Vacib infrastruktur sistemlərinin informasiya təhlükəsizliyinin xüsusiyyətləri

Havar Məmmədov[1], Zəfər Cəfərov[2], Rauf Həsənov[3]

Azərbaycan Texniki Universiteti

[2]c.zafar@mail.ru, [3]raufha@aztu.edu.az

***Xülasə*— Hazırki dövrdə vacib infrastruktur sistemlərində informasiya təhlükəsizliyi daha aktuallaşır. Məqalədə bu cür sistemlərinin təhlükəsizliyinin təmin olunmasının digər informasiya sistemlərindən fərqli cəhətləri araşdırılır və təhlükəsizlik modeli təklif olunur.**

Açar sözlər*— *informasiya təhlükəsizliyi; informasiya infrastukturu; vacib infrastruktur; kibertəhlükəsizlik; sənaye sistemləri.

I. GİRİŞ

Uzun illər sənaye təhlükəsizliyi informasiya təhdidlərinə (xüsusən də icazəsiz müdaxilələrə) diqqət ayrılmadan yalnız texnoloji şəbəkənin imtinaya davamlığı ilə təmin olunmuş və hesab edilidi ki, korporativ informasiya sistemləri istifadə şəbəkə ilə əlaqələndirilmir, İnternet kimi ümumxidmət şəbəkələrinə qoşulmur və texnoloji proseslərə kənardan müdaxilə ehtimalı demək olar ki, yoxdur. Müasir şəraitdə isə sənayenin bütün sahələri üzrə qabaqcıl informasiya-kommunikasiya texnologiyaları bazasında mövcud olan idarəetmə sistemləri geniş tətbiq olunur və vacib infrastruktur sistemlərinin avtomatlaşdırma və intellektullaşdırma dərəcəsi sürətlə artır.

Vacib infrastruktur dedikdə, cəmiyyət və milli sahələr üçün əhəmiyyətli obyektləri idarə edən sistemlər başa düşülür və hücumların və ya kompüter şəbəkələrinin iflic olunması nəticəsində milli təhlükəsizliyə təhdidlər yaranır. Fəaliyyətinin dayandırılması və ya qəzaya uğraması iqtisadiyyat, müdafiə, beynəlxalq münasibətlər və ölkənin digər təsərrüffat sahələri və obyektləri, eləcədə müvafiq ərazidə məskunlaşmış əhalinin həyatı üçün fövqaladə hallara və ya zərərli nəticələrə gətirib çıxardıqda və milli təhlükəsizlik üçün əhəmiyyət kəsb edən infrastruktur həyati vacib (əhəmiyyətli) hesab olunur [1].

Həyati vacib obyektlərin fəaliyyəti üzrə informasiya-idarəetmə sistemləri vacib informasiya infrastrukturlarını təsvir edir. İnformasiya infrastrukturlarına hücumlar fövqalədə hal yaradır və idarəetmə funksiyaları pozularaq zərərli nəticələrə səbəb olur. Bu anlayışlara görə infrastrukturun həyati vaciblik əlaməti ekoloji cəhətdən təhlükə və ya sosial yönümlü texnoloji proseslər daşımasıdır.

Vacib infrastruktur (sənaye) sistemlərinin fərqli cəhəti idarə etdikləri proseslərin həyat fəaliyyəti və təhlükəsizlik səviyyələri ilə bilavasitə əlaqəli olmasıdır. Bu sistemlərdən cəmiyyət və dövlətin asılılığı durmadan artır və onların informasiya təhlükəsizliyi məsələləri aktuallıq kəsb edir və vacib informasiya infrastruktur sistemlərinə nəzarət ön plana çıxır. Sənaye sistemləri təyinatlarına, istismar şərtlərinə, informasiya emalı xüsusiyyətlərinə, funsional tələblərə və s. digər əlamətlərə görə fərqlənirlər. Ona görə də bu cür sistemlərin informasiya təhlükəsizliyinin təmin olunması fərqli yanaşma tələb edir. Bu yanaşmanı müəyyənləşdirmək üçün problemlərin ciddiliyini qiymətləndirmək, zəifliklərin və təhdidlərin spesifikasını təhlil etmək və nəticədə vacib infrastrukturların informasiya təhlükəsizliyinin təmini üzrə xüsusi rejim bərqəqar etmək tələb ounur.

