanmasında iştirak edən istifadəçilərin aşkarlanması və fəaliyyətlərinin analizini həyata keçirməklə mümkündür.

Tədqiqatda aşağıdakı göstəricilərdən istifadə olunmuşdur:

Veb-səhifələrin həcmi həcmi (baytlarla);

Səhifələrlə əlaqədar aparılan onlayn müzakirələrin həcmi (baytlarla);

Səhifənin predmetini təyin edən ilk abzasdakı sözlər;

Müzakirələrdə iştirak edən İnternet istifadəçilərinin sayı;

Veb-səhifədə edilən düzəlişlərin sayı;

Veb-səhifədə "silib-bərpa etmək" (*Reverting*) əməliyyatlarının sayı.

İnformasiya qarşıdurmasına səbəb olan veb-səhifələri aşkarlanması üçün hər bir səhifədəkii "silib-bərpa etmək" əməliyyatları, səhifənin özünün və müzakirə səhifəsinin həcmi nəzərə alınmalıdır. Belə ki, informasiya qarşıdurmasına səbəb olan səhifələr aşağıda göstərilən əlamətlərə görə normal dənədlərdən fərqlənirlər :

1. Veb-səhifənin müzakirə səhifələrinin həcmi səhifənin öz həcmindən daha böyük olur;
2. Açıq səhifələrdə "silib-bərpa etmək" əməliyyatı həyata keçirilir.

Yuxarıda göstərilən şərtlərdən heç olmasa biri baş verərsə səhifə informasiya qarşıdurmasına səbəb olan veb-səhifələr siyahısına daxil edilməlidir.

Klasterləşmə alqoritmlərindən, o cümlədən qraflar nəzəriyyəsindən istifadə etməklə səhifələri müxtəlif şərtlər daxilində qruplara ayırmaq mümkündür. İnformasiya qarşıdurmasına səbəb olan səhifələr təyin edildikdən və qruplara ayrıldıqdan sonra bu məqalələrin yaradılmasında və redaktəsində iştirak edən sosial şəbəkələrin aşkarlanması məsələsi həll edilməlidir. Bunun üçün klasterlərə ayrılmış konfliktli məqalələrin loq-fayllarından istifadə etmək nəzərdə tutulmuşdur. Loq-faylları analiz etməklə səhifənin nə zaman, kim tərəfindən yaradılması və hansı redaktələrin edilməsi haqqında informasiya əldə etək mümkündür.

Loq-faylın analizi zamanı məlum olur ki, istifadəçilərin bir hissəsi açıq səhifələrdə yalnız bir və ya iki dəfə redaktə etdikləri halda, müəyyən sayda istifadəçilərin redaktələrinin sayı onlarladır. İstifadəçi səhifəni redaktə etdikcə və hər dəfə “Save page” düyməsini vurduqca onun istifadəçi adı (*user name*) verilənlər bazasında qeydiyyata düşür. Veb-səhifələrdə etdikləri redaktələrin sayına görə istifadəçiləri qruplara ayırmaq mümkündür. İstifadəçilərin qruplaşdırılması nəticəsində informasiya qarşıdurmasına səbəb istifadəçiləri aşağıdakı siniflər üzrə təsnifatlandırmaq mümkündür:

Təsadüfi istifadəçilər.

Veb-səhifənin hazırlanmasında iştirak edənlər.

Viki-səhifələri nəzarətdə saxlayan gizli qruplar.

İnternet mühitində informasiya hücumlarında istifadə olunan milli domen adlarının analizi həyata keçirilmişdir.

Milli domen adları dedikdə, virtual məkanda domen adı kimi qeydiyyatdan keçmiş Azərbaycan Respublikasına aid olan tarixi, mədəni, mənəvi və digər dəyərləri özündə əks etdirən adlar (coğrafi adları, əmtəə və xidmət nişanları, şirkət və digər qurumların adları) başa düşülür. Məsələn, www.azerbaijan.com, www.baku.su, www.nakhchivan.net, www.sharur.com, www.sumqait.net, www.aghdam.com, www.fizuli.com, www.koroglu.net, www.azer.info, www.zurna.net və s.

Tədqiqat nəticəsində məlum olmuşdur ki, son illər İnternetdə yüksək səviyyəli domenlərin kütləvi meydana gəlməsi və çox sürətlə artımı, eyni zamanda korporativ informasiya sistemlərinin, veb- saytların, portalların yaradılması domen adları sahəsində bir çox problemlərin yaranmasına səbəb olmuşdur.

Təhlillər göstərir ki, domen adlarının ilkin təyinatı İnternet mühitində ünvanlaşdırma atributu, əmtəə nişanlarının, şirkət və digər qurumların adlarının daşıyıcısı olmasına baxmayaraq, bu gün qeyri-sağlam, ədalətsiz rəqabət vasitəsinə çevrilmişdir. Bu məqsədlə aparılan araşdırmalar nəticəsində müəyyən olunmuşdur ki, Azərbaycana mənsub olan bəzi coğrafi adları, tarixi, mədəni və digər dəyərləri özündə əks etdirən milli domen adları müxtəlif ölkələrdə yaşayan xarici vətəndaşlar tərəfindən qeydiyyatdan keçirilmişdir. Bu da nəinki Azərbaycan, eyni zamanda dünya ölkələri üçün də xarakterik məsələ olaraq ciddi əhəmiyyət kəsb edir.

