İnformasiya sistemlərinin təhlükəsizliyinə vurulan ziyanların kompleks qiymətləndirilməsi məsələləri

Ələvsət Əliyev

AMEA İnformasiya Texnologiyaları İnstitutu

alovsat_qaraca@mail.ru

Xülasə— İşdə informasiya sistemlərinin təhlükəsizliyinə vurulan ziyanların kompleks qiymətləndirilməsi zamanı meydana çıxan problemlər təhlil olunmuşdur. İnformasiya təhlükəsizliyinə vurulan nisbi ziyanların təsir səviyyəsinin qeyri-səlis qiymətləndirilməsi metodikasının işlənilməsi aspektləri verilmişdir.

Açar sözlər— informasiya təhlükəsizliyi; informasiya sistemlərinə vurulan ziyanlar; ziyanın növləri; kompleks qiymətləndirmə; ekspert qiymətləndirmələri

I. GİRİŞ

Cəmiyyətin və iqtisadiyatın müxtəlif sahələrində müasir İKT-nin tətbiqi onların potensial imkanlarını olduqca genişləndirməyə və əlavə gəlir əldə etməyə imkan verir. Bununla yanaşı yeni texnoloji-iqtisadi problemlər də meydana gətirir. Belə ki, bir tərəfdən, istifadəçilərin müxtəlif mühafizə vasitələrinə malik informasiya və kompüter sistemlərinin vahid korporativ şəbəkədə birləşməsi adətən ümumi infrastrukturun zəifləməsinə səbəb olur. İnformasiya sisteminin zəif yerləri həm aşkar, həm də gizli xarakter daşıya bilər və onlar həmişə müdafiə oluna bilinmirlər. Digər tərəfdən, ümumi informasiya fəzasının təşkili informasiya resurslarının əlyetərliyini yüksəldir. Bu isə həm xarici, həm də daxili istifadəçilər tərəfindən informasiyaya icazəsiz giriş imkanlarının, eləcə də təhlükələrin artmasına gətirib çıxarır [1]. Bundan əlavə, İKT-nin tətbiqi infrastrukturun özündə də inteqrasiya prosesləri ilə nəticələnir ki, bu da informasiyaların təhlükəli həddə toplanmasına gətirib çıxarır. Bunun nəticəsində isə eyni yerdə o qədər informasiya yığılır ki, bu da təşkilat üçün idarəetmə və biznesin aparılmasının xarakterik texnologiyalarını rəqiblər üçün tamamilə aşkarlaya bilir. Belə informasiyanın itkisi və ya sızması təşkilat üçün ciddi təhlükə yarada bilər. İnformasiyanın təhlükəsizliyinin müxtəlif xarakterli təminat sistemlərinin vahid korporativ şəbəkədə birləşməsi informasiya təhlükəsizliyinin təminatı probleminin həllini olduqca çətinləşdirir. Bu isə informasiya təhlükəsizliyi problemini təşkilati-idarəetmə səviyyəsində daha da mürəkkəbləşdirir.

II. MƏSƏLƏNİN QOYULUŞU

Yuxarıda göstərilən amillər və təhlükə yaradan digər səbəblər nəticə etibarı ilə informasiya sistemlərinin (İS) risklərini və mümkün ziyanlarını dəfələrlə artırır. Vaxtında lazımi tədbirlər görülməzsə bu istənilən təşkilatın dayanıqlı inkişafı üçün ciddi təhlükə yarada bilər. Belə mənfi amil və tendensiyaların qarşısını yalnız həmin risklərin və ziyanların artmasına yol verməyən vaxtında qəbul edilmiş uyğun tədbirlər ala bilər. Belə tədbirlərdən biri olaraq informasiya təhlükəsizliyinin idarəetmə sistemlərinin işlənməsi üzrə risklərin müəyyənləşdirilməsi və qiymətləndirilməsi prosedurlarına əsaslanan ISO 27000 seriyalı standartların meydana çıxmasını hesab etmək olar [2]. Hazırda İS-in ziyanlarının qiymətləndirilməsinin kifayət qədər həm korporativ, həm də ümumi xarakterli metodika və alqoritmləri mövcuddur. Bu metodika və alqoritmlər belə sistemlərin auditi və monitorinqi zamanı bir çox məsələlərin həlli üçün müvəffəqiyyətlə istifadə olunmuşdur. Lakin informasiyanın təhlükəsizliyini idarəetmə sistemlərində təhlükə və ziyanların xarakter müxtəlifliyindən asılı olaraq İS-in risklərinin və ziyanlarının qiymətləndirilməsi metodika və alqoritmlərinə hər il müntəzəm olaraq daha yüksək tələblər irəli sürülür. Ona görə də hər hansı təşkilatın İS-in təhlükə və risklərinin hərtərəfli təhlilinə əsaslanan informasiya təhlükəsizliyinin risk və ziyanlarının kompleks qiymətləndirilməsi üzrə metodika və alqoritmlərin işlənilməsi zamanı meydana çıxan məsələlərin təhlil olunması və iş prosesində onların nəzərə alınması olduqca vacibdir.

