İnformasiya cəmiyyətində e-universitetin informasiya təhlükəsizliyi

Məsumə Məmmədova[1], Cavanşir Zeynalov[2], Hüseyn Qasımov[3]

[1,3]*AMEA İnformasiya Texnologiyaları İnstitutu*

[2]*Naxçıvan Dövlət Universiteti*

[1]mmg51@mail.ru, [2]c.zeynalov@mail.ru, [3]hqasimov@gmail.com

***Xülasə*— Məqalədə informasiya cəmiyyətində informasiya və kommunikasiya texnologiyalarının tətbiqi ilə əldə olunan nəticələrlə yanaşı, mövcud təhlükələr araşdırılmış, e–dövlətin strateji obyekti kimi e-unversitetlərin bu sahədə hansı təhlükələrin hədəfi ola biləcəyi və bu təhlükələrdən mümkün qorunma yolları göstərilmişdir.**

Açar sözlər— informasiya cəmiyyəti; e–unversitet; kompüter sabotajı; spam; log fayllar; gizli qapılar.

I. GİRİŞ

Bu gün elmin, texnikanın bütün sahələri sürətlə inkişaf edir. Bu inkişaf daha çox informasiya-kommunikasiya texnologiyaları (İKT) sahəsində özünü büruzə verir. İKT-nin inkişafı, demək olar ki, "işıq sürəti" ilə baş verir. Bu günün texnologiyası sabah artıq köhnəlmiş olur.

İKT-də baş verən inkişaf elmdən mədəniyyətə, ticarətdən əyləncəyə, dövlət sektorundan özəl sektora qədər bir çox sahələrdə klassikləşən anlayışları dəyişdirmiş, insanlara yeni bir yaşayış tərzi gətirmişdir.

Bu inkişaf sayəsində informasiya cəmiyyəti, e-dövlət, e-qurumlar meydana gəlmiş, e-xidmətlər formalaşmışdır ki, bu da cəmiyyətin hər bir üzvünün daha rahat yaşamasına, vaxta qənaət etməsinə, lazımi məlumatları daha rahat əldə etməsinə xidmət edir.

Ancaq bütün bu rahatlıqlarla bərabər, bir sıra neqativ hallar da həyatımıza daxil olur. Klassik düşüncəyə tamamilə yad olan bir sıra təhlükə və cinayətlər kibertəhlükə, kiberhücum, kiber-cinayət adı ilə tez-tez rast gəldiyimiz mövzulara çevrilmişdir.

Bu gün dünyada İKT sahəsində yüksək bacarıqları olan istənilən şəxs və ya qrup kompüter vasitəsilə aldatma və saxtakarlıq, səlahiyyətsiz qoşulma və dinləmə, kompüter sabotajı, proqramların lisenziyasız istifadəsi, məlumatların qanunsuz oğurlanması və yayılması, kiberterror, ödəmə sistemində saxtakarlıq və digər yollarla bütövlükdə cəmiyyətə, ayrı-ayrı qurum və vətəndaşlara ziyan vura bilər [1].

Bütün bu sadalananların fonunda, demək olar ki, artıq bütün dünya dövlətlərinin tam təhlükəsizlik məsələləri də sual altına düşmüş olur. İnformasiya cəmiyyətinin bu cür inkişafı cəmiyyətdə olan xüsusi əhəmiyyətli məlumatların kənar qüvvələr üçün də daha da əlyetərli olmasına şərait yaradır.

Öz müstəqilliyini ikinci dəfə əldə etdikdən sonra keçən bu qısa müddət ərzində vətənimiz Azərbaycan da dinamik inkişaf yolunda qətiyyətli və sürətli addımlar atır. Rabitə və İKT sahəsində daha qabarıq şəkildə baş verən bu inkişaf Azərbaycanın yaxın və uzaq qonşularını müəyyən mənada qıcıqlandırır. Buna görə də, dövlətimiz böyük və güclü, eyni zamanda, kiçik və "digərləri üçün maraqsız" dövlətlərə nisbətən daha çox informasiya təhlükələri hədəfinə çevrilir ki, bu da cəmiyyətimiz üçün informasiya təhlükəsizliyinin prioritet məsələ olduğunu göstərir.

