UOT 004.056 DOI: 10.25045/jpit.v10.i1.05

İmamverdiyev Y.N.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
yadigar@lan.ab.az

E-DÖVLƏTİN İNFORMASİYA TƏHLÜKƏSİZLİYİ ÜZRƏ KOORDİNASİYA SİSTEMİNİN ÇOXMEYARLI QİYMƏTLƏNDİRİLMƏSİ MODELİ

E-dövlətin informasiya təhlükəsizliyinin təmin edilməsində iştirak edən aktorların (dövlət təşkilatları, özəl sektor, ictimai təşkilatlar və vətəndaşlar) fəaliyyətinin effektiv koordinasiyası aktorlar arasında vaxtında və keyfiyyətli informasiya mübadiləsindən birbaşa asılıdır. Buna görə müvafiq informasiya axınlarının topoloji strukturunu əsas götürməklə və onun analizini aparmaqla koordinasiya sisteminin reinjinerinqini həyata keçirmək və onun iş effektivliyini yüksəltmək mümkündür. Bu məqsədlə təqdim olunan məqalədə e-dövlətin informasiya təhlükəsizliyi üzrə koordinasiya sistemini modelləşdirmək üçün sistem iyerarxik dördsəviyyəli struktura dekompozisiya edilir və onun multi-agent şəbəkə modeli qurulur. Baxılan koordinasiya sisteminin operativliyinin və effektivliyinin qiymətləndirilməsi üçün bu şəbəkə modeli əsasında koordinasiya sisteminin iyerarxiklik indeksi, inersiya dərəcəsi və bir sıra digər indekslər təklif edilir.

***Açar sözlər**: e-dövlət, informasiya təhlükəsizliyi, koordinasiya, iyerarxik struktur, inersiya dərəcəsi, koordinasiya dərəcəsi, sosial şəbəkə analizi.*

Giriş

E-dövlətin informasiya təhlükəsizliyinin təmin edilməsində koordinasiya olduqca mühüm rol oynayır və bu sahədə koordinasiya məsələləri olduqca çeşidli və müxtəlif xarakterlidir [1]. E-dövlətin informasiya təhlükəsizliyi sahəsində koordinasiya məsələləri milli informasiya təhlükəsizliyi strategiyasının işlənməsi, kiber-hücumların qarşısının alınması, informasiya təhlükəsizliyi insidentlərinin analizi (təhqiqatı), müvafiq normativ hüquqi aktların işlənməsi, informasiya təhlükəsizliyi üzrə birgə tədbirlərin və təşəbbüslərin vahid mərkəzdən idarə edilməsi, kapitaltutumlu informasiya təhlükəsizliyi sistemlərindən kollektiv istifadənin təşkili, informasiya təhlükəsizliyi sahəsində elmi-tədqiqat işlərinin koordinasiyası və prioritetlərin müəyyən edilməsi və s. məsələləri əhatə edir.

Dövlət informasiya təhlükəsizliyi sahəsində səyləri birləşdirmək üçün müxtəlif koordinasiya mexanizmləri tətbiq edir, bu istiqamətdə müxtəlif tədbirlər həyata keçirir, dövlət, özəl və ictimai sektorlar üçün kibertəhlükəsizlik üzrə koordinasiya mərkəzləri yaradır [2]. Bu mərkəzlərin vəzifəsi infrastruktur obyektlərinin, e-xidmətlərin, intellektual mülkiyyətin, fərdi məlumatların kiberhücumlardan müdafiəsi üçün göstərilən səylərin konsolidasiyasıdır. İnformasiya təhlükəsizliyi üzrə koordinasiya sisteminin təkmilləşdirilməsi üzrə təkliflər işləmək üçün koordinasiyanın mövcud səviyyəsini qiymətləndirmək vacibdir.

Lakin koordinasiyanın mövcud səviyyəsini və effektivliyini qiymətləndirmək olduqca çətin məsələdir. Bu məqalədə koordinasiya sisteminin qiymətləndirilməsi üçün informasiya yanaşması əsas götürülür. İnformasiya koordinasiya üçün əsas resursdur, bütün koordinasiya sisteminin effektivliyi onun keyfiyyətindən, həqiqiliyindən, vaxtında olmasından asılıdır. Məsələn, analizlər göstərmişdi ki, 2005-ci ildə ABŞ-da baş vermiş Katrina qasırğası zamanı dövlət orqanları arasında meydana çıxan koordinasiya problemləri əsasən informasiya mübadiləsi problemlərindən qaynaqlanmışdı [3]. T.Malone və K.Crowston koordinasiya anlayışına "bir neçə aktor bir aktorun təklikdə əldə edə bilməyəcəyi bir məqsədə nail olmağa çalışdıqda, informasiyanın yerinə yetirilən əlavə emalı" kimi tərif verirlər [4]. Təbii fəlakətlərlə mübarizə sistemlərində koordinasiyanın həyata keçirilməsində informasiyanın rolu [5]-də analiz edilir və vaxtında olan əlaqədar informasiyanın koordinasiyaya və fövqəladə halların aradan qaldırılmasının effektivliyinə birbaşa təsir etdiyi müəyyən edilir.

Fövqəladə halların digər növləri ilə müqayisədə informasiya təhlükəsizliyi insidentlərinin

qarşısının alınması, aşkarlanması və nəticələrinin aradan qaldırılması zamanı informasiyanın rolu daha qabarıqdır. Burada informasiya əsas resurs kimi çıxış edir, informasiyanın mübadiləsi və koordinasiyası bütün işlərin həyata keçirilməsi və qərar qəbulu üçün əsas təşkil edir. Buna görə informasiya təhlükəsizliyi üzrə koordinasiya sisteminin təkmilləşdirilməsinə onun bütün elementlərini birləşdirən və hərəkətə gətirən komponentindən – informasiya axınlarının optimallaşdırılmasından başlamaq ən məqsədəuyğun yanaşma olardı. Bu məqsədlə bu işdə e-dövlətin informasiya təhlükəsizliyi sistemində koordinasiya səviyyəsini xarakterizə etmək üçün qraflar nəzəriyyəsi [6] və sosial şəbəkə analizi [7, 8] əsasında bir sıra metrikalar təklif edilir.

Əlaqədar işlərin icmalı

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsində əsas problemlərdən biri dövlət orqanları arasında effektiv koordinasiyanın təmin edilməsidir. Lakin informasiyanın olmaması şəraitində effektiv koordinasiya mümkün deyil. İnformasiyanın olmaması təşkilatlar arasında koordinasiyanın səmərəliliyini məhdudlaşdırır, çünki koordinasiya fəaliyyət planları yalnız əldə olan informasiya əsasında qurulur. Ona görə də müvafiq təşkilatlar arasında informasiya mübadiləsi infrastrukturunu təkmilləşdirmək üçün ciddi səylər göstərilir. Təşkilat modeli əsasında idarələrarası koordinasiya modelinə [9]-da baxılır. Milli miqyaslı kiber-hücumlar zamanı dövlət orqanlarının fəaliyyətinin koordinasiyası üçün müvafiq potensialın yaradılması da aktual problemlərdən biridir [10].