III. İNFORMASİYA TƏHLÜKƏSİZLİYİ TƏLƏBLƏRİ

Ümumiyyətlə İS-in təhlükəsizliyi qanunvericilik, inzibati, təşkilati, proqram-texniki səviyyələrdə həyata keçirilir və onun səviyyəsi müvafiq təminat sisteminin qurulmasıyla bağlıdır. Həmin sistemi qurmaq üçün spesifik tələbləri, milli və beynəlxalq tələbləri, praktikada sınanmış tətbiqi nümunələri, standartları, metodologiyaları, məsuliyyət və vəzifə bölgüsünü, ümumi təhlükəsizlik siyasətini, təhlükəsizlik menecmentini, ziyanların mənbələrini, onların hesablanması və risklərin qiymətləndirilməsi üsullarını müəyyənləşdirmək lazımdır [3]. İnformasiya təhlükəsizliyinin əsas metrikası risklərin qiymətləndirilməsi mümkün ziyanların və onların başvermə ehtimallarının müəyyənləşdirilməsidir. Onlar bir çox dəyər göstəriciləri ilə əlaqədardır. Risklərin təhlilinin əsas məqsədi təhlükə mənbələrini qiymətləndirməkdir. Risklərin qiymətləndirilməsində resursların qiymətliliyi, təhlükənin əhəmiyyətliliyi, zəif yerlər, səmərəlilik və s. kimi amillər mütləq nəzərə alınmalıdır.

IV. İS-Ə VURULAN ZİYANLARIN TƏSNİFATI

İnformasiya təhlükəsizliyinin risk və ziyanlarının qiymətləndirilməsi metodikası və alqoritmlərini işləyərkən birinci növbədə digər informasiya təhlükələri ilə bərabər ziyanların təsnifatı üçün əsaslandırılmış seçimlərin aparılması zəruridir. İS-in nisbətən əsas ziyanlarının modelləşdirilməsi və hesablanması üçün təhlükələrin yayılma üsulları əlamətinə görə təsnifatından istifadə etmək olar. İnformasiya

təhlükələrinin yayılma üsullarını ekspert yolla təsvir etmək üçün qeyri-səlis yanaşmadan istifadə etmək olar.

Məlumdur ki, hazırkı dövrdə də İS-in idarə edilməsi və istifadəsi zamanı təhdidlər nəticəsində informasiyanın təhlükəsizliyinə, yəni İS-də informasiya təhlükəsizliyinin pozulmasına səbəb olan ziyanların qiymətləndirilməsi məsələsi kəskin olaraq qalmaqdadır.