II. E-UNIVERSITETLƏR VƏ ONLARIN TİMSALINDA BÜTÜN CƏMİYYƏT ÜÇÜN REAL İNFORMASİYA TƏHLÜKƏLƏRİ

Hər zaman olduğu kimi, informasiya cəmiyyətində də universitetlər müstəsna əhəmiyyətli strateji obyektlər kimi qiymətləndirilir.

Kompüter texnologiyalarının və proqram təminatının inkişafında universitetlər aparıcı rol oynayırlar. Universitetlərdə İKT sahəsində baş verən yeniliklər daha tez tətbiq olunaraq sınaqdan çıxarılır. Buna görə də, kibercinayətlərin sürətlə artdığı zamanda məxfi məlumatların mühafizəsində və işlənməsində təhsil müəssisələri xüsusi aktuallıq kəsb edir [2].

E-universitetlər müxtəlif xarakteli nəhəng məlumat bankına sahib olan infrastrukturlardır. Bu məlumat bankı təkcə hansısa metodik vəsaitin elektron variantı deyil, həm də cəmiyyətin və onun ayrı–ayrı üzvlərinin təhlükəsizliyi üçün xüsusi əhəmiyyətli məlumatlar toplusudur. Nəzərə alsaq ki, təhsil müəssisələrində cəmiyyətin bugünkü və gələcək elmi potensialı formalaşır, bu zaman bu məlumatların nə qədər əhəmiyyətli olduğu bir daha aydın görünür [2].

E-universitetin məlumat bazasına daxil olmağı bacaran məqsədli kənar qüvvə universitetin bugünkü və keçmiş tələbələri, əməkdaşları haqqında fərdi məlumatlar əldə etməklə yanaşı, universitetdə tədris olunan istənilən fənn, onun tədris və mənimsəmə səviyyəsi haqqında real informasiya əldə edə bilər. Bu da onun cəmiyyətin müəyyən bir hissəsi və ya bütövlükdə hamısı üçün planlaşdırdığı hücumun səviyyəsini müəyyən etmək və onu həyata keçirmək üçün əla əsas ola bilər.

Nəzərə alsaq ki, tələbələrin böyük əksəriyyəti 18-23 yaş arası gənclərdir və bu yaş dövrü insanın psixoloji cəhətdən daha həssas dövrüdür, bu zaman demək olar ki, sadə psixoloji sual-cavablarla tələbənin zəif və güclü yerlərini öyrənib, onu hər hansı bir planın ortağına, "iş alətinə" çevirmək də olar.

Bütün bunlar o demək deyil ki, universitetlər üçün təhlükə mənbəyi yalnız xarici qüvvələrdir. Öz kampusu daxilində təhsil verən və eyni zamanda, təhsildə e-xidmətlər göstərən universitetlərin məlumat bazaları hansısa müəllimdən narazı qalmış, İKT sahəsində yaxşı bacarığı olan tələbə tərəfindən "qisas" almaq məqsədilə və ya "özünü sübut edən" tələbələr tərəfindən də zərbələrə məruz qala bilər.

