UOT 004.056

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

E-DÖVLƏTİN İNFORMASİYA TƏHLÜKƏSİZLİYİNİN İDARƏ EDİLMƏSİNİN KONSEPTUAL MODELİ

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi çətin formallaşdırılan mürəkkəb məsələdir. Belə məsələlərin həllində ilkin mərhələ kimi konseptual modelin qurulması çox faydalıdır. Bu işdə e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin konseptual modeli təklif edilir. Konseptual modeldə e-dövlətin informasiya təhlükəsizliyinin əsas anlayışları, e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin məqsədləri, predmeti, obyektləri, subyektləri, əsas idarəetmə funksiyaları, ətraf və daxili mühitin e-dövlətin informasiya təhlükəsizliyinə təsir edən əsas faktorları müəyyən edilir.

***Açar sözlər**: elektron dövlət, informasiya təhlükəsizliyi, informasiya təhlükəsizliyinin idarə edilməsi, konseptual model.*

Giriş

Hazırda informasiya təhlükəsizliyi problemləri həm vətəndaşlar, həm də təşkilatlar üçün aktualdır. İnformasiya təhlükəsizliyi dövlət idarəçiliyində də vacib prosesə çevrilir. İnformasiya təhlükəsizliyinin təmin edilməsi problemlərinə müasir baxışlar xeyli genişlənib və indi onun vacib aspektlərini texnoloji məsələlər deyil, daha çox idarəetmə (menecment) problemləri və müvafiq idarəetmə sisteminin keyfiyyəti məsələləri təşkil edir. Qloballaşma şəraitində təşkilatlar daha yaxşı rəqabət qabiliyyətini təmin etmək üçün informasiya təhlükəsizliyi infrastrukturunun bütün elementlərinin mərkəzləşdirilmiş idarə edilməsinə üstünlük verirlər. İnformasiya təhlükəsizliyinin idarə edilməsinə belə yanaşma idarəetmənin geniş yayılmaqda olan texnologiyası kimi e-dövlət üçün də təbii seçimdir [1, 2].

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi olduqca mürəkkəb məsələdir: idarəetmə obyekti hər biri məqsədyönlü fəaliyyət göstərən avtonom komponentlərdən ibarət mürəkkəb sosial-texniki sistemdir, burada bir-birinə əhəmiyyətli dərəcədə qarşılıqlı təsir göstərən bir çox proses (sosial, texnoloji, siyasi) baş verir. Proseslərin xarakteri zamana görə dəyişkəndir, proseslərin dinamikası haqqında kifayət qədər kəmiyyət informasiyası yoxdur, qeyri-müəyyənliyin müxtəlif növləri iştirak edir [2, 3].

Həyat fəaliyyətinin bütün mərhələlərində e-dövlət müxtəlif növ informasiya təhlükəsizliyi təhdidlərinə məruz qalır. Mümkün təhdidlərin siyahısı kifayət qədər böyükdür və e-dövlətin informasiya təhlükəsizliyinə təhdidlər landşaftında sürətlə kəmiyyət və keyfiyyət dəyişiklikləri baş verir. E-dövləti əhatə edən xarici mühit potensial "düşmən" mühitdir. E-dövlətin həm öz elementləri, həm də xarici mühit informasiya təhlükəsizliyinin pozulmasına yönəlmiş çoxsaylı təhdidlərin mənbəyidir.

Eyni zamanda, İKT-nin artan istifadəsi və artan funksional tələblər nəticəsində e-dövlət sistemləri bir-birinə qarışır. Hər biri daxili demarkasiya edilmiş məsuliyyət rejimləri ilə bu sistemlərin separasiyasını təmin etmək mümkün deyil. Nəticədə, e-dövlətin daxili və xarici mühitləri arasında fərq və sərhədlər itir.

Mürəkkəb sistemlərdə baş verən proseslərin tədqiqi üçün əsas alətlərdən biri konseptual (latınca *conceptus* – anlayış) modelləşdirmədir [4-6]. Konseptual modellərin əsasında mürəkkəb sistemlərin dayanıqlı idarə edilməsinin məqsədləri və vəzifələri konkretləşdirilir. Bu modellər sistemin dinamikası haqqında bilikləri inteqrasiya etməyə, əsas prosesləri identifikasiya etməyə, proseslərin vəziyyətləri və identifikatorları arasında əlaqələri göstərməyə, mürəkkəb qarşılıqlı əlaqələrdə koordinasiyanı sürətləndirməyə imkan verir. Yaxşı qurulmuş konseptual modellər idarəetmə funksiyaları və idarəetmənin effektivlik indikatorlarının seçimini əsaslandırmaq üçün

elmi platformanı təmin edir. Konseptual modelin əsasında müvafiq riyazi aparatdan istifadə etməklə layihələndirilən və istismar edilən sistemlərin iş qabiliyyətini və dayanıqlığını əhəmiyyətli xərclər çəkmədən qiymətləndirməyə imkan verən riyazi modellər qurula bilər [6].

Bu məqalədə e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin konseptual modeli işlənilir. Konseptual modeldə e-dövlətin informasiya təhlükəsizliyinin mahiyyəti, idarəetmənin məqsədləri, predmeti, obyektləri, subyektləri, prinsipləri, funksiyaları, ətraf və daxili mühitin e-dövlətin informasiya təhlükəsizliyinə təsir edən əsas faktorları, e-dövlətin tərkibinin və strukturunun xüsusiyyətləri, e-dövlətin informasiya təhlükəsizliyini idarəetmə sisteminin tərkibini və strukturunu müəyyən edən əsas faktorlar, idarəetmənin effektivliyini qiymətləndirmək üçün indikatorlar müəyyən edilir. Qeyd etmək lazımdır ki, təklif edilən model informasiya təhlükəsizliyinin hüquqi, siyasi, hərbi, sosial, iqtisadi və s. problemlərinin bütün aspektlərini əhatə etmir. Bu modelin əsas məqsədi – e-dövlətin fəaliyyətinin üsul və vasitələri çərçivəsində reallaşdırılan informasiya təhlükəsizliyi sisteminin əsas elementlərini aşkarlamaqdır.