İnformasiyanı sürətlə mübadilə etmək və hərəkətləri koordinasiya etmək qabiliyyəti kiberhücumların qarşısının alınması, onların aşkarlanması və nəticələrinin aradan qaldırılması üçün ən vacib funksiyadır. Hazırda kiberhücumların aşkarlanmasının bir çox məsələləri təşkilat çərçivəsində həll edilir və təşkilatlararası informasiya mübadiləsi azdır. Lakin informasiya mübadiləsi genişmiqyaslı kiber-hücum situasiyalarını dərindən başa düşmək yolunda həlledici addımdır və gələcək şəbəkələrin müdafiəsində əsas konsepsiyalardan biridir. Dövlət orqanları arasında qarşılıqlı əlaqə reqlamentlərinin standartlaşdırılması, formal informasiya paylaşımının müəyyən edilməsi və qeyri-formal informasiya paylaşımının təşviq edilməsi də aktual problemlərdəndir [11].

Gizli kiberhücumların və yeni zərərli proqramların aşkarlanması, erkən xəbərdarlıqların və təhlükəsizliyin təmin edilməsi üzrə məsləhətlərin verilməsi, təhlükələr barədə məlumatların selektiv çatdırılması – informasiya mübadiləsinin bir çox istifadə variantlarından yalnız bəzilərıdir. [12] icmal məqaləsində kibertəhlükəsizlik sahəsində informasiya paylaşımı aspektləri analiz edilir. İnformasiya mübadiləsi sistemlərinə daha detallı tələblərin işlənməsi, təşkilati və texnoloji məsələlər, hüquqi aspektlər və standartlaşdırma istiqamətləri vurğulanır. Bununla əlaqədar, kompüter insidentlərini cavablandırma komandalarının (*ing. Computer Emergency Response Team, CERT*) strukturu, insidenti cavablandırma prosesləri, protokolları və alətləri qiymətləndirilir, informasiya mübadiləsi üzrə effektiv platformaların yaradılması üzrə bir sıra fikirlər irəli sürülür.

Kapucu N. və həmmüəllifləri [13]-də fövqəladə hadisələrin (11 sentyabr 2001-ci il terror hücumu) cavablandırılması zamanı təşkilatlarası şəbəkəyə baxır, dövlət, özəl və ictimai təşkilatlar arasında formalaşan qarşılıqlı əlaqələri analiz edirlər. Tədqiqatda dinamik şəbəkə nəzəriyyəsi və mürəkkəb adaptiv sistemlər nəzəriyyəsindən alınmış nəzəri metodlar istifadə edilir. Cavablandırma sistemində iştirak edən əsas təşkilatların müəyyən edilməsi üçün təşkilati analiz metodları tətbiq edilir. Tədqiqatın nəticələrinə görə, effektiv cavab və bərpa bütün səviyyələrdə dövlət orqanları arasında, dövlət və özəl sektorlar arasında yaxşı əlaqələndirilmiş təşkilati şəbəkələr və inam tələb edir.

Abbasi A. və həmmüəllifləri tərəfindən bir neçə təşkilatın iştirak etdiyi cavablandırma əməliyyatlarında koordinasiyanın təkmilləşdirilməsi yollarına baxılır [14]. Bu məqsədlə formalaşmış cavablandırma şəbəkəsində iştirakçıların rolu və şəbəkədə zaman dinamikası analiz edilir. Fövqəladə hadisənin cavablandırılması zamanı şəxslərarası koordinasiya əməliyyatları analiz edilərək dörd zaman periodu ərzində şəbəkənin evolyusiyasına baxılır. Nəticələr göstərir ki,

informasiya mübadiləsi üçün tələb edilən böyük həcmdə kommunikasiya səbəbindən zaman keçdikcə, şəbəkə daha da mərkəzləşməmiş olur.

[15]-də sosial şəbəkə nəzəriyyəsi böyük miqyaslı fövqəladə əməliyyatlar zamanı insidenti idarəetmə məntəqəsindən keçən informasiya axınlarını öyrənmək üçün istifadə olunur. Verilənlər hesabatlardan, mediadan və insident, yanğın və təcili yardım komandalarının rəhbərləri ilə müsahibələrdən toplanmışdı. Aparılmış analizlər göstərmişdi ki, hər bir xilasetmə xidmətində baş verən əsas daxili məlumatlar komandirlər arasında güclü əlaqələr vasitəsilə insidentləri idarəetmə nöqtəsində əlaqələndirilmiş və koordinasiya edilirmişdir. Əhəmiyyətli və yeni məlumatlar komandirlərə periferik aktorlardan zəif və qeyri-rəsmi əlaqələr vasitəsilə də çatdırılmışdır.

Uhr C. tərəfindən dissertasiya işində çox sayda təşkilatın iştirak etdiyi fövqəladə halların cavablandırılması proseslərində iştirak edən fiziki şəxslər və onların qarşılıqlı əlaqələri haqqında məlumatların toplanması və analizi metodları işlənmişdir [16]. Bu metodlar sosial şəbəkə analizinə əsaslanır və cəmiyyətin müxtəlif seqmentlərindən müxtəlif resursların cəlb edildiyi fövqəladə halların emalı problemlərini tədqiq etməyə, empirik analizlər aparmağa imkan verir. Koordinasiya əmsalı ilə aktorun mərkəziliyi arasında korrelyasiyanın olması (Spirmen əmsalı vasitəsilə) məsələsinə baxılır.

Koordinasiyanın effektivliyi xarakteristikaları ilə sosial şəbəkə analizindən götürülmüş kəmiyyətlərin əlaqəsi məsələsi bir sıra digər tədqiqatlarda da araşdırılmışdır. Sosial şəbəkədə aktorun əlaqələrini xarakterizə edən, geniş istifadə edilən metrika mərkəzilikdir. Mərkəzilik ilə layihələr üzrə işlərin koordinasiyasının keyfiyyəti arasındakı korrelyasiya əlaqəsinin aydınlaşdırılması məsələsi tədqiqatçıları çox cəlb edir. Dərəcə üzrə mərkəziliyi böyük olan aktorların daha keyfiyyətli koordinasiya nümayiş etdirməsi [17]-də qeyd edilir. Proqram təminatının işlənməsi layihələrində [18], tikinti layihələrində [19, 20] mərkəzilik ölçüsü ilə koordinasiyanın keyfiyyəti arasındakı əlaqə öz təcrübi təsdiqini tapır.

[21]-də əlaqəlilik ölçüsü ilə koordinasiyanın keyfiyyəti arasındakı korrelyasiya müəyyən edilir. Fövqəladə halların aradan qaldırılmasına cəlb olunmuş aktorlar şəbəkəsində əlaqəlilik ölçüsü böyük olduqca, fövqəladə hallar zamanı informasiyanın keyfiyyəti və əlyetərliyi artır. Əlaqənin gücü agentlər arasındakı münasibətlərin keyfiyyətini müəyyən etmək üçün vacib atributdur.