III. KİBERHÜCUMLARA MƏRUZ QALMIŞ BƏZİ UNİVERSİTETLƏR

İnformasiya cəmiyyətinin inkişafı fonunda cəmiyyətin bütün hüquqi və fiziki şəxsləri ilə yanaşı, təhsil müəssisələri də daim informasiya hücumlarının qurbanına çevrilirlər. Bunlardan bir neçəsinə nəzər salaq:

- *Austin Texas Universiteti*nin şəbəkəsi 2003-cü ilin fevral ayında naməlum hakerlərin hücumuna məruz qalmışdır. Hakerlər universitetin informasiya şəbəkəsinə daxil olduqdan sonra sosial sığorta nömrələrini (SSN) generasiya edən proqram vasitəsilə SSN-ləri uyğun gələn tələbə və universitet əməkdaşlarının digər məlumatlarını əldə etməyə müvəffəq olmuşlar. Fevral ayından başlayan hücumlar yalnız mart ayının 2-də aşkarlanmışdır. Hücum nəticəsində 55200 nəfər zərər çəkmişdir [3].
- *Batler Universiteti.* 2013-cü ildə unversitetin məruz qaldığı kiberhücum nəticəsində 163 min tələbə, məzun və əməkdaşın verilənləri oğurlanmışdır. Sızma faktı fləş-kartda əməkdaşlardan birinin fərdi məlumatlarının ortaya çıxmasından sonra məlum olmuşdur. Universitet zərərçəkmiş əməkdaşlara sığorta ödəyib, itmiş məlumatların hara getməsini öyrənmək üçün monitorinq elan etsə də, məlumatların necə və hansı məqsədlə oğurlanmasını müəyyən etmək mümkün olmamışdır [4].
- *Kaliforniya Universiteti.* 21 mart 2005-ci ildə universitetin rəhbərliyi 3 həftə əvvəldən başlayaraq universitetə haker hücumlarının olması və 59 min tələbə və əməkdaşın zərər çəkməsi barədə rəsmi məlumat yaymışdır [5].
- *Ohayo Universiteti.* Naməlum hücumlar nəticəsində hakerlər əvvəlcə universitet serverinin texniki parametrlərini öyrənmiş, daha sonra isə 760 min nəfərin şəxsi məlumatları daxil olan bütün bazanı oğurlayaraq, qara bazarda satmağa müvəffəq olmuşlar. Universitet rəhbərliyinin açıqlamasına görə, hücum nəticəsində universitetə 4 milyon ABŞ dolları ziyan dəymişdir [6].
- *Alabama Universiteti.* 1994-cü ildə naməlum haker tərəfindən universitetin 17 serverinə yönəlmiş hücum nəticəsində müayinə olunmuş xəstələrin analiz nəticələrini araşdırmaq üçün laboratoriya işlərinə cəlb olunmuş 37 min tələbənin bütün məlumatları və əldə olunmuş nəticələr oğurlanmışdır. Nəticədə universitetə 2 milyon dollar həcmində ziyan dəymişdir [7].
- *Virciniya Universiteti.* 2010–cu ildə kibercinayətkarların hücumu nəticəsində heç bir tələbə və əməkdaşın fərdi məlumatlarına zərər vermədən universitetin hesabından 1 milyon dollar məbləğində vəsait oğurlanmışdır [8].

Bütün bu sadalananlar informasiya cəmiyyətində hec kimin kibercinayətlərdən tam sığortalanmadığını və universitetlərin bu sahədə nə dərəcədə təhlükə hədəfi olduqlarını göstərir.

IV. UNİVERSİTETLƏRİN KİBERHÜCUMLARA QARŞI MÜMKÜN MÜHAFİZƏ VASİTƏLƏRİ

Yüksək texnologiyaların inkişafı nəticəsində artan kibercinayətlər mühiti təhsil müəssisələrində hesablama şəbəkələrinin xüsusi qaydada təhlükəsizliyini təmin etməyi tələb edir. Bu mühit hər bir təhsil müəssisəsinin xüsusi təhlükəsizlik sisteminin olmasını, bu sistemlərdən istifadə üçün normativ hüquqi bazanın yaradılmasını, təhlükəsiz fəaliyyət üçün müəyyən ölçü tədbirlərinin görülməsini tələb edir. Bu tələblər elektron formada istənilən səviyyədə fəaliyyət göstərən təhsil müəssisələrinə şamil edilir.