Konseptual model anlayışı

Konseptual modelləşdirmə və konseptual modellər predmet sahəsinin modelləşdirilməsində ən vacib yanaşmalardan hesab edilir. Kanada alimləri A. Gemino və Y. Vanda görə, "konseptual modelləşdirmə anlama və kommunikasiya məqsədi ilə bizi əhatə edən fiziki və sosial dünyanın bəzi aspektlərinin formal təsvirindən ibarət fəaliyyətdir" [7]. Konseptual modelləşdirmə obyektin, prosesin və ya hadisənin müəyyən modelini yaratmağa imkan verir, onların xassələrini, xarakteristikalarını, proseslərin baş vermə ardıcıllığını öyrənməyi, onların analizini və proqnozlaşdırılmasını təmin edir. Konseptual model modelləşdirilən sistemin fəaliyyətinin məqsədləri, sistemin vəziyyəti və təsir üsulları (idarəetmə) haqqında təsəvvürlər sistemini əks etdirir. Konseptual modeldə modelləşdirilən sistemin strukturu və onun elementlərinin xassələri müəyyən edilir, elementlər arasında səbəb-nəticə əlaqələrini təyin edən münasibətlər təsvir edilir.

"Konseptual model" anlayışı modelləşdirilən sistemin formal təsvirini tələb edən bütün insan fəaliyyəti sahələrində istifadə edilir. "Konseptual model" anlayışını ingilis psixoloqu A.T.Velford 1961-ci ildə Tətbiqi psixologiya üzrə XIV Beynəlxalq konqresdə təklif etmişdir. Konseptual model operatorun beynində formalaşan qlobal obraz kimi açıqlanır. A.T.Velforda görə, konseptual model operatora tam mənzərəni verir və buna görə prosesin müxtəlif hissələrini tamla qarşılaşdırmaq imkanını və uyğun olaraq effektiv hərəkət etməyi təmin edir [8].

Hazırda "konseptual model" anlayışı müxtəlif elm və praktiki fəaliyyət sahələrində – psixologiya, psixolinqvistika, suni intellekt, proqram təminatının işlənməsi, dövlət standartı və s. müəyyən edilir və bu sahədə vahid yanaşma mövcud deyil [9-13]. Mühəndis psixologiyasında konseptual model əmək fəaliyyətinin məqsədləri və vəzifələri, əmək predmetinin – texniki sistemlərin və ətraf mühitin vəziyyəti, idarəetmə təsirlərinin üsulları haqqında operatorun təsəvvürlər toplusudur [14].

Süni intellekt sahəsində konseptual model dedikdə, "predmet sahəsinin, bu sahənin xassələri və xarakteristikaları ilə birlikdə təsviri üçün istifadə edilən qarşılıqlı əlaqəli anlayışlardan, bu anlayışların predmet sahəsində mövcud tiplər, situasiyalar, əlamətlər və proseslərin başvermə qanunlarına görə təsnifatından ibarət model başa düşülür" [11]. Belə konseptual modelin məqsədi predmet sahəsinin terminlərinin və anlayışlarının mənasını düzgün ifadə etmək və müxtəlif anlayışlar arasındakı əlaqələri müəyyən etməkdir. Konseptual model müxtəlif terminlərin mənasını aydınlaşdırmağa, terminlərin və anlayışların müxtəlif cür yozulması ilə bağlı problemləri aradan qaldırmağa yönəlib. Müxtəlif yozumlar maraqlı tərəflər arasında, xüsusilə də, qərarların qəbul edilməsinə və reallaşdırılmasına cavabdeh olan tərəflər arasında səhv anlaşılmalara və münaqişələrə səbəb ola bilər.

Konseptual modelləşdirmə və konseptual model anlayışları verilənlər bazalarının layihələndirilməsi və proqram təminatının işlənilməsi sahəsində daha geniş istifadə edilir. Verilənlər bazalarının layihələndirilməsində konseptual model verilənlər bazasının nəzərdə tutulduğu predmet sahəsini əks etdirir. Proqram təminatı üçün konseptual model yüksək abstraksiya səviyyəsində predmet sahəsinin semantikasını təsvir edir. Proqram təminatında konseptual modellər:

1) subyektlər, münasibətlər və məhdudiyyətlər ilə struktur modellərini təsvir edir;
2) vəziyyətlər və vəziyyətlər arasında keçidlər, vəziyyətlərdə və keçidlərdə yerinə yetirilmiş hərəkətlər ilə davranışı və ya funksional modelləri təsvir edir;
3) göndərilmiş və alınmış məlumatlar və mübadilə edilmiş informasiya ilə qarşılıqlı əlaqələri və istifadəçi interfeyslərini təsvir edir.

Konseptual model kliyentlərə və analitiklərə bir-birlərini başa düşməyə, analitiklər və tətbiqi proqramçılar arasında uğurlu kommunikasiyaya və bəzi hallarda proqram təminatını (hissələrini) avtomatik generasiya etməyə imkan verir.

Konseptual model predmet sahəsi haqqında inteqrasiya edilmiş təsəvvür yaradır, o, zəif formallaşdırılmış verbal xarakter daşıya, yəni baxılan problemlərin və məsələlərin sözlü təsvirini verə bilər. Konseptual modelin təsviri üçün cədvəllər, qrafiklər, diaqramlar və s. istifadə edilə bilər. Verilənlər bazalarının layihələndirilməsində konseptual model obyekt-əlaqə diaqramı (ing. *Entity-Relationship - ER*) və ya *ER*-diaqram şəklində təsvir edilir [12]. Konseptual model müxtəlif notasiyaların köməyi ilə də təsvir oluna bilər, onlardan ən populyarı *UML* dilidir (*Unified Modeling Language* - universal modelləşdirmə dili) [15]. Konseptual model anlayışı ilə son dövrlər geniş yayılmış ontologiya anlayışı sıx əlaqəlidir. Ontologiya predmet sahəsi daxilində konseptlər çoxluğunun və bu konseptlər arasındakı əlaqələrin formal təsvirini nəzərdə tutur.

Elektron dövlət anlayışı

Analiz göstərir ki, hələlik elmi ədəbiyyatda "elektron dövlət" və "informasiya təhlükəsizliyi" anlayışlarının müəyyən edilməsində vahid yanaşma formalaşmayıb.

Qeyd etmək lazımdır ki, rusdilli elmi ədəbiyyatda ingilisdilli *"electronic government"* (*e-government*) anlayışının "elektron hökumət" kimi tərcüməsi geniş yayılıb. Lakin ingilis dilində "*government*" termini ilə yalnız icra hakimiyyəti orqanı kimi hökumət deyil, bütövlükdə dövlət (dövlət idarəçiliyi) nəzərdə tutulur. Məsələn, Avropa Birliyi Komissiyası "*electronic government*" terminini «xidmətlərin və demokratik proseslərin yaxşılaşdırılması və dövlət siyasəti üçün dəstəyin möhkəmləndirilməsi üçün İKT-nin dövlət idarəetməsində təşkilati dəyişikliklər və yeni vərdişlərlə əlaqələndirməklə istifadəsi» kimi müəyyən edir [16].

