Əlizadə C.Ş., Əliyev B.Ə.♦

DOI: 10.25108/2304-1730-1749.iolr.2018.56.21-28

Kompüter şəbəkəsində fiziki əhəmiyyətli məlumatların aşkarlanması, təsbit edilməsi və əldə olunması

Xülasə: Qloballaşma dövründə insanları ən çox narahat edən məsələlərdən biri və birincisi təhlükəsizlik və onun təminatı məsələsidir. Artıq qeyd etmək olar ki, kibertəhlükəsizlik dövlətin, cəmiyyətin bütün səviyyələrinə təsir edən strateji milli məsələyə çevrilir.

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, Internet 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.

Kompüter şəbəkələrinin genişlənməsi kibermünaqişələrdə şəbəkə texnologiyalarının imkanlarından daha geniş istifadə etməyə, şəbəkə istifadəçilərinin fəaliyyətlərində koordinasiyanın, əhatəliliyin və mürəkkəbliyin artmasına şərait yaradır. Bu isə kibercinayətlərin çoxalmasına, onların daha təcrübəli və müasir İKT vasitələri ilə təmin olunmuş istifadəçilər tərəfindən aparılmasına səbəb olur.

Yuxarıdakılara əsaslanaraq deyə bilərik ki,kibercinayətkarlığın müəyyən edilməsi vacib məsələdir. Bu məsələ ilə bağlı milli siyasət və bu siyasət

♦**Əlizadə Cavid Şirzad oğlu** - AMEA-nın Hüquq və İnsan Haqları İnstitutunun "Dövlət təhlükəsizliyinin hüquqi təminatı" şöbəsinin elmi işçisi (Azərbaycan).E-mail: cavid6455@mail.ru
Əliyev Bəxtiyar Əbdürəhman oğlu - h.ü.f.d.,dosent, AMEA-nın Hüquq və İnsan Haqları İnstitutunun "Dövlət təhlükəsizliyinin hüquqi təminatı" şöbəsinin müdiri (Azərbaycan). E-mail: antiterror-baku@mail.ru

çərçivəsində hazırlanmış bir kibertəhlükəsizlik strategiyası tələb olunur. Kiber hücumların, ümumiyyətlə mala və ehtimal daxilində də olsa cana təsir edən nəticələri ola biləcək olduğundan kiber təhlükəsizliyin təmin edilməsində bu nəticələrin və bu nəticələrə gətirib çıxaran hərəkət və üsulların cinayət olaraq təyin olunması və cəzalandırılması böyük əhəmiyyət kəsb edir.

Açar sözlər: kompüter cinayətkarlığı; məlumatların aşkarlanması; istintaq.

Kompüter cinayətlərini araşdırarkən ilk növbədə, kompüterlərin ümumi sayını, habelə istifadə olunan server və iş stansiyalarının sayını və növünü müəyyənləşdirmək lazımdır. Əlavə olaraq istifadə edilən şəbəkə sistemini və kompüter şəbəkəsində istifadə olunan tətbiq proqramının tərkibini tapmaq vacibdir. Həmçinin ehtiyat nüsxələrinin mövcudluğu və saxlanılma yeri müəyyən edilməlidir. Ünsiyyət üçün kommunikasiya vasitələrinin istifadəsinin qurulmasına xüsusi diqqət yetirilməlidir. Eyni zamanda, məlumatların qorunması və İnternetə çıxış imkanları müəyyənləşdirilməlidir [2].

İnformasiya təhlükəsizliyini təmin etmək üçün aşağıdakılar zəruridir:

- müəssisədə elektrik kəsintisinin qarşısını almaq, kommutatorun qorunmasını təmin etmək;
- təşkilatın işçilərinin və digər şəxslərin kompüter qurğularından istifadəsinə qadağa qoymaq;
- istintaq hərəkətinin bütün iştirakçılarını kompüterdə mövcud olan informasiya və ya məlumatlardan şəxsi mənafeləri üçün istifadə etməsinin yolverilməzliyi barədə xəbərdar etmək.

Hadisə yerinə baxış zamanı kompüter şəbəkəsinin mövcudluğunu və serverləri tapmaq lazımdır. Server üçün girişin məhdud olan mərkəzi server otağı təyin olunur. Lakin, mərkəzi server otağından əlavə digər məkanlarda yerli lokal serverlər mövcuddur. Kompüter şəbəkəsinə qoşulan kompüterlərin yerini kabellər vasitəsilə xaricdən müəyyənləşdirmək mümkündür. Kompüter şəbəkəsindən

cinayətlə əlaqədar əhəmiyyətli məlumatların əldə olunması ilə bağlı iki istiqamət mövcuddur:

- inzibati bina və ya binalar qrupu daxilində yerləşən yerli şəbəkədən (LAN) məlumatların toplanması;

- inzibati rayon və ya bir şəhər ərazisində yerləşən yerli şəbəkədən məlumat toplamaq (müəssisə və filial şəbəkəsindən) [4].