II. VACİB İNFRASTRUKTUR SİSTEMLƏRİ ÜZRƏ TƏHLÜKƏSİZLİK SAHƏLƏRİ

Vacib infrastrukturlara adətən telekommunikasiya, energetika, nəqliyyat, bank və maliyyə, su sistemləri, qəza xidmətləri və s. aid edilir. Bu cür infrastrukturları idarə edən sənaye sistemlərinin əsas tərkib hissələrindən biri informasiya sahəsidir. Bu sahə informasiyanı, informasiya infrastrukturunu, informasiya münasibət subyektlərini və onların tənzimlənməsi sistemini özündə ehtiva edir. Informasiya münasibətlərinin tənzimlənməsi üzrə bilavasitə kibernetik (idarəetmə) sistemin mövcudluğu tələb olunur və informasiya sahəsi daxilində kiber sahə yaranır. Bu sahə xüsusi növ idarəetmə informasiyası, subyekt (idaəedici hissə), infrastruktur (rabitə kanalları və informasiya emalı vasitələri) və idarəetmə prosesinin reallaşdırılması üçün alqoritmlərdən ibarətdir. Kiber və informasiya sahələri vəhdət təşkil etsə də, onlara qarşı təhdidləri fərqləndirən elementlər mövcuddur və sənaye sistemlərinin informasiya təhlükəsizliyinin təmin olunması zamanı bu xüsusiyyətlərin nəzərə alınması vacibdir [2].

İnformasiya təhlükəsizliyi təhdidlərin reallaşdırılması mümkün olmayan mühafizə vəziyyətinin təmin olunmasına istiqamətlənmiş fəaliyyət olduğu halda, kibernetik təhlükəsizlik idarəetmə sahəsi üzrə pozuntu hallarına yol verilməməsinin təmin edilməsidir.

İnformasiya təhlükəsizliyi, məzmunu aid olduğu obyekt və ya sistemlərin xüsusiyyətlərinin təsirinə nəzərə çarpaq dərəcədə məruz qalmadan və asanlıqla yayıla bilən kateqoriya hesab edilir. Bu fəaliyyət milli və ya ayrıca götürülmüş təşkilat, korporasiya səviyyəsində informasiya sahəsi üzrə təhlükəsizliyin təmin olunmasından ibarətdir. Informasiya sahəsi üzrə təhlükəsizliyin təmin olunması üçün səkkiz əsas mühafizə problemi həlli olunmalıdır: 1) Əlyetərliyin idarə olunması; 2) İstifadəçinin tanınması (authentication); 3) İstifadəçi səlahiyyətlərinin tanınması (authorization); 4) Məlumatın konfidensiallığının təmin olunması; 5)

Müəlliflikdən imtinanın mümkünsüzlüyü (ing. non-repudiability); 6) Məlumatın tamlığı; 7) Səbəblərin və yayınmaların aşkarlanması üçün müntəzəm nəzarət; 8) Üçüncü tərəfin mühafizəsi (başqasına ziyan vurulmaması) prinsipinin gözlənilməsi [3].

Müxtəlif idarəetmə növləri üzrə fərqli tələblər qoyulduğu üçün kibernetik təhlükəsizliyinin təmin olunması idarəetmə sistemi və proseslərinin xüsusiyyətlərindən asılıdır. Kiber təhlükəsizliyin təmin olunmasının mahiyyəti idarəetmə sistemi üzrə tələblər, onun təyinatı, idarəetmə obyektinin spesifikliyi, xarici mühitin, idarəetmə subyekti və vasitələrinin tərkibi və parametrlərindən, habelə idarəetmə qaydaları və protokollarından asılı olaraq fərqlənə bilər.

III. VACİB İNFRASTRUKTUR SİSTEMLƏRİ ÜZRƏ TƏHLÜKƏSİZLİK TƏHDİDLƏRİ

Sənaye sistemləri IBM standartlarına uyğun komputerlər, müasir əməliyyat sistemləri, TCP/IP protokolları, Web-brauzerləri, İnternet texnologiyaları və s. istifadə edən qabaqcıl aparat və proqram vasitələrinə qədər inkişaf etmişdir. Sadalanan açıq standartların və texnologiyaların geniş tətbiqi, korporativ və texnoloji şəbəkə seqmentləri arasında qarşılıqlı əlaqələrin artması sayəsində bu sistemlərə qarşı kiber təhdidlərin sayı çoxalmaqdadır. Kiber-təhdid – idarəetmə informasiyası, subyektləri, infrastrukturu və qaydalarına təhlükə törədən akt, hadisə, şərait, amil hesab olunur. Təhlükə ondan ibarətdir ki, göstərilən elementlərdən bir və ya bir neçəsinin korlanması idarəetmənin pozulmasına səbəb ola bilər. Hazırda sənaye və digər vacib infrastrukturlar üzrə avtomatlaşdırılmış idarəetmə sistemlərini sıradan çıxara bilən zərərli proqramların xüsusi nümunələri mövcuddur.