"Elektron dövlət" texnologiyasının tətbiqi dövlət idarəçiliyinin 1990-cı illərdə islahatlarından başlayır. E-dövlətin məqsədi İKT istifadə edilməklə dövlət sektoru təşkilatlarının işini yaxşılaşdırmaqdır. İslahatların siyasi motivasiyası dövlətə cəmiyyətə xidmət edən və cəmiyyətin özü üçün zəruri səlahiyyətləri icra etməyi tapşırdığı institut kimi baxan konsepsiyanın yaranmasına şərait yaratdı [16]. Beləliklə, "*e-government*" anlayışı "elektron dövlət idarəçiliyi"ni bildirir və İKT-nin yalnız icra orqanlarında deyil, hakimiyyətin qanunvericilik və idarəetmə qollarında da tətbiqini əhatə edir.

Müxtəlif müəlliflər e-dövlət üçün fərqli tərifər təklif edirlər: "şəbəkələrarası dövlət", "onlayn dövlət servisləri, yəni İnternet və ya vebdən istifadə etməklə istənilən şəxsin istənilən dövlət orqanı və ya agentliyi ilə qarşılıqlı əlaqəsi", "biznes tranzaksiyalarını onlayn yerinə yetirməkdən ötrü vətəndaşlar, federal işçilər və digər maraqlı tərəflər üçün xərclər baxımından effektiv modellərin reallaşdırılması" və s [17-19].

ABŞ alimləri S. Palvia və S. Şarma e-dövlətin müxtəlif tərifərini analiz edərək onu mobil dövlət (dövlət xidmətlərinin göstərilməsi üçün simsiz texnologiyalardan istifadə) və

e-idarəçilikdən (idarəetmənin təkmilləşdirilməsi məqsədi ilə dövlət və özəl sektor tərəfindən İKT-nin istifadəsi) fərqləndirirlər [20].

BMT-yə görə, "e-dövlət insanlara informasiyanın və dövlət xidmətlərinin təqdim edilməsi üçün dövlət tərəfindən İKT-nin istifadəsi və tətbiqidir. Bu səbəbdən, e-dövlətin məqsədi vətəndaşlara informasiya xidmətlərinin effektli dövlət idarəetməsi, vətəndaşlara daha yaxşı xidmətlər təqdim edilməsi, informasiyaya çıxış və dövlət siyasətinin qəbulunda iştirak yolu ilə insanlara səlahiyyət verilməsidir" [21].

Dünya Bankının tərifində "e-dövlət dövlət agentlikləri tərəfindən vətəndaşlarla, özəl sektorla və dövlətin digər qolları ilə münasibətləri dəyişdirmək imkanı olan texnologiyaların (məsələn, qlobal şəbəkələr, İnternet və mobil texnologiyalar kimi) istifadəsi" kimi müəyyən edilir [22].

Başqa tərifl ərdə e-dövlət məhsuldarlığı və səmərəliliyi artırmaq üçün vətəndaşlar və kommersiya institutları arasında informasiya, xidmətlər və malların mübadiləsində informasiya texnologiyalarından istifadə edən dövlət modeli kimi müəyyən edilir [23]. Daha geniş mənada e-dövlət layihələri daha yaxşı dövlət strukturunun yaradılmasına çalışır, bu o deməkdir ki, e-dövlət "e" üzərində yox, daha çox "dövlət"də fokuslanır [24]. Oxşar şəkildə "e-dövlət" anlayışı ənənəvi dövlət modelindən daha inkişaf etmiş və daha güclü informasiya texnologiyaları potensialına və əlaqələrə əsaslanan "daha yaxşı dövlət strukturunu" bildirir.

Mançester Universitetinin professoru R. Heeks "e-idarəçilik" terminini təklif edir. Onun fikrincə, bu termin İKT-ni tam əhatə etməlidir, lakin əsas innovasiyalar İntranetdən İnternet-ə kimi kompüter şəbəkələrinə, yeni rəqəmsal birləşmələr yaradan hissəsinə aiddir. R.Heeks fərz edir ki, e-idarəçiliyin fokusu e-idarəçilik hissələrindən e-vətəndaşlar, e-xidmətlər və e-cəmiyyətə doğru dəyişir [25].

"Virtual dövlət" termini Harvard Universitetinin siyasi elmlər üzrə professoru J.E.Fountain tərəfindən informasiya texnologiyalarının hökumətdə institusional dəyişikliklərə - daha konkret, dövlət bürokratiyasına təsirini araşdıran tədqiqatlarının nəticəsi kimi daxil edilmişdir [26]. J.E.Fountain virtual dövləti "... daha çox virtual agentliklər, strukturu və imkanları İnternet və vebdən asılı olan agentliklərarası və dövlət-özəl şəbəkələri kimi təşkil olunmuş hökumət" kimi müəyyən edir. Bu alimə görə, verilənlərin və kommunikasiyaların rəqəmsallaşması dövlətin və onun təşkilatlarının təbiətində fundamental dəyişikliklər edir. E-dövlətin əsas komponentləri e-firma, e-təşkilat və e-vətəndaşdır. Onların hər biri öz "e"-sini reallaşdırmaq üçün öz daxilində çalışırlar, onlar bir-biri ilə qarşılıqlı əlaqədə də işləyirlər və nəticədə, tədricən e-dövlət yaranır [26].

"Elektron hökumət", "elektron dövlət" və "informasiya cəmiyyəti" anlayışları arasında münasibətlərin araşdırılması da maraqlı mövzudur [16]. J.E.Fountain bu nəticəyə gəlir ki, "informasiya cəmiyyəti və dövlət onun geosiyasi aspektində üst-üstə düşür. …İnformasiya cəmiyyəti və elektron dövlət eyni tərtibli anlayışlardır."