Münasibətin keyfiyyəti fövqəladə hallar zamanı xüsusilə əhəmiyyətlidir və informasiya mübadiləsinin tezliyi ilə birbaşa əlaqəlidir [22]. [22]-də nəqliyyat qovşaqları, məktəblər, parklar, idman qurğuları kimi yumşaq hədəf təşkilatlarında koordinasiyaya hazırlıq səviyyəsi tədqiq edilir və şəbəkə əlaqələrinin gücü ilə koordinasiya keyfiyyətinin effektivliyi arasında korrelyasiyanın olması müəyyən edilir. Əlaqənin gücü ilə koordinasiyanın korrelyasiyasının analizi göstərir ki, münasibətin keyfiyyətinin artması informasiyanın keyfiyyəti və əlyetərliyi, həmçinin fövqəladə hallara ümumi hazırlıq səviyyəsi kimi koordinasiya atributlarını yaxşılaşdırır.

[23]-də xəstəlik epidemiyaları zamanı yuxarıdakı hər üç sosial şəbəkə xarakteristikası – mərkəzilik, əlaqələrin gücü və əlaqəlilik ölçüləri ilə koordinasiya keyfiyyəti arasında korrelyasiyanın olması müəyyən edilir. Qeyd edək ki, dərəcə mərkəziliyi, əlaqənin gücü və əlaqəlilik bir-birindən asılı olmayan dəyişənlərdir (onlar arasında korrelyasiya yoxdur).

Koordinasiya sisteminin multiagent şəbəkə modeli

Bu bölmədə koordinasiya sisteminin strukturuna makrosəviyyədə – ümumdövlət səviyyəsində baxılır və informasiya təhlükəsizliyi üzrə milli koordinasiya sisteminin multiagent şəbəkəsi şəklində modeli təklif edilir. Məlum olduğu kimi, koordinasiya formal və qeyri-formal formalarda həyata keçirilə bilər. Formal koordinasiya zamanı qarşılıqlı əlaqə prosesini tənzimləyən qaydaların sonlu çoxluğu verilir. Qeyri-formal koordinasiya etimad, qarşılıqlı fayda və münasibətlər əsasında meydana çıxır. Bu işdə formal koordinasiyaya baxılır.

Fərz olunur ki, e-dövlətin informasiya təhlükəsizliyi sistemi ayrı-ayrı informasiya təhlükəsizliyi domenlərindən (İTD-lərdən) ibarətdir və bu domenlər biznes proseslərinin təhlükəsiz korporativ mühitdə yerinə yetirilməsi üçün müvafiq informasiya təhlükəsizliyi

servisləri göstərirlər. Bu domenlərin fəaliyyəti və onlarda həyata keçirilən müvafiq informasiya təhlükəsizliyi tədbirləri mütləq koordinasiya edilməlidir. Bu işdə e-dövlətin informasiya təhlükəsizliyinin idarə edilməsi üzrə koordinasiya strukturunu dörd idarəetmə səviyyəsinə dekompozisiya etmək təklif olunur:

- ümumdövlət (eyni vaxtda iki və ya daha artıq İTD-ini əhatə edən informasiya təhlükəsizliyi tədbirləri – İTD-lər, xarici ölkələrin və beynəlxalq təşkilatların müvafiq qurumları arasında koordinasiya həyata keçirilir);
- korporativ (bir İTD ilə məhdudlaşan informasiya təhlükəsizliyi tədbirləri – İTD-nin əhatə etdiyi təşkilati strukturlar arasında koordinasiya tələb edilir);
- lokal (nəticələri bir servis (sistem) çərçivəsindən kənara çıxan informasiya təhlükəsizliyi tədbirləri – İTD bölmələrinin fəaliyyəti koordinasiya edilir);
- obyekt (nəticələri bir servis (sistem) çərçivəsində məhdudlaşan informasiya təhlükəsizliyi tədbirləri – obyektin istismarına məsul xidməti personal arasında koordinasiya tələb edilir).

Burada "informasiya təhlükəsizliyi tədbirləri" anlayışı geniş spektrdə tədbirləri nəzərdə tutur, xüsusi halda, məsələn, kiberhücumların aşkarlanması və nəticələrinin aradan qaldırılması tədbirləri nəzərdə tutula bilər. Qeyd etmək lazımdır ki, dördsəviyyəli dekompozisiya ideyası [24]-ün təsiri ilə formalaşmışdır.

Tutaq ki, e-dövlətin informasiya təhlükəsizliyini idarəetmə sistemi n sayda İTD-dən ibarətdir. Obyektlər çoxluğunu

$$A = \{A_{ij}\}$$

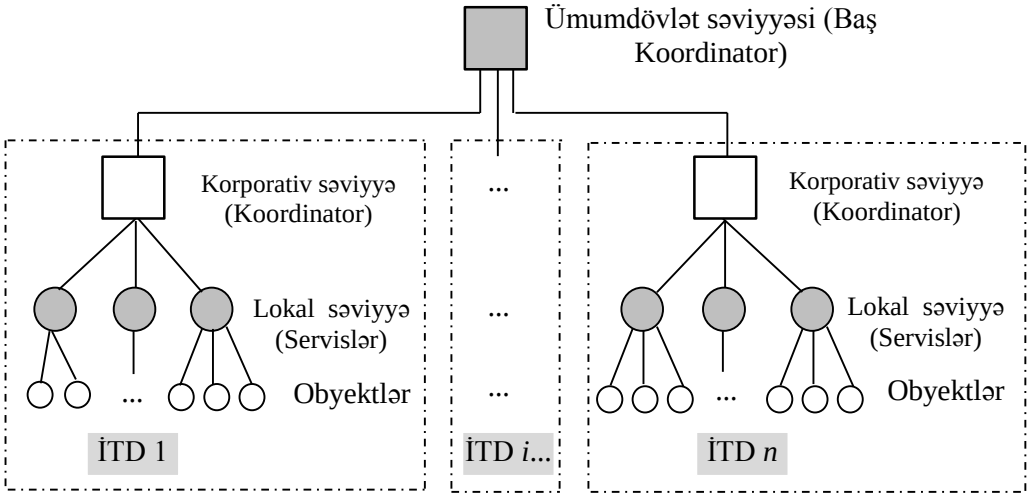
kimi verək, burada i – informasiya təhlükəsizliyi domeninin indeksidir, i-ci domendə m_i obyekt (servis, sistem) var, j – i-ci domenin konkret idarəetmə obyektinin indeksidir, $j \in [1, \dots, m_i]$.

Koordinasiya sistemi çərçivəsində istənilən səviyyənin idarə edilməsi insan – qərar qəbuledən şəxs (QQŞ) tərəfindən reallaşdırılır. QQŞ məqsədəuyğun şəkildə (məqsəd qoymaq, məsələləri müəyyən etmək, onların həlli üçün vasitə və resursları seçmək yolu ilə) qərar qəbul edilməsini həyata keçirir. Buna görə A çoxluğunun hər bir A_{ij} obyektini onun modeli ilə – agentlə əvəzləmək olar. Agent digər agentlərə nəzərən avtonom və asinxron hərəkət edir. Agentlərdən hər biri öz domeninə daxil olan digər agentlərlə qarşılıqlı təsirdə olur və fəaliyyət prosesində həm xarici mühiti (digər agentlər də baxılan agentə görə xarici mühit hesab olunur), həm də öz davranışını dəyişə bilər. Fərz olunur ki, hər bir domendə bir Koordinator təyin edilmişdir və onların vəzifəsi domendaxili və domenlərarası qarşılıqlı (informasiya) əlaqəsini həyata keçirməkdir. Hər hansı agent digər domenin agentləri ilə əlaqə saxlamaq üçün öz domeninin Koordinatoruna müraciət edir.

