E-dövlətə kiberhücumlar və onlarla mübarizə üsulları haqqında

Günay İskəndərli
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
gunayniftali@gmail.com

***Xülasə*— E-dövlət hökumətin öz vətəndaşları ilə münasibətlərin yaxşılaşdırılmasına yönəlmiş səylərinin nəticəsidir. E-dövləti kiber-məkanda mövcud təhlükələrdən qorumaq üçün informasiya təhlükəsizliyinin ən yaxşı təcrübələrinə ehtiyac var. Təhlükəsizliyə dair siyasət, praktika və prosedurlar, eyni zamanda, təhlükəsizlik texnologiyasından istifadə e-dövlət sistemlərinin hücumdan müdafiə edilməsinə, qeyri-normal fəaliyyət göstərən xidmətlərin aşkar edilməsinə kömək edə bilər. Bunları nəzərə alaraq məqalədə kiber-təhlükəsizlik, e-dövlətə olan əsas kiber-hücumlar haqqında məlumat verilmişdir.**

Açar sözlər— e-dövlət; informasiya təhlükəsizliyi, kiber hücumlar.

I. GİRİŞ

Kibertəhlükəsizlik XXI əsrin ən ciddi problemlərindəndir. Təhlükələr müxtəlif mənbələrdən yaranır və fərdlərə, biznesə, milli infrastrukturlara və hökumətlərə qarşı yönəlmiş dağıdıcı fəaliyyətlərdə özünü göstərir. Onların təsiri ictimai təhlükəsizlik, milli təhlükəsizlik və beynəlxalq ictimai sabitlik üçün ciddi risk daşıyır [1]. Bütün bunlar kiber təhlükəsizlik məsələlərinə, xüsusilə kiber-hüquqa olan diqqəti artırır.

Kiber hüquq qeyri-maddi rəqəmsal dünyada, məsələn, kiber məkanda qeyri-maddi məlumatlara hüquqi statusun verilməsi, belə məlumatların təhlükəsizliyi, məxfiliyinin təmin olunması, qanun pozuntularını tənzimləyən qanunlardır. Kiber-qanunlar kiber məsələləri tənzimləmək üçün əhəmiyyətli və etibarlı aktlar hesab olunur. Təhlükəsizlik dedikdə, əsasən hər hansı təşkilatın İKT aktivlərini qorumaq nəzərdə tutulur. Aktivlər dedikdə bura verilənlər, məlumatlar, bilik resursları, proqramlar, avadanlıqlar, şəbəkələr və s. kimi daxili və xarici resurslar daxildir. İKT sistemlərinin təhlükəsizliyinə olan təhdidlər bir çox mənbələrdən və müxtəlif formalarda ola bilər. Həmçinin təhdidlər fərqli növlərdə, ölçüdə və təsir gücündə ola bilər.

E-dövlət də hazırda bu cür təhdidlər üçün potensial resurs hesab olunur. E-dövlətdə daxili və xarici təhlükə mənbələri mövcuddur. Daxili təhlükə mənbələrindən bəziləri özəl və ya dövlət qurumlarının əməkdaşları, e-dövlət proqramlarının istifadəçiləri, xarici mənbələri isə xakerlər, cinayət/terrorçu qruplar və ya təşkilatlar, kəşfiyyat və istintaq orqanları ola bilər. Dövlət infrastrukturunu bu cür hücumlardan qorumaq hazırda aktual məsələlərdən biri hesab olunur. Bunları nəzərə alaraq məqalədə e-dövlət və kiber təhlükəsizlik məsələlərinə toxunulmuş, məqalənin ikinci bölməsində kiber təhlükəsizlik, üçüncü bölməsində e-dövlətə olan kiber hücumlar haqqında ətraflı məlumat verilmiş, onların həll yolları göstərilmişdir.

II. KİBER-TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

Kiber-təhlükəsizlik informasiya sistemlərinin (şəbəkələrin, kompüterlərin, məlumat bazalarının, məlumat mərkəzlərinin və tətbiqlərinin) müvafiq prosessual və texnoloji təhlükəsizlik tədbirləri ilə qorunmasıdır. Bu mənada kiber-təhlükəsizliyin təsviri olduqca ümumidir və bütün müdafiə tədbirlərini əhatə edir.