İnternet mühitində informasiya hücumlarında istifadə olunan milli domen adlarının analizində statistik məlumatlardan istifadə olunaraq müqayisəli təhlil aparılmışdır. Müqayisəli təhlil nəticəsində məlum olmuşdur ki, Azərbaycana məxsus domen adları çox zaman xarici vətəndaşlar tərəfindən qeydiyyatdan keçirilir.

Virtual məkanda yüksək səviyyəli domen adların hüquqi aspektləri araşdırılmış və mövcud vəziyyət qiymətləndirilmişdir.

Tədqiqatlar göstərir ki, domen adları üzrə mübahisələr əmtəə nişanına, firma adına olan hüququn pozulması hallarında baş verir. Obyektiv səbəblərə görə domen adı bir qayda olaraq konkret şəxsin soyadı, firma adı və ya əmtəə adı ilə uyğun gələ bilər. Domen adları bu və ya digər dərəcədə fərdiləşdirmə vasitələri funksiyasını yerinə yetirir. Virtual məkanda vandalizmə və müxtəlif növ cinayətkarlığa qarşı, o cümlədən domen adlarının həqiqi sahiblərinə qaytarılması üçün beynəlxalq səviyyədə qəbul olunmuş bir sıra sənədlər və mexanizmlər mövcuddur:

– İnformasiya cəmiyyəti məsələlərinə həsr olunmuş dünya sammitlərinin sənədləri (Cenevrə - 2003, Tunis - 2005);

– BMT-nin XI konqresi (aprel 2005);

– Avropa Şurasının “Kompyuter cinayətkarlığı ilə mübarizə haqqında” Konvensiyası (2001);

– WIPO və ICANN tərəfindən “Domen Adları Üzrə Mübahisələrin Araşdırılmasının Vahid Siyasəti və Qaydaları” (24.10.1999).

“Domen” işləri üzrə bir çox ölkələrin (məsələn, RF) məhkəmə praktikası göstərdi ki, məhkəmələr belə işlərə baxmağa hazır deyildir. İntellektual mülkiyyət, İnternet adları ilə bağlı işlər çox geniş yayılmış işlər kateqoriyasına aid deyil. Bu sahələr yeni yarandığına görə hələ lazımi hüquqi baza yaradılmamışdır. Bu sahələr üçün hüquqi kadrların hazırlanması tələb olunur.

Yüksək səviyyəli coğrafi domen zonalarının müqayisəli təhlili onu göstərir ki, domen adının qeydiyyatı və idarə edilməsi ilə bağlı yaranan mübahisələrin həlli yolları da müxtəlifdir. Domen adının qeydiyyatı və idarə edilməsi ilə bağlı yaranan mübahisələrə baxılma ölkələrin qeydiyyat qaydalarında öz əksini tapır. Bu qaydaların yerinə yetirilməsində zonanın inzibatçı/qeydiyyatçı təşkilatı məsuliyyət daşıyır. Domen adları ilə bağlı yaranan mübahisələrə baxılma bir neçə üsulla yerinə yetirilə bilər:

– ICANN tərəfindən qəbul edilmiş UDRP çərçivəsində;

– Beynəlxalq Arbitraj Mərkəzlərə müraciət etməklə;

– ölkənin müvafiq qanunvericiliyinə uyğun olaraq məhkəmələrə müraciət etməklə;

qanuni metodlardan istifadə etməklə mübahisə edən tərəflər arasında müstəqil razılaşma yolu ilə (danışıqlar yolu).

Virtual məkanda domen adlarının həqiqi sahiblərinə qaytarılması üçün beynəlxalq səviyyədə qəbul olunmuş sənədlər mövcuddur. ICANN və WIPO-nun Siyasət və Qaydalarının qüvvəyə mindiyi vaxtdan

domenlər haqqında mübahisələrə baxmağa səlahiyyətləri olan Arbitraj Mərkəzlər (onların sayı beşdir) təyin olunmuşdur:

– Ümumdünya Əqli Mülkiyyət Təşkilatının Arbitraj və Vasitəçi mərkəzi (World Intelectual Property Organitation Arbitration and Mediaation Center, WIPO Arbitraj-vasitəçi mərkəzi), 1 dekabr 1999-cu il;

– ABŞ-ın Minnesota ştatında yerləşən Milli Arbitraj Forumu (National Arbitration Forum, NAF), 23 dekabr 1999-cu il;

– Nyu-Yorkda yerləşən, mübahisələrin həlli üzrə CPR İnstitutu (CPR İnstitute for Dispute Resolition), 22 may 2000-ci il;

– Domen Adları Üzrə Mübahisələrin Asiya Mərkəzi (Asian Domain Dispute Resolition Center), 3 dekabr 2001-ci il;

– "eResolution Kanada təşkilatı," 1 yanvar 2000-ci il.