Hər bir domenin informasiya təhlükəsizliyi sahəsində öz maraqları var və domen Koordinatoru domenin maraqlarından çıxış edir. Bu maraqlar ümumi sistemin maraqları ilə uzlaşmaya bilər. Buna görə, maraqların uzlaşmasını və fəaliyyətin koordinasiyasını təmin etmək üçün e-dövlətin informasiya təhlükəsizliyi sistemində Baş Koordinator (BK) nəzərdə tutulur. BK ümumdövlət səviyyəsində fəaliyyət göstərir, domenlərin fəaliyyətini tənzimləyir və bu fəaliyyətin zamana görə paylanmasına (yəni planlaşdırmaya) görə cavabdehdir.

BK-nın əsas vəzifəsi dövlət orqanlarının informasiya təhlükəsizliyi üzrə öz missiyalarını yerinə yetirməsi üçün zəruri olan informasiyaya giriş əldə edə bilmələrini təmin etməkdir. O, bu vəzifəni aşağıdakı sahələrdə həyata keçirir – inteqrasiya, əməkdaşlıq və koordinasiya, situasiyadan məlumatlılıq, informasiya təhlükəsizliyi insidentlərinə reaksiya, analiz və hesabatlılıq, biliklərin idarə edilməsi, yeni texnologiyalar və idarəetmə.

Beləliklə, BK, domen koordinatorları və agentlər çoxluğu iyerarxik koordinasiya sisteminin modelini – multiagent şəbəkəsini əmələ gətirir (şəkil 1).



Şəkil 1. Koordinasiya sisteminin dördsəviyyəli strukturu

Məlumdur ki, müxtəlif şəbəkələrin ən sadə və əlverişli riyazi təsviri qraflar vasitəsilə əldə edilir. Tutaq ki, e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin koordinasiyası sistemində *n* agent iştirak edir və agentlərin qarşılıqlı əlaqələri qrafla göstərilir. Qrafın təpələri olaraq koordinasiya sistemində iştirak edən agentlər (sosial şəbəkə analizi termini ilə aktorlar), tilləri isə onlar arasındakı qarşılıqlı əlaqələrdir. Fərz edək ki, koordinasiya şəbəkəsinin əlaqələr qrafı agentlərin $A = \|a_{ij}\|$ insidentlik matrisi ilə təsvir olunur, onun elementləri məlum qaydada müəyyən olunur:

$$a_{ij} = \begin{cases} 1 - i \text{ və } j \text{ agentləri til ilə birləşir,} \\ 0 - \text{əks halda.} \end{cases} \quad (1)$$

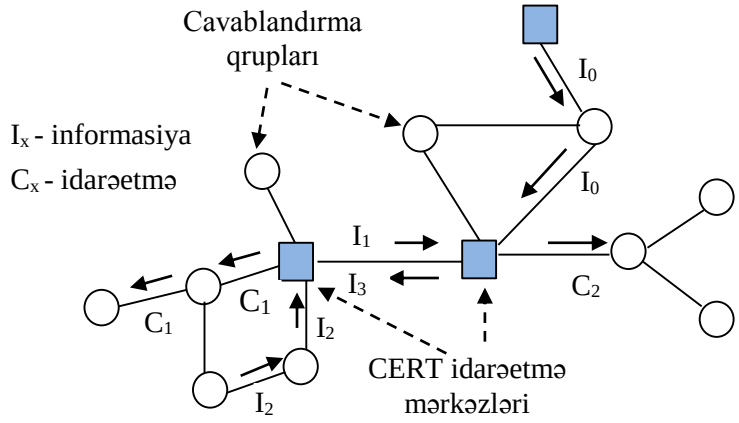
Topoloji struktur qarşılıqlı əlaqə və ya tabeçilik dərəcəsini əks etdirir, koordinasiya funksiyaları və informasiya axınları haqqında heç bir məlumat daşımır. Lakin topoloji strukturu əsas götürməklə və onun analizini aparmaqla koordinasiya sisteminin reinjinerinqini həyata keçirmək və onun iş effektivliyini yüksəltmək mümkündür.

Koordinasiya şəbəkəsinə aid misal

Bir və ya bir neçə İTD-yə daxil olan müxtəlif struktur bölmələri arasında koordinasiya məsələsi informasiya təhlükəsizliyi insidentlərinin emalı zamanı tez-tez meydana çıxır. İnformasiya təhlükəsizliyi insidentlərinin qarşısının alınması, vaxtında aşkarlanması və qısa müddətdə nəticələrin aradan qaldırılması üçün geniş yayılmış yanaşmalardan biri CERT-in təşkil olunmasıdır [25]. Hazırda müxtəlif ölkələrdə çox sayda CERT komandaları fəaliyyət göstərir. CERT komandaları akademik, dövlət, hərbi, milli, kritik infrastruktur, kommersiya, daxili, kiçik və orta biznes, ticarət kimi sektorlarda tətbiq edilir [26].

İnformasiya təhlükəsizliyi insidentlərini yayıldıqları sistemlərin miqyasından asılı olaraq adi insidentlərə, orta miqyaslı insidentlərə, böyük miqyaslı insidentlərə və kritik insidentlərə klassifikasiya etmək olar. Adi insidentlərə nəticələri bir sistem çərçivəsində məhdudlaşan insidentləri aid etmək olar. Orta miqyaslı insident dedikdə, təsiri bir təhlükəsizlik domeni ilə məhdudlaşan insidentlər nəzərdə tutulur. Böyük miqyaslı insidentlərə eyni vaxtda iki və ya daha artıq təhlükəsizlik domeninə yönəlmiş insidentlər aid edilir (bu domenlərdən bəziləri xarici ölkələrdə ola bilər). Kritik informasiya təhlükəsizliyi insidentləri iqtisadiyyata, kritik infrastruktura, dövlətin fəaliyyətinə və milli təhlükəsizliyə təsir göstərə bilər. Təbiətlərinə görə, bu insidentlər çox zaman bir deyil, bir neçə təşkilata təsir edir.

İnsidentlərin miqyasından asılı olaraq onların cavablandırılması lokal, milli və beynəlxalq səviyyədə koordinasiya tələb edir. Printerin sıradan çıxması kimi insidentlər, yəqin ki, cavablandırma üçün lokal administrator və istifadəçinin koordinasiyasını tələb edəcək. Kiçik və orta miqyaslı insidentlərdən fərqli olaraq, böyük miqyaslı və katastrofik insidentlər təşkilatlar arasında sıx əməkdaşlıq, milli və beynəlxalq səviyyədə koordinasiya tələb edir. Belə insidentlərin cavablandırılması prosesində milli CERT əsas koordinator (BK) kimi çıxış edir.