XXI əsrin başlanğıcında ictimai proseslərin artmaqda olan riskləri və qeyri-müəyyənliyi şəraitində dövlət idarəçiliyində islahatlar inzibati aparatın işinin optimallaşdırılması və xidmətlərin göstərilməsindən tədricən vətəndaşların dövlət siyasətinin işlənməsinə və həyata keçirilməsinə cəlb edilməsinə, dövlət və vətəndaş cəmiyyətinin daha effektli qarşılıqlı əlaqə sisteminin qurulmasına, dövlətin özəl sektor və qeyri-hökumət təşkilatları ilə əməkdaşlığının təmin edilməsinə yönəlir. E-dövlət ona elektron demokratiyanın qoşulması ilə zənginləşir. E-dövlətin *G2C* (dövlət-vətəndaş), *G2B* (dövlət-biznes) və *G2G* (dövlət-dövlət) kimi ilkin qarşılıqlı əlaqələri ilə yanaşı, *C2C* (vətəndaş-vətəndaş) münasibətləri meydana çıxmağa başlayır.

E-dövlətin informasiya təhlükəsizliyi anlayışı

Anlayışın düzgün, dəqiq və tam müəyyən edilməsinin həm nəzəri, həm də praktiki əhəmiyyəti vardır. "E-dövlətin informasiya təhlükəsizliyi" anlayışının dəqiq və tam açılması infomasiya təhlükəsizliyinin vəziyyətini düzgün qiymətləndirməyə, bu sahədə siyasəti düzgün

qurmağa, təşkilatlanmağa, resursları qiymətləndirməyə və müvafiq potensialı inkişaf etdirməyə, beynəlxalq əməkdaşlığın prioritetlərini müəyyən etməyə imkan verir.

İnformasiya təhlükəsizliyi kifayət qədər mürəkkəb və geniş anlayışdır, onun vahid, birmənalı elmi tərifi yoxdur. "İnfomasiya təhlükəsizliyi" anlayışı ayrı-ayrı müəlliflər tərəfindən müxtəlif cür müəyyən edilir, bu terminlər bir-biri ilə uzlaşmır və metodoloji işin nəzəri əsaslandırılması üçün yararsız olur. İnfomasiya təhlükəsizliyinin nəzəri əsaslarını tədqiq edən Q. V. İvaşşenko (Moskva Dövlət Universiteti, informasiya təhlükəsizliyi kafedrasının dosenti) öz icmalına belə yekun vurur: "Təhlükəsizlik sahəsində müasir nəşrlərin əhəmiyyətli hissəsi predmeti sistemsiz və səthi təsvir edir. Onların müəllifləri tez-tez ideallaşdırmağa, mif yaratmağa meyl edirlər və mövcud olanın izahından arzuolunanın izahına keçirlər" [27].

İnfomasiya təhlükəsizliyinin predmeti çox zaman infromasiyanın konfidensiallığının, tamlığının və əlyetərliliyinin təmin edilməsi kimi başa düşülür. Lakin infomasiya təhlükəsizliyinin predmeti daha genişdir. İnformasiya təhlükəsizliyi təkcə kompüter təhlükəsizliyindən və şəbəkə təhlükəsizliyindən ibarət deyil. Müasir cəmiyyətdə informasiya təhlükəsizliyi cəmiyyətin bütün sosial proseslərinə nüfuz edir, istənilən dövlətin milli təhlükəsizliyinin ayrılmaz tərkib hissəsinə çevrilir [28].

Elmi nəşrlərin icmalı göstərir ki, informasiya təhlükəsizliyi sahəsində işlərin əksəriyyəti iki əsas yanaşma ətrafında qruplaşır. Birinci yanaşmanı texnoloji yanaşma kimi müəyyən etmək olar. Bu yanaşmada dövlətin informasiya sferasında təhlükəsizliyinin təmin edilməsinə yalnız informasiyanın və informasiya (kommunikasiya) sistemlərinin mühafizəsi bucağından baxılır.

İkinci yanaşma dövlətin, cəmiyyətin və şəxsiyyətin maraqlarının informasiyanın zərərli təsirlərindən qorunması zəruriliyindən çıxış edir. Məsələn, bəzi rəsmi sənədlərdə təhlükəsizlik – "şəxsiyyətin, cəmiyyətin və dövlətin həyati vacib maraqlarının daxili və xarici təhdidlərdən mühafizəlilik vəziyyəti" kimi müəyyən edilir [29]. Lakin "təhlükəsizlik" terminə "mühafizəlilik" vasitəsilə tərif verməkqüsurludur, çünki bu sözlər müəyyən mənada sinonimdirlər və buna görə də bu tərifl ər tavtologiyadır [30, 31].

"İnformasiya təhlükəsizliyi" anlayışının "idarəetmə (menecment)" anlayışı ilə əlaqəsinin aydınlaşdırılması "e-dövlətin informasiya təhlükəsizliyi" anlayışının məzmununa daxil olan əsas əlamətlərin aşkarlanmasına imkan verir [32].

İnformasiya təhlükəsizliyi termini həmişə müəyyən şəraitdə (mühitdə) olan konkret idarəetmə obyekti ilə bağlı olur. Təhlükəzilik obyektin müəyyən vəziyyətidir və onu müvafiq keyfiyyət xüsusiyyətlərini göstərməklə müəyyən etmək olar. Təhlükəsizlik haqqında danışarkən obyektin varlığının müəyyən məqsəd funksiyası nəzərdə tutulur və təhlükəsizlik subyektin bu funksiyanı reallaşdırma qabiliyyəti kimi başa düşülür.

Beləliklə, idarəetmə nəzəriyyəsi baxımından e-dövlətin informasiya təhlükəsizliyini e-dövlətin normal fəaliyyətini pozmağa yönəlmiş məqsədyönlü daxili və xarici təsirlər şəraitində e-dövlətin normal rejimdən yolverilən kənarlaşmalar çərçivəsində dayanıqlı idarə edilməsi prosesi kimi müəyyən etmək olar.

Konseptual modelin digər anlayışları

İnformasiya təhlükəsizliyinə sistemli yanaşma onun obyektlərinin, subyektlərinin, prinsiplərinin, vasitələrinin, təhdidlərin və onların mənbələrinin müəyyən edilməsini tələb edir.

E-dövlətin informasiya təhlükəsizliyinin obyektləri insanların şüuru, psixikası, müxtəlif miqyaslı və təyinatlı informasiya sistemləri ola bilər. E-dövlətin informasiya təhlükəsizliyinin obyektlərinə aşağıdakıları aid etmək olar:

- milli informasiya infrastrukturu – ölkənin dövlət və qeyri-dövlət informasiya resurslarının, təşkilati-texniki strukturların, sistem və şəbəkələrin, onların təminat vasitələrinin toplusu;
- kritik informasiya infrastrukturu – sıradan çıxması və ya məhv olması müdafiə, iqtisadiyyat, səhiyyə və milli təhlükəsizlik sahəsində fəlakətli nəticələrə səbəb ola bildiyi

üçün dövlət üçün vacib fiziki və ya virtual sistemlərin və vasitələrin toplusu;
- ictimai şüurun (dünyagörüşü, siyasi baxışlar, mənəvi dəyərlər və s.) kütləvi informasiya və təbliğat vasitələrinə əsaslanan formalaşdırılması sistemi;
- vətəndaşların, hüquqi şəxslərin və dövlətin informasiyanın əldə edilməsi, yayılması və istifadəsi ilə bağlı hüquqlarının, konfidensial informasiyanın və intellektual mülkiyyətin qorunması.