İnternetin doğurduğu hüquqi problemlər "domen" fəzasına da aid olduğu üçün domen adlarının hüquqi tənzimlənməsinə böyük ehtiyac vardır. Bu problemlər ənənəvi hüquq praktikasında mövcud olmadığına görə onların həlli üçün tamamilə yeni metodların, mexanizmlərin işlənməsi tələb edilir. Çünki, domen adları ilə əlaqəli mübahisələr adətən əmtəə və ticarət nişanları, soyadları, fiziki və hüquqi şəxslərin fərdiləşdirmə vasitələri ətrafında baş verir. İntellektual mülkiyyətin qorunmasına dair ənənəvi qanunvericiliyin İnternetdəki müvafiq münasibətlərə tətbiq edilməsində böyük çətinliklər yaradır. Ona görə də İnternetdə intellektual mülkiyyət hüquqlarının qorunmasına dair xüsusi beynəlxalq konvensiyanın qəbul edilməsinə böyük ehtiyac duyulur.

Qeyd etmək lazımdır ki, bütün bu çətinliklərə baxmayaraq, son illər Birləşmiş Millətlər Təşkilatı (BMT) mandatı əsasında virtual mühitdəki idarəetmə, tənzimləmə problemlərinin həlli ilə məşğul olan İnternet İdarəçiliyi Forumu, BMT-nin müvafiq ixtisaslaşmış qurumları, elmi mərkəzləri, digər qurumlar İnternetlə bağlı hüquqi problemlərin həllinə cəhd göstərir, ölkələr üçün model qanunlar, tövsiyələr hazırlayırlar.

Virtual məkanda milli domen adlarından informasiya müharibəsində bir vasitə kimi istifadəsi ilə bağlı məsələlər araşdırılmış və problemin həlli ilə bağlı təkliflər verilmişdir.

Azərbaycan Respublikasının maraqları ilə bağlı domen adlarının real vəziyyətinin qiymətləndirilməsi məqsədi ilə aparılmış monitorinq onu göstərir ki, bəzi coğrafi adlar, tarixi, mədəni və digər dəyərləri özündə əks etdirən milli domen adları müxtəlif ölkələrdə yaşayan xarici vətəndaşlar tərəfindən qeydiyyatdan keçirilir (www.azerbaijan.tv, www.azer.info, www.baku.net, www.baku.su, www.nakhchivan.net, www.sumqait.net, www.aghdam.com və s.).

Domen adlarının xarici vətəndaşlar tərəfindən qeydiyyata alınmasının bir sıra səbəbləri var. Birinci səbəb açıq ölkə kodlu domenlərlə (məsələn, *.ru, *.de, *.cn, *.tv, *.ws, *.cc və s.) adların alınması və qeydiyyatdan keçirilməsi üçün, demək olar ki, heç bir məhdudiyyətin olmamasıdır. Buna görə də informasiya müharibəsi, qazanc əldə etmək və s. məqsədlərlə nüfuzlu adamların adları, tarixi-mənəvi dəyərlər, coğrafi adlar, əmtəə nişanları, xidmət nişanları, şirkət və digər qurumların adları və s.-dən istifadə etməklə domenlər yaradılır (www.baku.tv, www.karabakh.us, www.baku.ru və s.).

İkinci, yüksək səviyyəli ümumi domenlərin (*.com, *.info, *.org, *biz, *.net və s.) açıq qeydiyyatındakı boşluqların olmasıdır. Buna görə də bəzi şəxslər, dünyəvi dəyərləri, o cümlədən müxtəlif ölkələrə məxsus coğrafi adları, tarixi-mədəni dəyərləri və həqiqətləri əks etdirən milli adlara sahib çıxaraq, onları müxtəlif məqsədlərlə (siyasi, biznes və s.) domen adları kimi qeydiyyatdan keçirirlər (www.azerbaijan.com, www.karabakh.com, www.karabakh.info, www.lachin.com, www.sumgait.info və s.). Məsələn, aparılan

araşdırmalar göstərir ki, müxtəlif ölkələrdə yaşayan şəxslər Azərbaycanın maraqları ilə bağlı milli domen adlarını ələ keçirməklə virtual məkanda Azərbaycana qarşı İM aparırlar. Domen adlarından istifadə etməklə İM əsasən bir neçə istiqamətdə həyata keçirilir:

– aktiv İM, Veb-saytlarda Azərbaycana qarşı əks-təbliğat (dezinformasiyalar) aparılır (xalqımızın milli dəyərləri saxtalaşdırılaraq təhrif edilir);

– passiv İM, veb-saytlarda Azərbaycana aid olmayan informasiyalar verilir;

– informasiya blokadası, Azərbaycana məxsus məşhur adların əks olunduğu veb-saytlar məşğul edilir.