Cəmiyyətin bütün sahələrində olduğu kimi, təhsil sahəsində də informasiya təhlükəsizliyini təmin etmək üçün bir çox sistemlər, proqram təminatları və prosedur qaydalar mövcuddur. Bunlarla yanaşı, e-universitetlərin informasiya təhlükəsizliyini təmin etmək üçün bəzi digər tədbirlərin də görülməsi məqsədəuyğundur. Bunlar aşağıdakılar ola bilər:

Bu gün ixtisasından asılı olmayaraq bütün tələbələr üçün tədrisi məcburi olan bir çox fənnlər vardır ki, bunlar da, ölkə tarixi, konstitusiya və hüququn əsasları, xarici dil, mülki müdafiə və s. fənlərdir. Bütün bunlarla yanaşı, elektron xidmətlər göstərmə və təhsil səviyyəsindən asılı olmayaraq bütün təhsil müəssisələrində informasiya təhlükəsizliyi məsələlərini, təhlükə mənbə və formalarını, ondan qorunma yollarını özündə ehtiva edən "informasiya təhlükəsizliyi" fənninin tədrisi məqsədəuyğun hesab edilə bilər. Bu addım gələcəkdə hər hansı bir təşkilatda çalışan mütəxəssisin İKT sahəsində daha rahat və təhlükələrdən mümkün qədər sığortalanmış şəkildə fəaliyyət göstərməsinə səbəb olar.

Məlumdur ki, bir çox mütəxəssislər şəbəkələrini qurduqda və ya müəyyən proqram təminatı hazırladıqda, öz məqsədləri üçün sistemlərə giriş qapıları qoyurlar ki, bu da elmi ədəbiyyatlarda "gizli qapılar" adı ilə tanınır. Proqram təminatının hazırlanması və quraşdırma işlərinin yerli mütəxəssislər tərəfindən yerinə yetirilməsi məqsədli xarici qüvvələr üçün bu "gizli qapıları" bağlamış olur.

Demək olar ki, bütün müəssisələrdə informasiyalar öz məxfilik və əhəmiyyətlilik dərəcələrinə görə səviyyələrə bölünürlər. Bu informasiyalarla işləmək üçün sistemə giriş hüququ yalnız xüsusi kadrlarda olur. Bir çox müəssisələrdə bu informasiyalara daxil olmaq üçün ayrılmış kompüterlər olur ki, onların da İP ünvanları, istifadəçi adları, giriş şifrələri sistem tərəfindən tanınır. Bütün bunlarla yanaşı bu cür əhəmiyyətli məlumatları əldə etmək üçün ayrılmış kompüterlərin MAC ünvanlarının da sistem tərəfindən qeydə alınması və hər dəfə giriş zamanı yoxlanması da sistemin daha təhlükəsiz işləməsinə kömək etmiş olar.

NƏTİCƏ

Təhsil müəssisələri dövlətin strateji obyektləridir. İnformasiya cəmiyyətində mümkün qədər təhlükəsiz yaşamaq üçün bu sahədə yaxşı təhsil almış cəmiyyət nümayəndələrinin daha çox olması əsas şərtlərdəndir. Bunun üçün isə ilk növbədə təhsil müəssisələrinin özlərinin daha möhkəm informasiya təhlükəsizliyi olmalıdır.

ƏDƏBİYYAT

[1] Güncel Tehdit: Siber Suçlar. Ankara: Seçkin Yayıncılık yayın evi, 2014.
[2] http://www.itsec.ru/articles2/Oborandteh/obespechenie_ib_v_vuzah
[3] http://soft.compulenta.ru/38132/
[4] http://ko.com.ua/ataka_na_universitet_batlera_postradali_163_tys_chelovek_105902
[5] http://protoplex.ru/news_show/2159.html
[6] http://pd.rkn.gov.ru/press-service/news612.htm?print=1
[7] http://www.securitylab.ru/blog/company/breach_blog/7945.php
[8] https://xakep.ru/2010/09/06/53164/