E-dövlətin informasiya təhlükəsizliyinin subyektləri onun təmin edilməsi ilə məşğul olan orqanlar və strukturlar hesab olunur. E-dövlətin informasiya təhlükəsizliyinin subyektləri dövlət, cəmiyyət və vətəndaşlardır.

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi prinsiplərinə aşağıdakılar aiddir: qanuna əsaslanmaq, şəxsiyyətin, cəmiyyətin və dövlətin maraqlarının balanslaşdırılması, komplekslilik, sistemlilik, beynəlxalq təhlükəsizlik sistemləri ilə inteqrasiya, iqtisadi effektivlik və s.

E-dövlətin informasiya təhlükəsizliyinə təhdidlər – informasiya sferasında şəxsiyyətin, cəmiyyətin və dövlətin həyati vacib maraqlarına təhlükə yaradan şərtlərin və faktorların toplusudur.

Tədqiq olunan predmet sahəsinə müxtəlif baxışların icmalı göstərir ki, hazırda e-dövlətin informasiya təhlükəsizliyinə təhdidlərin və onların mənbələrinin kifayət qədər əsaslandırılmış və təfsilatlı ümumi təsnifatı yoxdur.

İnformasiya təhlükəsizliyinin idarə edilməsi funksiyaları

İdarəetmə funksiyaları və hər bir funksiya üzrə işlərin həcminin müəyyən edilməsi idarəetmə sisteminin strukturunun formalaşdırılması və onun komponentlərinin qarşılıqlı təsiri üçün əsas rolunu oynayır. İdarəetmə funksiyası dedikdə, idarə edən sistemdə əməliyyatların əmək bölgüsünə əsaslanan nizamlı toplusu başa düşülür. İdarəetmə funksiyaları bu növ fəaliyyətin müəyyən ehtiyacların ödənilməsinə yönəlmiş əsas istiqamətlərini təşkil edir [33].

İdarəetmə funksiyalarının, onların idarəetmədə əhəmiyyətinin və xüsusi çəkisinin müəyyən edilməsinin bir neçə metodu vardır. Onlardan biri – müvafiq ədəbiyyatın analizi və orada təsvir edilən idarəetmə məsələlərinin seçilməsidir. Belə prosedur həyata keçirildikdən sonra aşkarlanmış məsələlərin siyahısı onları vaciblik dərəcəsinə görə sıralamaq üçün menecerlərə təqdim edilir və bunun əsasında da əsas idarəetmə funksiyaları və onların əhəmiyyəti müəyyən olunur. Seçilmiş funksiyalar toplusu *idarəetmə sisteminin konsepsiyasını* təşkil edir.

Müasir ədəbiyyatda kifayət qədər çox idarəetmə funksiyası müəyyən edilir. İnformasiya təhlükəsizliyi üzrə mövcud ədəbiyyatın analizi əsasında e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin aşağıdakı funksiyalarını fərqləndirmək olar [33-35]:

İdarəetmənin informasiya təminatı – idarəetmə fəaliyyətinin həyata keçirilməsi üçün zəruri olan informasiyanın toplanması, emalı və analizidir.

Proqnozlaşdırma – sistemin gələcəkdə mümkün strukturu, xassələri və ya fəaliyyət qanunları haqqında qeyri-müəyyənliyin aradan qaldırılması vasitəsidir. Proqnoz – sistemin gələcəkdə mümkün vəziyyətləri, nəzərdə tutulmuş vəziyyətin əldə edilməsinin alternativ yolları və müddətləri haqqında elmi əsaslandırılmış fikirlərdir. Proqnozlaşdırma vacib idarəetmə qərarlarının qəbulunda zəruri alətdir, onsuz sosial proseslərin nəticələrini, gələcək vəziyyəti, fəaliyyətin effektivliyini müəyyən etmək mümkün deyil.

Planlaşdırma – e-dövlət maraqlarının və ətraf mühitin analizi nəticəsində məqsədlər sistemi müəyyən edilir, məqsədlər, ətraf mühitin və daxili mühitin vəziyyətləri əsasında alternativ strategiyalar işlənilir və seçilir, strategiyaların reallaşdırılması üçün taktika və prosedurlar işlənilir, onların əsasında operativ planlarla yerlərdə müvafiq işlər həyata keçirilir.

Təşkiletmə – nəzərdə tutulmuş məqsədlərin effektli şəkildə əldə edilməsini təmin etmək üçün sistemin bütün elementləri arasında daimi və müvəqqəti əlaqələrin qurulmasından, onların fəaliyyət nizamının və şərtlərinin müəyyən edilməsindən, sistemin komponentlərinin və

resurslarının birləşdirilməsindən ibarətdir. Təşkiletmə – müəyyən edilmiş prinsiplər və yanaşmalar əsasında idarəetmə sisteminin formalaşdırılması, idarəedən və idarə edilən sistemlərin strukturunun müəyyən edilməsidir.

Koordinasiya – sistemin məqsədlərinə, idarəetməyə uyğun olaraq altsistemlərin hərəkətlərinin razılaşdırılması və bu razılaşmanın idarəetmə tsikli ərzində saxlanmasıdır. Bir neçə idarəetmə obyektinin və altsistemlərin varlığı onların özəl məqsədləri arasında ziddiyyətə gətirib çıxarır. Bu da, öz növbəsində, hərəkətlər arasında əlaqəsizliyə səbəb olur. Bu ziddiyyətlərin aradan qaldırılması – koordinasiyanın əsas məsələsidir. Koordinasiya və təşkiletmə funksiyalarına çox zaman operativ idarəetmə məsələləri çərçivəsində baxırlar. İnformasiya təhlükəsizliyinin dövlət miqyasında təmin edilməsi müxtəlif icra hakimiyyəti orqanları arasında üfiqi və şaquli qarşılıqlı əlaqələrin inkişafını tələb edir.