Kiber-təhlükəsizlik nəzarətinin effektiv olduğu yerlərdə kiber-məkan etibarlı rəqəmsal infrastruktur hesab olunur. Kiber-təhlükəsizliyin qeyri-obyektiv və düzgün tərtib olunmadığı sahə rəqəmsal çağın “vəhşi qərbi” hesab edilir. Müvafiq dövrdə "kiberməkan" termini konsepsiyadan texniki səviyyəyə qədər olan anlayışlara malikdir və onun torpaq, dəniz və hava kimi dördüncü mühüm sahə olduğu iddia edilmişdir. Ədəbiyyatda kiber məkan və kiber təhlükəsizliyin çoxsaylı tərifləri mövcuddur. Kiber-təklükəsizlik ən çox aşağıdakı 3 terminlə əlaqələndirilir [2]:

- Qarşısını alma, aşkar edilmə və cavab verilmə;
- İnsanlar, proses, texnologiya;
- Məxfilik və bütövlük.

Bunlar kiber-təhlükəsizliyin hədəflərini, təmin edilməsi vasitələrini və kiber-təhlükəsizlik hədəflərinin əldə etdiyi mexanizmləri əks etdirir.

Birinci hissə fiziki və kiber-təhlükəsizliyə aid ümumi hədəflərin qarşısını almaq, aşkarlamaq, cavablandırmağa yönəlib. İkinci hissə ümumi olaraq texnologiya idarəçiliyinə və xüsusi bir sahə kimi kiber-təhlükəsizliyin idarə edilməsinə yönəlib. Üçüncü hissə isə məlumatlara aid olan təhlükəsizlik məqsədlərinə yönəlib.

Kiber-təhlükəsizlik e-kommersiya, e-bank, e-dövlət, e-səhiyyə və e-market üzrə kiberqaydalar ilə məşğul olur [3]. Təhlükəli kiberdünyadan istifadə edənlər istisna olmaqla, hər kəs təhlükəsizlik, gizlilik, məxfilik, bütövlüyün olduğu və etibarlı, orijinal məlumatların mövcudluğunu təmin edən etibarlı texnologiya mühitinə ehtiyac duyur. Bu baxımdan müxtəlif informasiya təhlükəsizliyi standartları mövcuddur. Bu

DOI: 10.25045/NCInfoSec.2018.37

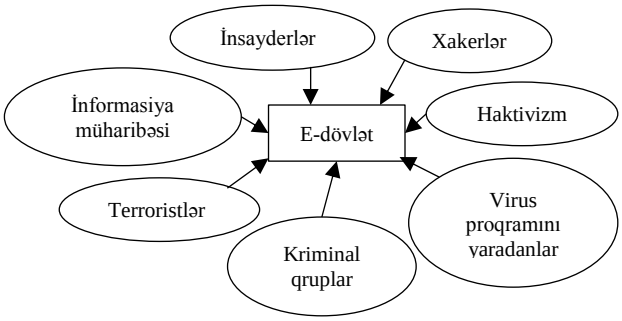
standartlar siyasətin nə kimi görünməsini məsləhət etməkdən başqa, informasiya təhlükəsizliyi siyasətini uğurla tətbiq etmək üçün lazım olan çoxsaylı prosesləri müəyyən etməyə çalışır. Təhlükəsizlik siyasəti informasiya sistemlərinin təhlükəsizliyi ilə bağlı bir qurumdan gözlənilənləri müəyyənləşdirmək üçün nəzərdə tutulub. Ümumiyyətlə, bu standartlar təsadüfən və ya qəsdən hərəkətlər nəticəsində informasiya aktivlərinə olan təhlükəni azaltmaq məqsədilə insan davranışını idarə etmək üçün hazırlanmışdır. Bu standartlar vasitəsilə, həmçinin, texnologiya üzrə aparıcı ölkələrin təcrübəsi ilə informasiya resurslarının təhlükəsizliyi və rifahını təmin etmək mümkündür.

III. E-DÖVLƏTƏ OLAN KİBER HÜCUMLAR

E-xidmətlərin inkişafı və yayılması e-dövlət sisteminin effektivliyinə təsir göstərməklə yanaşı, inkişaf etməkdə olan və inkişaf etmiş ölkələrdə dövlət üçün əlavə problemlər yaratmışdır. Belə ki, təklükəsizlik e-dövlətin hər bir prosesində ortaya çıxan əsas məsələlərdən biridir. Təhlükəsizliyi təmin etmək isə asan məsələ deyildir. Belə ki, vətəndaşların e-dövlət xidmətlərindən istifadə etməsini təşfiq etmək üçün bu mühitdə məlumatların gizliliyinin qorunub saxlanılmasını təmin etmək vacibdir [4, 5].