Şəkil 2. CERT-komandaların hipotetik şəbəkəsində informasiya axını

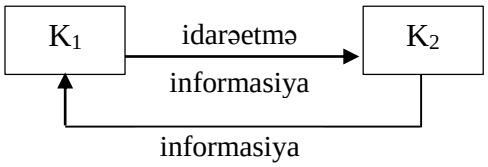
İnformasiya təhlükəsizliyi üzrə koordinasiya şəbəkəsi mürəkkəbləşdikcə, səlahiyyətli şəxslərin real zamanda informasiyaya girişini və qərar qəbul edilməsini təmin etmək üçün CERT-in xüsusi idarəetmə mərkəzlərinin yaradılması ehtiyacı meydana çıxır. Belə mərkəzlər dispetçer mərkəzi, situasiya mərkəzi, monitorinq mərkəzi, əməliyyat mərkəzi və s. kimi fəaliyyət göstərirlər.

CERT-in idarəetmə mərkəzi insidentlərin cavablandırılması şəbəkəsində informasiyanın yayılması və qərar qəbulu prosesində koordinasiya mərkəzi (Koordinator) rolunu oynayır. Şəkil 2-də koordinasiya şəbəkəsinin üzvləri arasında ikiistiqamətli rejimdə müxtəlif növ informasiya axınları (məsələn, xəbərdarlıq siqnalı, vəziyyət barədə hesabatlar, idarəetmə komandaları və s.) göstərilir. İnformasiya axını insidentin cavablandırılması proseslərinin gedişini obyektiv əks etdirən məlumatlar toplusudur, koordinasiyanın həyata keçirilməsi üçün kommunikasiya kanalları ilə ötürülür. Axınlar düz (idarə edən sistemdən idarə edilən sistemə) və əks (idarə edilən sistemdən idarə edən sistemə) ola bilər.

İnsidentin yeri, sinfi, ciddiliyi və s. haqqında informasiya cavablandırma vahidlərindən CERT idarəetmə mərkəzlərinə daxil olur. CERT idarəetmə mərkəzlərindən isə insidentin emalı prosedurları, tədbirlər, komandalar və s. kimi informasiya cavablandırma vahidlərinə doğru hərəkət edir. İstənilən insident cavablandırma şəbəkəsində informasiyanın ötürülməsi marşrutu və müddəti qərar qəbulu prosesinə əhəmiyyətli təsir edir və cavablandırma vahidinin və idarəetmə mərkəzinin şəbəkədəki yerindən (mövqeyindən) asılıdır.

Koordinasiya şəbəkəsinin iyerarxiya dərəcəsi

Koordinasiya şəbəkəsinin yuxarıda təklif edilmiş dördsəviyyəli struktukturu iyerarxik və mərkəzləşmişdir. İyerarxik struktur tabeçilik, yəni aktorlar arasında qeyri-bərabər əlaqələr olan struktura deyilir. Bu zaman bir istiqamətdəki təsir digər istiqamətdəki təsirdən daha əhəmiyyətli olur. "İnformasiya-idarəetmə" şəklində təsir vasitəsilə tipik iyerarxik əlaqəyə misal şəkil 3-də göstərilib. Aydındır ki, burada K_1 aktoru dominantlıq edir. Oxşar xarakterli əlaqələri CERT-komandaların şəkil 2-də göstərilmiş hipotetik şəbəkəsində də müşahidə etmək olar.

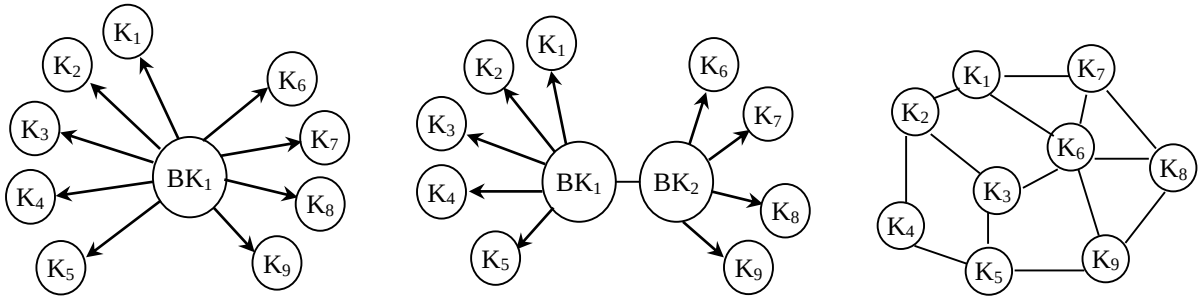


Şəkil 3. Tipik iyerarxik əlaqəyə misal

Qeyd edək ki, iyerarxiyanın daxil edilməsi sistemlərin yaradılmasını və işləməsini olduqca asanlaşdırır. Təbii sistemlərin mütləq əksəriyyətində bu və ya digər dərəcədə iyerarxiya müşahidə edilir. Lakin istənilən iyerarxiya sistemin imkanlarını, xüsusilə də çevikliyini (adaptivliyini) azaldır. Təşkilati strukturların bürokratikliyi inkişafa və dəyişikliklərə adekvat reaksiya proseslərini tormozlayır. Aşağı səviyyə elementlərinin təşəbbüslərini yuxarının dominantlığı ləğv edə bilir, aşağılar bu dominantlığa (idarəetməyə) yalnız qismən və bir qayda olaraq, gecikmə ilə təsir edə bilərlər.

İyerarxiyanın daxil edilməsinin mənfi nəticələrini agentlərə yuxarıdan ciddi tənzimləmə olmadan bir sıra təsirlərə müstəqil reaksiya göstərmək imkanı verməklə yumşaltmaq olar. Bu problemin həllərindən biri də Incident Command System (ICS) konsepsiyasıdır [27]. Bu konsepsiyanın əsasında təşkilatların yalnız stabil şəraitdə effektiv olan iyerarxik strukturlarından ətraf mühitin və əsas hədəflərin dəyişikliklərinə reaksiya dövrlərində daha çevik strukturlara keçilməsi ideyası dayanır.

Bu işdə iyerarxiyanın və mərkəzləşmənin mənfi təsirlərini azaltmaq üçün mərkəzləşmiş koordinasiya strukturundan (şəkil 4 A) demərkəzləşmiş (şəkil 4 B) və ya paylanmış (şəkil 4 C) struktura keçmək təklif edilir. Demərkəzləşmiş struktur bir neçə mərkəzləşmiş altşəbəkədən ibarətdir, altşəbəkələr bir-biri ilə mərkəzi qovşaqları ilə birləşir. Qeyd edək ki, hazırda Azərbaycan Respublikasında informasiya təhlükəsizliyi insidentlərinin cavablandırılması sahəsində koordinasiya strukturu demərkəzləşmişdir və şəkil 4 B-də göstərildiyi kimi iki koordinasiya mərkəzinə malikdir (şərti olaraq BK_1, dövlət təşkilatlarına, BK_2 isə özəl sektora, ictimai təşkilatlara və vətəndaşlara xidmət göstərir). Paylanmış şəbəkə infrastrukturunda (şəkil 4 C) mərkəzi qovşaq (BK) anlayışı yoxdur, bütün qovşaqlar eyniranqlıdır, koordinasiya Koordinatorlar arasında imzalanmış rəsmi razılaşmalar əsasında həyata keçirilir (şəkildə tillər belə razılaşmaların mövcudluğunu göstərir). Belə struktur koordinasiya mərkəzlərinin sıradan çıxmalarına qarşı olduqca dayanıqlıdır.