"Təhlükə agenti" kimi çıxış etməklərindən asılı olaraq sənaye sistemlərinə qəsdən törədilə bilən potensial təhdidləri aşağıdakı qruplara bölmək olar [4]:

Zərərli proqramlar. Sənayə sistemləri digər İT - sistemləri kimi məlum potensial kompüter (virusları, parazit, trojan, spyware və s.) prqoqramalrının təhdidlərinə məruz qala bilir.

İnsident (müdaxilə). Təcrübə göstərir ki, sistem ilə daxildən ətraflı tanış olan narazı əməkdaşlar, potensial təhlükə mənbələridir. Bu müdaxilə müəllifləri proqram və ya avadanlıqları qəsdən zədələyə bilər. Xidmət edən inzibatçı və mühəndislər də təsadüfən sistemin fəaliyyətinə zərər vurar və ya tənzim parametrlərinin və ya təhlükəsizlik qaydalarının pozulmasına səbəb olan müəyyən bir səhvlərə yol verə bilər.

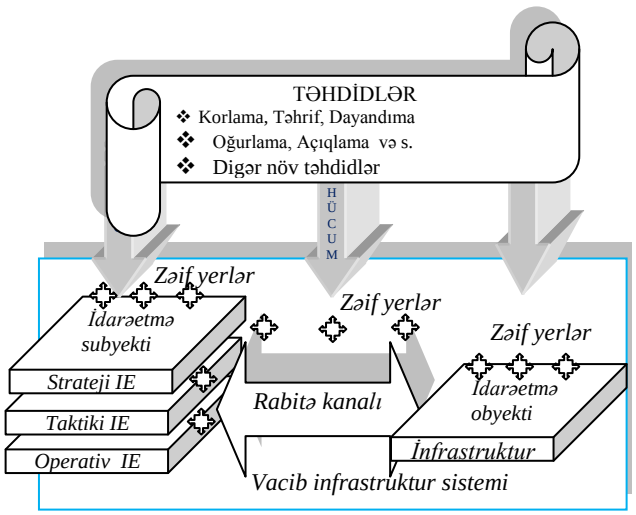
Hakerlər. Kənar şəxslər sistemə daxil olmaq və sistem üzərində nəzarət etmək, trafik monitorinqinin və xidmətdən imtina hücumlarının həyata keçirilməsində maraqlı ola bilər.

Terrorçular. Bu, vacib infrastrukturları idarə edən və adi IT sistemləri ilə arasında əsas fərqlər yaradan, ən ciddi təhlükədir. Terrorçular sənaye sistemini sıradan çıxarmaq, idarərəetmə və monitorinq proseslərini pozmaq, sistemə nəzarət etmək və bu infrastruktura mümkün qədər daha iri miqyasla zərər vurmaqda maraqlıdırlar.

Fərqli haldır ki, kibercinayətkarlıq üçün iki əsas həvəsləndirici amil vacib sənaye sahələri üzrə informasiya sistemlərində istifadə edilmir. Bunlar bir çox kompüter cinayətlərinin əsas məqsədini təşkil edən kredit kartları və elektron hesab-fakturasının əldə edilməsinə aid olan iqtisadi stimulları və sənaye casusluğu üzrə kommersiya sirləridir.

Kiber hucum idarəetmə sahəsi üzrə pozuntulara yönəlmiş fəaliyyət növüdür. Müxtəlif elmi-tədqiqat institutlarının statistikalarına görə vacib infrastrukturları idarə edən sənaye sistemlərinə qarşı kiberterrorizm istisna olunmaqla bütün növ kiberhucumlar üzrə kütləvi təhlükəsizlik hadisələri qeydə alınmışdır. Bu statistikaların təhlilinin nəticələrinə görə sənaye sistemlərinə ildə 100-dən artıq belə hucumlar təşkil olunur və onların müntəzəm artım dinamikası müşahidə edilməkdədir [5]. Vacib infrastruktura malik müəssisə və təşkilatlar kiberhucumların qarşısını almaqda öz hazırlıqlarına güvənmirlər.