Lakin təəssüf ki, e-dövlətin özü də bədniyyətlilərin hədəfi ola bilər. Belə ki, kiber məkanda bədniyyətli fərdlər potensial hədəfləri tapmaq, zəifliklər müəyyən etmək və ya istismar etmək, fərqli məlumatları əldə etmək və inteqrasiya etmək üçün hökumət veb-saytlarının məzmunundan istifadə edə bilərlər [6, 7]. Dövlət veb-saytlarına çoxsaylı kiberhücumlar ola bilər. Belə ki, bu hücumlar vasitəsilə infrastrukturun (kompüter sistemi, elektrik şəbəkəsi və s.) zədələnməsi və ya məhv edilməsi dövlətə külli miqdarda zərər verə bilər. Belə hücumların vaxtında aşkarlanması, qarşısının alınması və profilaktik işlərin görülməsi vacib məsələlərdən biridir. Bunun üçün isə dövlətə ola biləcək əsas kiber hücumları əvvəlcədən müəyyənləşdirmək və analiz etmək məqsədəuyğundur.

E-dövlətə olan əsas kiber-təhlükələr şəkil 1-də təsvir olunmuşdur [8].



Şəkil 1. E-dövlətə kiber təhlükələr

İnsayderlər: narazı insayderlər (keçmiş əməkdaş) kompüter cinayətinin əsas mənbəyidir;

Hakerlər: Hakerlər qərəzli məqsədlər və maliyyə mənfəəti üçün şəbəkələrə hücum edirlər;

Haktivizm: siyasi mesajlar göndərmək, saxta görüntü yaratmaq və ya məlumat vermək, mətni dəyişdirmək üçün veb səhifələrə və ya e-poçt xidmətlərinə siyasi əsaslı hücumlardır;

Virus proqramını yaradanlar: dağıdıcı kompüter viruslarının yayılması dünyada şəbəkələr və proqram təminatları üçün getdikcə ciddi təhlükə yaradır;

Kriminal qruplar: cinayətkarlar tərəfindən mənfəət əldə etmək üçün sistemlərə hücum cəhdləridir;

Terroristlər: bu qruplar informasiya texnologiyaları və İnternetdən planlar hazırlamaq, pul vəsaitlərini artırmaq, təbliğat və təhlükəsiz ünsiyyət qurmaq üçün istifadə edirlər;

İnformasiya müharibəsi: xarici qüvvələrin kritik infrastrukturlara qarşı "informasiya müharibəsi" milli təhlükəsizliyə ciddi təhdiddir.

Ədəbiyyatda dövlətə qarşı olan bu cür kiber hücumların qarşısının alınması məqsədilə bir sıra çıxış yolları göstərilmişdir. Bunlar aşağıdakılardır [1]:

- Müvafiq reaksiyanı müəyyənləşdirmək və həyata keçirmək üçün İKT infrastrukturuna qarşı təhlükələrlə bağlı zəruri biliklərin yaradılması;
- Təhlükəsiz kiberməkanı dəstəkləmək üçün əlverişli hüquqi mühitin yaradılması, e-əməliyyatlarda inam və etibarın təmin olunması; maraqlı tərəflər tərəfindən məsuliyyətli hərəkətlərin təmin edilməsi və effektiv cinayət təqibinə imkan verən hüquq-mühafizə imkanlarının artırılması;
- İKT şəbəkələrinin, kritik kommunikasiya və informasiya infrastrukturlarının qorunması;
- Effektiv proqnozlaşdırıcı, profilaktik, qoruyucu, cavab və bərpa tədbirləri vasitəsilə kiber təhlükə və böhranın idarə edilməsi üçün 24 x 7 mexanizmlərinin yerləşdirilməsi;
- Beynəlxalq Təhlükəsizlik təcrübələrinin, siyasət, təşviq və tədbirlərin öyrənilməsi;
- Kiber-təhlükəsizliyin yaradılması məqsədilə istifadəçilərdə İKT-dən istifadə davranışı mədəniyyətinin yaradılması;
- Təhlükəsiz mühit yaratmaq üçün həssas fərdi məlumatların işlənməsi, idarə edilməsi, saxlanması, tranziti və məlumatların qorunması.

Bütün bunlarla yanaşı e-dövlətə olan kiber-hücumların qarşısının alınması üçün hökumət şöbələrinin və ya qurumların yüksək səviyyəli rəhbərliyi müvafiq informasiya təhlükəsizliyi siyasətini həyata keçirməli və təşkilatdakı müvafiq texnologiya və tətbiqlərin istifadəsini təşviq etməlidir. O cümlədən təşkilatlarda "İnformasiya Təhlükəsizliyi Çərçivəsi" yaratmaq, idarə etmək lazımdır [9].