A) Mərkəzləşmiş B) Demərkəzləşmiş C) Paylanmış

Şəkil 4. Koordinasiya şəbəkələrinin müxtəlif növləri

Mərkəzləşmiş şəbəkədə hər hansı səbəbdən mərkəzi qovşaq sıradan çıxsa, bütün şəbəkə dağılar. Demərkəzləşmiş şəbəkədə bir altşəbəkənin mərkəzi qovşağının sıradan çıxması yalnız bu altşəbəkənin işini pozur, şəbəkənin qalan hissəsi isə öz fəaliyyətini davam etdirir. Paylanmış şəbəkədə isə hər hansı qovşaq sıradan çıxsa, bu yalnız onun özünə təsir edir, digər qovşaqlar qalan əlaqələrin hesabına əlyetər ola bilər. Paylanmış strukturun imtinalara dayanıqlığı olduqca yüksəkdir.

Koordinasiya şəbəkələrinin iyerarxiya səviyyəsini ölçmək üçün iyerarxiya dərəcəsi kəmiyyətindən

istifadə etmək olar. Şəbəkə iyerarxiyası aktorlar arasındakı münasibətlərin rəsmi səlahiyyət, status və ya prestij əsasında qurulduğu və idarə edildiyi şəbəkələrdə mövcuddur. Şəbəkə iyerarxiyası aktorlar cütü arasındakı birbaşa münasibətlərin (əlaqələrin) istiqamətinə baxır və biristiqamətli münasibətlərin nisbi sayını qiymətləndirir [28]. Biristiqamətli əlaqə (məsələn, tabeçilik) dedikdə, nəzərdə tutulur ki, məsələn, A-dan B-yə əlaqə var, lakin B-dən A-ya əlaqə yoxdur. Şəbəkənin iyerarxiya dərəcəsi aşağıdakı kimi müəyyən edilir. Tutaq ki, V birbaşa əlaqələri simmetrik olan aktor cütlərinin sayıdır. $maxV$ isə birbaşa əlaqəsi olan aktor cütlərinin maksimal sayıdır (A ilə B, yaxud B ilə A arasında birbaşa əlaqə var). Onda şəbəkənin iyerarxiya dərəcəsini

$$H = 1 - [V/maxV] \quad (2)$$

kimi hesablamaq olar.

Bu şəbəkə metrikasından koordinasiya sistemində iyerarxiya strukturunun varlığını yoxlamaq və iyerarxiya səviyyəsini ölçmək üçün istifadə etmək olar.

Koordinasiya sisteminin operativliyi metrikaları

Bu işdə koordinasiya sisteminin operativliyini xarakterizə etmək üçün sistemin inersiallıq dərəcəsindən istifadə edilməsi təklif edilir [29]. Ümumiyyətlə, sistemin inersiallıq dərəcəsi ($\Delta\tau$) sistemdə çıxış siqnalı (t_{out}) ilə giriş siqnalı (t_{in}) arasındakı gecikmə kimi müəyyən olunur ($\Delta\tau = t_{out} - t_{in}$). Sistemin inersiya dərəcəsi nə qədər böyükdürsə, sistem təsirlərə bir o qədər "tənbəl" reaksiya verir.

Tutaq ki, koordinasiya sistemini təsvir edən müəyyən qraf verilib və onun hər bir (i, j) tili üçün iki ədəd təyin edilib: (In_{ij}, Fb_{ij}). In_{ij} informasiyanın i-dən j-a ötürülməsi müddəti, Fb_{ij} isə bu informasiyaya j-dan i-yə reaksiya müddətidir. Hər hansı μ yolunun $K(\mu)$ inersiyası informasiyanın bu yol ilə toplam ötürmə müddəti $In(\mu) = \sum_{(i,j)\in\mu} In_{ij}$ ilə reaksiyanın toplam ötürmə müddəti $Fb(\mu) = \sum_{(i,j)\in\mu} Fb_{ij}$ arasındakı fərq kimi müəyyən edilir:

$$K(\mu) = In(\mu) - Fb(\mu). \quad (3)$$

Verilmiş koordinasiya strukturu üçün "inersiya diametri" anlayışını da daxil etmək olar. Qrafın diametri koordinasiya strukturunun kompaktlığını xarakterizə edir. Qrafın diametri $d(G)$ onun iki təpəsini birləşdirən ən qısa yolun maksimal uzunluğu kimi müəyyən edilir, yəni qrafın iki a və b təpəsi arasındakı maksimal məsafədir:

$$d(G) = \max_{a,b\in V(G)} d(a,b), \quad (4)$$

burada a və b qrafın ixtiyari iki təpəsidir, $V(G)$ – bütün təpələrin çoxluğudur, $d(a,b)$ – a və b təpələri arasındakı məsafədir. Bu məsələni həll etmək üçün Floyd-Uorşell alqoritmi [6] ilə qrafda bütün təpələr cütləri arasında ən qısa yolları tapmaq və onlardan maksimum olanı seçmək olar.

Diametr ən uzaqda yerləşən bölmədən informasiyanın idarəetmə qərarlarının qəbul edildiyi mərkəzə ötürülməsi və qəbul edilmiş idarəetmə qərarının ən uzaqda yerləşən digər bölməyə çatdırılması üçün zəruri olan marşrutun maksimal uzunluğunu müəyyən edir. Aydındır ki, diametrin kiçik olması informasiyanı daha tez qəbul edib ötürməyə imkan verir. Beləliklə, Qrafın diametri nə qədər kiçikdirsə, koordinasiya sisteminin arxitekturasının effektivliyi bir o qədər yüksək olar.

Reaksiya müddətinə direktiv tələblər irəli sürülə bilər. Əgər reaksiya direktiv müddətdə göstərilməsə, cərimə mexanizmi nəzərdə tutmaq olar. Cərimə mexanizmi nəzərə alınmaqla koordinasiyanın operativliyinin qiymətləndirilməsinə baxaq. Tutaq ki, qrafın hər bir (i,j) tili üçün iki çəki verilib: (Out_{ij}, T_{ij}). Burada Out_{ij} – yuxarıda olduğu kimi cari reaksiya müddəti, T_{ij} – direktiv reaksiya müddətidir. Verilmiş başlanğıc aktordan son aktora hər bir yol müəyyən informasiya prosesini təyin edir. Baxılan halda yolun uzunluğu onun tilləri üzrə reaksiya müddətlərinin cəmidir. Əgər baxılan prosesin müddəti əvvəlcədən verilmiş T_{ij} müddətindən fərqlidirsə, onda kənarlaşmaya mütənasib olan cərimə müəyyən edilir:

$$\chi_{ij} = \begin{cases} \alpha\left(T_{ij} - Out_{ij}\right), Out_{ij} \le T_{ij} \\ \beta\left(T_{ij} - Out_{ij}\right), T_{ij} \le Out_{ij} \end{cases} \quad (5)$$

burada α və β əmsalları həm müsbət, həm də mənfi ola bilər.

Gecikməyə görə cərimələr nəzərə alınmaqla koordinasiya sisteminin operativliyinin qiymətləndirilməsi məsələsini cəriməni minimallaşdıran yolların tapılması kimi qoymaq və onu həll etmək üçün Bellman-Ford alqoritmindən istifadə etmək olar [6]. Deykstra alqoritmindən fərqli olaraq, bu alqoritm çəkisi mənfi olan tillərlə də işləyir və qrafın bir təpəsindən digər bütün təpələrə olan ən qısa yolları tapır.