İS-in ziyanları informasiyanın məxfiliyinin, tamlığının və əlyetərliyinin pozulması nəzərə alınmaqla, təhlükəsizlik təhdidlər nəticəsində təşkilatın fəaliyyətinə vurulmuş zərərin dəyər baxımından miqdarı kəmiyyəti kimi özünü göstərir. İS-in informasiya təhlükəsizliyinə təhdidlər nəticəsində vurulan əsas ziyan növləri aşagıdakılardır [4]:

1) *İnformasiyanın təhlükəsizliyinin pozulmasıyla bağlı vurulan ziyanlar:*
   - İstifadəçi məlumatının müxtəlifliyinin pozulması səbəbindən vurulan ziyanlar;
   - İstifadəçi məlumatının tamlığının və ya əlyetərliyinin pozulması səbəbindən vurulan ziyanlar;
   - Texnoloji informasiyanın tamlığının və ya əlyetərliyinin pozulması səbəbindən vurulan ziyanlar.
2) *Maliyyə ziyanları və itkiləri:*
   - İstifadəçi verilənlərinin təkrar yaradılmasına, tətbiqi və ya sistem proqram təminatının işlənilməsi, alınması və quraşdırılmasına çəkilən xərclər;
   - İnformasiyanın mühafizəsinə çəkilən xərclər - mühafizə vasitələrinin alışı, quraşdırılması, istismar edilməsi, proqram və aparat vasitələrinin ehtiyatda saxlanılması, mühafizə üzrə təşkilati-texniki tədbirlərin təşkili və keçirilməsi, fərdlərin təlimi və s.;
   - Aparat təminatının bərpasına, təmirinə və ya dəyişdirilməsinə çəkilən xərclər;
   - Sistemin istifadəsinin imkansızlığı və boş dayanması nəticəsində yaranan itkilər;
   - Məxfi informasiyanın təşkilatın zərərinə istifadəsi və ya verilənlərə və ya tətbiqi proqramlara icazəsiz dəyişikliyin edilməsiylə bağlı itkilər;
   - Sazişlərin və ya hüquq normalarının pozulmasına görə cərimələr.
3) *Maddi ziyanlar:*
   - Aparat təminatının və informasiya daşıyıcısının sıradan çıxması;
   - İdarəetmə qurğusunun sıradan çıxması;
   - Digər maddi vəsaitlərin sıradan çıxması və ya məhv olması.
4) *Ekoloji ziyanlar:*
   - Təbiət hadisələrinin və fövqaladə vəziyyətlərin meydana çıxması və inkişafı ilə bağlı ziyanlar.
5) *İqtisadi ziyanlar:*
   - Qurğuların bərpasının, təmirinin əmək məsrəfləri;
   - Tətbiqi və sistem proqram təminatının bərpası və sazlanmasındakı əmək məsrəfləri.
6) *Fərdin sağlamlığına bilavasitə vurulan zərərlər;*
7) *Mənəvi ziyanlar:*
   - Təşkilatın işgüzar imicinin aşağı düşməsi və ya itirməsi ilə bağlı ziyanlar;
   - Üzərinə götürdüyü öhdəliklərin yerinə yetirilməsinin imkansızlığı ilə baglı ziyanlar;
   - Ayrı-ayrı şəxslərin fərdi məlumatlarının yayılması ilə bağlı zıyanlar;
   - Təşkilatın fəaliyyətində intizamsızlıq törətməklə bağlı ziyanlar;
   - Hüquqi normaların pozulmasından irəli gələn ziyanlar;
   - Beynəlxalq saziş və razılaşmaların pozulmasından irəli gələn ziyanlar və s.

V. İNFORMASİYA TƏHLÜKƏSİZLİYİNİN POZULMASI İLƏ BAĞLI VURULAN ZİYANLAR

Bəzən ziyanların qiymətləndiriilməsi yalnız informasiya və proqram təminatına vurulmuş ziyanlarla, başqa sözlə informasiya ziyanlarıyla məhdudlaşdırılır. İnformasiya ziyanları dedikdə informasiya resursunun sistemin bütün məsələlərinin yerinə yetirilməməsinə, təhlükəsizlik funksiyasının pozulmasına, əlverişsiz qərarların qəbuluna, fəaliyyət prosesinin pozulmasına və s. səbəb olan halların yaranmasına və ya son məqsədin əldə edilməsinə çəkilən xərclərin yüksəldilməsinə, eləcə də böyük maddi itkilərə səbəb olan neqativ proseslər başa düşülür. Bu cür ziyanların qiymətləndirilməsi onların aradan qaldırılmasının xüsusi itki funksiyasının və ziyanlar üzrə yekun göstəricilərin daxil edilməsinə əsaslana bilər. İnformasiya ziyanları informasiyanın təhlükəsizliyinin pozulması ilə bağlı olub, aşağıdakı şəkildə özünü büruzə verir [5]:

- Giriş subyektlərinin və obyektlərinin icazəsiz müdaxilə və qarşılıqlı təsir hallarında informasiyanın məxfiliyinin pozulması, dəyərinin itməsi;
- İnformasiya resursunun bərbad hala salınması, dağıdılması, onun tam və ya hissə-hissə itməsi, bazaların müxtəlif cədvəllərinin pozulması;
- İnformasiya resursunun əlyetərsizliyi və ya müəyyən vaxt ərzində əlyetərli olmaması;
- Verilənlərin yığılması, mübadiləsi, tədarükü və ötürülməsi zamanı informasiya resursunun təhrif olunması;

proqram təminatında qərəzli və qərəzsiz xətaların, nəzərdə tutulmayan imkanların aşkarlanması.

İnformasiya ziyanlarının qiymətləndirilməsinin ümumiləşdirilmiş kriteriyaları aşağıdakılar ola bilər:

- Milli təhlükəsizliyə vurulan ziyanlar;
- qanunvericiliyin tələblərinin pozulmasıyla bağlı vurulan ziyanlar;
- İnformasiyanın dəyərinin itməsi nəticəsində maliyyə xərclərinə səbəb olan ziyanlar;
- Təşkilatın imicinə vurulan ziyanlar;
- Beynəlxaiq informasiya mübadiləsinə vurulan ziyanlar;
- İnformasiya resurslarının bərpası ilə bağlı maliyyə itkilərinə səbəb olan ziyanlar;
- Təşkilatın fəaliyyətində qüsurların törədilməsiylə bağlı vurulan ziyanlar;
- Fərdi məlumatların yayılmasıyla bağlı vurulan ziyanlar.

İnformasiya təhlükəsizliyinin qiymətləndirilməsi üçün zərərlərin müəyyən yekun səviyyəsinə uyğun olaraq beş ballıq reytinq şkalasından istifadə etmək olar: çox yüksək - 5 bal, yüksək - 4 bal, orta - 3 bal, aşağı - 2 bal, olduqca aşağı- 1bal.

İnformasiya təhlükəsizliyinin pozulmasının reytinq şkalasının qiymətinin təyini hər hansı konkret təşkilatın informasiya təhlükəsizliyinin pozulması faktlarının təhlili zamanı toplanmış ilkin verilənlər əsasında ekspert yolu ilə aşağıdakı yekun göstəricilərə görə həyata keçirilir:

- Pozulmuş, təhrif olunmuş və məhv edilmiş informasiyanın həcmi;
- Pozulmuş, təhrif olunmuş və məhv edilmiş ümumi və xüsusi proqram təminatının həcmi;
- Sıradan çıxarılmış verilənlər bazası serverlərinin miqdarı;
- Sıradan çıxarılmış əlaqə kanallarının və kommuilkasiya qurğularının miqdarı;
- İnternet şəbəkədən ümumi istifadənin konkret informasiya resurslarına neqativ təsirlərin miqdarı;
- Sistemin və şəbəkənin bərpasına sərf olunan vaxt.

Hazırda sistemə vurulan informasiya ziyanlarının qiymətləndirilməsinin ümumiləşdirilmiş kriteriyası üçün xüsusi reytinq şkalası işlənilməkdədir. Məsələn, müəyyən vaxt intervalıda sistemin xidməti informasiyalarına əlyetərliyin qeyri-mümkün olması nəticəsində təşkilatda fəaliyyətin pozulması ilə vurulan ziyanlar belə bir xüsusi şkala şəklində qurula bilər: (5,4,3,2,1) - xidməti informasiyaya müvafiq surətdə bir gündən çox, 8 saatdan bir günədək, 3 saatdan 8 saatadək, 1saatdan 3 saatadək, 1saatdan az müddət ərzində girişin olmaması;

Ümumiyyətlə, ziyanların göstəricilərinin təyini zamanı sistemin bəzi funksiyalarının pozulması və bu pozğunluqların dərəcəsinin xarakterizə edilməsiylə informasiya ziyanları əmsalının da təyin edilməsinin mühm rolu vardır. Bunlar isə təşkilatda informasiya təhlükəsizliyi sisteminə yarana bilən ziyanlarla qarşılıqlı əlaqədə olmaqla informasiya resurslarının dəyərini müəyyən etməyə imkan verir.