NƏTİCƏ

Vətəndaşların vaxtında və səmərəli xidmətlərə olan tələbi nəticəsində e-dövlət xidmətlərinin sayı günbəgün artmaqdadır. E-dövlət, eləcə də e-idarəetmə artıq qlobal iqtisadiyyatda əhəmiyyətli yer tutmuşdur. E-dövlətdən istifadənin artması ilə

yanaşı bu mühitdə təhlükəsizlik məsələləri də əsas istiqamətlərdən birinə çevrilmişdir.

Bu sistemdə informasiya sistemlərinin təhlükəsizliyi üçün tədbirlər müxtəlif səviyyələrdə aparılmalıdır. Hökumət öz fəaliyyətində şəffaf olmalı və lazım olduğu təqdirdə qanunvericiliyi təqdim etməlidir. Kibercinayətkarların arzuolunmaz fəaliyyətini dayandırmaq və aradan qaldırmaq üçün kifayət qədər güclü qanunvericilik aktları mövcud olmalıdır. Bu işdə həm hökumət həm də hər bir şəxs öhdəsinə düşən məsuliyyəti yerinə yetirməlidir. Belə ki, şəbəkə xidmətləri təminatçıları (İSS), iri müəssisələr və kiçik istifadəçilər/ev istifadəçiləri kimi digər maraqlı tərəflər də ölkənin kiberməkanının təhlükəsizliyini artırmaq üçün öz öhdələrinə düşən vəzifəni yerinə yetirməlidirlər. Bu mərhələdə və gələcəkdə rəqəmsal irəliləyişlər və e-dövlət ətrafında təhlükəsiz mühitin yaradılması məqsədilə daha geniş tədqiqatlar aparılmalıdır.

Ədəbiyyat

[1] D. Kumar , Dr. N. Panchanatham, “A case study on Cyber Security in E-Governance”, International Research Journal of Engineering and Technology, 2015,Vol.2, No.8, pp.272-275.

[2] L. Kumari, R. Kumar, “Impact of Cyber Security in different application of e-Governance: Case Study”, Proceedings of the 4th International Conference on System Modeling & Advancement in Research Trends, 2015, pp. 365-374.

[3] J. L.Bayuk, J. Healey, P. Rohmeyer, M. Hsachs, J. Schmidt, J. Weies, “Cyber security policy guidebook first edition”, 2012.

[4] A.Conklin, G. B. White, “e-Government and Cyber Security: The Role of Cyber Security Exercises”, Proceedings of the 39th Hawaii International Conference on System Sciences, 2006, pp.1-8.

[5] Y.N. İmamverdiyev, “E-dövlətin informasiya təhlükəsizliyi təhdidlərinin konsensus ranqlaşdirilmasi metodu”, İnformasiya texnologiyaları problemləri, 2018, №2, s.34–45.

[6] L. Carter, F. Belanger, “The utilization of egovernment services: citizen trust, innovation and acceptance factors”, Journal of Information Systems, 2005, Vol.15, No.1, pp. 5-25.

[7] Sh. M. Shareef, “Enhancing Security of Information in E-Government”, Journal of Emerging Trends in Computing and Information Sciences, 2016,Vol. 7, No. 3, pp. 139-144.

[8] R. M. Alguliyev, R.M. Aliguliyev, G. Y. Niftaliyeva, “Filtration of Terrorism-Related Texts in the E-Government Environment”, International Journal of Cyber Warfare and Terrorism, 2018,Vol. 8, No.4, pp.35-48.

[9] D. Kumar, N. Panchanatham, “Strategies for Rebooting the Government in e-Mode”, Global Journal for Research Analysis, 2014,Vol. 3, No. 8, pp.129-130.

ABOUT CYBER ATTACKS TO E-GOVERNMENT AND STRUGGLE AGAINST THEM

Gunay Iskenderli
Institute of Information Technology of ANAS,
Baku, Azerbaijan

Abstract -- E-government is the result of efforts by the government to improve relations with its citizens. To protect the e-government from existing threats in cybercrime, there is a need for best practices in information security. Security policies, practices and procedures, furthermore the use of security technology, can help to protect the e-government systems from attack, and detect non-standard services. Taking into account, the information about cyber-security and major cyber-attacks on e-government is given in this article.

Keywords -- e-government; information security, cyber attacks.