Yuxarıdakıları nəzərə alaraq domen adları sahəsində olan əsas problemlər kimi aşağıdakıları göstərmək olar:

– domen adı qeydiyyatının tənzimlənməsi sahəsində mövcud olan nöqsanlar;

– domen adlarının qeydiyyat prosesindəki şəffaflığın yetərincə olmaması;

– domen adı sahibi tərəfindən qeydiyyat qaydalarının pozulması;

– domen adının məsuliyyətsiz qeydiyyata alınması və istifadəsi;

– domen adını zəbt edənlərə (kiberskvottinq, fişinq və s.) qarşı vahid siyasətin işlənməməsi;

– domen adları sahiblərinin İP-ünvanlara, elektron poçta, ünvana, ada, soyada, yaşa, millətə, dövlətə, NS serverə, təşkilata və s. əlamətlərə görə dəqiq (intellektual) analizini aparmağa imkan verən proqram vasitələrinin olmaması;

– domen zonaları üzrə qiymətləndirilmə metodikasının olmaması;

– domen adları sahiblərinin hüququnun qorunması üçün mexanizimlərin çox zəif olması və s.

Bu problemlər bütövlükdə bütün İnternet şəbəkəsi üçün xarakterikdir.

Bütün bunları nəzərə alaraq WIPO, İCANN, Avropa Şurası, BMT kimi müvafiq qurumlara müraciət etməklə, virtual məkanda Azərbaycan adlarına təcavüz etmiş adamlara qarşı mübarizə aparmaq mümkündür. Belə ki, zəbt olunmuş domen adlarının qaytarılması ilə bağlı bəzi şirkətlərin bir neçə dəfə beynəlxalq Arbitraj məhkəmələrinə cəlb olunması, onlar tərəfindən qeyri-qanuni ələ keçirilmiş domen adlarının qanuni sahiblərinə qaytarılması faktları var. Bundan başqa virtual məkanda məşhur, strateji əhəmiyyət daşıyan domen adlarını qeydiyyatdan keçirərək, onları məşğul (bron) etməklə qismən də olsa problemin qarşısını almaq olar.

Dünya informasiya fəzasında Azərbaycanın öz yerini müəyyən etməsi möhkəmləndirməsi və ölkəmiz üçün ciddi əhəmiyyət kəsb edən İM-də üstünlük əldə etməsi üçün aşağıda sadalanan bəzi məsələlərin həlli çox vacibdir:

– virtual məkanda milli resurslarımız artırılmalı və qorunmalıdır;

– Azərbaycana məxsus olan coğrafi, tarixi, mədəni, mənəvi və digər dəyərləri özündə əks etdirən – domen adları müəyyənləşdirib qeydiyyatdan keçirilməlidir;

– İKT-də əldə olunan ən son nailiyyətləri Azərbaycanın milli dəyərlərinin qorunması işlərinə tətbiq olunmalıdır.

Kiberməkanda baş verən münaqişələr və informasiya qarşıdurmaları ilə bağlı problemlər analiz edilmiş, kiberhücumların məqsəd və hədəfləri göstərilmiş, kiberməkanda informasiya qarşıdurmasının üsul və vasitələri təsnifatlandırılmışdır.

Tədqiqat nəticəsində məlum olmuşdur ki, kiberməkanda baş verən münaqişələr informasiya müharibəsinin tərkib hissəsidir. Bu gün kibermünaqişə müxtəlif formalarda – sosial şəbəkələrdə baş verən qarşıdurmalardan başlamış dövlətin milli dəyərlərini əks etdirən domen adların ələ keçirilməsi, haker

hücumlarına kimi bütün istiqamətlərdə həyata keçirilir.

Münaqişə tərəflər arasında obyektiv və subyektiv ziddiyyətlərin təzahürüdür. Kibermünaqişə isə kiberməkanda yaranan kəskin qarşıdurmadır. Kibermünaqişələr gizli, təhlükəli, passiv, məkrli ola bilirlər və enerji, maliyyə sistemlərinin dağılmasından 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:

Qlobal şəbəkədə nəzarət mexanizminin olmaması;

Şəbəkə istifadəçilərinin sayının durmadan artması;

İstifadəçilərin anonimliyi, proksi-serverdən istifadə;

Şəbəkədə boşluqların olması;

Avtomatlaşma, şəbəkədə zaman və məkandan asılılğın aradan qaldırılması;

Kibermühitdə hüquqi əməkdaşlıqla bağlı problemlər.

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

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.

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 olunan hücumların aktiv təyini, analizi, şəbəkə təhlükəsizliyinin pozulması nəticəsində yaranan fəsadların tez bir zamanda aradan qaldırılması və real zaman çərçivəsində aqressuv 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.

Qloballaşma kibermüdafiə əməliyyatlarında bir sıra çətinliklərə səbəb olur. Bir tərəfdən informasiya sistemləri və şəbəkələri arasındakı asılılıq 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

Kiberhücum əməliyyatını ilk dəfə xüsusi informasiya təminatından istifadə edən hakerlər həyata keçirmişlər. Kiberhücumlarda 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.

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 proqramların müdaxiləsi, xidmətdən imtina ilə bağlı DoS hücumlar (Denial of Service Attack) və müxtəlif zərərli proqramların tətbiqidir.