Koordinasiya sistemi üçün sosial şəbəkə metrikaları

Koordinasiya sistemini xarakterizə etmək üçün sosial şəbəkə analizinin anlayışlarını və qiymətləndirmə metodlarını tətbiq etmək olar [7, 8]. Sosial şəbəkə strukturlarının qiymətləndirilməsi metodlarına mərkəzi aktorların müəyyən edilməsi, aparıcı aktorların və şəbəkə elementlərini birləşdirən vasitəçilərin axtarışı, şəbəkə strukturlarının identifikasiyası və s. metodları daxildir [7, 8].

Şəbəkənin ilkin analizi, bir qayda olaraq, mərkəzi aktorların axtarışından ibarətdir. Aktorun vacibliyinin ölçüsü kimi istiqamətlənməmiş qraflarda mərkəzilik, istiqamətlənmiş qraflarda isə daxil olan əlaqələr üçün prestij, çıxan əlaqələr üçün ekspansivlik anlayışları istifadə edilir. Aktorlar üçün çox sayda mərkəzilik indeksləri təklif edilib: aktorun mərkəziliyi üçün dərəcə əsasında mərkəzilik, yaxınlıq əsasında mərkəzilik, vasitəçilik üzrə mərkəzilik, məxsusi vektorlar əsasında mərkəzilik və s. kəmiyyətlər istifadə edilir [7, 8].

Dərəcəyə görə mərkəzilik qovşaqdan çıxan və qovşağa daxil olan tillərin cəmi kimi hesablanır. Tilin varlığı informasiyanın ötürülməsini bildirir. Onda ən böyük mərkəziliyə malik aktorlar ən informasiyalı aktor hesab oluna bilər, nəticədə belə aktorlar informasiya axınlarına nəzarət etmək imkanına sahib ola bilərlər.

Dərəcə üzrə mərkəzilik (C^D) aktorun mərkəziliyinin ən sadə tərifidir. O ideyaya əsaslanır ki, şəbəkədə vacib aktorların digər aktorlarla əlaqələrinin sayı ən böyükdür. i aktorunun dərəcə mərkəziliyi belə müəyyən edilir:

$$C_i^D = \frac{\sum_{j=1}^{n} a_{ij}}{n-1} = \frac{k_i}{n-1}, \quad (6)$$

burada k_i i aktorunun dərəcəsidir, yəni ona qonşu olan aktorların sayıdır.

Əlaqəlilik əmsalı – sistemdə qarşılıqlı əlaqələrin sayı çox olduqda, kommunikasiyaların effektivliyinin artmasını əks etdirir. Kommunikasiya qrafı tam əlaqəli olduqda, bütün aktorlar arasında birbaşa əlaqə olur. Mümkün birbaşa əlaqələrin sayı $n(n-1)$ olduğu üçün əlaqəlilik əmsalını belə hesablamaq olar:

$$E_{conn} = exp\left\{-\left[1 - \frac{\sum_i \sum_j a_{ij}}{n(n-1)}\right]\right\} \quad (7)$$

İnformasiya təhlükəsizliyi sisteminin *koordinasiya potensialını* analiz etmək üçün informasiya kanallarının xüsusi sayı kriteriyasını tətbiq etmək olar. İnformasiya kanallarının xüsusi sayı

$$E_{cap} = exp(N/n) \quad (8)$$

kimi müəyyən edilir, burada N – tillərin sayı və n – təpələrin sayıdır. Bu kəmiyyət təşkilati strukturun idarəetmə potensialını xarakterizə edir. Koordinasiya kanallarının xüsusi sayı nə qədər çoxdursa, bir koordinatora düşən koordinasiya əlaqələrinin sayı da bir o qədər çoxdur və koordinasiya sistemi daha effektivdir.

Koordinasiya dərəcəsi – koordinasiya şəbəkəsində aktorların informasiya mübadiləsi qabiliyyətini ölçür. Bu kəmiyyəti modelləşdirmək üçün bir neçə yanaşma mövcuddur, ən sadə üsul

koordinasiya dərəcəsinin aktorlar arasındakı məsafədən və aktorlar arasındakı əlaqənin gücündən eksponensial asılı olmasını fərz etməkdir. Bu üsulda i və j agentləri arasındakı koordinasiya dərəcəsi

$$\gamma_{ij} = exp(-\xi_{ij} d_{ij}) \quad (9)$$

kimi müəyyən edilir, burada d_{ij} i və j agentləri arasındakı məsafədir, ξ_{ij} isə münasibətin gücünü ölçür.

Əlaqənin gücü agentlər arasındakı kommunikasiyanın tezliyi haqqında (gündə, həftədə, ayda, kvartalda, yarımildə, ildə, lazım gəldikdə) toplanmış məlumat əsasında Ridit metodu ilə müəyyən edilir [23].

i təpəsinin ümumi koordinasiya dərəcəsi bu təpənin yerdə qalan təpələrlə koordinasiya dərəcələrinin cəminə bərabərdir:

$$\Gamma_i = \sum_{j=1}^{n} \gamma_{ij} \quad (10)$$

burada *n* baxılan qrafda təpələrin sayıdır. Təpənin ümumi koordinasiya dərəcəsi bu təpənin mənsub olduğu şəbəkədən ala biləcəyi informasiyanın miqdarını ölçür.

Bütün koordinasiya şəbəkəsinin *orta koordinasiya dərəcəsini* də oxşar şəkildə müəyyən etmək olar:

$$\bar{\Gamma} = \frac{1}{n} \sum_{i=1}^{n} \Gamma_i \quad (11)$$

Bu orta qiyməti baxılan şəbəkənin effektivliyinin ölçüsü kimi interpretasiya etmək olar, çünki o, ayrıca bir aktorun şəbəkəyə nə qədər töhfə verdiyini ölçür.

Nəticə

E-dövlətin informasiya təhlükəsizliyinin təmin edilməsində koordinasiya əsas idarəetmə funksiyalarından biridir. E-dövlət inkişaf etdikcə, kəskinləşən informasiya təhlükəsizliyi mühitində koordinasiya məsələləri daha da mürəkkəbləşir və bütün sistemin etibarlı və təhlükəsiz fəaliyyəti üçün həyati vacib əhəmiyyət daşıyır. Müxtəlif maraqlar güdən aktorlar arasında effektiv koordinasiyada aparıcı rol koordinasiya prosesində iştirak edən aktorlar arasında keyfiyyətli informasiya kommunikasiyalarına məxsusdur. Bu işdə e-dövlətin informasiya təhlükəsizliyinin təmin edilməsi üzrə mərkəzləşmiş koordinasiya sistemi dörd səviyyəyə dekompozisiya edilmiş və sistemin multi-agent şəbəkə modeli qurulmuşdur. Sonra bu şəbəkə modelindən istifadə edilməklə e-dövlətin informasiya təhlükəsizliyi sahəsində təşkilatlararası koordinasiyanın operativliyinin və effektivliyinin qiymətləndirilməsi üçün qraflar nəzəriyyəsi və sosial şəbəkə analizi əsasında çoxmeyarlı yanaşma təklif edilmişdir. Təklif edilmiş kriteriyaların qraflar nəzəriyyəsindən gələn əsas üstünlükləri onların sadəliyi, minimum ilkin informasiya tələb etmələri və təsvirin əyaniliyidir. Gələcək tədqiqatlarda koordinasiya sistemi üçün şəbəkə qrafında hərəkətlə əlaqəli indikatorların (PageRank tipli) və hibrid indikatorların işlənməsi nəzərdə tutulur.