VI. ZİYANLARIN QİYMƏTLƏNDİRİLMƏSİNƏ BƏZİ YANAŞMALAR

İS-ə vurulan ziyanların kəmiyyətcə qiymətləndirilməsi üçün bir çox keyfiyyət və kəmiyyət şkalaları vardır. Məsələn, emprik əməliyyatlar və riyazi anlayışlara əsaslanan sistemdə ad, sıra, interval, nisbət və s. kimi adlanan şkalalar nəzərdən keçirilir.

Ziyanların kəmiyyət qiymətləndirilməsi üçün ən azı iki əks, yəni şkalada zərərlərin qiymətlərinin ifrat əks nəticələrini (məsələn, heç bir ziyanın olmaması və qəbuledilməz dərəcədə ziyan) müəyyən edən qütb nöqtələrinin qurulmasına əsaslanan əks qütblər şkalası daha münasib hesab olunur. Belə şkalalarda nöqtələr şəklində kəmiyyət, interval, verbal qiymətləndirmənin bir neçə növünə baxılır. Bununla bərabər metrik və ya sıra şkalalarından da istifadə edilə bilər. Ancaq belə şkalaların istifadəsi müxtəlif təhdidlərin nəticəsində yaranan ziyanların kompleks qiymətləndirilməsinə imkan vermir [6].

Ziyanın dərəcəsinin təhlükələrdən və İS-in fəaliyyət parametrlərindən analitik asılılığı olmadıqda, belə uygunluq qeyri-səlis çoxluqlar mexanizmi əsasında qurula bilər. Ekspert vasitəsilə ziyanların qurulmuş şkalasında bölgülərlə ifadə olunmuş təhlükələr və mümkün ziyanlar arasındakı uyğunluq qurulur. Ziyanın dərəcəsi haqqında ekspert biliklərinin qeyri-müəyyənliyini hesablamaq üçün ziyanın qeyri-səlis üçbucaq ədədi və mənsubiyyət funksiyası şəklində təqdim olunan ölçüsündən istifadə edilə bilər. Bu zaman ekspertlərin fərdi fikir müxtəlifliyi ənənəvi yolla konkordasiya (razılaşdırma, uyğunlaşdırma) əmsalının hesablanması əsasında qiymətləndirilə bilər.

Müxtəlif növ ziyanların qiymətləndirilməsini ümumi şkalaya gətirmək üçün ziyanların bütun kəmiyyətlərini maksimum mümkün ziyanlar əsasında normallaşdırılması zəruridir. Bu halda bu cür ziyanın qiymətləndirilməsinin onun maksimum dəyərinə nisbəti alınır. Bu nisbəti təhlükə nəticəsində yaranan zərərin indeksi adlandırmaq olar.

Qeyd etmək lazımdır ki, İKT-nin müasir inkişaf mərhələsində müxtəlif tətbiqi məsələlərin həlli üçün daha çox qeyri-səlis çoxluqlar nəzəriyyəsindən istifadə edirlər. Bu tendensiya informasiya təhlükəsizliyi sahəsində problemlərin həlli üçün qeyri-səlis model və sistemlərin yaradılmasına təsir göstərmişdir. Hər şeydən əvvəl bu onunla bağlıdır ki, tədqiq olunan obyektdə baş verən proseslər yüksək dərəcədə qeyri-müəyyənlik, təsadüfilik, qeyri-sabitlik, müxtəlif təsirlər və s. ilə xarakterizə olunurlar. Göstərilən faktorlar klassik nəzəriyyələrə və modellərə əsaslanan dəqiq modellərin qurulmasına son dərəcə çətinliklər törədirlər.