Kiberhücumlarda informasiya mübadiləsinə zərər yetirən, qarşı tərəfin informasiya şəbəkəsindən lazım olan informasiyanı çıxara bilən vasitələr də mövcuddur. Kiberhücum vasitələrinə dövlət və korporativ informasiya sistemlərinə daxil etməyə imkan yaradan və bu sistemləri uzaq məsafədən idarə edən xüsusu proqramlar daxildir.

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 sistemlərini 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 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:

– dövlət təşkilatları tərəfindən idarəetmə funksiyalarını yerinə yetirən kompüter və əlaqə 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 idarəedici 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;

Terroristlər;

Xarici dövlətlərin orqanları.

8. Kibermünaqişədə effektivliyin əldə edilməsi üçün yrinə yetirilməsi vacib olan şərtlər göstərilmiş, təklif və tövsiyələr verilmişdir.

Aparılan tədqiqatlar nəticəsində təyin edilmişdir ki, 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.

Kibermünaqişədə nəzərə alınmalı əsas şərtlər aşağıdakılardır:

münaqişə pedmeti;

münaqişə tərəfləri;

kibermünaqişənin davamlı olması üçün şərtlər;

kibermünaqişənin miqyası: təşkilatlararası, dövlətlərarası və s.;

tərəflərin strateji və taktiki davranışı;

kibermünaqişənin fəsadları.

Kiberhmünaqişə 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 olunması, insanların həyatına təhlükə 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 sistemin normal fəaliyyətinin pozulması və informasiyanın oğurlanması;

təhlükəsizlik sistemlərini sıradan çıxarmaqla insanların həyatının təhlükəyə məruz qalması.

9. **Azərbaycan Respublikasının informasiya məkanında informasiya təhlükisizliyi vasitələrindən effektiv istifadə üçün metod və mexanizm təklif olunmuşdur.**

Təklif edilmişdir ki, İnternet məkanında informasiya müharibəsinin 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.

İnformasiya müharibəsində qarşı tərəf üzərində üstünlüyün əldə olunması ilə əlaqədar məsələləri həll etmək üçün İnternet şəbəkəsində münaqişələrin hər üç aspekti nəzərə alınmalıdır. Bu aspektlər aşağıdakılardır:

Kompüter şəbəkəsinə icazəsiz müdaxilənin vaxtında aşkar edilməsi və müvafiq tədbirlərin görülməsi;

Şəbəkənin yüklənməsinin qarşısının alınması.

Əkshücumun təşkil edilməsi: 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 yaradılmasında 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 olmasını

	təmin etmək nəzərdə tutulur ki, bu da şəbəkənin informasiya təhlükəsizliyində bir nömrəli məsələdir. Dövlətin və vətəndaşların informasiya, intellektual mülkiyyəti ilə bağlı qanuni hüquqlarına istiqamətlənmiş açıq siyasəti 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 sistematik, 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.
2	Layihənin həyata keçirilməsi üzrə planda nəzərdə tutulmuş işlərin yerinə yetirilmə dərəcəsi (faizlə qiymətləndirməli)
	Layihənin həyata keçirilməsi üzrə planda nəzərdə tutulmuş işlərin yerinə yetirilmə dərəcəsi yüksək faizlə ölçülə bilər
3	Hesabat dövründə alınmış **elmi nəticələr** (onların yenilik dərəcəsi, elmi və təcrübi əhəmiyyəti, nəticələrin istifadəsi və tətbiqi mümkün olan sahələr aydın şəkildə göstərilməlidir)
	İnternet mühitində fəaliyyət göstərən sosial şəbəkələrin cəmiyyətdə və elekrton dövlətin formalaşmasında rolu göstərilmişdir. Tədqiqatın nəticəsi kimi təklif olunmuş viki-cəmiyyətin e-dövlət proqramında iştirakının konseptual modeli dövlət və yerli özünüidarəetmə təşkilatlarının fəaliyyətində viki-cəmiyyətdən səmərəli istifadə edilməsini təmin edə bilər ki, bu da öz növbəsində dövlət orqanları ilə vətəndaşlar arasında münasibətlərdə maddi resurslara və vaxta qənaət etməklə, inzibati xidmətlərin keyfiyyətinin yüksəlməsinə təsir edə bilər. Bu məqsədlərə çatmaq üçün təklif olunan viki-cəmiyyətin e-dövlət çərçivəsində fəaliyyətinin konseptual modeli viki-cəmiyyətin bu və ya digər dövlətdə fəaliyyətinin səmərəliliyinə təsir etməklə, idarəetmə məsələlərinin həllini əhəmiyyətli dərəcədə asanlaşdıra və Azərbaycan Respublikasının İnternet məkanında təhlükəsizlik məsələlərinə yardım göstərə bilər. Ölkədə sağlam və aktiv viki-cəmiyyətin formalaşması dövlətin informasiya resurslarının İnternetdə çoxalması, informasiya cəmiyyətinin inkişafı, sosial-iqtisadi əlaqələrin genişlənməsi və nəhayət dünyada siyasi və iqtisadi nüfuzunun yüksəlməsinə yardım edə bilər. İnternet mühitində fəaliyyət göstərən gizli sosial şəbəkələrin aşkarlanması üçün yeni model işlənmişdir. Təklif edilən model sosial şəbəkələrdə, açıq layihələrdə, forumlarda və virtual ensiklopediyalarda konfliktə səbəb olan ziyanlı, təbliğat xarakterli və informasiya təsiri əməliyyatları üçün nəzərdə tutulmuş informasiya yaradan və onları nəzarətdə saxlayan gizli sosial şəbəkələri aşkar etməyə kömək edə bilər. Virtual məkanda reallaşdırılan reallaşdırılan informasiya qarşıdurmalarının qarşısının alınmasına və İnternetdə informasiya təhlükəsizliyi probleminin həllinə yardım edə bilər. Təklif olunan model, həmçinin, web2.0 texnologiyası əsasında fəaliyyət göstərən bir çox sosial şəbəkələrin analizində də istifadə oluna bilər. Domen adları sahiblərinin hüquqlarının qorunması üçün normativ-hüquqi bazanın imkanları xarakterizə olunmuş və bu sahədə mövcud olan problemlərin həlli üçün tövsiyələr verilmişdir. Ölkələrdə domenlərin və milli resursların inkişafı, idarəçiliyi və qiymətləndirilməsi prosesində problemlər hələ də qalmaqdadır. Bu onu göstərir ki, milli İnternet ünvanların qeydiyyatının tənzimlənməsi istiqamətində bir sıra işlərin aparılması zəruridir. Belə ki, mövcud qeydiyyat prosesi beynəlxalq normalara və ölkə qanunvericiliyinə cavab verməlidir. Telekommunikasiya haqında Azərbaycan Respublikasının Qanununa uyğun olaraq İnternet ictimaiyyətinin maraqlarına cavab verən Qeydiyyat qurumunun indiyədək formalaşmaması, ümumi maraqlara cavab verən Qeydiyyat Qaydalarının olmaması mənfi hal kimi qeyd olunmalıdır.