Kiber hücumların səmərəli təşkili üçün sistemin daxili quruluşu mükəmməl öyrənilir. Bu hücumların ən əsas hədəfləri, ilk növbədə, vacib obyektləri idarə edən mühüm informasiya infrastruktur sistemləridir (şəkil 1). Belə obyektlərin texniki sıradan çıxarılması xaos və fəlakətlərlə nəticələnə bilər.

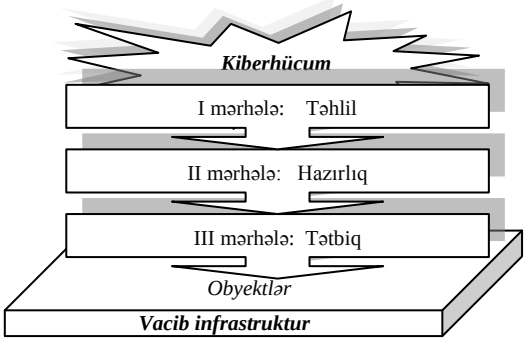


Şəkil 1. Təhdid modeli

Insan həyatına və sağlamlığına zərər, kütləvi qırğın və digər fəlakətlər törətməsə də, kiber hücumların ciddi nəticələri ola bilər. Məsələn, xüsusi planlaşdırılmış kütləvi kiber hücumlar əhalinin sıx məskunlaşdığı ərazilərdə telekommunikasiya və ya energetika sisteminin fəalliyyətini sıradan çıxara bilər.

Təhlil göstərir ki, vacib infrastrukturları idarə edən sənaye sistemlərinə elektron müdaxilə yolu ilə ciddi təhlükəsizlik, o cümlədən fiziki təhdidləri yaratmaq və sistem üzərində nəzarəti ələ keçirmək çox çətin hadisə hesab olunsa da nəzəri cəhətdən mümkündür. Məhz buna görə kiberhücum bir neçə mərhələdən təşkil olunur (şəkil 2). Başlanğıcda, kəşfiyyat mərhələsində obyektin daxili quruluşu, istifadə olunan avadanlıqlar və proqram təminatı haqqında geniş məlumat toplanır. İkinci mərhələdə isə toplanan məlumat diqqətlə təhlil edilir, zəif yerlər müəyyənləşdirilir və ən effektli hücum vektoru seçilib, hazırlanır. Nəhayət, üçüncü mərhələdə sadə sosial mühəndislikdən tutmuş yüksək texnologiyalara qədər müxtəlif

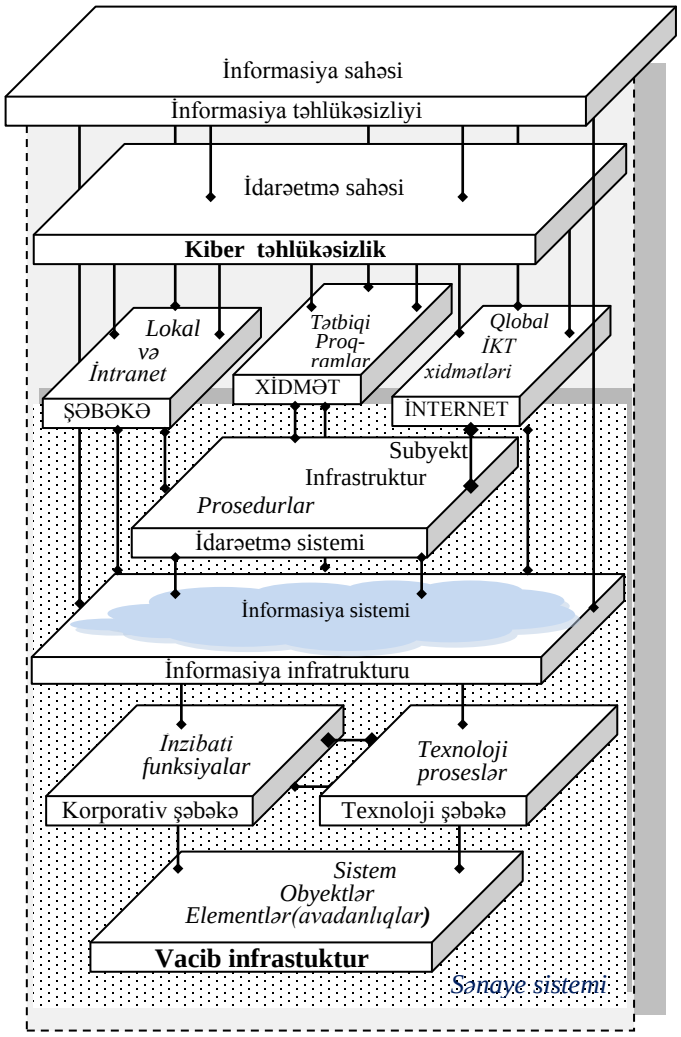
metodlardan istifadə etməklə zərərli proqramın obyektdə yerləşdirilməsi – tətbiqi problemi həll olunur.