Ədəbiyyat

1. İmamverdiyev Y.N. E-dövlətin informasiya təhlükəsizliyi üzrə koordinasiya problemləri // İnformasiya cəmiyyəti problemləri, 2014, №2, s.24–30.
2. Tabansky L., Ben-Israel I. Cybersecurity in Israel. SpringerBriefs in Cybersecurity. Heidelberg: Springer Cham, 2015, 84 p.
3. Chua A., Kaynak S., Foo S. An analysis of the delayed response to hurricane Katrina through the lens of knowledge management // Journal of the American Society for Information Science and Technology, 2007, vol.58, no.3, pp.391–403.
4. Malone T., Crowston K. What is coordination theory and how can it help design cooperative work systems?. / Proceedings of the ACM conference on Computer-supported cooperative

work, 1990, pp.357–370.
5. Comfort L.K., Ko K., Zagorecki A. Coordination in rapidly evolving disaster response systems: the role of information // American Behavioral Scientist, 2004, vol.48, no.3, pp.295–313.
6. Омельченко А.В. Теория графов. М: МЦНМО, 2018, 416 с.
7. Wasserman S., and Faust K. Social network analysis: Methods and applications. Cambridge university press, 1994, 857 p.
8. Holder L. B., Cook D.J. Mining Graph Data. Wiley, 2007.
9. Hocevar S., Jansen E., Thomas G. Building collaborative capacity for homeland security. Monterey, California. Naval Postgraduate School, 2004.
10. Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative. United States Government Accountability Office. March 2010.
11. Adam N., Kozanoglu A., Paliwal A., Shafiq B. Secure Information Sharing in a Virtual Multi-Agency Team Environment // Electronic Notes in Theoretical Computer Science, 2007, vol.179, pp.97–109.
12. Skopik F., Settanni G., Fiedler R. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing // Computers & Security, 2016, vol 60, pp.154–176.
13. Kapucu N. Interorganizational coordination in dynamic context: Networks in emergency response management // Connections, 2005, vol.26, no.2, pp.33–48.
14. Abbasi A., Sadeghi-Niaraki A., Jalili M., & Choi S.M. Enhancing response coordination through the assessment of response network structural dynamics // PloS One, vol.13, no.2, e0191130.
15. Rimstad R., Njå O., Rake E., Braut G.S. Incident command and information flows in a large-scale emergency operation // Journal of Contingencies and Crisis Management, 2014, vol.22, no.1, pp.29–38.
16. Uhr C. Multi-organizational emergency response management – A framework for further development: Doctoral thesis. Lund University, 2009, 254 p.
17. Hossain L., Wu A., and Chung K. K. Actor centrality correlates to project based coordination / Proceedings of the 20th anniversary conference on Computer supported cooperative work, pp. 363–372.
18. Kiesling S., Klünder J., Fischer D., Schneider K., Fischbach K. Applying social network analysis and centrality measures to improve information flow analysis / International Conference on Product-Focused Software Process Improvement, 2016, pp.379–386.
19. Hossain L. Communications and coordination in construction projects // Construction Management and Economics, 2009, vol.27, no.1, pp.25–39.
20. Dogan S. Z., Arditi D., Gunhan S., Erbasaranoglu B. Assessing coordination performance based on centrality in an e-mail communication network // Journal of Management in Engineering, 2013, vol.31, no.3, 04014047. DOI: 10.1061/(ASCE)ME.1943-5479.0000255.
21. Hossain L., Kuti M. Disaster response preparedness coordination through social networks // Disasters, vol.34, no.3, pp.755–786.
22. Uddin M. S., Hossain L. Towards coordination preparedness of soft-target organisation / International Conference on Electronic Government, 2009, pp.54–64.
23. Bdeir F. Networks of inter-organisational coordination during disease outbreaks. PhD thesis. The University of Sydney, 2014, 350 p.
24. Ляшенко Е.Н., Шерстюк В.Г. Разработка модели координации сил и средств в иерархической системе гражданской защиты населения // Технологический аудит и резервы производства, 2015, т.4, №2, с.4–10.
25. Имамвердиев Я.Н. Создание CERT-команды для научной компьютерной сети

AzScienceNet // Проблемы информационного общества, 2011, №1, с.15–26.
26. Əliquliyev R. M., İmamverdiyev Y. N. İnformasiya təhlükəsizliyi insidentləri. Bakı: İnformasiya Texnologiyaları, 2012, 212 s.
27. Bigley G. The incident command system: high-reliability organizing for complex and volatile task environments // Academy of Management Journal, 2001, vol. 44, no.6, pp.1281–1299.
28. Krackhardt D. Graph theoretical dimensions of informal organizations // Computational organization theory, 1994, pp.89–111.
29. Richard J. P. Time-delay systems: an overview of some recent advances and open problems // Automatica, 2003, vol.39, no.10, pp.1667–1694.

УДК 004.056

Имамвердиев Ядигар Н.
Институт Информационных Технологий НАНА, Баку, Азербайджан
yadigar@lan.ab.az

Модель многокритериальной оценки системы координации по информационной безопасности электронного государства

Эффективная координация деятельности субъектов (государственных организаций, частного сектора, общественных организаций и граждан), участвующих в системе обеспечения информационной безопасности электронного государства, напрямую зависит от своевременного и качественного обмена информацией между этими субъектами. Поэтому построив топологическую структуру соответствующих информационных потоков и выполнив ее анализ, можно провести реинжиниринг и повысить эффективность системы координации. В этой статье система координации обеспечения информационной безопасности электронного государства разбита на иерархическую четырехуровневую структуру, и для нее построена многоагентная сетевая модель. Для оценки оперативности и эффективности рассматриваемой системы координации на основе этой сетевой модели предлагаются индекс иерархии, индекс инерции и ряд других показателей.

Ключевые слова: *электронное государство, информационная безопасность, координация, иерархическая структура, индекс инерции, степень координации, анализ социальных сетей.*

Yadigar N. Imamverdiyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
yadigar@lan.ab.az

A multi-criteria evaluation model for e-government information security coordination system

Effective coordination of the activities of actors (state organizations, private sector, public organizations and citizens), which are engaged in the system of ensuring the information security of the e-government, is of decisive importance. The effectiveness of coordination directly depends on the timely and qualitative exchange of information between these actors. Therefore, by building the topological structure of the corresponding information flows and analyzing them, reengineering can be implemented and the efficiency of the coordination system can be improved. To this end, in this paper, the coordination system is decomposed into a hierarchical four-level structure for modeling the e-government coordination system, and a multi-agent network model is built for it. To assess the efficiency and effectiveness of the coordination system under consideration, using this network model, the hierarchy index, inertia index, and a number of other indicators are proposed.

Keywords: *e-government, information security, coordination, hierarchical structure, inertia index, coordination degree, social network analysis*.