İnternetin normal inkişafı və ölkə domeninin daha da şəffaf istifadəsi üçün domenlərin paylanma mexanizmi Azərbaycan dövlətinin maraqları nəzərə alınmaqla həyata keçirilməlidir.

Virtual məkanda milli informasiya resurslarının artırılması və qorunması ilə bağlı təklif və tövsiyələr verilmişdir. Azərbaycanda son dövrlərdə milli informasiya resurslarının inkişafı və xarıcə axınının qarşısının alınması istiqamətində müəyyən işlər aparılır. Lakin beynəlxalq standartların daha uğurla tətbiq olunması üçün onların uyğun təcrübəsini həyata keçirmək, Azərbaycanda hostinq xidmətləri sahəsində uyğunluğu təmin etmək lazımdır. Eyni zamanda milli informasiya fəzasının inkişaf etdirilməsi olduqca önəmlidir. Hostinq xidmətlərin tənzimlənməsi üçün bütün tərəflərin maraqlarını təmin edən metodların seçilməsi və tətbiq edilməsi vacibdir. Müxtəlif beynəlxalq təşkilatlar və şirkətlər tərəfindən hazırlanan və təklif edilən hostinq xidmətlərin müvafiq qurumlar tərəfindən öyrənilməsi, milli maraqlara uyğunlaşdırılması və səmərəli qərarların verilməsi zəruridir.

Virtual Azərbaycanın hərtərəfli inkişafına əhəmiyyətli dərəcədə təsir edən amillərə daim nəzarət olunmalı, bu istiqamətdə işlər sürətləndirilməli, monitorinq və qiymətləndirilmə müntəzəm aparılmalıdır. Aparılan işlər virtual Azərbaycanın inkişafını ləngidən amillərin aradan qaldırılmasına imkan verəcəkdir.

Dövlətə qarşı informasiya müharibəsində istifadə olunan bəzi informasiya müharibəsi modellərinin analizi və təsnifatı aparılmışdır. E-dövlətin effektli idarə olunması üçün hökumət siyasi, hüquqi və diplomatiya sahələrində istifadə olunan informasiya resurslarının və şəbəkənin təhlükəsizliyini təmin etməlidir. Araşdırmalar göstərir ki, e-dövlətdə informasiya müharibəsi ilə bağlı problemləri yalnız informasiya sisteminin və ya kompüter şəbəkəsinin təhlükəsizliyini gücləndirməklə həll etmək mümkün deyil. E-dövlət quruculuğunda istənilən informasiya şəbəkəsinin layihələndirilməsini həyata keçirərkən, artıq sabah onun informasiya əməliyyatları meydanına çevriləcəyini nəzərə almaq lazımdır.

Tədqiq edilən informasiya müharibəsi modellərinin tətbiqi yüksək səviyyəli informasiya əməliyyatlarına aid olduğundan və yönəldici xarakterlərinə görə daha yüksək infrastrukturun müdafiəsində istifadə edilə bilər. İnformasiya müharibəsi hədəfləri ilə kritik infrastruktur eyni deyil və bu səbəbdən informasiya müharibəsi modelinin bütün mümkün ssenarilərdə tətbiqini gözləmək düzgün deyil. Hər bir model ilk növbədə müəyyən konseptual səviyyədə, mühitə uyğun insidentlər üçün tətbiq oluna bilər. İnformasiya müharibəsinin fundamental modellərinin bəzilərinin analizi və müqayisəsi e-dövlətdə kritik infrastrukturun müdafiəsində mühüm rol oynaya bilər.