Nəzarət – idarəetmə obyektinin vəziyyətinin müəyyən edilməsini (idarəetmə obyekti haqqında verilənlərin ölçülməsi, toplanması, dəqiqləşdirilməsi) və verilmiş effektlilik meyarları üzrə cari vəziyyətin tələb ediləndən uzaqlaşma dərəcəsini qiymətləndirməyi təmin edən funksiyalar sistemidir.

İnformasiya təhlükəsizliyinin təmin edilməsi – informasiya və telekommunikasiya sistemlərinin fəaliyyətinin təhlükəsizliyi, terrorizm, ekstremizm ideologiyalarının yayılmasına, zorakılığın təbliğinə əks təsir, konfidensial məlumatların təhlükəsizliyi üzrə tədbirlərin həyata keçirilməsidir.

Təhsil – informasiya təhlükəsizliyi sahəsində zəruri bilik, bacarıq və səriştəyə malik kadrların hazırlanması funksiyasıdır.

Elmi tədqiqatlar – həm mövcud, həm də gələcək sistem və servislərin təhlükəsizliyini təmin etmək üçün fundamental nəzəri tədqiqatların və yeni texnologiyaların prioritet inkişafının təmin edilməsidir.

Mədəni-tərbiyəvi – informasiya təhlükəsizliyi mədəniyyətinin, yüksək mənəviyyatın və vətəndaşlıq mövqeyinin formalaşdırılmasına yönəlmiş funksiyadır.

Ekstremal situasiyalar barəsində əhalinin məlumatlandırılması – böyük miqyaslı insidentlərə hazırlığın yüksəldilməsi, reaksiya vaxtının azaldılması, qəzalardan sonra bərpa planının işlənməsi (məsələn, xüsusi şəraitdə milli fəaliyyət planı, kiberfəzada davranış qaydası, situasiya barəsində məlumatlandırma) nəzərdə tutulur.

Hüquq-mühafizə – kibercinayətkarlıqla mübarizə üçün dövlətin imkanlarının inkişafı və zəruri qanunvericilik bazasının müəyyən edilməsi nəzərdə tutulur.

Tənzimləmə – idarəetmə sisteminin təşkili və fəaliyyəti prosesində idarəetmə obyekti və müxtəlif hüquq subyektləri üçün məcburi tələblərin və prosedurların müəyyən edilməsidir.

Beynəlxalq əməkdaşlıq – qanunvericilik tədbirləri, insidentlərin cavablandırılması, elmi-tədqiqatlar, aparat və proqram təminatının sertifikatlaşdırılması və s. kimi sahələrdə qarşılıqlı faydalı beynəlxalq əməkdaşlığın təmin edilməsidir.

İnformasiya təhlükəsizliyinin idarə edilməsi funksiyaları müəyyən təşkilati, inzibati, iqtisadi və sosial-psixoloji və s. metodların köməyi ilə həyata keçirilir.

Sadalanmış funksiyalar idarəetmə funksiyalarının tam siyahısını əhatə etmir. Onlar bir-biri ilə qismən kəsişə də bilər. Lakin sadalanmış funksiyalar da idarəetmə fəaliyyətinin spesifik növü kimi e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin məzmunu və predmeti haqqında yetərli təsəvvür yaradır.

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi modeli

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin konseptual modelinin işlənməsi zamanı bu modelin əsasına hansı idarəetmə konsepsiyasının qoyulacağı aydın şəkildə müəyyən edilməlidir. İdarəetmə konsepsiyasının müəyyən edilməsi zamanı praktikada yaxşı yoxlanılmış elmi idarəetmə metodologiyalarına əsaslanmaq məqsədəuyğundur.

Təşkilatda olduğu kimi, e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinə də üç müxtəlif səviyyədə baxmaq olar: strateji, taktiki və operativ. Strateji səviyyədə e-dövlətin informasiya təhlükəsizliyinin müxtəlif məsələləri üzrə strateji siyasət müəyyən edilir, taktiki səviyyə təhlükəsizliyin idarə edilməsi üçün istifadə edilən proseslərə və metodologiyalara aiddir, operativ səviyyə informasiya təhlükəsizliyi vəziyyətinin dinamik monitorinqi, informasiya təhlükəsizliyi insidentlərinin qarşısının alınması və aradan qaldırılması üzrə operativ koordinasiya məsələlərini əhatə edir.

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi adaptiv olmalı və proses, sistemli və situasiya idarəetmə yanaşmalarını birləşdirməlidir.

Proses yanaşması idarəetməyə qarşılıqlı əlaqəli idarəetmə funksiyalarının fasiləsiz ardıcıllığı kimi baxır. Sistemli yanaşmada təşkilata dəyişən xarici mühit şəraitində müxtəlif məqsədlərə çatılmasına yönəldilən insanlar, struktur, məsələlər və texnologiyalar kimi qarşılıqlı əlaqəli elementlərin toplusu kimi baxılır. Situasiya yanaşması o fikirdən çıxış edir ki, müxtəlif idarəetmə metodlarının yararlılığı situasiya ilə müəyyən edilir. Situasiya verilmiş konkret zamanda obyektin fəaliyyətinə əhəmiyyətli dərəcədə təsir göstərən hadisələrin (şəraitin) konkret toplusudur. Həm obyektin daxilində, həm də onu əhatə edən mühitdə mövcud faktorların sayı o qədər çoxdur ki, obyektin idarə edilməsinin vahid "ən yaxşı" üsulu yoxdur. Konkret situasiyada ən effektli metod verilmiş situasiyaya daha uyğun olan situasiyadır.

Adaptiv idarəetmə yanaşması o fərziyyəyə əsaslanır ki, idarə edilən obyektin giriş parametrləri çoxluğunu çıxış parametrləri çoxluğuna inikas etdirən ötürmə funksiyasının dəqiq formasını qurmaq olar. Belə idarəetmə metodlarının tətbiq sahələri yaxşı formallaşdırılan, yəni xassələri aşkar olan sadə idarəetmə obyektləridir. E-dövlətin informasiya təhlükəsizliyi isə pis formallaşdırılan idarəetmə obyektləri sinfinə aiddir. Belə sistemlərin xassələri üzrə aprior yaxşı məlum deyil və ya fəaliyyət prosesində dəyişir, bu sistemlər üçün müxtəlif elementlərin qarşılıqlı təsiri, daha mürəkkəb səbəb-nəticə əlaqələri xarakterikdir. Onların xassələrini analitik təsvir etmək cəhdləri riyazi modellərin katastrofik mürəkkəbləşməsinə gətirib çıxarır.