VII. ZİYANLARIN QEYRİ-SƏLİS QİYMƏTLƏNDİRİLMƏSİ

Məlum olduğu kimi qeyri-səlis çoxluqlar nəzəriyyəsinin əsas anlayışı mənsybiyyət funksiyasıdır. Ona görə də elementlərin çoxluğa aid olması dərəcəsinin təyini və mənsubiyyət funksiyasının qurulması, onların hansı sahəyə aid olmasından asılı olmayaraq praktiki realizasiyanın əsas məsələsi hesab olunur.

İS-in informasiya təhlükəsizliyinə vurulan ziyanların qiymətləndirilməsi məsələlərinin həllində, eləcə də göstərilən sahədə qeyri-müəyyən şəraitlərdə idarəetmə qərarlarının qəbulu proseslərinin modelləşdirilməsində mənsubiyyət funksiyasının formalaşdırılmasının müxtəlif üsullarından istifadə etmək olar [7]. Bu zaman göstərilən məsələnin səmərəli həlli üçün mənsubiyyət funksiyasının formalaşdırılmasının lazımi üsulunun düzgün seçilməsi də zəruridir. Bütün bu amillər İS-in ziyanlarının inteqral qiymətləndirilməsinin qəbul edilmiş metodikasının vaxtında seçilməsinin və işlənilməsinin zəruriliyini göstərir. İS-in ziyanlarının dərəcəsinin qeyri-səlis çoxluğunun qurulmasıyla əlaqədar olan belə metodikalarda bir qayda olaraq ekspertlərin informasiya təhlükəsizliyi sahəsindəki mülahizələrindən istifadə olunur. Bununla əlaqədar ekspertlər informasiya sisteminə müəyyən təhlükələrin təsir səviyyəsinin başlanğıc qeyri-səlis çoxluqlarını yaradırlar. Bunlar isə təhlükələrin bütün sinif və dərəcələrinin ümumi yekun təsirlərinin qeyri-səlis çoxluğunda ümumiləşdirilir. İS-in ziyanlarının qiymətləndirilməsi bütün növ təhlükələrin yekun ümumi təsirinin bütün ekspertlər üzrə ümumiləşdirilmiş mənsubiyyət funksiyasının nəticəsi kimi alınır.

Qeyd etmək lazımdır ki, ziyanların hesablanmasıyla bağlı olan metodikaların təşkilata vurulan ziyanlarının səviyyəsi daha çox aşağıdakı şkalalar şəklində təqdim olunur [4].

1. *Kiçik ziyan.* Maddi aktivlərin cüzi itkisinə səbəb olir, tez bərpa olunur və ya təşkilatın imicinə cüzi təsir edir.
2. *Orta ziyan.* Maddi aktivlərin aşkar və gözə çarpan itkisinə səbəb olur və təşkilatın imicinə orta səviyyədə təsir edir.
3. *Orta ağırlıqlı ziyan.* Maddi resursların əhəmiyyətli dərəcədə itkisinə və təşkilatın imicinin əhəmiyyətli dərəcədə zəifləməsinə səbəb olur.
4. *Böyük ziyan.* Maddi resursların böyük itkisinə səbəb olur və təşkilatın imicinə böyük zərbə vurur.
5. *Çox ağır və qorxulu ziyan.* Maddi resursların çox böyük və ağır itkisinə səbəb olur. Bazarda təşkilatın imic və etibarının tamamilə itməsinə səbəb olur ki, bu da onun gələcək fəaliyyətini tamamilə imkansız edir.

Burada bu və ya digər təhlükənin yaranma xüsusiyyətindən, tezliyindən, dərəcəsindən, şəraitindən asılı olaraq İS-in ziyanlarının səviyyəsinin qiymətləndirilməsi qeyri-səlis çoxluq şəklində olur.