Kibermünaqişə və kibercinayətkarlıqla bağlı problemlərin ümumi informasiya müharibəsi problemləri ilə müqayisəli analizi aparılmış, İnternetin genişlənməsi ilə əlaqədar son onillikdə informasiya əməliyyatları ilə bağlı təhlükələr aşkarlanmışdır. Məsələnin həllində sistemin dəyişən situasiyaya adaptasiya olması, potensial kiberdüşmənin qısa zaman intervalında proqnozlaşdırılması və özünütəşkil xüsusiyyətinə malik olması kimi məsələlərin həlinin vacibliyi sübut olunmuşdur. Təyin edilmişdir ki, informasiya müharibəsi və kibercinayətkarlıqla bağlı problemlər ümumi informasiya müharibəsi problemləri ilə müqayisədə daha cavandırlar və İnternetin genişlənməsindən asılı olaraq son onillikləri əhatə edir. Hazırkı vəziyyət və gələcək perspektivlərlə bağlı konkret fikir söyləmək çətindir. 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.

4	Layihə üzrə **elmi nəşrlər** (elmi jurnallarda məqalələr, monoqrafiyalar, icmallar, konfrans materiallarında məqalələr, tezislər) (dərc olunmuş, çapa qəbul olunmuş və çapa göndərilmişləri ayrılıqda qeyd etməklə, uyğun məlumat - jurnalın adı, nömrəsi, cildi, səhifələri, nəşriyyat, indeksi, İmpact Factor, həmmüəlliflər və s. bunun kimi məlumatlar -

	ciddi şəkildə dəqiq olaraq göstərilməlidir) *(surətlərini kağız üzərində və CD şəklində əlavə etməli!)*
	Ələkbərova İ.Y. Viki-mühitdə gizli sosial şəbəkələrin aşkarlasnması metodunun işlənməsi / "E-dovlət quruculuğu problemləri" I Respublika Elmi-Praktiki Konfrans, 4-5 dekabr, 2014 (çap olunmuşdur). Qasımova R.T. Domen adlarinin hüquqi aspektləri // İnformasiya Cəmiyyəti Problemləri, 2014, səh. 61-68 (çap olunmuşdur). Ələkbərova İ.Y. E-dövlətin formalaşmasında viki-cəmiyyətin rolu haqqında // İnformasiya Cəmiyyəti Problemləri, 2014, səh. 40-49 (çap olunmuşdur). Ələkbərova İ.Y. Kibermünaqişələrin yaratdiği problemlər və onlarin həlli yollari / "İnformasiya təhlükəsizliyinin multidissiplinar problemləri" üzrə II Respublika elmi-praktiki konfransı, 14 may, 2015 (çapdadır). Qasımova R.T. Qlobal domen infrastrukturunun təhlükəsizliyi –DNSSEC texnologiyası / "İnformasiya təhlükəsizliyinin multidissiplinar problemləri" üzrə II Respublika elmi-praktiki konfransı, 14 may, 2015 (çapdadır).
5	İxtira və patentlər, səmərələşdirici təkliflər
	Kibermünaqişənin vətəndaşların davranışlarının idarə olunması və informasiya resurslarının sıradan çıxması və ya funksional nasazlıqların yaradılması kimi nəticələrin iqtisadi böhranın yaranmasına və əhali arasında narazılıqların artmasına yönəldilməsi aşkarlanmışdır. Dövlətin iqtisadi və elmi-texniki siyasətinin bir istiqaməti kimi dünya açıq şəbəkəsinə qoşulmazdan öncə milli informasiya təhlükəsizliyi məsələsinin həlli tövsiyyə edilmişdir. Azərbaycan Respublikasının və onun vətəndaşlarının informasiya, intellektual mülkiyyəti ilə bağlı qanuni hüquqlarına istiqamətlənmiş açıq siyasəti ölkə daxilində şəbəkə vasitələrinin mühafizəsi fəaliyyətini dəstəkləmək və bu şəbəkəyə informasiya silahının gizli elementlərinin daxil olmasının qarşısının alınması və s. kimi məsələlərin həlli istiqamətləri müəyyənləşdirilmişdir. Şəbəkənin informasiya təhlükəsizliyinin təmin edilməsi üçün sistematik, kompleks yanaşma təklif olunmuşdur. Bu sahədə əlaqədar qurumlar tərəfindən konseptual, təşkilati, elmi-metodoloji, qanunvericilik, maddi-texniki əsasların yaradılması üzrə işlərin aparılması müasir dövrün ən vacib tələbi kimi irəli sürülmüşdür.
6	Layihə üzrə ezamiyyətlər (ezamiyyə baş tutmuş təşkilatın adı, şəhər və ölkə, ezamiyyə tarixləri, həmçinin ezamiyyə vaxtı baş tutmuş müzakirələr, görüşlər, seminarlarda çıxışlar və s. dəqiq göstərilməlidir)
	(burada doldurmalı)
7	Layihə üzrə elmi ekspedisiyalarda iştirak (əgər varsa)
	(burada doldurmalı)
8	Layihə üzrə digər tədbirlərdə iştirak
	(burada doldurmalı)
9	Layihə mövzusu üzrə elmi məruzələr (seminar, dəyirmi masa, konfrans, qurultay, simpozium və s. çıxışlar) (məlumat tam şəkildə göstərilməlidir: a) məruzənin növü: plenar, dəvətli, şifahi və ya divar məruzəsi; b) tədbirin kateqoriyası: ölkədaxili, regional, beynəlxalq)
	İradə Ələkbərova tərəfindən AMEA-nın İnformasiya Texnologiyaları İnstitutunun elmi seminarında məruzə edilmişdir. Mövzu: "Viki-mühitdə gizli sosial şəbəkələrin aşkarlasnması modeli" (24 aprel, 2014-cü il).