Hər iki halda, istintaq qrupu şəbəkənin yerləşdiyi bütün kompüterləri eyni vaxtda baxış və ya axtarış etməlidir. Bu növ istintaq hərəkətlərini həyata keçirərkən qabaqcadan hazırlıq işləri görülür. Silinmiş mənbəyə daxil olmaq istənilən kompüterdə olan informasiyaya zərər verə bilər. Bu vəziyyət kompüterə axtarış və baxış zamanı effektivliyi azaldır. Həmçinin, kompüter şəbəkələrinin həcmi həmişə geniş miqyaslı istintaq hərəkətləri aparmaq üçün lazımi sayda işçi və şahidlərin səfərbər edilməsinə imkan vermir. Bu baxımdan lokal şəbəkəyə həbs qoyulur. Bu hərəkətlər prossesual qaydalara uyğun olaraq həyata keçirilən tədbirlərə nəzarət etmək üçün kompüter vasitələrinə baxış və nəzarəti gücləndirə bilər.Yalnız bu halda araşdırılan cinayət araşdırılaraq tam, obyektiv, hərtərəfli tədqiqat aparılır.Təbii ki, bu kimi vəziyyətlərdə kompüter cinayətinin həbs müddəti yoxa çıxmış informasiyanın həcmindən və ölçüsündən asılıdır. Hətta törədilmiş qısa, minimal həbs cəzasının verilməsi əməliyyat axtarış qrupunu şəraitə uyğunlaşdırmağa, kompüterdə mövcud informasiyanın yoxaçıxma həcmini qiymətləndirməyə imkan verir. Kompüter şəbəkəsinin sökülməsi, istintaq və ya ekspert orqanlarına çatdırılması baha başa gəlir və vaxt aparan prosesdir [3].

Beləliklə, yerli kompüter şəbəkəsində saxlanılan informasiya ehtiyatlarının vəziyyətində minimum dəyişiklik təmin etmək, habelə kompüter məlumatlarının icazəsiz şəkildə dəyişdirilməsinin qarşısını almaq olar. Qeyd edək ki, yerli kompüter şəbəkələrinə həbs qoyulması praktiki olaraq artıq bir çox ölkələrdə (Hollandiya, Belçika, ABŞ və s.) mövcuddur. Bu ölkələrdə icazə verilən kompüter şəbəkələrində həbslərin tətbiq edilməsi kompüter şəbəkəsinin və məlumat

daşıyıcılarının keyfiyyətsiz idarə olunmasından, qəsdən və təsadüfən silinən və ya asanlıqla silinə bilən mühüm məlumatları qorumağa imkanverir [5].

Hal-hazırda Azərbaycanın kompüter infrastrukturlarına asılılığı artmaqdadır. Bu günə qədər kompüter sistemlərinə zərər vermiş hücumlar, hakerlərin dünya səviyyəsində computer viruslarından ibarət olsa da, kiber fəzada mövcud təhdidlər gələcəkdə genişlənə və narahatverici səviyyəyə çata bilər. Çünki texnologiya sistemlərinin təhlükəsizliyini qorumaq çətin məsələdir. Azərbaycanın rəsmi və qeyri-rəsmi texnologiya infrastrukturları daha təhlükəsiz hala gətirilməzsə bu gələcəkdə böyük fəsadlar yarada bilər.

Biblioqrafiya

1. Gorman, Sean P. (2006). A Cyber Threat to National Security? (Edited By: Philip E. Auerswald, Lewis M. Branscomb, Todd M. La Porte, and Erwann O. Michel-Kerjan). Seeds of Disaster, Roots of Response. Cambridge: Cambridge University Press, s. 239-257.

2. Wall D. S. The Transformation of Crime in the Information Age, 2007, Wiley, 2007.

3. Батурин Ю.М. Проблемы компьютерного права. - М.: Юрид. лит., 1991.

4. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. - М.: Право и Закон, 1996. Крылов В.В. Информационные компьютерные преступления. - М.: Юринфор, 1997.

5. Яковлев А.Н. Теоретические и методические основы экспертного исследования документов на машинных магнитных носителях информации. Дис. ... канд. юрид. наук. Саратов, 2000.