Şəkil 2. Kiber hücum mərhələləri

IV. VACİB İNFRASTRUKTUR SİSTEMLƏRİNİN İNFORMASİYA MÜHAFİZƏ MODELİ

Vacib infrastuktur sistemlərinin təhlükəsizliyi informasiya təhlükəsizliyinin tərkib hissəsi olaraq *Tətbiqi* (xidmət), *Şəbəkə*, *İnternet* təhlükəsizlikləri ilə inteqrasiya edir. (şək.3).



Şəkil 3. Vacib infrastruktur sisteminin təhlükəsizlyinin konseptual modeli

Tətbiqi (xidmət) təhlükəsizlik infrastukturun fəaliyyətində iştirak edən informasiya-proqram resurslarına və proseslərinə görə müəyyən olunur. Şəbəkə təhlükəsizliyi müəssisədaxili, müəssisələrarası, müəssisə və istifadəçilər arasında əlaqənin layihələndirilməsi və təşkili ilə əlaqəlidir. İnternet təhlükəsizliyi bu şəbəkənin xidmətlərini və qlobal informasiya-kommunikasiya sistem və şəbəkələrlə əlaqələri əhatə edir.

Fərz edək ki, sistem üzrə $\Omega = \{\Omega_i\}$ $(i = \overline{1,n})$ informasiya təhlükəsizliyi atributları çoxluğudur. Onda, kiber təhlükəsizlik atributları

$$K = \{K_j\} \ (j = \overline{1,m};\ 1 \le m \le n)$$

bu çoxluğun altçoxluğu olacaqdır: $K \subseteq \Omega$.

Şəbəkə, Tətbiqi (xidmət), İnternet təhlükəsizliyi atributları domenlərini uyğun olaraq

$$N = \{N_j\},\ T = \{T_j\},\ A = \{A_j\}$$

ilə işarə edək. Nəzərə alsaq ki, kiber-təhlükəsizlik bu üç təhlükəsizlik növü ilə relyasion münasibət təşkil edir, onda

$$K \subseteq TxAxN \subseteq \Omega$$

Bu model vacib infrastruktur sistemlərinin informasiya təhlükəsizliyi üzrə mümkün təhdidləri və onlarin əlaqələrini təhlil etməyə imkan verir.

NƏTİCƏ

Beləliklə, qeyd olunan mülahizələr vacib infrastuktur sistemlərinin informasiya təhlükəsizliyinin təmin olunmasına yeni yanaşmalar tələb edir. Klassik təhlükəsizlik tədbirləri ilə yanaşı, vacib infrastruktur sistemlərinin mühafizəsinə, tərkib hissələrindəki mümkün boşluqların aşkarlanmasına və aradan qaldırılmasına ciddi diqqət ayrılmasını tələb edir.

ƏDƏBİYYAT

[1] А. Астахов, “Реалии и мифы кибертерроризма,” Открытые системы № 5, 2003.

[2] A. Hildick-Smith, “Security for Critical Infrastructure SCADA Systems,” GSEC Practical Assignment, Version 1.4c, Option 1, 2009.

[3] B. Gellman, “Cyber-attacks by Al Qaeda feared,” Washington Post, 27 June 2012Ş

[4] Digital Bond Inc., “Control Center Protection Profile for Industrial Control Systems.” Version 0.50, Draft, 17 Feb 2011.

[5] “The National Strategy To Secure Cyberspace,” Feb 2013.