	Rəna Qasımova tərəfindən “E-dovlət quruculuğu problemləri” I Respublika Elmi-Praktiki Konfransda məruzə ilə çıxış edilmişdir: Mövzu: “Milli domen adlarının intellektual monitorinqi sisteminin yaradılması” (4-5 dekabr, 2014). İradə Ələkbərova tərəfindən “E-dovlət quruculuğu problemləri” I Respublika Elmi-Praktiki Konfransda məruzə ilə çıxış edilmişdir. Mövzu: “İnformasiya müharibəsi modellərinin müqayisəli analizi” (4-5 dekabr, 2014).
10	Layihə üzrə əldə olunmuş cihaz, avadanlıq və qurğular, mal və materiallar, komplektləşdirmə məmulatları
	Noutbuk kompüter – 1 ədəd P Pavilion 17-e074er Core i7-3632QM, 2.2GHz, 8 GB RAM, Tb HDD, DVD+/-RW, 1 GB AMD RN HD 8670M, 02.11b/g/n WLAN, BT, 17.3 HD+ w/CAM display, Win8 64 Rus N: 5CD33804LL Çoxfunksiyalı printer 3-ü 1-də – 1 ədəd P Pro M1132 MFP A4, 18 ppm, 1200 dpi, MB, USB, Faltbed *N: CNJ8FDXG58* 3-ü 1-də çoxfunksiyalı printer üçün – katric – 1 ədəd P LaserJet CE285 A Blak *N: 11373808768* Lisenziyalı proqram təminatı – MS OFİCE 2013 std (ingilis dilində) – 1 ədəd 1 illik lisenziyalı proqram təminatı – Kaspersky Antivirus 2014 – 1 ədəd
11	Yerli həmkarlarla əlaqələr
	(burada doldurmalı)
12	Xarici həmkarlarla əlaqələr
	(burada doldurmalı)
13	Layihə mövzusu üzrə kadr hazırlığı (əgər varsa)
	AMEA-nın İnformasiya Texnologiyaları İnstitutununda Viki-Mərkəz yaradılmış və viki-mühitdə Azərbaycanla bağlı kontentin artırılması və qorunmasının təşkili məqsədilə mühazirələr və praktiki seminarlar keçirilmişdir (1–30 aprel, 15 sentyabr – 15 oktyabr, 2014-cü il). “İnformasiya müharibəsi texnologiyaları ” və “Vikipediya virtual ensiklopediyasında informasiya müharibəsi” mövzusu ilə doktorant və dissertantlara mühazirə deyilmişdir.
14	Sərgilərdə iştirak (əgər baş tutubsa)
	(burada doldurmalı)
15	Təcrübəartırmada iştirak və təcrübə mübadiləsi (əgər baş tutubsa)

	(burada doldurmalı)
16	Layihə mövzusu ilə bağlı elmi-kütləvi nəşrlər, kütləvi informasiya vasitələrində çıxışlar, yeni yaradılmış internet səhifələri və s. (məlumatı tam şəkildə göstərilməlidir)
	Ələkbərova İ.Y., AzTV, "Səhər" proqramı, "Azərbaycan maraqları İnternet məkanında necə qorunur?", 15.05.2014 Ələkbərova İ.Y., ATV, "Xəbərlər" proqramı, "Azərbaycan həqiqətlərinin İnternetdə yayılması haqqında",16.01.2015 Ələkbərova İ.Y., Lider TV, "Xəbərlər" proqramı, "İnternetdə 20 yanvar hadisələri necə işıqlanır?", 20.01.2015.

SİFARİŞÇİ:
Elmin İnkişafı Fondu

Müşavir
Babayeva Ədilə Əli qızı

_____
(imza)
" __" _____ 201_-ci il

Baş məsləhətçi
Daşdəmirova Xanım Faiq qızı

_____
(imza)
" __" _____ 201_-ci il

İCRAÇI:

Layihə rəhbəri
Ələkbərova İradə Yavər qızı

_____
(imza)
" _02_" __dekabr__ 2016-cı il