İS-in ziyanlarının səviyyəsinin başlanğıc qeyri-səlis çoxluqlarının mənsubiyyət funksiyasının qurulması zamanı ekspertlər qrupuna qeyd olunmuş təhlükə növlərinin meydana çıxma tezlikləri və xüsusiyyətləri ilə təşkilata vurulan uyğun ziyanların səviyyəsi arasındakı asılılığın qiymətləndirilməsi təklif olunur. Bu asılılıq adətən xətti, eksponensial, loqarifmik, çoxhədli kimi əsas trendlərdən birinin analitik funksiyası kimi özünü göstərir [6]. Həm də nəzərə almaq lazımdır ki, xətti trend artan, eksponensial və loqarifmik trend qeyri-xətti monoton artan, çoxhədli trend isə dövri artan və azalandır. Ekspertlər üçün daha dəqiqi, hər bir təhlükə üçün İS-in ziyanlarının səviyyəsinin tipik mənsubiyyət funksiyasının seçilməsi zəruridir. Hər bir ekspert öz qiymətləndirməsinin nəticələrini sorğu kitabçasına daxil edir. Onun tamamilə doldurulması hər bir konkret təhlükənin nəticəsində İS-ə vurulan ziyanların səviyyəsinin qeyri-səlis funksiyasını formalaşdırmağa imkan verir. Bütün növ təhlükələr nəticəsində İS-ə vurulan ziyanların səviyyəsinin ümumiləşdirilmiş qeyri-səlis çoxluğunu almaq üçün əldə olunmuş ilkin qeyri-səlis çoxluqları cəbri üsullarla cəmləmək lazımdır. İS-in ziyanlarının yekun qeyri-səlis çoxluğu əvvəlcədən ümumiləşdirilmiş bütün qeyri-səlis çoxluqların nəticəsi kimi özünü təqdim edir. İS-in ziyanlarının bütün ekspertlər tərəfindən alınmış yekun qeyri-səlis çoxluqlarının emalının nəticəsi inteqral qiymətləndirmədir .

NƏTİCƏ

Beləliklə, qeyd etmək olar ki, İS-ə vurulan ziyanlarının inteqral qiymətləndirilməsinin izah olunan metodikası başlanğıc qeyri-səlis çoxluqların mənsubiyyət funksiyasının qurulmasının ekspert yanaşmasına əsaslanmışdır. Bu zaman bütün növ təhlükələr nəticəsində İS-ə vurulan ziyanların ümumiləşdirilmiş qeyri-səlis çoxluğunu yaratmaq üçün başlanğıc qeyri-səlis çoxluqların cəbri cəmlənməsindən istifadə olunur.

Yekunda xatırlatmaq istərdik ki, İKT-in elmi-texniki əsasları inkişaf etdikcə, onun tətbiq dairəsi genişləndikcə İS-ə yarana biləcək təhlükələrin də xarakteri və miqyası dəyişir. Bu isə avtomatik olaraq İS-ə və müvafiq təşkilata vurula biləcək ziyanların da forma və məzmununu dəyişir. Ona görə də həmin ziyanların hesablanması üzrə zəruri metod və vasitələrin mütamadi yenilənməsinə, yenidən işlənməsinə və daha yenilərinin yaradılmasına da daimi ehtiyac qalmaqdadır.

ƏDƏBİYYAT

[1] Васильев Ю.С., Зегжда П.Д., Маховенко Е.Б. Информационная безопасность. Санкт-Петербург, 2012 .

[2] Дубинин Е.А. Оценка относительного ущерба безопасности информационной системы предприятия на основе модифицированного метода сложения функций принадлежности. Автореферат диссертации. Ставрополь, 2012.

[3] Варфоломеев А.А.Основы информационной безопасности. - Москва, 2008.

[4] Язов Ю.К., Григорьева Т.В. К вопросу о построении единой количественной шкалы оценок разнородных ущербов от реализации угроз безопасности информации в компьютерных системах. Информация и безопасность, 2008, №1.

[5] Климов С.М. Методика оценки возможного ущерба от нарушения безопасности информации автоматизированной системы. Известия ЮФУ. Технические Науки. №4, 2003.

[6] Дубинин Е.А., Копытов В.В., Тебуева Ф.Б. Обработка результатов экспертной оценки ущерба информационной системе для вывода интегральной функции принадлежности. Инфокоммуникационные технологии. № 1, 2012.

[7] Росенко А.П., Аветисов Р.С. Методика оценки величины ущерба от воздействия на автоматизированную информационную систему внутренних угроз. Известия СГУ. №8, 2006.