Əgər idarəetmə obyektinin və ya ətraf mühitin məlum parametrləri idarəetmə obyektinin davranışını tam və birqiymətli müəyyən etmək üçün kifayət deyilsə, onda yalnız giriş parametrlərini bilməklə idarəetmə obyektinə idarəetmə təsiri haqqında qərar qəbul etmək olmaz. İdarəetmə obyektin parametrlərinə görə deyil, onun vəziyyətlərinə görə həyata keçirilsə, obyektin davranışını daha yaxşı müəyyən etmək olar.

Sistemin vəziyyəti hər bir zaman anında sistemin malik olduğu əhəmiyyətli xassələrin toplusuna deyilir [36]. Sosial-texniki sistemlərdə çox zaman "zəif bənd" insan olur, buna görə də e-dövlətin informasiya təhlükəsizliyinin vəziyyətini insan faktorunu nəzərə almadan qiymətləndirmək olmaz. E-dövlətin informasiya təhlükəsizliyi vəziyyətinin informasiya təhlükəsizliyini və onun əlaqələrini xarakterizə edən faktorların bütün müxtəlifliyini əhatə edən indikatorlar sistemi əsasında kəmiyyət və keyfiyyət səviyyələrində adekvat qiymətləndirilməsi olduqca çətindir. E-dövlətin informasiya təhlükəsizliyi vəziyyətinin qiymətləndirilməsini vəziyyət sinifləri müəyyən etmək və bu siniflər üzrə aparmaq daha məqsədəuyğundur.

Aprior informasiya əsasında idarəedici təsirlərə idarəetmə obyektinin reaksiyası məlum olan vəziyyət siniflərini formalaşdırmaq mümkün olarsa, onda idarəedici təsirlərə idarəetmə obyektinin bir sinifdən digər sinfə inikası kimi baxmaq olar. Əgər bu mümkün olarsa, onda idarəetmə obyektinin vəziyyətlərini idarəetmə baxımından bir-birinə ekvivalent vəziyyətlərə bölmək və onlara obyektin vəziyyətlər sinfi kimi baxmaq olar.

İnformasiya təhlükəsizliyinin idarə edilməsinin effektivliyinin qiymətləndirilməsi

"İdarəetmənin effektliliyi" anlayışı hələlik elmi ədəbiyyatda aydın müəyyən edilməyib [36]. İdarəetmənin effektliliyini bir-birini tamamlayan müxtəlif meyarlar üzrə qiymətləndirmək olar:

– funksional effektlilik - tədbirlərin keyfiyyətini və nəticəliliyini xarakterizə edir;

- sosial effektlilik - vətəndaşların dövlətin zəmanət verdiyi həcmdə xidmətlə təmin edilməsi səviyyəsini əks etdirir;
- iqtisadi effektlilik - maddi, maliyyə və insan resurslarının rasional istifadə səviyyəsini göstərir.

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsini qiymətləndirmək üçün indikatorlar sistemindən istifadə edilməsi məqsədəuyğundur. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin texnoloji, sosial, iqtisadi, hüquqi və insan faktorlarını xarakterizə edən indikatorlar çoxluğunu müəyyən etmək, indikatorları məqsədlərlə əlaqələndirmək, sərhəd qiymətlərindən istifadə etməklə indikatorları interpretasiya etmək, müqayisə etmək, ranqlaşdırmaq olar.

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin effektliliyi, ilk növbədə, qərarların vaxtında qəbul olunması, məqsədəuyğunluğu, adekvatlığı və qərarların həyata keçirilməsinin nəticələrinə görə qiymətləndirilə bilər. Eyni zamanda, informasiya təhlükəsizliyi insidentlərindən vurulan ziyanın azaldılması, informasiya təhlükəsizliyinə xərclərin optimallaşdırılması, informasiya təhlükəsizliyi mədəniyyətinin yüksəldilməsi, informasiya təhlükəsizliyinin idarə edilməsi yetkinliyinin yüksəlməsi də informasiya təhlükəsizliyinin idarə edilməsi effektivliyinin meyarları kimi istifadə edilə bilər.

Nəticə

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi sisteminin qurulmasının ümummetodoloji tələblərindən və prinsiplərindən biri konseptual yekdillikdir, yəni həm bütövlükdə, bu sistemin özünün, həm də onun tərkib komponentlərinin arxitekturu, texnologiyası, fəaliyyətinin təşkili və təmin edilməsi informasiya təhlükəsizliyinin idarə edilməsinin məqsədlərini və məsələlərini əks etdirən vahid konsepsiyanın əsas müddəalarına uyğun olaraq baxılmalı və həyata keçirilməlidir. Bu baxımdan, e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin vacib modellərindən biri konkret detallara baxmadan e-dövlətin informasiya təhlükəsizliyinin vahid idarəetmə sisteminin strukturlaşdırılmış təsvirindən ibarət olan konseptual modeldir.

Bu işdə predmet sahəsinin və informasiya təhlükəsizliyinin tədqiqi üzrə son elmi nailiyyətlərin analizi əsasında e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin konseptual modeli təklif edilmişdir. Təklif edilmiş konseptual model onun bu və ya digər dövlətdə konkret gerçəkləşdirilməsinə nəzərən invariantdır. Bununla yanaşı, model konkret dövlətin xüsusiyyətlərinə asanlıqla uyğunlaşdırıla bilər.

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin bütün predmet sahəsinin konseptual model şəklində göstərilməsi idarəetmə məsələsinin həllini əhəmiyyətli dərəcədə asanlaşdırır. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin konseptual modelinin qurulması universallaşdırmaya doğru vacib addımdır, çünki sistemin karkasını qurmağa, onun ümumi strukturunu müəyyən etməyə imkan verir, onu sonradan əlavə elementlərlə zənginləşdirmək, təfsilatı ilə işləmək olar.

Ədəbiyyat

1. Wimmer M, von Bredow B. E-government: aspects of security on different layers / Proc. of the 12th International Workshop on Database and Expert Systems Applications, 2001, pp. 350-355.
2. Chen Y.-S., Chong P.P., Zhang B. Cyber security management and e-government // Electronic Government, 2004, vol. 1, no. 3, pp. 316-327.
3. Əliquliyev R.M., İmamverdiyev Y.N. E-dövlətin informasiya təhlükəsizliyi: aktual tədqiqat istiqamətləri // İnformasiya cəmiyyəti problemləri, 2010, № 1, s. 3-13.
4. Embley D. W., Thalheim B. (Eds.) Handbook of Conceptual Modeling, 2011.
5. NATO Science and Technology Organization: RTO-TR-MSG-058 - Conceptual Modeling (CM) for Military Modeling and Simulation (M&S), 2012, 334 p., http://www.cso.nato.int/pubs/rdp.asp?RDP=RTO-TR-MSG-058
6. Robinson S., Brooks R., Kotiadis K., and Van Der Zee D.-J. (Eds.) Conceptual Modeling for Discrete-Event Simulation, 2010.
7. Gemino A., Wand Y. A framework for empirical evaluation of conceptual modeling techniques // Requirements Engineering, 2004, vol. 9, no. 4, pp. 248-260.
8. Welford A.T. On the human demands of automation: Mental work conceptual model, satisfaction and training // Industrial and business psychology, 1961, Vol. 5, 182–193.
9. Большой психологический словарь. Сост. Мещеряков Б., Зинченко В. Олма-пресс, 2004.
10. Фесенко Т.А., Концептуальное моделирование как метод познания ментальной реальности человека. / Сб. статей: Язык, сознание, коммуникация. Ред. Красных В.В., Изотов А.И. М.: Диалог-МГУ, 2000, вып. 12, с.5-8.
11. Аверкин А.Н., Гаазе-Рапопорт М.Г., Поспелов Д.А. Толковый словарь по искусственному интеллекту, М., Радио и связь, 1992, 256 с.
12. Кузнецов С.Д., Основы баз данных, 2-е изд, М., Интернет-Университет Информационных Технологий, 2007, 484 с.
13. ГОСТ Р 43.0.3-2009: Информационное обеспечение техники и операторской деятельности. Ноон-технология в технической деятельности. Общие положения, М., Стандартинформ, 2010, 25 с.
14. Дружилов С.А., Концептуальная модель профессиональной деятельности как психологическая детерминанта профессионализма // Психологические исследования, 2013, т. 6, № 29, с. 4.
15. Буч, Г. UML: Руководство пользователя / Г. Буч, Д. Рамбо, А. Джекобсон. – М.: ДМК Пресс, 2001. – 432 с.
16. Бачило И.Л. Правовая платформа построения электронного государства / Информационное право, 2008, №4, с. 3-9.
17. Tapscott D. The Digital Economy, New York: McGraw Hill, 1996.
18. Luling D. Taking it online: anyway, anyplace, anytime. Tennessee anytime // Journal of Government Financial Management, 2001, vol. 50, no. 2, pp. 42-49.
19. Whitson T.L., and Davis L. Best practices in electronic government: comprehensive electronic information dissemination for science and technology // Government Information Quarterly, 2001, 18(4), pp. 79-91.
20. Palvia S.C.J., Sharma S.S., E-Government and E-Governance: Definitions/Domain Framework and Status around the World / Proc. 5th International. Conference on E-governance (ICEG), 2007, pp.1-12.
21. UN Global E-government Readiness Report. From E-government to E-inclusion, UNPAN/2005/14, United Nations publication, United Nations, 2005.

22. Grönlund Å., and Horan T.A., Introducing E-Gov: History, Definitions, and Issues // Communications of the Association for Information Systems, 2004, vol. 15, pp. 713-729.
23. OECD. The e-government imperative: main findings, Policy Brief, Public Affairs Division, Public Affairs and Communications Directorate, OECD, 2003.
24. Howard M. E-Government across the globe: How will "e" change government? // Government Finance Review, 2001, 17(4), pp. 6-9.
25. Heeks R. Understanding eGovernance for Development // Electronic Journal on Information Technology in Developing Countries (EJISDC), 2001, 11.
26. Fountain J. Building the Virtual State: Information Technology and Institutional Change. Brookings Institution Press, 2001.
27. Иващенко Г.В. Доктрина информационной безопасности и методические проблемы теории безопасности / Материалы круглого стола "Глобальная информатизация и социально-гуманитарные проблемы человека, культуры, общества", МГУ, 2000, с. 48-63.
28. Информационная безопасность систем организационного управления. Теоретические основы: в 2 т. / Н.А. Кузнецов, В.В.Кульба, Е.А.Микрин и др., М., Наука, 2006.
29. Безопасность России. Словарь терминов и определений. М.: МГФ "Знание", 1998, 208 с.
30. Еркин А.В. Понятия "информация" и "информационная безопасность": от индустриального общества к информационному // Информационное общество, 2012, вып. 1, с. 68-74.
31. Стюгин М.А., Информационная безопасность "по существу" / Сб. науч. трудов: Актуальные проблемы безопасности информационных технологий/ Под общей ред. О.Н.Жданова, В.В.Золотарева, Красноярск, СибГАУ, 2007, с. 102-123, http://psyfactor.org/lib/styugin6.htm
32. Райков А.Н. Информационная безопасность и управление // Информационное общество, 1999, № 5, с. 6-9.
33. Черемушкин С.В. Государственное управление: учебник, М., Проспект, 2003, 549 с.
34. Атаманчук Г.В. Теория государственного управления, учебник, издательство: Омега-Л, 2010, 526 с.
35. Репин В.В., Елиферов В.Г. Процессный подход к управлению. Моделирование бизнес-процессов, М., РИА "Стандарты и качество", 2008, 408 с.
36. Друкер П.Ф. Эффективный управляющий, М., Вильямс, 2000, 534 с.

УДК 004.056

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

Концептуальная модель управления информационной безопасностью электронного государства

Управление информационной безопасностью электронного государства представляет собой комплекс трудно формализуемых сложных проблем. Разработка концептуальной модели в качестве первого шага в решении таких проблем является очень полезной. В этой работе создается концептуальная модель управления информационной безопасностью электронного государства. В концептуальной модели определены основные понятия управления информационной безопасностью, цели, объекты, субъекты и основные функции управления информационной безопасностью электронного государства, а также факторы внешней и внутренней среды, влияющие на информационную безопасность электронного государства.

Ключевые слова: *электронное государство, информационная безопасность, концептуальная модель, управление информационной безопасностью.*

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

Conceptual model of e-government information security management

E-government information security management is a complex problem which is difficult to formalize. The development of a conceptual model as a first step in the solution of such problems is very useful. In this paper, the conceptual model of e-government information security management is proposed. The conceptual model determines main concepts of e-government information security, e-government information security management purposes, objects, subjects, key management functions, and external and internal environment factors that affect e-government information security.

Keywords: *e-government, information security, conceptual model, information securitymanagement.*